Prep

Hacking Bluetooth Devices and Controlling Them with Your Browser

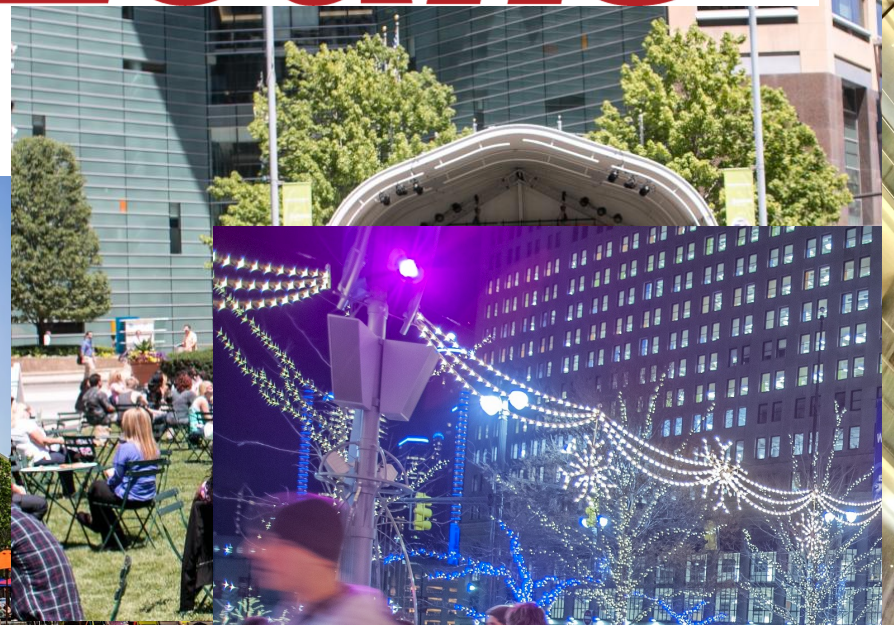
Aydin Akcasu

Sr. Software Engineer

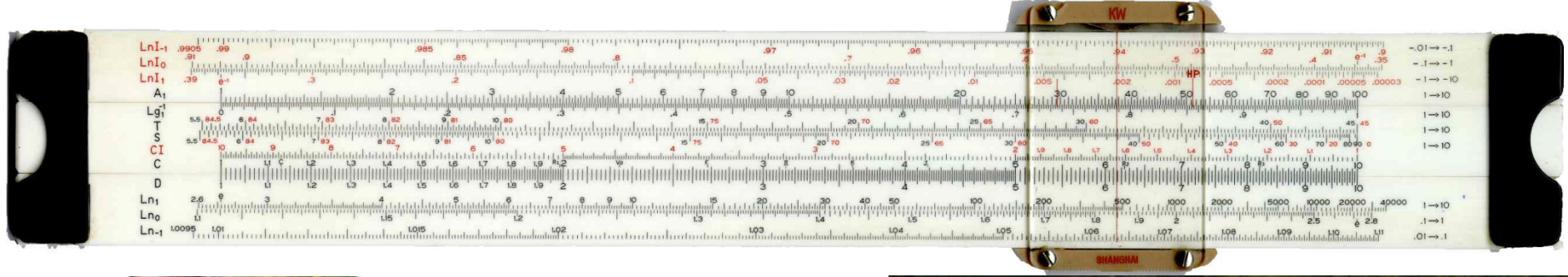
Quicken Loans

Quicken Loans®

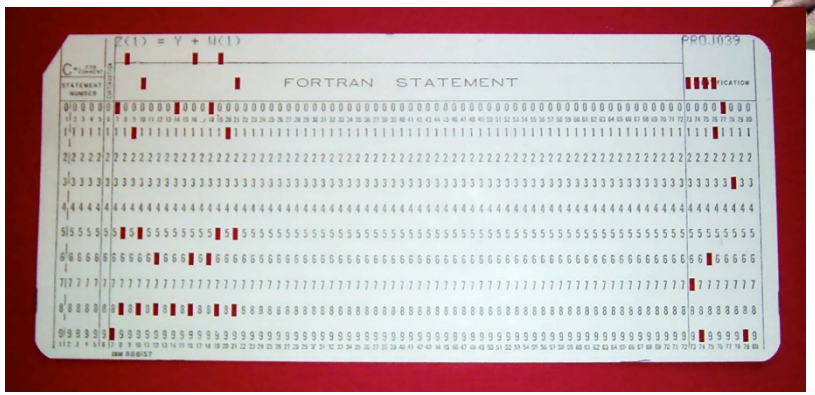
- We are hiring!
- Let me know!



30+ (10+) years

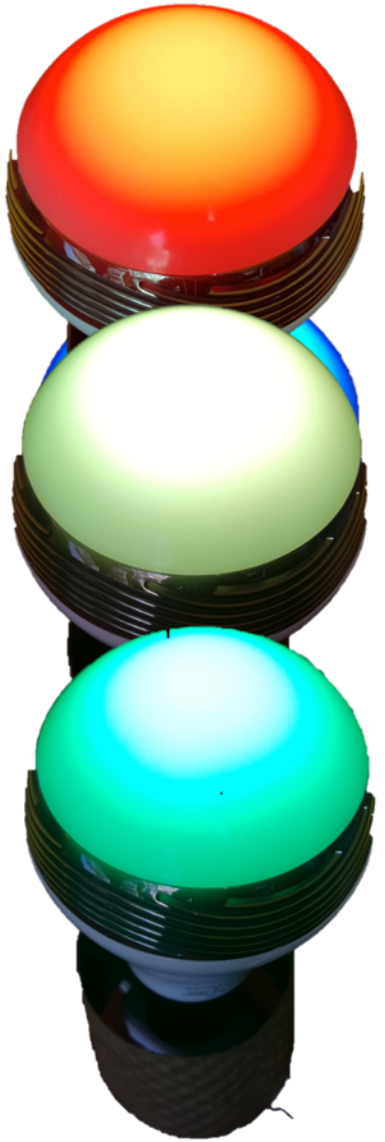


$300, 1973==$1,700



$10 K, 1983==$25K

What you will learn:



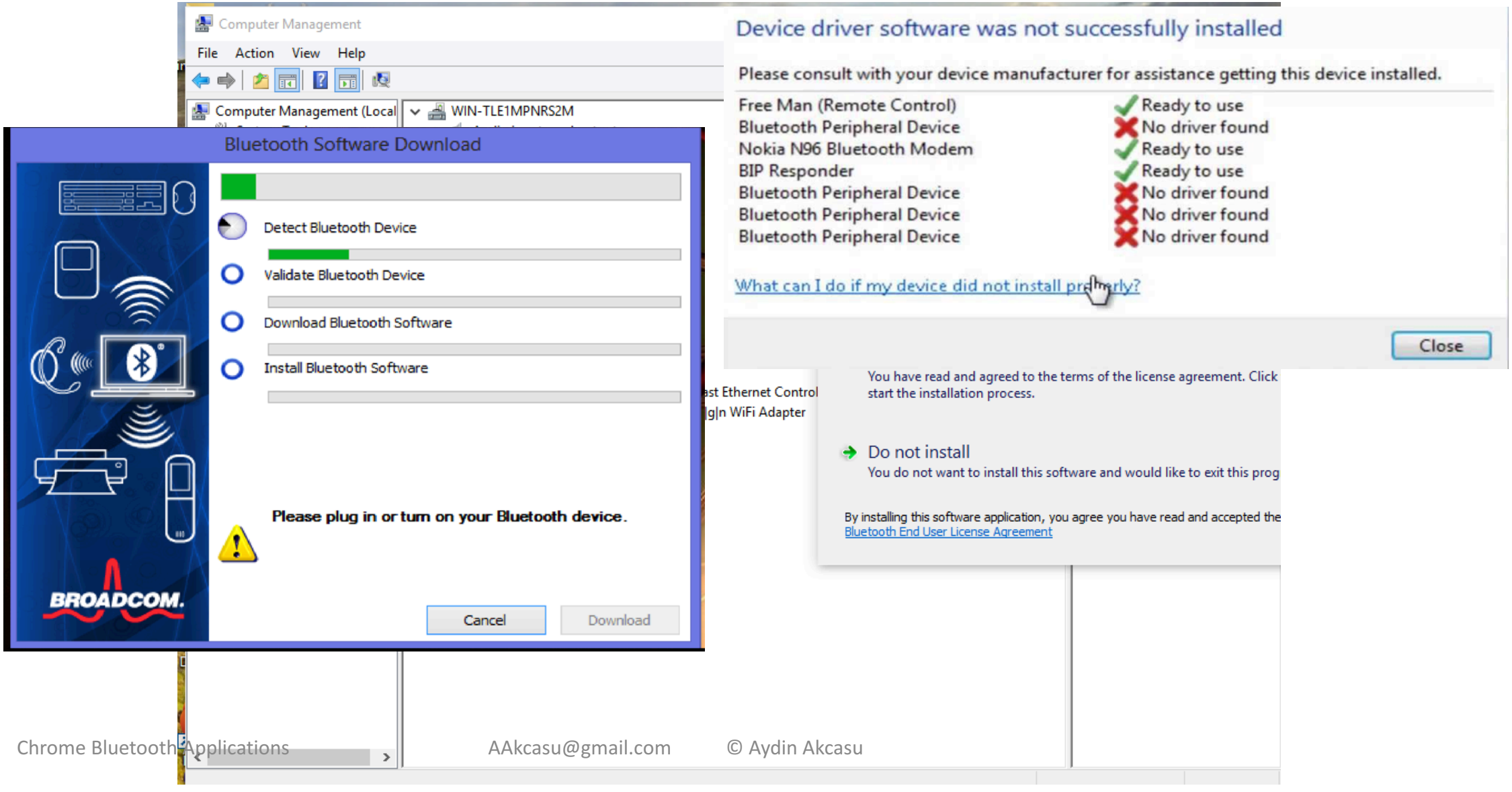
BLUETOOTH IS EVERYWHERE NOW AND CONTINUES TO EXPAND

