BRICK ALL THE THINGS EP. 1

a crash course in hw

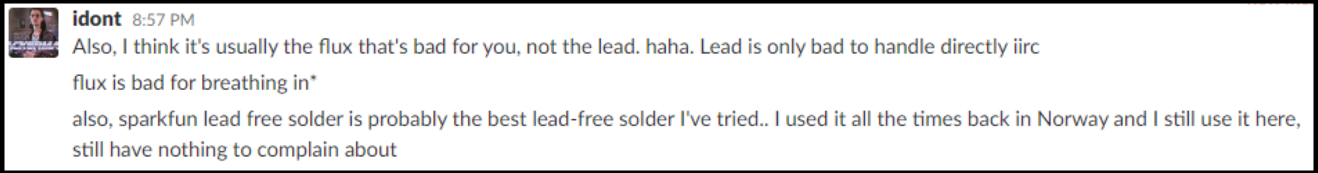
HOW2PLAY NOT BRICKING YOURSELF

Be aware of static electricity.

Think before you touch.

Solder in a well ventilated space.
(also, fuck lead-free*)

If you’re not sure, don’t touch it.



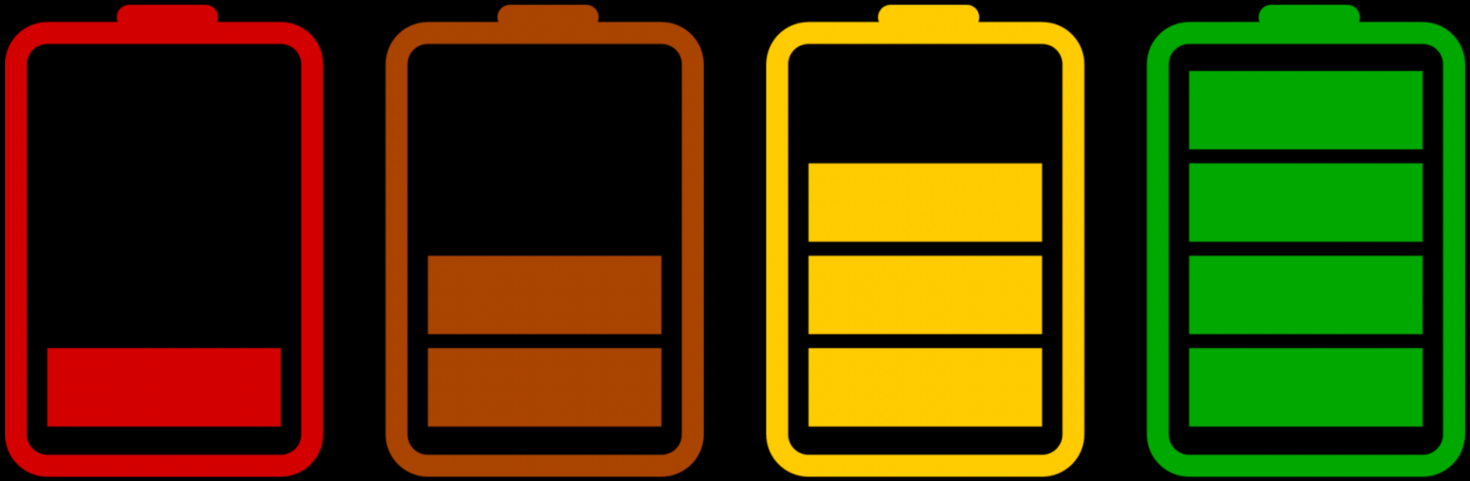
idont 8:57 PM

Also, I think it's usually the flux that's bad for you, not the lead. haha. Lead is only bad to handle directly iirc

