Mason Competitive Cyber

Take the “Hard” out of Hardware with Science- not really

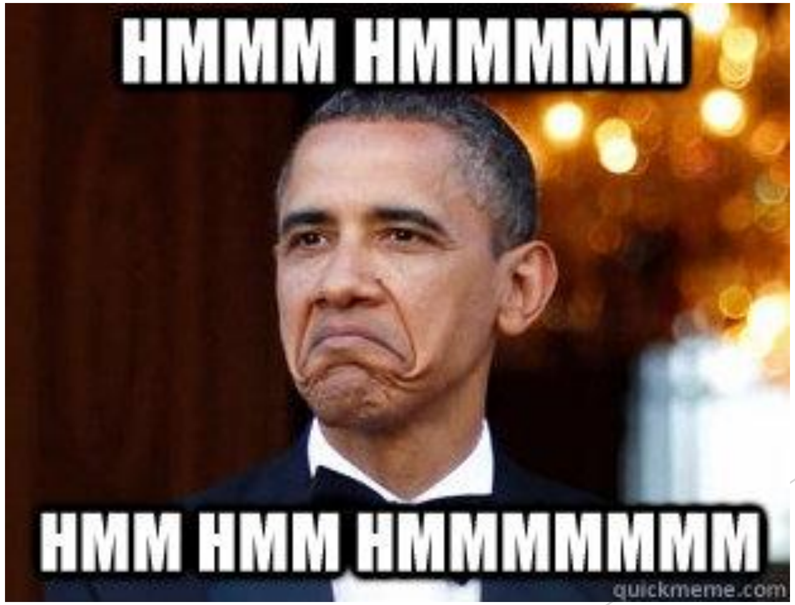
http://lacrossearthscience.weebly.com/extrasscience-memes.html

Agenda

- whoami
- Information Gathering
- Tear down
- Debugging port
- Firmware/data extraction

whoami

- Security Researcher
  - @ Uffect Corp / Strange Labs
- Competition Officer for MasonCC
- Insta: @tthuc_3496 ; Twitter: @its_EZBB
- I’m on Slack – ping me if you have any question.



http://www.quickmeme.com/meme/3rov5x

Researching/ Information Gathering

- As Much Information As Possible.
  - THE WEB
    - Google
    - Forums / Blogs
    - Manufacture site
- Product specification, design documents, etc.
- Acquiring Hardware:
  - Amazon – 2 days shipping <3
  - Ebays
  - Buy, borrow, rent, … and don’t steal !!
- AND ALSO …….

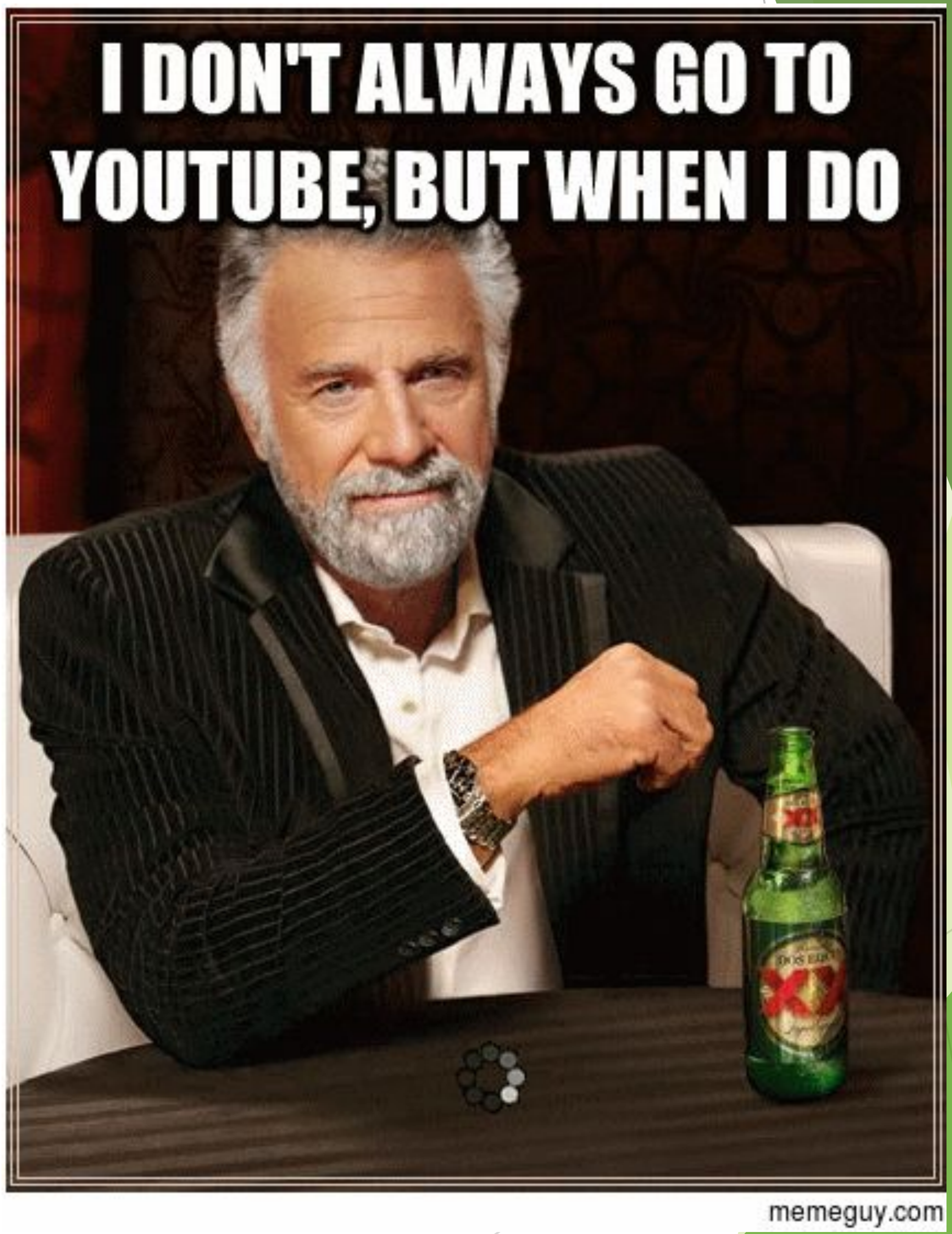
Researching/ Information Gathering

- “Making Friends”
  - Go talk to people for once.
  - You can learn a lot.

http://www.quickmeme.com/meme/3qda31

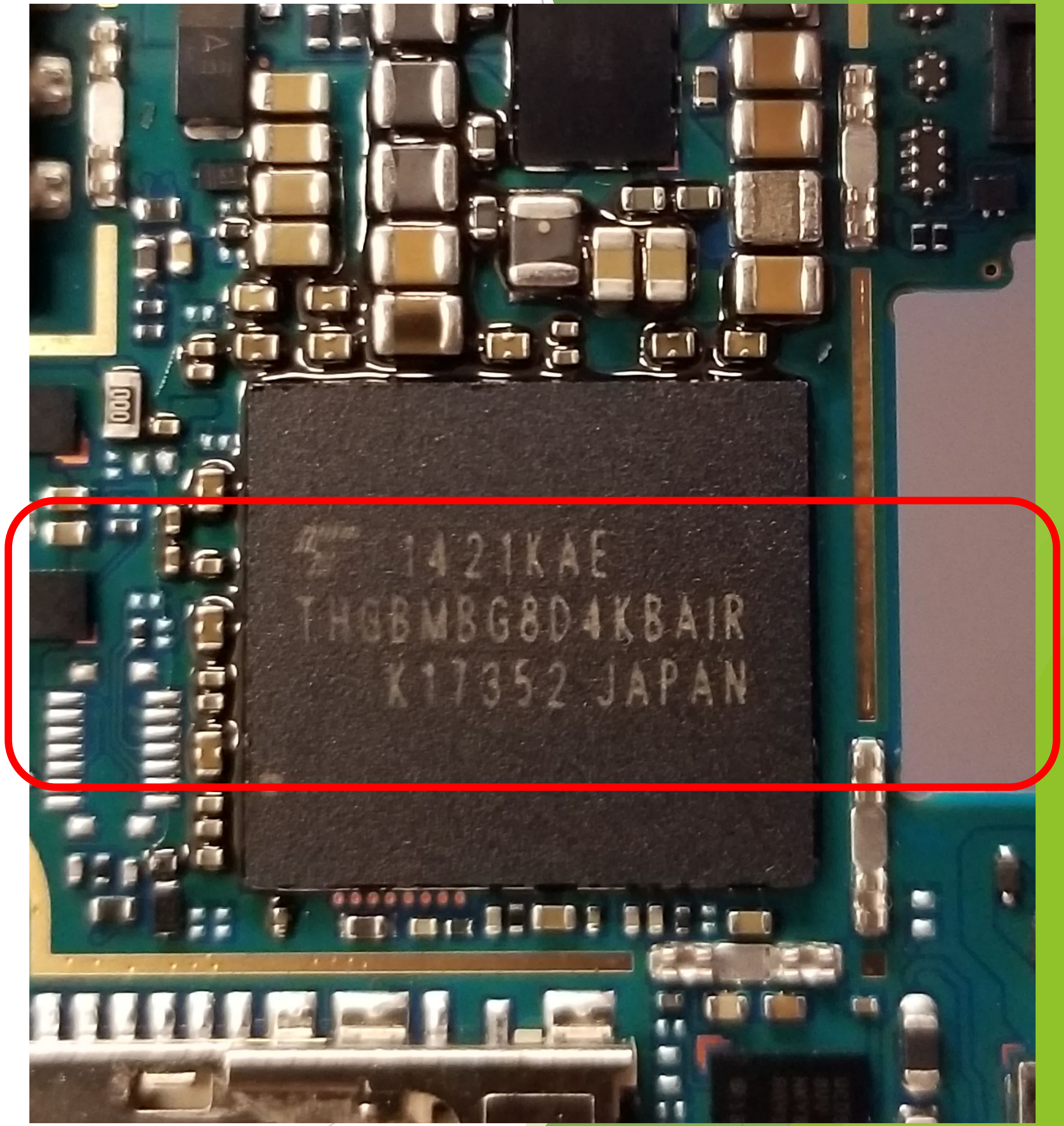
Tearing down

- Taking it apart
  - Screws, glues, tapes
- GOAL:
  - To get to the juice aka the main board.
- Lots of time, screws are hidden:
  - Under labels, rubber “thing”
- Guides:
  - https://www.ifixit.com/
  - And https://www.youtube.com/

