REVERSE ENGINEERING A LEDGER NANO X HARDWARE IMPLANT

JOE GRAND AKA KINGPIN

TROPICON 2026, COZUMEL, MEXICO

FIRST CONTACT

I ordered a Nano X off of a shopping platform (Lazada) from a seller LedgerXXX in Thailand. The only reason I wanted it was to cannibalize the battery out of it to put it into my nano x as the battery holds no charge. The price was too good to be true, so I knew immediately it would be fake. I have posted to Ledger on X, and I will be contacting law enforcement here about this.

Here are some photos of the device.

They sent me the wrong colour and graciously allowed me to keep it when I asked for it to be exchanged for another colour.

Just beware these things are out there in the wild.

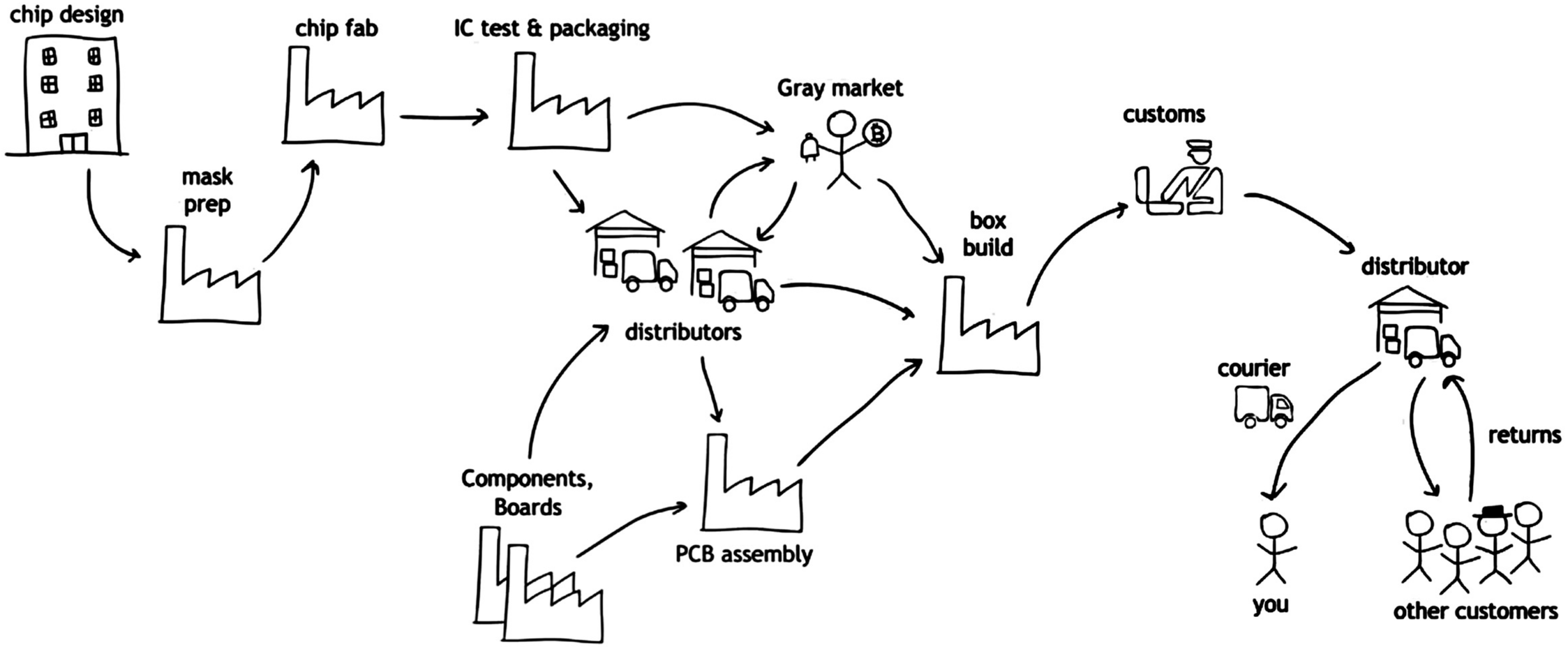
Reddit: "Nano X" being sold to steal your crypto, August 2025


Battery too low
Shutting down

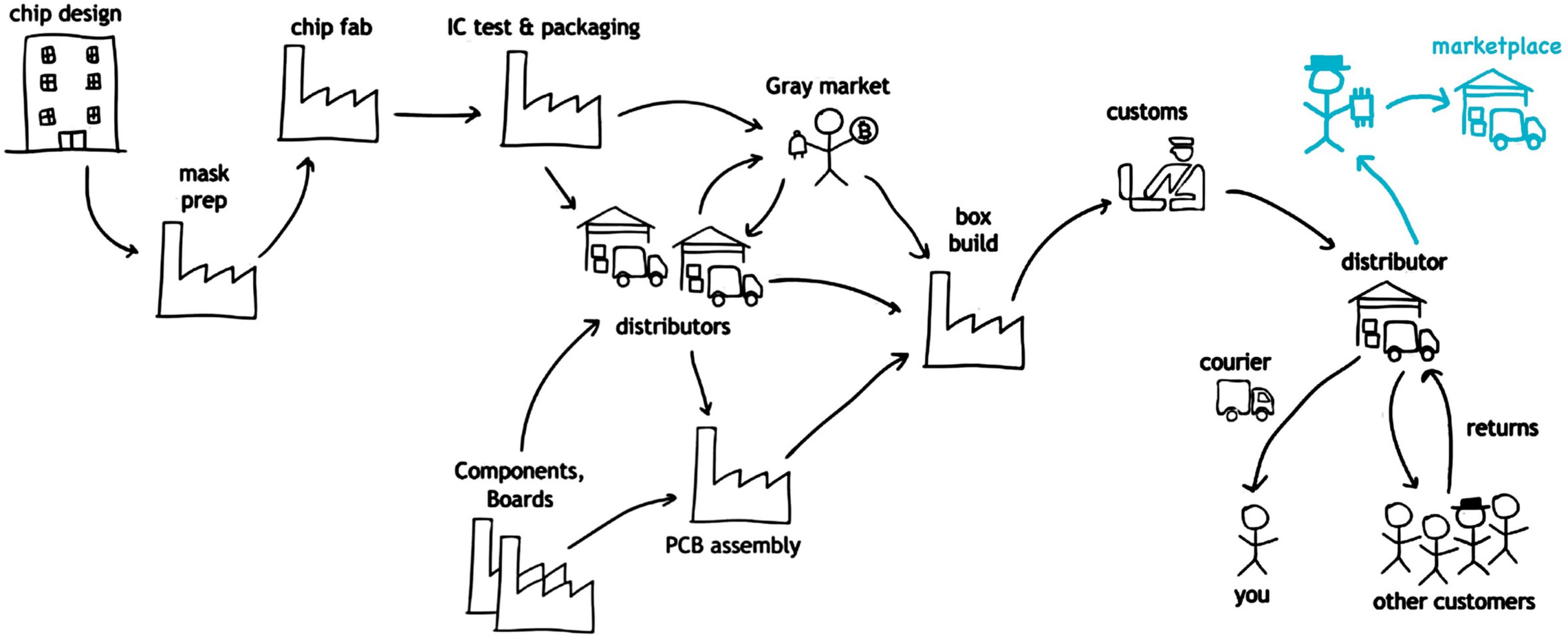
HARDWARE ESPIONAGE

HARDWARE ESPIONAGE

- Not all devices follow the rules
  - Operate in ways unintended by the original designer
  - Can provide unexpected / alternate behavior
- Can exist within any layer of the product
  - HW, FW, or SW modification
  - Supply chain attacks
  - Malicious / corrupt / deceived insiders
- Could be implemented at any part of the lifecycle
  - Each step is an opportunity for compromise



Supply Chain Security: If I were a Nation State, Huang, BlueHat IL 2019

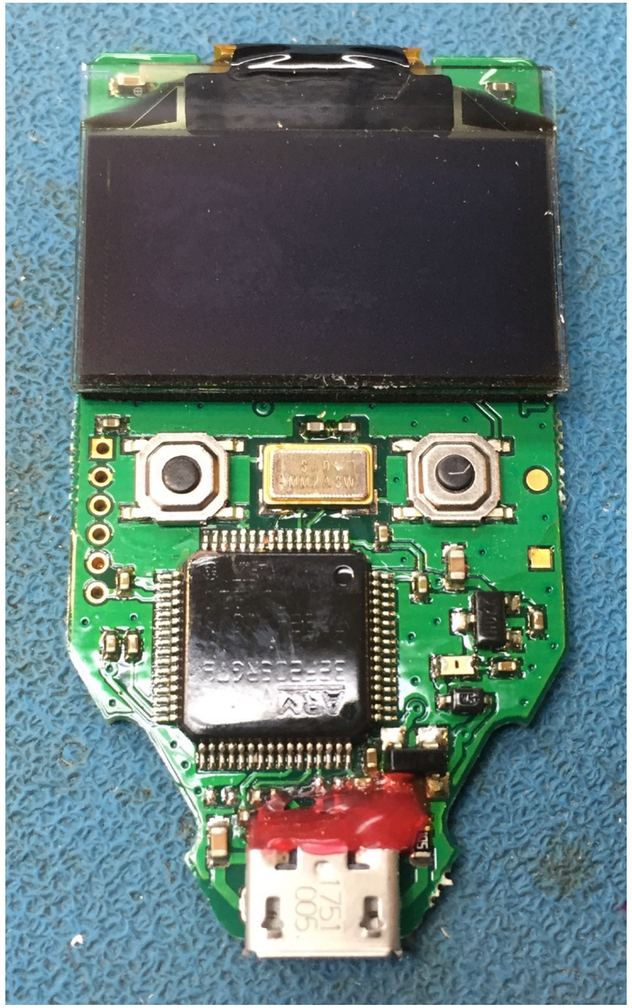


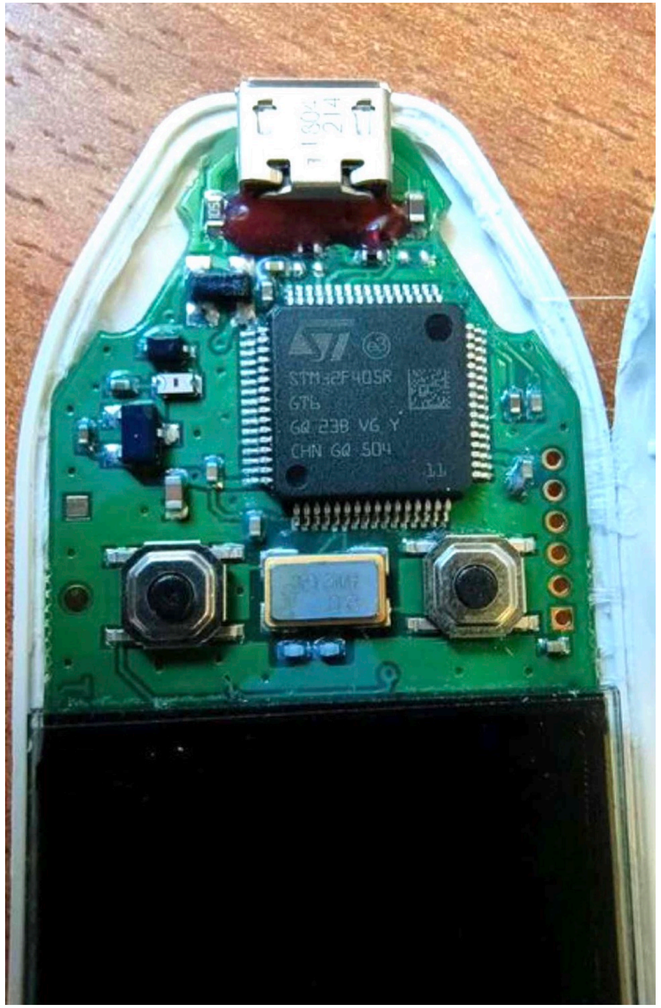
Supply Chain Security: If I were a Nation State, Huang, BlueHat IL 2019

TREZOR ONE + MODEL T

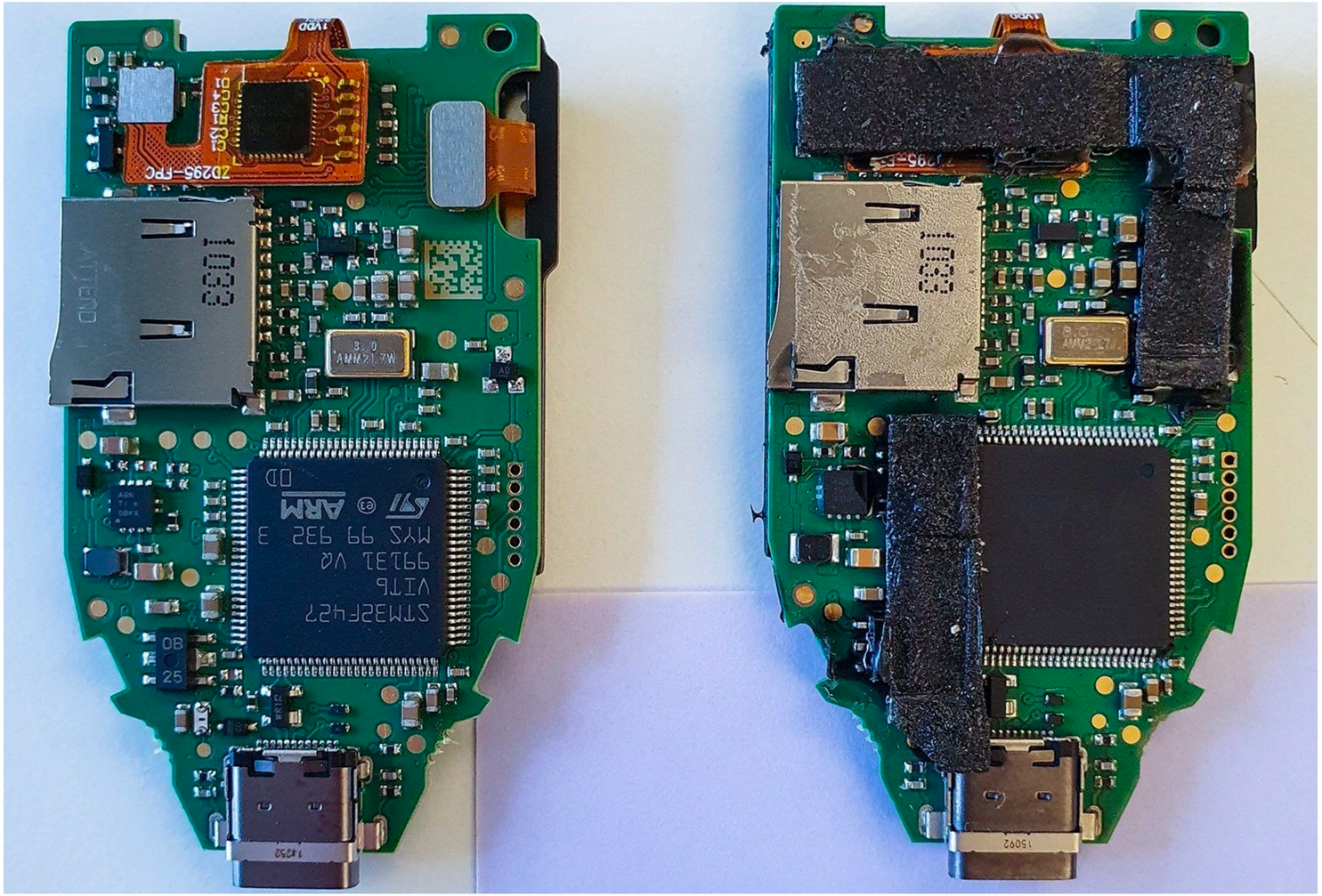
- Legitimate devices, original locked STM32 MCU replaced w/ unlocked version running malicious code
- Compromised recovery seed generation
  - Fixed number of pre-generated seed phrases instead of randomly generated
- Sold on Russian marketplace
- www.kaspersky.com/blog/fake-trezor-hardware-crypto-wallet/48155/
- blog.trezor.io/stay-safe-shopping-for-hardware-wallets-543f144e3d24

TREZOR ONE

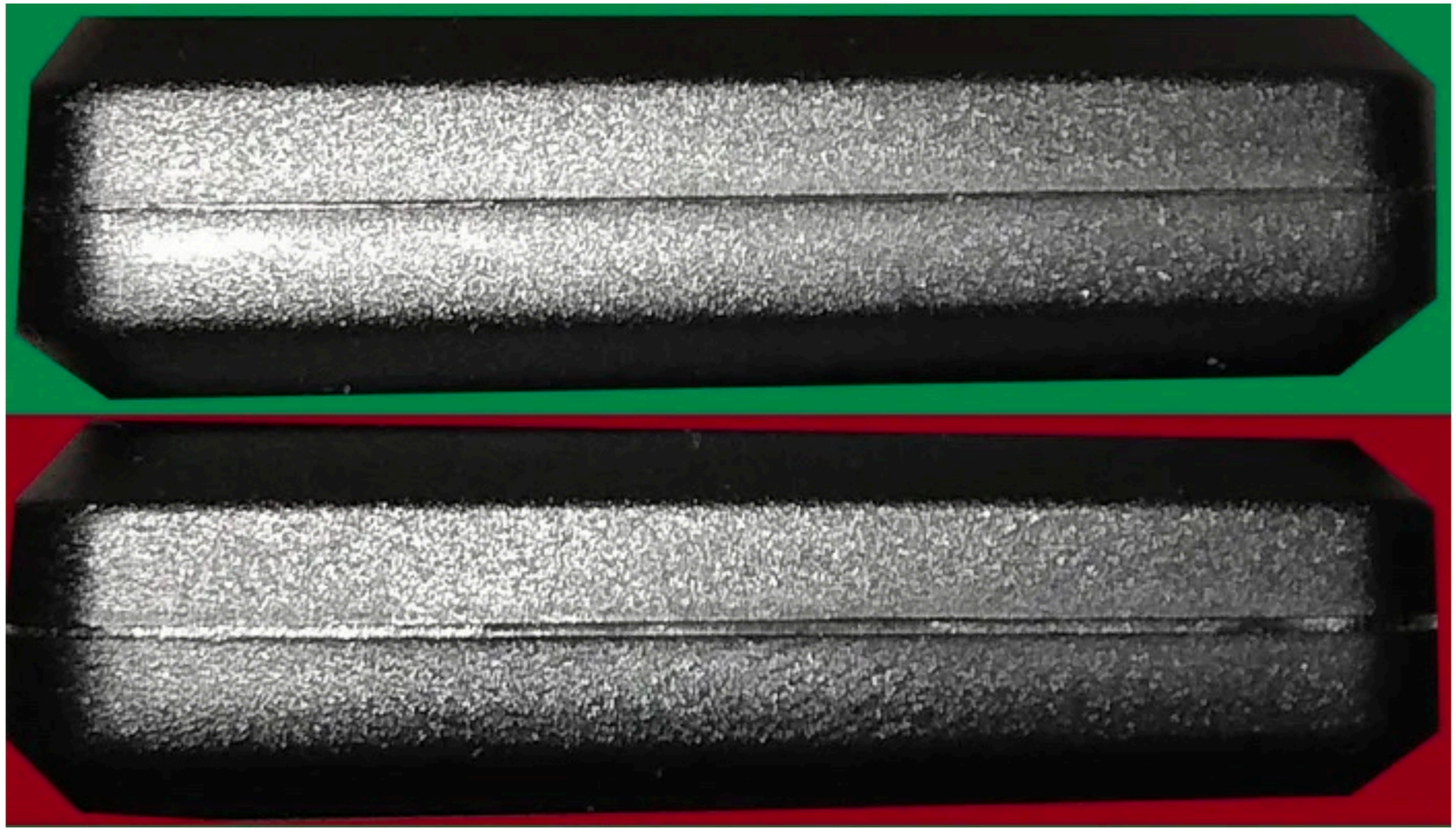




TREZOR MODEL T

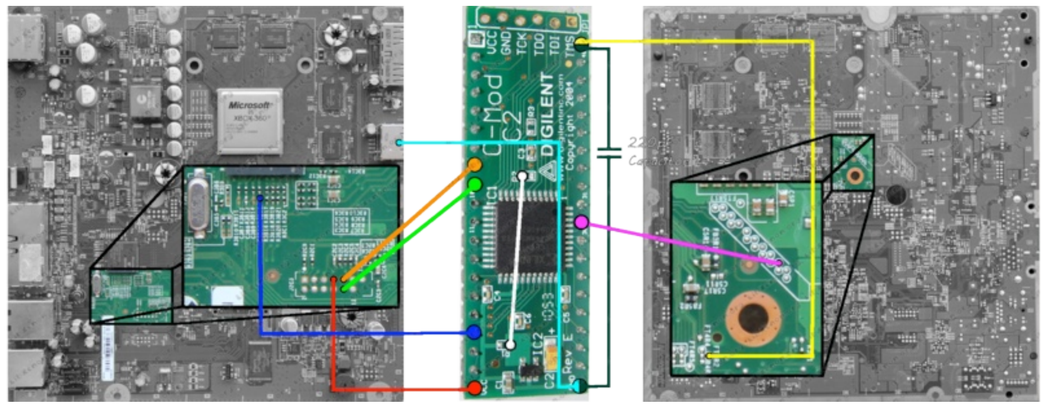


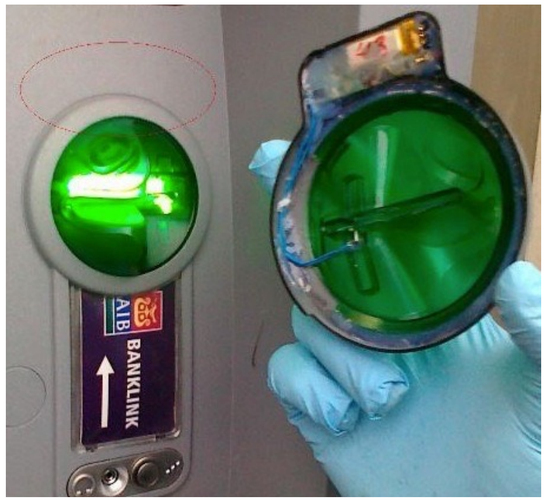
TREZOR MODEL T

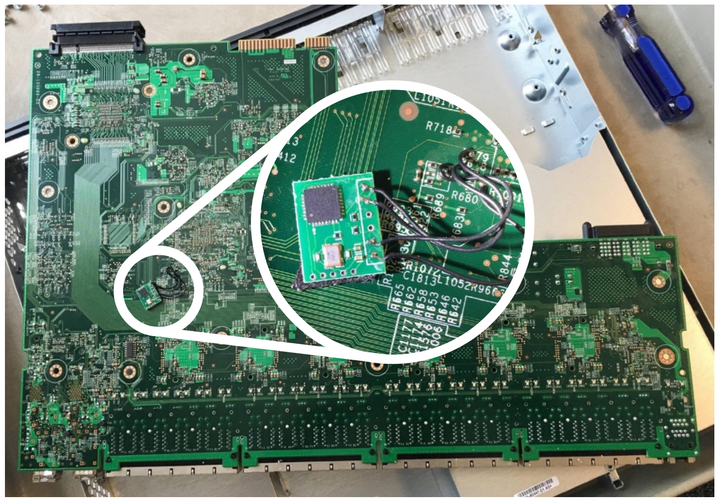


HARDWARE IMPLANTS

- Add circuitry in tandem w/ normally functioning system
  - Injection point depends on product / attack goal
- Connects to internal communication buses, control signals, user-facing interfaces
  - Capture, replay, spoof, MITM
- Can create backdoor / remote access, dump / exfiltrate data, manipulate memory



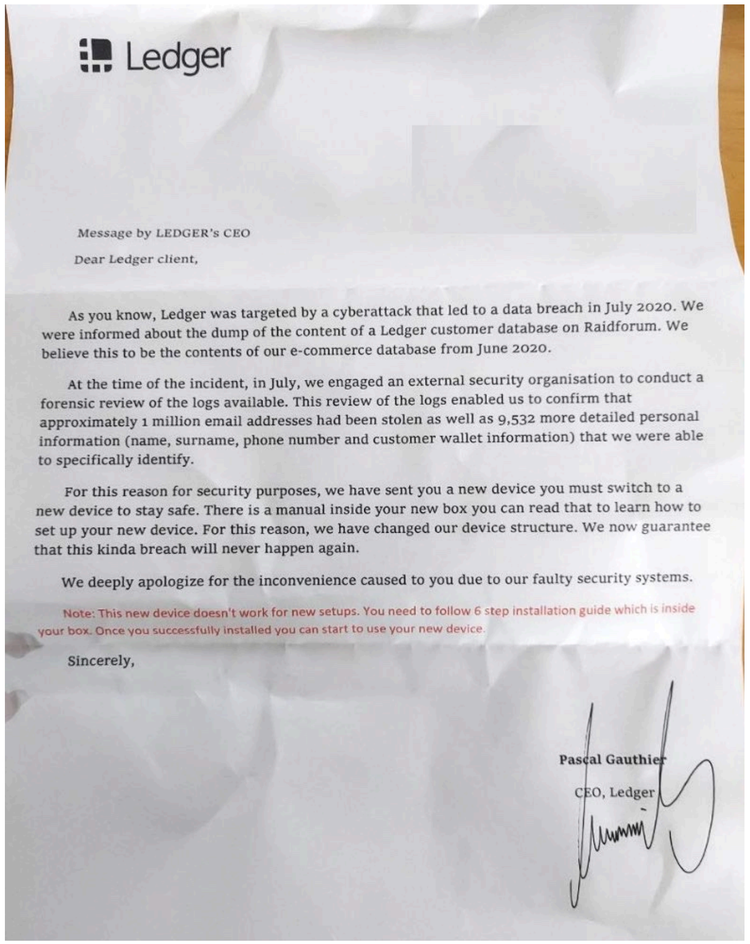




LEDGER NANO X

- Tampered devices sent to customers leaked via June 2020 database breach
- Legitimate Ledger w/ implanted USB thumbdrive soldered to test points
- Phishing attempt by stealing user's cryptocurrency recovery seed via malware
- www.reddit.com/r/ledgerwallet/comments/o154gz/package_from_ledger_is_this_legit/
- www.bleepingcomputer.com/news/cryptocurrency/criminals-are-mailing-altered-ledger-devices-to-steal-cryptocurrency/

LEDGER NANO X



Ledger

Message by LEDGER's CEO

Dear Ledger client,

As you know, Ledger was targeted by a cyberattack that led to a data breach in July 2020. We were informed about the dump of the content of a Ledger customer database on Raidforum. We believe this to be the contents of our e-commerce database from June 2020.

