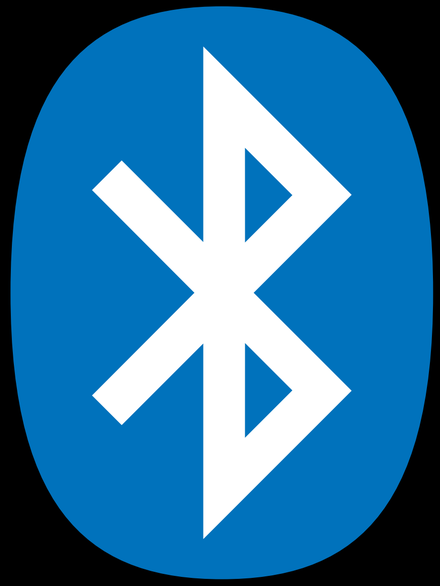
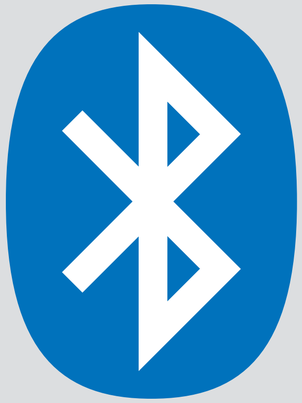
fun with



bluetooth



bluetooth sucks

classic bluetooth

the reason everybody hates bluetooth

vs.

