Hardware Hacking 101

Finding Entry Point

Jeong Wook Oh

oh.jeongwook@gmail.com

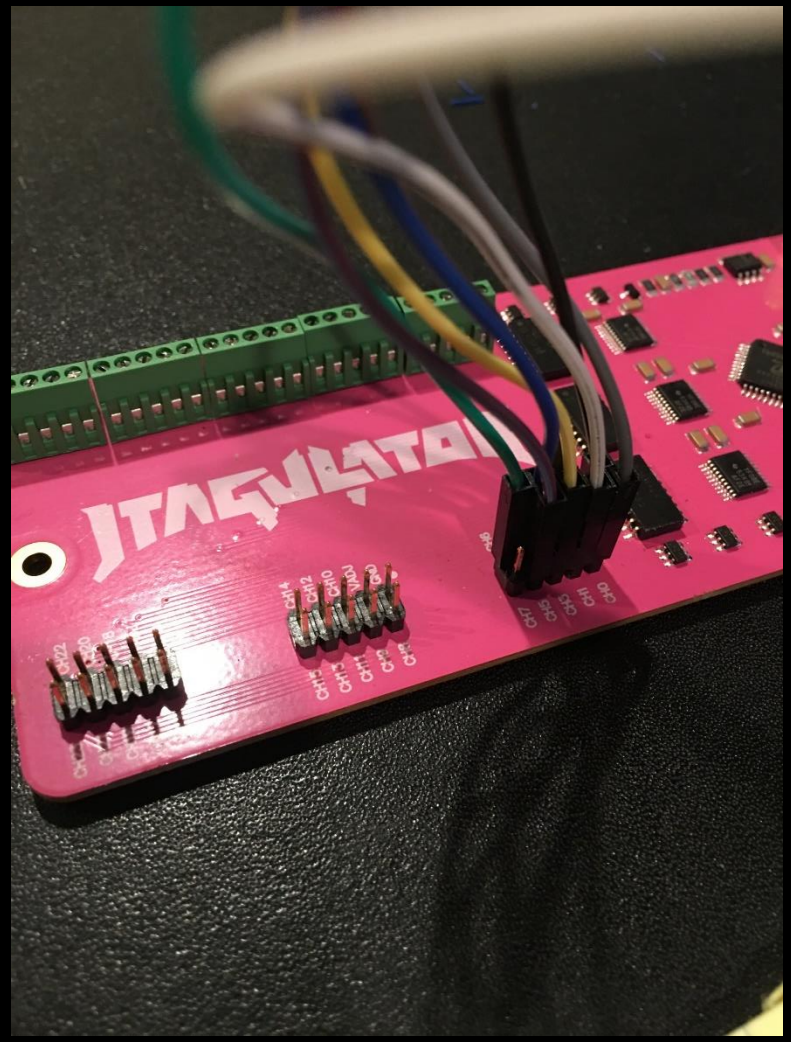
Objectives

- Finding Vulnerabilities
- Forensic Analysis
- Modding
- Just for fun

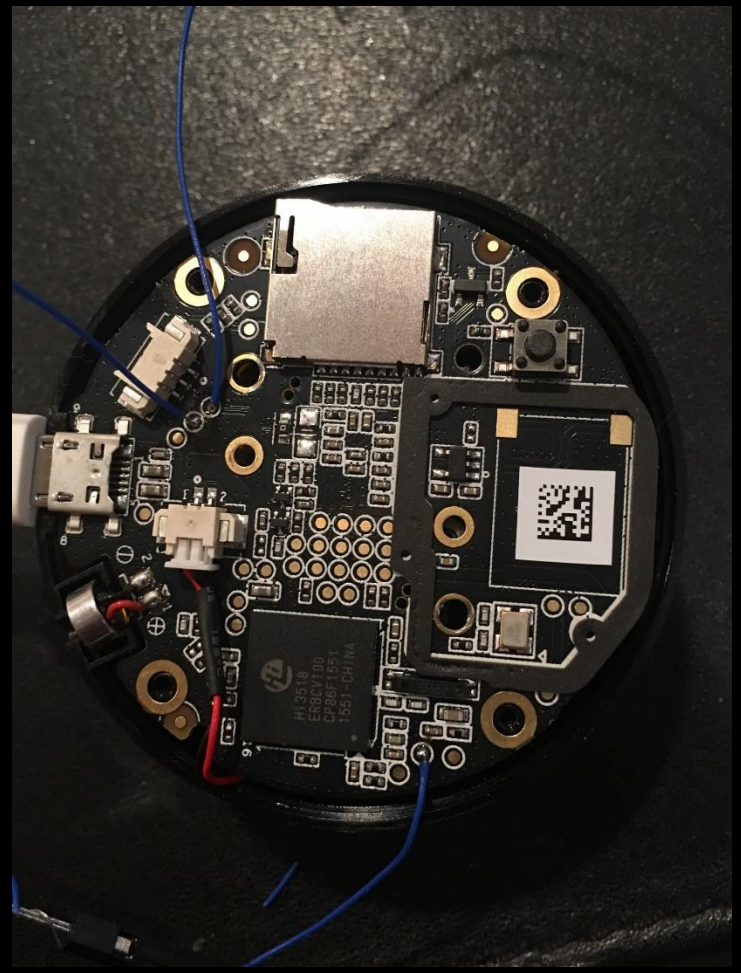
Entry Point

- UART
- JTAG
- Storage
- Bus?

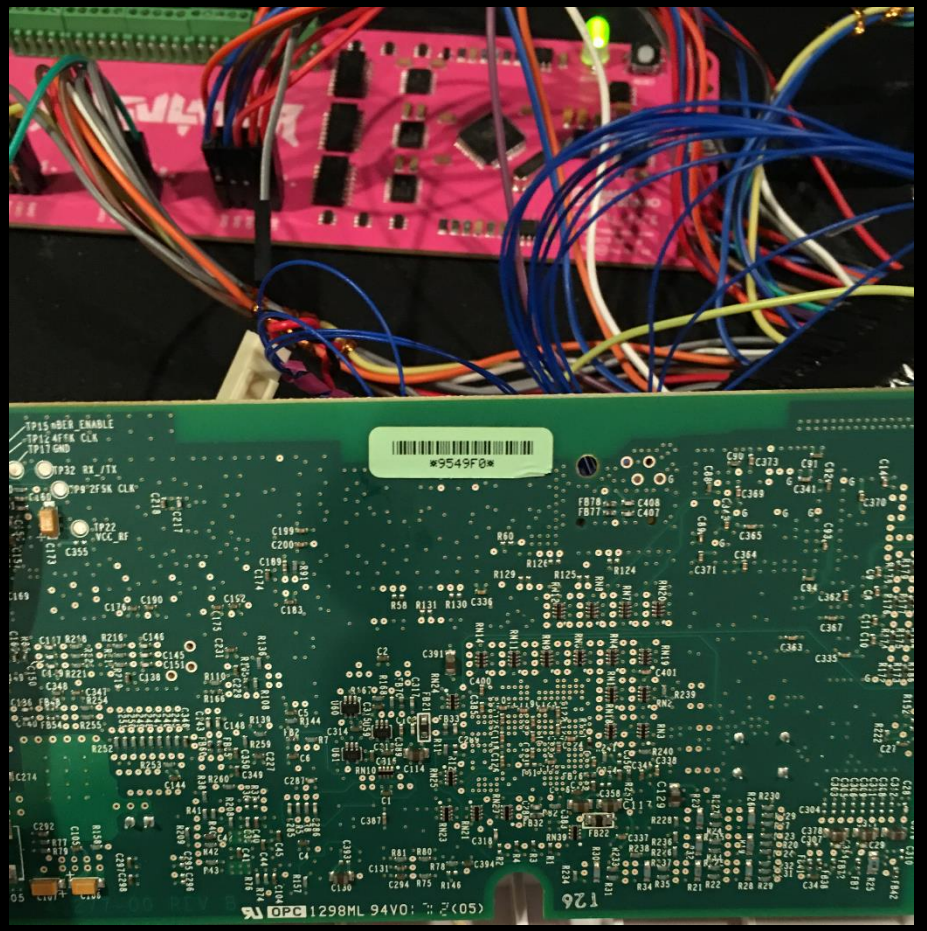
JTAGulator – automation with finding entry point



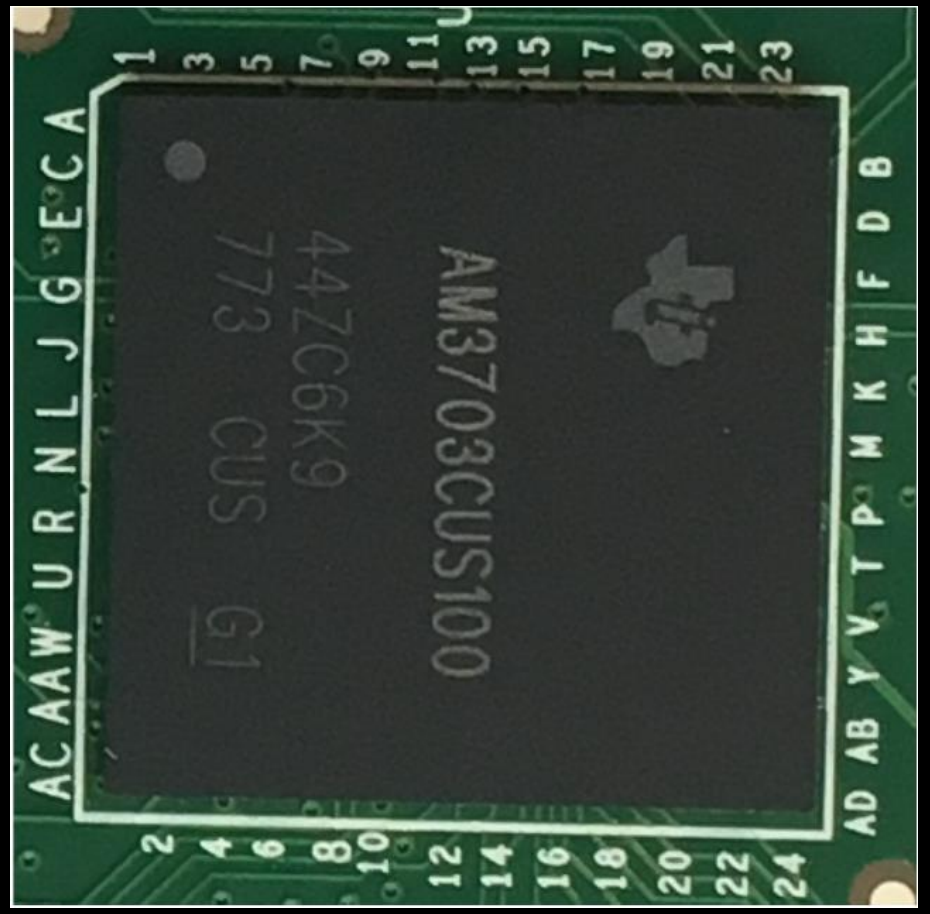
JTAGulator - works sometimes?