flux is bad for breathing in*

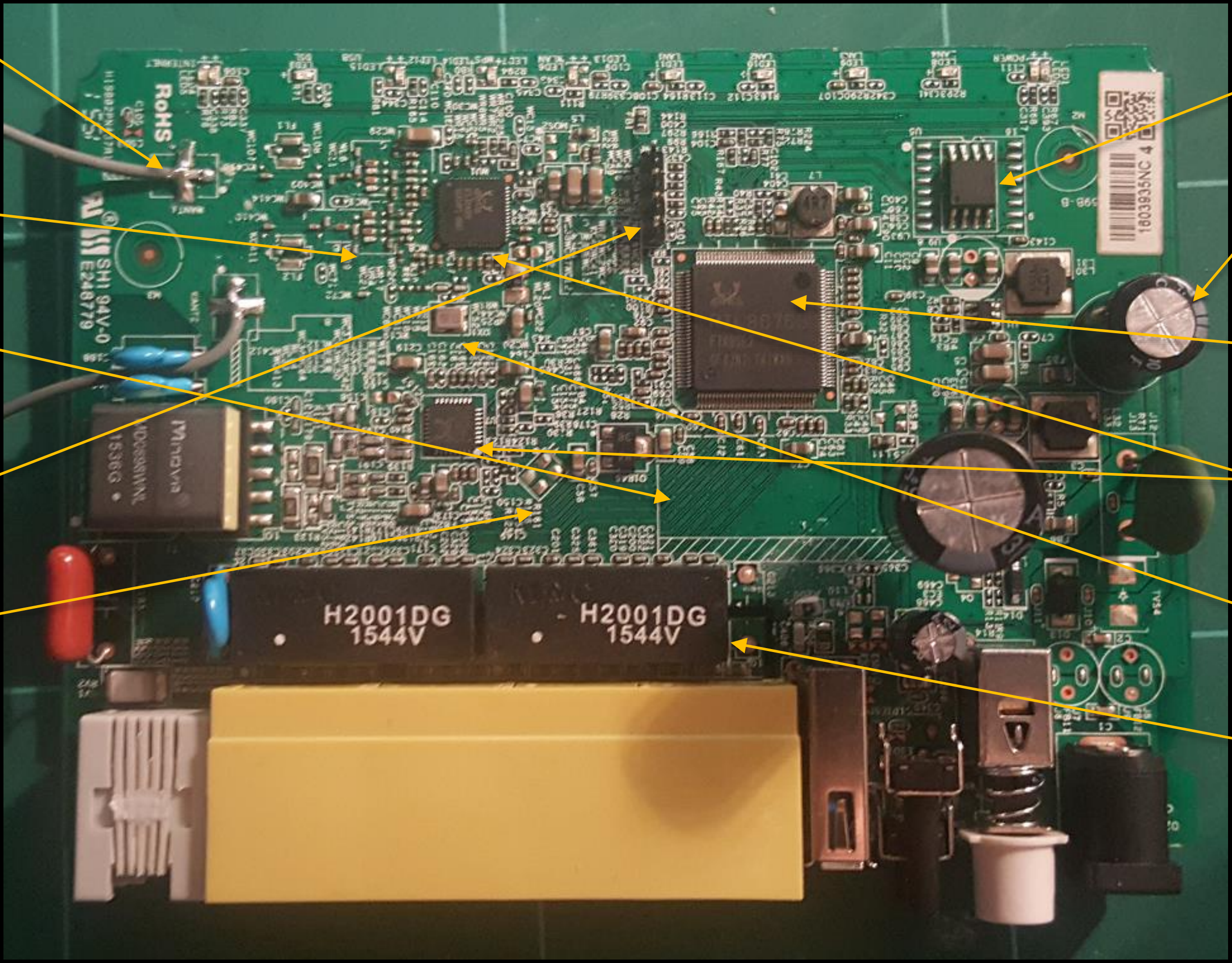
also, sparkfun lead free solder is probably the best lead-free solder I've tried.. I used it all the times back in Norway and I still use it here, still have nothing to complain about

TTL, GROUND, AND YOU.



DISASSEMBLING EQUIPMENT

LET’S GO: DSL2750U



These go out to the WiFi Antennas.

SMD Resistors and Caps. Many can be removed.

Scrape away the solder mask to reveal copper.

Pre-soldered test points ☺

Missing components? Test points?!

This is the Flash chip. This is like a hard drive

These are capacitors, they stabilize power.

This is a microcontroller. It’s your CPU.

Components will have their own controllers

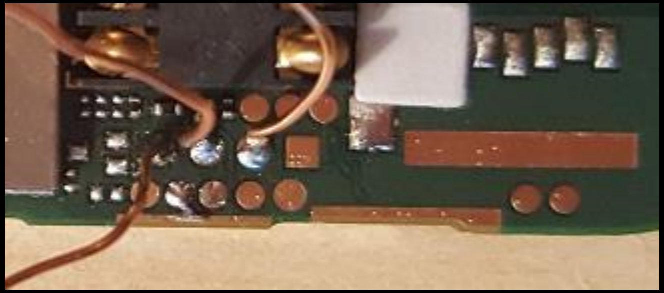
This is an oscillator. It’s the “clock” for the board.

These are DC-DC voltage converters.

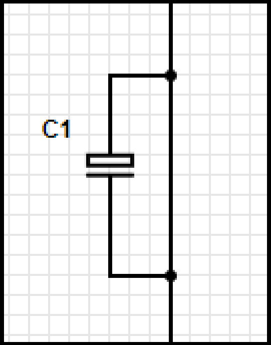
TEST POINTS AND YOU

- Exposed circular pads
  - Group of 4/6 = UART
  - Group of ~10 = Maybe JTAG
  - Individual = “Is XYZ Powered”
- Scrape away solder mask to reveal copper
- Solder directly to components
  - Solder directly onto a pin = passively read signal
  - Remove the component and “intercepting” the signal = interact with the component
- Typically not pre-soldered

Anything’s a test point if you’re brave enough



NOISE REDUCTION

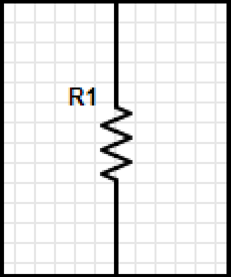


Capacitors store charge, if power is reduced on the “host” wire, a decoupling capacitor will discharge, providing power until power is restored (like a micro-UPS).

