LOW POWER TO THE PEOPLE

PROGRAMMING BLE THE HARD WAY

LOW POWER TO THE PEOPLE

PROGRAMMING BLE THE HARD WAY

BY

MILOSCH MERIAC

HTTPS://MERIAC.COM

MILOSCH@MERIAC.COM

WHO AM I ?

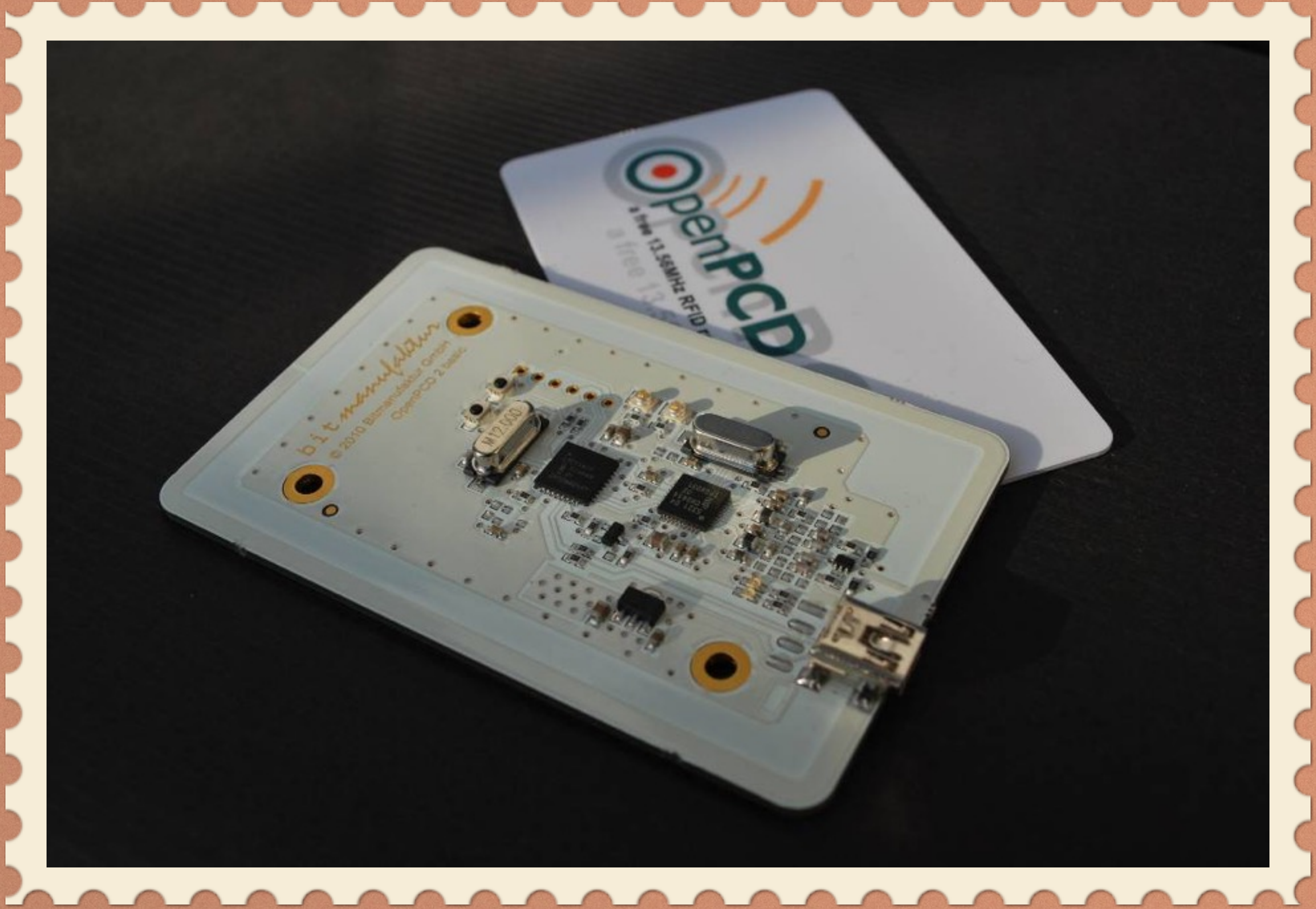
MILOSCH MERIAC

RFID- & HW SECURITY EXPERT

- ★ Love breaking things
- ★ Co-Founder of various open source and open hardware projects like OpenPCD.org, OpenBeacon.org where I designed the first open 13.56MHz hardware design.
- ★ RFID & Hardware Security Researcher (broke HID iClass security)
- ★ Enjoy designing secure ultra low power wireless sensors with privacy-enabled protocols and services.
- ★ In my private time I love making/grokking things. I am currently playing with RGB strips to create light paintings.

OPENPCD.ORG

Fork me on GitHub



PASSIVE RFID

13.56 MHZ WITH NFC SUPPORT

- ★ Open Hardware and Open Firmware
- ★ ARM Cortex-M3 LPC134x - flashed via USB Mass Storage
- ★ Security Research Tool: boatload of test signals for Oscilloscope via two U.FL sockets
- ★ Compatible to LibNFC and MIFARE Classic cracking tools
- ★ See also RFID sniffer tools