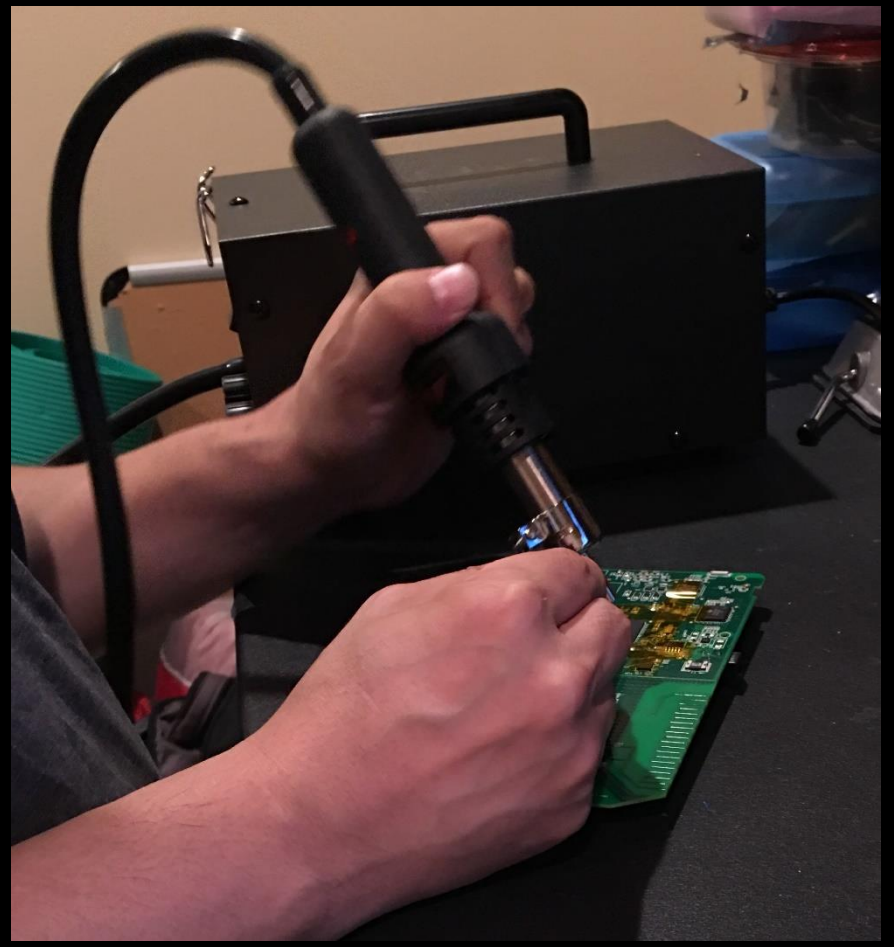
JTAGulator - usually fails



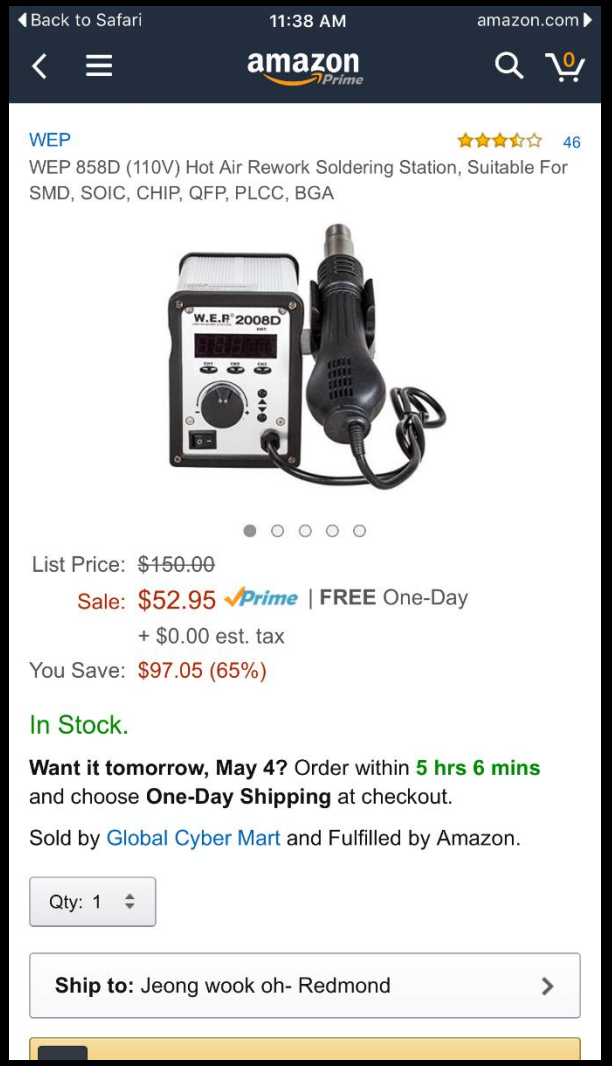
CPU



Desoldering

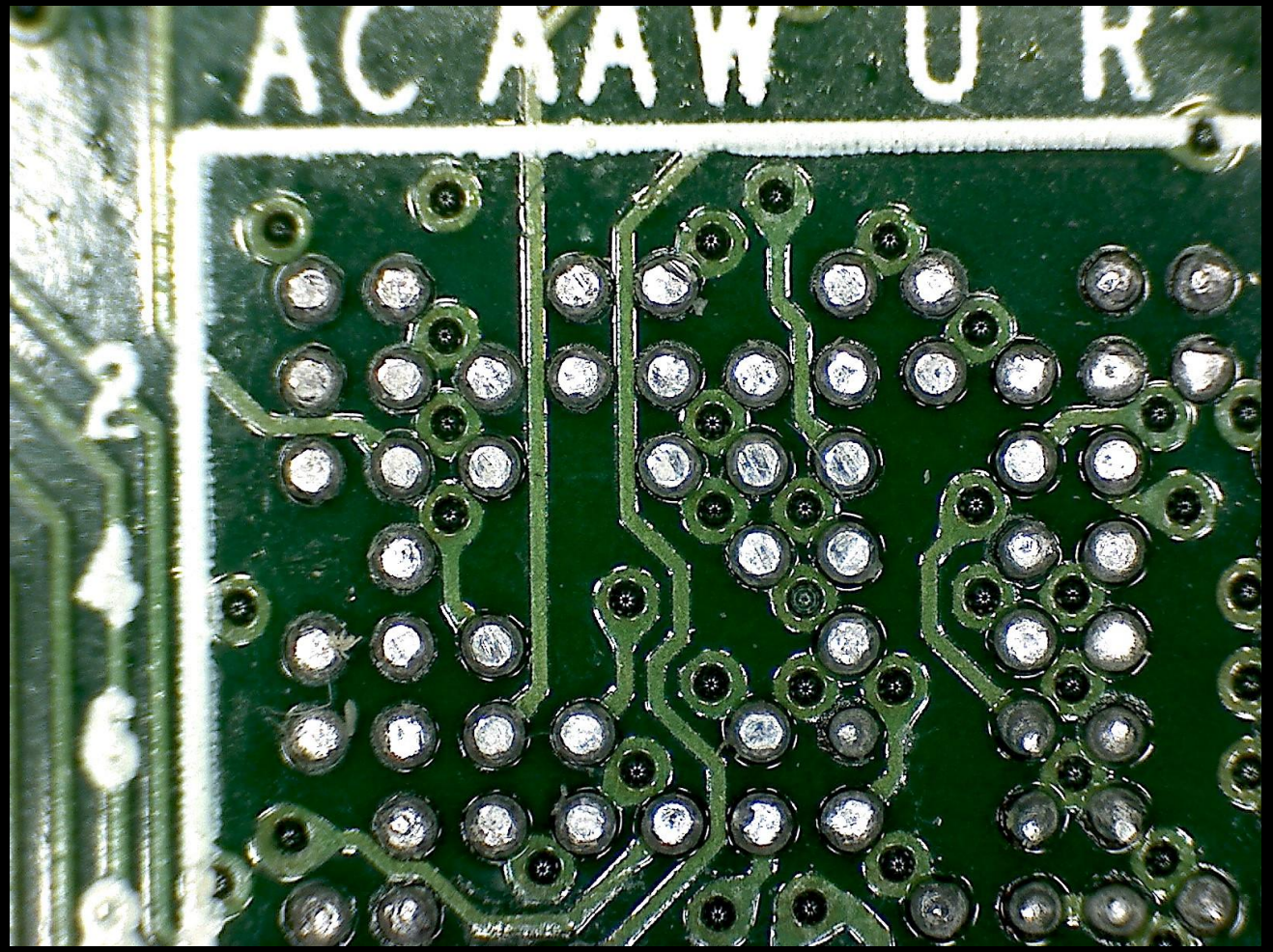


Cheap hot air blower

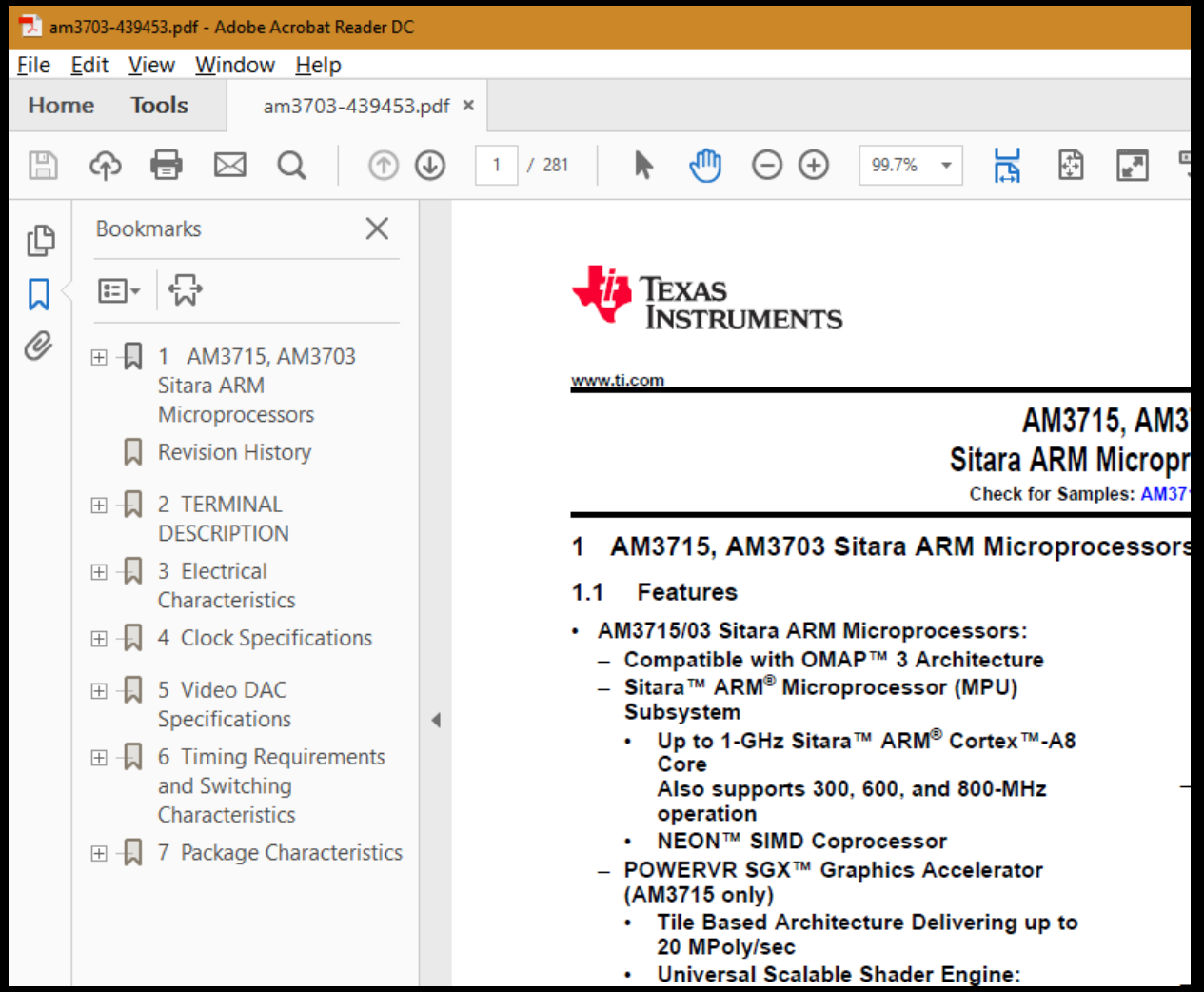


Pins exposed

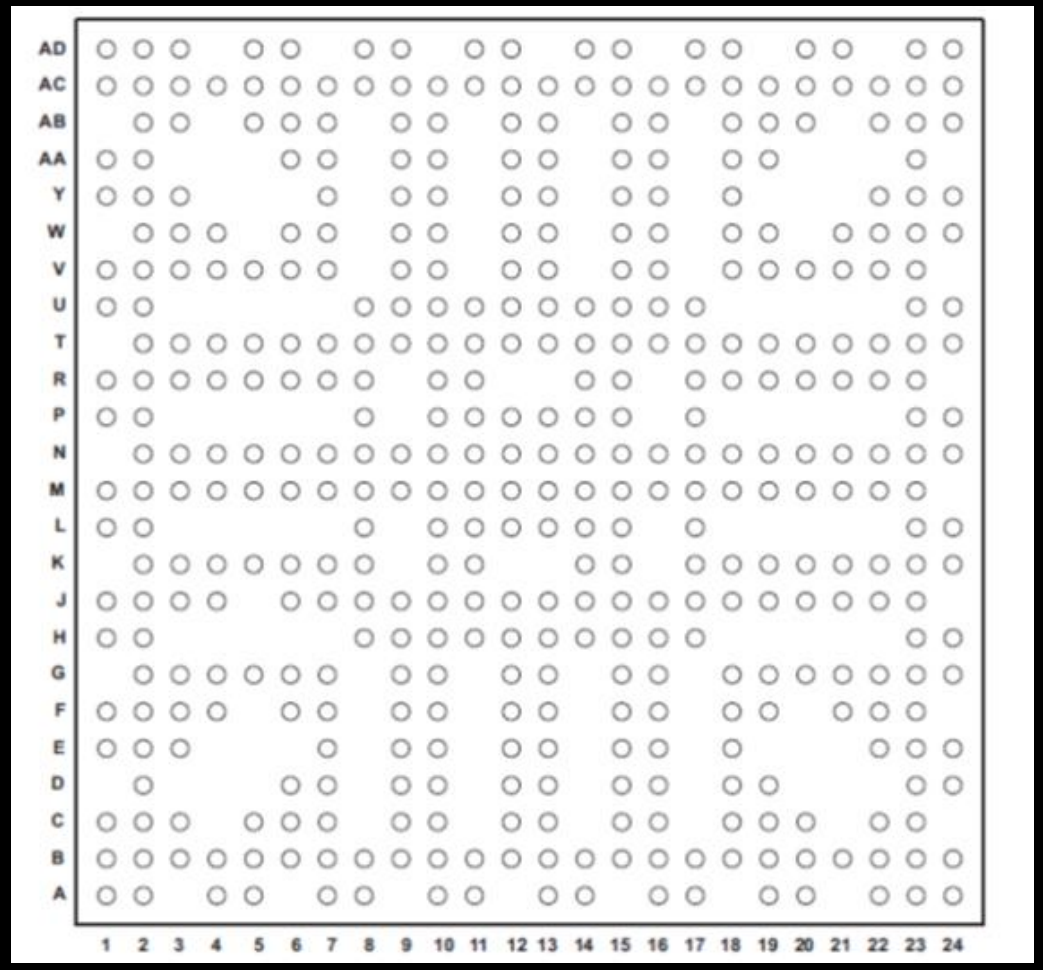
Finding pins and connection points



Finding spec documents



Pin layout

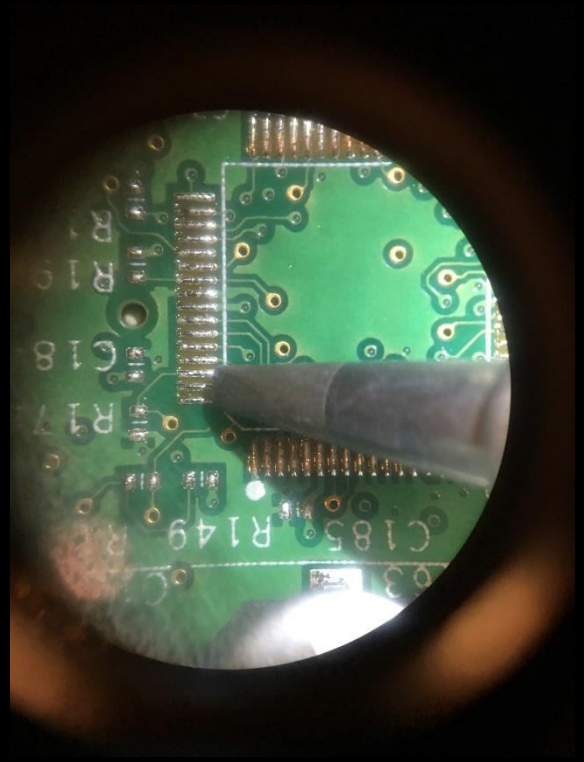


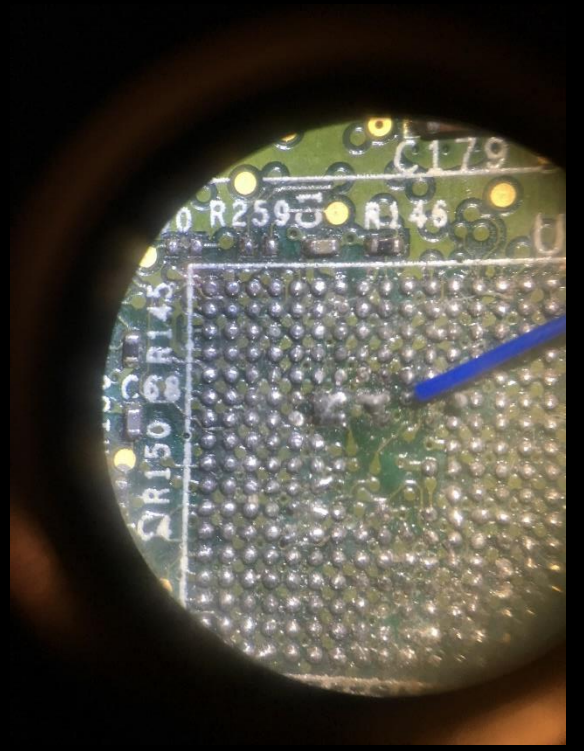
	1	2	3	4	5	6	7	8	9	10	11	12
N		gpmc_d3	mcspi2_somi	mcspi2_simo	mcspi2_clk	vdd_mpu_iva	vdd_mpu_iva	vdd_mpu_iva	vss	vss	vss	vss
P	gpmc_d5	gpmc_d6						vss		vss	vss	vss
R	gpmc_d7	gpmc_d8	gpmc_d11	mcspi1_simo	mcbsp1_cs3	vdd_mpu_iva	vdd_mpu_iva	vdd_mpu_iva		vss	vss	
T		gpmc_d9	gpmc_d12	mcspi1_somi	mcspi1_clk	mcspi1_cs0	vdd_mpu_iva	vdd_mpu_iva	vss	vss	vss	vss
