

# **JOE GRAND'S ADVENTURES OF WALLET HACKING**

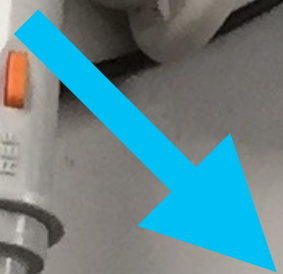
**HARDWEAR.IO USA 2022**





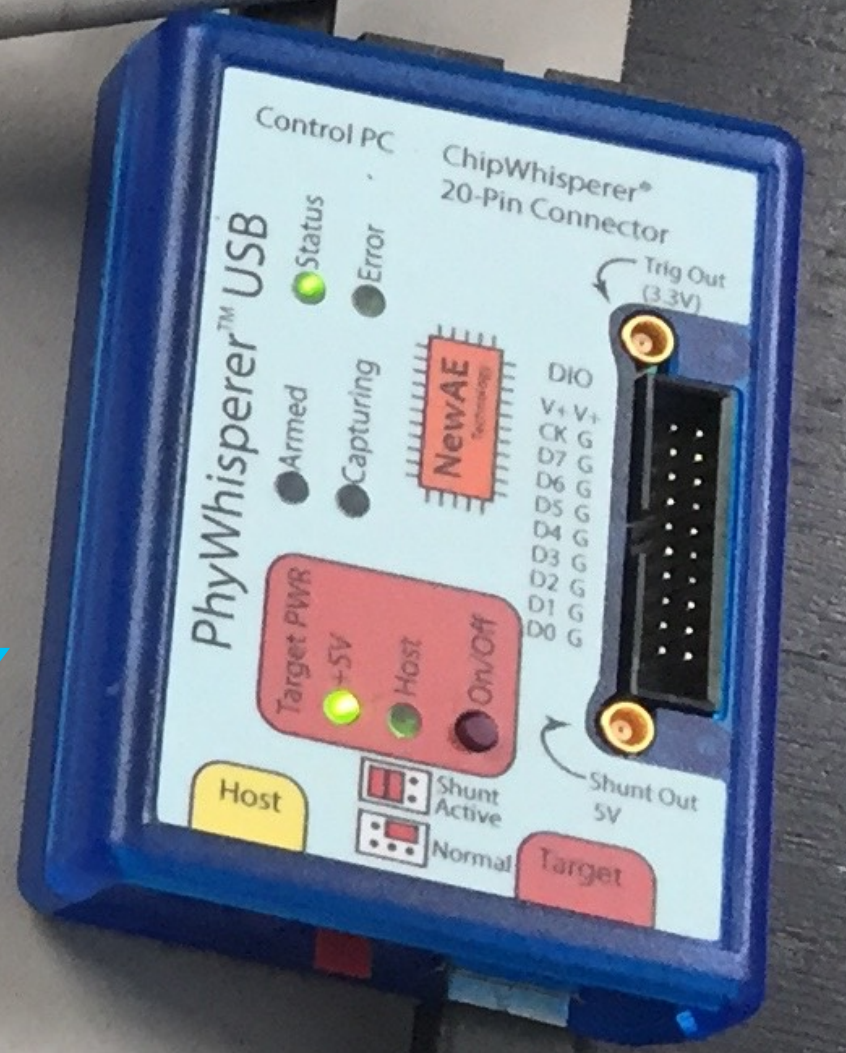


SEGGER J-LINK



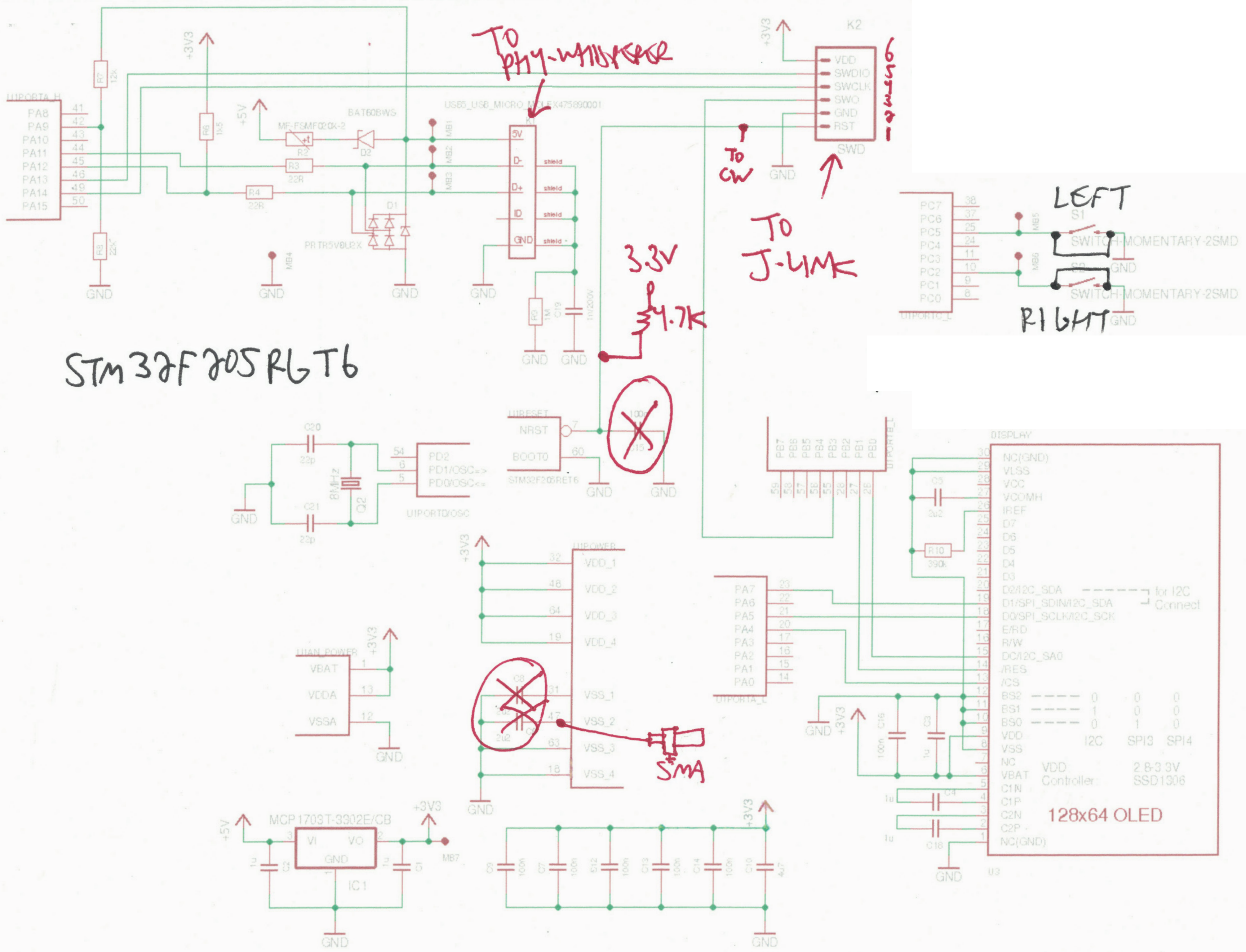
CHIPWHISPERER

PHYWHISPERER

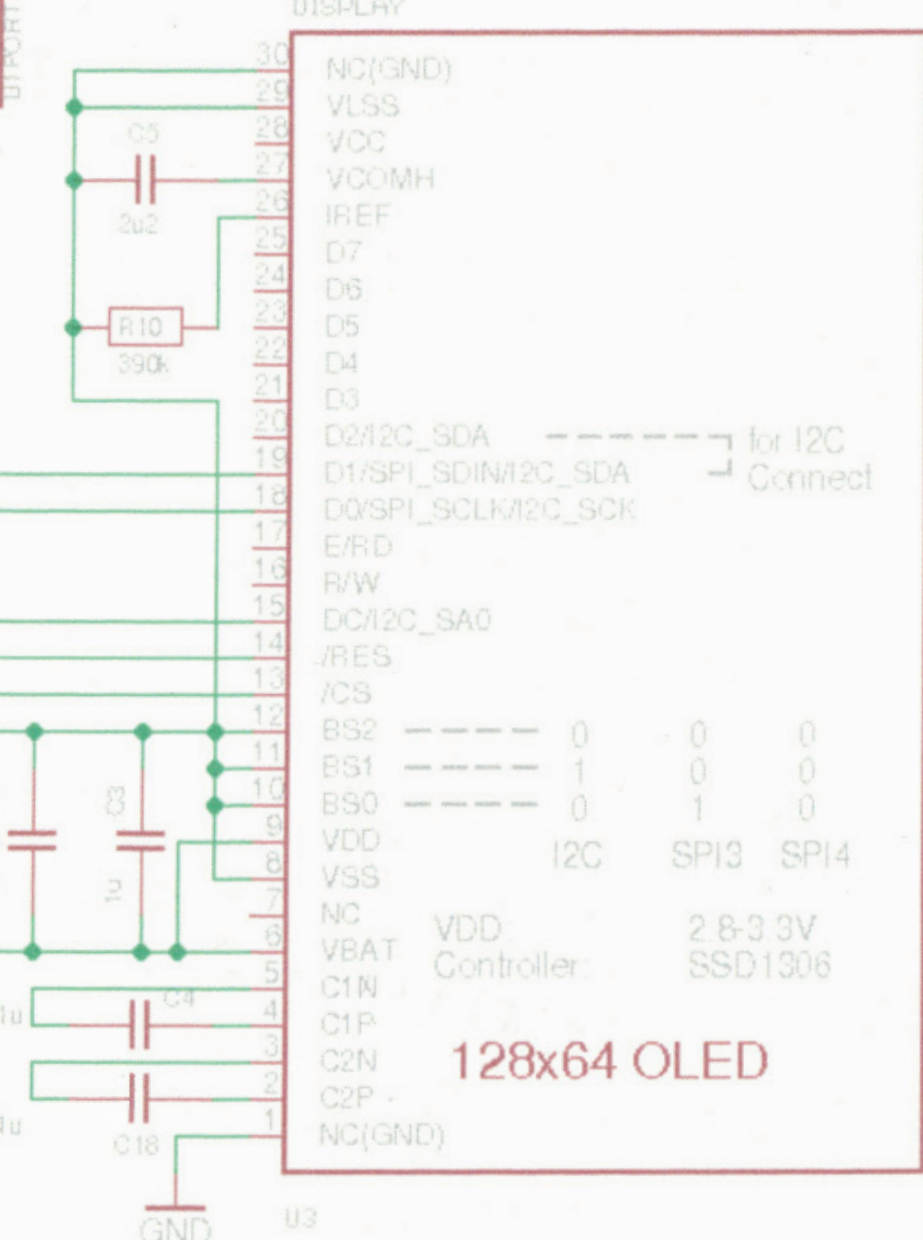
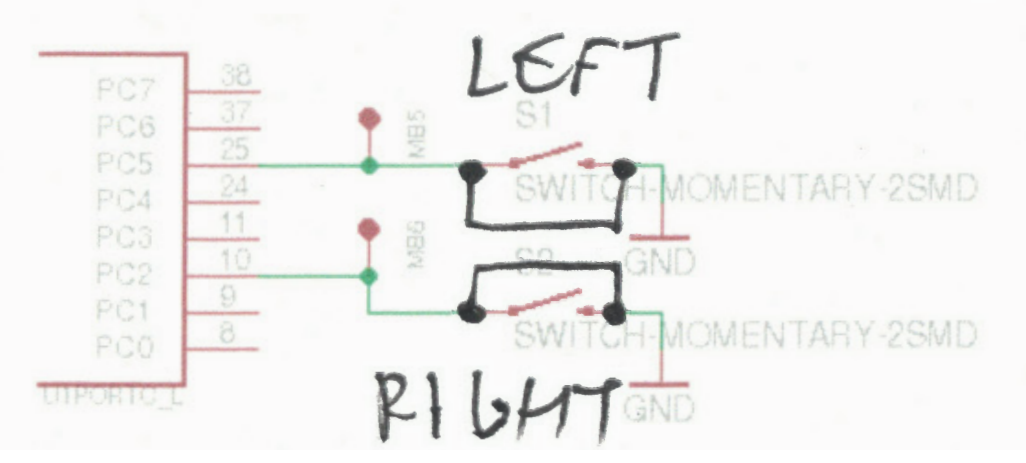




