그림으로 보는

EMBEDDED HACKING 101

WITH VOLANTRAT

INDEX

- EMBEDDED?
- BEFORE YOU START HACK
- ATTACK BACTOR
  - uart, jtag
- CASE STUDY

EMBEDDED?

IT'S ALL.

SMART HOME

- Head-worn

- Straps

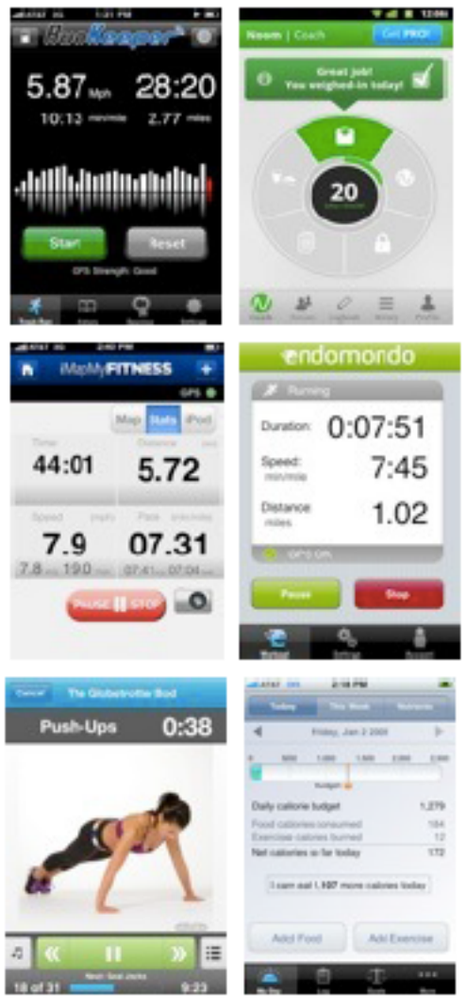
- Shirts

- Wrist-worn

- Clips

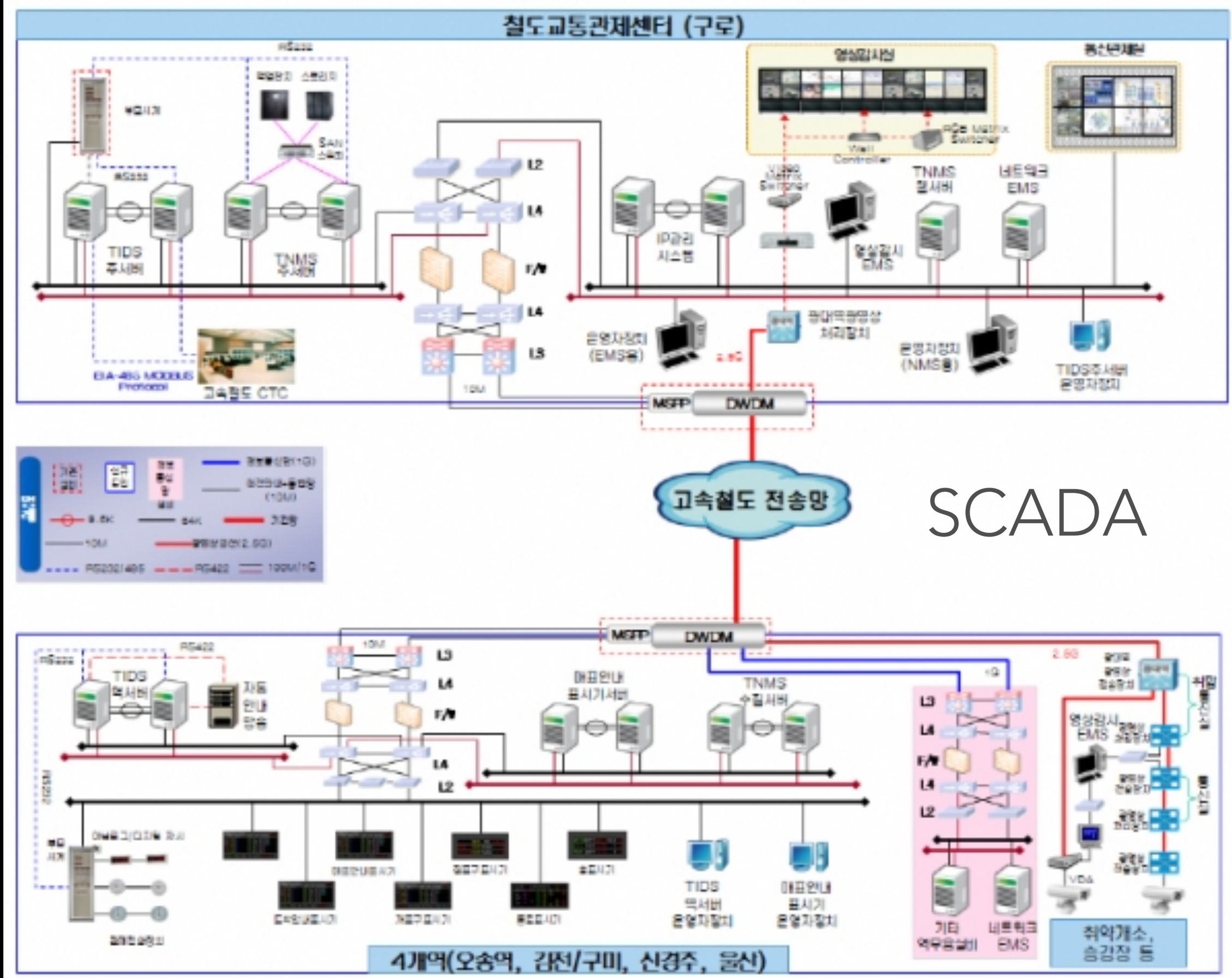
- Shoe-worn / Foot pods

Apps



Wearable devices

SCADA


철도교통관제센터 (구로)
TIDS 주서버
TNMS 주서버
고속철도 CTC
L2
L4
L3
L5
IP관리 시스템
영상감시 EMS
TNMS 클서버
네트워크 EMS
운영자장치 (EMS용)
운영자장치 (NMS용)
TIDS주서버 운영자장치
MSPP
DWDM
고속철도 전송망
TIDS 백서버
자동 안내 장송
TNMS 수집서버
TIDS 백서버 운영자장치
안내표시기 운영자장치
기타 역무용설비
네트워크 EMS
취약개소, 승강장 등
4개역(오송역, 김천/구미, 신경주, 울산)

EMBEDDED?

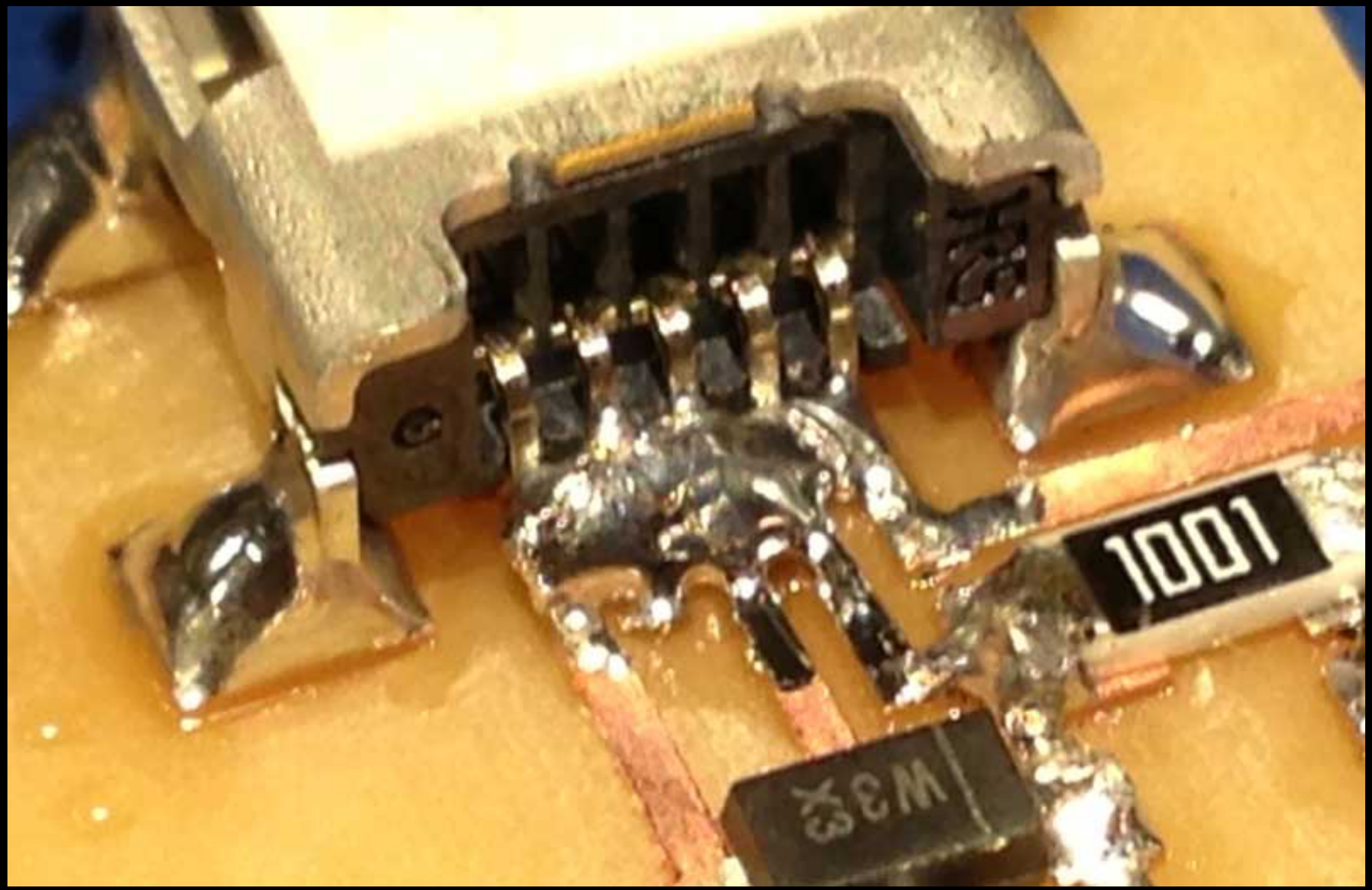
YES, IT'S ALL.

BEFORE YOU START HACK

- What will you do If your target has broken?

Looks Like…

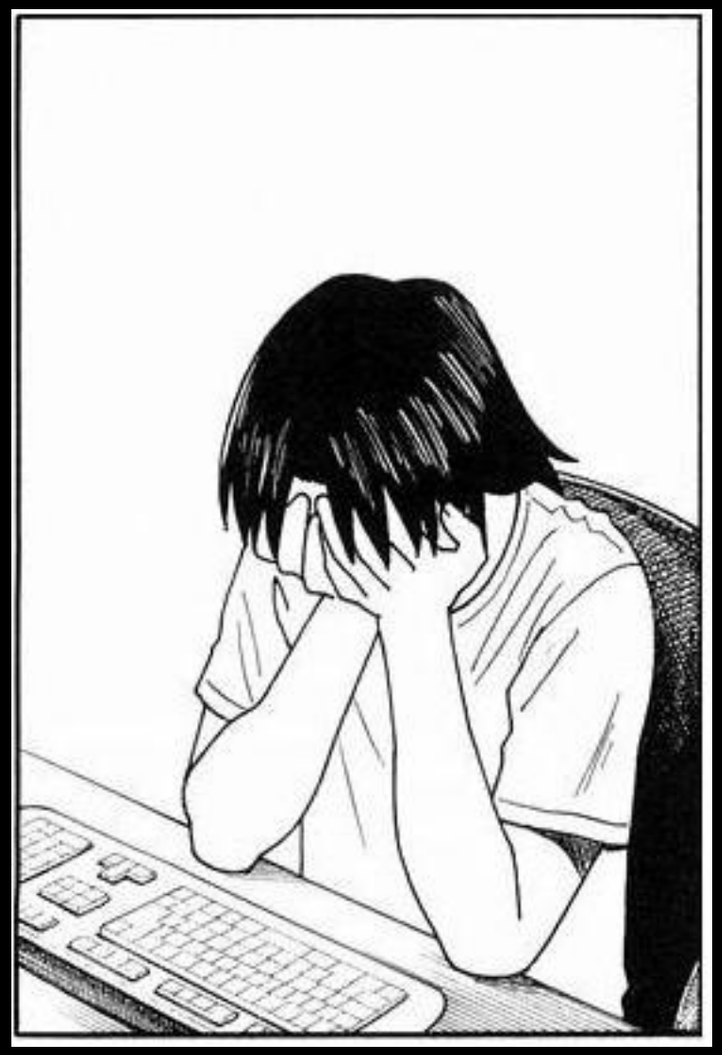
THIS



OR THIS


KBS1
컴퓨터 상태가
심각해요
대전 박무
5.8 ℃


(심각한 표정)

