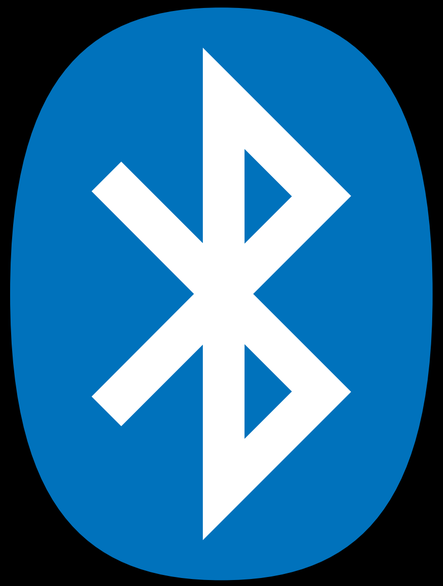
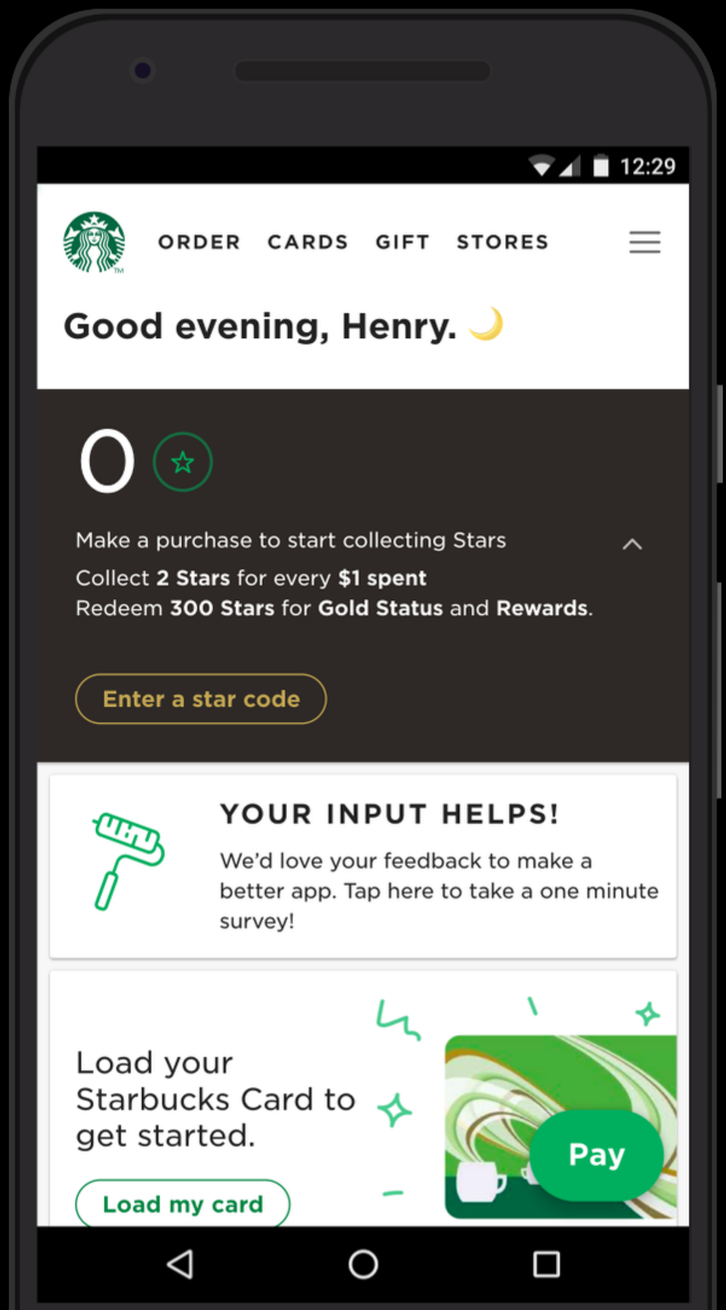
fun with bluetooth



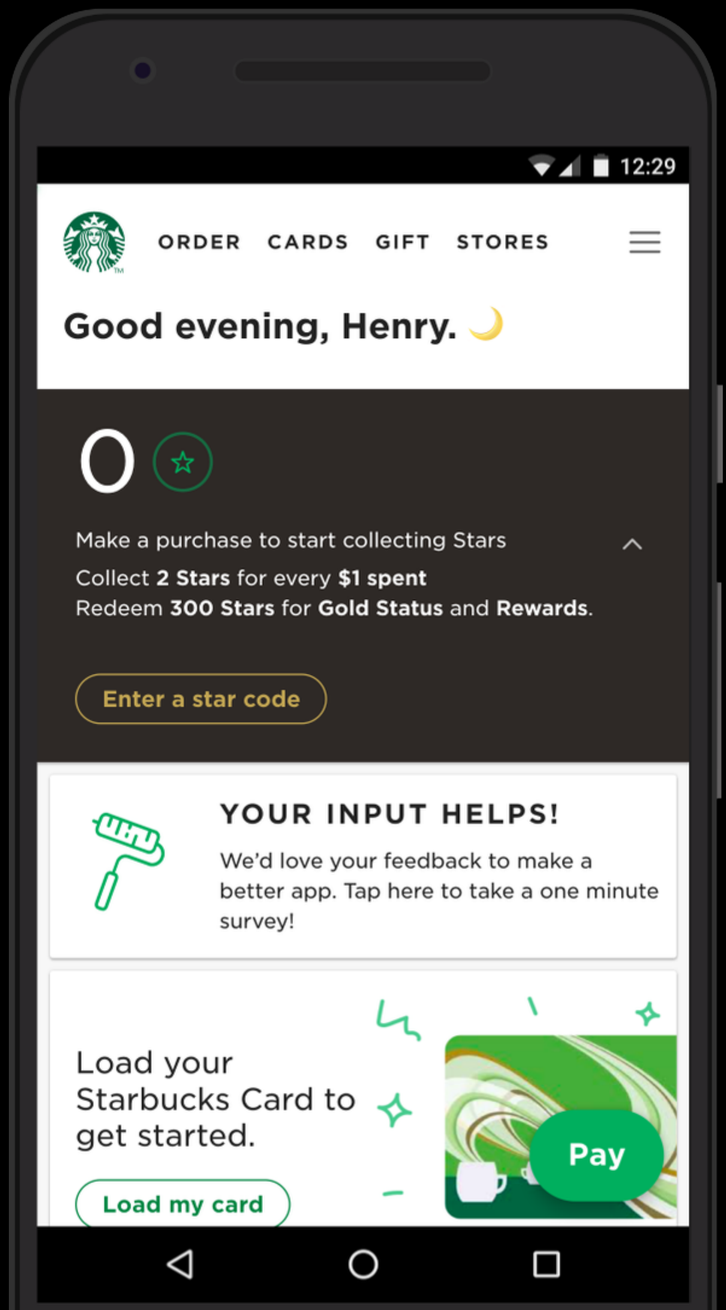
why?