In and Out of Our Homes

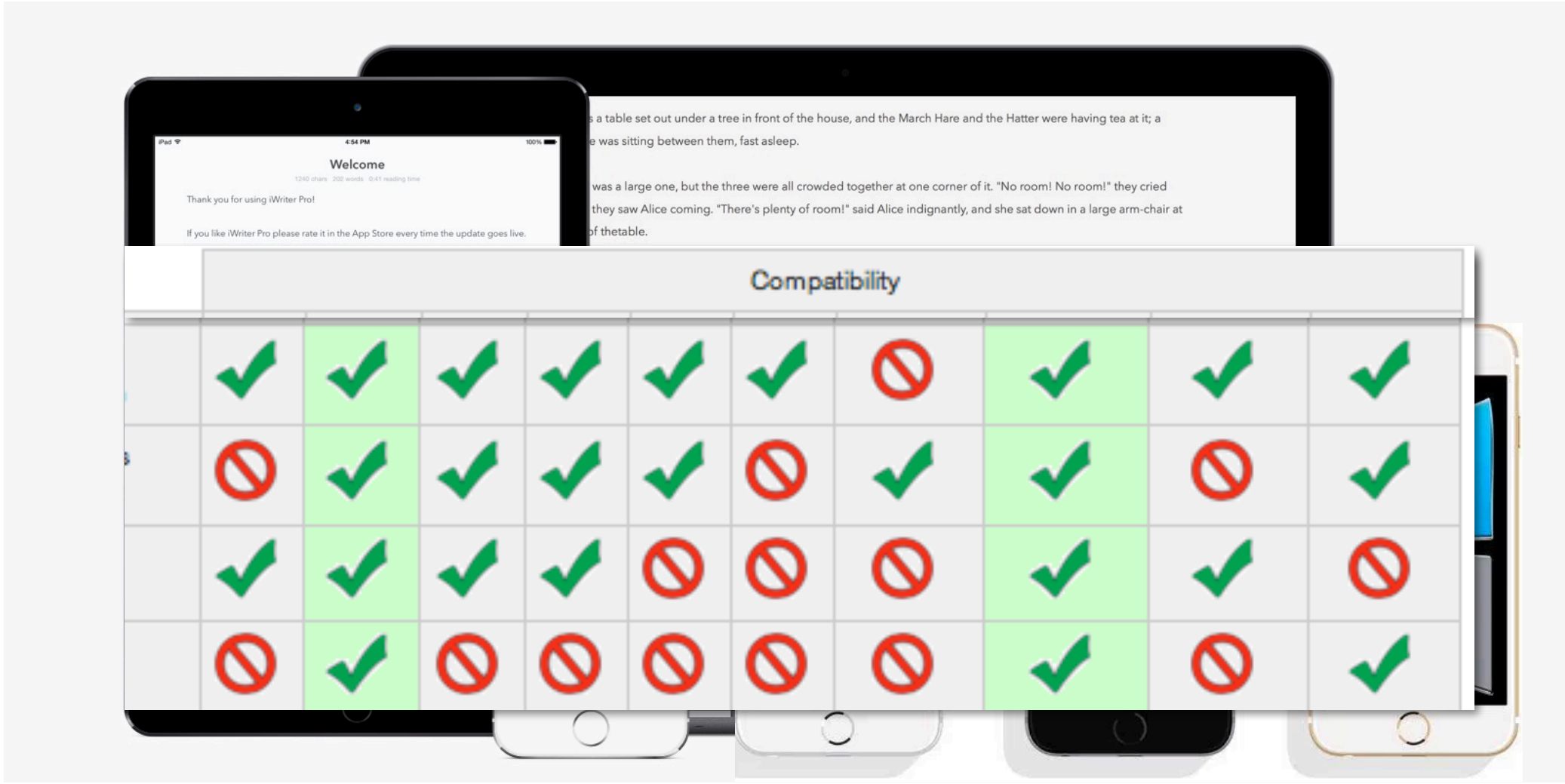
Near or around our Bodies to Measure Health:

ARE THERE ANY PROBLEMS WITH CREATING BLUETOOTH APPS?

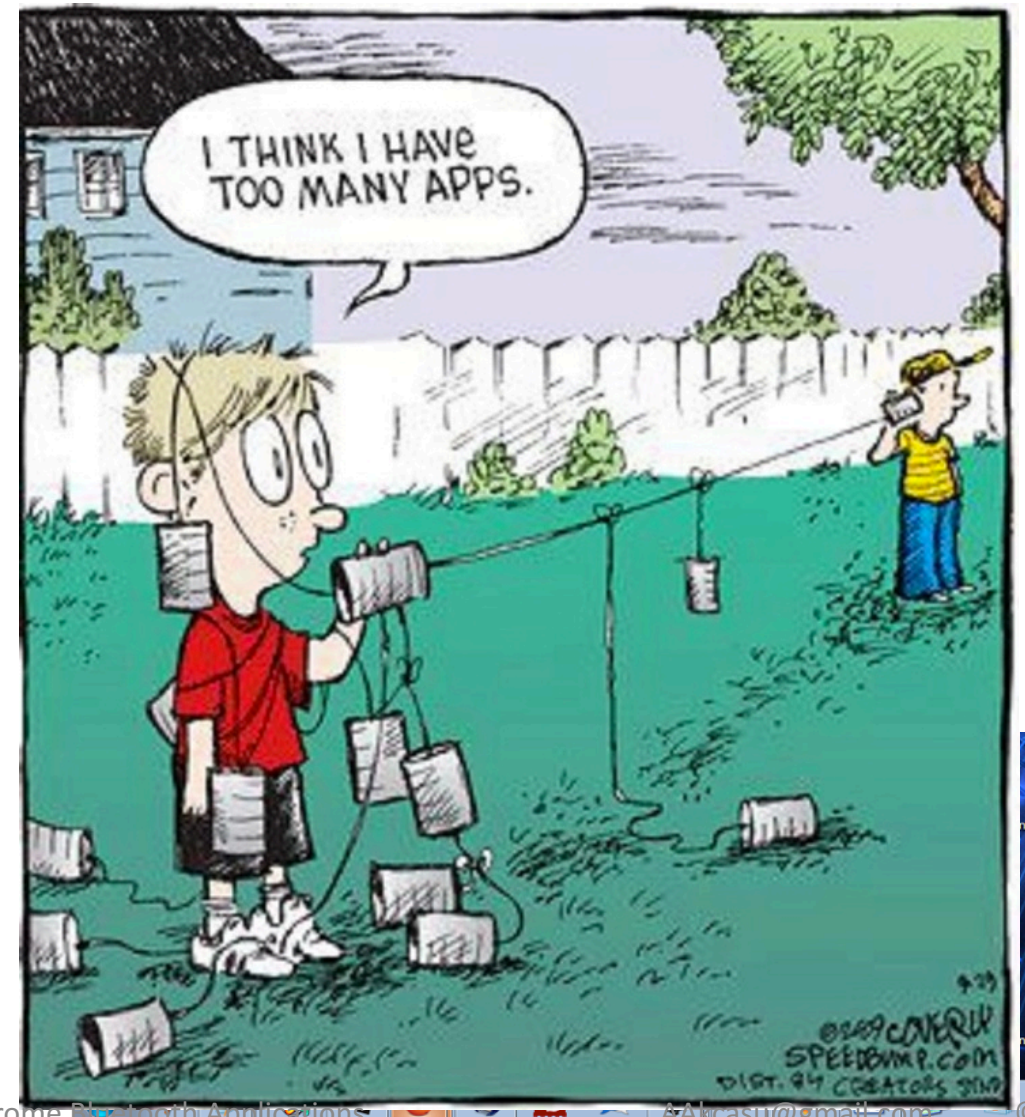
Creating Apps with Bluetooth Capability is Hard

