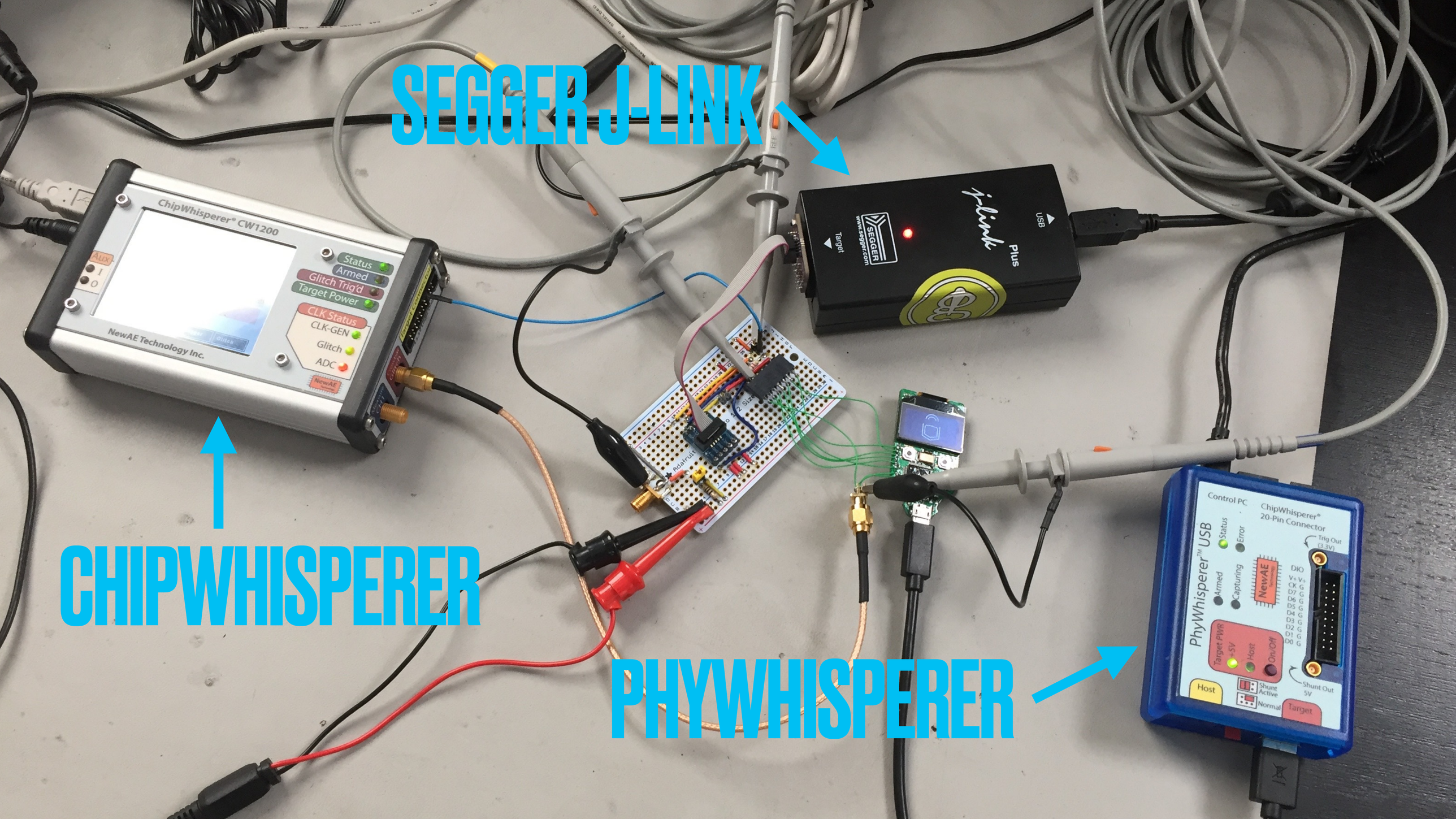
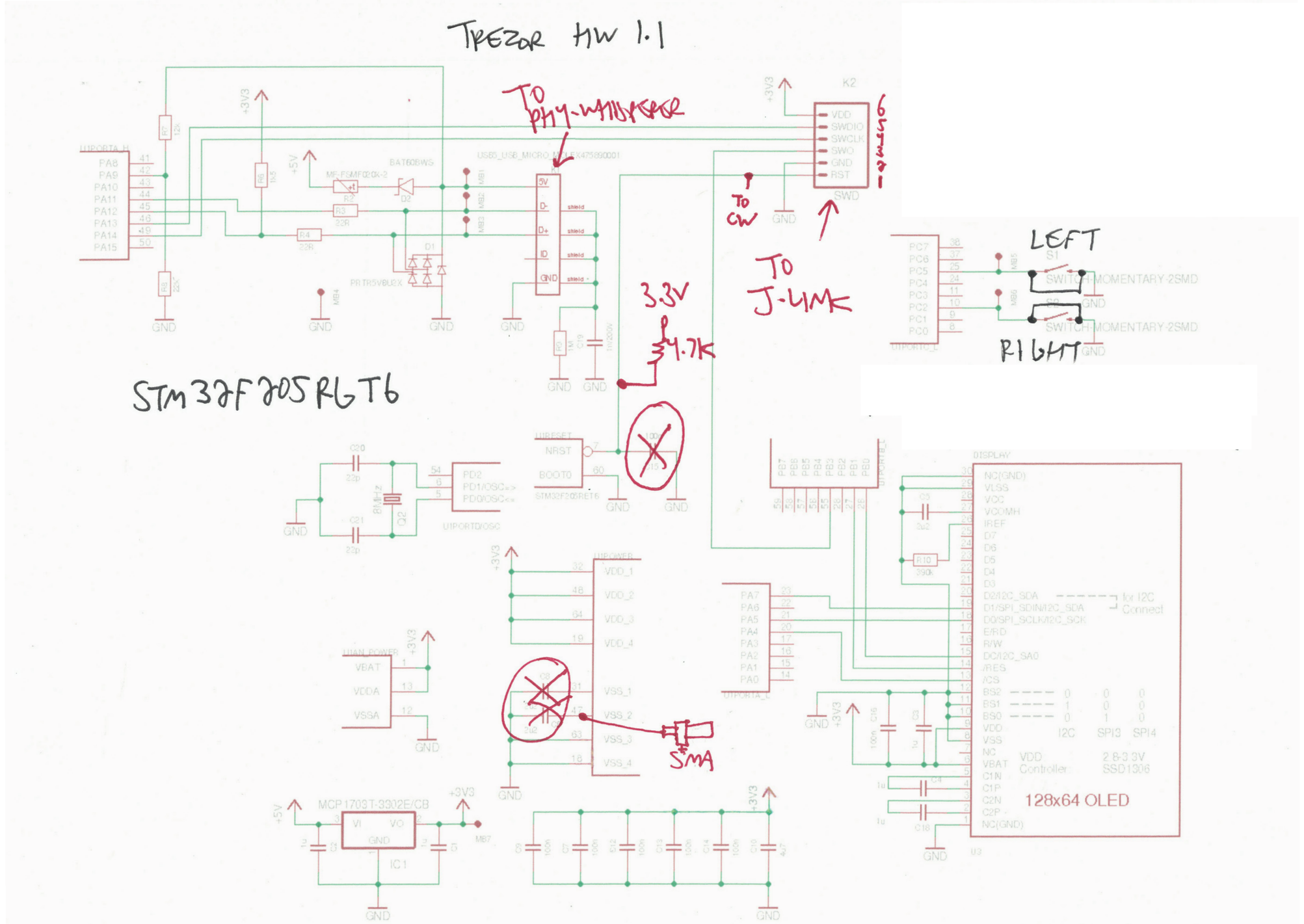
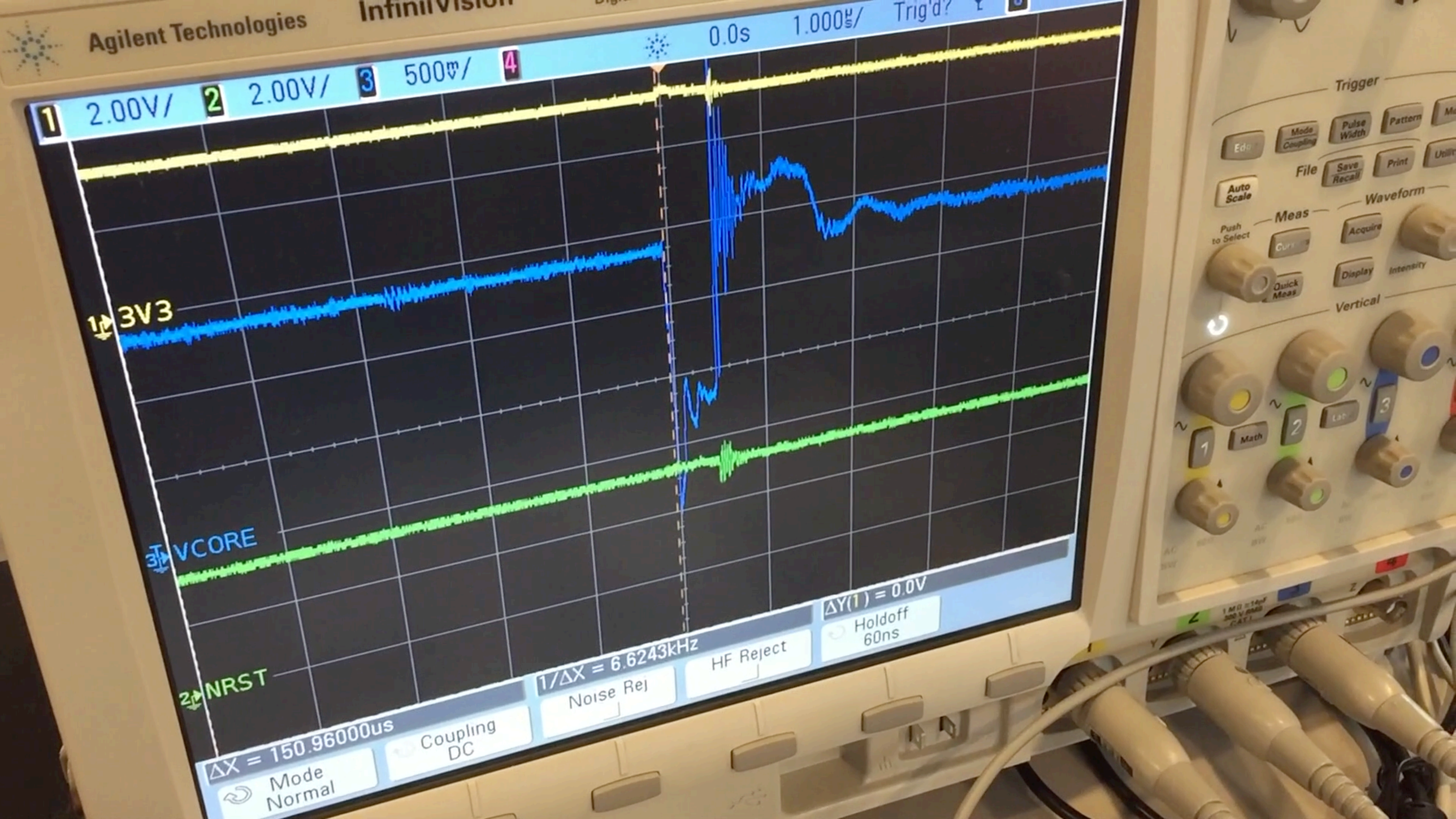
JOE GRAND'S ADVENTURES OF WALLET HACKING

