EXPLIOT
www.expliot.io

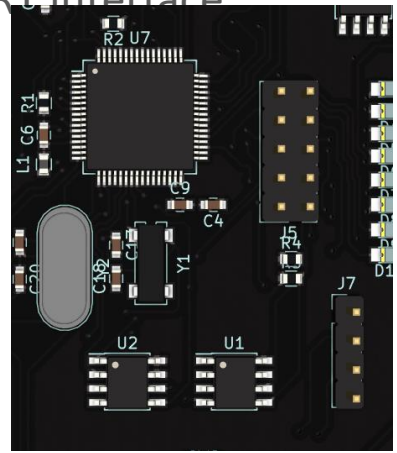
Attacking Hardware

UART

UART Interfacing

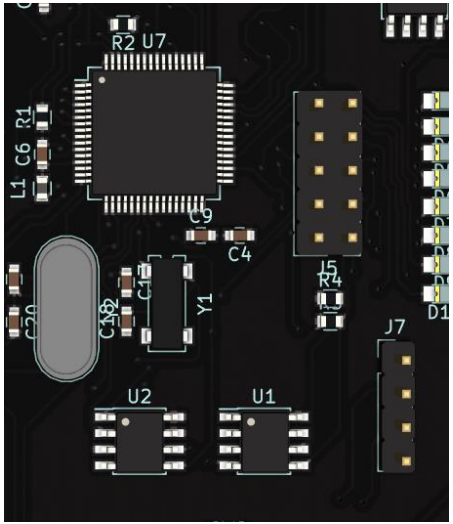
UART identification

- First step in accessing the device is to identify the UART interface
- UART usually has 4 pins
  - GND – Ground
  - Rx – Receive
  - Tx – Transmit
  - Vcc – Voltage
- If we find a set of 4 pins together, we can hope it’s a UART port



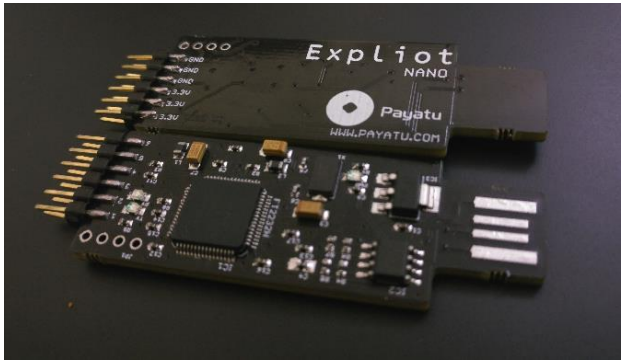
UART identification

- Manual Identification methods
- Method 1 - Digital Multimeter Conductivity Test
- Method 2 - Analyzing PIN voltage and conductivity
- Automated Identification methods
- Using interface scanners like Jtagulator



UART Interfacing

- Identify the UART pins on the board
- Connect the device to your PC
- By connecting UART pins to a USB-Serial convertor
- Access via minicom or any other terminal emulator program



Access UART

- Four step process to access UART on devices

- Locate – Locate the potential UART pins
- Identify – Identify individual pins (GND, Vcc, Tx, Rx)
- Interface – Connect with USB-TTL convertor
- Access – Access the device UART from your computer

UART Pin Identification with Jtagulator

- UART Pin Identification using Jtagulator
- Connect Jtagulator pins with the unknown pins on the
- Board
- Open serial terminal and press ‘h’ for menu then press ‘u’ for UART then press ‘h’ again
- Press ‘v’ for setting the voltage e.g: 3.3v and then press ‘u’ for identifying UART pinout

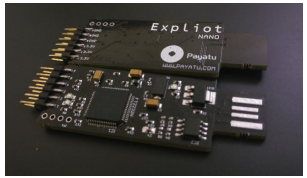
```
> h
Target Interfaces:
J   JTAG/IEEE 1149.1
U   UART/Asynchronous Serial
G   GPIO

General Commands:
V   Set target I/O voltage (1.2V to 3.3V)
I   Display version information
H   Display available commands

> u

UART> h
UART Commands:
U   Identify UART pinout
T   Identify UART pinout (TXD only)
P   UART passthrough
```

UART: Things you need



- Device
- Multimeter
- Expliot Nano and cables
- Wires
- Terminal Emulator (minicom etc)
- Pair of eyes
- Phone flashlight just in case
- Soldering kit if the wires need to be soldered to the pins

