Hack Everything

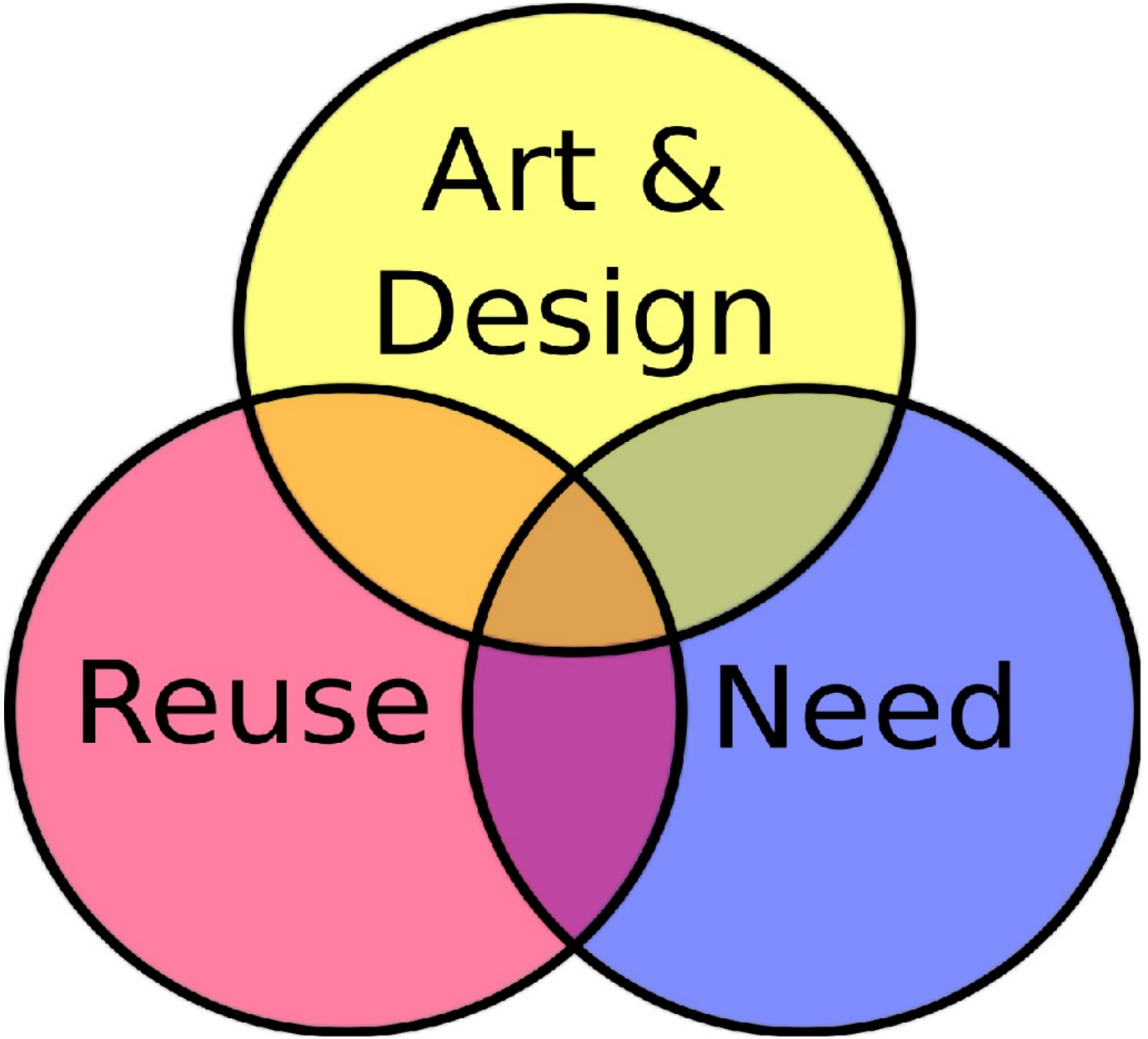
or:
Pull apart electronic stuff and invent new things with the insides

Matt Evans, IBM OzLabs

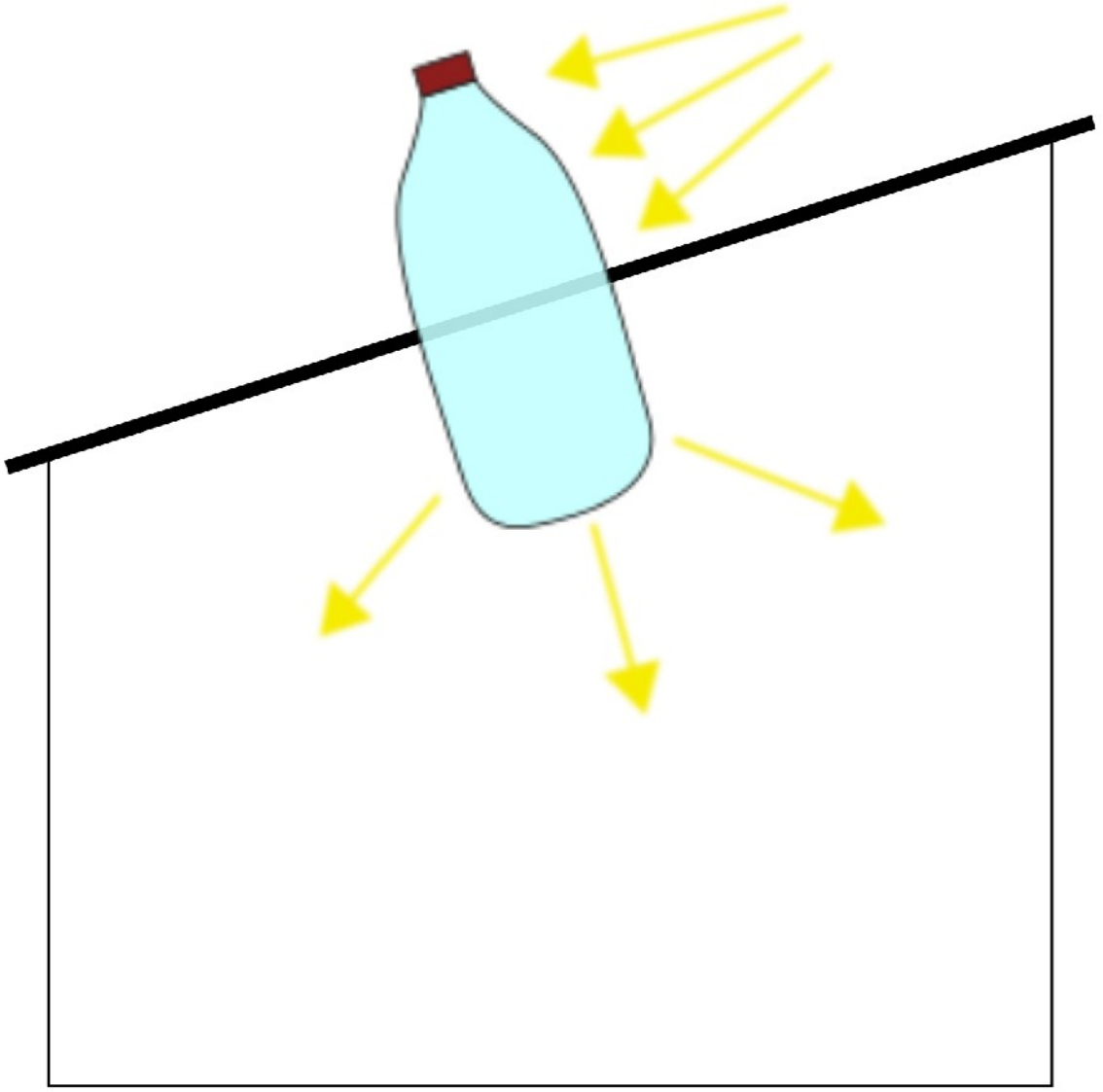
Re-using electronic devices

1. Philosophy
2. Technical stuff

Philosophy of re-use/hacking


Art &
Design
Reuse
Need

Litron Liwanag (Litre of Light)



Gambiarra:

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

– With an emphasis on an artful nature!


V
0
1
2
3
4
5
6
7
8
9
10
WILD
HEERBRUGG
SWITZERLAND


FX/D/198
Aldis


Fear me!
MEGADUCK


Wii
NOKIA

Save resources:

Re-use > Recycling > Landfill

Save money:

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

Take things apart, learn by example

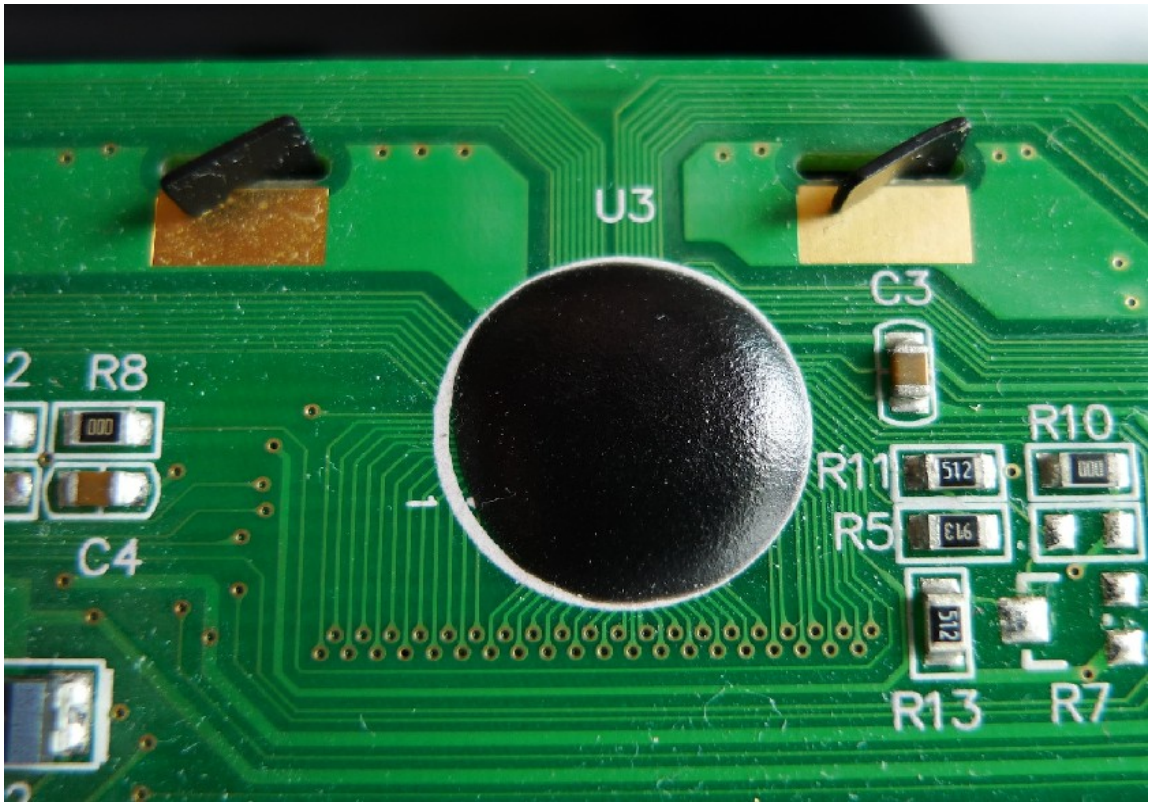
Difficult things are fun

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

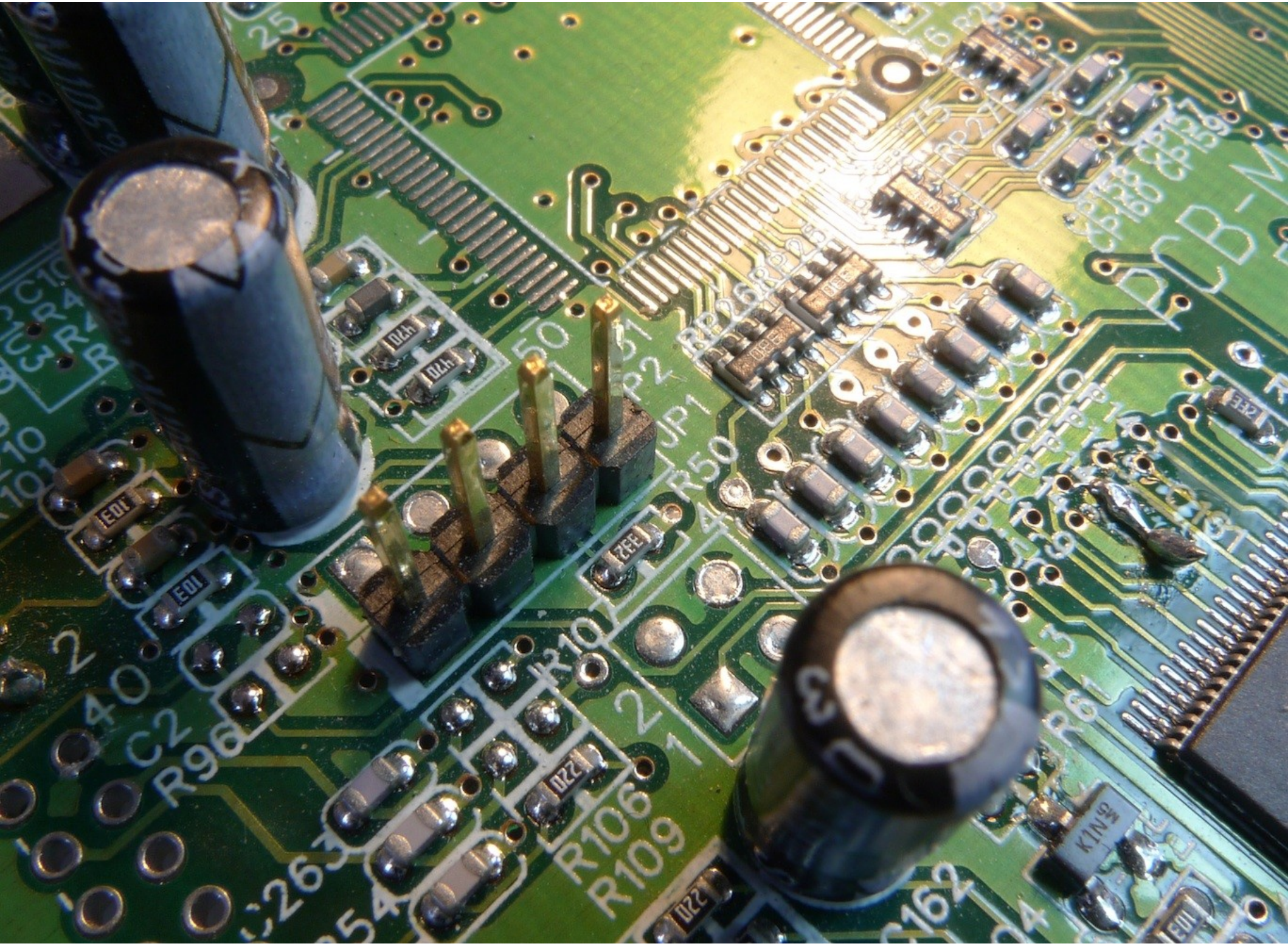
Rejoice!

Some products are open hardware designs!

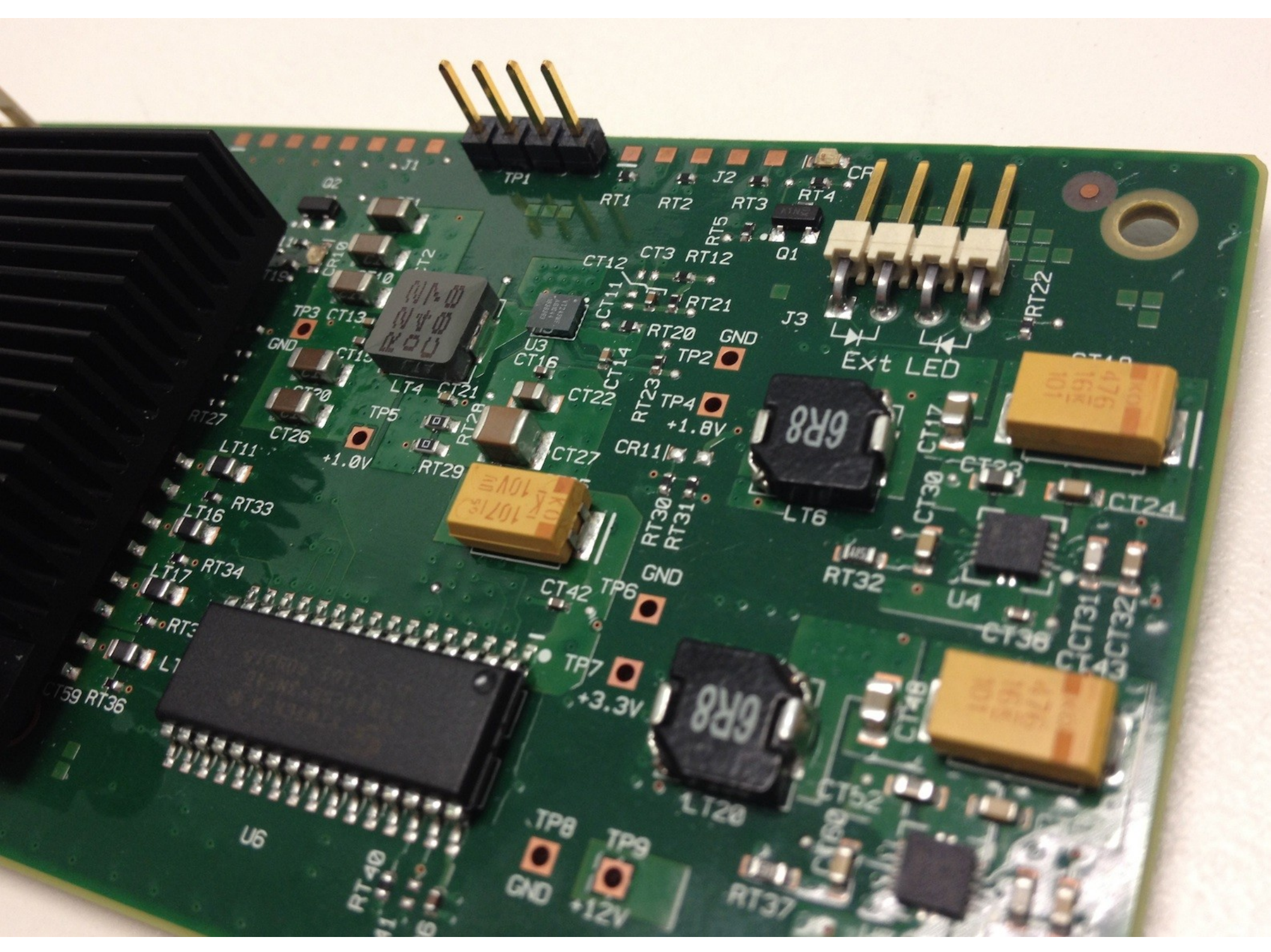
Things to look for in a device:

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

My CD player has a serial port

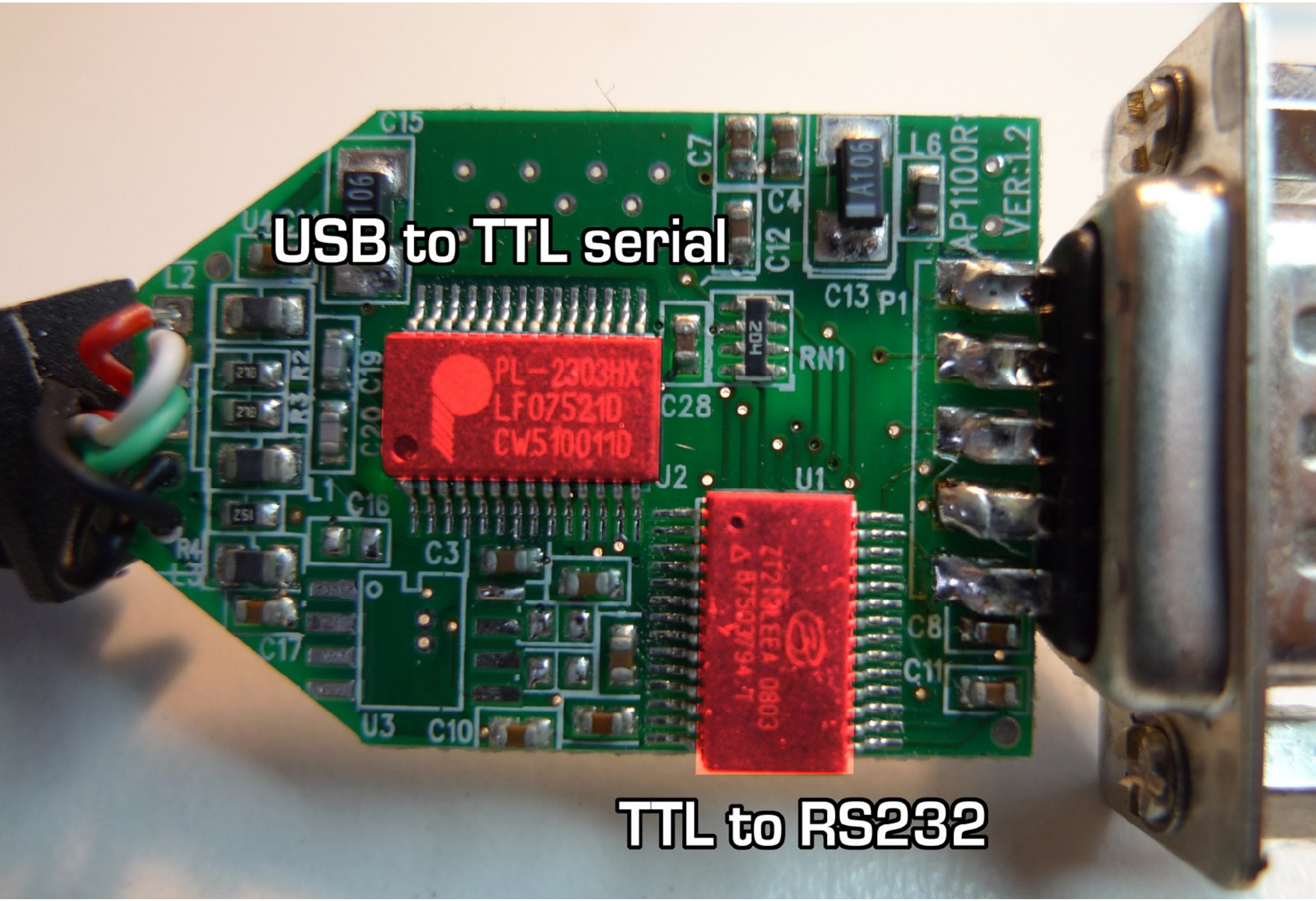

JP1
R50
R106
R109
R98
C2

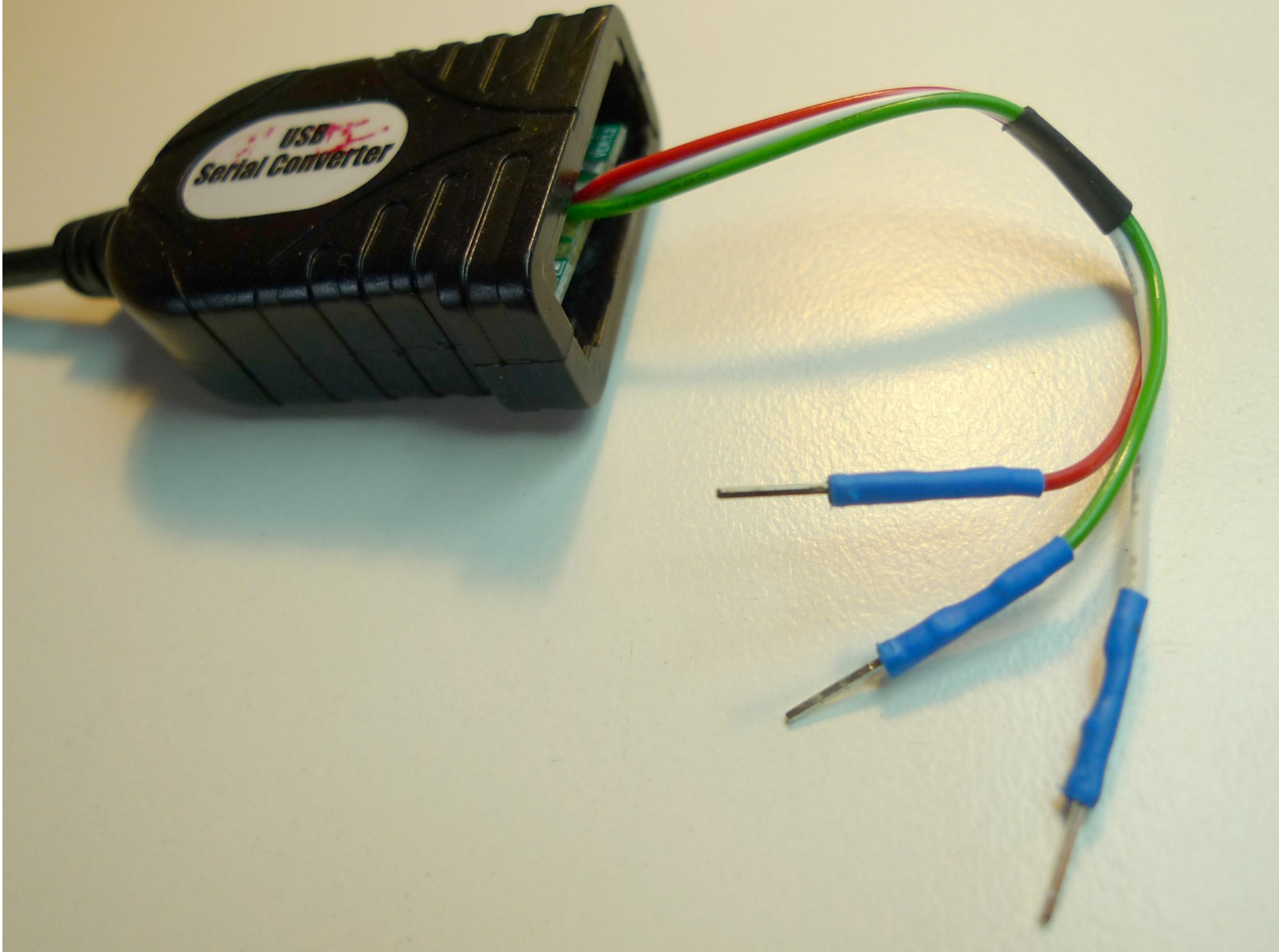

RS-232C
TV ANT IN
LOOP OUT
HDMI


TP1
J1
J2
CR
RT1
RT2
RT3
RT4
RT5
Q1
Q2
CT12
CT3
RT12
CT11
RT21
RT20
J3
RT22
Ext LED
TP3
CT13
GND
U3
CT16
CT14
TP2
GND
LT4
CT21
CT22
RT23
TP4
+1.8V
TP5
+1.0V
RT28
RT29
CT26
CT27
CR11
LT11
RT33
LT16
RT34
LT17
RT30
RT31
LT6
CT17
CT30
RT32
U4
CT24
CT42
TP6
GND
TP7
+3.3V
CT38
CT31
CT32
CT43
CT59
RT36
U6
LT20
CT52
TP8
GND
TP9
+12V
RT37
RT40


Q5861-
18005(P)
FW:R0042
U138
CR191
CR190
R190
R191
J190
R133
C202
C201
E201

Acquire a 'logic level' serial-USB cable


USB to TTL serial
PL-2303HX
LF07521D
CW5100110
TTL to RS232


USB
Serial Converter

Other useful ports:

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

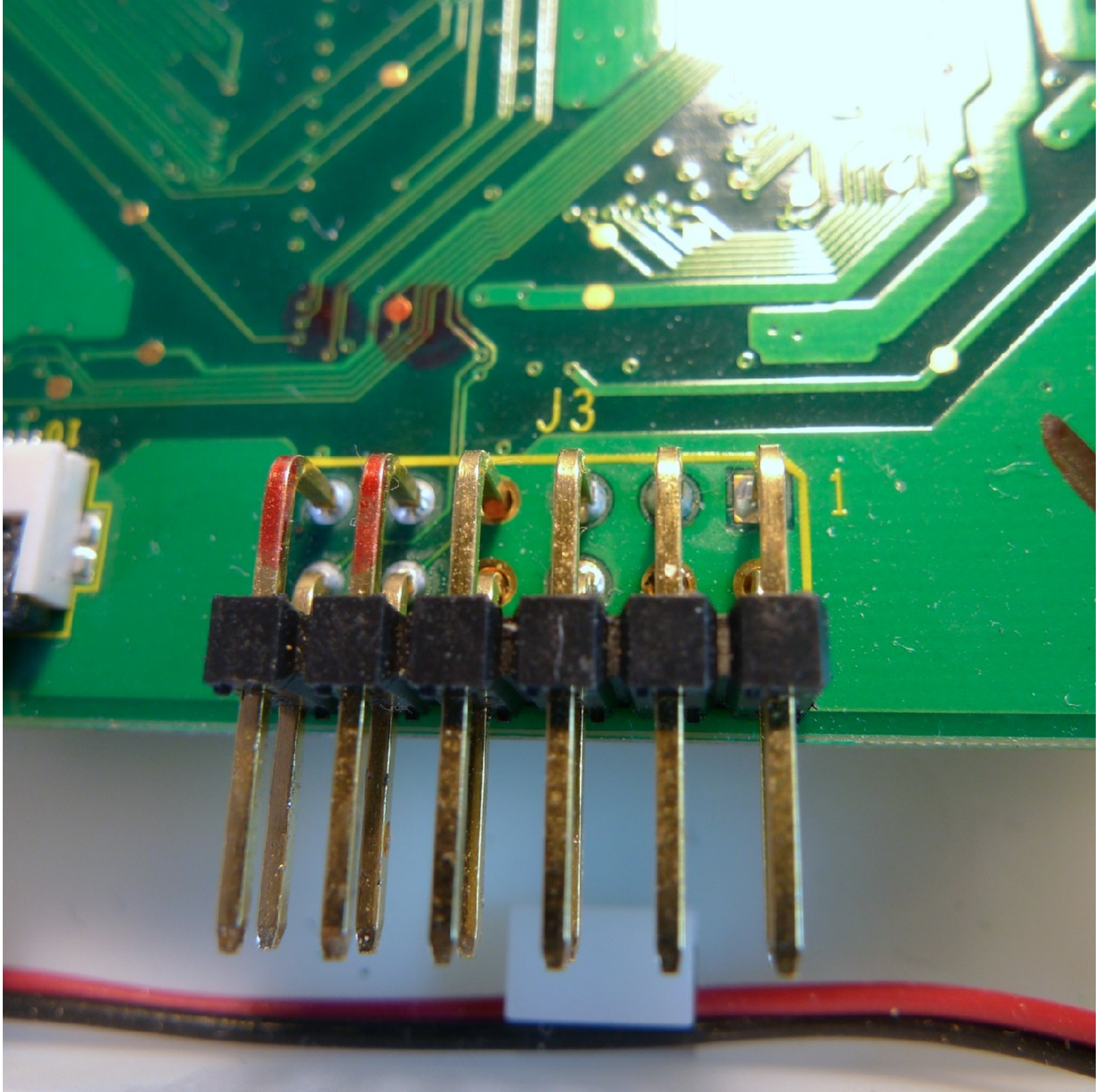
Hacked device example

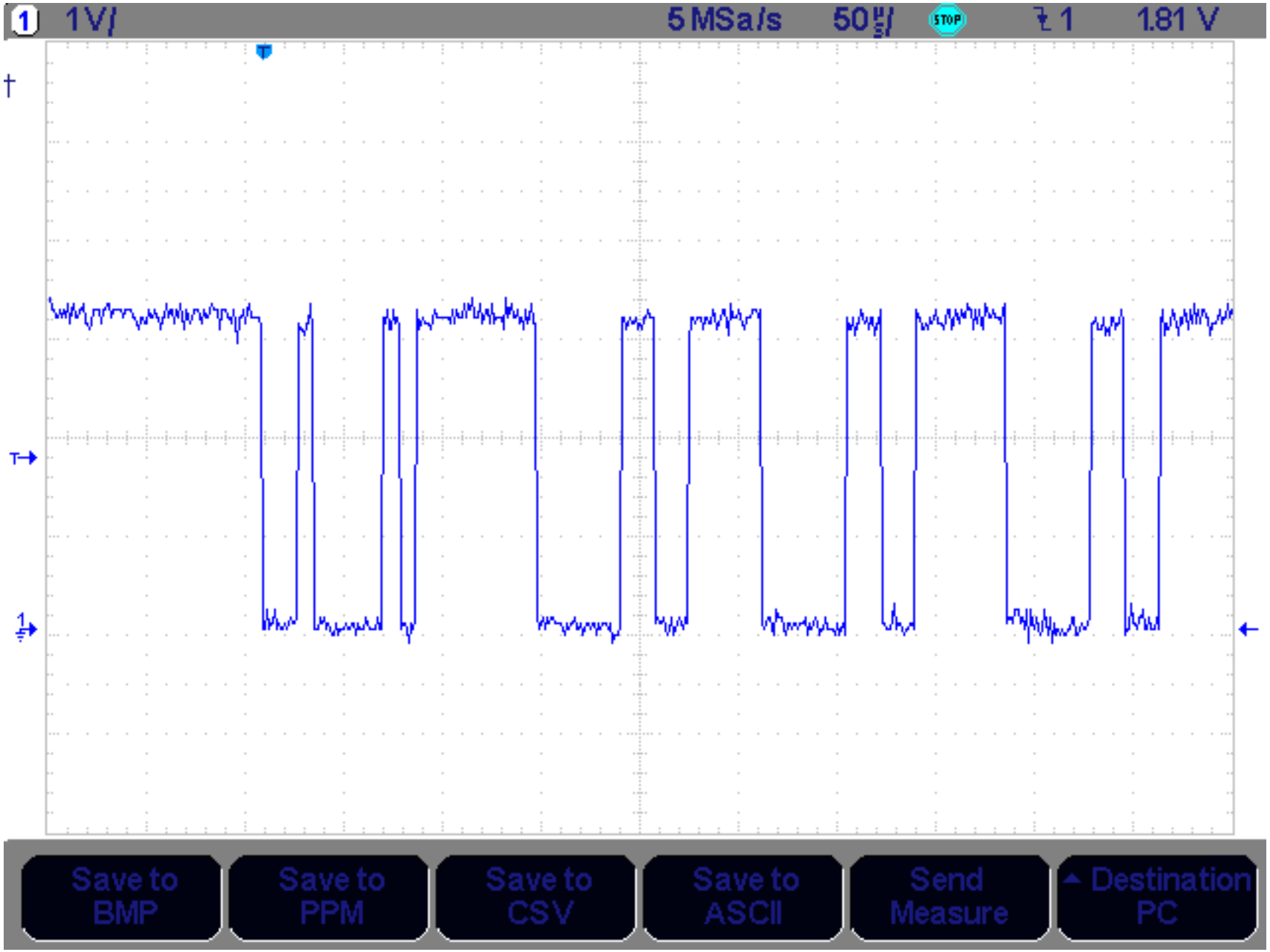
Twirly graphics for a bookshelf


00:21
MON JAN 01

EON
EN29LV320AT-70TCP
16BJ22D
0706KDA
Icatch
SUNPLUS
0638
EtronTech
EM63A165TS-6G
24.576H7C
A709B
MIRAGE
PLOTECH 6
94V-0
E169497

