

Hack Everything

or:

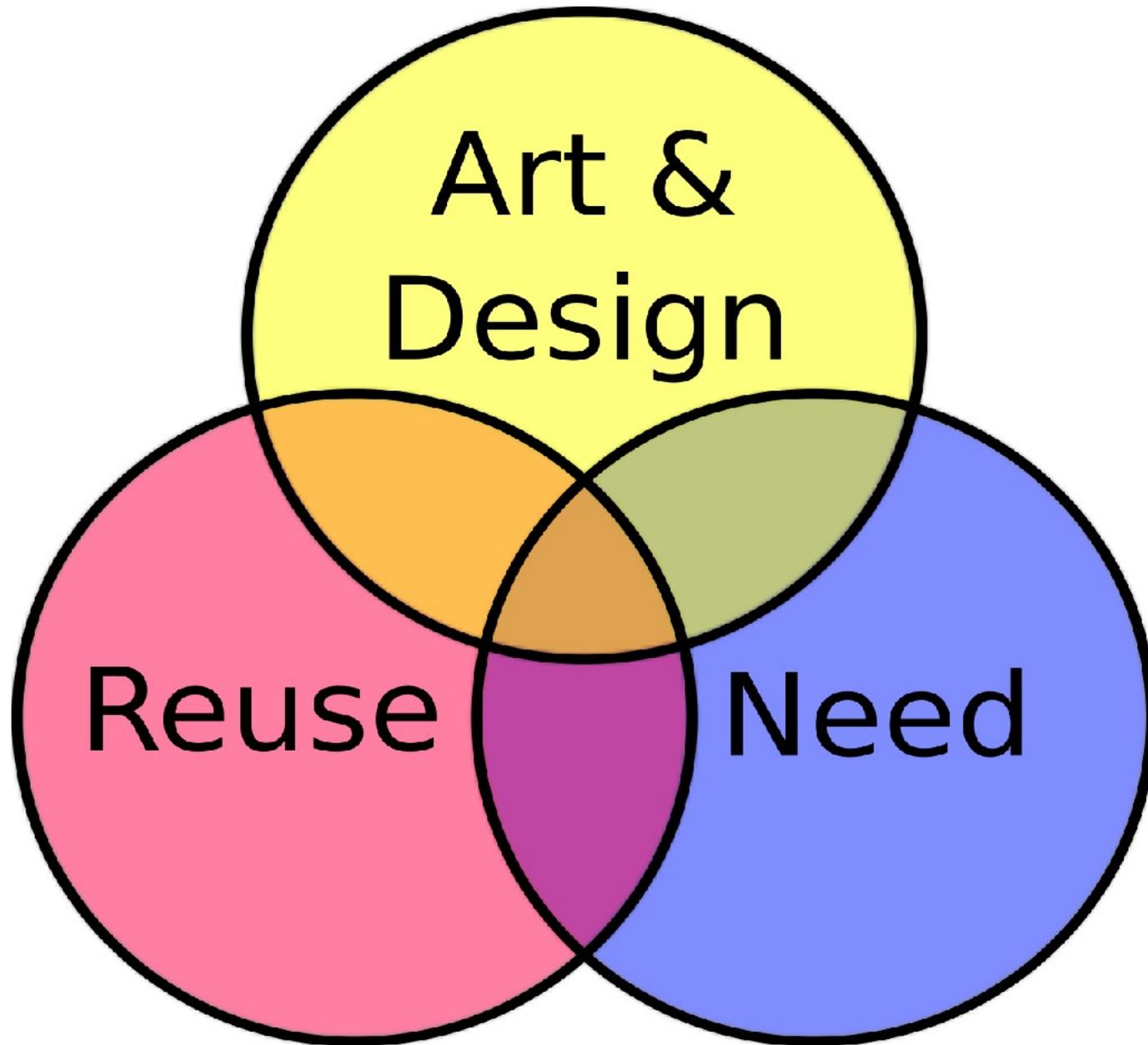
Pull apart electronic stuff and invent
new things with the insides

Matt Evans, IBM OzLabs

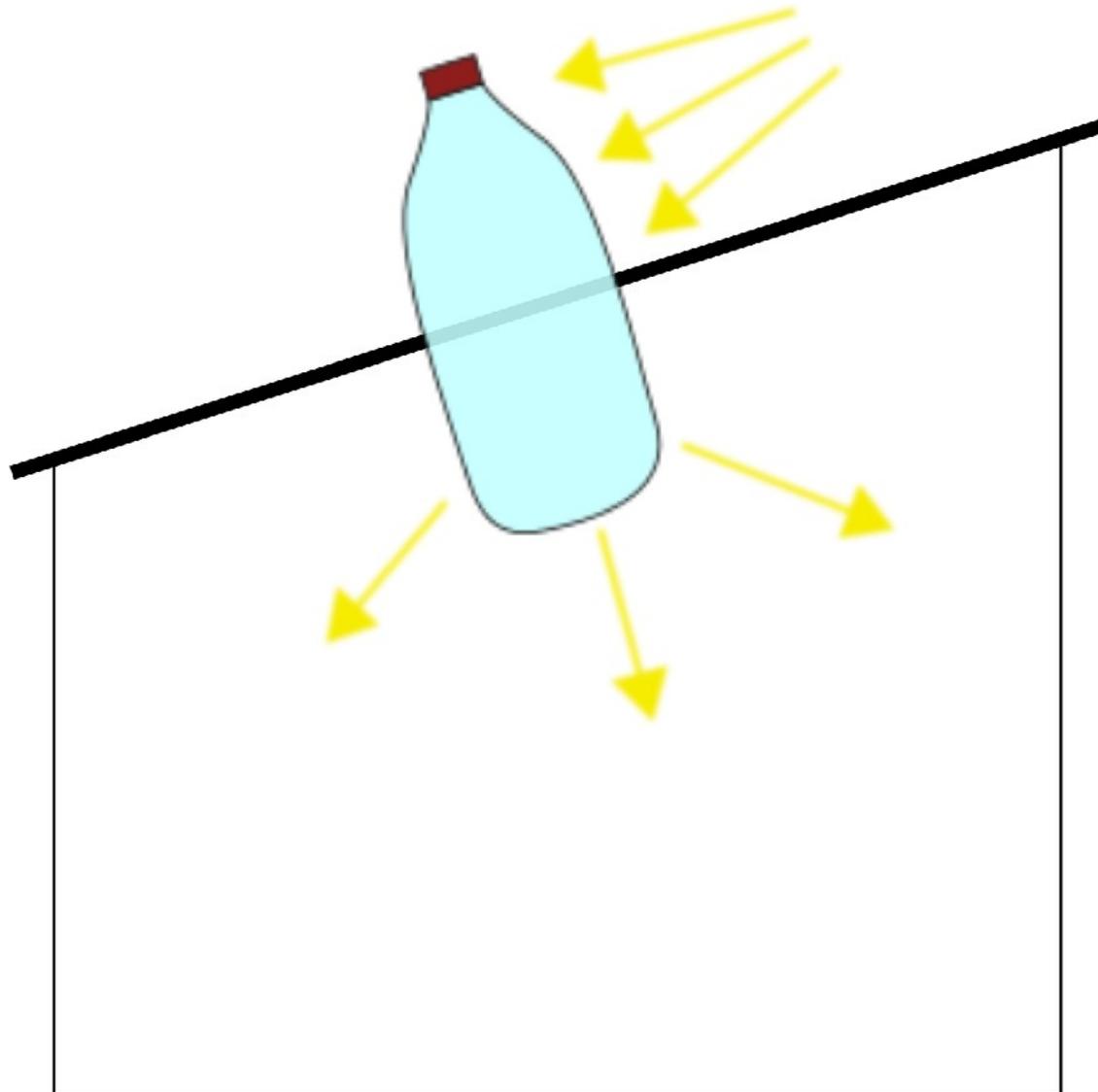
Re-using electronic devices

1. Philosophy
2. Technical stuff

Philosophy of re-use/hacking



Litron Liwanag (Litre of Light)



Gambiarra:

The Brazilian art of the improvised fix, kludge or creation.

- With an emphasis on an artful nature!



A white rectangular control panel with a black rotary knob in the center. The knob has ten positions labeled with numbers 0 through 9. The numbers are arranged in two columns: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. The knob is currently set to position 4. Below the knob, the text "WILD HEERBRUGG SWITZERLAND" is printed.

WILD
HEERBRUGG
SWITZERLAND



FY/O/198

ALDIS
SLIDE PROJECTOR
SERIAL NO. 100000000
MFG. NO. 100000000



A yellow rubber duck is perched on top of a black, cylindrical speaker. A black microphone is attached to the side of the speaker. The entire setup is on a plain white background.

Fear me!

MEGADUCK



Save resources:

Re-use > Recycling > Landfill

Save money:

What's the coolest thing you can
build for \$0?

Take things apart, learn by
example

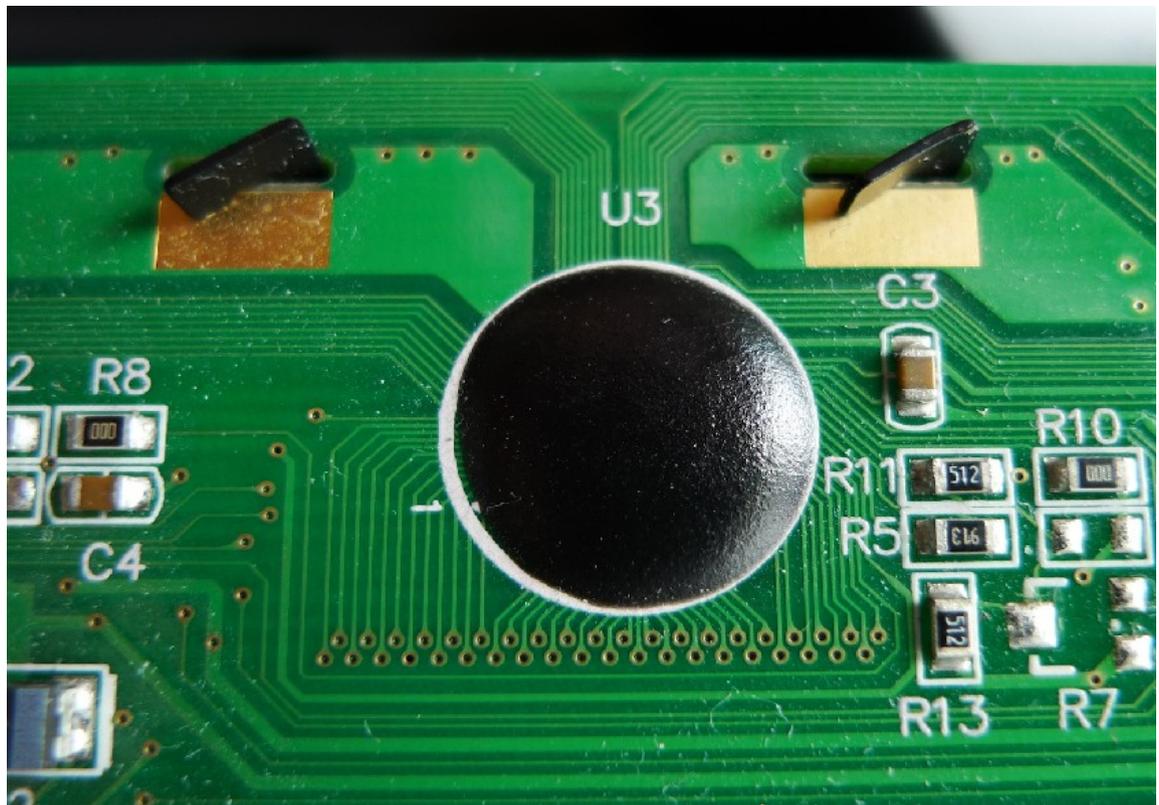
Difficult things are fun

Easy things are fun too

What makes some devices easy to
hack and others difficult?