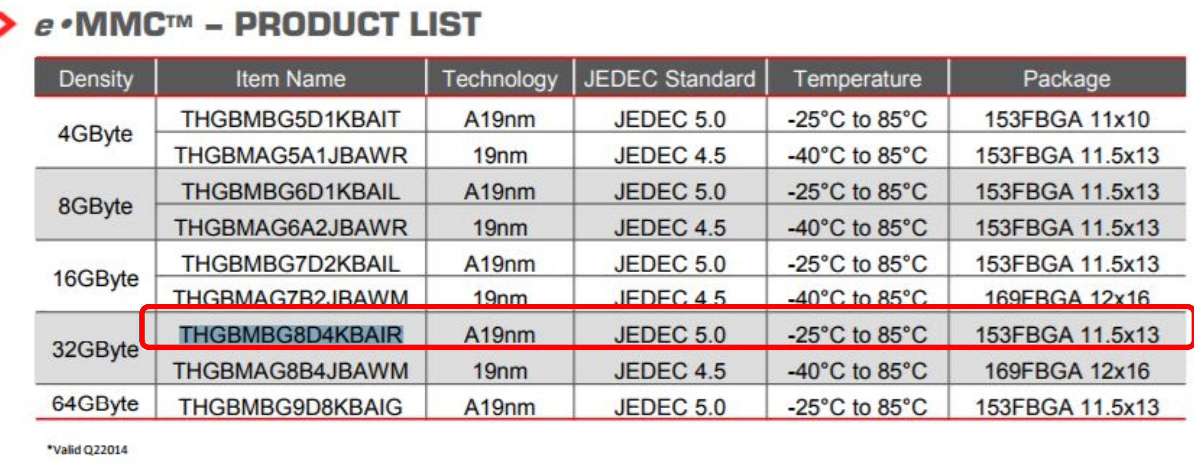


More Info Gathering

- Chips
  - What they are.
    - WiFi, RAM, CPU, …
  - Datasheets
    - Search engine: Google, Baidu
    - Datasheet sites: datasheet360, datasheetcatalog.
    - Alibaba
- THGBMBG8D4KBAIR
  - Let’s search for it.



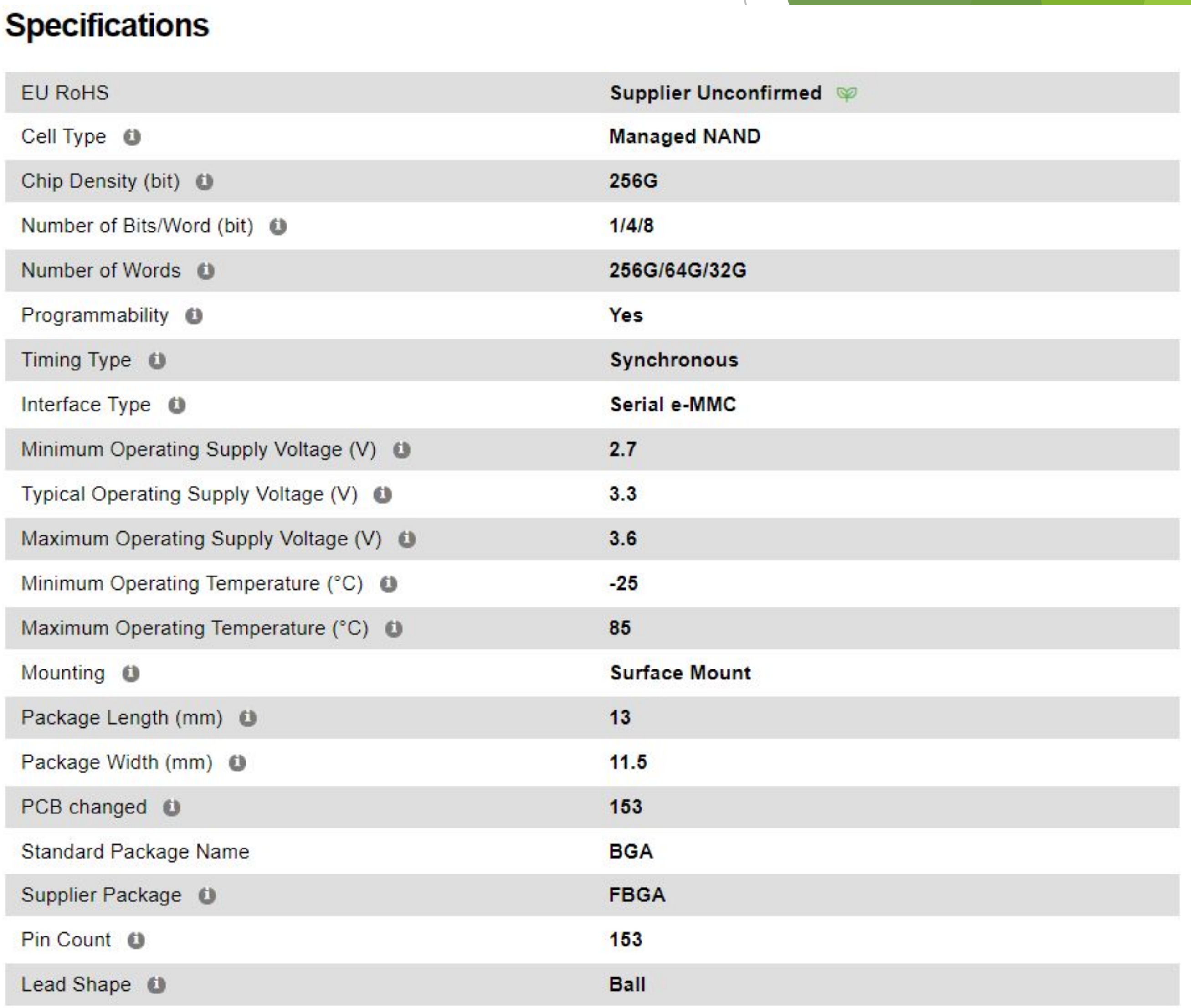
More Info Gathering



e•MMC™ – PRODUCT LIST

Density	Item Name	Technology	JEDEC Standard	Temperature	Package
4GByte	THGBMBG5D1KBAIT	A19nm	JEDEC 5.0	-25°C to 85°C	153FBGA 11x10
	THGBMAG5A1JBAWR	19nm	JEDEC 4.5	-40°C to 85°C	153FBGA 11.5x13
8GByte	THGBMBG6D1KBAIL	A19nm	JEDEC 5.0	-25°C to 85°C	153FBGA 11.5x13
	THGBMAG6A2JBAWR	19nm	JEDEC 4.5	-40°C to 85°C	153FBGA 11.5x13
16GByte	THGBMBG7D2KBAIL	A19nm	JEDEC 5.0	-25°C to 85°C	153FBGA 11.5x13
	THGBMAG7B2JBAWM	19nm	JEDEC 4.5	-40°C to 85°C	169FBGA 12x16
32GByte	THGBMBG8D4KBAIR	A19nm	JEDEC 5.0	-25°C to 85°C	153FBGA 11.5x13
	THGBMAG8B4JBAWM	19nm	JEDEC 4.5	-40°C to 85°C	169FBGA 12x16
64GByte	THGBMBG9D8KBAIG	A19nm	JEDEC 5.0	-25°C to 85°C	153FBGA 11.5x13