U	gpmc_d10	gpmc_d13						cap_vdd_sram_mpu_iva	vss	vdds	vss	vdd_mpu_iva
V	gpmc_d14	gpmc_d15	mmc2_dat3	mcbsp3_fsx	mcbsp3_dr	mcbsp3_dx	uart1_rx		vdds	vdds		vdd_mpu_iva
W		gpmc_clk	mmc2_dat2	mcbsp3_clkx		uart1_rts	uart1_tx		vdds	vdds		vdd_mpu_iva
Y	mmc2_clk	mmc2_dat6	mmc2_dat1				sys_clkout1		vdds	sys_nres warm		cap_vddu_wkup_logic
AA	mmc2_dat7	mmc2_dat5				sys_clkout2	jtag_rtck		jtag_tms_tmsc	sys_nres pwron		vdds_sram
AB		mmc2_dat4	mmc2_dat0		mmc2_cmd	jtag_tck	jtag_ntrst		jtag_tdo	jtag_tdi		sys_boot0
AC	etk_clk	uart1_cts	etk_d10	etk_d8	etk_d4	etk_d1	etk_d2	etk_d6	etk_d11	etk_d12	etk_d14	i2c3_sda
AD	NC	etk_d5	etk_ctl		etk_d9	etk_d0		etk_d3	etk_d7		etk_d13	etk_d15

Figure 2-16. CUS Pin Map [Quadrant C - Top View]