At the time of the incident, in July, we engaged an external security organisation to conduct a forensic review of the logs available. This review of the logs enabled us to confirm that approximately 1 million email addresses had been stolen as well as 9,532 more detailed personal information (name, surname, phone number and customer wallet information) that we were able to specifically identify.

For this reason for security purposes, we have sent you a new device you must switch to a new device to stay safe. There is a manual inside your new box you can read that to learn how to set up your new device. For this reason, we have changed our device structure. We now guarantee that this kinda breach will never happen again.

We deeply apologize for the inconvenience caused to you due to our faulty security systems.

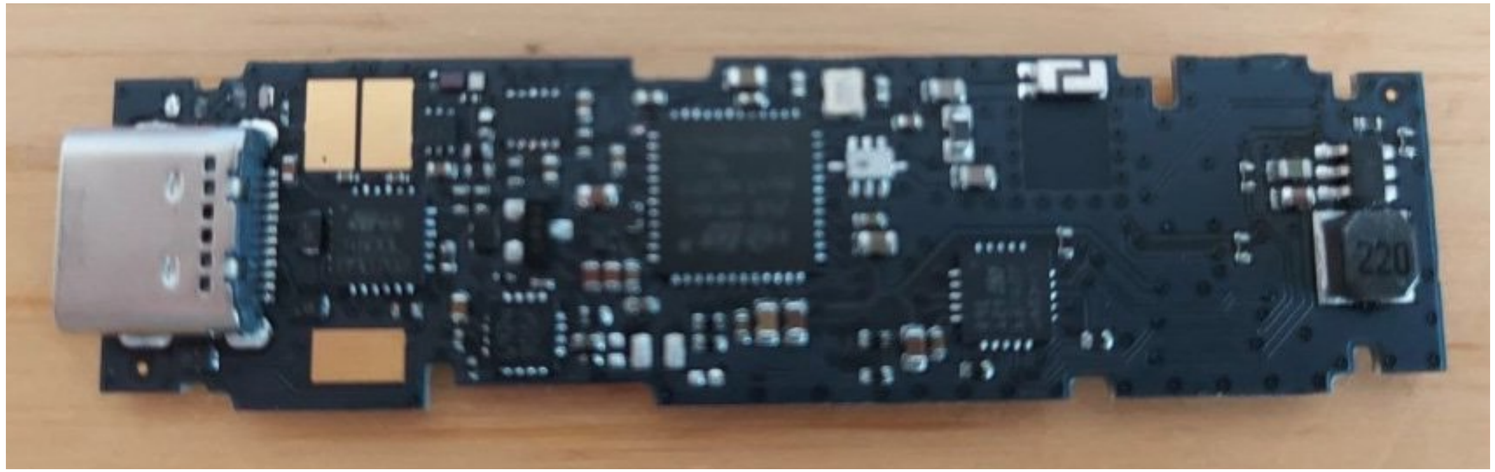
Note: This new device doesn't work for new setups. You need to follow 6 step installation guide which is inside your box. Once you successfully installed you can start to use your new device.

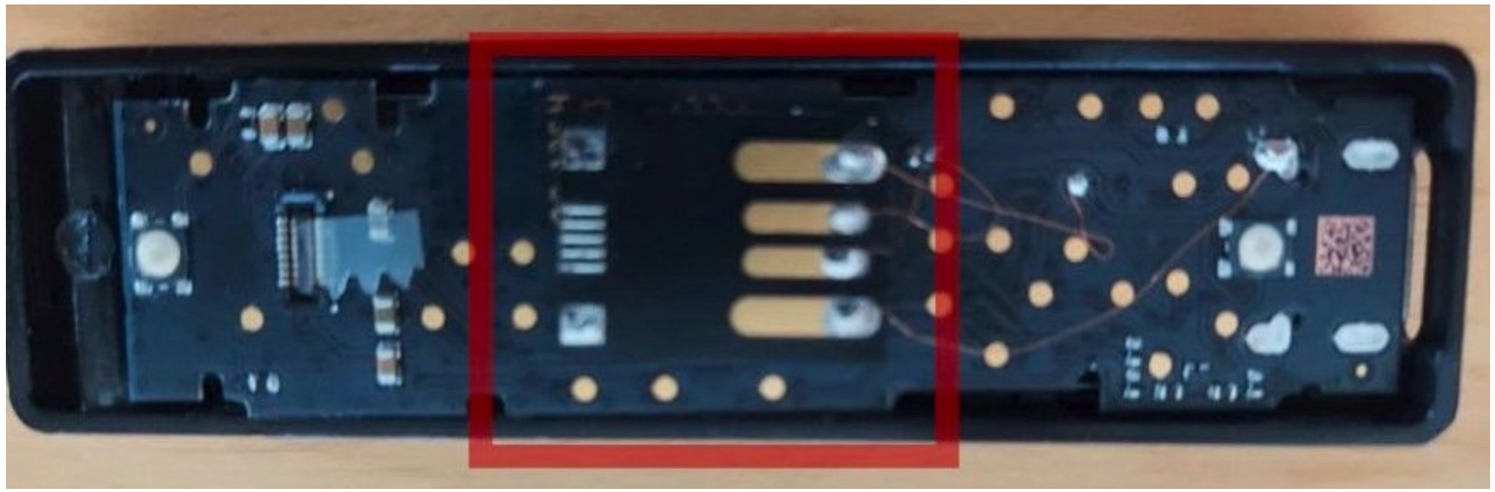
Sincerely,

Pascal Gauthier

CEO, Ledger

LEDGER NANO X





ACQUISITION

Ledger Thailand Official Onlin

https://www.lazada.co.th/shop/ledger

New Chrome available

SUGGESTIONS | SHOP SMARTER THAN EVER ON THE APP. | SELLING PRODUCTS ON LAZADA. | HELP | TRACK ORDER | LOG IN | REGISTER | CHANGE LANGUAGE

Lazada

Search on Lazada.

ลูกค้าใหม่ซื้อของชิ้นแรกฟรี*

Category | LazMall

Ledger

LazMall ร้านค้าที่ได้รับอนุญาต | 138 Followers

99% positive store ratings.

Chat Now | FOLLOW

Authorized Reseller

Shop Homepage | All products | profile

Search In Store

Throughout the entire store.
5% off
Minimum purchase ฿1.5K
03/04 09:43 ~ 30/04 23:59
Get a coupon

Throughout the entire store.
7% off
Minimum purchase ฿2.5K
15/04 00:00 ~ 17/04 23:59
Get a coupon

Throughout the entire store.
7% off
Minimum purchase ฿2.5K
03/04 09:43 ~ 30/04 09:43
Get a coupon

For participating products.
฿2,080.00
Minimum purchase ฿6,280
24/03 10:00 ~ 31/08 23:59
Get a coupon

Browse by Mobile

message

SUGGESTIONS | SHOP FOR BETTER VALUE ON THE APP | SELL PRODUCTS WITH LAZADA | HELP | TRACK YOUR PRODUCT | SIGN IN | APPLY FOR MEMBERSHIP

Lazada | Search on Lazada | CHANGE LANGUAGE

Popmart | iPhone | mobile phone | Women's shoes | Bluetooth headphones

Category | LazMall

Electronic spare parts and acc... > Network equipment > USB Wireless Connection Devi... > Good news! Official Ledger Nano X distributor! Brand new, authentic, and fully packaged. The

Good news! Official Ledger Nano X distributor! Brand new, authentic, and fully packaged. The Bitcoin wallet connects to your phone via Bluetooth. If you'd like to purchase, please order directly. Thank you!

Brand : Ledger | More network devices from Ledger

฿4,699.00

promotion : ฿200

Shipping options : Pathum Wan/ Pathum Wan in Bangkok/ Bangkok, 10110 change

Will be received between 27-29 Sep.

Standard type, with shipping fee ฿35.00

Returns and Warranty : Change your mind · Free returns within 7 days · 1-year international manufacturer's w...

color : pink

black | gold | pink

quantity : 1 — The product is almost out of stock. Hurry and buy it now!

Buy now | Add to Cart | Share | Like

TH-ledger nano x

Chat | Go to the store

review | Product details

review

Oops

This product has no reviews yet.
Please leave a review for others to know.

Product details

Good news, Ledger Nano

Good news! Official Ledger Nano X distributor! Brand new, authentic, and fully packaged. The Bitcoin wallet connects to your phone via Bluetooth. If you'd like to purchase, please order directly. Thank you!

฿4,699.00

SUGGESTIONS | SHOP FOR BETTER VALUE ON THE APP | SELL PRODUCTS WITH LAZADA | HELP | TRACK YOUR PRODUCT | SIGN IN | APPLY FOR MEMBERSHIP

Lazada | Search on Lazada | CHANGE LANGUAGE

Popmart | iPhone | mobile phone | Women's shoes | Bluetooth headphones

Category | LazMall

Bags and luggage > Men's bags > Backpack > Ledger Nano X – Your gateway to the Web3 world. Protect your assets in style.

Ledger Nano X – Your gateway to the Web3 world. Protect your assets in style.

Brand : No Brand | Men's bags, more from No Brand

฿4,874.00

promotion : ฿500

Shipping options : Pathum Wan/ Pathum Wan in Bangkok/ Bangkok, 10110 change

Will be received between 27-29 Sep.

Standard type, with free shipping fee

Returns and Warranty : Change your mind · Free returns within 7 days · 1-year international manufacturer's w...

color : black

black | gold | pink | purple

quantity : 1

Buy now | Add to Cart | Share | Like

THLedger nano x

Store rating100% | Recommended shops

Chat | Go to the store

SUGGESTIONS | SHOP FOR BETTER VALUE ON THE APP | SELL PRODUCTS WITH LAZADA | HELP | TRACK YOUR PRODUCT | SIGN IN | APPLY FOR MEMBERSHIP

Lazada | Search on Lazada | CHANGE LANGUAGE

Popmart | iPhone | mobile phone | Women's shoes | Bluetooth headphones

Category | LazMall

Bags and luggage > Men's bags > Business card holder > Ledger Nano X Bluetooth Hardware Wallet | Manage Multi-Blockchain Crypto & NFTs | 100% Brand New & Authentic

Ledger Nano X Bluetooth Hardware Wallet | Manage Multi-Blockchain Crypto & NFTs | 100% Brand New & Authentic

Brand : No Brand | Men's bags, more from No Brand

฿4,664.00

promotion : 23% off

Shipping options : Pathum Wan/ Pathum Wan in Bangkok/ Bangkok, 10110 change

Will be received between 27-29 Sep.

Standard type, with shipping fee ฿35.00

Returns and Warranty : Change your mind · Free returns within 7 days · 1-year international manufacturer's w...

color : gold

black | gold | pink | purple

quantity : 1

Buy now | Add to Cart | Share | Like

TH-Ledger

Store rating:83%

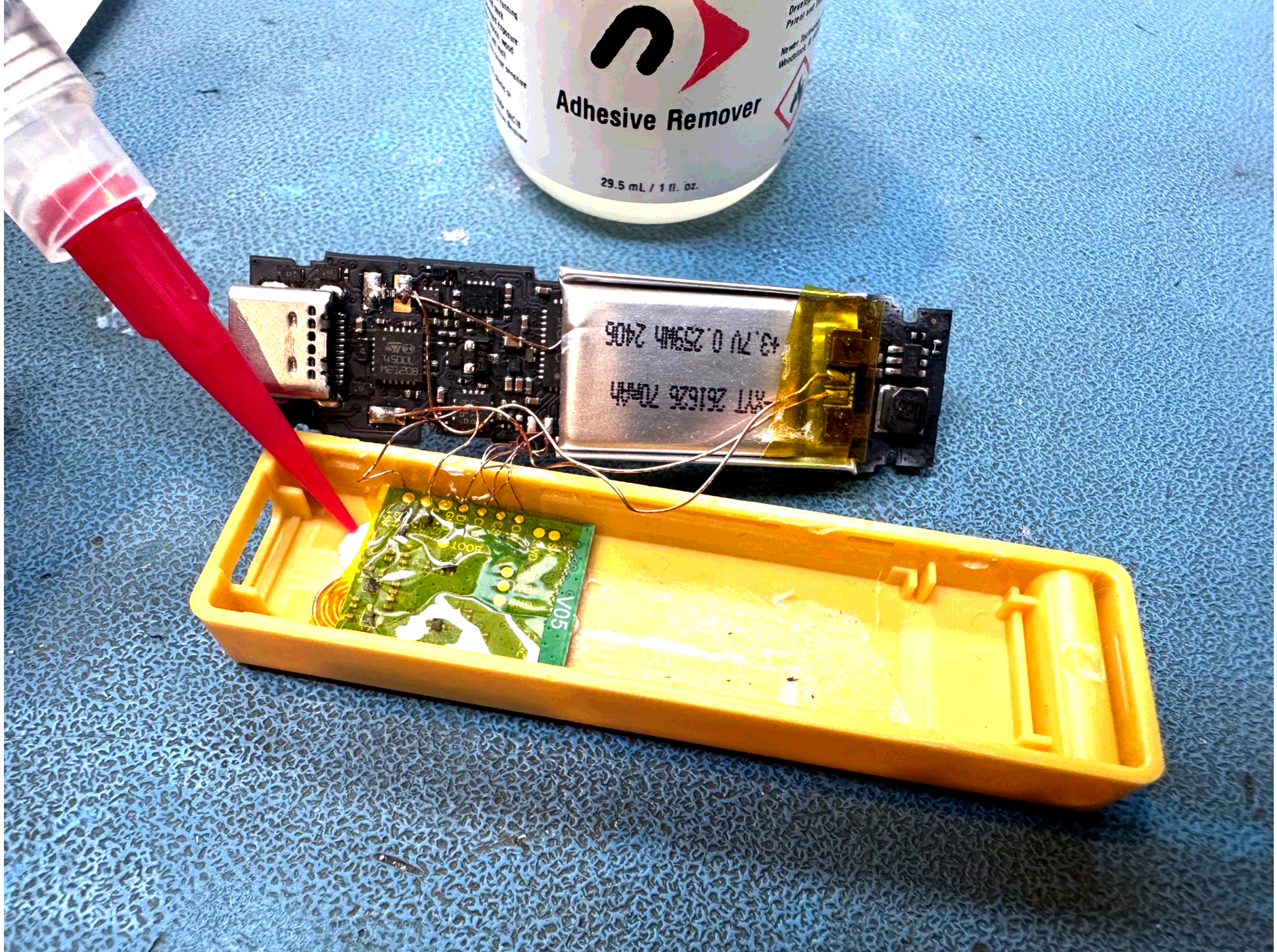
Chat | Go to the store

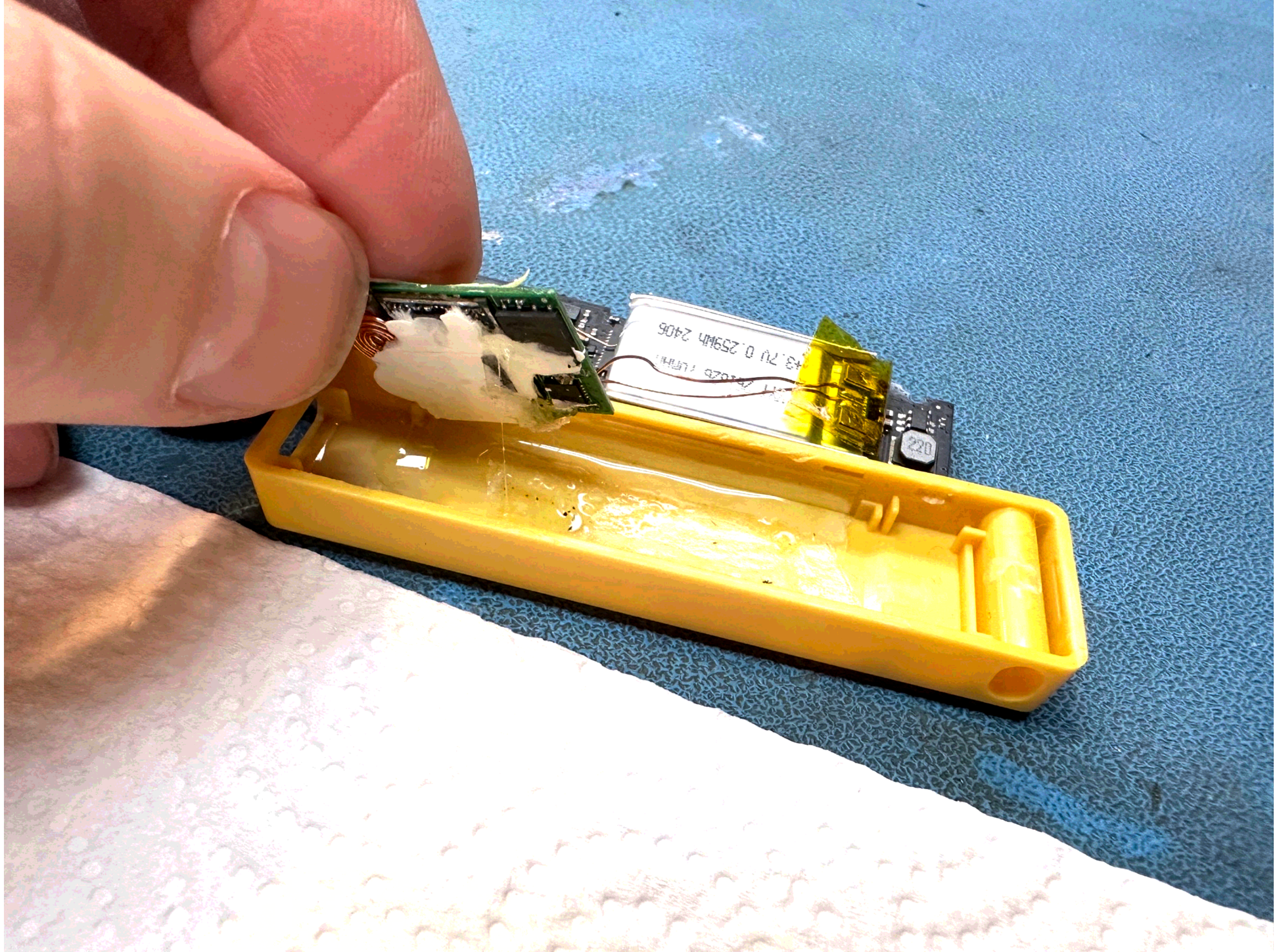

LEDGER-NANO-X
Bitcoin
KEEP YOUR CRYPTO AND NFTS SECURE
LEDGER NANO X
The most secure crypto wallet
LEDGER NANO X
The most secure crypto wallet