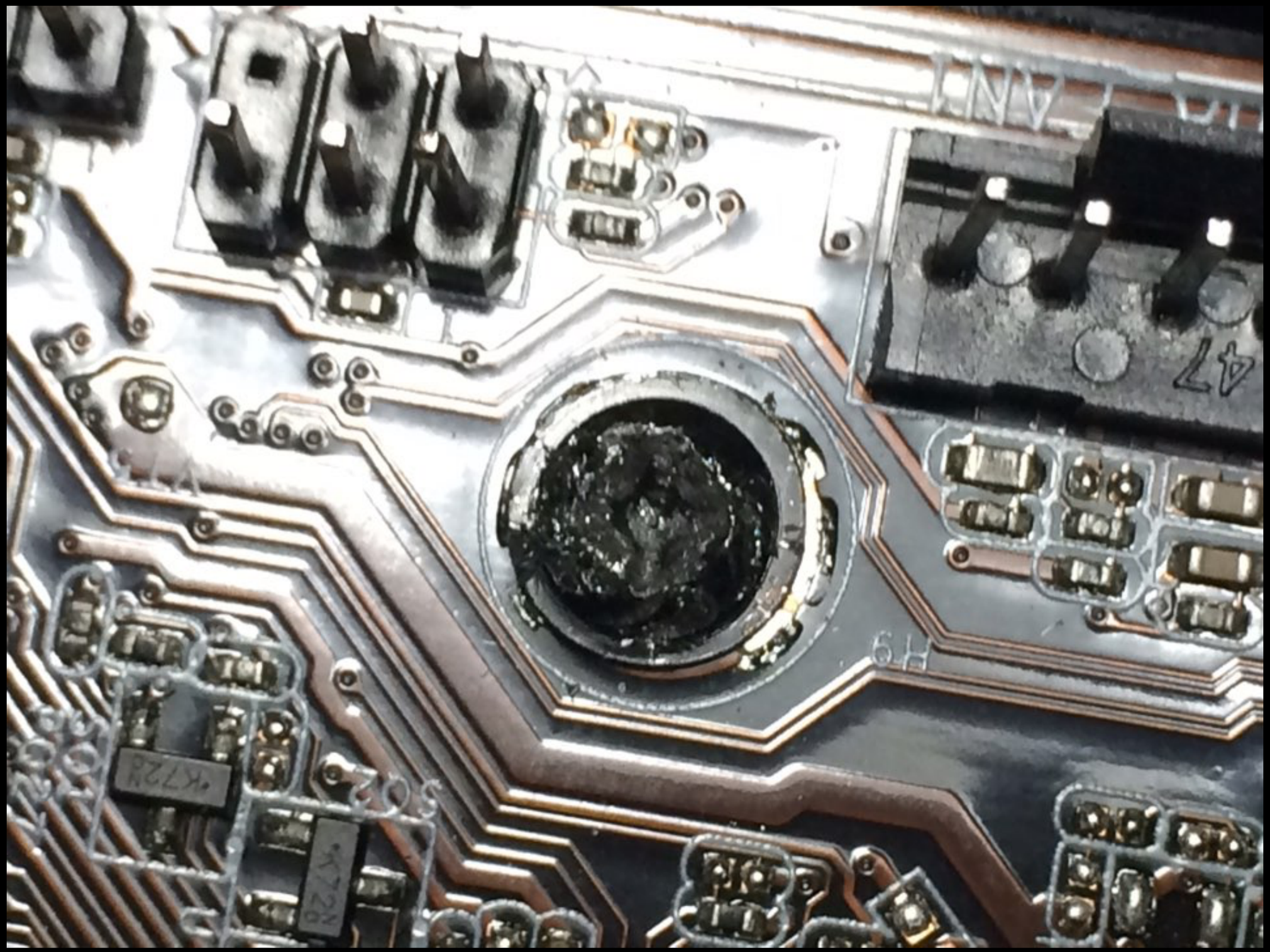



이때는 대략
정신이 멍해진다
헉

그렇다면 AS를 받을 수 있게 삽질하자

Bad case 1

Bad case 2



빠가~빠가~ Bad case3

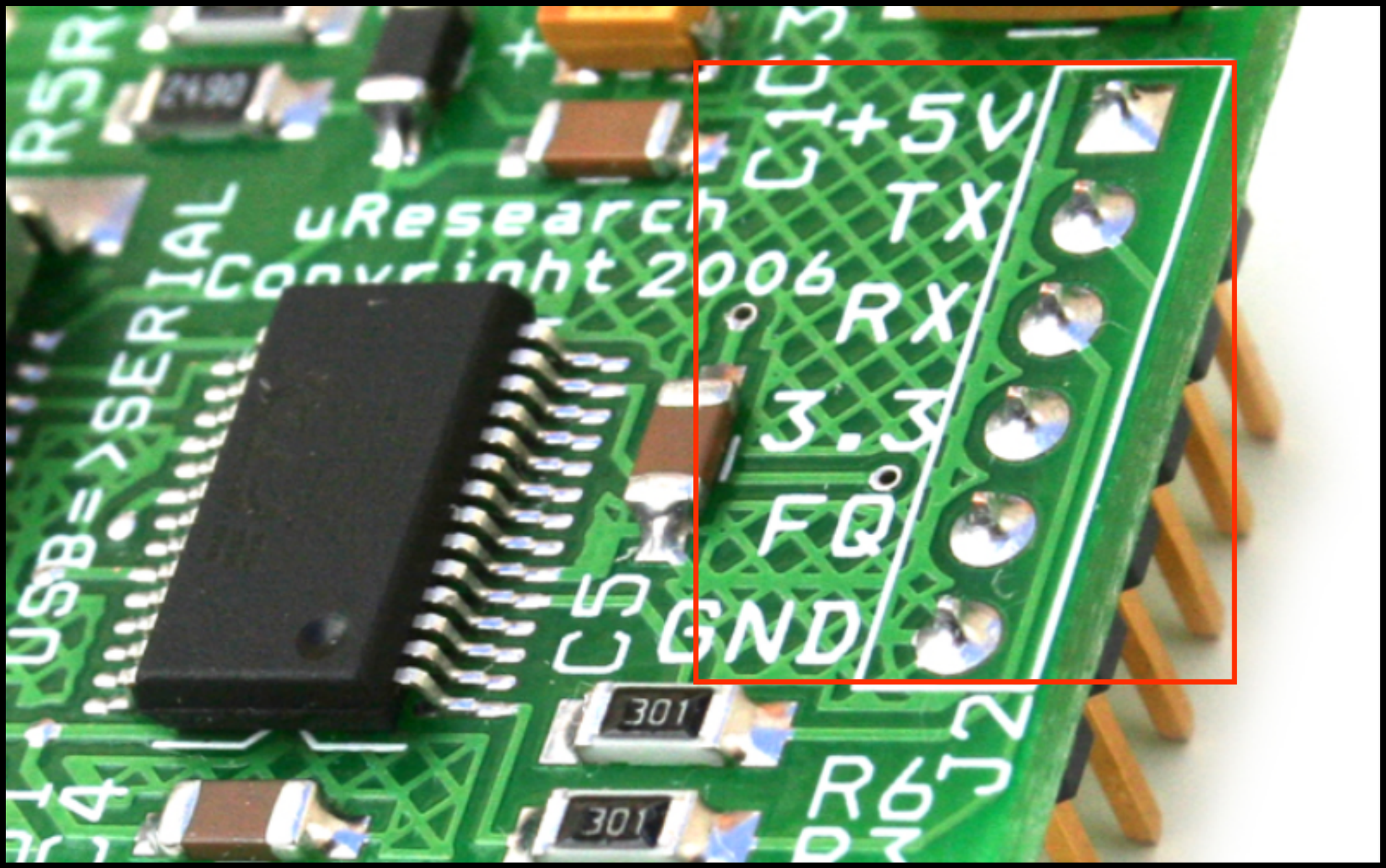
뽀각♡ Bad case4

그러니까.. 이것만 지키고 호갱 코스프레를 하면 AS가 된다 이말입니다.

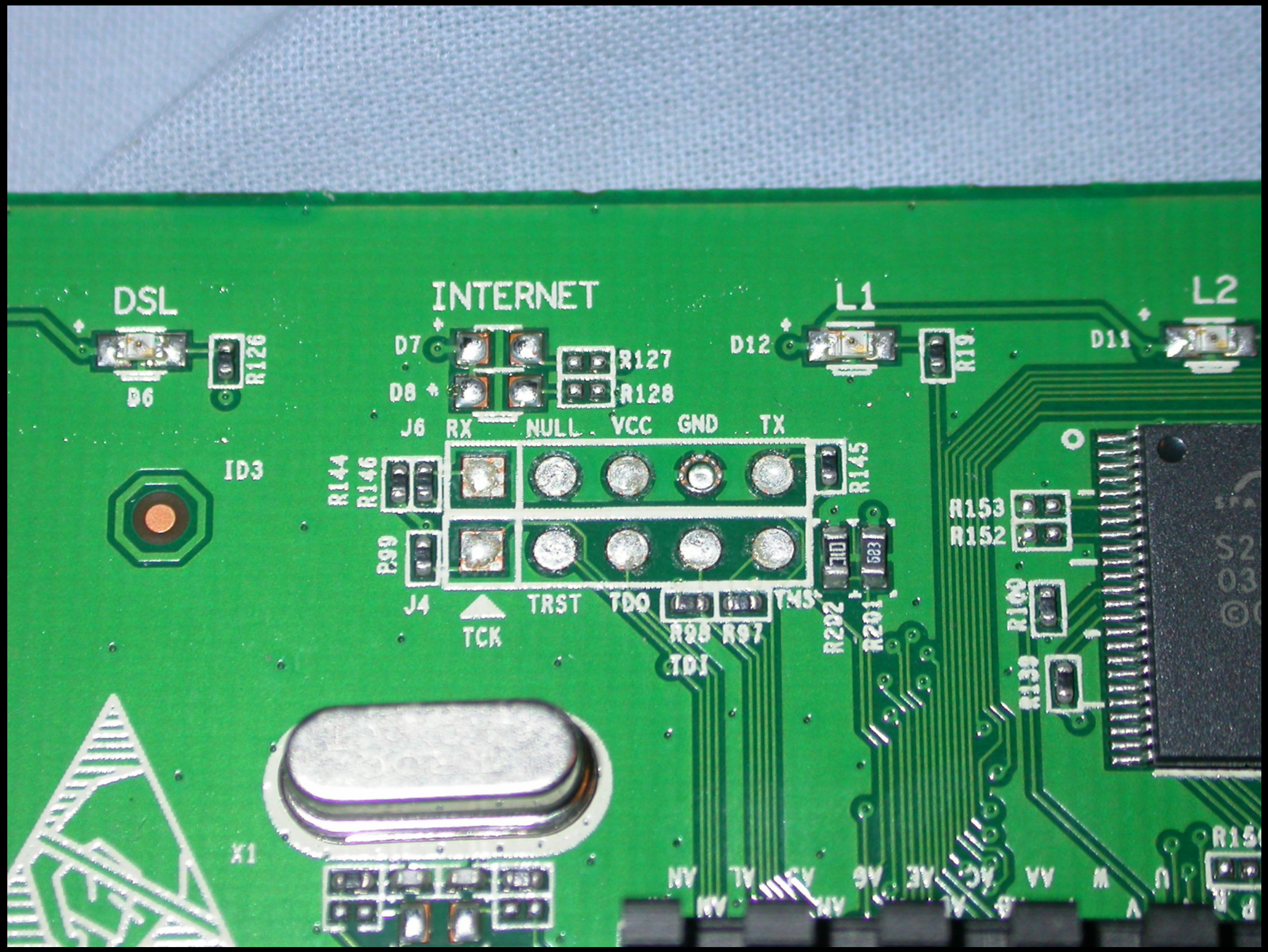
- 워런티 스티커가 훼손되지 않게 조심히 떼어내 모셔두고 나사를 푼다.
- 재봉인 방지 스티커는 일단 뗏다가, 강력하지 않은 접착체로 재봉인한다. (그러면 뗄때 처음 떼는 기분이 듭니다. 연습필요)
- 나사는 항상 정격규격의 드라이버로, 절도있게 풀어야 합니다.
- 케이스는 힘으로 뜯는게 아니라 요령으로 뜯는 것입니다.
- 진짜 호갱이 되면 안됩니다. (유상AS는 최후의 보루)

