# IoT Reversing Field Manual Cheat Sheet

by djf via cheatography.com/68878/cs/17477/

## Serial Protocols

https://learn.sparkfun.com/tutorials/serial-communication - Good Introduction

## UART

**Details**

UART is a serial protocol used for intere cting with the system. May return a shell, and or access to the fi .

**Enumerate Pinout [Multimeter]**

TX - Voltage fluctuates at boot[1] from 0 to 3.3/5.5v

RX - Constant low value below VCC and above GND

GND - Voltage is constant 0, has 4 traces in a crosss shape[2]

VCC - Normally not used to if device already powered,

[1] Fluctu ation is caused from the debug messages be ing sent.

[2] Testing continuity of GND to other pins, shows ot her pins that may be grounded

Square outlined pin, normally is "pin 1"

## JTAG

**Details**

Used for on-chi p-d ebu gging, generally allows for access to a GNU Debugger (GDB) for the JTAG host. Pinout tware.

## Accessing Serial Consoles

**BASH**

```
sudo dmesg | grep -iC 5 usb
sudo screen -L /dev/t tyUSB0 115200
```

Altern ati vely, use the **Arduino IDE** serial console. y

In the screen command, 115200 is the baud rate of the serial commun ica tions

The baud rate can be determined using - https: //g ith ub.c om /de vtt ys0 /ba udr ate.git

## Hardware Physical Tools

| | |
|---|---|
| JTAGulator | Identifies JTAG & UART pinouts. |
| JTAGenum[1] | Identifies JTAG pinouts |
| Bus Pirate[2] | FT232RL - USB to Serial, Use SOIC8 Clip to dump firmwarez |
| Shikra[3] | FT232H(Q) - USB to Serial |
| RS-232 Generic Adapter[4] | USB to Serial |

[1] JTAGenum Setup Tutorial: https: //p.16.p.ra.eto.xia.n.c.om/.blo.g/j.tag.ula tor -vs -jt age num -to ols -fo r-i den tif yin g -j tag -pi ns- in- iot -de vices

[2] Bus Pirate Pinout Inform ation http:/ /da nge rou spr oto typ es.c om /do cs/ Com mon _Bu s_P ira te_ cab le_ pinouts

[3] Shikra Pinout [UART] D0 - TX, D1 - RX See also, Adafruit FT232H Breakout - https: //c dn- lea rn.a da fru it.c om /do wnl oad s/p df/ ada fru it- ft2 32h -br eak out.pdf

[4] Male DB9: GND - Pin 5, TX - Pin 3, RX - Pin 2