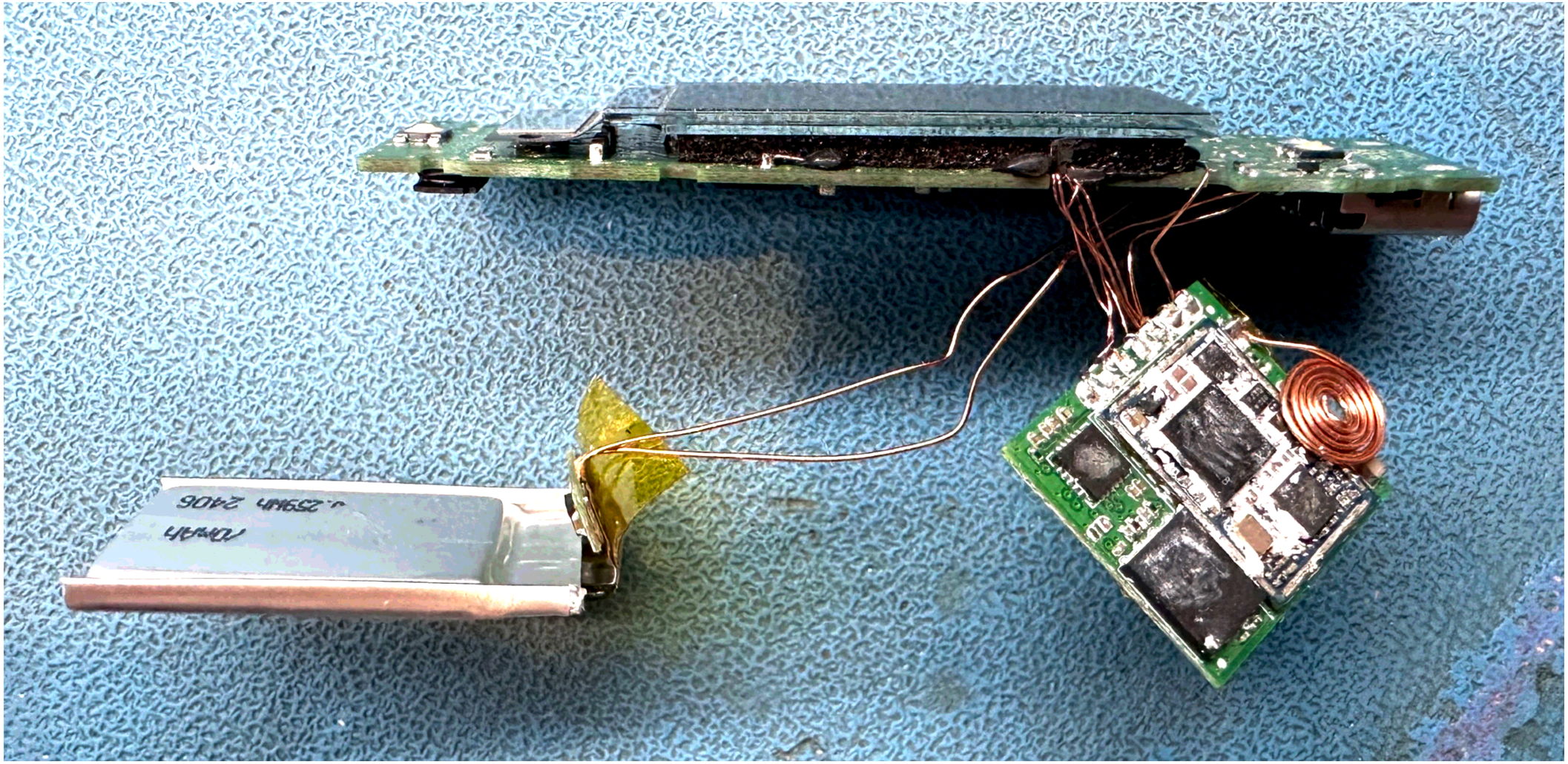
TEARDOWN

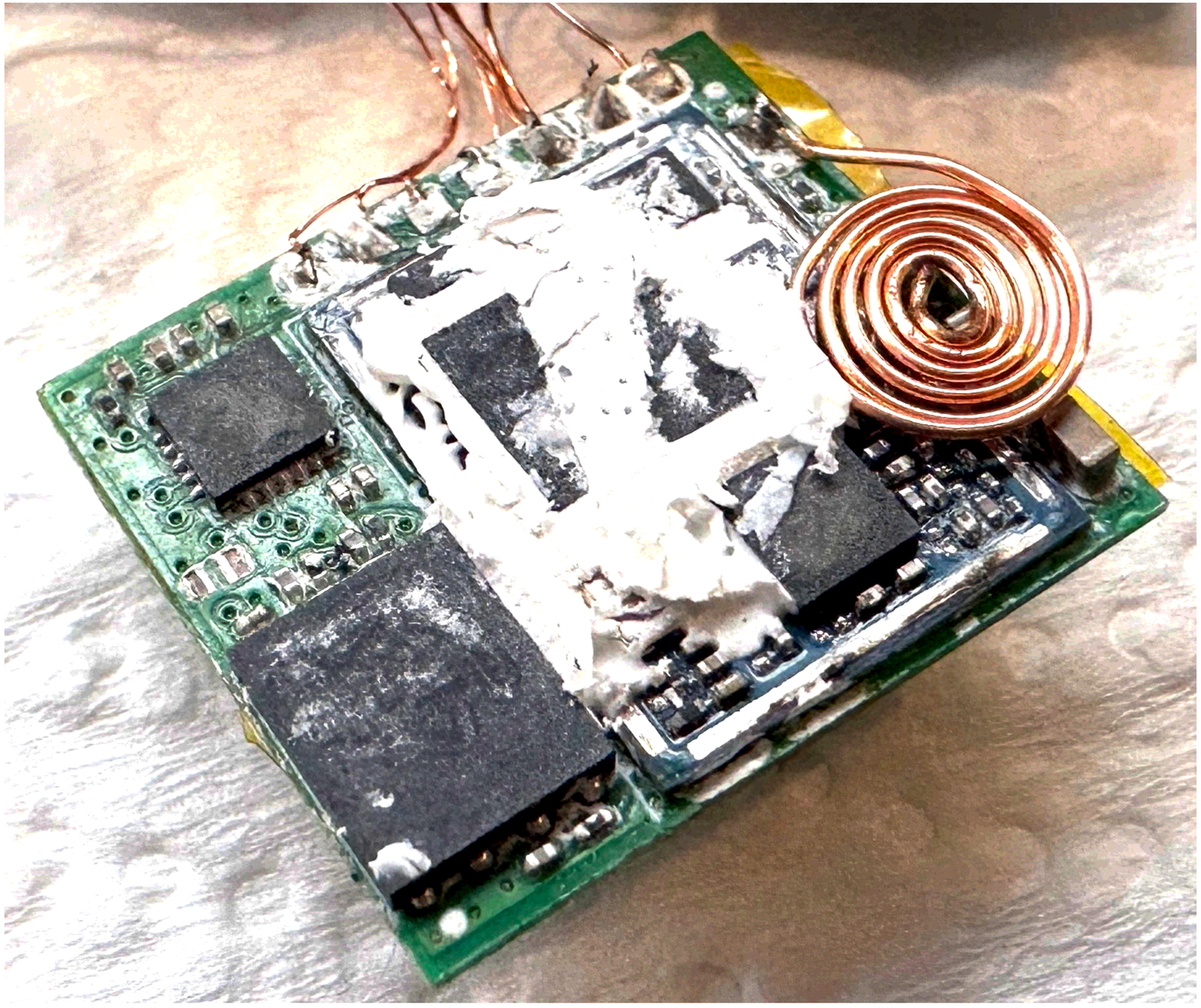

TECHSPRAY
ISOPROPYL ALCOHOL
LEDGER NANO X
LEDGER NANO X
LEDGER-NANO-X
Bitcoin
KEEP YOUR CRYPTO AND NFTS SECURE
IFIXIT

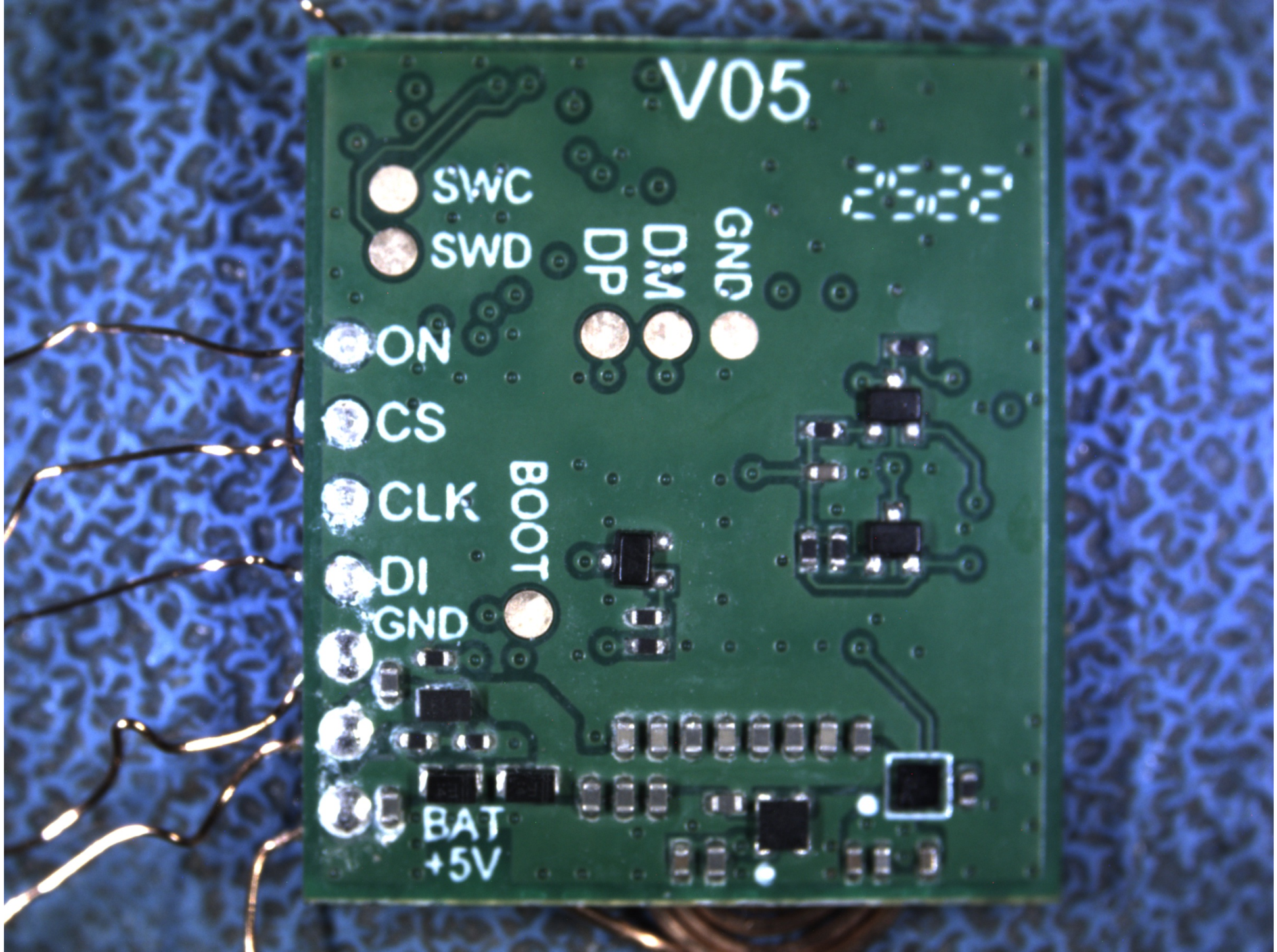

V05
261626 70mAh
3.7V 0.259Wh 2406
220


Adhesive Remover
29.5 mL / 1 fl. oz.
V05

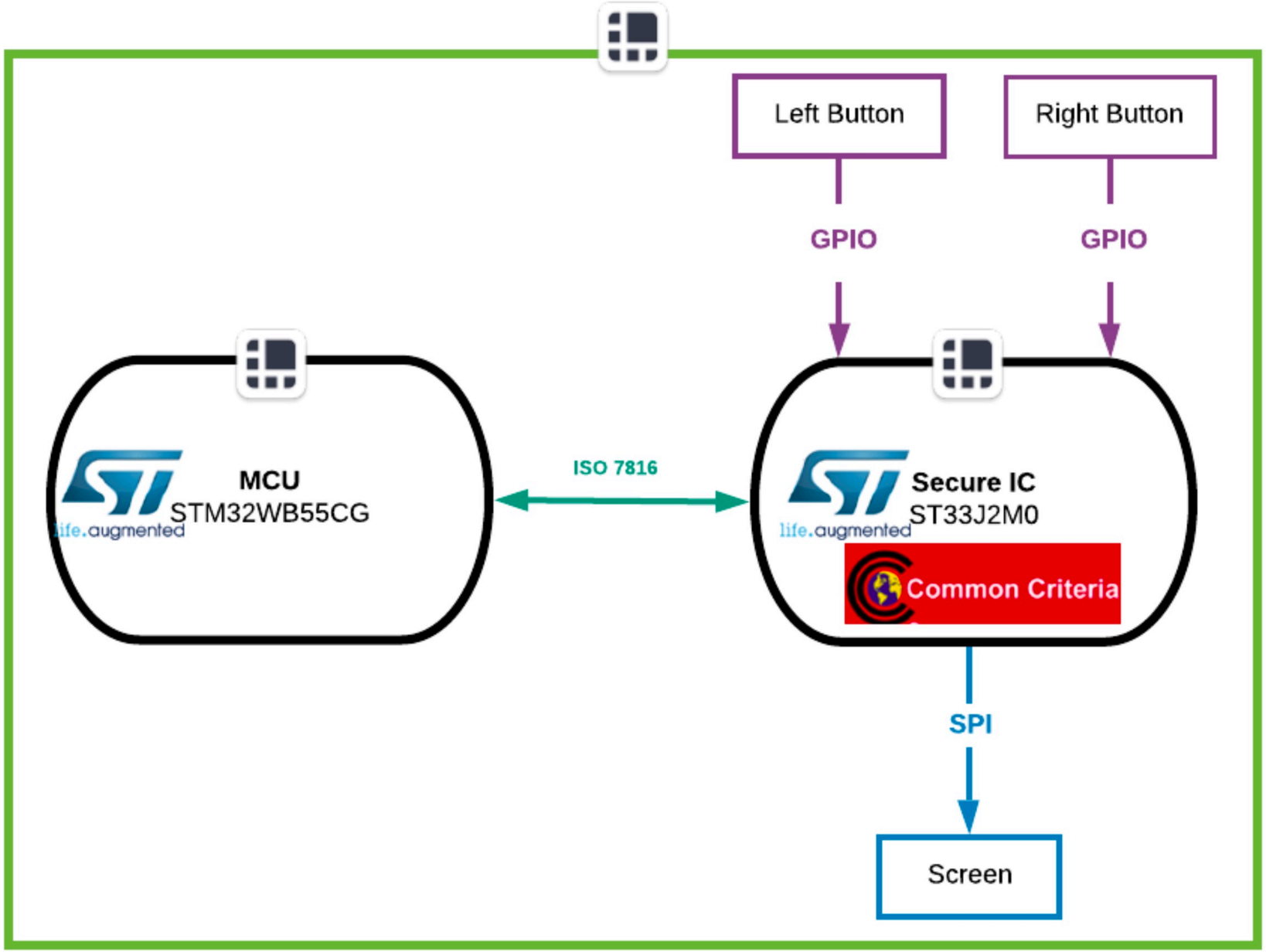

3.7V 0.259Wh 240
220



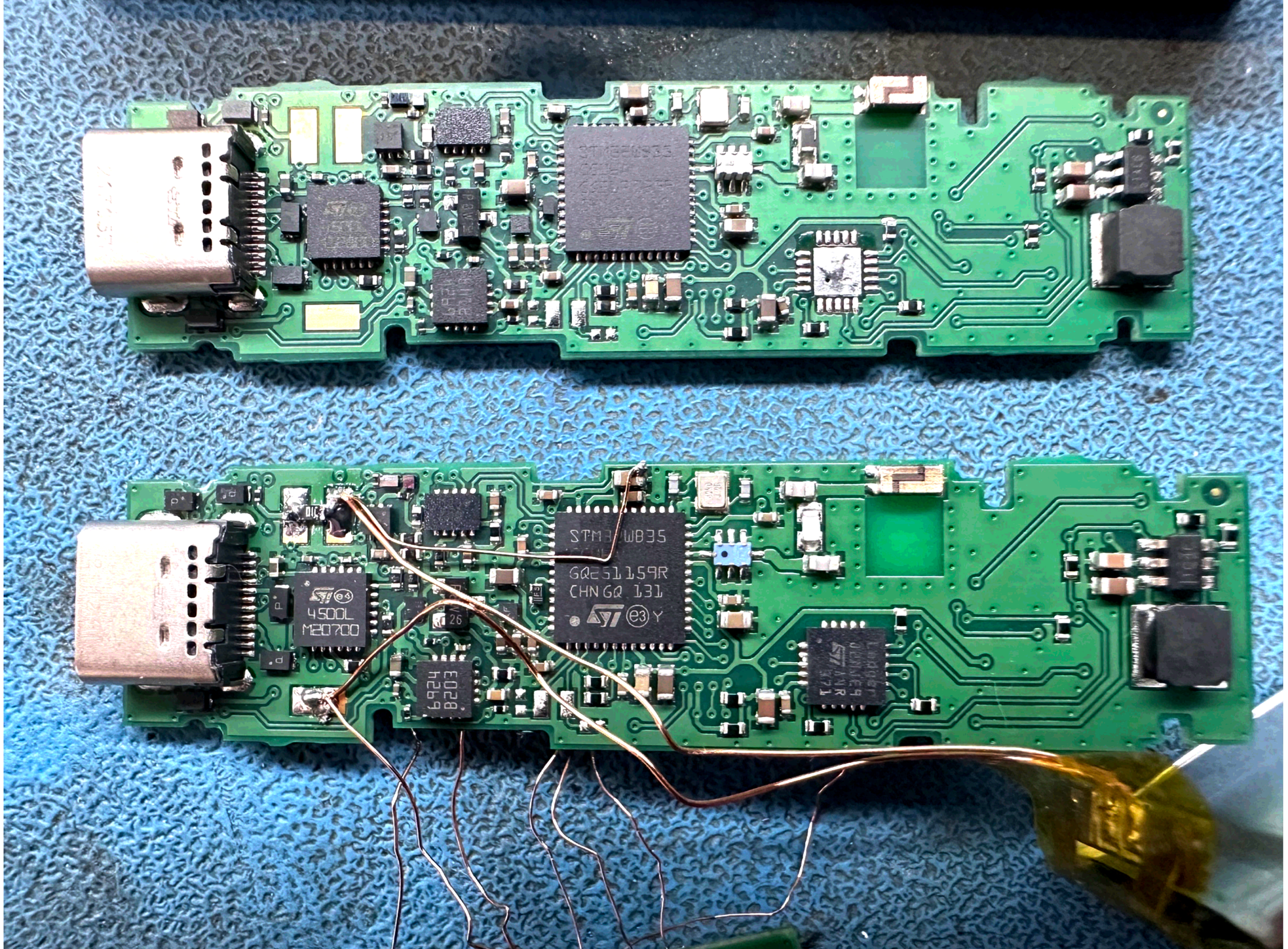



V05
2022
SWC
SWD
DP
DM
GND
ON
CS
CLK
DI
GND
BOOT
BAT
+5V

HW REVERSE ENGINEERING

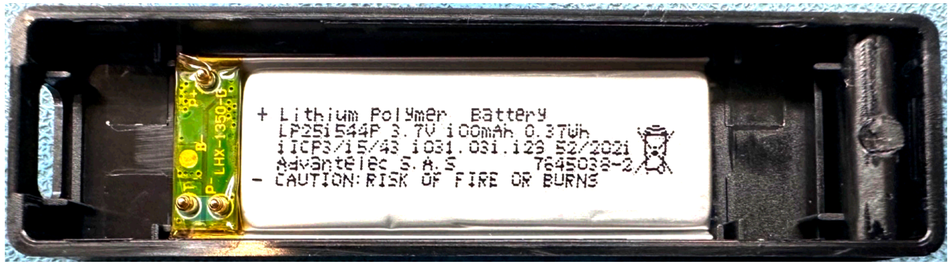


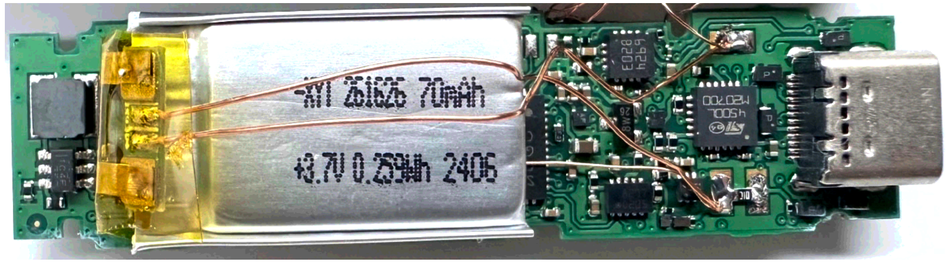
Ledger Nano X Security Target v1.2

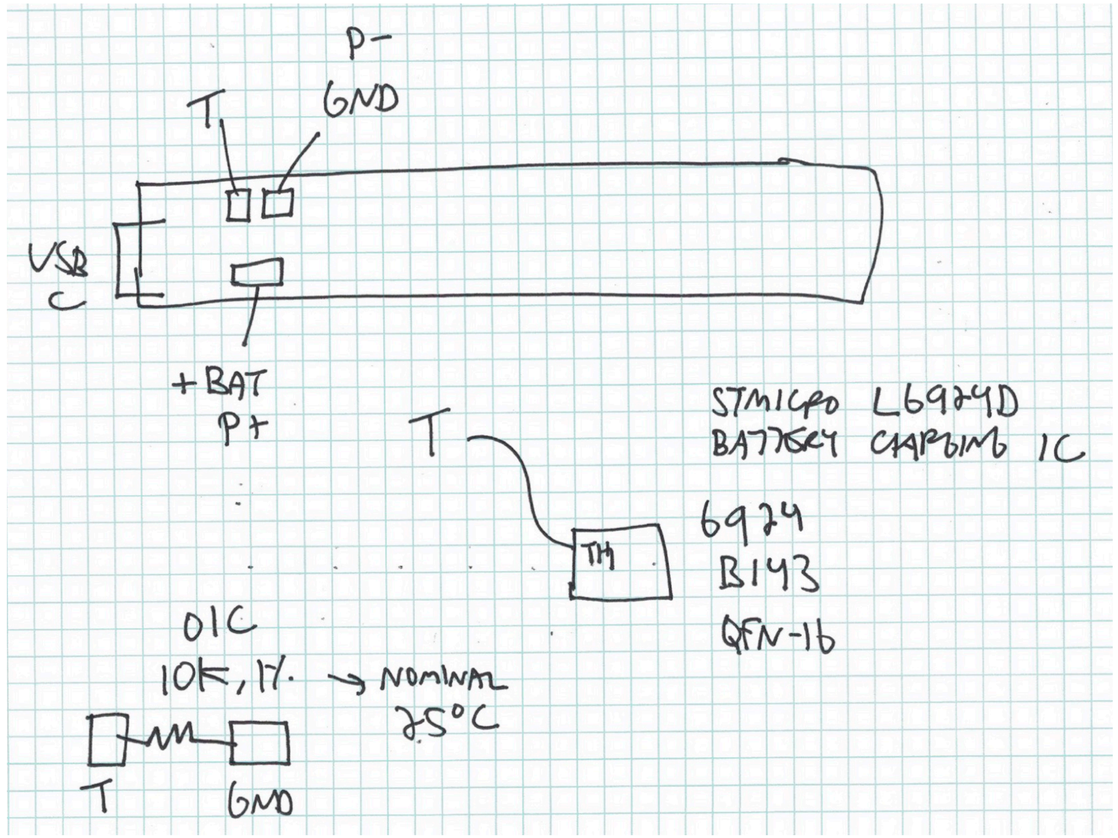

4500L
M20700
E028
h26h
GQ251159R
CHN GQ 131
Y

FRONT-SIDE MODIFICATIONS

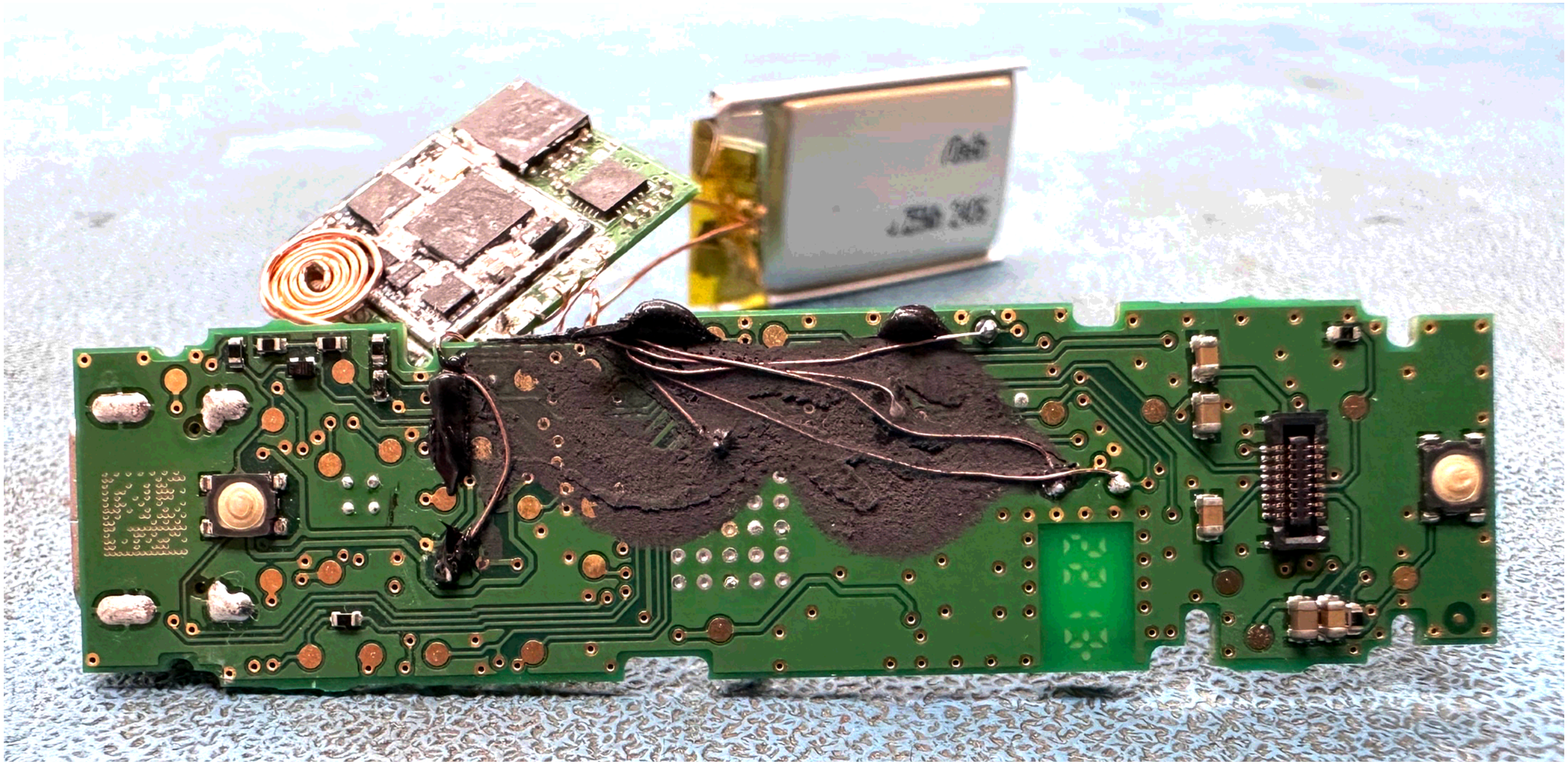
- Battery has reduced size in order to fit implant
- Fixed 10k resistor replaces NTC thermistor from original battery
- Fuel gauge resistor bypassed to always appear 100% full





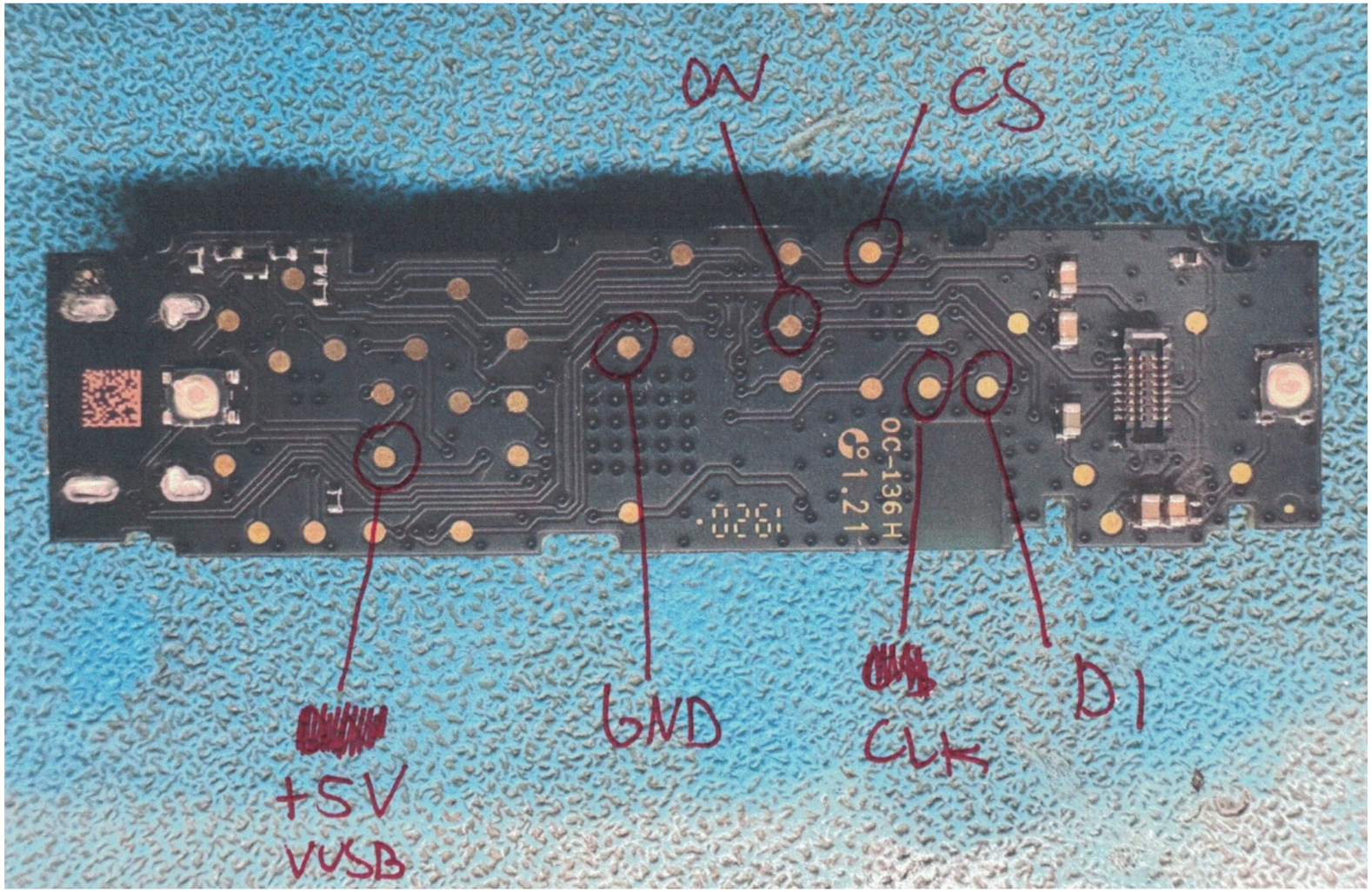


BACK-SIDE MODIFICATIONS




10pF / 22pF / 220pF
15pF / 20pF / 100pF
Misc pF
Misc uF
Plastic / Rubber / Glass
Heatsinks
LED: Red / Orange
LED: Green / Yellow
LED: White
Jumper Wires
MANTIS
PIXO
Vision
ENGINEERING
ISOPROPYL ALC
0.0002 VDC

IMPLANT MCU → OLED SPI INTERFACE



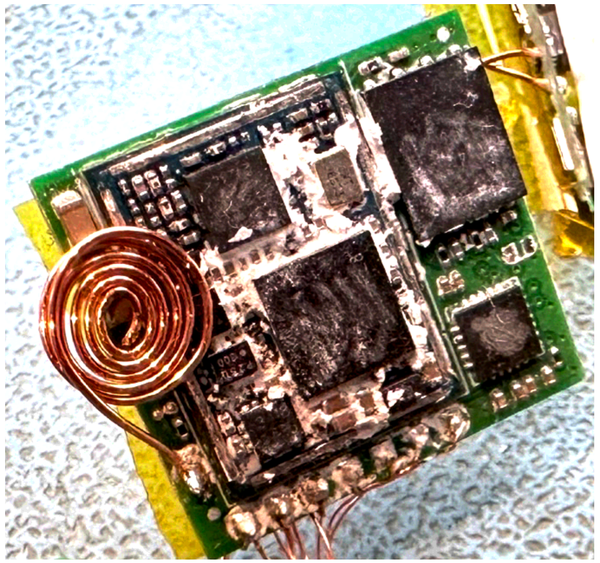
WHY?