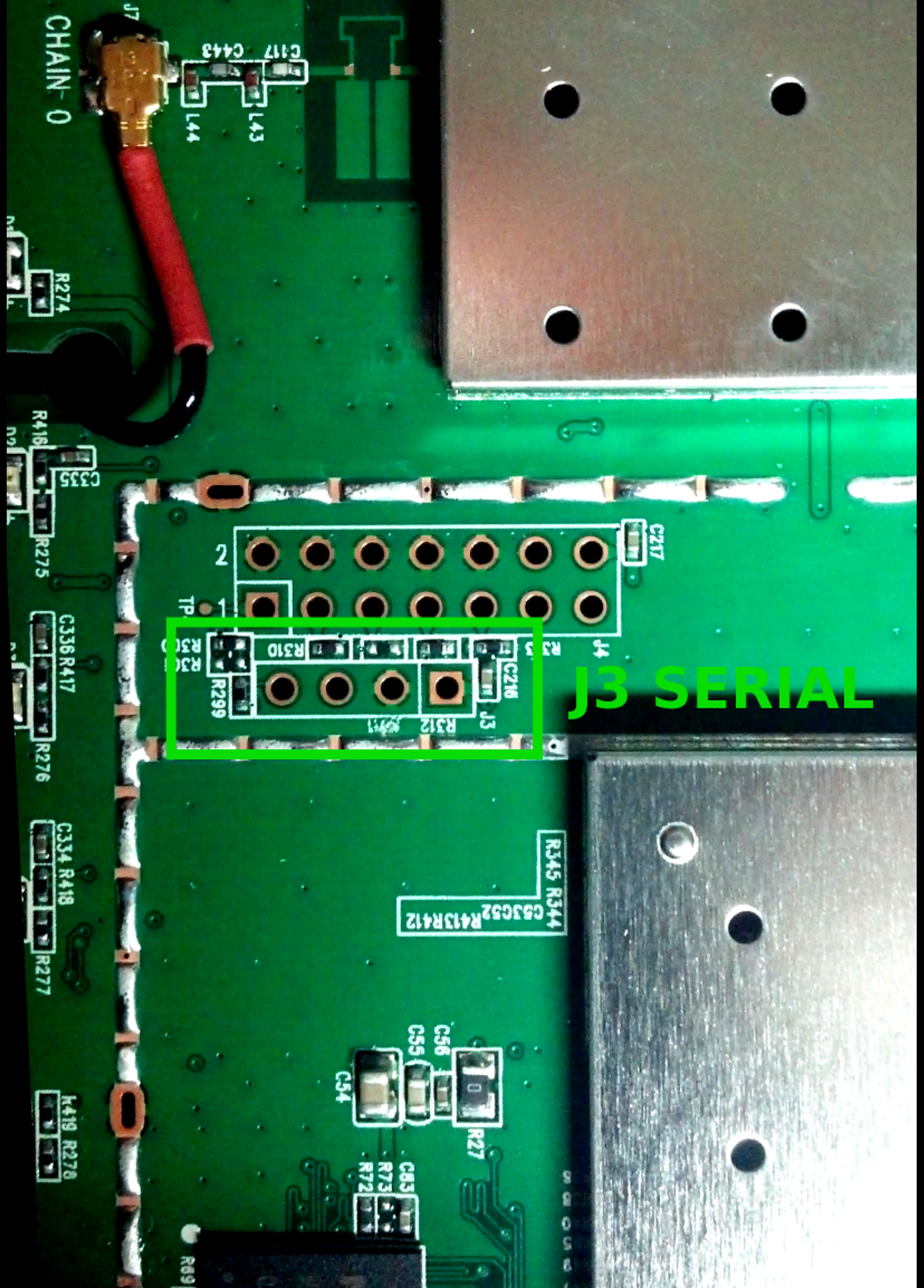
ATTACK VECTOR (UART)

kind :)



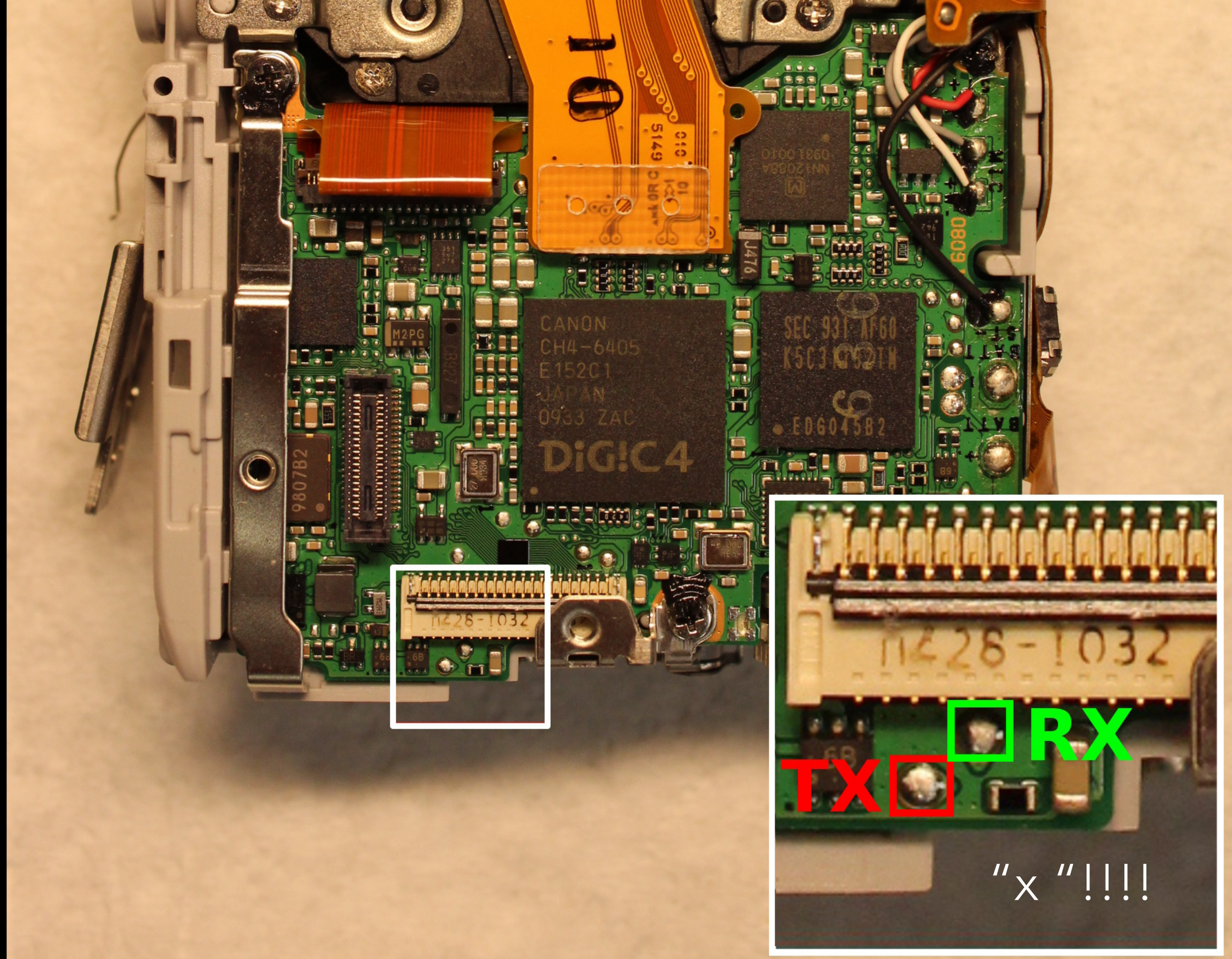
still kind :)


DSL
D6
R126
INTERNET
D7
D8
R127
R128
J6
RX
NULL
VCC
GND
TX
R144
R146
R145
R99
J4
TRST
TDO
TMS
TCK
R98
R97
TDI
R202
R201
D12
L1
R19
D11
L2
R153
R152
R140
R139
ID3
X1

