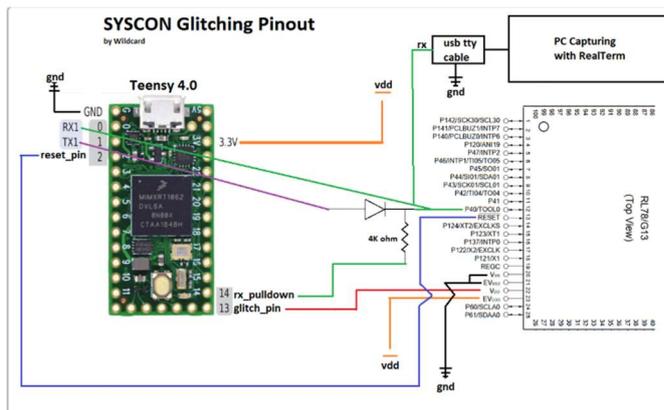


User Manual for DOWNGRADE PS4 through the SYSGLITCH procedure

Material:

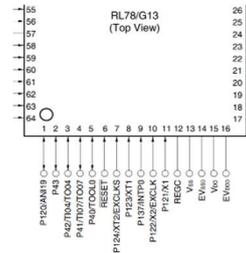
- R5F100PLA (for SAA and SAB) or
- R5F100LLA (for SAC, SAD ecc ecc) RL78 family stock
- E2 Lite Renesas
- Teensy 4.0 (sysglitch)
- Teensy 2.0++ (dump nor)
- Serial UART to USB
- TQFP 100pin 0.5mm
- Soldering station (my AOYUE 968A+)
- A lot of patience and a lot of passion

1.SYSGLITCH wiring diagram by Wildcard



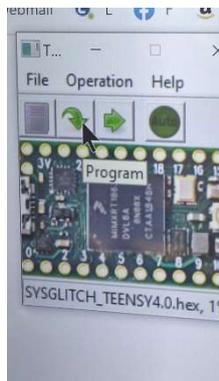
This is the schematic for a R5F100PL which is SAA and SAB motherboards and has a 100pin pinout.

While the R5F100LL chip for SAC SAD etc has 64pin and the schematic is

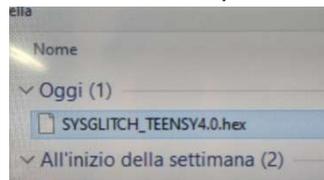


2. Assemble the pieces

Getting a Millefori Tablet (Bakelite) Amazon is your friend.



