Flash dump(l)ing 101

(You can thank my boyfriend for this joke)

$USER

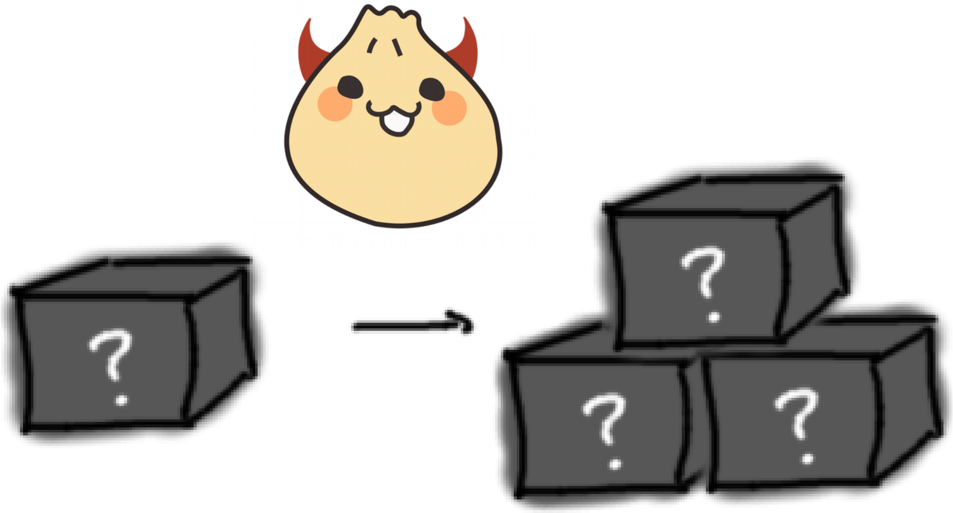
- **Security researcher at Quarkslab (Paris)**
  SECURING EVERY BIT OF YOUR DATA
- **Love**
  - (de)soldering stuff
  - hardware attacks

- **R&D project with:**
  - Philippe Teuwen (@doegox)
  - Guillaume Heilles (@PapaZours)

The magic box

- Box provides a service
- Users pay for that service

→ What if the box can be duplicated ?

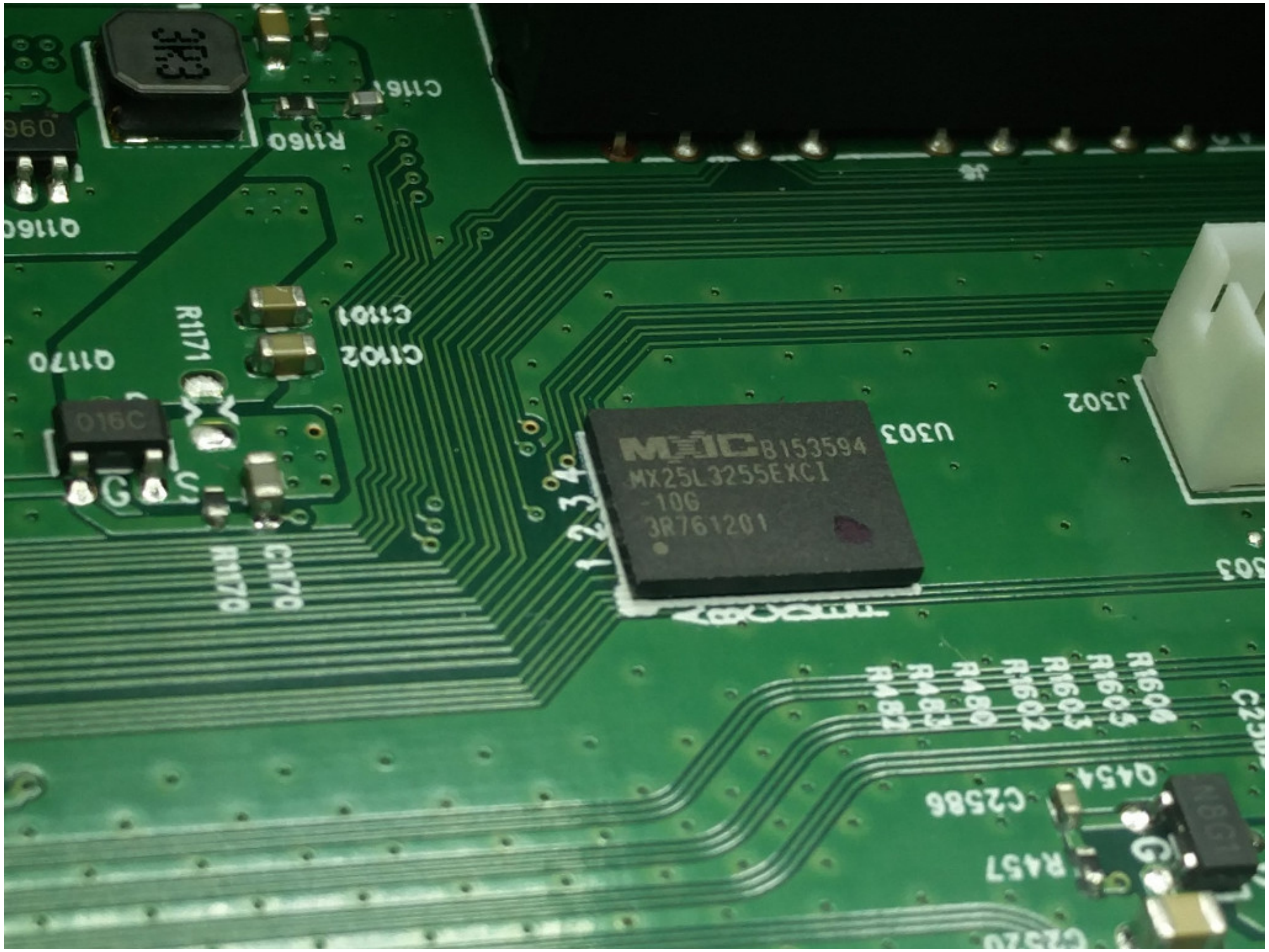


Opening up the black box

- **The easy part**
  - No proprietary screws
  - No fuse
  - No sensor

- **No picture of the black box or its PCB**
- **Here is a cute dumpling instead**

Inside the black box



Battleplan to attack the magic box

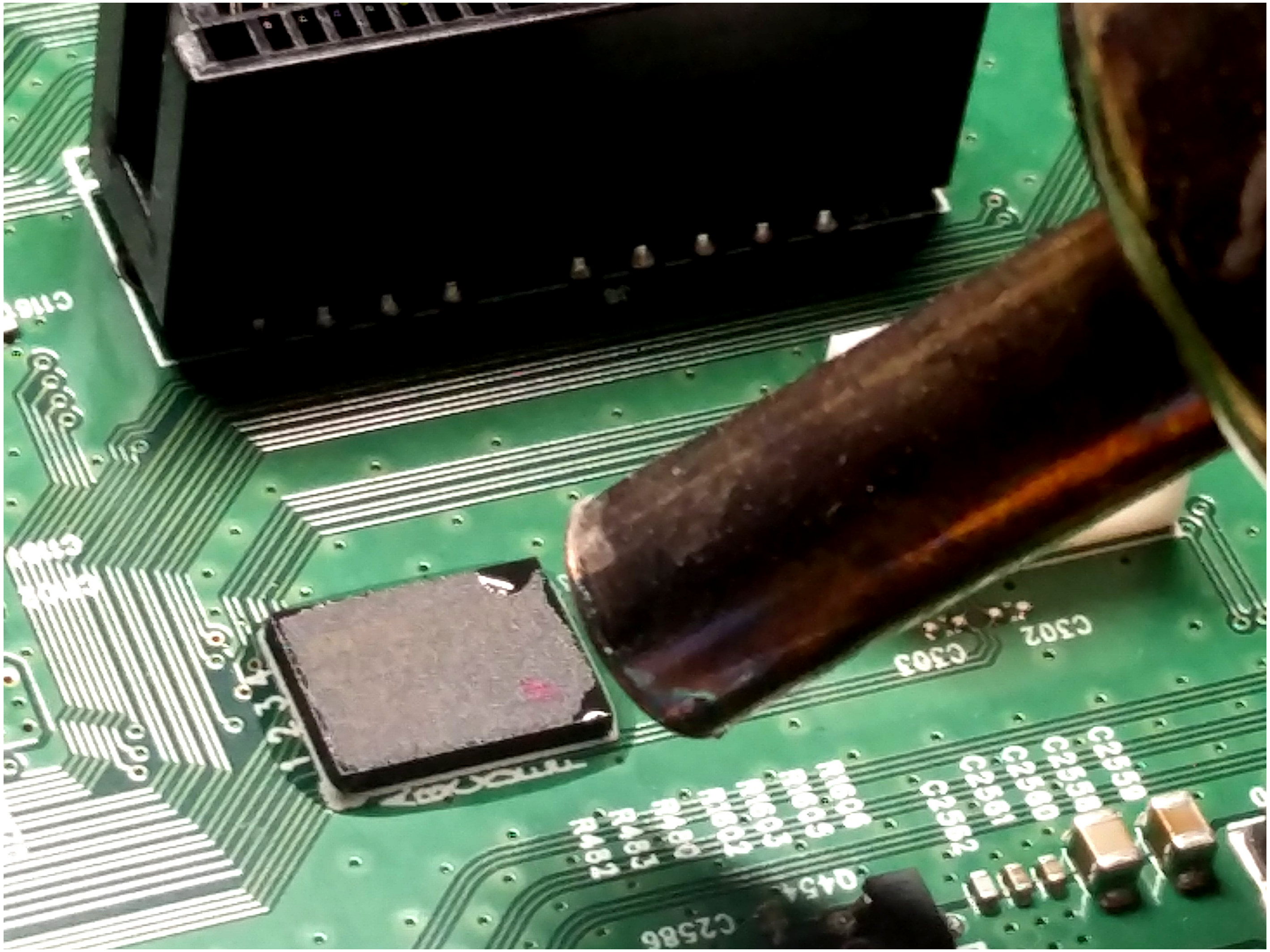
→ Target the flash chip which contains the firmware

1) Extract the flash chip from the board
2) Design a breakout PCB adapted to the chip
3) Craft the breakout PCB
4) Microsolder the chip to the breakout board
5) Make the chip talk! Dump it/reprogram it!