Effort put into making a
device 'unhackable'

Low cost manufacturing makes hacks difficult



Cheap development *can*
make for *easier* hacks

Rejoice!

Some products are open
hardware designs!

Things to look for in a device:

- Similarity to reference designs
- Debug code left in
- Unused features/footprints
- Factory test points/ports

My CD player has a serial
port



RS-232C

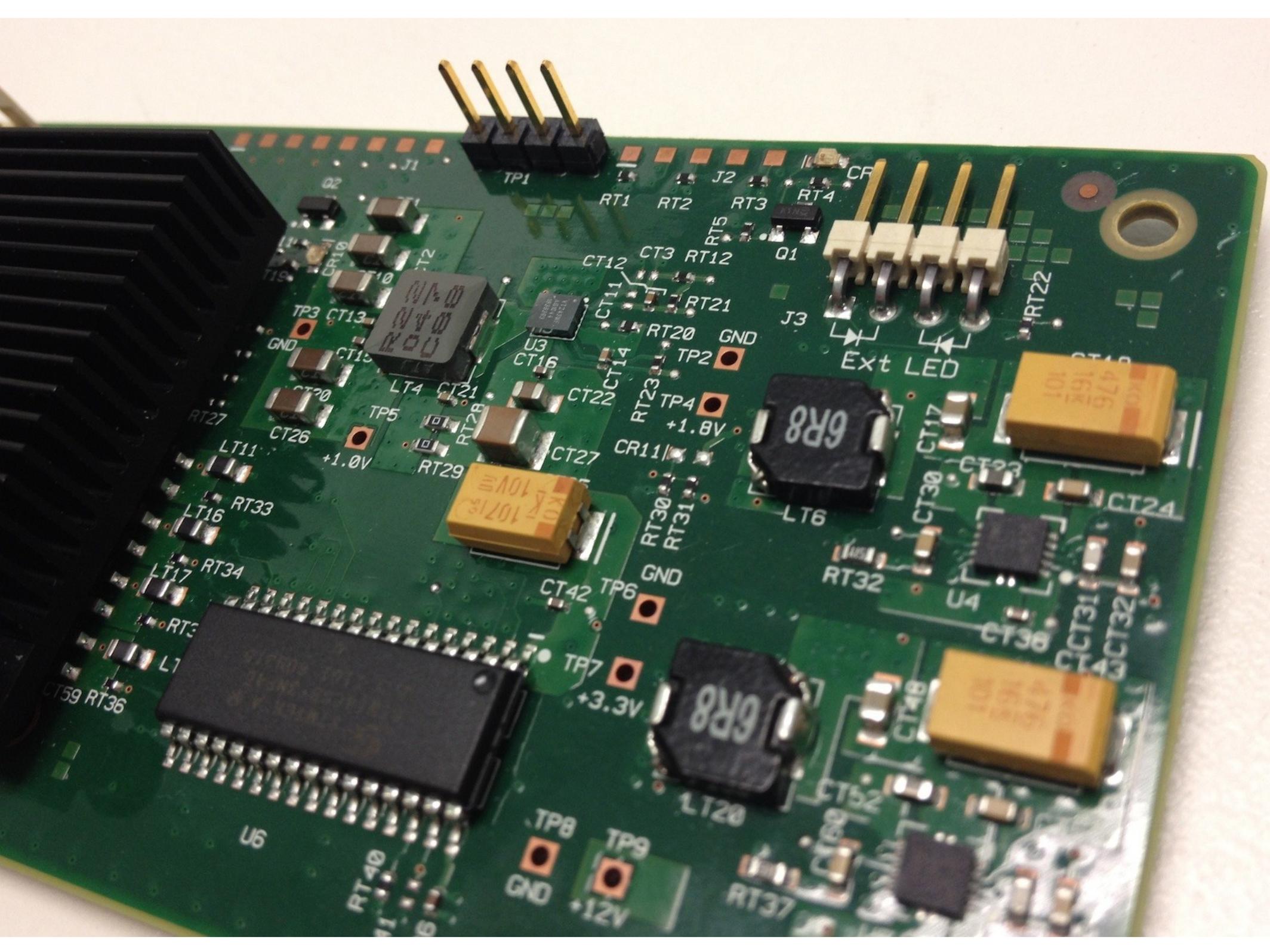
N11776

TV ANT IN

LOOP OUT

HDMI

S/PO





Q5861-
18005(P)
FW:R0042

R190R191

U138

CR191

CR190

J190

R133

C202

C201

E201

C203

C204

C205

C206

C207

C208

C209

C210

C211

C212

C213

C214

C215

C216

C217

C218

C219

C220

C221

C222

C223

C224

C225

C226

C227

C228

C229

C230

C231

C232

C233

C234

C235

C236

C237

C238

C239

C240

C241

C242

C243

C244

C245

C246

C247

C248

C249

C250

v
v
v
v

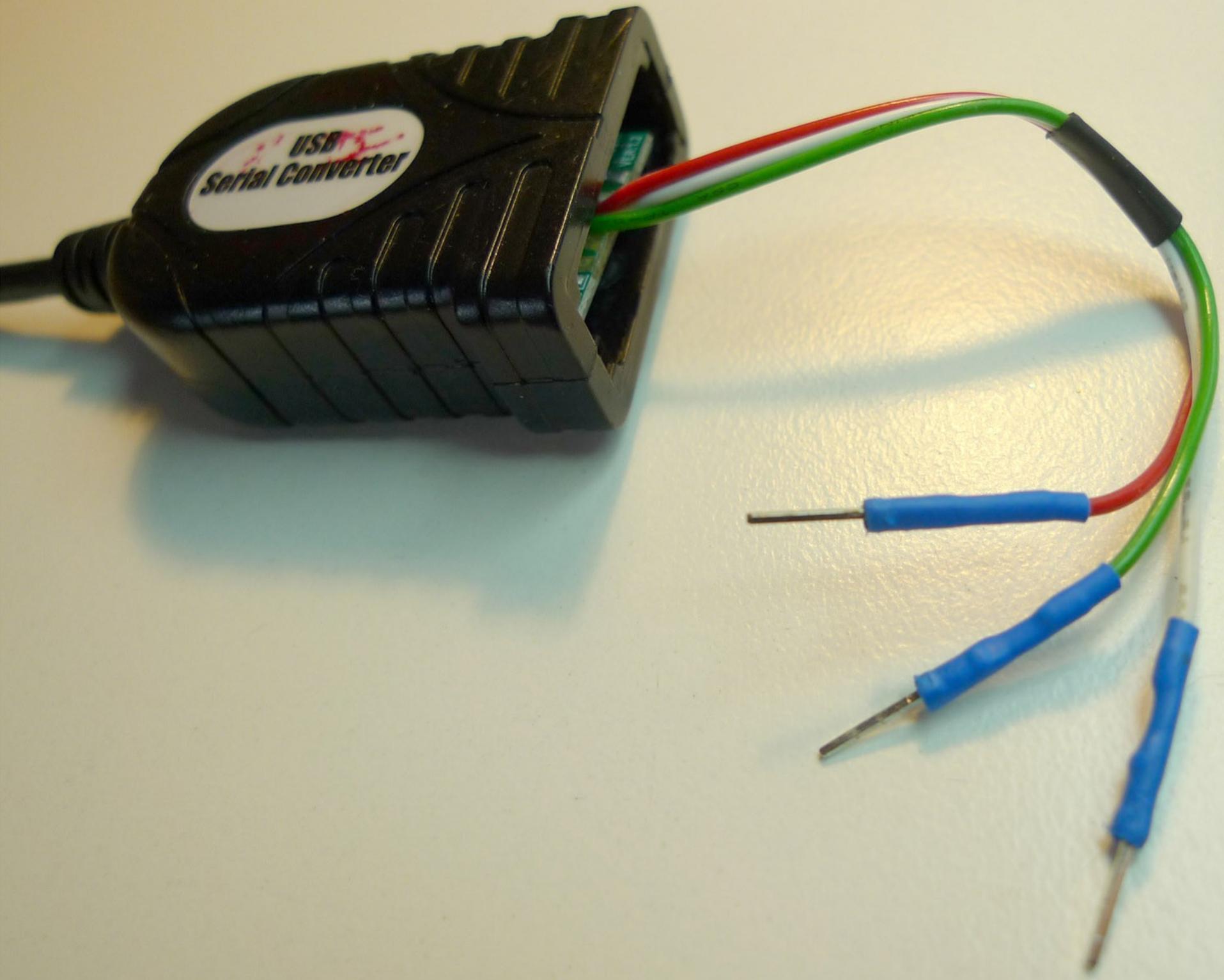
Acquire a 'logic level' serial-
USB cable

