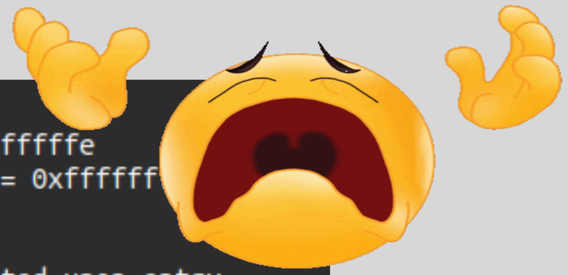
2. Dumping the Firmware

Using the exposed SWD interface quickly revealed that the firmware on the STM32F1 was read-out protected. Unfortunately, AKAI has never released a firmware update for the device and after a failed attempt to receive a firmware binary via AKAI's tech support, I researched possible exploits that could be used to dump the firmware.

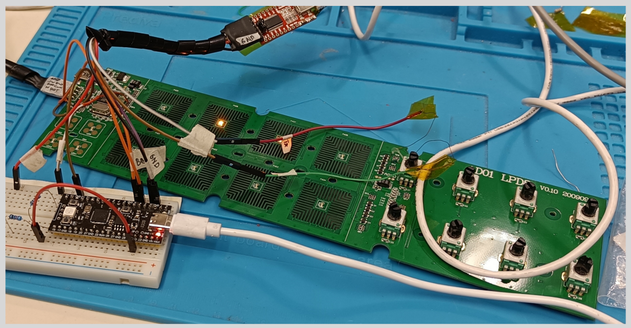


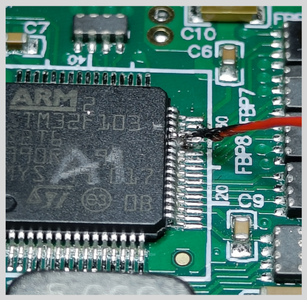
```
> stm32f1x options_read 0
option byte register = 0x3ffffe
write protection register = 0xffffff
read protection: on
watchdog: software
stop mode: no reset generated upon entry
standby mode: no reset generated upon entry
user data = 0xffff

>
[0] 0:telnet*Z
```

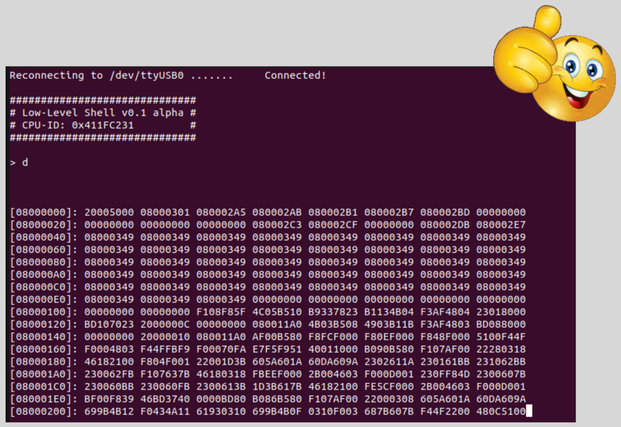
RDP Lock Conditions:

1. Debug Probe connected (req. **power cycle** to remove)
2. The device is booted into "bootloader mode" (req. **rst** to remove)
3. The device boots from SRAM (req. **rst** to remove)

A research paper published by Johannes Obermaier, Marc Schink, and Kosma Moczek, called "One Exploit To Rule Them All?", uncovered an exploit that fully circumvents the readout protection using an attack board to apply a power glitch and leveraging an oversight of the STM32F1 access to the Flash Patch and Breakpoint Unit (FPB). This inspired its own project, the **stm32f1-picopwner (search on github!)**, where I ported the exploit to work with a Pi Pico, fixed compatibility with some other STM32F1 chips, and made executing the exploit more user-friendly. Using the exploit, I successfully managed to dump a firmware binary.







```
Reconnecting to /dev/ttyUSB0 .......     Connected!

##############################
# Low-Level Shell v0.1 alpha #
# CPU-ID: 0x411FC231         #
##############################

> d


[08000000]: 20005000 08000301 080002A5 080002AB 080002B1 080002B7 080002BD 00000000
[08000020]: 00000000 00000000 00000000 080002C3 080002CF 00000000 080002DB 080002E7
[08000040]: 08000349 08000349 08000349 08000349 08000349 08000349 08000349 08000349
[08000060]: 08000349 08000349 08000349 08000349 08000349 08000349 08000349 08000349
[08000080]: 08000349 08000349 08000349 08000349 08000349 08000349 08000349 08000349
[080000A0]: 08000349 08000349 08000349 08000349 08000349 08000349 08000349 08000349
[080000C0]: 08000349 08000349 08000349 08000349 08000349 08000349 08000349 08000349
[080000E0]: 08000349 08000349 08000349 00000000 00000000 00000000 00000000 00000000
[08000100]: 00000000 00000000 F108F85F 4C05B510 B9337823 B1134B04 F3AF4804 23018000
[08000120]: BD107023 2000000C 00000000 080011A0 4B03B508 4903B11B F3AF4803 BD088000
[08000140]: 00000000 20000010 080011A0 AF00B580 F8FCF000 F80EF000 F848F000 5100F44F
[08000160]: F0004803 F44FFBF9 F00070FA E7F5F951 40011000 B090B580 F107AF00 22280318
[08000180]: 46182100 F804F001 22001D3B 605A601A 60DA609A 2302611A 230161BB 231062BB
[080001A0]: 230062FB F107637B 46180318 FBEEF000 2B004603 F000D001 230FF84D 2300607B
[080001C0]: 230060BB 230060FB 2300613B 1D3B617B 46182100 FE5CF000 2B004603 F000D001
[080001E0]: BF00F839 46BD3740 0000BD80 B086B580 F107AF00 22000308 605A601A 60DA609A
[08000200]: 699B4B12 F0434A11 61930310 699B4B0F 0310F003 687B607B F44F2200 480C5100
```