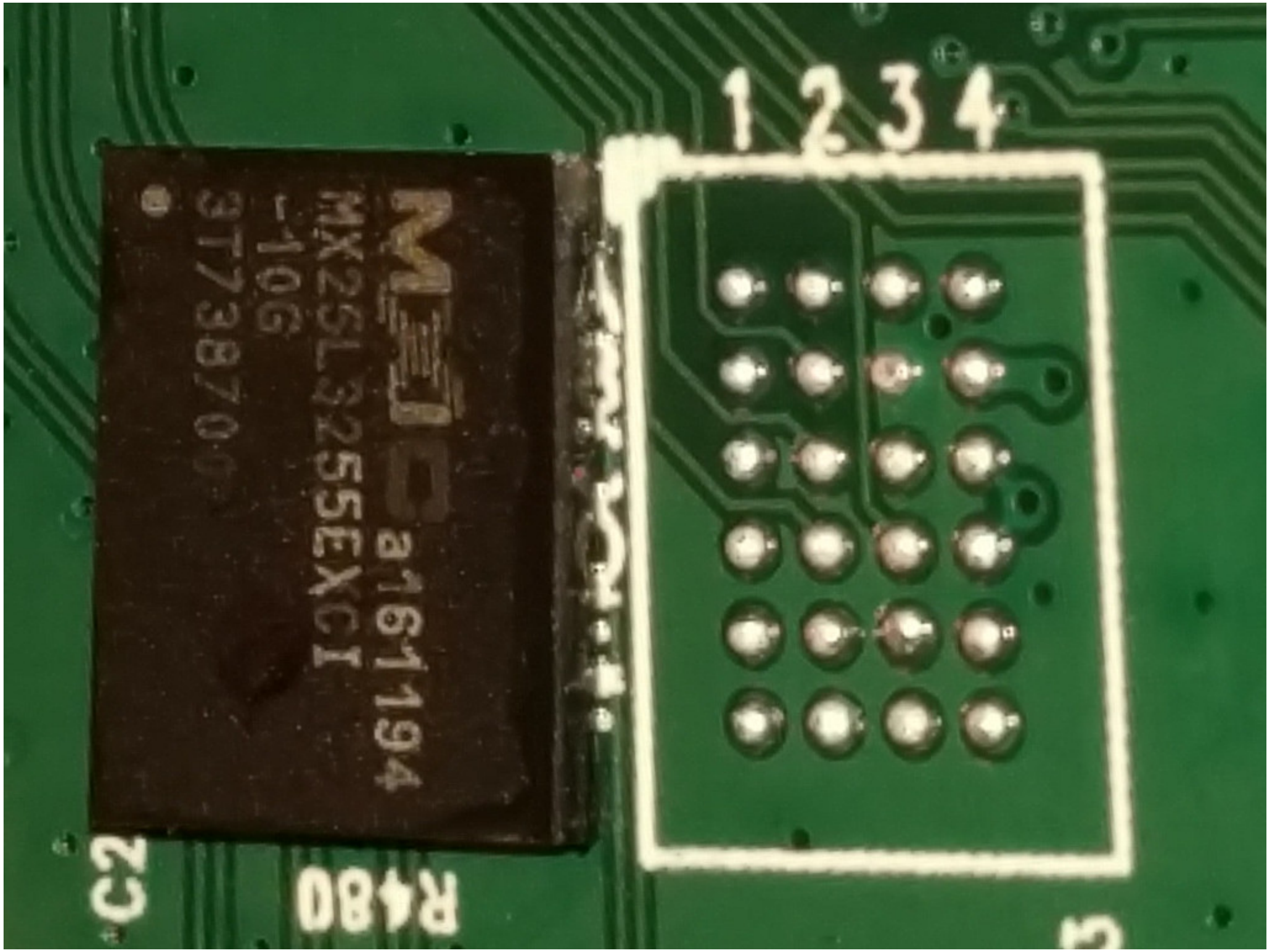
Step 1: Extracting the flash chip

http://www.aoyue.eu/aoyue-int860-smd-rework-station-hot-air-soldering-station.html

Step 1: Extracting the flash chip



Desoldered Flash



Step 2: Design a breakout board

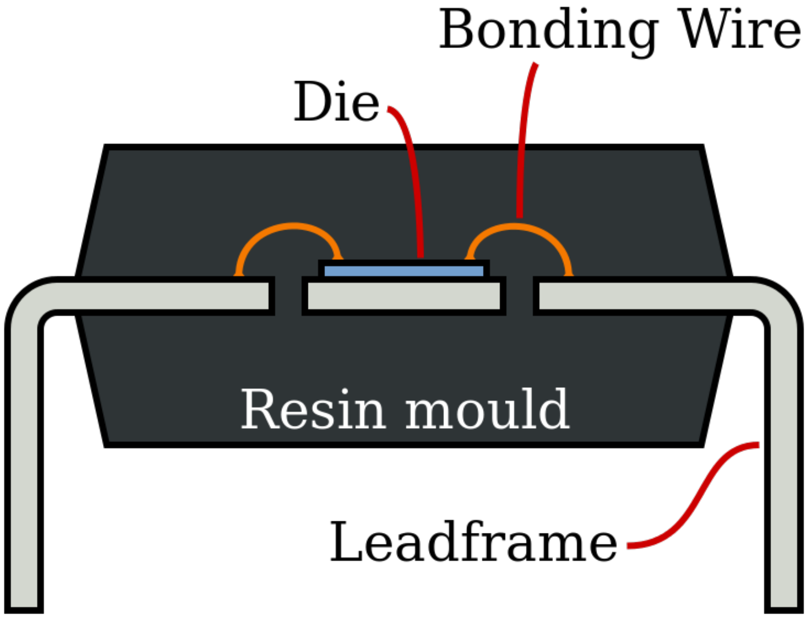
- **Breakout board gives an easy access to each pin of the chip**
- **Translate one type of chip package to another**

→ Need more information on the chip

- What is the source chip package ?
- What is the target chip package ?
- What are the useful pins of the chip ?

Chip packages?

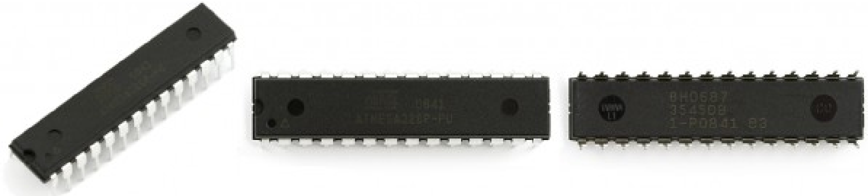
Chip packages



https://en.wikipedia.org/wiki/File:DIP_Cross-section.svg

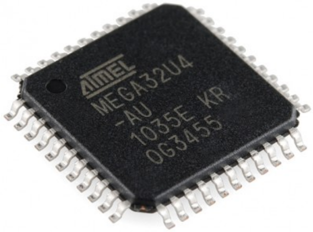
Chip packages

- Dual In-Line Package (DIP)

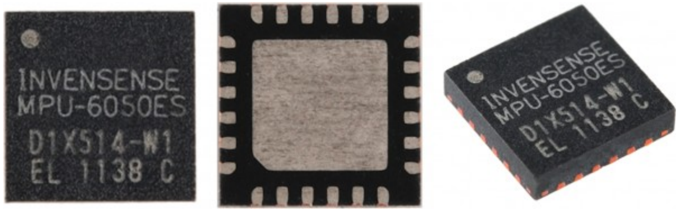


- Small Outline Package (SOP)

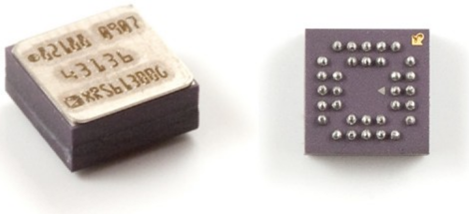
- Quad Flat Package (QFP)



- Leadless Chip Carrier (LCC)



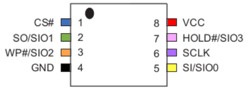
- Ball Grid Array (BGA)



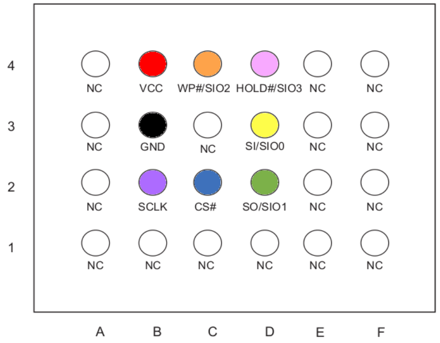
Pins of the breakout board

3. PIN CONFIGURATION

8-PIN SOP (200mil)

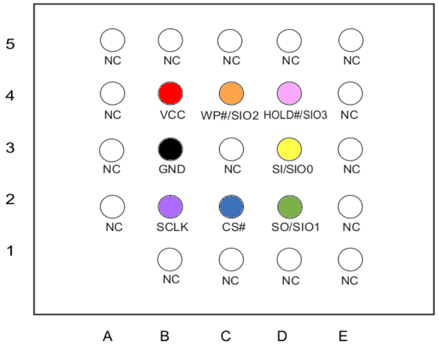


24-Ball TFBGA (6x8 mm, 4x6 Ball Array)



	A	B	C	D	E	F
4	NC	VCC	WP#/SIO2	HOLD#/SIO3	NC	NC
3	NC	GND	NC	SI/SIO0	NC	NC
2	NC	SCLK	CS#	SO/SIO1	NC	NC
1	NC	NC	NC	NC	NC	NC

24-Ball TFBGA (6x8 mm, 5x5 Ball Array)