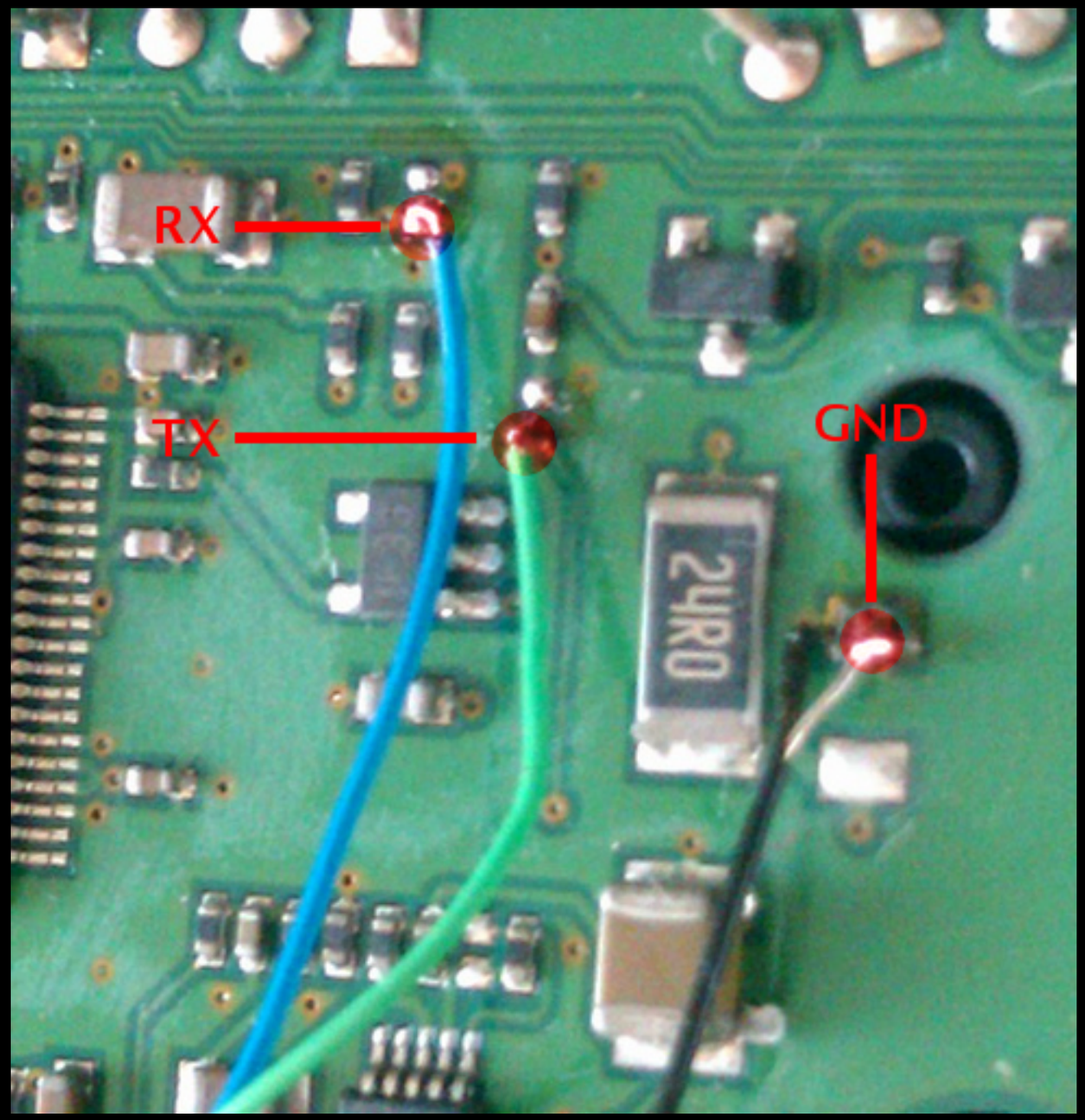


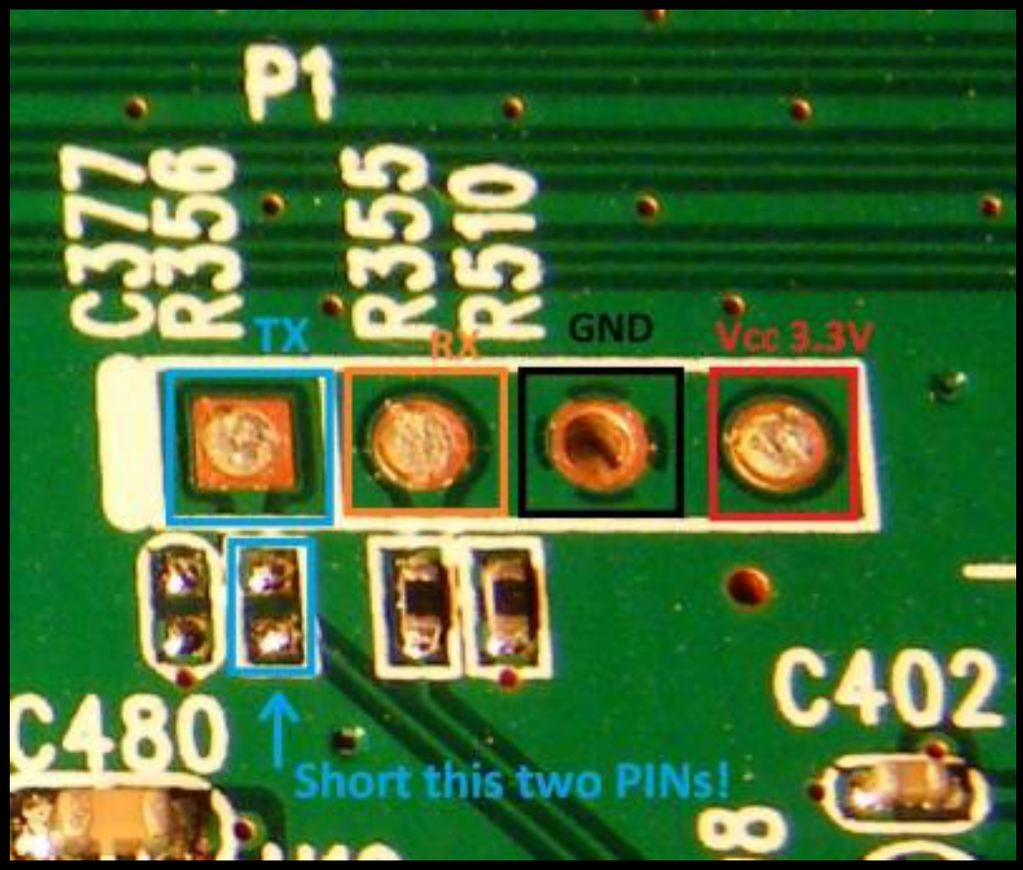
Not printed pinmap

but still kind :p

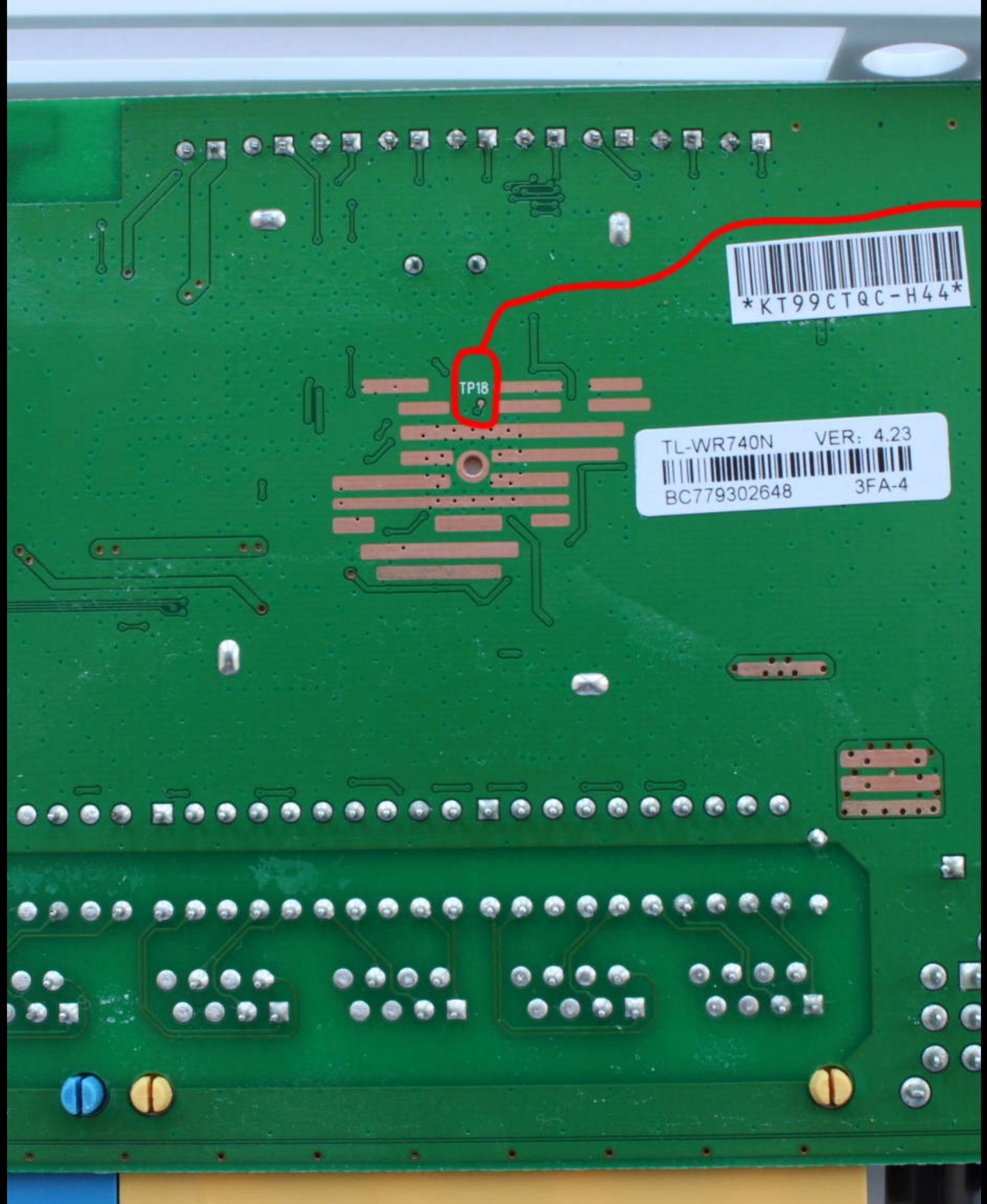

CANON
CH4-6405
E152C1
JAPAN
0933 ZAC
DiG!C4
M2PG
J476
11Z28-1032
TX
RX
"x "!!!!

umm.. :{





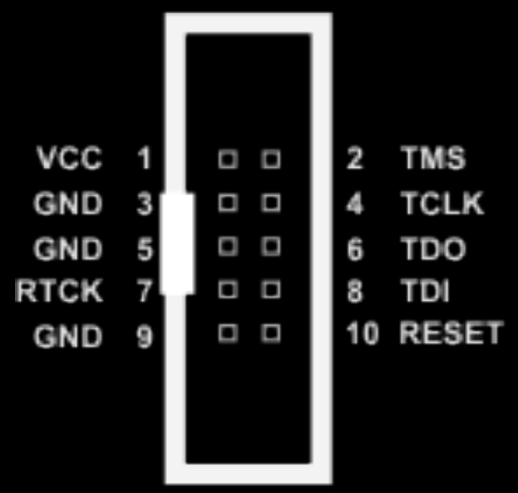
register cut. : (



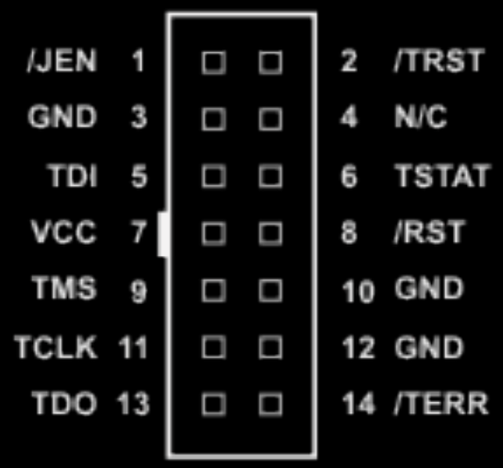
Kidding me? :!!!

ATTACK BACTOR (JTAG)