# TREZOR HW 1.1



STM32F205R6T6



128x64 OLED



1 2.00V/ 2 2.00V/ 3 500ns/ 4

3V3

V CORE

NRST

$\Delta X = 150.96000\mu s$   
Mode Normal

Coupling DC

$1/\Delta X = 6.6243kHz$   
Noise Rej

HF Reject

$\Delta Y(1) = 0.0V$   
Holdoff 60ns

Trigger

Mode Coupling Pulse Width Pattern

File Save Recall Print

Auto Scale

Meas Curves Acquire

Quick Meas Display Intensity

Vertical

1 Math 2 3

AC BW

1 M $\Omega$  10pF 300 V CAT I



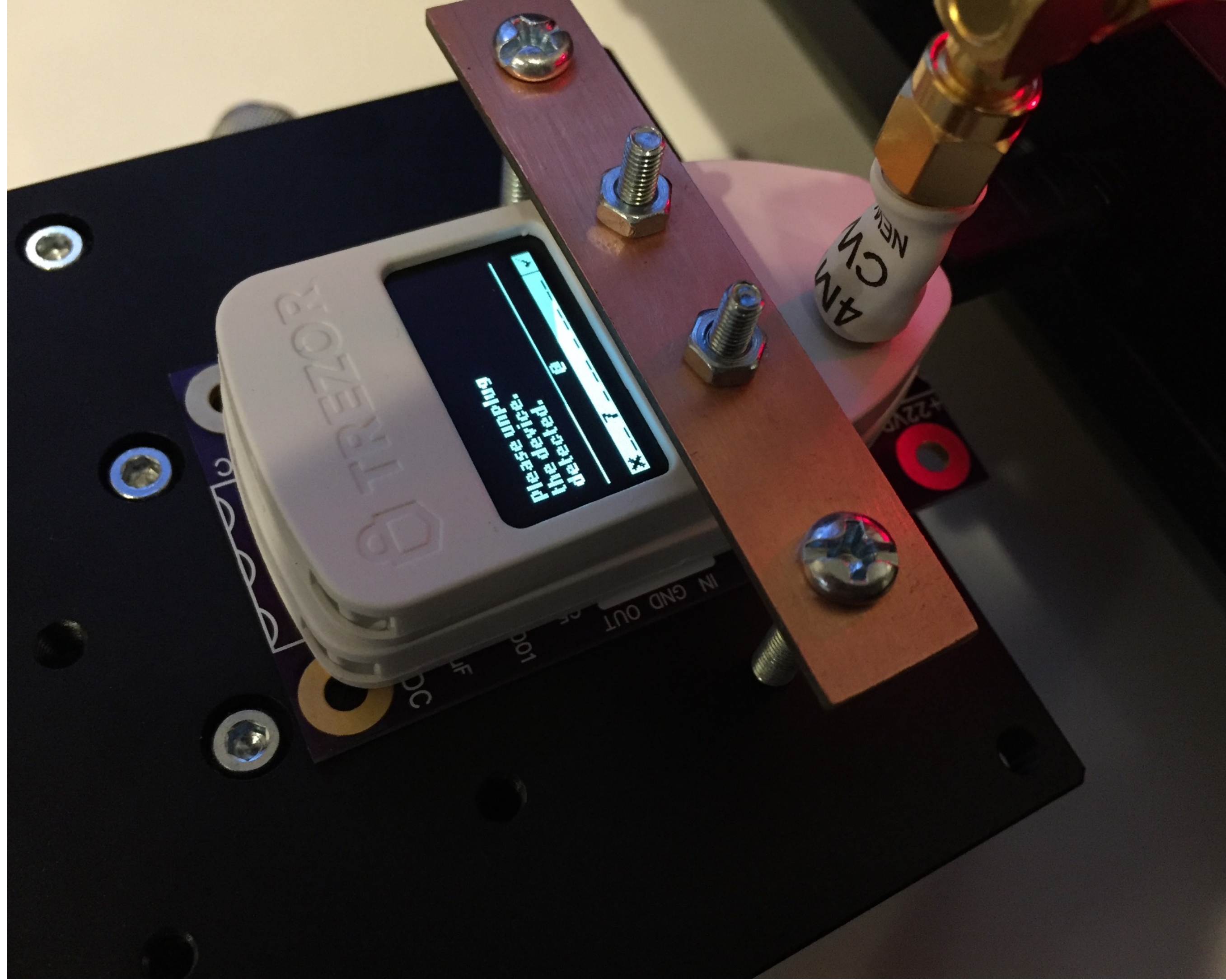
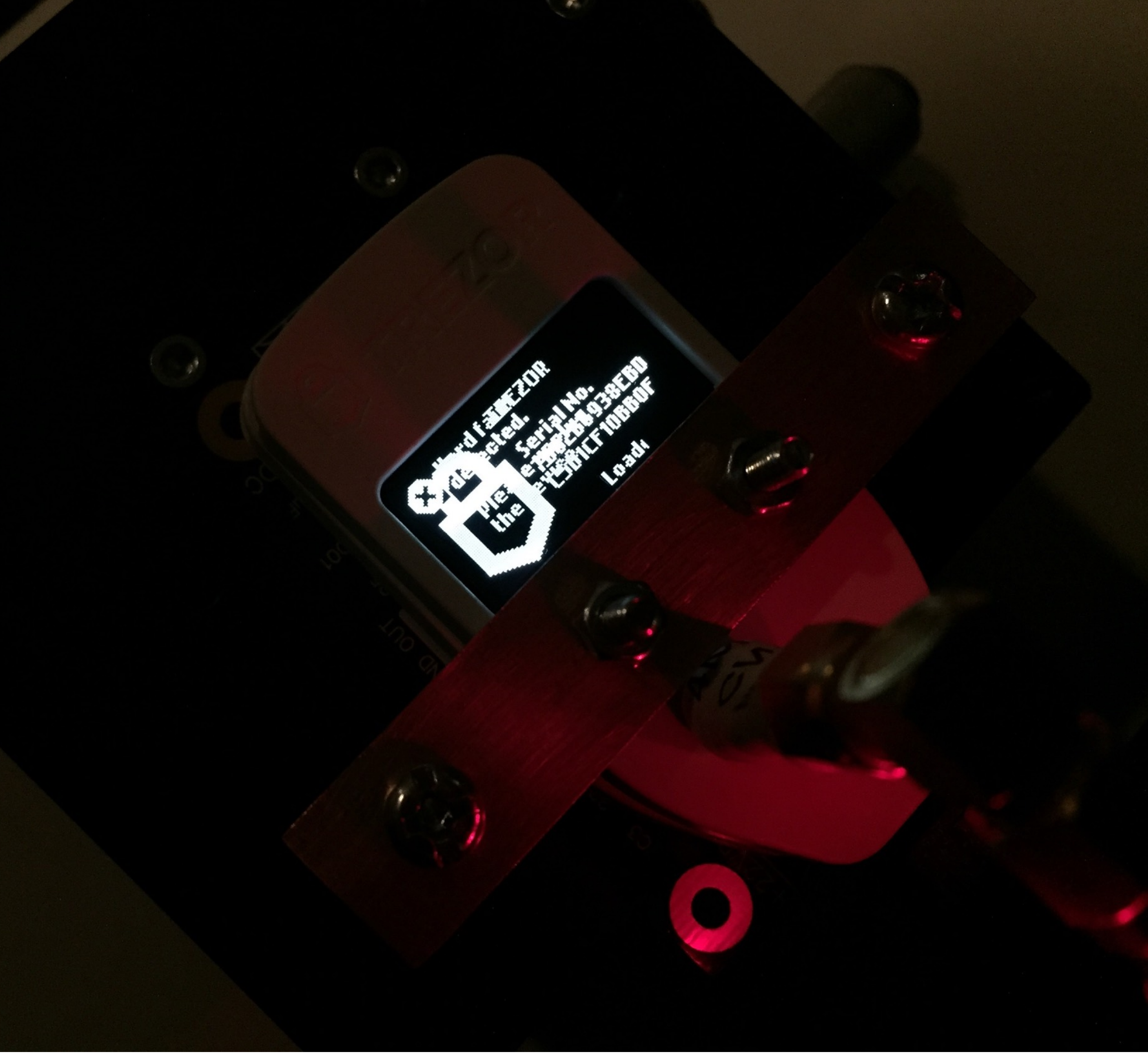