1. Let's take teensy 4.0 and program with hex (glitch Marcan):



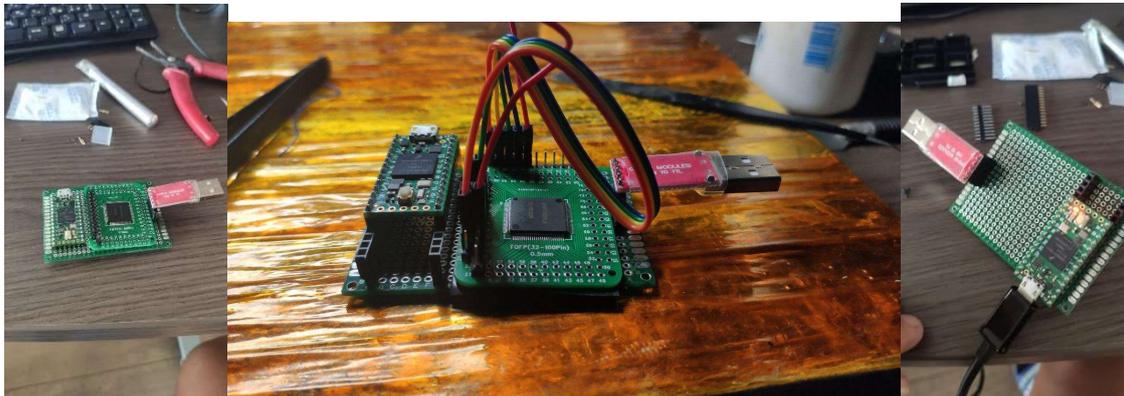


2. Place the syscon on the board (only the desired pinout)

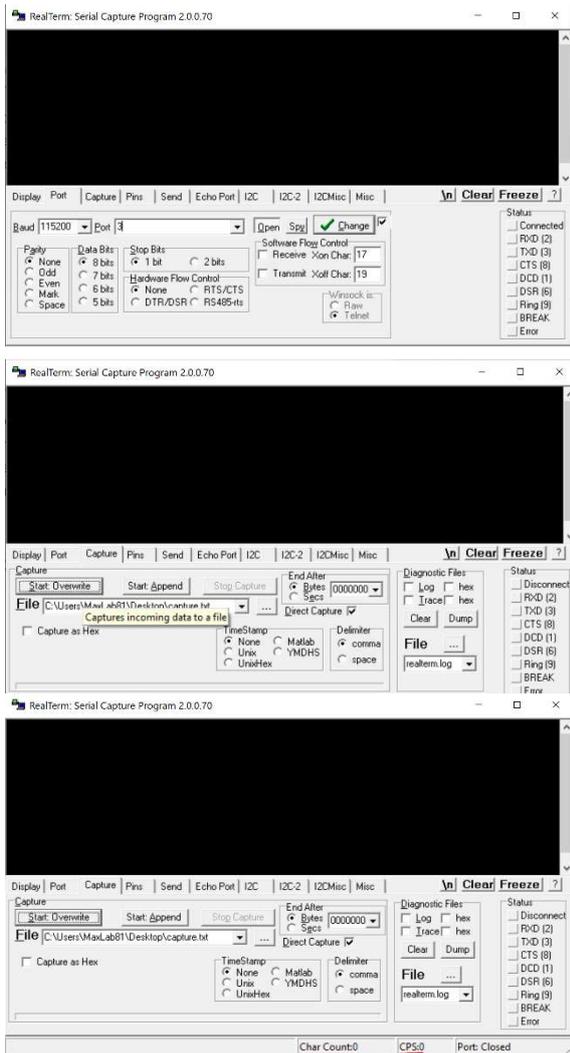


3. So we begin to compose the circuit.
for the pulldown we have to use a 4k ohm resistor and a small diode, I used a jumper so that when ready we start the glitch

4. This is the final result



3. Dump SYSCON with REALTERM



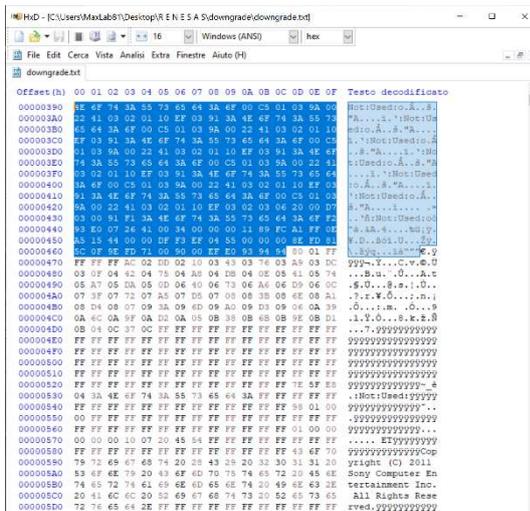
1. We connect the device via USB (the pull-down jumper must be disconnected) now we start Realterm and set the baud speed to 115,200 bps and choose the serial port now click on change.

2. We choose where to write the dump and then click on Start: Overwrite.

Well if you did everything right it should turn red and we can "pull-down" the jumper to start the GLITCH

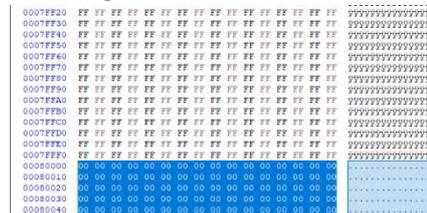
3. the count of characters will begin, we arrive at about 4Mb and then we stop