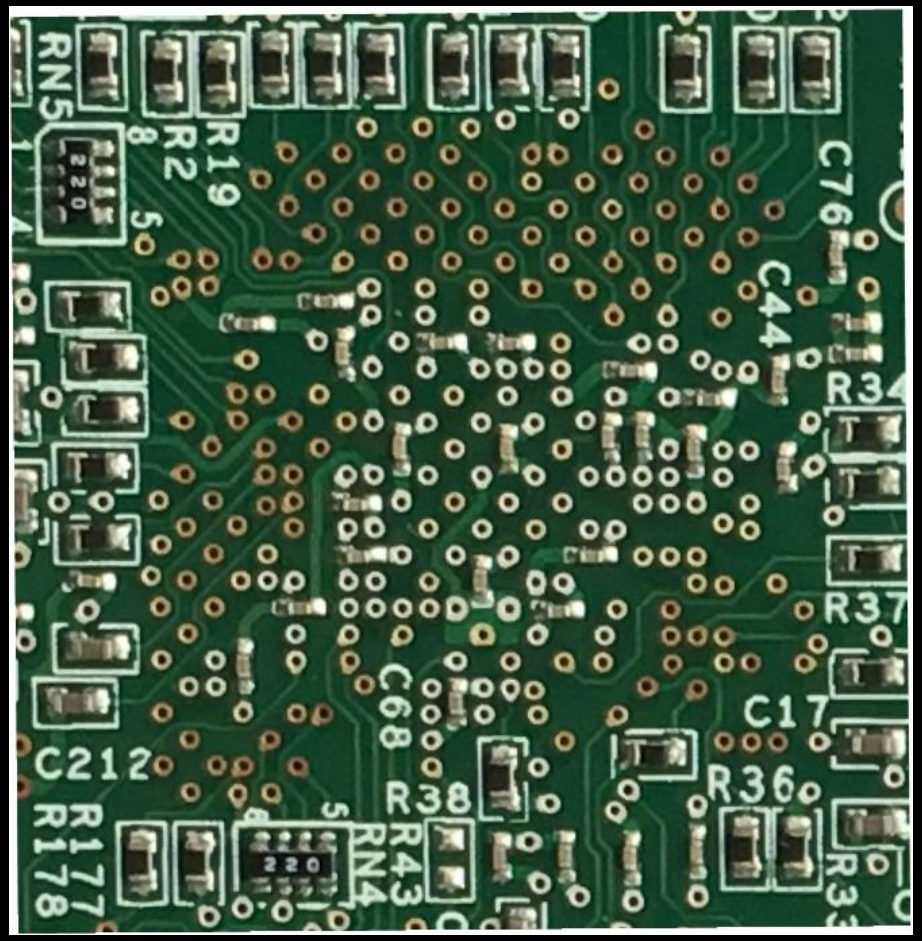
Microscope

Increased performance





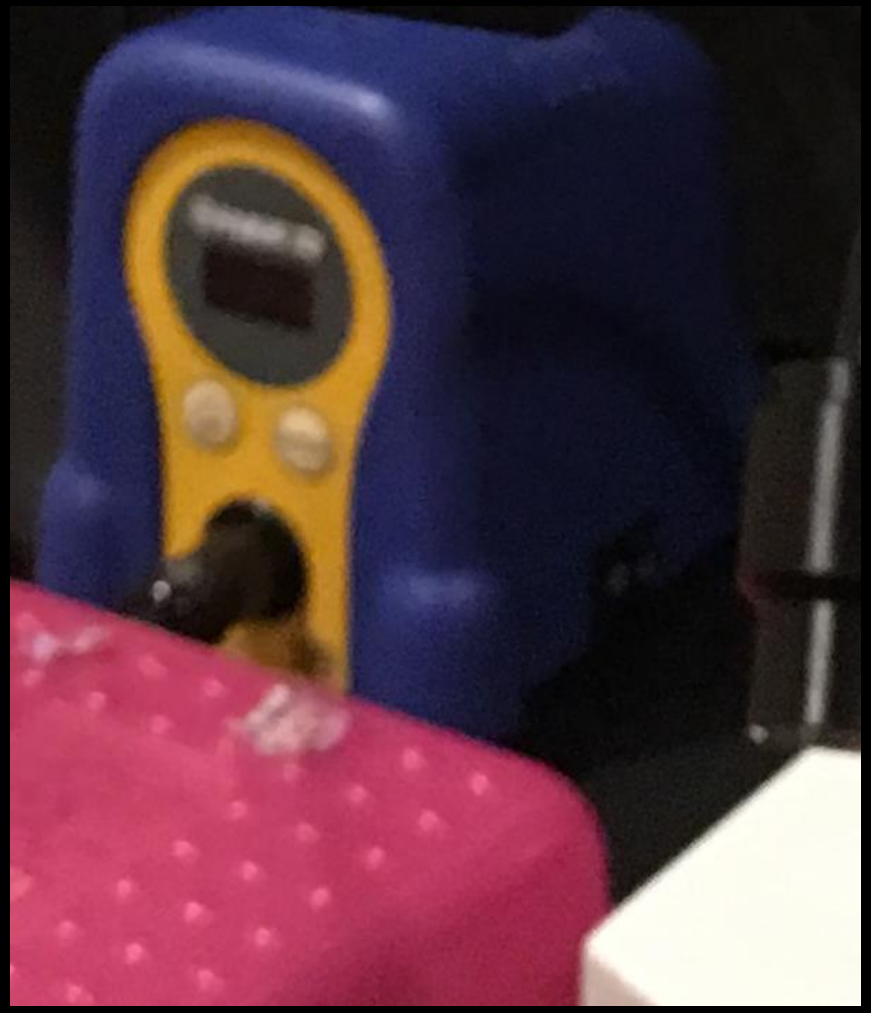
Possible connection points

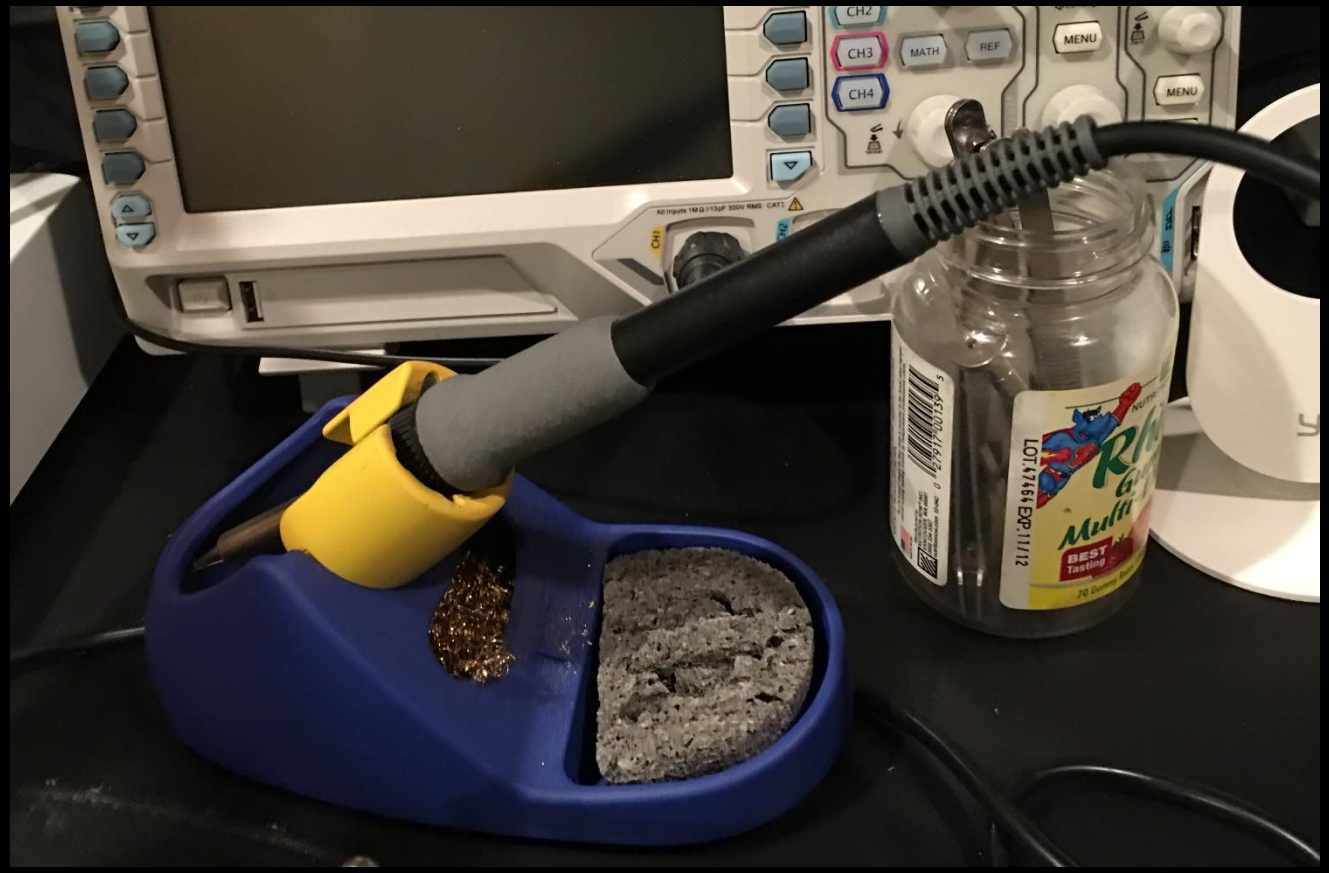


Tools of choice

Finding ground

