

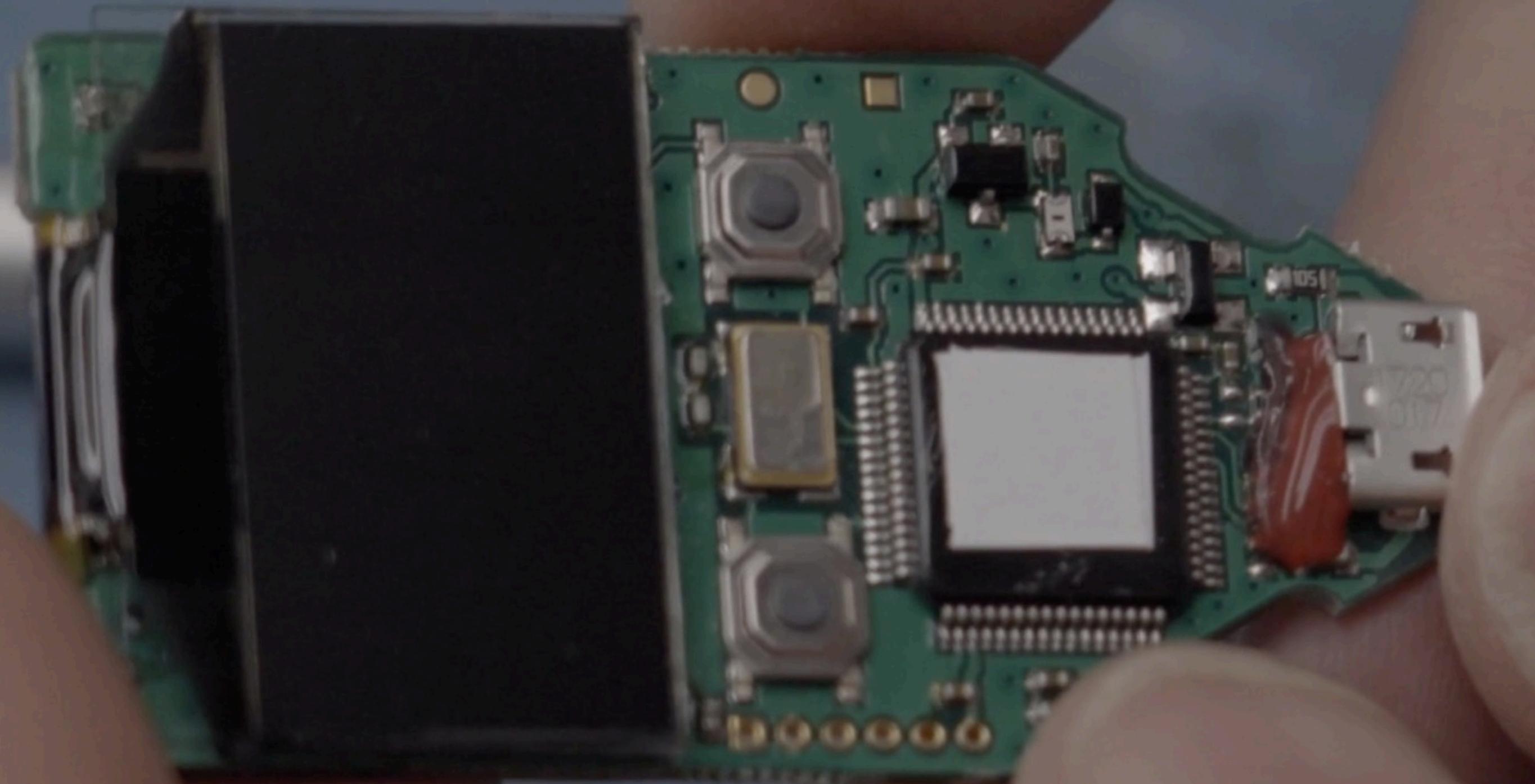
JOE GRAND'S ADVENTURES OF WALLET HACKING