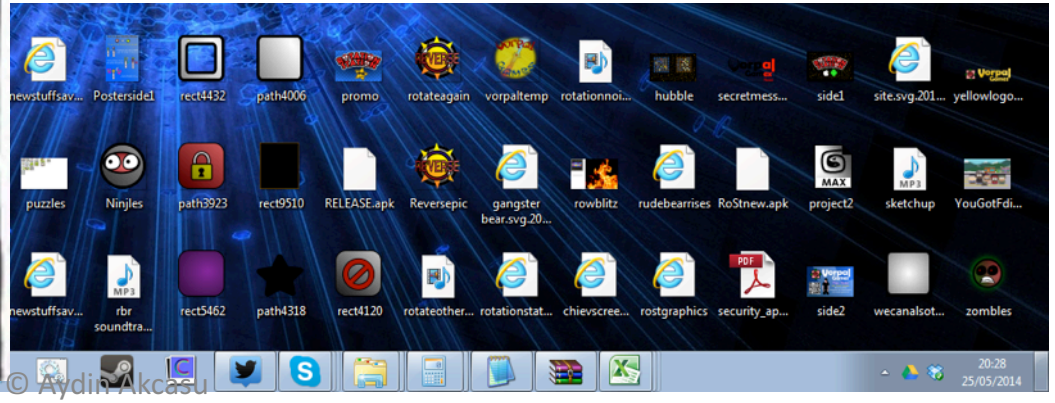


Some may not run on all devices



Most need a seldom used dedicated app





Most don’t communicate with other Devices

Extensibility

IF ONLY THERE WAS A SOLUTION TO ALL THESE PROBLEMS…

Did you know Chrome **NOW supports Bluetooth?**

chrome

Chrome

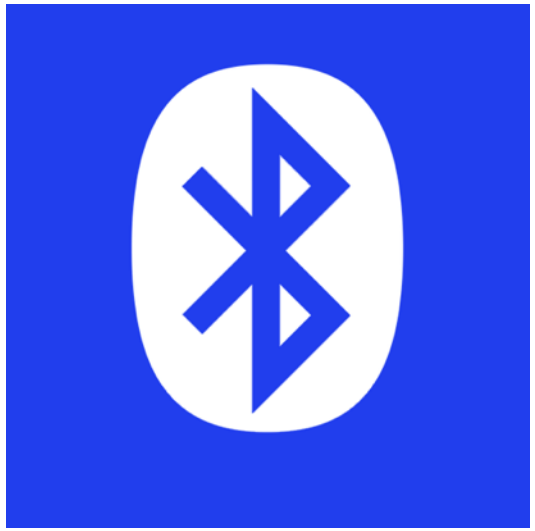
Bluetooth™

Runs on ALL Devices

Version 56+

navigator.bluetooth.*

Getting Started



Bluetooth Device

Chrome Browser

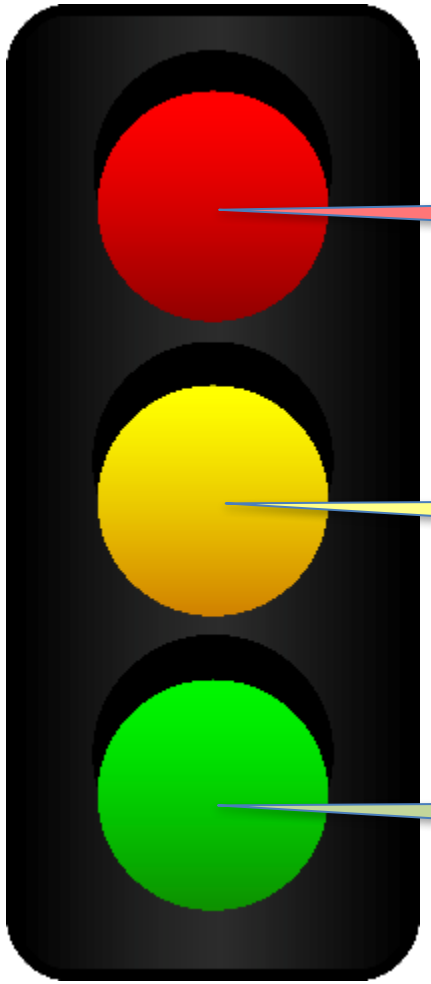
Text Editor

TO DEMONSTRATE AND RESOLVE THESE ISSUES, HERE IS OUR PROBLEM …

Can you detect if someone is stressed?

Which photo shows the most or least stress?

What if people were more like a traffic light?

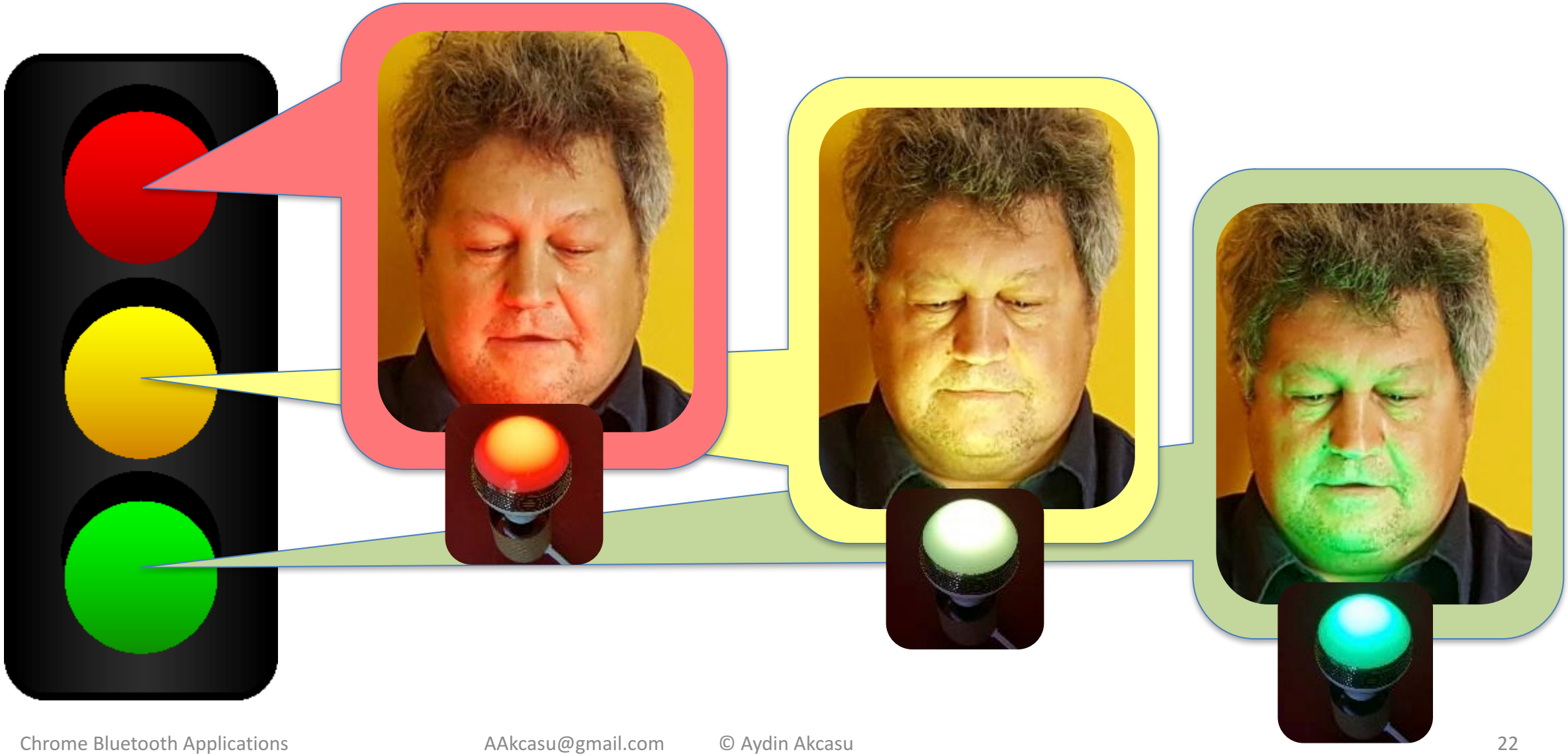


I'm very stressed,
"Leave me alone!!!

I'm a bit stressed,
"Proceed with Caution!"

I'm relaxed,
"Can I help you?"

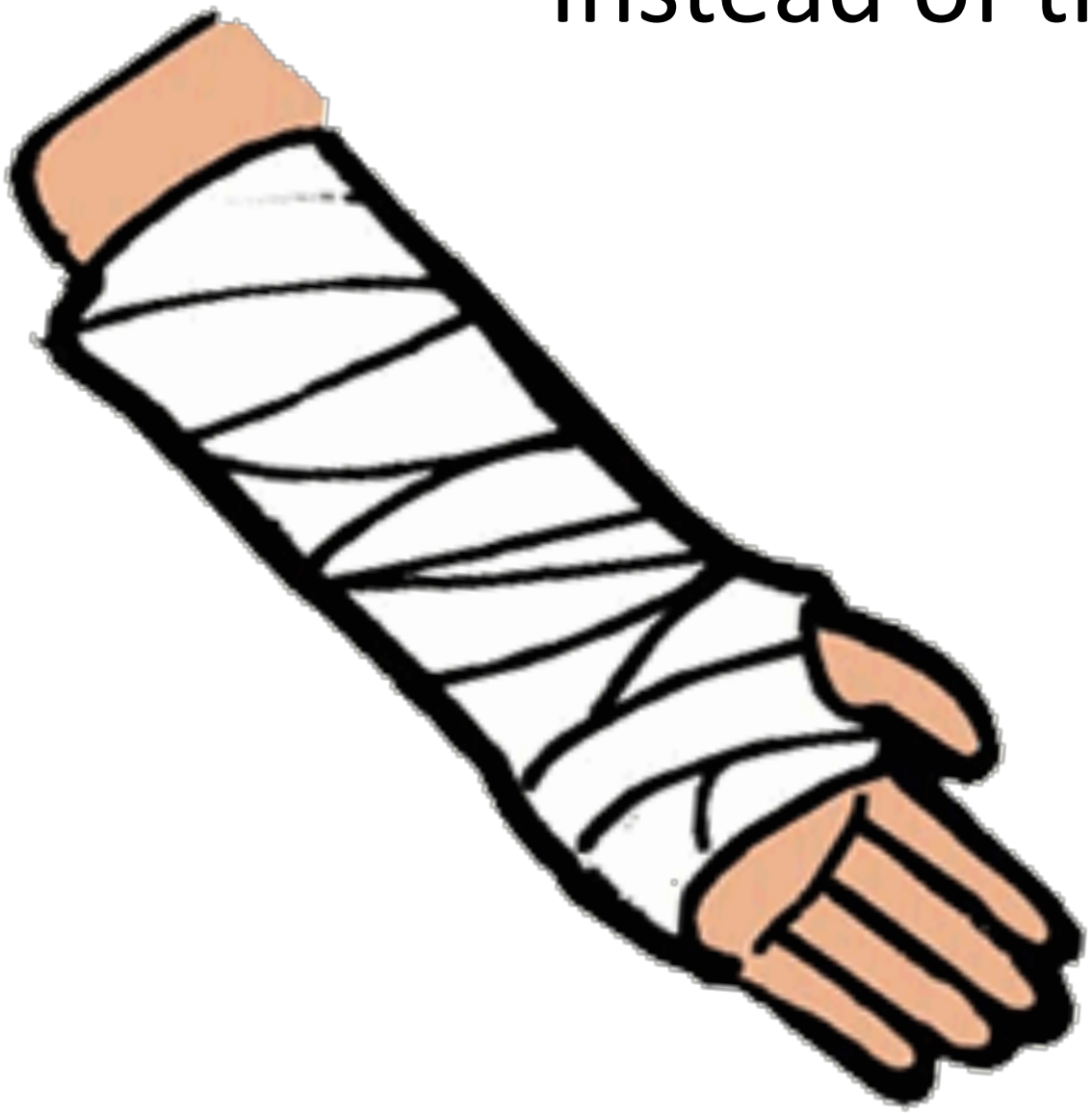
What if a light bulb could show Stress?



