HOW DOES YOUR MCDONALD’S BURGER GET TO YOU?

The burger knows where it is at all times. It knows this because it knows where it isn't.

About me

- Over caffeinated wolf
- Voiding warranties for a living since 2018
- Projects :
  - Done :
    - Bypassing the Hantek DSO software limitation
    - GPS spoofing on DJI Inspire 1
    - Recovering and exploiting IP cameras
  - WIP :
    - Freeway toll gate token reverse engineering
    - NOVAL 4G IoT xxxxx 😏

Twitter / X : @CyberWolf_2077

Blog : whiterose-infosec.super.site/

What this talk is about

How to reverse engineer an electrical device

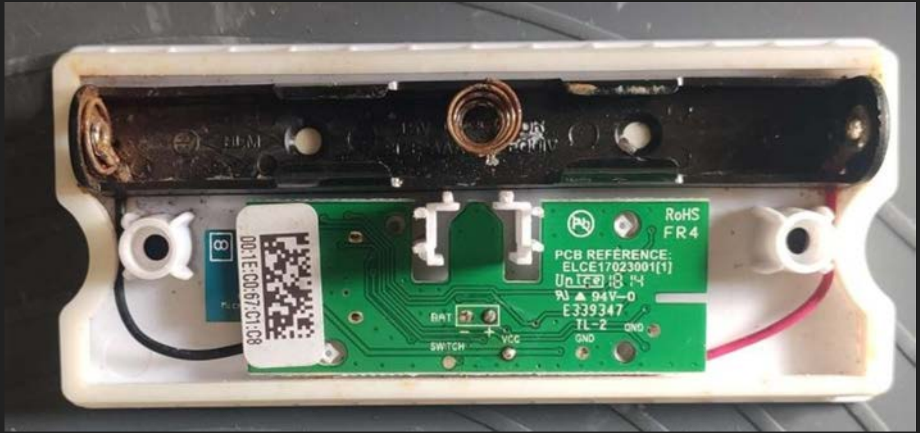
How mcdonalds manage to find you in their restaurant

What this talk isn’t about

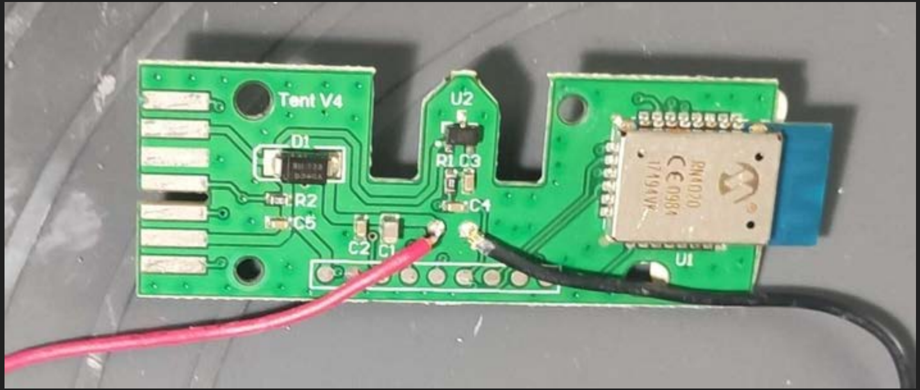
How to get free food

Introduction

Let’s take a look at what is inside : A simple overview



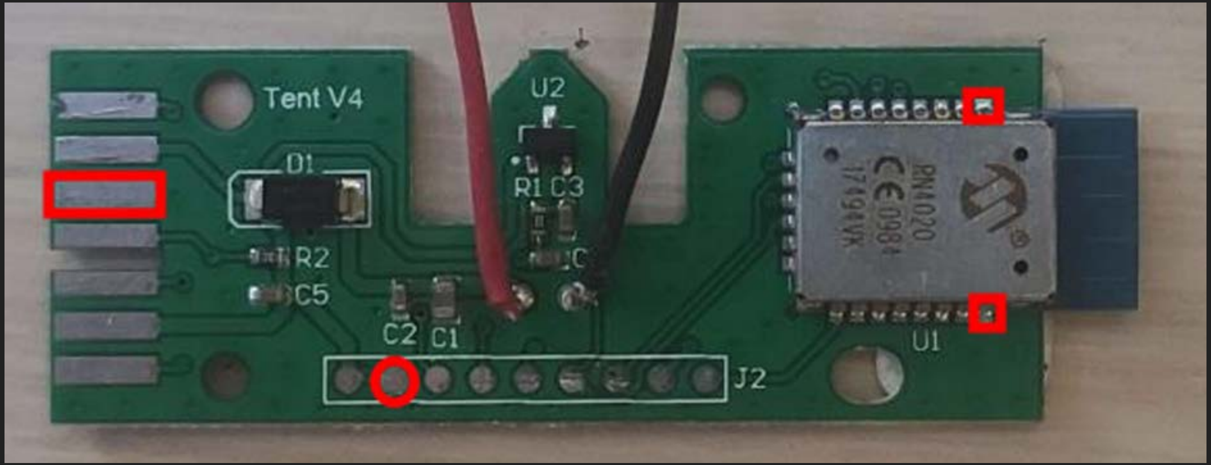
Getting the paws on the device
Looking inside the hopping to find cool stuff
There is only a RN4020 and 2 AAA batteries
There is only a RN4020 and 2 AAA batteries