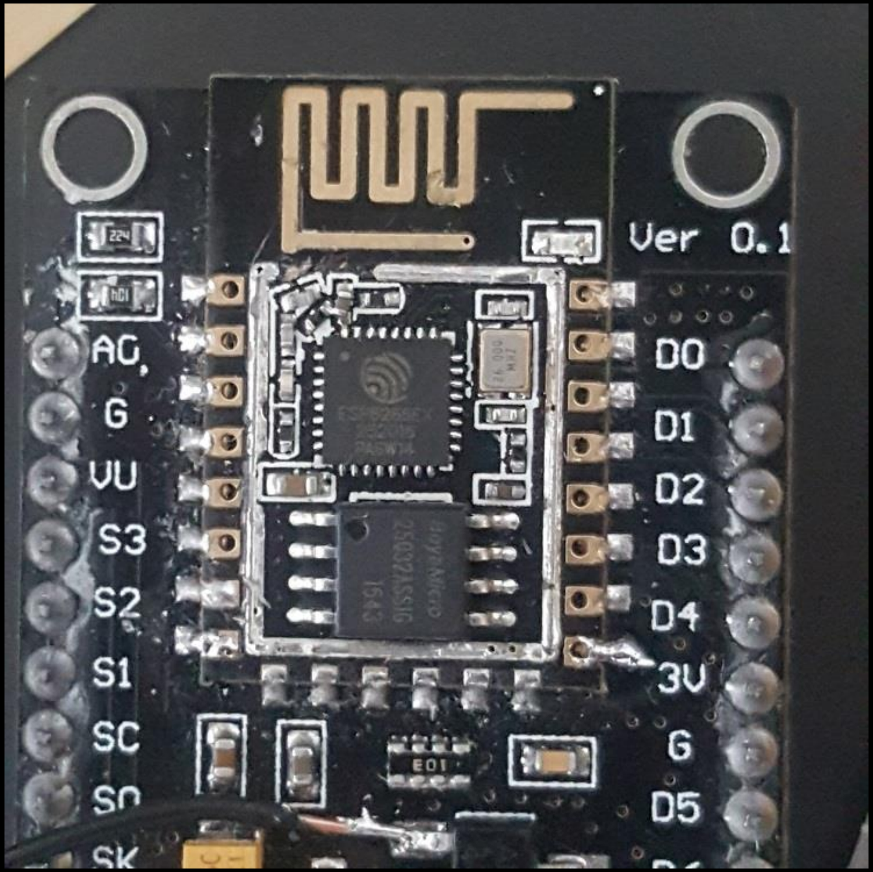
If the capacitor is “full”, it won’t charge (and will act like an open circuit). This is used for power supply wires.

Resistors resist current. Long story short, resistors in series at either end of a signal line act to reduce noise.

For the full explanation:
https://electronics.stackexchange.com/questions/7709/why-put-a-resistor-in-series-with-signal-line