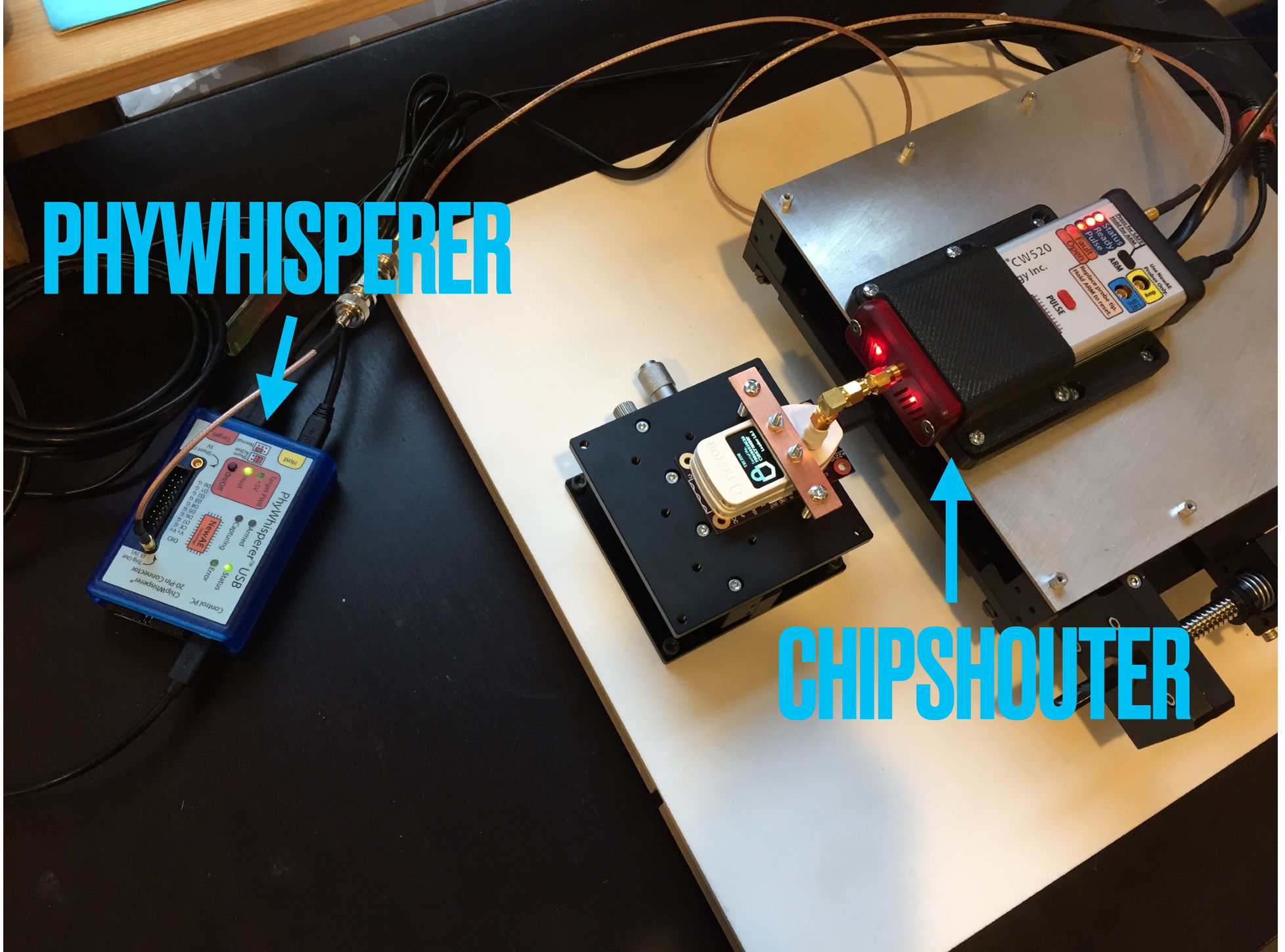
HARDWEAR.IO USA 2022

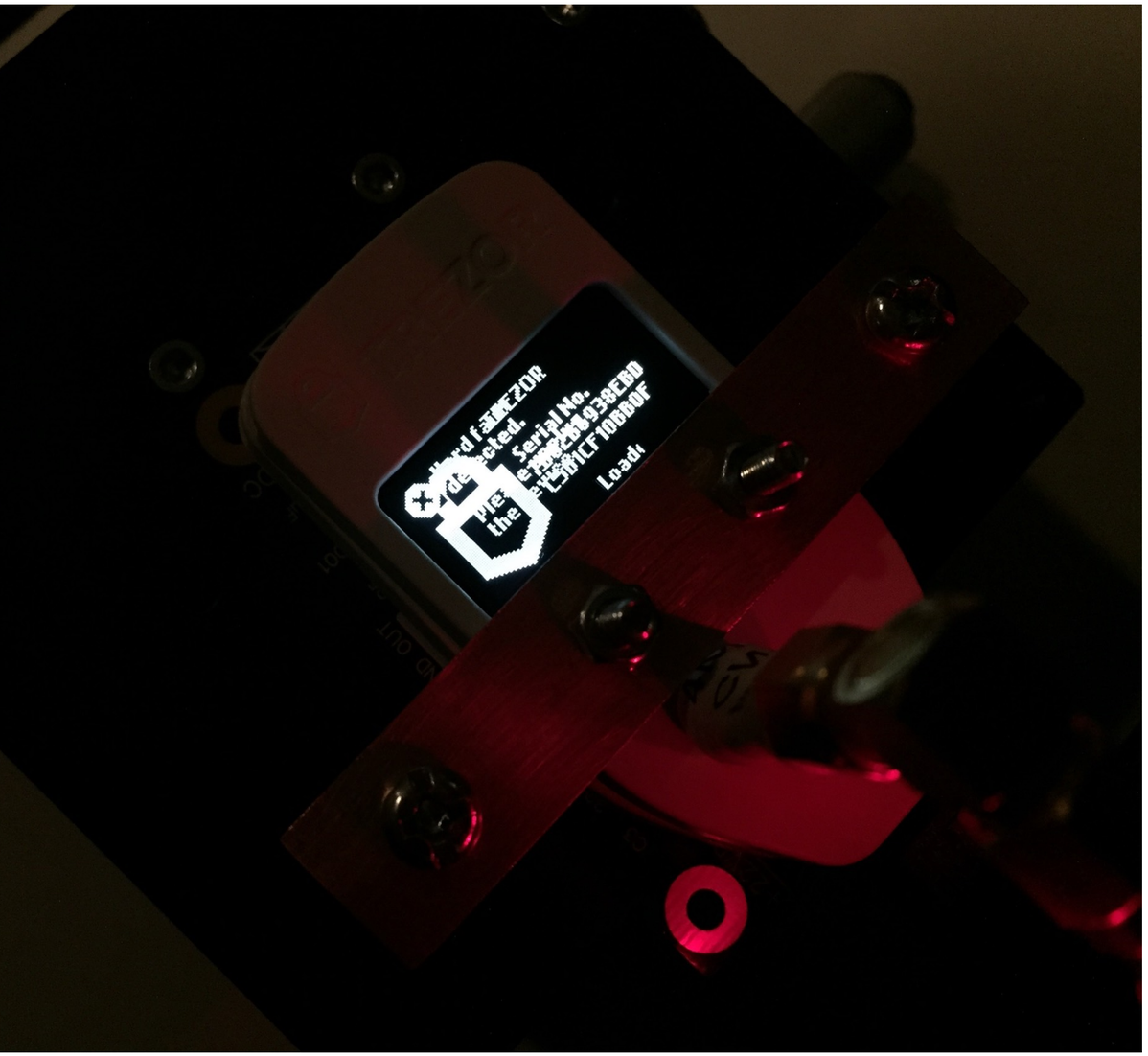

SEGGER J-LINK
CHIPWHISPERER
PHYWHISPERER
ChipWhisperer® CW1200
NewAE Technology Inc.
Status
Armed
Glitch Trig'd
Target Power
CLK Status
CLK-GEN
Glitch
ADC
SEGGER
www.segger.com
Target
USB
Plus
Control PC
ChipWhisperer®
20-Pin Connector
PhyWhisperer™ USB
Armed
Capturing
Target PWR
+5V
Host
On/Off
Shunt
Active
Normal
Host
Target
Trig Out
(3.3V)
Shunt Out
5V

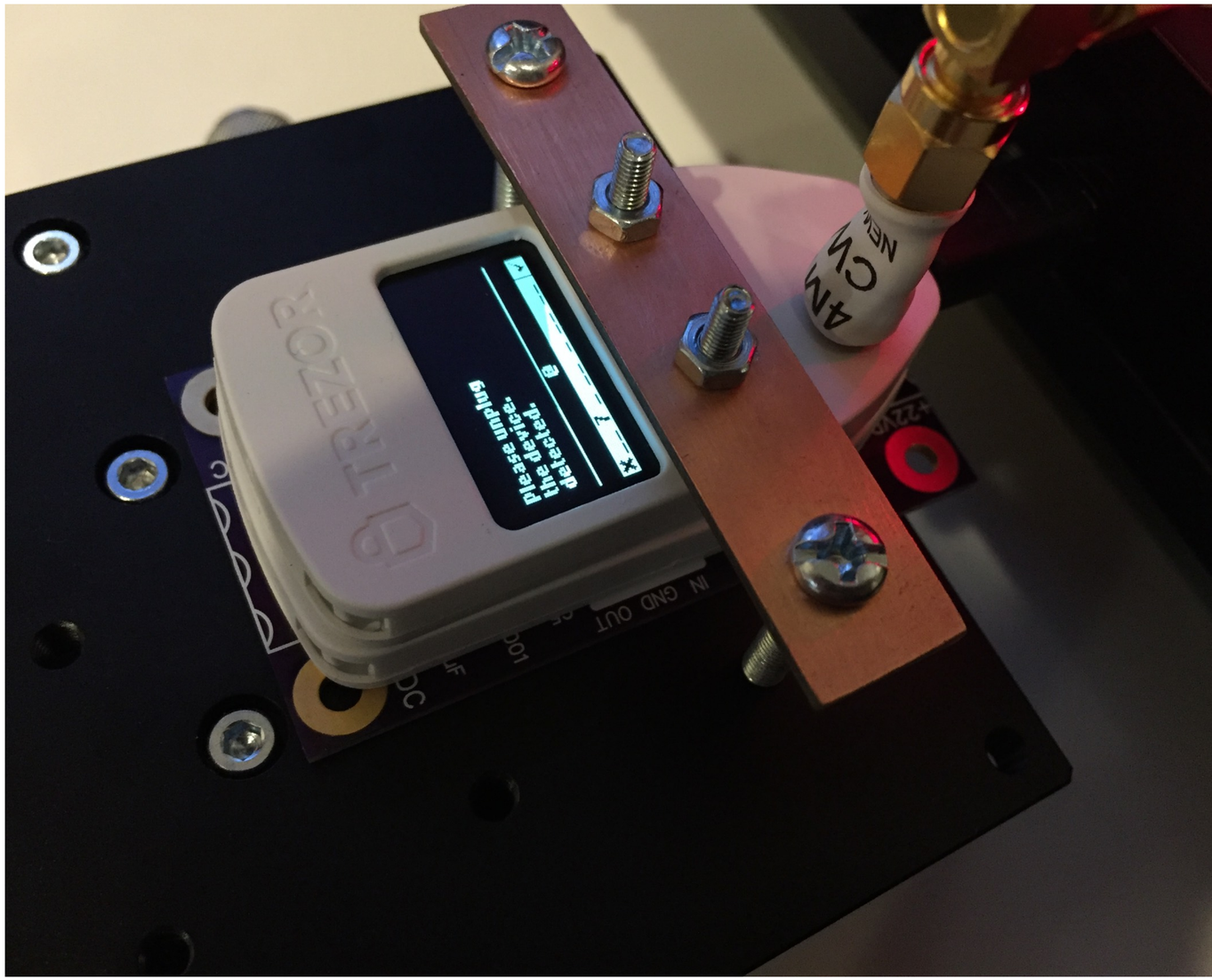

TREZOR HW 1.1
TO PHY-MASTER
TO CW
TO J-LINK
3.3V
4.7K
STM32F205RGT6
LEFT
RIGHT
SWITCH-MOMENTARY-2SMD
SMA
MCP1703T-3302E/CB
128x64 OLED
DISPLAY
for I2C Connect
SWD
K2