With a “Stress Display”:

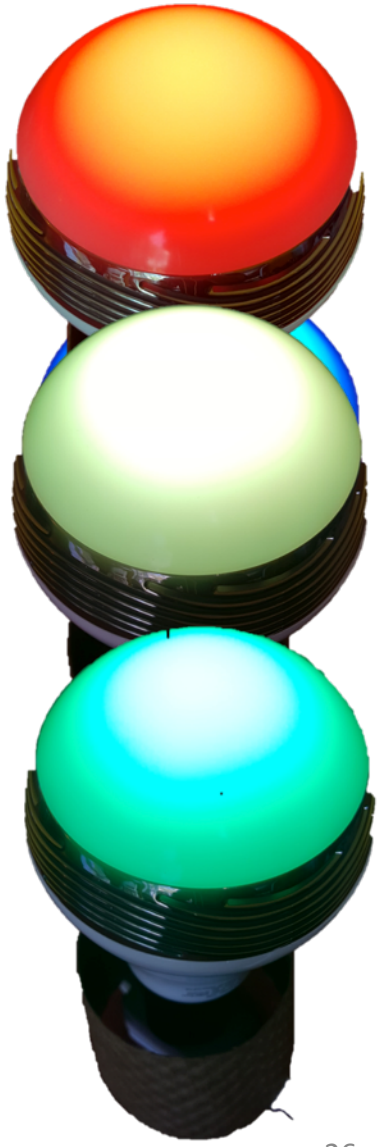
We could have this outcome

Instead of this!

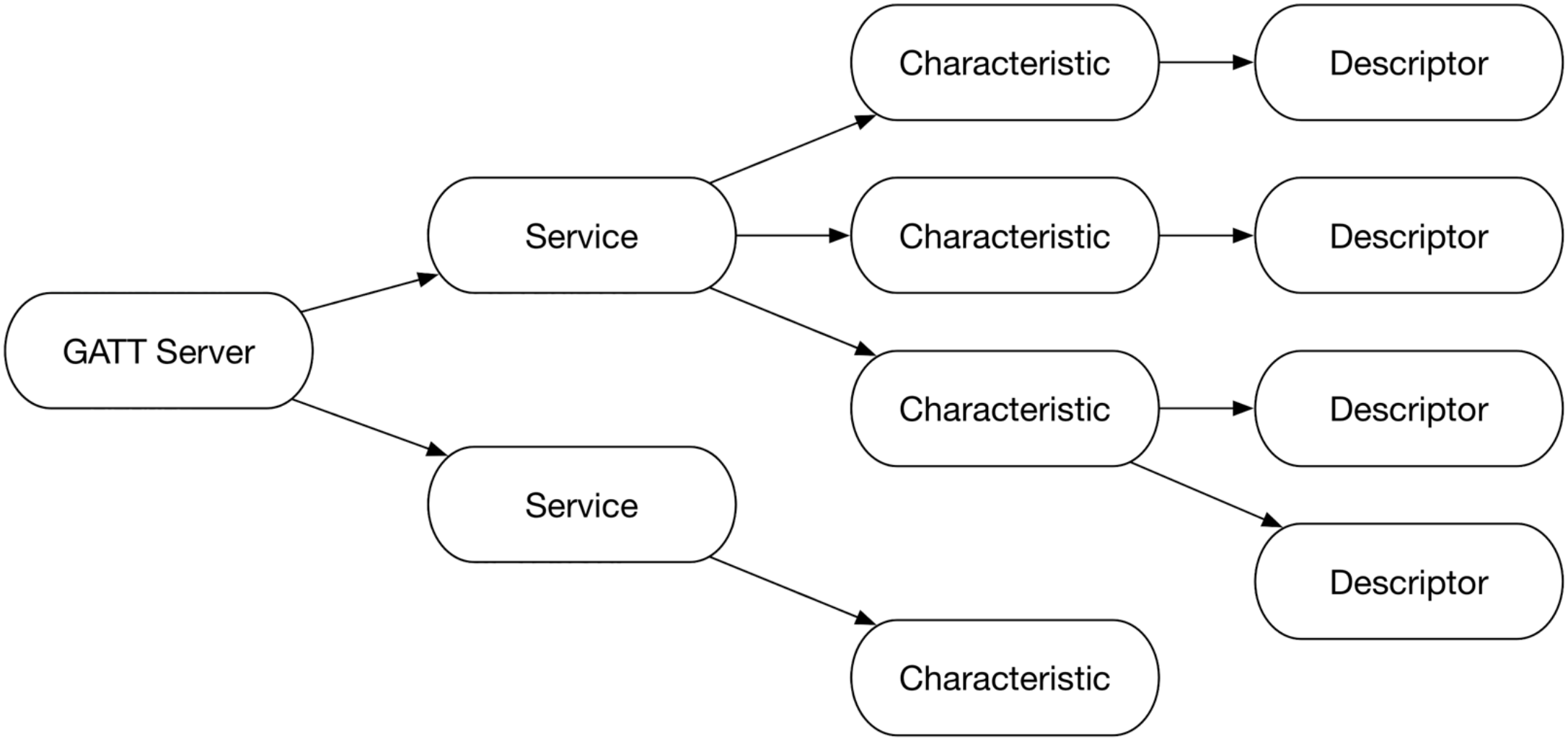


THIS IS THE PROBLEM WE WILL SOLVE

What we will cover:



Terminology



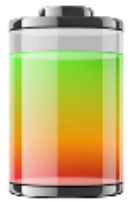
Terminology

- BLE
- “Bluetooth Low Energy”
- "Bluetooth Smart",
- “Bluetooth 4.0”

Terminology

Peripheral

Services
(ServiceUUID)



(“battery_service”)

(“heart_rate”)

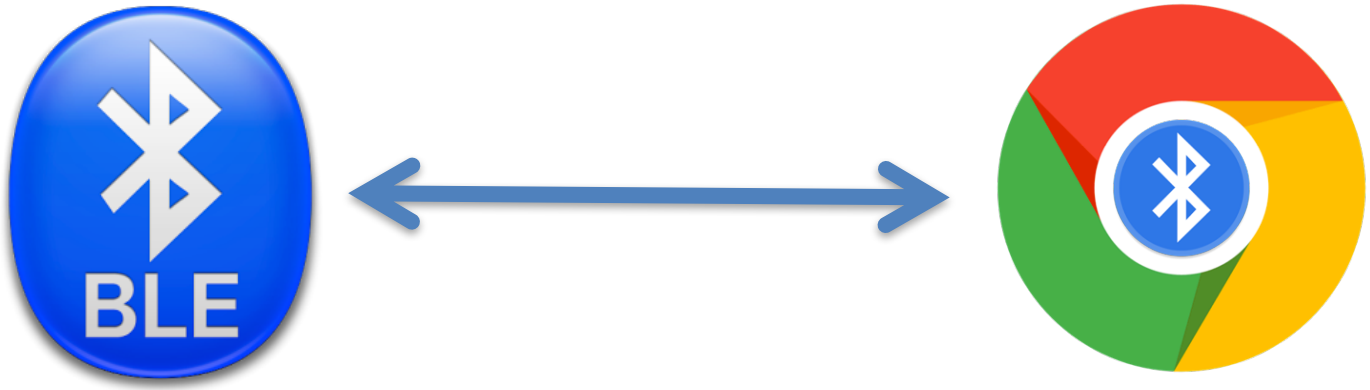
Characteristics
(CharacteristicUUID)

Battery Level: 90%

(“battery_level”)

Heart Rate Measurement: 80BPM
(“heart_rate_meaurement”)

Heart Rate Max: 200 BPM
(“heart_rate_max”)



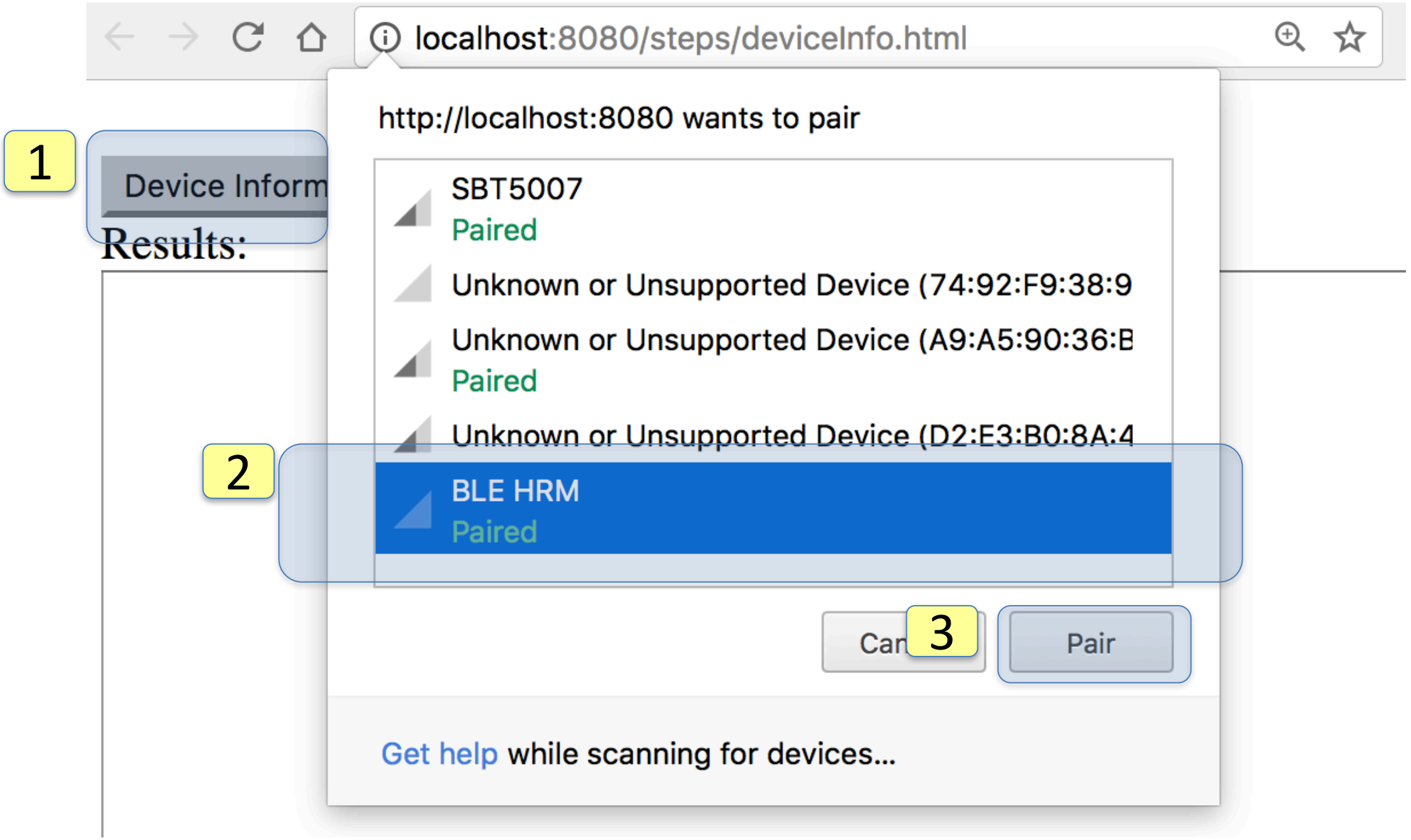
OVERVIEW OF CONNECTING TO A DEVICE

```
1  function deviceInfo_connect() {
2
3      navigator.bluetooth.requestDevice
4          ({
5              acceptAllDevices: true
6          })
7          .then(device => {
8              log('----------');
9              log('> Name:       ' + device.name);
10             log('> Id:         ' + device.id);
11             log('> Connected: ' + device.gatt.connected);
12         })
13         .catch(error => {
14             console.log('Error: ' + error);
15         });
16 }
```