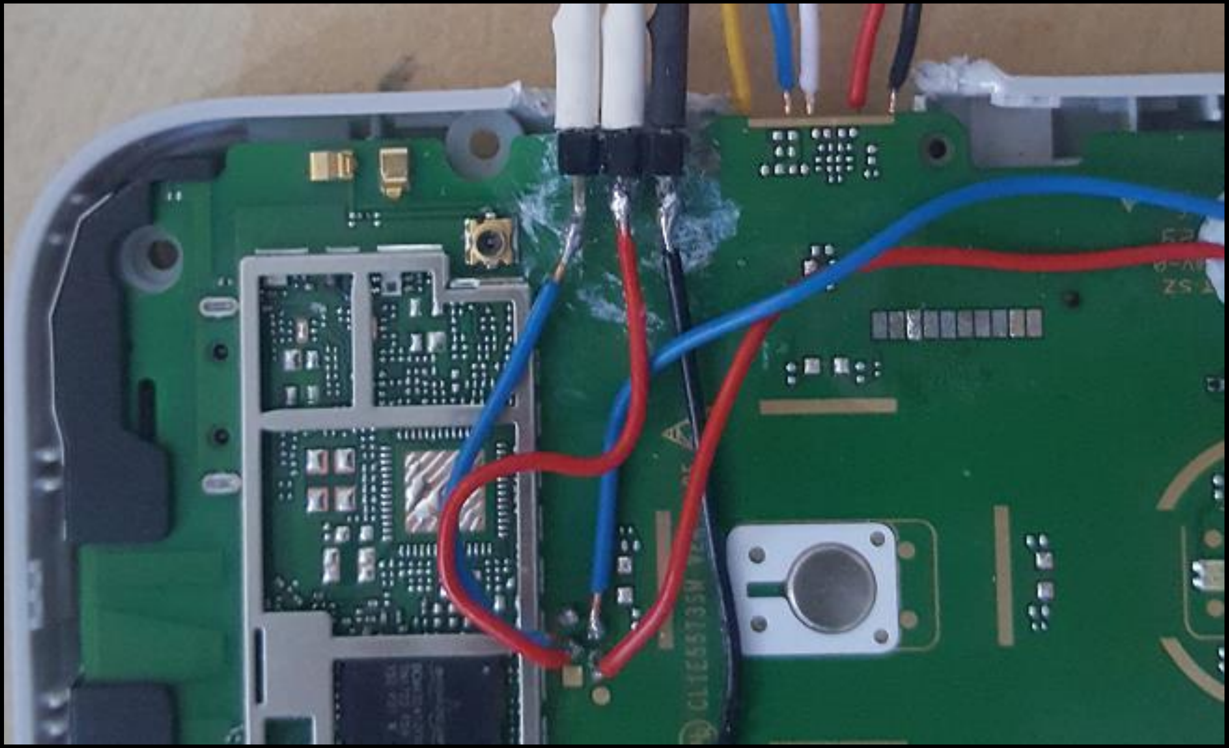
NOISE REDUCTION



UART

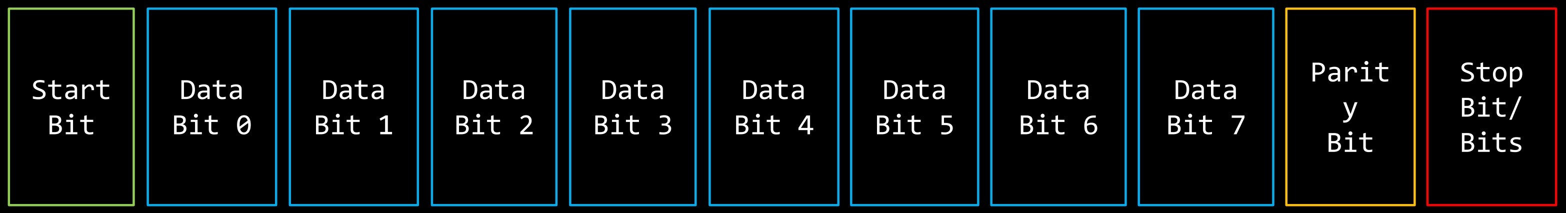
- Universal Asynchronous Receiver/Transmitter
- In serial communication, one device sends data one bit at a time to another device.
- UART is a serial communications protocol – it defines the format of these bits so that both devices can understand each other
- 2 pins:
  - RX – This is how a device receives incoming data.
  - TX – This is how a device sends data to the other device
  - The RX of one device connects to the TX of the other device – a full duplex connection

UART



UART

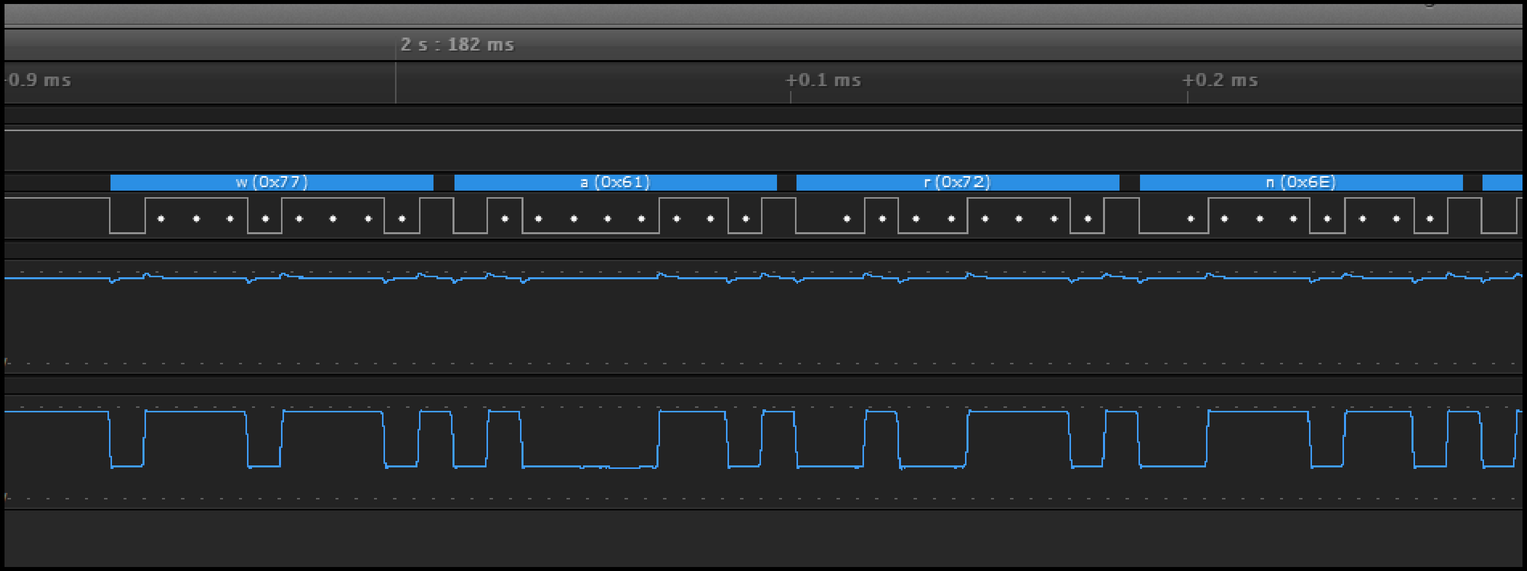
- What’s in a UART packet?



Start Bit	Data Bit 0	Data Bit 1	Data Bit 2	Data Bit 3	Data Bit 4	Data Bit 5	Data Bit 6	Data Bit 7	Parity Bit	Stop Bit/Bits