USB to TTL serial

TTL to RS232



USB
Serial Converter



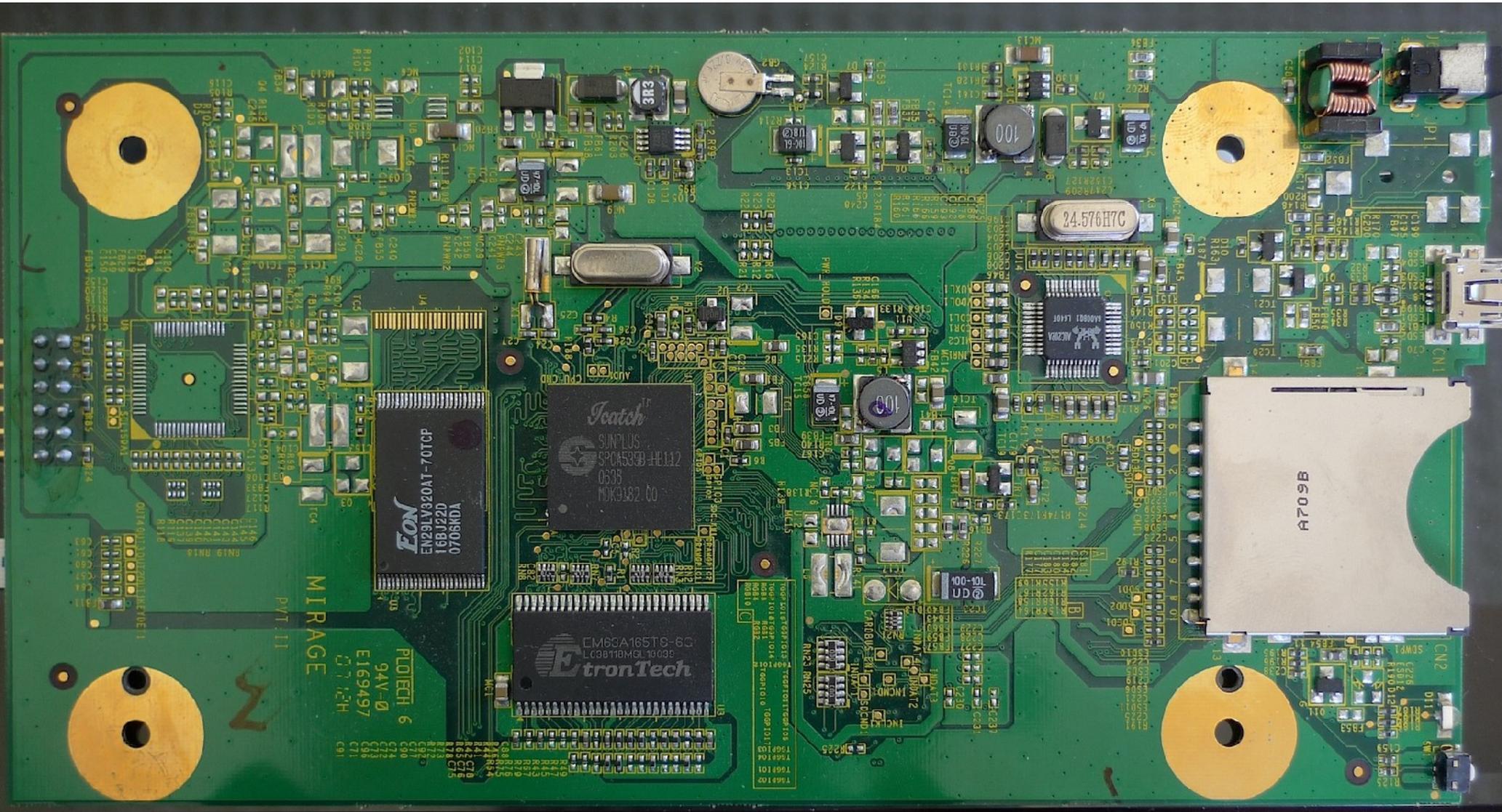
Other useful ports:

- JTAG
(PCB test, CPU debug)
- In-System Programming

Hacked device example

Twirly graphics for a bookshelf





FON
EN29LV320AT-70TCP
166J22D
0706NDA

Teatch
SUNPLUS
SPCA5330-HE132
0635
MOK9182.CO

EtronTech
EM63A165T6-63
LC98110MCL16000

PLDTECH 6
94V-0
E169497
0712H

MIRAGE
PVT II

24.576HTC

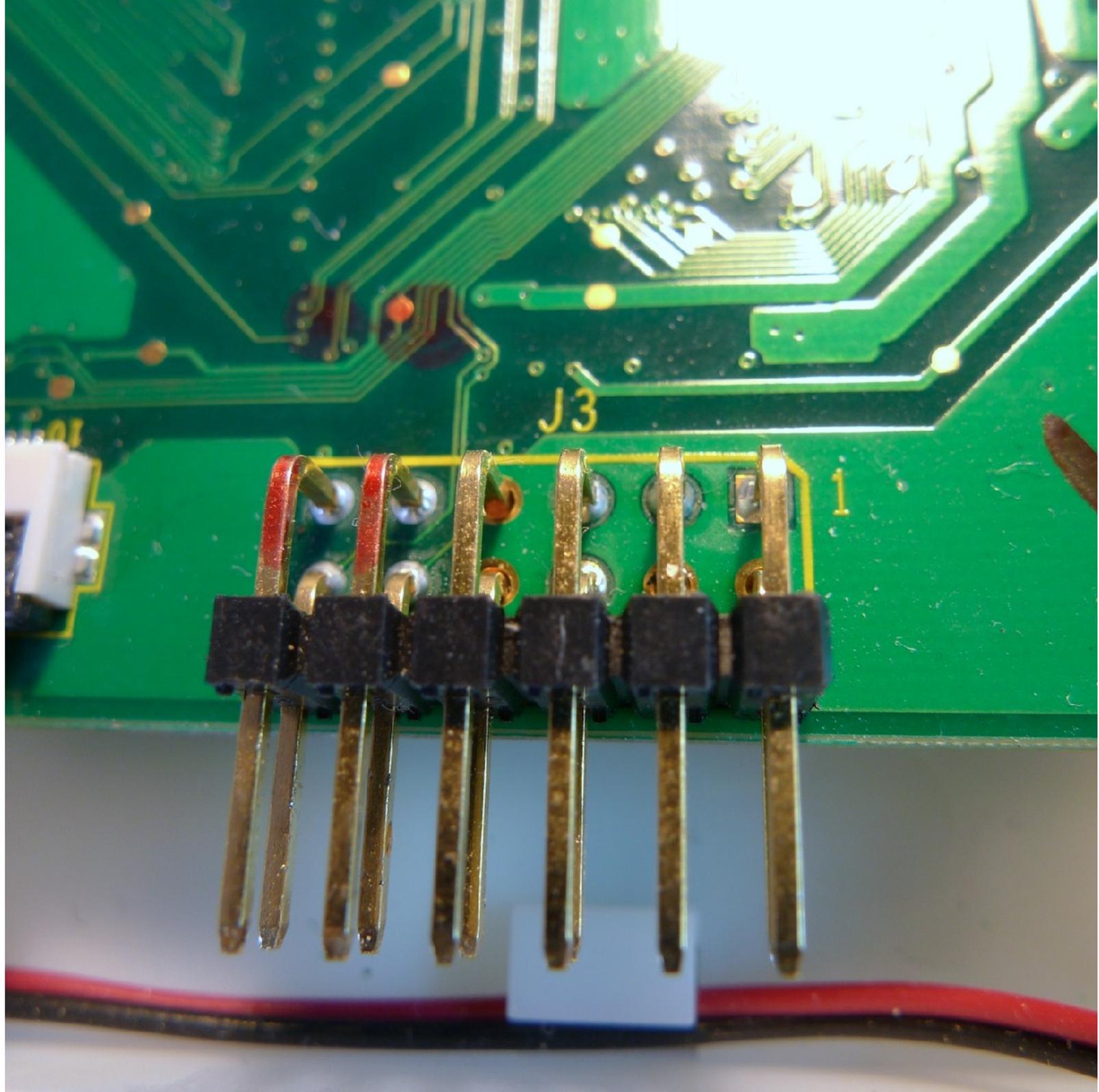
100

100-00

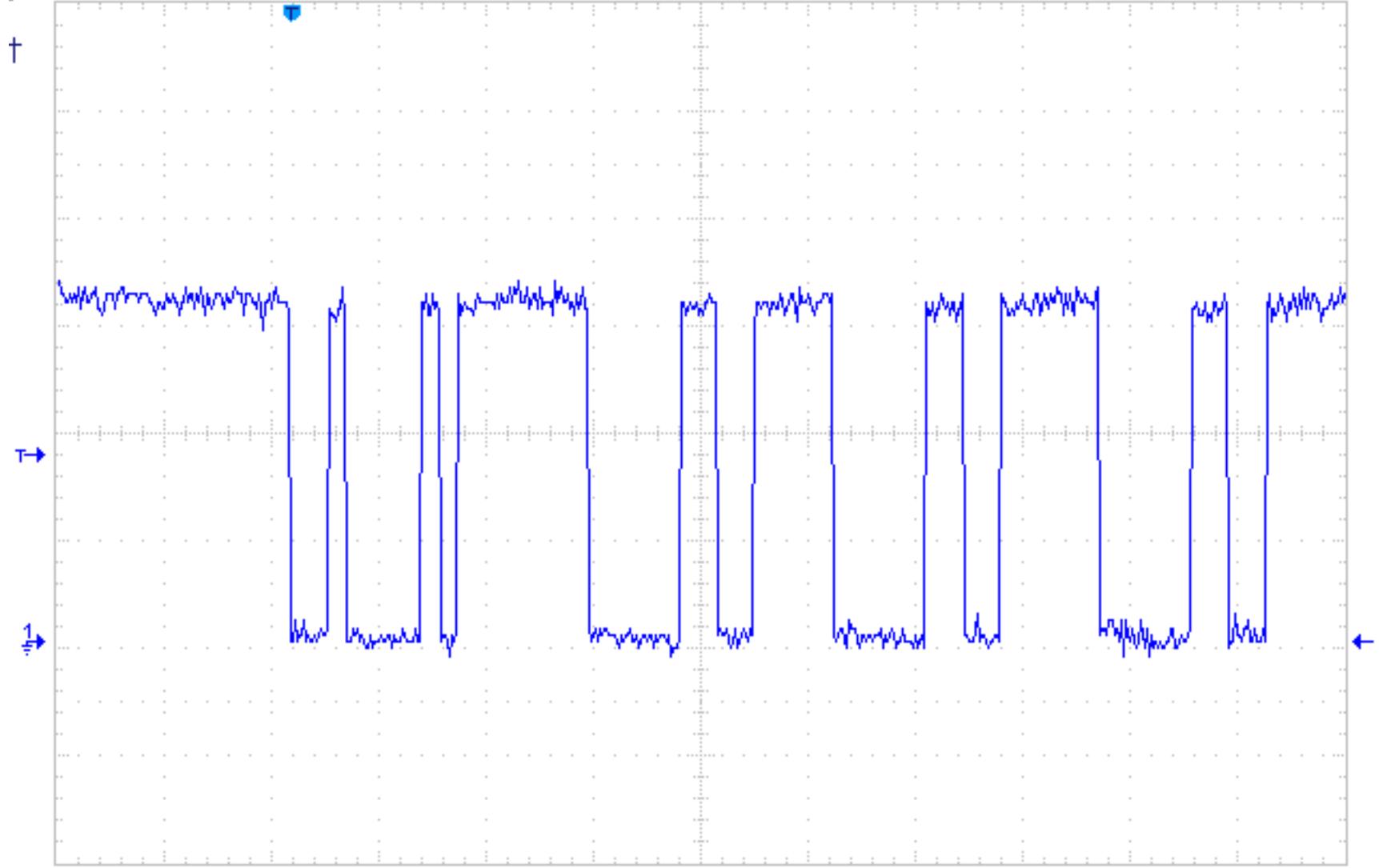
A709B

574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625

1647105
1647104
1647103
1647102
1647101
1647100
1647099
1647098
1647097
1647096
1647095
1647094
1647093
1647092
1647091
1647090
1647089
1647088
1647087
1647086
1647085
1647084
1647083
1647082
1647081
1647080
1647079
1647078
1647077
1647076
1647075
1647074
1647073
1647072
1647071
1647070
1647069
1647068
1647067
1647066
1647065
1647064
1647063
1647062
1647061
1647060
1647059
1647058
1647057
1647056
1647055
1647054
1647053
1647052
1647051
1647050
1647049
1647048
1647047
1647046
1647045
1647044
1647043
1647042
1647041
1647040
1647039
1647038
1647037
1647036
1647035
1647034
1647033
1647032
1647031
1647030
1647029
1647028
1647027
1647026
1647025
1647024
1647023
1647022
1647021
1647020
1647019
1647018
1647017
1647016
1647015
1647014
1647013
1647012
1647011
1647010
1647009
1647008
1647007
1647006
1647005
1647004
1647003
1647002
1647001
1647000



1 1V/ 5MSa/s 50% STOP 1 1.81V



Save to BMP Save to PPM Save to CSV Save to ASCII Send Measure Destination PC

```
=====
main() start
-----
Product Model: MIRAGE
Sensor Model:  MI2000
VER: 092_AYFF
2007/07/27      17:00
Rel by Axisoft
-----
DCF Dir Name:  AXH10
DCF File Name: FILE
=====
```

```
#####Check RTC Date#####
[Main::Last EPC=0x0]

[Main::irqInit() Done]
[Main::osInit() Done]
[Main::uartInit() Done]
SPCA536 EVB V1.0
```

F/W compiled at 17:30:35, Jul 27 2007

cmd>help

abort

custom

do

help

ostsk

pbcrop

pblcdstart

read

snap

snapprv

snapyuv

ver

wmapause

wmastop

cd

del

dump

info

pan

pbdramplay

pbresize

res

snapdel

snapqt

speed

wmacontent

wmaplay

write

center

dir

fill

mkdir

pause

pblcdrestore

pbrot

rmdir

snaphance

snapr gb

stillmemdisp

wmaffwd

wmaplayall

zoom

clip

disp

fmt

osmem

pb

pblcdrot

play

search

snaptop

snapsize

thumb

wmainfo

wmarew

Why is there a useful CLI hidden inside a closed box?