progressive web apps

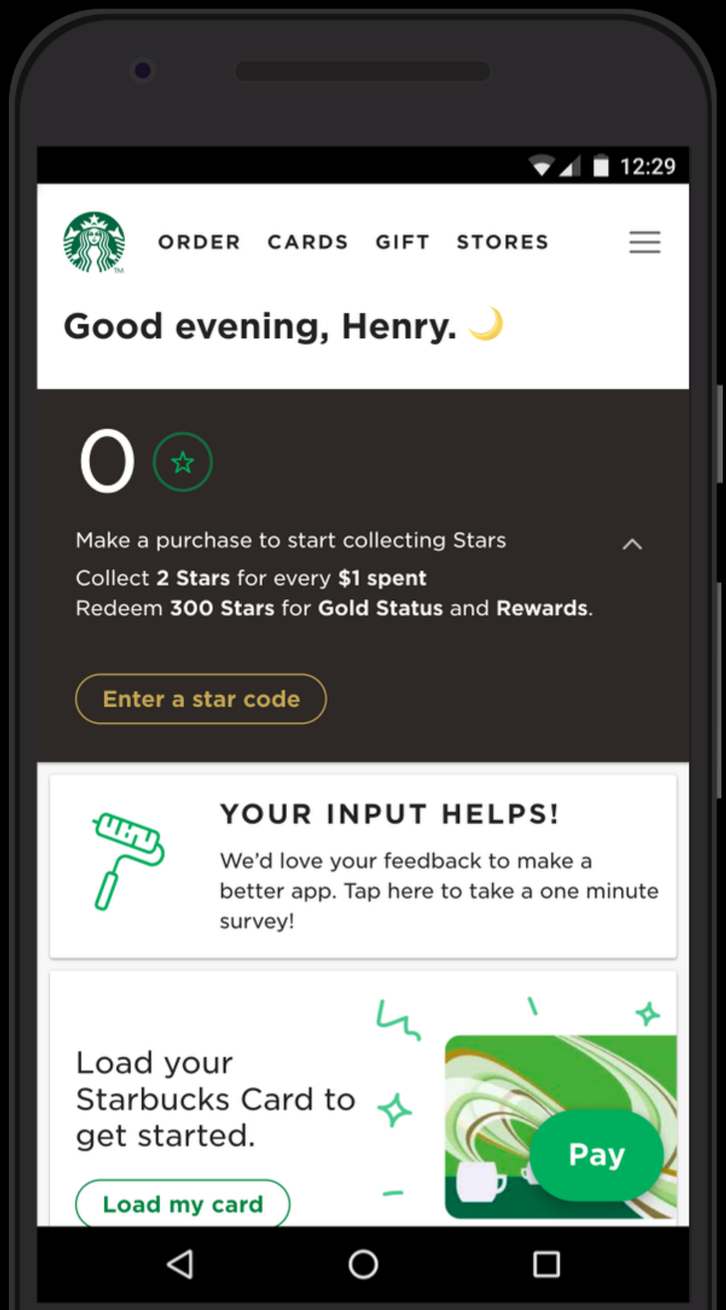
pwa's are great!

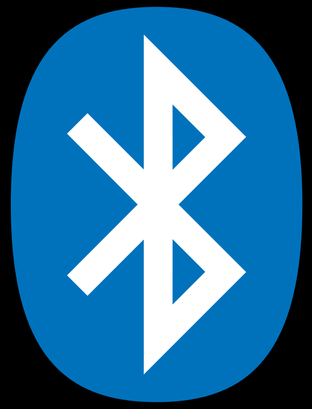


but...

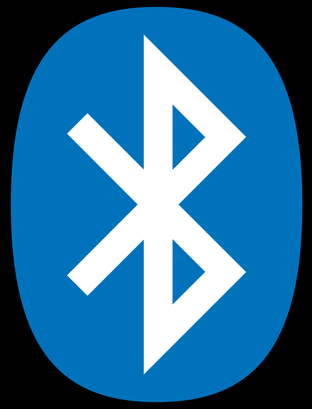

12:29
ORDER CARDS GIFT STORES
Good evening, Henry.
0
Make a purchase to start collecting Stars
Collect 2 Stars for every $1 spent
Redeem 300 Stars for Gold Status and Rewards.
Enter a star code
YOUR INPUT HELPS!
We'd love your feedback to make a better app. Tap here to take a one minute survey!
Load your Starbucks Card to get started.
Load my card
Pay

but...


