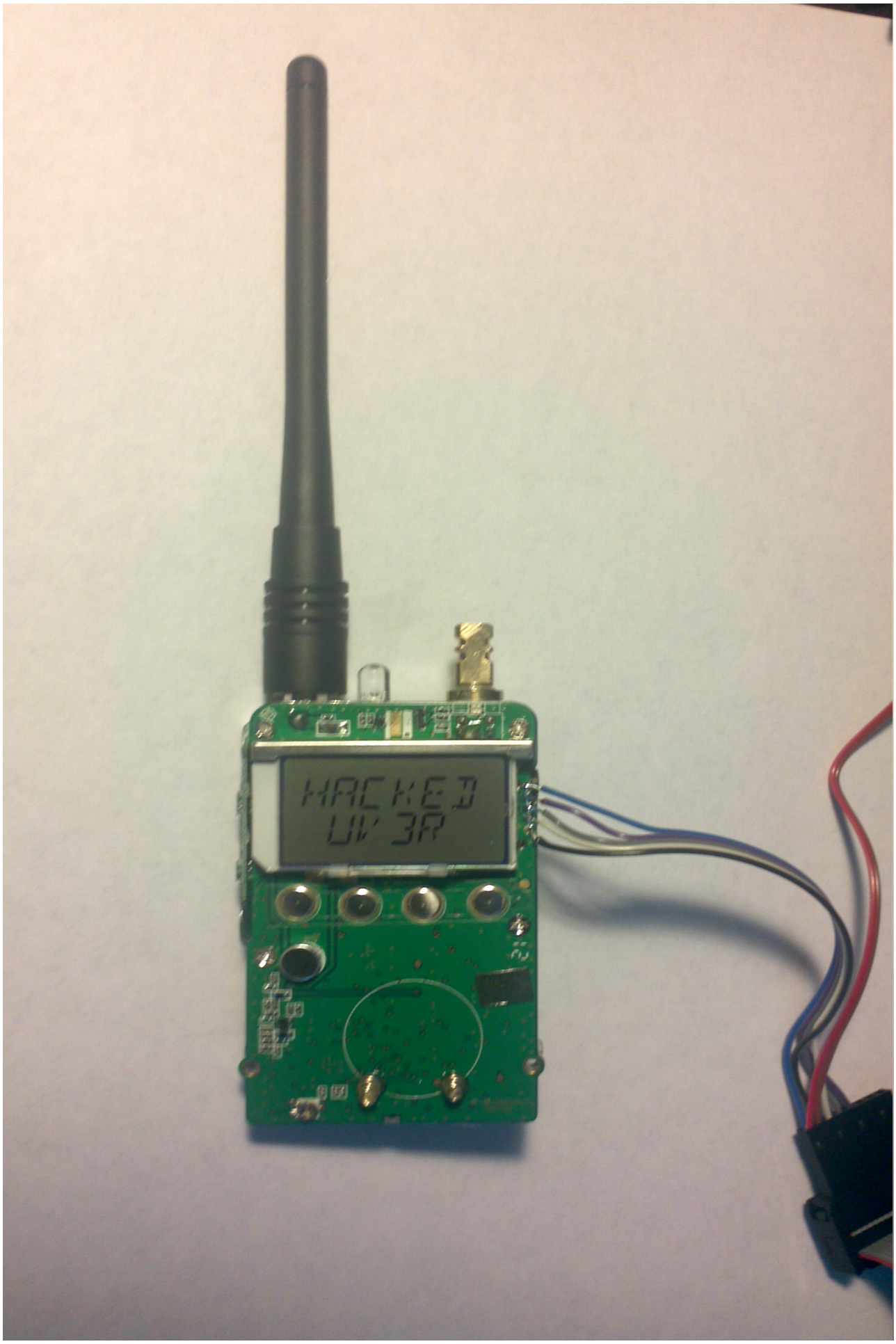