Fork me on GitHub

ACTIVE RFID TAG

REAL TIME CONFERENCE TRACKING

★ Started with tracking 1000 people at the CCC conference in Berlin in 2006

★ 2.4GHz + 8bit PIC microcontroller

★ Detects human interaction in real time

★ Open Hardware & Software

BLINKENLIGHT STEREOSCOPE

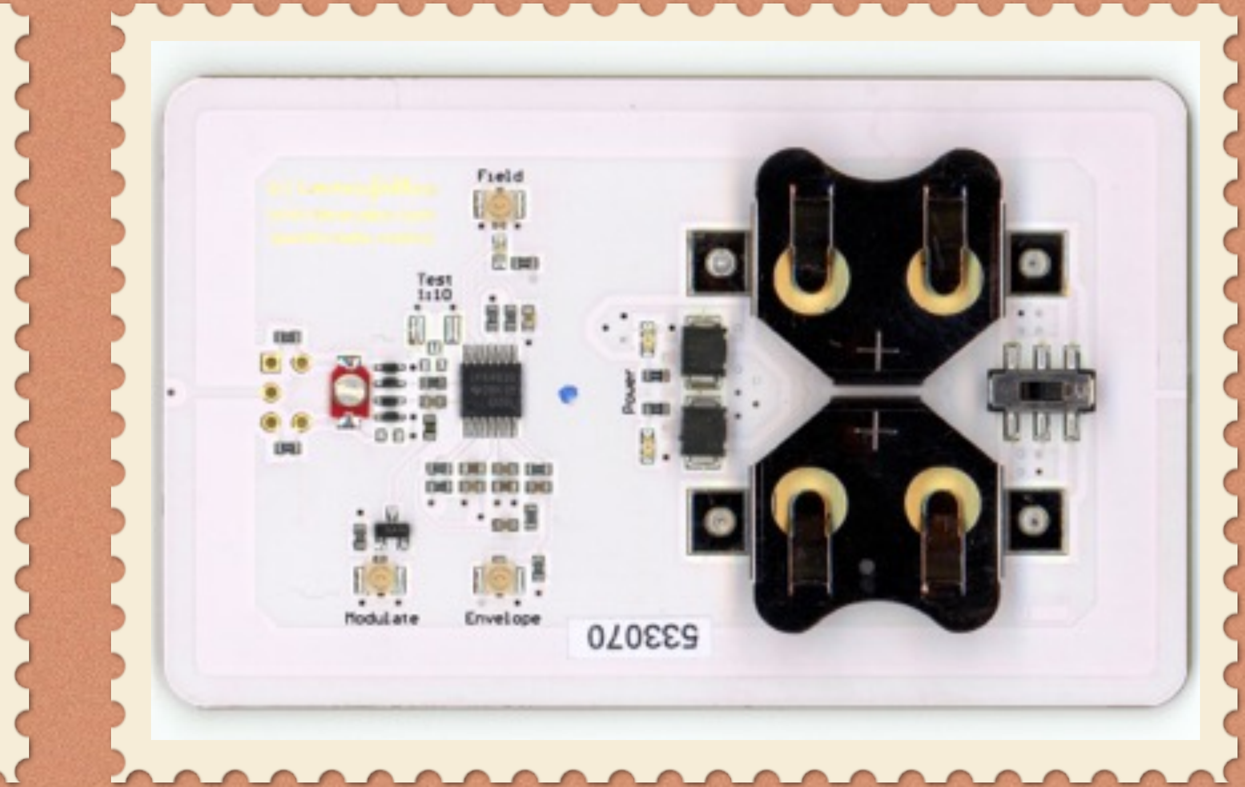
Fork me on GitHub

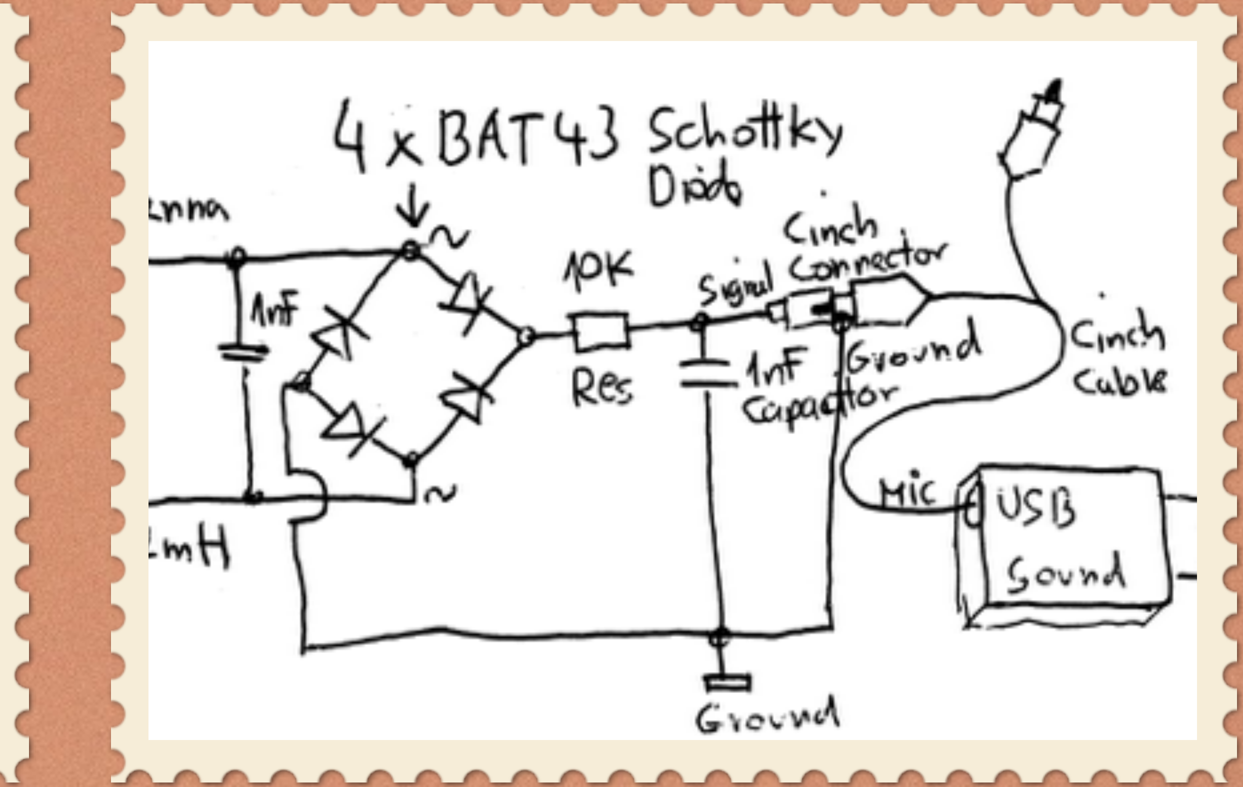
NUIT BLANCHE

TORONTO, CANADA

- ★ 960 wireless OpenBeacon 2.4GHz AC dimmers
- ★ per-floor wireless-toEthernet gateways
- ★ real time UDP protocol, each floor forwards only the data for it's lights
- ★ one wireless packet per floor
- ★ Chaos Communication Protocol for resilient realtime animations

OTHER PROJECTS





If you have interesting projects or need my help - feel free to contact me at meriac.com

GET.OPENBEACON.ORG

ABOUT BLUETOOTH
QUICK AND DIRTY

HARDWARE
WHAT WE HAVE

SOFTWARE
DEVELOPMENT FLOW

APPLICATIONS
EPLOITING THE INTERNET OF THINGS

BLUETOOTH LOW ENERGY

2.4GHZ ISM

- 2402-2480 MHz
- 1 Mbps
- GFSK (modulation index 0.5)
- range between 30m to 150m