HACKINBO[®]
Winter 2025 Edition

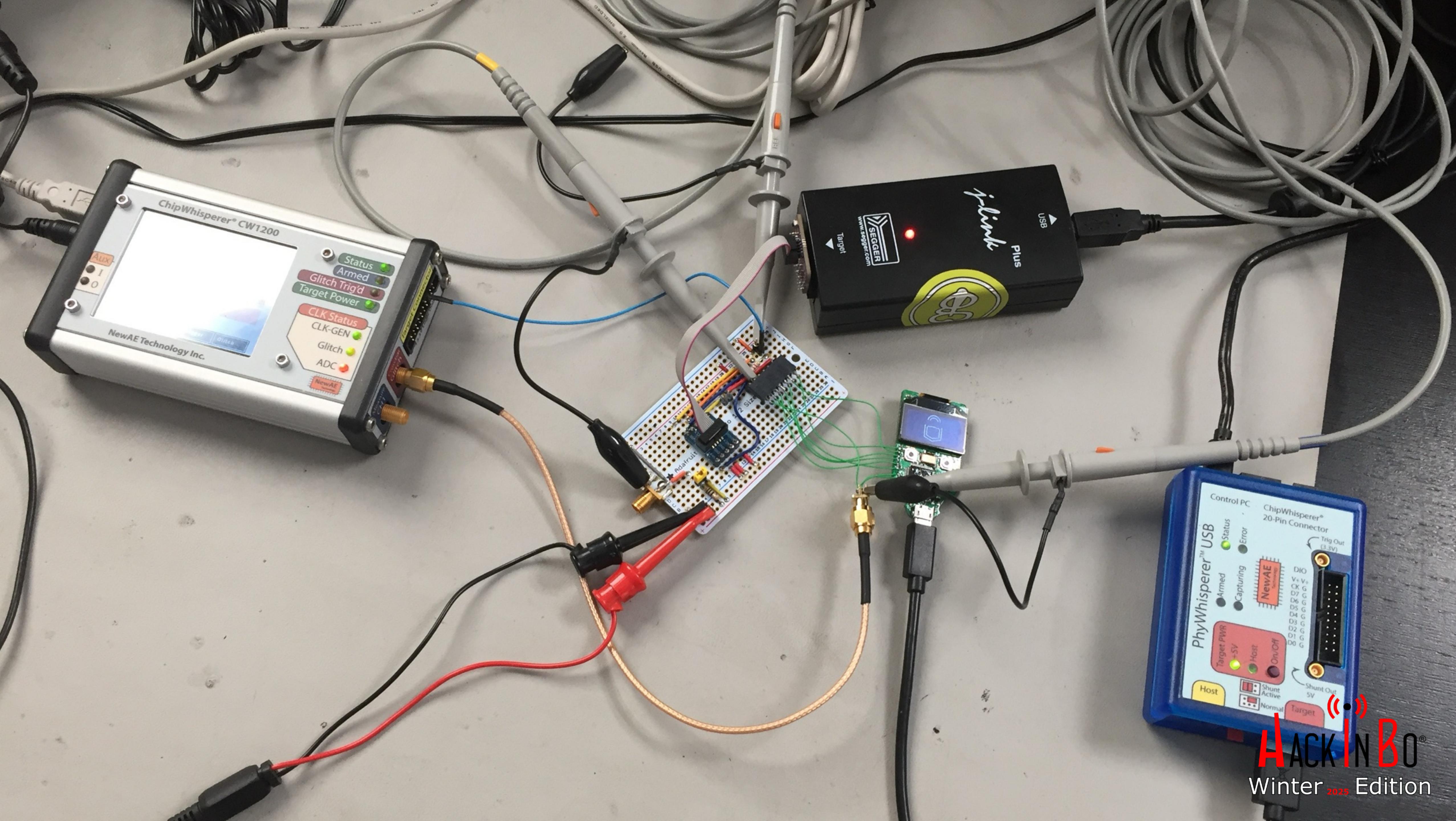
25^a EDIZIONE



HACKINBO®
Winter 2025 Edition

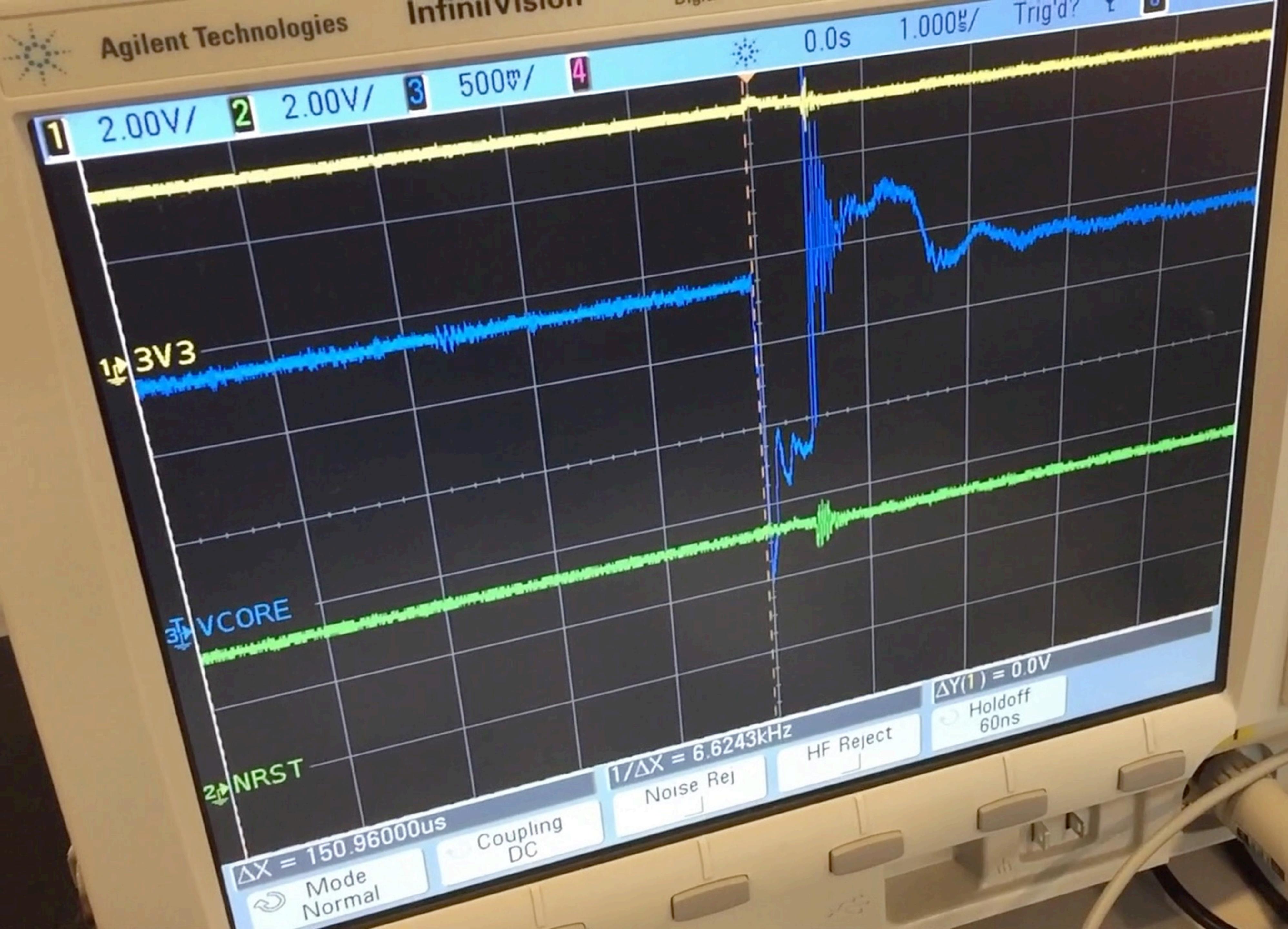


HACKINBO®
Winter 2025 Edition



HACKINBO®

Winter 2025 Edition



Home Page - Select or create a × Tribble - Jupyter Notebook × +

http://localhost:8888/notebooks/Tribble.ipynb

jupyter Tribble Last Checkpoint: 5 hours ago (unsaved changes) Logout

File Edit View Insert Cell Kernel Widgets Help Trusted Python 3

Run

ERROR:pylink.jlink:STM32: Connecting to CPU via connect under reset failed.

ERROR:pylink.jlink:STM32: Connecting to CPU via connect under reset failed.

ERROR:pylink.jlink:STM32: Connecting to CPU via connect under reset failed.

ERROR:pylink.jlink:STM32: Connecting to CPU via connect under reset failed.

ERROR:pylink.jlink:STM32: Connecting to CPU via connect under reset failed.

Step 2: Extract RAM Contents

On Trezor One firmware versions <= 1.6.0, the critical metadata (recovery seed + PIN) are stored in RAM on power-up. We can now use OpenOCD to extract the contents.

In [9]:

```
1 # Close PyLink to give control of Segger back to OS
2 jlink.close()
```

In [10]:

```
1 # Launch OpenOCD to extract RAM
2 # openocd -f interface/jlink.cfg -c "transport select swd" -f target/stm32f2x.cfg -c "init" -c "dump_image SRAM.bin"
3 result = subprocess.run(['openocd', '-f', 'openocd_swd_trezor.cfg'], capture_output=True, text=True)