HTML

```
2   <html>
3
4   <head>
5       <script src="../tools/misc.js"></script>
6       <script src="../deviceInfo.js"></script>
7       <title>Chrome Bluetooth Demo</title>
8   </head>
9
10  <body>
11      <br/> <button onclick="deviceInfo_connect()">Device Information</button>
12
13      <br/>Results:
14      <br/> <textarea id="results" cols="130" rows="20" style="font-family:Courier
15  </body>
16
17  </html>
```

Needs a Pop-up for security


localhost:8080/steps/deviceInfo.html
1
Device Inform
Results:
http://localhost:8080 wants to pair
SBT5007
Paired
Unknown or Unsupported Device (74:92:F9:38:9
Unknown or Unsupported Device (A9:A5:90:36:B
Paired
Unknown or Unsupported Device (D2:E3:B0:8A:4
2
BLE HRM
Paired
Can
3
Pair
Get help while scanning for devices...

Device Information

Results:

```
---------
> Name:         BLE HRM
> Id:           WeFeDxilTQJVkajdzfXSVQ==
> Connected:    false
```

Battery Level: 90%

READING THE BATTERY LEVEL FROM A BLUETOOTH DEVICE

```
3   let serviceUuid = "battery_service";
4   let characteristicUuid = "battery_level"
5
6   navigator.bluetooth.requestDevice
7       ({
8           filters: [{ services: [serviceUuid] }]
9           , optionalServices: [serviceUuid]
10      })
11      .then(device => { return device.gatt.connect(); })
12      .then(server => { return server.getPrimaryService(serviceUuid); })
13      .then(service => { return service.getCharacteristic(characteristicUuid); })
14      .then(characteristic => { return characteristic.readValue(); })
15      .then(value => {
16          log('Battery percentage is ' + value.getUint8(0));
17      })
18      .catch(error => {
19          log('Error! ' + error);
20      });
21  }
```

```
3   let serviceUuid = "battery_service";
4   let characteristicUuid = "battery_level"
5
6   navigator.bluetooth.requestDevice
7       ({
8           filters: [{ services: [serviceUuid] }]
9           , optionalServices: [serviceUuid]
10      })
11      .then(device => { return device.gatt.connect(); })
12      .then(server => { return server.getPrimaryService(serviceUuid); })
13      .then(service => { return service.getCharacteristic(characteristicUuid); })
14      .then(characteristic => { return characteristic.readValue(); })
15      .then(value => {
16          log('Battery percentage is ' + value.getUint8(0));
17      })
18      .catch(error => {
19          log('Error! ' + error);
20      });
21  }
```

```
3   let serviceUuid = "battery_service";
4   let characteristicUuid = "battery_level"
5
6   navigator.bluetooth.requestDevice
7       ({
8           filters: [{ services: [serviceUuid] }]
9           , optionalServices: [serviceUuid]
10      })
11      .then(device => { return device.gatt.connect(); })
12      .then(server => { return server.getPrimaryService(serviceUuid); })
13      .then(service => { return service.getCharacteristic(characteristicUuid); })
14      .then(characteristic => { return characteristic.readValue(); })
15      .then(value => {
16          log('Battery percentage is ' + value.getUint8(0));
17      })
18      .catch(error => {
19          log('Error! ' + error);
20      });
21  }
```

```
3   let serviceUuid = "battery_service";
4   let characteristicUuid = "battery_level"
5
6   navigator.bluetooth.requestDevice
7       ({
8           filters: [{ services: [serviceUuid] }]
9           , optionalServices: [serviceUuid]
10      })
11      .then(device => { return device.gatt.connect(); })
12      .then(server => { return server.getPrimaryService(serviceUuid); })
13      .then(service => { return service.getCharacteristic(characteristicUuid); })
14      .then(characteristic => { return characteristic.readValue(); })
15      .then(value => {
16          log('Battery percentage is ' + value.getUint8(0));
17      })
18      .catch(error => {
19          log('Error! ' + error);
20      });
21  }
```

```
3   let serviceUuid = "battery_service";
4   let characteristicUuid = "battery_level"
5
6   navigator.bluetooth.requestDevice
7       ({
8           filters: [{ services: [serviceUuid] }]
9           , optionalServices: [serviceUuid]
10      })
11      .then(device => { return device.gatt.connect(); })
12      .then(server => { return server.getPrimaryService(serviceUuid); })
13      .then(service => { return service.getCharacteristic(characteristicUuid); })
14      .then(characteristic => { return characteristic.readValue(); })
15      .then(value => {
16          log('Battery percentage is ' + value.getUint8(0));
17      })
18      .catch(error => {
19          log('Error! ' + error);
20      });
21  }
```

```
3   let serviceUuid = "battery_service";
4   let characteristicUuid = "battery_level"
5
6   navigator.bluetooth.requestDevice
7       ({
8           filters: [{ services: [serviceUuid] }]
9           , optionalServices: [serviceUuid]
10      })
11      .then(device => { return device.gatt.connect(); })
12      .then(server => { return server.getPrimaryService(serviceUuid); })
13      .then(service => { return service.getCharacteristic(characteristicUuid); })
14      .then(characteristic => { return characteristic.readValue(); })
15      .then(value => {
16          log('Battery percentage is ' + value.getUint8(0));
17      })
18      .catch(error => {
19          log('Error! ' + error);
20      });
21  }
```

Results:

```
Battery percentage is 96
```

Heart Rate
Measurement: 80BPM

CONNECT TO HEART RATE MONITOR

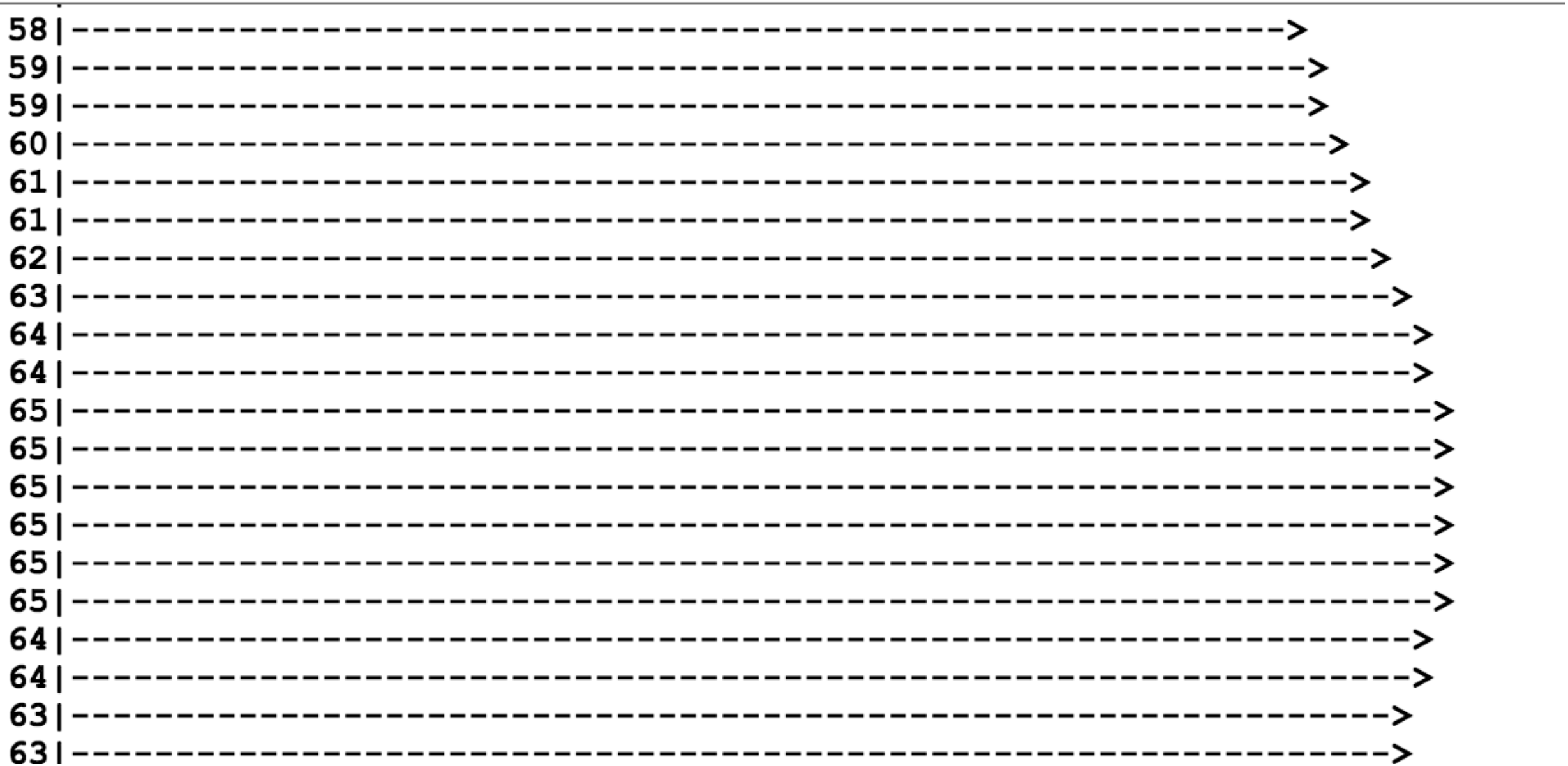
```
6       let serviceUuid = "heart_rate";
7       let characteristicUuid = "heart_rate_measurement"
8
9       navigator.bluetooth.requestDevice
10          ({…
12          })
13          .then(device => { return device.gatt.connect(); })
14          .then(server => { return server.getPrimaryService(serviceUuid); })
15          .then(service => { return service.getCharacteristic(characteristicUuid); })
16          .then(characteristic => {   // Save characteristic…
19          })
20          .then(characteristic => {   // Start notification…
27          })
28          .catch(error => {…
30          });
31  }
```

```
13          .then(device => { return device.gatt.connect(); })
14          .then(server => { return server.getPrimaryService(serviceUuid); })
15          .then(service => { return service.getCharacteristic(characteristicUuid); })
16          .then(characteristic => {   // Save characteristic
17            heartRate_Characteristic = characteristic;
18            return characteristic;
19          })
20          .then(characteristic => {   // Start notification…
27          })
28          .catch(error => {   // Handle Errors
29              log('Error! ' + error);
30          });
31  }
```