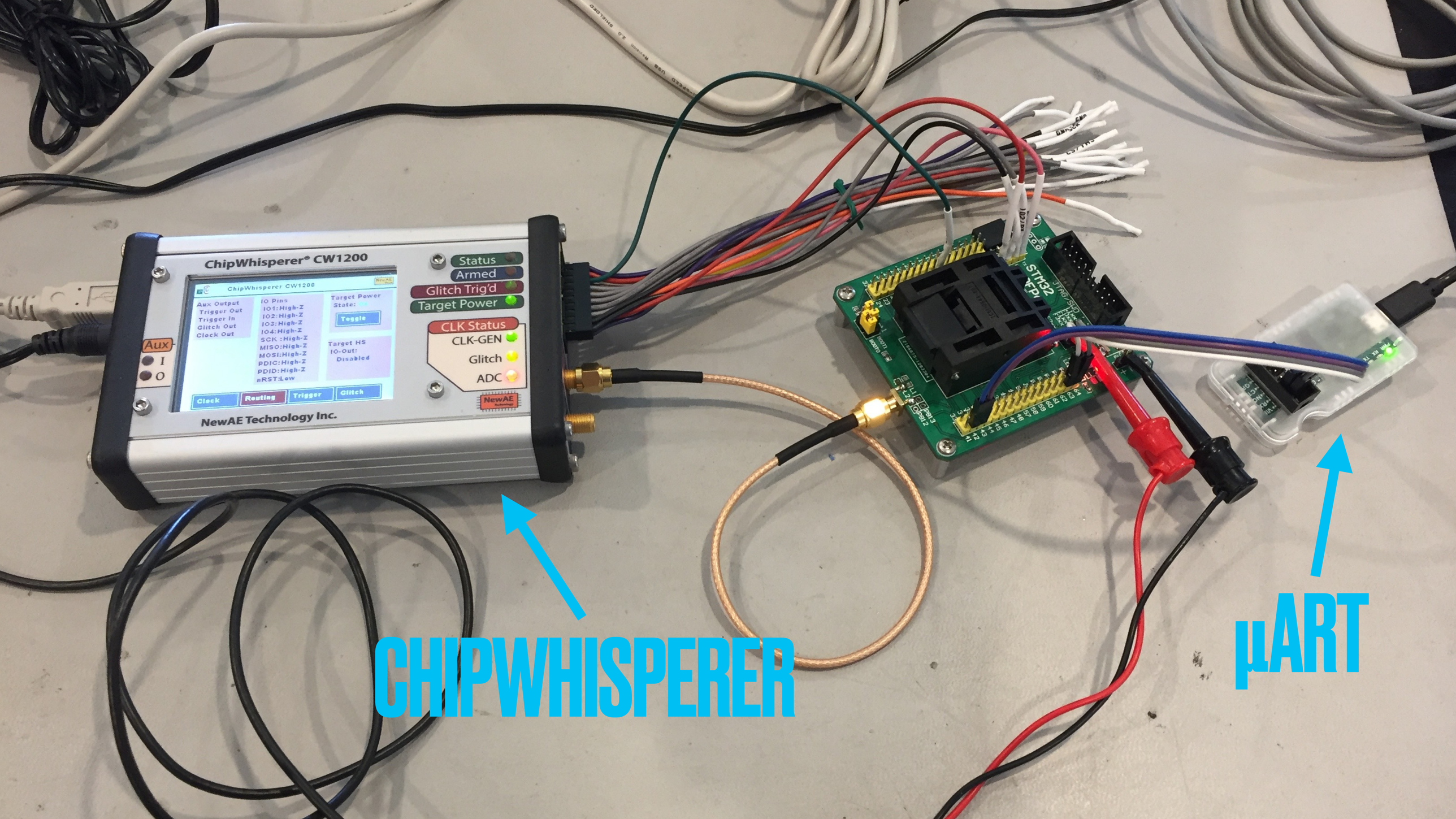

Agilent Technologies
InfiniiVision
0.0s
1.000µs/
Trig'd?
1 2.00V/
2 2.00V/
3 500mV/
4
3V3
VCORE
NRST
ΔX = 150.96000us
1/ΔX = 6.6243kHz
ΔY(1) = 0.0V
Mode
Normal
Coupling
DC
Noise Rej
HF Reject
Holdoff
60ns
Trigger
Edge
Mode
Coupling
Pulse
Width
Pattern
File
Save
Recall
Print
Auto
Scale
Waveform
Meas
Push
to Select
Acquire
Quick
Meas
Display
Intensity
Vertical
Math

