Hard Disk Heart Attack

Felix Bauer

IT-Sicherheitsmensch

felix-tuebix@ai4me.de

11.06.2016

Disclaimer

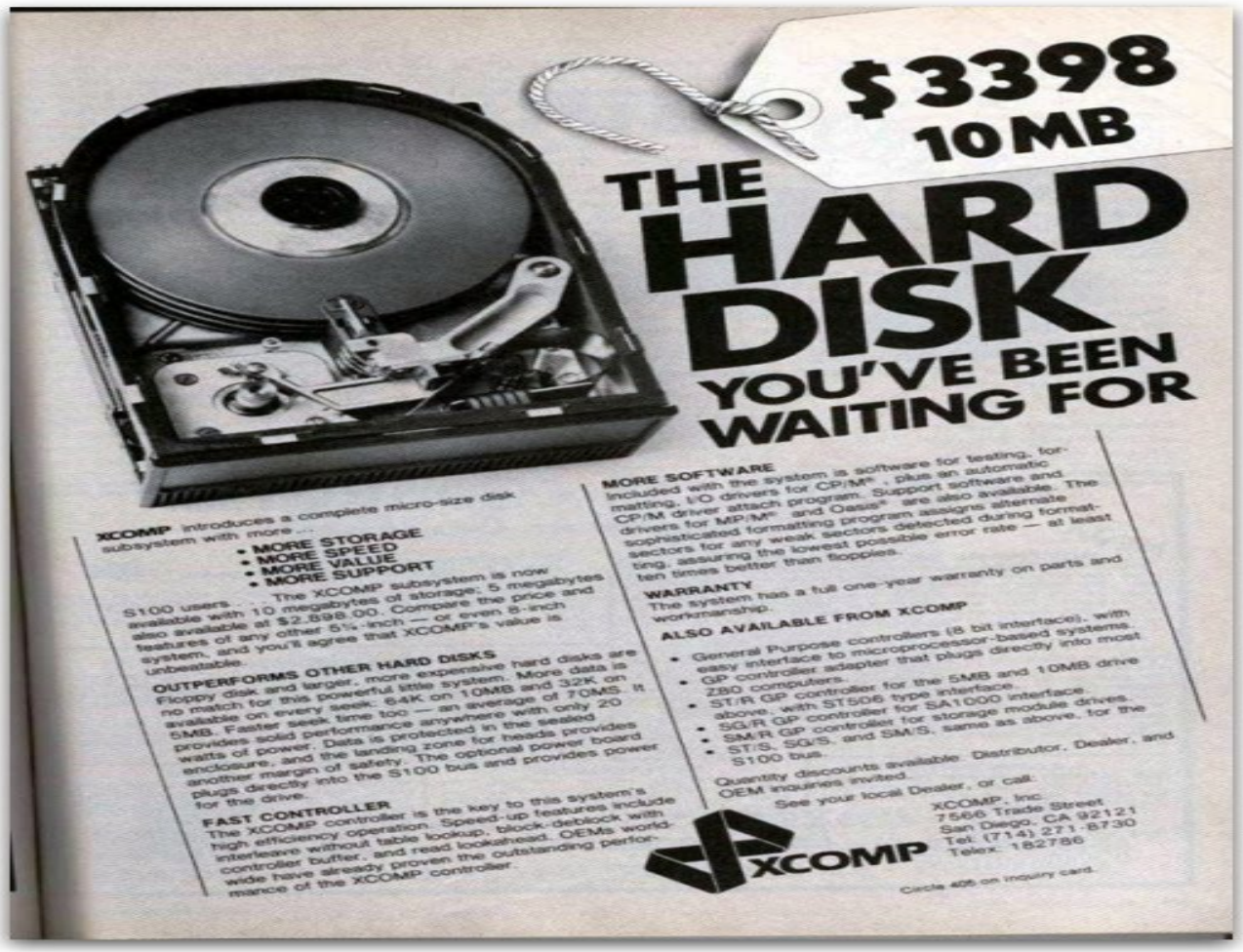
Das folgende Material enthält Szenen brutaler Gewalt gegenüber Festplatten