12:29
ORDER CARDS GIFT STORES
Good evening, Henry.
0
Make a purchase to start collecting Stars
Collect 2 Stars for every $1 spent
Redeem 300 Stars for Gold Status and Rewards.
Enter a star code
YOUR INPUT HELPS!
We'd love your feedback to make a better app. Tap here to take a one minute survey!
Load your Starbucks Card to get started.
Load my card
Pay



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 and 5

bluetooth low energy

also known as

Bluetooth Smart

Bluetooth LE

BLE

Bluetooth 4 and 5

10 million

bluetooth devices
shipping every day

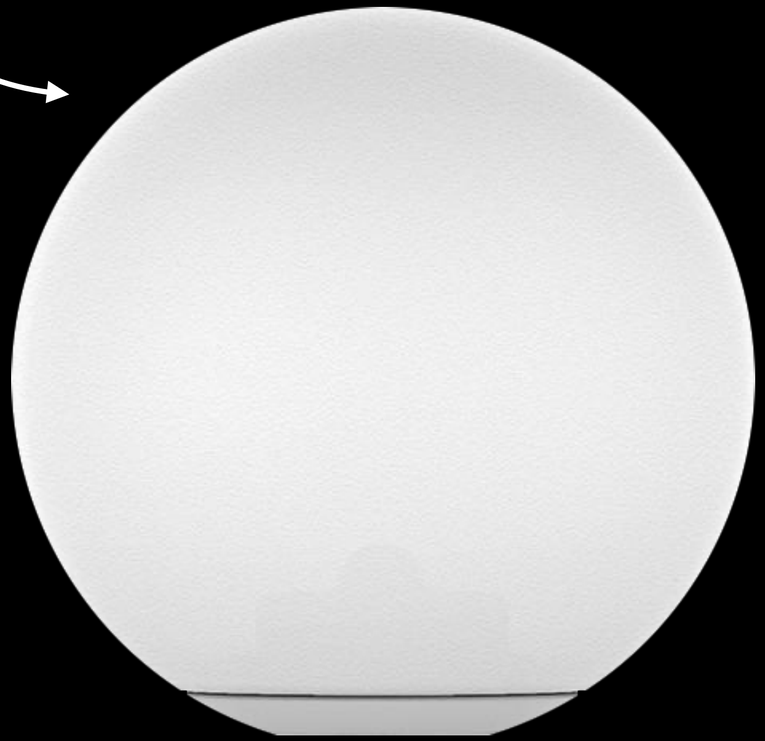

9:41 AM
100%
Messages
Calendar
Tuesday
9
Photos
Camera
Weather
Clock
Maps
Videos
Notes
Reminders
Stocks
Game Center
Newsstand
iTunes Store
App Store
iBooks
Health
Passbook
Settings
Phone
Mail
Safari
Music
mobile phone

computer


glucose monitor
MEM
5.8
mmol/L
308 2015
8:00 AM
GLU
CHOL
MEMORY
somebody's hand

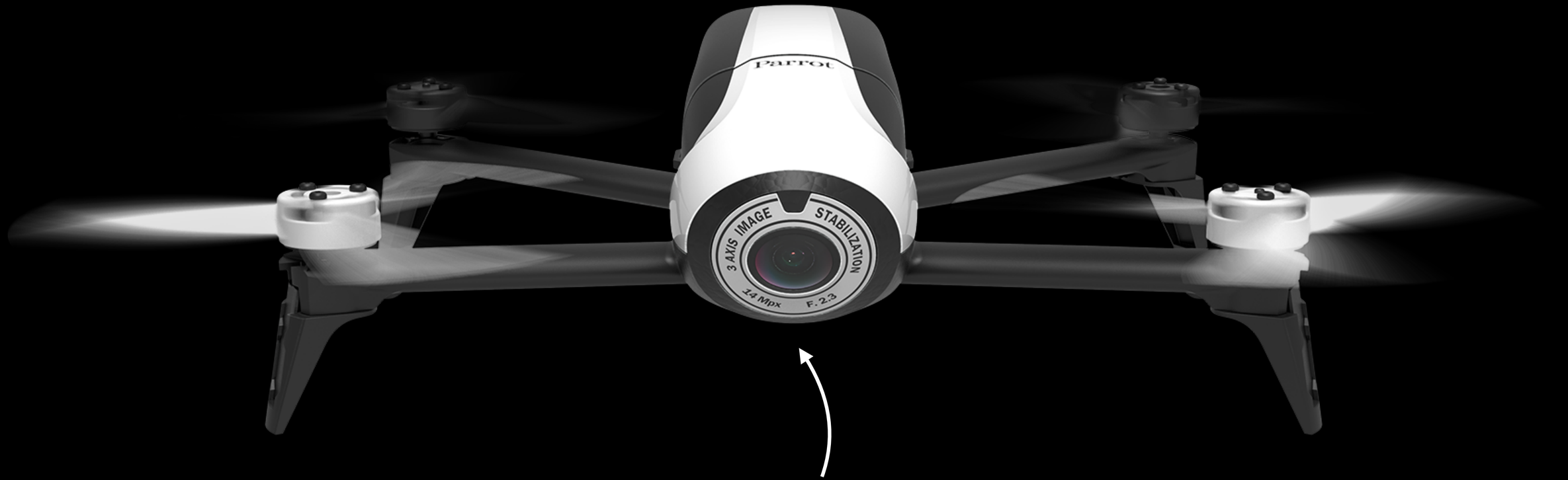

activity tracker

playbulb sphere



playbulb

spherio bb-8



parrot mini drone

fidget spinner

the boring theoretical stuff

central

peripheral

central

generic attribute profile

generic attribute profile ?

generic attribute profile

~~central~~

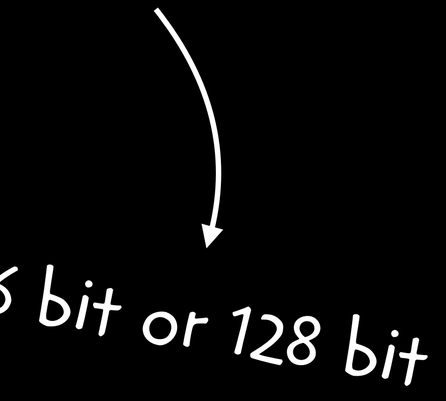
client

~~peripheral~~

server

server	array of objects
service	object
characteristic	property
value	value

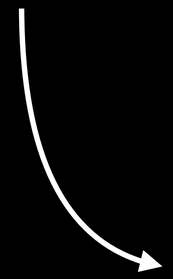
services and characteristics are identified by uuid's