Good solder iron

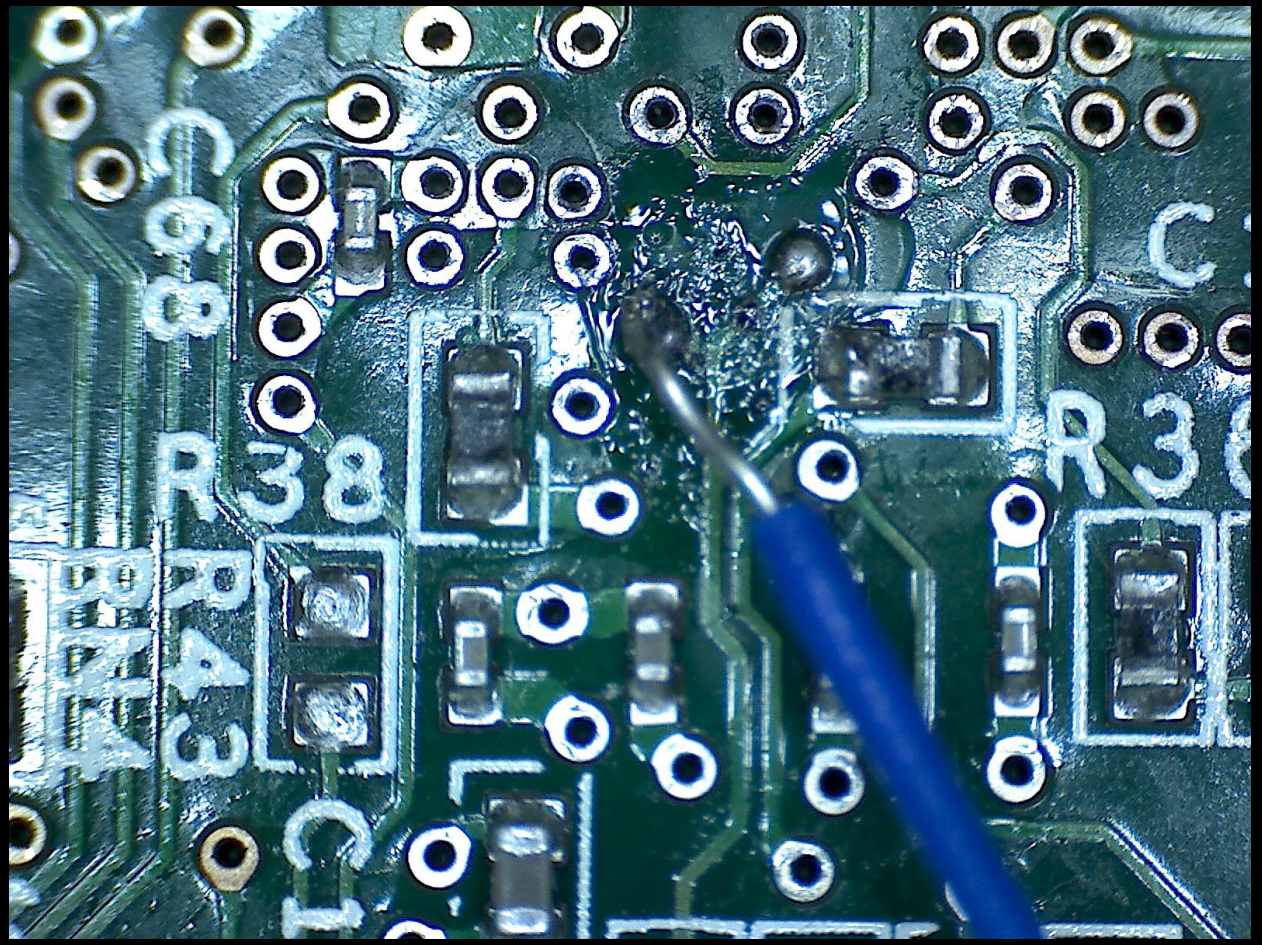




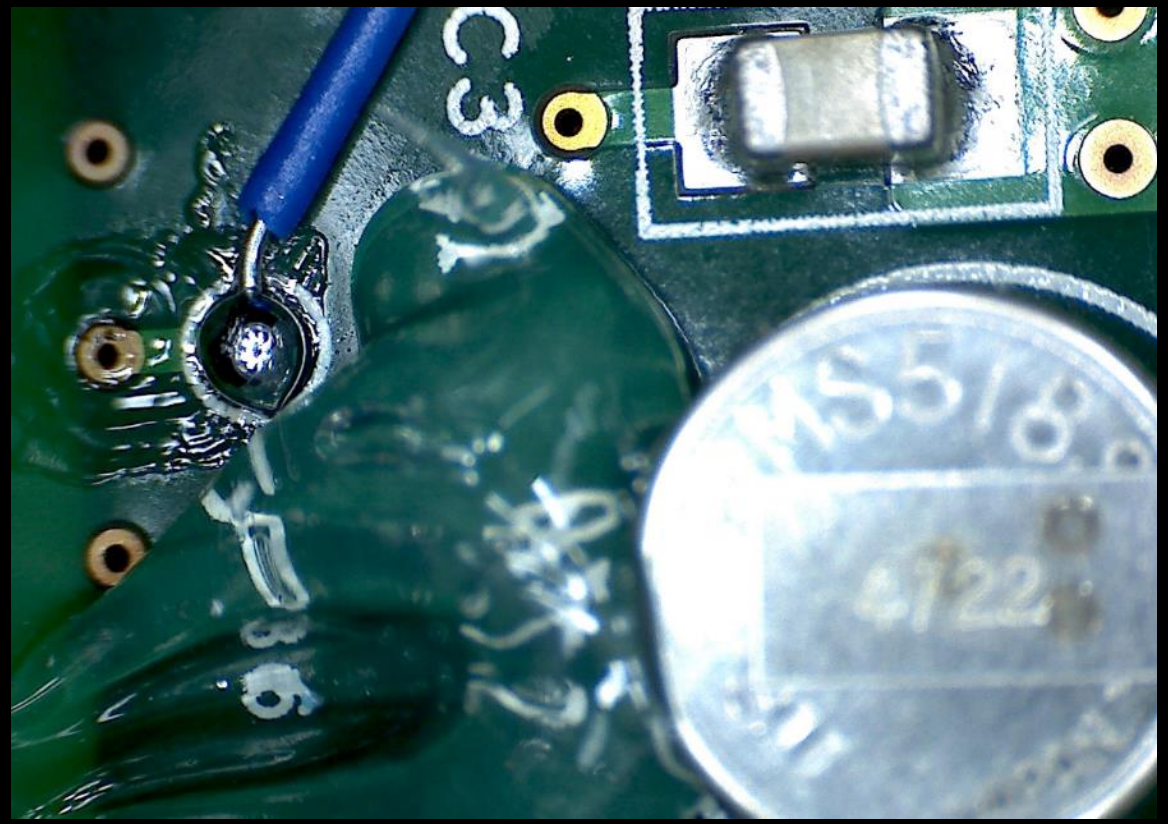
Good solder


62/36/2 SILVER-BEARING SOLDER
.015-in. Diameter • High-Tech
Net Wt.: 1 oz. (28.3g)
64-035
RadioShack®

