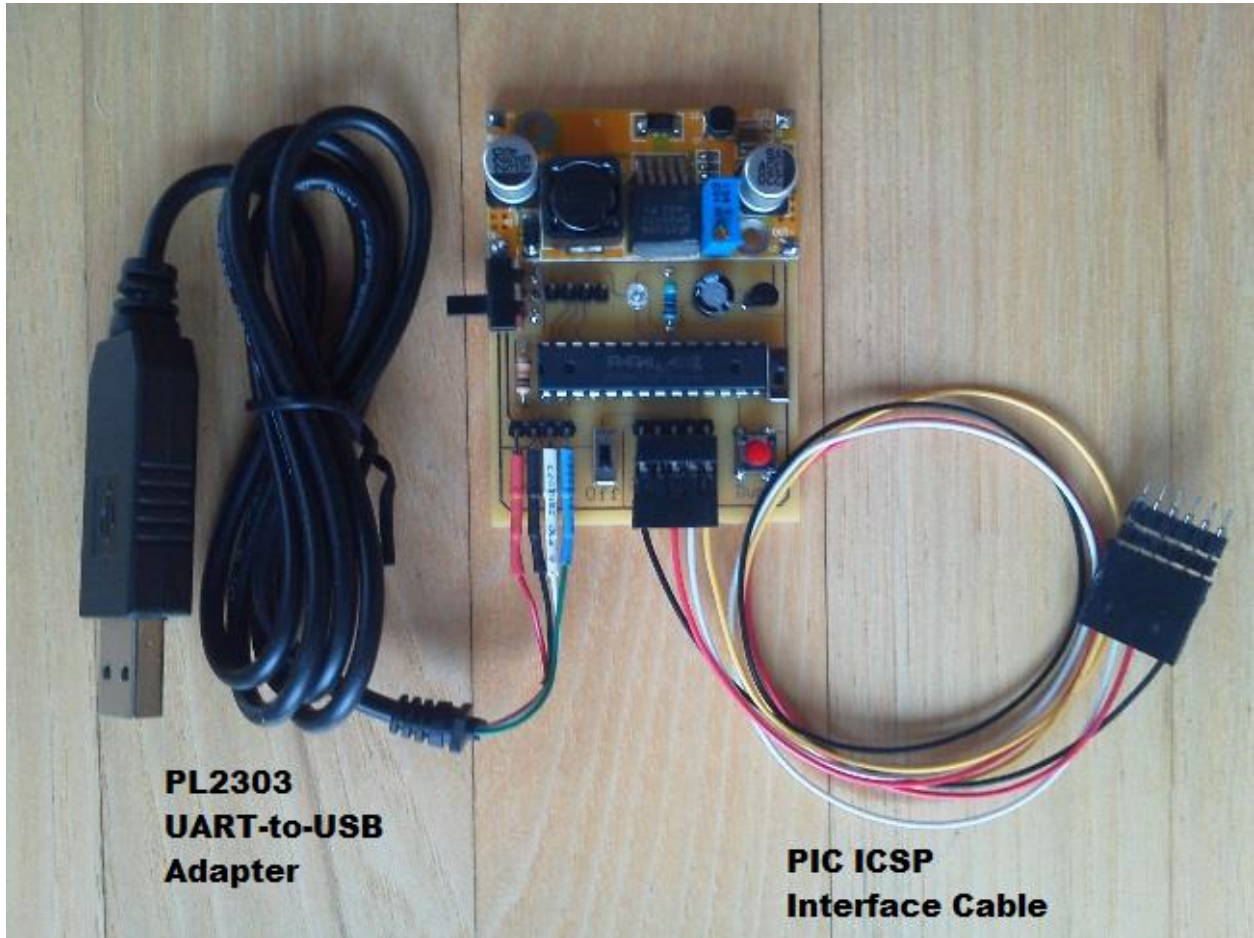


iClass Reader (RevA)  
PIC 18F452/18F6621 RAM Dumper  
Operating Instructions



Proxclone.com  
Revision 2.0  
December2015

## Overview

The RAM dumper circuit is used in conjunction with a HID iclass RevA reader to dump the contents of the PIC microcontroller RAM memory. The circuit is powered from a standard PC USB port. All of the required voltages (including the Vpp programming signal) are generated from a dc-dc booster circuit that is fed from the +5Vdc USB power input.

The extracted RAM data is output on a serial UART interface that is fed into a UART-to-USB adapter that appears as a virtual COM port interface on the PC.