Inhalt

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

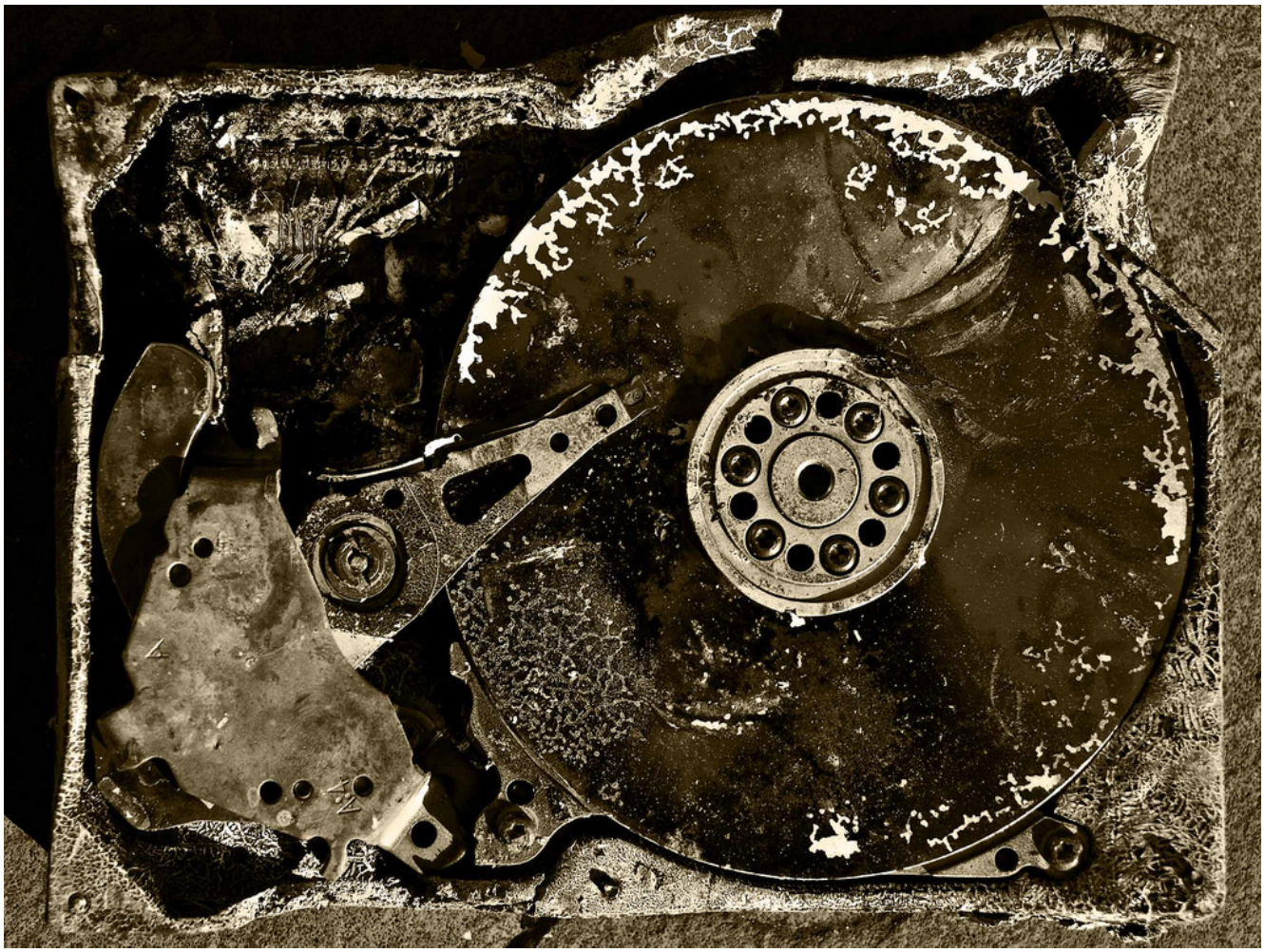
Hard Disks

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



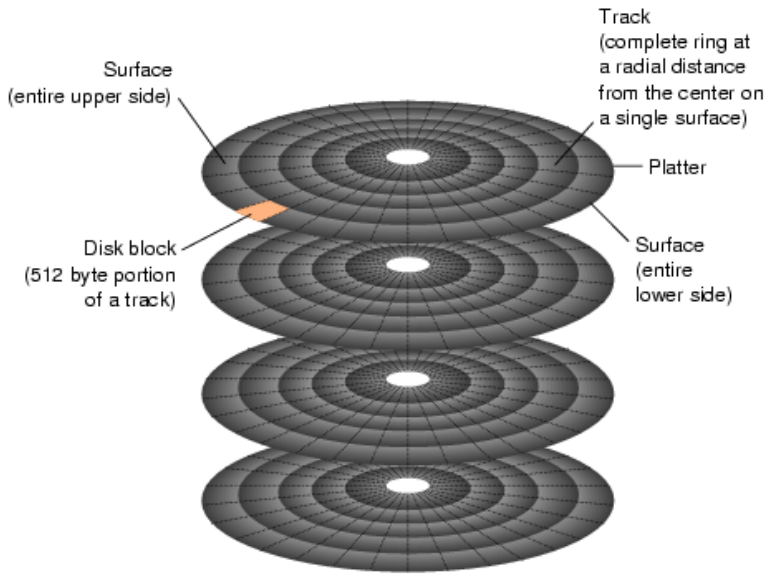
www.coolpicturegallery.net


Maxtor
SERIAL ATA
Made in Singapore



davidrvetter @ flickr.com

Ein Block Device



techpubs.sgi.com

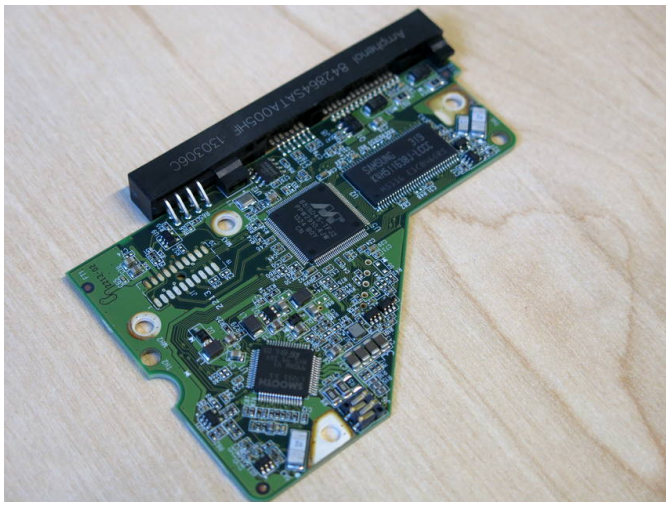
Aber es braucht mehr

- Partitionen
- Dateisysteme
- ...

www.opensourceforu.com

Aber Moment !

Da ist mindestens ein Prozessor, Speicher und ziemlich viel Plattenspeicher



Also ist es eher sowas?

Vielleicht nicht ganz

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

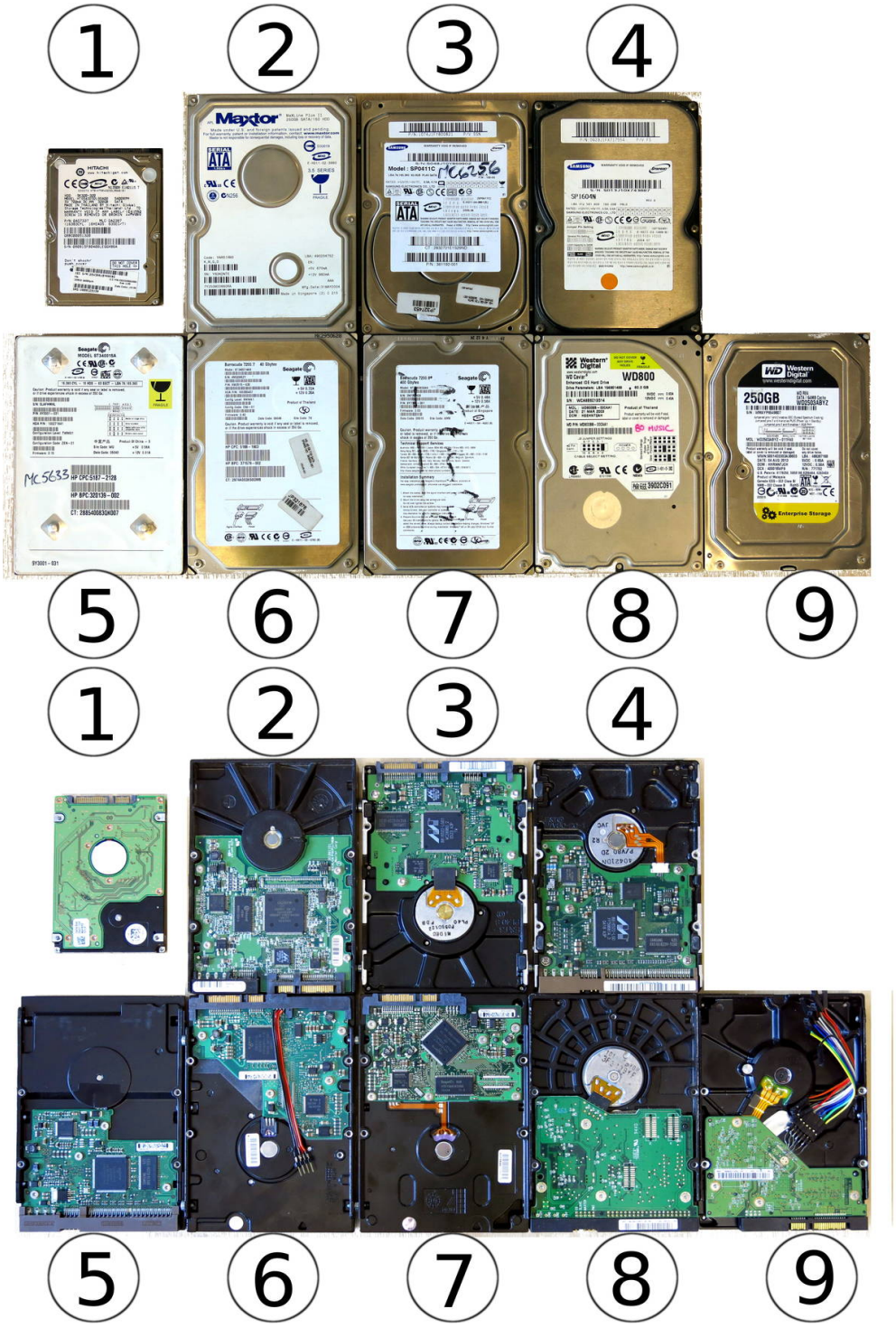
Man findet da:

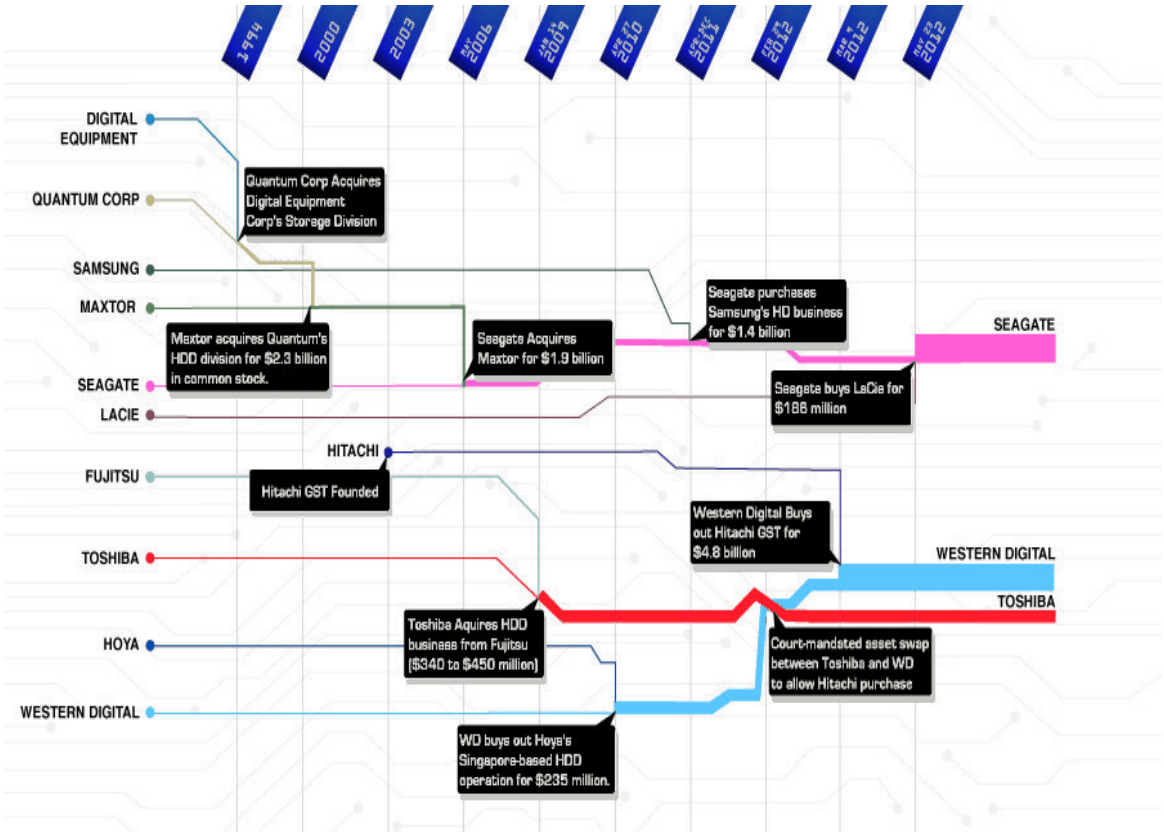
- +/- 400 MHz controller (multicore)
- 64 MB RAM
- 256 KB ROM
- 1.5 bis 6 Gbit SATA interface

Außerdem kennt man:

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

Mal schauen was man damit anstellen können!