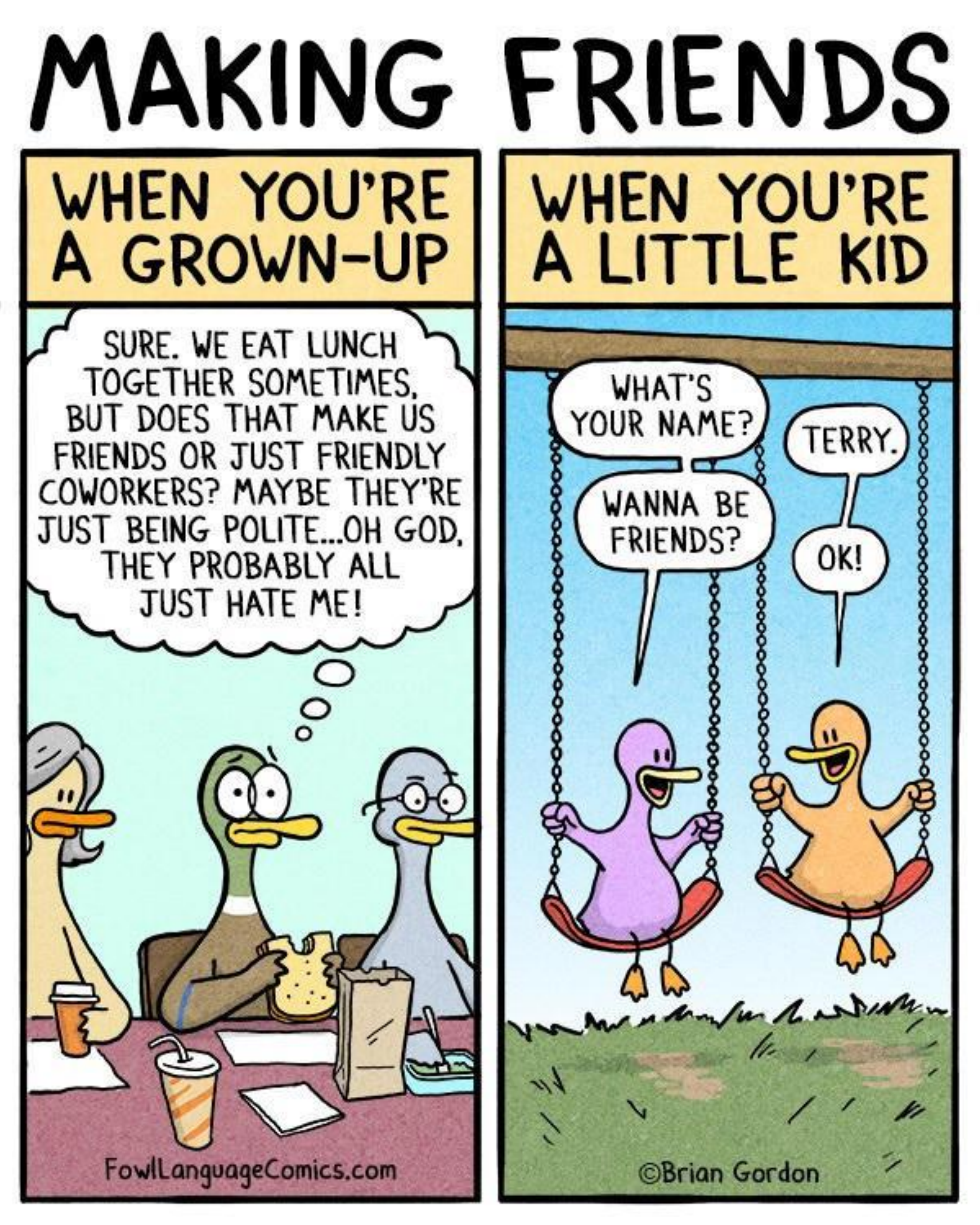
- The packet will have a start bit and either 1 or 2 stop bits at the end
- Can be 5-8 data bits (or up to 9 data bits if no parity bit)
- A parity bit may also be sent.
  - If there is an even number of 1’s in the data bits, the parity bit will be 0. Otherwise it will be 1
  - Useful to check if there was an error (bit flip)
- Baud rate – how fast data is transmitted. 9600 baud = 9600 bits per second