Data is captured using any standard serial terminal software (e.g. CoolTerm or Hyperterminal) which is capable of accepting a serial ascii data stream.

A photo of the RAM Dumper circuit board layout is shown in Figure 1 below.

## Setup

The PL2303 UART-to-USB driver software can be downloaded from the following website:

[http://www.prolific.com.tw/us/showproduct.aspx?p\\_id=225&pcid=41](http://www.prolific.com.tw/us/showproduct.aspx?p_id=225&pcid=41)

The terminal software that is being used should be setup to receive serial data as 19200,8,N,1.

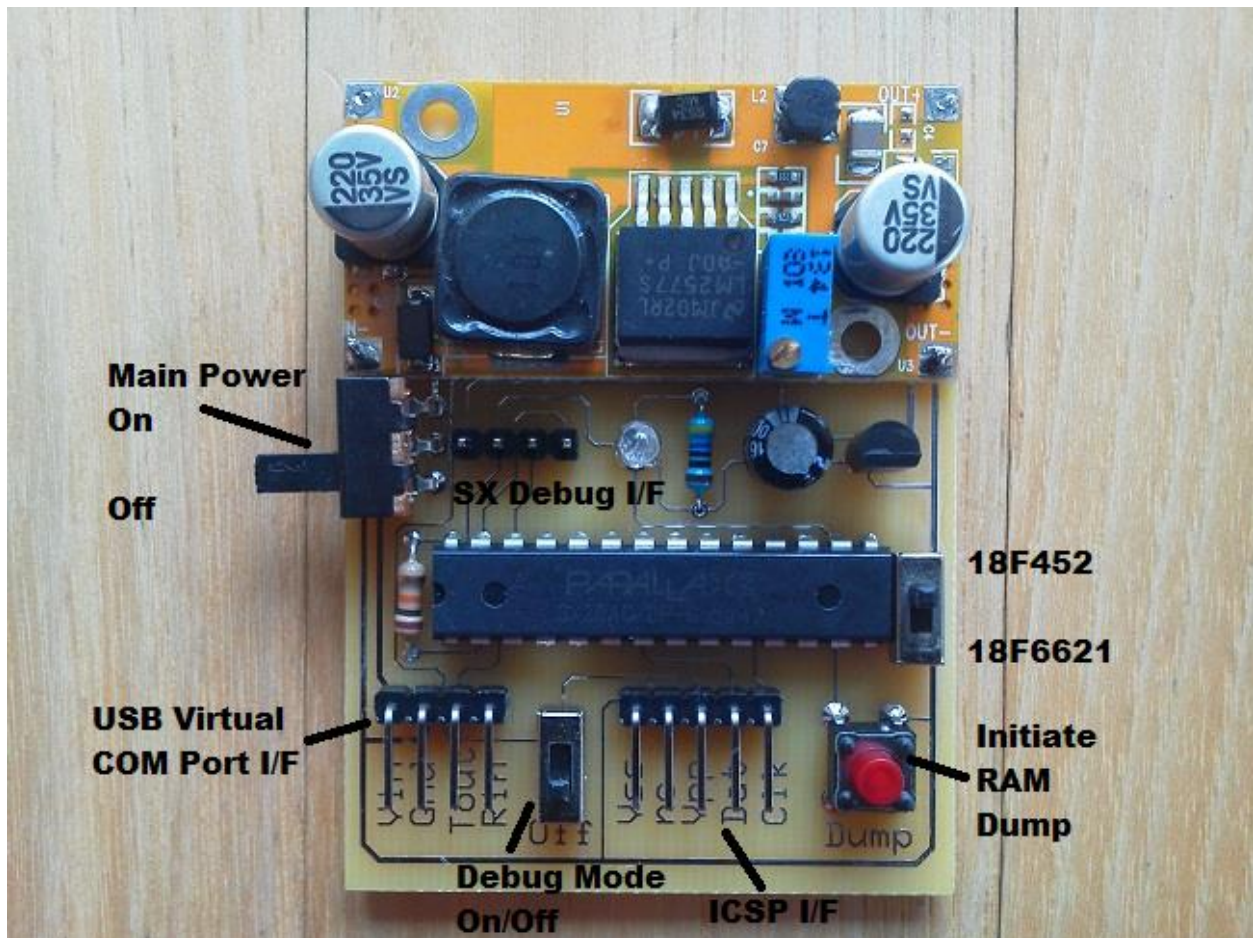


Figure 1. RAM Dumper Circuit Board Layout

## Operation

1. Ensure that the PL2303 Driver software has been properly installed before proceeding to step 2.
2. Attach the PIC ICSP Debug interface cable between the RAM Dumper unit and the iclass reader target hardware. Note that the ICSP debug interface signals on the iclass readers are **NOT** always arranged the same. A connection to an R40 reader is depicted in Figure 2.