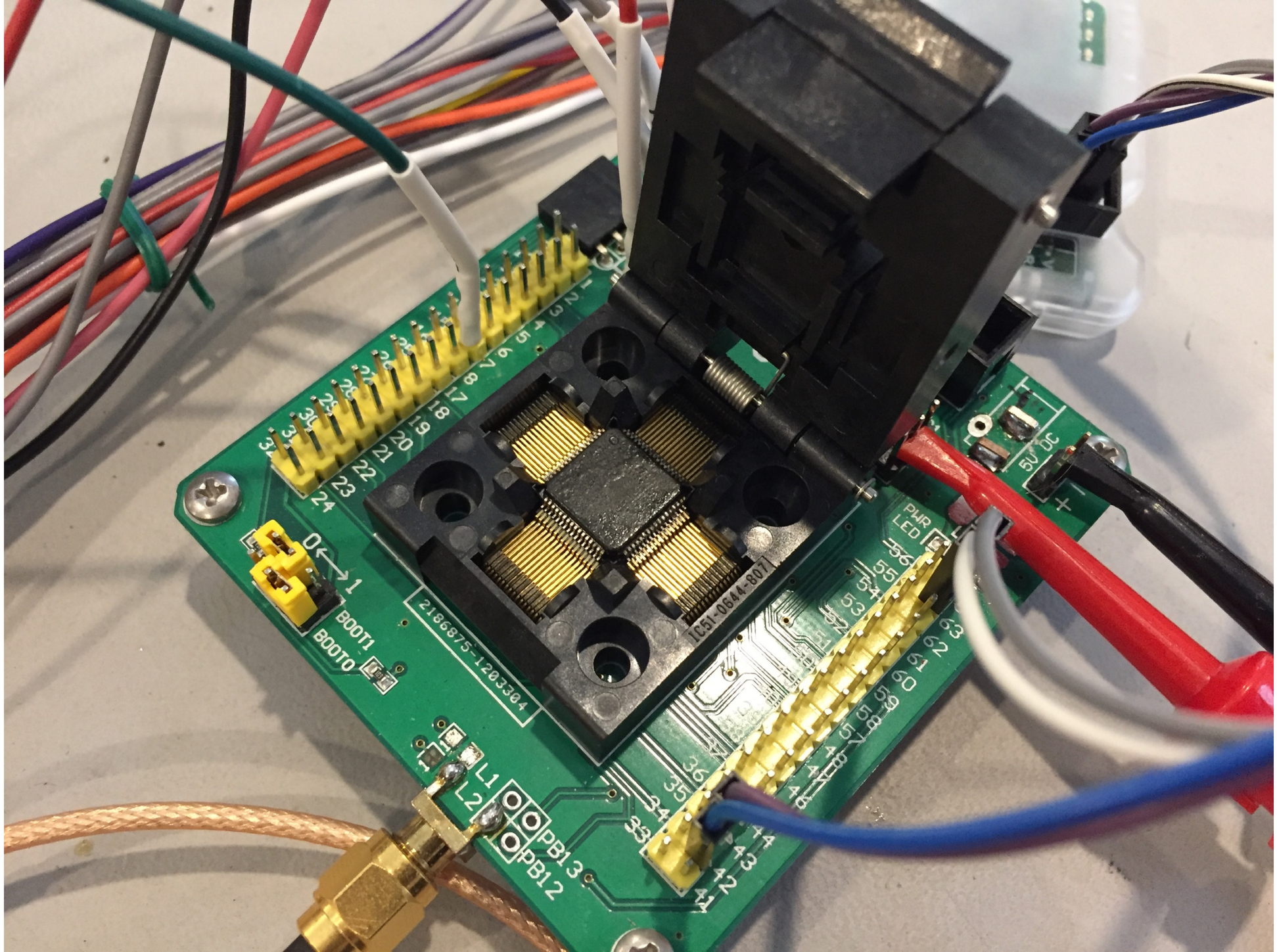

MERCURY
SONY
LANTRONIX
amazon.com
DigiKey
brother
BENRO
SONY

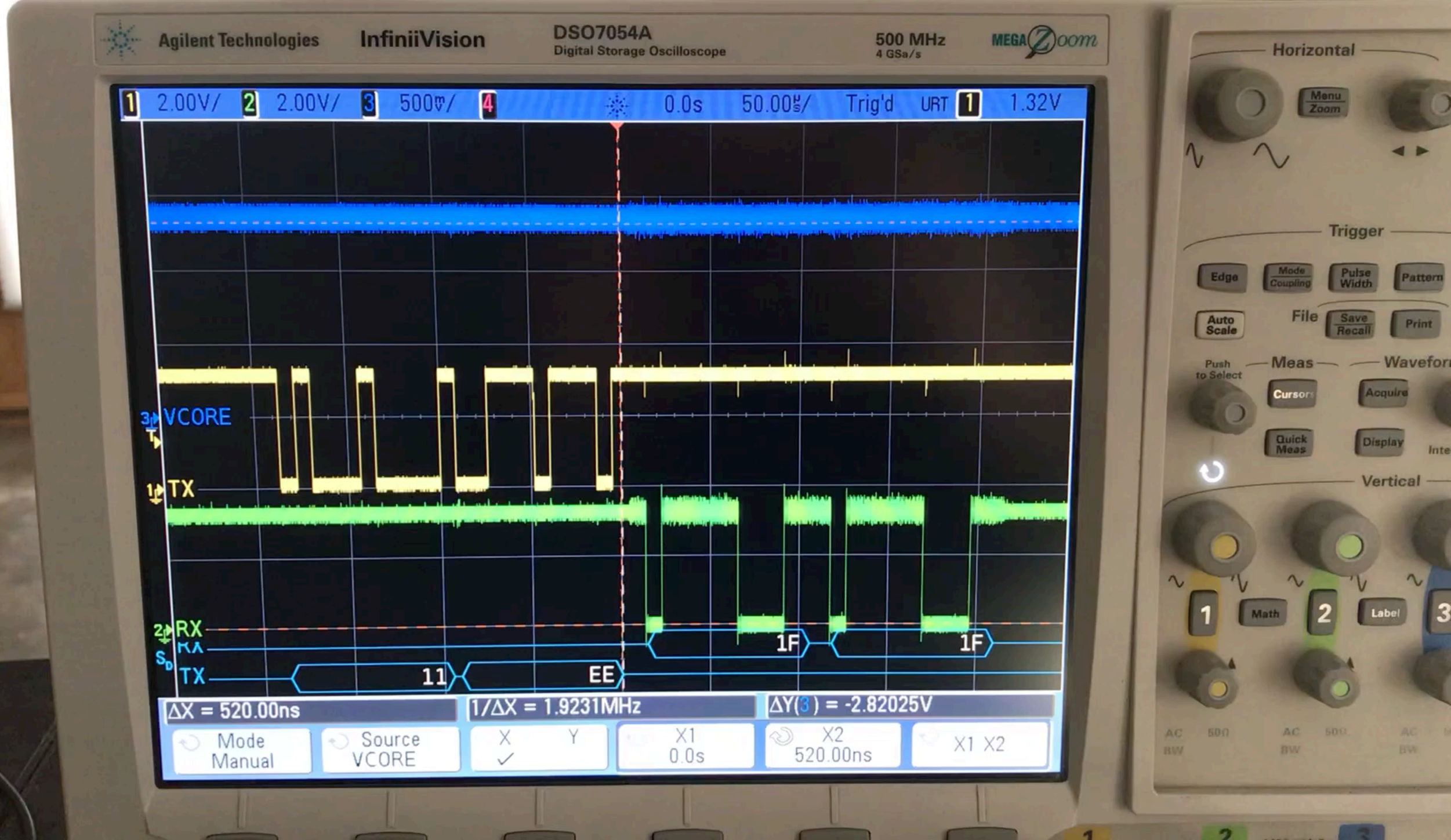

PHYWHISPERER
CHIPSHOUTER
PhyWhisperer-USB
CW520
Status
Ready
Pulse
Fault
Open
ARM
PULSE


Serial No.
Loadi

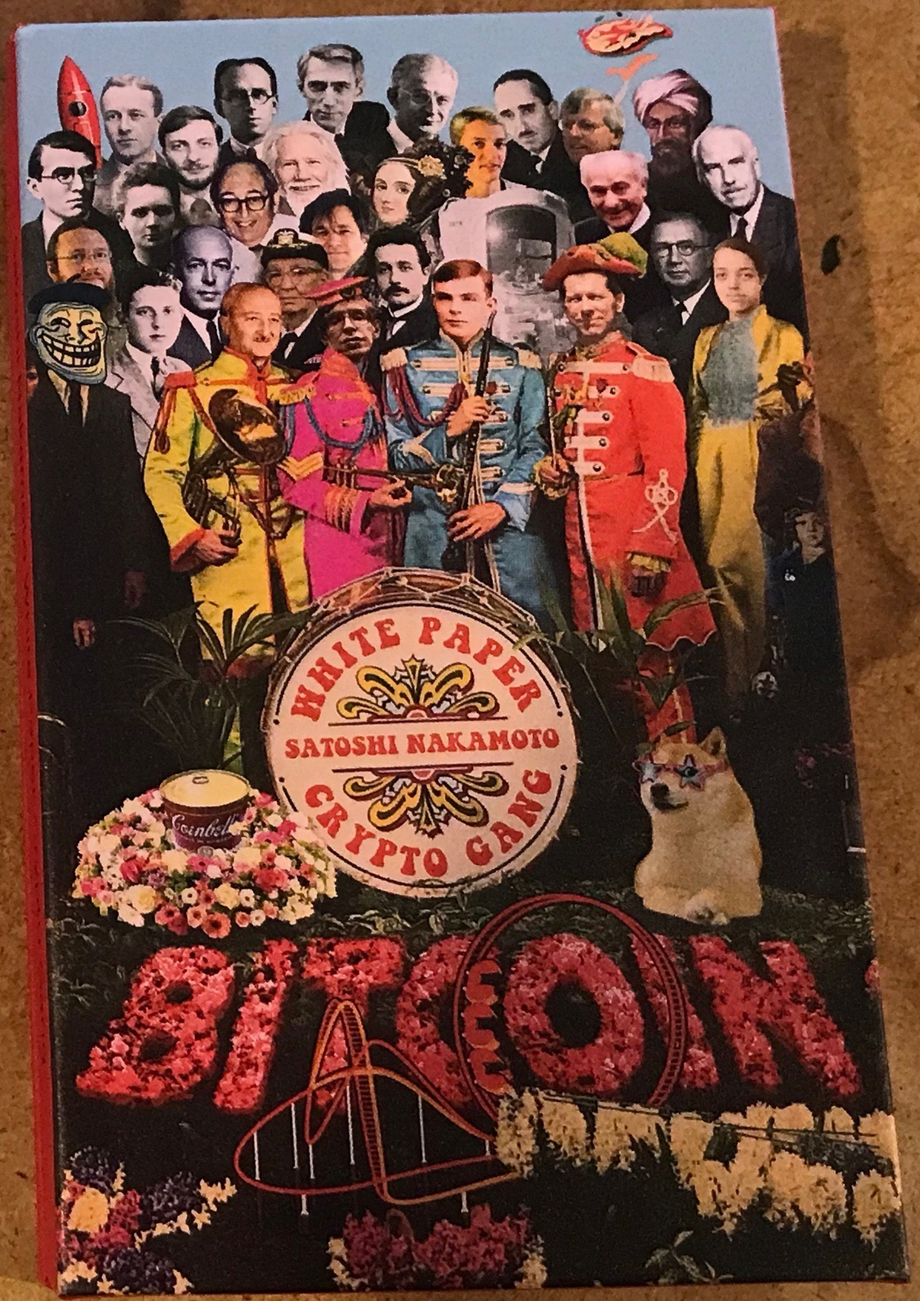

Please unplug
the device.
detected.
IN GND OUT

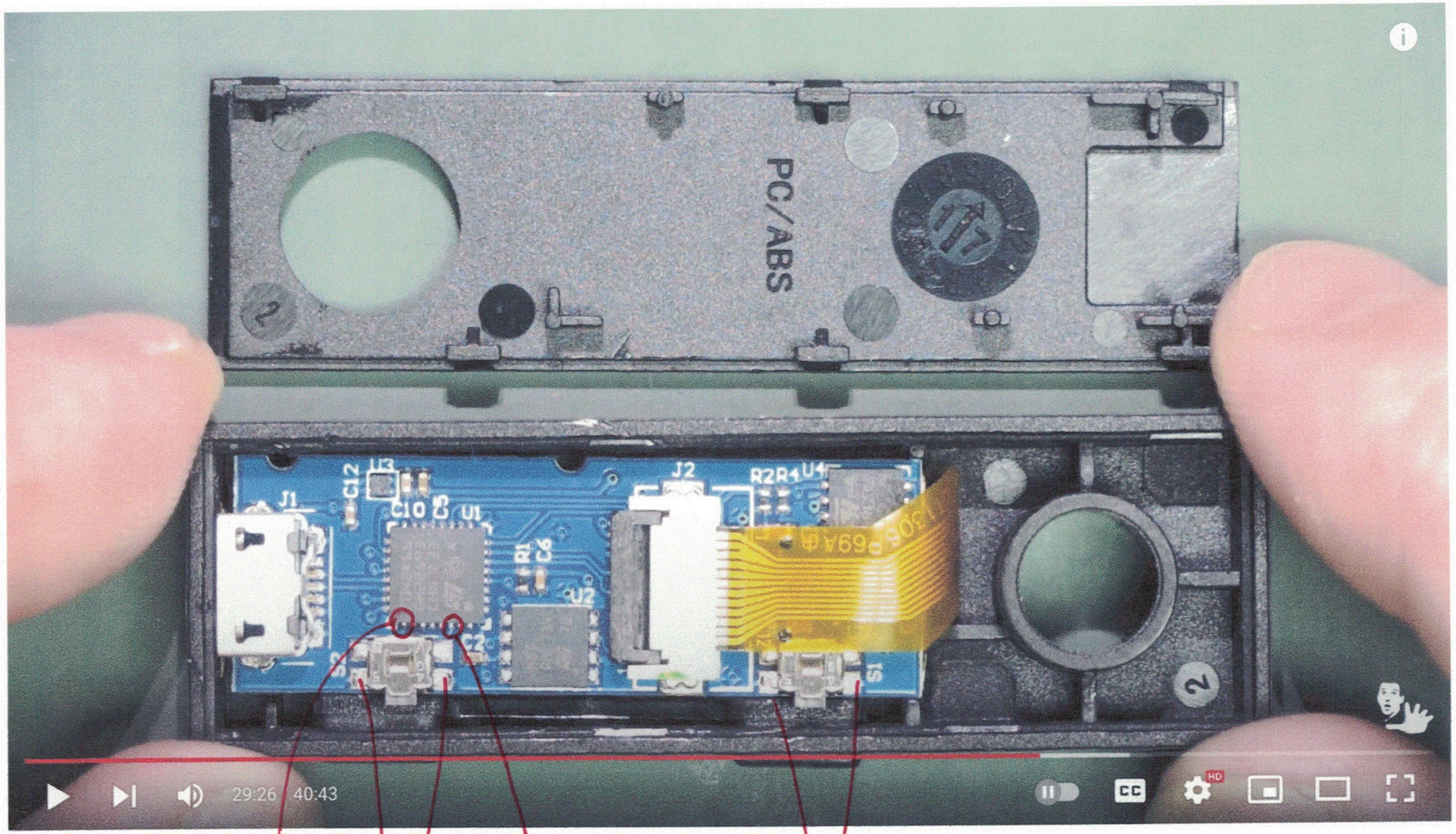

ChipWhisperer® CW1200
NewAE Technology Inc.
Status
Armed
Glitch Trig'd
Target Power
CLK Status
CLK-GEN
Glitch
ADC
Aux
Clock
Routing
Trigger
Glitch
CHIPWHISPERER
µART