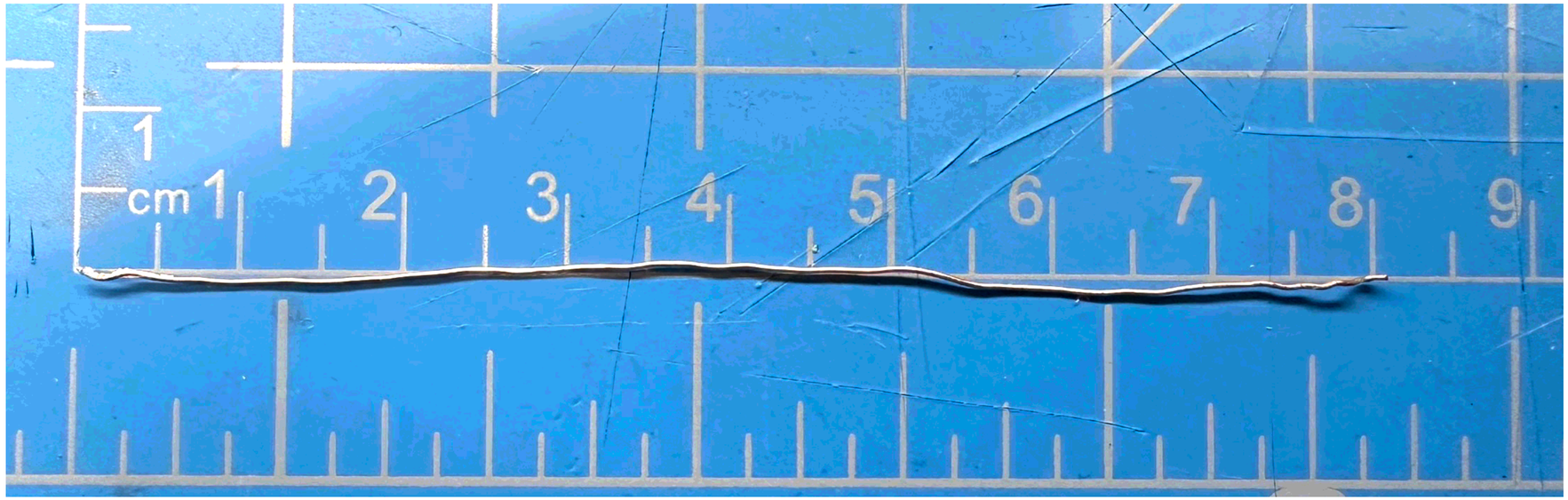
- Watch while user enters PIN, steal device at a later date?
- See transaction amounts to determine if user is worth targeting for robbery?
- Capture recovery seed during initial setup or restore?

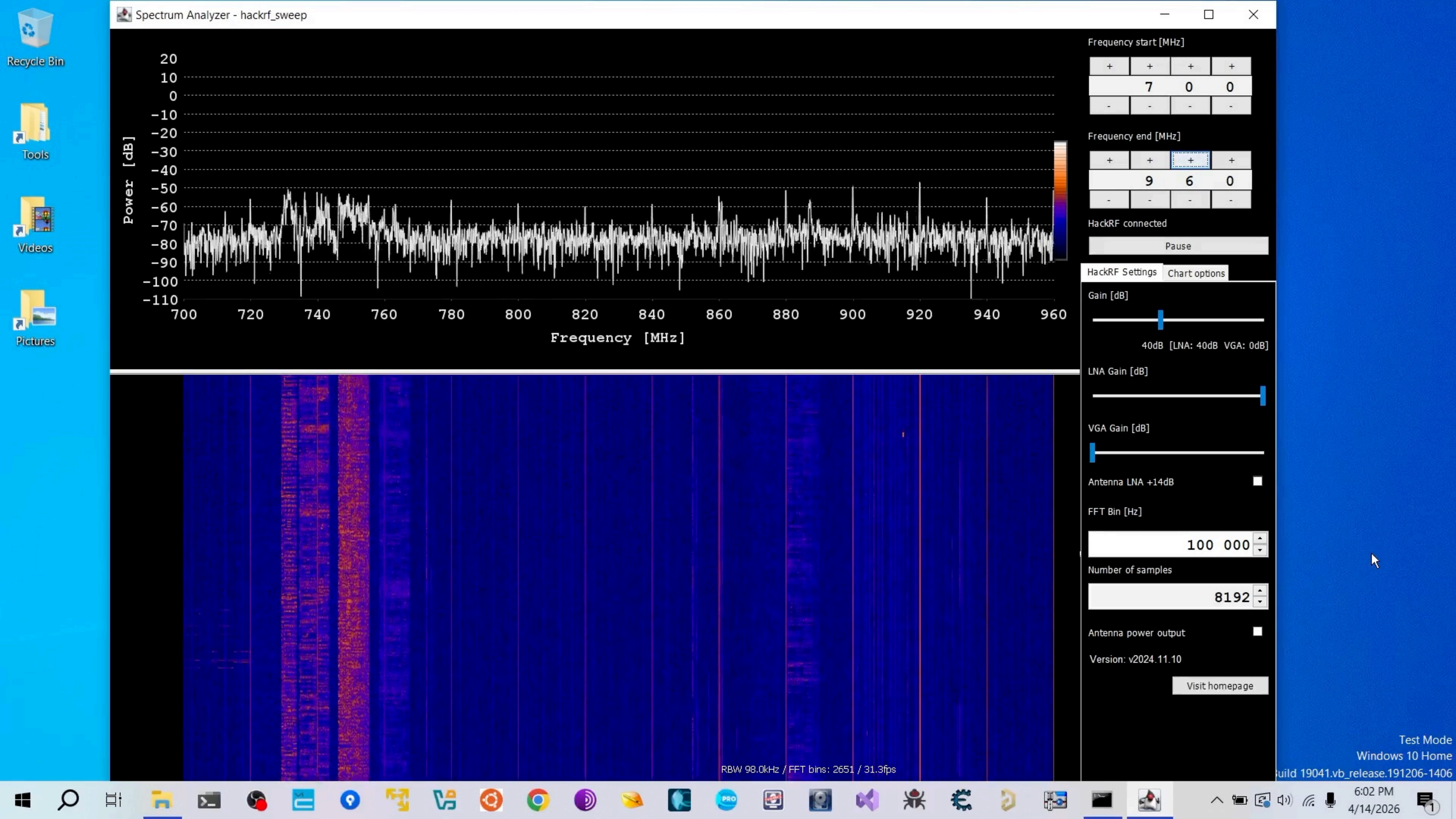
INTERFACING

RF

- Antenna = 8 cm hand-wound coil -> f ≈ 937 MHz @ 1/4 wave
- HackRF + hackrf-spectrum-analyzer to identify transmissions?

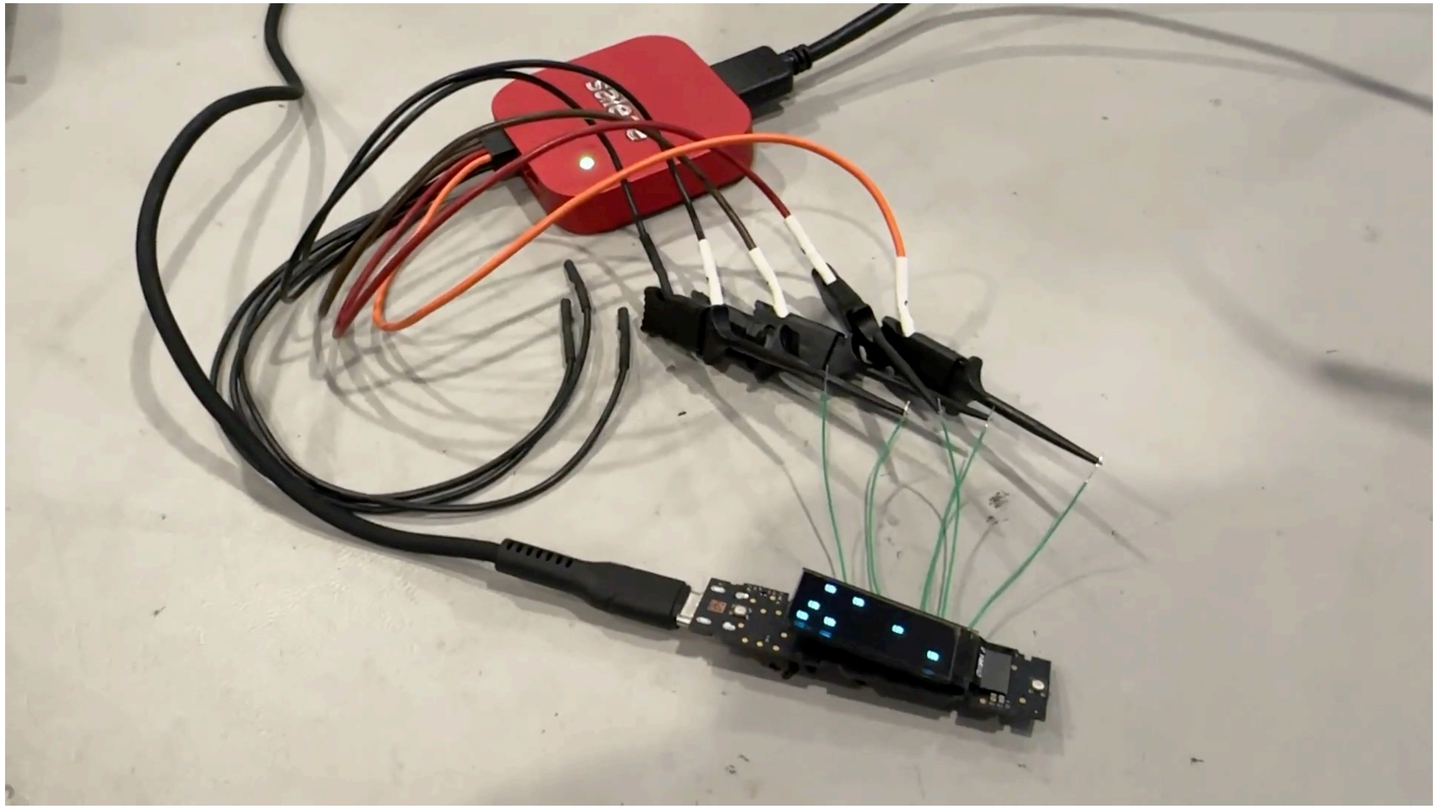


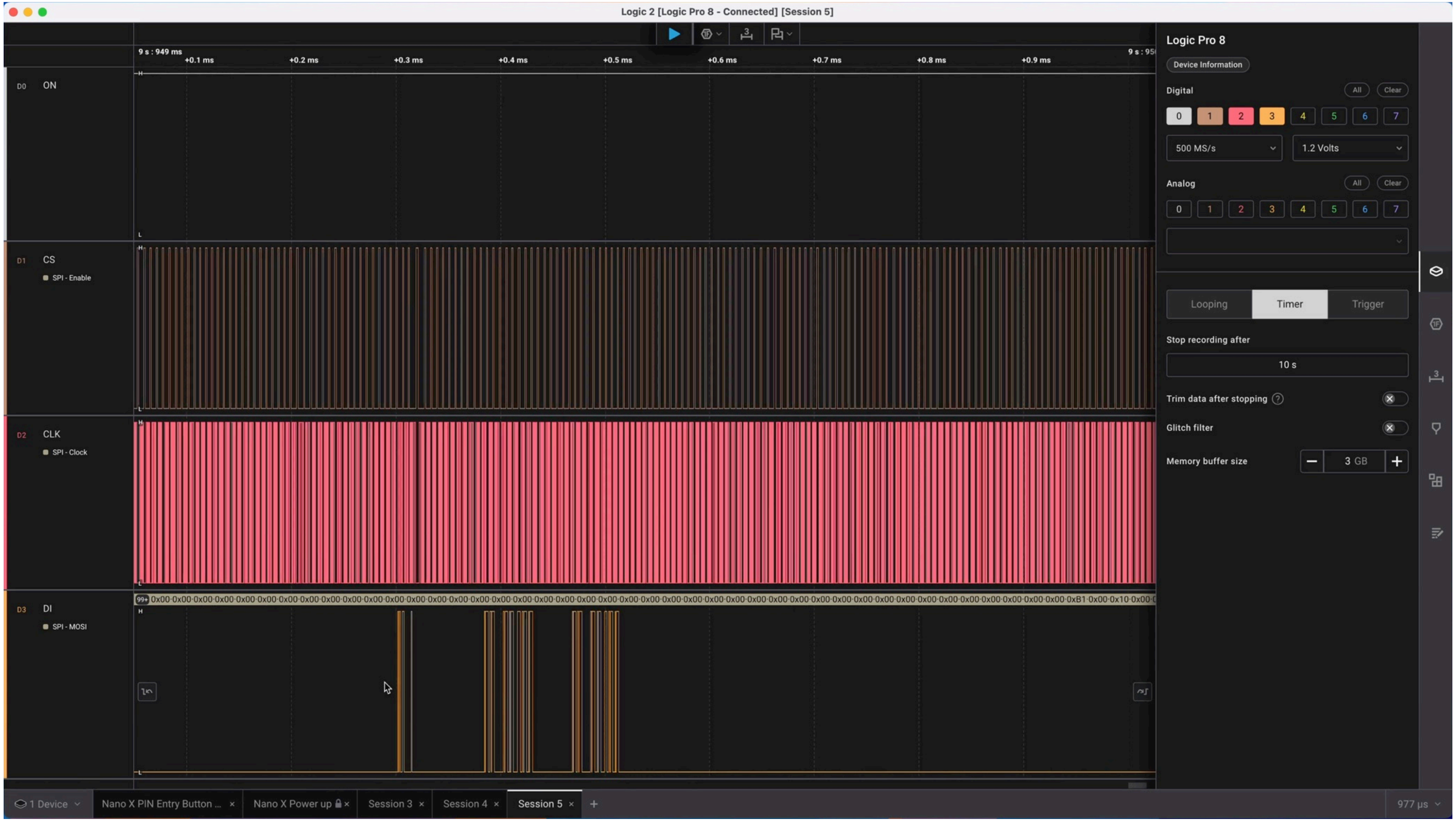



Spectrum Analyzer - hackrf_sweep
Power [dB]
20
10
0
-10
-20
-30
-40
-50
-60
-70
-80
-90
-100
-110
700
720
740
760
780
800
820
840
860
880
900
920
940
960
Frequency [MHz]
RBW 98.0kHz / FFT bins: 2651 / 31.3fps
Frequency start [MHz]
7 0 0
Frequency end [MHz]
9 6 0
HackRF connected
Pause
HackRF Settings
Chart options
Gain [dB]
40dB [LNA: 40dB VGA: 0dB]
LNA Gain [dB]
VGA Gain [dB]
Antenna LNA +14dB
FFT Bin [Hz]
100 000
Number of samples
8192
Antenna power output
Version: v2024.11.10
Visit homepage
Recycle Bin
Tools
Videos
Pictures
Test Mode
Windows 10 Home
Build 19041.vb_release.191206-1406
6:02 PM
4/14/2026

OLED

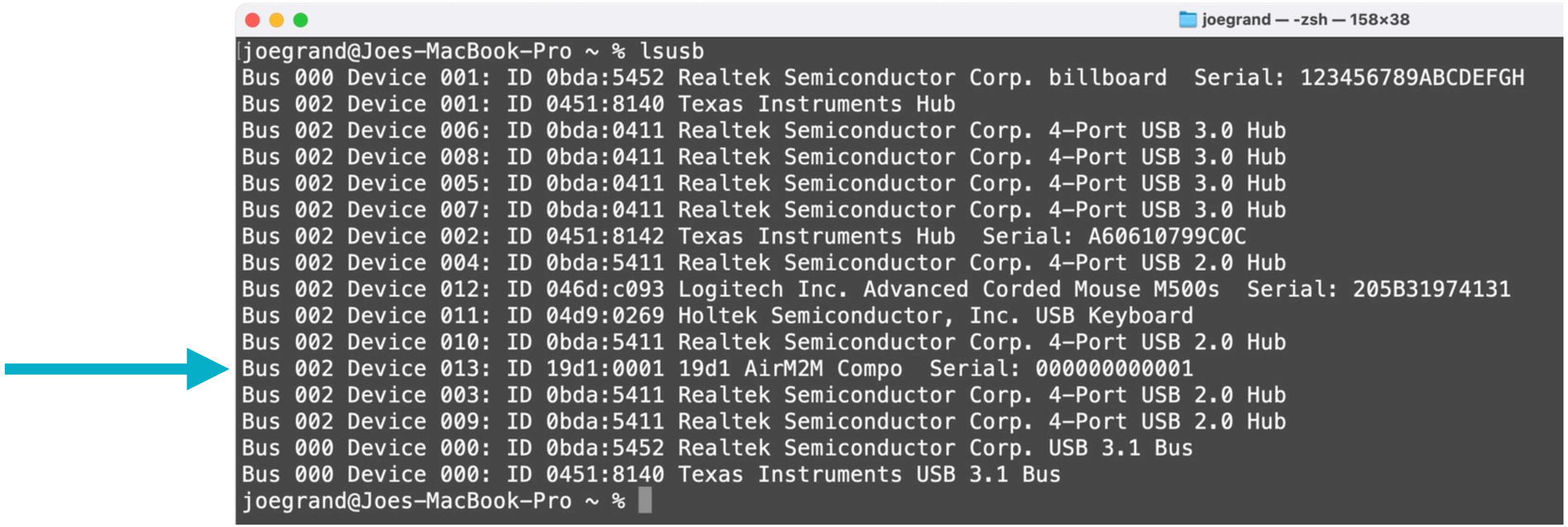
- OLED connects to the Nano X Secure Element via Serial Peripheral Interface (SPI)
- Monitor SPI w/ Logic 8 Pro to get a sense of activity

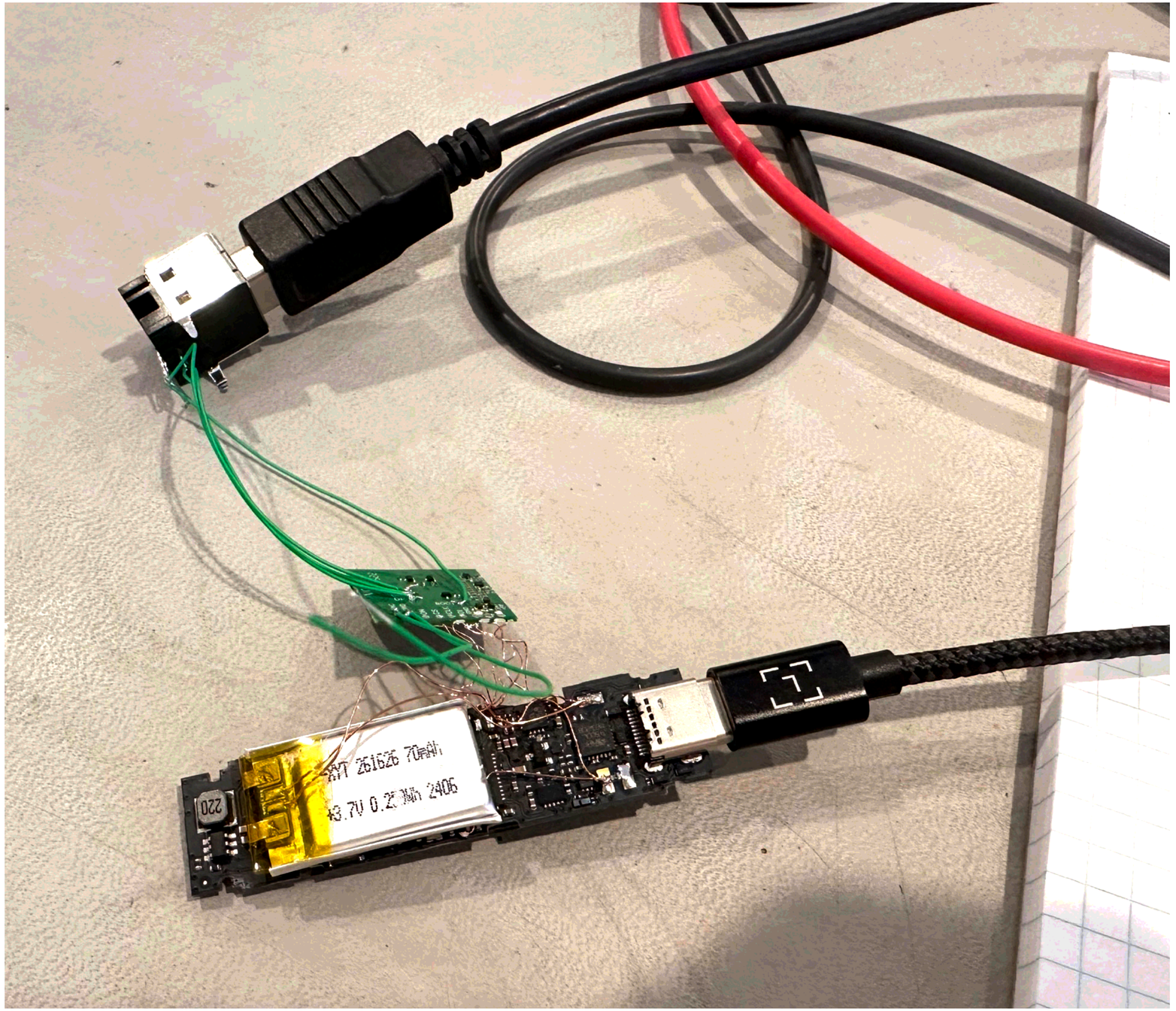


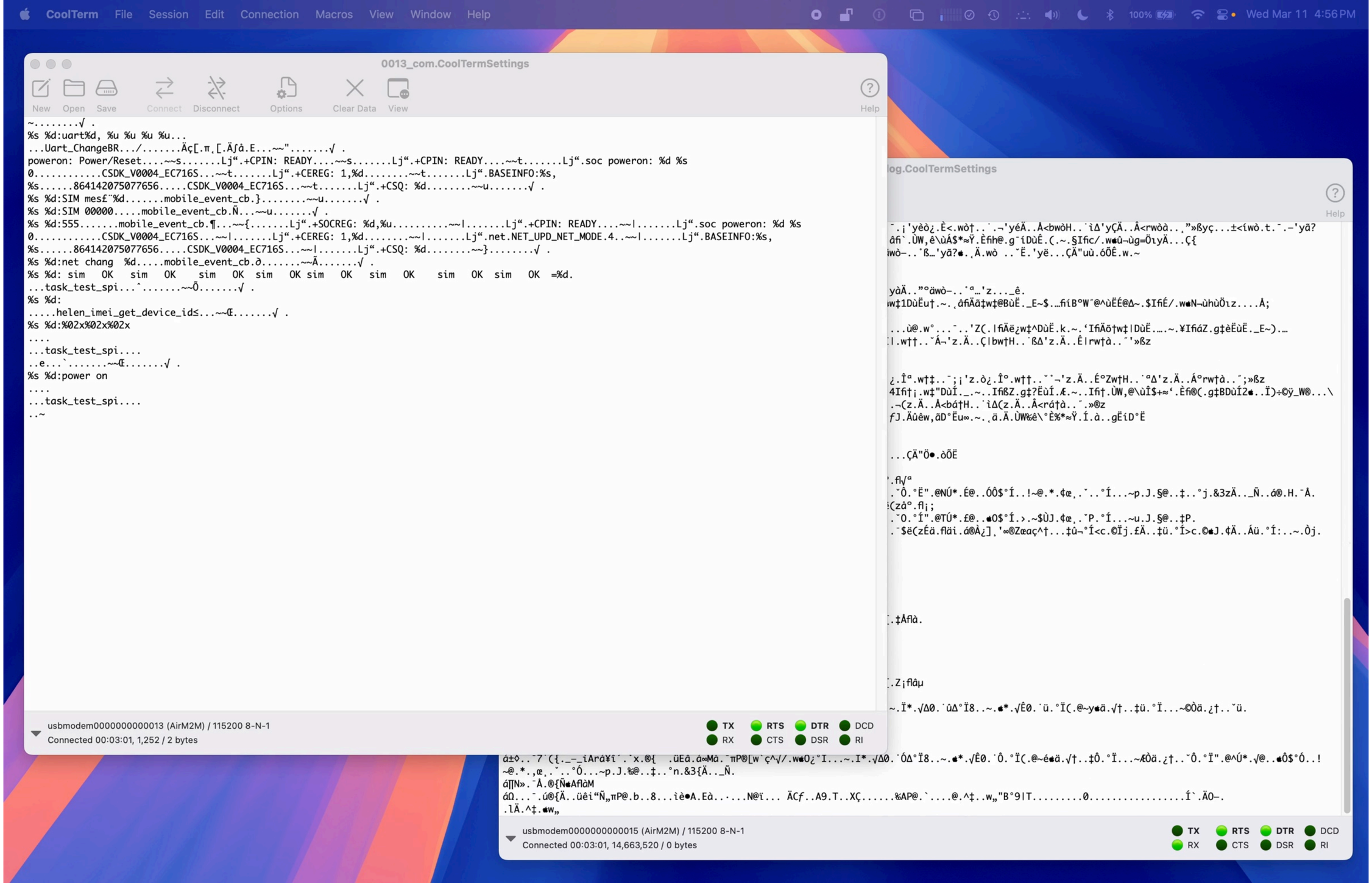

Logic 2 [Logic Pro 8 - Connected] [Session 5]
9 s : 949 ms
+0.1 ms
+0.2 ms
+0.3 ms
+0.4 ms
+0.5 ms
+0.6 ms
+0.7 ms
+0.8 ms
+0.9 ms
D0 ON
D1 CS
SPI - Enable
D2 CLK
SPI - Clock
D3 DI
SPI - MOSI
Logic Pro 8
Device Information
Digital
All
Clear
0 1 2 3 4 5 6 7
500 MS/s
1.2 Volts
Analog
All
Clear
0 1 2 3 4 5 6 7
Looping
Timer
Trigger
Stop recording after
10 s
Trim data after stopping
Glitch filter
Memory buffer size
3 GB
1 Device
Nano X PIN Entry Button ...
Nano X Power up
Session 3
Session 4
Session 5
977 µs