- Firmware from common codebase
- Debug code left in
 - Rushed to market!

```
printf("fopen: out of mem\n");
```

```
printf("[irqInit() Done]\n");
```

```
==[OnEnterASKTypeMode End]==  
[hwPowerEnable(MODULE_JPEG)] in [src/axPhot  
[hwPowerEnable(MODULE_MPEG)] in [src/axPhot  
[hwPowerDisable(MODULE_CDSP)] in [src/axPhot  
==[OnEnterSlideMode End]==
```

```
cmd>
```

```
cmd>
```

```
cmd>read PF.BIN 0x8d420000
```

```
file size=76832 bytes
```

```
time difference=24040 us
```

```
cmd>do 0x8d420000
```

```
JMHowdy! sp is 8dffffb0
```

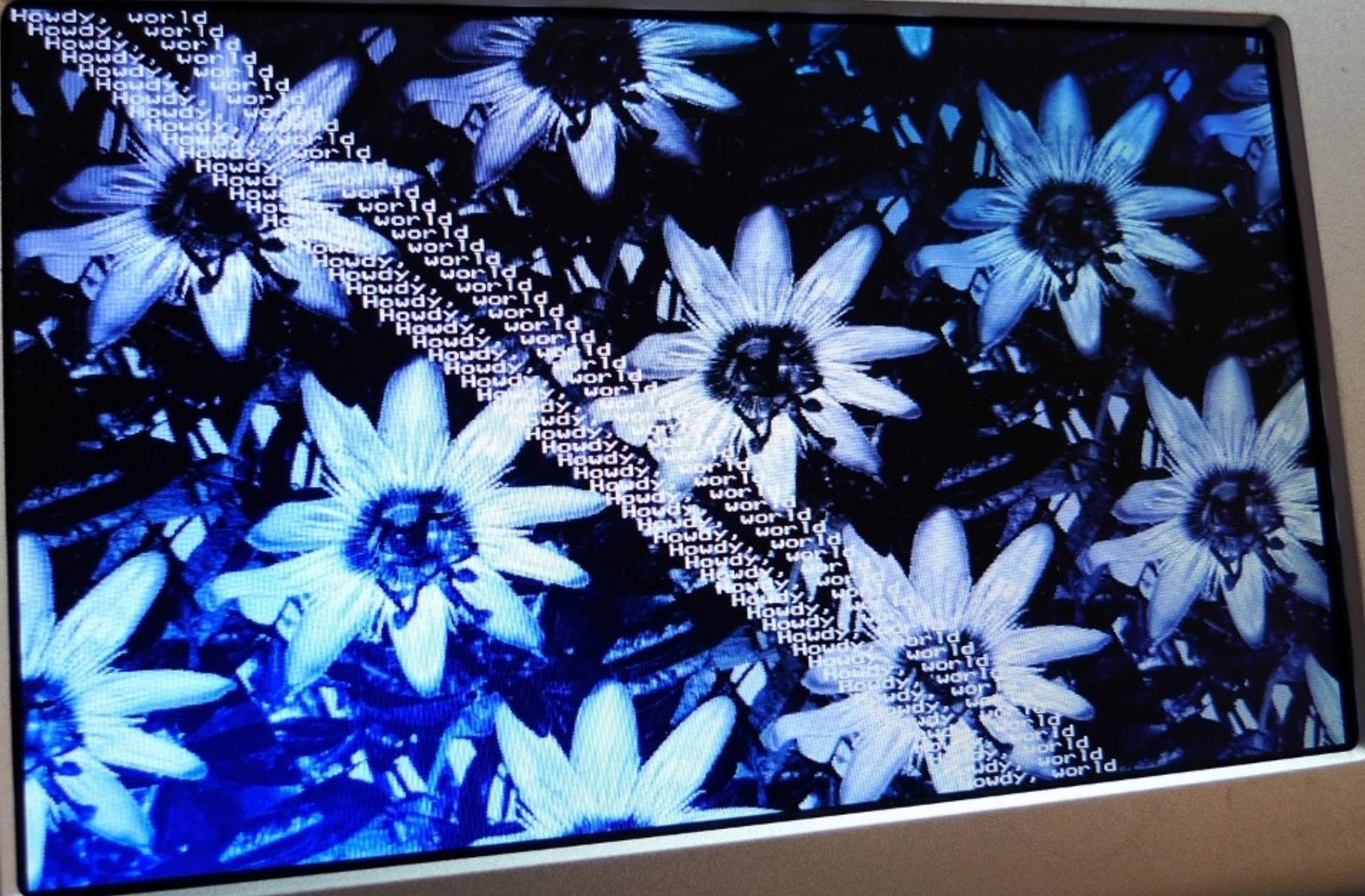
```
-
```

```
20:44
```

```
51x160
```

```
16k
```

```
115200 N81
```



Hacked device example

Building bench equipment



TL-WR340G
54M Wireless Router

PWR SYS WLAN WAN 1 2 3 4

TP-LINK

DSL

Reset

USB

Ethernet

12VDC

I <3 OpenWRT

Fun WiFi/ADSL box hacks:

- Espresso machine heater PID controller
- Streaming mp3 radios
- R/C cars with streaming video