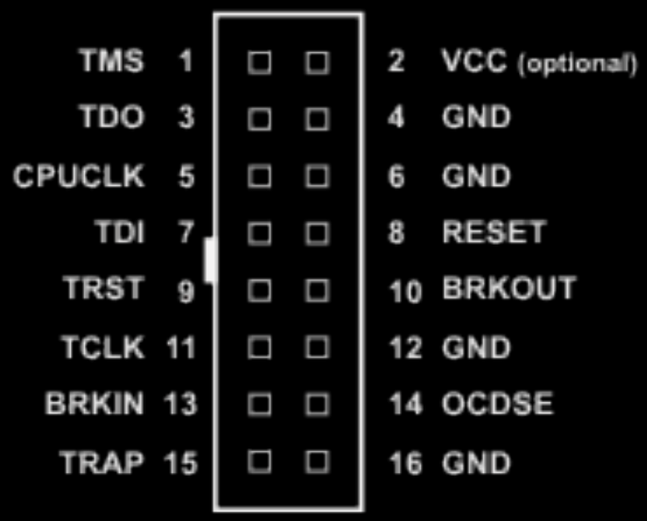
ARM 10-PIN Interface



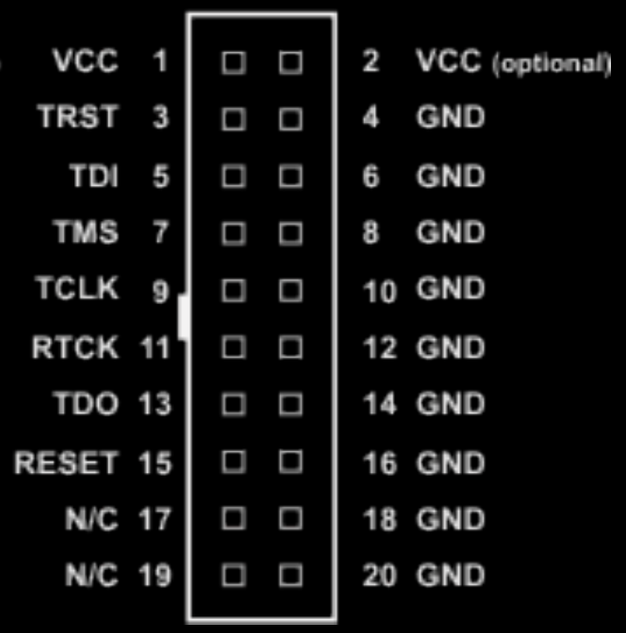
ST 14-PIN Interface



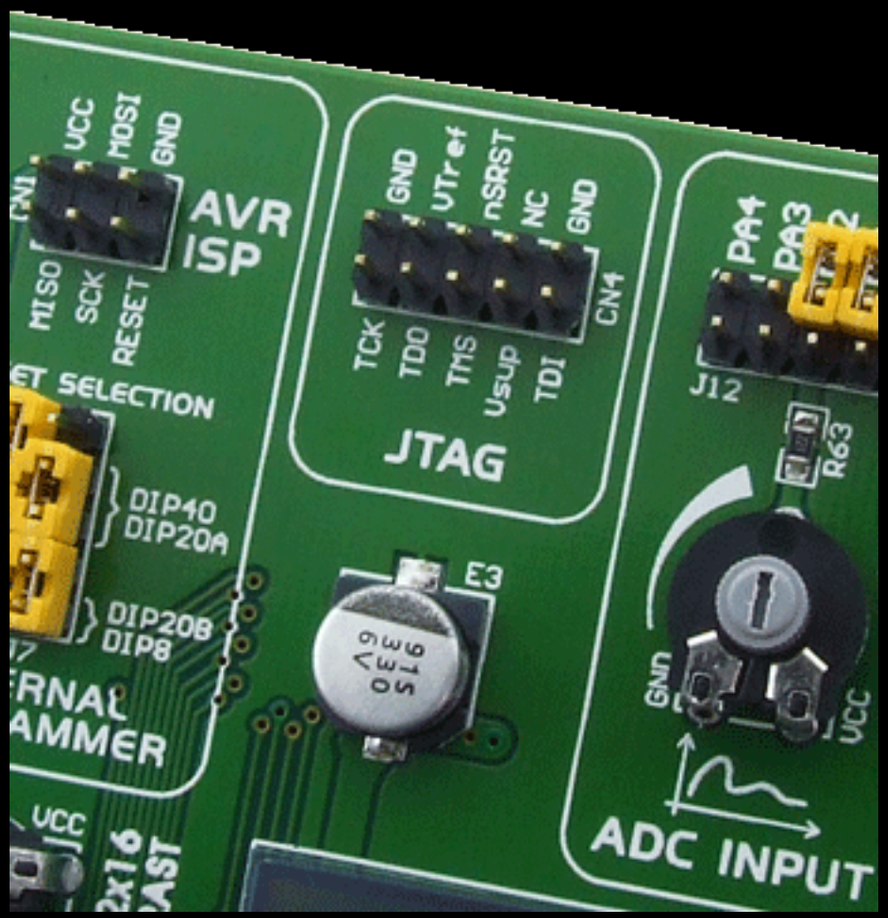
OCDS 16-PIN Interface



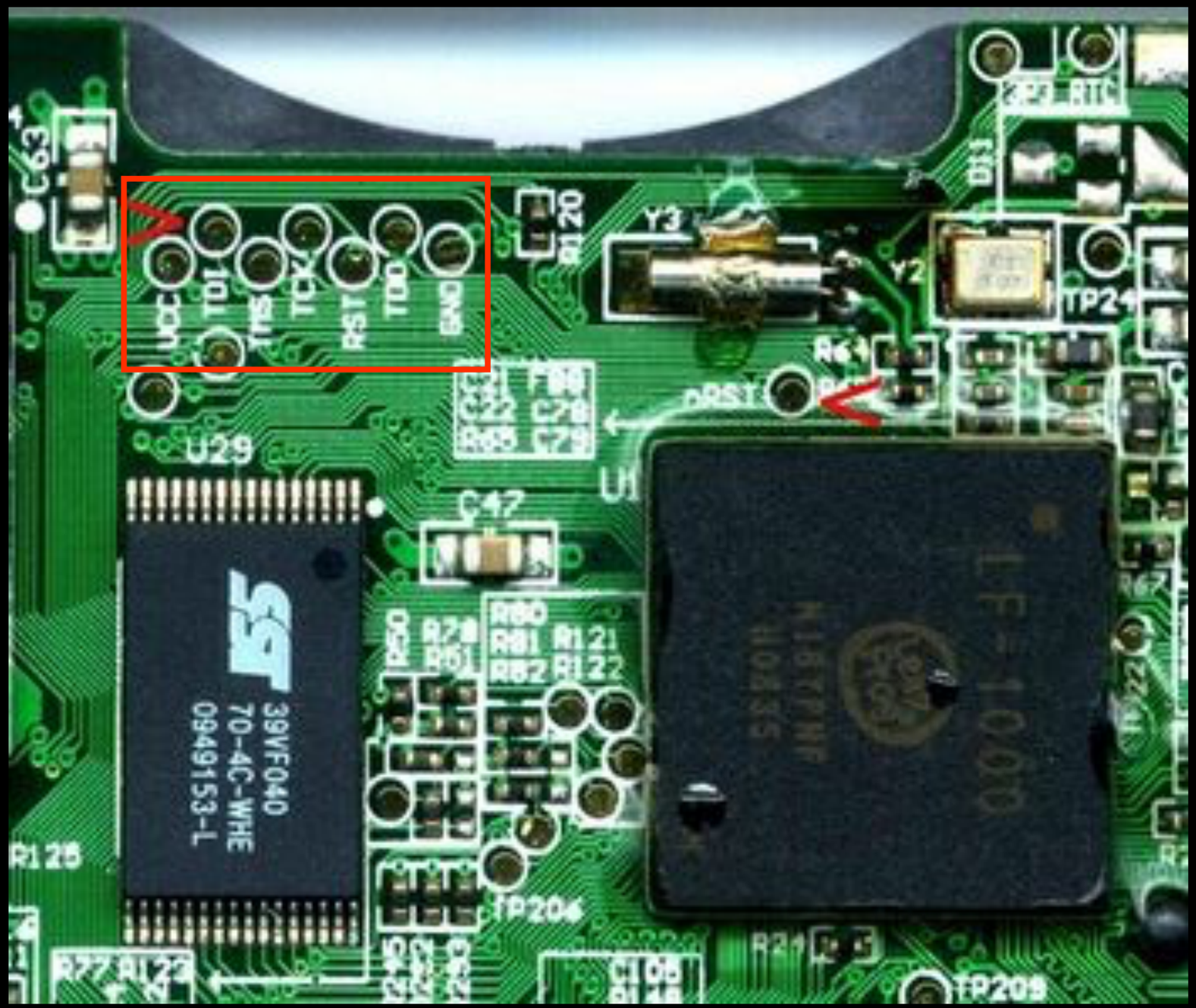
ARM 20-PIN Interface



let’s start again from kind pinout!

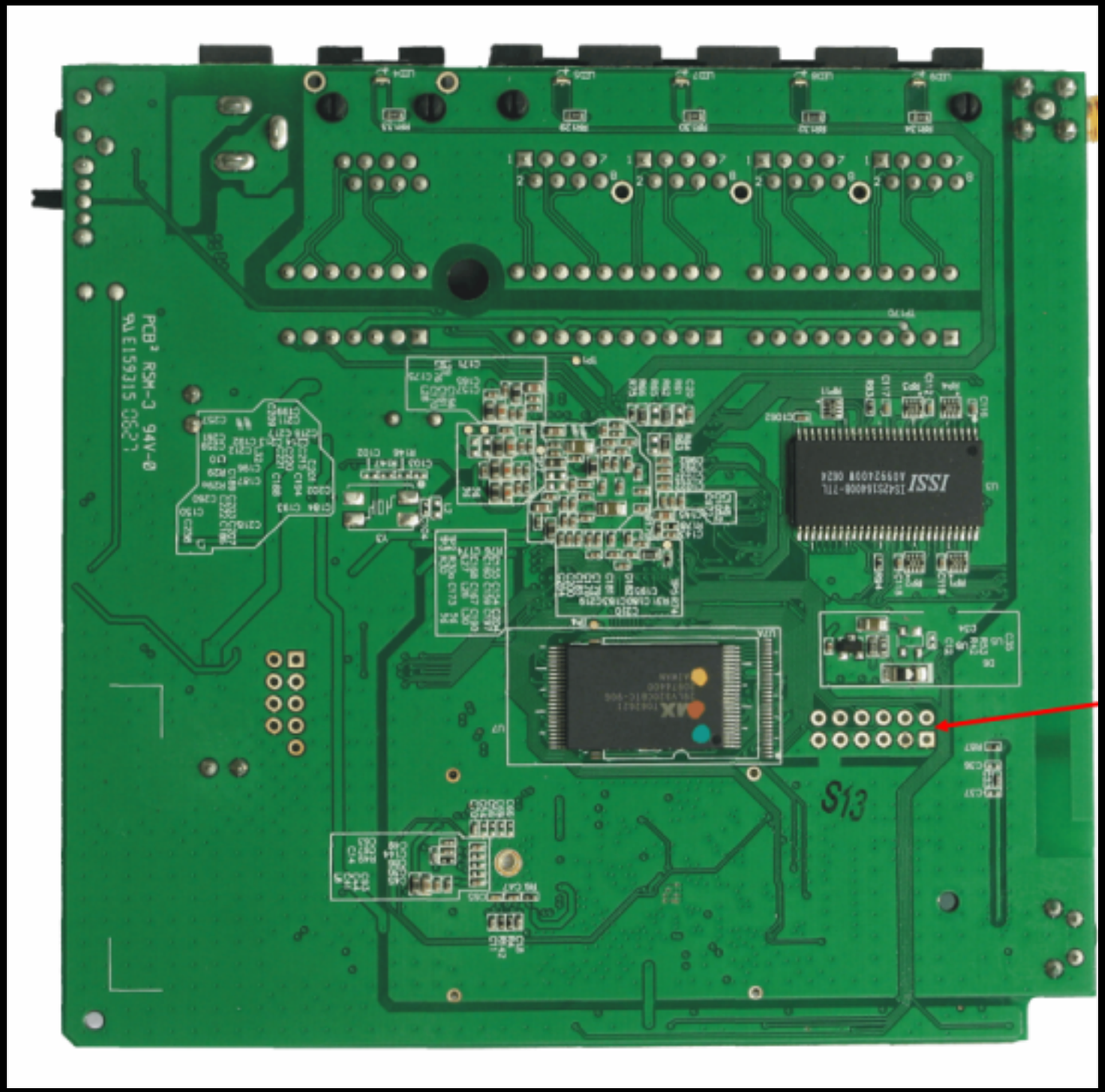


Lovely…:))

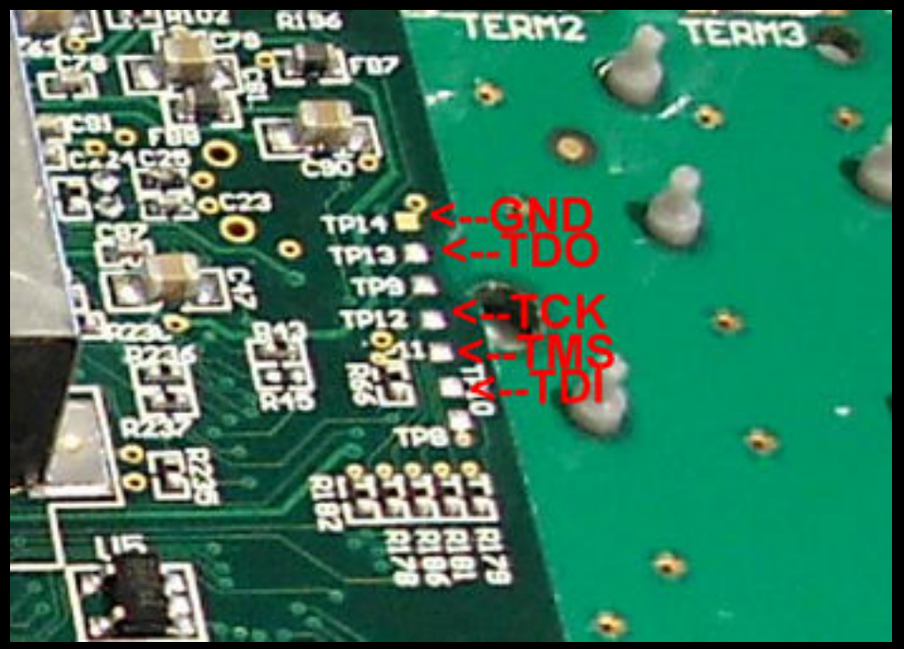


kind pinmap print :)

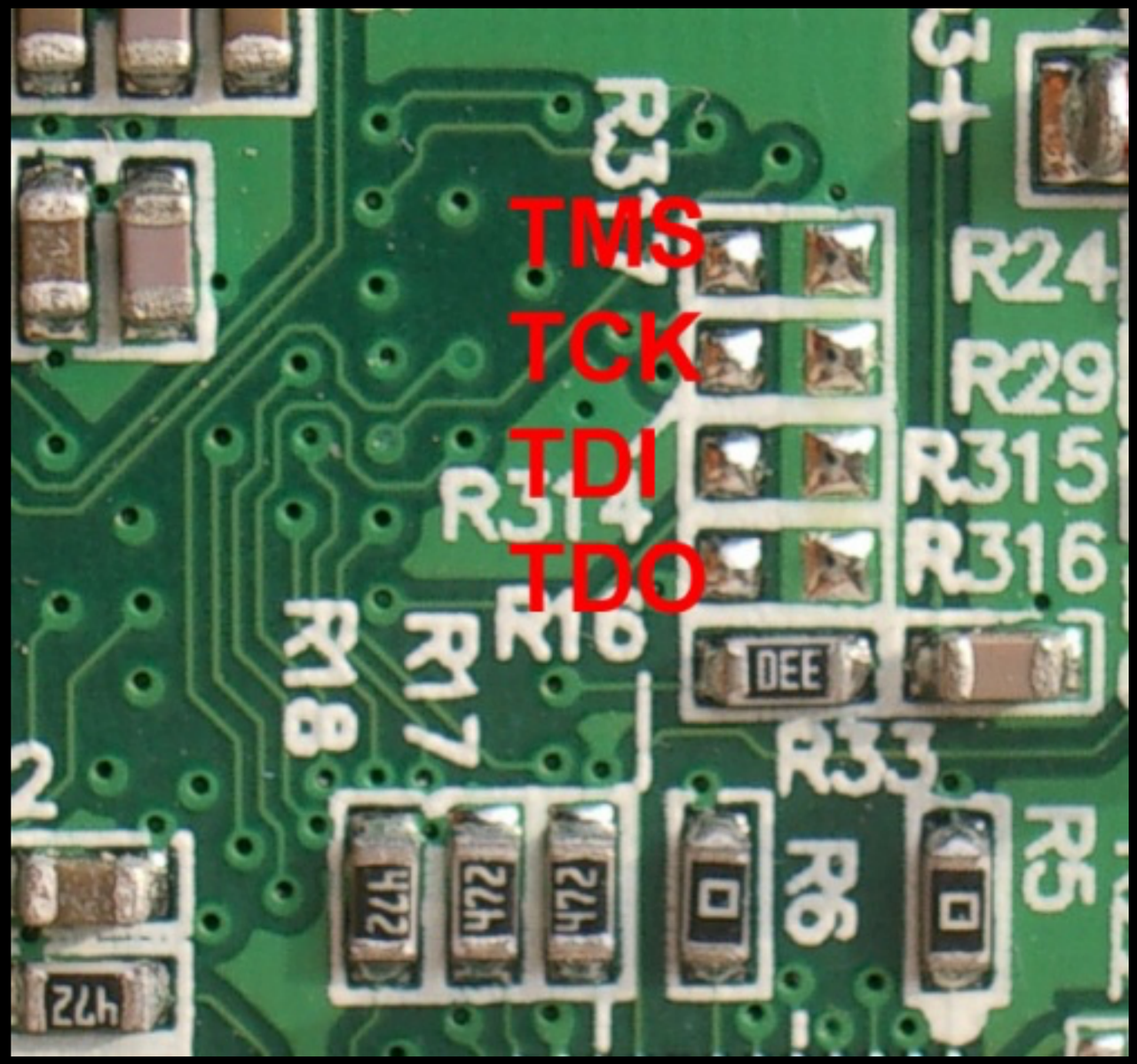
pinmap not printed..
but displayed it’s JTAG