JS7300WMP8B


J3
1


1
1V/
5 MSa/s
50
STOP
1
1.81 V
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       cd          center      clip
custom      del         dir         disp
do          dump        fill        fmt
help        info        mkdir       osmem
ostsk       pan         pause       pb
pbcrop      pbdramplay  pblcdrestore pblcdrot
pblcdstart  pbresize    pbrot       play
read        res         rmdir       search
snap        snapdel     snapenhance snapopt
snapprv     snapqt      snaprgb     snapsize
snapyuv     speed       stillmemdisp thumb
ver         wmacontent  wmaffwd     wmainfo
wmapause    wmaplay     wmaplayall  wmarew
wmastop     write       zoom
```

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");
```

```
==[OnEnterAskingMode 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 8dfffbb0
_

 20:44    51x160   16k    115200 N81
```


Howdy, world

Hacked device example

Building bench equipment

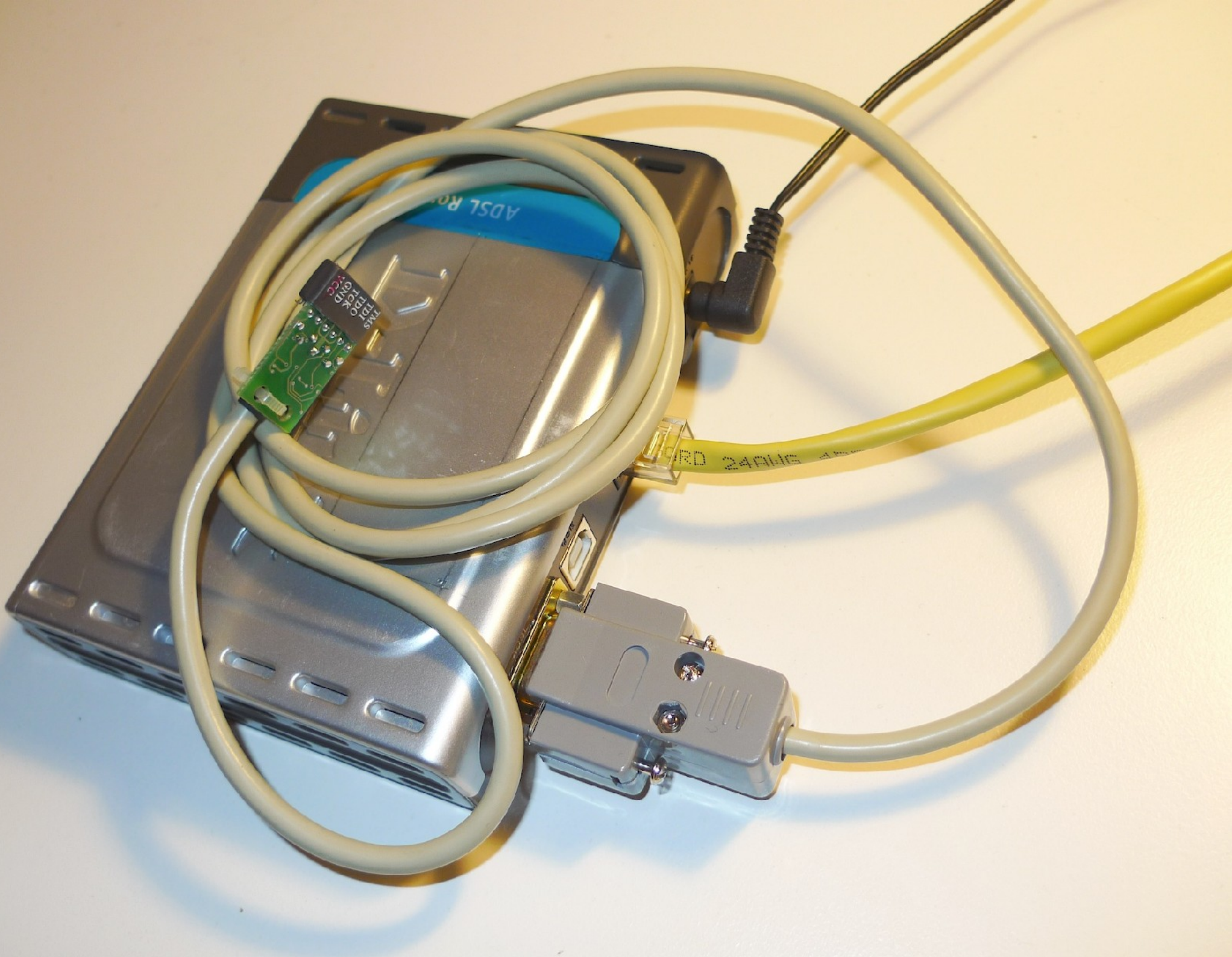

TP-LINK
TL-WR340G
54M Wireless Router
PWR SYS WLAN WAN 1 2 3 4
DSL
Reset
USB
Ethernet
12VDC

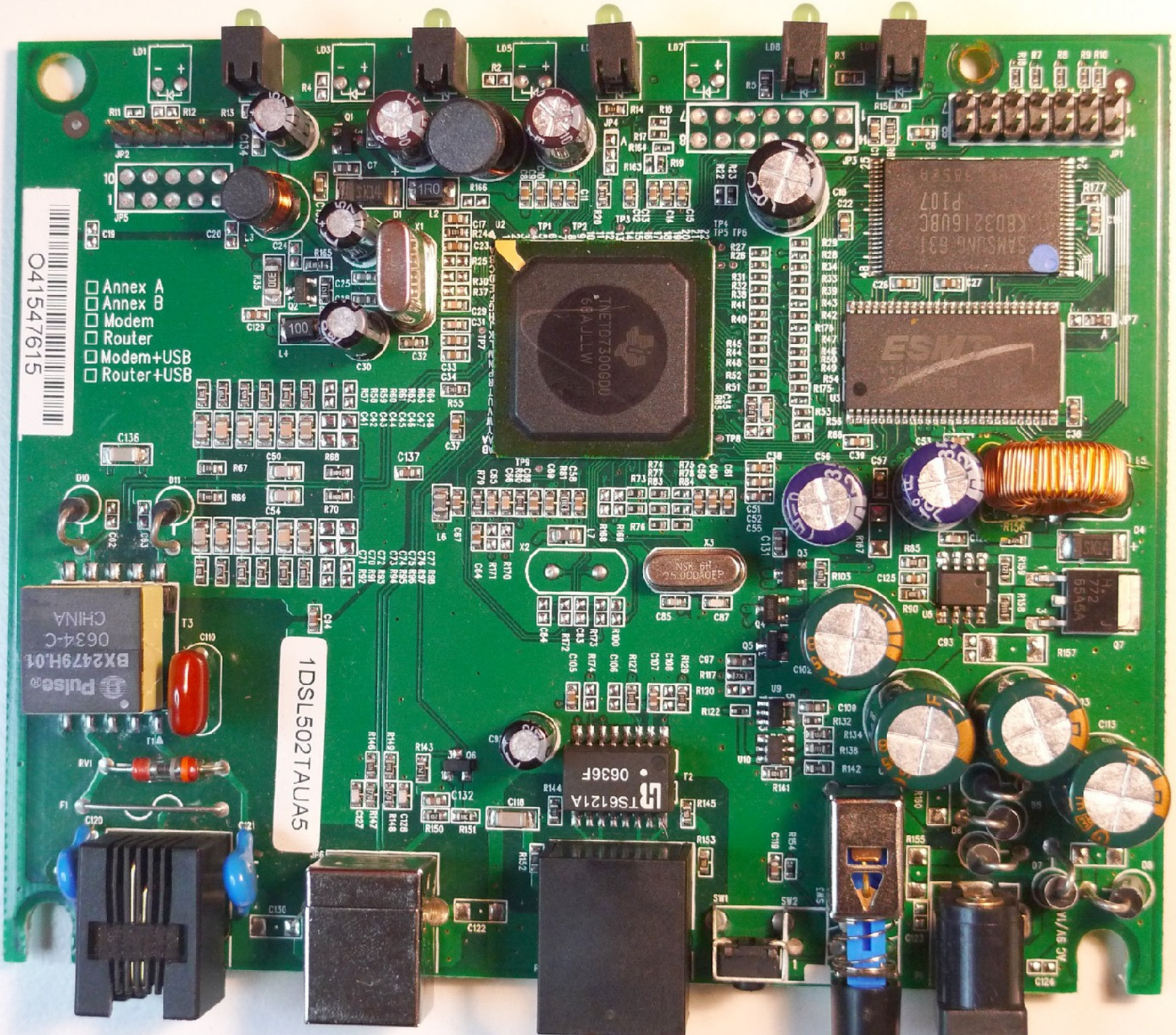
I <3 OpenWRT

Fun WiFi/ADSL box hacks:

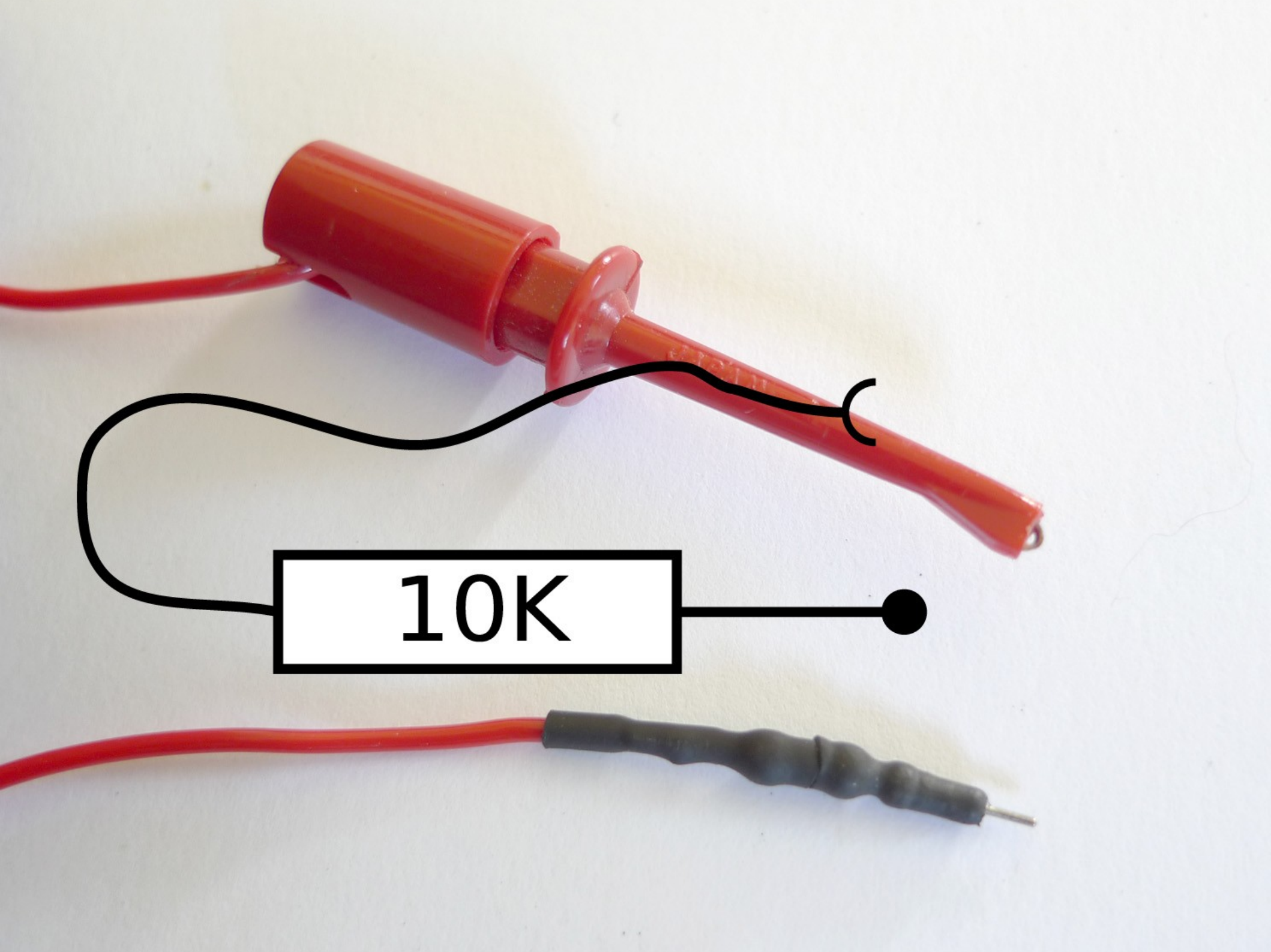
- Espresso machine heater PID controller
- Streaming mp3 radios
- R/C cars with streaming video


ADSL Router
Power Status
ADSL
Link/Act
Ethernet
Link/Act
USB
Link/Act
DSL-502T

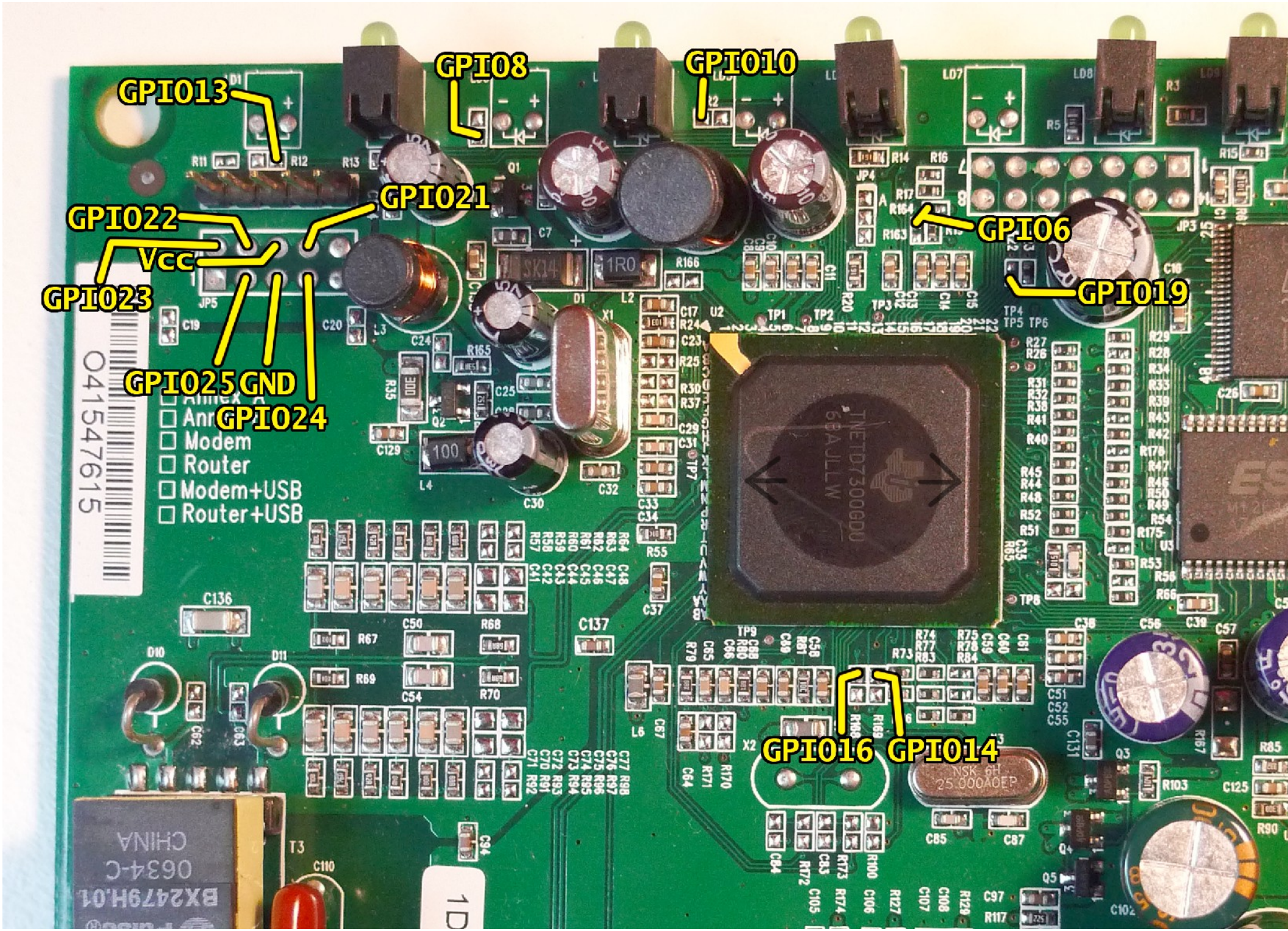

TMS
TDI
TDO
TCK
GND
VCC

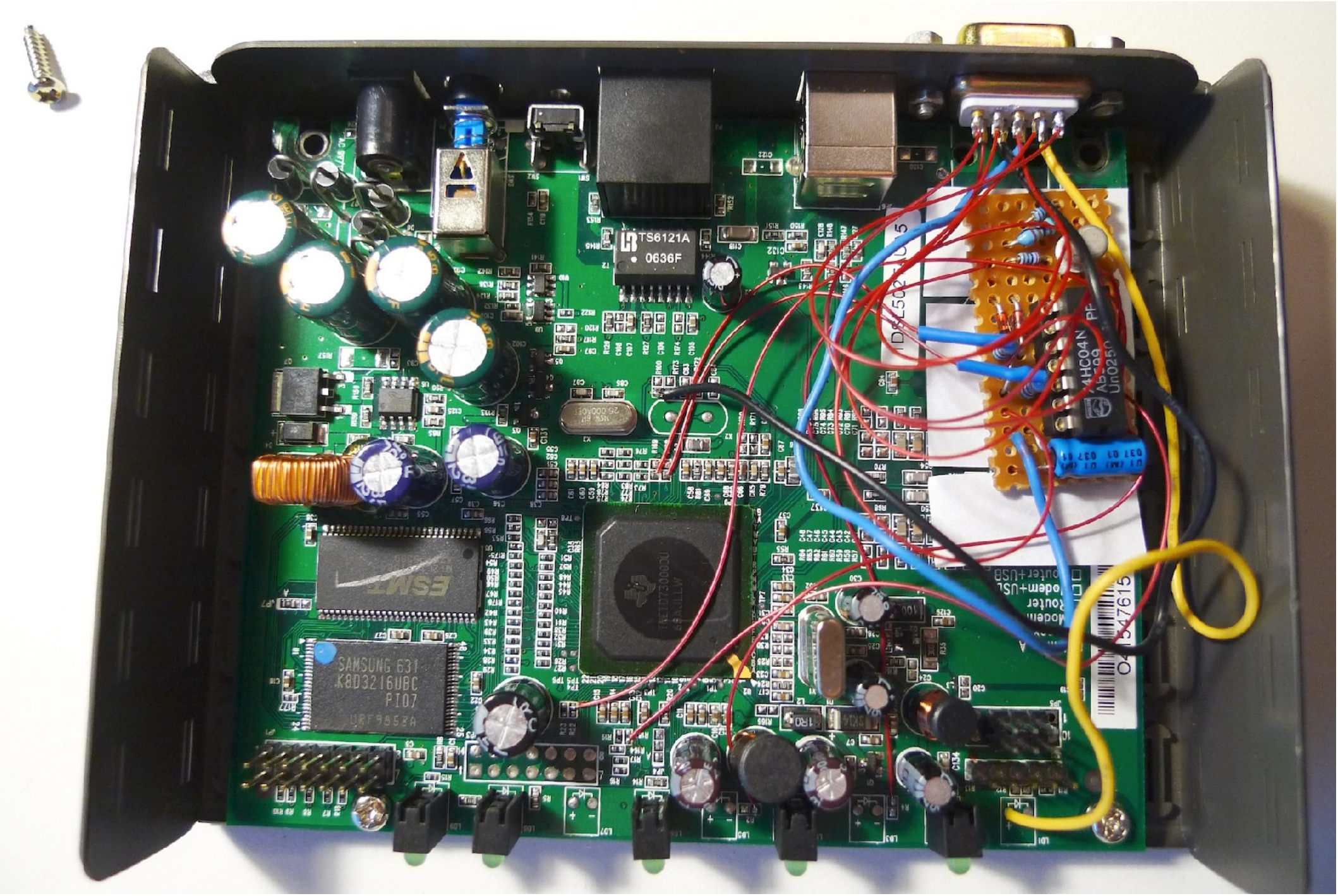

O41547615
Annex A
Annex B
Modem
Router
Modem+USB
Router+USB
1DSL502TAUA5
TNETD7300GDU
TS6121A
NSK 6H
25.000AOEP
BX2479H.01
CHINA