	A	B	C	D	E
5	NC	NC	NC	NC	NC
4	NC	VCC	WP#/SIO2	HOLD#/SIO3	NC
3	NC	GND	NC	SI/SIO0	NC
2	NC	SCLK	CS#	SO/SIO1	NC
1		NC	NC	NC	NC

4. PIN DESCRIPTION

SYMBOL	DESCRIPTION
CS#	Chip Select
SI/SIO0	Serial Data Input (for 1xI/O)/ Serial Data Input & Output (for 2xI/O or 4xI/O mode)
SO/SIO1	Serial Data Output (for 1xI/O)/Serial Data Input & Output (for 2xI/O or 4xI/O mode)
SCLK	Clock Input
WP#/SIO2	Write protection: connect to GND or Serial Data Input & Output (for 4xI/O mode)
HOLD#/ SIO3	To pause the device without deselecting the device or Serial data Input/Output for 4 x I/O mode
VCC	+ 3.0V Power Supply
GND	Ground
NC	No Connection

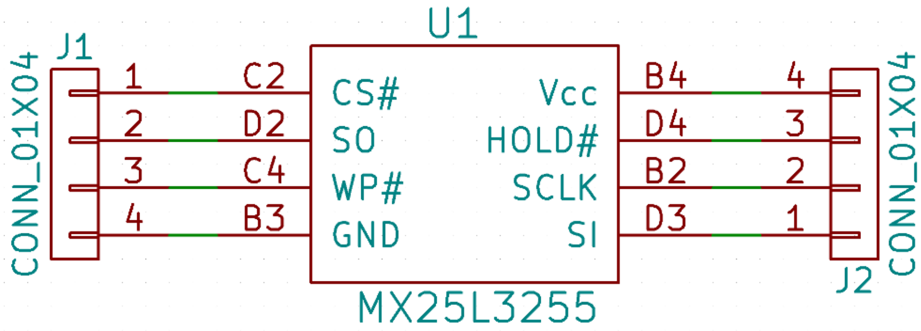
Note:
1. The HOLD# pin is internal pull high.

- Translate BGA to DIP8
- Expose only the 8 pins used

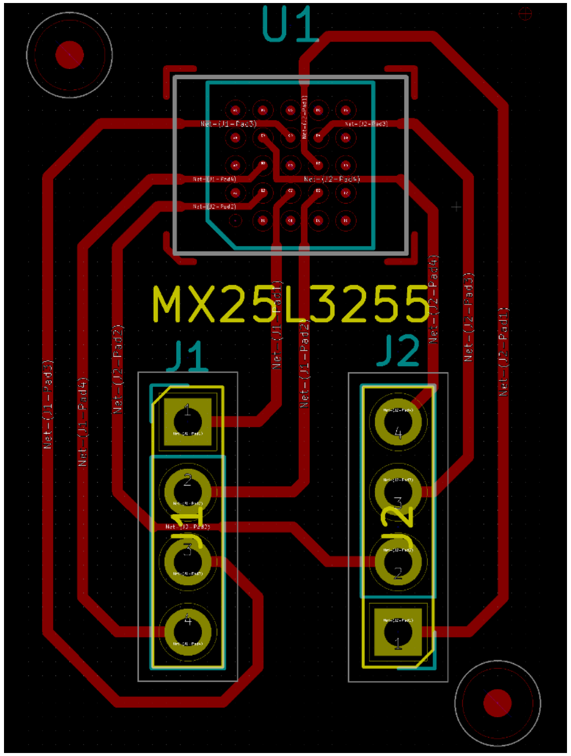
Actual PCB Design

- **PCB design with KiCad**

  1) create an electronic schematic

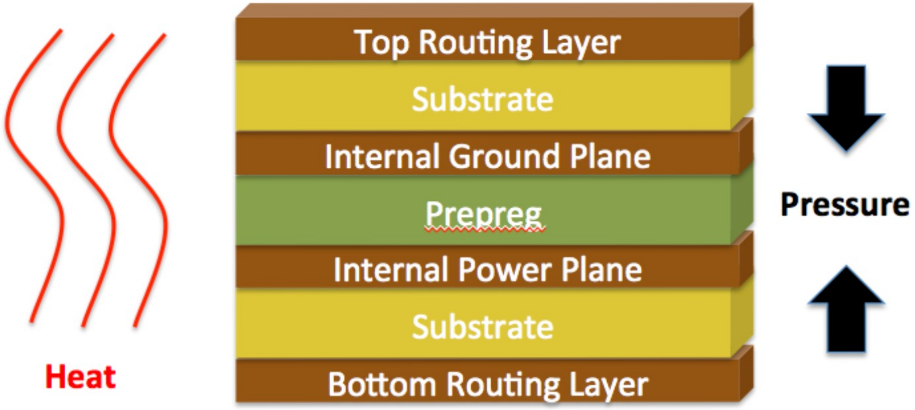


  2) Create the footprint of the flash chip

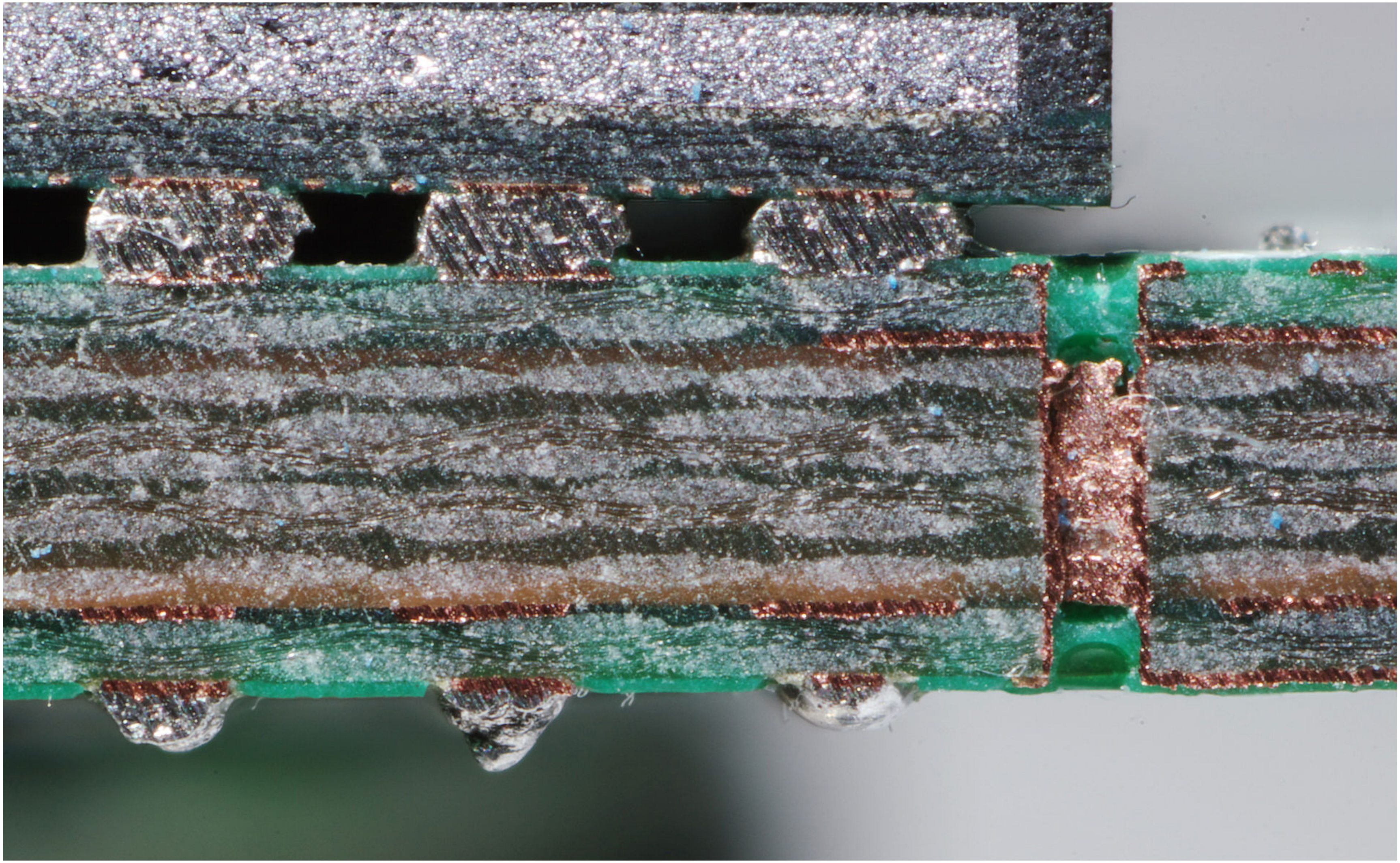


Step 3 : Craft a breakout PCB

- **PCB 101**
  - It’s a sandwich
  - Substrate, non-conductive layer, FR4 (epoxy + fiberglass)
  - Conductive layer: copper
  - Soldermask on top



PCB sandwich

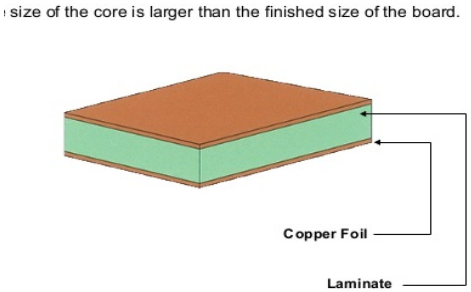


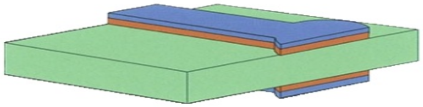
PCB fabrication

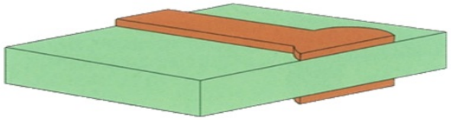
- **We tried 2 different techniques:**
  - Etching which uses chemical component
  - Milling which uses mechanical drilling bit