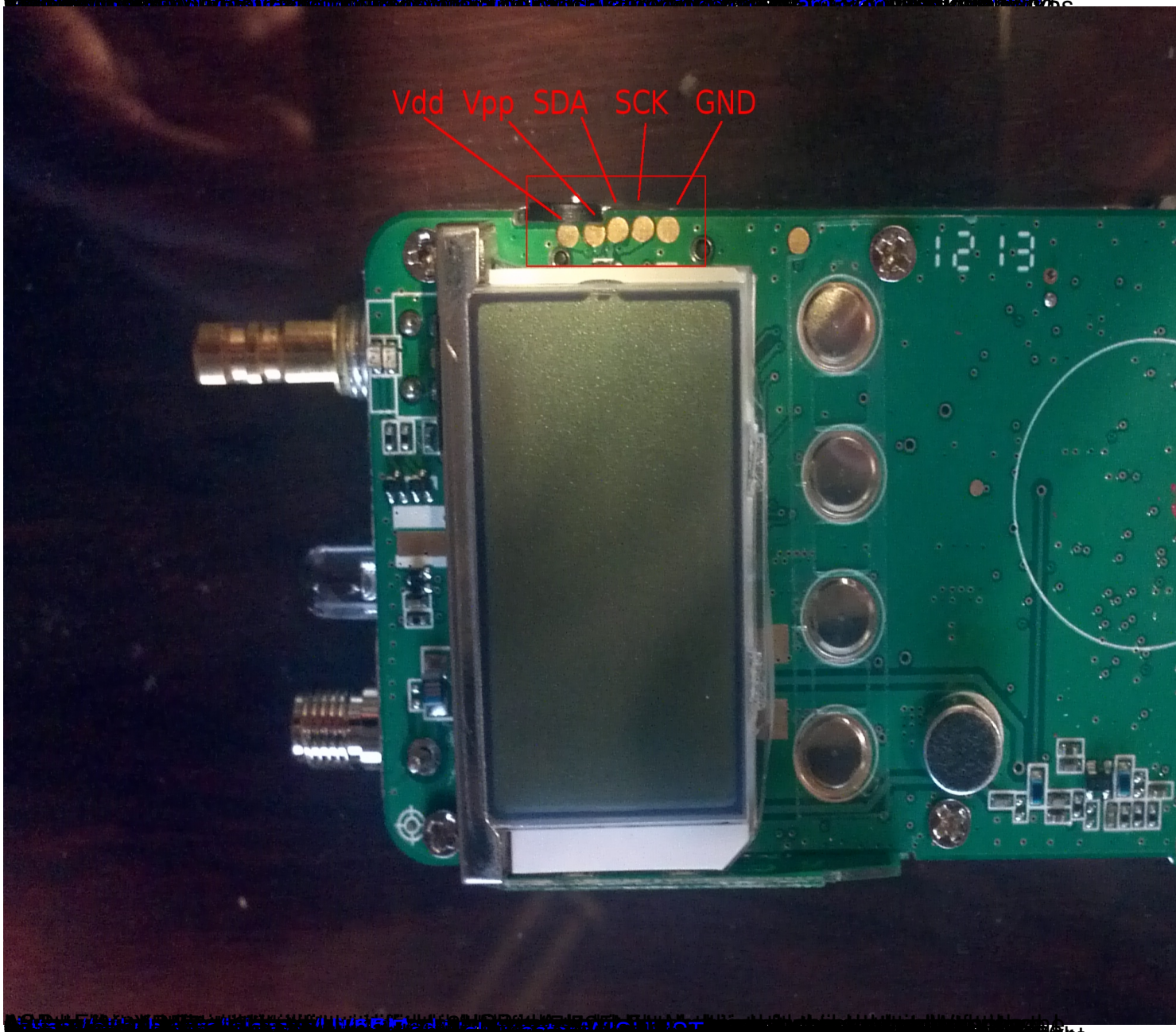
Introduction