control drones and other cool shit

bluetooth low energy

bluetooth low energy

also known as

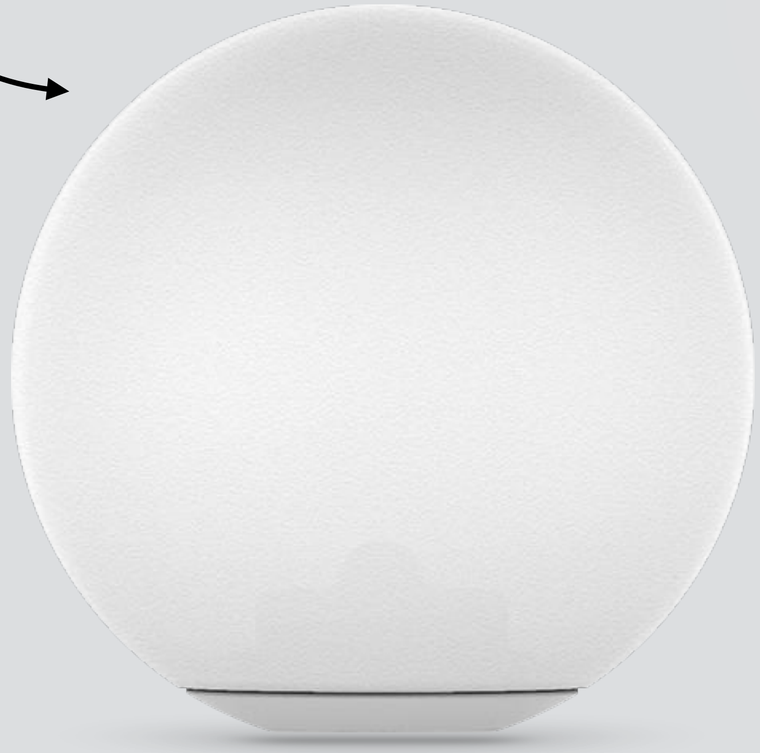
Bluetooth Smart

Bluetooth LE

BLE

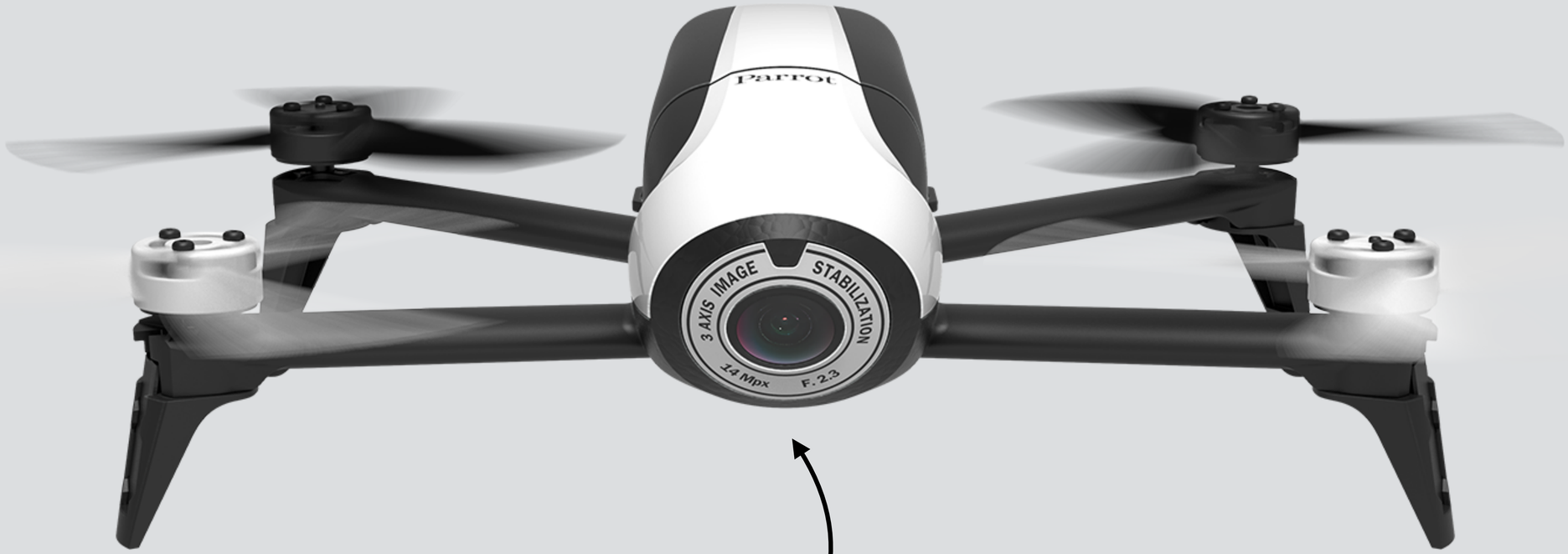
Bluetooth 4

playbulb sphere



playbulb

spherio bb-8



parrot mini drone


activity tracker

the boring theoretical stuff

central

peripheral

central

generic attribute profile

gatt, because gap was already taken

~~central~~

client

~~peripheral~~

server

device information

light

multiple services per device

device information

battery

flight control

device information

battery

steering control

- device information
- battery
- heart rate

dev inf on

b y

heart rate

device information

battery

heart rate

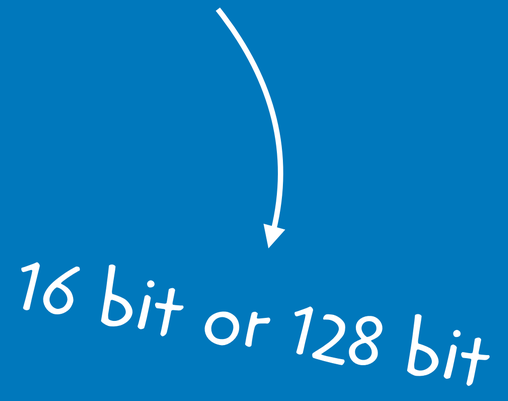
device information

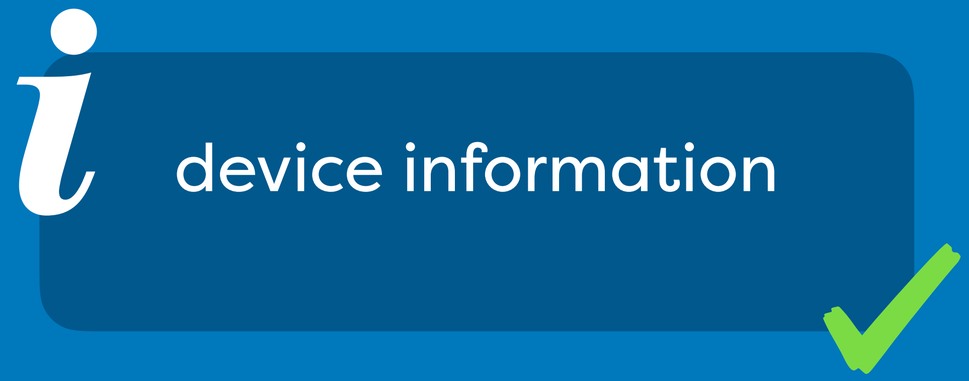
manufacturer
model number
serial number
hardware revision
firmware revision
software revision
...

multiple characteristics per service

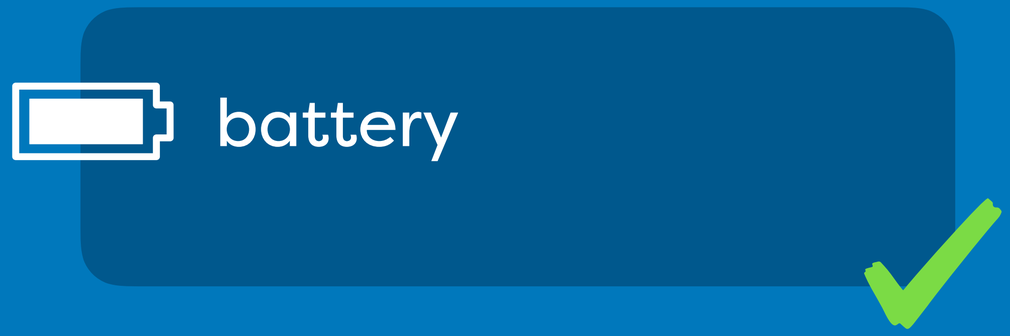
server	array of objects
service	object
characteristic	property
value	value

services and characteristics are identified by uuid's





16 bit	0x180A
128 bit	0000180A-0000-1000-8000-00805F9B34FB



16 bit `0x180F`

128 bit `0000180F-0000-1000-8000-00805F9B34FB`

light

steering control

flight c

still, everybody does this

16 bit `not recommended`

128 bit `any UUID outside of the range`

`xxxxxxxx-0000-1000-8000-00805F9B34FB`

device information

manufacturer
model number
serial number
hardware revision
firmware revision
software revision
...