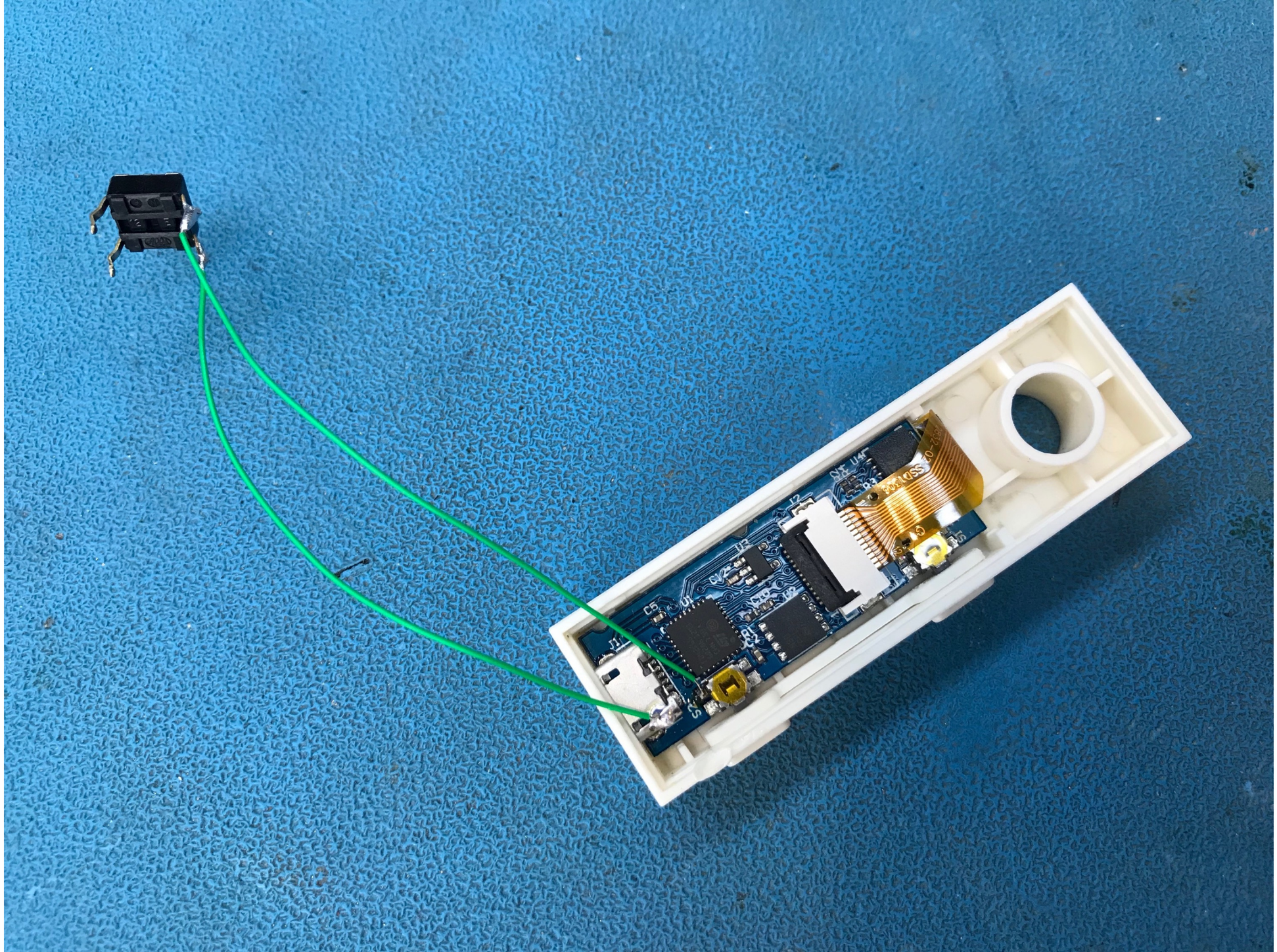

0
1
BOOT1
BOOT0
2186875-1203304
IC51-0644-807
PWR LED
5V DC
L1
L2
PB13
PB12

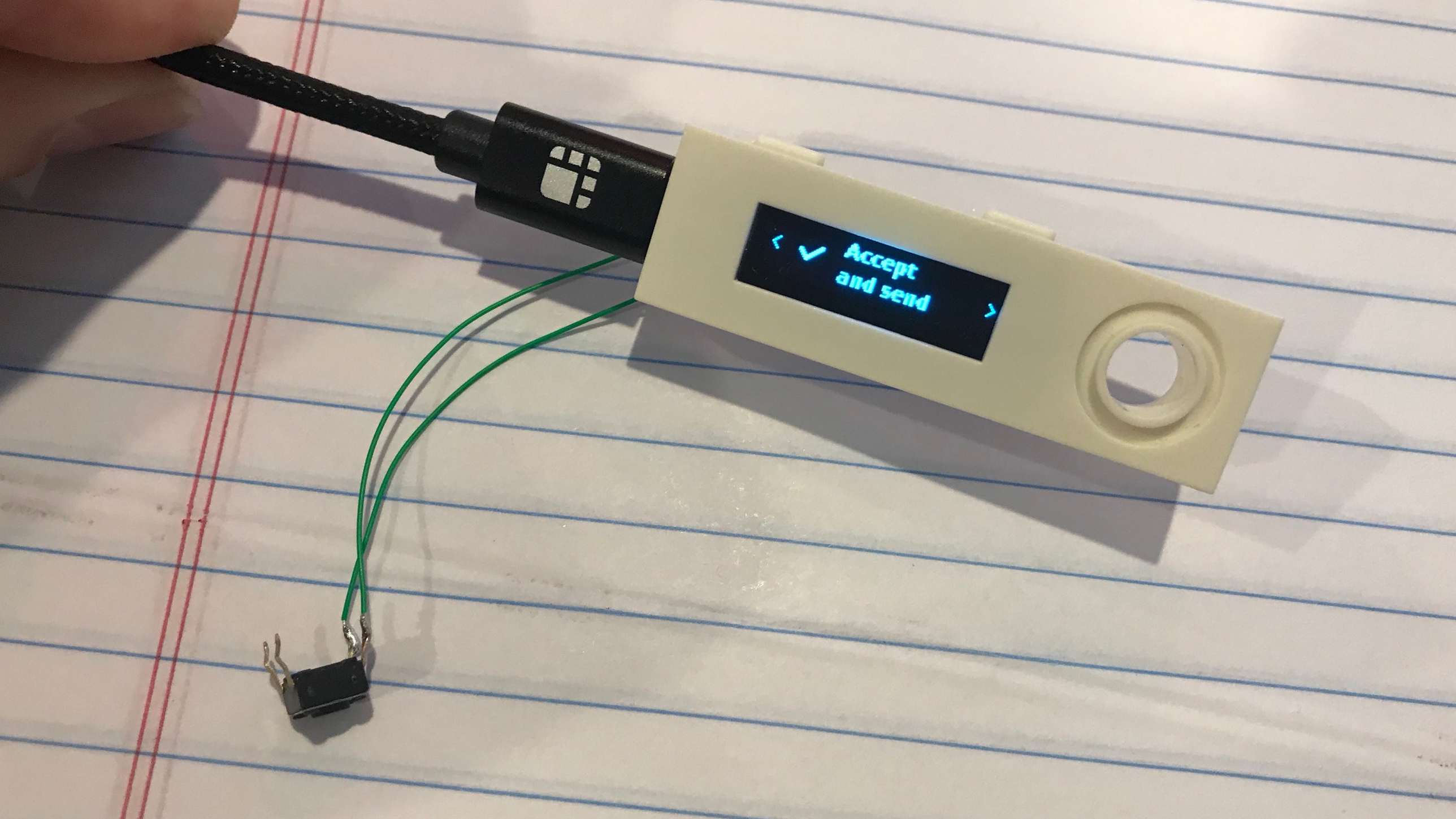

Agilent Technologies
InfiniiVision
DSO7054A
Digital Storage Oscilloscope
500 MHz
4 GSa/s
MEGA Zoom
1 2.00V/ 2 2.00V/ 3 500mV/ 4 0.0s 50.00ns/ Trig'd URT 1 1.32V
VCORE
TX
RX
TX
11
EE
1F
1F
ΔX = 520.00ns
1/ΔX = 1.9231MHz
ΔY(3) = -2.82025V
Mode Manual
Source VCORE
X Y
X1 0.0s
X2 520.00ns
X1 X2
Horizontal
Menu Zoom
Trigger
Edge
Mode Coupling
Pulse Width
Pattern
Auto Scale
File
Save Recall
Print
Push to Select
Meas
Cursors
Acquire
Quick Meas
Display
Vertical
1
Math
2
Label