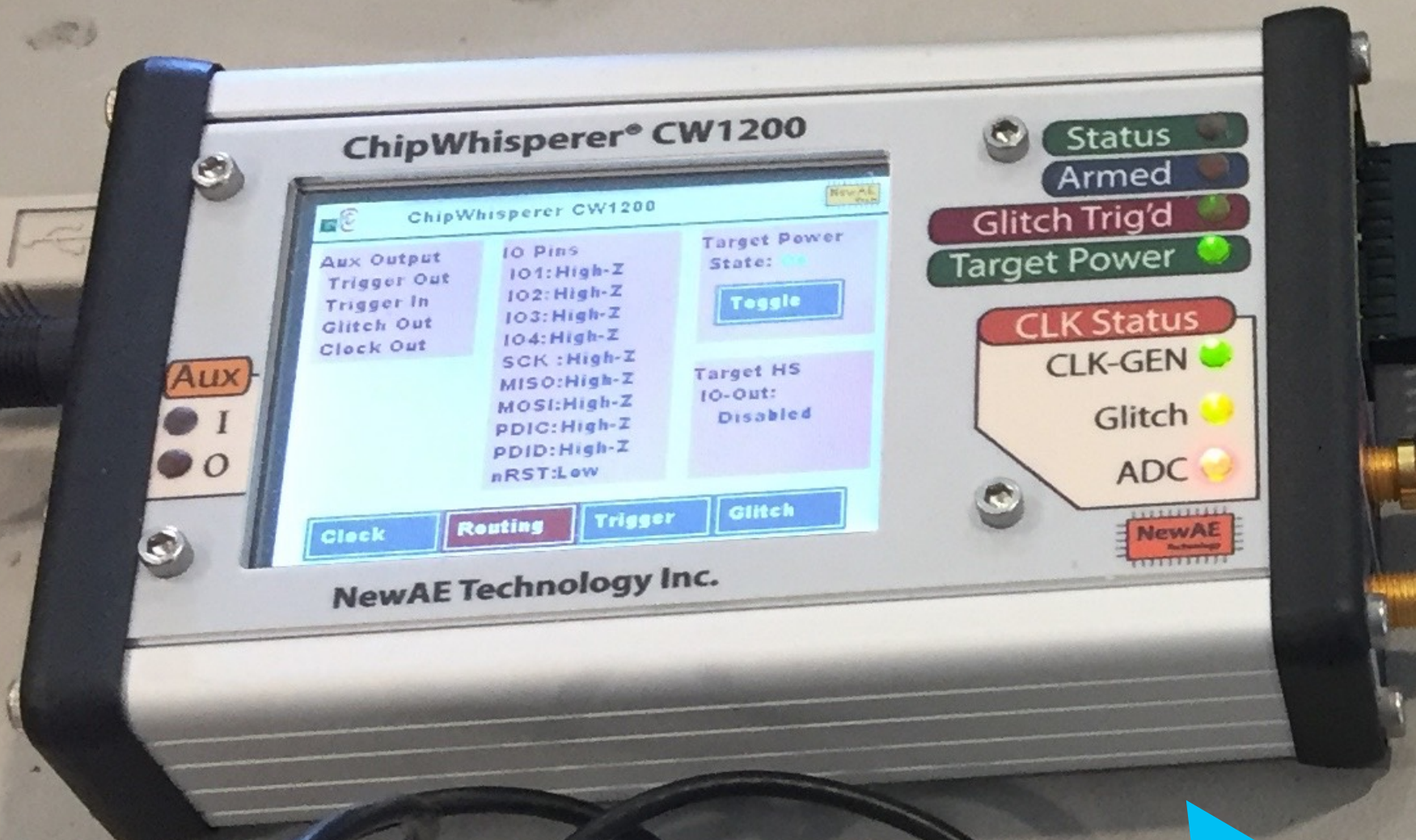




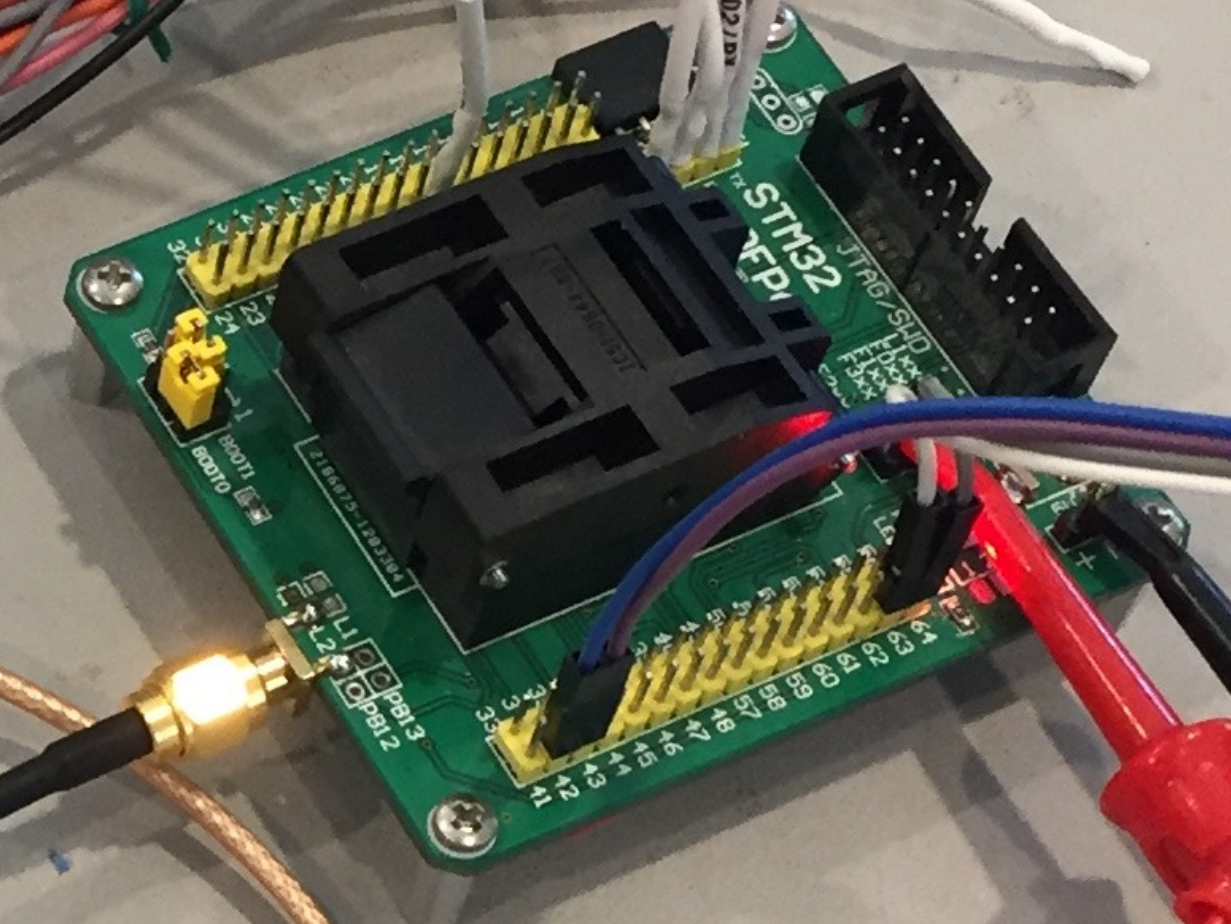








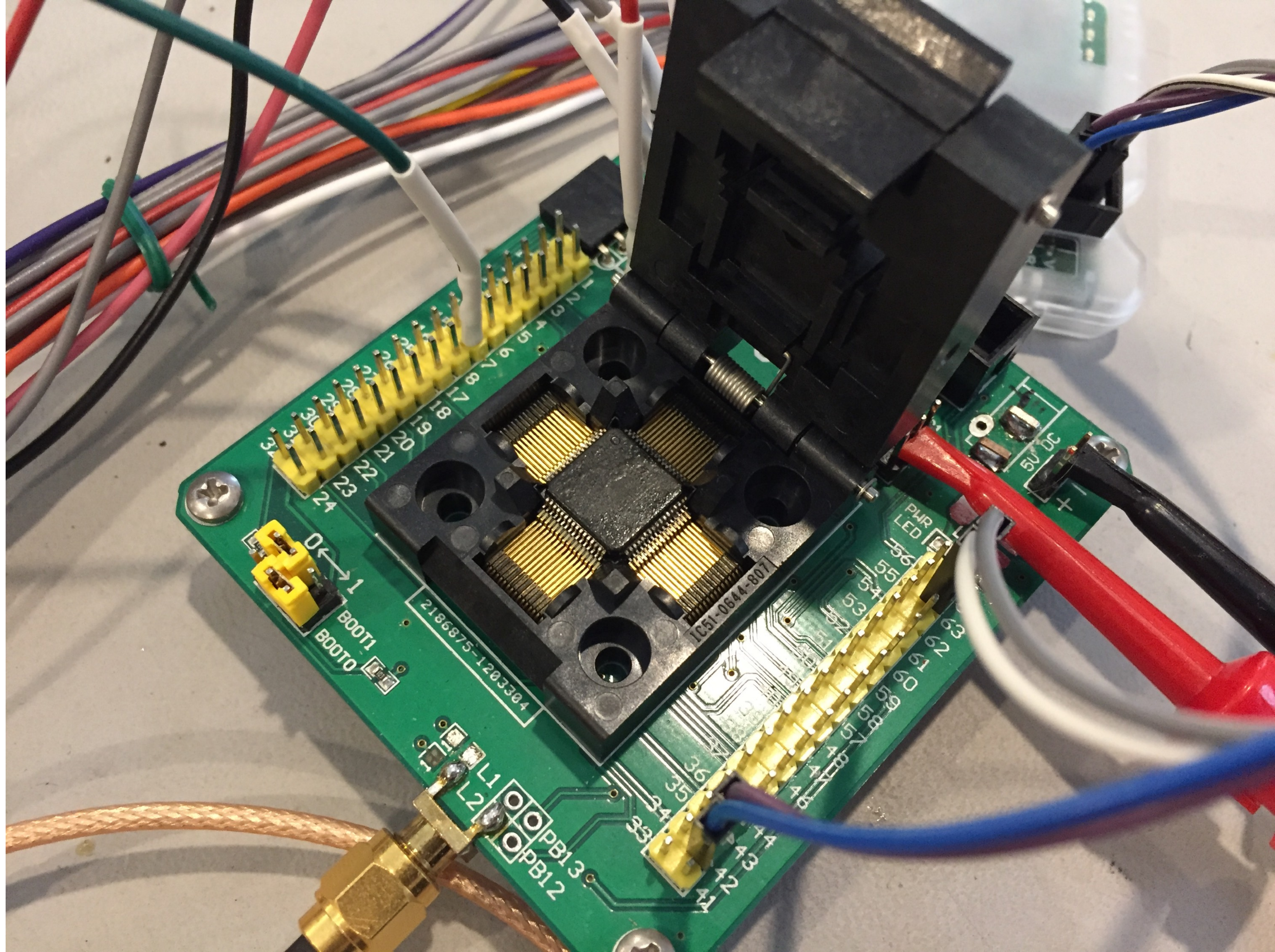
CHIPWHISPERER



μART











Agilent Technologies

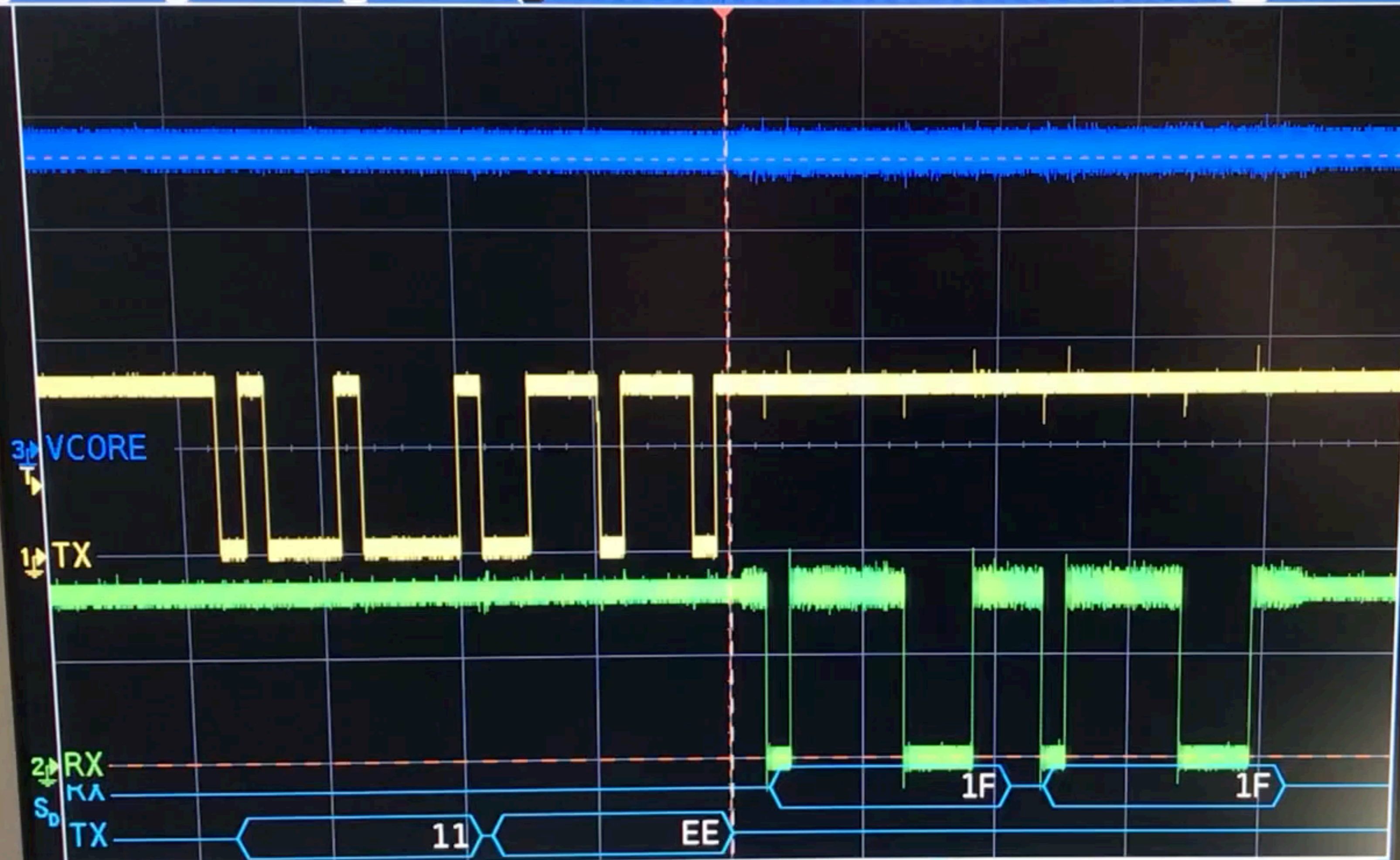
InfiniiVision

DSO7054A  
Digital Storage Oscilloscope

500 MHz  
4 GSa/s

MEGA Zoom

1 2.00V/ 2 2.00V/ 3 500ns/ 4 0.0s 50.00ns/ Trig'd URT 1 1.32V



$\Delta X = 520.00\text{ns}$   $1/\Delta X = 1.9231\text{MHz}$   $\Delta Y(3) = -2.82025\text{V}$