### **R30/R40/RW300/RW400/RK40/RKW400 Pinout is as follows:**

Pin 1 Vss/Gnd (leftmost pin looking at backside of reader)

Pin 2 Vdd (not used)

Pin 3 Vpp

Pin 4 PGD/Data

Pin 5 PGC/Clock

Pin 6 Aux (not used)

### **R90 Reader Pinout is as follows:**

Pin 1 – Vpp (pin nearest tamper switch)

Pin 2 – Vss/Gnd

Pin 3 – Vdd (not used)

Pin 4 – PGC/Clk

Pin 5 – PGD/Data

3. Attach a separate power source (5-16Vdc nominal) to the iClass Reader.  
Power up the reader and verify that the reader plays its startup tune signifying that the reader is operational and that the factory default firmware is currently loaded.
4. Place an iclass credential near the reader. This will ensure that the HID Global Master keys are loaded into RAM from the PIC's EEPROM memory.
5. Position the PIC chip selector switch "Up" for a PIC18F452 device or "Down" for a PIC18F6621 device. This switch defines the size of the RAM file that is to be dumped .
6. Plug the RAM Dumper USB interface into a PC USB port. (note in Windows Device Manager the COM port that has been assigned)
7. Turn on the RAM Dumper Main Power Switch (Up position) .  
The blue LED will illuminate to indicate that the microcontroller has been initialized and proper voltage levels are being generated.
8. Bring up the terminal software(e.g. CoolTerm,HyperTerminal) being used to capture the dumped RAM data. This software must be setup to receive data using the following UART parameters: COM-TBD,19200,8,N,1.
9. Position the "Debug Mode" switch in the up/ON position. This will apply the Vpp programming voltage to the PIC chip, placing it into a debug mode of operation.
10. Press and release the "Dump" pushbutton switch. The LED will blink 8 times and then turn off while the serial ascii data is being transferred. The LED will turn on again once the entire contents of the RAM have been transferred (approx. 10-15 sec)



11. Position the “Debug Mode” switch in the down/OFF position to exit debug mode.
12. Turn off the RAM Dumper Main Power switch.