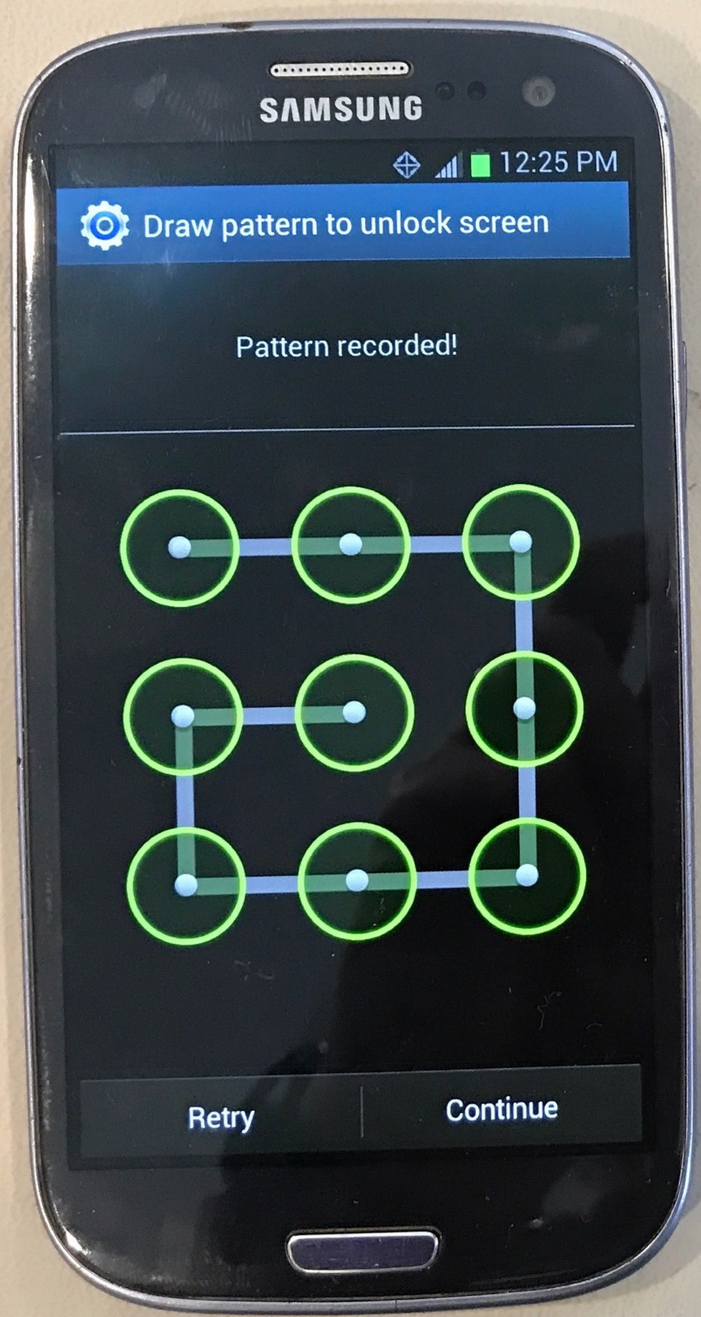
LEDGER NANO S
LIMITED EDITION
#2

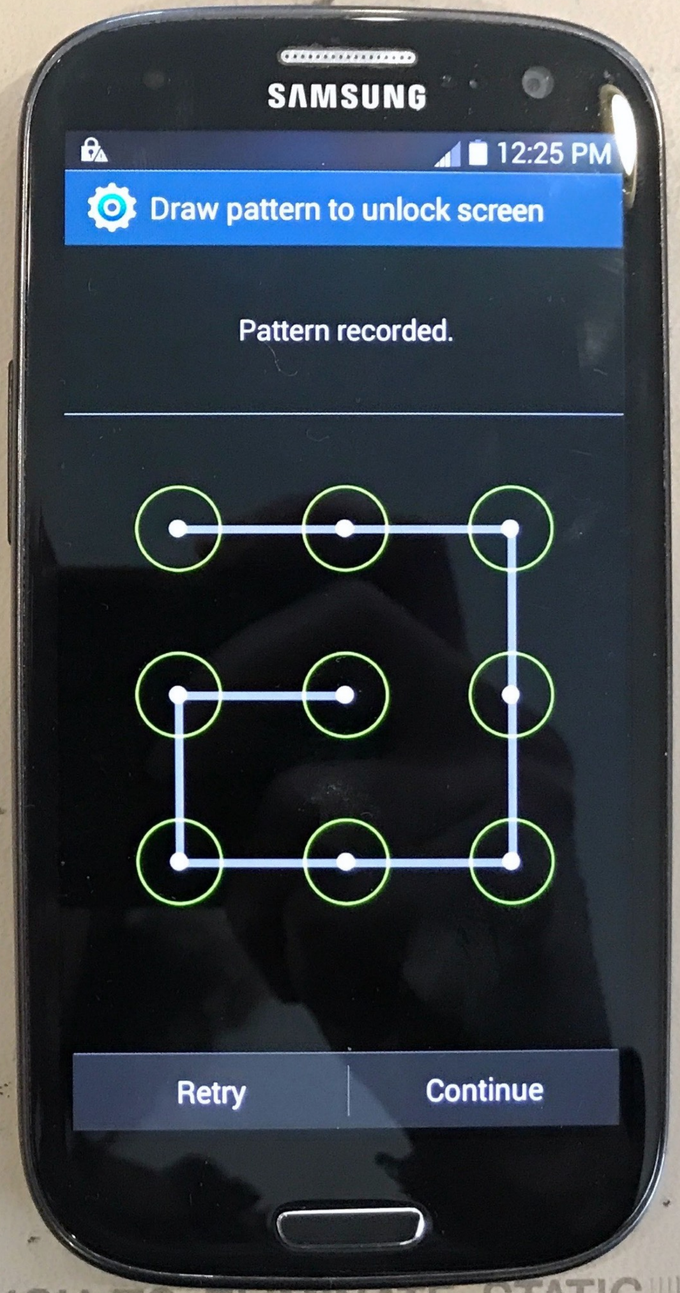


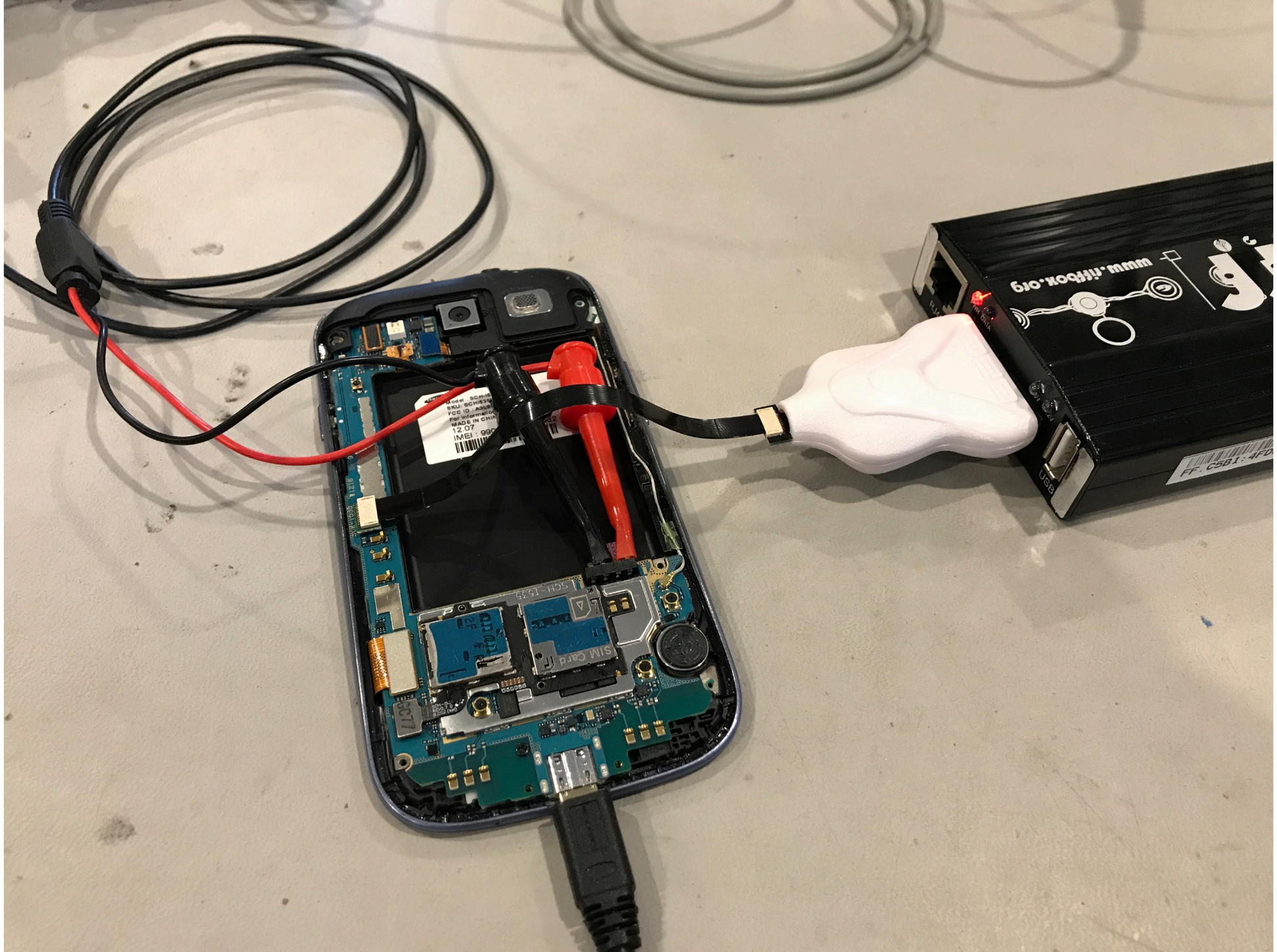

PC/ABS
J1
J2
U1
U2
U4
29:26
40:43
S2
GND
S1
GND

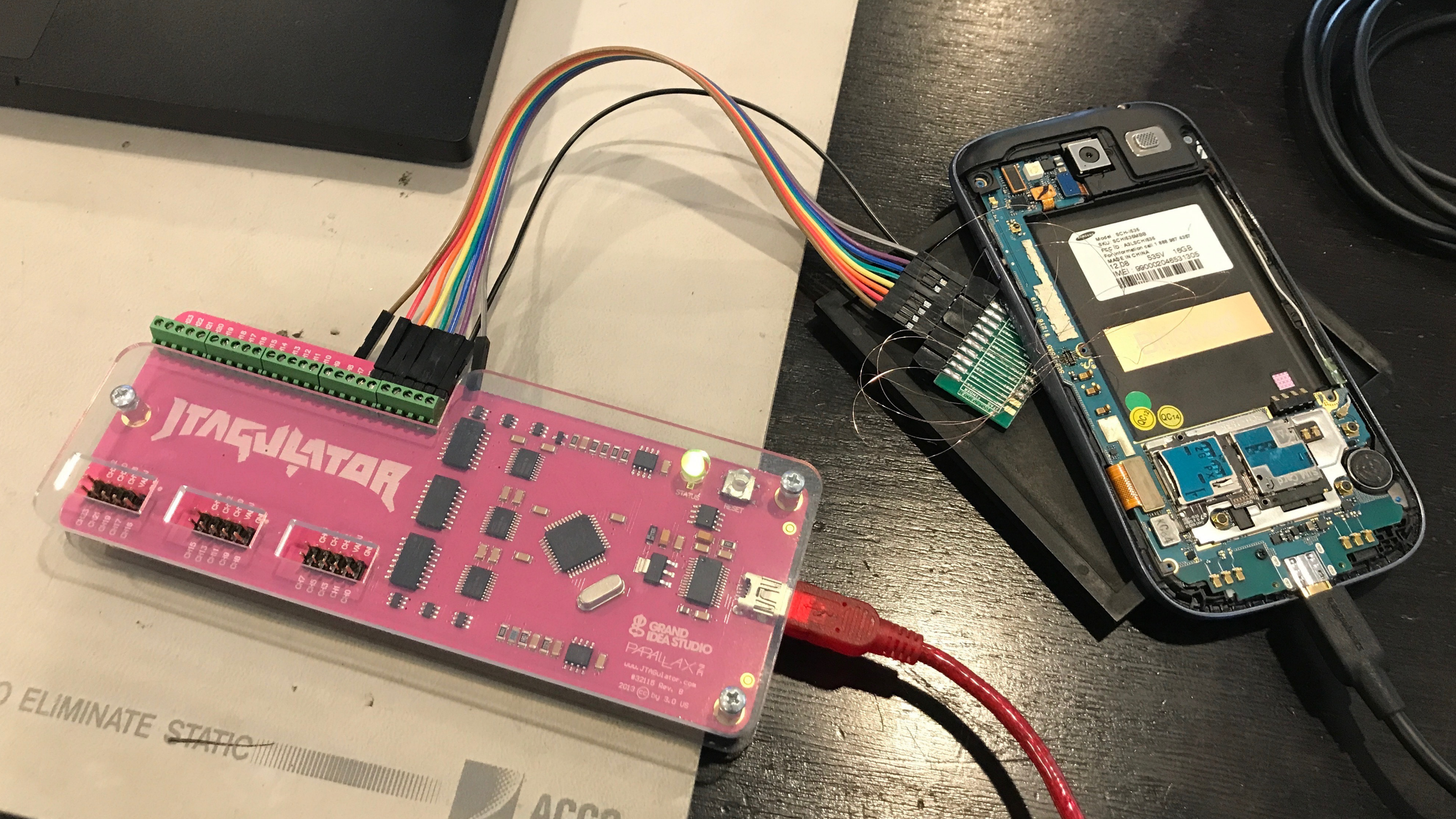


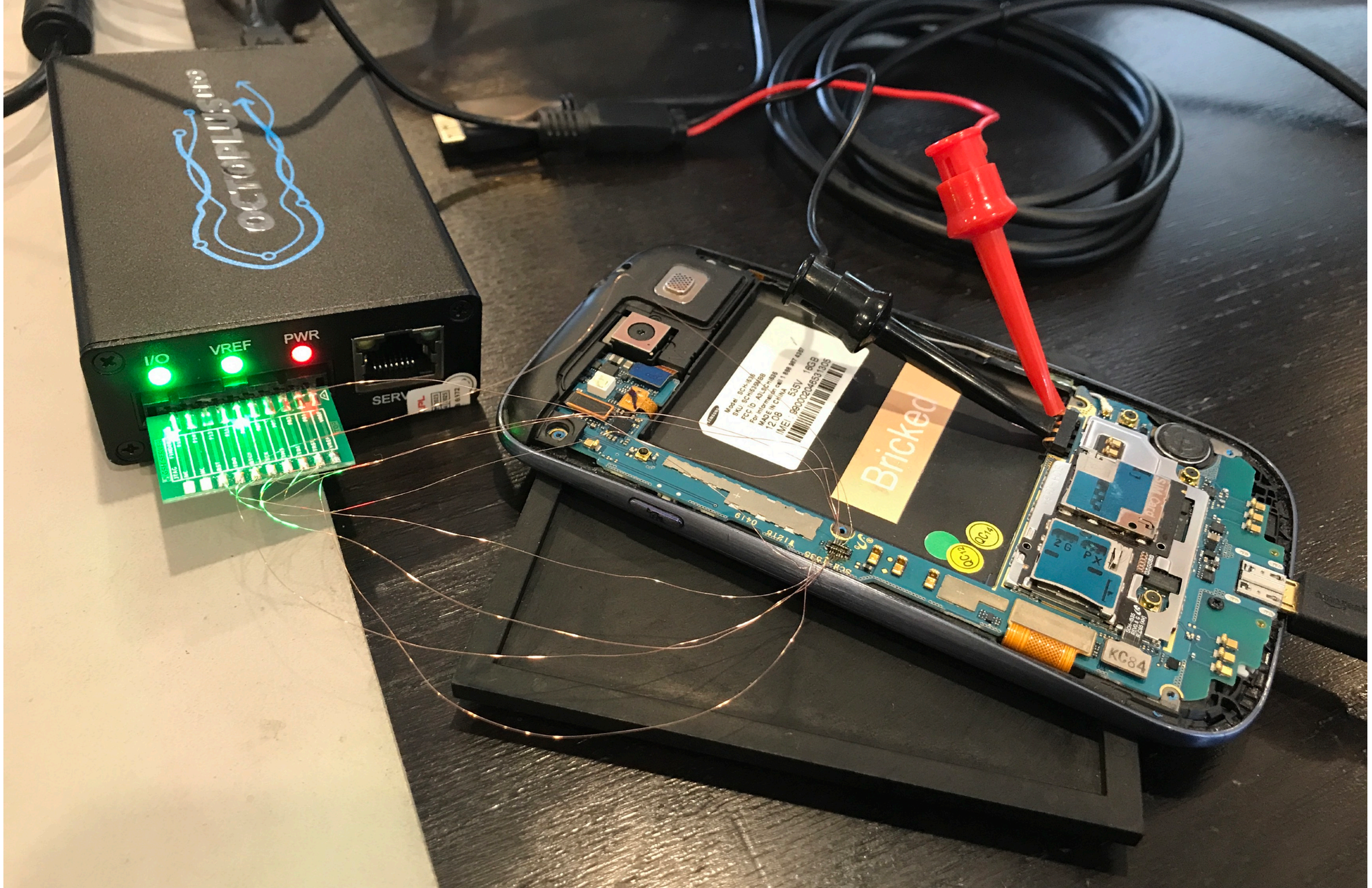

Accept
and send

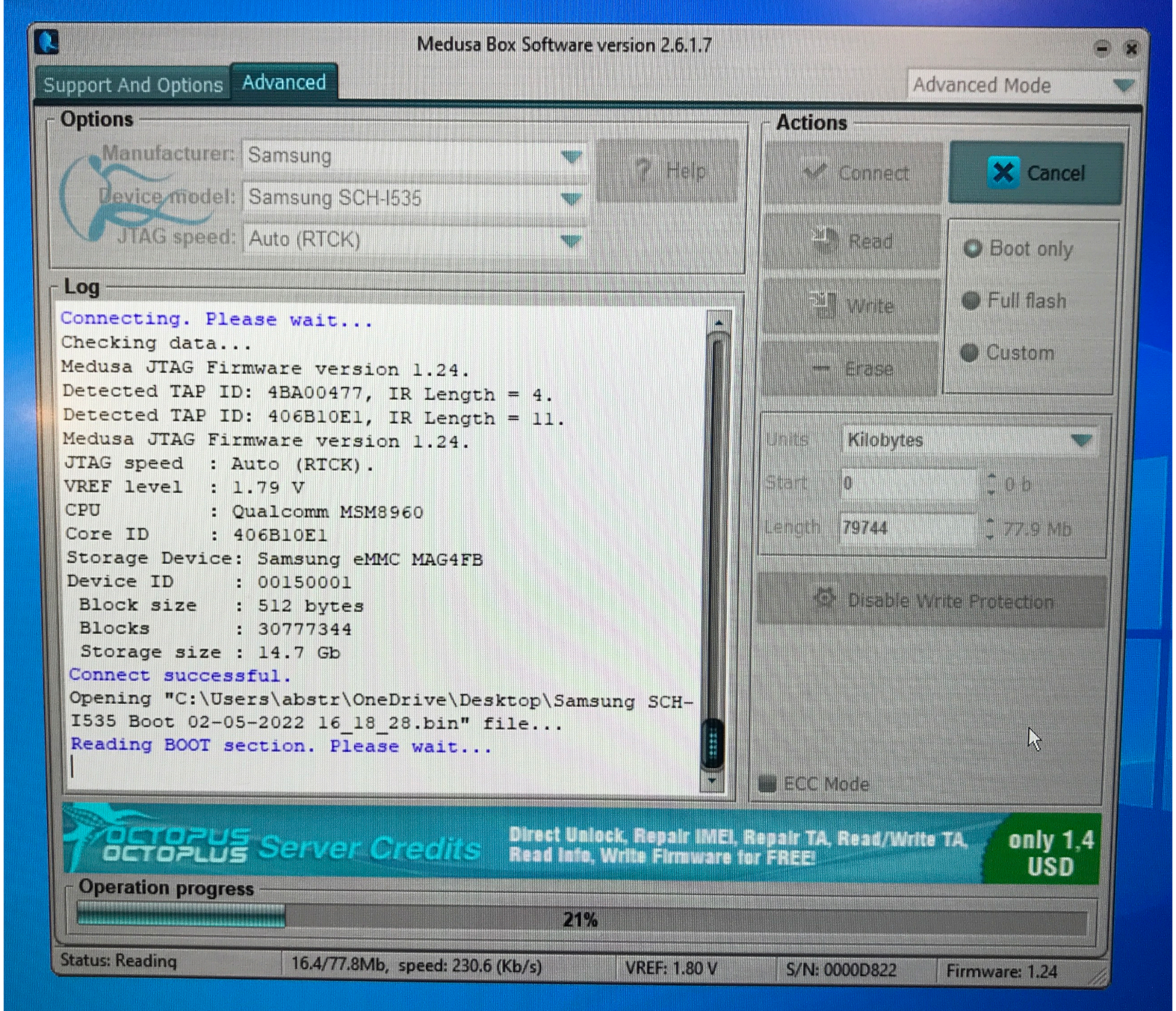


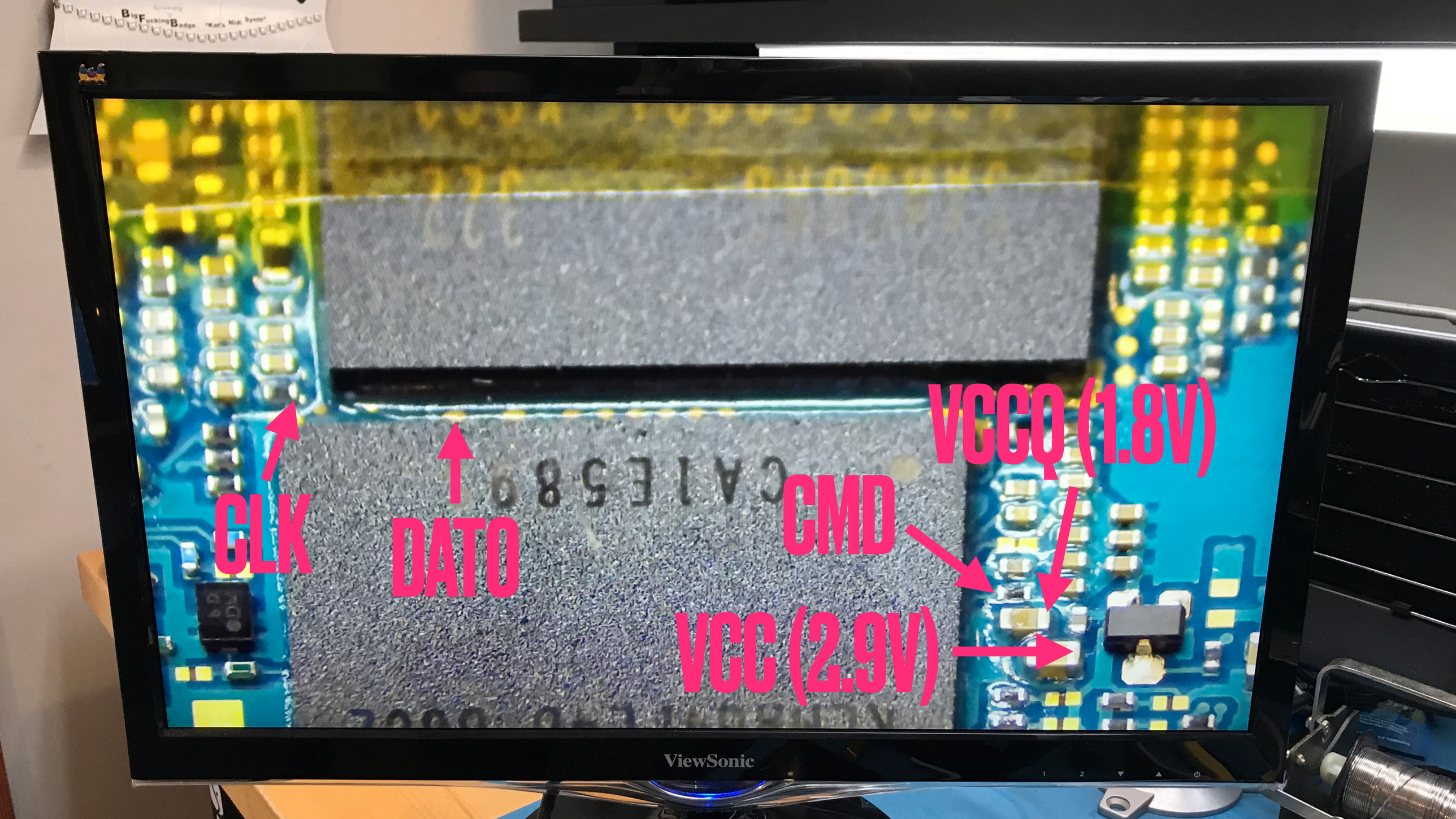


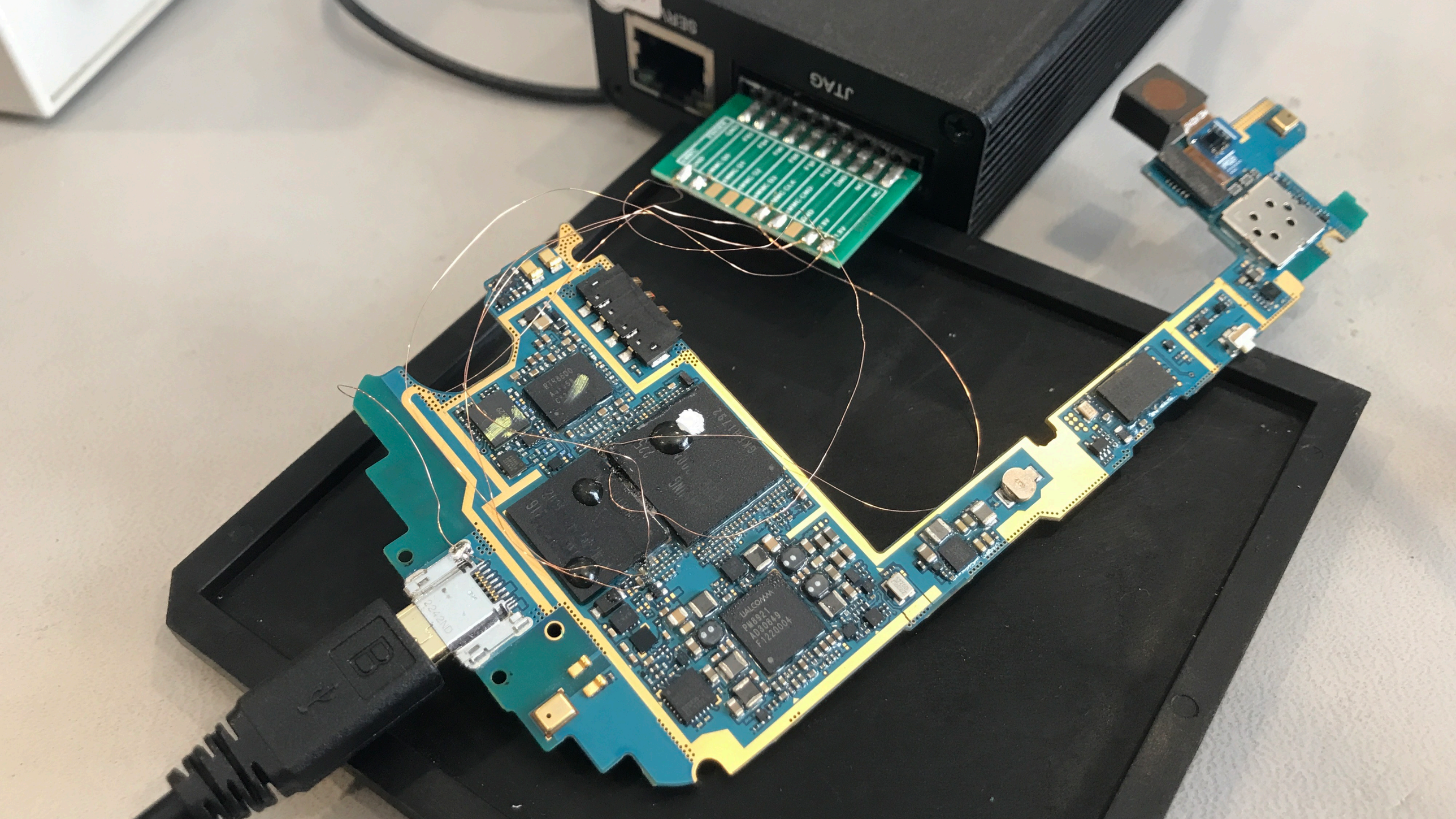

www.riffbox.org
SIM Card
USB

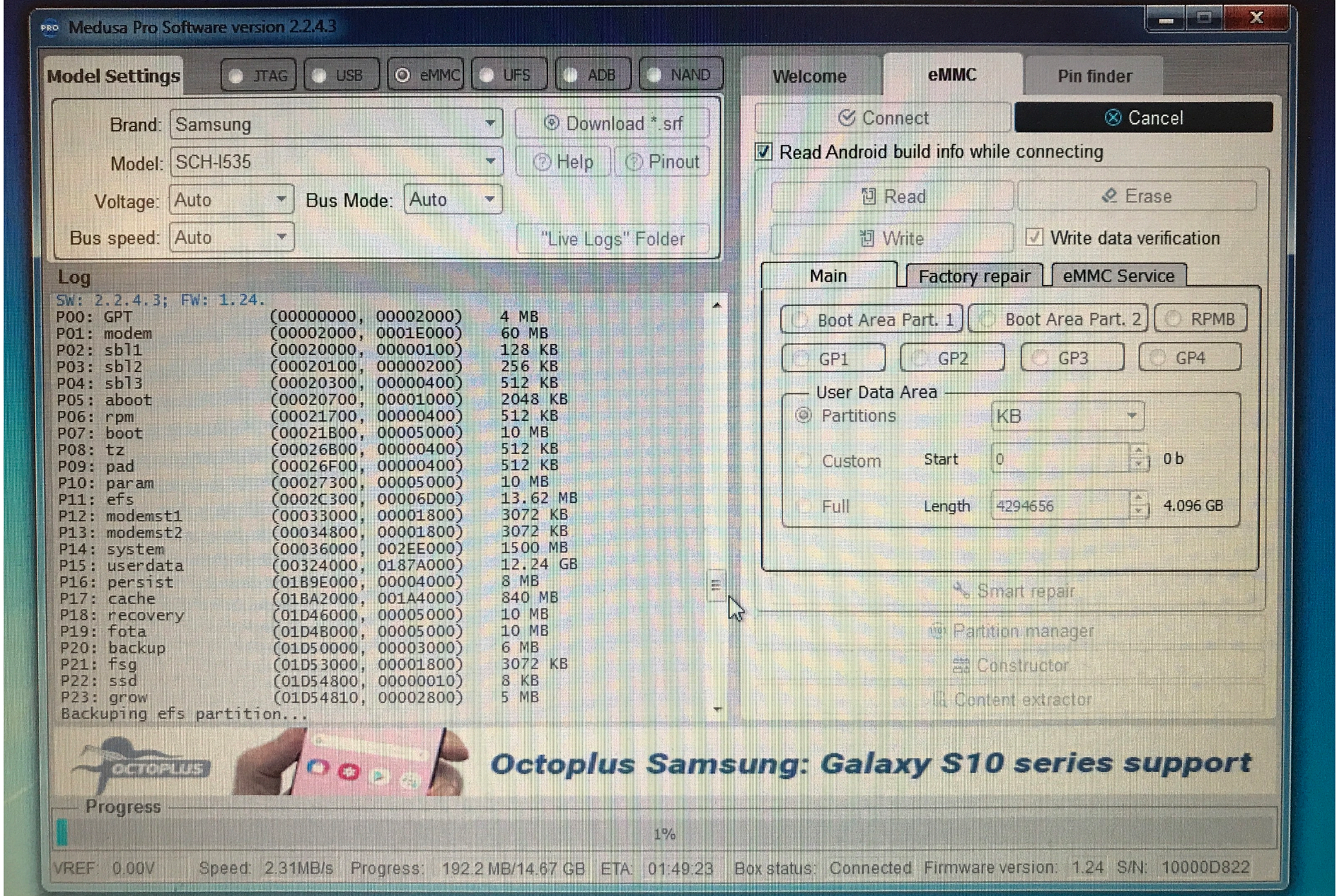

JTAGULATOR
STATUS
RESET
GRAND IDEA STUDIO
PARALLAX
www.JTAGulator.com
#32115 Rev. B
2013 cc by 3.0 US
ELIMINATE STATIC

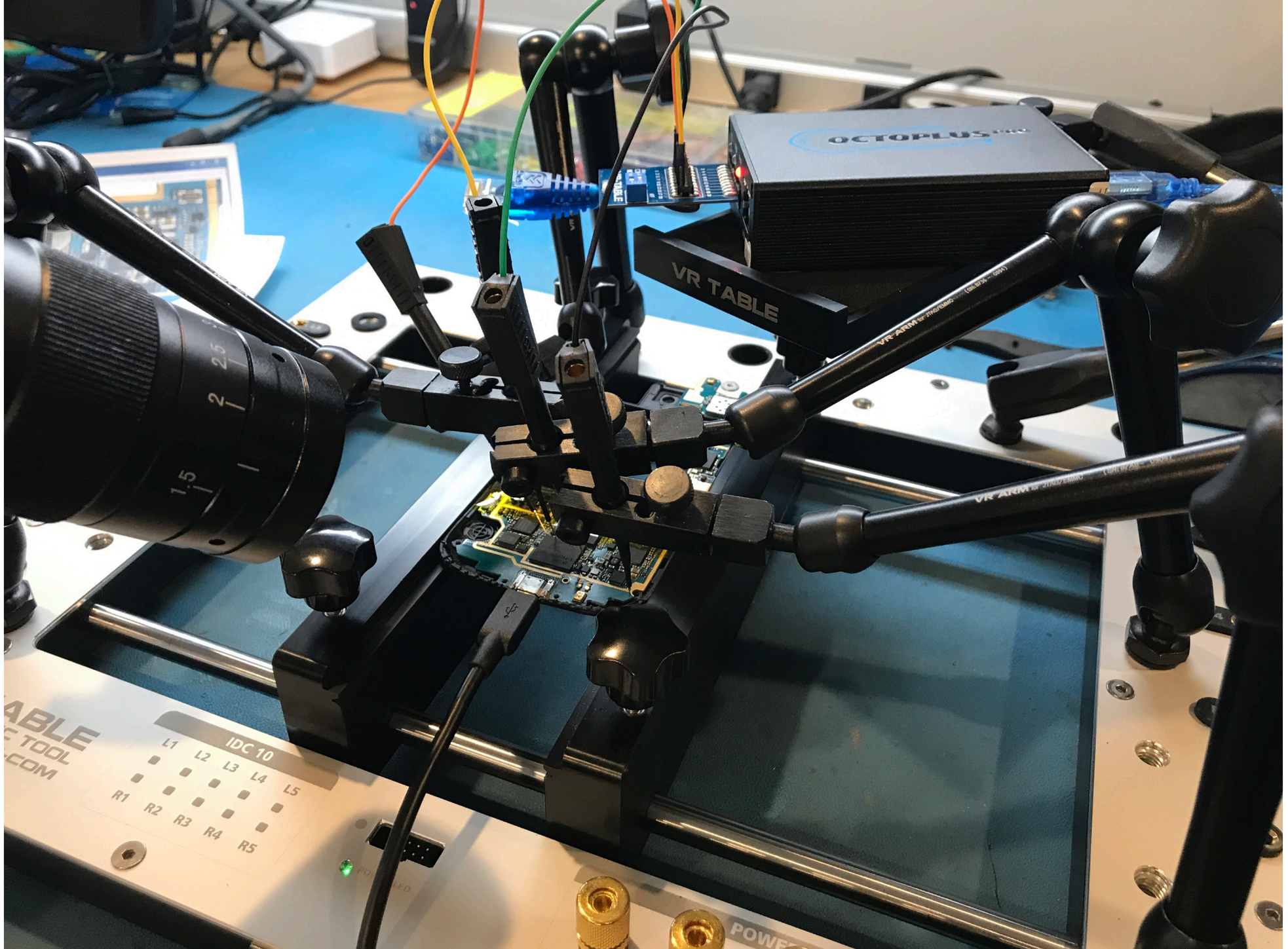

I/O