041547615

- Annex A
- Annex B
- Modem
- Router
- Modem+USB
- Router+USB

Pulse®
BX2479H.01
0634-C
CHINA

1DSL502TAUAS

0636F
ST6121A

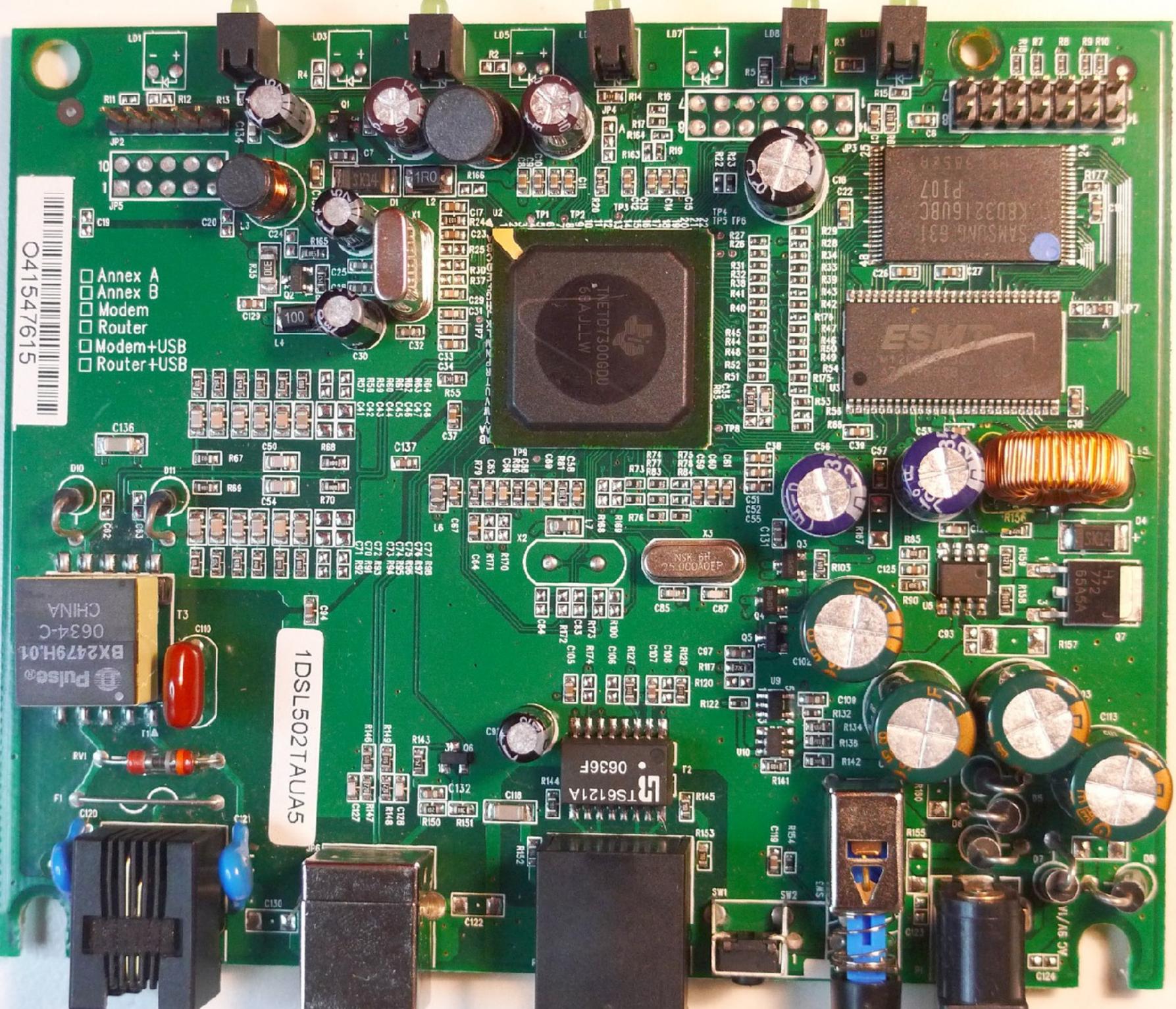
SAMSUNG 631
K8D3216UBC
P107

ESAT

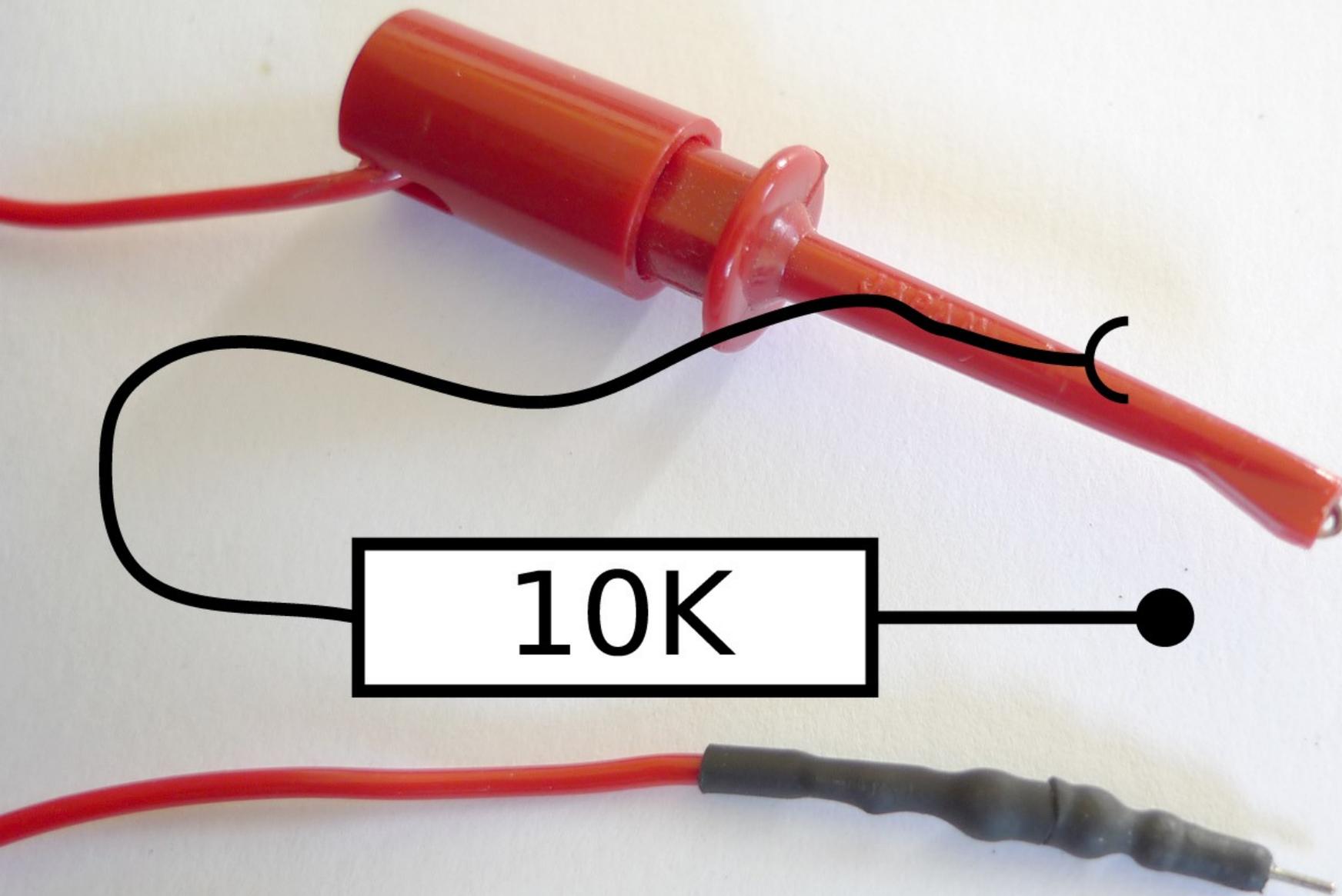
INTEL D7300600
69ALLW

NSR 6H
25.00000EP

772
65A5A



Mapping out GPIOs



10K

```
/* Page containing GPIO MMIO registers: */
unsigned int phys_addr = 0x08610000;

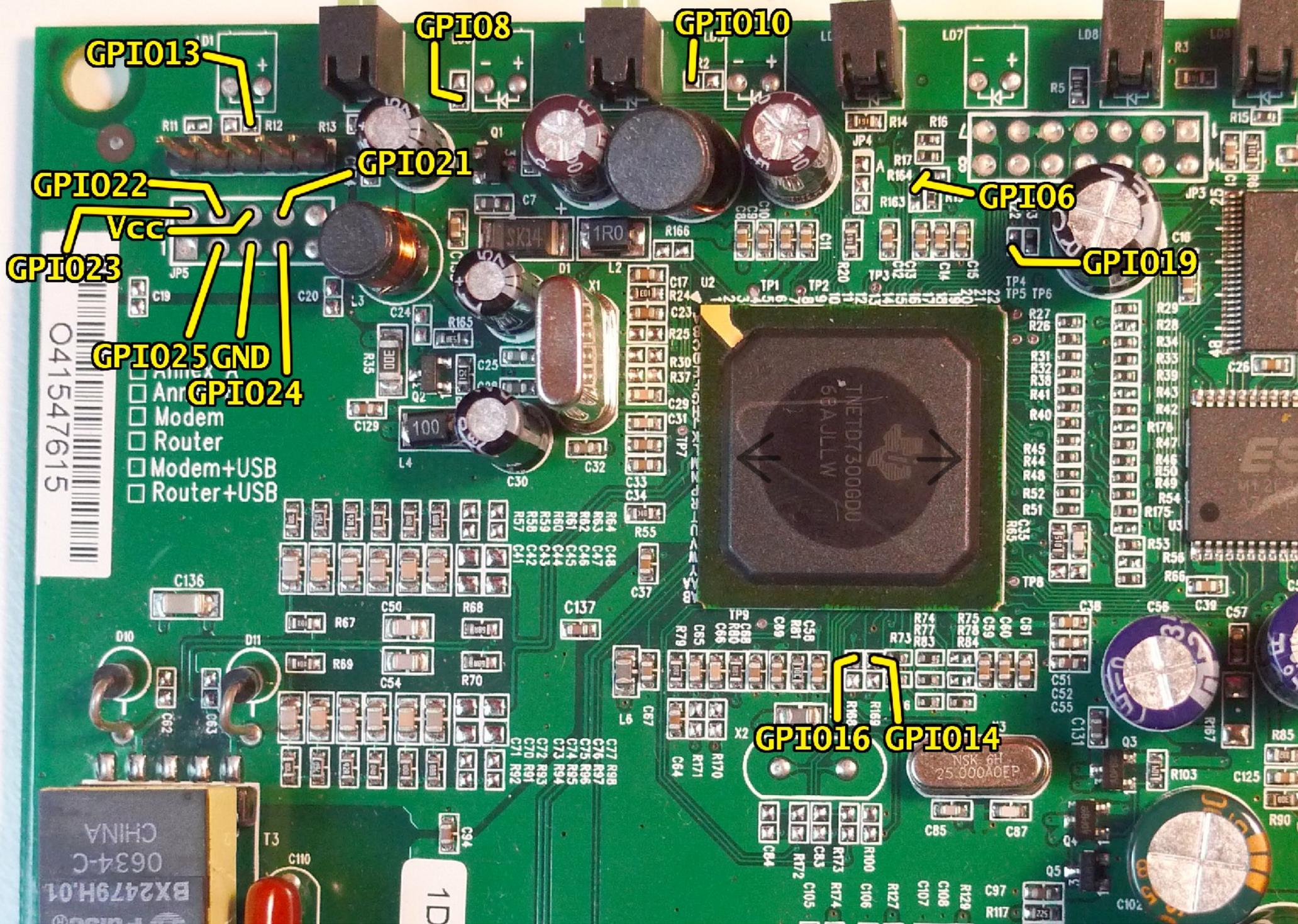
int main(void)
{
    int mfd;
    volatile unsigned int *vaddr;

    mfd = open("/dev/mem", O_RDWR | O_SYNC);

    vaddr = mmap(0, 4096, PROT_READ | PROT_WRITE,
                 MAP_SHARED, mfd, phys_addr);

    vaddr[GPIO_DIRECTION] = 0xffffffff; /* All pins input */

    while (1) {
        /* Read 32 input pins */
        printf("%08x\n", vaddr[GPIO_INPUT]);
    }
    return 0;
}
```



GPI013

GPI08

GPI010

GPI022

GPI021

GPI06

GPI019

GPI023

GPI025 GND

GPI024

GPI016

GPI014

041547615

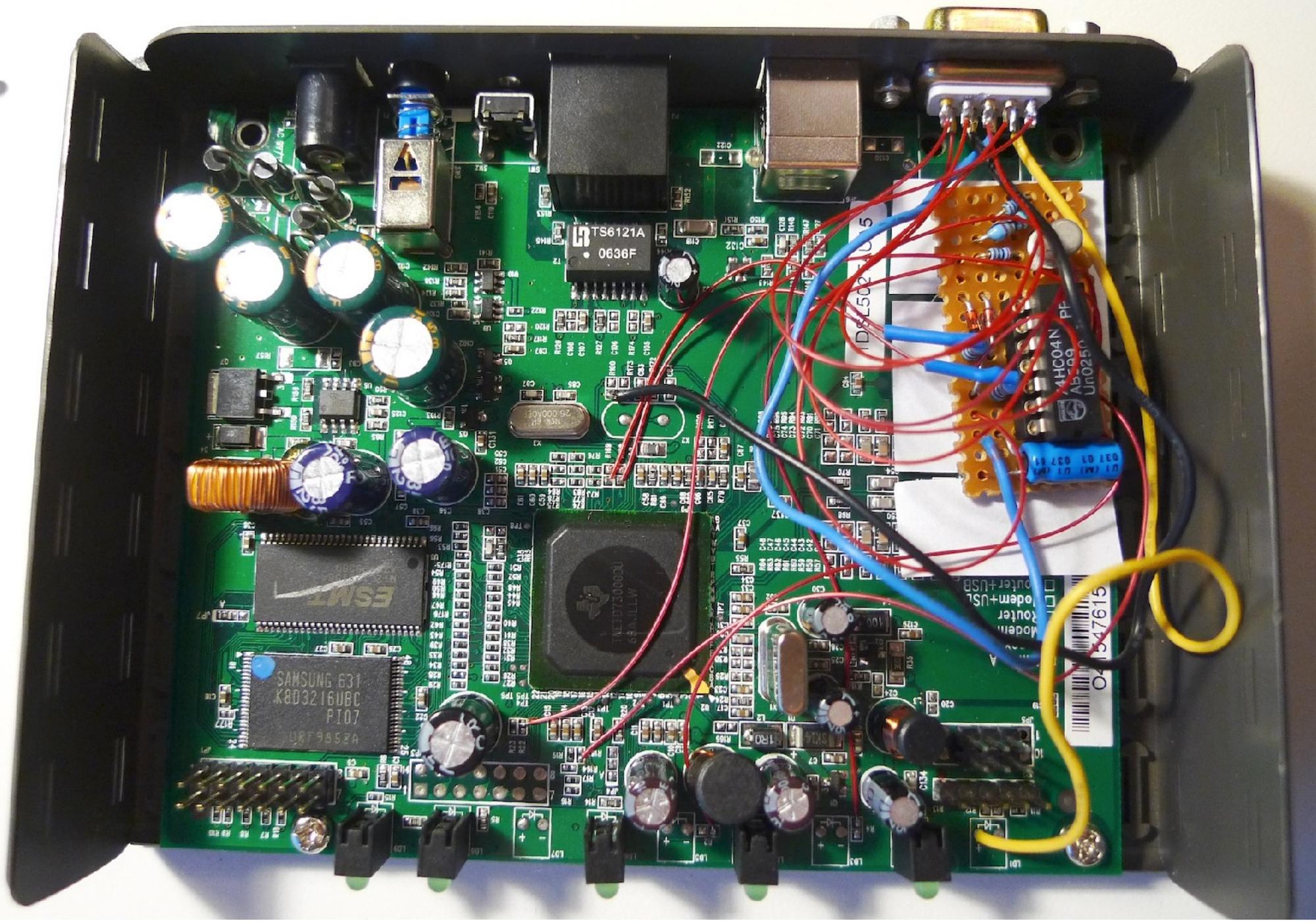
- Anr
- Modem
- Router
- Modem+USB
- Router+USB