*Valid Q22014

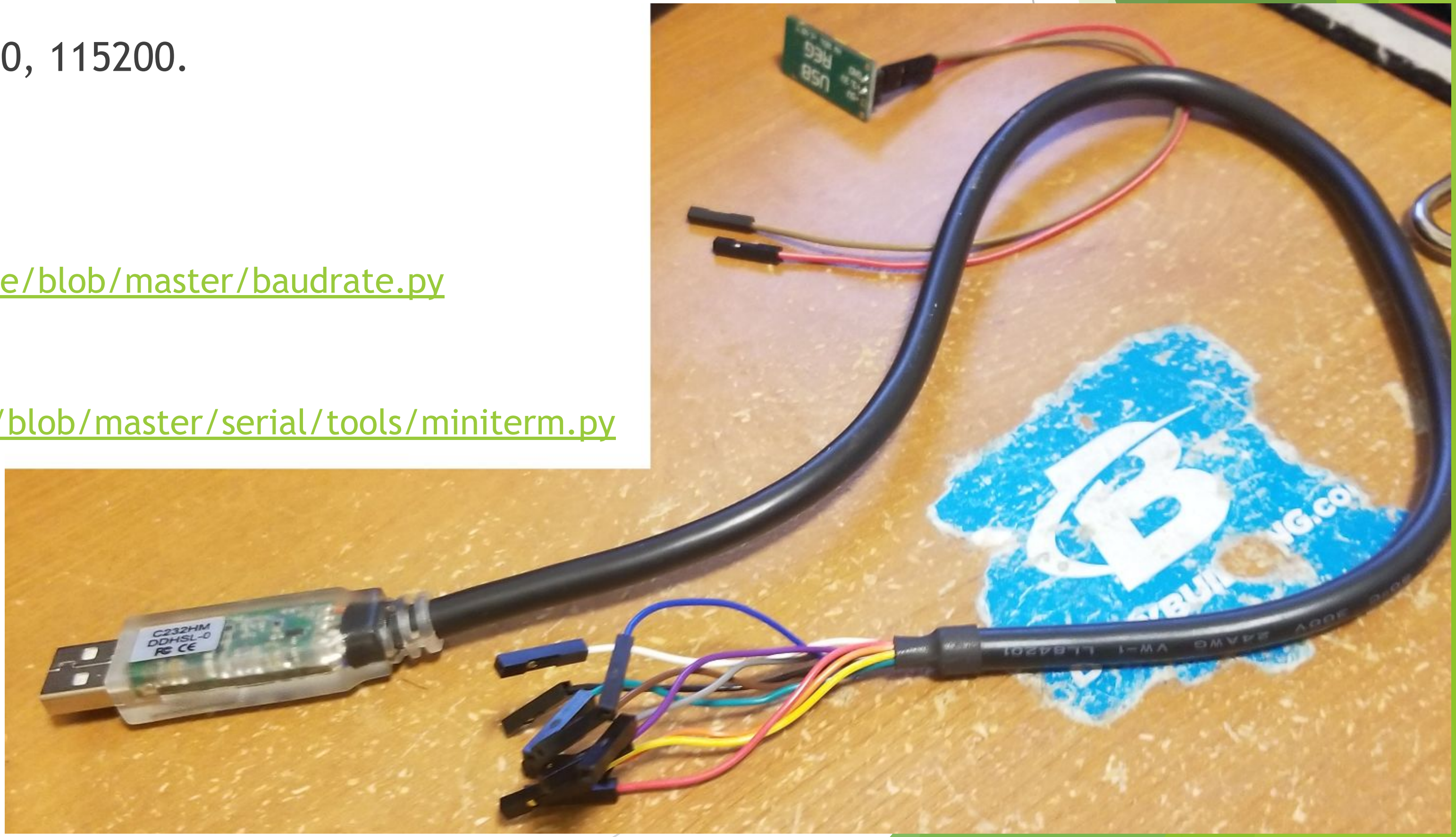


Specifications

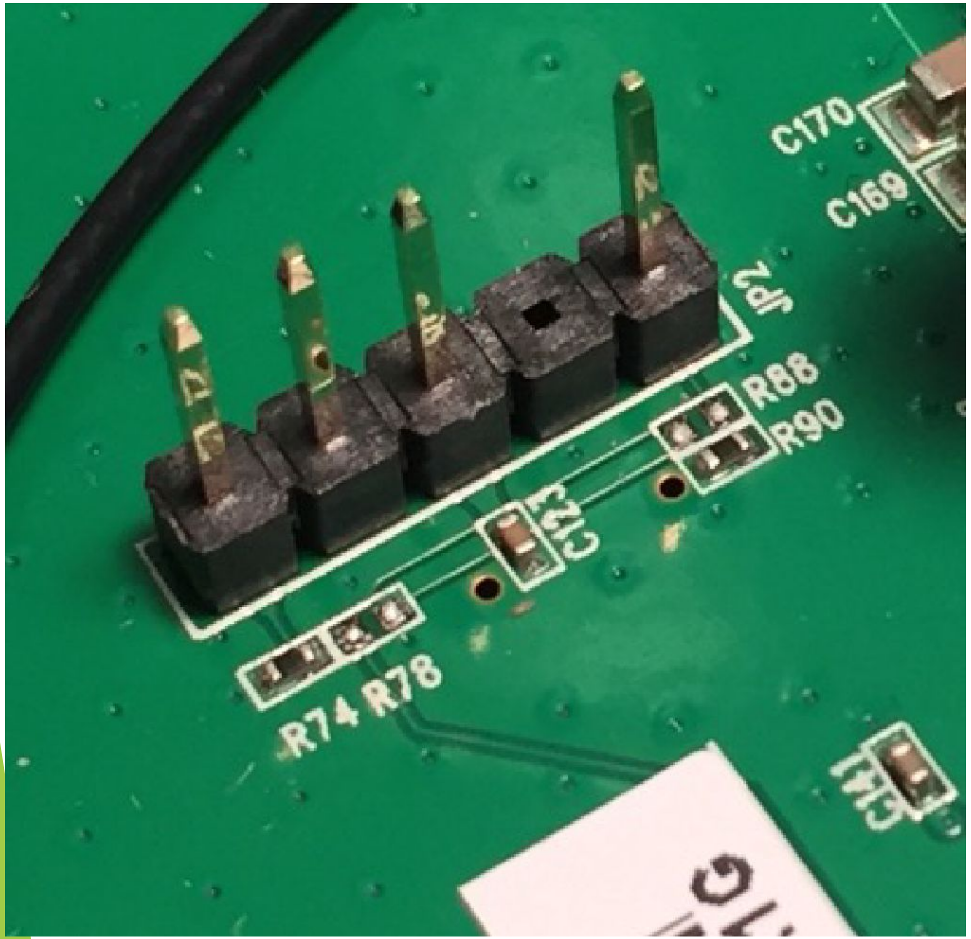
EU RoHS	Supplier Unconfirmed
Cell Type	Managed NAND
Chip Density (bit)	256G
Number of Bits/Word (bit)	1/4/8
Number of Words	256G/64G/32G
Programmability	Yes
Timing Type	Synchronous
Interface Type	Serial e-MMC
Minimum Operating Supply Voltage (V)	2.7
Typical Operating Supply Voltage (V)	3.3
Maximum Operating Supply Voltage (V)	3.6
Minimum Operating Temperature (°C)	-25
Maximum Operating Temperature (°C)	85
Mounting	Surface Mount
Package Length (mm)	13
Package Width (mm)	11.5
PCB changed	153
Standard Package Name	BGA
Supplier Package	FBGA
Pin Count	153
Lead Shape	Ball

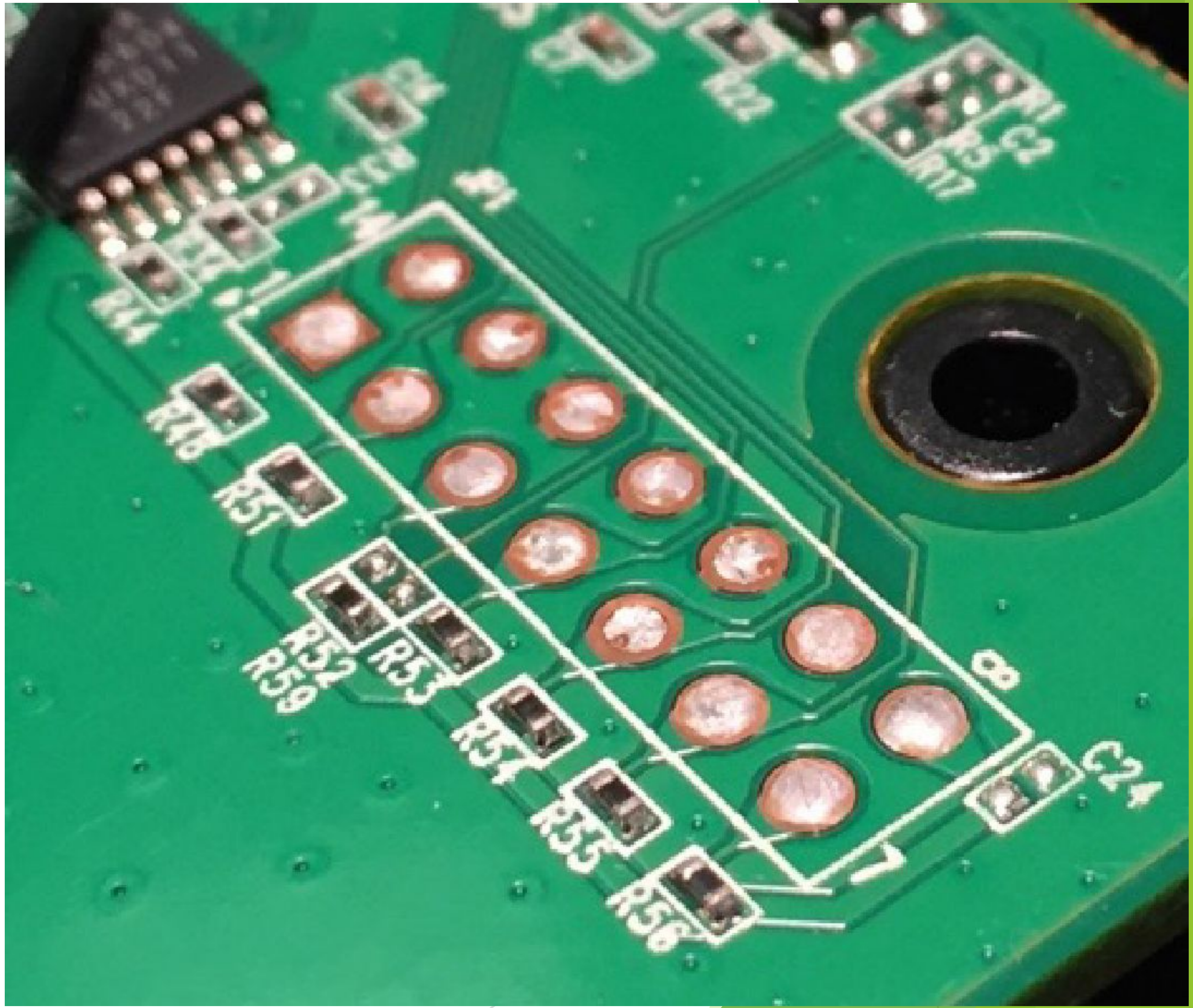
Debugging ports/interfaces

- UART interfaces.
- Baud rate aka bits per sec
  - 1200, 2400, 4800, 19200, 38400, 57600, 115200.
- Tools:
  - Baudrate
    - https://github.com/devttys0/baudrate/blob/master/baudrate.py
  - Miniterm.py
    - https://github.com/pyserial/pyserial/blob/master/serial/tools/miniterm.py
  - And this USB cable! →
  - Multi-Meter