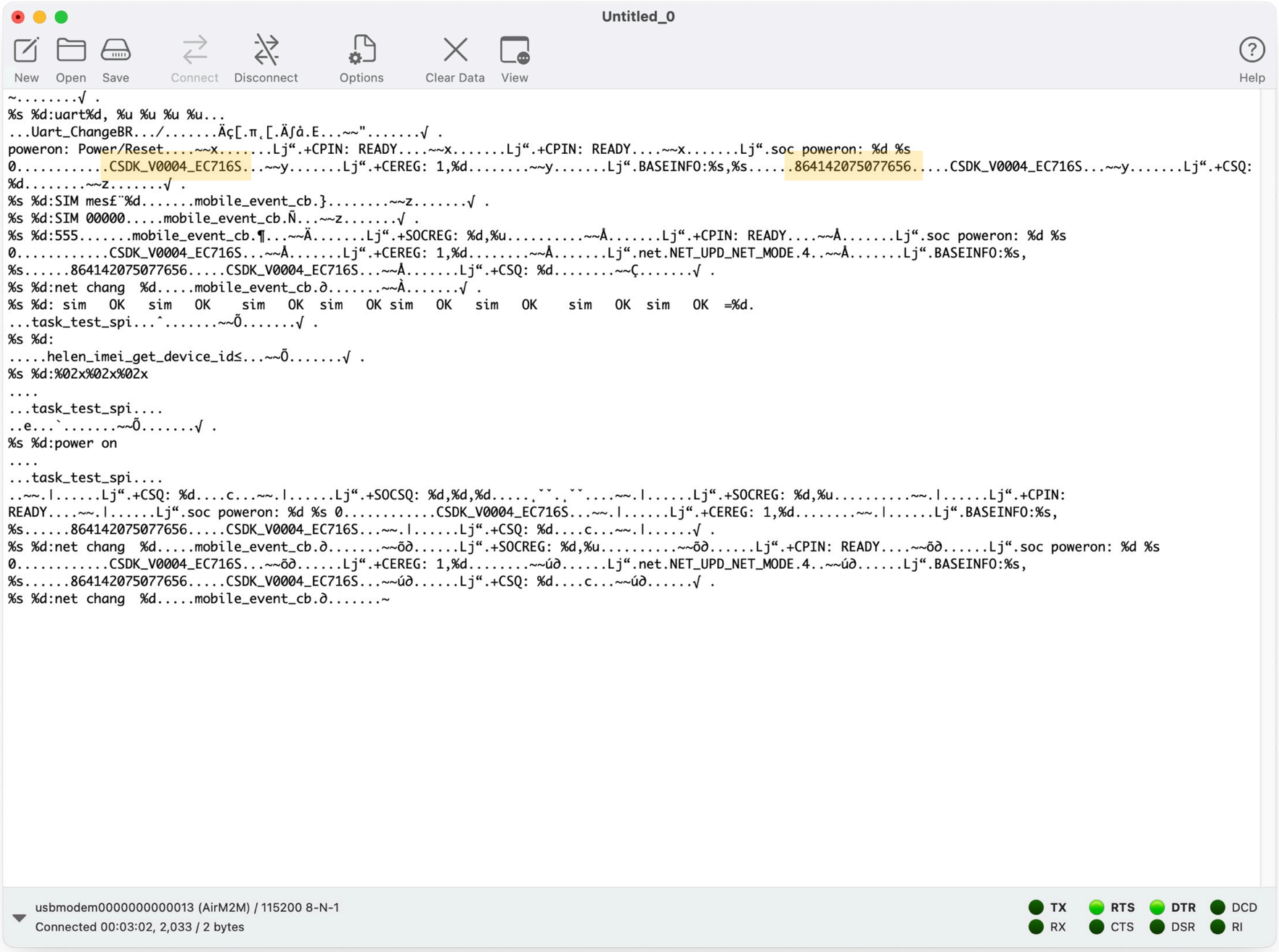
USB

- Soldered DP/DM test points to USB Type A connector
- BOOT pin pulled HIGH (VUSB/+5V) -> Bootloader 15 seconds -> 3x USB CDC-ACM + 1x RNDIS
- BOOT pin pulled LOW -> Ports appear for 1 second then disappear




3.7V 0.2Wh 2406
220


CoolTerm File Session Edit Connection Macros View Window Help
Wed Mar 11 4:56 PM
0013_com.CoolTermSettings
New Open Save Connect Disconnect Options Clear Data View Help
~........√ .
%s %d:uart%d, %u %u %u %u...
...Uart_ChangeBR.../.......Äç[.π¸[.Äƒå.E...~~".....√ .
poweron: Power/Reset....~~s.....Lj“.+CPIN: READY....~~s.....Lj“.+CPIN: READY....~~t.....Lj“.soc poweron: %d %s
0...........CSDK_V0004_EC716S...~~t.....Lj“.+CEREG: 1,%d.....~~t.....Lj“.BASEINFO:%s,
%s.....864142075077656.....CSDK_V0004_EC716S...~~t.....Lj“.+CSQ: %d.....~~u.....√ .
%s %d:SIM mes£¨%d.....mobile_event_cb.}.....~~u.....√ .
%s %d:SIM 00000.....mobile_event_cb.Ñ...~~u.....√ .
%s %d:555.....mobile_event_cb.¶...~~{.....Lj“.+SOCREG: %d,%u.....~~|.....Lj“.+CPIN: READY....~~|.....Lj“.soc poweron: %d %s
0...........CSDK_V0004_EC716S...~~|.....Lj“.+CEREG: 1,%d.....~~|.....Lj“.net.NET_UPD_NET_MODE.4..~~|.....Lj“.BASEINFO:%s,
%s.....864142075077656.....CSDK_V0004_EC716S...~~|.....Lj“.+CSQ: %d.....~~}.....√ .
%s %d:net chang %d.....mobile_event_cb.∂.....~~Ã.....√ .
%s %d: sim OK sim OK sim OK sim OK sim OK sim OK =%d.
...task_test_spi...^.....~~Õ.....√ .
%s %d:
.....helen_imei_get_device_id≤...~~Œ.....√ .
%s %d:%02x%02x%02x
....
...task_test_spi....
..e...`.....~~Œ.....√ .
%s %d:power on
....
...task_test_spi....
..~
usbmodem0000000000013 (AirM2M) / 115200 8-N-1
Connected 00:03:01, 1,252 / 2 bytes
TX RX RTS CTS DTR DSR DCD RI
log.CoolTermSettings
Help
usbmodem0000000000015 (AirM2M) / 115200 8-N-1
Connected 00:03:01, 14,663,520 / 0 bytes
TX RX RTS CTS DTR DSR DCD RI


Untitled_0
New
Open
Save
Connect
Disconnect
Options
Clear Data
View
Help
~........√ .
%s %d:uart%d, %u %u %u %u...
...Uart_ChangeBR.../.......Äç[.π¸[.Äſå.E...~~".......√ .
poweron: Power/Reset....~~x.......Lj“.+CPIN: READY....~~x.......Lj“.+CPIN: READY....~~x.......Lj“.soc poweron: %d %s
0...........CSDK_V0004_EC716S..~~y.......Lj“.+CEREG: 1,%d.......~~y.......Lj“.BASEINFO:%s,%s.....864142075077656....CSDK_V0004_EC716S...~~y.......Lj“.+CSQ:
%d.......~~z.......√ .
%s %d:SIM mes£¨%d.......mobile_event_cb.}........~~z.......√ .
%s %d:SIM 00000.....mobile_event_cb.Ñ...~~z.......√ .
%s %d:555.......mobile_event_cb.¶...~~Ä.......Lj“.+SOCREG: %d,%u..........~~Å.......Lj“.+CPIN: READY....~~Å.......Lj“.soc poweron: %d %s
0...........CSDK_V0004_EC716S...~~Å.......Lj“.+CEREG: 1,%d.......~~Å.......Lj“.net.NET_UPD_NET_MODE.4..~~Å.......Lj“.BASEINFO:%s,
%s......864142075077656.....CSDK_V0004_EC716S...~~Å.......Lj“.+CSQ: %d.......~~Ç.......√ .
%s %d:net chang %d.....mobile_event_cb.∂.......~~À.......√ .
%s %d: sim   OK   sim   OK   sim   OK sim   OK sim   OK   sim   OK   sim   OK sim   OK =%d.
...task_test_spi...ˆ.......~~Õ.......√ .
%s %d:
.....helen_imei_get_device_id≤...~~Õ.......√ .
%s %d:%02x%02x%02x
....
...task_test_spi....
..e...`.......~~Õ.......√ .
%s %d:power on
....
...task_test_spi....
..~~.|......Lj“.+CSQ: %d....c...~~.|......Lj“.+SOCSQ: %d,%d,%d.....¸˘˘.¸˘˘....~~.|......Lj“.+SOCREG: %d,%u..........~~.|......Lj“.+CPIN:
READY....~~.|......Lj“.soc poweron: %d %s 0...........CSDK_V0004_EC716S...~~.|......Lj“.+CEREG: 1,%d.......~~.|......Lj“.BASEINFO:%s,
%s......864142075077656.....CSDK_V0004_EC716S...~~.|......Lj“.+CSQ: %d....c...~~.|......√ .
%s %d:net chang %d.....mobile_event_cb.∂.......~~õ∂......Lj“.+SOCREG: %d,%u..........~~õ∂......Lj“.+CPIN: READY....~~õ∂......Lj“.soc poweron: %d %s
0...........CSDK_V0004_EC716S...~~õ∂......Lj“.+CEREG: 1,%d.......~~ú∂......Lj“.net.NET_UPD_NET_MODE.4..~~ú∂......Lj“.BASEINFO:%s,
%s......864142075077656.....CSDK_V0004_EC716S...~~ú∂......Lj“.+CSQ: %d....c...~~ú∂......√ .
%s %d:net chang %d.....mobile_event_cb.∂.......~
usbmodem0000000000013 (AirM2M) / 115200 8-N-1
Connected 00:03:02, 2,033 / 2 bytes
TX
RX
RTS
CTS
DTR
DSR
DCD
RI

Cat.1 Bis Series

Not Secure http://www.eigencomm.com/Content/3006141.html

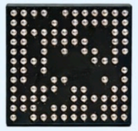
New Chrome available

EIGENCOMM
More than connection

Products and Services About Us Contact Us

EN

NB-IoT Series Cat.1 Bis Series 5G Redcap&Cat.4



EC618

Standard: 3GPP R13/R14 Cat.1bis

Key Features:
· Integrated BB, RF, and PMIC
· Super power-saving

Package: LFBGA 6.1mm × 6.1mm × 1.14mm

Voltage Range: 3.1V to 4.5V

EC716

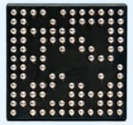
Standard: 3GPP R13/R14 Cat.1bis

Key Features:
· Integrated BB, RF, and PMIC
· Super power-saving
· Optimized for data-only modules

Package: LFBGA 5mm × 5mm × 0.89mm (smallest size in the industry)

Supply Chain: Domestic integration for cost optimization

Sub-models: EC716S/E with configurable Flash size (2M/4M)



EC718

Standard: 3GPP R13/R14 Cat.1bis

Key Features:
· Integrated BB, RF, and PMIC
· Super power-saving
· Voice capacity
· Edge AI and multimedia support
· Memory enhancement
· Open CPU enhancement

Sub-models

EC718:
LFBGA 6.1mm × 6.1mm × 0.84mm; scalable CPU, RAM, and Flash (2M/4M/8M)

EC718V:
Voice over LTE


alpha.imeicheck.com/api/mod
https://alpha.imeicheck.com/api/modelBrandName?imei=864142075077656
New Chrome available
IMEI: 864142075077656
Brand: Shanghai Hezhou Communication Technology Co Ltd
Model: Air700E
Model Name: Air700E

上海合宙 www.openluat.com

Luat Air700EMQ

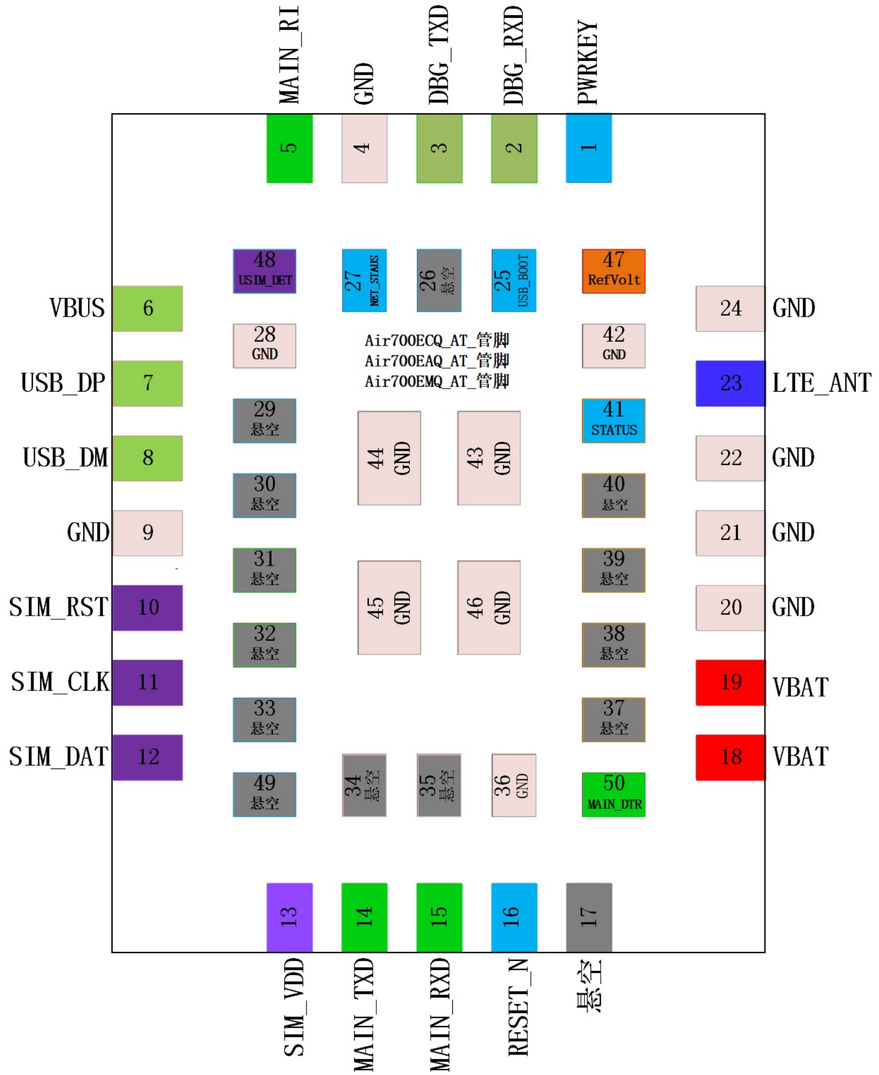
LTE Cat.1模块

Air700EMQ是合宙通信推出的 LTE Cat.1 bis通信模块；
Air700EMQ采用移芯EC716E平台，支持 LTE 3GPP Rel.13 技术；
Air700EMQ支持联通频段，超小封装，极致成本，满足小型化低成本需求。

Air700EMQ支持单1.8/3.0V USIM接口；
Air700EMQ支持1.8；
Air700EMQ支持USB 2.0；
Air700EMQ支持远程OTA固件升级；

Air700EMQ支持多种开发方式，如USB上网、标准AT开发，并可提供专业且及时的在线技术支持，欢迎登录 www.openluat.com 进一步了解。

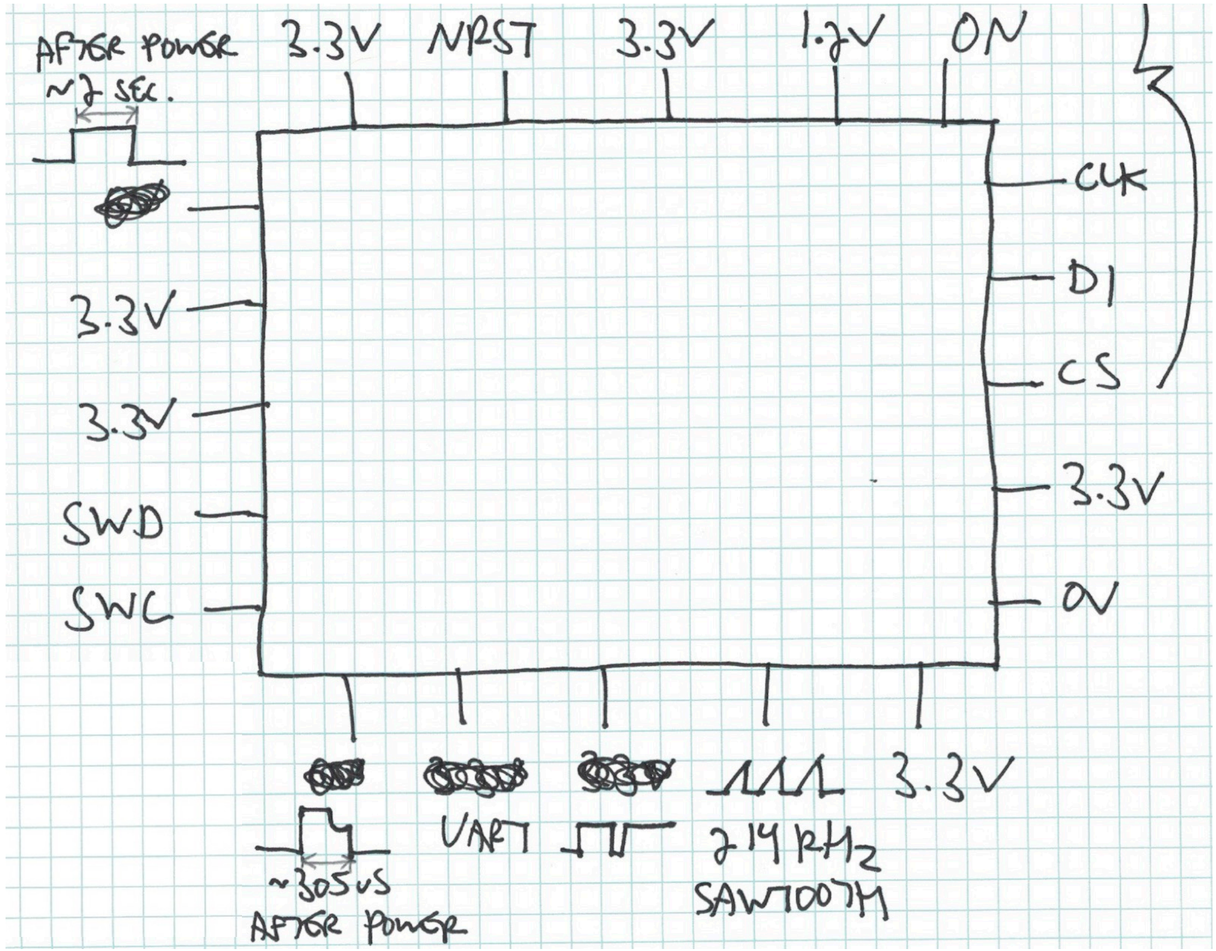
Air700EMQ内置丰富的网络协议，集成多个工业标准接口，并支持多种驱动和软件功能（如Windows 7/8/8.1/10，Linux，Android等操作系统下的 USB 驱动等），极大地拓展了其在 M2M 领域的应用范围，如 CPE、路由器、数据卡、平板电脑、车载、安防以及工业级 PDA 等。



https://docs.openluat.com/air700emq/

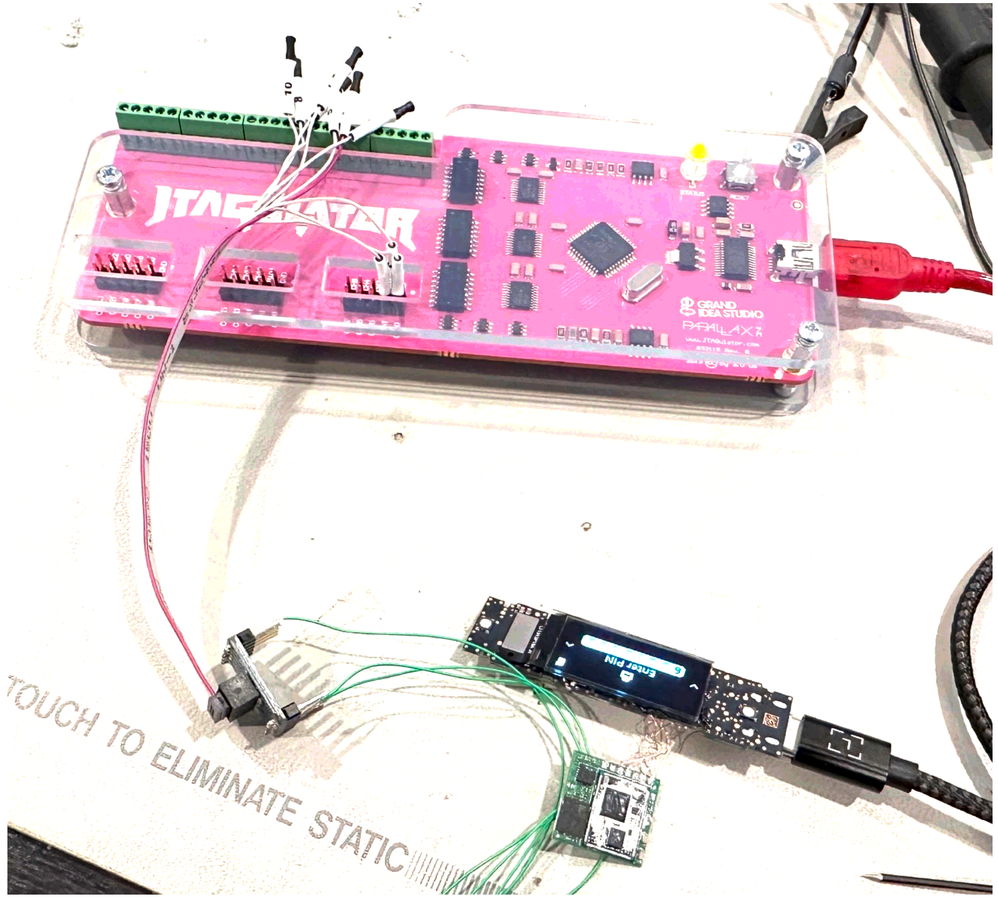
MCU

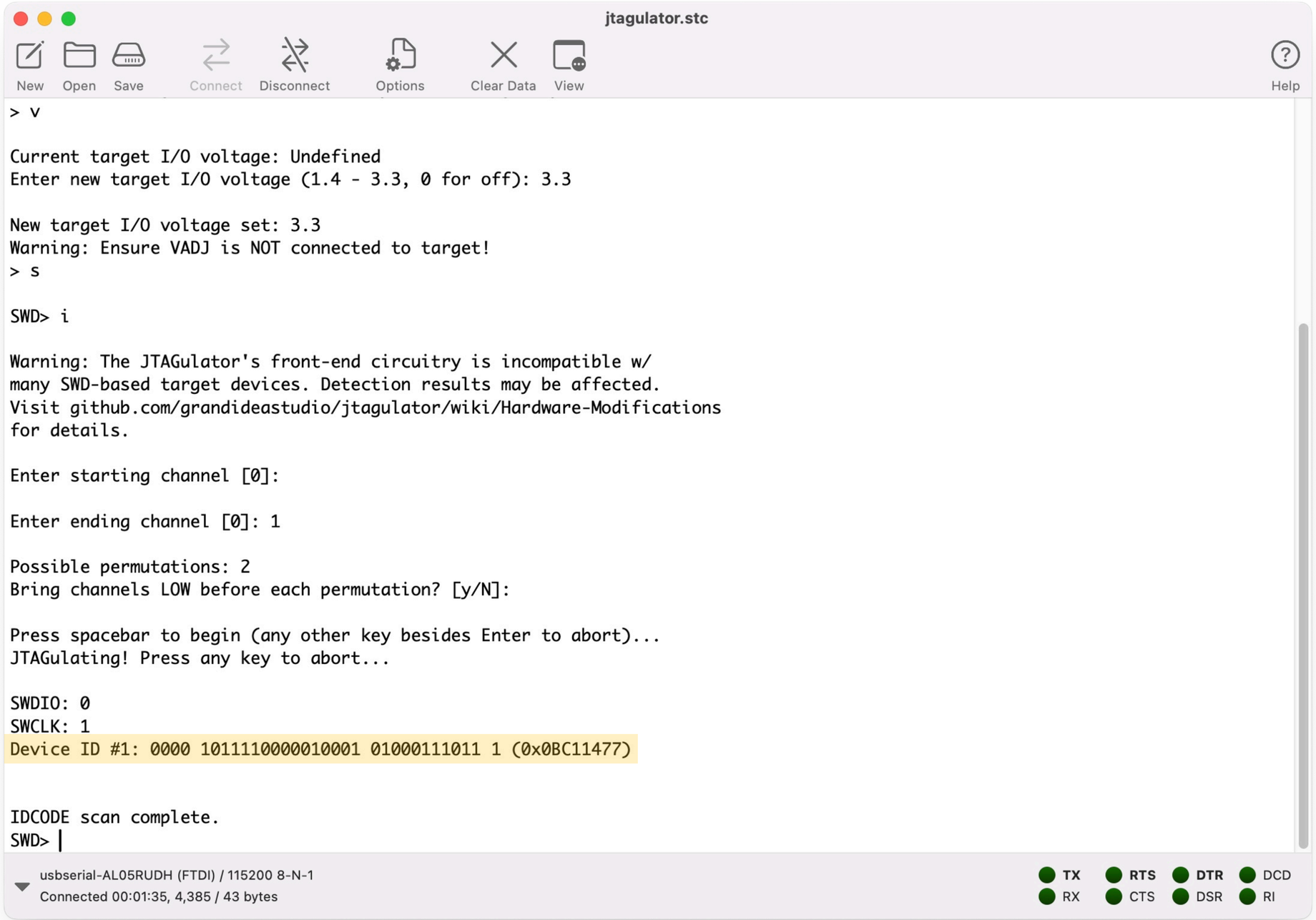
- QFN-20 / UFQFPN-20
- 3 x 3mm, 0.5 or 0.6mm pitch
- Can't find any matching from US/Europe