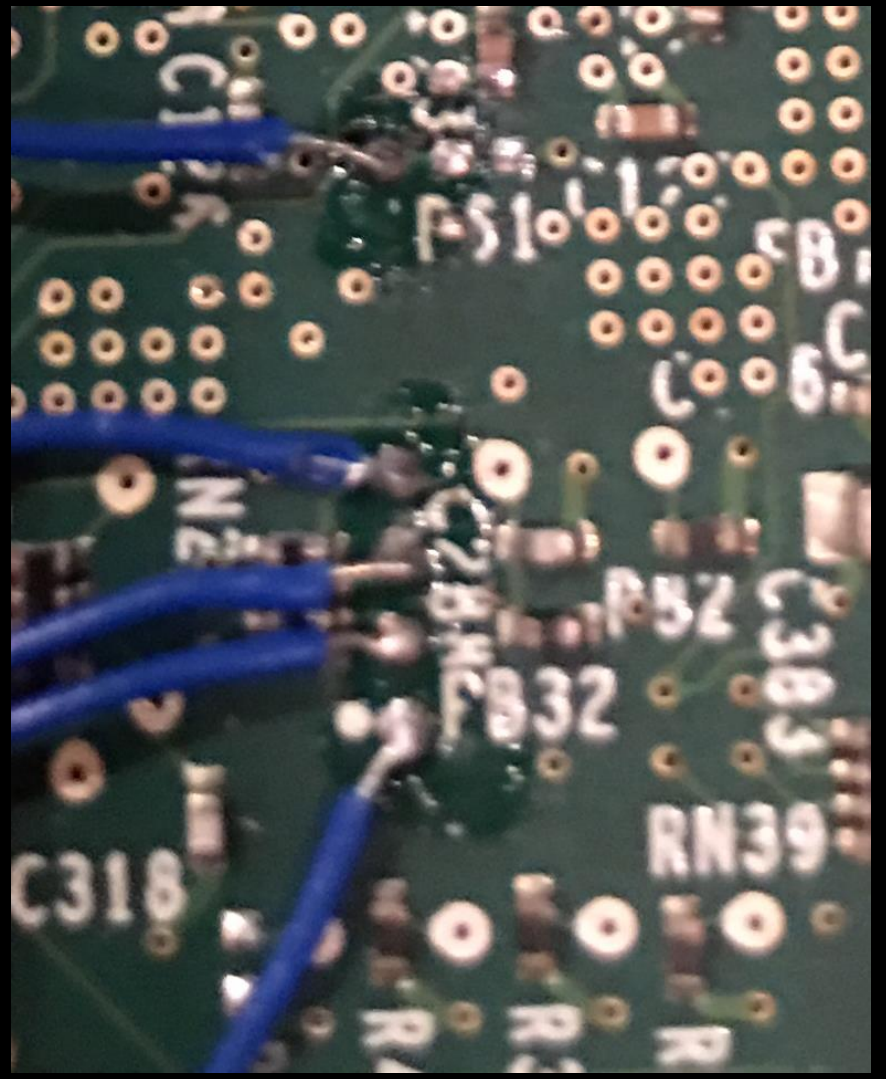
Soldering example



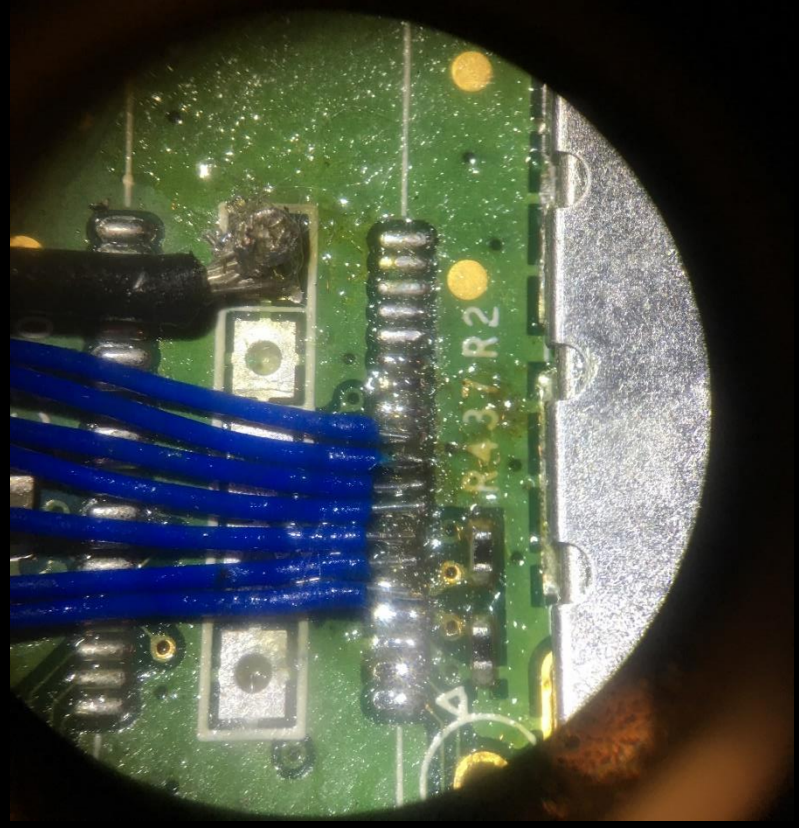
Soldering example



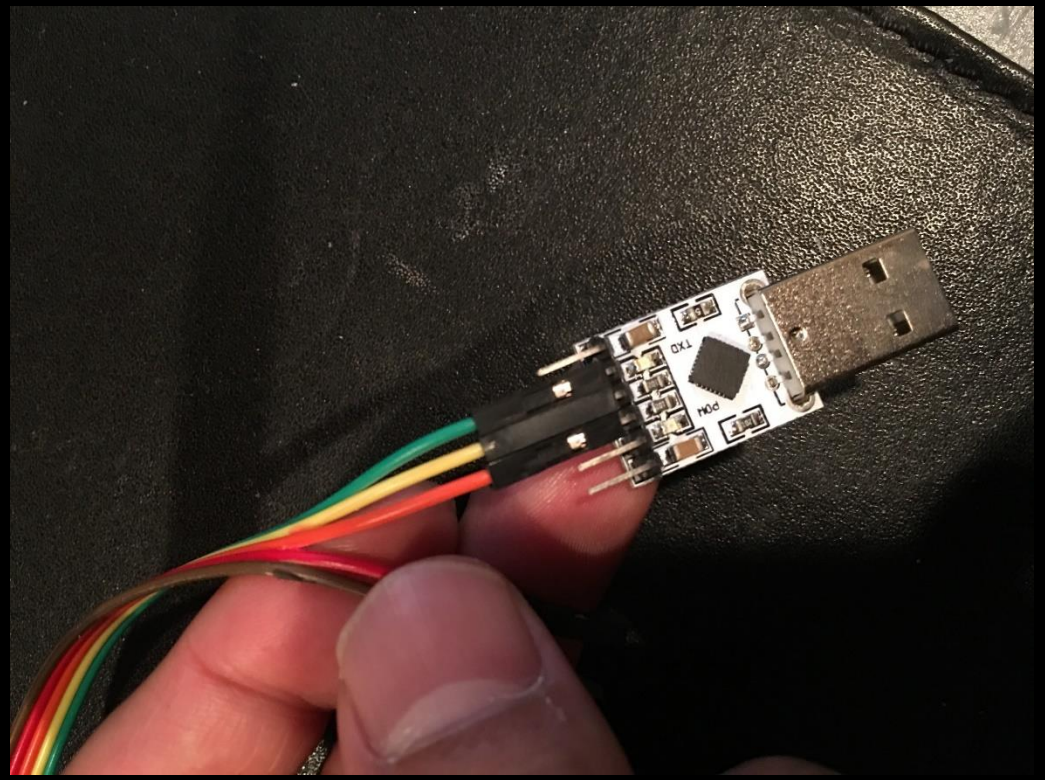
Soldering example

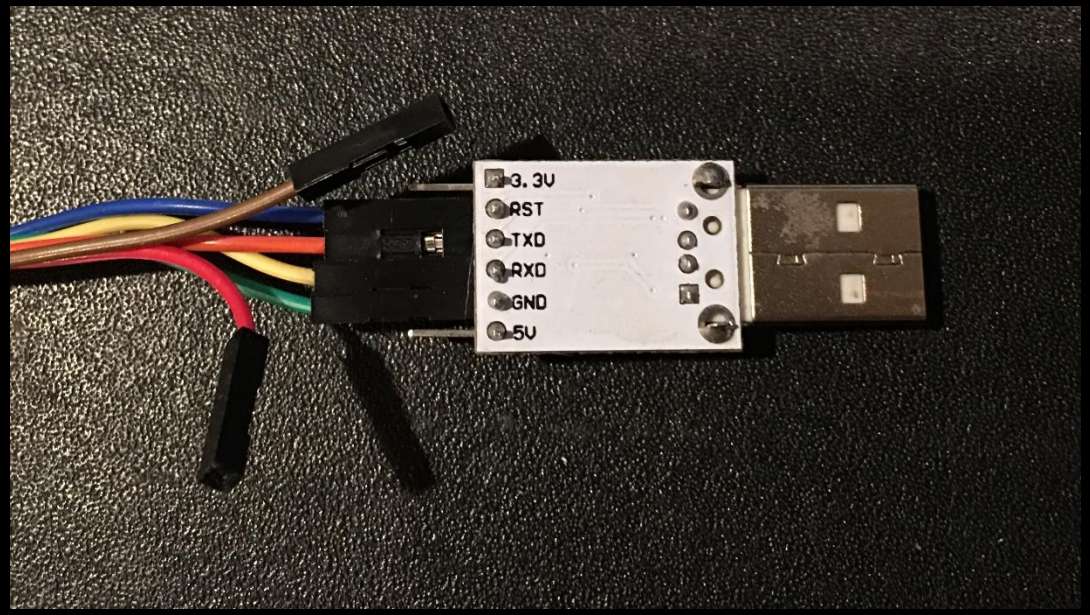


Soldering example



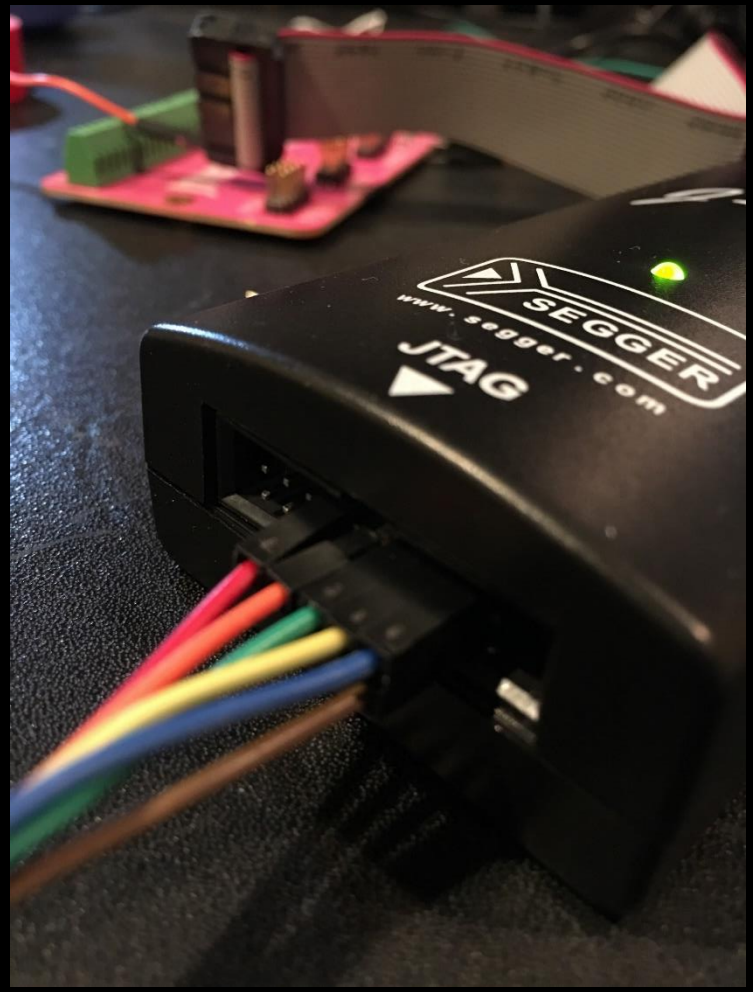
USB-to-TTL



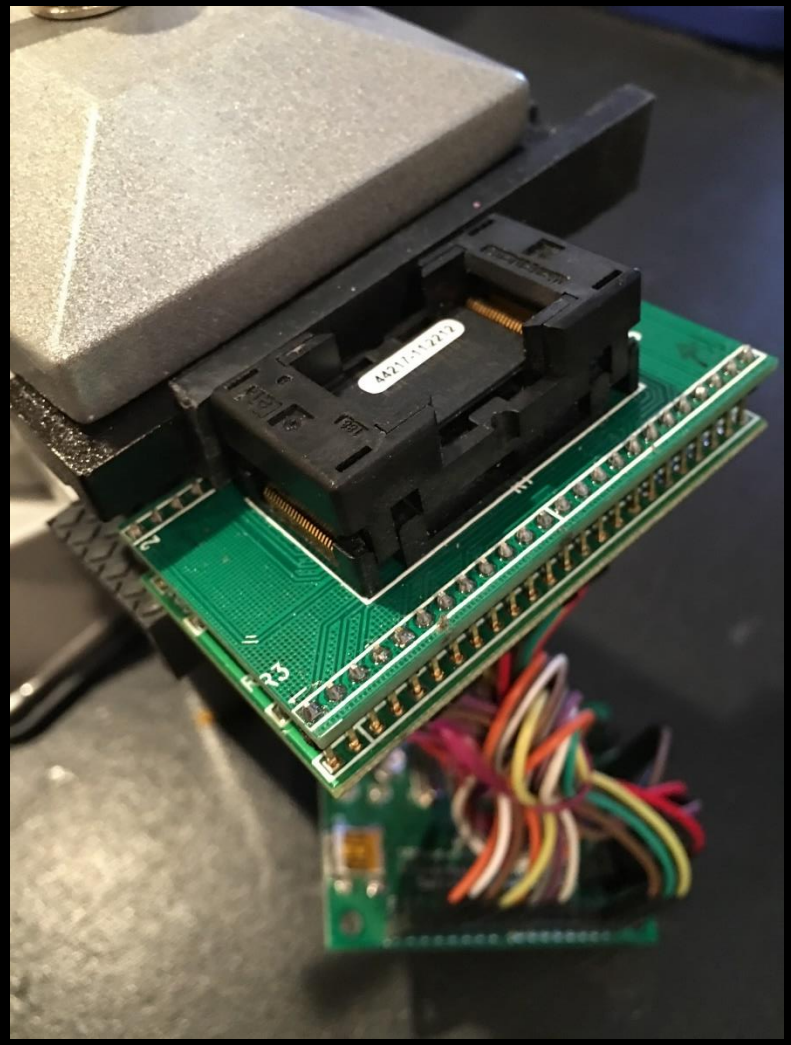


USB-to-TTL

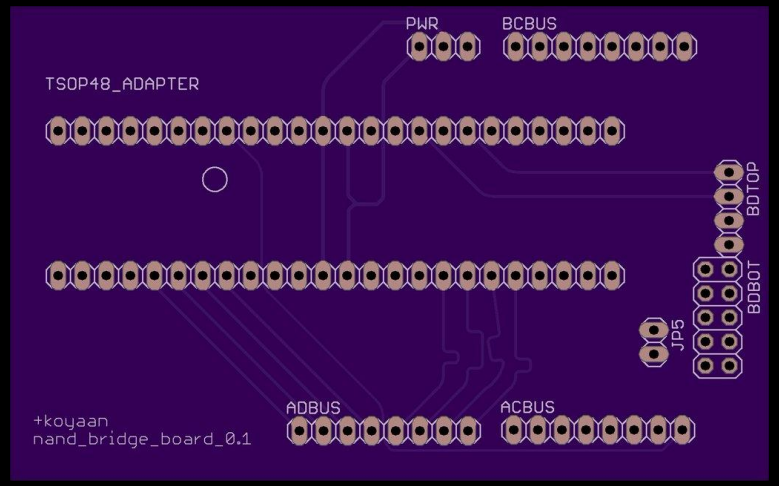
SEGGER J-Link