Identify UART



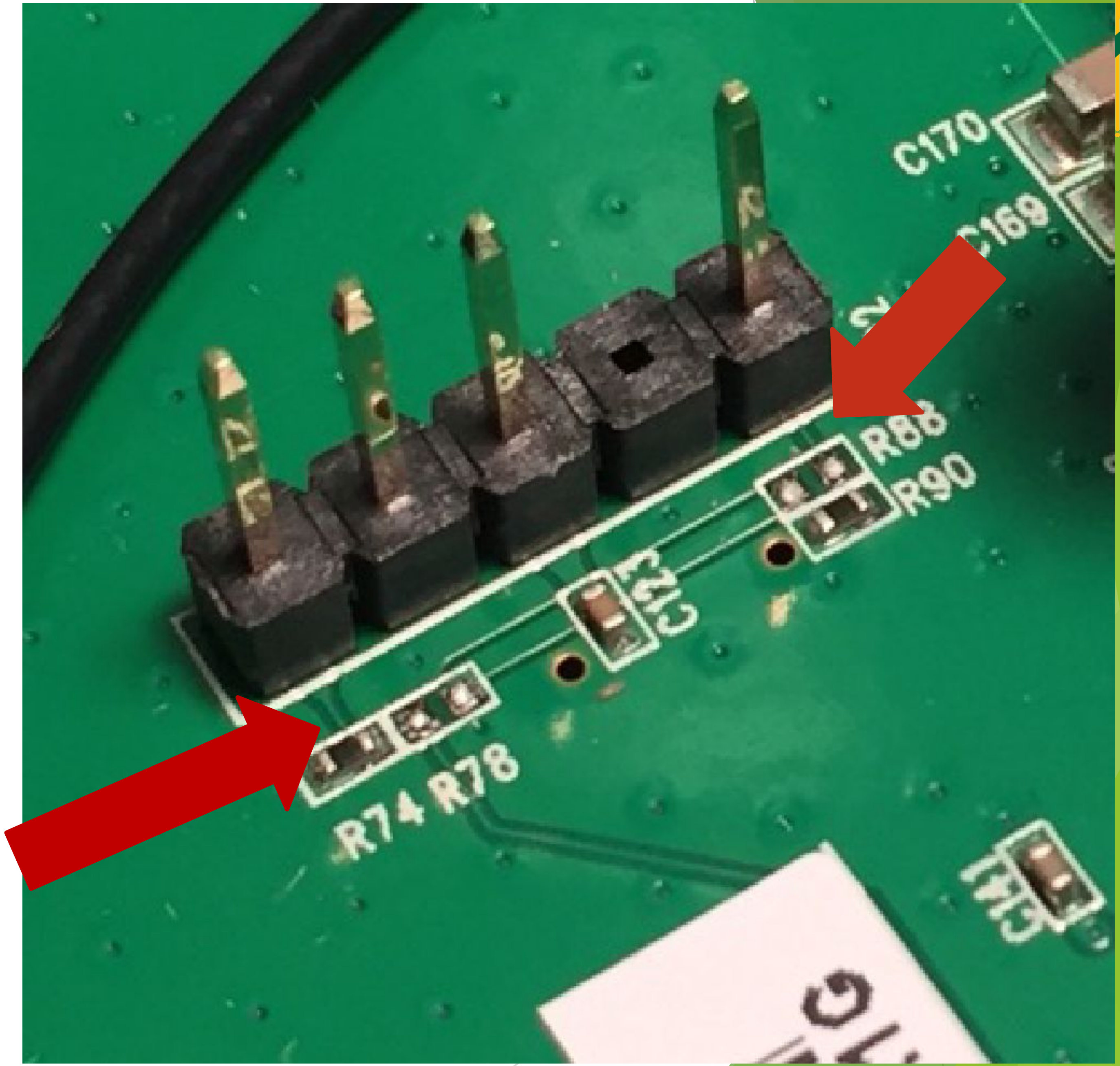


WTf is UART?

- A port for communication
- Security? What security.
  - Many IoT, routers will just drop you straight to root shell. C Y B E R!
- You can do a lot with bootloader/uboot.
- PINS:
  - Power
  - Ground
  - TX - Transmit
  - RX – Receive

Identify PINS

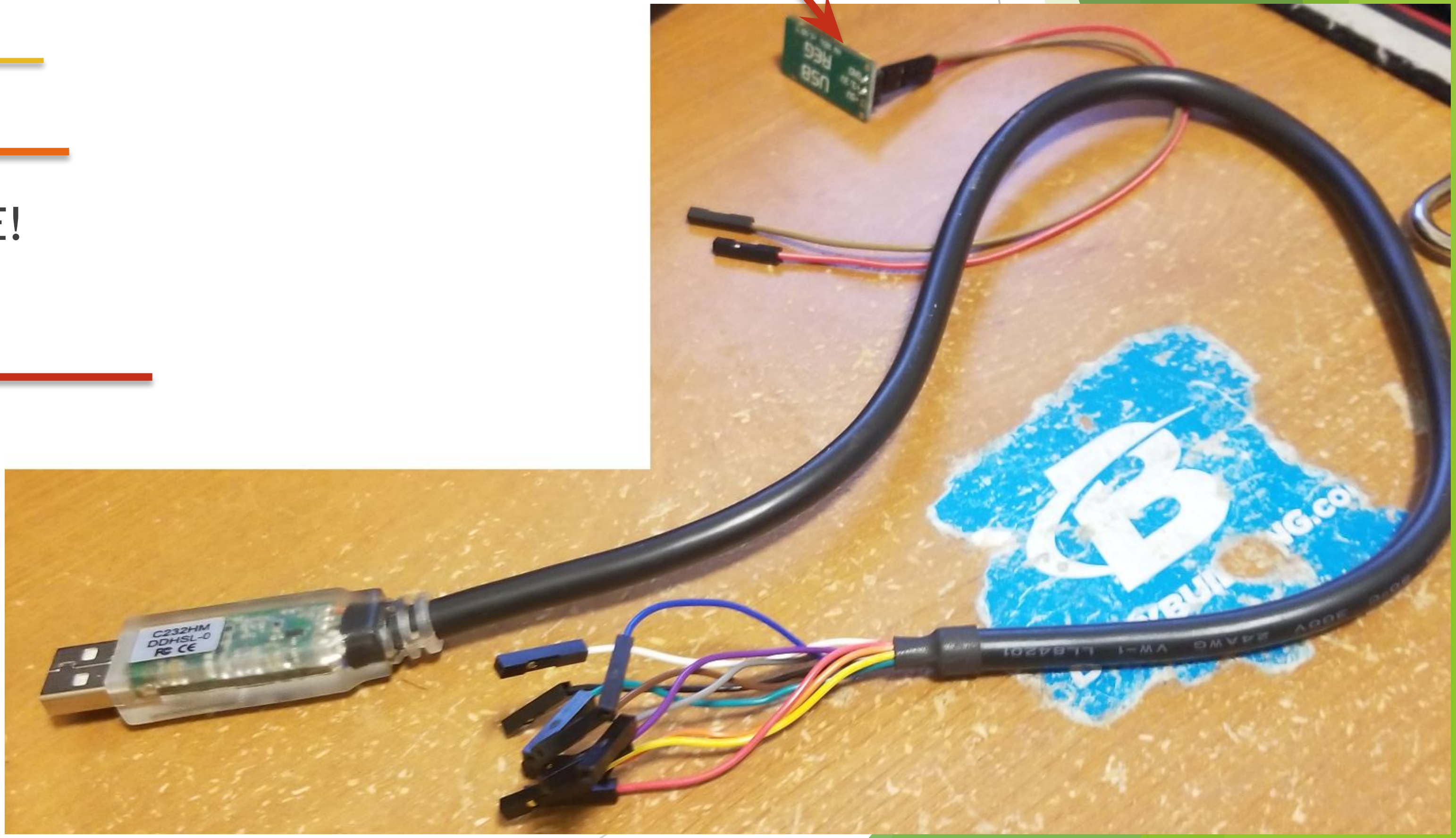
- Soldering
  - Video
- TX and RX
  - Have bus going from PINS to chip
  - If it's not TX, it's RX
- Power and Ground
  - Multi-meter
  - Touch the ground pad and a pin
    - If *BEEP*, it's ground