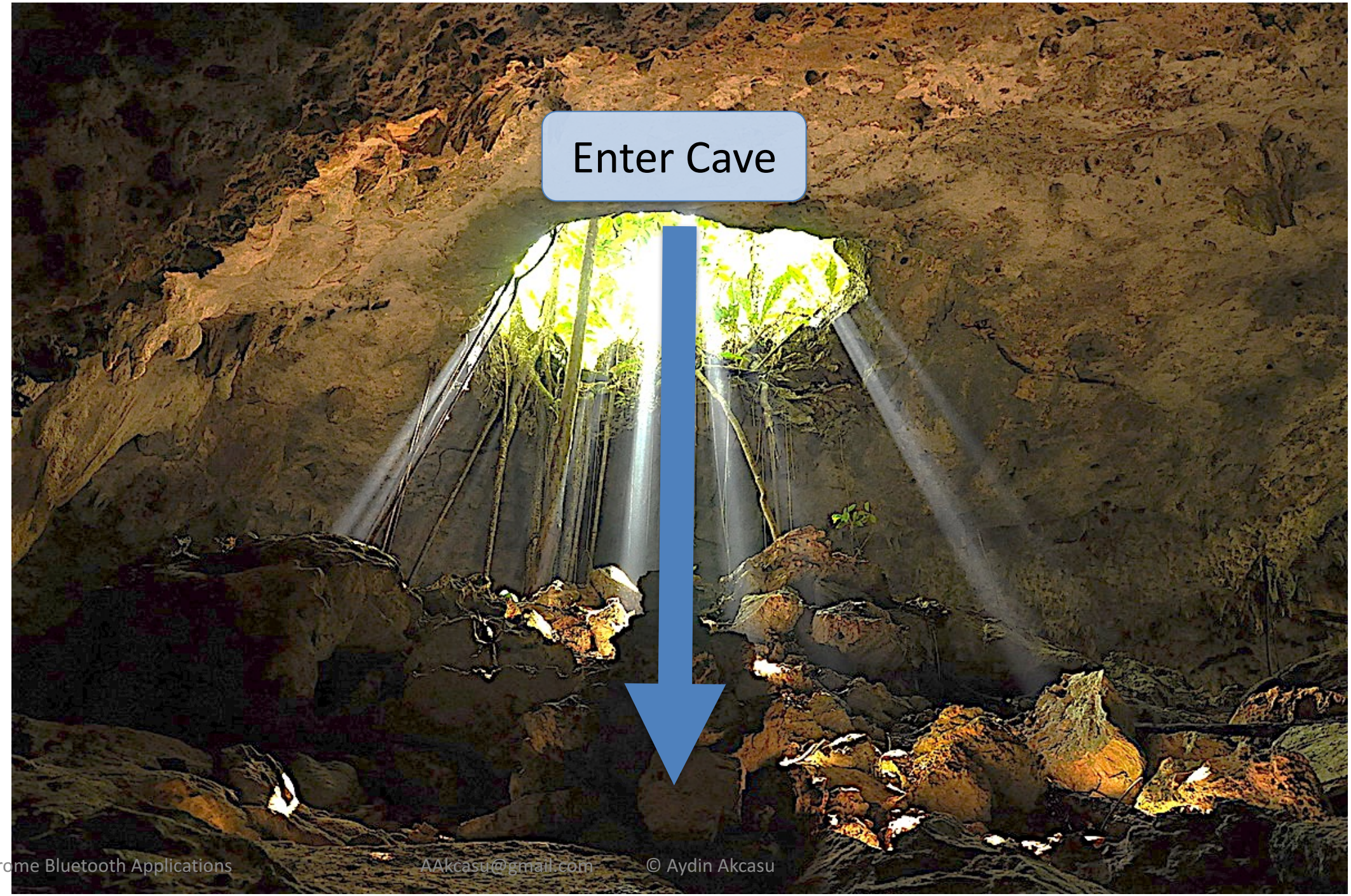
```
14      .then(device => { return device.gatt.connect(); })
15      .then(server => { return server.getPrimaryService(serviceUuid); })
16      .then(service => { return service.getCharacteristic(characteristicUuid); })
17  +   .then(characteristic => {   // Save characteristic…
20      })
21  -   .then(characteristic => {   // Start notification
22  -       return heartRate_Characteristic.startNotifications()
23  -           .then(_ => {
24  -               heartRate_Characteristic.addEventListener(
25                      'characteristicvaluechanged',
26                      heartRate_read);
27              });
28      })
```

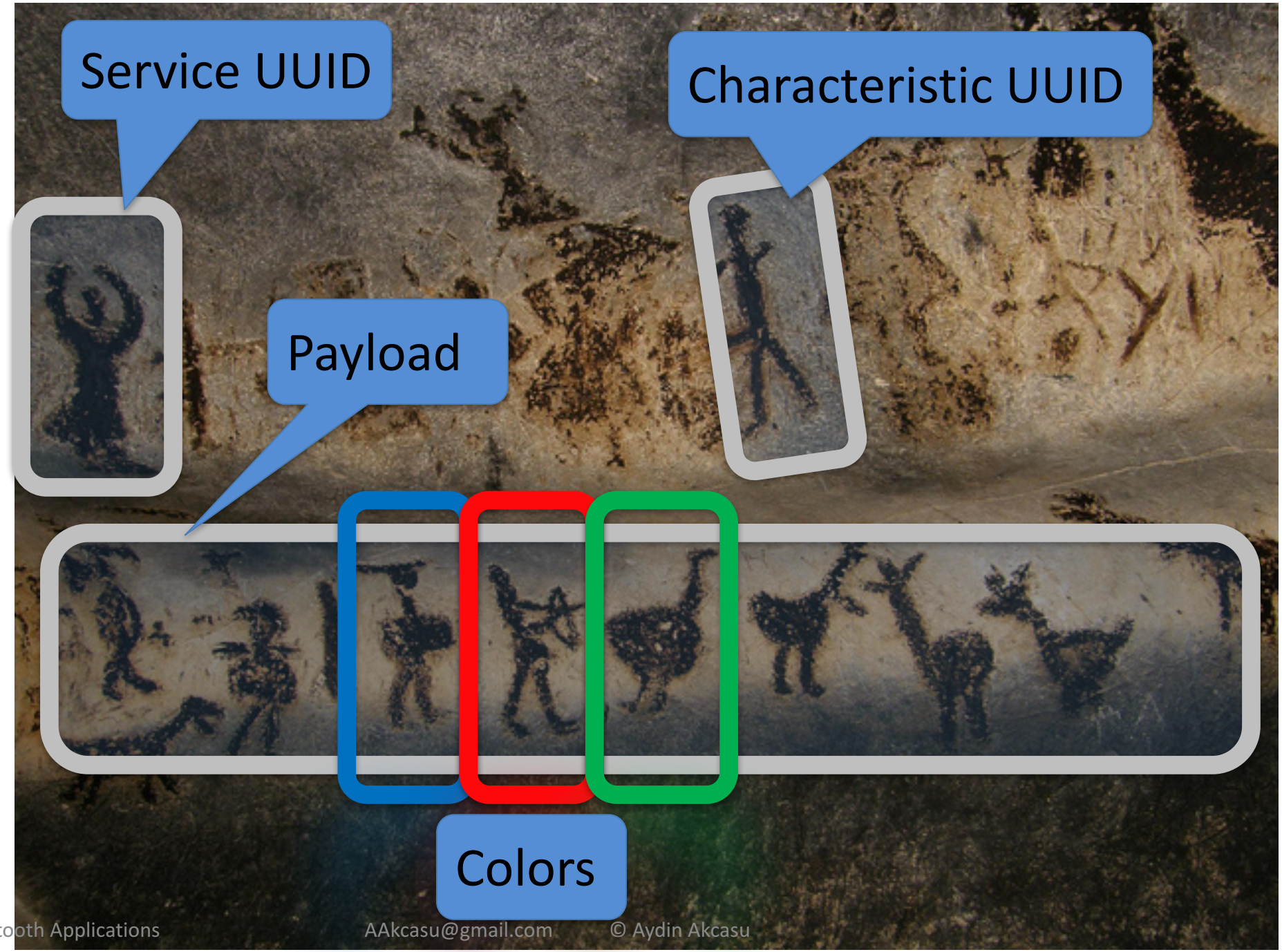
```
34    function heartRate_read(event) {
35        let value = event.target.value;
36
37        var bpm = value.getUint8(1);
38        setHeartRateValue(bpm);
39
40        log(bpm.toString().padStart(3) + '|' + '-'.repeat(bpm-40) + '>');
41    }
```