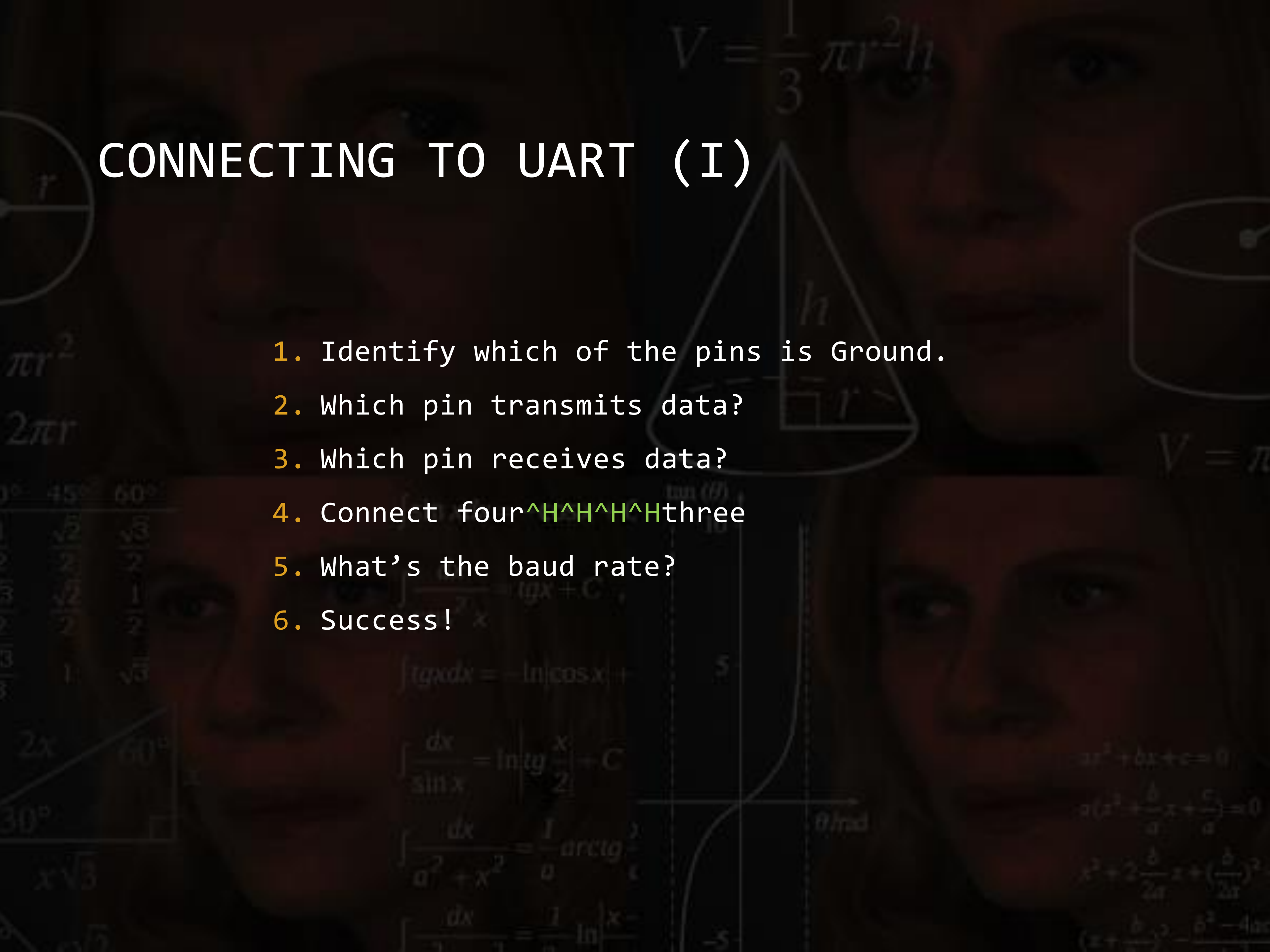
UART



UART AND TTL

- UART is the protocol – it says what bits should be logic 1 and logic 0
- TTL describes the voltage levels – it says what the voltage level for logic 1 and logic 0 is.
  - TTL logic 0 is 0 V, and logic 1 is 1.?V to 5V
- There other standards as opposed to TTL, like RS-232 which uses UART. An RS-232 connection can have -3V to -25V for logic 1 and +3V to +25V for logic 0.
- We can’t connect two UART devices with RS-232 and TTL together directly!


MAKING FRIENDS
WHEN YOU'RE A GROWN-UP
SURE. WE EAT LUNCH TOGETHER SOMETIMES, BUT DOES THAT MAKE US FRIENDS OR JUST FRIENDLY COWORKERS? MAYBE THEY'RE JUST BEING POLITE...OH GOD, THEY PROBABLY ALL JUST HATE ME!
FowlLanguageComics.com
WHEN YOU'RE A LITTLE KID
WHAT'S YOUR NAME?
TERRY.
WANNA BE FRIENDS?
OK!
©Brian Gordon



CONNECTING TO UART (I)

1. Identify which of the pins is Ground.
2. Which pin transmits data?
3. Which pin receives data?
4. Connect four^H^H^H^Hthree
5. What’s the baud rate?
6. Success!

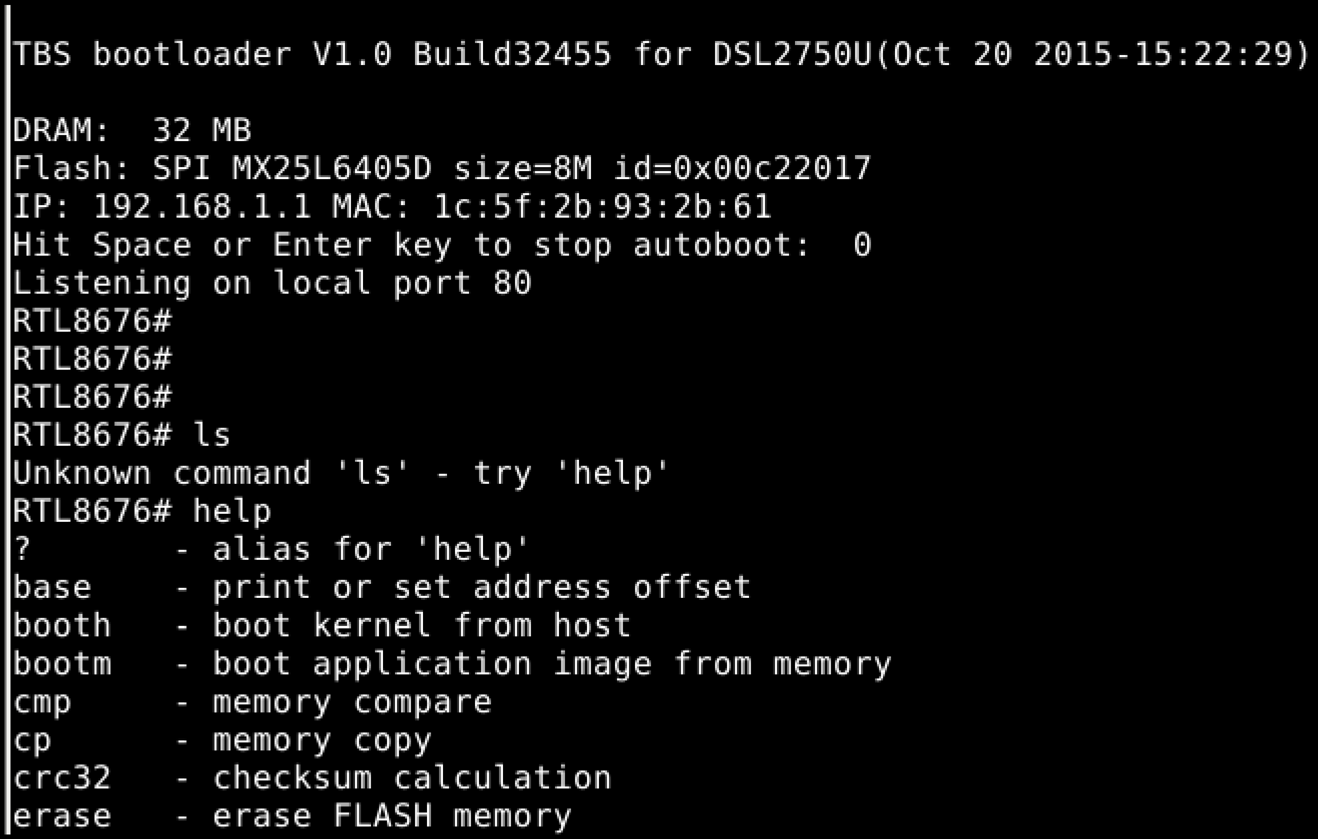
CONNECTING TO UART (II)

```
minicom -s
```

```
screen /dev/ttyUSB0 115200
screen /dev/cu.usbserial 115200
```

```
putty.exe (COM Port)
```