4 print(result.stderr)
```

Open On-Chip Debugger 0.11.0-rc2+dev-00006-gf68ade529-dirty (2021-02-03-18:32)
Licensed under GNU GPL v2
For bug reports, read
<http://openocd.org/doc/doxygen/bugs.html>
Info : J-Link V9 compiled Dec 13 2019 11:14:50
Info : Hardware version: 9.30
Info : VTARGET = 3.319 V
Info : clock speed 1000 kHz
Info : SWD DPIDR 0x2ba01477
Info : stm32f2x.cpu: hardware has 6 breakpoints, 4 watchpoints
Error: stm32f2x.cpu -- clearing lockup after double fault
Polling target stm32f2x.cpu failed, trying to reexamine
Info : stm32f2x.cpu: hardware has 6 breakpoints, 4 watchpoints
Info : starting gdb server for stm32f2x.cpu on 3333
Info : Listening on port 3333 for gdb connections

In []:

```
1 # Display any printable ASCII data within the extracted binary
2 result = subprocess.run(['strings', 'SRAM.bin'], capture_output=True, text=True)
3 print(result.stdout)
```

HACKINBO®
Winter 2025 Edition

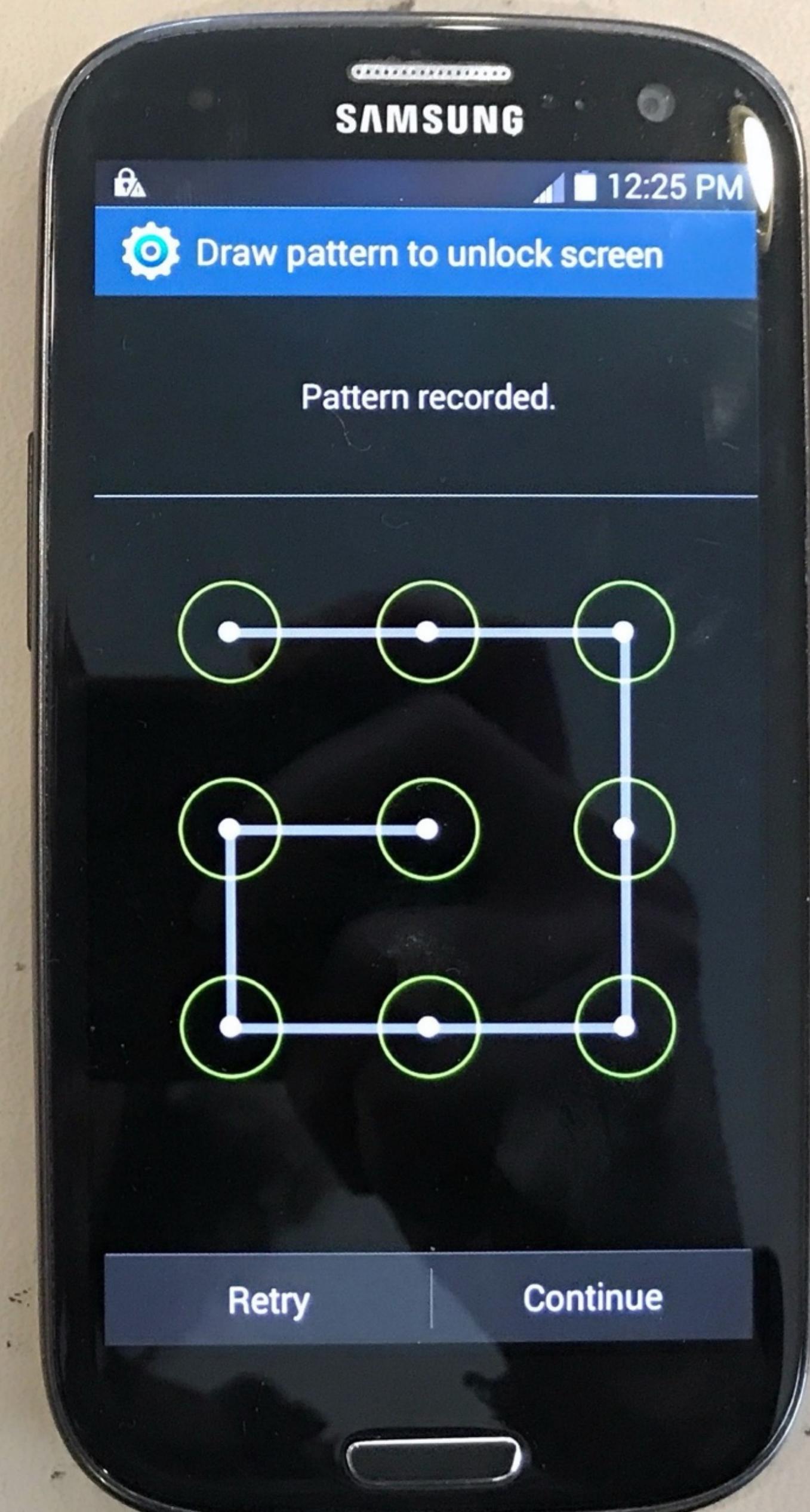
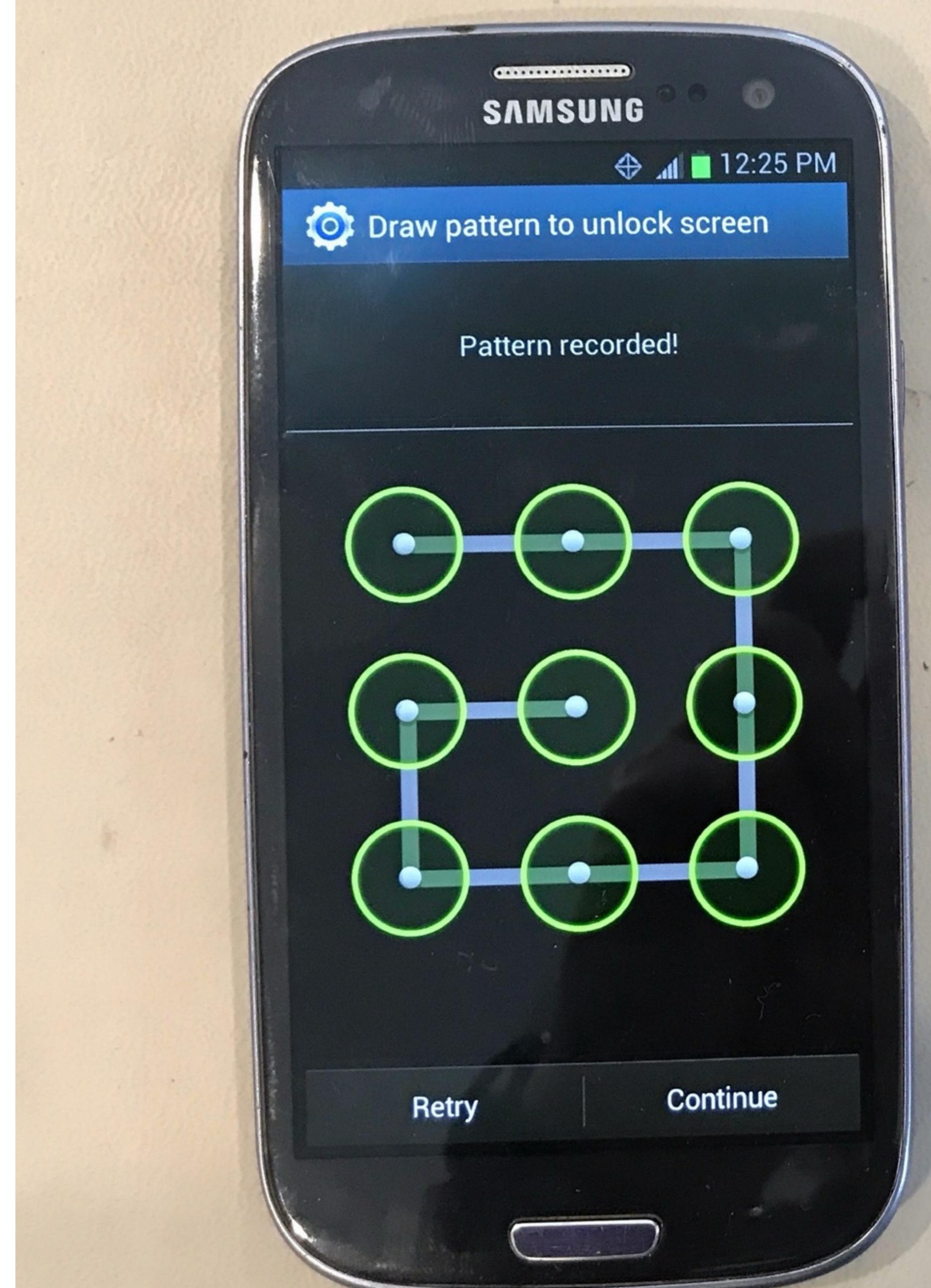
```
Info : stm32f2x.cpu: hardware has 6 breakpoints, 4 watchpoints
Info : starting gdb server for stm32f2x.cpu on 3333
Info : Listening on port 3333 for gdb connections
```

```
In [11]: 1 # Display any printable ASCII data within the extracted binary
          2 result = subprocess.run(['strings', 'SRAM.bin'], capture_output=True)
          3 print(result.stdout)

12514
jl trezor
XXXXXXXXXX
F74113D4B4F08319871F9120
"2:.&
```