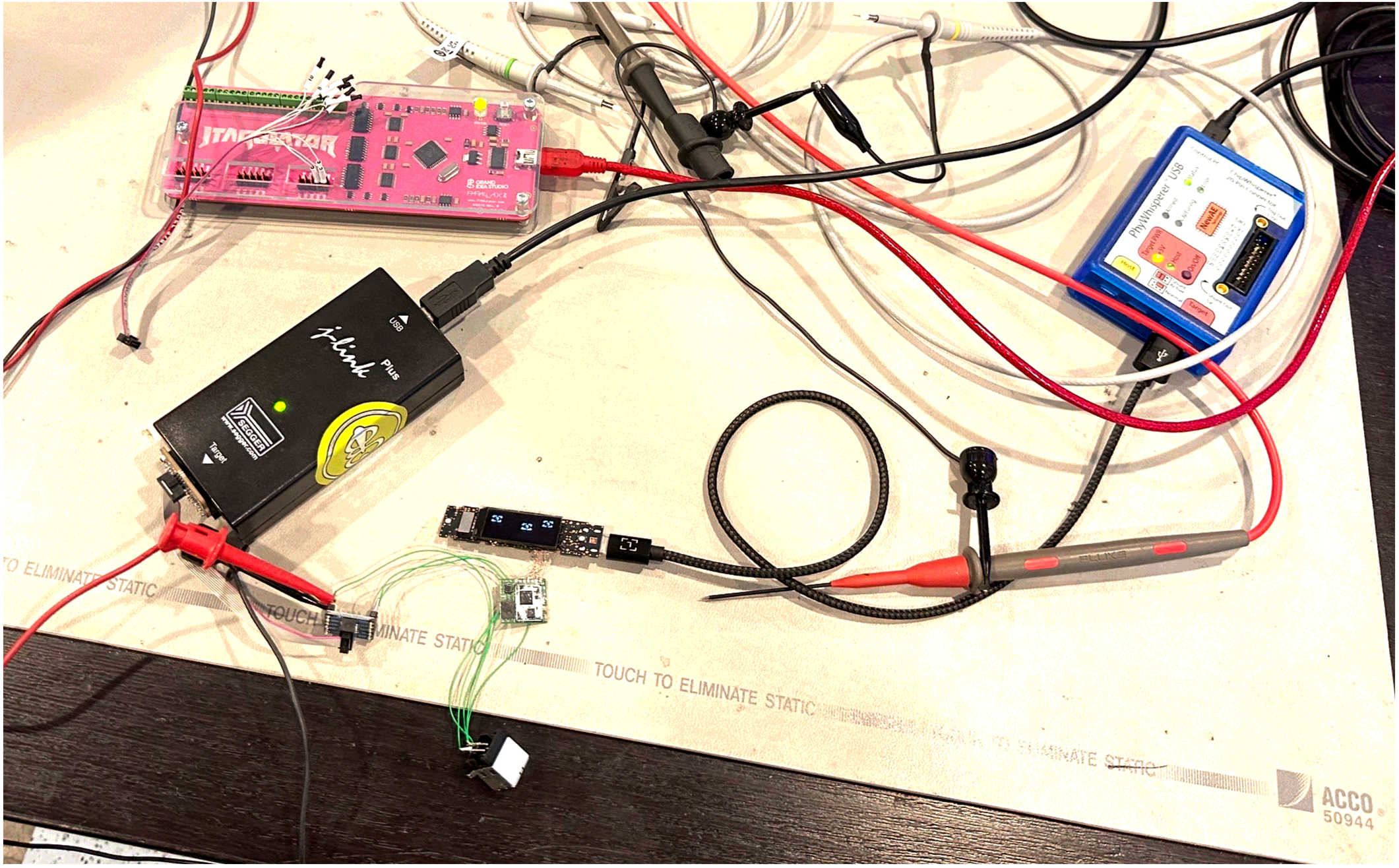


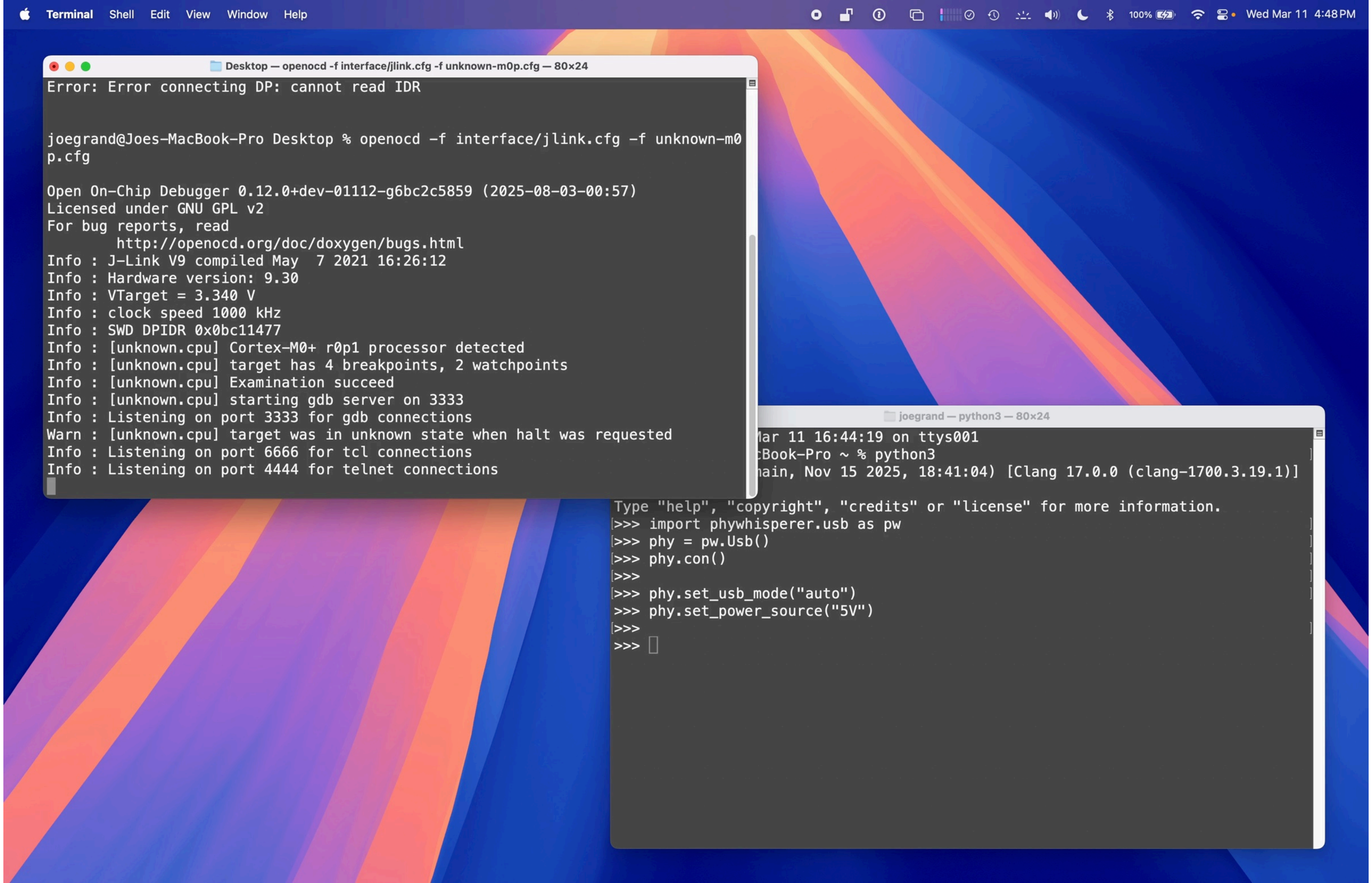
SWD

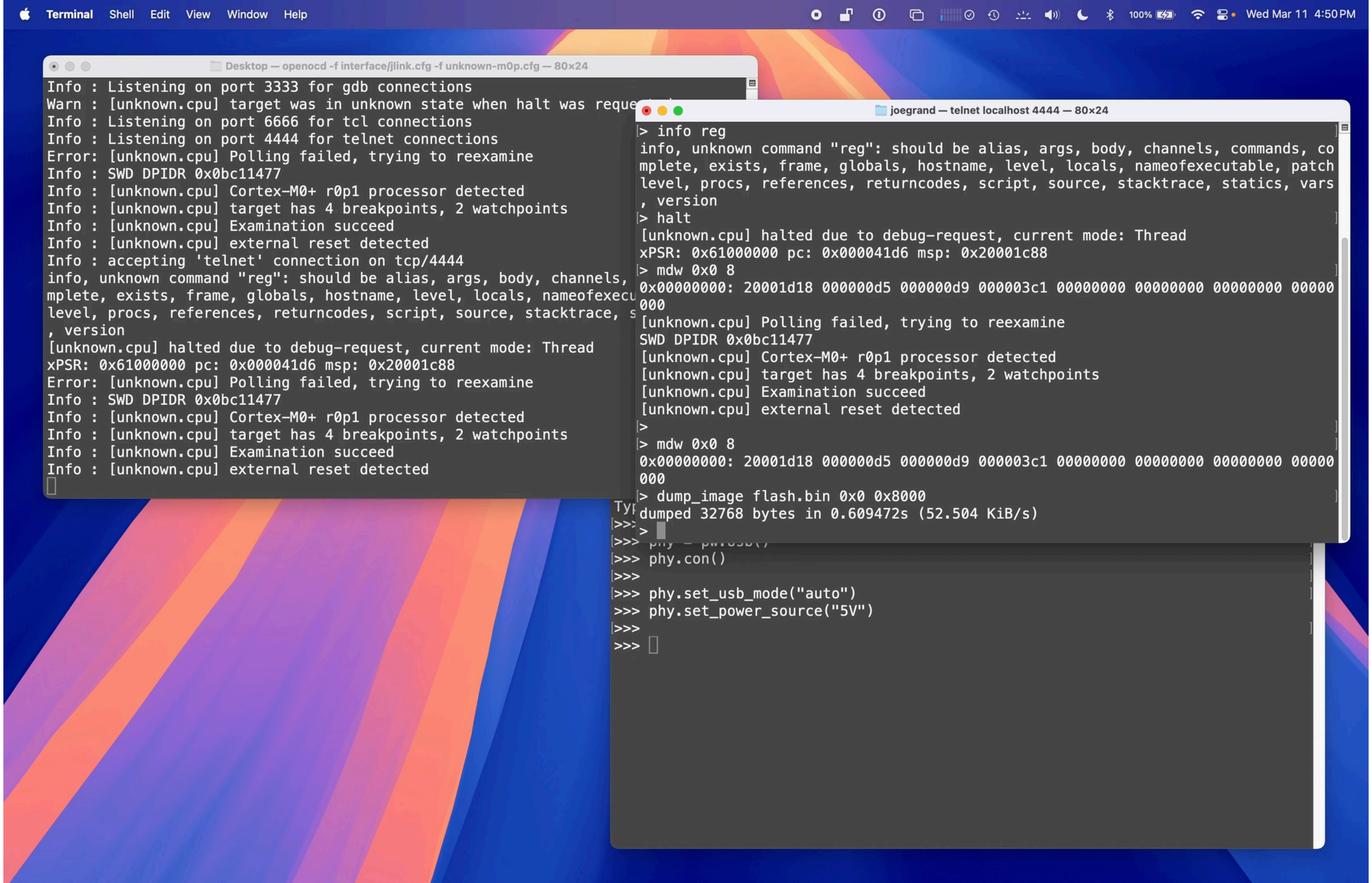
- JTAGulator for initial debug interface verification
- OpenOCD + SEGGER J-Link
- ARM Cortex-M0+, 32KB Flash, 8KB RAM
- No code protection!

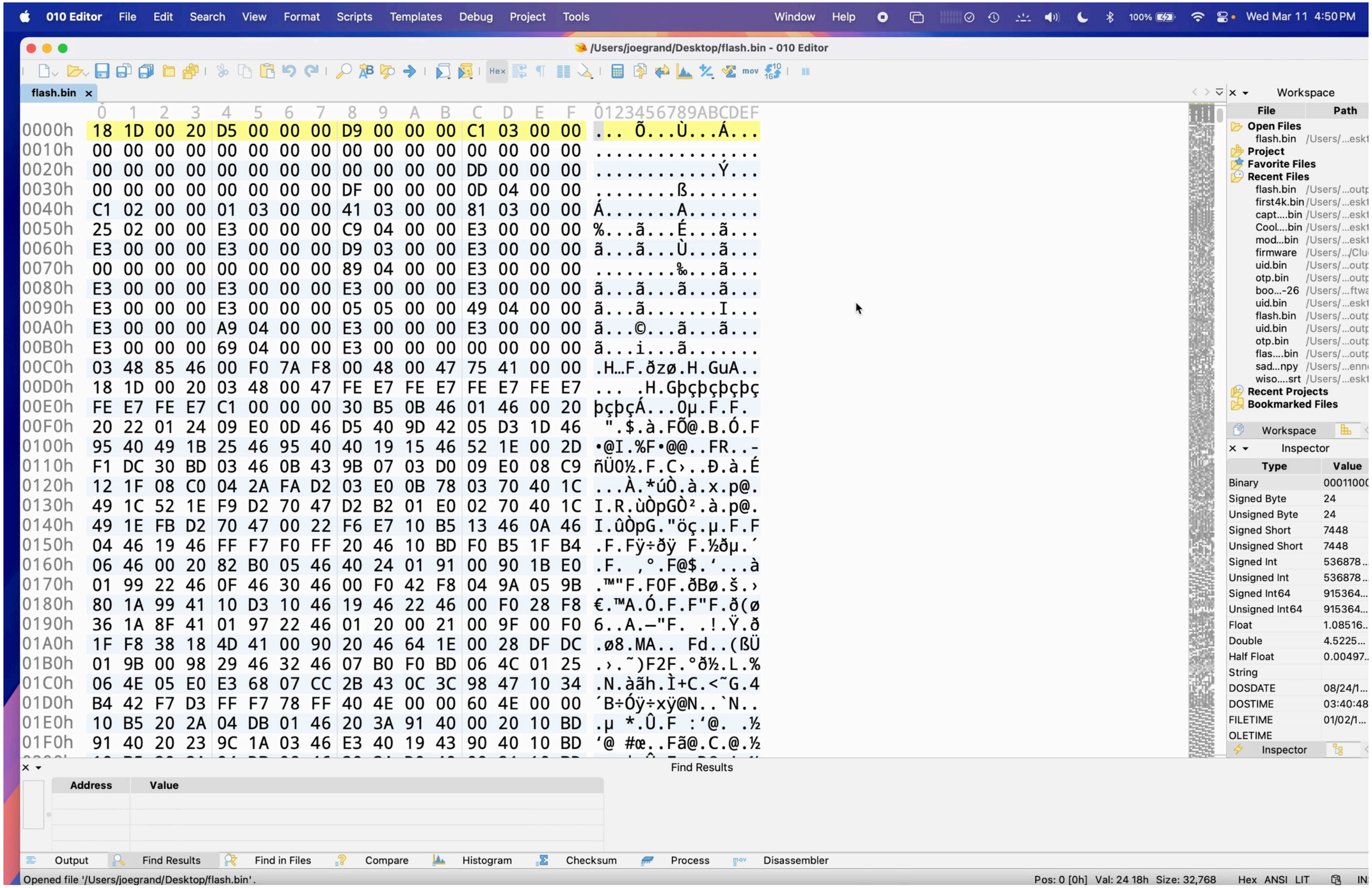



jtagulator.stc
New
Open
Save
Connect
Disconnect
Options
Clear Data
View
Help
> v
Current target I/O voltage: Undefined
Enter new target I/O voltage (1.4 - 3.3, 0 for off): 3.3
New target I/O voltage set: 3.3
Warning: Ensure VADJ is NOT connected to target!
> s
SWD> i
Warning: The JTAGulator's front-end circuitry is incompatible w/
many SWD-based target devices. Detection results may be affected.
Visit github.com/grandideastudio/jtagulator/wiki/Hardware-Modifications
for details.
Enter starting channel [0]:
Enter ending channel [0]: 1
Possible permutations: 2
Bring channels LOW before each permutation? [y/N]:
Press spacebar to begin (any other key besides Enter to abort)...
JTAGulating! Press any key to abort...
SWDIO: 0
SWCLK: 1
Device ID #1: 0000 1011110000010001 01000111011 1 (0x0BC11477)
IDCODE scan complete.
SWD>
usbserial-AL05RUDH (FTDI) / 115200 8-N-1
Connected 00:01:35, 4,385 / 43 bytes
TX
RX
RTS
CTS
DTR
DSR
DCD
RI


USB
j-link
Plus
SEGGER
Target
PhyWhisperer-USB
NewAE
TOUCH TO ELIMINATE STATIC
ACCO
50944

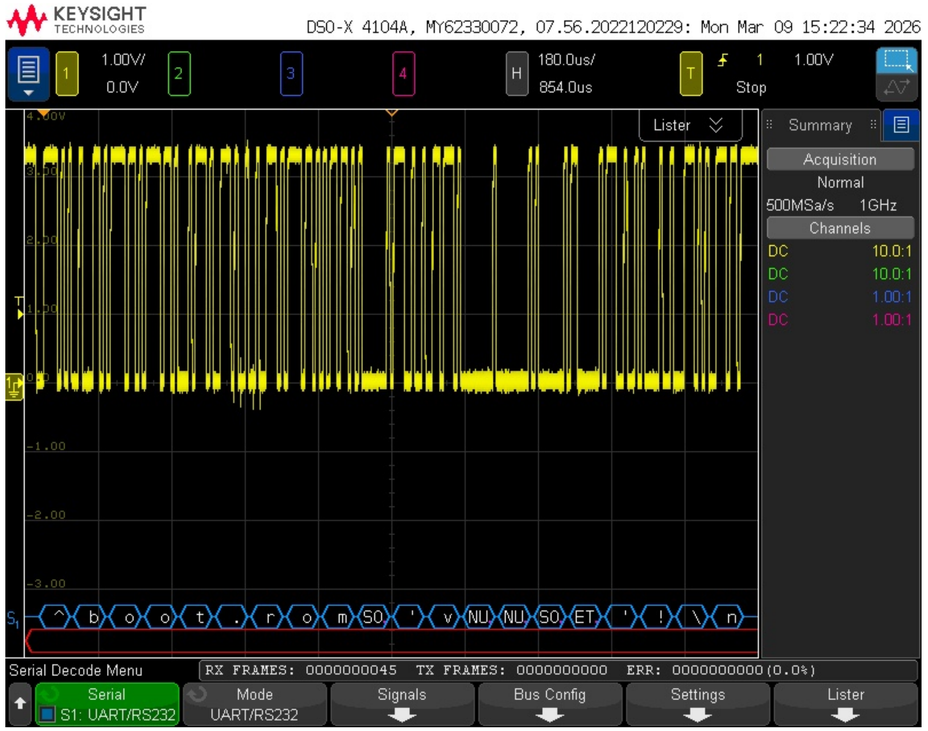

Terminal Shell Edit View Window Help
100% Wed Mar 11 4:48 PM
Desktop — openocd -f interface/jlink.cfg -f unknown-m0p.cfg — 80×24
Error: Error connecting DP: cannot read IDR
joegrand@Joes-MacBook-Pro Desktop % openocd -f interface/jlink.cfg -f unknown-m0
p.cfg
Open On-Chip Debugger 0.12.0+dev-01112-g6bc2c5859 (2025-08-03-00:57)
Licensed under GNU GPL v2
For bug reports, read
http://openocd.org/doc/doxygen/bugs.html
Info : J-Link V9 compiled May 7 2021 16:26:12
Info : Hardware version: 9.30
Info : VTarget = 3.340 V
Info : clock speed 1000 kHz
Info : SWD DPIDR 0x0bc11477
Info : [unknown.cpu] Cortex-M0+ r0p1 processor detected
Info : [unknown.cpu] target has 4 breakpoints, 2 watchpoints
Info : [unknown.cpu] Examination succeed
Info : [unknown.cpu] starting gdb server on 3333
Info : Listening on port 3333 for gdb connections
Warn : [unknown.cpu] target was in unknown state when halt was requested
Info : Listening on port 6666 for tcl connections
Info : Listening on port 4444 for telnet connections
joegrand — python3 — 80×24
Type "help", "copyright", "credits" or "license" for more information.
>>> import phywhisperer.usb as pw
>>> phy = pw.Usb()
>>> phy.con()
>>>
>>> phy.set_usb_mode("auto")
>>> phy.set_power_source("5V")
>>>
>>>


Terminal Shell Edit View Window Help
Wed Mar 11 4:50 PM
Desktop — openocd -f interface/jlink.cfg -f unknown-m0p.cfg — 80×24
Info : Listening on port 3333 for gdb connections
Warn : [unknown.cpu] target was in unknown state when halt was reque
Info : Listening on port 6666 for tcl connections
Info : Listening on port 4444 for telnet connections
Error: [unknown.cpu] Polling failed, trying to reexamine
Info : SWD DPIDR 0x0bc11477
Info : [unknown.cpu] Cortex-M0+ r0p1 processor detected
Info : [unknown.cpu] target has 4 breakpoints, 2 watchpoints
Info : [unknown.cpu] Examination succeed
Info : [unknown.cpu] external reset detected
Info : accepting 'telnet' connection on tcp/4444
info, unknown command "reg": should be alias, args, body, channels,
mplete, exists, frame, globals, hostname, level, locals, nameofexecu
level, procs, references, returncodes, script, source, stacktrace, s
, version
[unknown.cpu] halted due to debug-request, current mode: Thread
xPSR: 0x61000000 pc: 0x000041d6 msp: 0x20001c88
Error: [unknown.cpu] Polling failed, trying to reexamine
Info : SWD DPIDR 0x0bc11477
Info : [unknown.cpu] Cortex-M0+ r0p1 processor detected
Info : [unknown.cpu] target has 4 breakpoints, 2 watchpoints
Info : [unknown.cpu] Examination succeed
Info : [unknown.cpu] external reset detected
joegrand — telnet localhost 4444 — 80×24
> info reg
info, unknown command "reg": should be alias, args, body, channels, commands, co
mplete, exists, frame, globals, hostname, level, locals, nameofexecutable, patch
level, procs, references, returncodes, script, source, stacktrace, statics, vars
, version
> halt
[unknown.cpu] halted due to debug-request, current mode: Thread
xPSR: 0x61000000 pc: 0x000041d6 msp: 0x20001c88
> mdw 0x0 8
0x00000000: 20001d18 000000d5 000000d9 000003c1 00000000 00000000 00000000 00000
000
[unknown.cpu] Polling failed, trying to reexamine
SWD DPIDR 0x0bc11477
[unknown.cpu] Cortex-M0+ r0p1 processor detected
[unknown.cpu] target has 4 breakpoints, 2 watchpoints
[unknown.cpu] Examination succeed
[unknown.cpu] external reset detected
>
> mdw 0x0 8
0x00000000: 20001d18 000000d5 000000d9 000003c1 00000000 00000000 00000000 00000
000
> dump_image flash.bin 0x0 0x8000
dumped 32768 bytes in 0.609472s (52.504 KiB/s)
>
>>> phy.con()
>>>
>>> phy.set_usb_mode("auto")
>>> phy.set_power_source("5V")
>>>
>>>


010 Editor File Edit Search View Format Scripts Templates Debug Project Tools Window Help Wed Mar 11 4:50 PM
/Users/joegrand/Desktop/flash.bin - 010 Editor
flash.bin
Workspace
Inspector
Find Results
Address Value
Output Find Results Find in Files Compare Histogram Checksum Process Disassembler
Opened file '/Users/joegrand/Desktop/flash.bin'.
Pos: 0 [0h] Val: 24 18h Size: 32,768 Hex ANSI LIT

UART

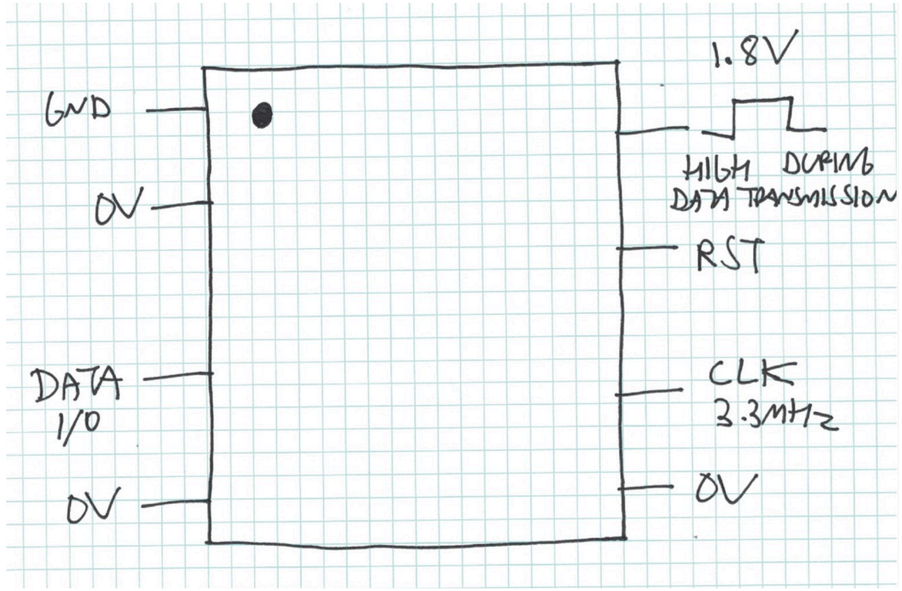
- Two UART interfaces available on Luat Air700E
  - MAIN_TXD/RXD: Connects to MCU @ 115.2kbps, 8N1
  - DBG_TXD/RXD: 115.2kbps then switches to 6Mbps for continuous output ala USB