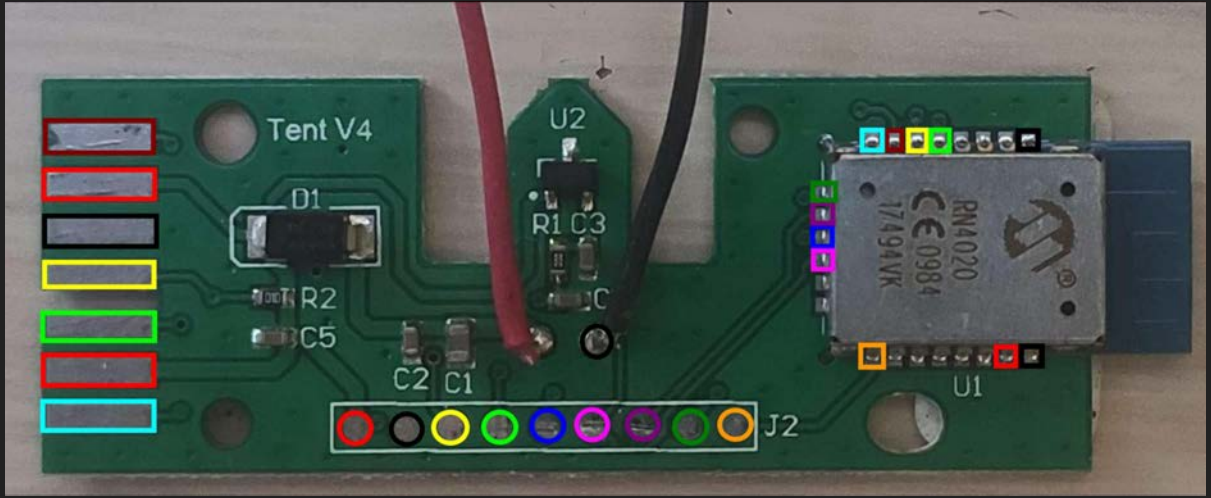
Mapping the board

And sniffing the traces

Finding the ground pins

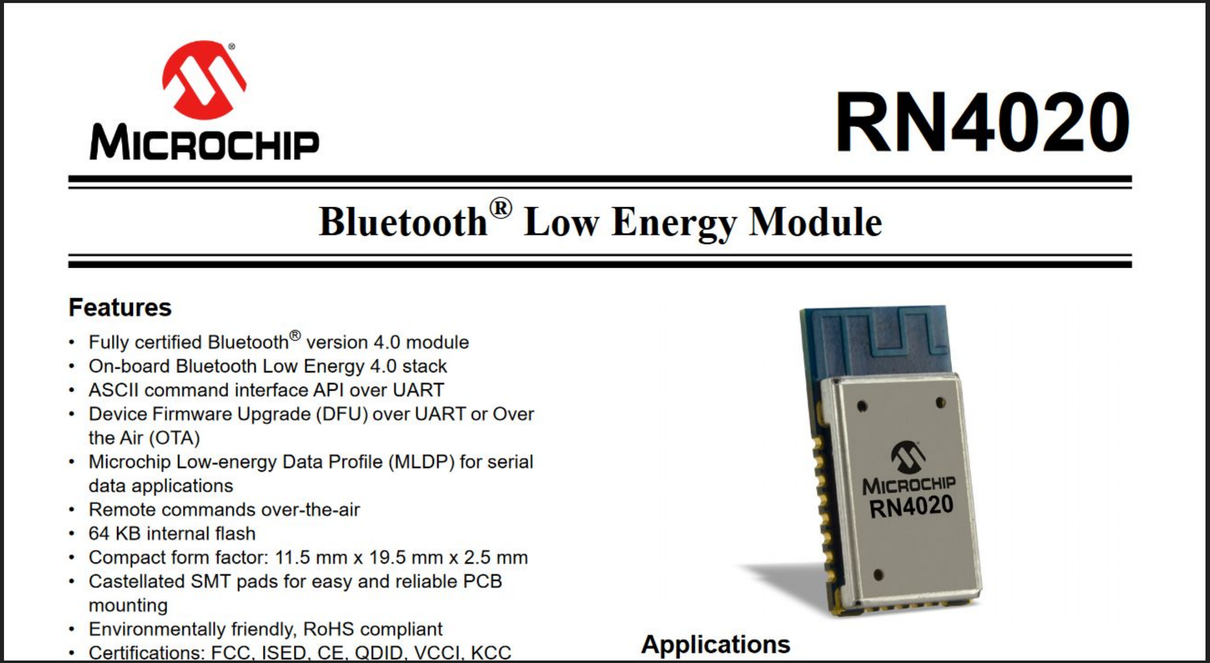


Probing them all



Yes, it takes some time to do these pics

Scrolling the datasheets



MICROCHIP

RN4020

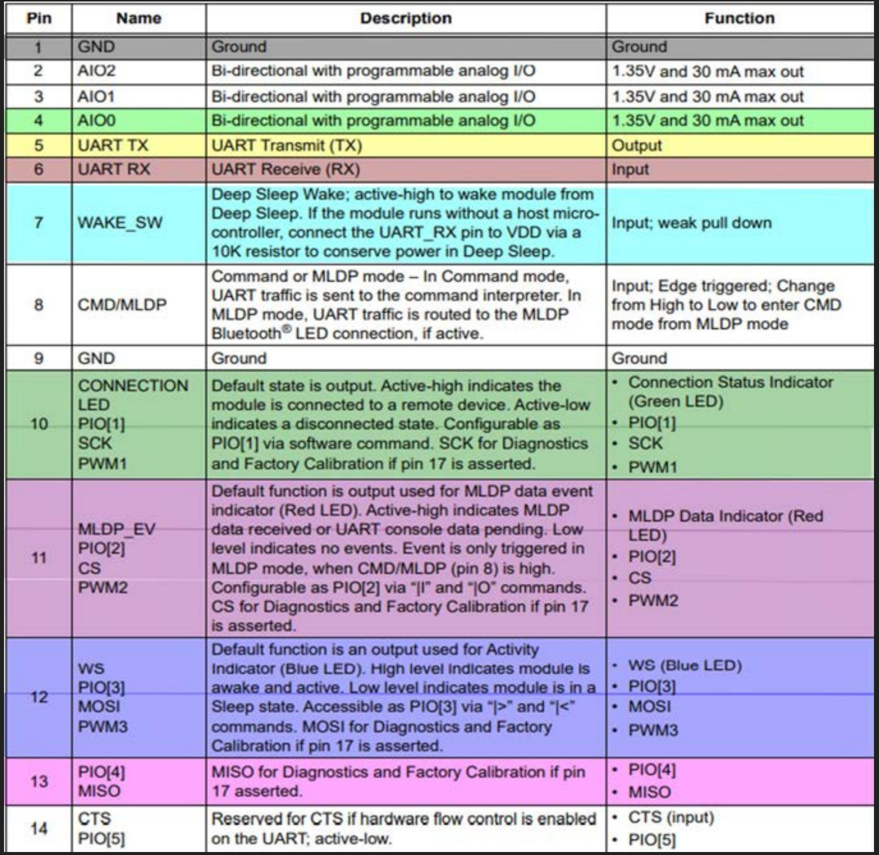
Bluetooth® Low Energy Module

Features

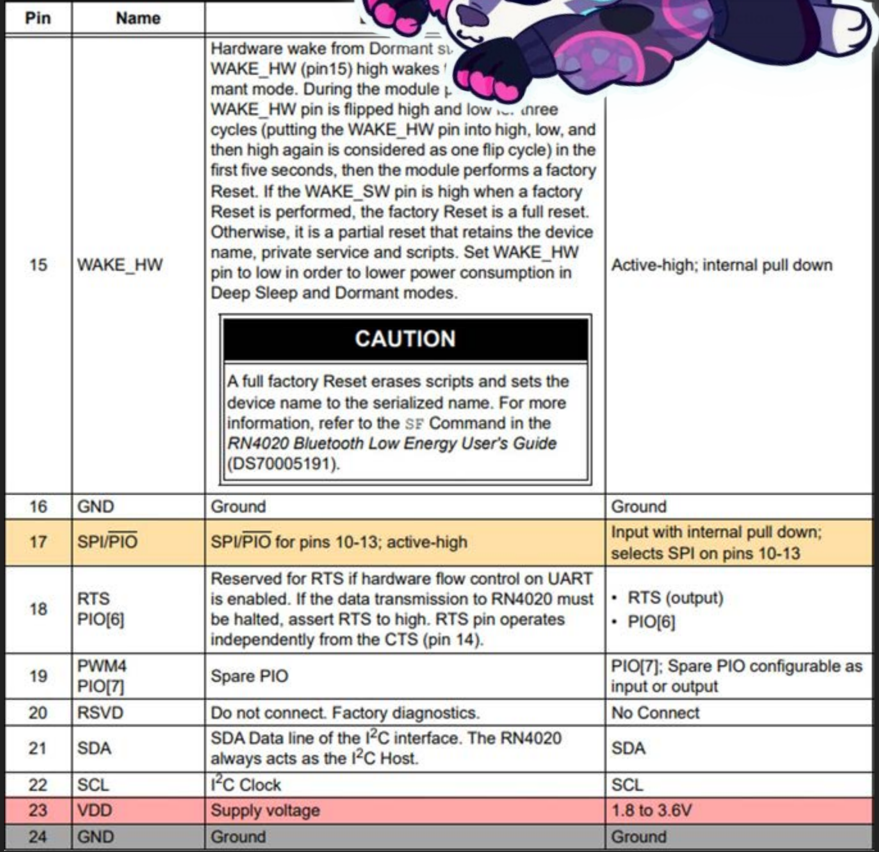
- Fully certified Bluetooth® version 4.0 module
- On-board Bluetooth Low Energy 4.0 stack
- ASCII command interface API over UART
- Device Firmware Upgrade (DFU) over UART or Over the Air (OTA)
- Microchip Low-energy Data Profile (MLDP) for serial data applications
- Remote commands over-the-air
- 64 KB internal flash
- Compact form factor: 11.5 mm x 19.5 mm x 2.5 mm
- Castellated SMT pads for easy and reliable PCB mounting
- Environmentally friendly, RoHS compliant
- Certifications: FCC, ISED, CE, QDID, VCCI, KCC