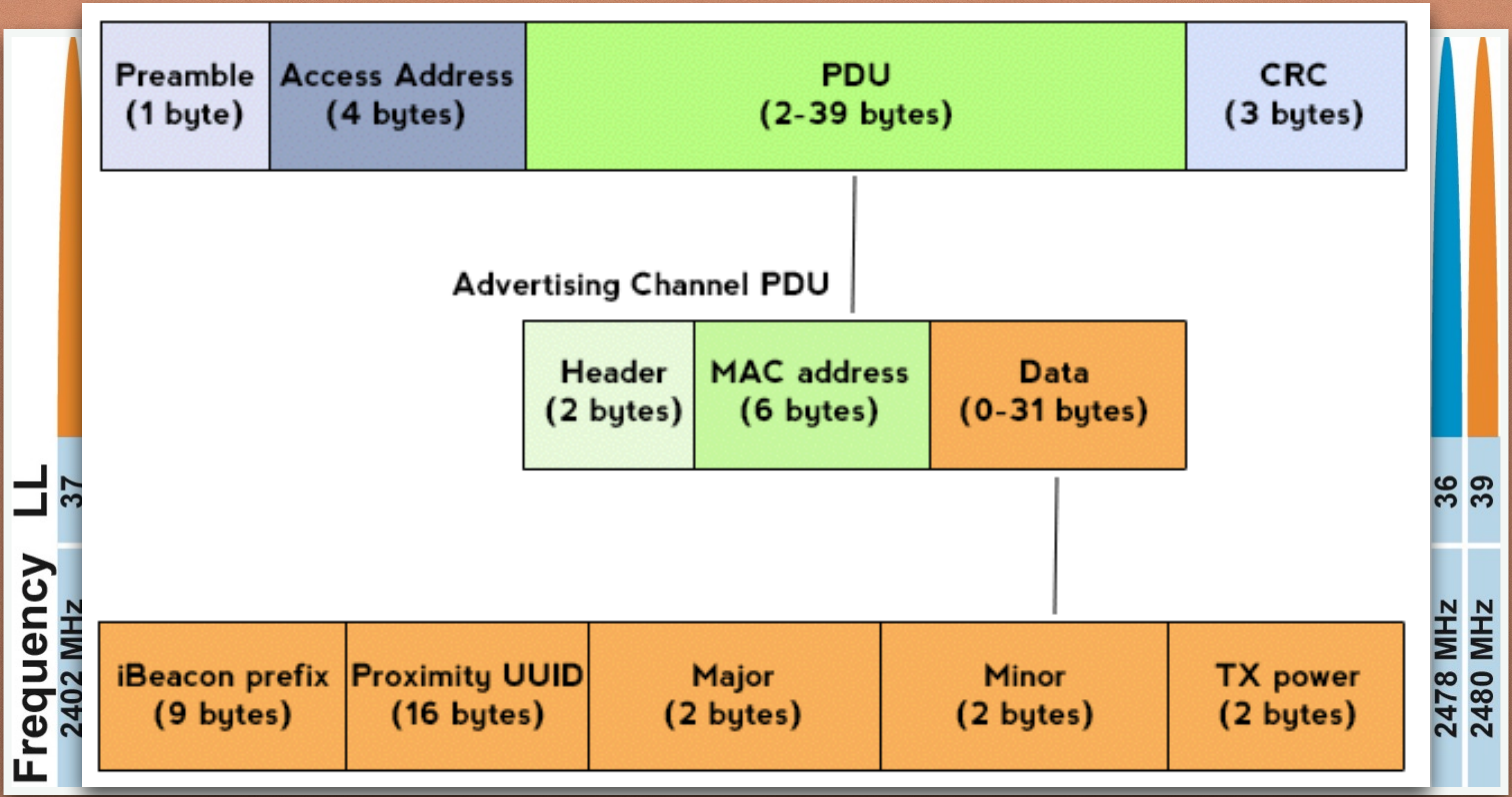
40 CHANNELS

- 3 advertisement channels (2402, 2426 and 2480 MHz)
- 37 data channels with 2 MHz spacing

SIMPLE

- 1 byte preamble 0xAA or 0x55
- 4 byte access address for target (0x8E89BED6 for advertisement channel)
- 2 to 29 byte Protocol Data Unit
- 3 byte CRC for PDU
- PDU & CRC whitened per channel

IBEACON PROTOCOL EXAMPLE



Preamble (1 byte)	Access Address (4 bytes)	PDU (2-39 bytes)	CRC (3 bytes)

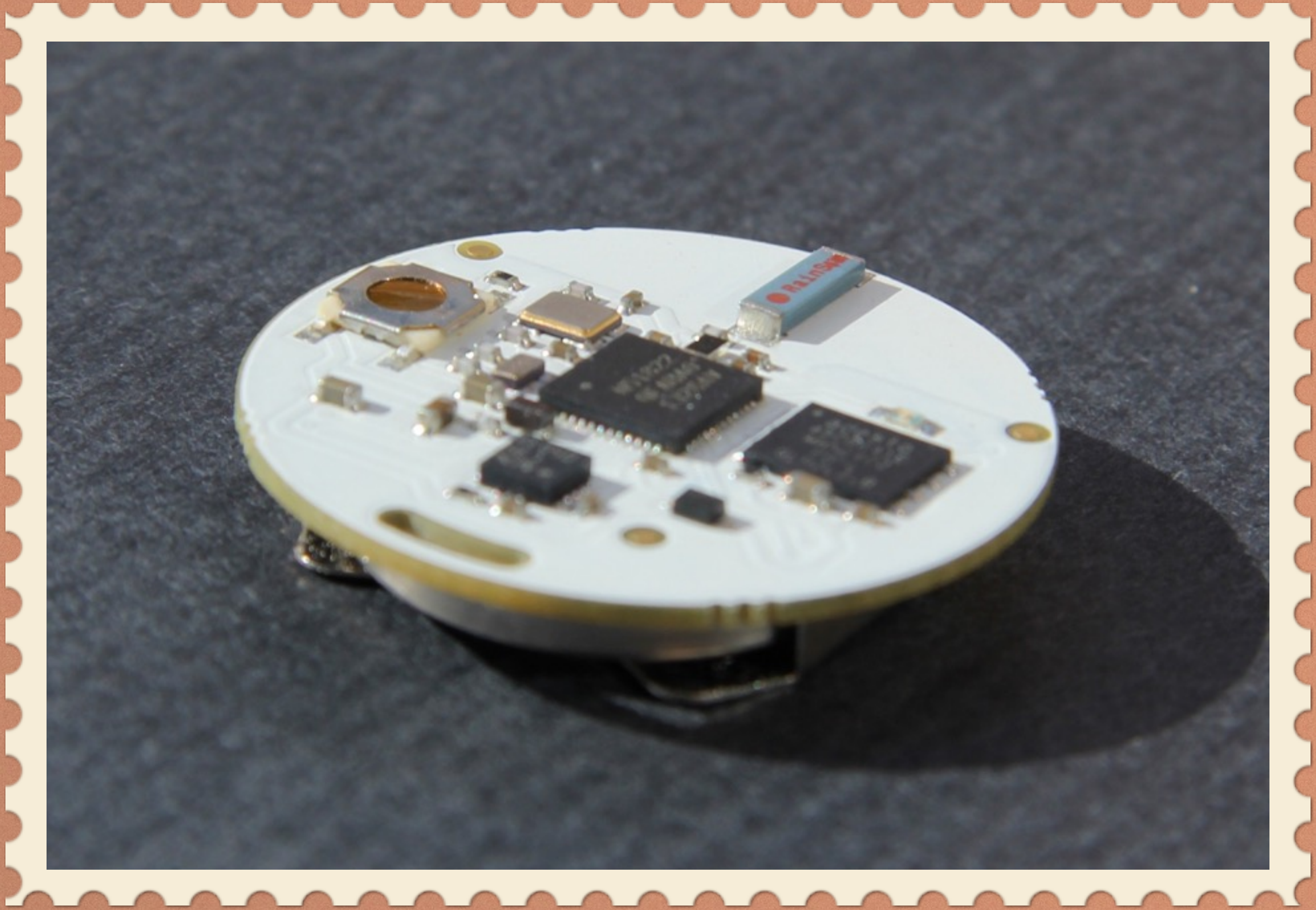
Advertising Channel PDU

Header (2 bytes)	MAC address (6 bytes)	Data (0-31 bytes)