Mode Manual Source VCORE X Y X1 0.0s X2 520.00ns X1 X2

Horizontal

Menu Zoom

Trigger

Edge Mode Coupling Pulse Width Pattern  
Auto Scale File Save Recall Print

Meas

Waveform

Push to Select Cursors Acquire  
Quick Meas Display

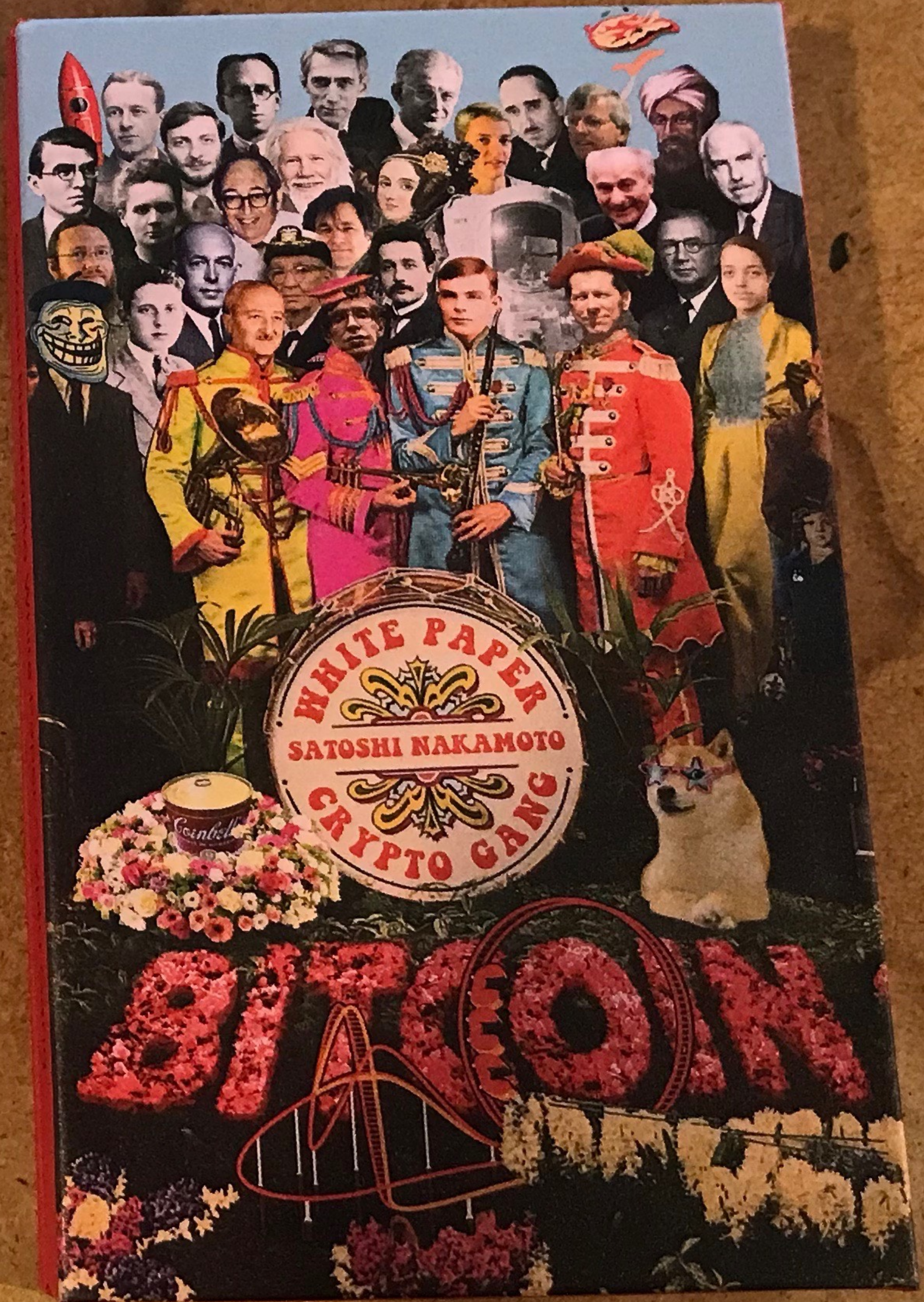
Vertical

1 Math 2 Label 3

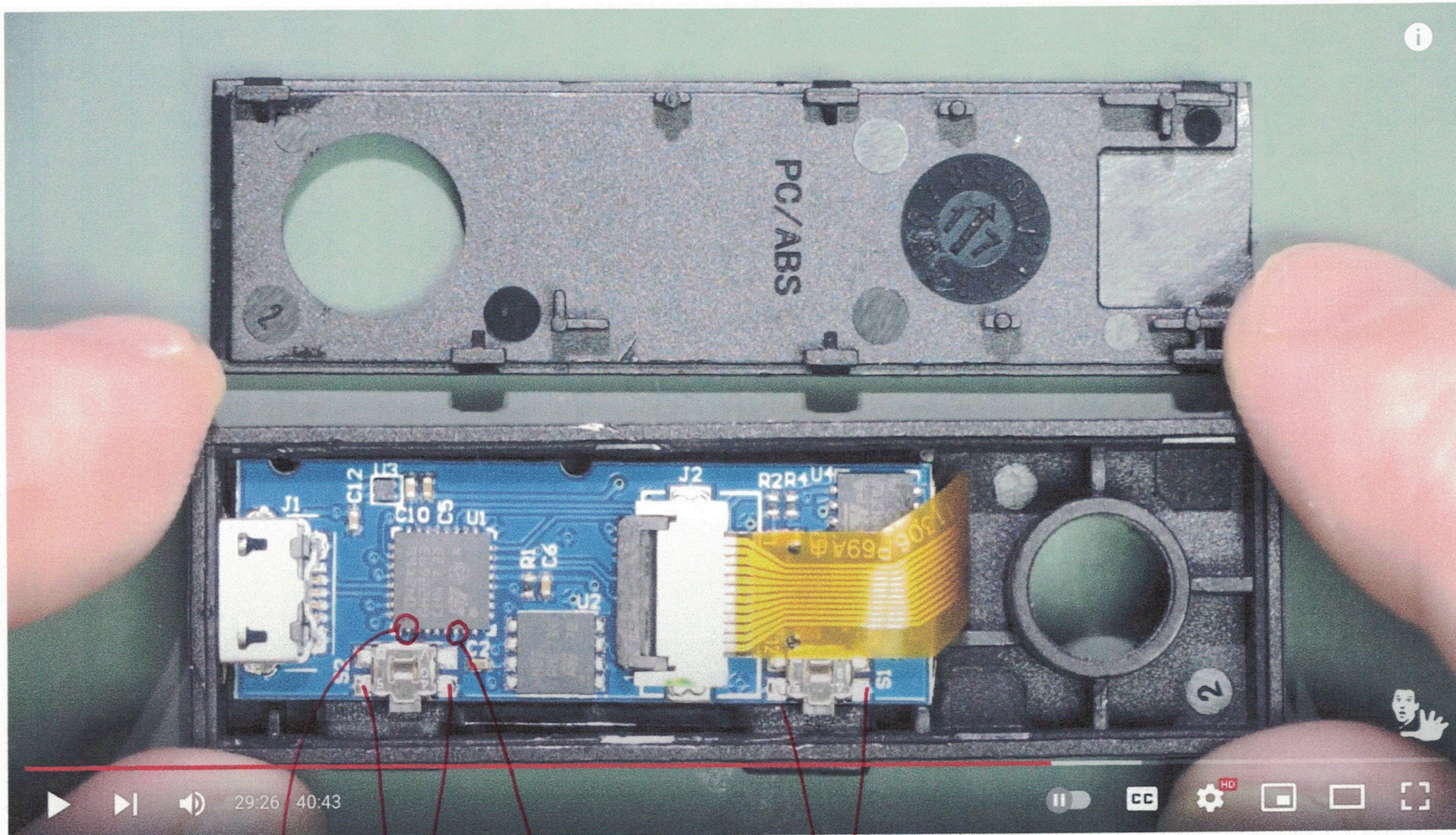
AC 500 AC 500 AC 500  
BW BW BW



LEDGER NANO S  
LIMITED EDITION  
#2







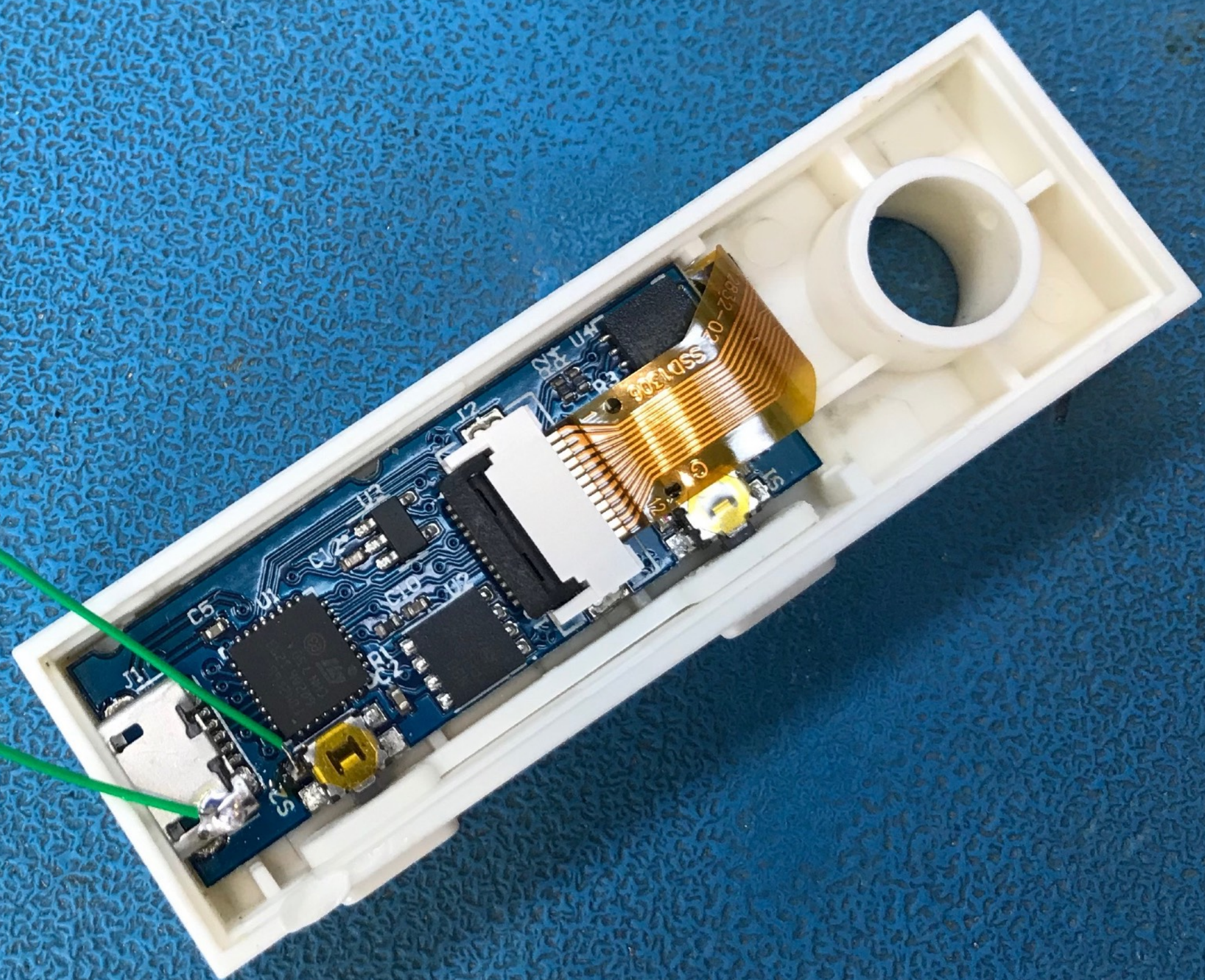
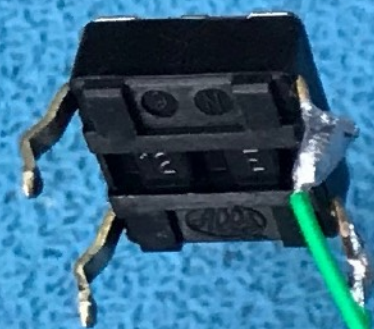
S2