PCB fabrication by etching

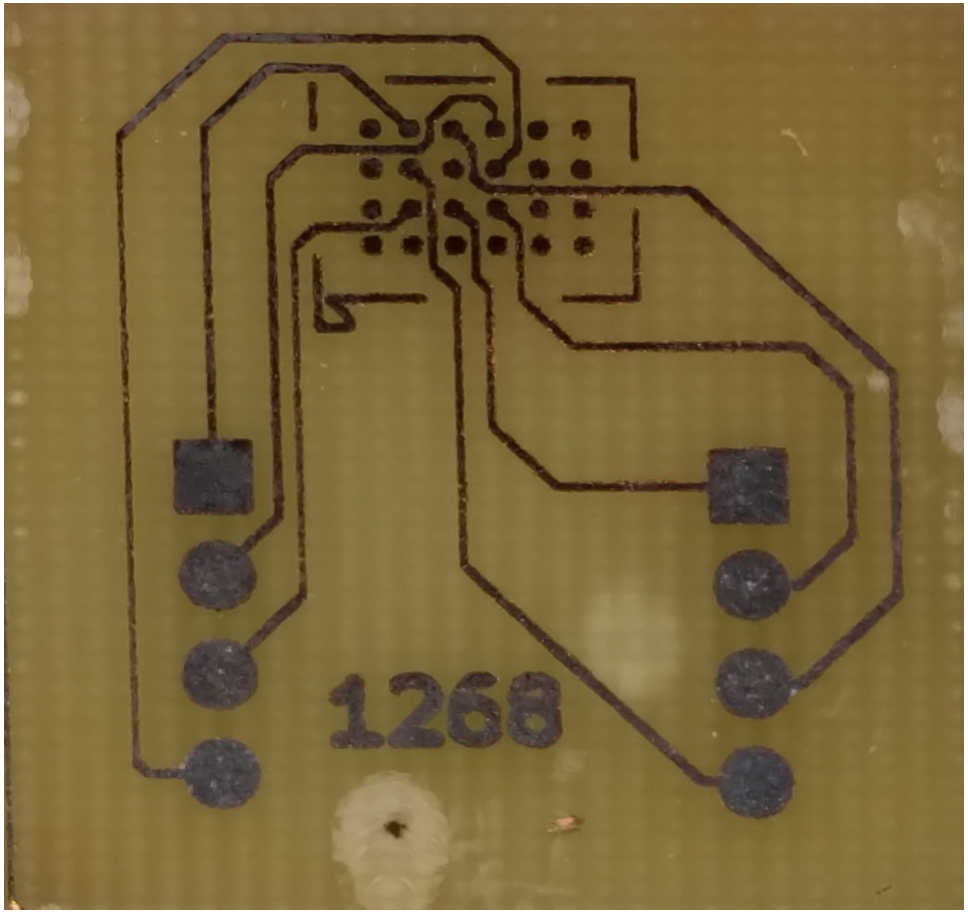
- Transfer ink to the substrate
- Exposed copper is eaten away by chemicals
- Ink is removed

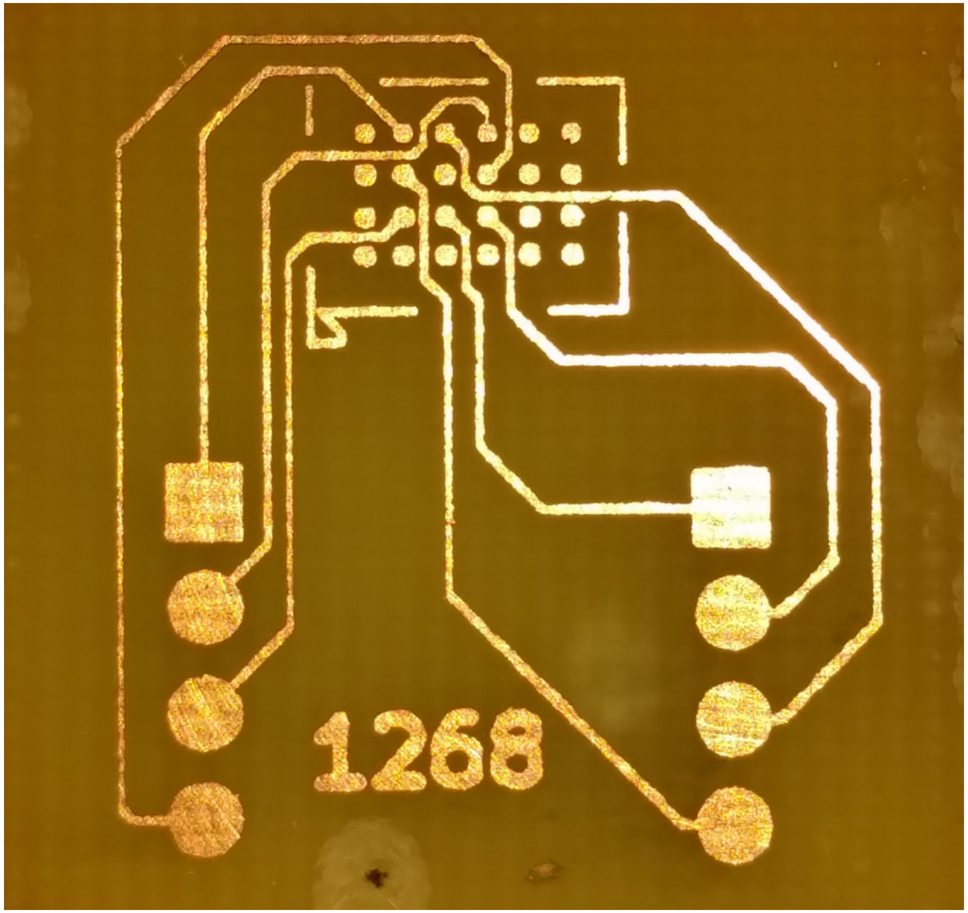

size of the core is larger than the finished size of the board.
Copper Foil
Laminate