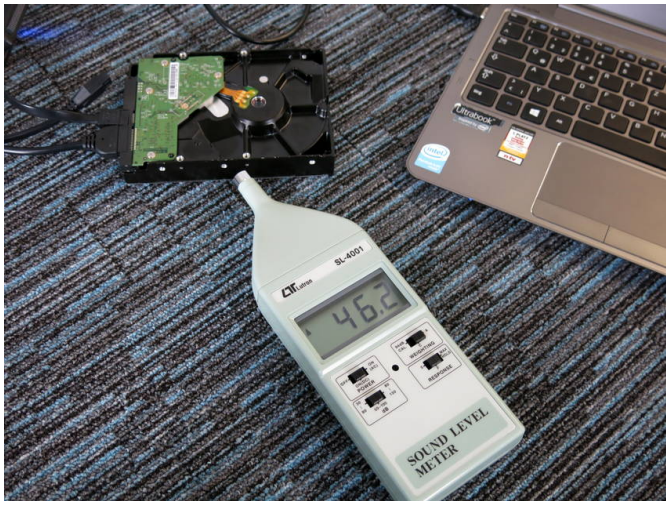

1
2
3
4
Maxtor
WD800
250GB
5
6
7
8
9
1
2
3
4
5
6
7
8
9



Seitenkanäle

- Geräusche
- Wärme
- Energieverbrauch
- Elektromagnetische Abstrahlung

Geräusch



Wärme

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

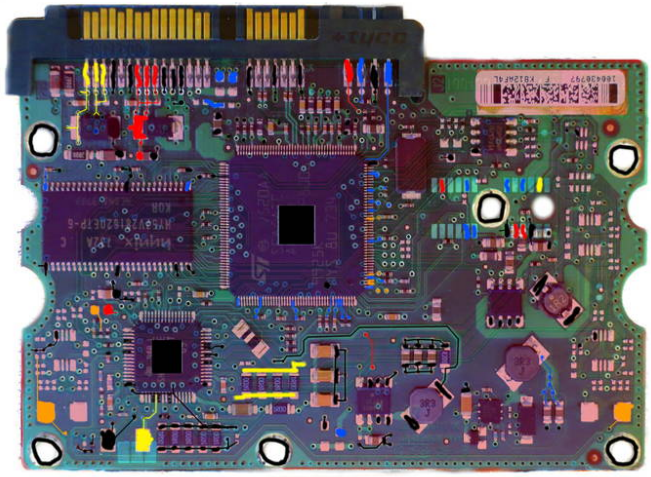
Energieverbrauch

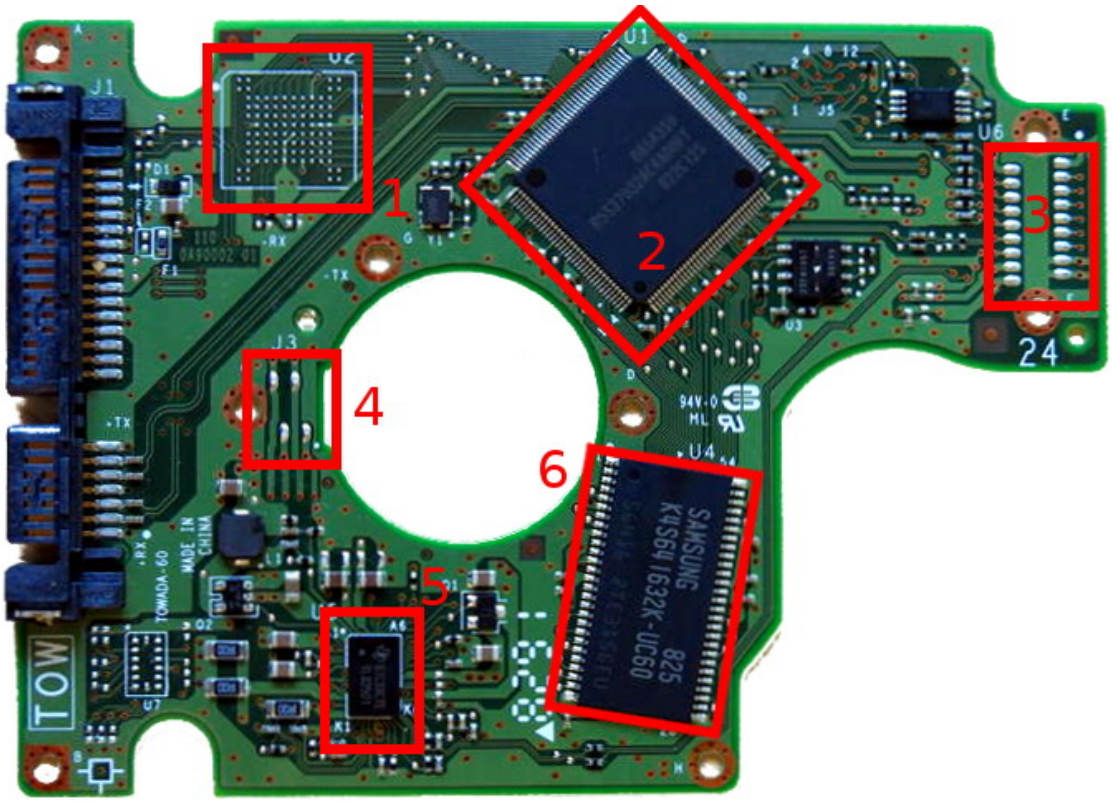
NIEMALS eine laufende Festplatte schütteln!

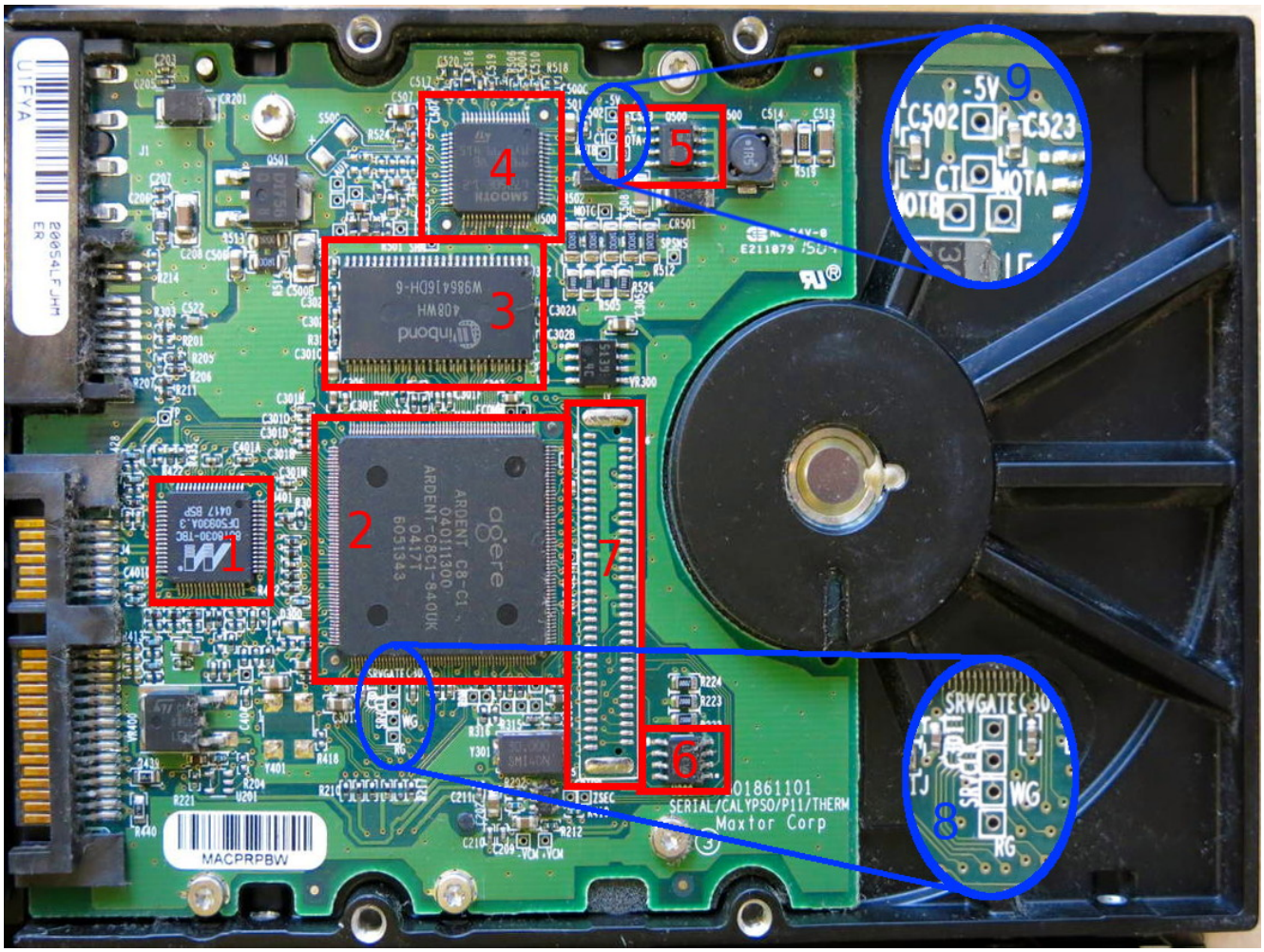
aber wenn mans tut verbraucht sie mehr Strom