GND

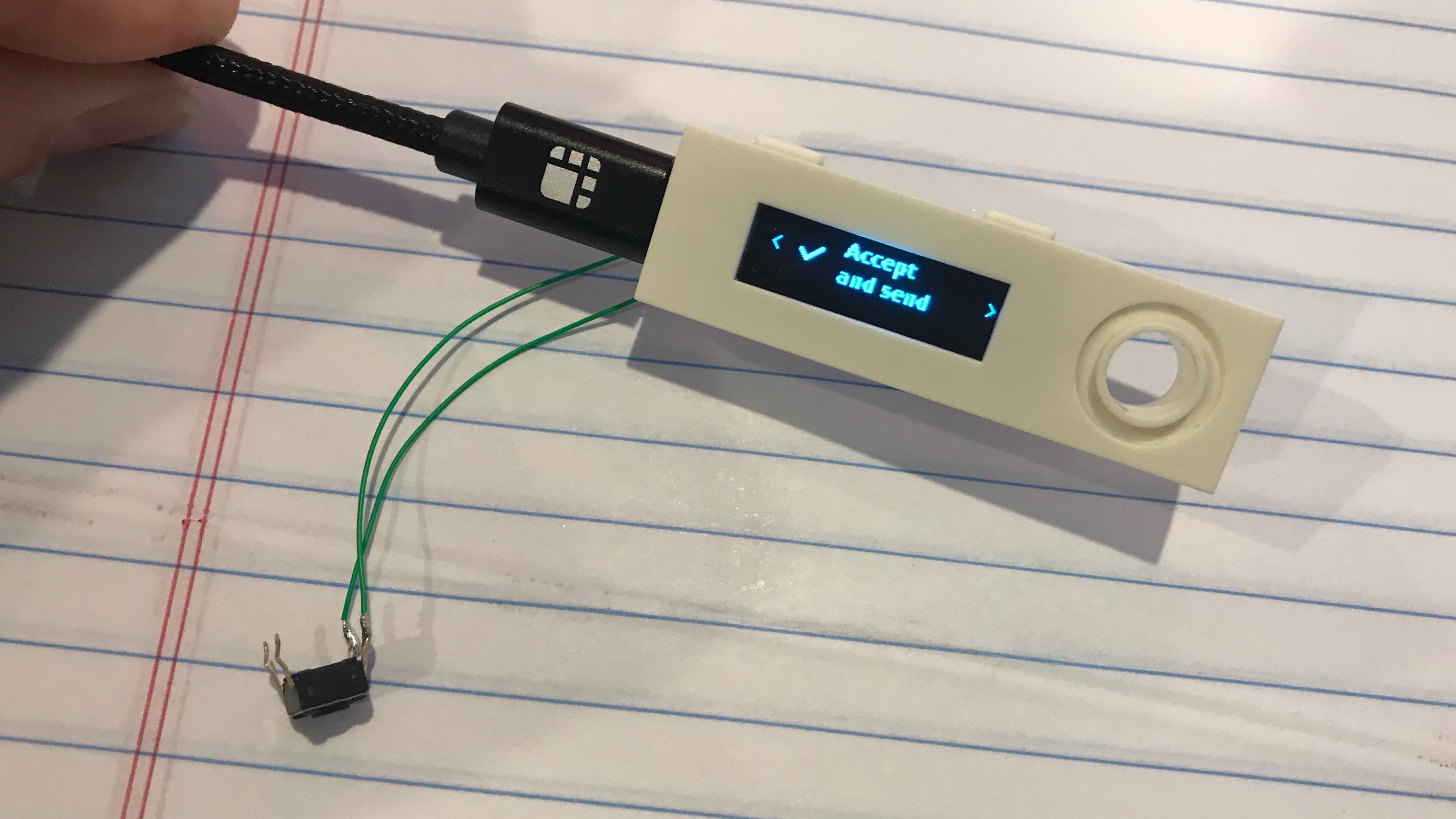
S1

GND

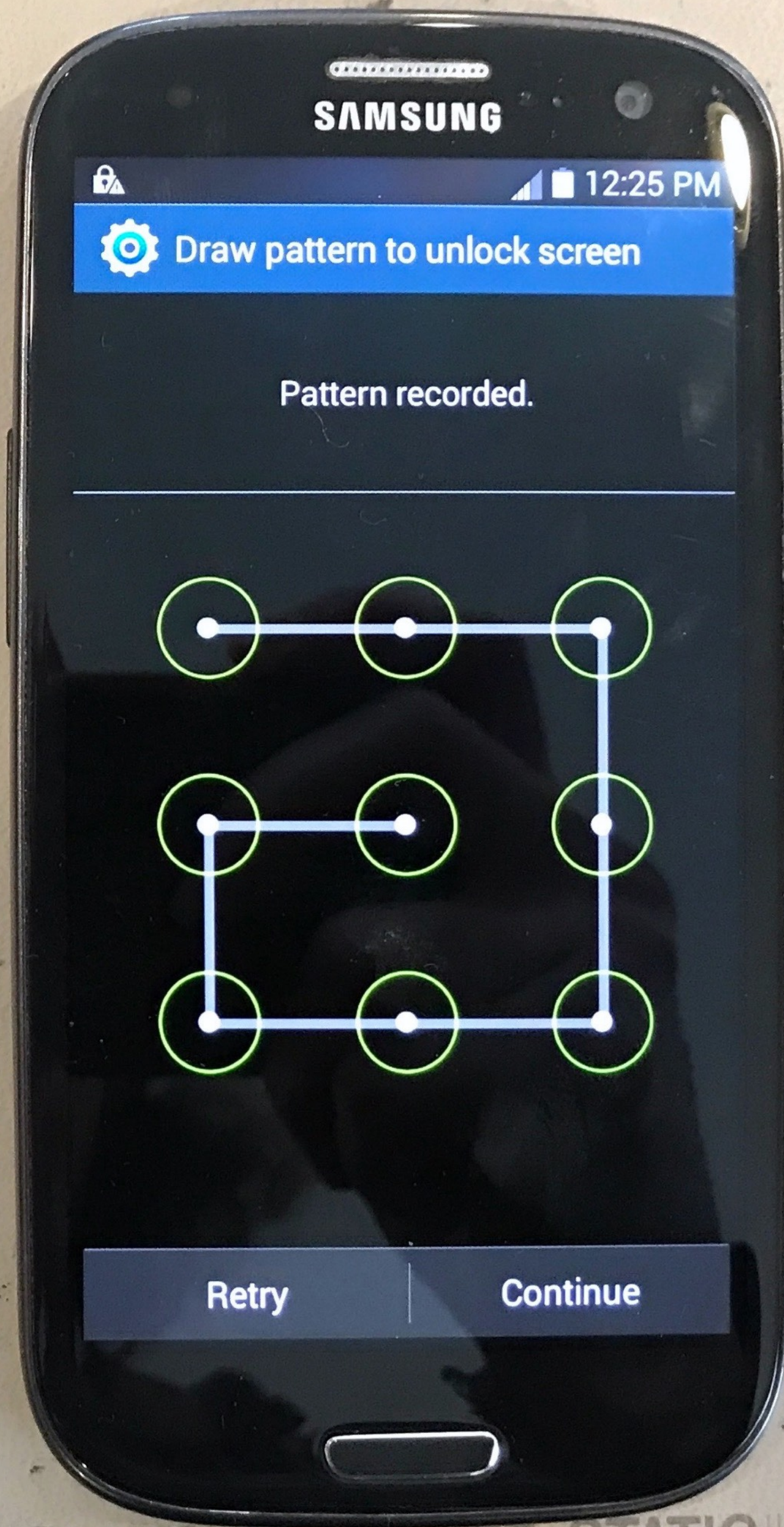
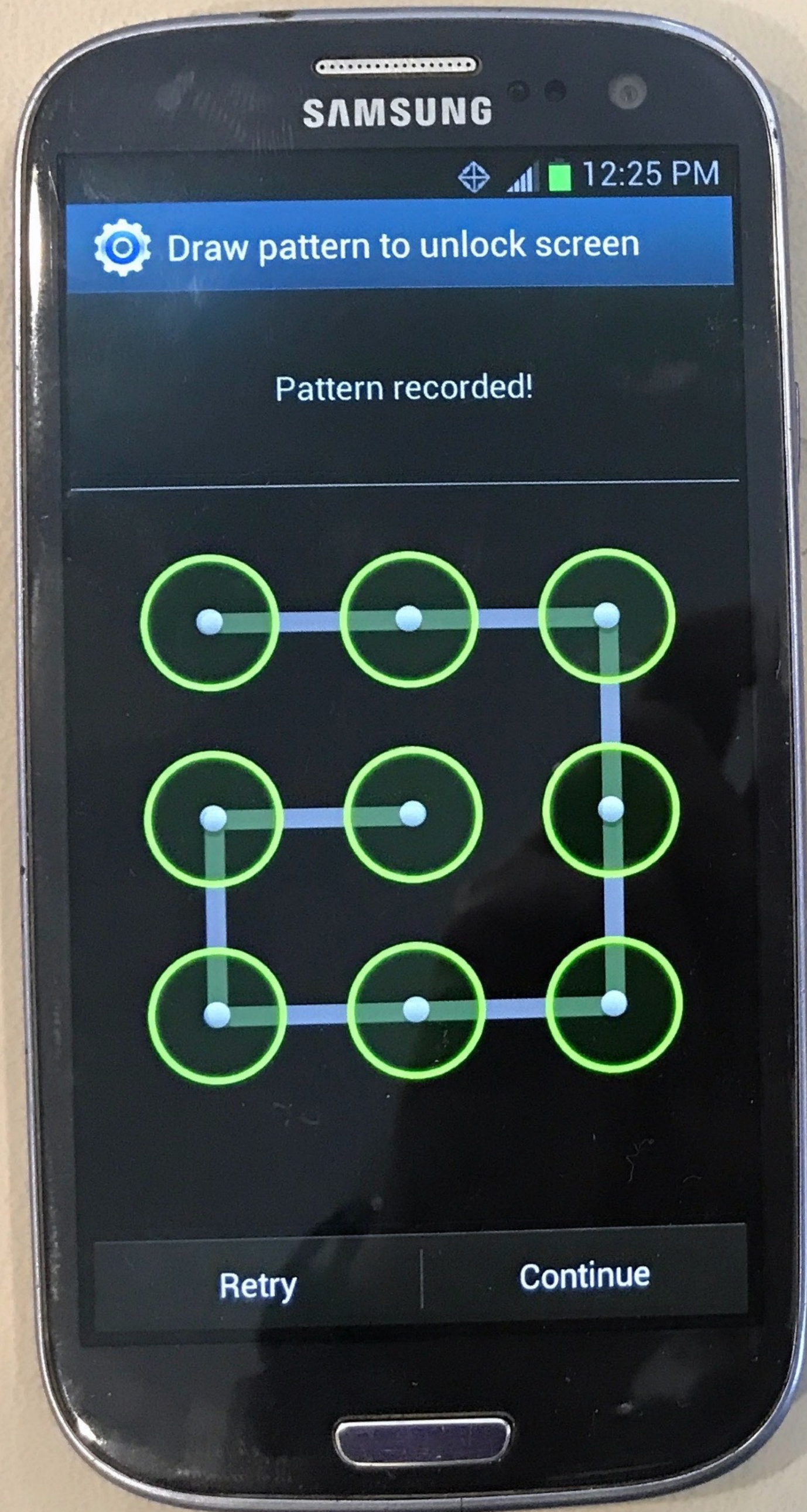