Results:

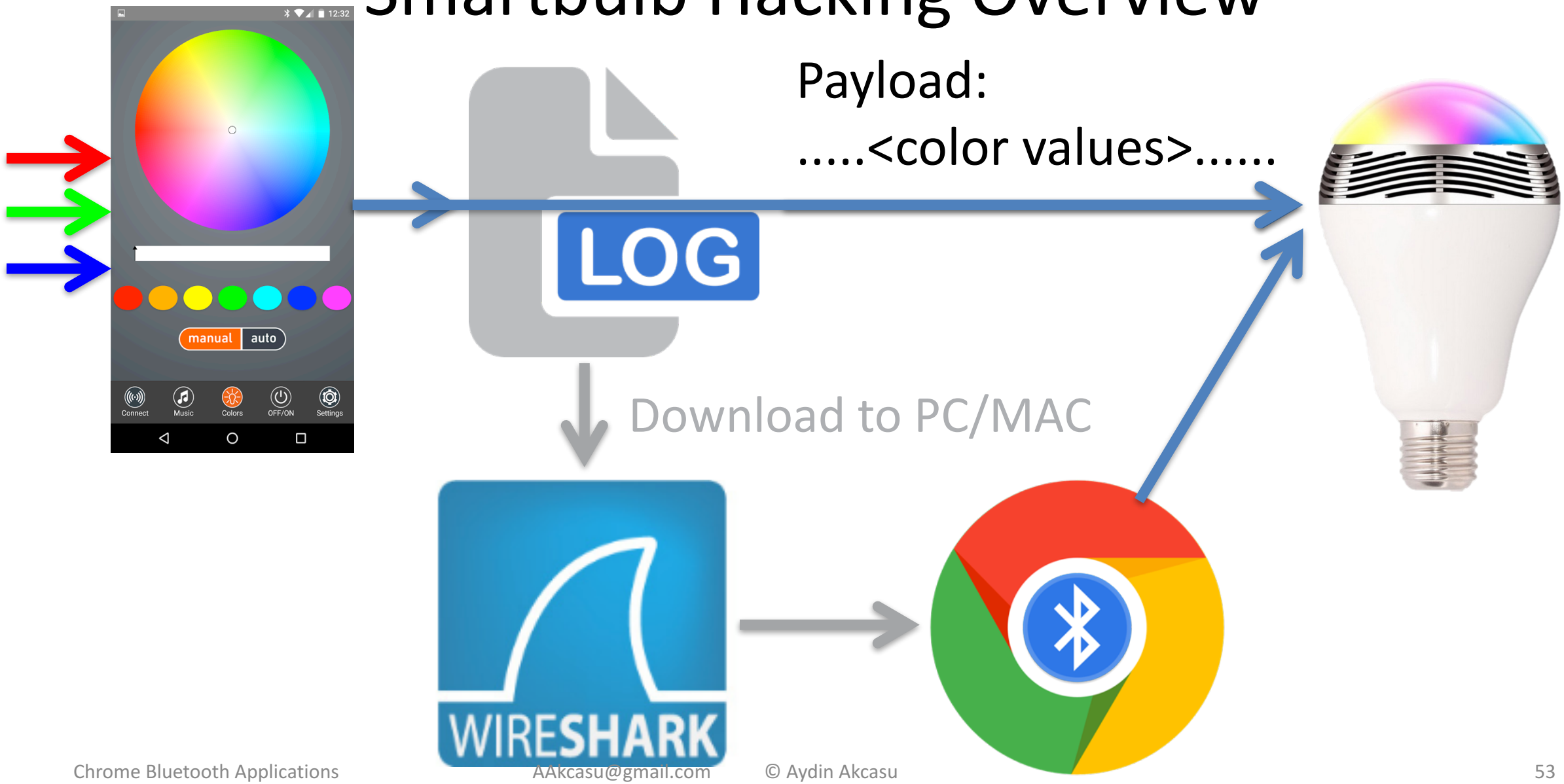


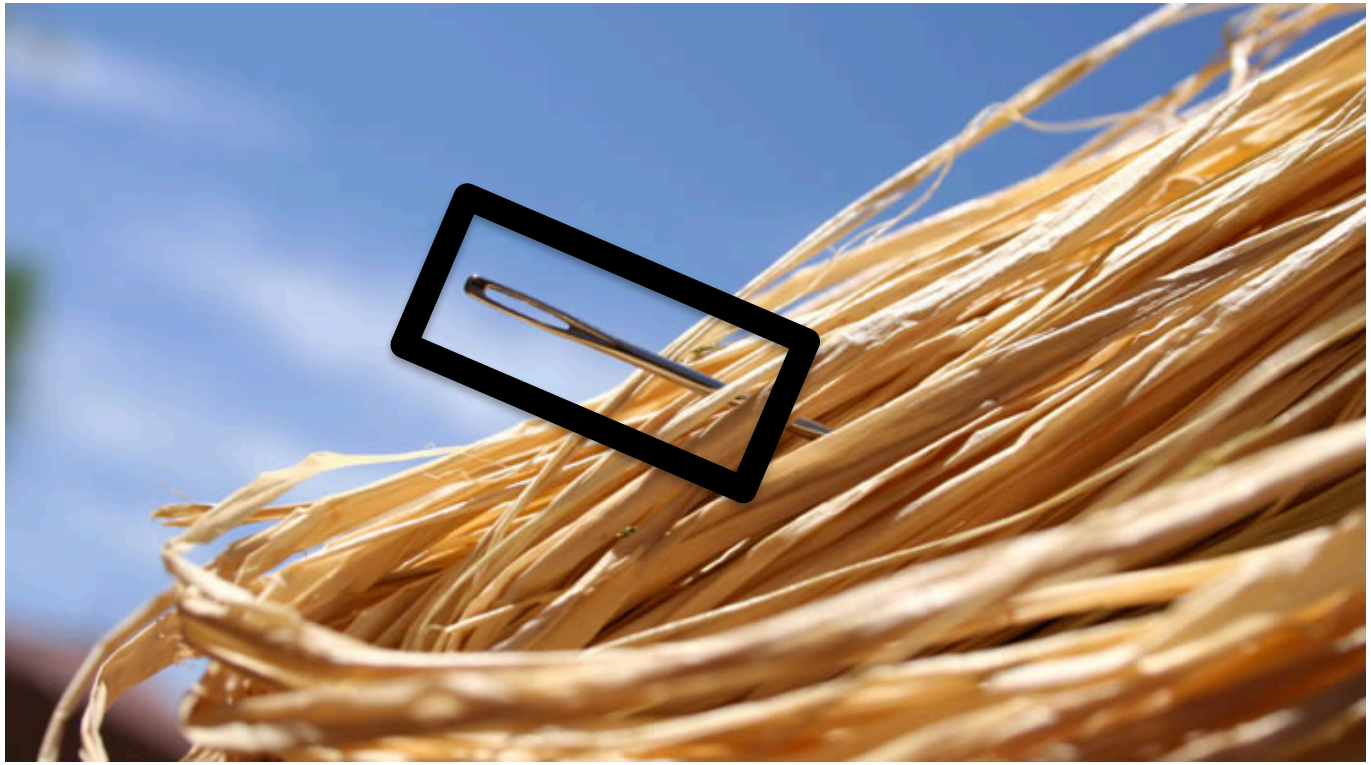
CONNECT TO AN UNKNOWN DEVICE


Enter Cave


Service UUID
Characteristic UUID
Payload
Colors

Smartbulb Hacking Overview





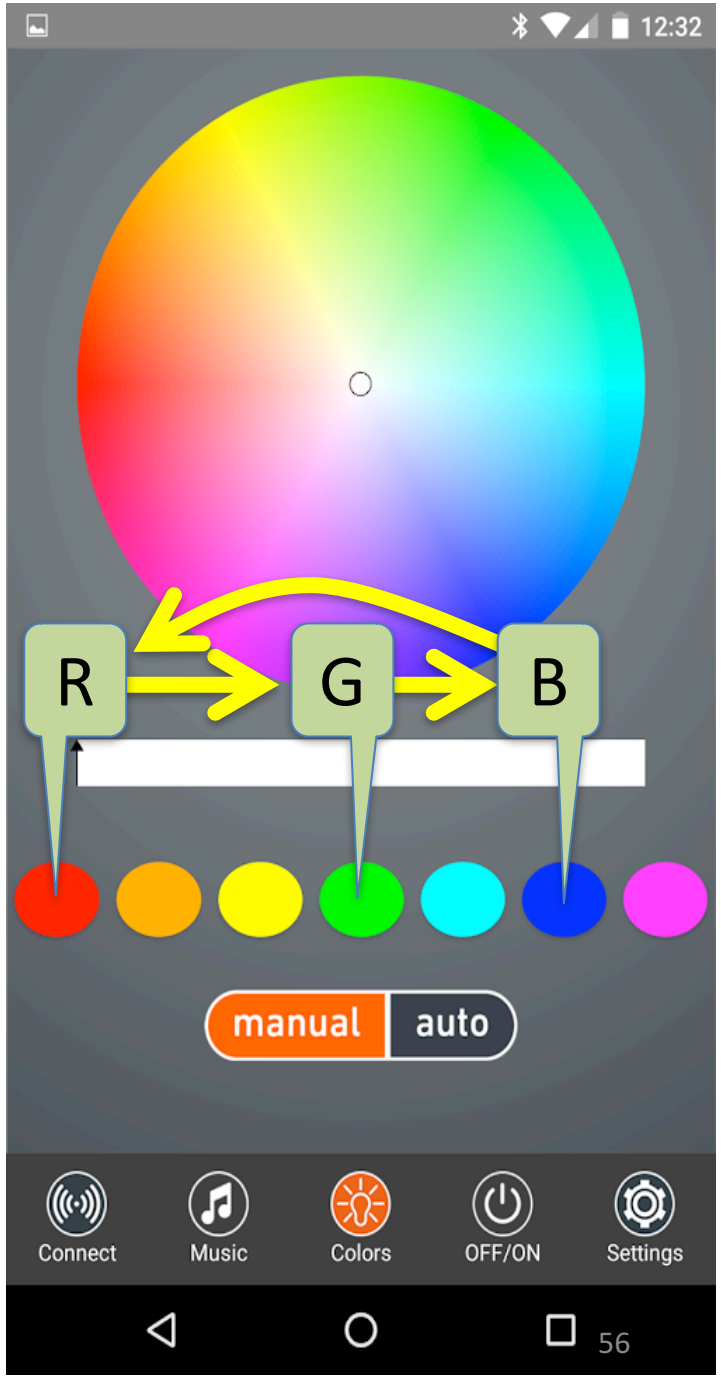
RUN APP TO CREATE AN IDENTIFIABLE COLOR PATTERN

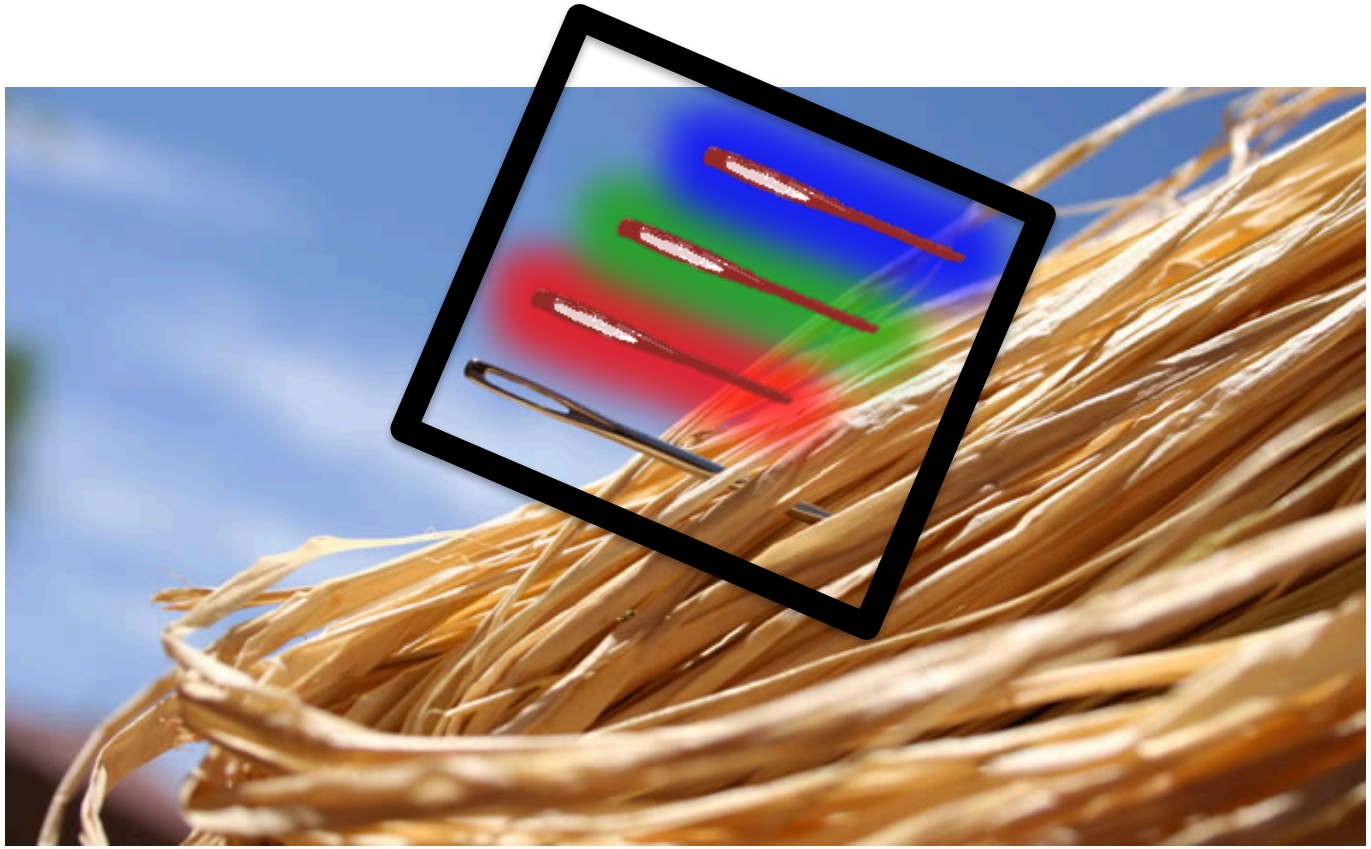
Intro to Bits, bytes…

- Byte
  - 0-255 (base 10)
  - 0x00-0xff (base 16), or Hex