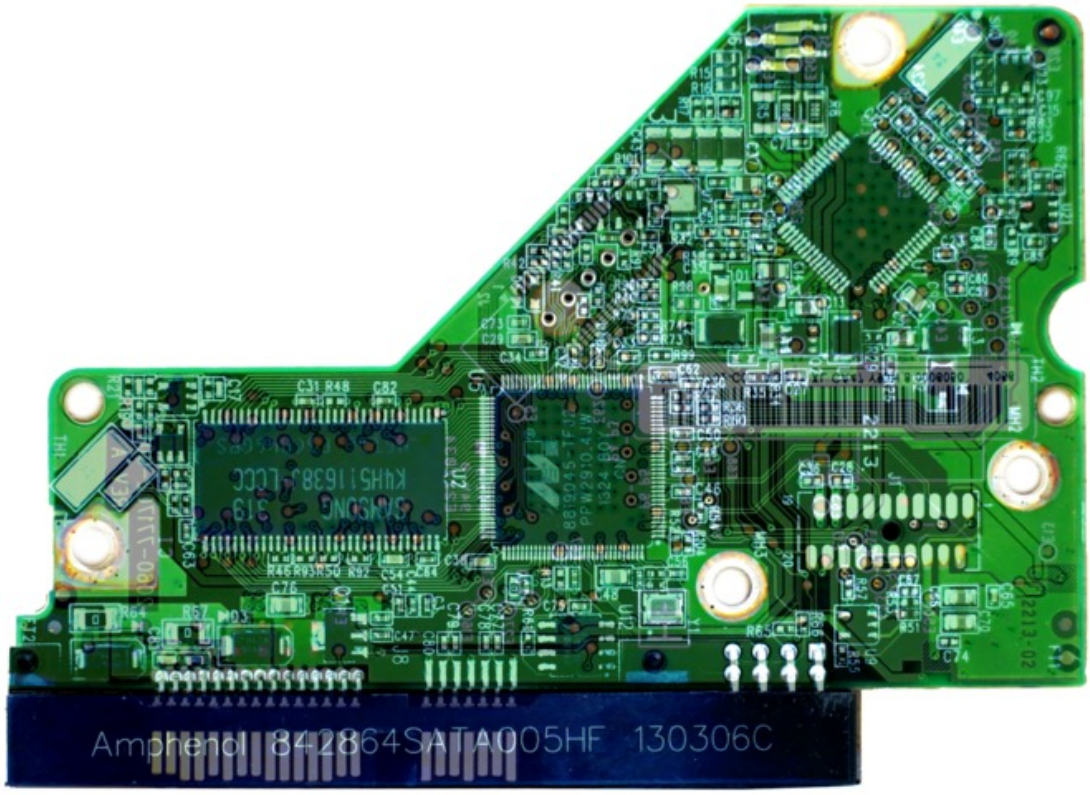
Elektromagnetische Abstrahlung

Schauen wir uns die Elektronik an

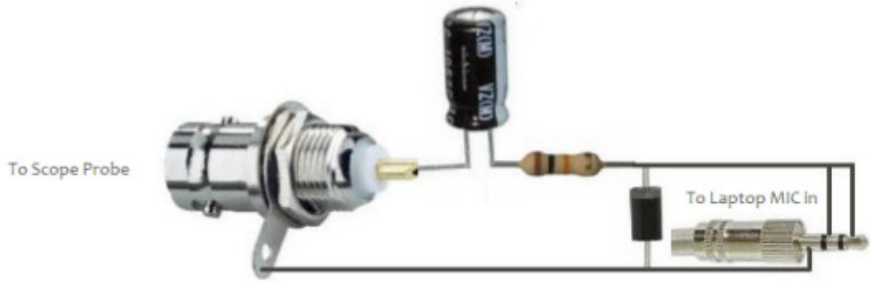



1
2
3
4
5
6
SAMSUNG
K9S6416328-UC60
TOW

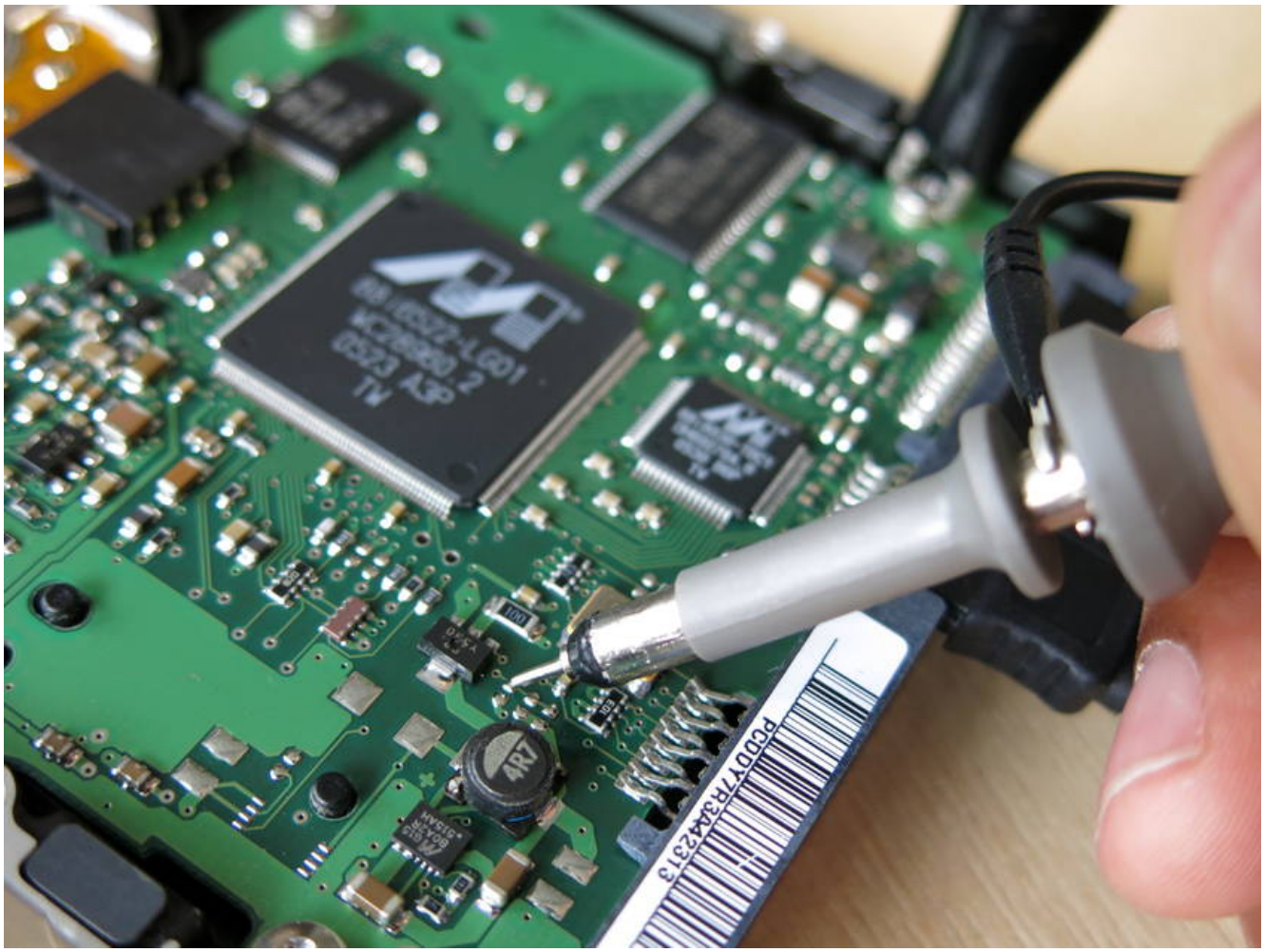

1
2
3
4
5
6
7
8
9
-5V
C502
C523
CT
MOTA
MOTB
SRVGATE
WG
RG
MACPRPBW
SERIAL/CALYPSO/P11/THERM
Maxtor Corp

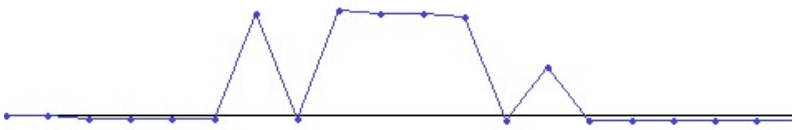