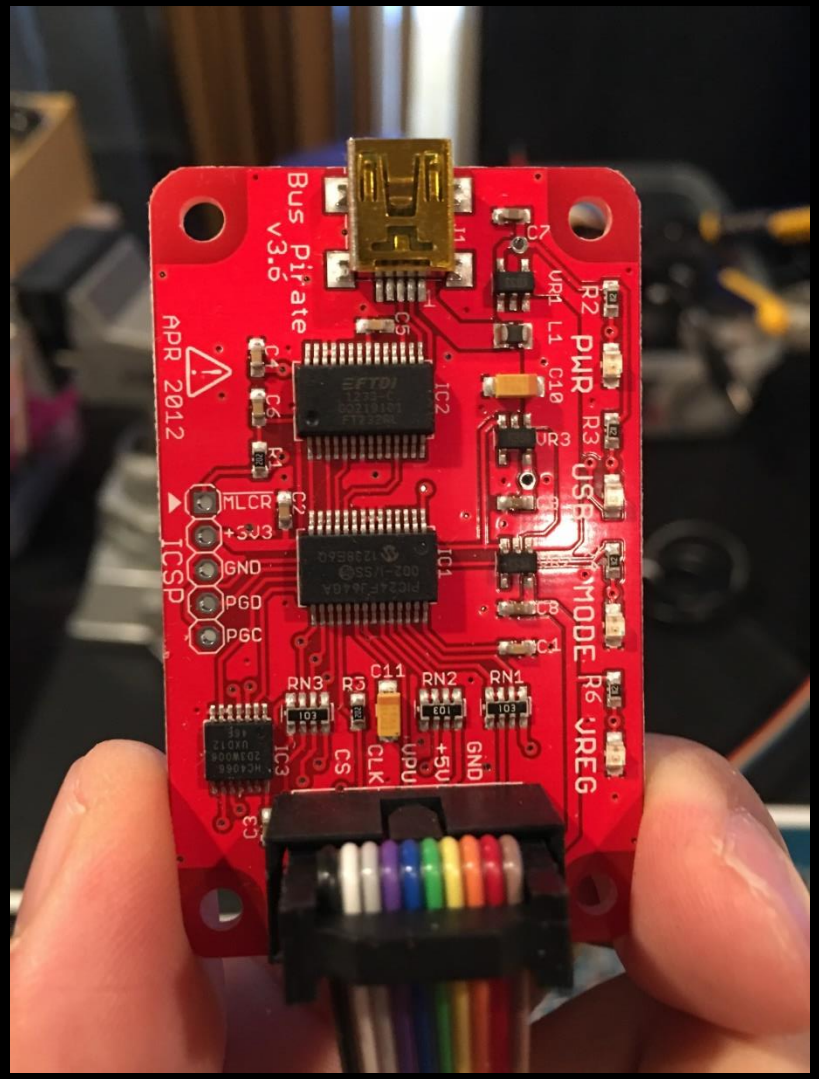
NAND Dump



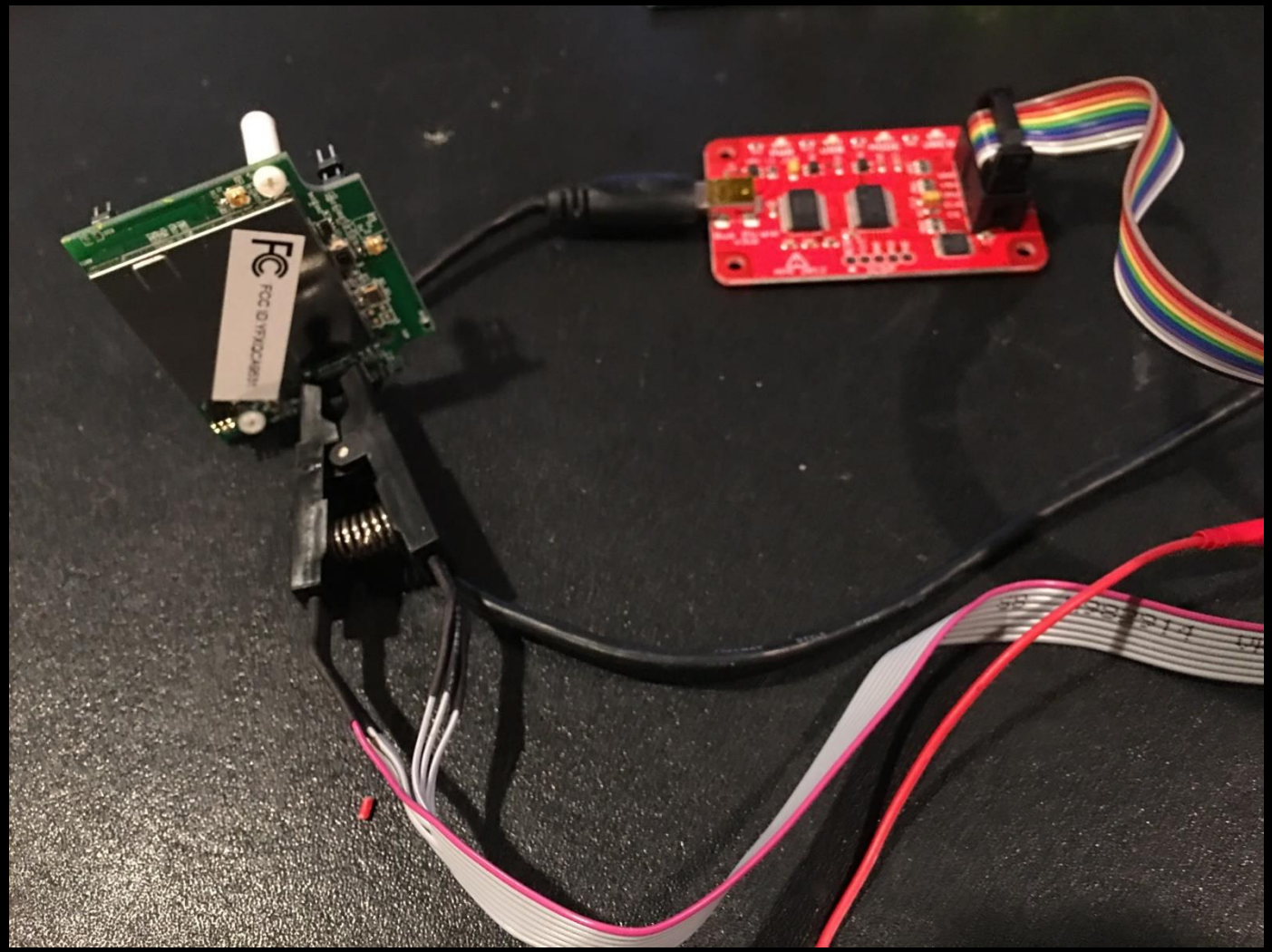
NAND Adapter



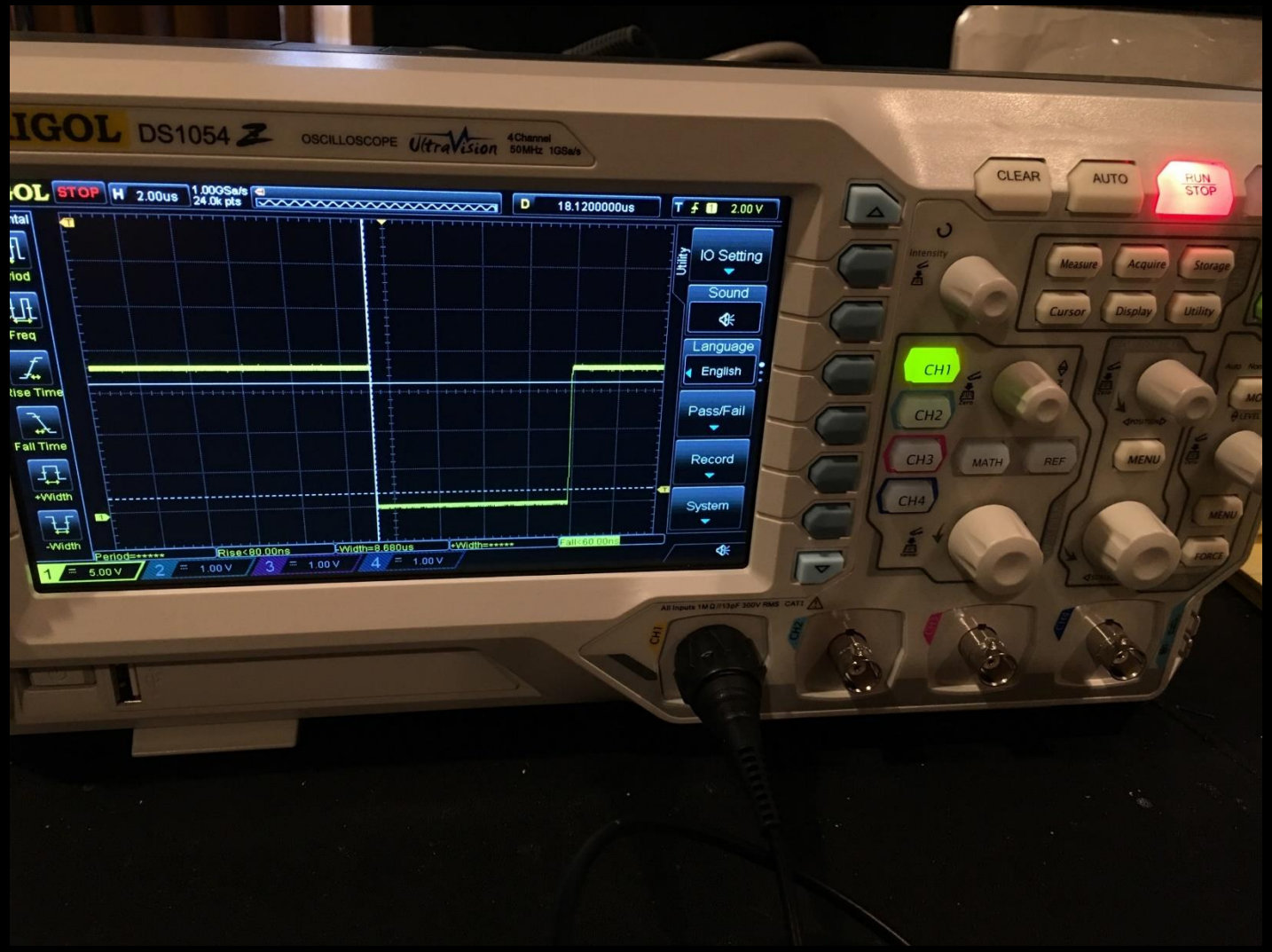
Bus pirate


Bus Pirate
v3.6
APR 2012
MLCR
+3V3
GND
PGD
PGC
ICSP
PWR
USB
MODE
VREG
RN3
R3
C11
RN2
RN1
CS
CLK
+5V
GND

Dumping Flash memory with SPI interface

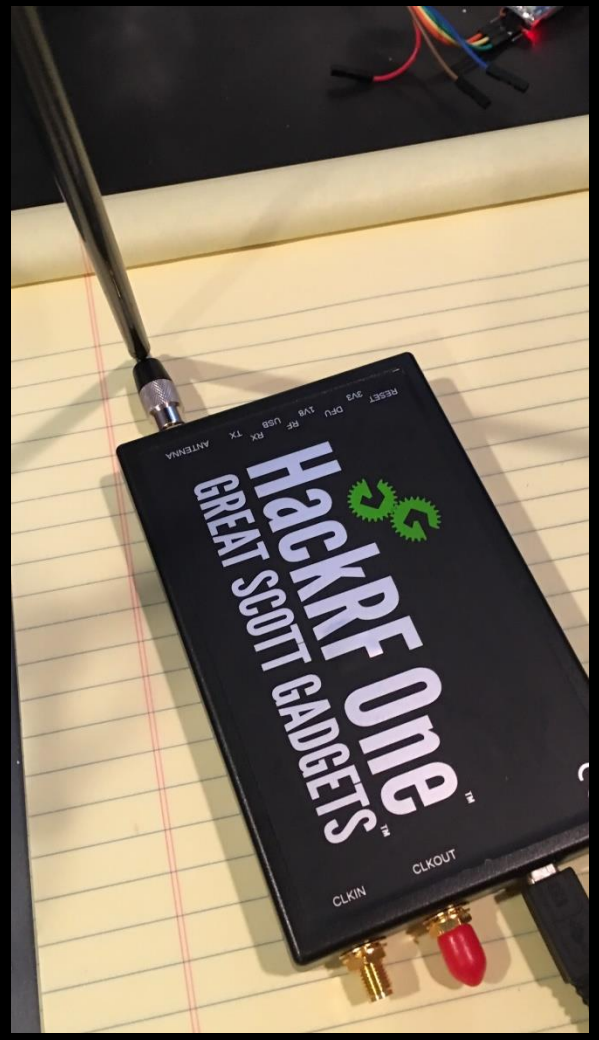


Oscillator


RIGOL DS1054Z
OSCILLOSCOPE
UltraVision
4 Channel
50MHz 1GSa/s
STOP
2.00us
1.000GSa/s
24.0k pts
18.1200000us
2.00 V
IO Setting
Sound
Language
English
Pass/Fail
Record
System
Utility
Rise Time
Fall Time
+Width
-Width
Period=*****
Rise<80.00ns
+Width=8.680us
+Width=*****
5.00 V
1.00 V
1.00 V
1.00 V
CLEAR
AUTO
RUN
STOP
Measure
Acquire
Storage
Cursor
Display
Utility
CH1
CH2
CH3
CH4
MATH
REF
MENU
FORCE

Logic analyzer

HackRF



Conclusion

- 하드웨어 해킹 – 참 쉽죠?