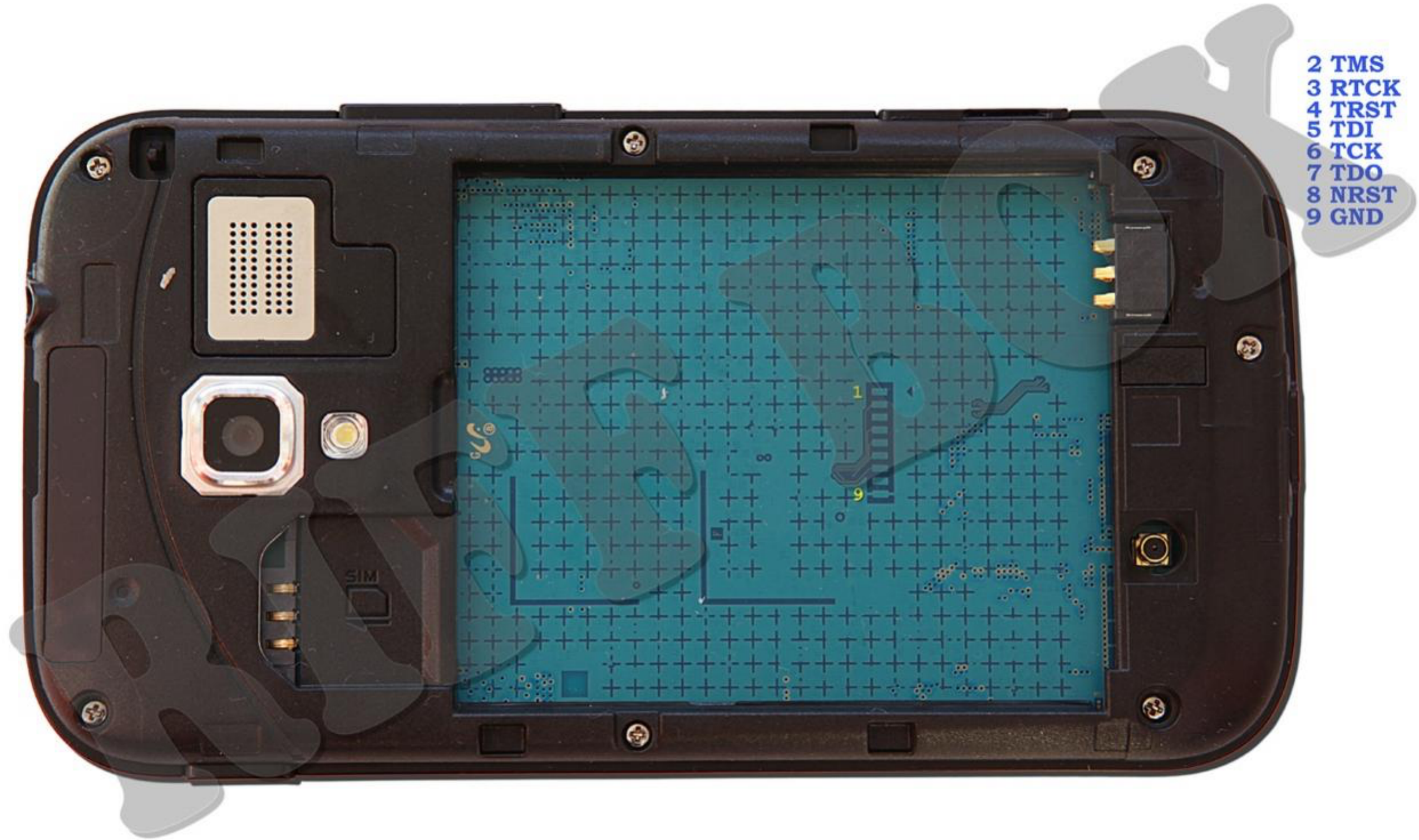
well.. we can guessing yet that is jtag port.



harder and harder to find jtag port.

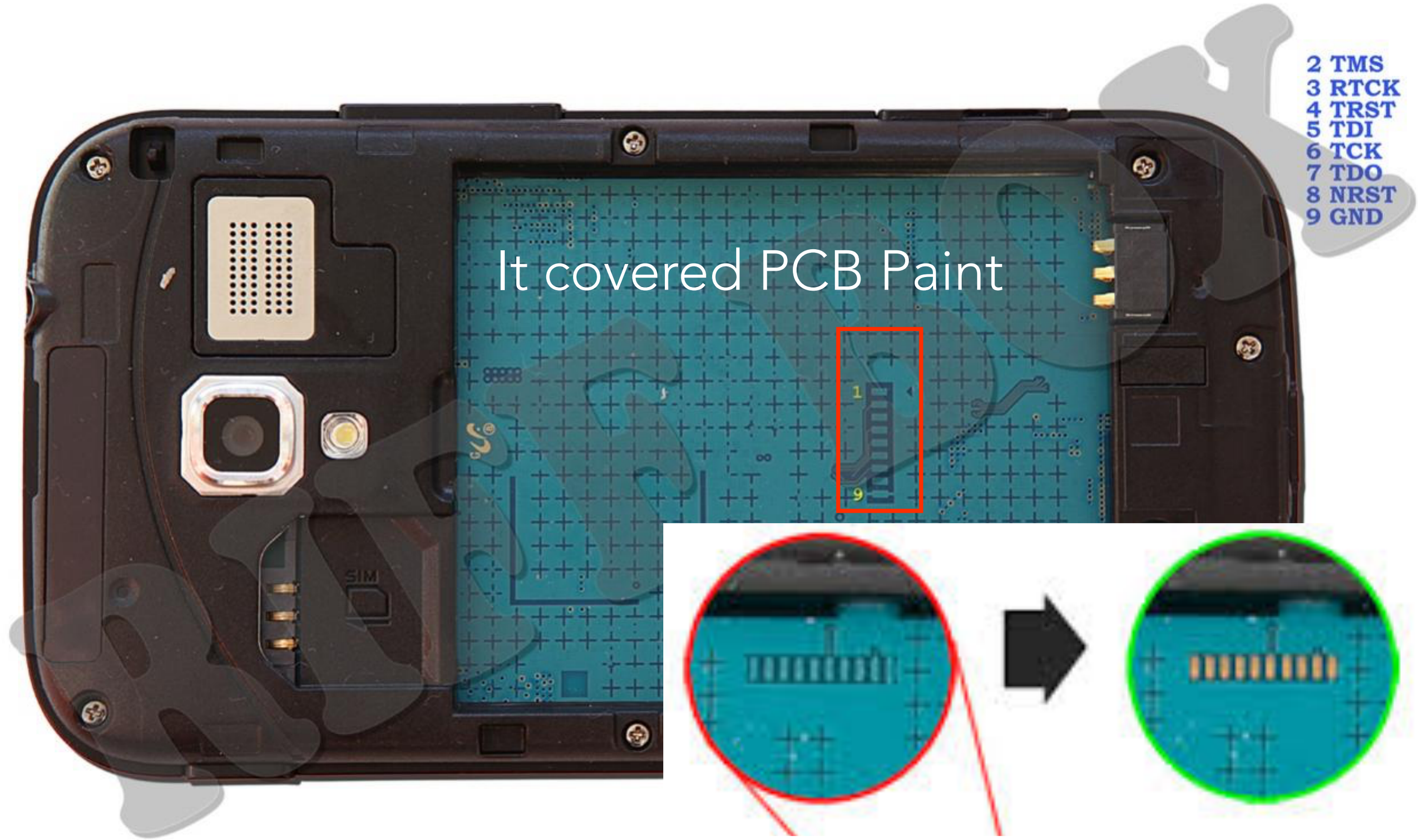

TMS
TCK
TDI
TDO
R24
R29
R315
R316
R314
R16
R17
R18
R33
DEE
472
472
472
472

• • • •

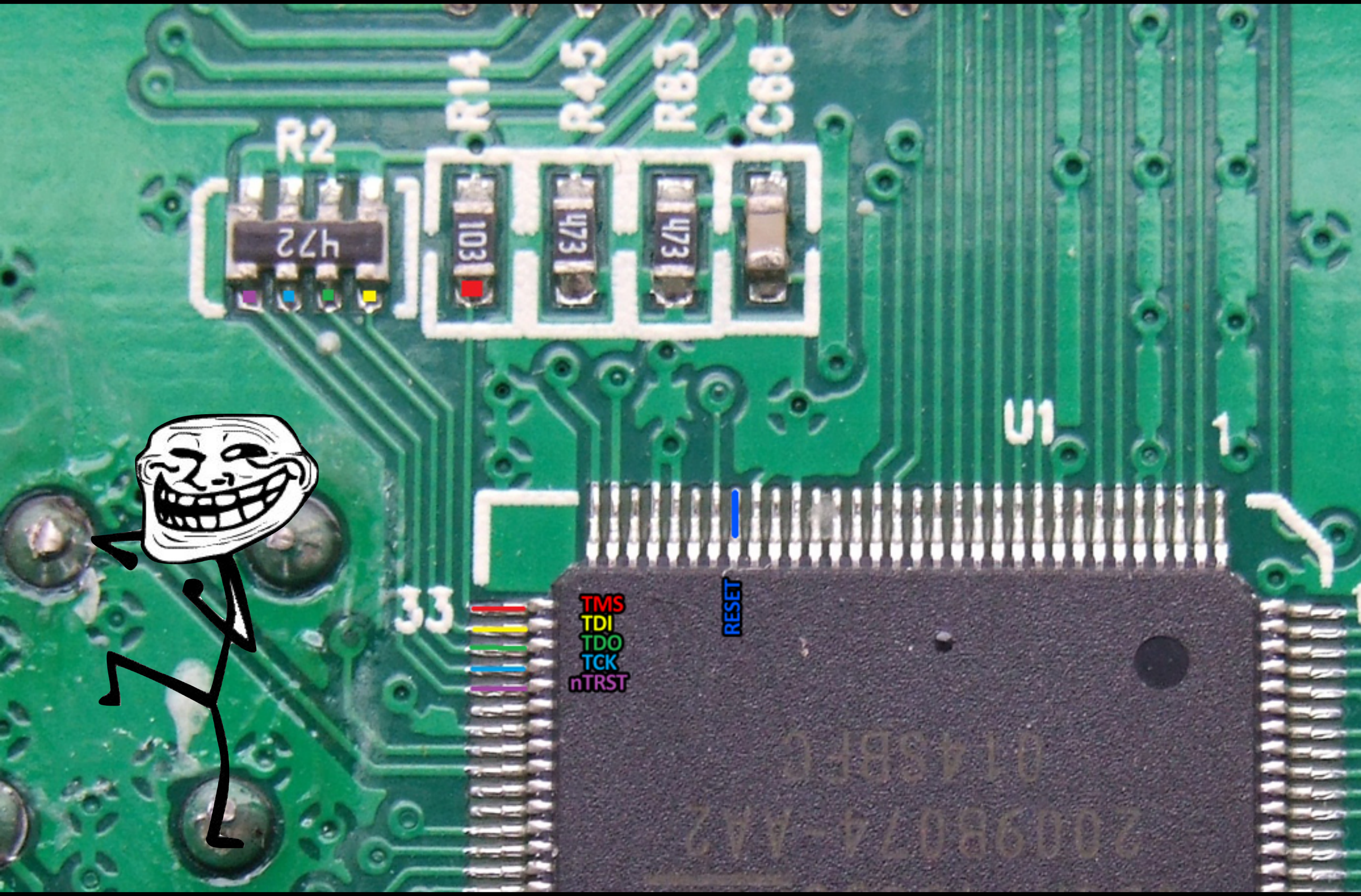


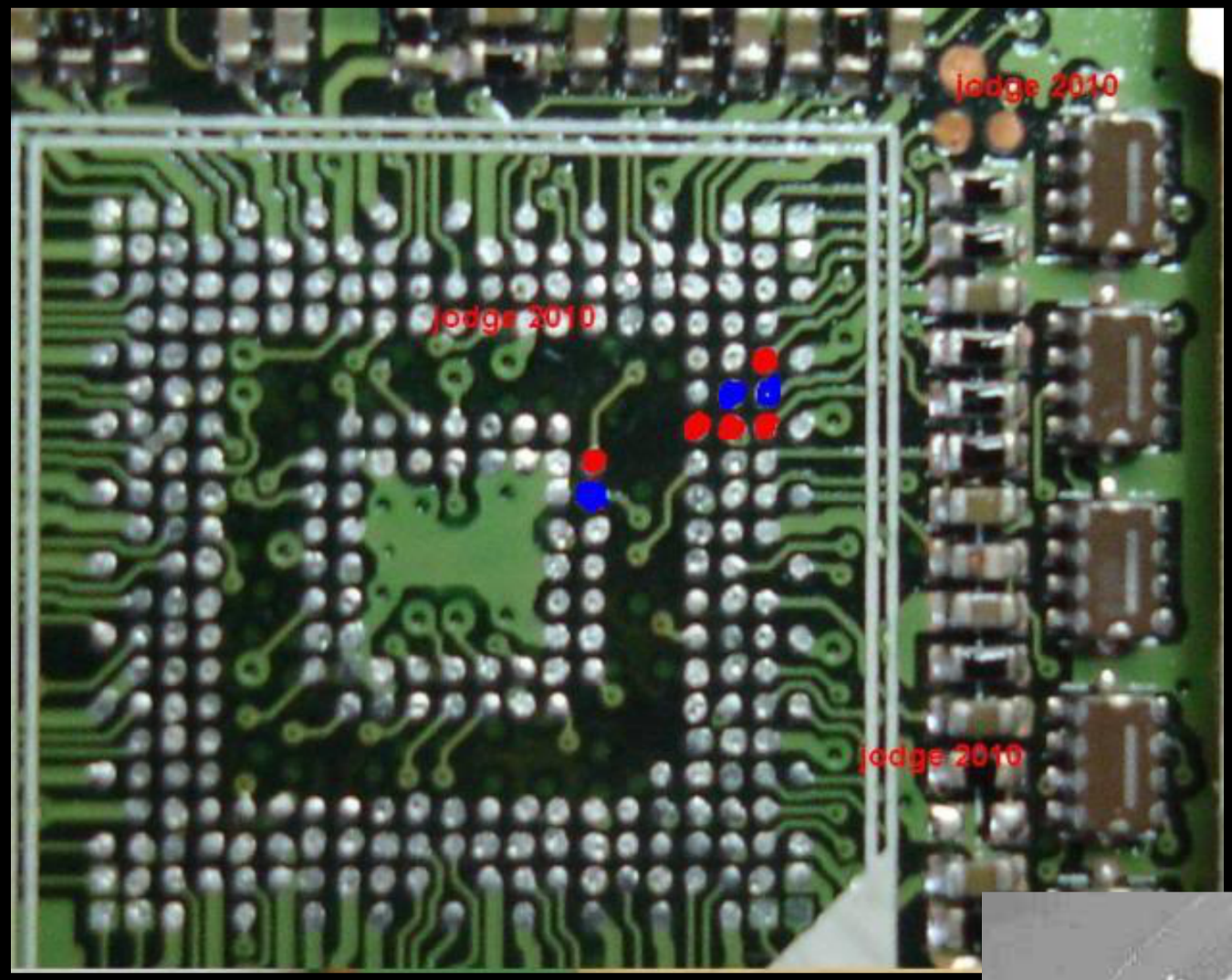
This is Galaxy S3

Where is JTAG Pinout?