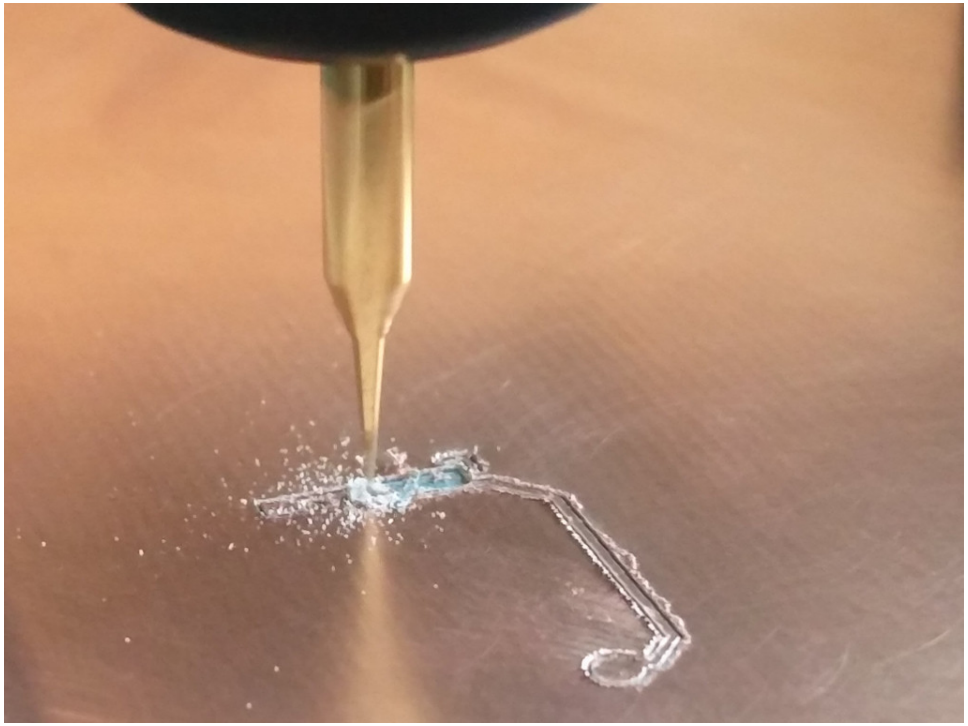
Pics of etching



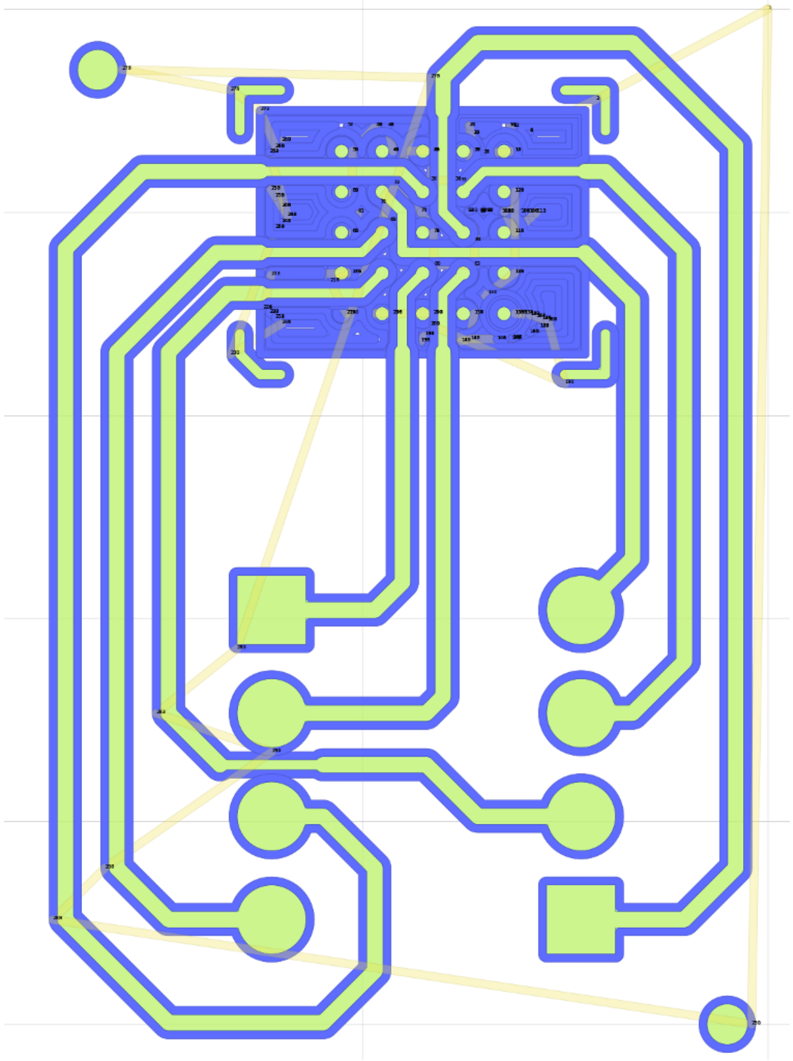


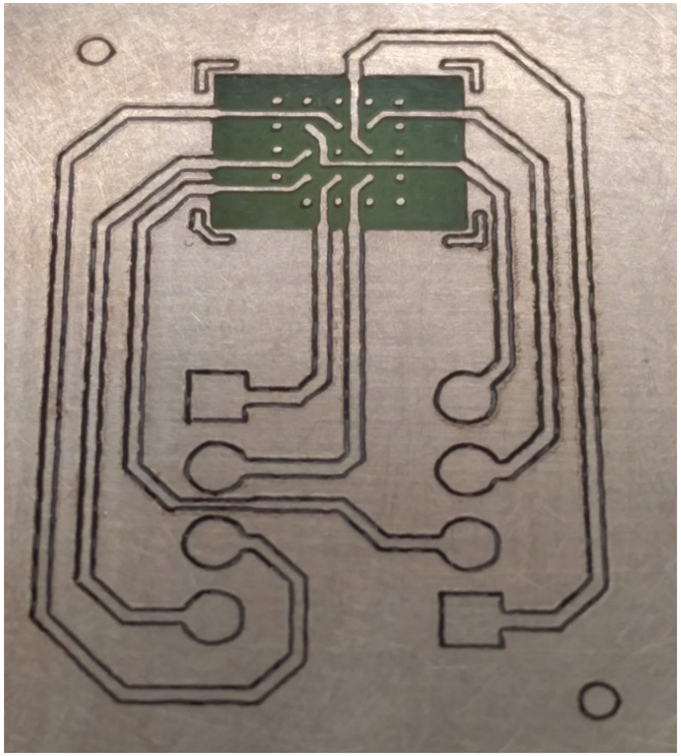
PCB fabrication by milling

- CNC (Computer Numerical Control) milling machine
- Rotating cutter shaves chips of material