bad for readability,
good for saving bandwidth

each characteristic supports one or more of these

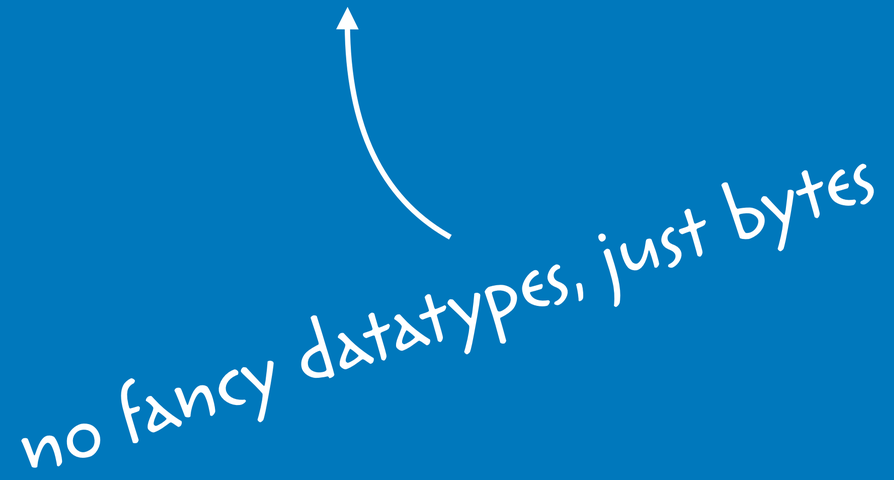
read

write

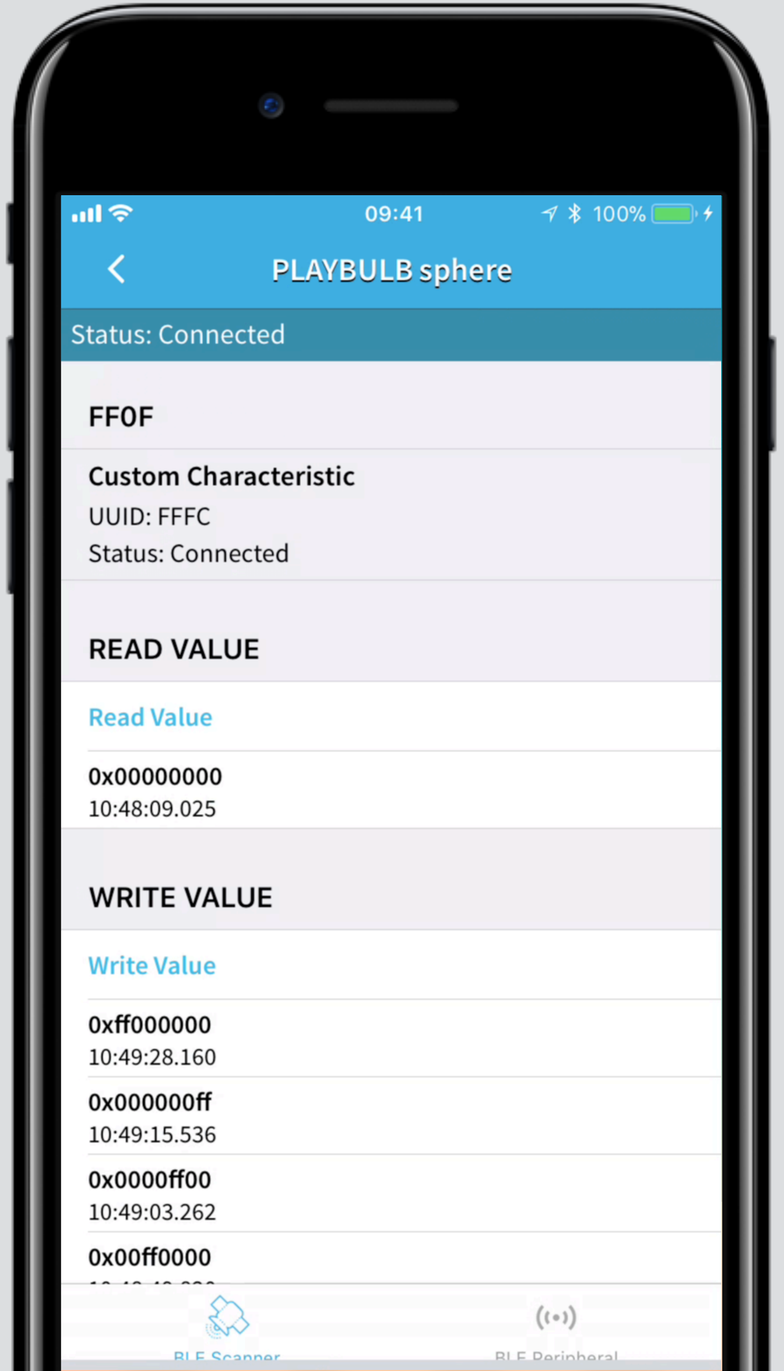
write without response

notify

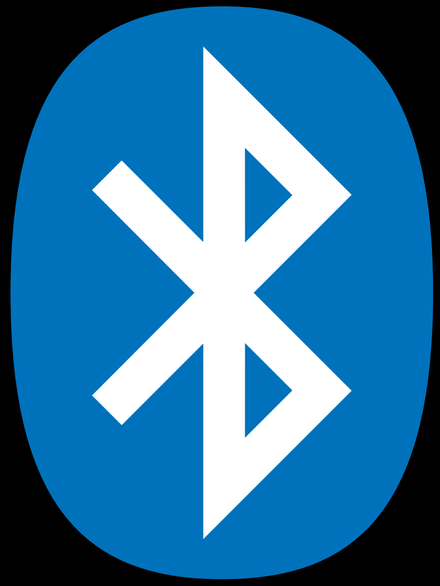
every value is an array of bytes



pfew...

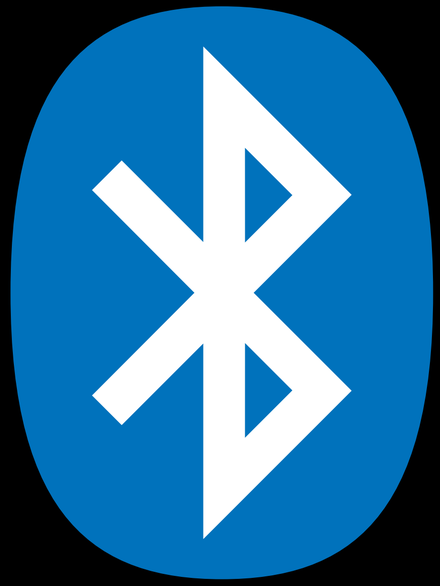

09:41
100%
PLAYBULB sphere
Status: Connected
FF0F
Custom Characteristic
UUID: FFFC
Status: Connected
READ VALUE
Read Value
0x00000000
10:48:09.025
WRITE VALUE
Write Value
0xff000000
10:49:28.160
0x000000ff
10:49:15.536
0x0000ff00
10:49:03.262
0x00ff0000