iBeacon prefix (9 bytes)	Proximity UUID (16 bytes)	Major (2 bytes)	Minor (2 bytes)	TX power (2 bytes)

OPENBEACON HARDWARE

Fork me on GitHub



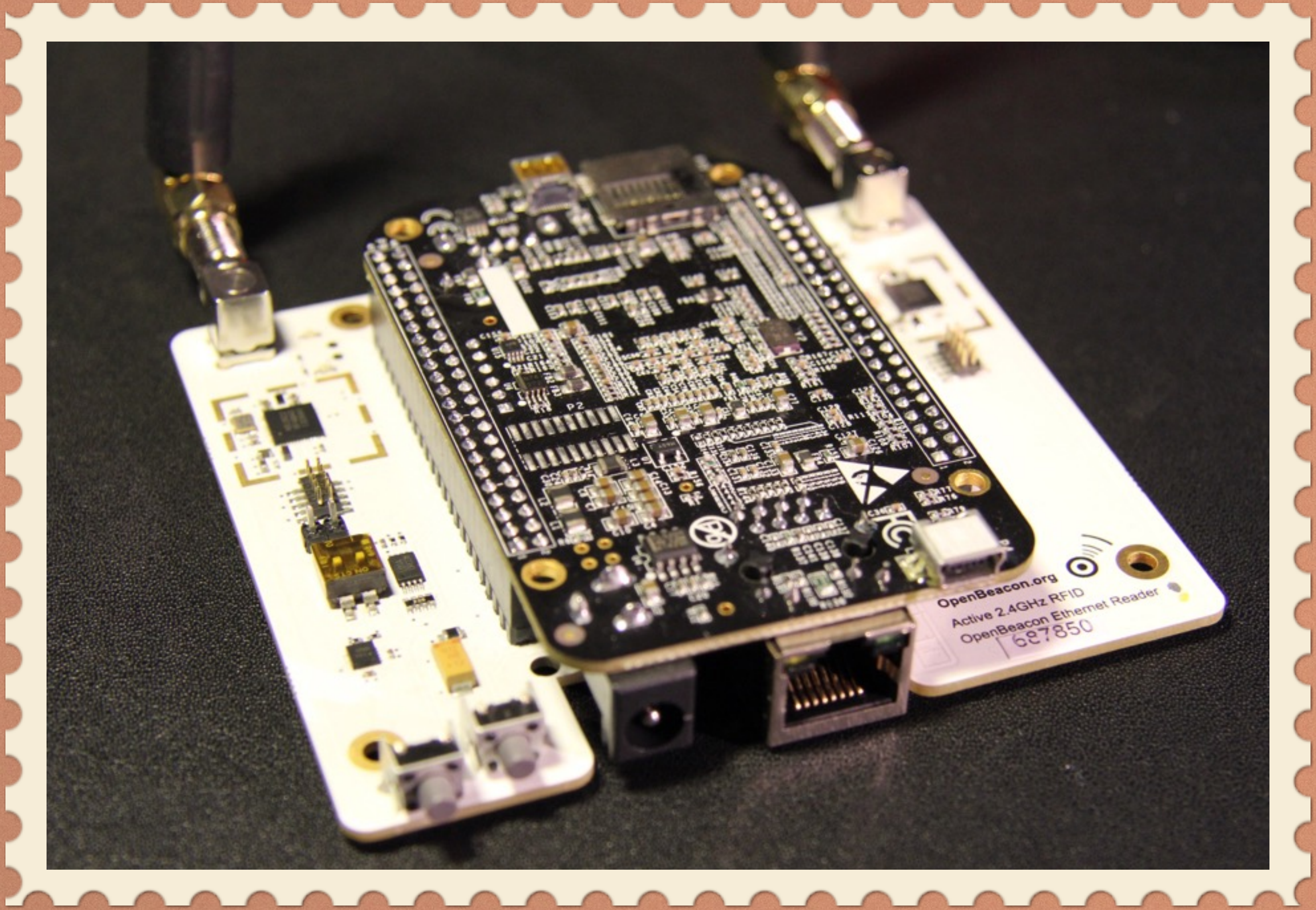
LATEST HARDWARE

HARDWARE SPECIFICATION

- ★ Bluetooth Low Energy Protocol
- ★ 3D accelerometer for real-time movement detection
- ★ OpenBeacon proximity & tracking protocol
- ★ 8MB of external flash for offline-logging of tag-to-tag proximity encounters and movement
- ★ 32-bit ARM Cortex M0 CPU based on the nRF51822 SoC from Nordic Semiconductors
- ★ 256KB flash & 16KB SRAM