Applications

Scrolling the datasheets

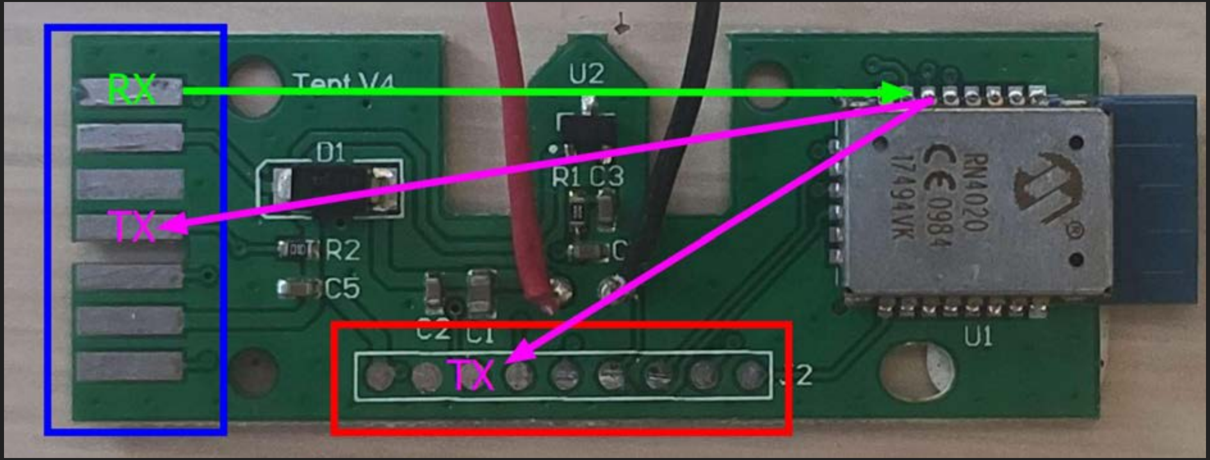


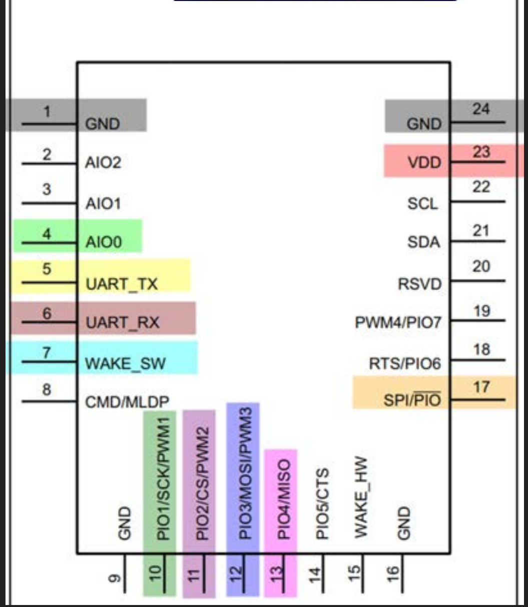
Pin	Name	Description	Function
1	GND	Ground	Ground
2	AIO2	Bi-directional with programmable analog I/O	1.35V and 30 mA max out
3	AIO1	Bi-directional with programmable analog I/O	1.35V and 30 mA max out
4	AIO0	Bi-directional with programmable analog I/O	1.35V and 30 mA max out
5	UART TX	UART Transmit (TX)	Output
6	UART RX	UART Receive (RX)	Input
7	WAKE_SW	Deep Sleep Wake; active-high to wake module from Deep Sleep. If the module runs without a host micro-controller, connect the UART_RX pin to VDD via a 10K resistor to conserve power in Deep Sleep.	Input; weak pull down
8	CMD/MLDP	Command or MLDP mode – In Command mode, UART traffic is sent to the command interpreter. In MLDP mode, UART traffic is routed to the MLDP Bluetooth® LED connection, if active.	Input; Edge triggered; Change from High to Low to enter CMD mode from MLDP mode
9	GND	Ground	Ground
10	CONNECTION LED PIO[1] SCK PWM1	Default state is output. Active-high indicates the module is connected to a remote device. Active-low indicates a disconnected state. Configurable as PIO[1] via software command. SCK for Diagnostics and Factory Calibration if pin 17 is asserted.	• Connection Status Indicator (Green LED) • PIO[1] • SCK • PWM1
11	MLDP_EV PIO[2] CS PWM2	Default function is output used for MLDP data event indicator (Red LED). Active-high indicates MLDP data received or UART console data pending. Low level indicates no events. Event is only triggered in MLDP mode, when CMD/MLDP (pin 8) is high. Configurable as PIO[2] via "|I" and "|O" commands. CS for Diagnostics and Factory Calibration if pin 17 is asserted.	• MLDP Data Indicator (Red LED) • PIO[2] • CS • PWM2
12	WS PIO[3] MOSI PWM3	Default function is an output used for Activity Indicator (Blue LED). High level indicates module is awake and active. Low level indicates module is in a Sleep state. Accessible as PIO[3] via "|>" and "|<" commands. MOSI for Diagnostics and Factory Calibration if pin 17 is asserted.	• WS (Blue LED) • PIO[3] • MOSI • PWM3
13	PIO[4] MISO	MISO for Diagnostics and Factory Calibration if pin 17 asserted.	• PIO[4] • MISO
14	CTS PIO[5]	Reserved for CTS if hardware flow control is enabled on the UART; active-low.	• CTS (input) • PIO[5]



Pin	Name		
15	WAKE_HW	Hardware wake from Dormant st WAKE_HW (pin15) high wakes mant mode. During the module WAKE_HW pin is flipped high and low three cycles (putting the WAKE_HW pin into high, low, and then high again is considered as one flip cycle) in the first five seconds, then the module performs a factory Reset. If the WAKE_SW pin is high when a factory Reset is performed, the factory Reset is a full reset. Otherwise, it is a partial reset that retains the device name, private service and scripts. Set WAKE_HW pin to low in order to lower power consumption in Deep Sleep and Dormant modes. **CAUTION** A full factory Reset erases scripts and sets the device name to the serialized name. For more information, refer to the SF Command in the *RN4020 Bluetooth Low Energy User's Guide* (DS70005191).	Active-high; internal pull down
16	GND	Ground	Ground
17	SPI/$\overline{\text{PIO}}$	SPI/$\overline{\text{PIO}}$ for pins 10-13; active-high	Input with internal pull down; selects SPI on pins 10-13
18	RTS PIO[6]	Reserved for RTS if hardware flow control on UART is enabled. If the data transmission to RN4020 must be halted, assert RTS to high. RTS pin operates independently from the CTS (pin 14).	• RTS (output) • PIO[6]
19	PWM4 PIO[7]	Spare PIO	PIO[7]; Spare PIO configurable as input or output
20	RSVD	Do not connect. Factory diagnostics.	No Connect
21	SDA	SDA Data line of the I^{2}C interface. The RN4020 always acts as the I^{2}C Host.	SDA
22	SCL	I^{2}C Clock	SCL
23	VDD	Supply voltage	1.8 to 3.6V
24	GND	Ground	Ground