boring facts about ~~fun with~~



bluetooth

fun with



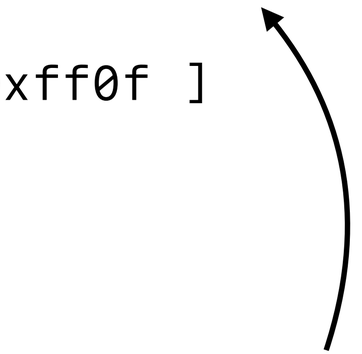
bluetooth

web bluetooth api

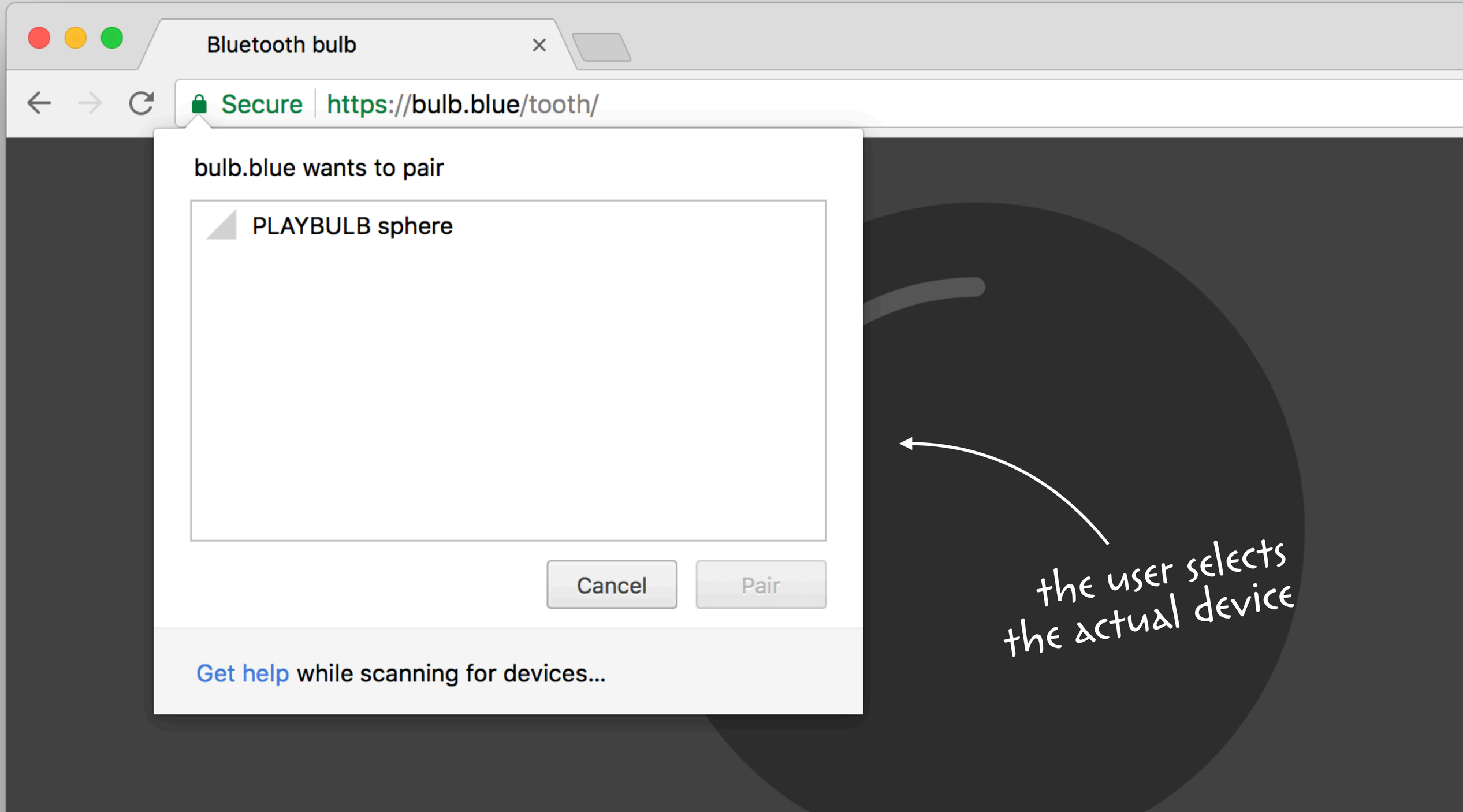
connecting to a device

1

```
navigator.bluetooth.requestDevice({
    filters: [
        { namePrefix: 'PLAYBULB' }
    ],
    optionalServices: [ 0xff0f ]
})
```



we tell the browser what kind of device we want

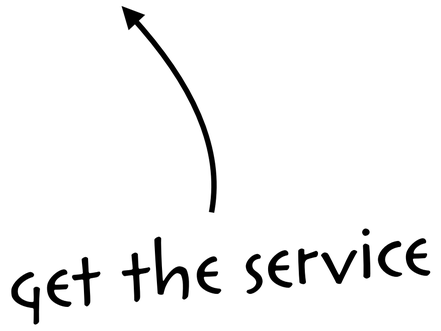

Bluetooth bulb
Secure
https://bulb.blue/tooth/
bulb.blue wants to pair
PLAYBULB sphere
Cancel
Pair
Get help while scanning for devices...
the user selects
the actual device

2

```
navigator.bluetooth.requestDevice({
    filters: [
        { namePrefix: 'PLAYBULB' }
    ],
    optionalServices: [ 0xff0f ]
})

.then(device => device.gatt.connect())
```

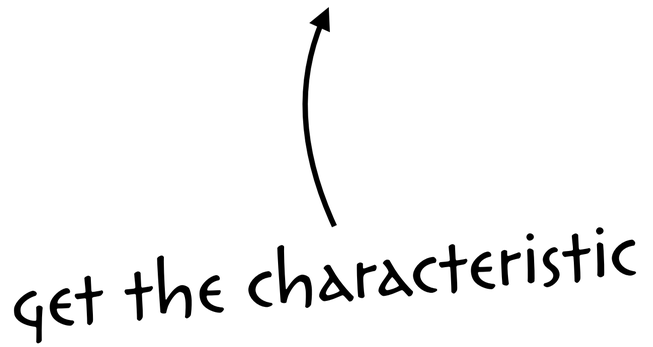
3

```
navigator.bluetooth.requestDevice({
    filters: [
        { namePrefix: 'PLAYBULB' }
    ],
    optionalServices: [ 0xff0f ]
})

.then(device => device.gatt.connect())
.then(server => server.getPrimaryService(0xff0f))
```



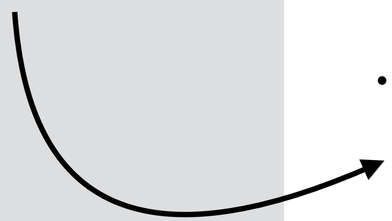
4

```
navigator.bluetooth.requestDevice({
    filters: [
        { namePrefix: 'PLAYBULB' }
    ],
    optionalServices: [ 0xff0f ]
})

.then(device => device.gatt.connect())
.then(server => server.getPrimaryService(0xff0f))
.then(service => service.getCharacteristic(0xfffc))
```



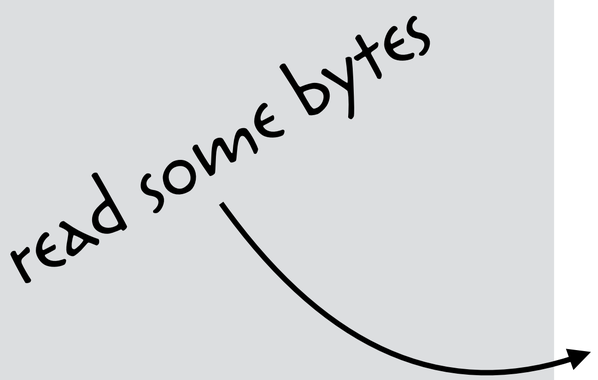
writing data

write some bytes



```
navigator.bluetooth.requestDevice({ ... })
.then(device => device.gatt.connect())
.then(server => server.getPrimaryService(0xff0f))
.then(service => service.getCharacteristic(0xfffc))

.then(c => {
    return c.writeValue(
        new Uint8Array([ 0x00, r, g, b  ])
    );
})
```