Ein Oszilloskop muss her



by Paul Marsh

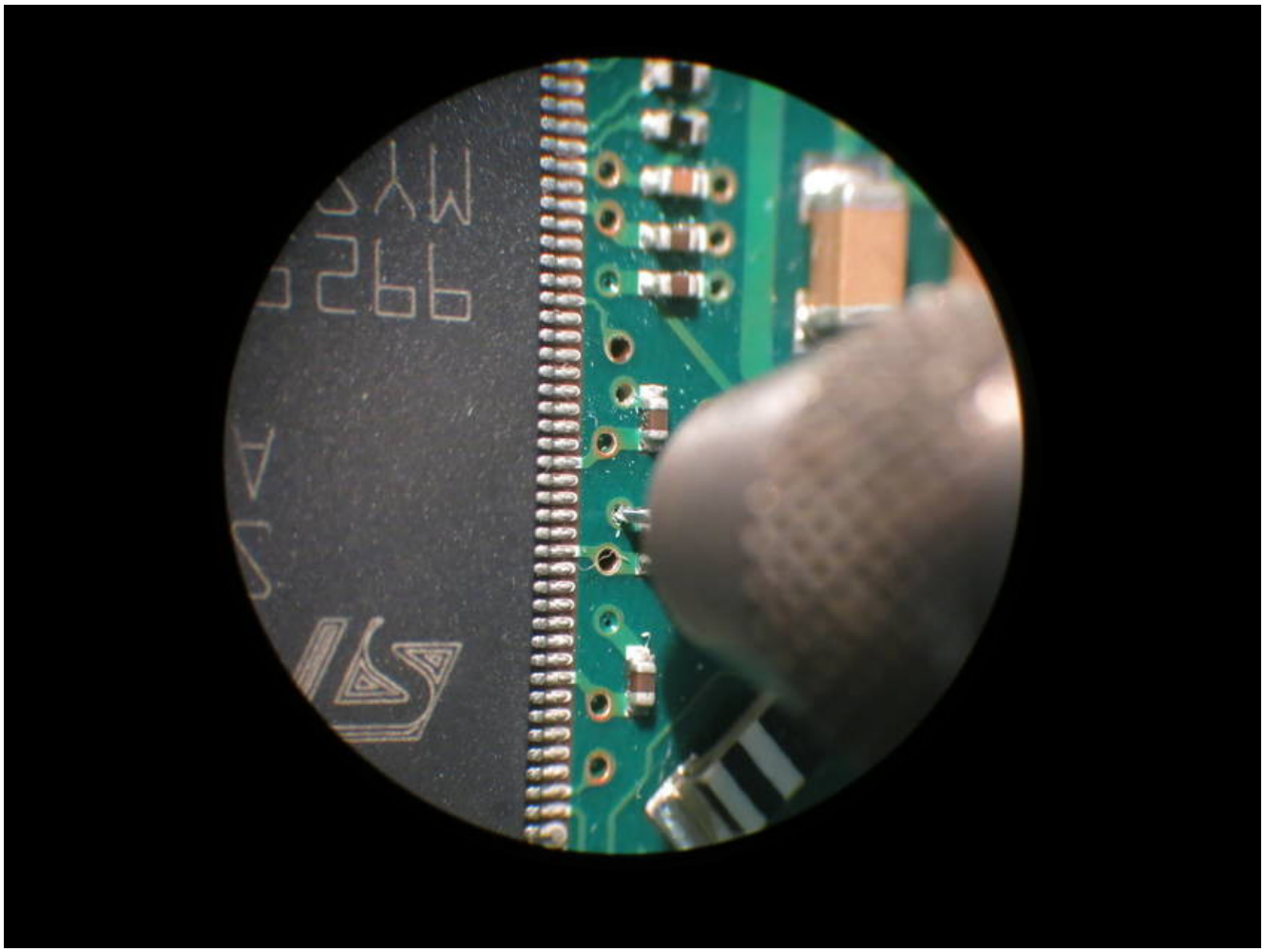




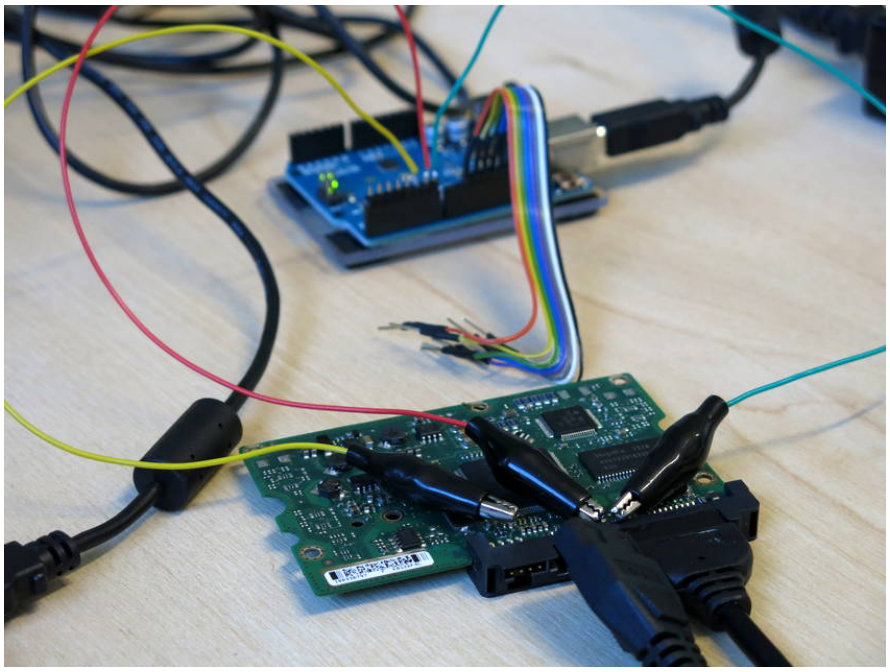
```
0 0 0 0 0 0 0 1 0 1 1 1 1 0 1 0 0 0 0 0
- - - - - - - S 0 1 1 1 1 0 1 S - - - -

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

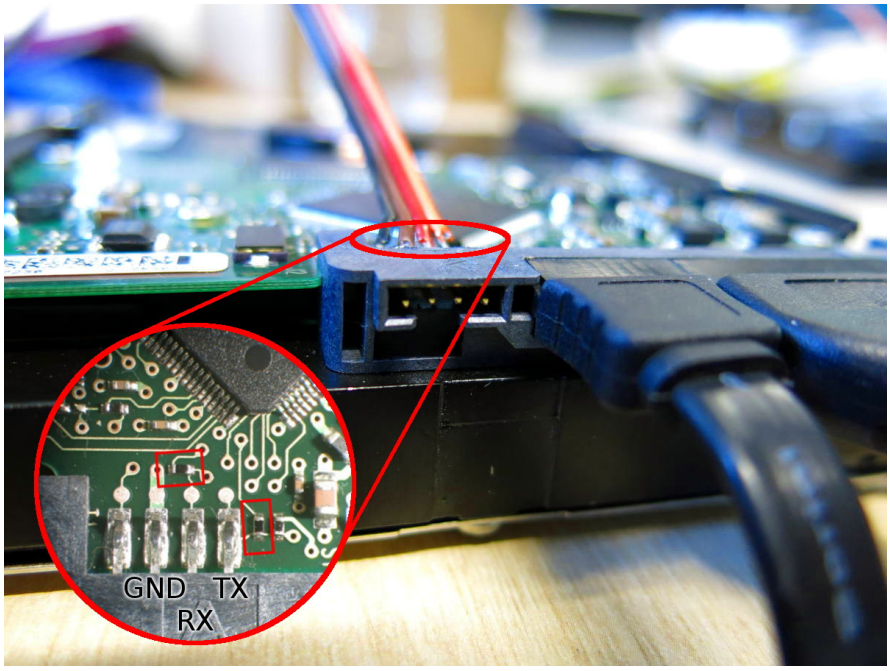
Und jetzt mehr und parallel