Connect to it

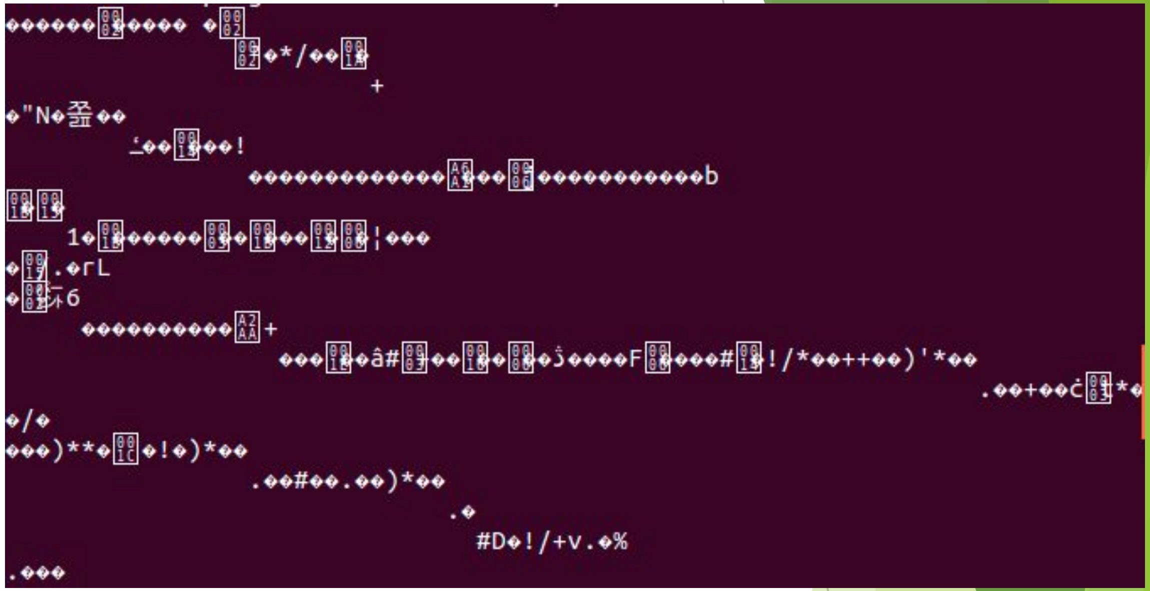
- GND – BLACK
- RX – YELLOW
- TX – ORANGE
- VCC – IF YOU HAVE A POWER CABLE!
  - No need
- Else, VCC –RED. 3.3 V
  - Still no power?
    - External power source

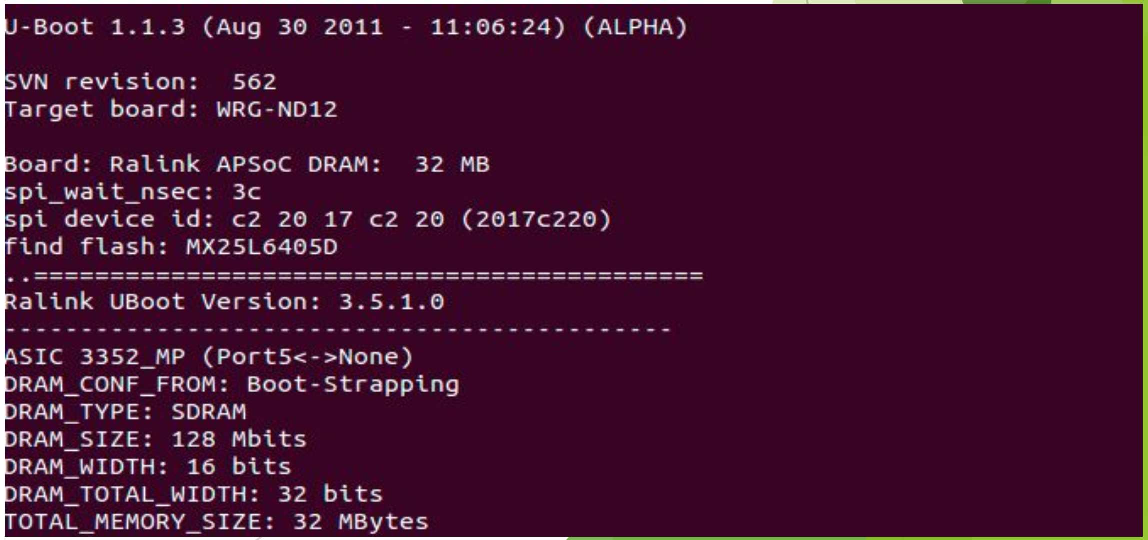
External power –
5V, and 3.3V



BAUDRATE BRUTE-FORCING

- https://github.com/devttys0/baudrate
- Magic command:
  - sudo ./baudrate.py –p /dev/ttyUSB0
  - replace /dev/ttyUSB0 to be the correct port
- Most UART occurs at system boot!!
- UP & DOWN arrow – SUPER ADVANCED
- Step
  - Choose a rate to start
  - Turn on device
  - If text is READABLE -> that the baudrate you want.
  - If not turn off, change rate, repeat!





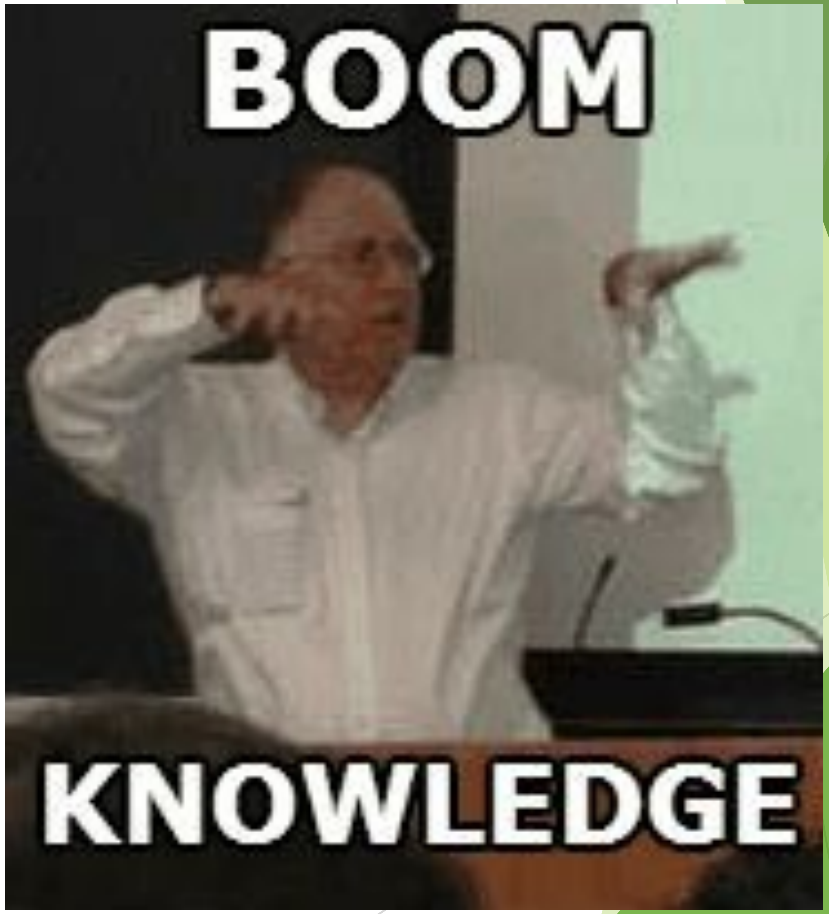
```
U-Boot 1.1.3 (Aug 30 2011 - 11:06:24) (ALPHA)

SVN revision:  562
Target board: WRG-ND12

Board: Ralink APSoC DRAM:  32 MB
spi_wait_nsec: 3c
spi device id: c2 20 17 c2 20 (2017c220)
find flash: MX25L6405D
..============================================
Ralink UBoot Version: 3.5.1.0
--------------------------------------------
ASIC 3352_MP (Port5<->None)
DRAM_CONF_FROM: Boot-Strapping
DRAM_TYPE: SDRAM
DRAM_SIZE: 128 Mbits
DRAM_WIDTH: 16 bits
DRAM_TOTAL_WIDTH: 32 bits
TOTAL_MEMORY_SIZE: 32 MBytes
```

Interacting with UART

- Miniterm
  - https://github.com/pyserial/pyserial/tree/master/serial/tools
- Command:
  - sudo ./miniterm.py <DEVICE> <BAUDRATE>
  - DEVICE: /dev/tty___ : Should know this from Baudrate brute forcing
  - BAUDRATE: We knew this from the hackery thing we did.
  - Final command:
    - sudo ./miniterm.py /dev/ttyUSB0 115200
- WE SHOULD GET A SHELL. lit
- Documentation:
  - http://pyserial.readthedocs.io/en/latest/tools.html

Interacting with the shell

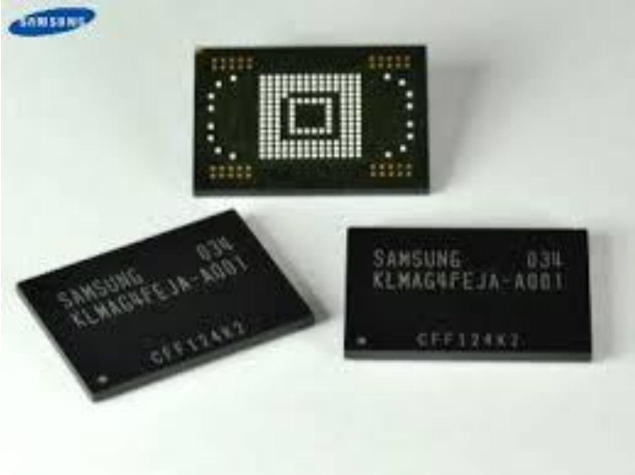
- Control?
  - What kind of control we have
- What we can do?
- Can we have a /bin/sh shell?
- Bootloader/Uboot init modification?
- Login credentials?
- Binary exploitation?
- More info - the better
- KNOWLEDGE!