reading data




```
navigator.bluetooth.requestDevice({ ... })
.then(device => device.gatt.connect())
.then(server => server.getPrimaryService(0xff0f))
.then(service => service.getCharacteristic(0xfffc))

.then(c => c.readValue())
.then(value => {
    let r = value.getUint8(1);
    let g = value.getUint8(2);
    let b = value.getUint8(3);
})
```

get notified of changes

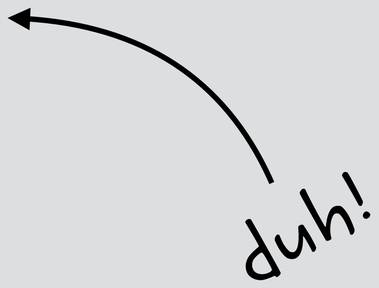
add event listener

```
navigator.bluetooth.requestDevice({ ... })
.then(device => device.gatt.connect())
.then(server => server.getPrimaryService(0xff0f))
.then(service => service.getCharacteristic(0xfffc))

.then(c => {
    c.addEventListener('characteristicvaluechanged', e => {
        let r = e.target.value.getUint8(1);
        let g = e.target.value.getUint8(2);
        let b = e.target.value.getUint8(3);
    });

    c.startNotifications();
})
```

don't forget to start listening

things you need to know:

- javascript
- the webbluetooth api
- promises
- typed arrays



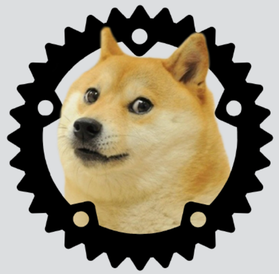
browser support

Chrome

Opera

Samsung

(behind flag)



Servo

(soon)

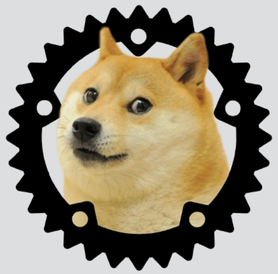
browser support

kinda works

Chrome

Opera

Samsung
(behind flag)



Servo
(soon)

WebBLE
for iOS

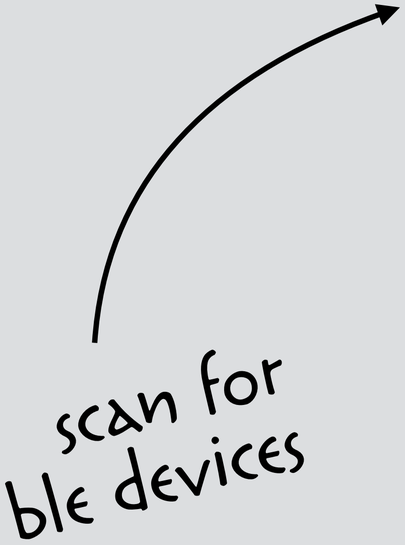
and...

```
npm install node-web-bluetooth
```

and... the puck.js

(linux) command-line tools

Oh, come on!

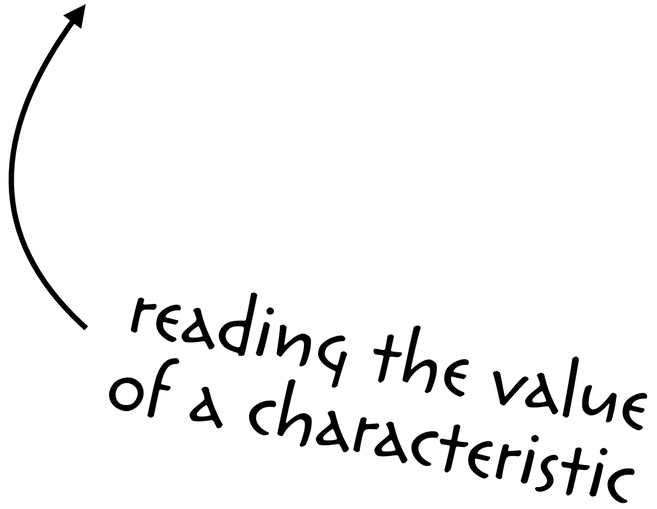



```
hcitool lescan

LE Scan ...
82:4C:4B:17:AC:E6 PLAYBULB sphere
11:75:58:1B:52:85 TimeBox-mini-light
D9:97:A2:35:42:2C BB-422C
D5:72:4A:3F:C2:1F Puck.js c21f
```

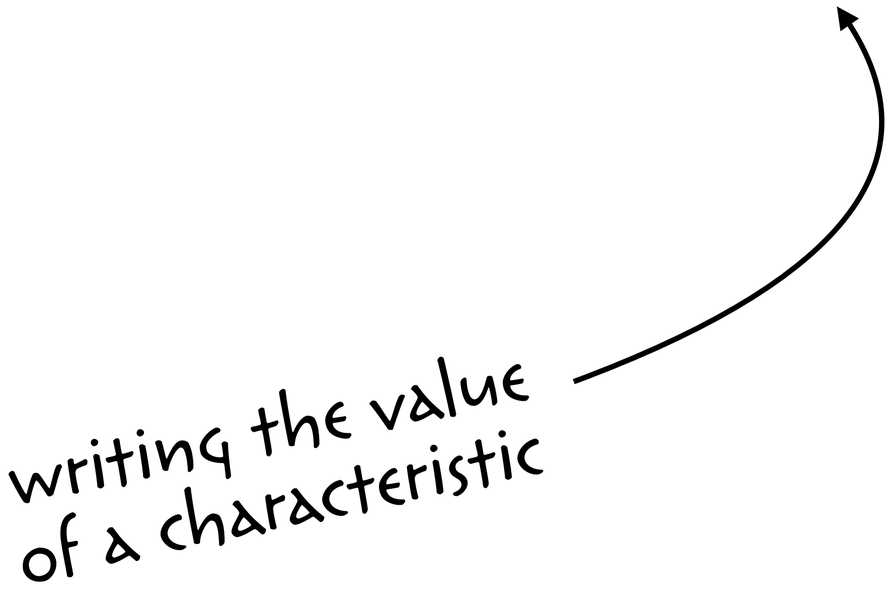
get a list of all characteristics

```
gatttool --device=82:4C:4B:17:AC:E6 --characteristics

handle = 0x0002, char properties = 0x20,
  char value handle = 0x0003,
  uuid = 00002a05-0000-1000-8000-00805f9b34fb
handle = 0x0028, char properties = 0x06,
  char value handle = 0x0029,
  uuid = 0000fffc-0000-1000-8000-00805f9b34fb
handle = 0x004a, char properties = 0x02,
  char value handle = 0x004b,
  uuid = 00002a50-0000-1000-8000-00805f9b34fb
```

```
gatttool --device=82:4C:4B:17:AC:E6
  --char-read --handle=0x0029

Characteristic value/descriptor: 00 00 00 ff
```



```
gatttool --device=82:4C:4B:17:AC:E6
  --char-write --handle=0x0029 --value=0000ff00
```



