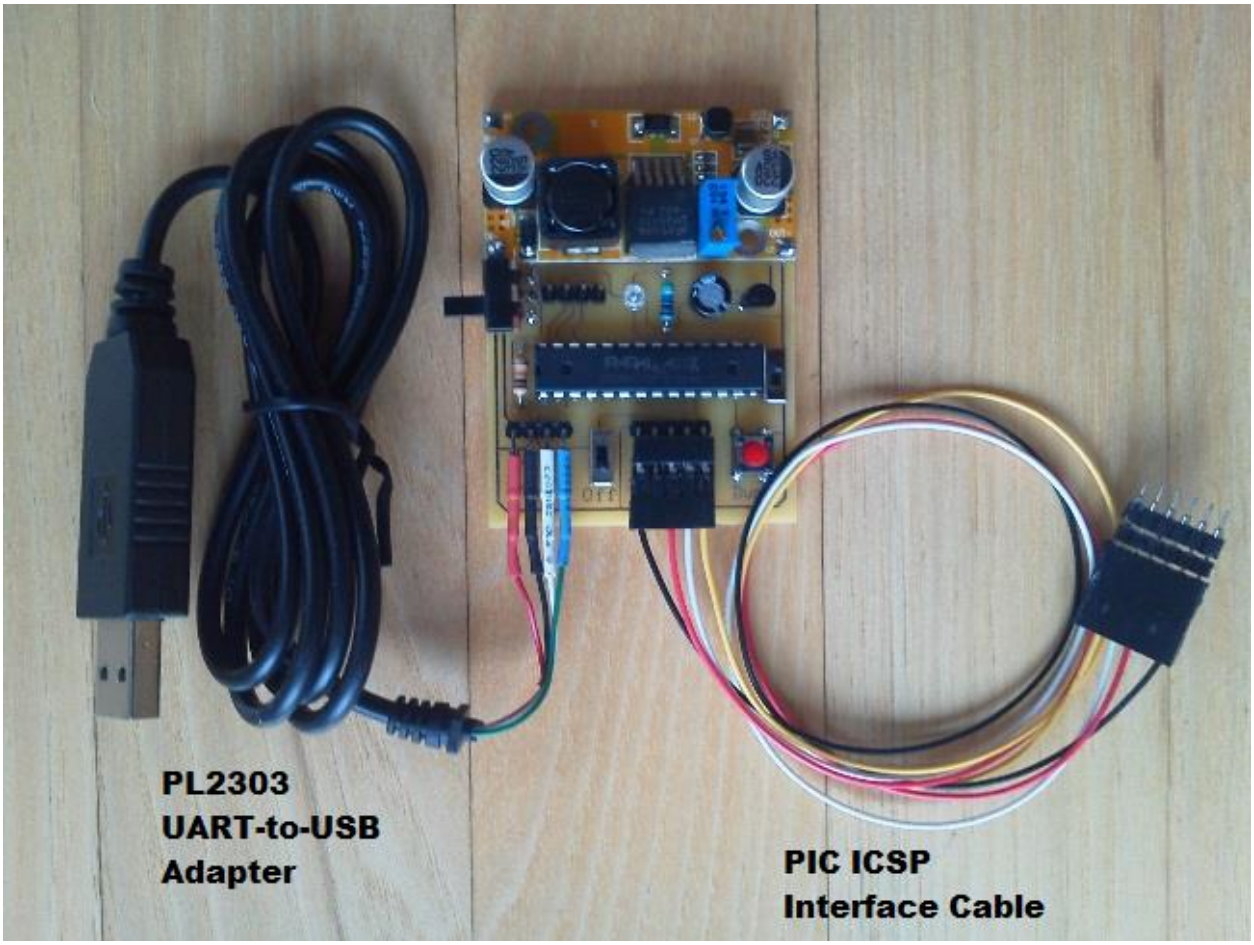
iClass Reader (RevA)
PIC 18F452/18F6621 RAM Dumper
Operating Instructions