Getting the firmware/filesystem

- Memory chips!
  - How do u know? From reconnaissance.
- Types of memory chip:
  - EEPROM
  - FLASH ⚡
    - NOR
    - NAND
    - eMMC
- Interfaces:
  - SPI - 1
  - Parallel - 2
  - BGA - 3

3.

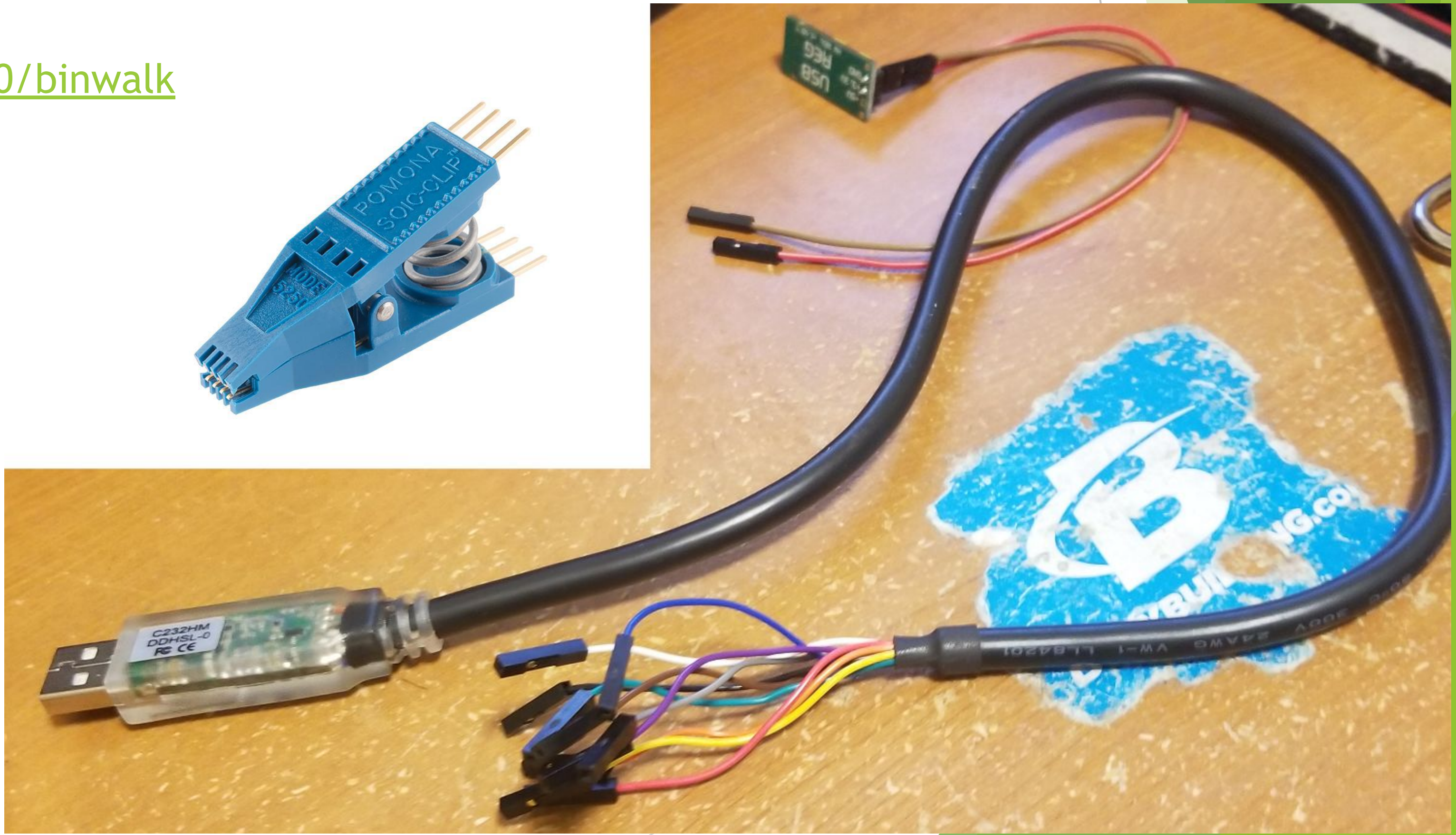


1.

2.

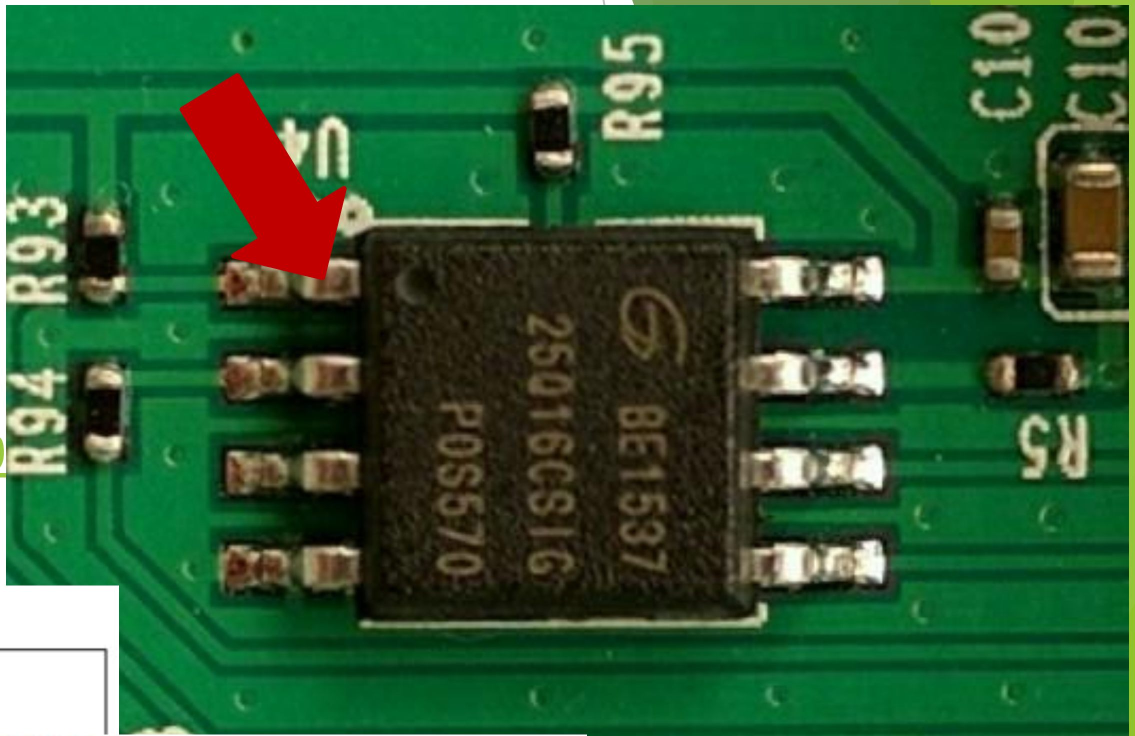
Reading SPI?!?!

- Tools:
  - spiflash-winbond
    - https://github.com/devttys0/libmpsse/tree/master/src/examples
  - binwalk
    - https://github.com/devttys0/binwalk
  - file
  - Magic USB cable
  - Soic clip
  - The datasheet