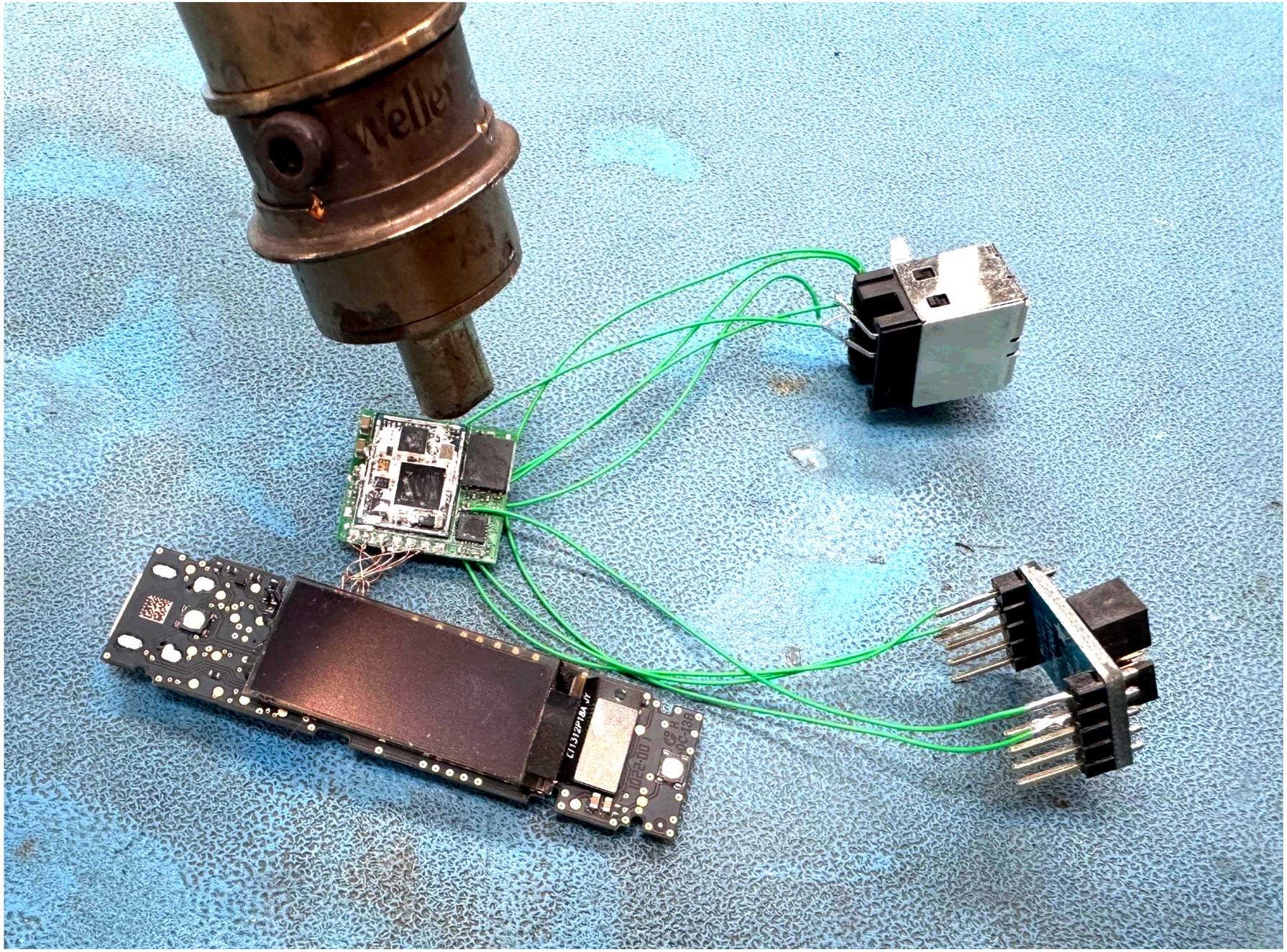


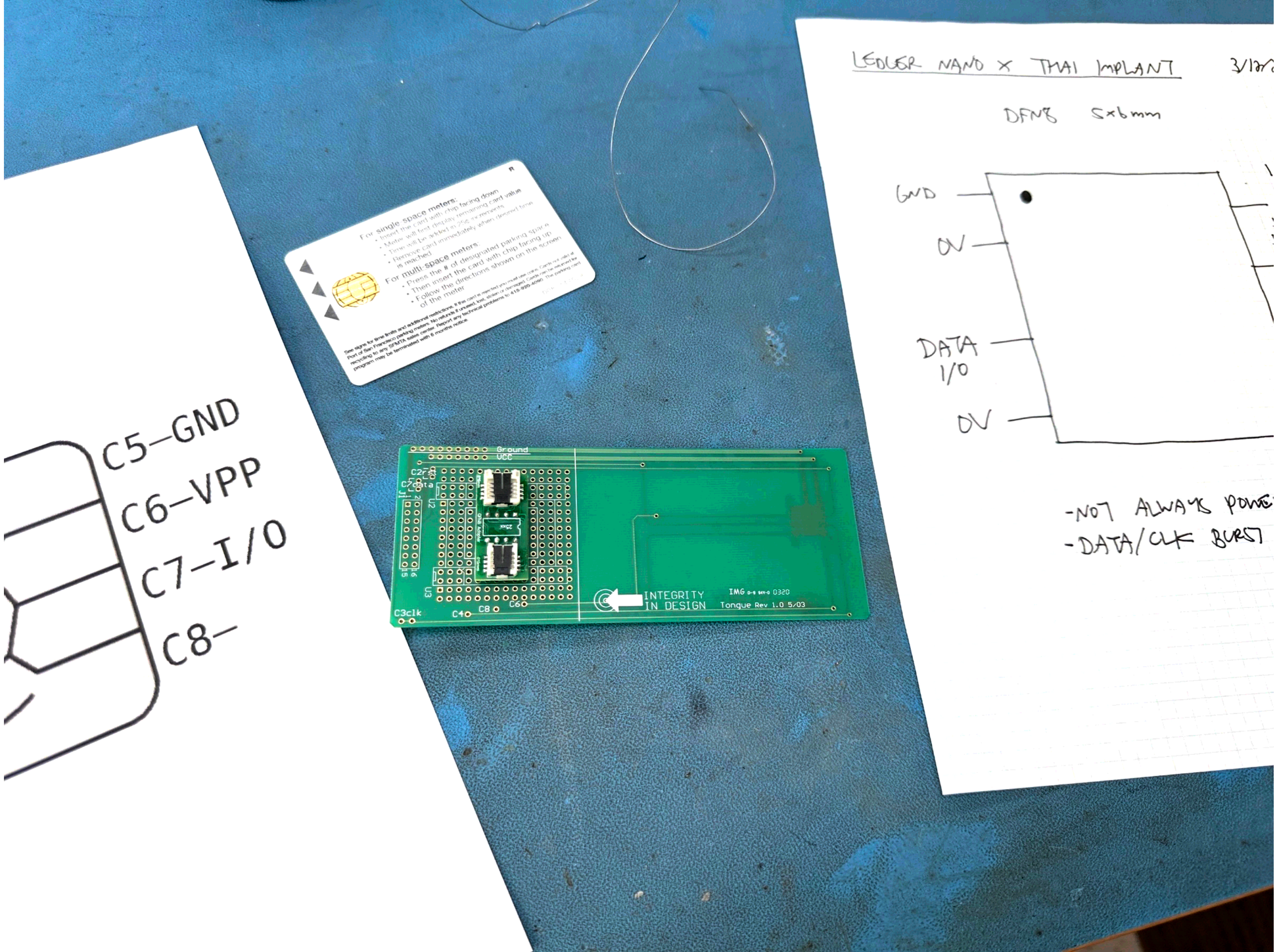

```
(E) Welcome to EiGENCOM D-Fota Time!
 ___       _____ ___ _____  _
| _ \     |  ___/ _ \_   _|/ \
||  \| -- | |_  || || | | / _ \
||_/| -- |  _| ||_|| | |/ ___ \
|___/    |_|   \___/ |_/_/   \_\

(C) Copyright 2020, All Rights Reserved.
(V) Version(2.5), Built @Jan 22 2024 17:20:56

uart(0) urc baud: 115200
total length(40):
[1/1] 6a790221864850f6b5d9022194f8a221944850f6afd9944b1d78002de9d1099b002be6d0d4f87e31
no par(0x5846) found!
exit...
bootloader flashXIPLimit(0x809978), try normal boot system start!
```

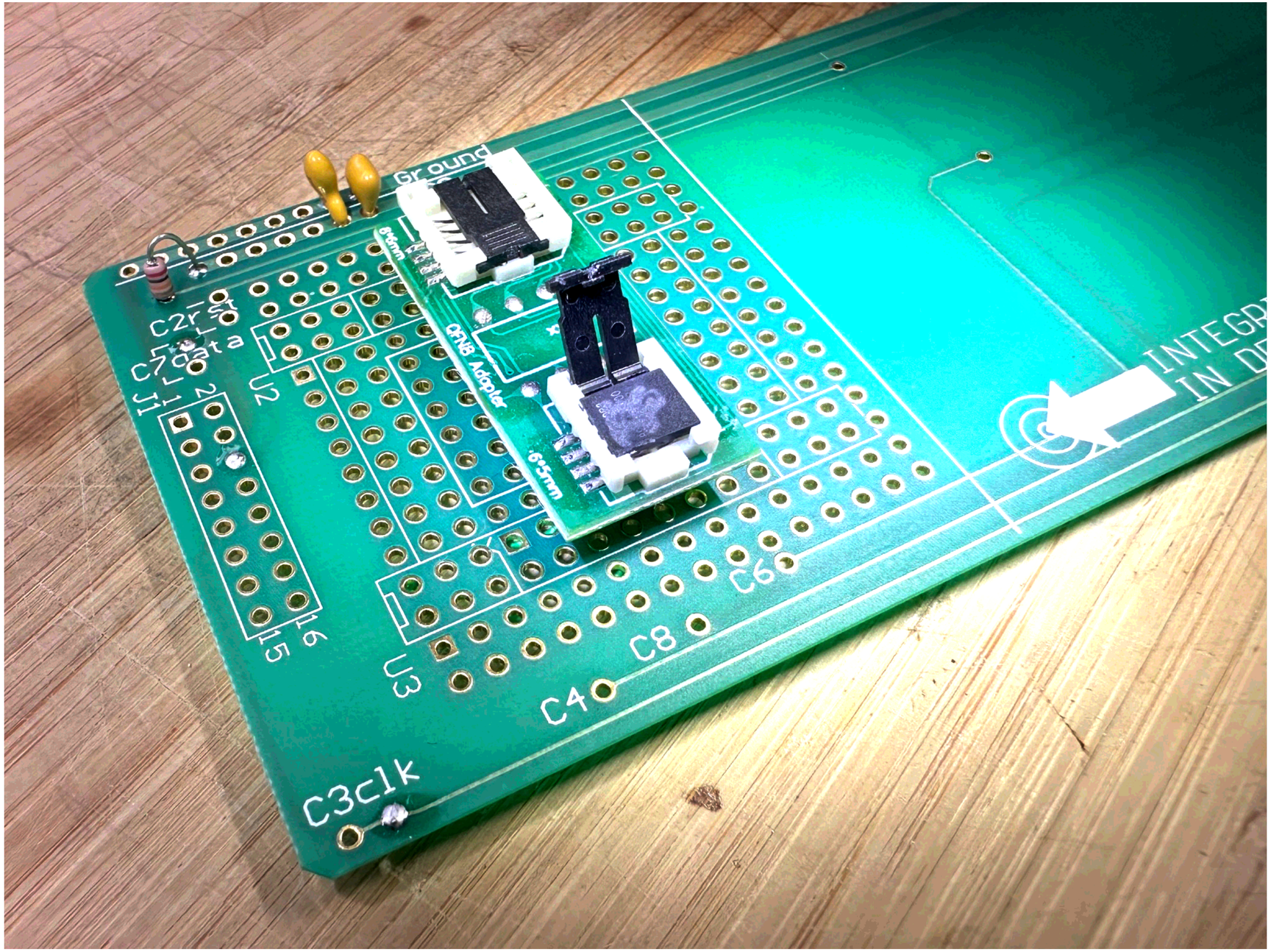
eSIM

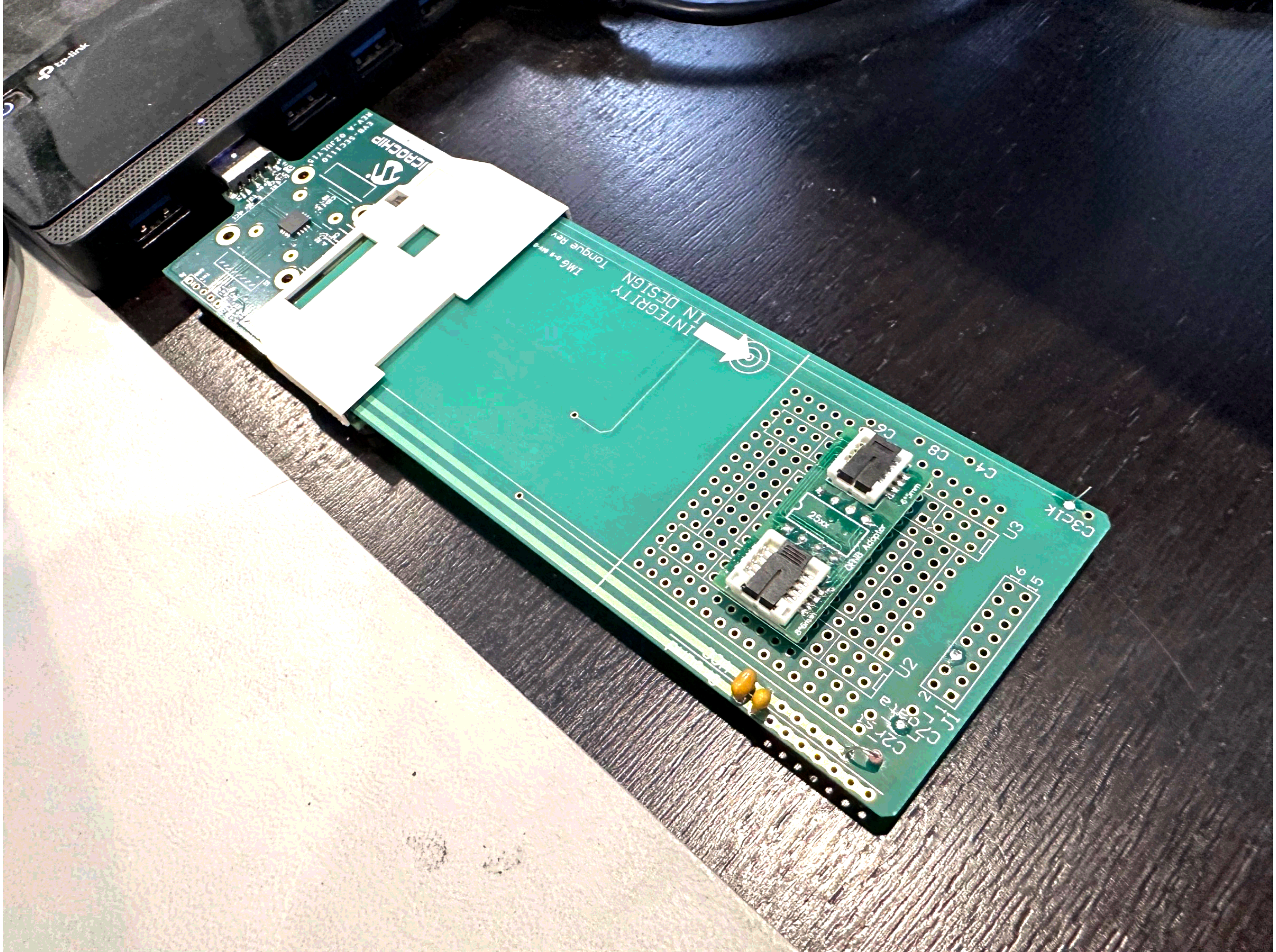
- Embedded Subscriber Identity Module
  - MFF2 (Machine Form Factor 2) ala DFN-8 5x6mm
  - Can communicate w/ it like a physical SIM card
- Microchip SEC1110 PC/SC evaluation board -> smartcard extender -> DFN-to-DIP adapter
- PySim

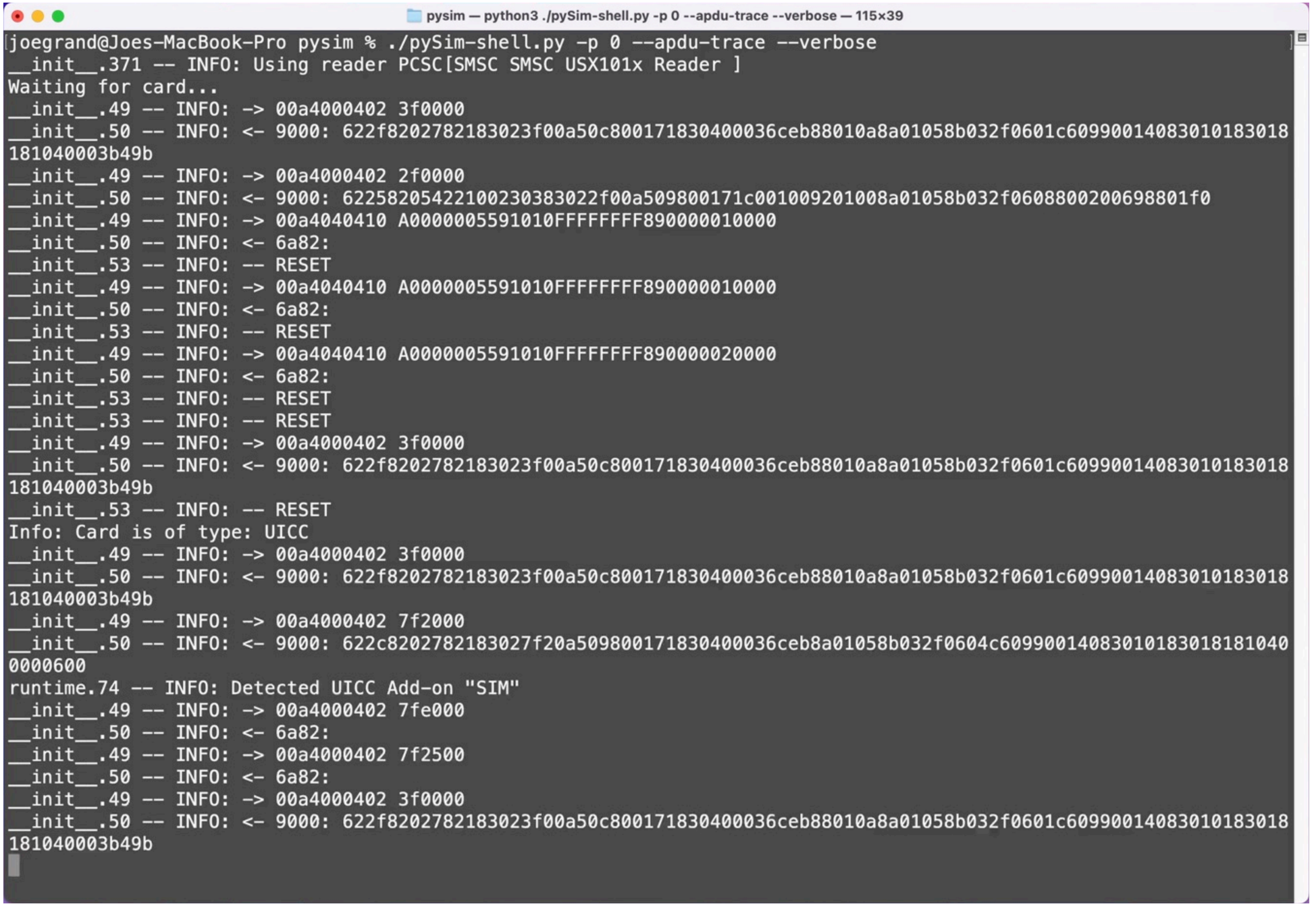


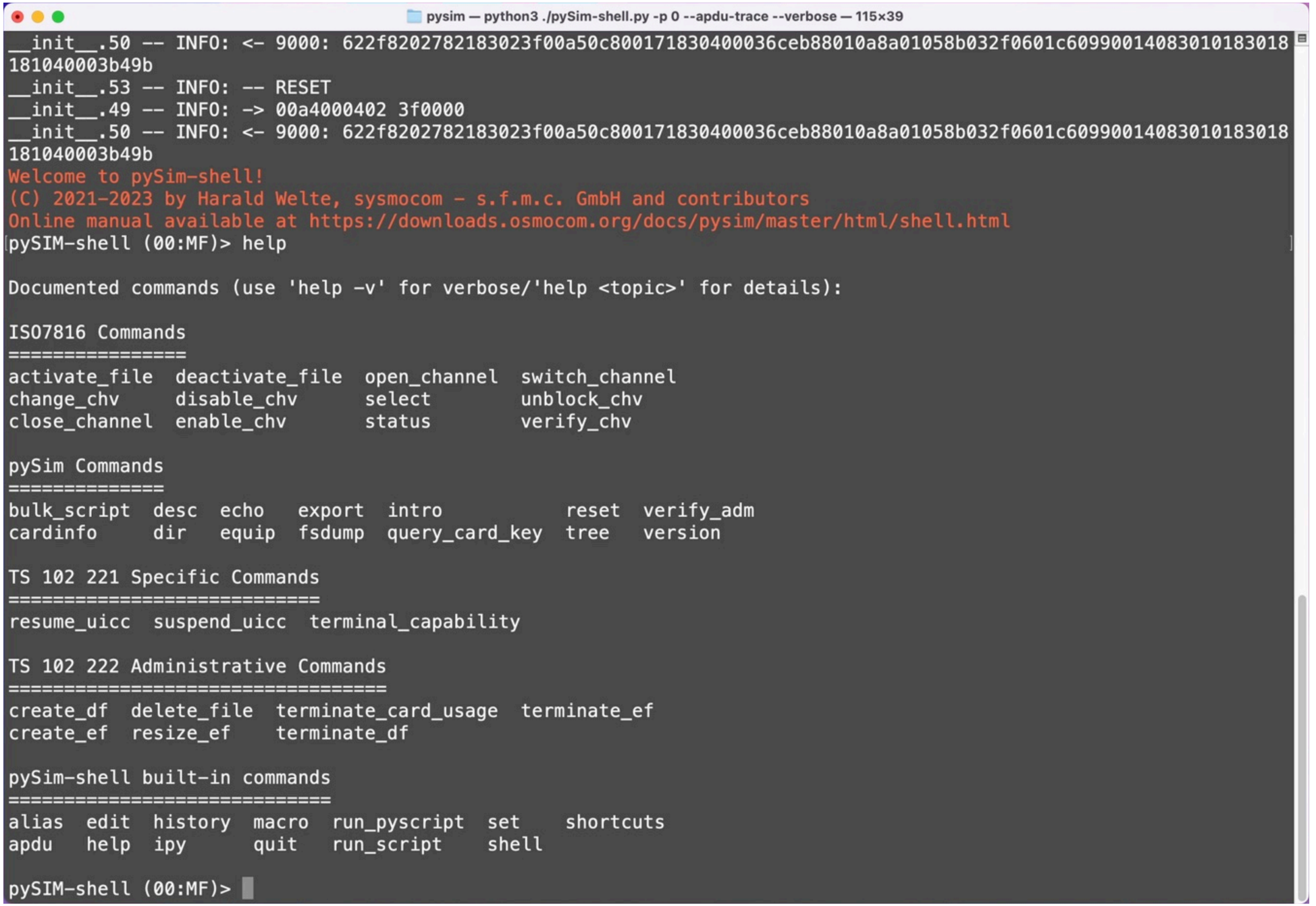

Weller


LEDGER NANO X THAI IMPLANT
DFN8 5x6mm
GND
0V
DATA I/O
0V
-NOT ALWAYS POWE
-DATA/CLK BURST
C5-GND
C6-VPP
C7-I/O
C8-
For single space meters:
For multi-space meters:
Ground
VCC
INTEGRITY IN DESIGN
Tongue Rev 1.0 5/03


Ground
C2r
C7
Data
J1
U2
U3
C3clk
C4
C8
C6
QFN8 Adapter
.65mm
.65mm


tp-link
INTEGRITY
IN DESIGN
Tongue Rev
C8
C4
U3
U2


pysim — python3 ./pySim-shell.py -p 0 --apdu-trace --verbose — 115×39
joegrand@Joes-MacBook-Pro pysim % ./pySim-shell.py -p 0 --apdu-trace --verbose
__init__.371 -- INFO: Using reader PCSC[SMSC SMSC USX101x Reader]
Waiting for card...
__init__.49 -- INFO: -> 00a4000402 3f0000
__init__.50 -- INFO: <- 9000: 622f8202782183023f00a50c80017183040003 6ceb88010a8a01058b032f0601c6099001 4083010183018
181040003b49b
__init__.49 -- INFO: -> 00a4000402 2f0000
__init__.50 -- INFO: <- 9000: 6225820542210023038302 2f00a509800171c001009201008a01058b032f0608800200698801f0
__init__.49 -- INFO: -> 00a4040410 A0000005591010FFFFFFFF890000010000
__init__.50 -- INFO: <- 6a82:
__init__.53 -- INFO: -- RESET
__init__.49 -- INFO: -> 00a4040410 A0000005591010FFFFFFFF890000010000
__init__.50 -- INFO: <- 6a82:
__init__.53 -- INFO: -- RESET
__init__.49 -- INFO: -> 00a4040410 A0000005591010FFFFFFFF890000020000
__init__.50 -- INFO: <- 6a82:
__init__.53 -- INFO: -- RESET
__init__.53 -- INFO: -- RESET
__init__.49 -- INFO: -> 00a4000402 3f0000
__init__.50 -- INFO: <- 9000: 622f8202782183023f00a50c80017183040003 6ceb88010a8a01058b032f0601c6099001 4083010183018
181040003b49b
__init__.53 -- INFO: -- RESET
Info: Card is of type: UICC
__init__.49 -- INFO: -> 00a4000402 3f0000
__init__.50 -- INFO: <- 9000: 622f8202782183023f00a50c80017183040003 6ceb88010a8a01058b032f0601c6099001 4083010183018
181040003b49b
__init__.49 -- INFO: -> 00a4000402 7f2000
__init__.50 -- INFO: <- 9000: 622c8202782183027f20a5098001718304000 36ceb8a01058b032f0604c6099001 4083010183018181040
0000600
runtime.74 -- INFO: Detected UICC Add-on "SIM"
__init__.49 -- INFO: -> 00a4000402 7fe000
__init__.50 -- INFO: <- 6a82:
__init__.49 -- INFO: -> 00a4000402 7f2500
__init__.50 -- INFO: <- 6a82:
__init__.49 -- INFO: -> 00a4000402 3f0000
__init__.50 -- INFO: <- 9000: 622f8202782183023f00a50c80017183040003 6ceb88010a8a01058b032f0601c6099001 4083010183018
181040003b49b


pysim — python3 ./pySim-shell.py -p 0 --apdu-trace --verbose — 115×39
__init__.50 -- INFO: <- 9000: 622f8202782183023f00a50c800171830400036ceb88010a8a01058b032f0601c60990014083010183018181040003b49b
__init__.53 -- INFO: -- RESET
__init__.49 -- INFO: -> 00a4000402 3f0000
__init__.50 -- INFO: <- 9000: 622f8202782183023f00a50c800171830400036ceb88010a8a01058b032f0601c60990014083010183018181040003b49b
Welcome to pySim-shell!
(C) 2021-2023 by Harald Welte, sysmocom - s.f.m.c. GmbH and contributors
Online manual available at https://downloads.osmocom.org/docs/pysim/master/html/shell.html
pySIM-shell (00:MF)> help
Documented commands (use 'help -v' for verbose/'help <topic>' for details):
ISO7816 Commands
activate_file deactivate_file open_channel switch_channel
change_chv disable_chv select unblock_chv
close_channel enable_chv status verify_chv
pySim Commands
bulk_script desc echo export intro reset verify_adm
cardinfo dir equip fsdump query_card_key tree version
TS 102 221 Specific Commands
resume_uicc suspend_uicc terminal_capability
TS 102 222 Administrative Commands
create_df delete_file terminate_card_usage terminate_ef
create_ef resize_ef terminate_df
pySim-shell built-in commands
alias edit history macro run_pyscript set shortcuts
apdu help ipy quit run_script shell
pySIM-shell (00:MF)>