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;
}
```


GPIO13
GPIO8
GPIO10
GPIO22
GPIO21
Vcc
GPIO6
GPIO23
GPIO19
GPIO25
GND
GPIO24
Modem
Router
Modem+USB
Router+USB
GPIO16
GPIO14
O41547615
TNETD7300GDU
NSK 6H
25.000AOEP


TS6121A
0636F
SAMSUNG 631
K8D3216UBC
PI07
74HC04N

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

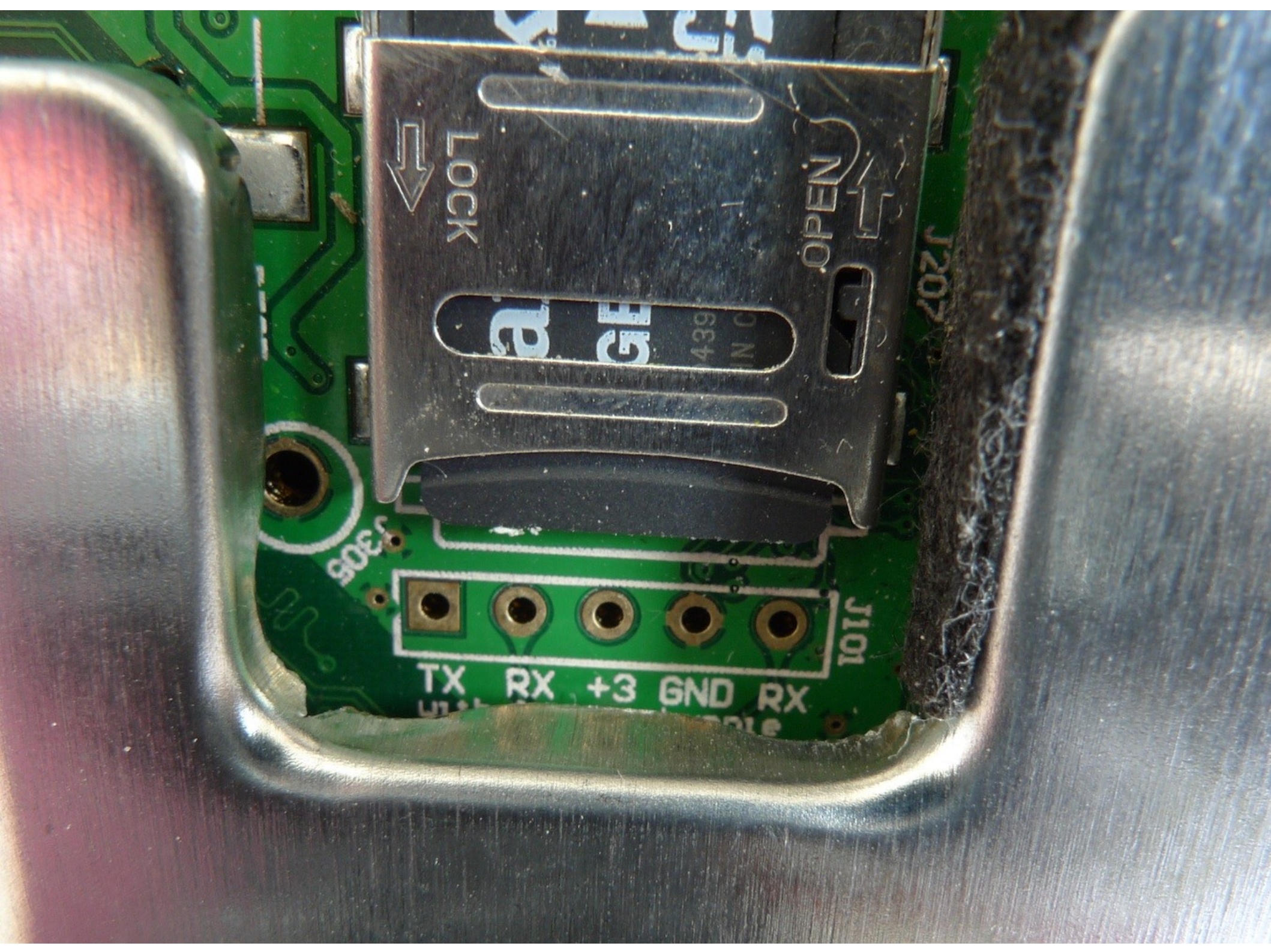
Open design:

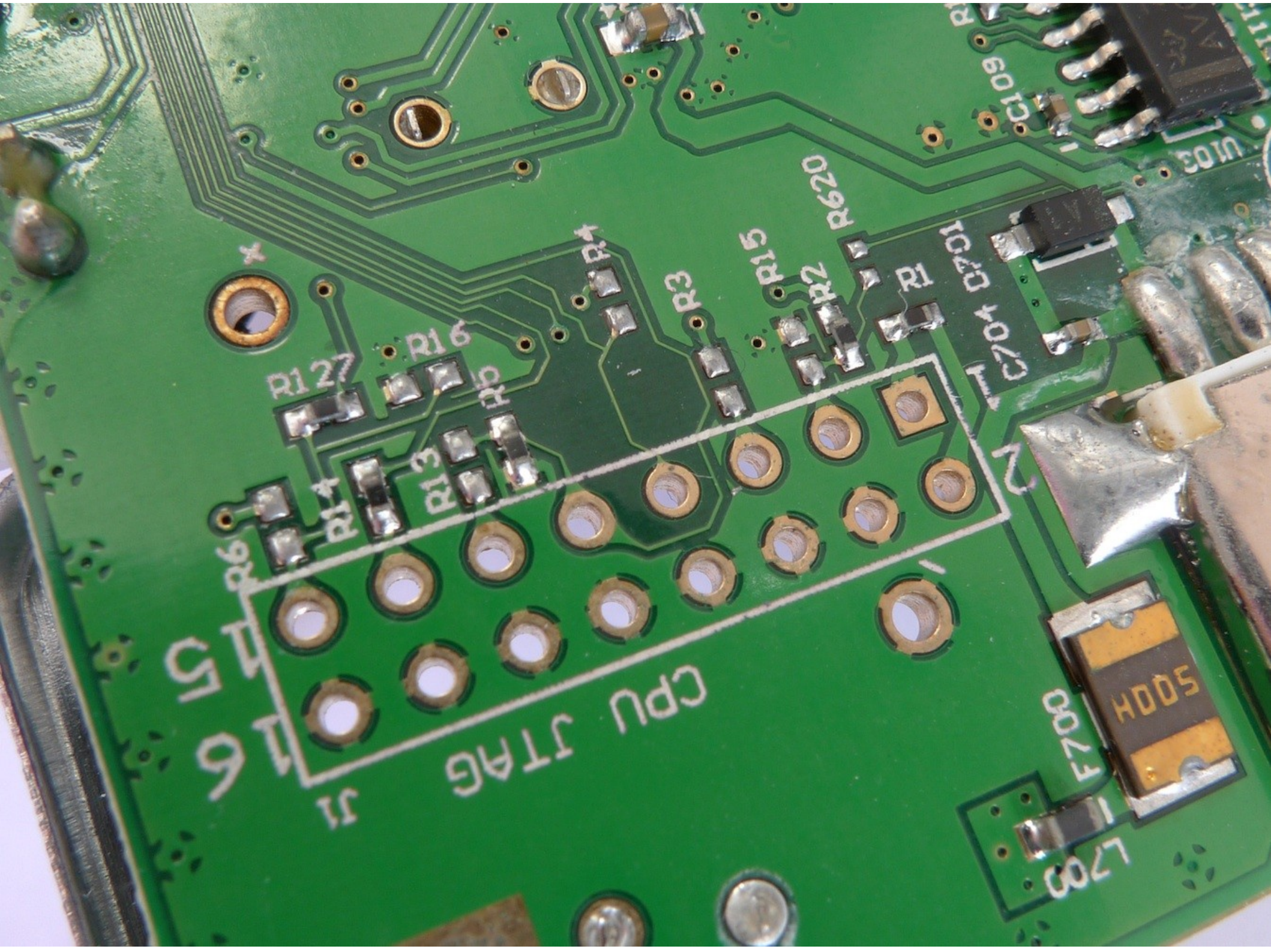
- PCB
- Schematics
- Firmware

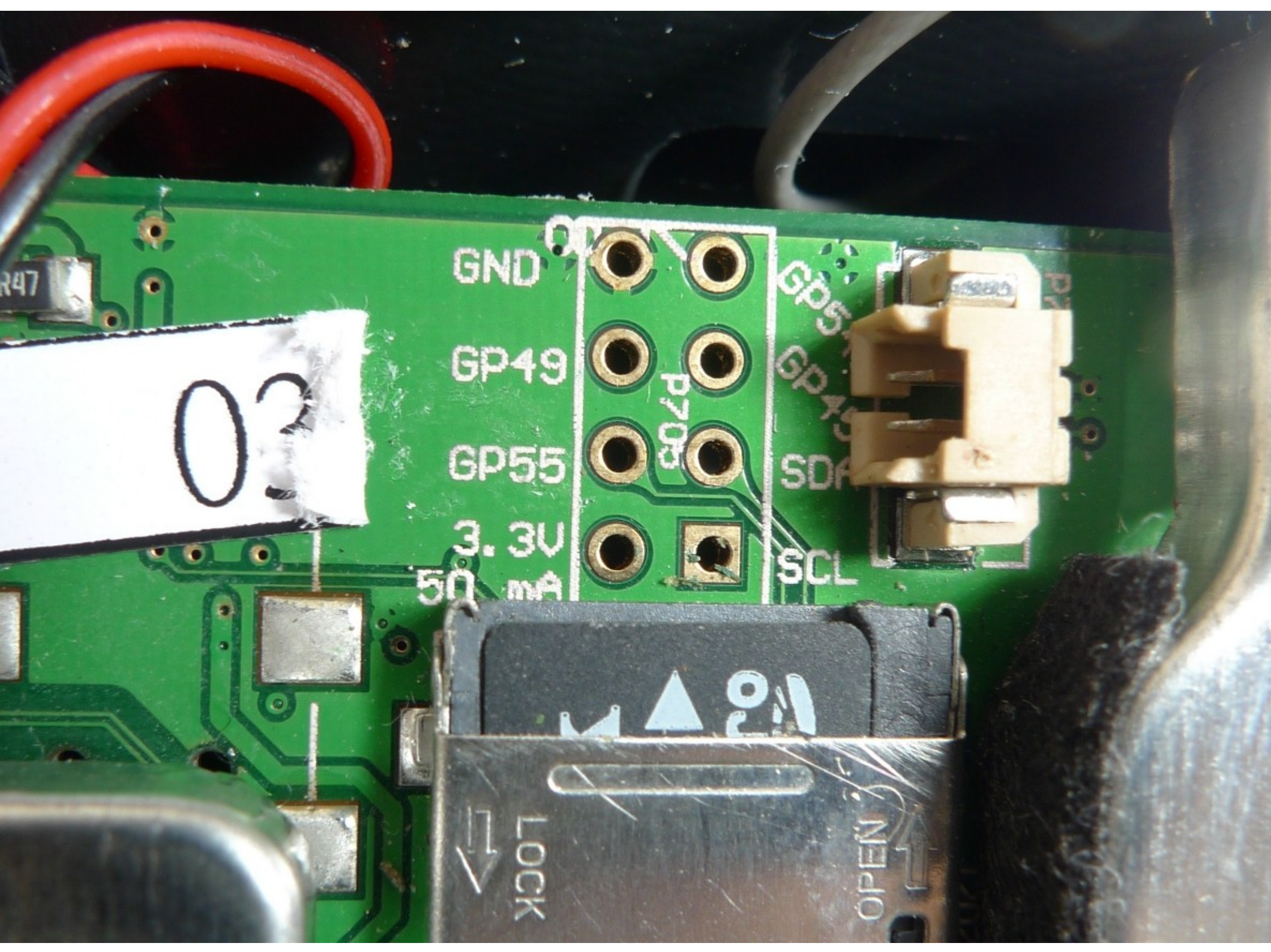
DEMO

Viewable at:
http://youtu.be/azE5-3fAjUs

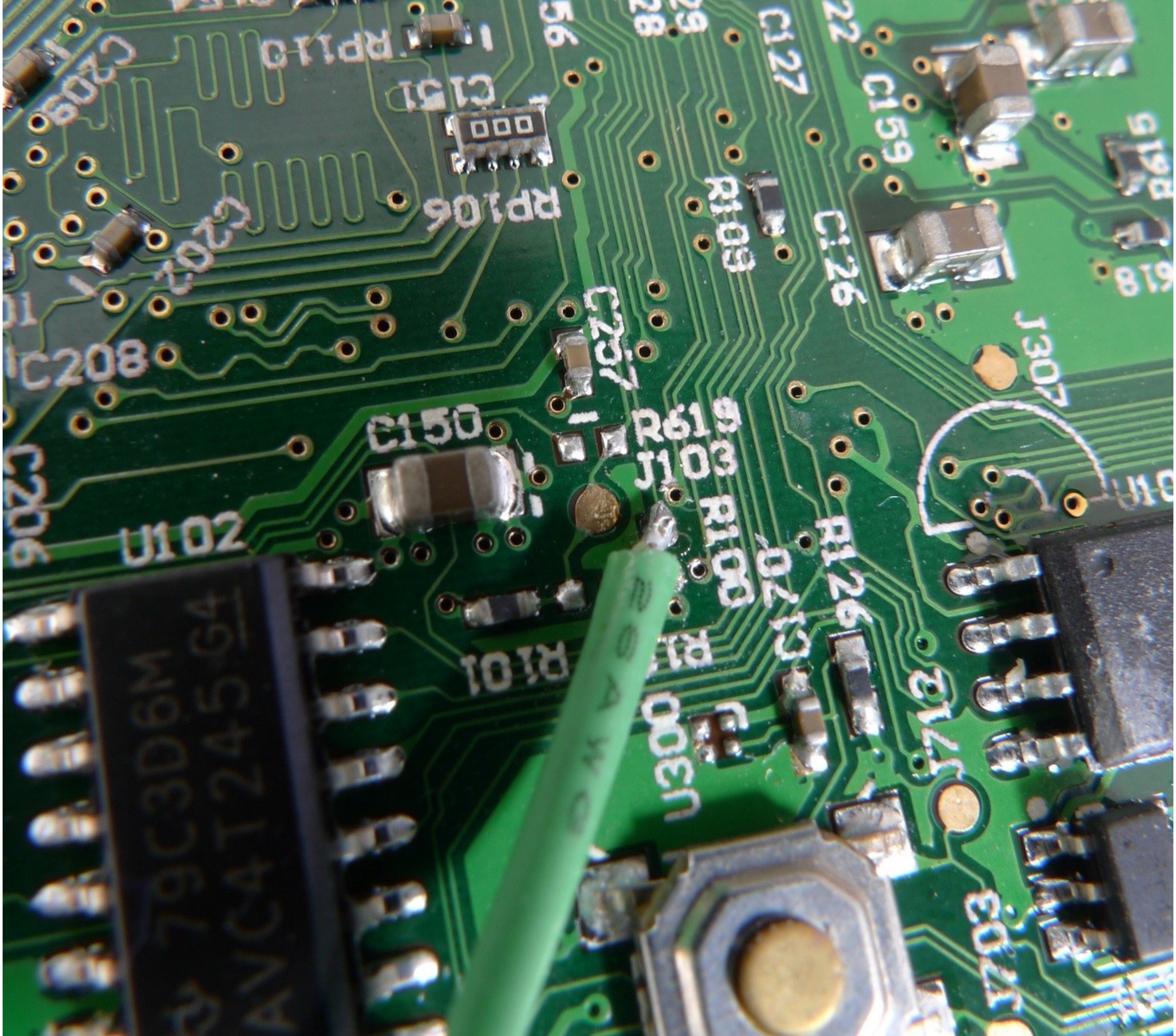