Fork me on GitHub

OPENBEACON HARDWARE



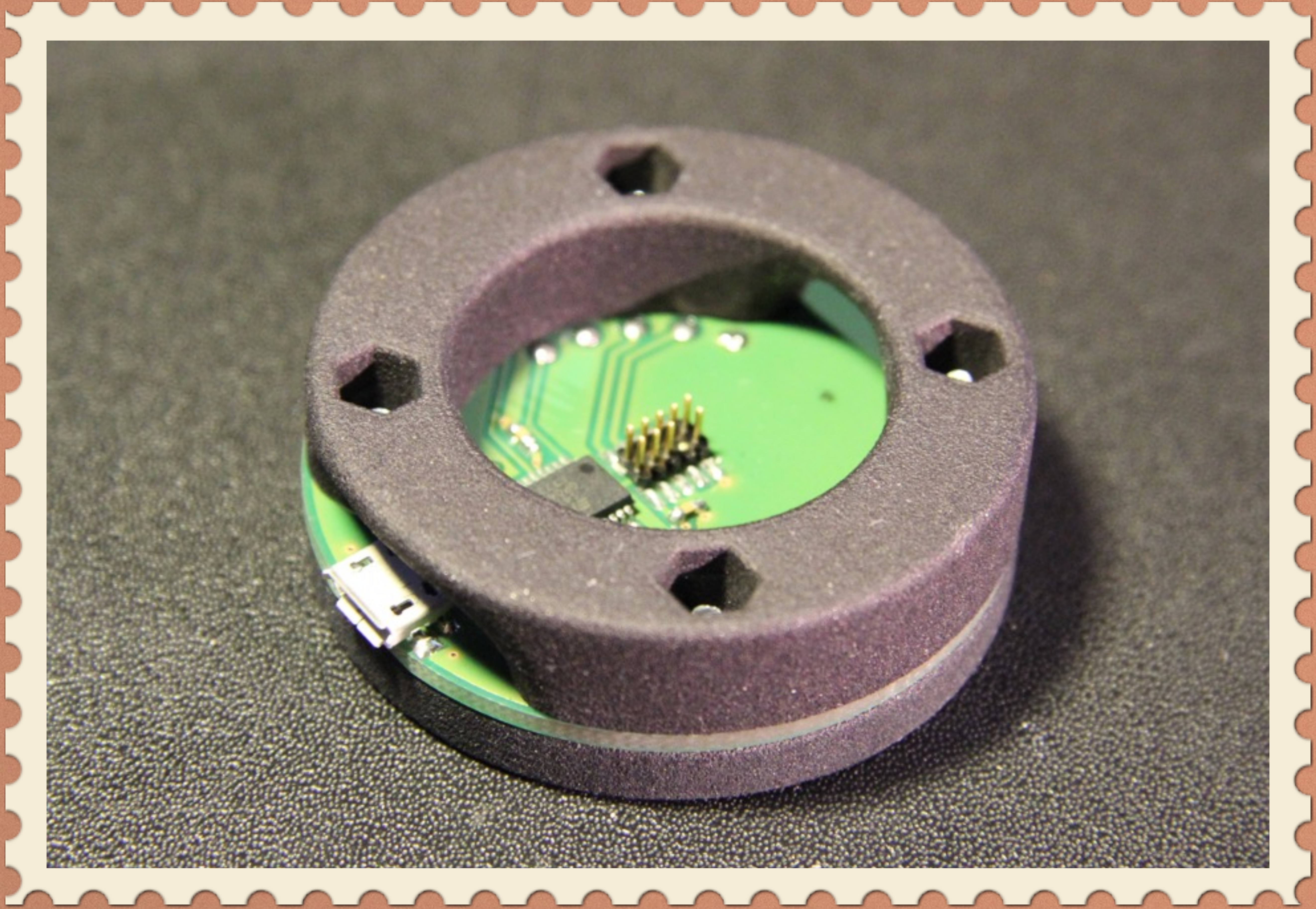
LATEST READER

HARDWARE SPECIFICATION

★ BeagleBone Black Cape
★ Add precision RTC with CR2032 battery buffering
★ 3D accelerometer for theft detection
★ 2 nRF51822 Interfaces better reception (Diversity)
★ WIFI-Compatible RPSMA antennas (5dBi)
★ 100 MBit Ethernet
★ WIFI Meshing planned

OPENBEACON HARDWARE

Fork me on GitHub



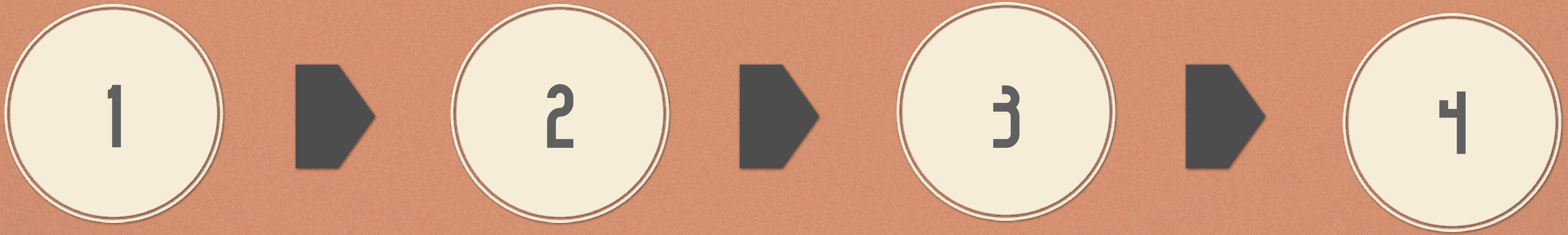
DEBUG ADAPTER

USER FRIENDLY INTERFACE

- ★ Interfaces to JLink SQO/JTAG Debugger or nRF51-DK with integrated SWO debug interface
- ★ provides serial over USB serial interface for convenient printf debugging
- ★ Spring loaded pogo pins for flashing a large number of tags
- ★ provides 3.3V power over USB
- ★ Can act as a reader in combination with a tag
- ★ Fastening clip for tags available

TOOLCHAIN INSTALLATION

Development is possible on OS X, Linux (Fedora or Ubuntu). Development on Windows might work with Cygwin, but is not supported by our Makefiles



1. GET ARM TOOLCHAIN
   LAUNCHPAD.NET/GCC-ARM-EMBEDDED
2. GET DEBUGGER
   NORDICSEMI.COM
3. GET JLINK SOFTWARE
   SEGGER.COM
4. GET OPENBEACON-NG
   GITHUB.COM/MERIAC/OPENBEACON-NG

BLUETOOTH LOW ENERGY

EXAMPLE CODE

IBEACON

In our source tree you can find both an iBeacon reader and an iBeacon tag example.
The reader decodes iBeacon advertisements and prints them on a 3.3V serial interface in text format.
The reader can be connected with little effort to Arduino or similar devices.