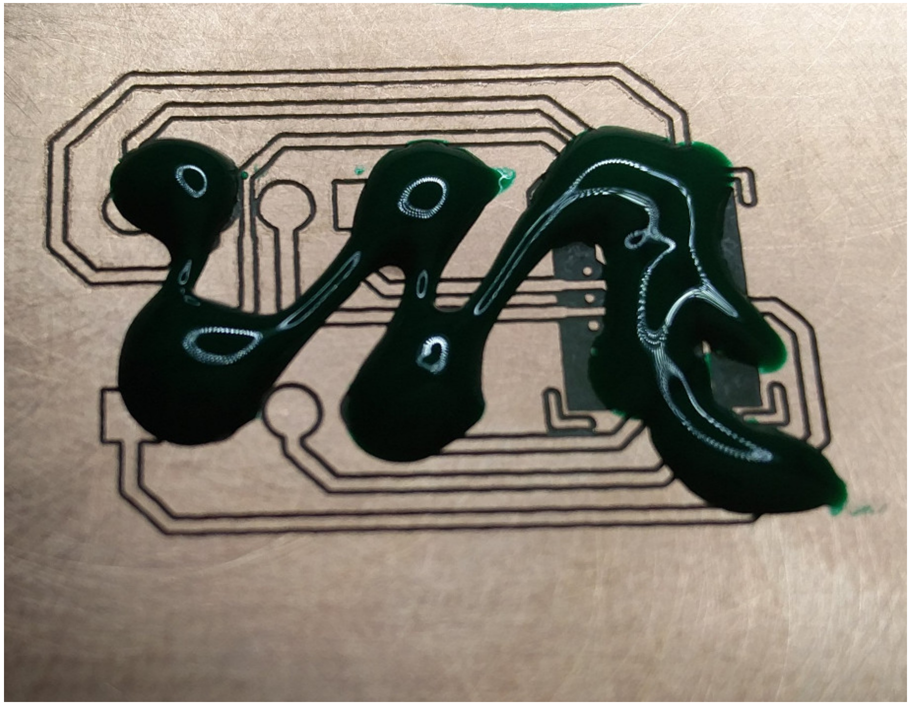
PCB fabrication by milling

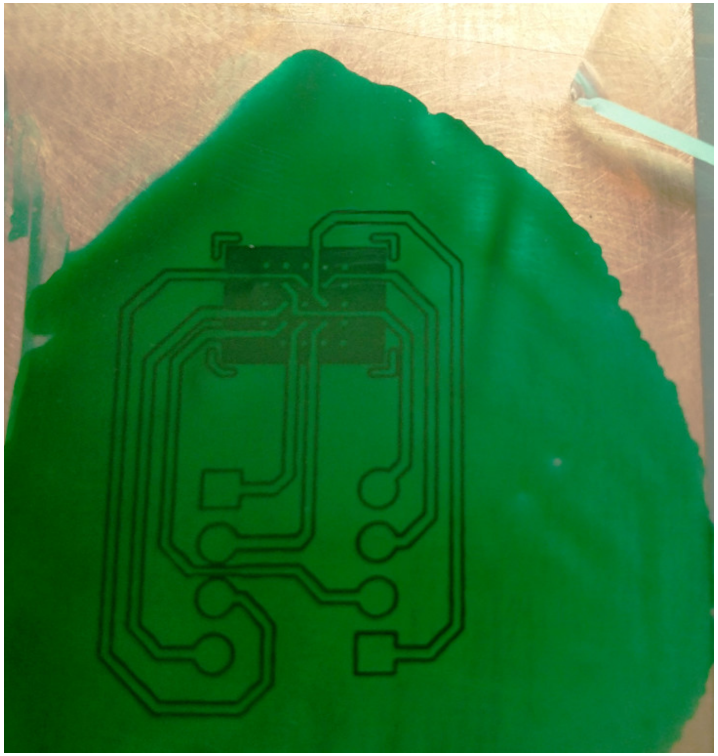




Add the soldermask

- Protect the copper from oxydation

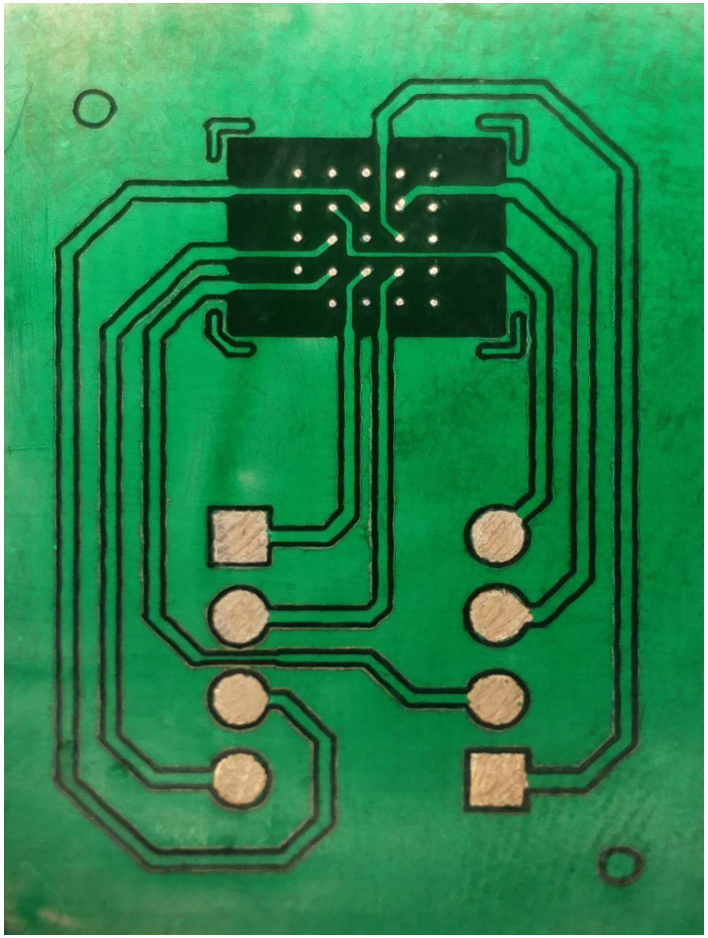




- Lost access to copper pads :(

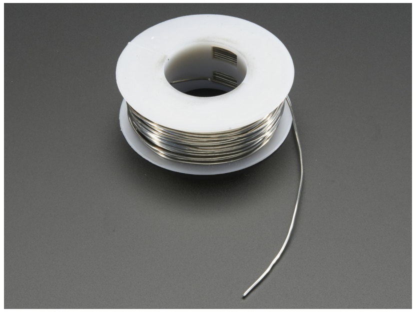
Fix the soldermask

- **Scratch the soldermask to (re)gain access to the pads**



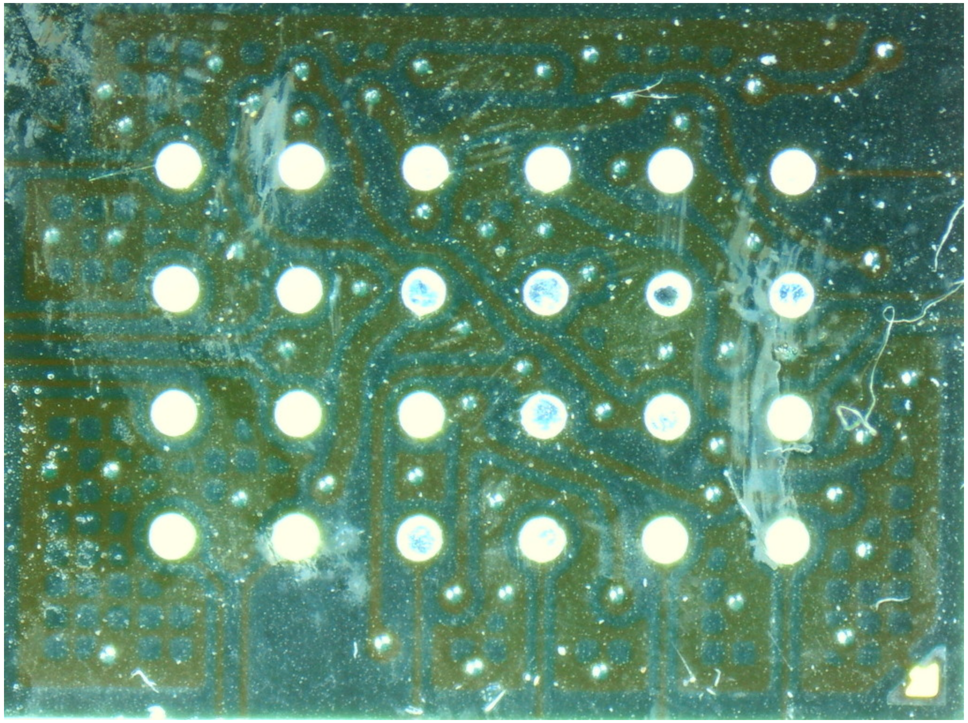
Step 4: Solder the chip to the breakout board

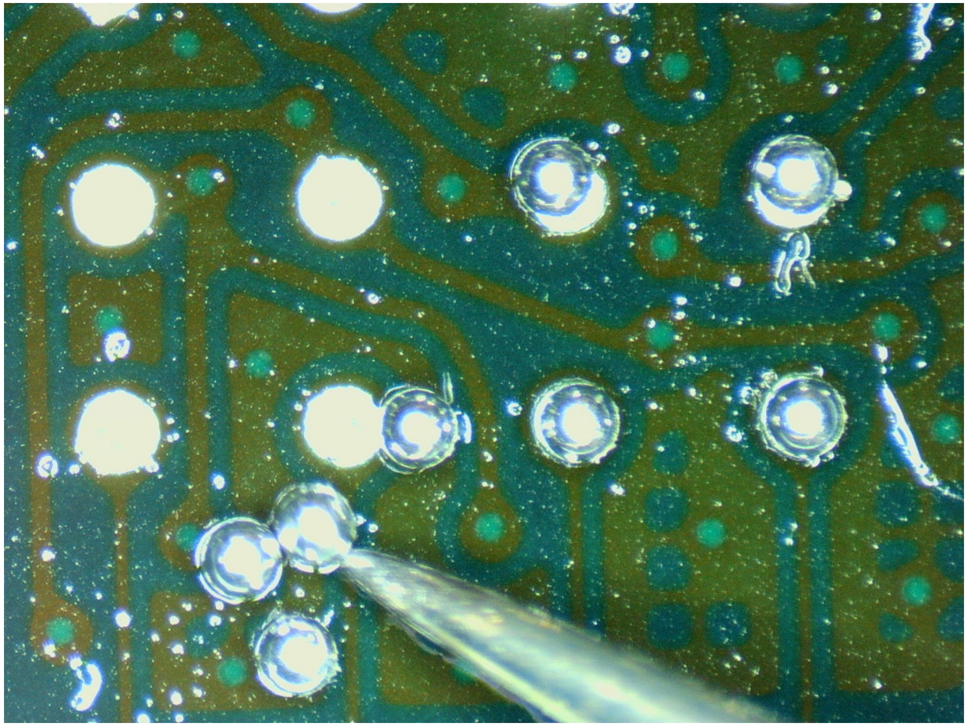
- BGA soldering
- Usage of microscope recommended
- Solder spool vs solder balls



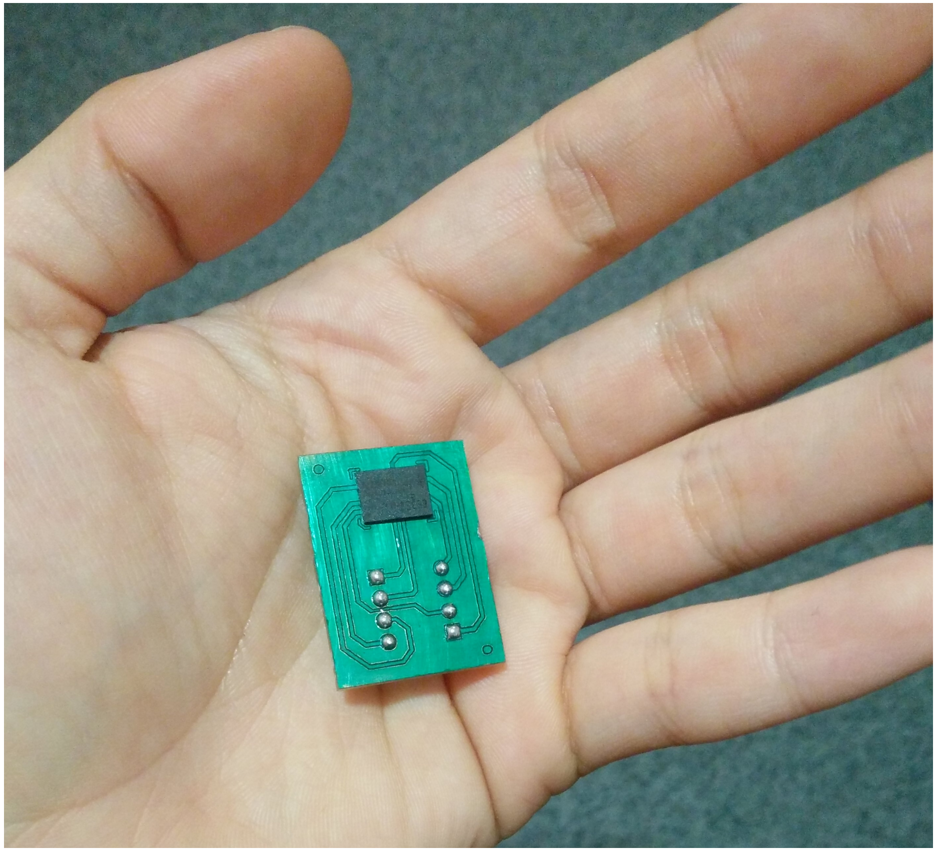
- A solder ball must be placed in each slot of the BGA
- Requires lots of patience and steady hands :D