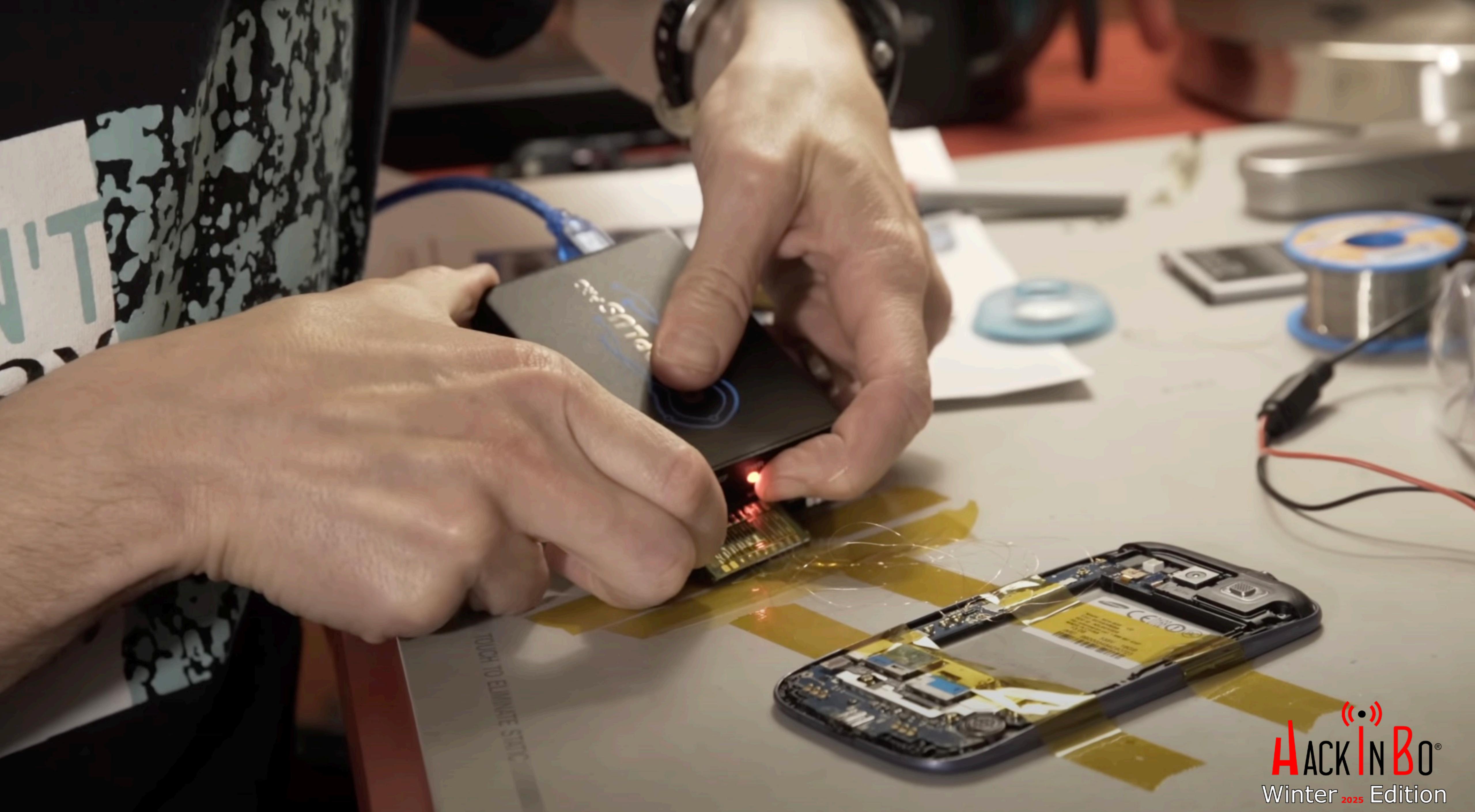
HACKINBO[®]
Winter 2025 Edition



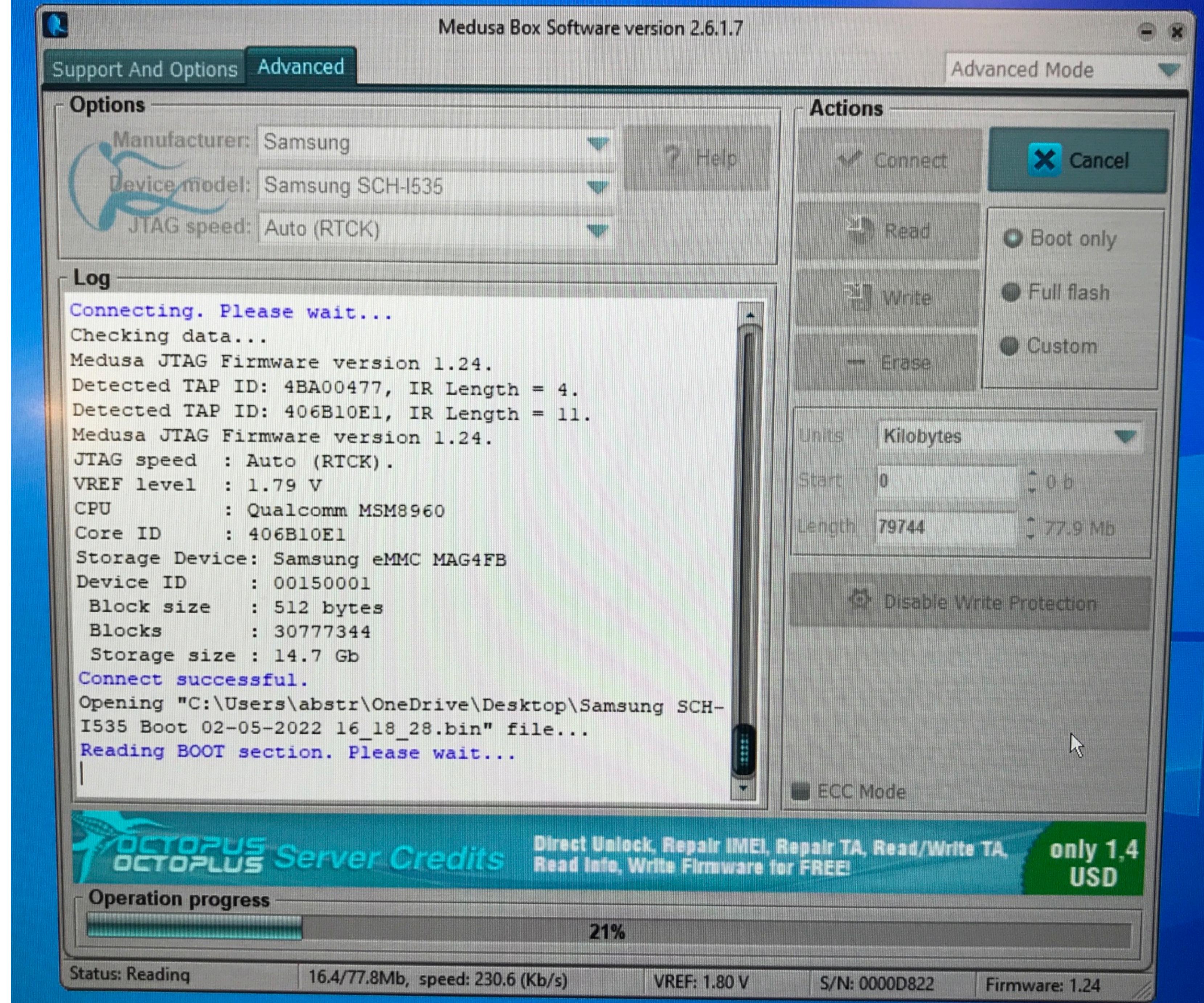
TOUCH TO ELIMINATE STATIC | TOUCH TO ELIMINATE STATIC