Arduino und RS232enum



YAY



Terminal Mode

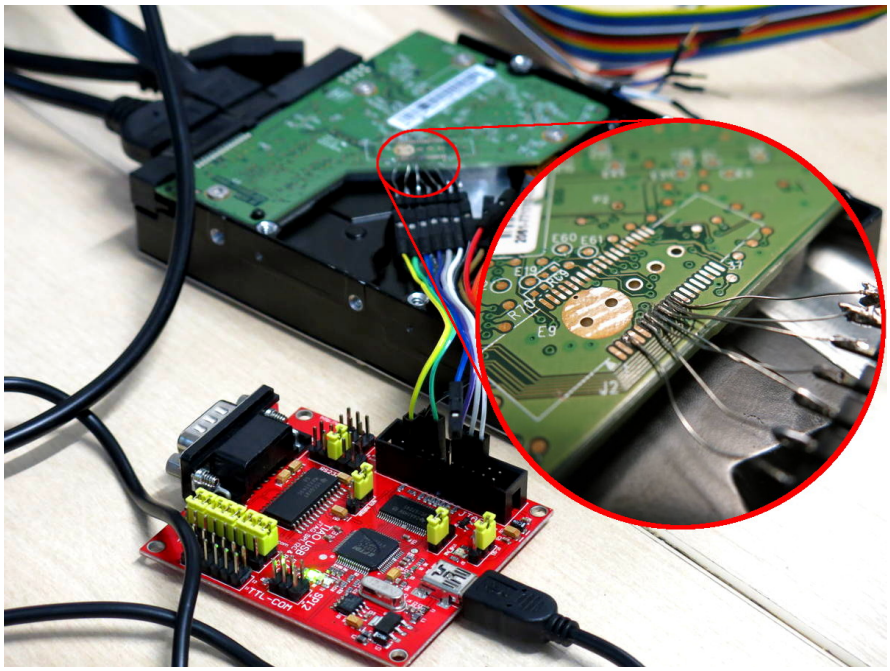
```
# boot up message
Interface task reset
```

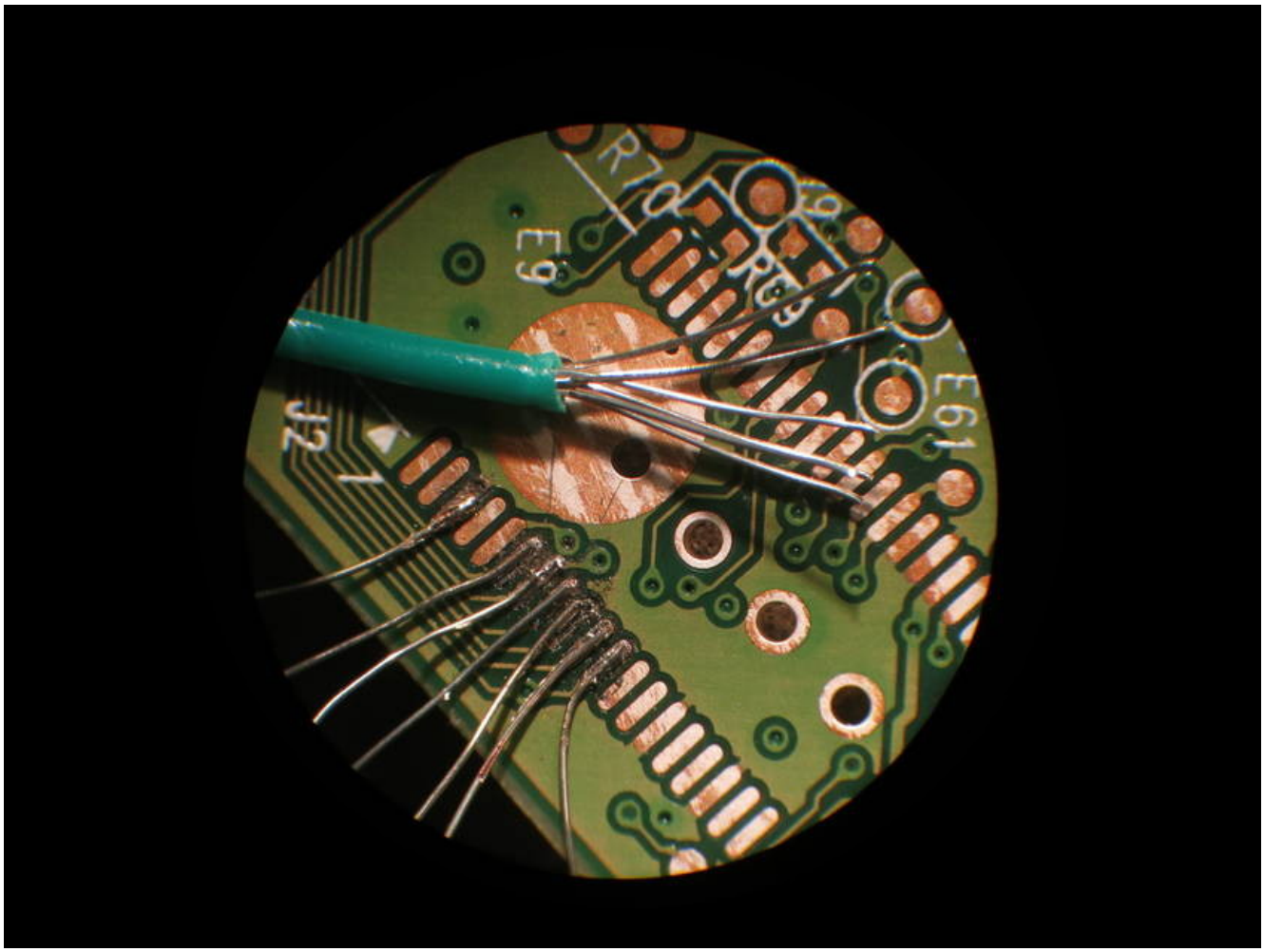
```
4096k x 16 buffer detected
TONKA - 1 Disk M-27 03-30-05 11:42


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?

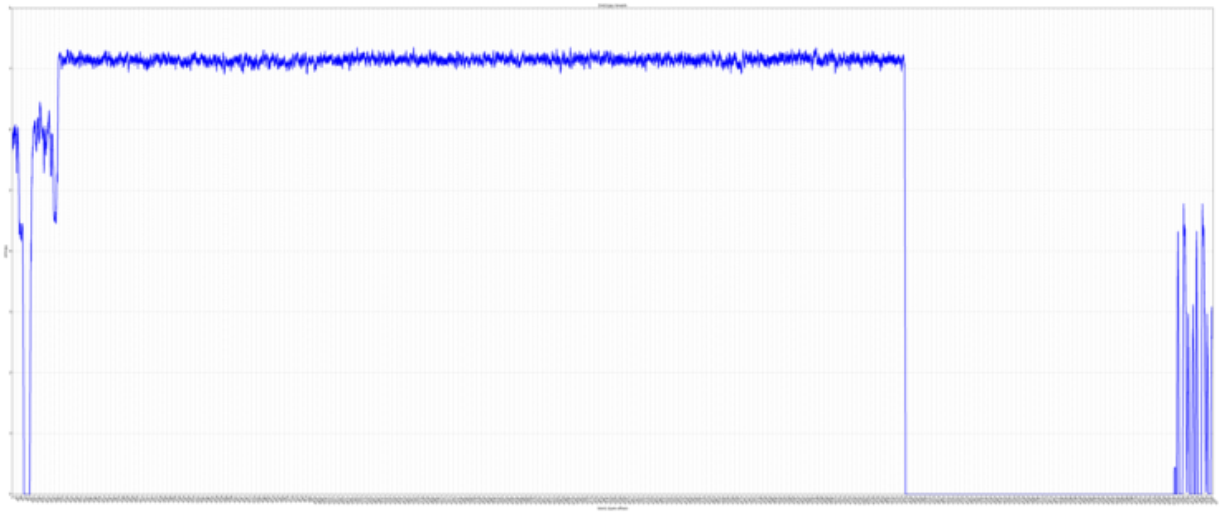




Was kommt als Nächstes?