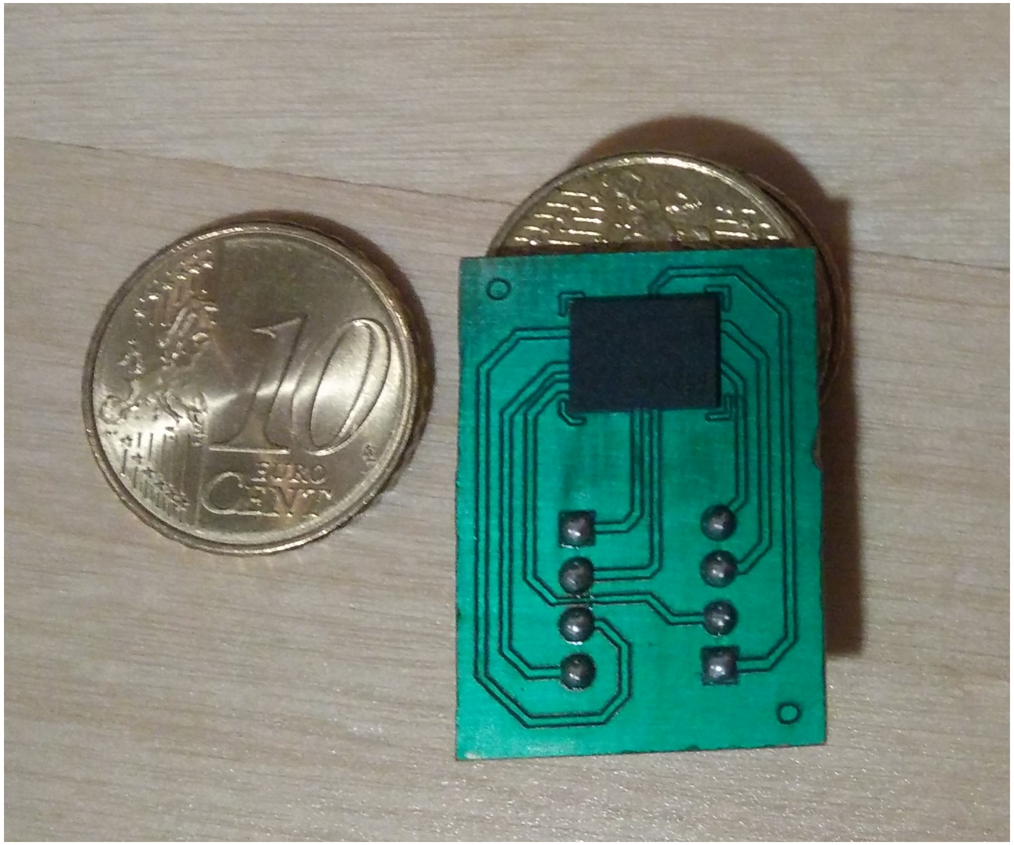
Pics of BGA reballing



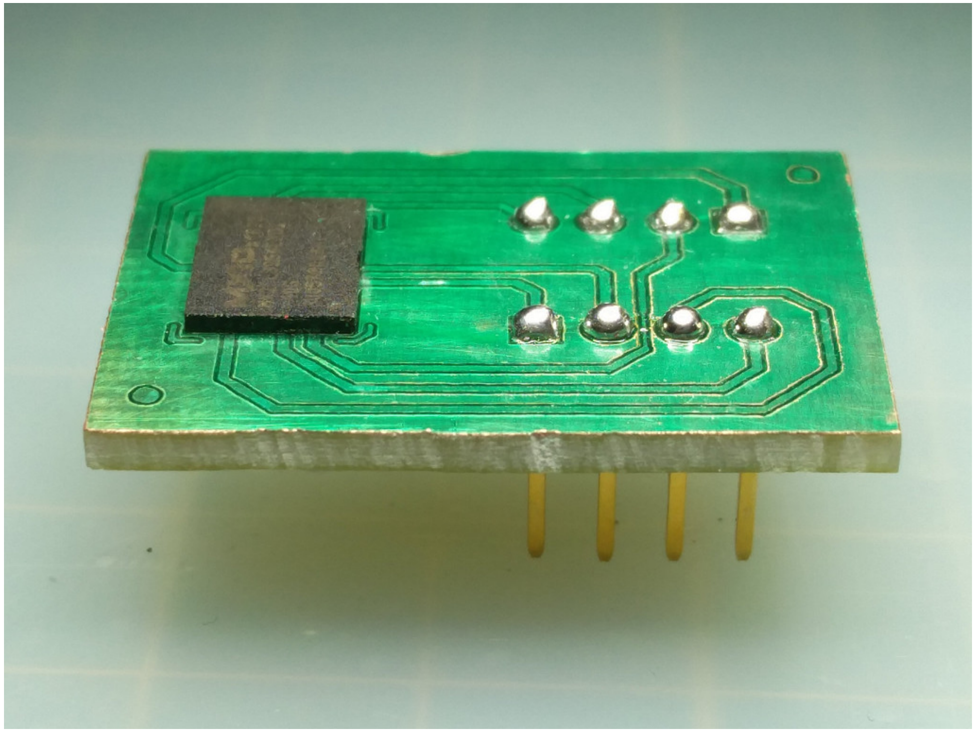


Finished breakout board

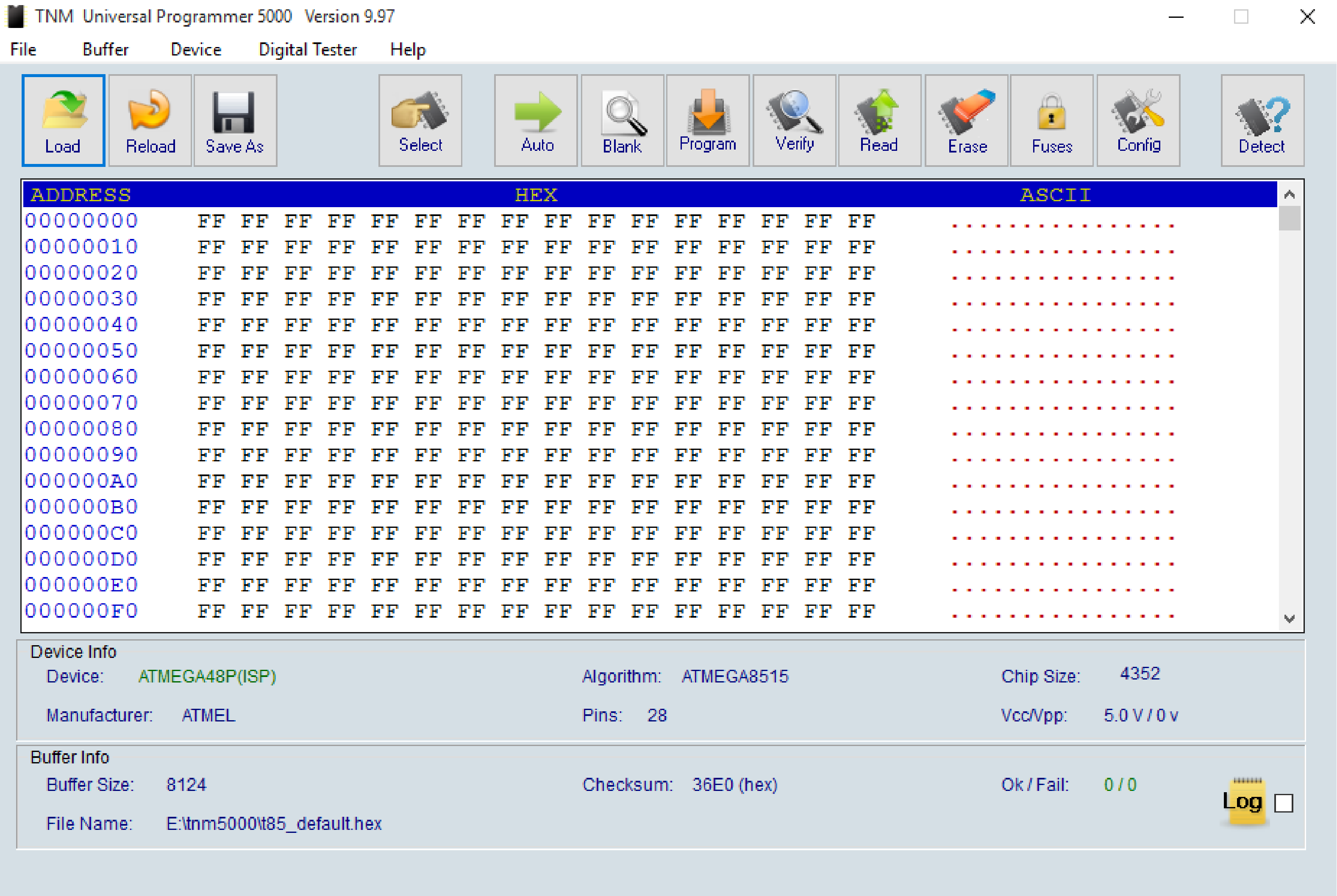




Step 5: Dump the flash



Dump the flash



```
ADDRESS                              HEX                                         ASCII
00000000    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF     ................
00000010    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF     ................
00000020    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF     ................
00000030    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF     ................
00000040    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF     ................
00000050    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF     ................
00000060    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF     ................
00000070    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF     ................
00000080    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF     ................
00000090    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF     ................
000000A0    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF     ................
000000B0    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF     ................
000000C0    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF     ................
000000D0    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF     ................
000000E0    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF     ................
000000F0    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF     ................
```

Device Info

Device: ATMEGA48P(ISP) Algorithm: ATMEGA8515 Chip Size: 4352

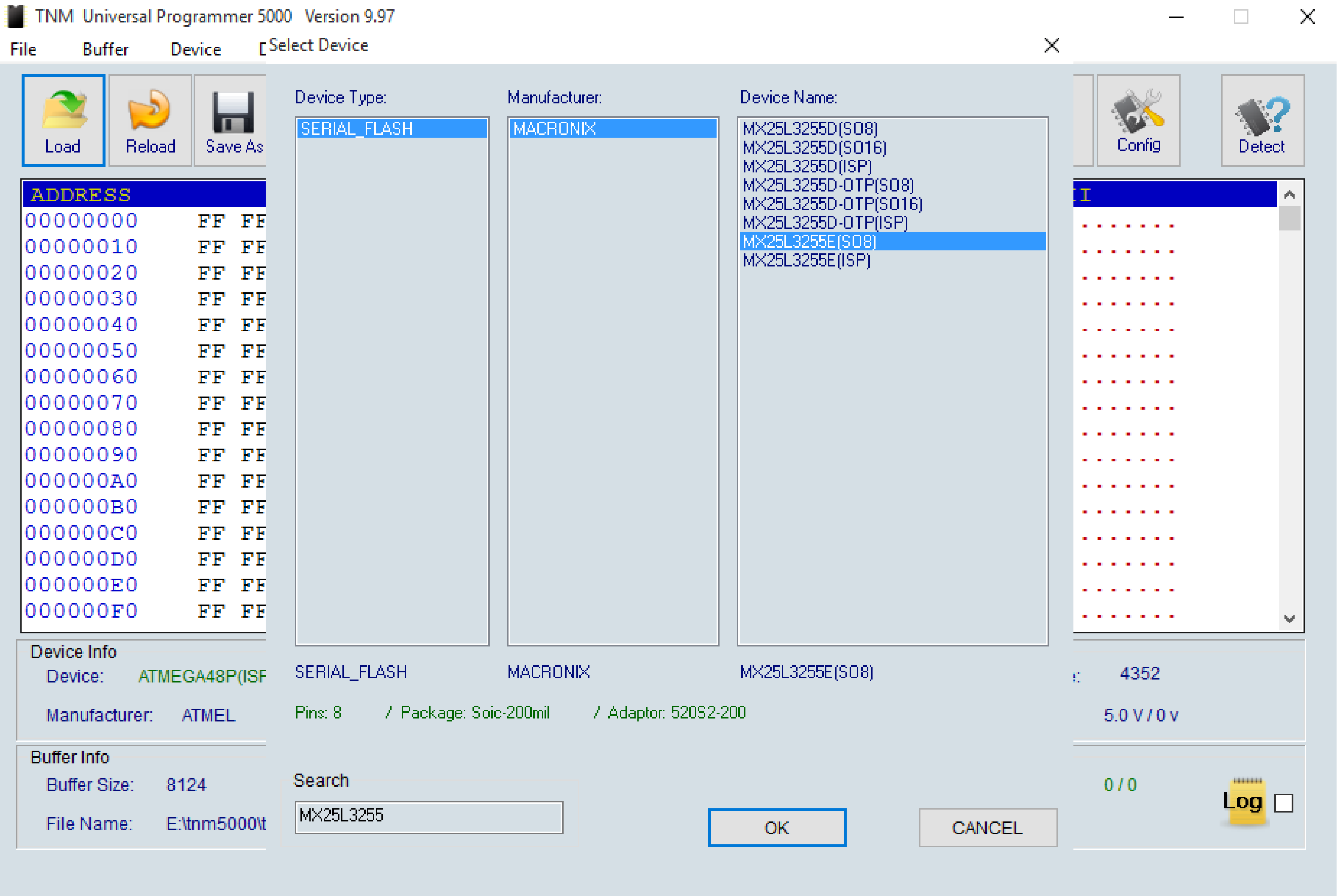
Manufacturer: ATMEL Pins: 28 Vcc/Vpp: 5.0 V / 0 v