Identifying the pins in use

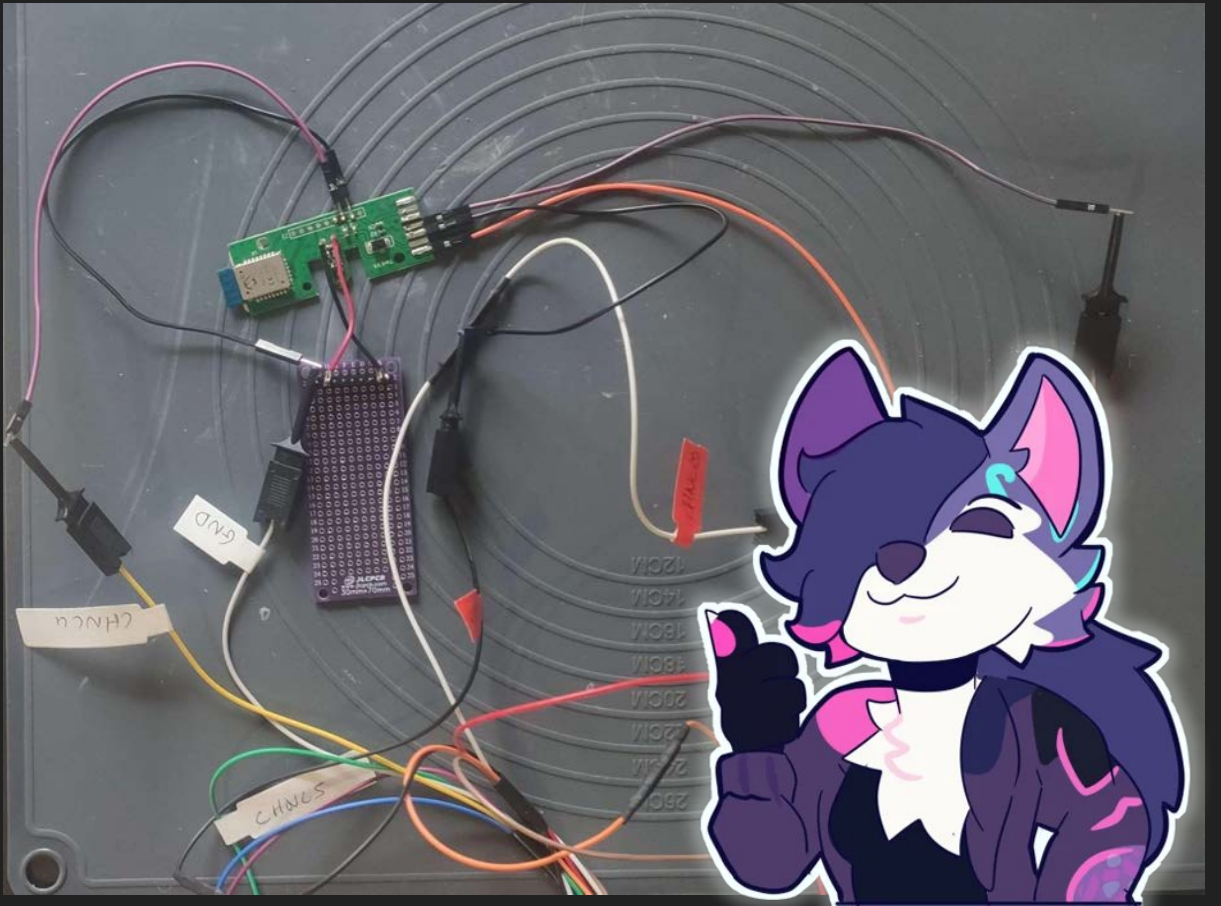




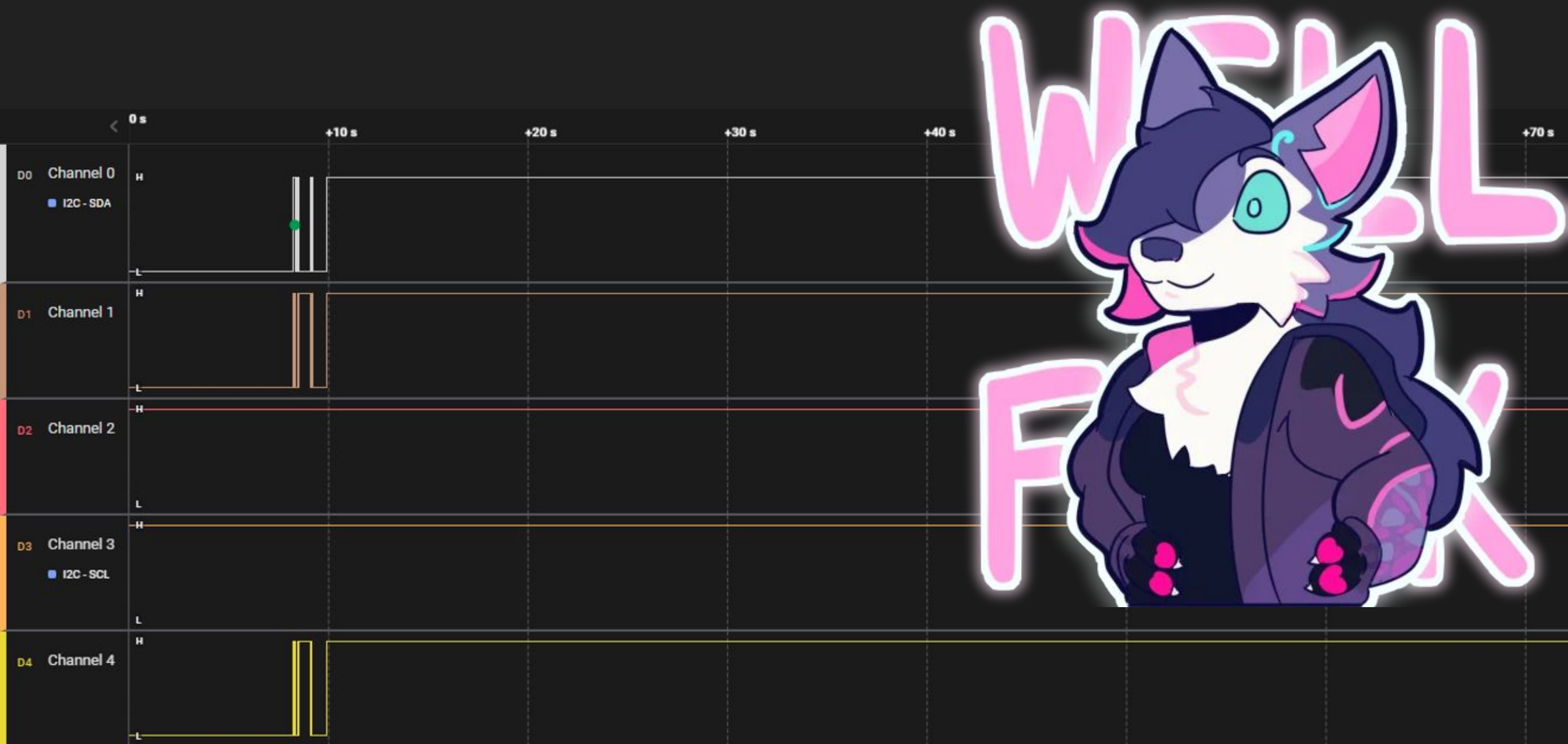
Exploiting the UART port

Probing the chip

Pin	Probe
GND	GND
RX	CH0
TX	CH1
GND	GND 2
TX	CH4

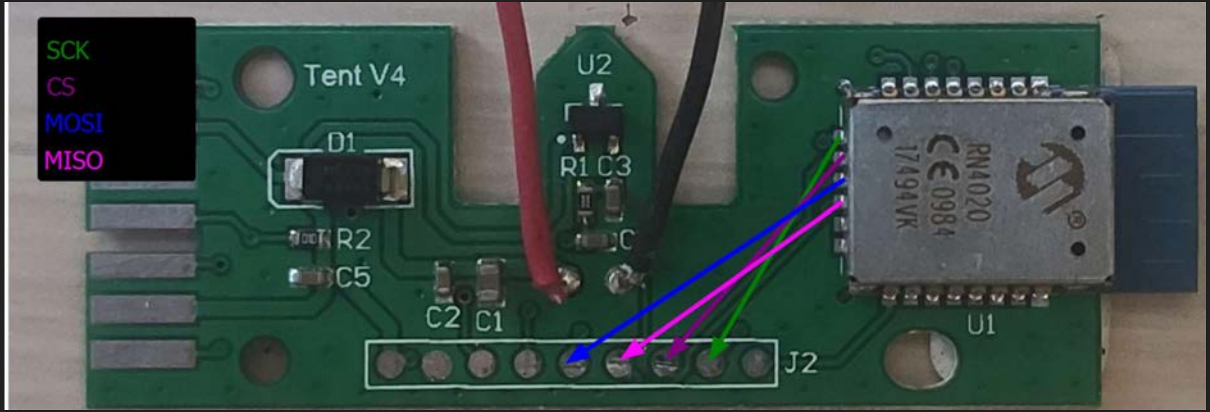


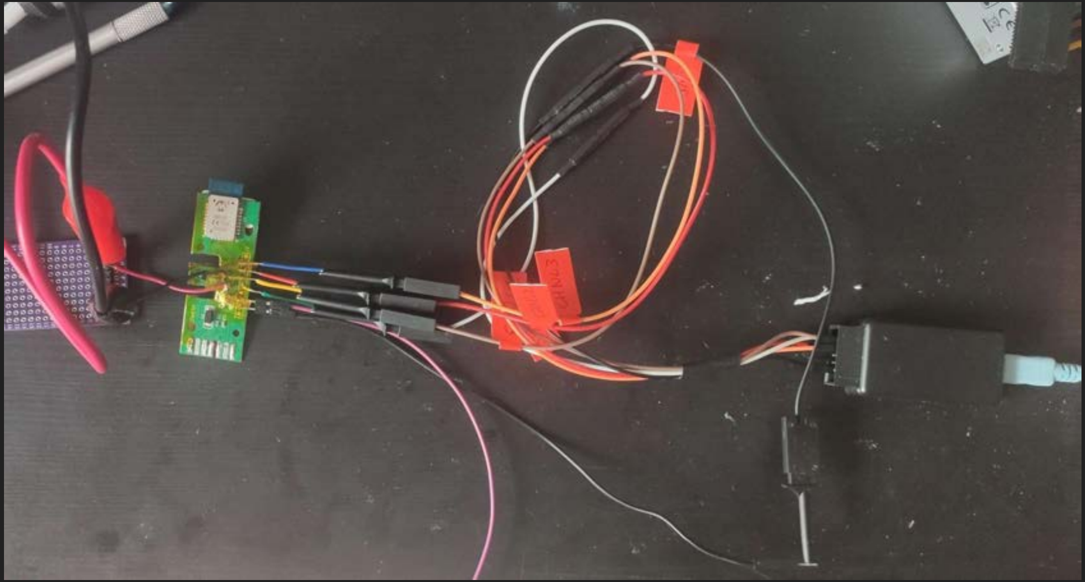
Results


0 s
+10 s
+20 s
+30 s
+40 s
+70 s
D0 Channel 0
I2C - SDA
D1 Channel 1
D2 Channel 2
D3 Channel 3
I2C - SCL
D4 Channel 4
H
L