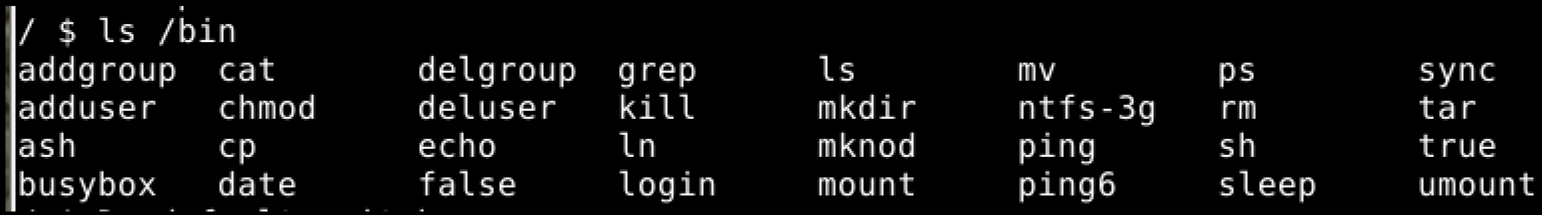
BUSYBOX (I)



```
TBS bootloader V1.0 Build32455 for DSL2750U(Oct 20 2015-15:22:29)

DRAM:  32 MB
Flash: SPI MX25L6405D size=8M id=0x00c22017
IP: 192.168.1.1 MAC: 1c:5f:2b:93:2b:61
Hit Space or Enter key to stop autoboot:  0
Listening on local port 80
RTL8676#
RTL8676#
RTL8676#
RTL8676# ls
Unknown command 'ls' - try 'help'
RTL8676# help
?       - alias for 'help'
base    - print or set address offset
booth   - boot kernel from host
bootm   - boot application image from memory
cmp     - memory compare
cp      - memory copy
crc32   - checksum calculation
erase   - erase FLASH memory
```

BUSYBOX (II)



```
/ $ ls /bin
addgroup  cat       delgroup  grep      ls        mv        ps        sync
adduser   chmod     deluser   kill      mkdir     ntfs-3g   rm        tar
ash       cp        echo      ln        mknod     ping      sh        true
busybox   date      false     login     mount     ping6     sleep     umount
```

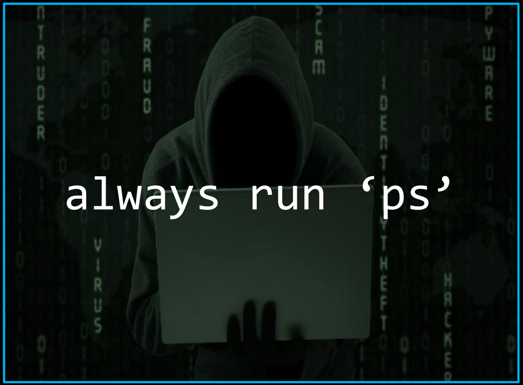
FUN THINGS TO DO...

uploading files, no wget?

```
echo “\x01\x02\x03” > a
```

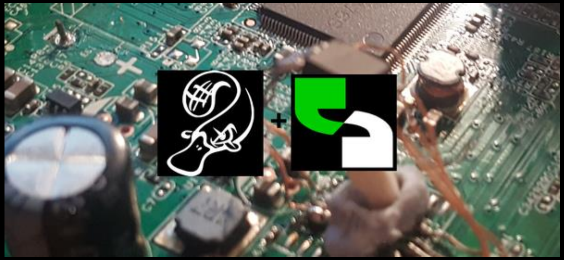
need to dump flash?

```
cat /mtd*
```



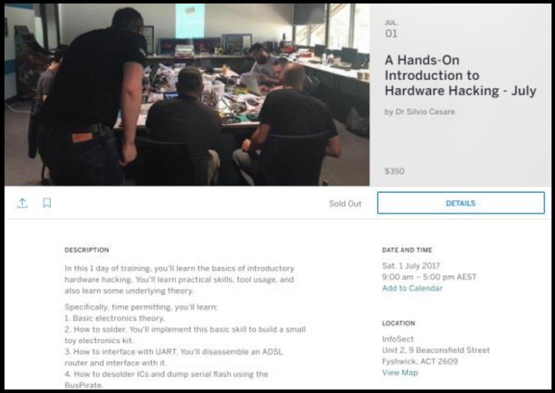
always run ‘ps’

I WANT TO LEARN MORE!