EASY OPEN EASY OPEN
tomatoes in tomato juice.
ITALIAN
Blueberry
yoplait


LOCK
OPEN
J207
J305
J101
TX RX +3 GND RX


CPU JTAG J1
R127
R16
R14
R13
R6
R4
R3
R15
R22
R620
R1
C704
C701
C109
U03
L700
F708
HDD5


GND
GP49
GP55
3.3V
50 mA
SDA
SCL
LOCK
OPEN
03

500H
F701
L702
P701
P702
3.3V
USER
GND

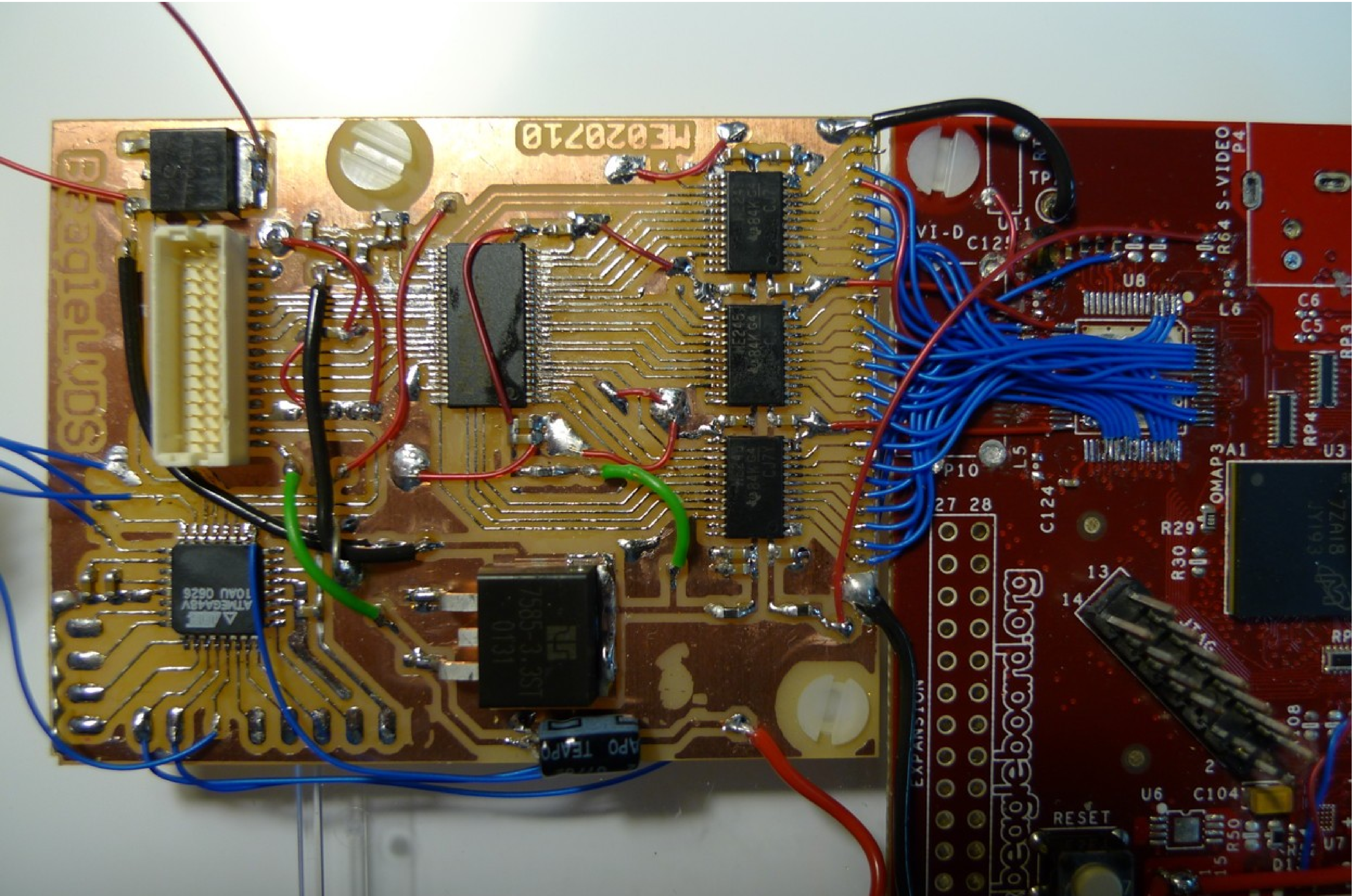


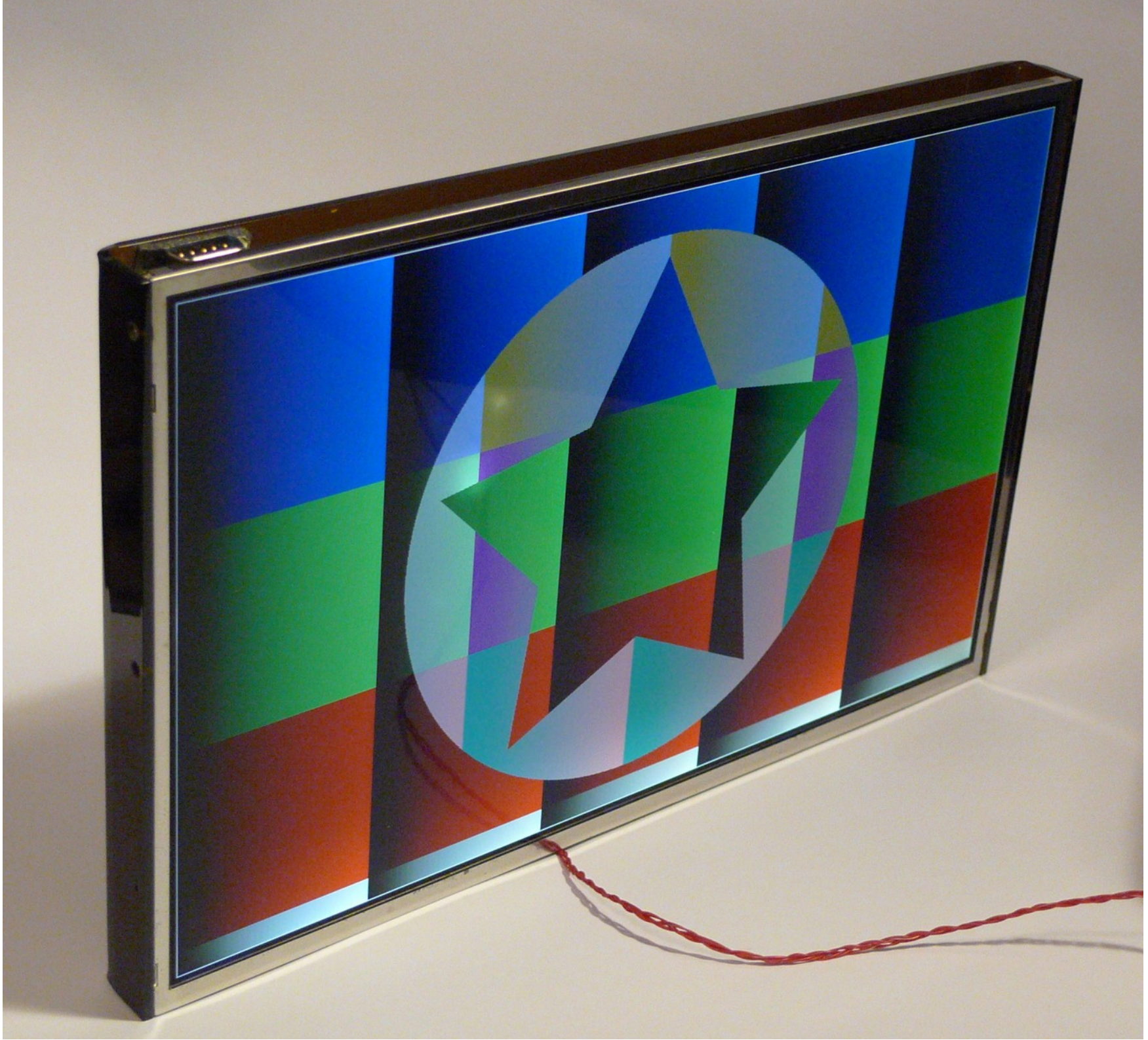
RP110
C151
RP106
C209
C202
C208
C127
C159
R109
C126
J307
C257
R619
J103
C150
U102
R101
R126
U300

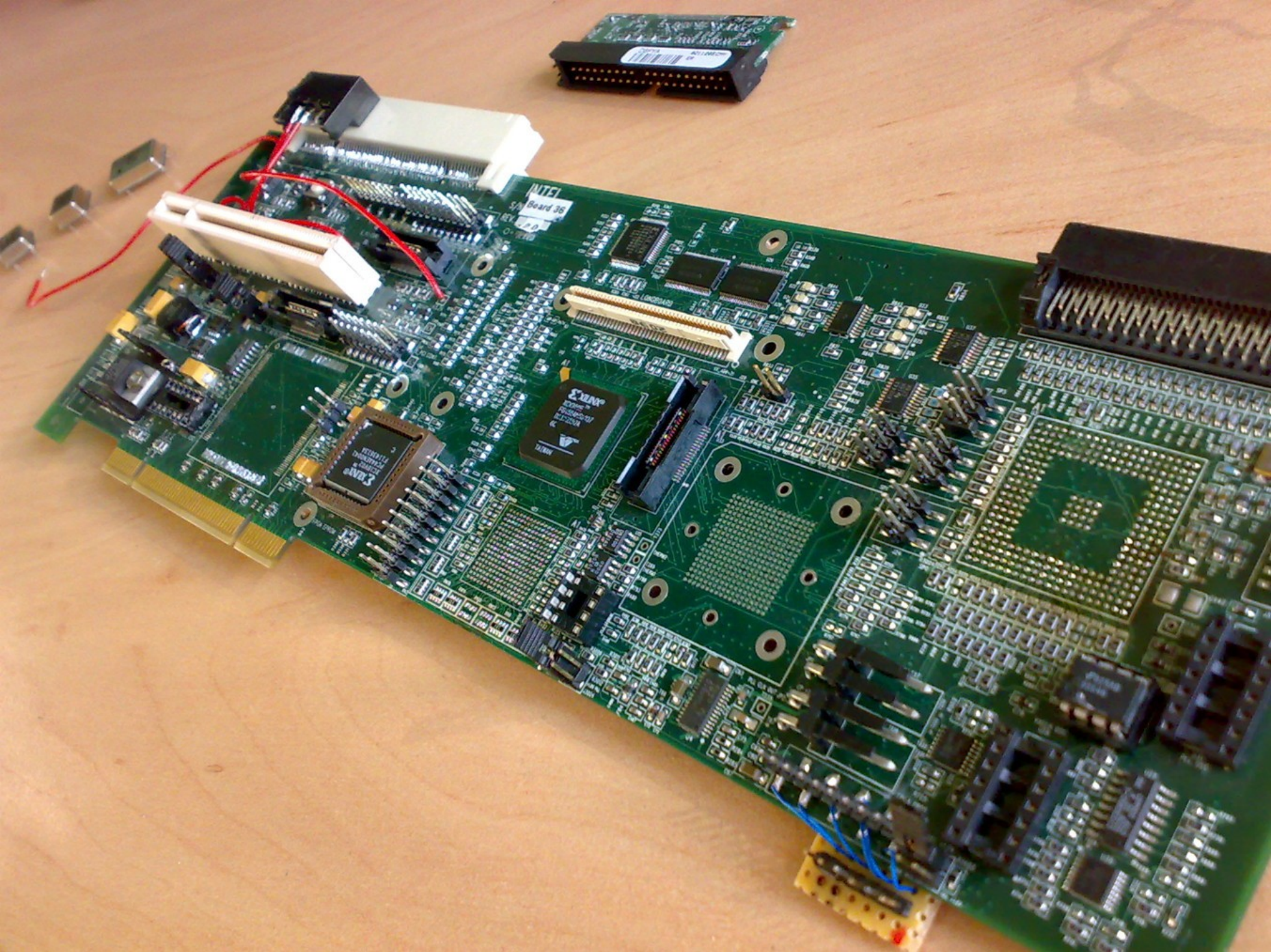
```
# Ugly pin multiplexer config, timer and PWM
# init:

./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
```

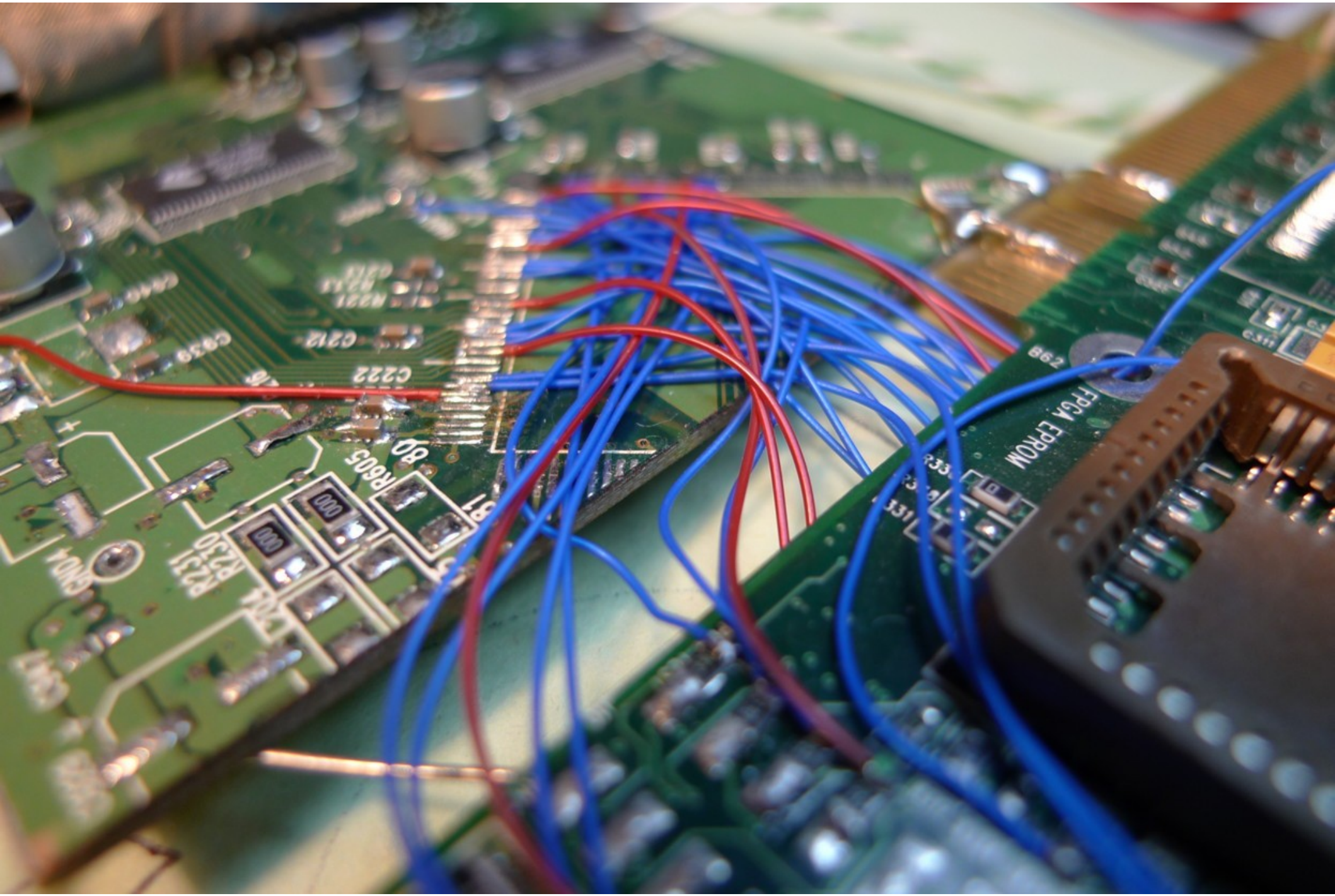
Other Examples

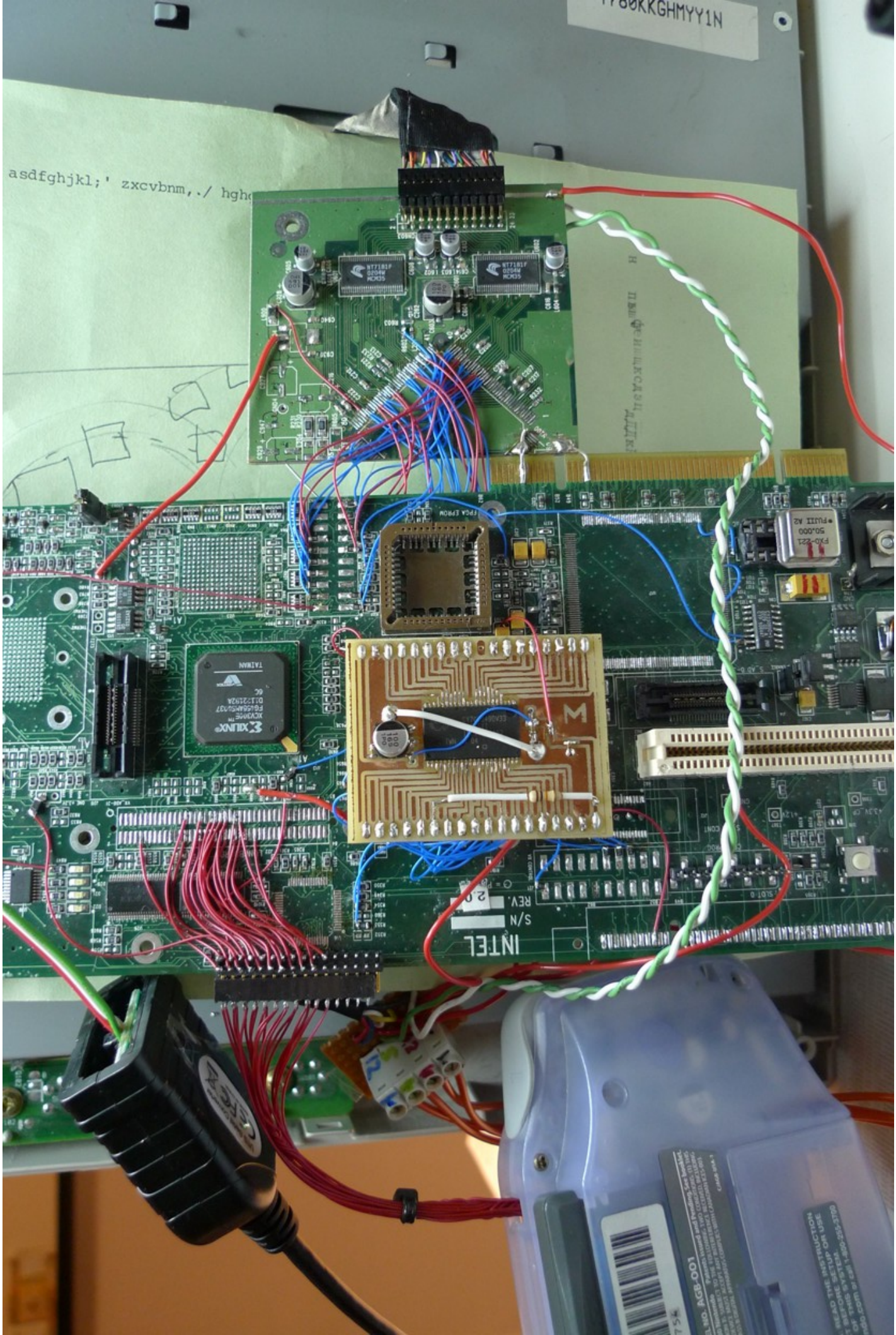

1-962-761-11
beagleboard.org
crucial
128 MB
LTD133EX2X
MADE IN JAPAN
Toshiba Matsushita Display Technology Co.,Ltd.


S-VIDEO
OMAP3
beagleboard.org
EXPANSION
RESET
JTAG




Board 38


FPGA EPROM


asdfghjkl;' zxcvbnm,./ hgh
INTEL
XILINX

METROID™

1PLAYER 2PLAYER

©1989 Nintendo

iiyama

AUTO MENU

GAME BOY ADVANCE


MARIO KART
SUPER CIRCUIT
SINGLE PLAYER
©1992,2001 Nintendo
iiyama

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/gambiologia.php

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