custom characteristics *wtf!*

writing a value:

```
function(r, g, b) {
    return new Uint8Array([ 0x00, r, g, b  ]);
}
```

reading a value:

```
function(buffer) {
    return {
        r: buffer.getUint8(1),
        g: buffer.getUint8(2),
        b: buffer.getUint8(3)
    }
}
```

writing to and reading
from the same characteristic

writing a value:

```
function(r, g, b) {
    return new Uint8Array([
        0x01, g, 0x01, 0x00, 0x01,
        b, 0x01, r, 0x01, 0x00
    ]);
}
```

reading the current color is not possible

writing a value:

```
function(r, g, b) {
    var buffer = new Uint8Array([
        0xaa, 0x0a, 0xfc, 0x3a, 0x86, 0x01, 0x0d,
        0x06, 0x01, r, g, b, 0x00, 0x00,
        (Math.random() * 1000) & 0xff, 0x55, 0x0d
    ]);

    for (var i = 1; i < buffer.length - 2; i++) {
        buffer[15] += buffer[i];
    }

    return buffer;
}
```

reading the current color is not possible

reading a value:

service 0xffe0
characteristic 0xffe4

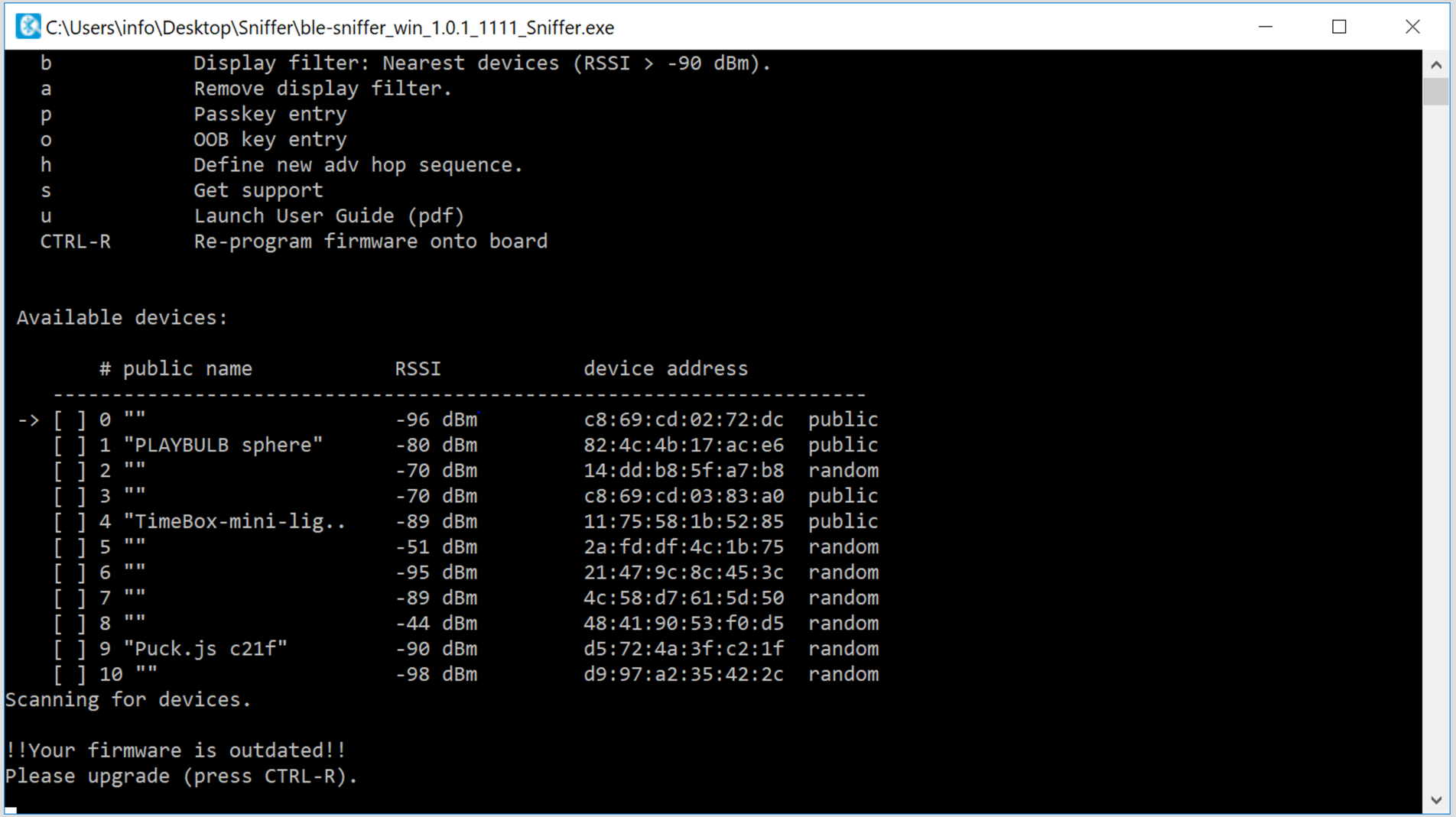
1 add event listener

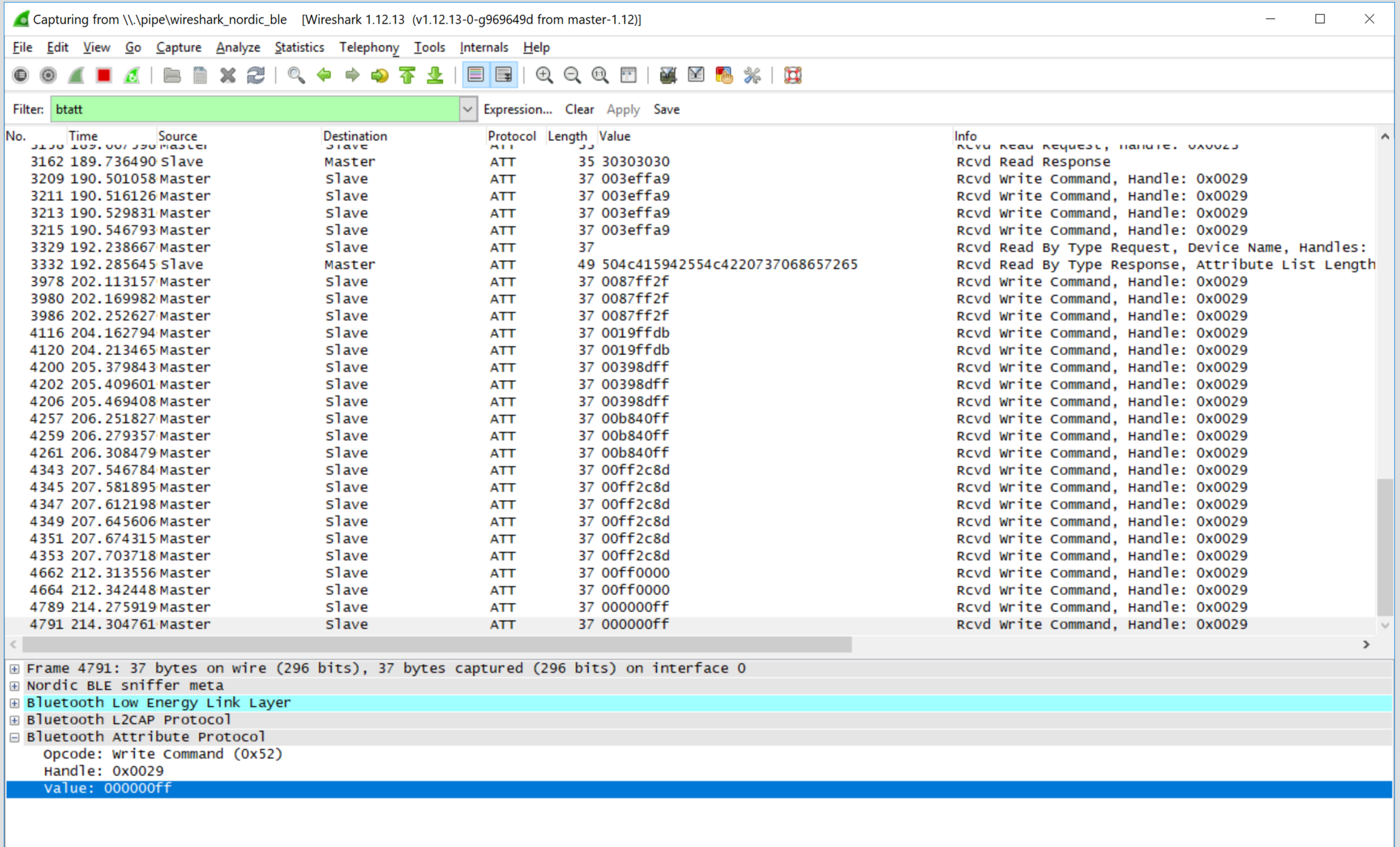
2 write a specific value

service 0xffe5
characteristic 0xffe9

3 get the event with the color

adafruit bluetooth sniffer


C:\Users\info\Desktop\Sniffer\ble-sniffer_win_1.0.1_1111_Sniffer.exe
b Display filter: Nearest devices (RSSI > -90 dBm).
a Remove display filter.
p Passkey entry
o OOB key entry
h Define new adv hop sequence.
s Get support
u Launch User Guide (pdf)
CTRL-R Re-program firmware onto board
Available devices:
public name RSSI device address
-> [ ] 0 "" -96 dBm c8:69:cd:02:72:dc public
[ ] 1 "PLAYBULB sphere" -80 dBm 82:4c:4b:17:ac:e6 public
[ ] 2 "" -70 dBm 14:dd:b8:5f:a7:b8 random
[ ] 3 "" -70 dBm c8:69:cd:03:83:a0 public
[ ] 4 "TimeBox-mini-lig.. -89 dBm 11:75:58:1b:52:85 public
[ ] 5 "" -51 dBm 2a:fd:df:4c:1b:75 random
[ ] 6 "" -95 dBm 21:47:9c:8c:45:3c random
[ ] 7 "" -89 dBm 4c:58:d7:61:5d:50 random
[ ] 8 "" -44 dBm 48:41:90:53:f0:d5 random
[ ] 9 "Puck.js c21f" -90 dBm d5:72:4a:3f:c2:1f random
[ ] 10 "" -98 dBm d9:97:a2:35:42:2c random
Scanning for devices.
!!Your firmware is outdated!!
Please upgrade (press CTRL-R).


Capturing from \\.\pipe\wireshark_nordic_ble [Wireshark 1.12.13 (v1.12.13-0-g969649d from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: btatt
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Value Info
3162 189.736490 Slave Master ATT 35 30303030 Rcvd Read Response