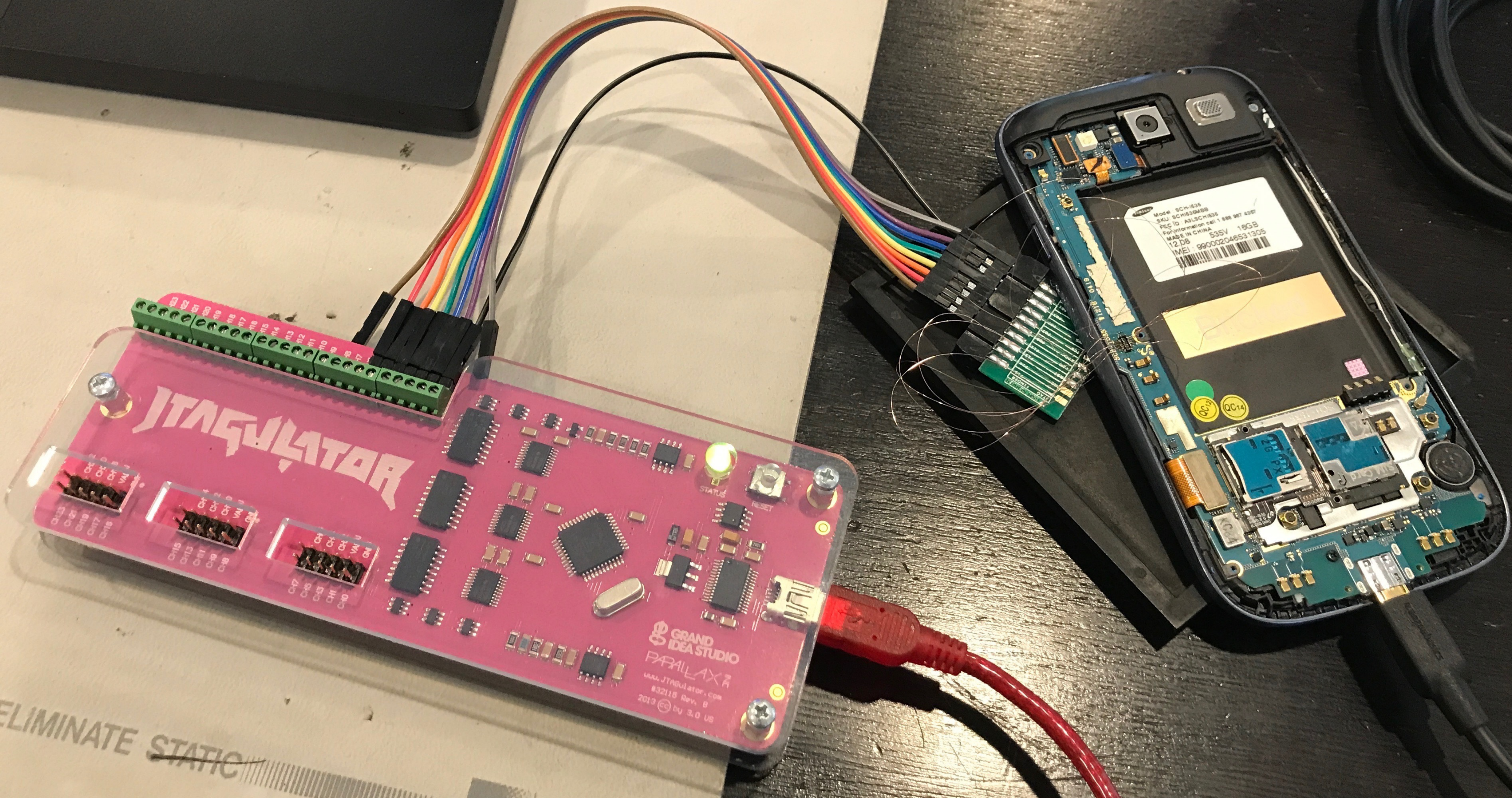












JTAGULATOR

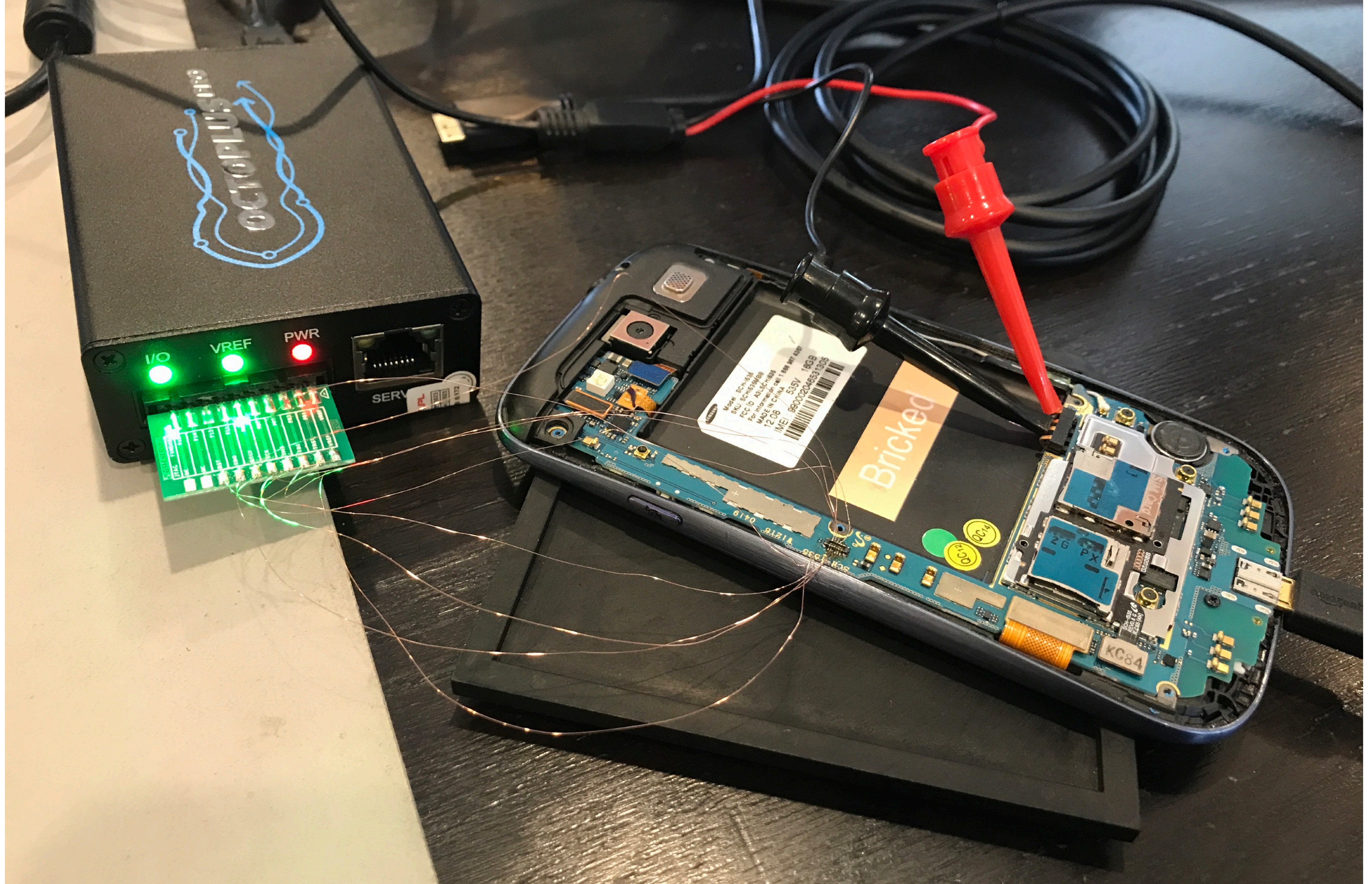
GRAND  
IDEA STUDIO  
PARALLAX  
www.JTAGulator.com  
#32118 Rev. B  
2013 © by 3.0 US

Model: SCH-I535  
SKU: SCHI535MBB  
PCC ID: A3L2SCH1835  
For information call 1 888 987 4387  
MADE IN CHINA  
12 GB 535V 16GB  
IMEI: 990002048531305

ELIMINATE STATIC

ACCP







Medusa Box Software version 2.6.1.7

Support And Options **Advanced** Advanced Mode

### Options

Manufacturer: Samsung  
 Device model: Samsung SCH-I535  
 JTAG speed: Auto (RTCK)

? Help

### Actions

Connect  Cancel  
 Read  Boot only  
 Write  Full flash  
 Erase  Custom

Units: Kilobytes  
 Start: 0  
 Length: 79744 (77.9 Mb)

Disable Write Protection

ECC Mode

### Log

```

Connecting. Please wait...
Checking data...
Medusa JTAG Firmware version 1.24.
Detected TAP ID: 4BA00477, IR Length = 4.
Detected TAP ID: 406B10E1, IR Length = 11.
Medusa JTAG Firmware version 1.24.
JTAG speed : Auto (RTCK).
VREF level : 1.79 V
CPU : Qualcomm MSM8960
Core ID : 406B10E1
Storage Device: Samsung eMMC MAG4FB
Device ID : 00150001
Block size : 512 bytes
Blocks : 30777344
Storage size : 14.7 Gb
Connect successful.
Opening "C:\Users\abstr\OneDrive\Desktop\Samsung SCH-I535 Boot 02-05-2022 16_18_28.bin" file...
Reading BOOT section. Please wait...

```

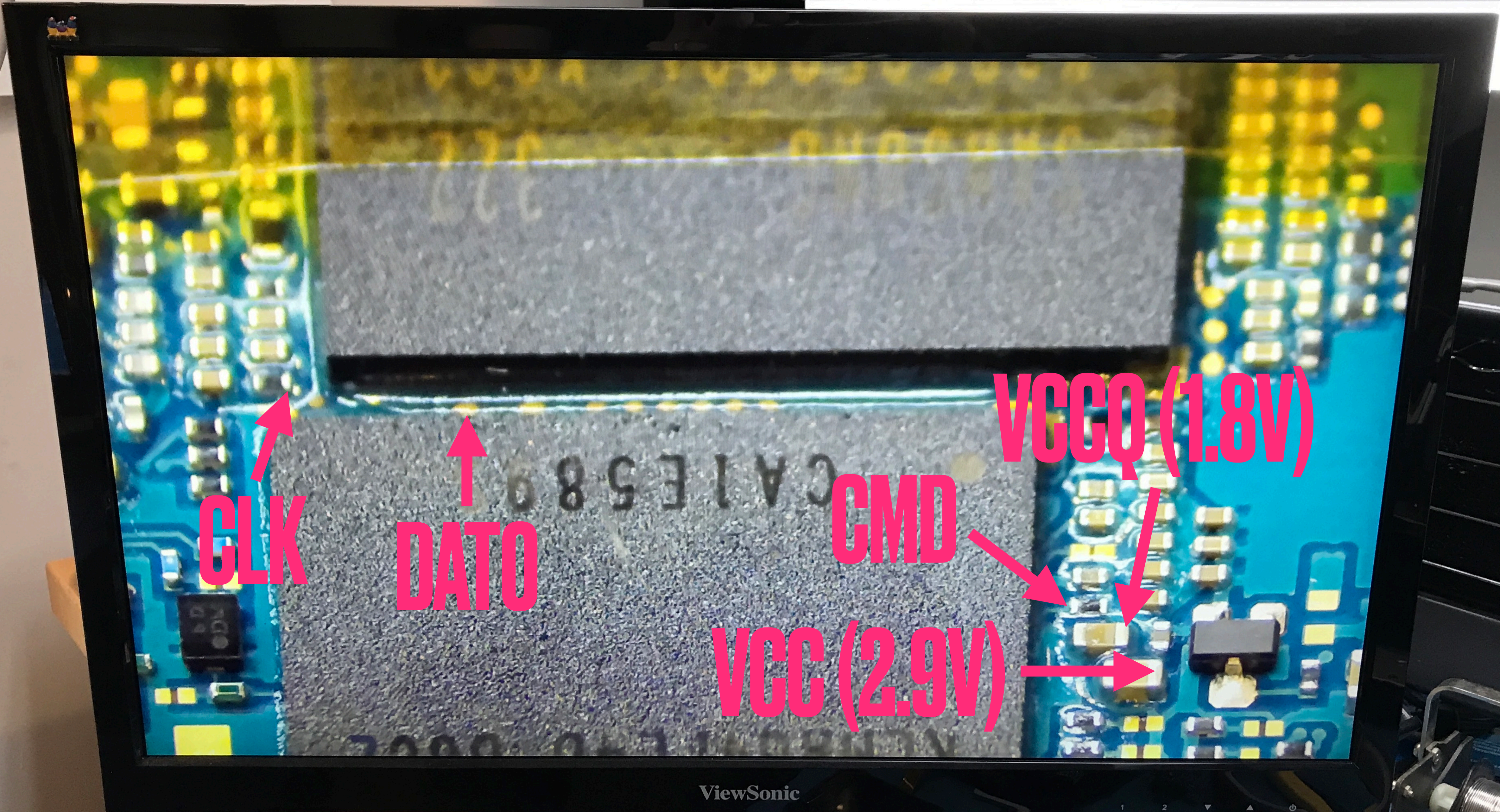
**OCTOPLUS Server Credits**
Direct Unlock, Repair IMEI, Repair TA, Read/Write TA, Read Info, Write Firmware for FREE!
only 1,4 USD

**Operation progress**

21%

Status: Reading
16.4/77.8Mb, speed: 230.6 (Kb/s)
VREF: 1.80 V
S/N: 0000D822
Firmware: 1.24