TINETD7300GDDU
6BAJLLW

NSK 6H
25.000A0EP

CHINA
0634-C
BX2479H.01

1D



Hacked device example

Happy cat

The New York Times | Top Stories

MICHAEL D. SHEAR and NICHOLAS CONFESSORE



Romney Times Four

Jan 08, 2012
ASHLEY PARKER



Bold Lie Turns Run-In at Sea Into Dramatic Rescue

Jan 08, 2012
C. J. CHIVERS



In Offensive Display, Saints Overpower Lions

Jan 08, 2012
GREG BISHOP



Latest Hacking Scandal Arrest Suggests Focus on Cover-Up

Jan 08, 2012
JOHN F. BURNS

INSIGNIA

Open design:

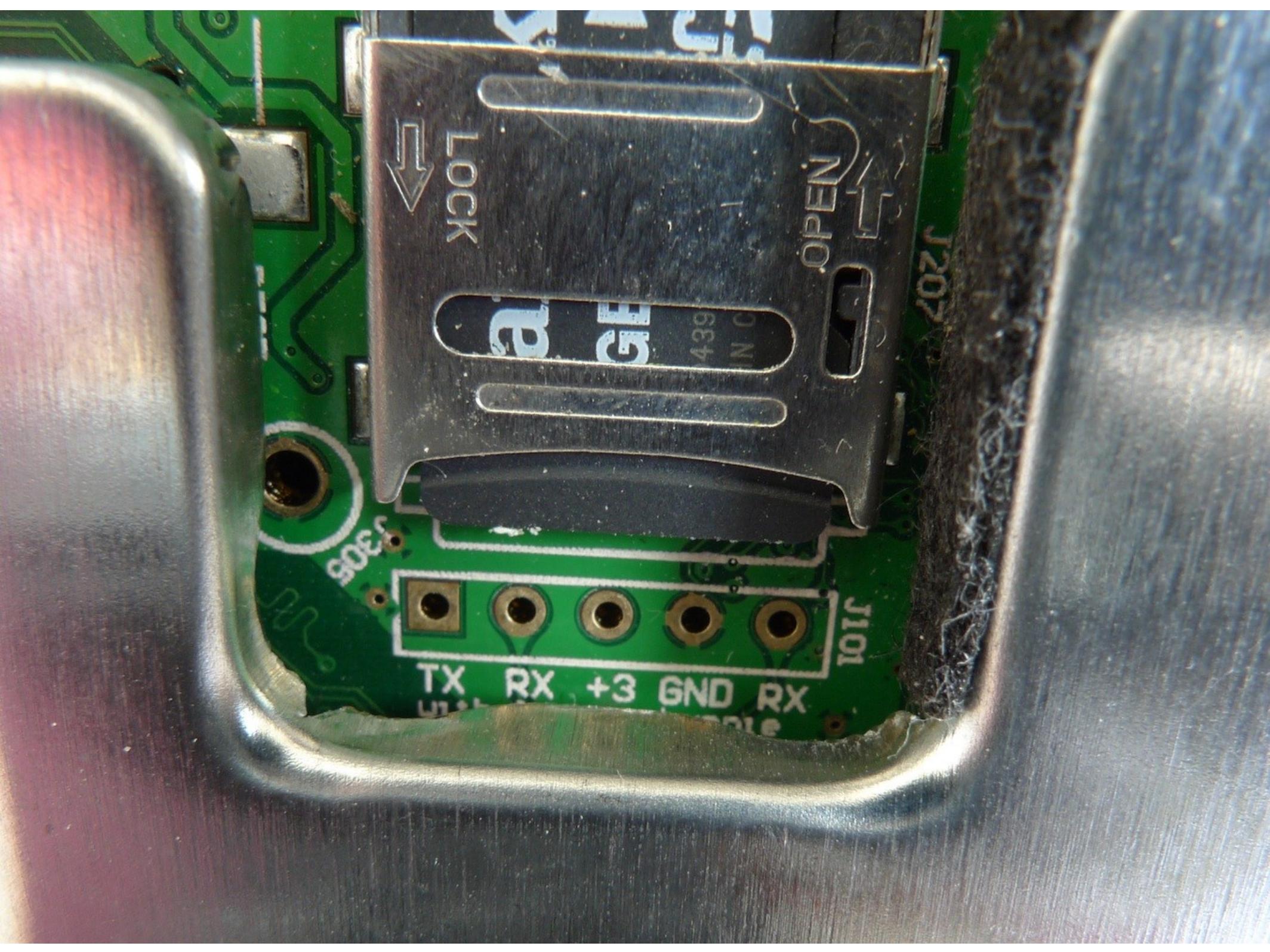
- PCB
- Schematics
- Firmware

DEMO

Viewable at:

<http://youtu.be/azE5-3fAjUs>





LOCK

OPEN

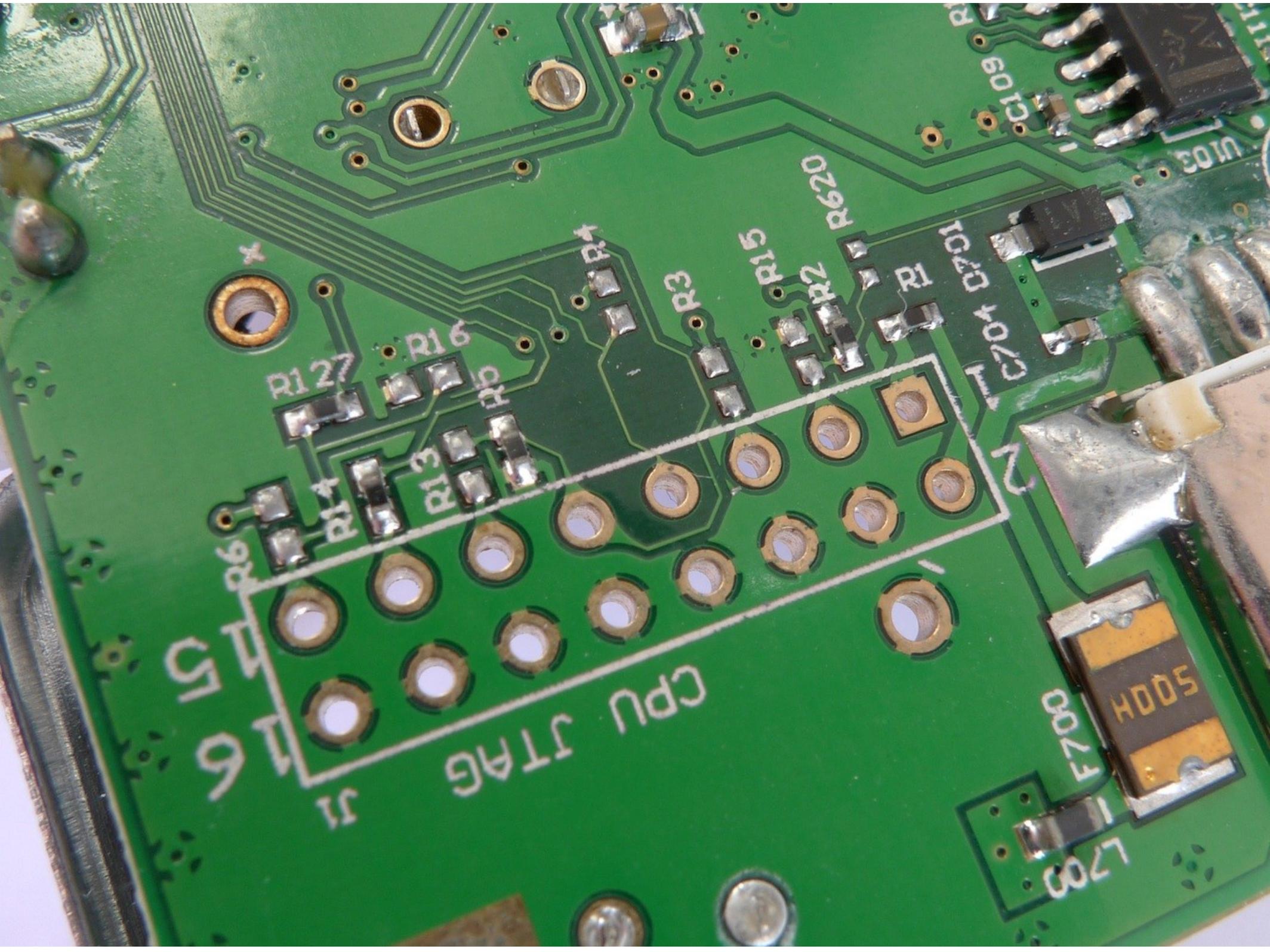
a G 439 N C

TX RX +3 GND RX

J101

J305

J207



16

R127

R16

R14

R13

R14

R3

R15

R2

R620

R1

IC104 03701

CPU JTAG

E700

500H

L700

R47

03

GND

GP49

GP55

3.3V

50 mA

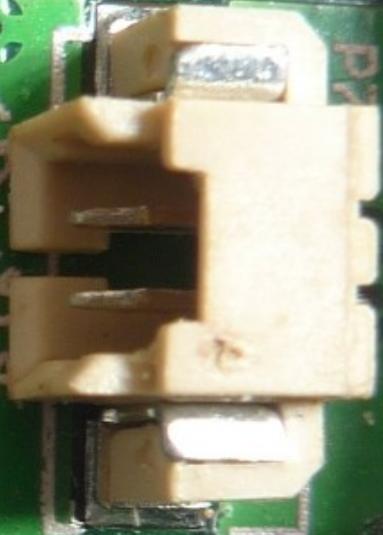
P705

GP5

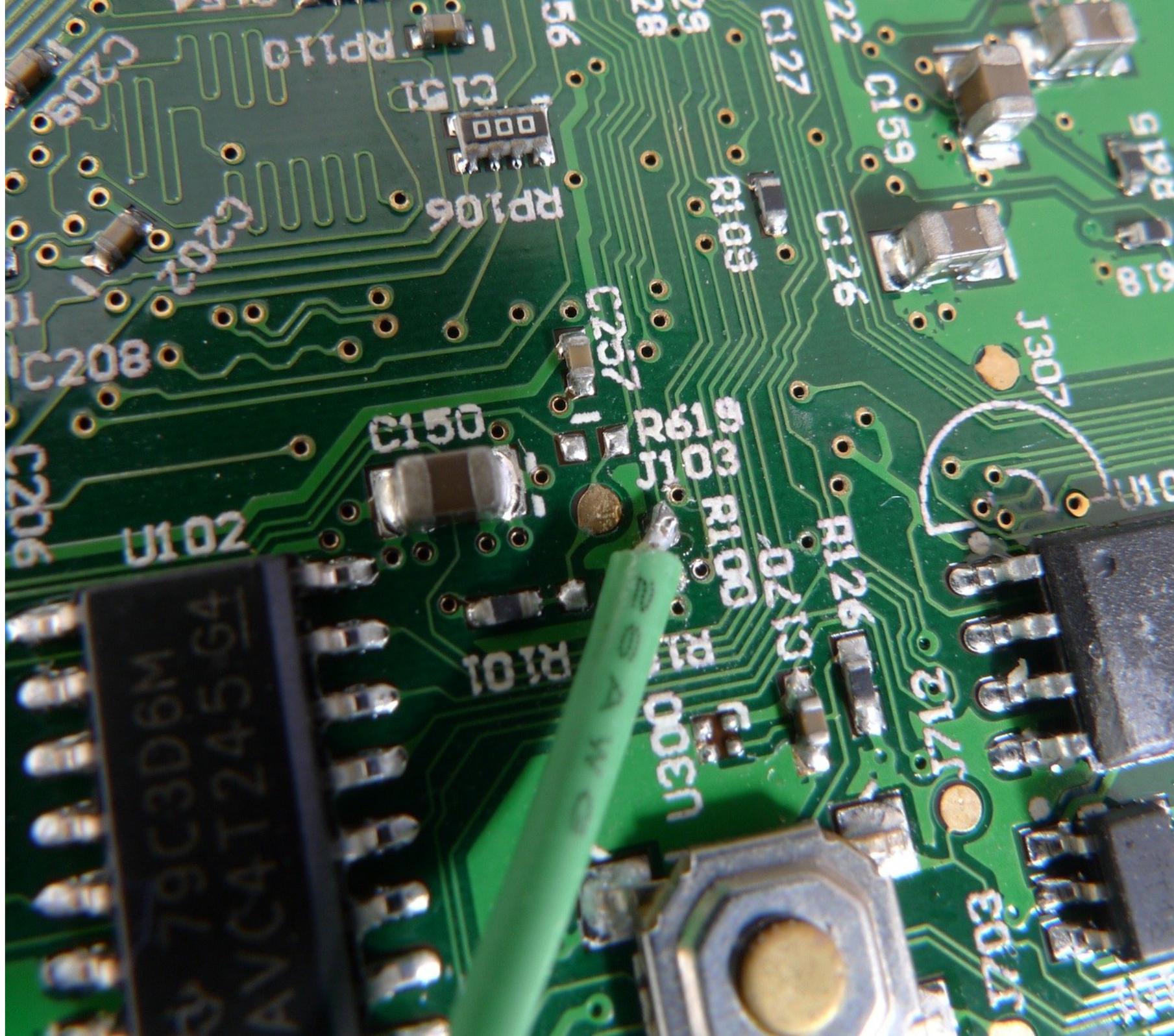
GP4

SDA

SCL







U102

C150

RP106

C207

J103

R103

C126

R126

C159

J307

R101

J300

R124

R302

C209

C207

C208

C206

RP110

C151

C127

C22

R198

R199

R199

U102



```
# Ugly pin multiplexer config, timer and PWM
# init:
```

```
./poke 0xd401e208 0x4c42
./poke 0xd401500c 0x13
./poke 0xd401a000 0x0
./poke 0xd401a004 0x15
./poke 0xd401a008 0x28f
```

```
# Turn servo to open position:
```

```
./poke 0xd401a004 0x40
```

```
# Turn servo to closed position:
```

```
./poke 0xd401a004 0x15
```

Other Examples



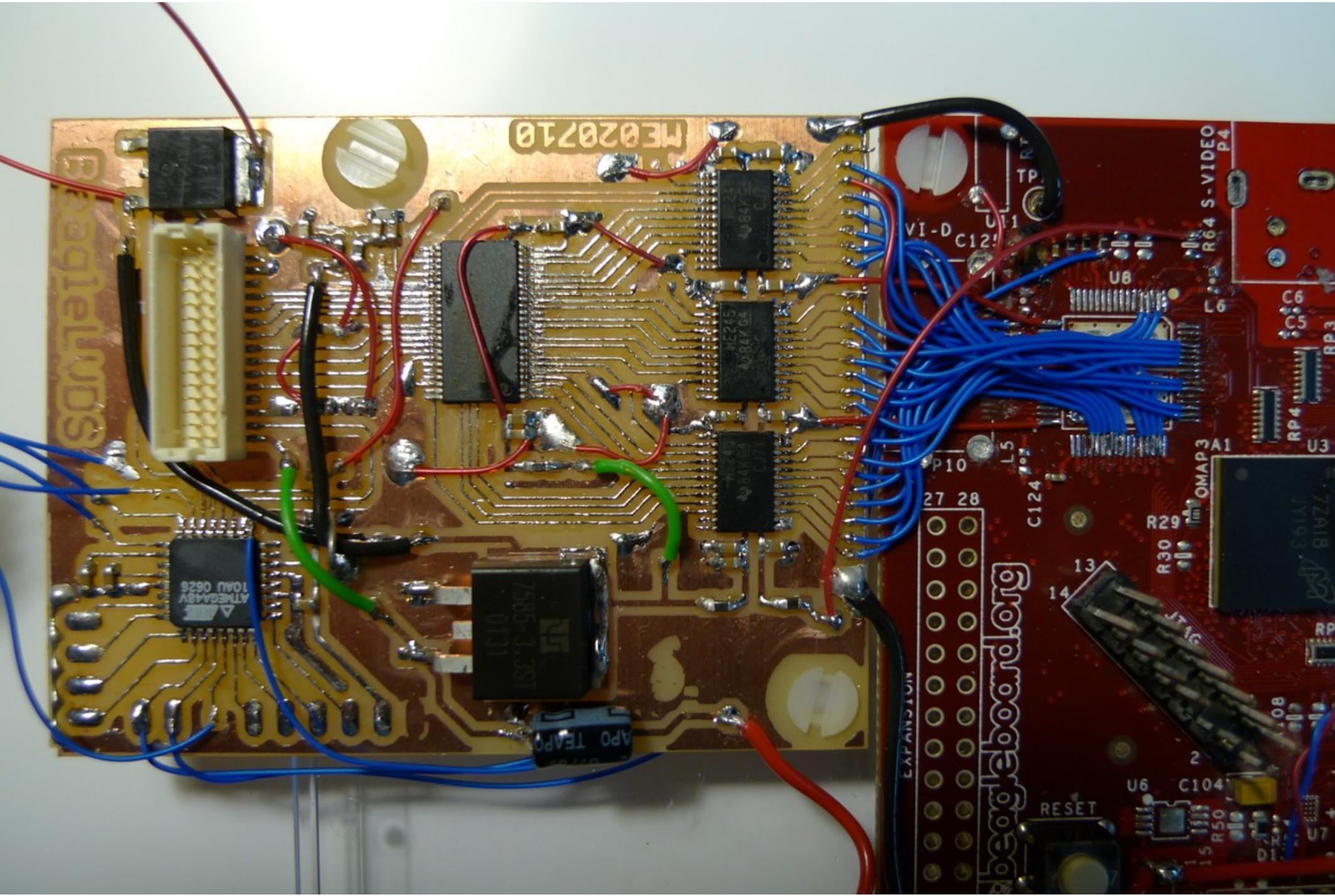
COULD CAUSE FLUORESCENCE
TAKING A SMALL AMOUNT OF
REPAIRING OR REPAIRING
REPAIRING OR REPAIRING
REPAIRING OR REPAIRING

CAUTION
HIGH VOLTAGE
DANGER
DO NOT TOUCH
INTERNAL PARTS

1-11-19-762-962-11

LTD133EX2X
MADE IN JAPAN
Toshiba Matsushita Display Technology Co., Ltd.
CAC4H004735
147886411 118