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

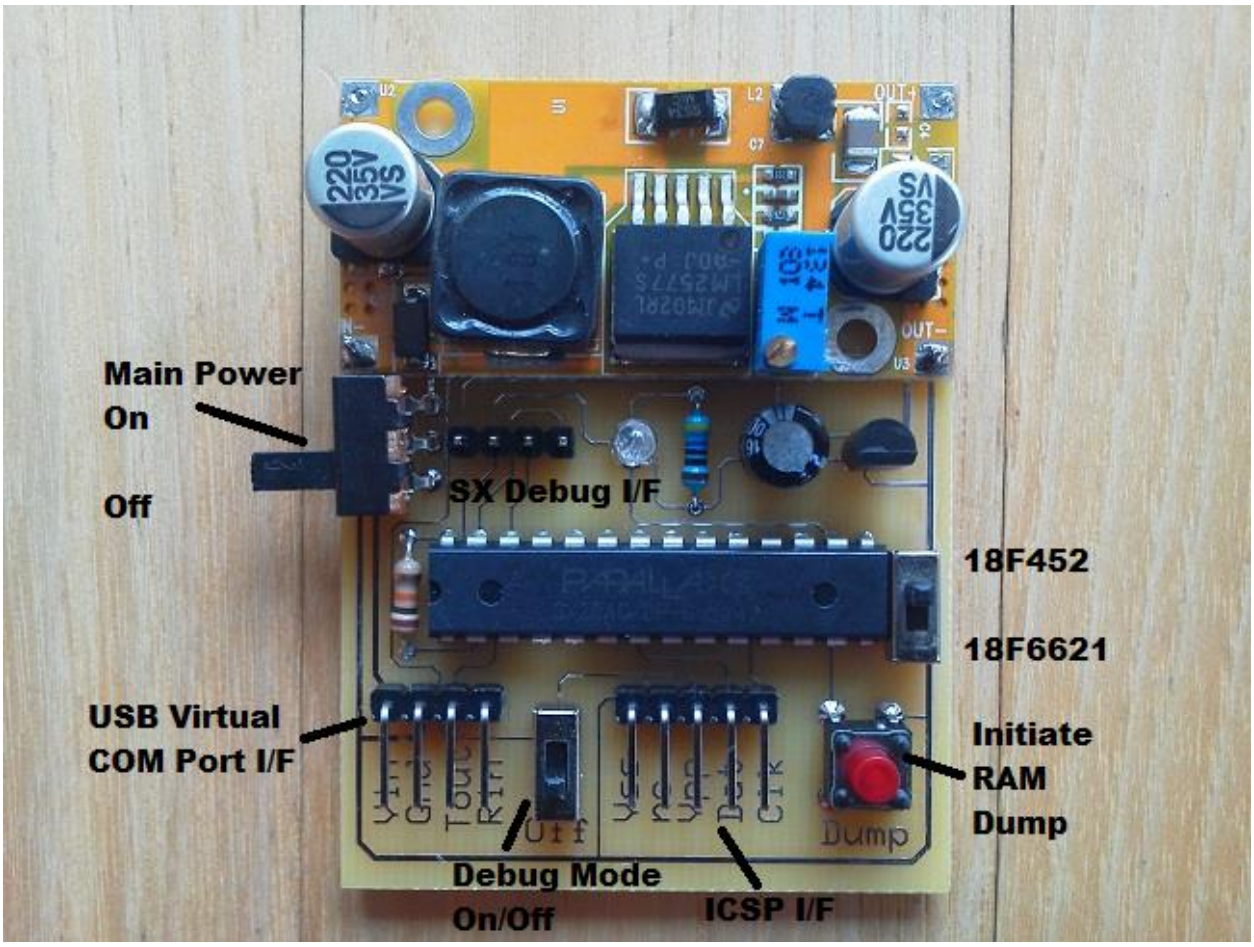


Figure 1. RAM Dumper Circuit Board Layout

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.