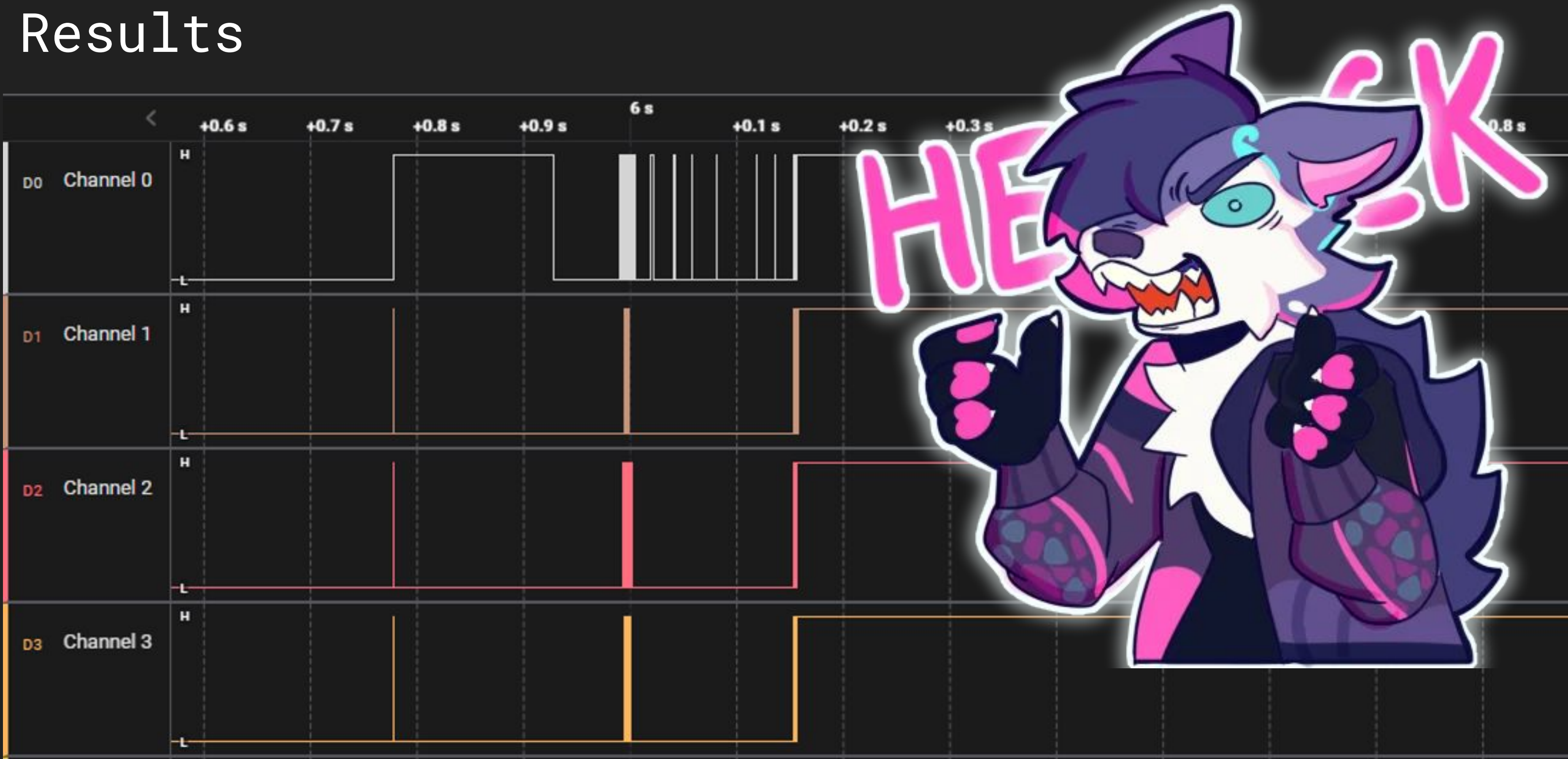
Exploiting the MISO/MOSI port

Exploiting the MISO / MOSI port





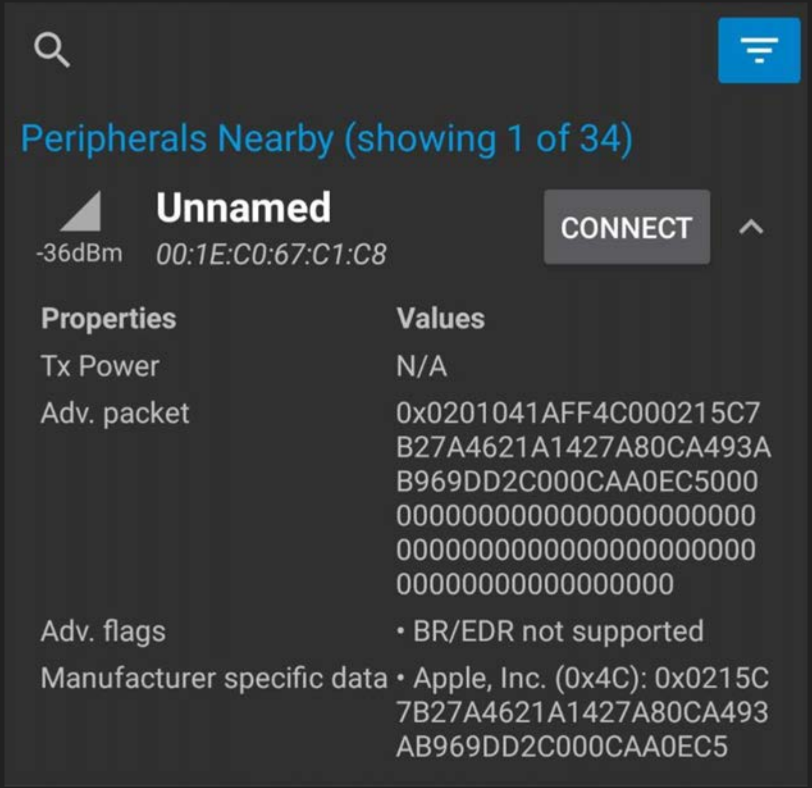
Results


6 s
+0.6 s
+0.7 s
+0.8 s
+0.9 s
+0.1 s
+0.2 s
+0.3 s
0.8 s
D0 Channel 0
D1 Channel 1
D2 Channel 2
D3 Channel 3
H
L
HE
CK

Let’s mess up with the bluetooth

Listening for the Bluetooth chip

LightBlue®



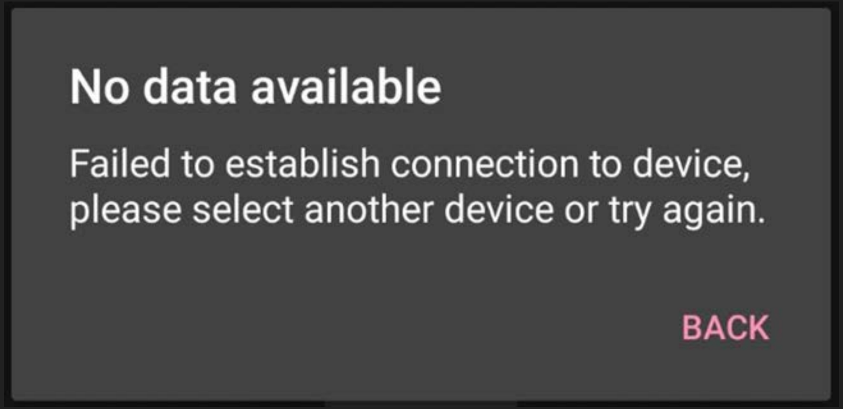
Peripherals Nearby (showing 1 of 34)

Unnamed

00:1E:C0:67:C1:C8

Properties	Values
Tx Power	N/A
Adv. packet	0x0201041AFF4C000215C7 B27A4621A1427A80CA493A B969DD2C000CAA0EC5000 0000000000000000000000 0000000000000000000000 00000000000000000
Adv. flags	• BR/EDR not supported
Manufacturer specific data	• Apple, Inc. (0x4C): 0x0215C 7B27A4621A1427A80CA493 AB969DD2C000CAA0EC5

Connecting with the bluetooth chip



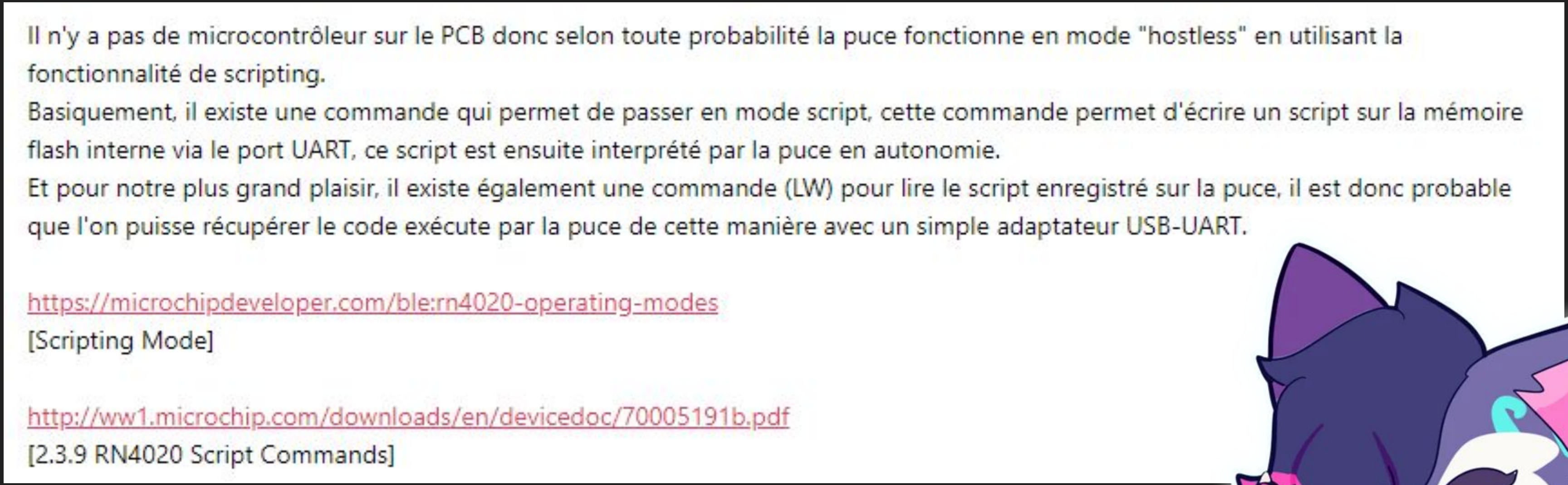
No data available

Failed to establish connection to device, please select another device or try again.