We’re running 2 more of these sessions in the future. If you’re keen on presenting, let me or pi3ch know.

Also, Silvio runs an epic hardware course (and actually knows what he’s doing). Find him at .au cons =]



JUL
01

A Hands-On Introduction to Hardware Hacking - July

by Dr Silvio Cesare

$350

DESCRIPTION

In this 1 day of training, you'll learn the basics of introductory hardware hacking. You'll learn practical skills, tool usage, and also learn some underlying theory.

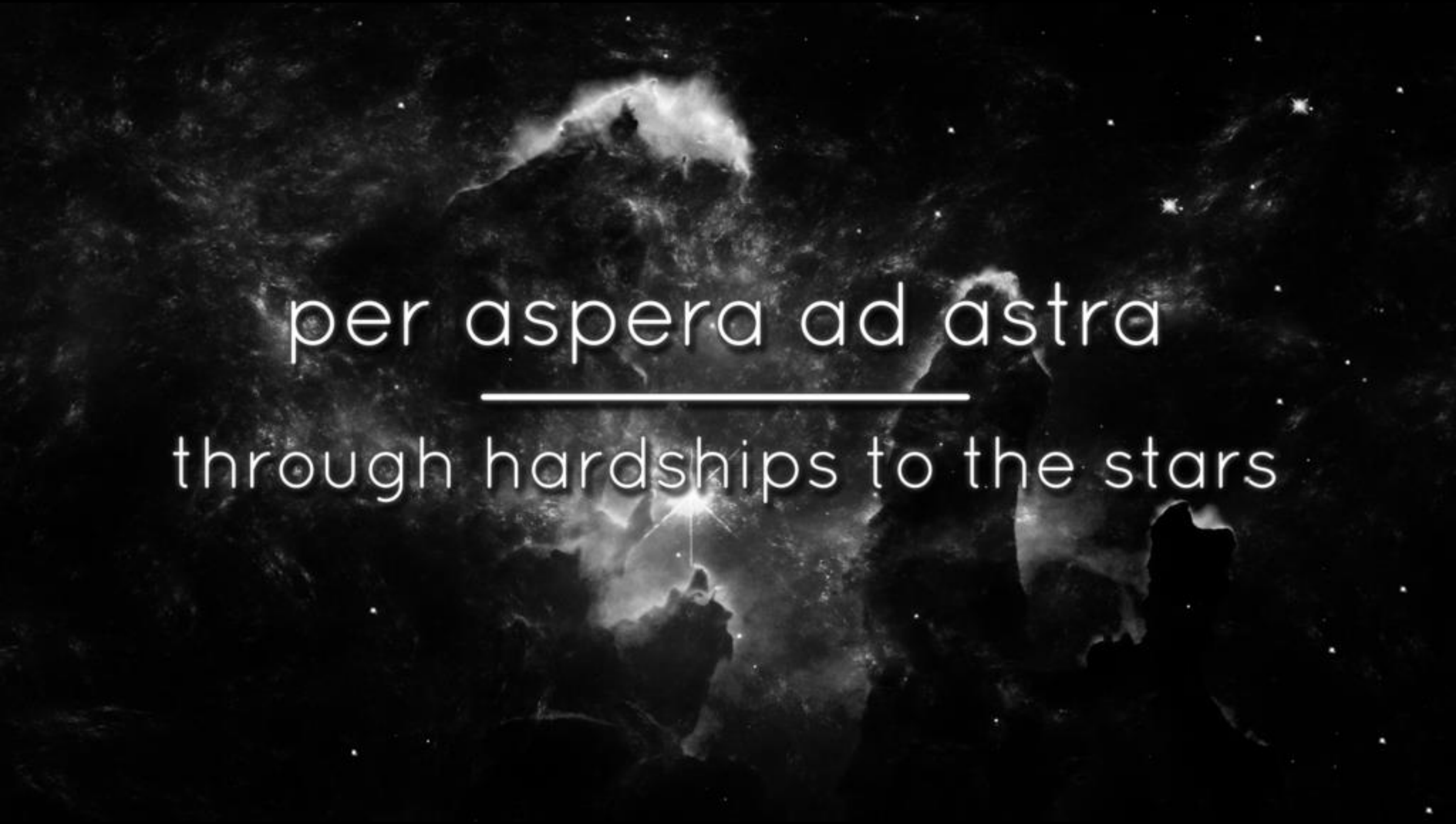
Specifically, time permitting, you'll learn:
1. Basic electronics theory.
2. How to solder. You'll implement this basic skill to build a small toy electronics kit.
3. How to interface with UART. You'll disassemble an ADSL router and interface with it.
4. How to desolder ICs and dump serial flash using the BusPirate.

DATE AND TIME

Sat, 1 July 2017
9:00 am – 5:00 pm AEST
Add to Calendar

LOCATION

InfoSect
Unit 2, 9 Beaconsfield Street
Fyshwick, ACT 2609
View Map



per aspera ad astra

through hardships to the stars

THANKYOU

questions? lin_s on slack

thankyou everyone for making this awesome =]