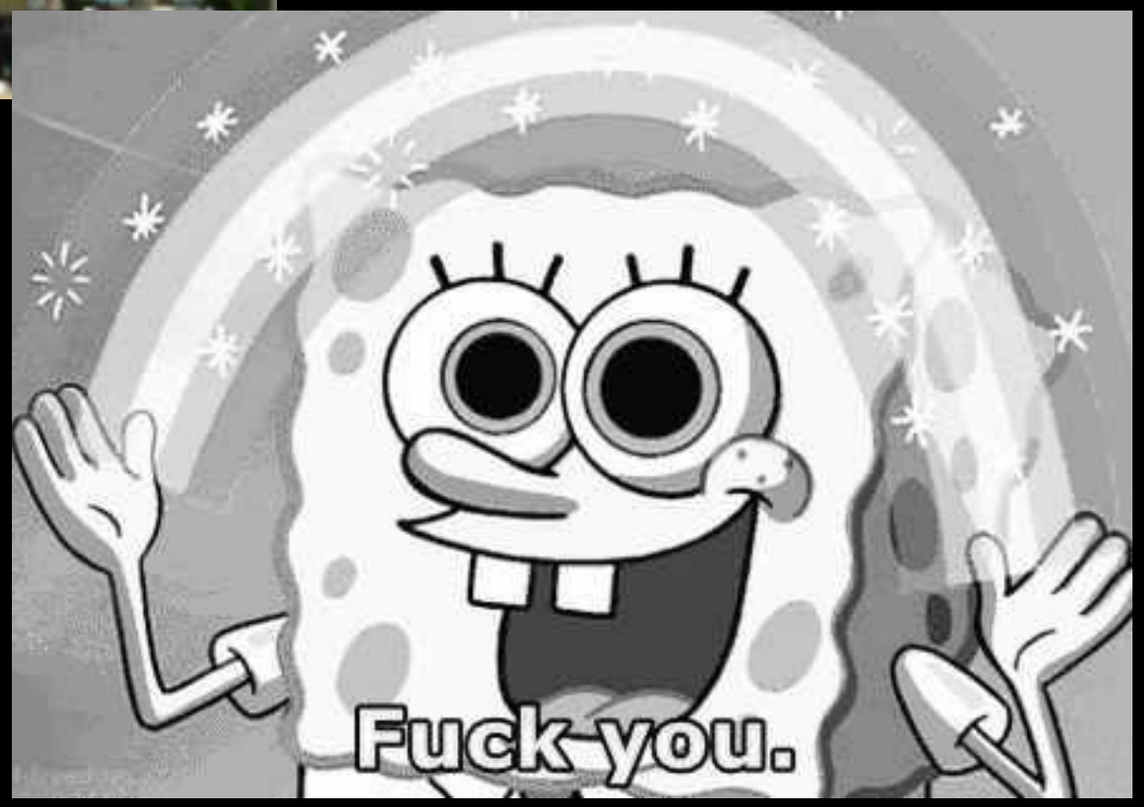
We can use it by scraping paint.


R2
R14
R45
R83
C68
472
103
473
473
U1
1
33
TMS
TDI
TDO
TCK
nTRST
RESET



MCU pinmap tracing directly

(need MCU datasheet)



D22 - TDI I 3.3 CPUs debug port and TAP data input no internal pullup
or pull-down
resistors
E21 - TMS I 3.3 CPUs debug port and TAP mode select
D21 - TCK I 3.3 CPUs debug port and TAP clock
D20 - NOTTRST I 3.3 CPUs debug port and TAP logic reset
E22 - TDO O 3.3 CPUs debug port and TAP data output

Philips DSR 7201 - JTAG

STI 7109

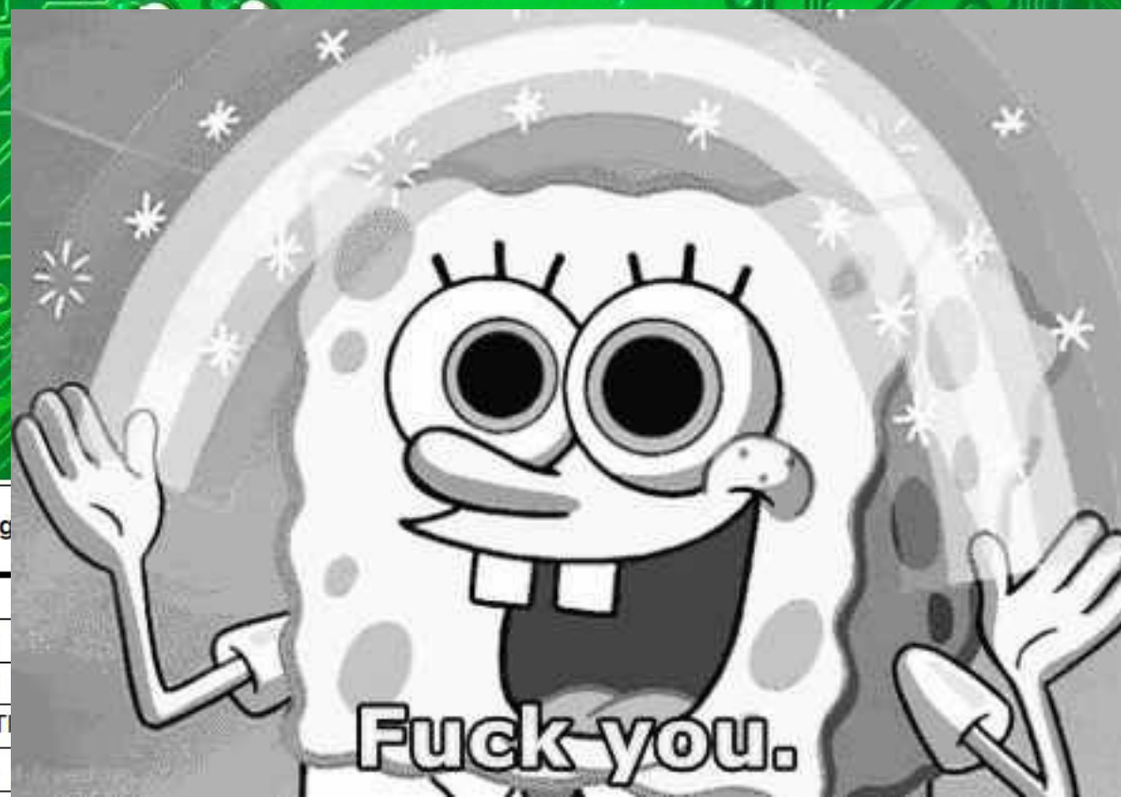
TDI
TDO
TCK
TMS
NOTTRST

Sometime You need tracing

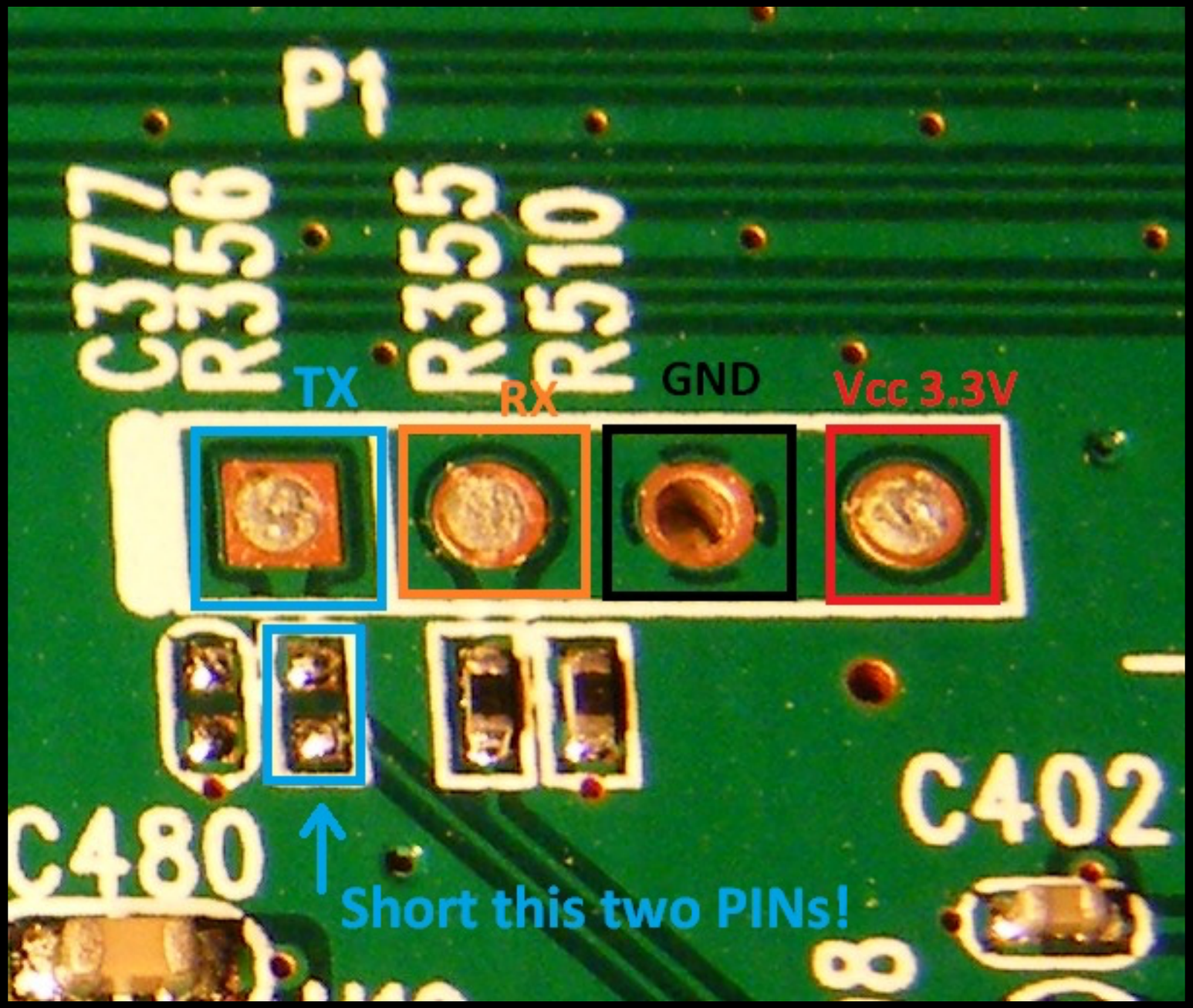
(need MCU datasheet)

TDO
TMS
22
21
20
TDI
TCK
NOTTRST
1
E
D

Pin	Assig
D22	TDI
E21	TMS
D21	TCK
D20	NOTT
E22	TDO



CASE STUDY (UART CIRCUIT HACK)