What about a possible firmware ?

Messing with the UART again

Some information has been given after publishing the paper

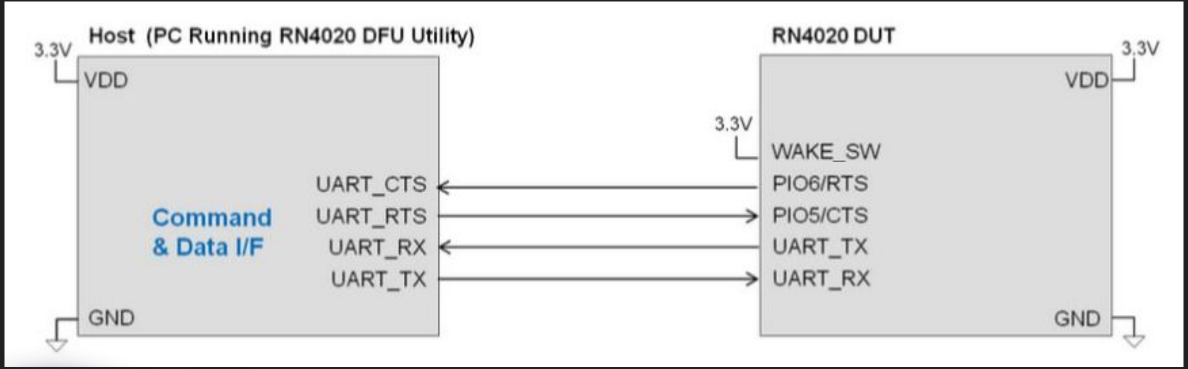


Il n'y a pas de microcontrôleur sur le PCB donc selon toute probabilité la puce fonctionne en mode "hostless" en utilisant la fonctionnalité de scripting.
Basiquement, il existe une commande qui permet de passer en mode script, cette commande permet d'écrire un script sur la mémoire flash interne via le port UART, ce script est ensuite interprété par la puce en autonomie.
Et pour notre plus grand plaisir, il existe également une commande (LW) pour lire le script enregistré sur la puce, il est donc probable que l'on puisse récupérer le code exécute par la puce de cette manière avec un simple adaptateur USB-UART.

https://microchipdeveloper.com/ble:rn4020-operating-modes
[Scripting Mode]

http://ww1.microchip.com/downloads/en/devicedoc/70005191b.pdf
[2.3.9 RN4020 Script Commands]

Time for more documentation crawling



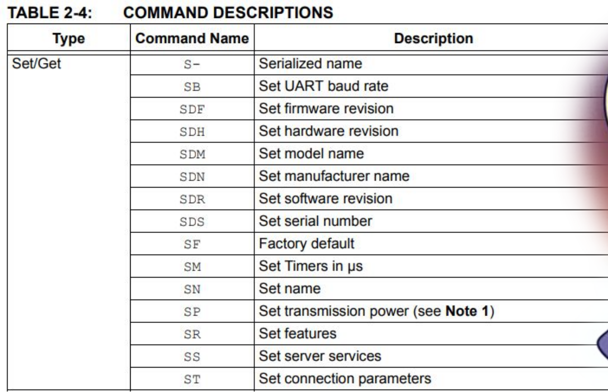


TABLE 2-4: COMMAND DESCRIPTIONS

Type	Command Name	Description
Set/Get	S-	Serialized name
	SB	Set UART baud rate
	SDF	Set firmware revision
	SDH	Set hardware revision
	SDM	Set model name
	SDN	Set manufacturer name
	SDR	Set software revision
	SDS	Set serial number
	SF	Factory default
	SM	Set Timers in µs
	SN	Set name
	SP	Set transmission power (see **Note 1**)
	SR	Set features
	SS	Set server services
	ST	Set connection parameters

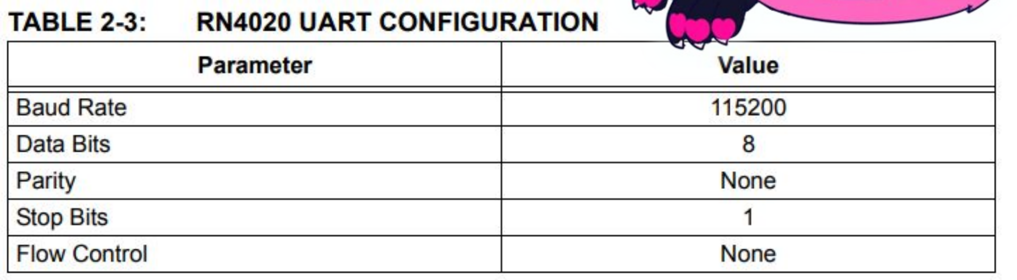
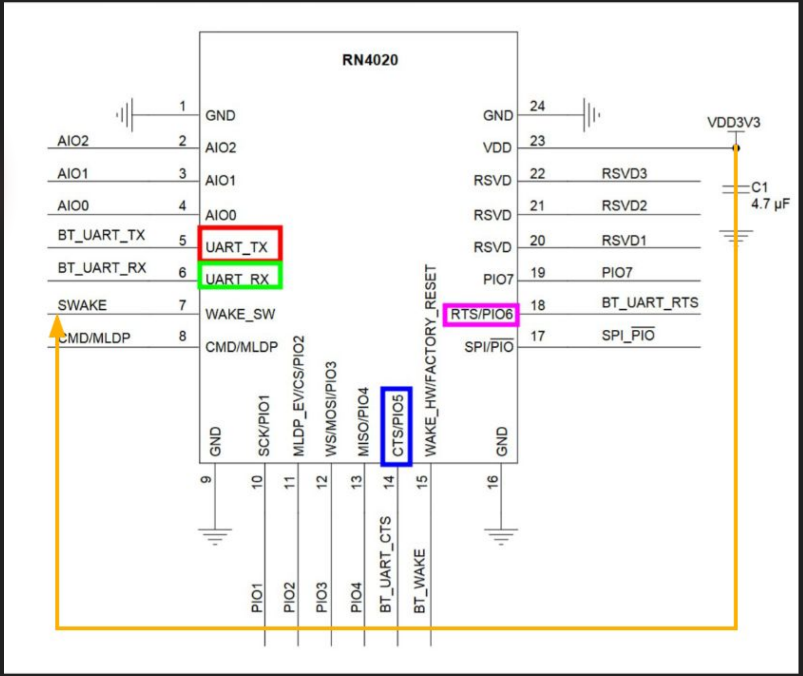
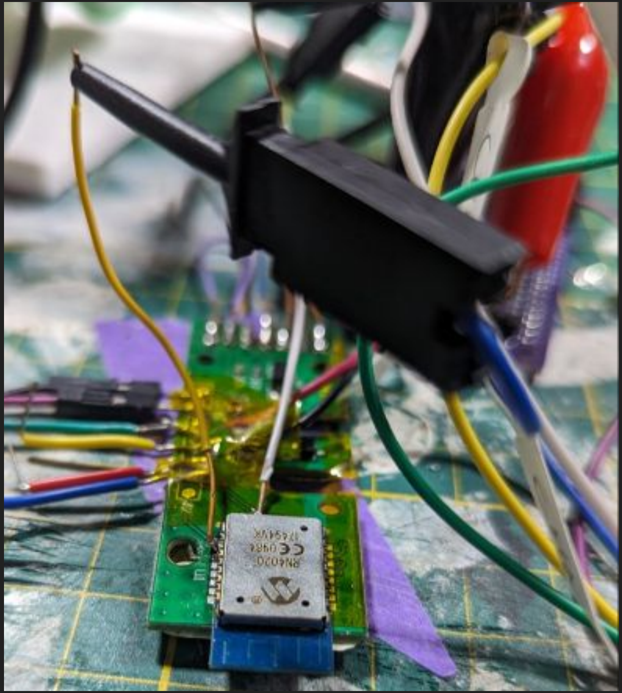