crucial!
128 MB
MultiMediaCard



ME020710

BeagleBoard

beagleboard.org

ATMEGA48V
10AU 0626

AP0 TEAP0

ATMEGA162

ATMEGA162

OMAP3
7ZA18
V193

R64 S-VIDEO
P4

RESET

JTAG

EXPANSTION

P10
27 28

VI-D
C124

U6

C104

R50

R29

R30

U3

OMAP3
A1

U8

C6

C5

C3

RP3

RP4

U7

RESET

TP

U1

U2

U3

U4

U5

U6

U7

U8

U9

U10

U11

U12

U13

U14

U15

U16

U17

U18

U19

U20

U21

U22

U23

U24

U25

U26

U27

U28

U29

U30

U31

U32

U33

U34

U35

U36

U37

U38

U39

U40

U41

U42

U43

U44

U45

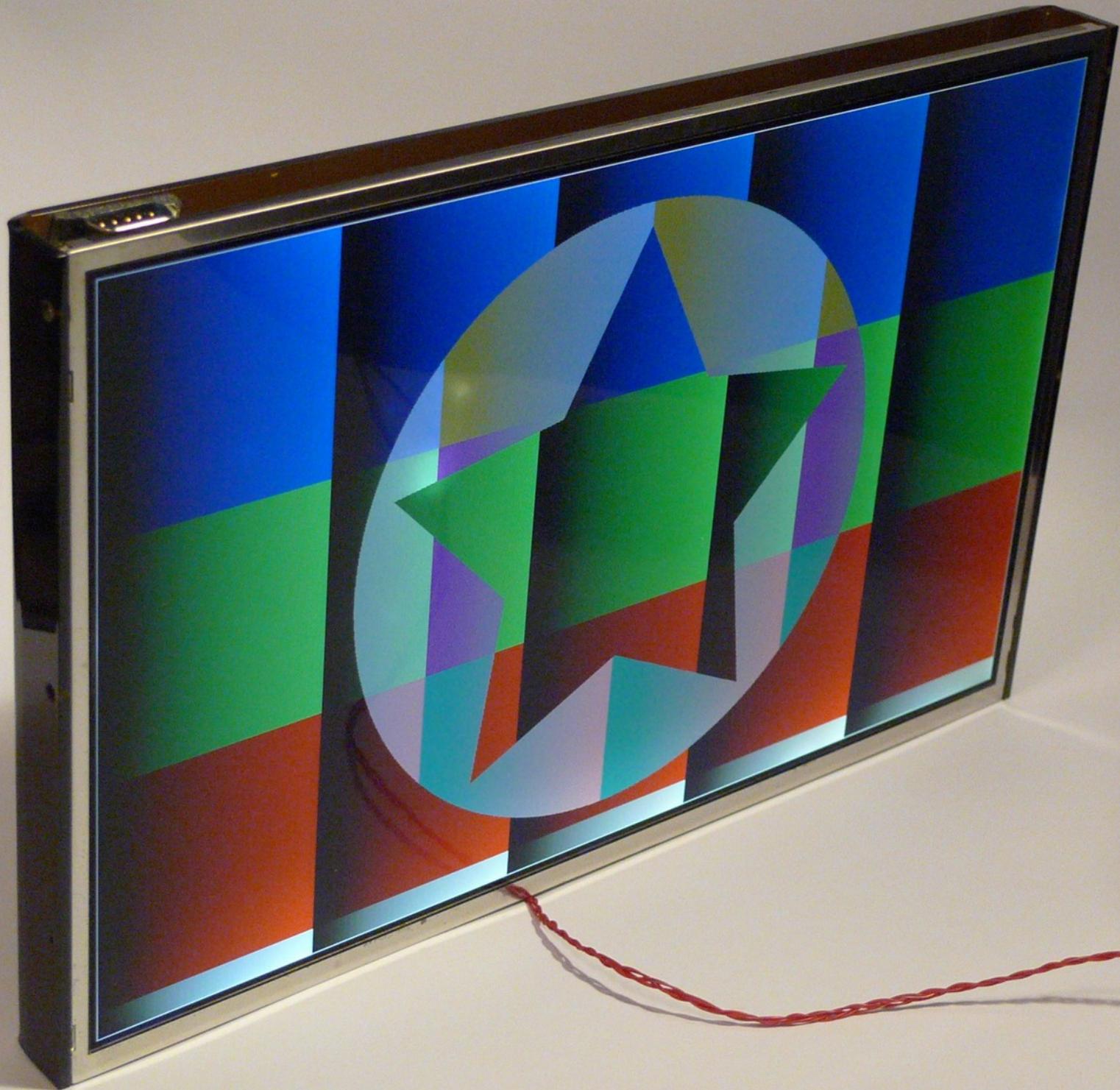
U46

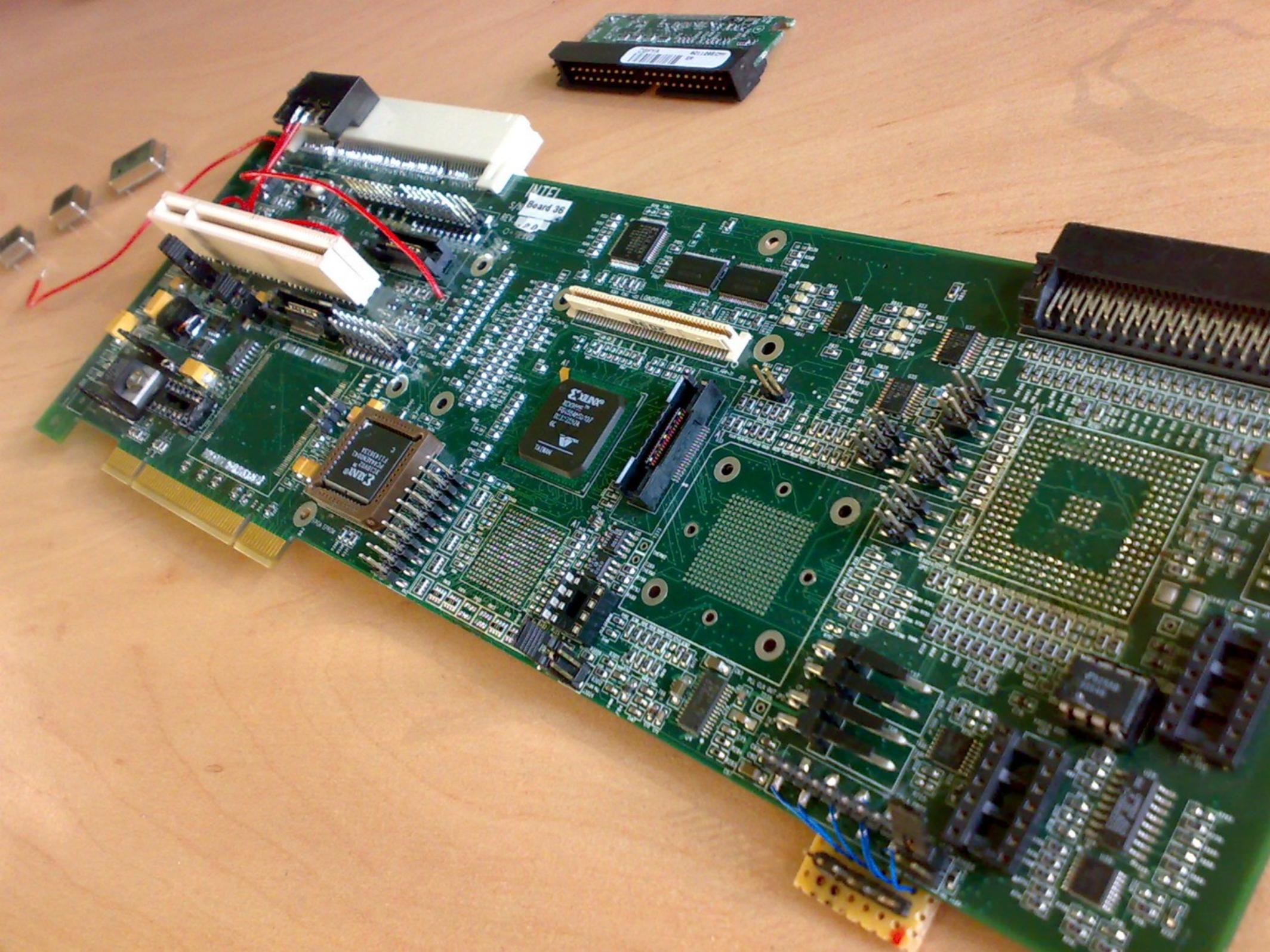
U47

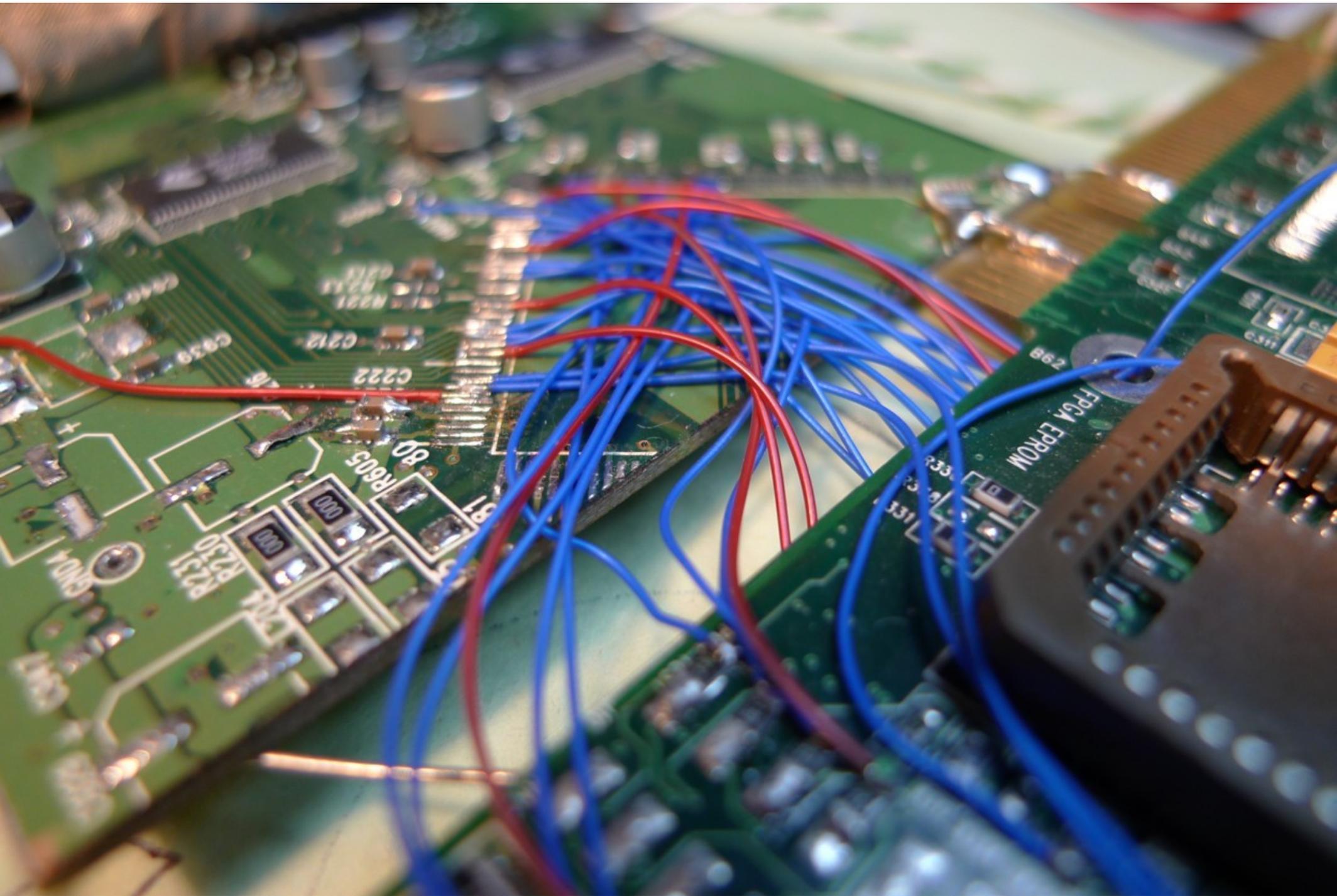
U48

U49

U50









1 PLAYER 2 PLAYER
© 1989 Nintendo

iivama

AUTO MENU



Handwritten notes on a piece of paper in the foreground, including numbers like 20, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100.



MARIO KART™
SUPER CIRCUIT™

SINGLE PLAYER

© 1992, 2001 Nintendo

Hitachi

Handwritten notes on a piece of paper on the desk, including the words "Den - Bank", "Life", "100", "200", "300", "400", "500", "600", "700", "800", "900", "1000", "1100", "1200", "1300", "1400", "1500", "1600", "1700", "1800", "1900", "2000", "2100", "2200", "2300", "2400", "2500", "2600", "2700", "2800", "2900", "3000", "3100", "3200", "3300", "3400", "3500", "3600", "3700", "3800", "3900", "4000", "4100", "4200", "4300", "4400", "4500", "4600", "4700", "4800", "4900", "5000", "5100", "5200", "5300", "5400", "5500", "5600", "5700", "5800", "5900", "6000", "6100", "6200", "6300", "6400", "6500", "6600", "6700", "6800", "6900", "7000", "7100", "7200", "7300", "7400", "7500", "7600", "7700", "7800", "7900", "8000", "8100", "8200", "8300", "8400", "8500", "8600", "8700", "8800", "8900", "9000", "9100", "9200", "9300", "9400", "9500", "9600", "9700", "9800", "9900", "10000".

Re-use hardware stuff!

- Don't just consume... re-consume :-)
- If you discover something cool, teach others and tell the world
- Collaborate at a local hackerspace

Merci – and questions?

<http://www.hackaday.com/>

<http://axio.ms/projects/>

<http://www.ifixit.com/Manifesto/>

<http://www.we-make-money-not-art.com/archives/2011/07/gambilogia.php>

<http://obaru.tumblr.com/post/3748881704/creating-a-linux-based-pid>