0000180F-0000-1000-8000-00805F9B34FB

180F

each characteristic supports one or more of these



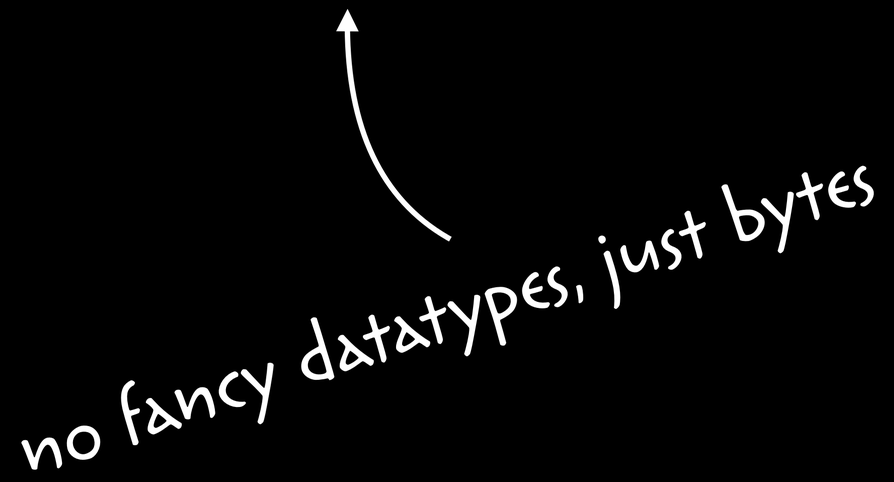
read

write

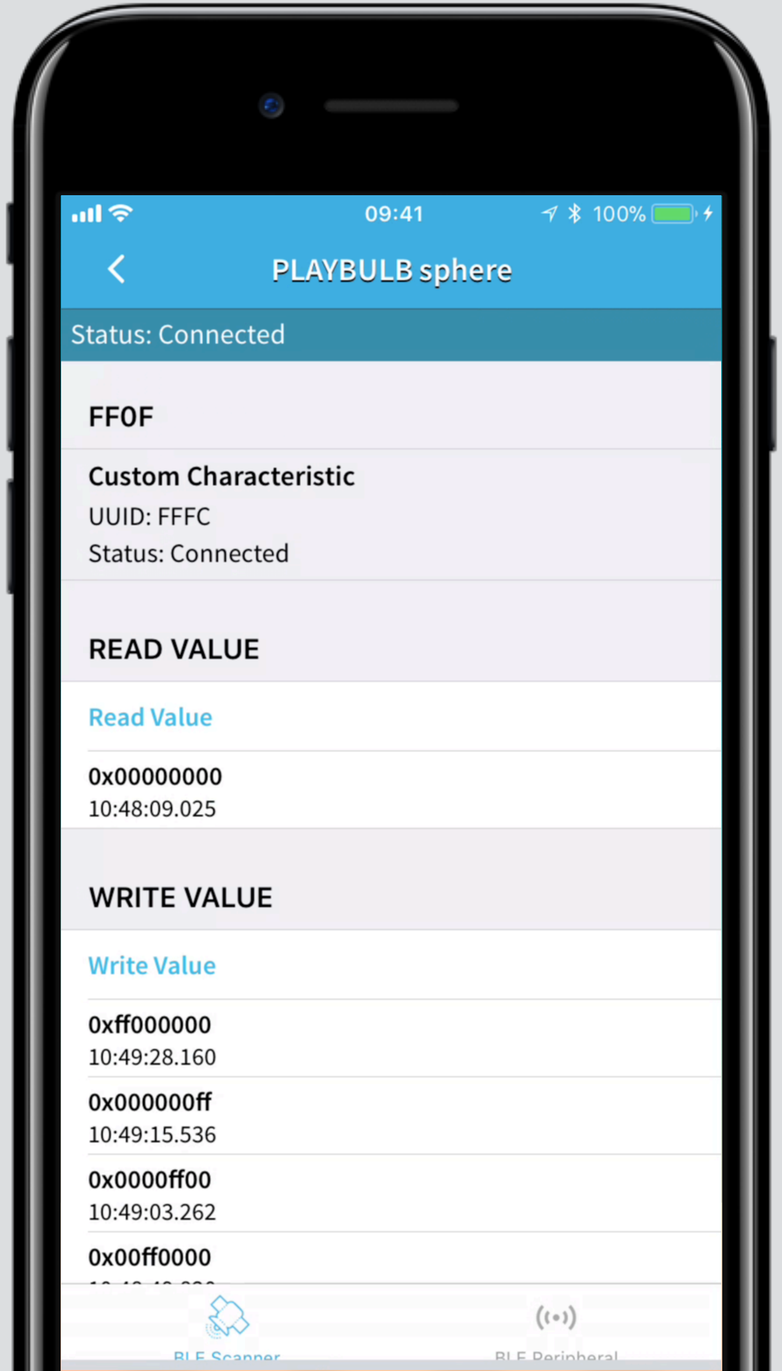
write without response

notify

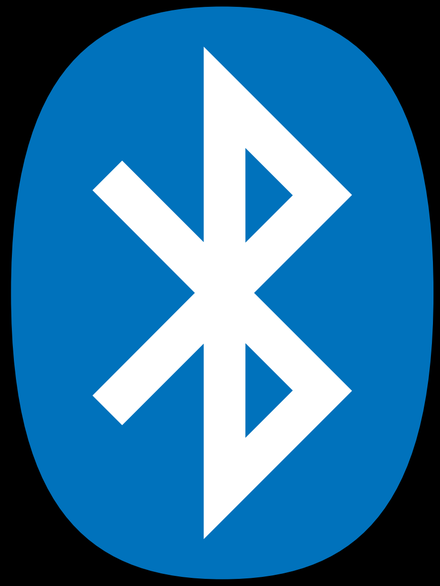
every value is an array of bytes



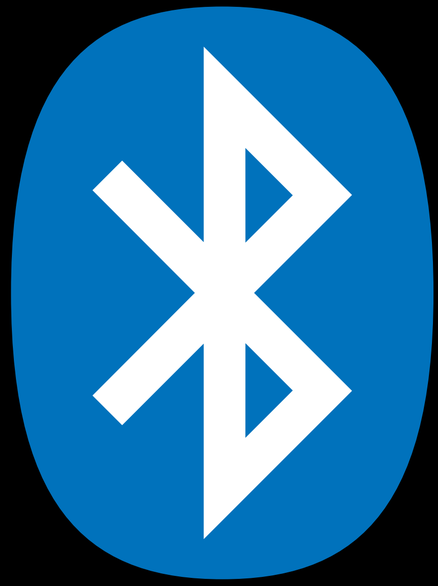
pfew...