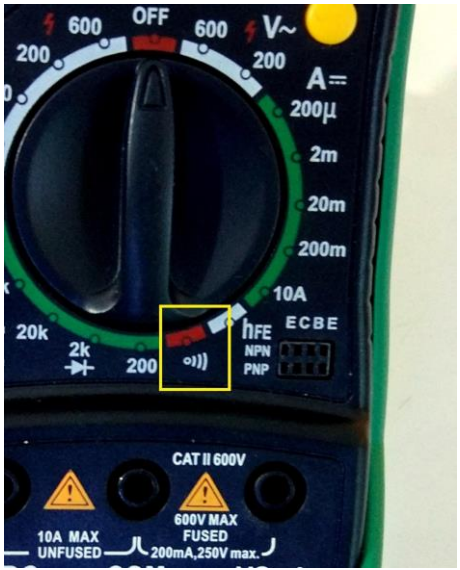
Labs

Lab 1: UART Identification Method 1

- Objective: To identify UART using datasheet and DMM
- Location: <course-dir>/labs/device-uart-lab-1
- If microcontroller is easily identified then download its datasheet. (datasheet copied on the above directory. Go to page 3)
- Go to Pin configuration page and locate UART pins(pin numbers)
- Set your DMM in conductivity mode(yellow box from the picture), touch one probe on the port which is to be identified and another probe on the located UART pins of microcontroller

Lab 1: UART Identification Method 1

- Repeated this test of all the pins until identified
- Vcc and GND can also be identified with the same method



Lab 2: UART Identification Method 2

- Objective:

- Identify the UART pins using voltage tests
- Access the device over the identified UART interface

- Location: NA

Lab 2: Step 1 - Locate

- Objective: Identify the UART pins using voltage tests and access the device using the UART interface
- Open up the device and analyse the board
- Locate any potential UART pin groups
- Typically 4 or more pins in a series
- Mark all the areas that look like potential UART pins
- Test all of them

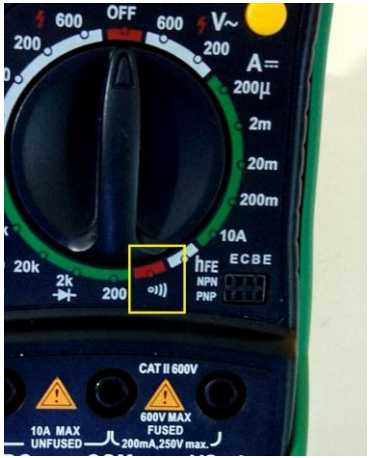
Lab 2: Step 2 - Identify

- Test each pin with multimeter to identify its purpose
- Start with GND
- Vcc
- Tx
- Rx

Lab 2: Step 2 – Identify GND

- Make sure device is powered off
- GND may also look like this -->
- Multimeter continuity test

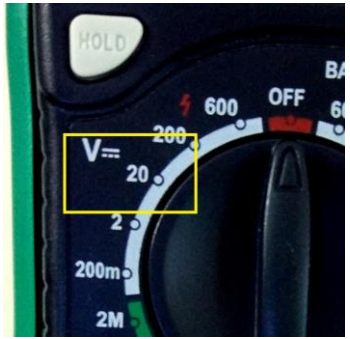
- Point the rotary switch to continuity test
  - the option that looks like this -> o)))
- Identify any metallic sheet area
- Put the red probe on the pin to be tested
- Put the black probe to the GND of input supply
- If the multimeter makes continuous beep it is a GND pin



Lab 2: Step 2 – Identify Vcc

- NOTE: Vcc is not used when connecting to serial interface, but identifying it helps in narrowing our search for Tx and Rx
- Power on the device
- Multimeter Voltage test

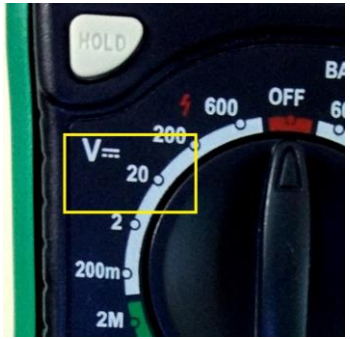
- Point the rotary switch to V (20)
  - (assuming voltage under 20)
  - Incidentally the rotary switch is pointing to V 20 in the image :)
  - Put the red probe on the pin to be tested
  - Put the black probe on the identified GND pin or GND of input supply
  - If the multimeter displays fairly constant voltage (for ex. 3.3) it is Vcc