HACKED
UV 3R



Programmer Protocol

The implementation of this protocol along with the arduino code and the ongoing firmware can be cloned from github.

https://github.com/lelazary/UV3RMod

Here is the protocol used to get into the chip and program it: A 9V is set on the reset pin (VPP) to enter programing mode.

Protocol sending over SPI LSB first. After almost every byte, the chip will pulse the data line to indicate ACK.

Get Chip ID: 0x55 0xAA 0x5A 0xA5 0x01 0x00 0x00 0x05 0x00 wait 1ms for response should be 0x82

Program fuse bits

Get Chip ID : 0x55 0xAA 0x5A 0xA5 0x01 0x00 0x00 0x05 0x00 wait 1ms for response should be 0x82
30ms delay
Set Mode : 0x55 0xAA 0x5A 0xA5 0x01 0x00 0x00 0x05 0x08 wait 1ms for response should be 0x01
30ms delay
set 20FF to 0 : 0x55 0xAA 0x5A 0xA5 0x02 0x00 0x00 0x03 0x05 0x00 wait 1ms for response should be 0x55

Erase Chip :
Get Chip ID : 0x55 0xAA 0x5A 0xA5 0x01 0x00 0x00 0x05 0x00 wait 1ms for response should be 0x82
30ms delay
Erase : 0x55 0xAA 0x5A 0xA5 0x01 0x00 0x00 0x03 0x01 wait 1ms for response should be 0x55
2 sec delay
set 20FF to 0 : 0x55 0xAA 0x5A 0xA5 0x02 0x00 0x00 0x03 0x05 0x00 wait 1ms for response should be 0x55

Read Data:
Get Chip ID : 0x55 0xAA 0x5A 0xA5 0x01 0x00 0x00 0x05 0x00 wait 1ms for response should be 0x82
30ms delay30ms delay
Set Read range: 0x55 0xAA 0x5A 0xA5 0x05 0x00 0x00 0x04 0xC0 0x00 0xC0 0xFF 0x00
<wait for data to go high> read 255 bytes
30ms delay
Set Memory Mode: 0x55 0xAA 0x5A 0xA5 0x01 0x00 0x00 0x05 0x08 wait 1ms for 0x00

Program Data:
Get Chip ID : 0x55 0xAA 0x5A 0xA5 0x01 0x00 0x00 0x05 0x00 wait 1ms for response should be 0x82
30ms delay
Set Memory Mode : 0x55 0xAA 0x5A 0xA5 0x01 0x00 0x00 0x05 0x08 wait 1ms for 0x00
30ms delay
Set program range and data : 0x55 0xAA 0x5A 0xA5 0x80 0xC0 0x00 0x00 <128 bytes> wait