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

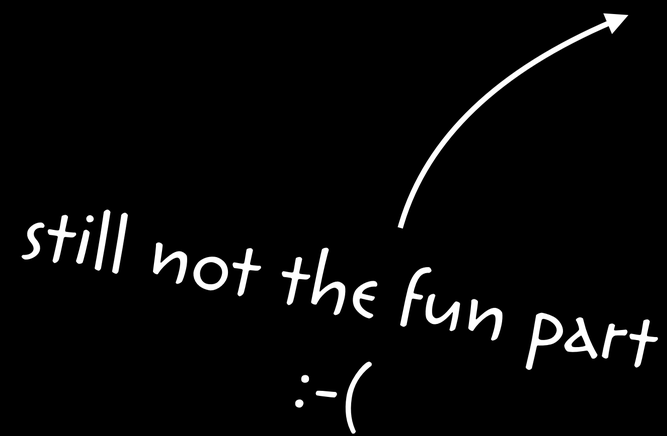


fun with



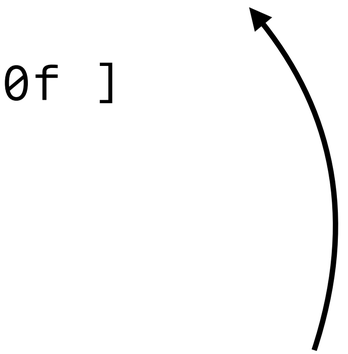
bluetooth

web bluetooth api

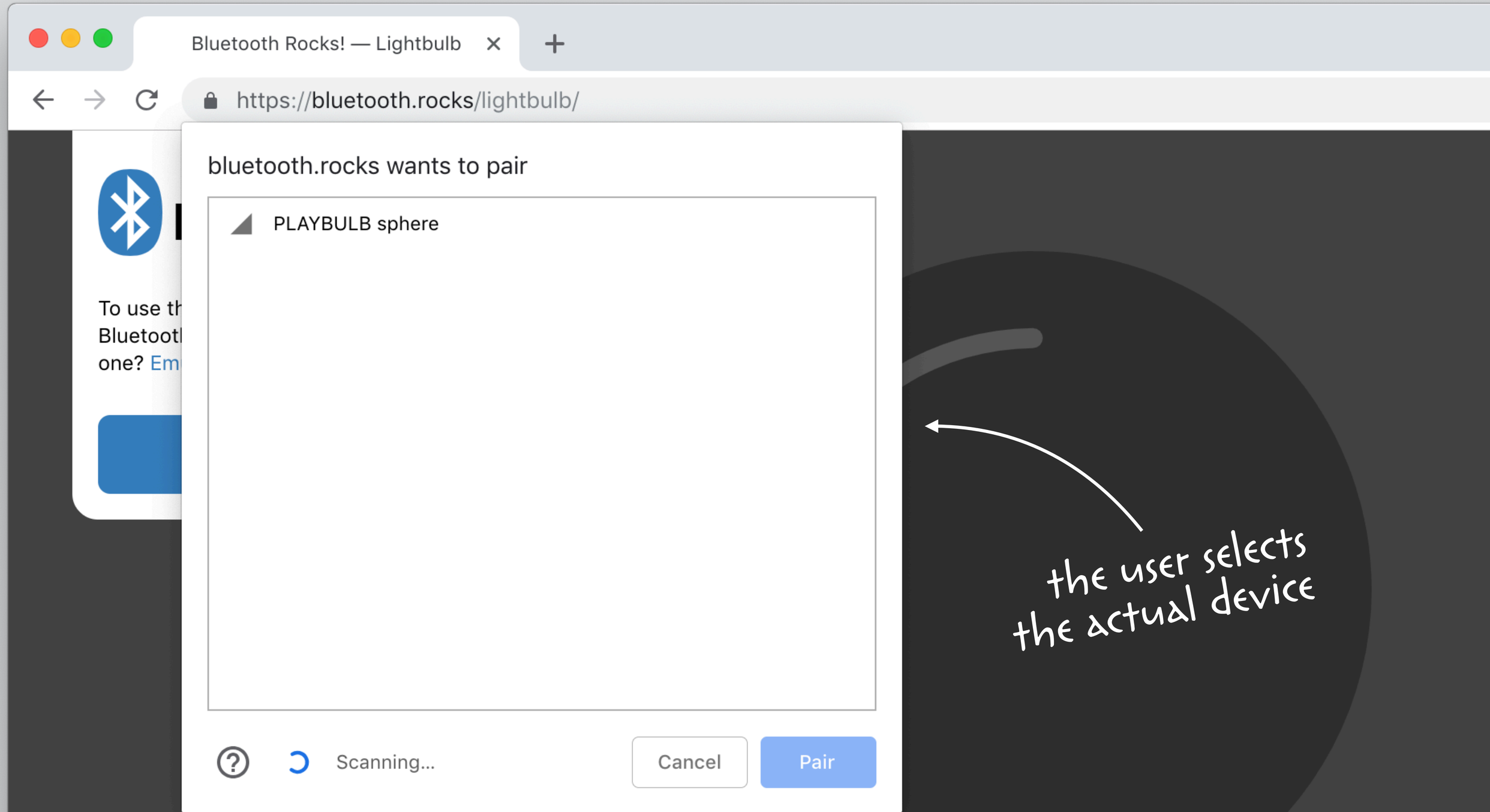


connecting to a device

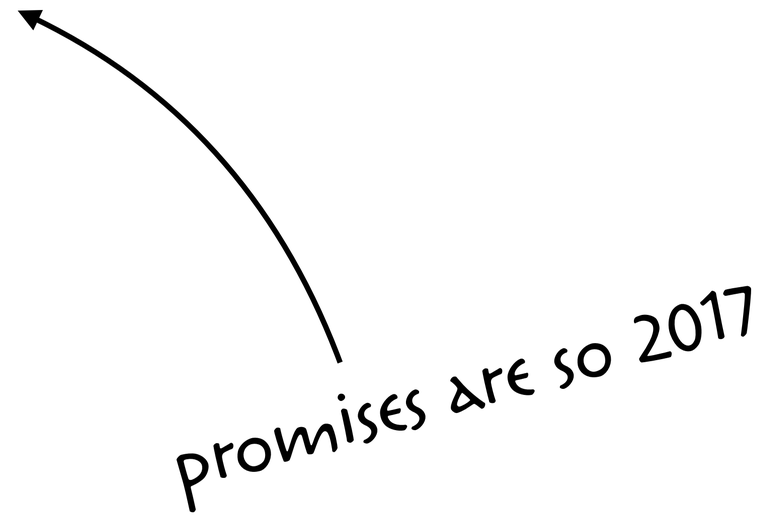
```
navigator.bluetooth.requestDevice({
    filters: [
        { namePrefix: 'PLAYBULB' }
    ],
    optionalServices: [ 0xff0f ]
})
```



we tell the browser what kind of device we want


Bluetooth Rocks! — Lightbulb
https://bluetooth.rocks/lightbulb/
bluetooth.rocks wants to pair
PLAYBULB sphere
Scanning...
Cancel
Pair
the user selects
the actual device

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



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

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

let server = await device.gatt.connect());
let service = await server.getPrimaryService(0xff0f));
let characteristic = await service.getCharacteristic(0xfffc));
```

connect to the server

get the service

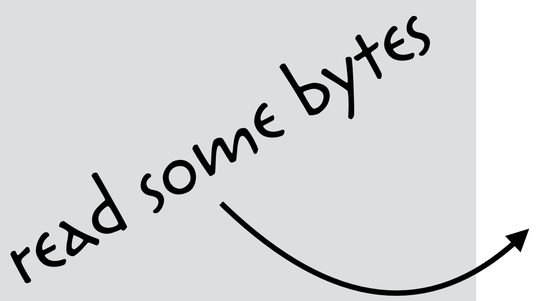
get the characteristic

writing data

write some bytes

```
let device = await navigator.bluetooth.requestDevice({ ... });
let server = await device.gatt.connect());
let service = await server.getPrimaryService(0xff0f));