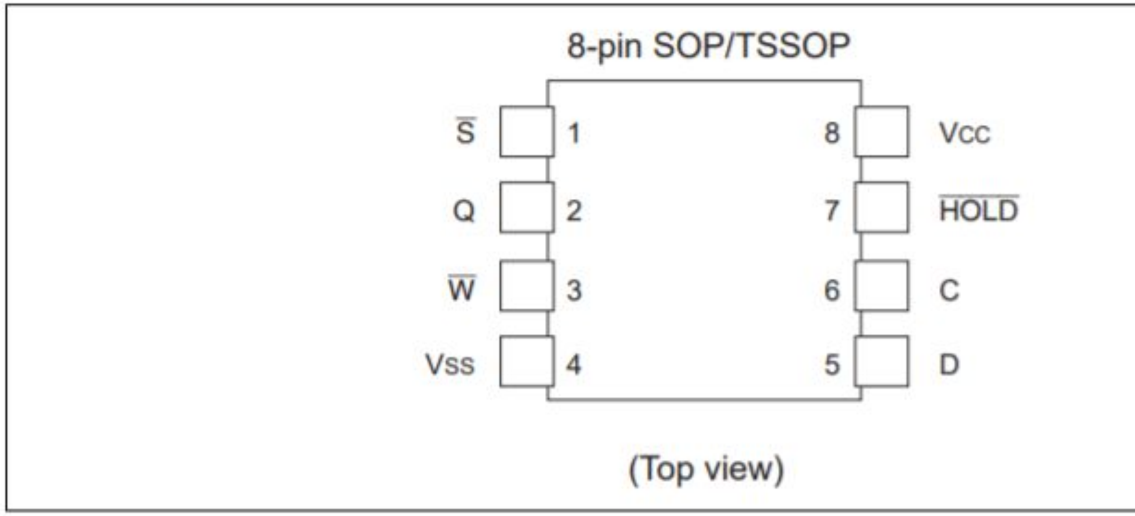


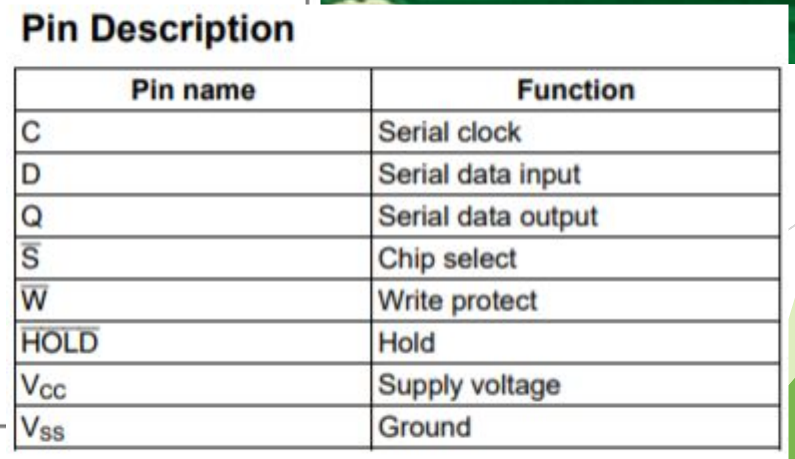
Connecting the cable

- Datasheet
- THE DOT
  - Pin 1
- http://www.datasheets360.com/pdf/34730753952930



Pin Arrangement



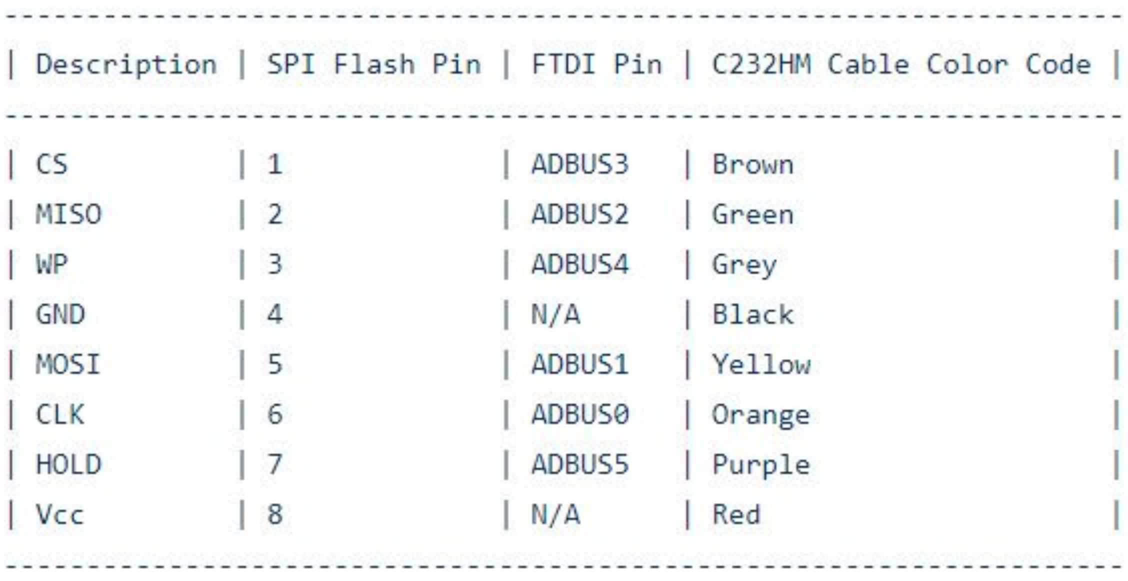


Pin Description

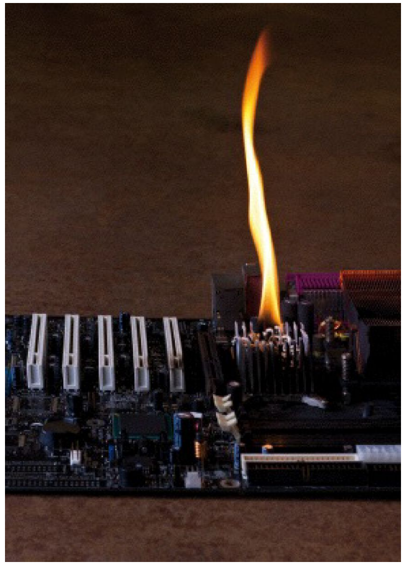
Pin name	Function
C	Serial clock
D	Serial data input
Q	Serial data output
$\overline{S}$	Chip select
$\overline{W}$	Write protect
$\overline{HOLD}$	Hold
V_{CC}	Supply voltage
V_{SS}	Ground

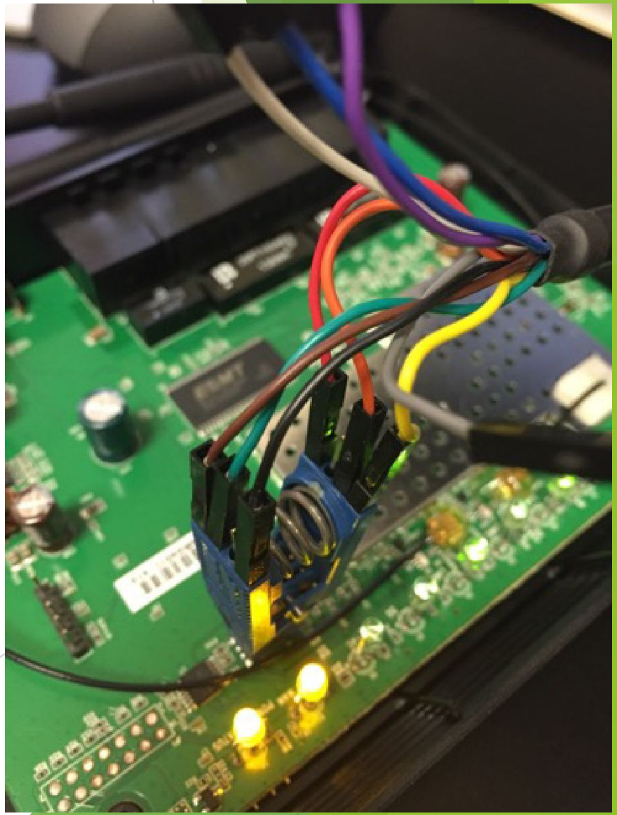
Connect the cable

- Spiflash gives you the pins and colors
  - Don’t connect the power cord if you have VCC plugged in
    - ELSE it’s gonna be REAL LIT
- Plug into your computer



```
-----------------------------------------------------------------
| Description | SPI Flash Pin | FTDI Pin | C232HM Cable Color Code |
-----------------------------------------------------------------
| CS          | 1             | ADBUS3   | Brown                   |
| MISO        | 2             | ADBUS2   | Green                   |
| WP          | 3             | ADBUS4   | Grey                    |
| GND         | 4             | N/A      | Black                   |
| MOSI        | 5             | ADBUS1   | Yellow                  |
| CLK         | 6             | ADBUS0   | Orange                  |
| HOLD        | 7             | ADBUS5   | Purple                  |
| Vcc         | 8             | N/A      | Red                     |
-----------------------------------------------------------------
```

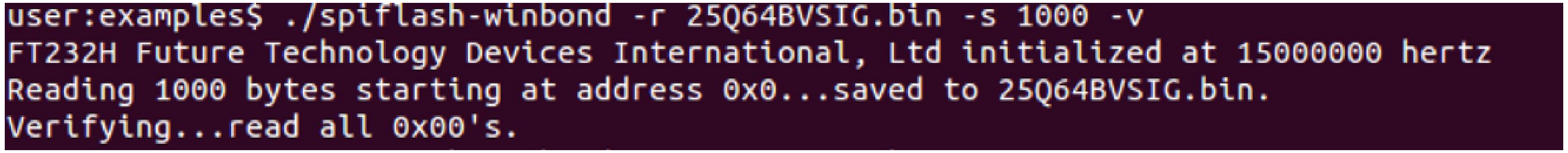




Spiflash and pull the goods

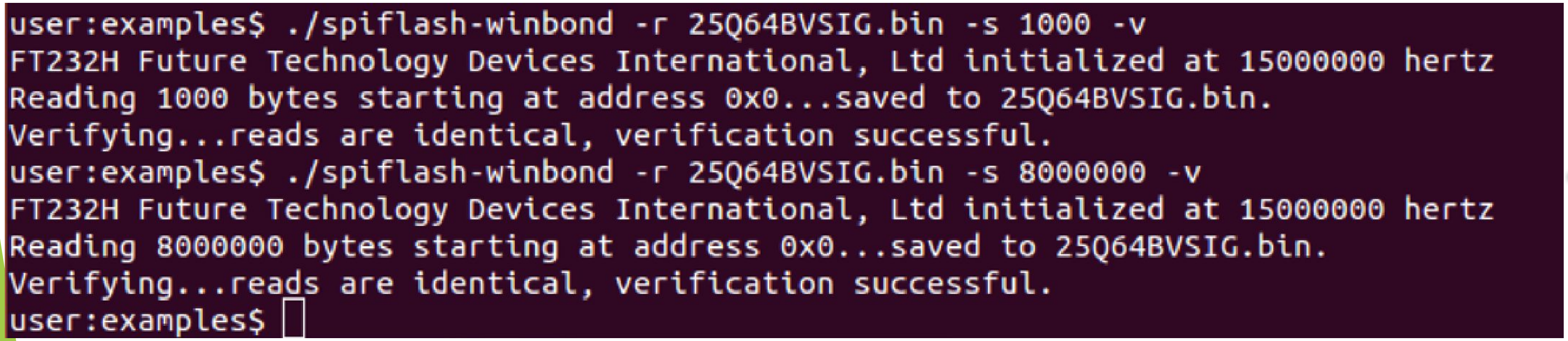
- ./spiflash –r <filename.bin> -s <bytes>
- Read 8MBs???
- ./spiflash –r thegoodness.bin -s $((0x800000)) –v
  - thegoodness.bin - > the output file will be named this
  - -s $((0x800000)) -> Read 8 M bytes
  - -v -> Verifying the read by reading it 2x and compare both.
    - Identical -> good!
- **NOTE : If it says “read all 0x00’s”
  - Incorrect input, output

You want pics??



```
user:examples$ ./spiflash-winbond -r 25Q64BVSIG.bin -s 1000 -v
FT232H Future Technology Devices International, Ltd initialized at 15000000 hertz
Reading 1000 bytes starting at address 0x0...saved to 25Q64BVSIG.bin.
Verifying...read all 0x00's.
```

S****T,**
FAILED!!