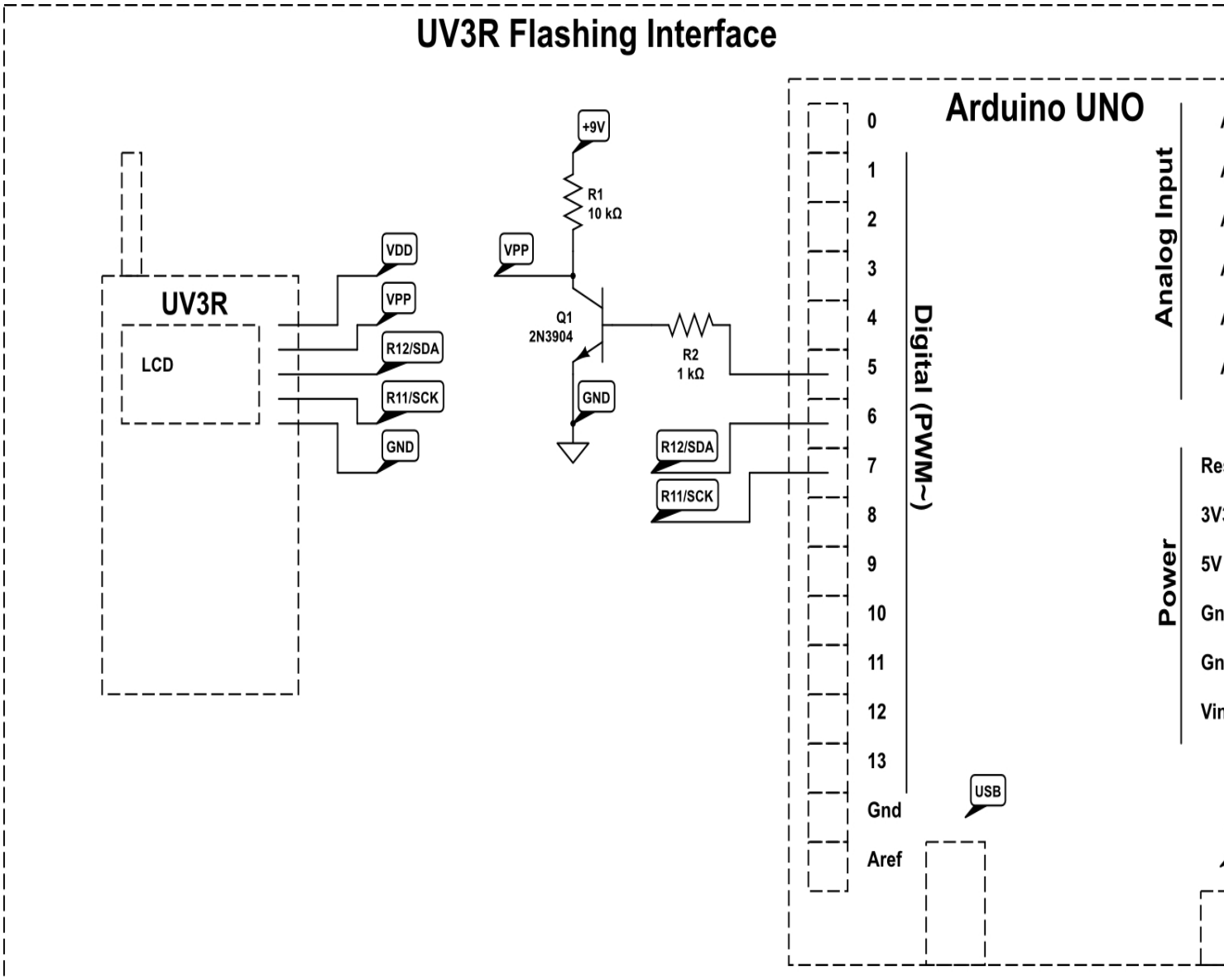
1ms for 0x55

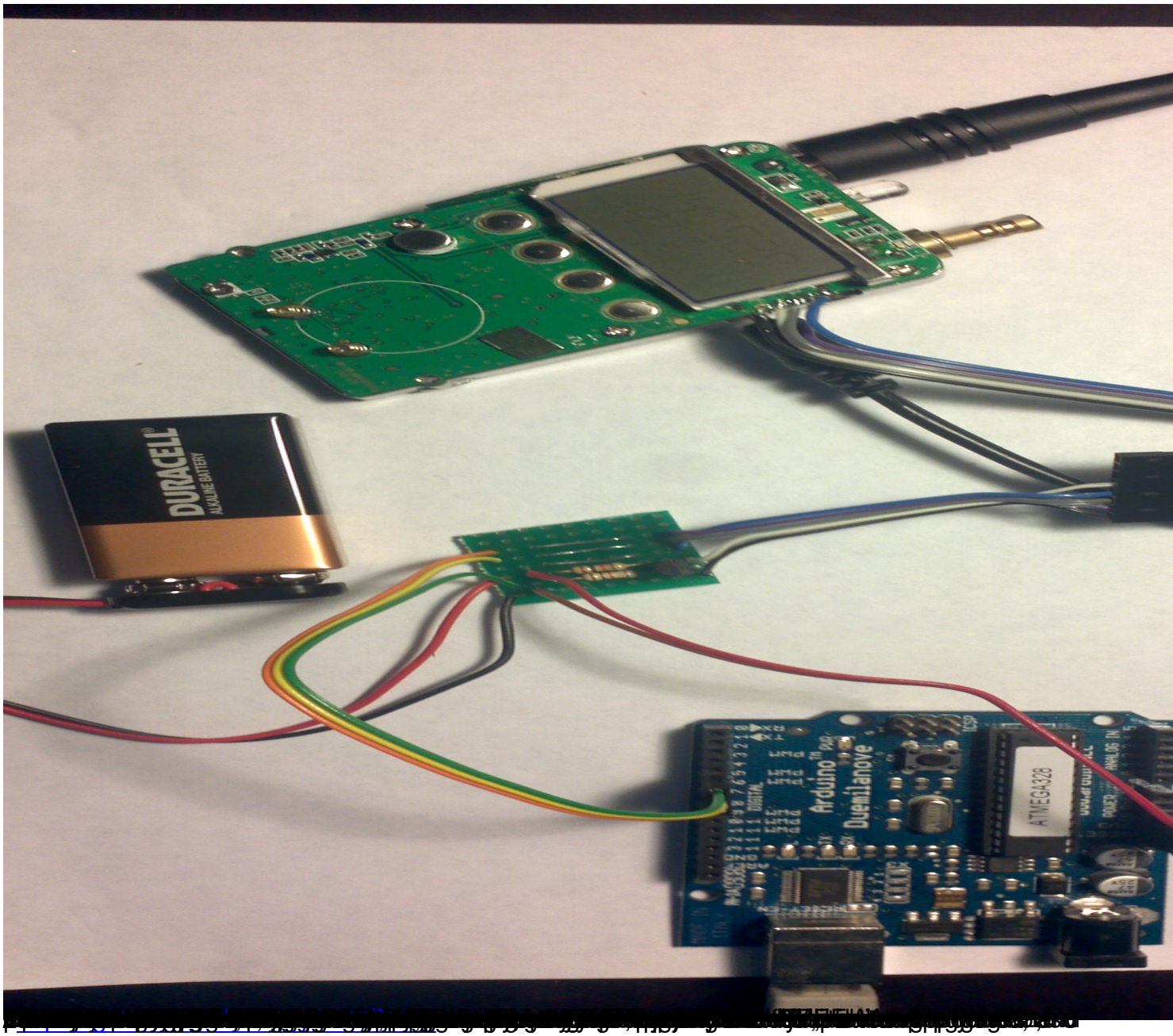
Set Memory Mode: 0x55 0xAA 0x5A 0xA5 0x01 0x00 0x00 0x05 0x08 wait 1ms for 0x00

DIY instructions for performing this hack

Disclaimer: This hack is a work in progress. If you perform this hack you might transmit on frequencies outside the allowable amateur bands. For now I am keeping the TX amplifiers off, so the radio will not transmit more then a hundred feet. However, anyone can always go into the code and turn them back on. If you do so, you are responsible to insure that you know what you are doing, and take the necessary precaution when transmitting. I will not be responsible for any damage cause by the radio or to the radio. Remember, once you erase the original firmware, there is no way of getting it back, so the radio will be a brick until you upload the firmware; but if you got this far, then that is exactly what you want.

For this hack you will need an arduino, NPN transistor (I used 2n394), 1K and 10K resistors, and a 9 volt battery. You could just use a 9V battery and a 10K resistor, but you would need to manually connect the VPP to 10K -> 9V and GND. If you want to do any kind of development, then the transistor is your option.
Connect everything according to the diagram bellow:


UV3R Flashing Interface
Arduino UNO
UV3R
LCD
VDD
VPP
R12/SDA
R11/SCK
GND
+9V
R1
10 kΩ
Q1
2N3904
R2
1 kΩ
Digital (PWM~)
Analog Input
Power
0
1
2
3
4
5
6
7
8
9
10
11
12
13
Gnd
Aref
USB


DURACELL
ALKALINE BATTERY
Arduino
Duemilanove
ATMEGA328