- openOCD
- debugging
- firmware dump

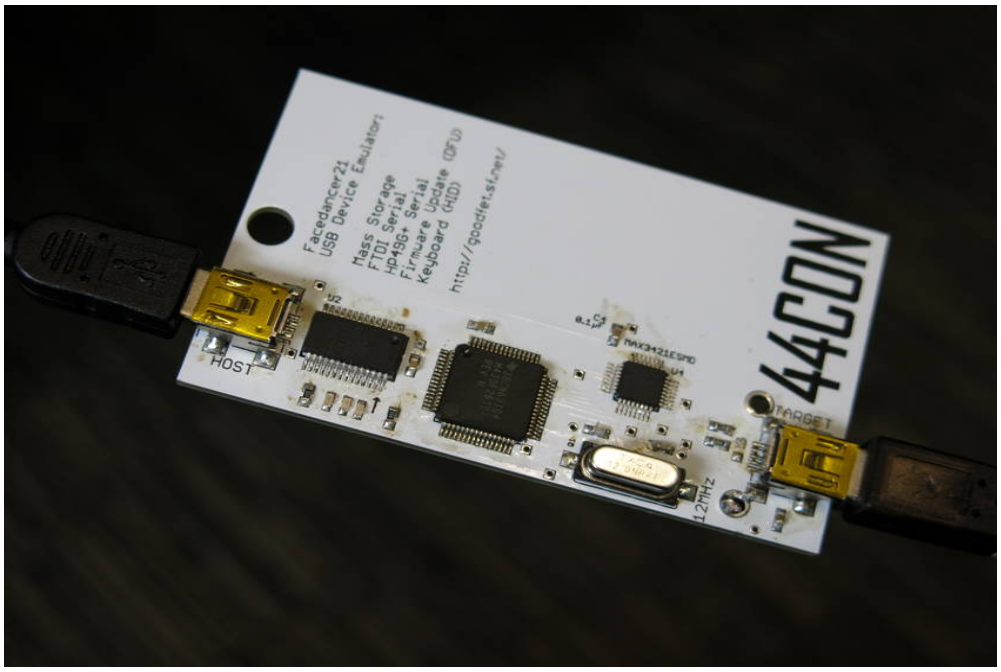
Die Firmware



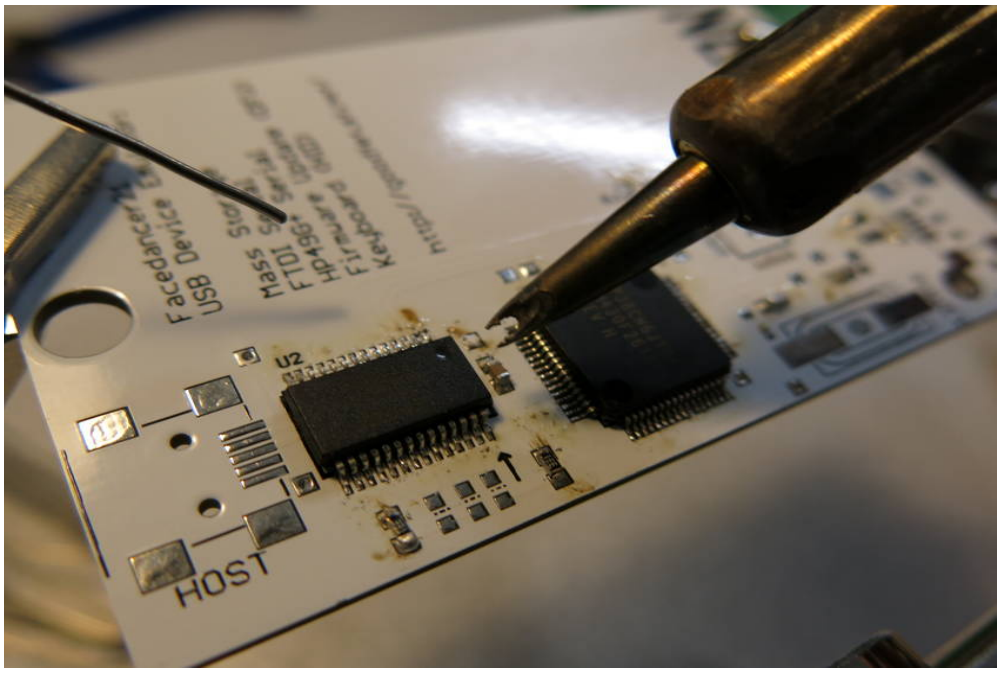
Und jetzt mehr böse Dinge

Sachen verstecken

POC mit facedancer



Sauron's Lötkolben



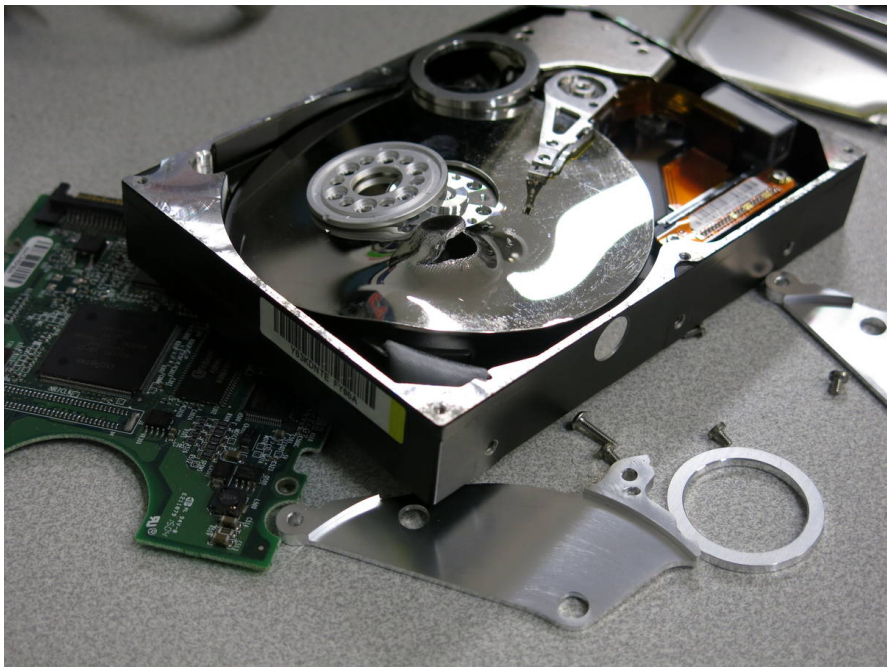
Was geht mit dem Facedancer?

- funktioniert
- schön und funkelnd
- 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

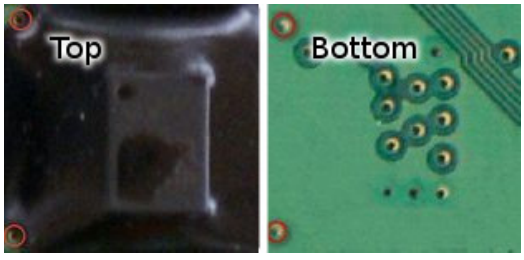
DEMO



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