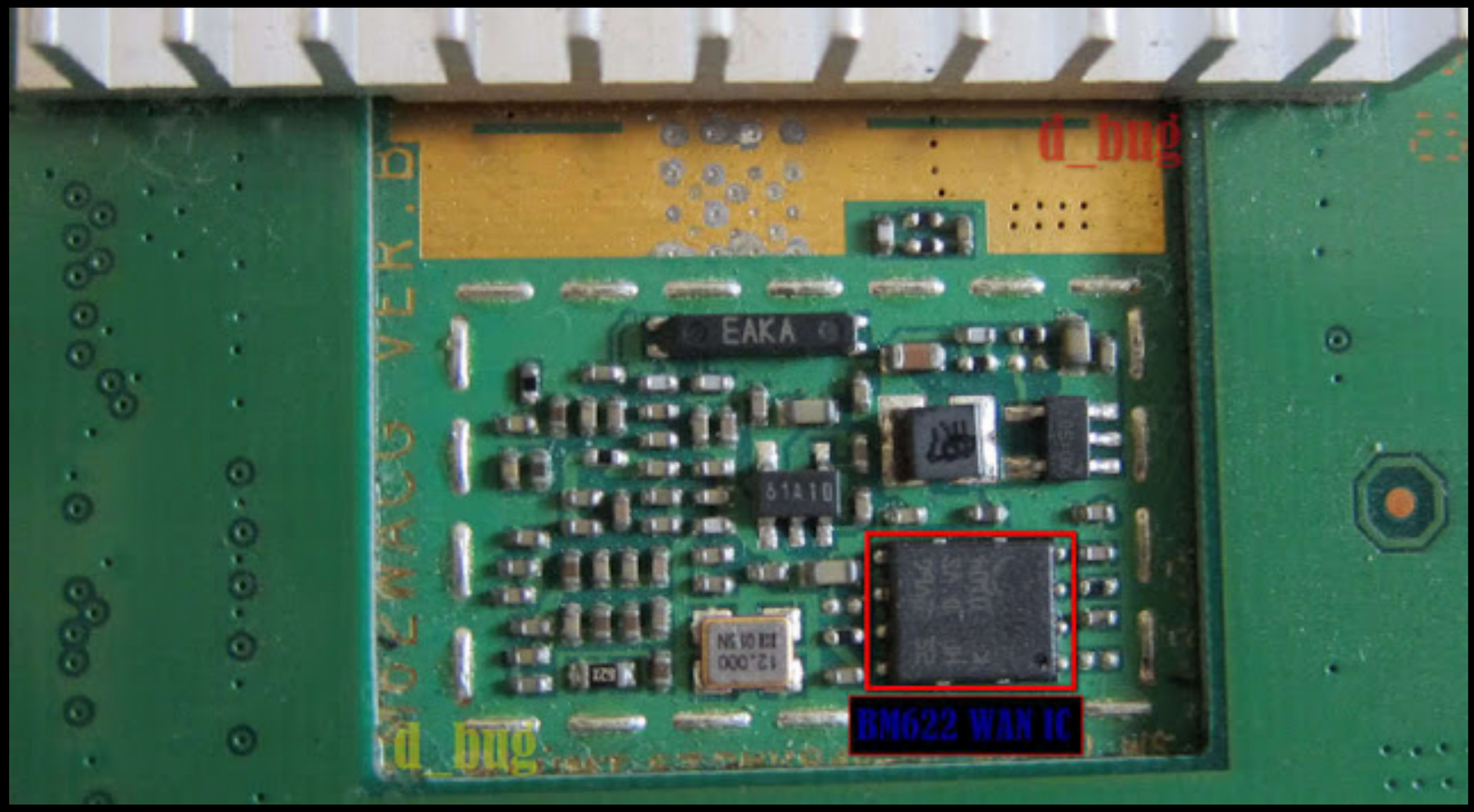
1. trace curcuit.

2.check again using multi tester.

3. short cutted curcuit.

4. enjoy Fun

CASE STUDY (SERIAL FLASH DUMP)



Desoldering It.

And then.. use flashrom

Visit the main page

Main page | Discussion | Read | View source | View hist

flashrom

Home
Recent wiki changes
Hardware support
Programmer support
Latest release

flashrom is a utility for identifying, reading, writing, verifying and erasing flash chips. It is designed to flash BIOS/EFI/coreboot/firmware/optionROM images on mainboards, network/graphics/storage controller cards, and various other programmer devices.

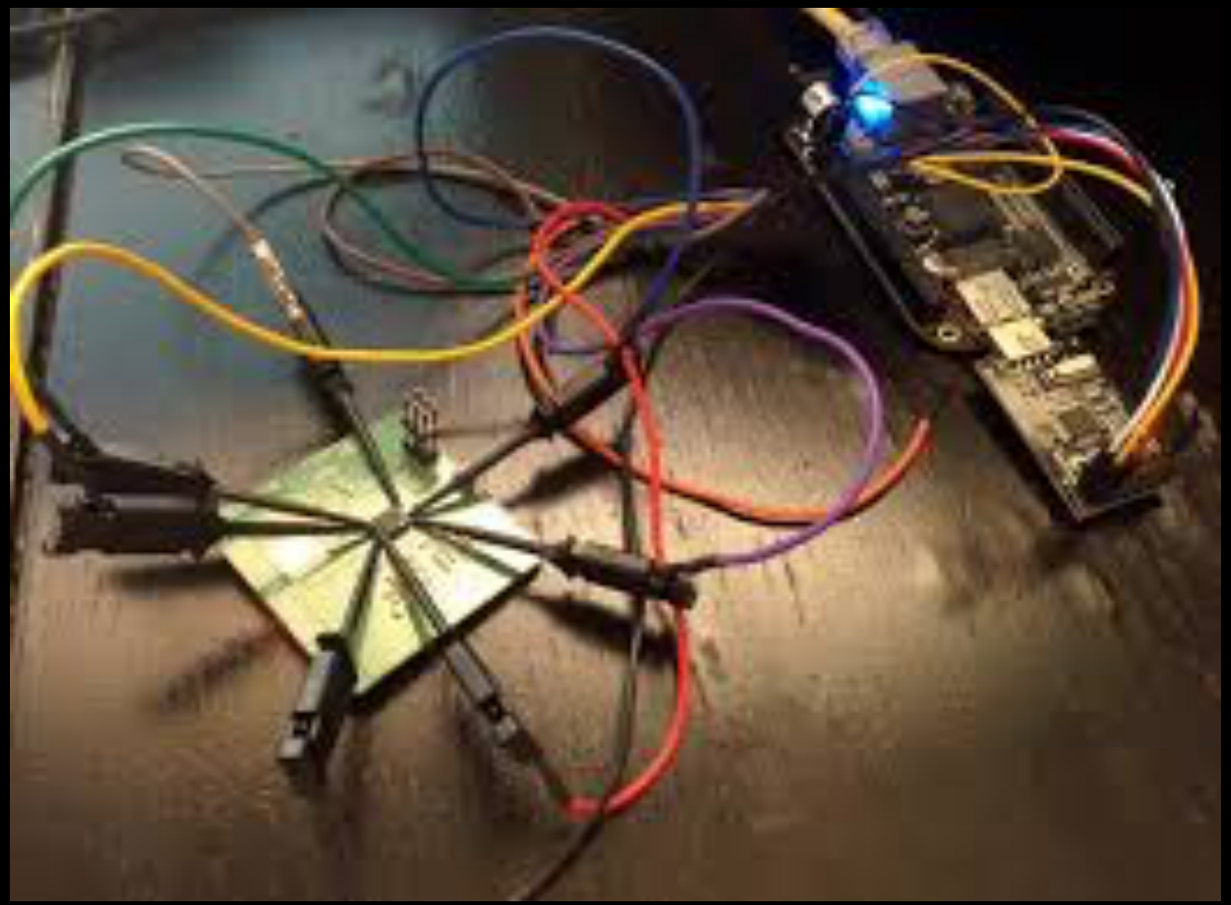
- Supports more than 450 flash chips, 286 chipsets, 450 mainboards, 75 PCI devices, 13 USB devices and various parallel/serial port-based

www.flashrom.org/Supported_hardware

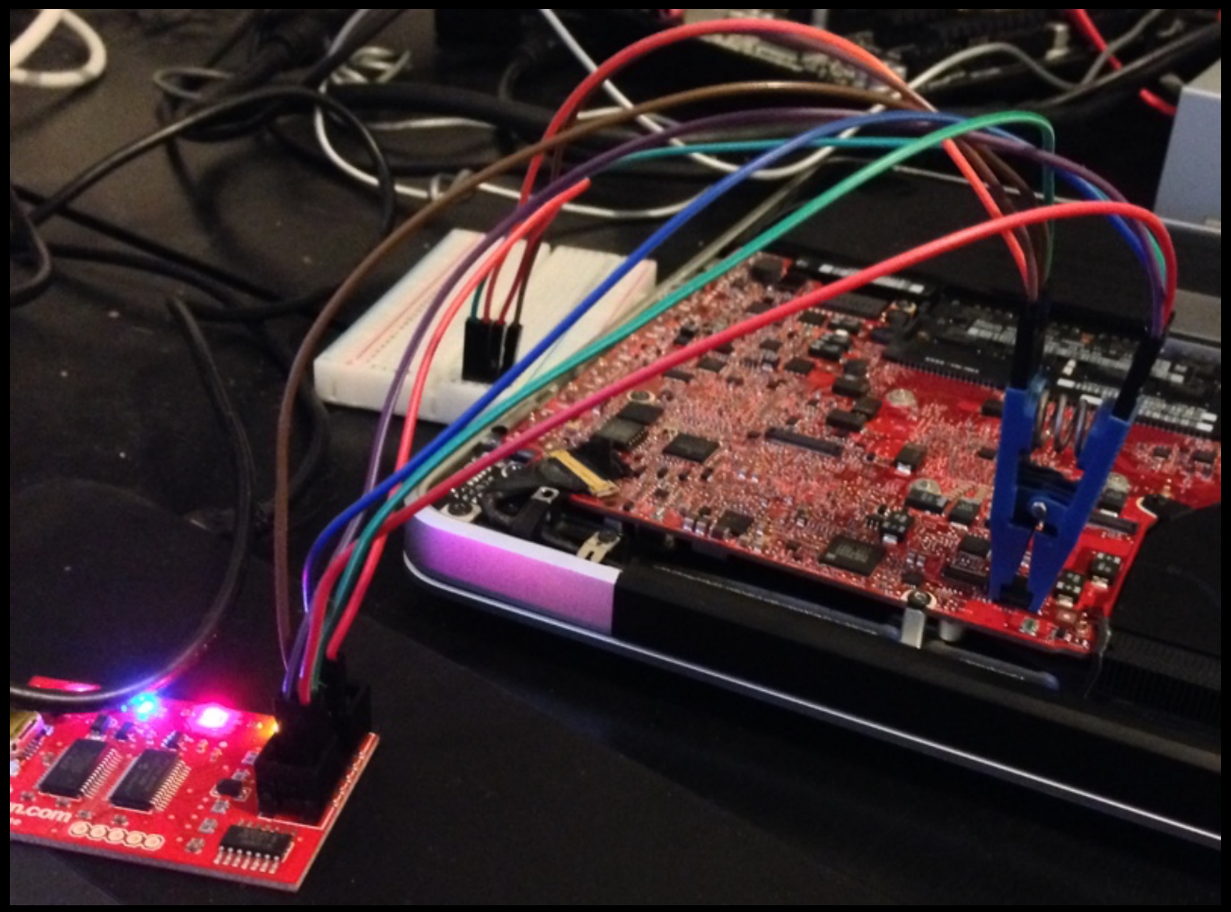
?	?	?	2.700	3.600	Micron/Numonyx/ST	M25PE16	2048	SPI	?	?	?	?	2.7
?	?	?	2.700	3.600	Micron/Numonyx/ST	M25PX80	1024	SPI	OK	OK	OK	OK	2.7
?	?	?	2.700	3.600	Micron/Numonyx/ST	M25PX16	2048	SPI	OK	OK	OK	OK	2.3
?	?	?	2.700	3.600	Micron/Numonyx/ST	M25PX32	4096	SPI	OK	OK	OK	?	2.7
?	?	?	2.700	3.600	Micron/Numonyx/ST	M25PX64	8192	SPI	OK	OK	OK	OK	2.7
OK	OK	OK	2.700	3.600	Micron/Numonyx/ST	M45PE10	128	SPI	?	?	?	?	2.7
?	?	?	2.700	3.600	Micron/Numonyx/ST	M45PE20	256	SPI	?	?	?	?	2.7
?	?	?	2.700	3.600	Micron/Numonyx/ST	M45PE40	512	SPI	?	?	?	?	2.7
?	?	?	2.700	3.600	Micron/Numonyx/ST	M45PE80	1024	SPI	?	?	?	?	2.7
?	?	?	4.500	5.500	Micron/Numonyx/ST	M45PE16	2048	SPI	?	?	?	?	2.7

(Support hardware list)

R is well
R is well
R is well
R is well
R is well



(the case of
soldering to empty pcb)



(the case of
using SPI adhering tool
instead of desoldering)

```
administrator@administrator-VirtualBox: ~/flashrom/flashrom
administrator@administrator-VirtualBox:~/flashrom/flashrom$ sudo ./flashrom -p ft2232_spi:type=t
umpa,port=B -r flash.bin
[sudo] password for administrator:
flashrom v0.9.8-r1889 on Linux 3.16.0-30-generic (x86_64)
flashrom is free software, get the source code at http://www.flashrom.org

Calibrating delay loop... OK.
Found PMC flash chip "Pm25LD020(C)" (256 kB, SPI) on ft2232_spi.
===
This flash part has status UNTESTED for operations: PROBE READ ERASE WRITE
The test status of this chip may have been updated in the latest development
version of flashrom. If you are running the latest development version,
please email a report to flashrom@flashrom.org if any of the above operations
work correctly for you with this flash chip. Please include the flashrom log
file for all operations you tested (see the man page for details), and mention
which mainboard or programmer you tested in the subject line.
Thanks for your help!
Reading flash... done.
administrator@administrator-VirtualBox:~/flashrom/flashrom$
```

identifying target hardware.

done

flashrom drop dump data to -> ./flash.bin

CONCLUSION

- 임베디드의 미티게이션 앞에 두려움이 생길 수 있지만
  케바케로 공략이 가능합니다.

- 사람은 실수의 동물이기 때문에 보드를 태워먹을 수 있지만
  무상 AS기간을 잘 이용합시다. (기사님들 죄송해요 ><)

- 분석대상의 건강과 분석자의 정신건강을 잘 챙겨서
  엔조이 임베디드 해킹 하세요~

- 우리는 답을 찾을 것입니다 늘 그래왔듯이.