Buffer Info

Buffer Size: 8124 Checksum: 36E0 (hex) Ok / Fail: 0 / 0 □

File Name: E:\tnm5000\t85_default.hex

Dump the flash



TNM Universal Programmer 5000 Version 9.97

```
ADDRESS
00000000    FF  FF
00000010    FF  FF
00000020    FF  FF
00000030    FF  FF
00000040    FF  FF
00000050    FF  FF
00000060    FF  FF
00000070    FF  FF
00000080    FF  FF
00000090    FF  FF
000000A0    FF  FF
000000B0    FF  FF
000000C0    FF  FF
000000D0    FF  FF
000000E0    FF  FF
000000F0    FF  FF
```

Device Type: SERIAL_FLASH

Manufacturer: MACRONIX

Device Name:
MX25L3255D(SO8)
MX25L3255D(SO16)
MX25L3255D(ISP)
MX25L3255D-OTP(SO8)
MX25L3255D-OTP(SO16)
MX25L3255D-OTP(ISP)
MX25L3255E(SO8)
MX25L3255E(ISP)

SERIAL_FLASH   MACRONIX   MX25L3255E(SO8)

Pins: 8 / Package: Soic-200mil / Adaptor: 520S2-200

Search: MX25L3255

Device Info
Device: ATMEGA48P(ISF
Manufacturer: ATMEL

4352
5.0 V / 0 v

Buffer Info
Buffer Size: 8124
File Name: E:\tnm5000\t

0 / 0

Conclusion: funky stats

- **PCB by CNC milling:**
  - ~12 drilling bits died
  - 4 PCBs made before calibration of the CNC was correct
  - 2 PCBs to test the soldermask
- **PCB by etching:**
  - 5 PCBs made before the ink transfer was correct
  - 3 PCBS for etching (worked on the first try)

Conclusion: Bill of materials

- **Bootstrap: ~1000€**
  - Hot air soldering station: ~100€
  - Flash programmer (TNM5000): ~300€
  - CNC machine: ~300€
  - Microscope: ~500€

- **Consumables: ~50€**
  - Soldering balls, soldering flux, desoldering braid ~10€
  - Chemicals (isopropanol, Ferric Chloride, ...) ~30€
  - Epoxy Fiber FR4 Copper Clad Plate ~10€

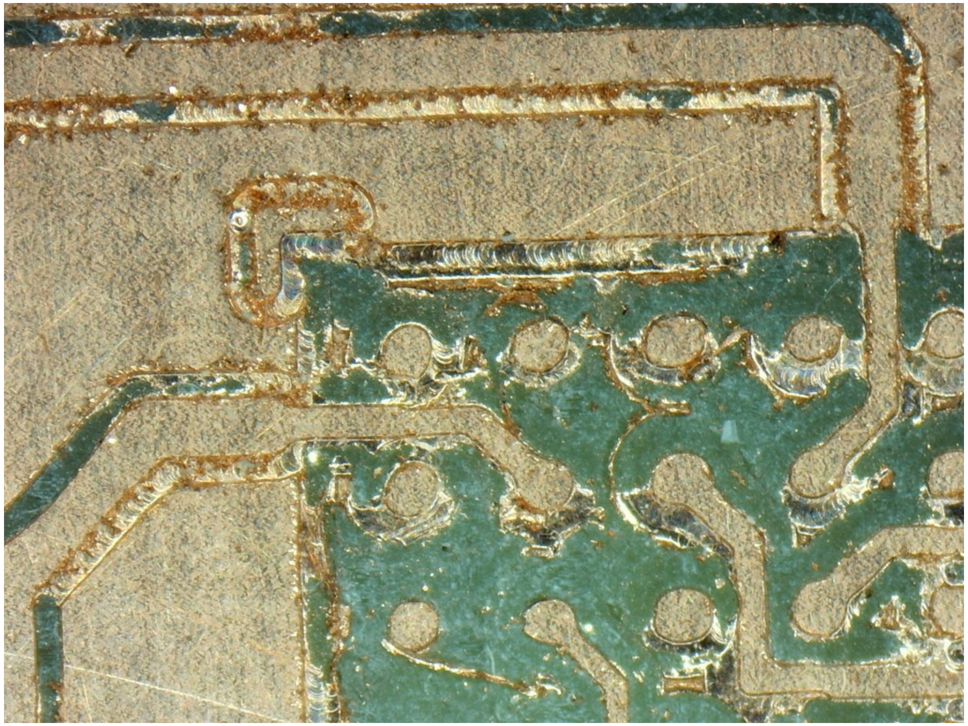
→ Crafting custom PCB is not that hard/expensive

Conclusion: and the magic box ?

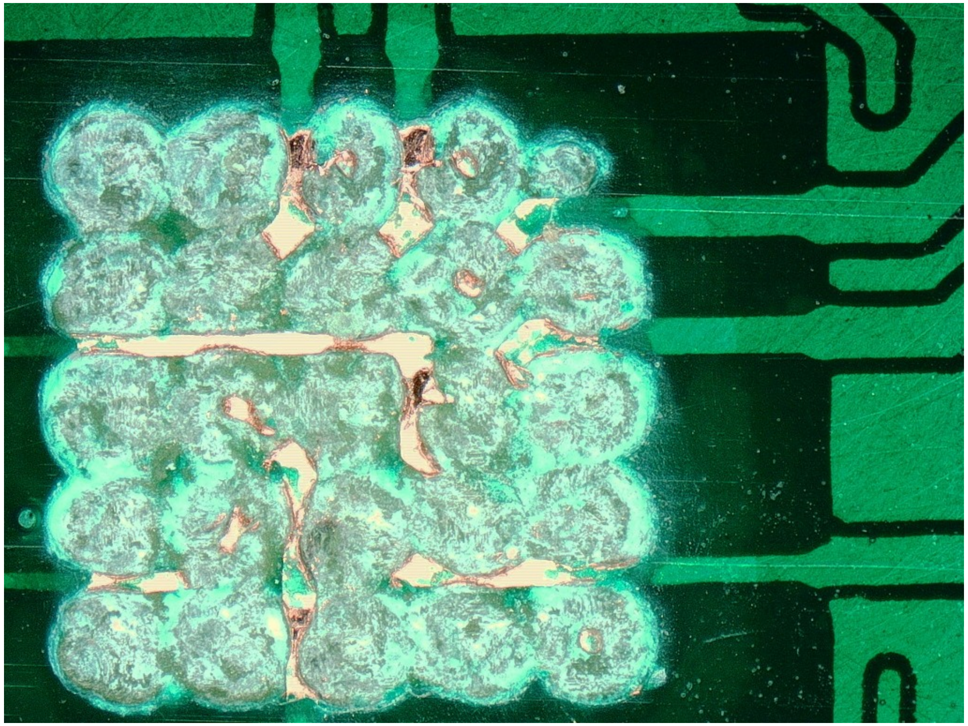
- **Attacks tested:**
  - Transplantation: success
  - Clone: success
  - Impersonating a competitor’s box: success

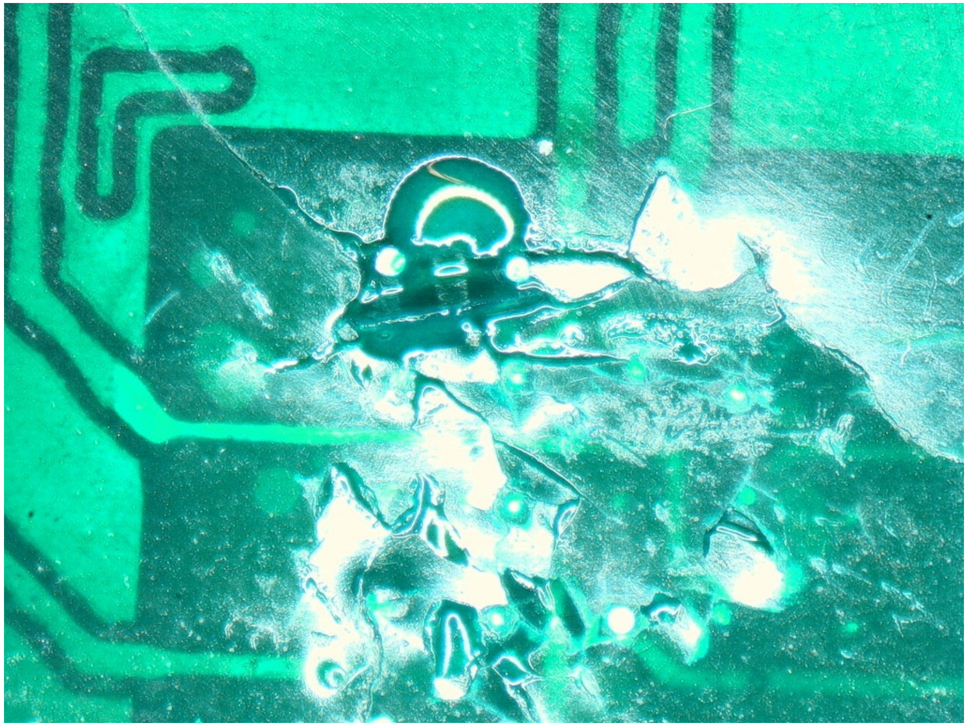
- ***The magic box is still commercially available… :)***

Bonus: the horror show



Bonus: the horror show (2)





?