4. Data analysis and payload preparation

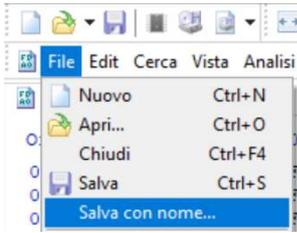


1. Let's open the dump with HxD and delete until we find the 2 hexadecimal values 94 94.

2. Let's go to offset 7FFFF and delete everything else

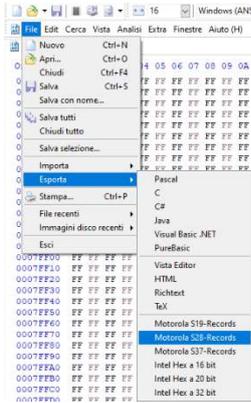


HxD - [C:\Users\MaxLab81\Desktop] 3. Let's go to File \ Save As

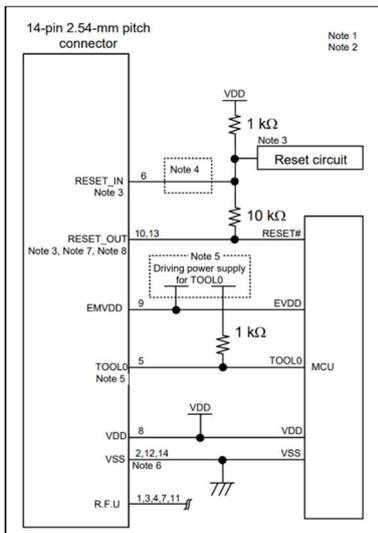


4. In order for the dump to be read by the program, we need to convert it to the appropriate language.

File \ Export \ Motorola S28 Records

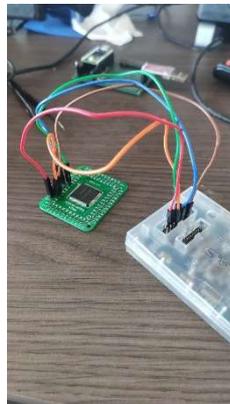


5. Connect E2 Lite with stock RL78

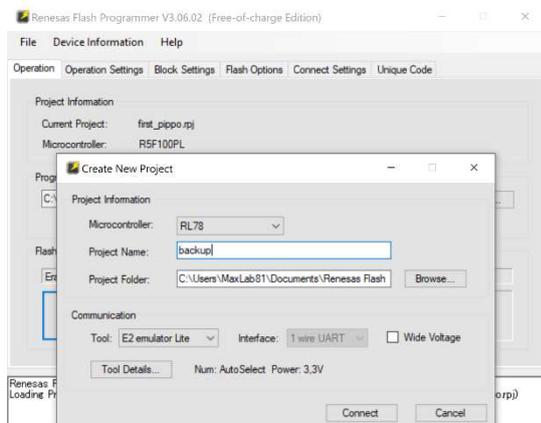


1. Let's take the pinout of the E2 Lite at 14pin, while we already know it for the RL78

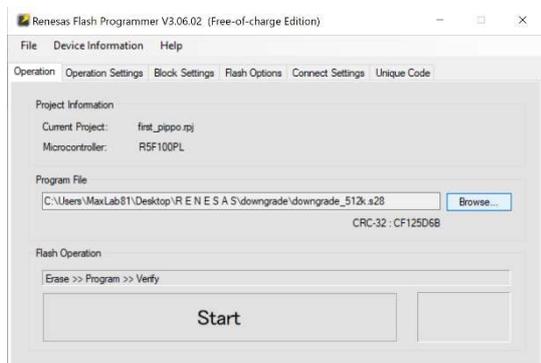
2. This is the result:



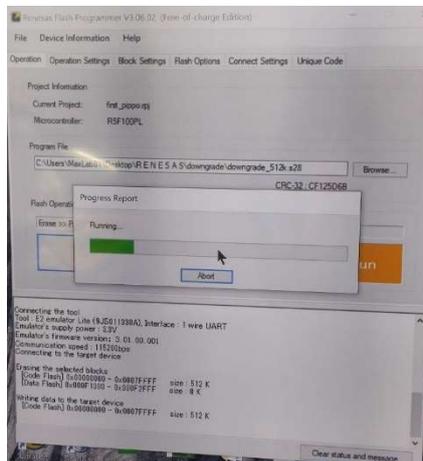
6. Renesas Flash Programmer



1. We connect the E2 Lite device via the USB cable and launch the Renesas Flash Program, create a new project with the following parameters:
 - .Microcontroller: RL78
 - .Tool: E2 Emulation Lite
 - .Tool Detail select 3.3v



2. Select the file previously created with HxD with extension s28 and press START.

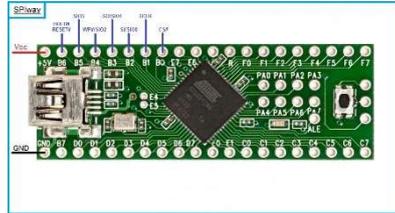
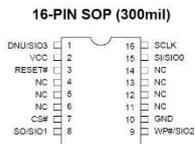


3. If you've done everything right so far, writing your syscon backup will begin

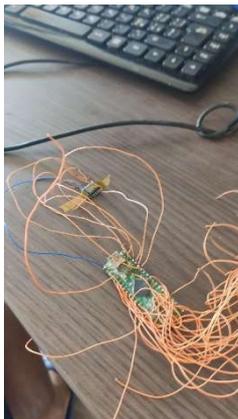
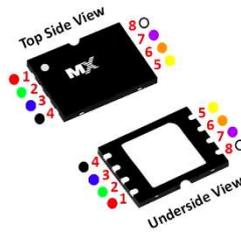
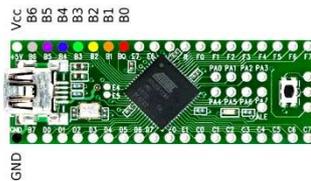
7. NOR BACKUP with Teensy 2.0++

1. Version SAA and SAB

MX25L25635F



2. Version SAC, SAD etc.



3. Soldering 10 testpoints or anyone with a TSOP avoids soldering

```
SPIway v0.40 - Teensy++ 2.0 SPI Flasher for PS4
Copyright (C) 2017 judges@eEcho.com

Pinging Teensy...
Available memory: 4060 bytes

SPI information
-----
Chip manufacturer: Macronix (0xc2)
Chip type: MX25L25635F (0x18)

Chip size: 32 MB
Sector size: 4096 bytes
Block size: 65536 bytes
Sectors per block: 16
Number of blocks: 512
Number of sectors: 8192

Dumping...
1216 KB / 32768 KB
```

4. I assume that the teensy must be set with HEX SPI, so we also start the dump backup of our Downgrade



File Pack -> <https://gofile.io/d/i1e8UD>

Special Thanks to Wildcard

Facebook: Massimiliano Caprabanca

Twitter: MaxLab81