**CLK**

**DAT0**

**CMD**

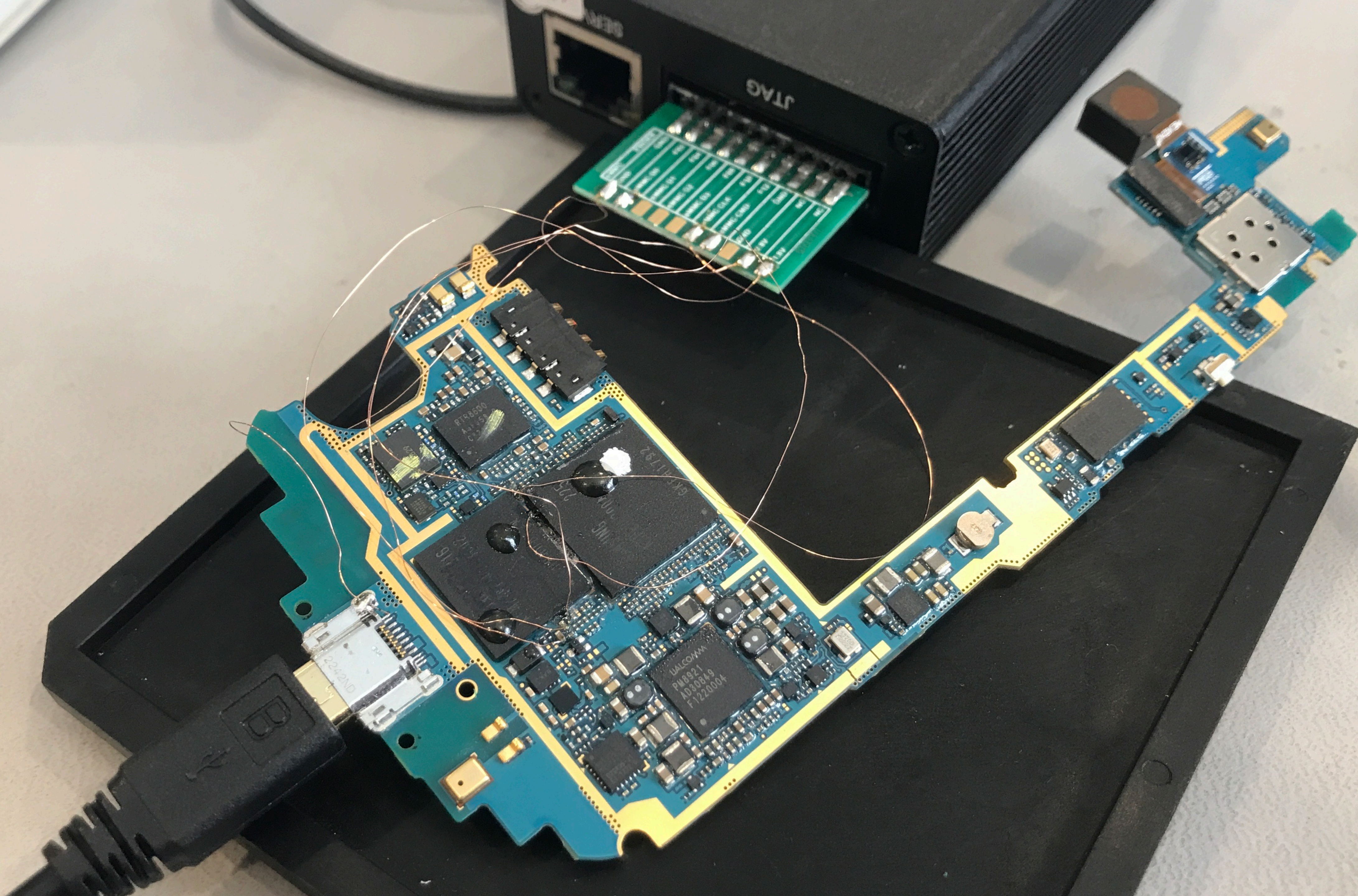
**VCCQ (1.8V)**

**VCC (2.9V)**

ViewSonic

1 2







Model Settings

- JTAG
- USB
- eMMC
- UFS
- ADB
- NAND

Brand: Samsung

Model: SCH-I535

Voltage: Auto Bus Mode: Auto

Bus speed: Auto

Log

SW: 2.2.4.3; FW: 1.24.

P00: GPT	(00000000, 00002000)	4 MB
P01: modem	(00002000, 0001E000)	60 MB
P02: sb11	(00020000, 00000100)	128 KB
P03: sb12	(00020100, 00000200)	256 KB
P04: sb13	(00020300, 00000400)	512 KB
P05: aboot	(00020700, 00001000)	2048 KB
P06: rpm	(00021700, 00000400)	512 KB
P07: boot	(00021B00, 00005000)	10 MB
P08: tz	(00026B00, 00000400)	512 KB
P09: pad	(00026F00, 00000400)	512 KB
P10: param	(00027300, 00005000)	10 MB
P11: efs	(0002C300, 00006D00)	13.62 MB
P12: modemst1	(00033000, 00001800)	3072 KB
P13: modemst2	(00034800, 00001800)	3072 KB
P14: system	(00036000, 002EE000)	1500 MB
P15: userdata	(00324000, 0187A000)	12.24 GB
P16: persist	(01B9E000, 00004000)	8 MB
P17: cache	(01BA2000, 001A4000)	840 MB
P18: recovery	(01D46000, 00005000)	10 MB
P19: fota	(01D48000, 00005000)	10 MB
P20: backup	(01D50000, 00003000)	6 MB
P21: fsg	(01D53000, 00001800)	3072 KB
P22: ssd	(01D54800, 00000010)	8 KB
P23: grow	(01D54810, 00002800)	5 MB

Backuping efs partition...

Welcome

eMMC

Pin finder

Read Android build info while connecting

Write data verification

Main | Factory repair | eMMC Service

Boot Area Part. 1  Boot Area Part. 2  RPMB

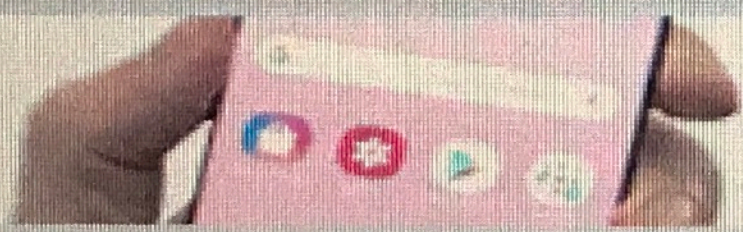
GP1  GP2  GP3  GP4

User Data Area

Partitions

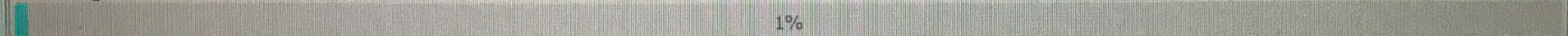
Custom Start  0b

Full Length  4.096 GB

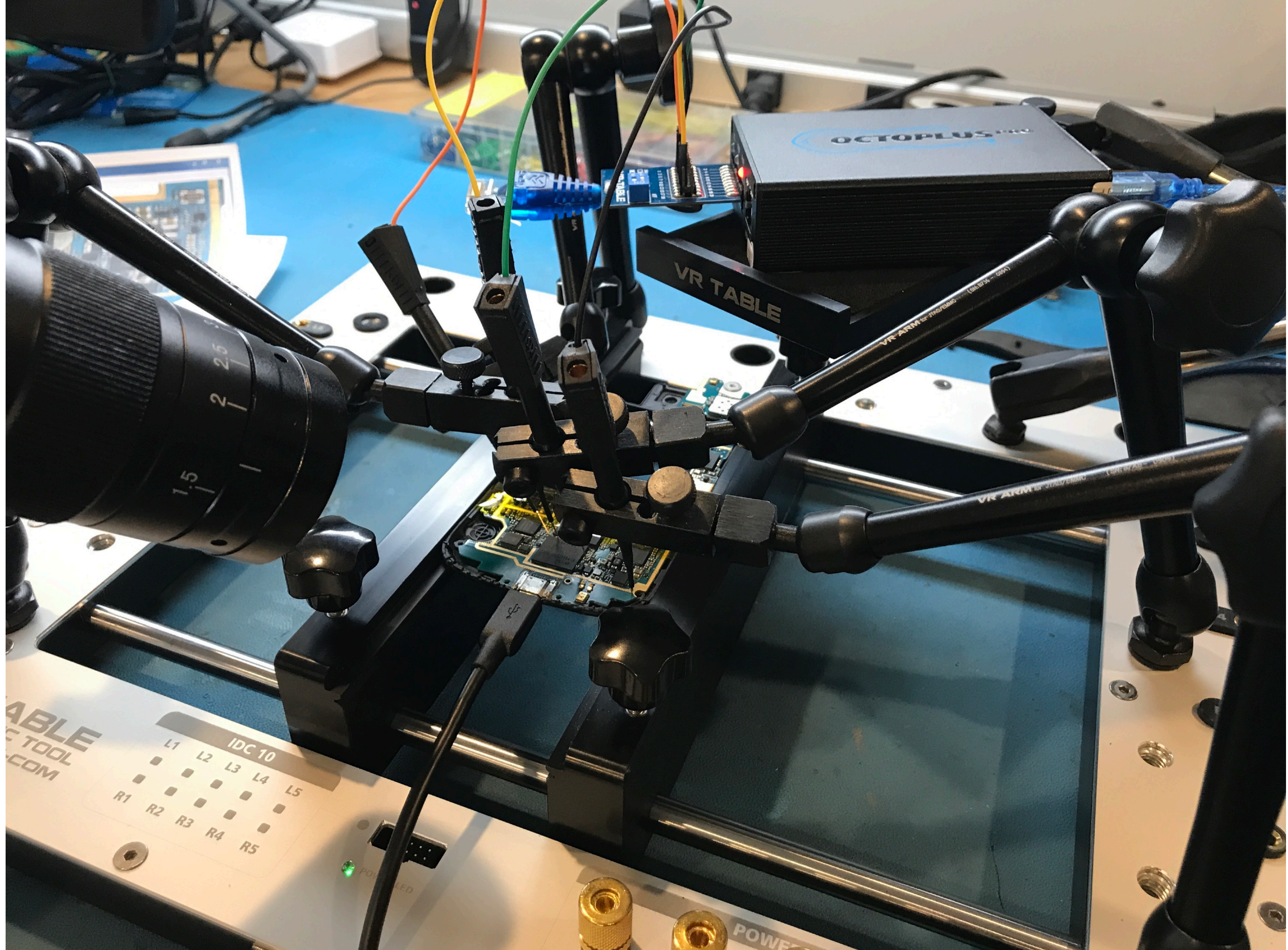


Octoplus Samsung: Galaxy S10 series support

Progress







VR TABLE  
VR TOOL  
COM

	L1	L2	L3	L4	L5
R1	R2	R3	R4	R5	

POWER







# RESOURCES

- [Joe's YouTube Channel](#)
- [Grand Idea Studio](#)
- [offspec.io](#)
- [ChipWhisperer](#)
- [PhyWhisperer-USB](#)
- [SEGGER J-Link](#)
- [ChipSHOUTER](#)
- [μArt](#)
- [STM32 LQFP-64 Socket Adapter](#)
- [JTAGulator](#)
- [Octoplus PRO Box](#)
- [Multi-Com VR-TABLE](#)
- [HAYEAR 16MP HDMI Microscope Camera + 180x Zoom Lens](#)



HACKED BY  
JOE GRAND  
\$KINGPIN\$