VREF
PWR
Bricked


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
Write
Erase
Boot only
Full flash
Custom
Units Kilobytes
Start 0 0 b
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...
OCTOPUS 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


JTAG
QUALCOMM
PM8921
A030849
F1220004


Medusa Pro Software version 2.2.4.3
Model Settings
JTAG
USB
eMMC
UFS
ADB
NAND
Brand: Samsung
Download *.srf
Model: SCH-I535
Help
Pinout
Voltage: Auto
Bus Mode: Auto
Bus speed: Auto
"Live Logs" Folder
Log
SW: 2.2.4.3; FW: 1.24.
P00: GPT (00000000, 00002000) 4 MB
P01: modem (00002000, 0001E000) 60 MB
P02: sbl1 (00020000, 00000100) 128 KB
P03: sbl2 (00020100, 00000200) 256 KB
P04: sbl3 (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 (01D4B000, 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
Connect
Cancel
Read Android build info while connecting
Read
Erase
Write
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
KB
Custom
Start
0
0 b
Full
Length
4294656
4.096 GB
Smart repair
Partition manager
Constructor
Content extractor
OCTOPLUS
Octoplus Samsung: Galaxy S10 series support
Progress
1%
VREF 0.00V
Speed: 2.31MB/s
Progress: 192.2 MB/14.67 GB
ETA: 01:49:23
Box status: Connected
Firmware version: 1.24
S/N: 10000D822


OCTOPLUS
VR TABLE
VR ARM
IDC 10
L1 L2 L3 L4 L5
R1 R2 R3 R4 R5

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