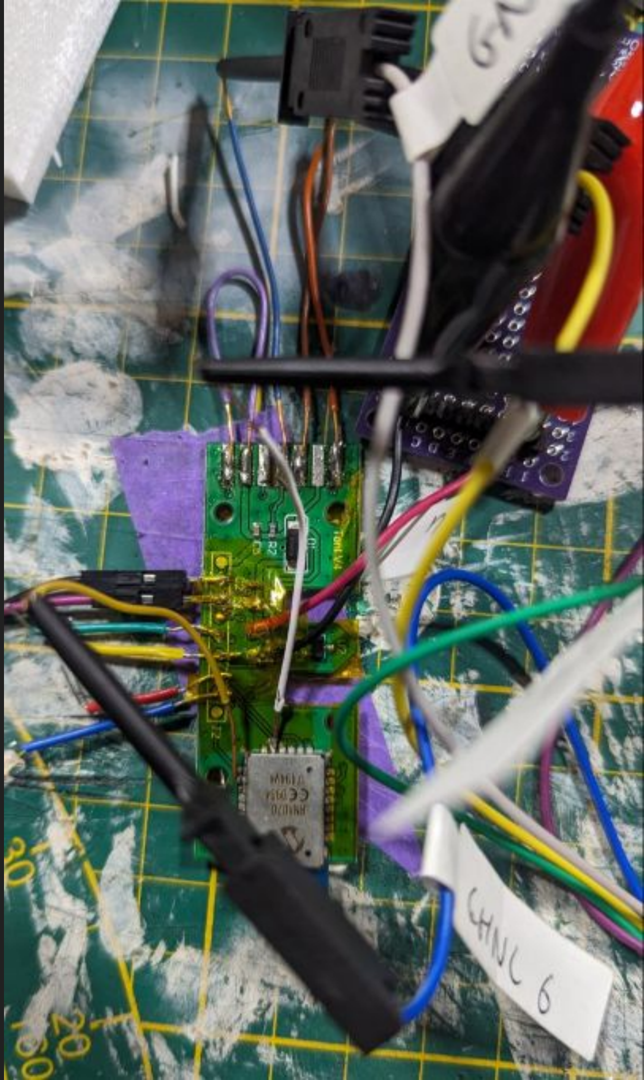
TABLE 2-3: RN4020 UART CONFIGURATION

Parameter	Value
Baud Rate	115200
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

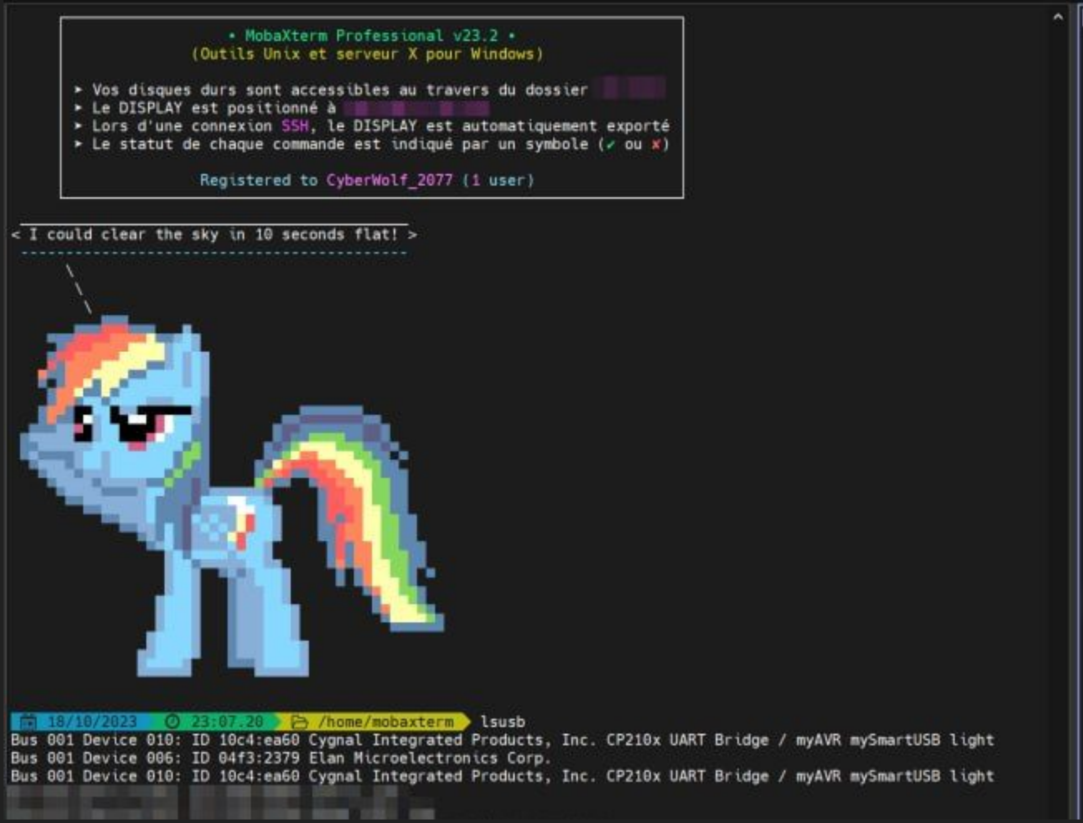


Probing the chip again



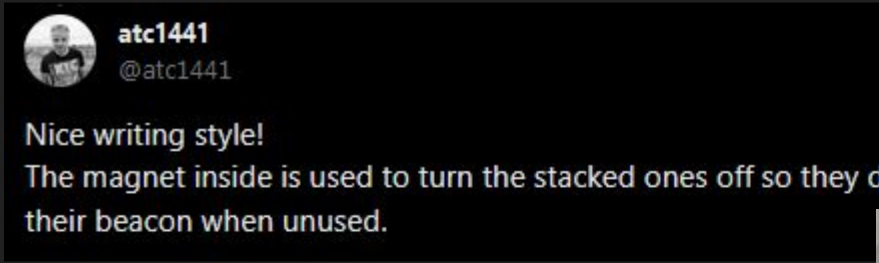


Dumping a firmware ?



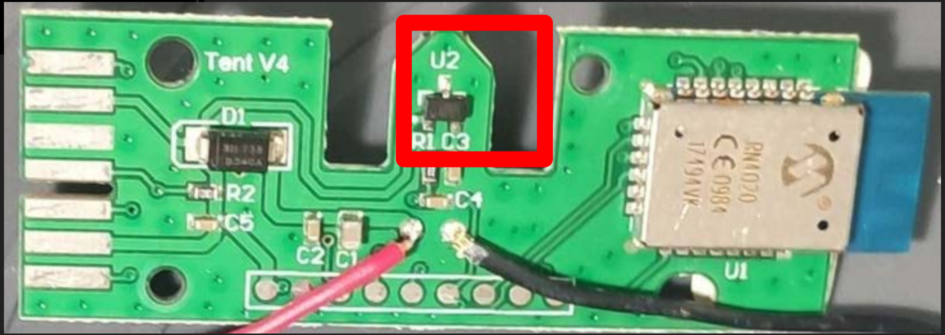
```
                    • MobaXterm Professional v23.2 •
                (Outils Unix et serveur X pour Windows)

   ➤ Vos disques durs sont accessibles au travers du dossier [redacted]
   ➤ Le DISPLAY est positionné à [redacted]
   ➤ Lors d'une connexion SSH, le DISPLAY est automatiquement exporté
   ➤ Le statut de chaque commande est indiqué par un symbole (✓ ou ✗)

                  Registered to CyberWolf_2077 (1 user)

 ___________________________________________
< I could clear the sky in 10 seconds flat! >
 -------------------------------------------
       \
        \
         \

 18/10/2023   23:07.20   /home/mobaxterm  lsusb
Bus 001 Device 010: ID 10c4:ea60 Cygnal Integrated Products, Inc. CP210x UART Bridge / myAVR mySmartUSB light
Bus 001 Device 006: ID 04f3:2379 Elan Microelectronics Corp.
Bus 001 Device 010: ID 10c4:ea60 Cygnal Integrated Products, Inc. CP210x UART Bridge / myAVR mySmartUSB light
[redacted]
```