HACKINBO®
Winter 2025 Edition



HACKINBO®
Winter 2025 Edition



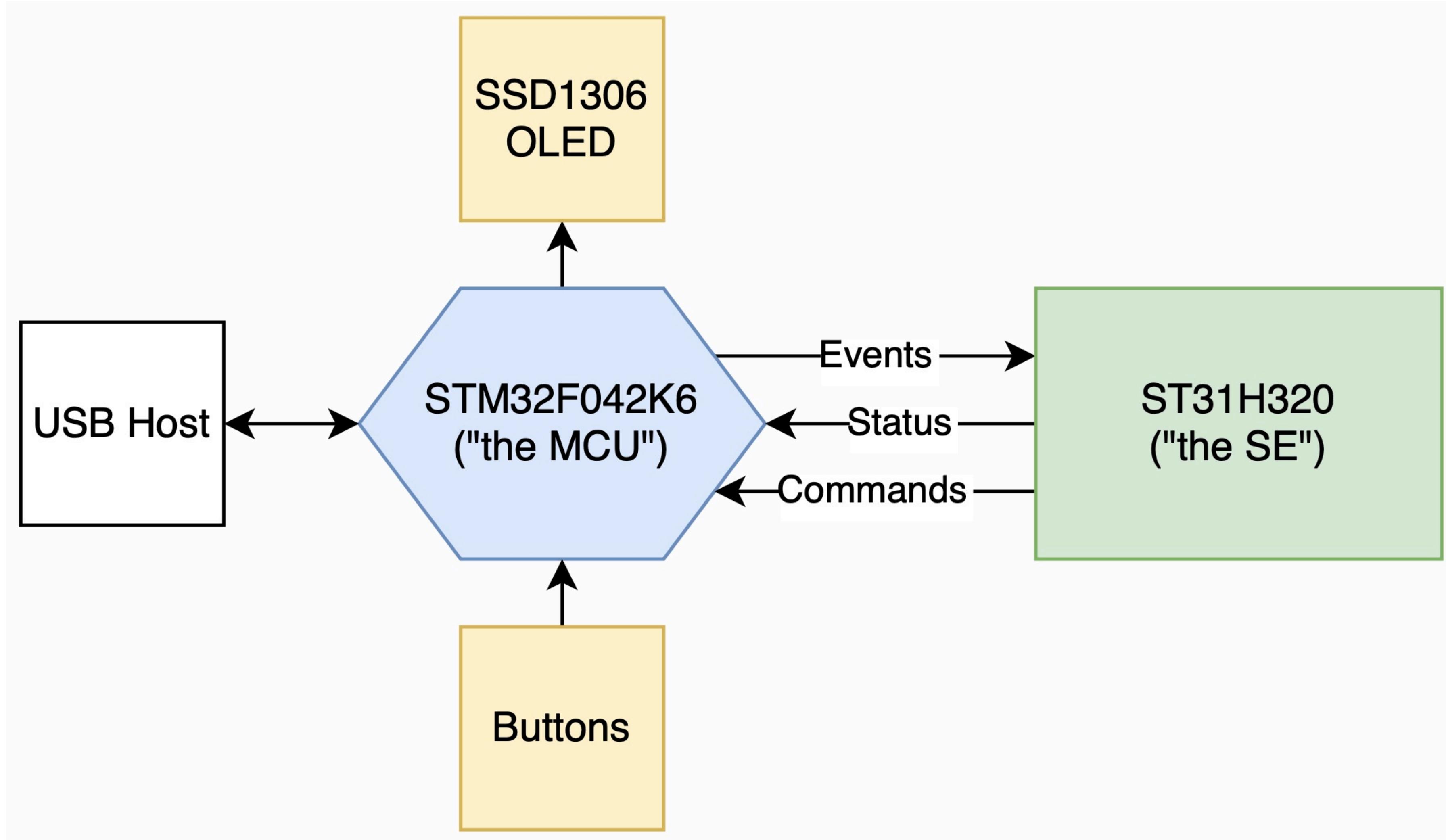


HACKINBO®
Winter 2025 Edition

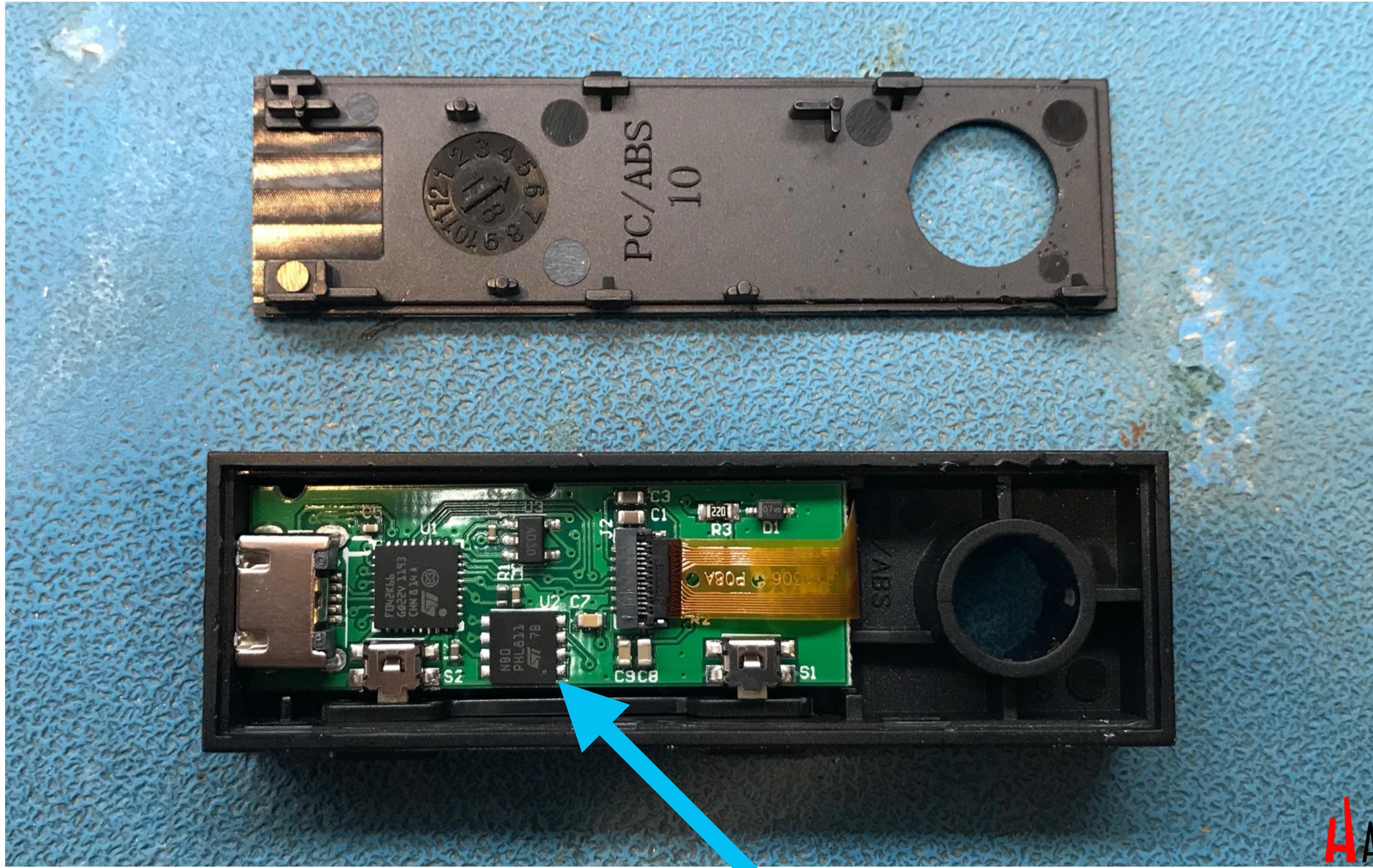




HACKINBO®
Winter 2025 Edition



SALEEM RACHID: BREAKING THE LEDGER SECURITY MODEL

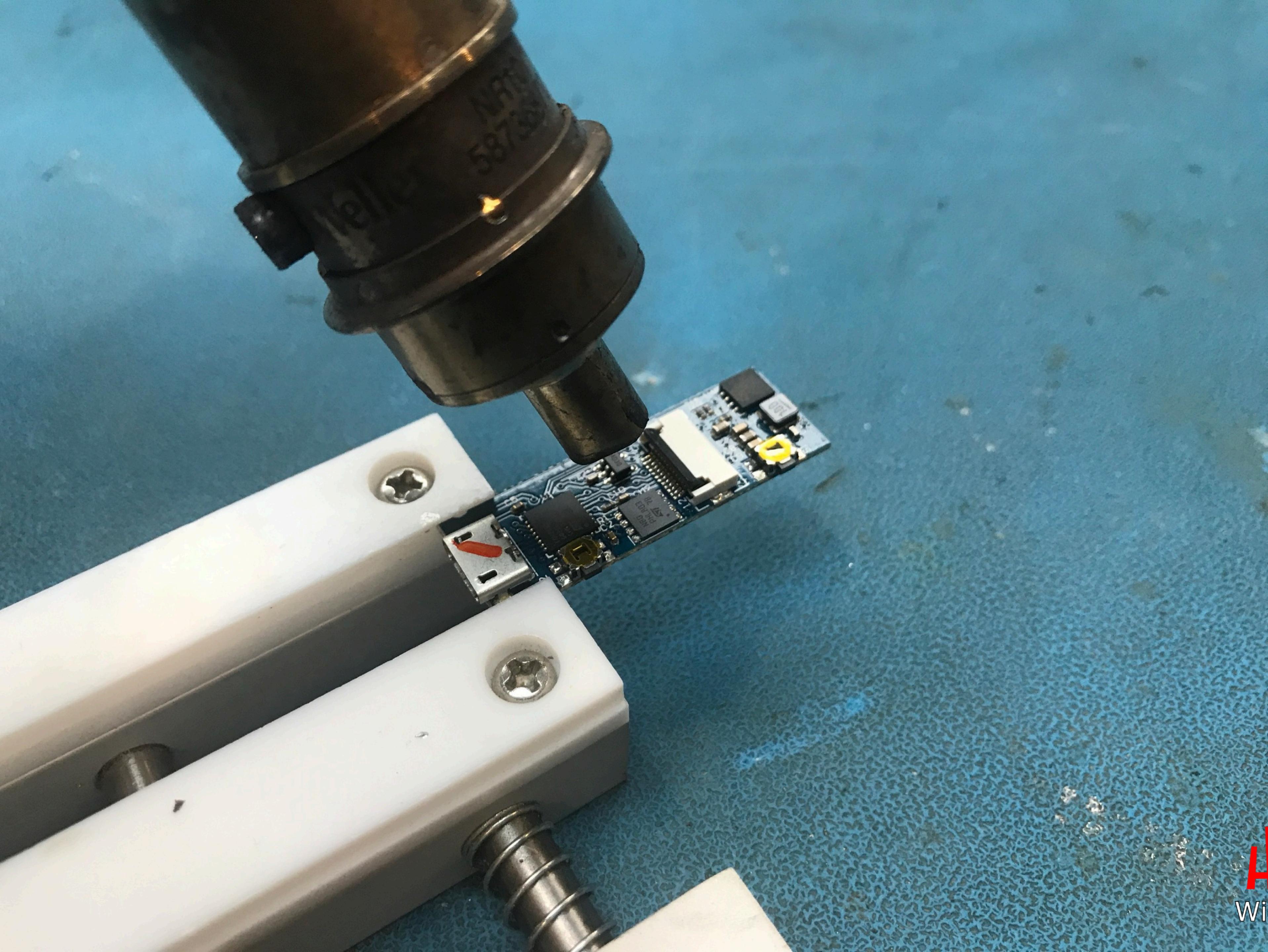




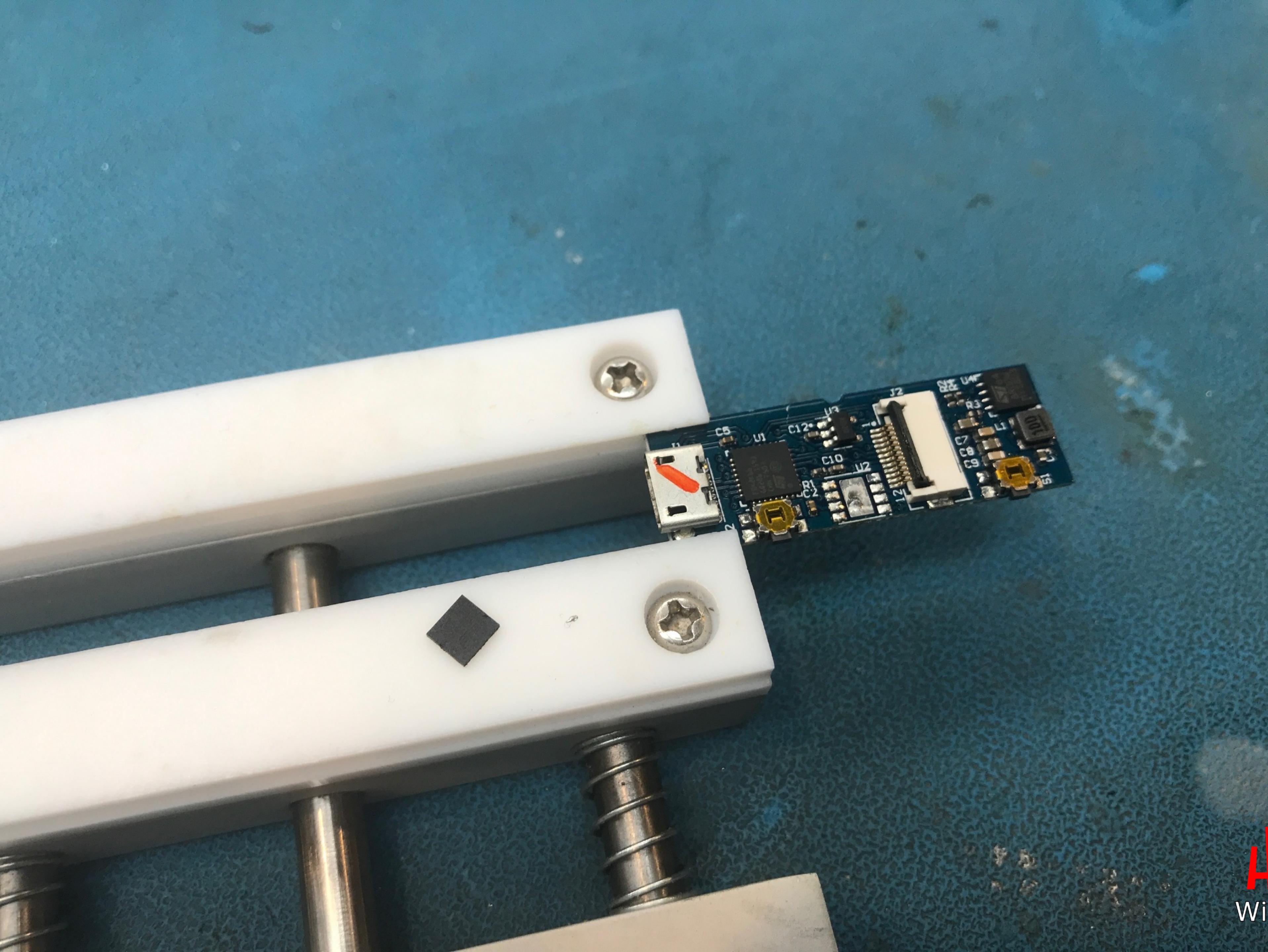
HACKINBO®
Winter 2025 Edition



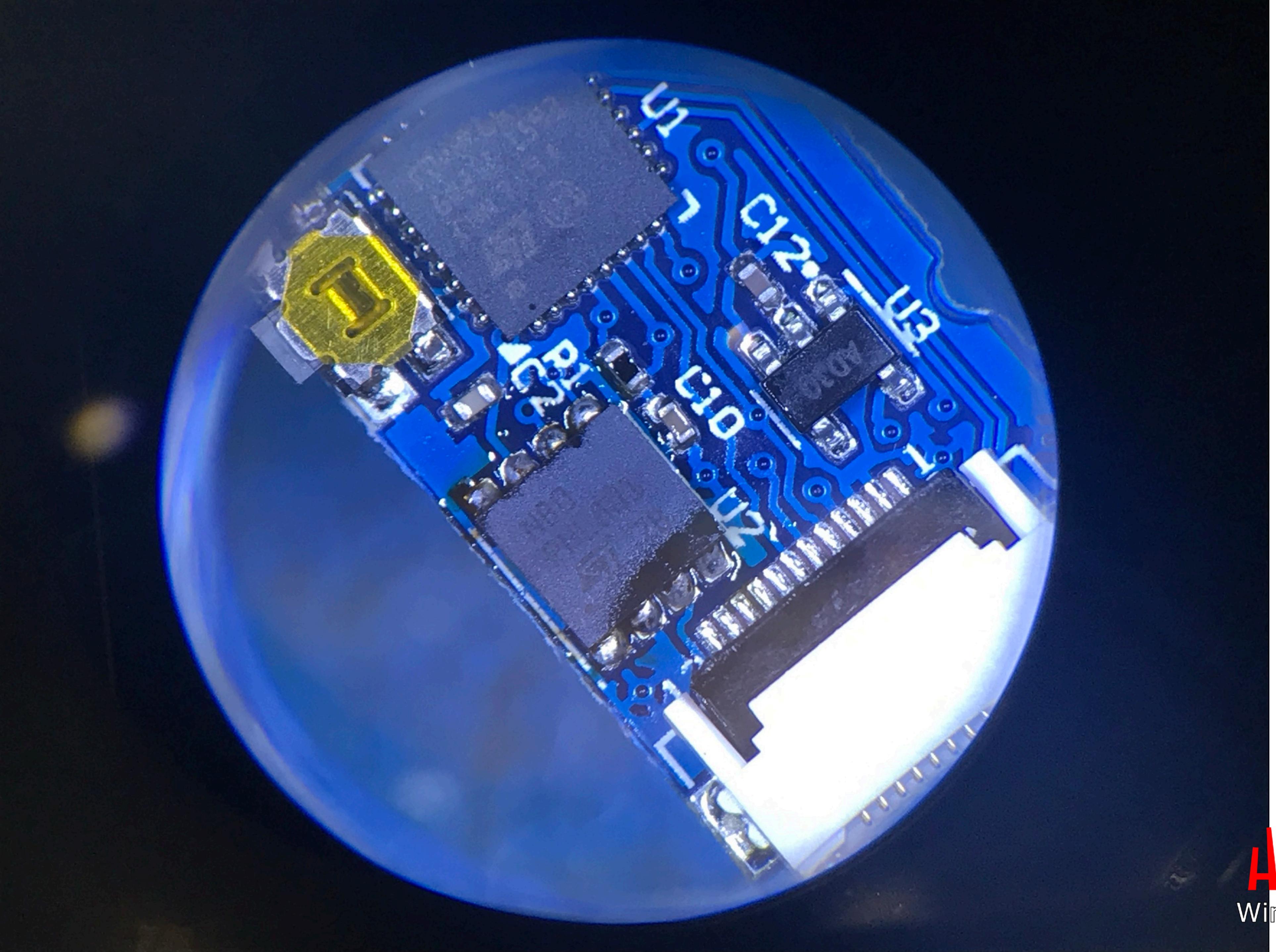
HACKINBO®
Winter 2025 Edition



HACKINBO®
Winter 2025 Edition



HACKINBO®
Winter 2025 Edition



HACKINBO®
Winter 2025 Edition





HACKINBO®
Winter 2025 Edition

Eee PC



American Megatrends

AMIBIOS (C) 2009 American Megatrends, Inc.
ASUS 1005HA ACPI BIOS Revision 1102
CPU : Intel(R) Atom(TM) CPU N270 @ 1.60GHz
Speed : 1.60 GHz

Press ESC for BBS POPUP

Press F9 for image recovery

Press ALT+F2 to execute ASUS EZ Flash

DDRII-533/CL4, Single-Channel Mode

Initializing USB Controllers .. Done.

1016MB OK (Installed Memory Size:1024MB)

USB Device(s) : 1 Storage Device

Auto-Detecting Pri Master..IDE Hard Disk

Pri Master: Hitachi HTS543216L9SA00 FB20C40C

Ultra DMA Mode-5, S.M.A.R.T. Capable and Status OK

Hard Disk locked, enter user password:

(Press <ESC> to switch to Master Password)



1988528 20582 Solar

HACKINBO®
Winter 2025 Edition

Eee PC

BIOS SETUP UTILITY

Main Advanced Security Boot Exit

Security Settings

Supervisor Password :Not Installed
User Password :Not Installed