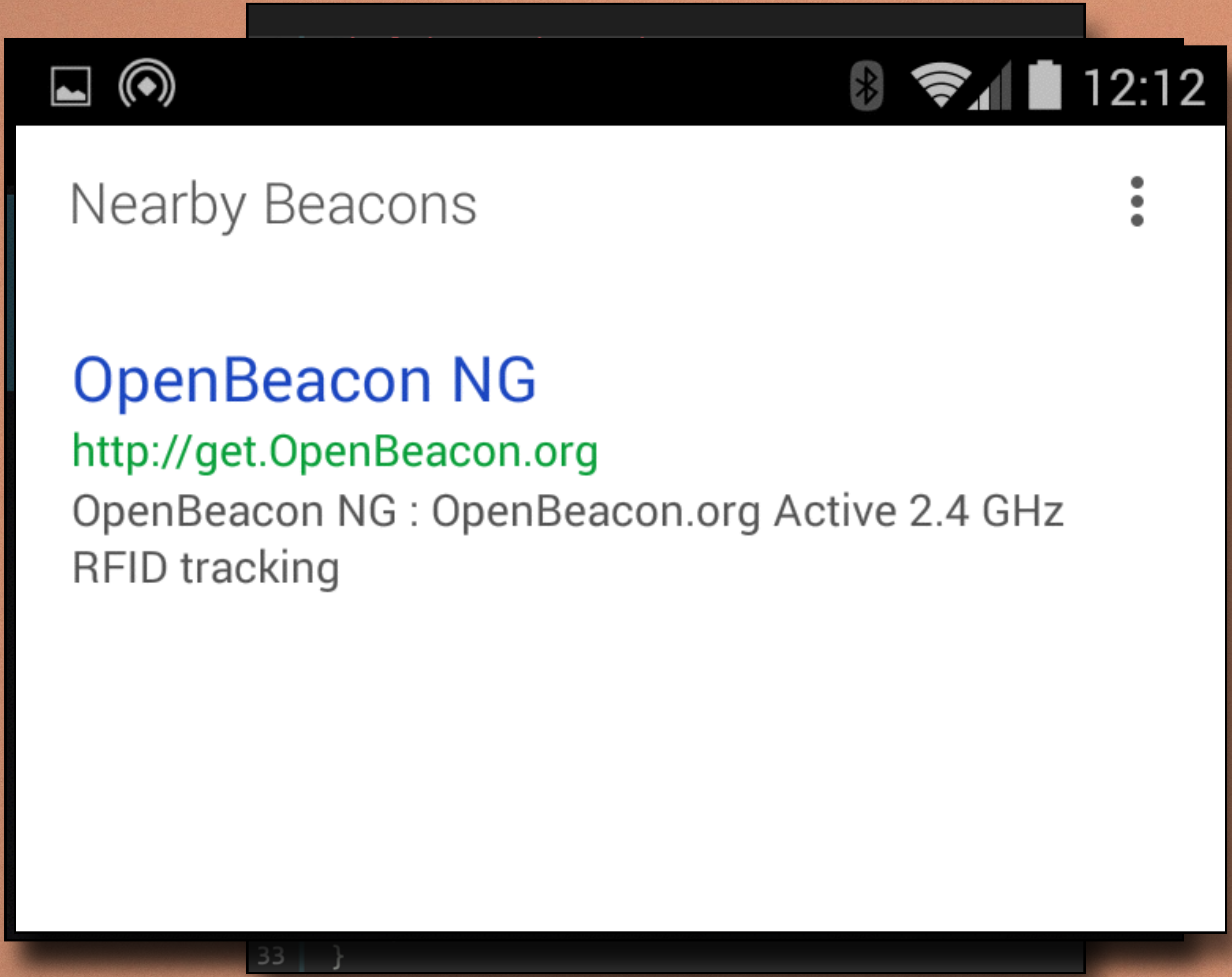
PHYSICAL WEB

The physical web beacon firmware allows advertising of URL's - clients are available for IOS and Android

MISCHIEF

Due to Bare Metal Access to the radio interface, mischievous Bluetooth devices can be easily created.
The first example in a series of upcoming devices allows the creation of an arbitrary amount of virtual BLE devices on the fly to confuse people scanning for their devices.

ENTRY LEVEL EXAMPLE



Nearby Beacons

OpenBeacon NG

http://get.OpenBeacon.org

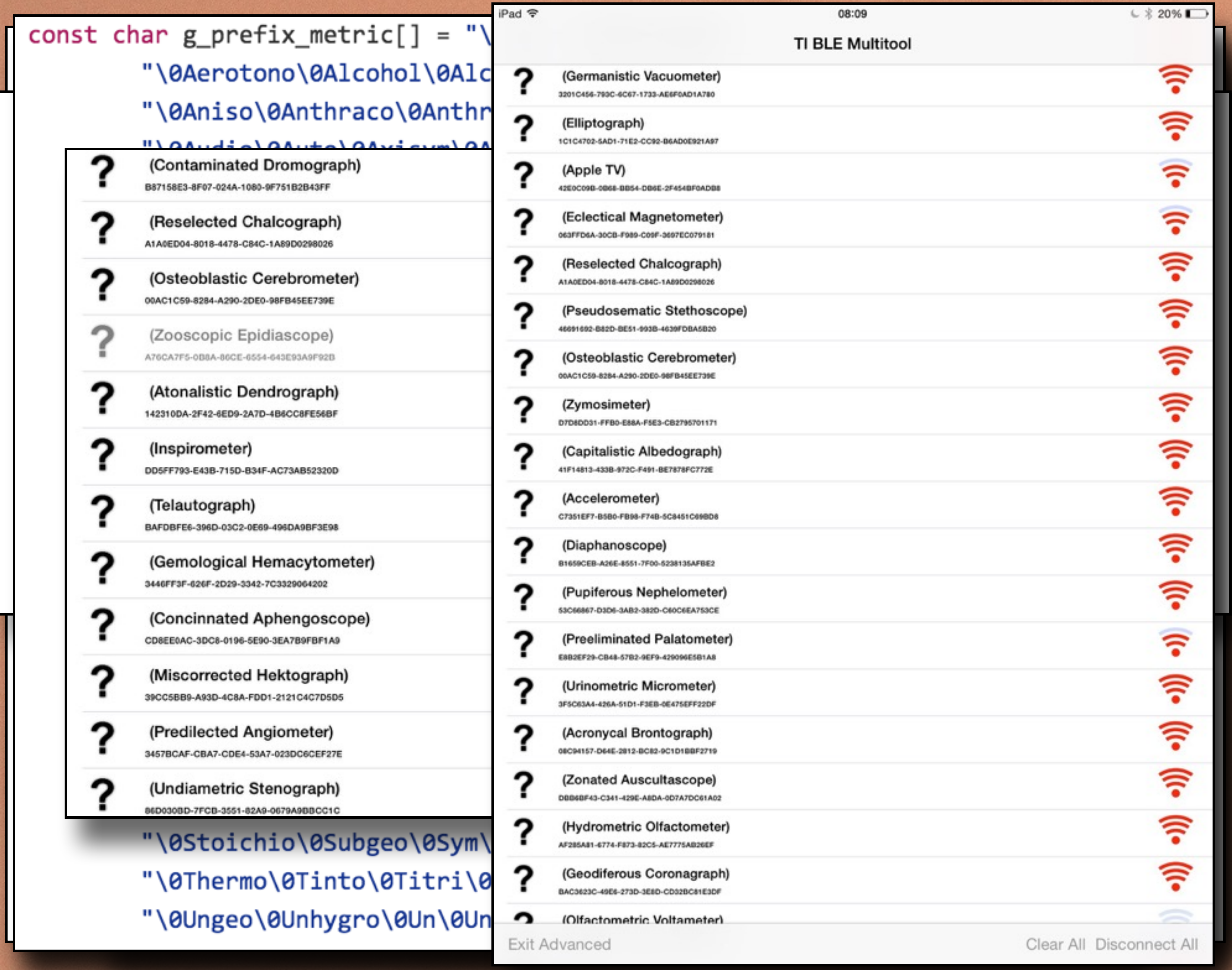
OpenBeacon NG : OpenBeacon.org Active 2.4 GHz RFID tracking