Lab 2: Step 2 – Identify Tx

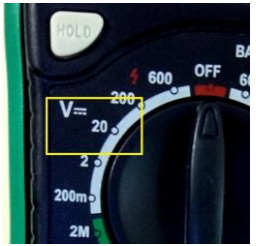
- Power on the device and immediately do the multi-meter test
- Multimeter Voltage test

- Point the rotary switch to V (20)
  - Assuming voltage under 20
  - Incidentally the rotary switch is pointing to V 20 in the image :)
- Put the red probe on the pin to be tested
- Put the black probe on the metallic area
- If the multimeter displays varying voltage it is likely a Tx pin
- If not, Repeat with other pins till you find one



Lab 2: Step 2 – Identify Rx

- Little difficult to identify Rx as there are no specific traits
- Power on the device and immediately do the multimeter test
- Multimeter Voltage test
- Point the rotary switch to V (20)
    - Assuming voltage under 20
    - Incidentally the rotary switch is pointing to V 20 in the image :)
- Put the red probe on the pin to be tested
- Put the black probe on the metallic area



Lab 2: Step 2 – Identify Rx

- Multimeter Voltage test

- Put the black probe on the metallic area
- In some cases will show constant voltage either low or high
- In some cases it will show varying voltage
- In my experience I have encountered constant low voltage
- If not found, Repeat with other pins, if any left, till you find one

NOTE: If we identify the other 3 pins successfully, and there are only 4 pins then the one left is Rx

Lab 2: Step 2 – Identify Rx

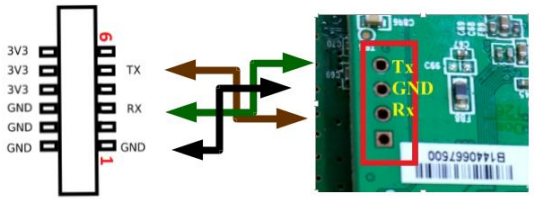
- Multimeter Voltage test

- Put the black probe on the metallic area
- In some cases will show constant voltage either low or high
- In some cases it will show varying voltage
- In my experience I have encountered constant low voltage
- If not found, Repeat with other pins, if any left, till you find one

NOTE: If we identify the other 3 pins successfully, and there are only 4 pins then the one left is Rx

Lab 2: Step 3 - Interface

- Connect the Expliot Nano with the UART pins on the board using wires and breakaway headers.
- Check Expliot Nano Specs for pin details
- Solder wires/headers if required



Expliot Nano TX <---------- > RX UART Pin on board

Expliot Nano RX <---------- >TX UART Pin on board

Expliot Nano GND <----------> GND UART Pin on board

Lab 2: Step 4 - Access

- The port can be accessed via /dev/ttyUSB0
- Power on the device and immediately run a serial console utility
- Utilities for serial console access

- Minicom
- Screen

- Cmd: sudo minicom -b <baudrate> -D <device>

  -b <baudrate>: baudrate to use, default is 115200

  -D <device>: serial port to use for ex. /dev/ttyUSB0

  Ex: sudo minicom -b 115200 -D /dev/ttyUSB0

Lab 2: Step 4 - Access

- Most devices will have default baudrate of 115200
- If you see binary garbage data it is most likely that the baudrate specified is wrong.
- Use Baudrate.py – An excellent tool to detect baudrate created by Craig Heffner
- Source: https://code.google.com/p/baudrate/
- Next slide shows how to use baudrate.py

Lab 2: Step 4 - Access

- Power on the machine and immediately run baudrate.py
- Cmd: sudo baudrate.py -p <serial port>
- Ex: baudrate.py -p /dev/ttyUSB0
- Down arrow key will cause baudrate.py to shift to a lower baudrate
- Up arrow key will cause baudrate.py to shift to a higher baudrate
- It starts with 115200. if you see garbage press down arrow and test with lower baudrate, repeat it till you find the correct baudrate
- Baudrate.py -a option auto detect mode, so you dont have to press Up/Down arrow keys

Lab 2: Step 4 - Access

- Once it is detected Press CTL-C and baudrate will ask you for a name to save the config for minicom (give any name, you can later run sudo minicom <name> to use the correct configuration)
- It will also ask you if you want to run minicom, choose yes and run it.
- NOTE: You may not get shell in baudrate.py, so you may have to let baudrate.py run minicom(CTL-C in baudrate.py as mentioned above), once minicom runs, press enter to check the shell
- To exit from a minicom session Press CTL-A and then X

The End