<Enter> to change password.
<Enter> again to disable password.

Change Supervisor Password

Hard Disk Security

Primary Master HDD Password Status :Enabled
Primary Master HDD User Password
Primary Master HDD Master Password

↔ Select Screen
↑↓ Select Item
Enter Change
F1 General Help
F10 Save and Exit
ESC Exit

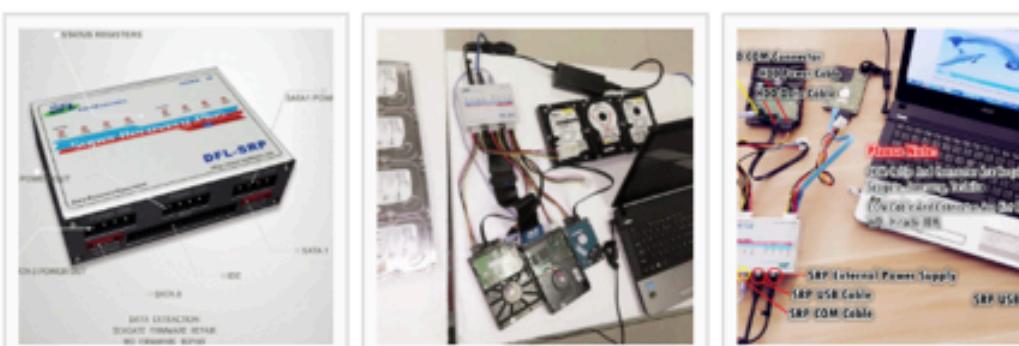
v02.58 (C) Copyright 1985-2009, American Megatrends, Inc.

Manufacturer MAX From Hunan, China

HRS1005LH2110250062

ESC F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 Pause Break Prt Sc Insert Delete Num LK Scr LK

HACKINBO®
Winter 2025 Edition



DFL-SRP All-In-One USB3.0 Data Recovery Equipment

 (339 customer reviews)

Categories: [Data Recovery Hardware](#), [Featured Data Recovery Tools](#), [HDD Firmware Repair & Data Recovery Equipment](#) Tags: [data recovery equipment](#), [data recovery hardware](#), [usb3.0 data recovery tool](#)

Description Reviews (339)

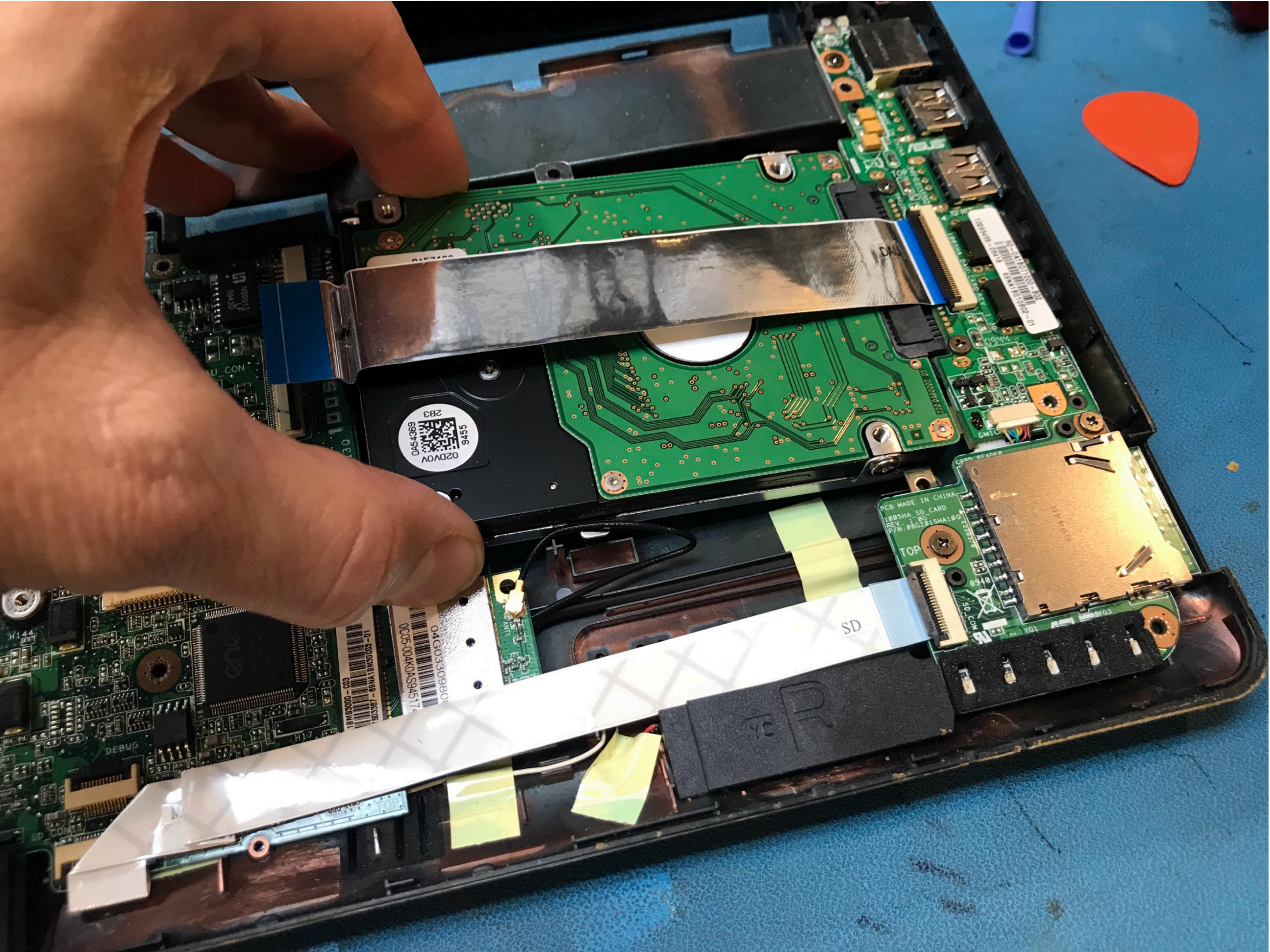
Description

DFL-SRP All-In-One USB3.0 Data Recovery Equipment is the world's top data recovery equipment supporting all hard drive brands (Seagate, WD, Hitachi/IBM, Samsung, Toshiba, Fujitsu) on **logical data recovery, bad sector data recovery, repairing bad sectors, editing models, editing SN and capacities, password removal, reset smart, repairing firmware failures, updating firmware, repairing undetected and busy hard drives and getting lost data back.**