3209 190.501058 Master Slave ATT 37 003effa9 Rcvd Write Command, Handle: 0x0029
3211 190.516126 Master Slave ATT 37 003effa9 Rcvd Write Command, Handle: 0x0029
3213 190.529831 Master Slave ATT 37 003effa9 Rcvd Write Command, Handle: 0x0029
3215 190.546793 Master Slave ATT 37 003effa9 Rcvd Write Command, Handle: 0x0029
3329 192.238667 Master Slave ATT 37 Rcvd Read By Type Request, Device Name, Handles:
3332 192.285645 Slave Master ATT 49 504c415942554c4220737068657265 Rcvd Read By Type Response, Attribute List Length
3978 202.113157 Master Slave ATT 37 0087ff2f Rcvd Write Command, Handle: 0x0029
3980 202.169982 Master Slave ATT 37 0087ff2f Rcvd Write Command, Handle: 0x0029
3986 202.252627 Master Slave ATT 37 0087ff2f Rcvd Write Command, Handle: 0x0029
4116 204.162794 Master Slave ATT 37 0019ffdb Rcvd Write Command, Handle: 0x0029
4120 204.213465 Master Slave ATT 37 0019ffdb Rcvd Write Command, Handle: 0x0029
4200 205.379843 Master Slave ATT 37 00398dff Rcvd Write Command, Handle: 0x0029
4202 205.409601 Master Slave ATT 37 00398dff Rcvd Write Command, Handle: 0x0029
4206 205.469408 Master Slave ATT 37 00398dff Rcvd Write Command, Handle: 0x0029
4257 206.251827 Master Slave ATT 37 00b840ff Rcvd Write Command, Handle: 0x0029
4259 206.279357 Master Slave ATT 37 00b840ff Rcvd Write Command, Handle: 0x0029
4261 206.308479 Master Slave ATT 37 00b840ff Rcvd Write Command, Handle: 0x0029
4343 207.546784 Master Slave ATT 37 00ff2c8d Rcvd Write Command, Handle: 0x0029
4345 207.581895 Master Slave ATT 37 00ff2c8d Rcvd Write Command, Handle: 0x0029
4347 207.612198 Master Slave ATT 37 00ff2c8d Rcvd Write Command, Handle: 0x0029
4349 207.645606 Master Slave ATT 37 00ff2c8d Rcvd Write Command, Handle: 0x0029
4351 207.674315 Master Slave ATT 37 00ff2c8d Rcvd Write Command, Handle: 0x0029
4353 207.703718 Master Slave ATT 37 00ff2c8d Rcvd Write Command, Handle: 0x0029
4662 212.313556 Master Slave ATT 37 00ff0000 Rcvd Write Command, Handle: 0x0029
4664 212.342448 Master Slave ATT 37 00ff0000 Rcvd Write Command, Handle: 0x0029
4789 214.275919 Master Slave ATT 37 000000ff Rcvd Write Command, Handle: 0x0029
4791 214.304761 Master Slave ATT 37 000000ff Rcvd Write Command, Handle: 0x0029
Frame 4791: 37 bytes on wire (296 bits), 37 bytes captured (296 bits) on interface 0
Nordic BLE sniffer meta
Bluetooth Low Energy Link Layer
Bluetooth L2CAP Protocol
Bluetooth Attribute Protocol
Opcode: Write Command (0x52)
Handle: 0x0029
Value: 000000ff