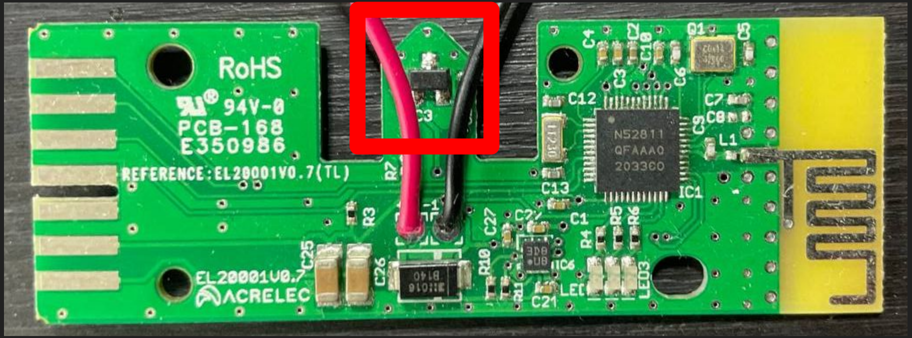
Some random stuff found on the way



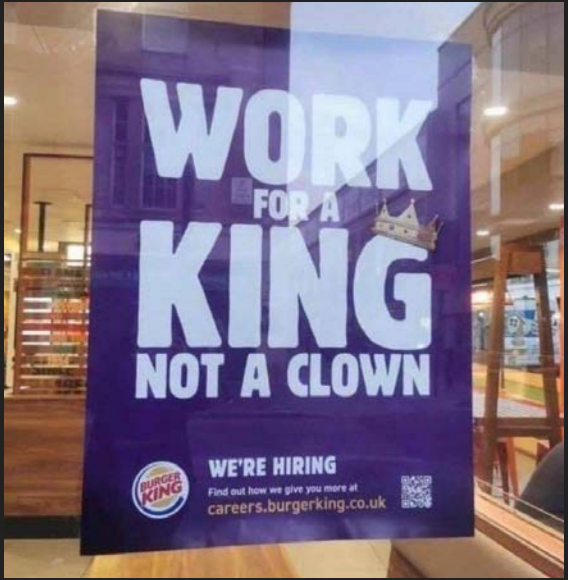
atc1441
@atc1441

Nice writing style!
The magnet inside is used to turn the stacked ones off so they do no beac
their beacon when unused.





Is the king better than the clown ?



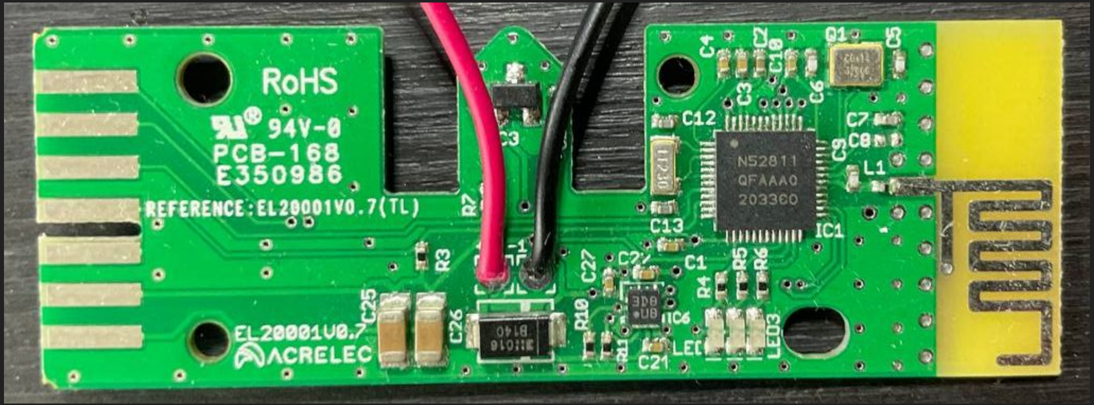
WORK FOR A KING NOT A CLOWN

WE'RE HIRING

Find out how we give you more at careers.burgerking.co.uk

PCB of the king beacon

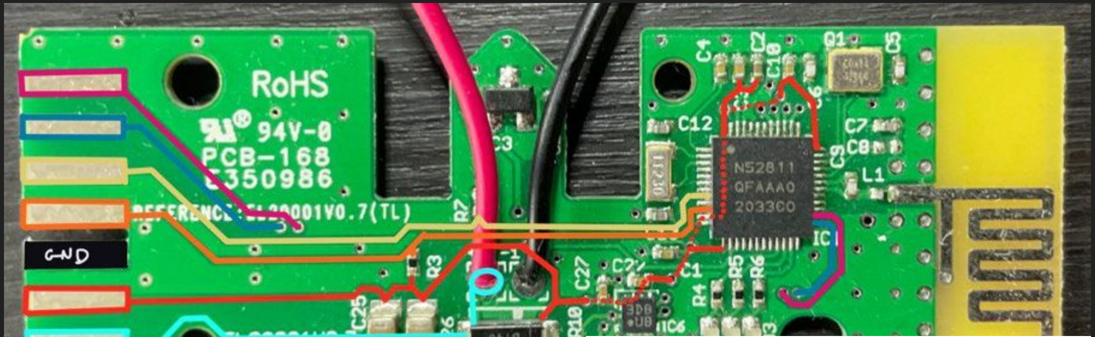
nRF52811 SoC Bluetooth 5.4 supporting Bluetooth Low Energy, Bluetooth Direction Finding and Thread

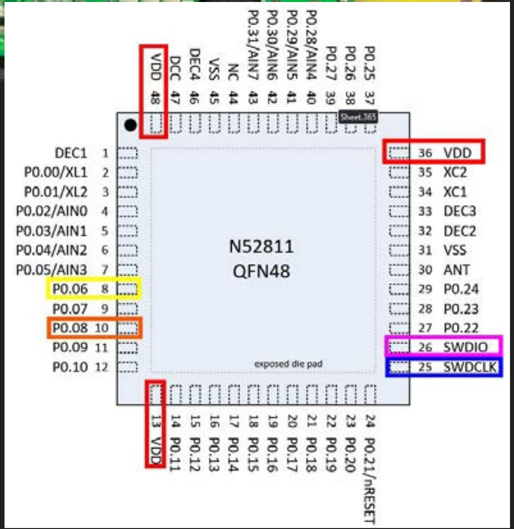


⚠️ This section still is WIP, information may evolve over time

PCB of the king beacon

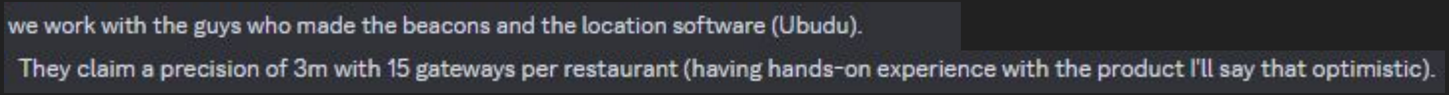
Pin	Name	Type	Description
8	P0.06	Digital I/O	General purpose I/O
10	P0.08	Digital I/O	General purpose I/O
13/36/48	VDD	Power	Power supply
25	SWDCLK	Digital input	Serial wire debug clock input for debug and programming
26	SWDIO	Digital I/O	Serial wire debug I/O for debug and programming





⚠️ This section still is WIP, information may evolve over time

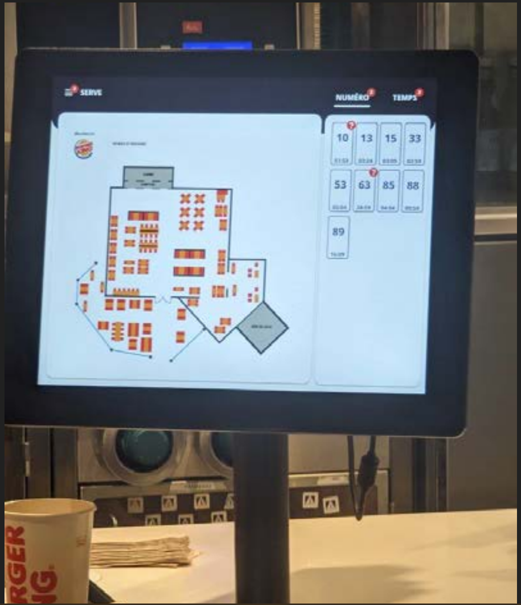
On site mapping system



we work with the guys who made the beacons and the location software (Ubudu).

They claim a precision of 3m with 15 gateways per restaurant (having hands-on experience with the product I'll say that optimistic).

ubudu



⚠ This section still is WIP, information may evolve over time

Next steps

- Doing same work on KFC beacon
- Beacon spoofing
- Overload of beacon usage
- ...

Questions

Ressources

- RN4020 datasheet : https://www.microchip.com/en-us/product/RN4020 https://ww1.microchip.com/downloads/aemDocuments/documents/WSG/ProductDocuments/DataSheets/50002279E.pdf https://ww1.microchip.com/downloads/en/devicedoc/70005191b.pdf
- ATC1441 twitte about U2 : https://twitter.com/atc1441/status/1678707482452008960
- nRF52811 datasheet : https://infocenter.nordicsemi.com

Tools list

- Logic Analyzer
- USB > UART
- TS100 Soldering Iron
- ANENG Q1 multimeter
- Saleae Logic 2.4.1
- Lightblue android app