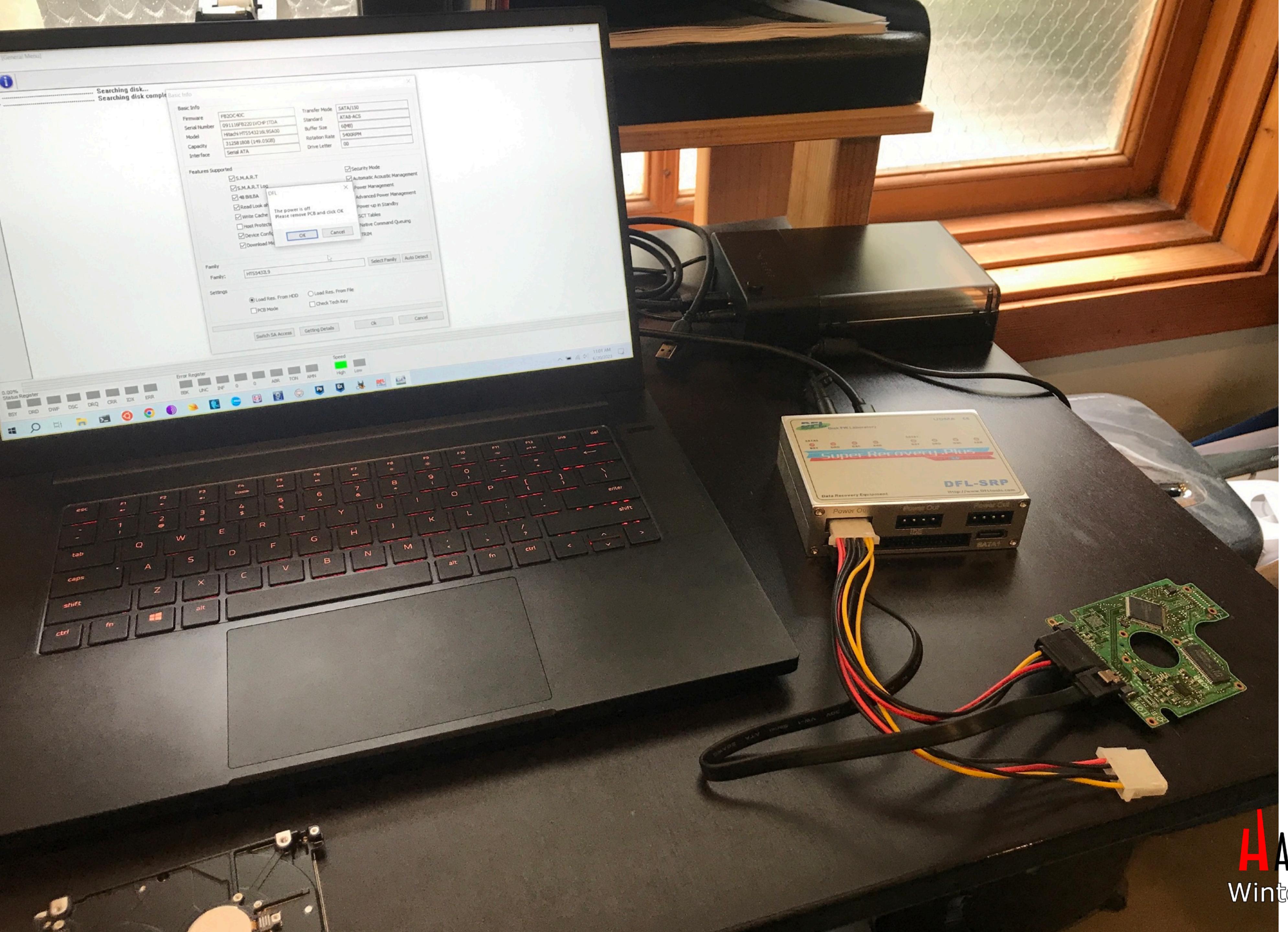
DFL-SRP=DFL-Super Recovery Plus and it's one real professional and cost-effective data recovery equipment from Dolphin Data Lab supporting data recovery from three faulty hard drives at the same time with independent channels at high speed.

DFL-SRP All-In-One USB3.0 Data Recovery Equipment contains the following modules:

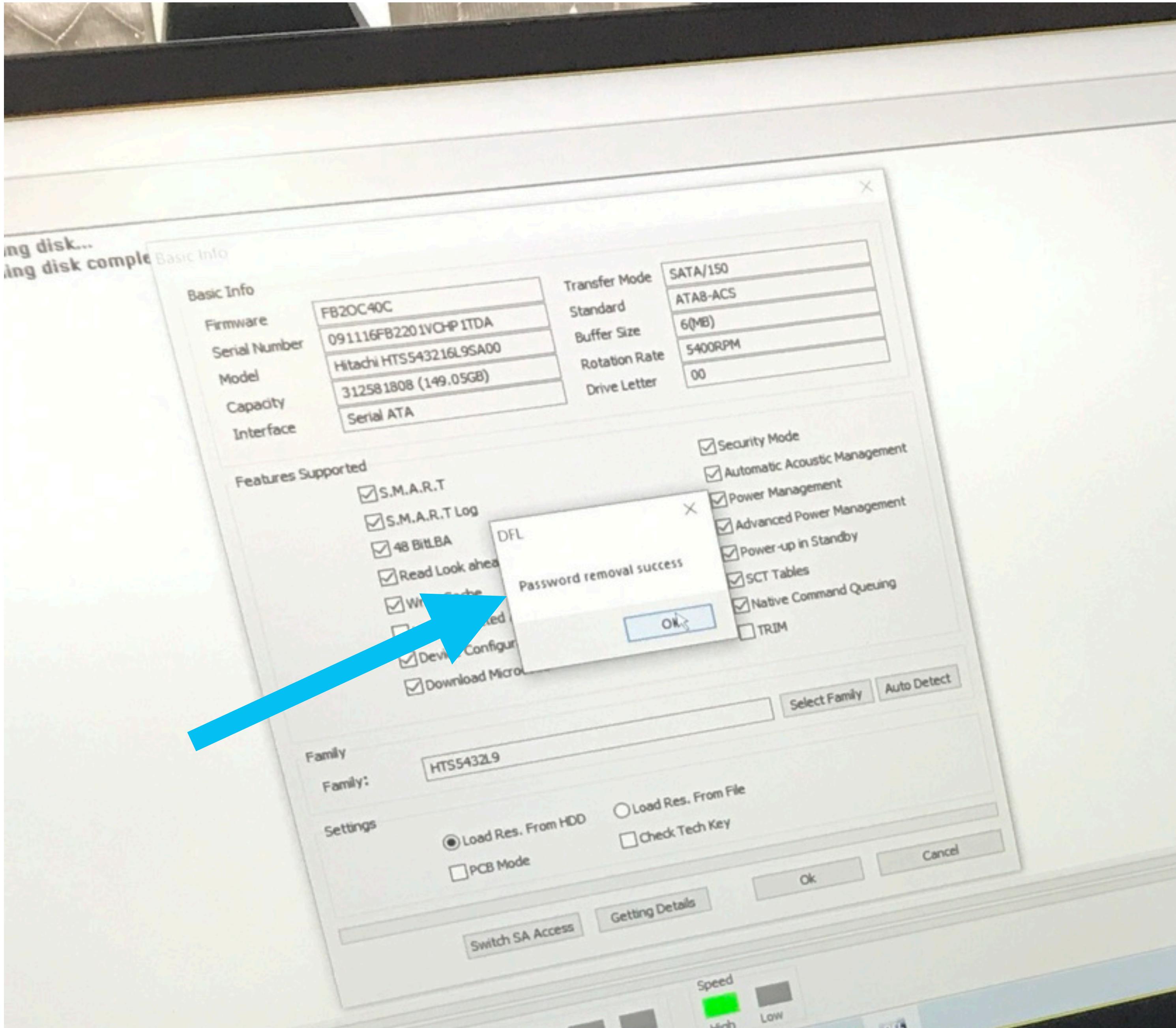
- [DFL-SRP USB3.0 For Data Extraction](#)
- [DFL-SRP USB3.0 For Seagate Firmware Repair](#)
- [DFL-SRP USB3.0 For WD Firmware Repair](#)
- [DFL-SRP USB3.0 For Hitachi/IBM Firmware Repair](#)
- [DFL-SRP USB3.0 For Samsung Firmware Repair](#)
- [DFL-SRP USB3.0 For Toshiba/Fujitsu Firmware Repair](#)



HACKINBO®
Winter 2025 Edition



HACKINBO® Winter Edition



Eee PC



American
Megatrends

Press ESC for BBS POPUP

Press F9 for image recovery

Press ALT+F2 to execute ASUS EZ Flash

DDRII-533/CL4, Single-Channel Mode

Initializing USB Controllers .. Done.