finally the fun part

demo

warning

experimental technology

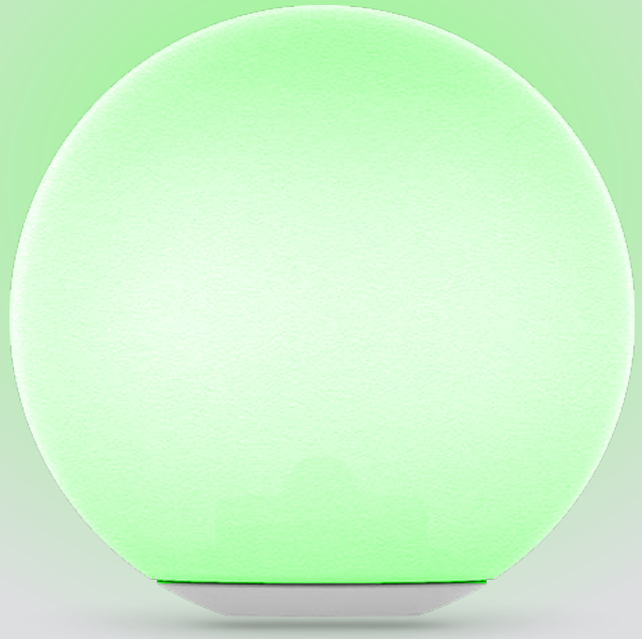
setting low expectations

warning

wifi interference

lowering them even further

change the colour of a lightbulb



https://bluetooth.rocks/lightbulb

https://github.com/NielsLeenheer/BluetoothBulb

control a lego racer
using a gamepad

use css animations to
define a path

https://bluetooth.rocks/racer

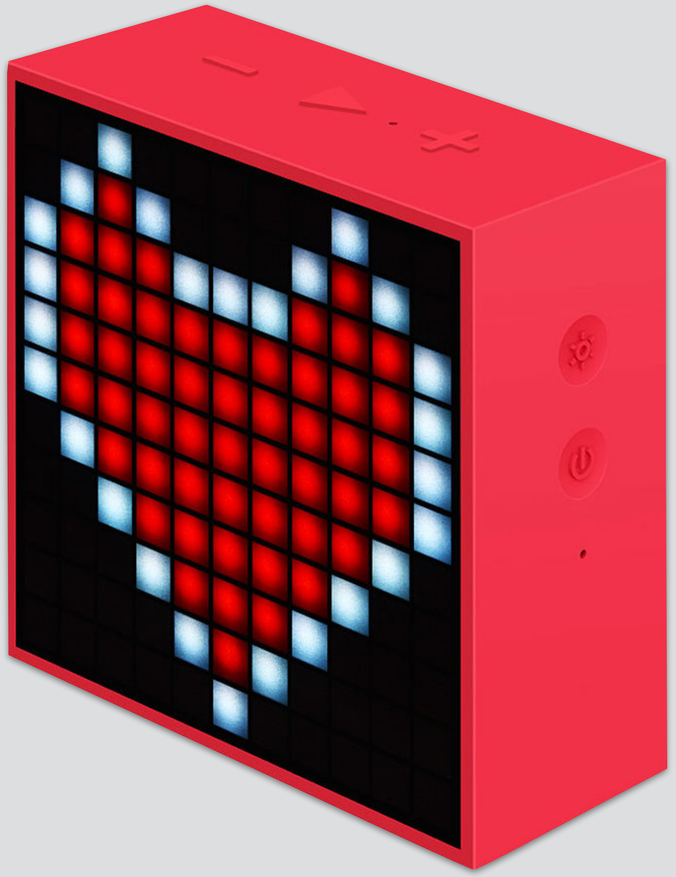
https://github.com/NielsLeenheer/BluetoothRacer

control a drone
from your browser

https://bluetooth.rocks/drone

https://github.com/poshaughnessy/web-bluetooth-parrot-drone

pixel matrix display



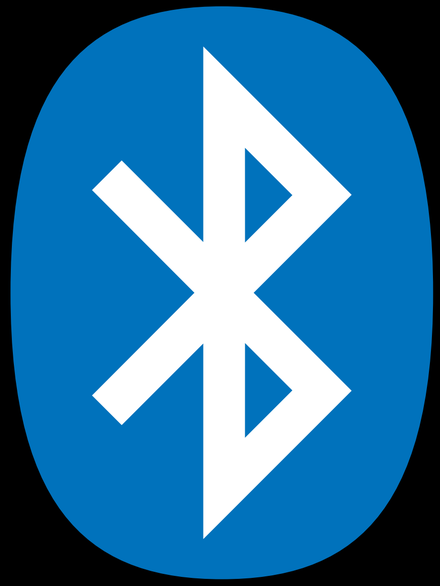
https://bluetooth.rocks/pixel

find out your
current heartbeat

https://bluetooth.rocks/pulse

https://github.com/NielsLeenheer/BluetoothPulse

fun with



bluetooth!

questions?