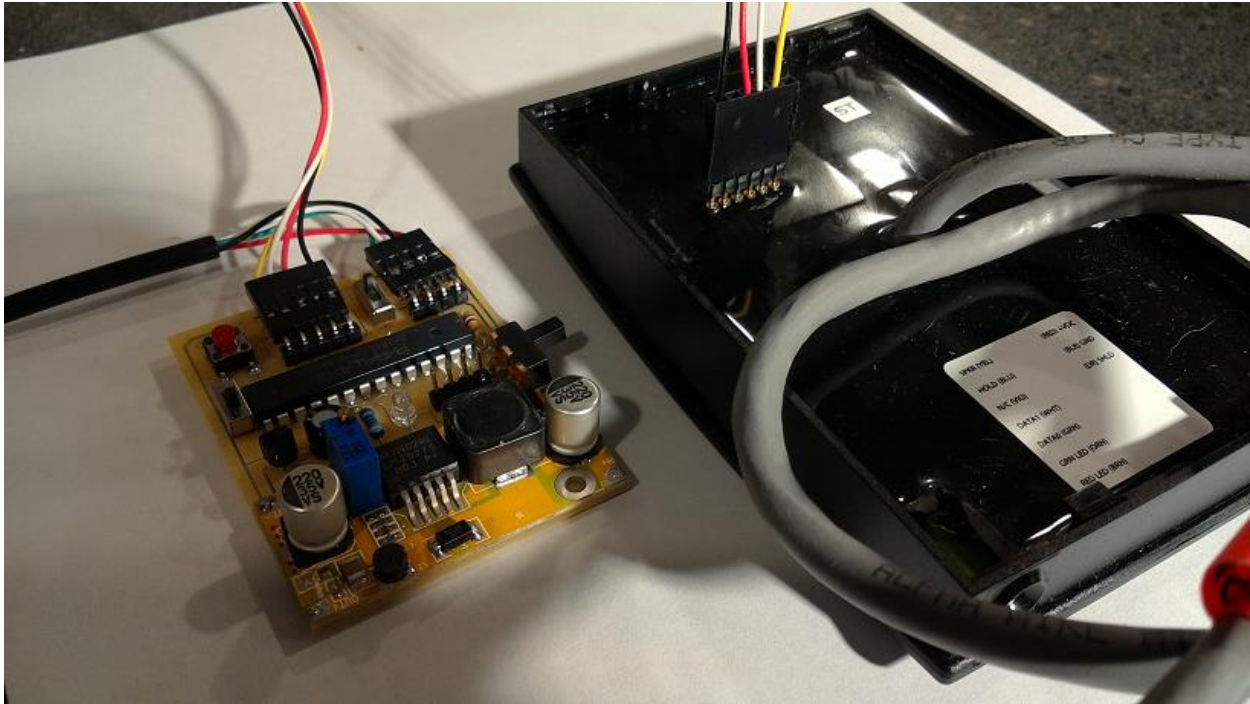


Figure 2. ICSP Connection to R40 Reader (Black Vss/Gnd on outside pin)

### Example RAM Dump

The captured data shown in the screenshot below is an actual dump obtained from an iClass R40 reader using the CoolTerm Terminal application program.

[Note: Sensitive authentication key and encryption key information has been obscured].

The freeware version of CoolTerm can be found here: <http://coolterm.findmysoft.com/#>

The PIC RAM data that is outputted has been pre-formatted to simplify its readability.

The leftmost column is the RAM address. All data is dumped as ASCII hex bytes.

CoolTerm\_0\*

File Edit Connection View Window Help

New Open Save Connect Disconnect Clear Data Options View Hex Help

```

0000 01 00 01 00 00 00 00 00 00 08 42 00 10 00 00
0010 52 01 00 00 00 00 10 40 00 00 00 00 02 80 20
0020 10 18 00 00 00 00 00 00 01 42 80 20 00 00 80
0030 00 01 08 00 41 00 00 00 00 10 40 00 22 00 10
0040 81 00 00 00 80 00 08 00 00 00 12 00 05 01 40 80
0050 00 00 00 08 10 00 04 00 04 00 12 00 01 00 32 40
0060 00 00 00 00 0A 00 30 00 00 00 8C 00 00 00 00 08
0070 1D 01 70 00 08 80 00 00 00 80 05 08 40 80 00 00
0080 04 01 C0 00 00 10 10 00 03 01 00 00 20 10 00 07
0090 08 20 10 20 80 00 08 80 02 08 00 00 00 00 88 00
00A0 00 20 01 24 20 04 09 00 00 02 00 04 20 02 00 40
00B0 02 80 03 02 81 00 00 00 20 00 00 00 00 00 00 00
00C0 00 03 00 03 E4 17 B3 E7 71 42 FE 1C 2C EF 00 00
00D0 00 20 21 22 33 00 00 00 00 44 17 21 17 32 17 32
00E0 12 FF FE FF FF 63 63 E0 12 01 03 11 1B 00 0E 00
00F0 03 02 03 02 FF FF 80 00 A7 01 FF FF 9B FF FF FF
0100 40 02 00 20 08 00 60 00 08 ████████████████████
0110 ████████████████████
0120 ████████ 00 00 20 00 00 88 00 00 20 80 00 00 08 00 08
0130 00 00 00 00 00 00 00 00 00 00 00 00 01 0F FF FF
0140 00 00 00 00 00 00 00 00 00 00 00 00 01 0F FF FF 90 07
0150 08 0F 0F FF 02 FC 09 00 00 E3 61 00 00 87 BA FF
0160 0E 68 B5 07 03 0A 27 01 07 50 28 19 00 AA 60 A0
0170 9F 00 88 01 00 0D 00 00 42 1E 01 00 00 00 00 00
0180 00 00 00 00 00 00 00 00 CD A7 36 00 00 00 00 40
0190 00 00 00 00 00 00 04 90 00 A6 00 00 00 A0 10 14
01A0 00 20 00 00 48 00 02 12 34 00 00 00 00 00 00 00
01B0 00 00 00 00 00 00 00 00 00 08 0C A1 03 BB 06

```

Sample Dump  
(R40 RevA Reader)  
Key data blanked out.

COM6 / 19200 8-N-1  
Connected 00:55:12

TX RTS DTR DCD  
RX CTS DSR RI