

0x0a364a0 [0,0]

Contents: [Dobrica Pavlinu's random unstructured stuff]

- Dobrica Pavlinu's random unstructured stuff (IM-ME)
 - ◆ Dobrica Pavlinu's random unstructured stuff (console)
 - ◇ Dobrica Pavlinu's random unstructured stuff (pinout)
 - ◇ Dobrica Pavlinu's random unstructured stuff (flasing using RaspberryPi)
 - ◆ Dobrica Pavlinu's random unstructured stuff (dongle)
- Dobrica Pavlinu's random unstructured stuff (rfcat)
- Dobrica Pavlinu's random unstructured stuff (links)

IM-ME

- <http://davesshacks.blogspot.com/2010/01/im-me-hacking.html>
- <http://travisgoodspeed.blogspot.com/2010/03/im-me-goodfet-wiring-tutorial.html>
- <https://github.com/m0nk/IMME>

console

pinout

- (square pad) RESET_N
- P2_1 = debug data
- P2_2 = debug clock
- +2.5 volts (CC1110 VDD max 3.9V)
- Gnd

Spectrum analyzer <https://github.com/mossmann/im-me>

flasing using RaspberryPi

```
git clone https://github.com/tobyjaffey/cctl
```

```
pi@raspberrypi ~/cctl $ git diff
diff --git a/ccpil/dbg.c b/ccpil/dbg.c
index 9ca33da..2b4a796 100644
--- a/ccpil/dbg.c
+++ b/ccpil/dbg.c
@@ -30,9 +30,9 @@
```

```
#define NUM_ATTEMPTS 100
```

```

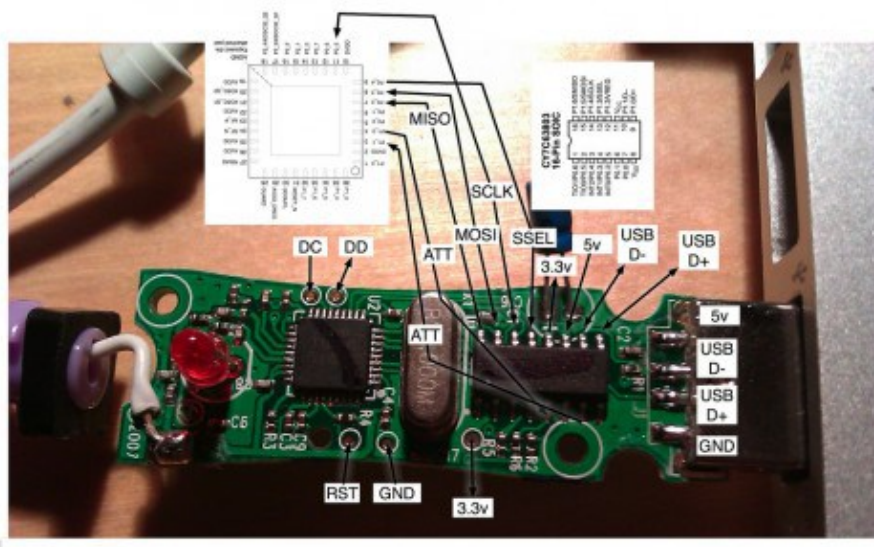
-#define PIN_DD RPI_GPIO_P1_11
-#define PIN_DC RPI_GPIO_P1_12
-#define PIN_RST RPI_GPIO_P1_13
+#define PIN_DD RPI_GPIO_P1_21
+#define PIN_DC RPI_GPIO_P1_23
+#define PIN_RST RPI_GPIO_P1_24
```

```
#define ST_CHIP_ERASE_DONE 0x80
```

```
wget https://github.com/mossmann/im-me/raw/master/specan/specan.hex
```

```
sudo ./ccpil -f specan.hex
```

dongle



Mine is different board revision

rfcat

- <https://bitbucket.org/atlas0fd00m/rfcat>

links

- <https://github.com/mossmann/cc11xx> - Hardware designs for CC11xx
- <https://github.com/tobyjaffey/cctl> - ChipCon Tiny Loader, a 1KB serial bootloader for CC1110/CC1111
- <https://github.com/samyk/opensesame> - OpenSesame attacks wireless garages and can open most fixed-code garages and gates in seconds