let characteristic = await service.getCharacteristic(0xfffc));

characteristic.writeValue(
    new Uint8Array([ 0x00, r, g, b  ])
);
```

reading data




```
let device = await navigator.bluetooth.requestDevice({ ... });
let server = await device.gatt.connect());
let service = await server.getPrimaryService(0xff0f));
let characteristic = await service.getCharacteristic(0xfffc));

let value = await characteristic.readValue();

let r = value.getUint8(1);
let g = value.getUint8(2);
let b = value.getUint8(3);
```

get notified of changes

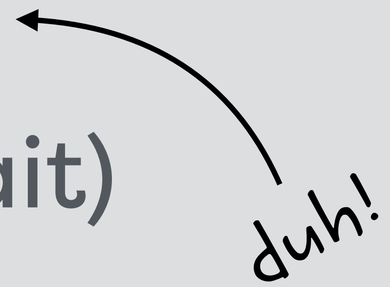
add event listener

```
let device = await navigator.bluetooth.requestDevice({ ... });
let server = await device.gatt.connect());
let service = await server.getPrimaryService(0xff0f));
let characteristic = await service.getCharacteristic(0xfffc));

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

characteristic.startNotifications();
```

don't forget to start listening

things you need to know:

- the webbluetooth api
- promises (or async await)
- typed arrays



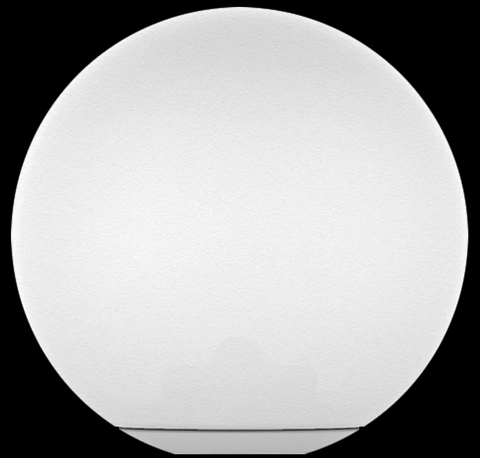
custom characteristics. *wtf!*

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;
}
```

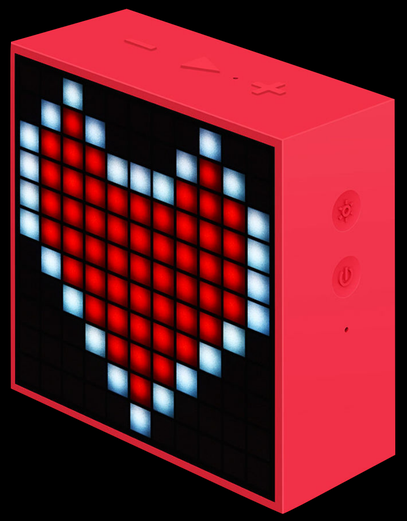
reading the current color is not possible

writing a value:

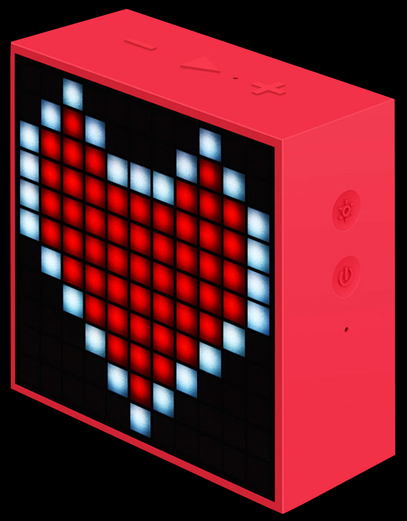
```
function(r, g, b, position) {
    let buffer = new Uint8Array([
        0x07, 0x02, position + 1, r, g, b
    ]);

    return buffer;
}
```

writing a value:

```
function(r, g, b, position) {
    let buffer = new Uint8Array([
        0x58, r, g, b, 0x01, position
    ]);

    ...
```

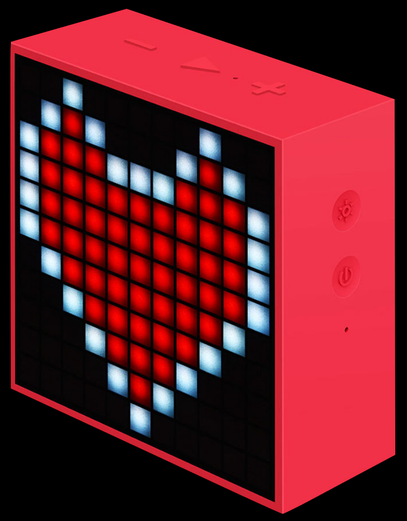


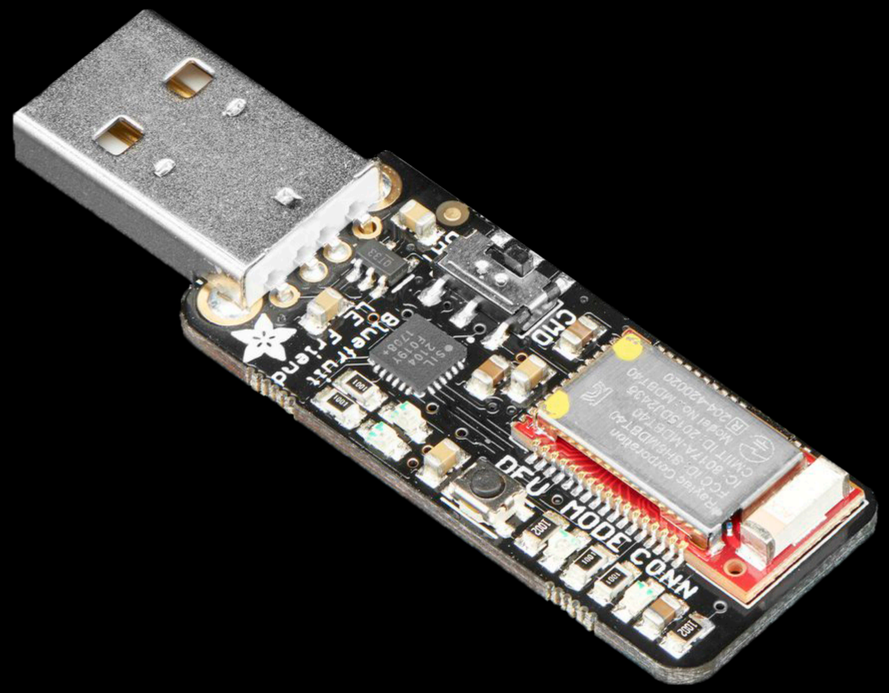
writing a value:



```
function(r, g, b, position) {
    let buffer = new Uint8Array([
        0x58, r, g, b, 0x01, position
    ]);

    let payload = new Uint8Array(buffer.length + 4);
    payload[0] = payload.length - 2;
    payload[1] = payload.length - 2 >>> 8;
    payload.set(buffer, 2);

    let checksum = payload.reduce((a, b) => a + b, 0);
    payload[payload.length - 2] = checksum;
    payload[payload.length - 1] = checksum >>> 8;

    let extra = payload.filter(value => {
```

```
                message[m + 1] = 0x05;
                m += 2;
            }
            else if (payload[i] === 0x03) {
                message[m] = 0x03;
                message[m + 1] = 0x06;
                m += 2;
            }
            else {
                message[m] = payload[i];
                m++;
            }
        }

        message[0] = 0x01;
        message[message.length - 1] = 0x02;

        return message;
    }
```