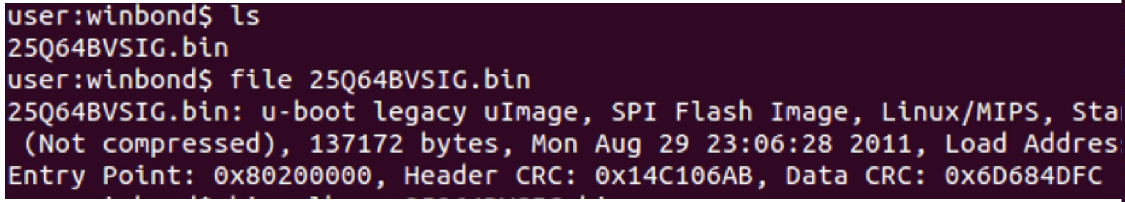


```
user:examples$ ./spiflash-winbond -r 25Q64BVSIG.bin -s 1000 -v
FT232H Future Technology Devices International, Ltd initialized at 15000000 hertz
Reading 1000 bytes starting at address 0x0...saved to 25Q64BVSIG.bin.
Verifying...reads are identical, verification successful.
user:examples$ ./spiflash-winbond -r 25Q64BVSIG.bin -s 8000000 -v
FT232H Future Technology Devices International, Ltd initialized at 15000000 hertz
Reading 8000000 bytes starting at address 0x0...saved to 25Q64BVSIG.bin.
Verifying...reads are identical, verification successful.
user:examples$ 
```

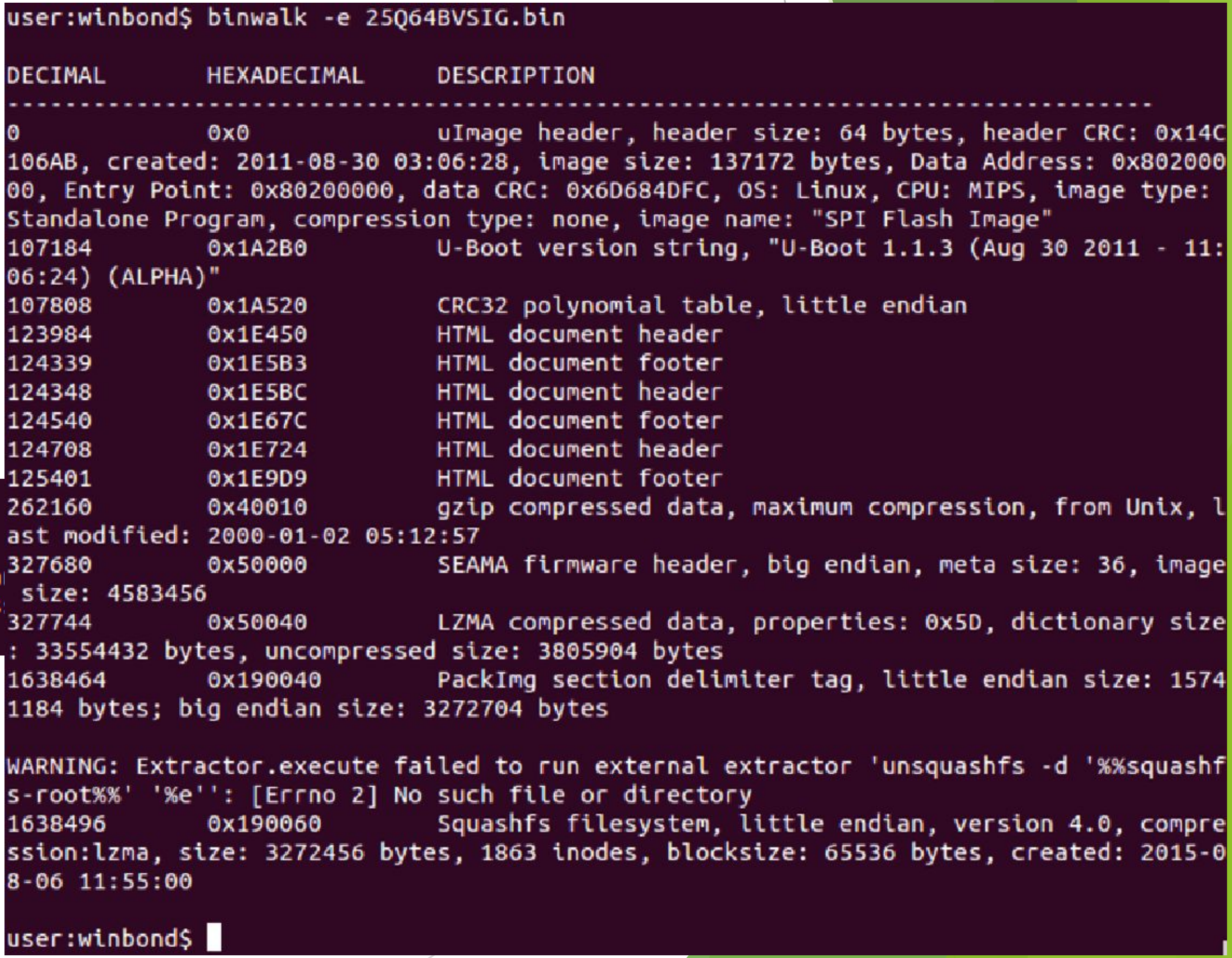
Oo HELL
YEAH,
SUCCEED

What to do with the *.bin file?

- file
- Binwalk
  - Extract binwalk –e



```
user:winbond$ ls
25Q64BVSIG.bin
user:winbond$ file 25Q64BVSIG.bin
25Q64BVSIG.bin: u-boot legacy uImage, SPI Flash Image, Linux/MIPS, Sta
 (Not compressed), 137172 bytes, Mon Aug 29 23:06:28 2011, Load Addres
Entry Point: 0x80200000, Header CRC: 0x14C106AB, Data CRC: 0x6D684DFC
```



```
user:winbond$ binwalk -e 25Q64BVSIG.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             uImage header, header size: 64 bytes, header CRC: 0x14C
106AB, created: 2011-08-30 03:06:28, image size: 137172 bytes, Data Address: 0x802000
00, Entry Point: 0x80200000, data CRC: 0x6D684DFC, OS: Linux, CPU: MIPS, image type:
Standalone Program, compression type: none, image name: "SPI Flash Image"
107184        0x1A2B0         U-Boot version string, "U-Boot 1.1.3 (Aug 30 2011 - 11:
06:24) (ALPHA)"
107808        0x1A520         CRC32 polynomial table, little endian
123984        0x1E450         HTML document header
124339        0x1E5B3         HTML document footer
124348        0x1E5BC         HTML document header
124540        0x1E67C         HTML document footer
124708        0x1E724         HTML document header
125401        0x1E9D9         HTML document footer
262160        0x40010         gzip compressed data, maximum compression, from Unix, l
ast modified: 2000-01-02 05:12:57
327680        0x50000         SEAMA firmware header, big endian, meta size: 36, image
 size: 4583456
327744        0x50040         LZMA compressed data, properties: 0x5D, dictionary size
: 33554432 bytes, uncompressed size: 3805904 bytes
1638464       0x190040        PackImg section delimiter tag, little endian size: 1574
1184 bytes; big endian size: 3272704 bytes

WARNING: Extractor.execute failed to run external extractor 'unsquashfs -d '%%squashf
s-root%%' '%e'': [Errno 2] No such file or directory
1638496       0x190060        Squashfs filesystem, little endian, version 4.0, compre
ssion:lzma, size: 3272456 bytes, 1863 inodes, blocksize: 65536 bytes, created: 2015-0
8-06 11:55:00

user:winbond$
```

OK we done

- NEW SKILLZ

- QUESTIONS?

Cooperate Rant – Who is Strange Labs

- R&D group – Under Uffect
  - Humanity cause
  - Human-trafficking
- I break stuff
- We all break stuff
- Work Environment
  - Casual, like SUPER casual
  - Benefits? Pretty dang good!
- Internship? Part-time? Full-time?
  - Students?
    - Education first !!!!!
- Bonnie.King@strange-labs.com
- Or Me!