EXAMPLE CODE

PHYSICAL WEB BEACON

- ★ Nice starter example - try modifying the URL in the example software.
- ★ Make sure to update the length field in the protocol header to reflect your new string length
- ★ Resulting firmware is around 4.7k - including C-lirary functions like printf
- ★ UART debug support

ADVANCED EXAMPLE



```
const char g_prefix_metric[] = "\
        "\0Aerotono\0Alcohol\0Alc
        "\0Aniso\0Anthraco\0Anthr
        "\0Audio\0Auto\0Axisym\0A
        "\0Stoichio\0Subgeo\0Sym\
        "\0Thermo\0Tinto\0Titri\0
        "\0Ungeo\0Unhygro\0Un\0Un
```

? (Contaminated Dromograph)
B87158E3-8F07-024A-1080-9F751B2B43FF

? (Reselected Chalcograph)
A1A0ED04-8018-4478-C84C-1A89D0298026

? (Osteoblastic Cerebrometer)
00AC1C59-8284-A290-2DE0-98FB45EE739E

? (Zooscopic Epidiascope)
A76CA7F5-0B8A-86CE-6554-643E93A9F92B

? (Atonalistic Dendrograph)
142310DA-2F42-6ED9-2A7D-4B6CC8FE56BF

? (Inspirometer)
DD5FF793-E43B-715D-B34F-AC73AB52320D

? (Telautograph)
BAFDBFE6-396D-03C2-0E69-496DA9BF3E98

? (Gemological Hemacytometer)
3446FF3F-626F-2D29-3342-7C3329064202

? (Concinnated Aphengoscope)
CD8EE0AC-3DC8-0196-5E90-3EA7B9FBF1A9

? (Miscorrected Hektograph)
39CC5BB9-A93D-4C8A-FDD1-2121C4C7D5D5

? (Predilected Angiometer)
3457BCAF-CBA7-CDE4-53A7-023DC6CEF27E

? (Undiametric Stenograph)
86D030BD-7FCB-3551-82A9-0679A9BBCC1C

TI BLE Multitool

? (Germanistic Vacuometer)
3201C456-793C-6C67-1733-AE6F0AD1A780

? (Elliptograph)
1C1C4702-5AD1-71E2-CC92-B6AD0E921A97

? (Apple TV)
42E0C09B-0B68-BB54-DB6E-2F454BF0ADB8

? (Eclectical Magnetometer)
063FFD6A-30CB-F989-C09F-3697EC079181

? (Reselected Chalcograph)
A1A0ED04-8018-4478-C84C-1A89D0298026

? (Pseudosematic Stethoscope)
46691692-B82D-BE51-993B-4639FDBA5B20

? (Osteoblastic Cerebrometer)
00AC1C59-8284-A290-2DE0-98FB45EE739E

? (Zymosimeter)
D7D8DD31-FFB0-E88A-F5E3-CB2795701171

? (Capitalistic Albedograph)
41F14813-433B-972C-F491-BE7878FC772E

? (Accelerometer)
C7351EF7-B5B0-FB98-F74B-5C8451C69BD8

? (Diaphanoscope)
B1659CEB-A26E-8551-7F00-5238135AFBE2

? (Pupiferous Nephelometer)
53C66867-D3D6-3AB2-382D-C60C6EA753CE

? (Preeliminated Palatometer)
E8B2EF29-CB48-57B2-9EF9-429096E5B1A8

? (Urinometric Micrometer)
3F5C63A4-426A-51D1-F3EB-0E475EFF22DF

? (Acronycal Brontograph)
08C94157-D64E-2812-BC82-9C1D1BBF2719

? (Zonated Auscultascope)
DBB6BF43-C341-429E-A8DA-0D7A7DC61A02

? (Hydrometric Olfactometer)
AF285A81-6774-F873-82C5-AE7775AB26EF

? (Geodiferous Coronagraph)
BAC3623C-49E6-273D-3E8D-CD32BC81E3DF

? (Olfactometric Voltameter)

MISCHIEVOUS TAG

ANNOY YOUR PEER GROUP

★ Shows chaining of hardware Events to allow low power

★ Radio initialisation and BLE advertisement state machine is just 259 lines of code

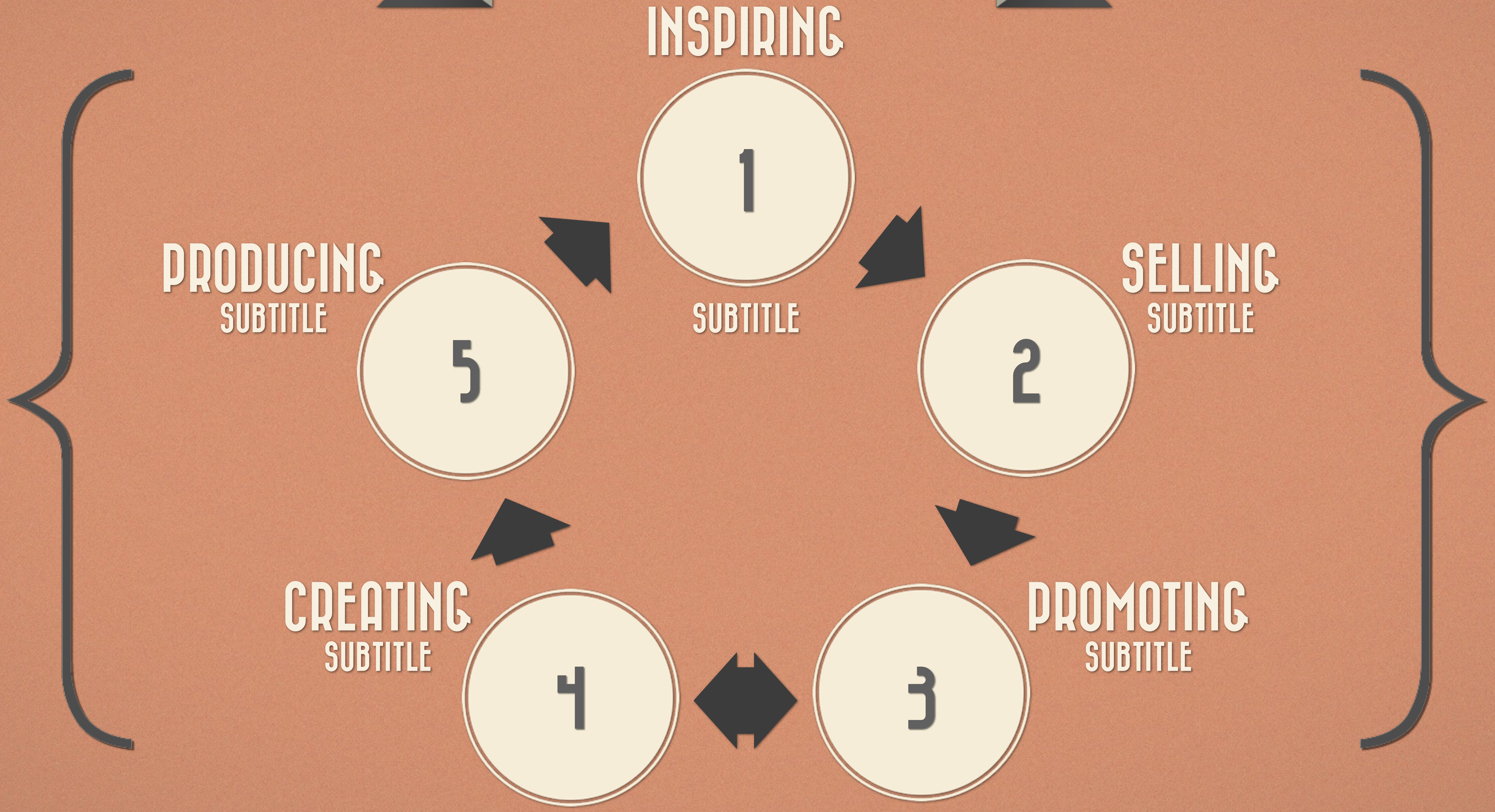
★ Simulates at any given time 23 concurrent BLE beacon with names that are constantly changing