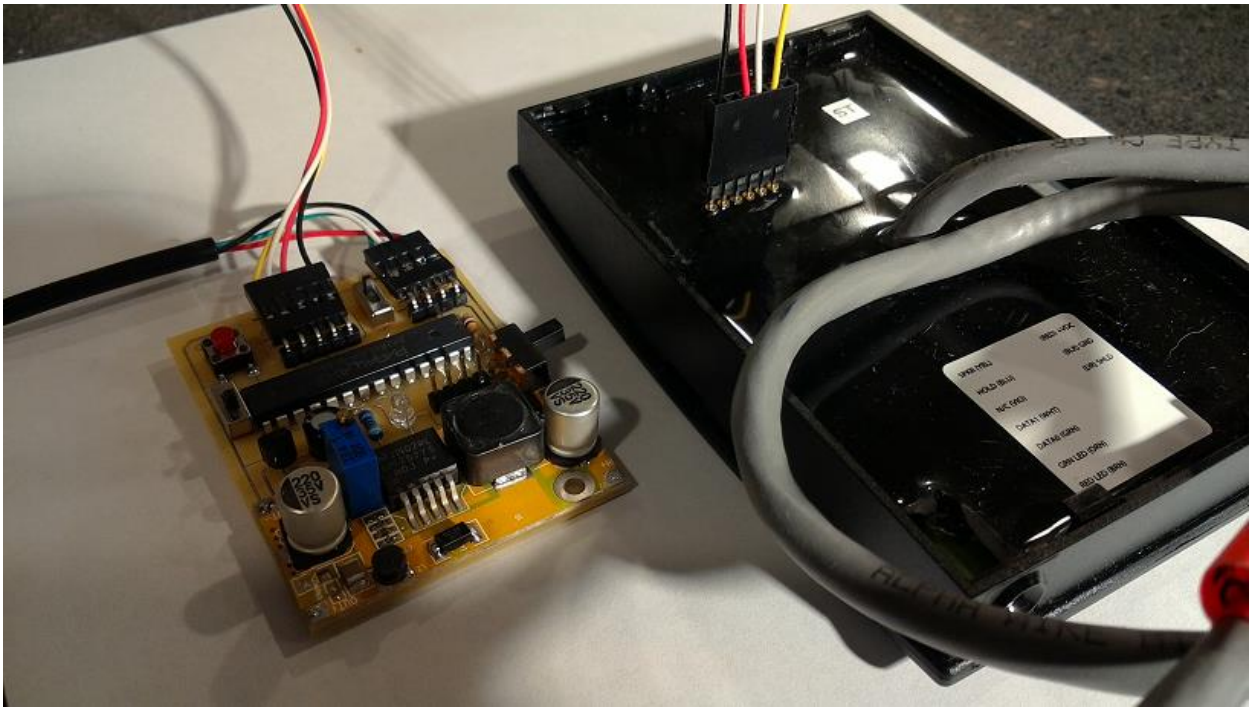
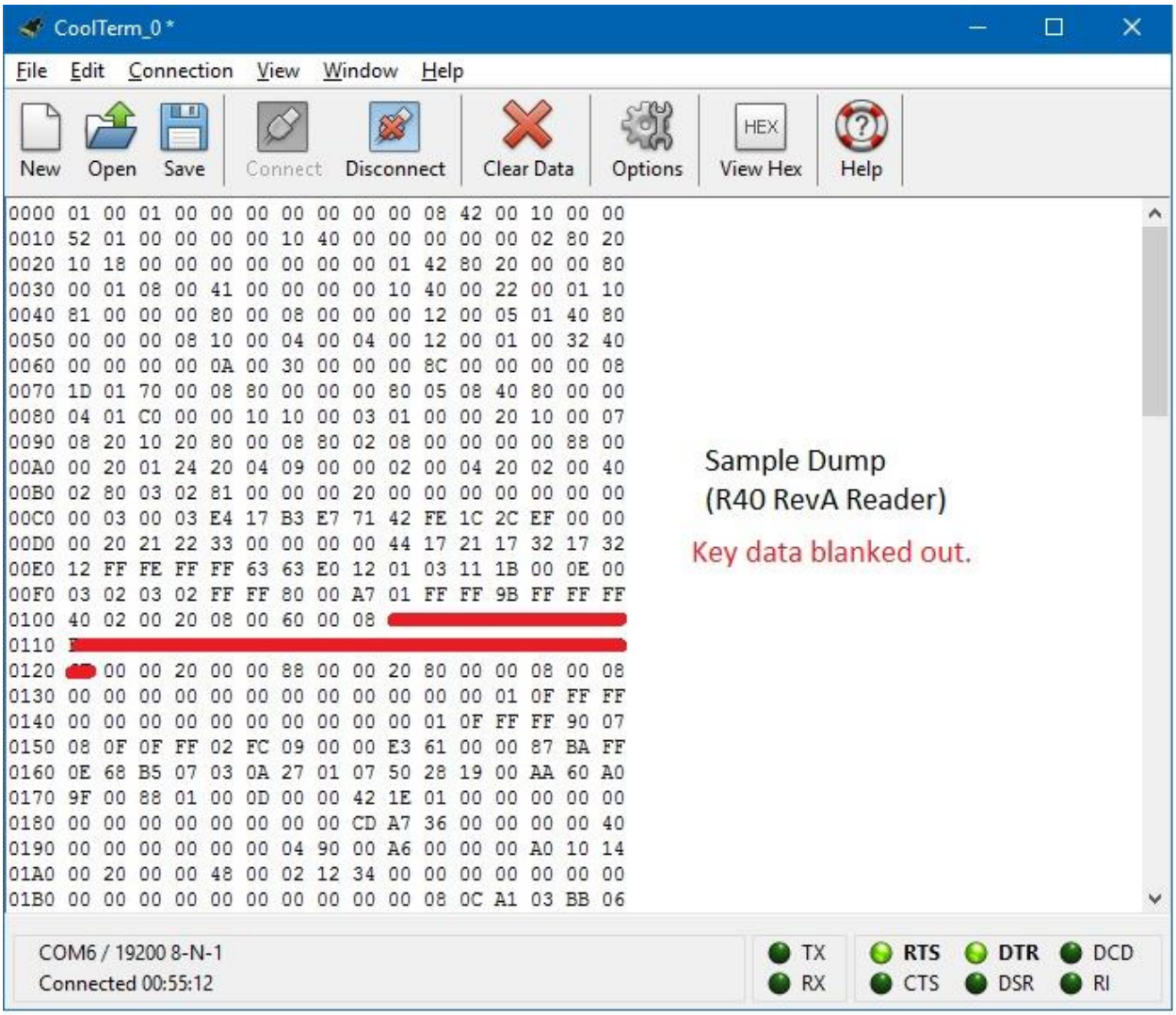


Figure 2. ICSP Connection to R40 Reader (Black Vss/Gnd on outside pin)

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.



Sample Dump
(R40 RevA Reader)

Key data blanked out.