pysim — python3 ./pySim-shell.py -p 0 --apdu-trace --verbose — 115×39

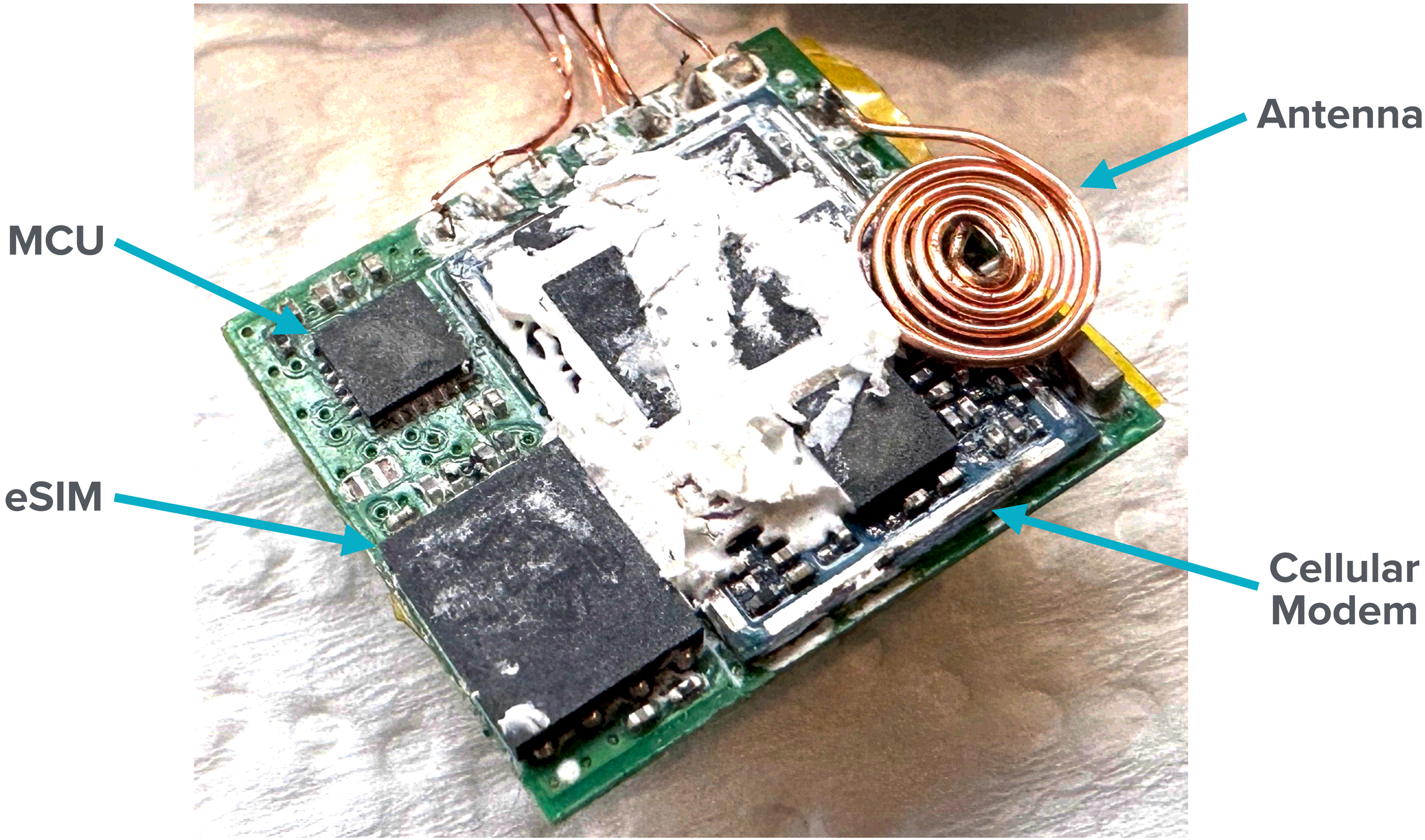
```
update_binary 0100050203ff
#
###############################################################################
# MF/DF.GSM/EF.IMSI                                                           #
###############################################################################
# directory: MF/DF.GSM/EF.IMSI (3f00/7f20/6f07)
# file: EF.IMSI (6f07)
# structure: transparent
# RAW FCP Template: 62388202412183026f07a520800171c001009101009a129b0ca0000000871002ffffffff899c026f079201008a01058
b036f060a800200098800
# Decoded FCP Template: {'file_descriptor': {'file_descriptor_byte': {'shareable': True, 'file_type': 'working_ef',
 'structure': 'transparent'}, 'record_len': None, 'num_of_rec': None}, 'file_identifier': b'o\x07', 'proprietary_in
formation': {'uicc_characteristics': b'q', 'special_file_info': {'high_update_activity': False, 'readable_and_updat
able_when_deactivated': False}, 'unknown_ber_tlv_ie_91': {'raw': '00'}, 'unknown_ber_tlv_ie_9_a': {'raw': '9b0ca000
0000871002ffffffff899c026f07'}, 'unknown_ber_tlv_ie_92': {'raw': '00'}}, 'life_cycle_status_integer': 'operational_
activated', 'security_attrib_referenced': {'ef_arr_file_id': b'o\x06', 'ef_arr_record_nr': 10}, 'file_size': 9, 'sh
ort_file_identifier': None}
select MF/DF.GSM/EF.IMSI
update_binary 082940401738767429
#
###############################################################################
# MF/DF.GSM/EF.Kc                                                             #
###############################################################################
# directory: MF/DF.GSM/EF.Kc (3f00/7f20/6f20)
# file: EF.Kc (6f20)
# structure: transparent
# RAW FCP Template: 62408202412183026f20a528800171c001009101009a149b0ca0000000871002ffffffff899c045f3b4f20920100930
4000000018a01058b036f0603800200098800
# Decoded FCP Template: {'file_descriptor': {'file_descriptor_byte': {'shareable': True, 'file_type': 'working_ef',
 'structure': 'transparent'}, 'record_len': None, 'num_of_rec': None}, 'file_identifier': b'o ', 'proprietary_infor
mation': {'uicc_characteristics': b'q', 'special_file_info': {'high_update_activity': False, 'readable_and_updatabl
e_when_deactivated': False}, 'unknown_ber_tlv_ie_91': {'raw': '00'}, 'unknown_ber_tlv_ie_9_a': {'raw': '9b0ca000000
0871002ffffffff899c045f3b4f20'}, 'unknown_ber_tlv_ie_92': {'raw': '00'}, 'unknown_ber_tlv_ie_93': {'raw': '00000001
'}}, 'life_cycle_status_integer': 'operational_activated', 'security_attrib_referenced': {'ef_arr_file_id': b'o\x06
', 'ef_arr_record_nr': 3}, 'file_size': 9, 'short_file_identifier': None}
select MF/DF.GSM/EF.Kc
update_binary ffffffffffffff07
#
```

Card info:
Name: UICC
ATR: 3b9e96801fc78031e073fe211b66d0024421150072
ICCID: 89314404001365967271
Class-Byte: 00
Select-Ctrl: 0004
AIDs: a0000000871002

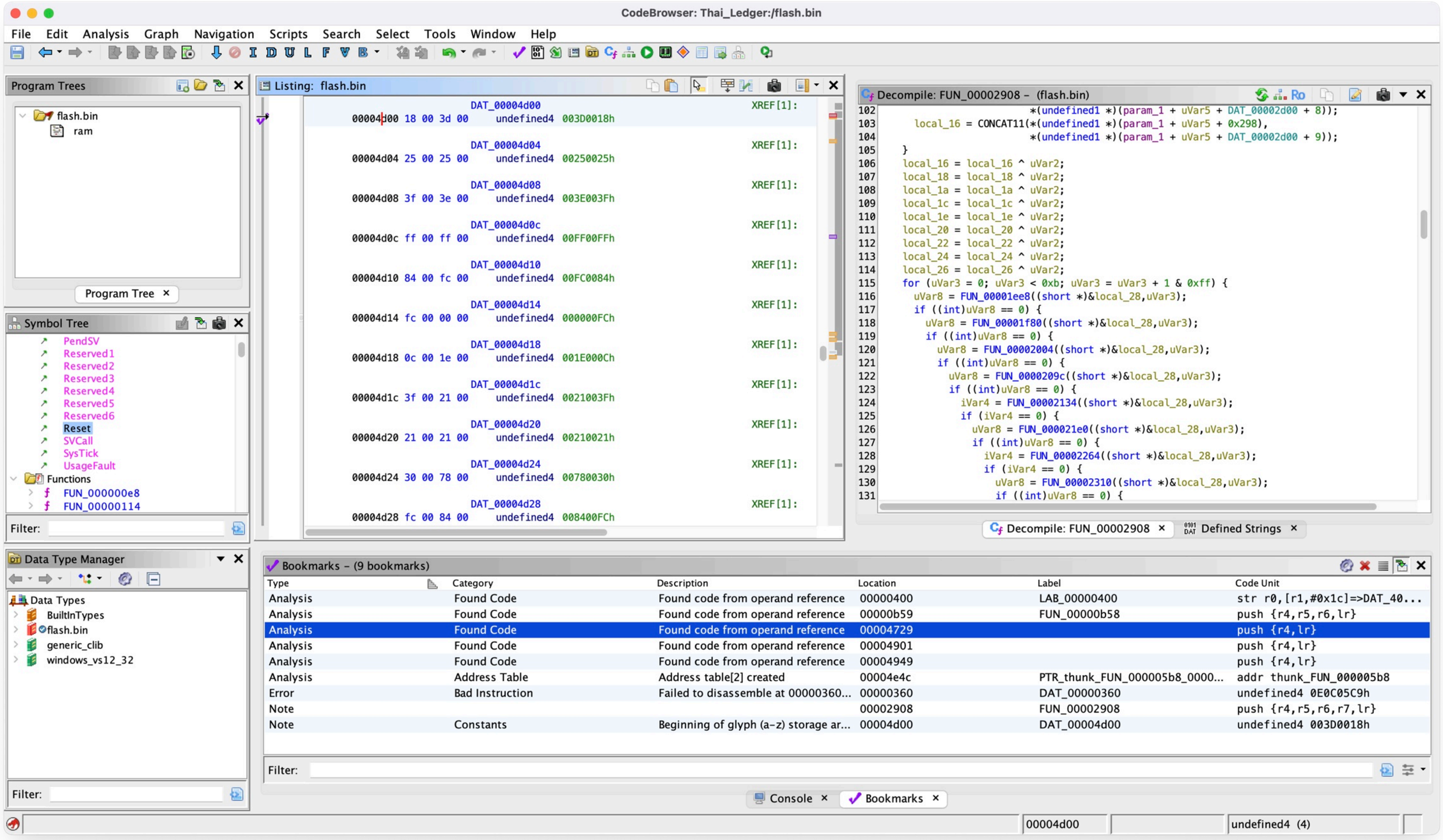
IMSI (subscriber identity): 082940401738767429
MCC: 204 (Netherlands)
MNC: 04 (Vodafone NL)
MSIN: 01738767429

Service Provider Name (EF.SPN): 0044415441204F4E4C59 ("DATA ONLY")
SMS Parameters (EF.SMSP): "Vodafone"

EF.EPSLOCI -> Philippines (Smart, 515-03)
EF.LOCIGPRS -> USA (T-Mobile, 310-260)


Antenna
MCU
eSIM
Cellular
Modem

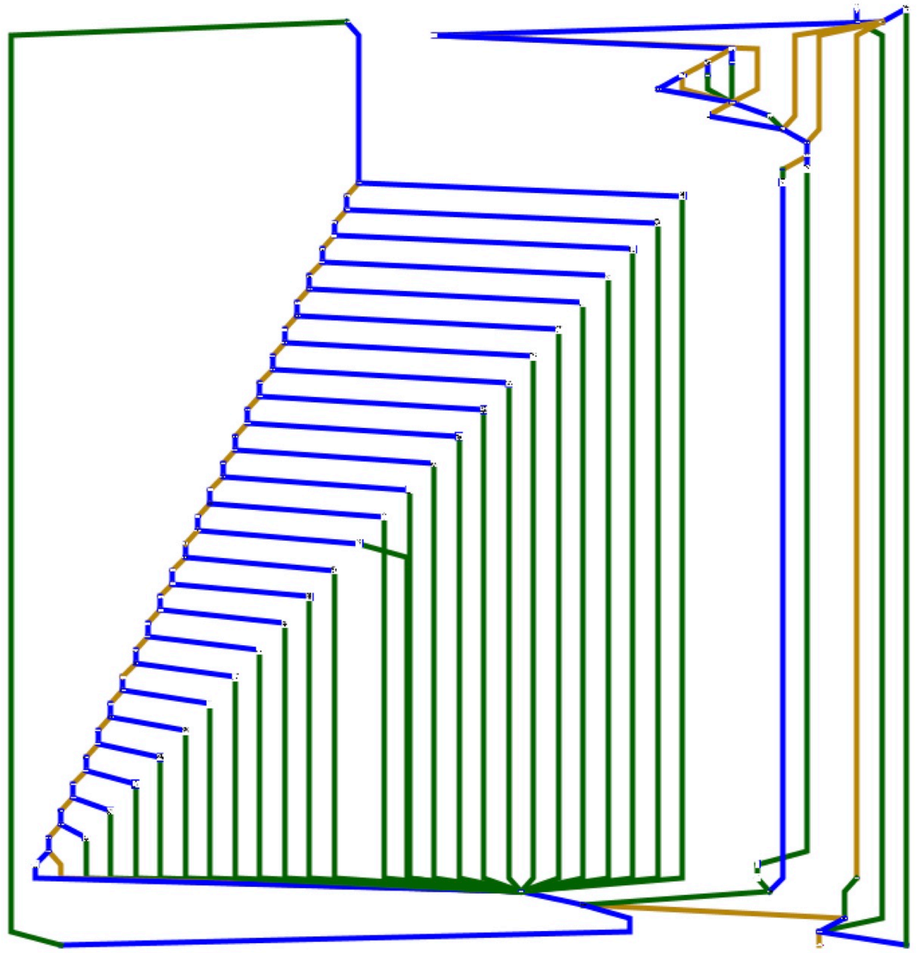
FW REVERSE ENGINEERING (MCU)

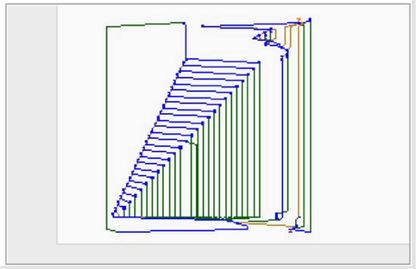

CodeBrowser: Thai_Ledger:/flash.bin
File Edit Analysis Graph Navigation Scripts Search Select Tools Window Help
Program Trees
flash.bin
ram
Program Tree
Symbol Tree
PendSV
Reserved1
Reserved2
Reserved3
Reserved4
Reserved5
Reserved6
Reset
SVCall
SysTick
UsageFault
Functions
FUN_000000e8
FUN_00000114
Filter:
Data Type Manager
Data Types
BuiltInTypes
flash.bin
generic_clib
windows_vs12_32
Filter:
Listing: flash.bin
DAT_00004d00 XREF[1]:
00004d00 18 00 3d 00 undefined4 003D0018h
DAT_00004d04 XREF[1]:
00004d04 25 00 25 00 undefined4 00250025h
DAT_00004d08 XREF[1]:
00004d08 3f 00 3e 00 undefined4 003E003Fh
DAT_00004d0c XREF[1]:
00004d0c ff 00 ff 00 undefined4 00FF00FFh
DAT_00004d10 XREF[1]:
00004d10 84 00 fc 00 undefined4 00FC0084h
DAT_00004d14 XREF[1]:
00004d14 fc 00 00 00 undefined4 000000FCh
DAT_00004d18 XREF[1]:
00004d18 0c 00 1e 00 undefined4 001E000Ch
DAT_00004d1c XREF[1]:
00004d1c 3f 00 21 00 undefined4 0021003Fh
DAT_00004d20 XREF[1]:
00004d20 21 00 21 00 undefined4 00210021h
DAT_00004d24 XREF[1]:
00004d24 30 00 78 00 undefined4 00780030h
DAT_00004d28 XREF[1]:
00004d28 fc 00 84 00 undefined4 008400FCh
Decompile: FUN_00002908 - (flash.bin)
*(undefined1 *)(param_1 + uVar5 + DAT_00002d00 + 8));
local_16 = CONCAT11(*(undefined1 *)(param_1 + uVar5 + 0x298),
*(undefined1 *)(param_1 + uVar5 + DAT_00002d00 + 9));
}
local_16 = local_16 ^ uVar2;
local_18 = local_18 ^ uVar2;
local_1a = local_1a ^ uVar2;
local_1c = local_1c ^ uVar2;
local_1e = local_1e ^ uVar2;
local_20 = local_20 ^ uVar2;
local_22 = local_22 ^ uVar2;
local_24 = local_24 ^ uVar2;
local_26 = local_26 ^ uVar2;
for (uVar3 = 0; uVar3 < 0xb; uVar3 = uVar3 + 1 & 0xff) {
uVar8 = FUN_00001ee8((short *)&local_28,uVar3);
if ((int)uVar8 == 0) {
uVar8 = FUN_00001f80((short *)&local_28,uVar3);
if ((int)uVar8 == 0) {
uVar8 = FUN_00002004((short *)&local_28,uVar3);
if ((int)uVar8 == 0) {
uVar8 = FUN_0000209c((short *)&local_28,uVar3);
if ((int)uVar8 == 0) {
iVar4 = FUN_00002134((short *)&local_28,uVar3);
if (iVar4 == 0) {
uVar8 = FUN_000021e0((short *)&local_28,uVar3);
if ((int)uVar8 == 0) {
iVar4 = FUN_00002264((short *)&local_28,uVar3);
if (iVar4 == 0) {
uVar8 = FUN_00002310((short *)&local_28,uVar3);
if ((int)uVar8 == 0) {
Decompile: FUN_00002908
Defined Strings
Bookmarks - (9 bookmarks)
Type Category Description Location Label Code Unit
Analysis Found Code Found code from operand reference 00000400 LAB_00000400 str r0,[r1,#0x1c]=>DAT_40...
Analysis Found Code Found code from operand reference 00000b59 FUN_00000b58 push {r4,r5,r6,lr}
Analysis Found Code Found code from operand reference 00004729 push {r4,lr}
Analysis Found Code Found code from operand reference 00004901 push {r4,lr}
Analysis Found Code Found code from operand reference 00004949 push {r4,lr}
Analysis Address Table Address table[2] created 00004e4c PTR_thunk_FUN_000005b8_0000... addr thunk_FUN_000005b8
Error Bad Instruction Failed to disassemble at 00000360... 00000360 DAT_00000360 undefined4 0E0C05C9h
Note 00002908 FUN_00002908 push {r4,r5,r6,r7,lr}
Note Constants Beginning of glyph (a-z) storage ar... 00004d00 DAT_00004d00 undefined4 003D0018h
Filter:
Console
Bookmarks
00004d00
undefined4 (4)

Graph [Call Graph: (Entire Program), Code Flow Graph: FUN_00002908] [CodeBrowser: Thai_Ledger:/flash.bin]

Edit Help

Code Flow Graph: FUN_00002908





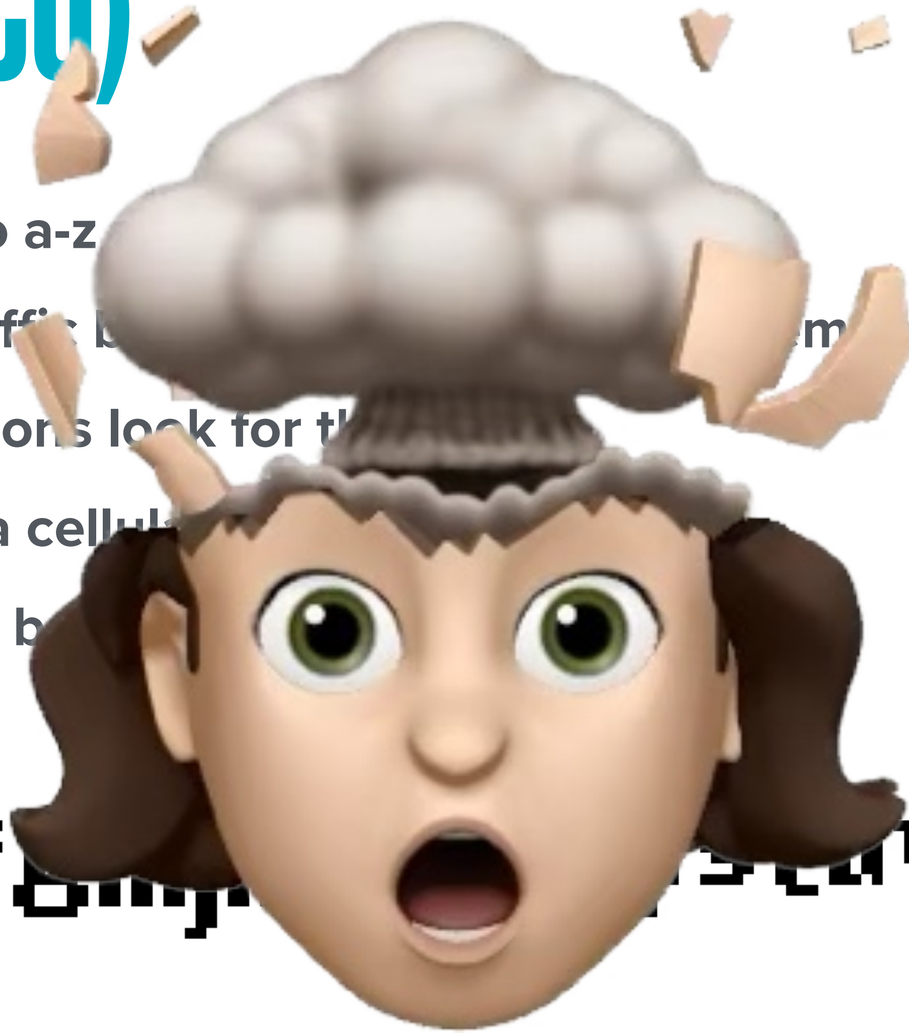
Call Graph: (Entire Pr... × Code Flow Graph: FUN_0... ×

FIRMWARE (MCU)

- Glyphs corresponding to a-z stored at 0x4d00-0x4e40
- Implant monitors SPI traffic between Nano X Secure Element and OLED
- Template matcher functions look for the glyphs
- Contents transmitted via cellular module
  - Recovery seed/wallet backup

FIRMWARE (MCU)

- Glyphs corresponding to a-z
- Implant monitors SPI traffic b[illegible]t and OLED
- Template matcher functions look for t[illegible]
- Contents transmitted via cellu[illegible]
  - Recovery seed/wallet b[illegible]



abcdefghijklmnopqrstuvwxyz

FINAL WORDS

FUTURE WORK

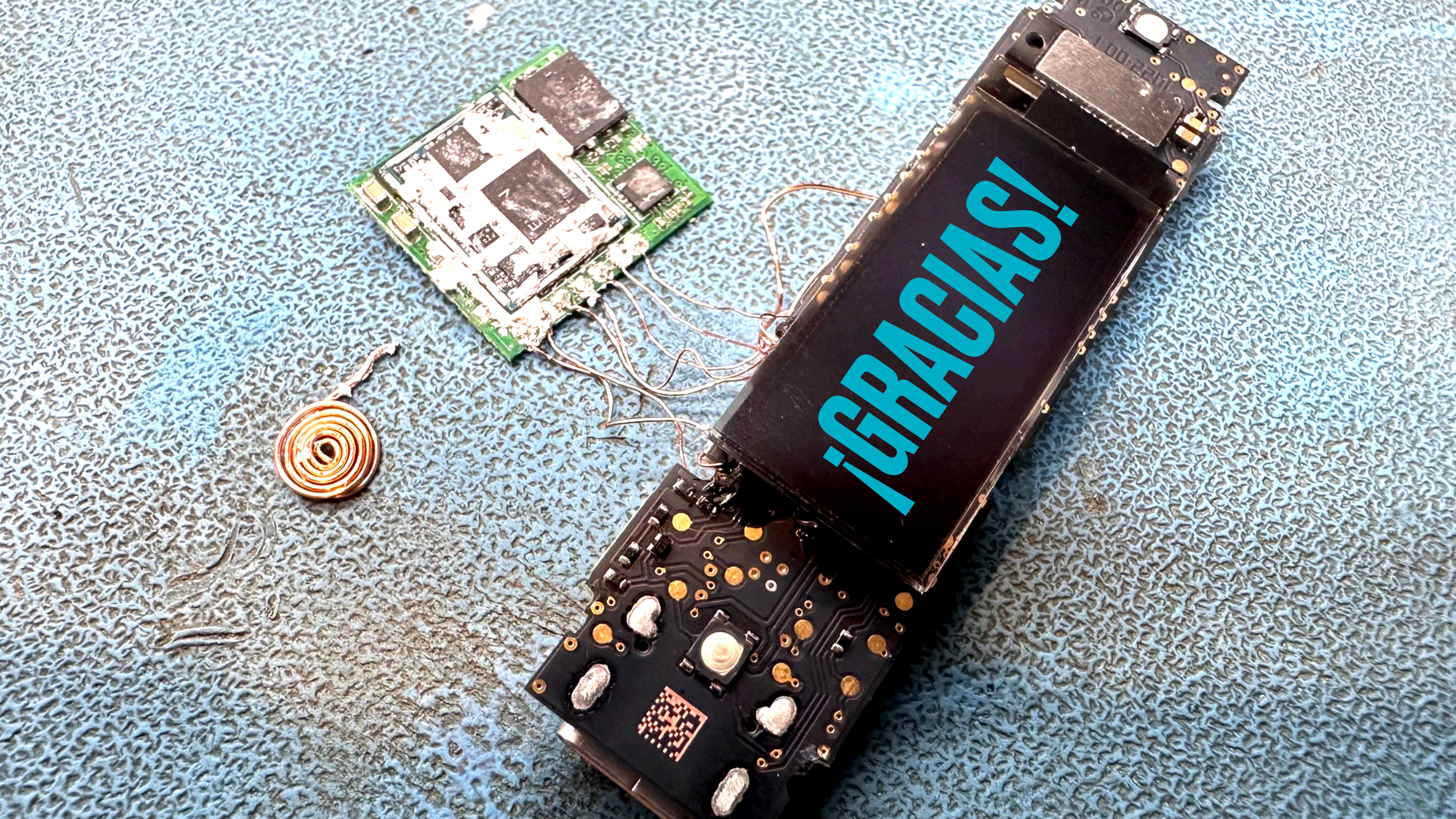
- More FW reverse engineering
- Explore MCU <-> Air700E UART interface
- Monitor / MITM cellular transmissions
  - srsRAN 4G + SignalSDR Pro
- Learn more about the adversary
  - Who, what, where, how successful the attack has been

LEDGER

- Check hardware integrity against known-good pictures
- Follow best practices when buying a device
  - Directly from Ledger or authorized resellers
- Ledger is looking into further hardening for future products
  - Nano Gen5 has a sealed unibody for tamper evidence

SUMMARY

- Risks of hardware espionage and supply chain attacks are real
- The Ledger Nano X hardware implant exfiltrates data displayed on the screen
  - Monitors the OLED's SPI bus, detects letters used in recovery seed, transmits over 4G LTE
  - New iteration of implant has already been spotted


¡GRACIAS!