1016MB OK (Installed Memory Size:1024MB)

USB Device(s) : 1 Storage Device

Auto-Detecting Pri Master..IDE Hard Disk

Pri Master: Hitachi HTS543216L9SA00 FB20C40C

Ultra DMA Mode-5, S.M.A.R.T. Capable and Status OK

Auto-detecting USB Mass Storage Devices ..

Device #01 : Single Flash Reader *HiSpeed*

01 USB mass storage devices found and configured.

Please enter setup to recover BIOS setting

CMOS Date/Time Not Set

Press F1 to Run SETUP

Press F2 to load default values and continue

Manufactured MAX From Hunan, China
Model: EEEPC901SPGMAK6X NBBGQVAVWVX And 009

HRS1005LH211025062

ESC F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 Pause Break Prt Sc Insert Delete NumLK Scr LK

! @ # \$ % ^ & * () - + Backspace ←

HACKINBO®
Winter 2025 Edition

Eee PC

TrueCrypt Boot Loader 7.0a

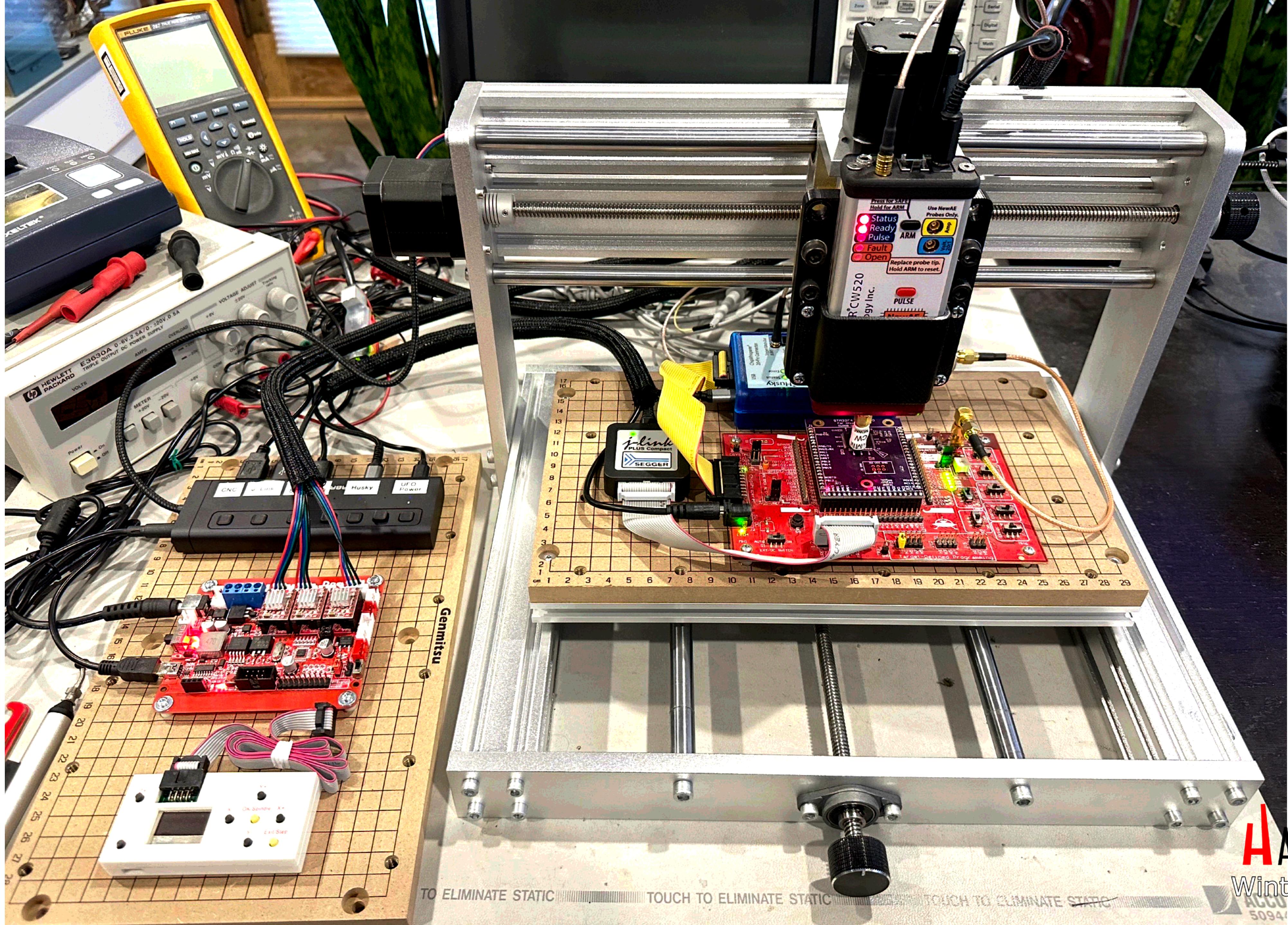
YHfa|fδ²\boot

Keyboard Controls:

[Esc] Skip Authentication (Boot Manager)

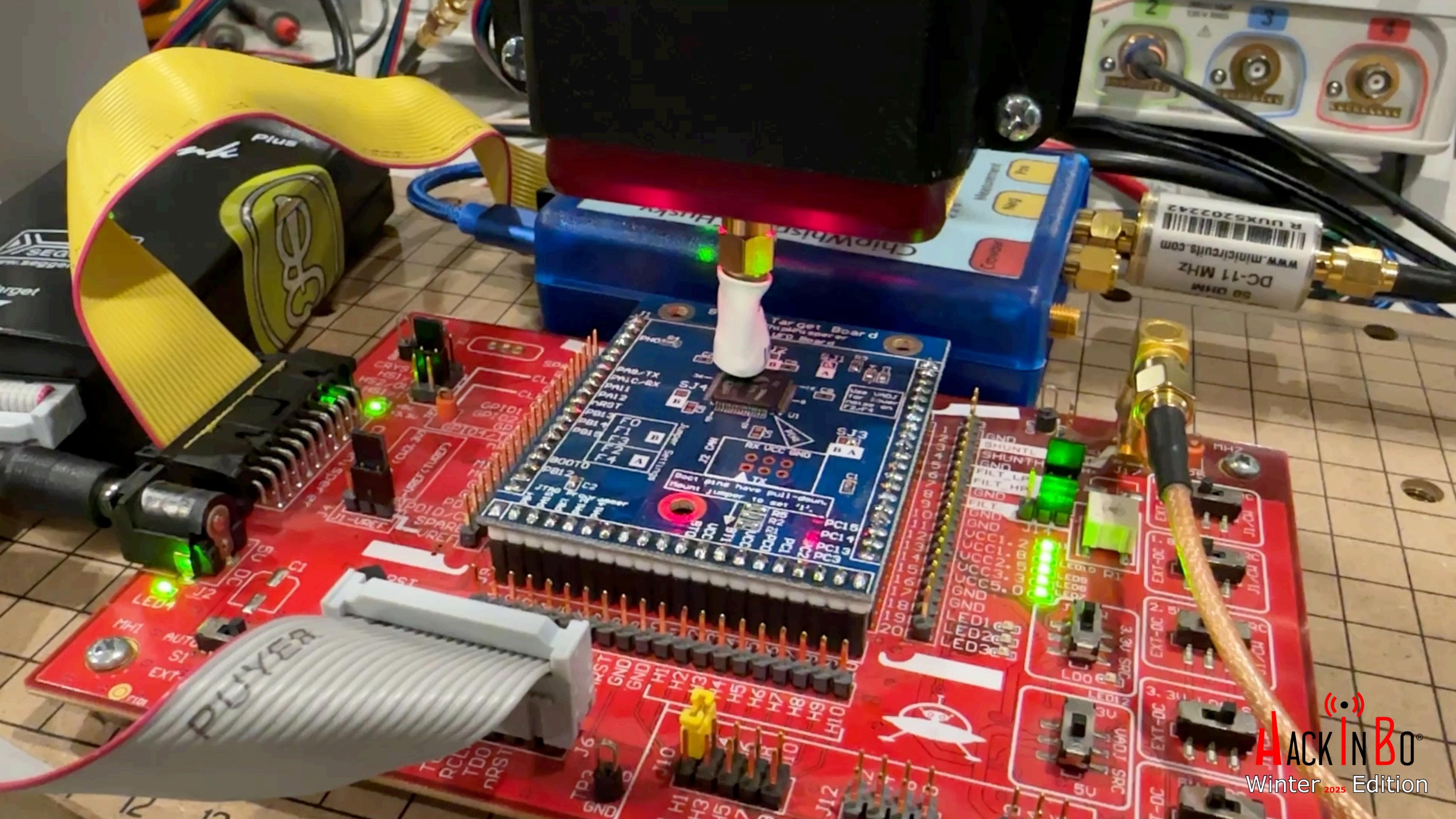
Enter password: _

HACKINBO®
Winter 2025 Edition



HACKINBO
Winter 2025 Edition







HACKINBO®
Winter 2025 Edition



25^a EDIZIONE