★ To confuse people more, the names are made up on the fly from a word snippet database

QUESTIONS ?

See OpenBeacon Tracker API Installation for setting up the server API and example code applications on your own server. Feel free to browse our git source code repository or download the source code as Unix tar.bz2 archive file or Windows ZIP file.

HOW WE WORK



INSPIRING

1

SUBTITLE

SELLING

SUBTITLE

2

PROMOTING

SUBTITLE

3

CREATING

SUBTITLE

4

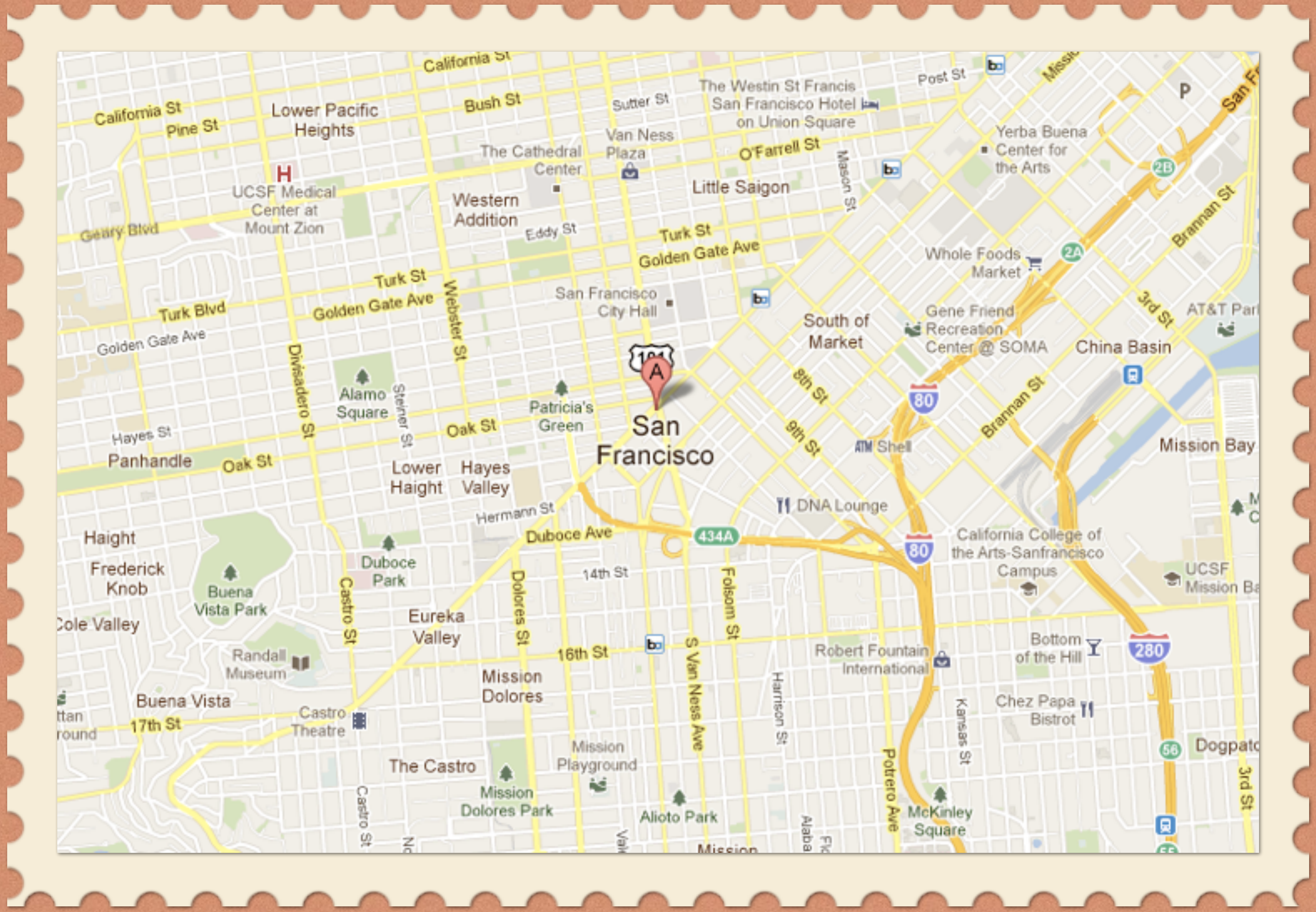
PRODUCING

SUBTITLE

5

CONTACT US

MAP



WWW.RETROSLIDES.XX

INFO@RETROSLIDES.XX

(650) 695-143236

Whe are in 1571-1599 Market Street
San Francisco, CA 94103 TEL. (650) 695-143236

FOLLOW US

FACEBOOK
WWW.FACEBOOK.COM/RETROSLIDES

TWITTER
WWW.TWITTER.COM/RETROSLIDES

FLICKR
WWW.FLICKR.COM/RETROSLIDES

VIMEO
WWW.VIMEO.COM/RETROSLIDES

MYSPACE
WWW.MYSPACE.COM/RETROSLIDES

LINKEDIN
WWW.LINKEDIN.COM/RETROSLIDES

TUMBLR
WWW.TUMBLR.COM/RETROSLIDES

DEVIANTART
WWW.DEVIANTART.COM/RETROSLIDES

OPENBEACON.ORG

THANK YOU

FOR YOUR ATTENTION.

HTTP://WWW.OPENBEACON.ORG/