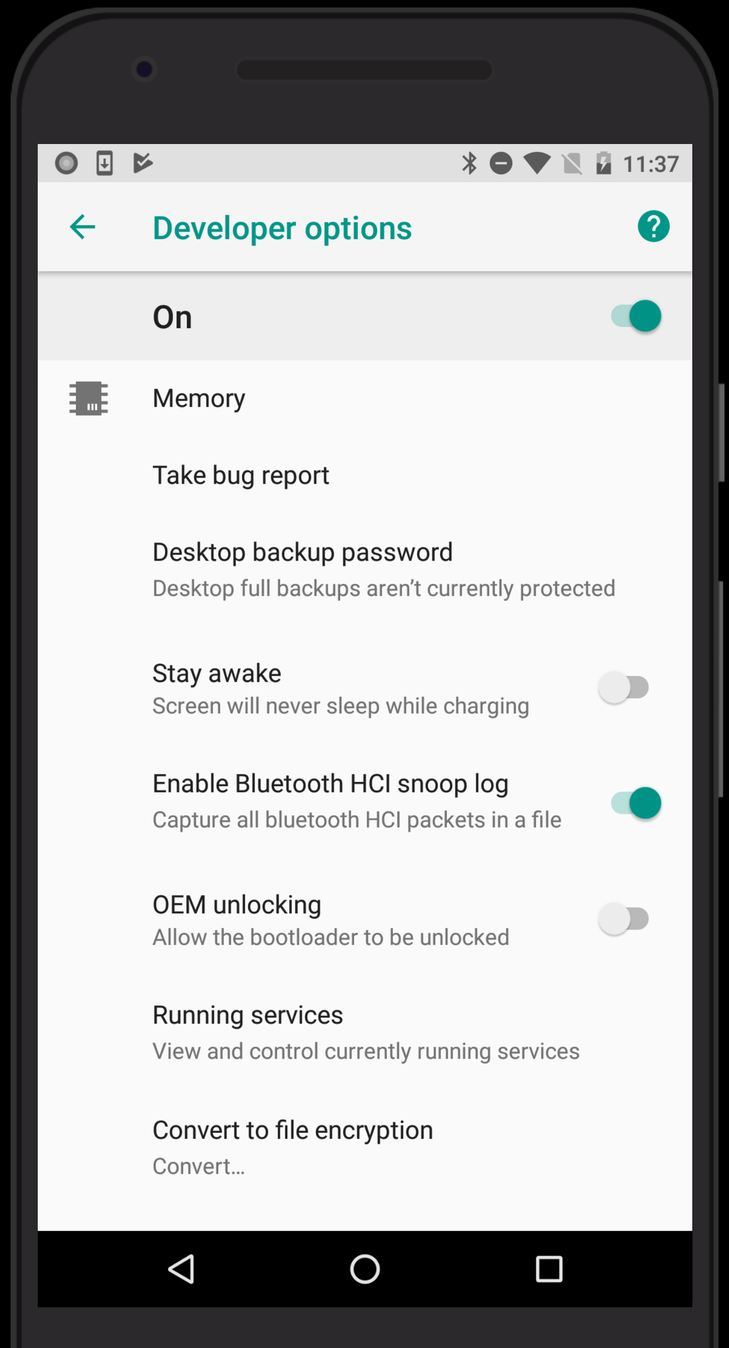




adafruit bluetooth sniffer

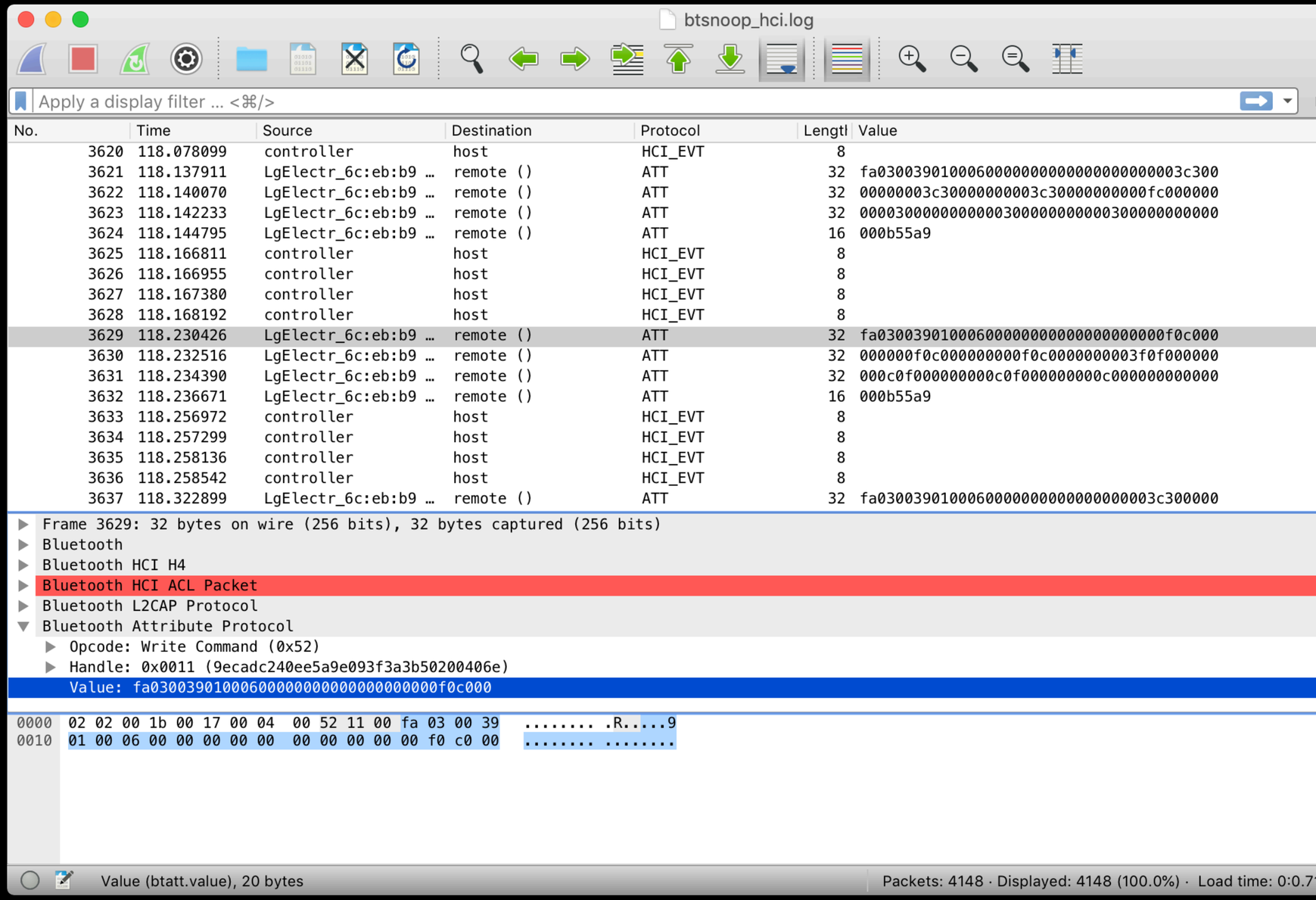
log all bluetooth packets

on your phone



and use adb to transfer the log

use wireshark to look at the data



decompiling the apk

don't tell anyone!

finally the fun part

demo

warning

experimental technology

setting low expectations

warning

wifi interference

lowering them even further

questions?