- RGB
  - Red, Green, Blue
- Payloads
  - List of Bytes

Install and Run App

- Name: “Switcher by Sharper Image”
- Run some “Identifiable data”:
  - RR GG BB RRGGBB
  - R: (0xff,0x00,0x00) = 0xff0000
  - G: (0x00,0xff,0x00) = 0x00ff00
  - B: (0x00,0x00,0xff) = 0x0000ff
  - R: (0xff,0x00,0x00) = 0xff0000
  - G: (0x00,0xff,0x00) = 0x00ff00
  - B: (0x00,0x00,0xff) = 0x0000ff

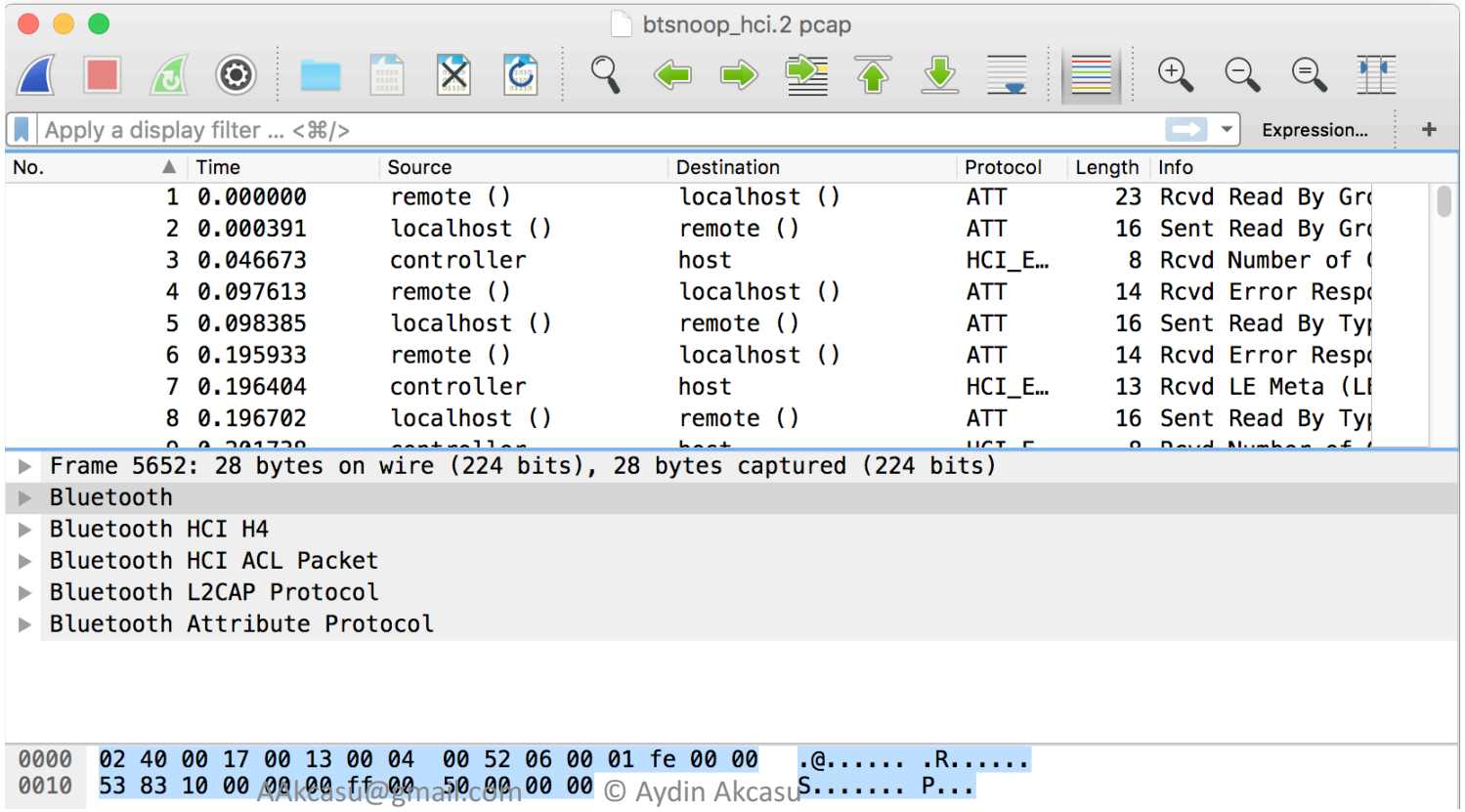


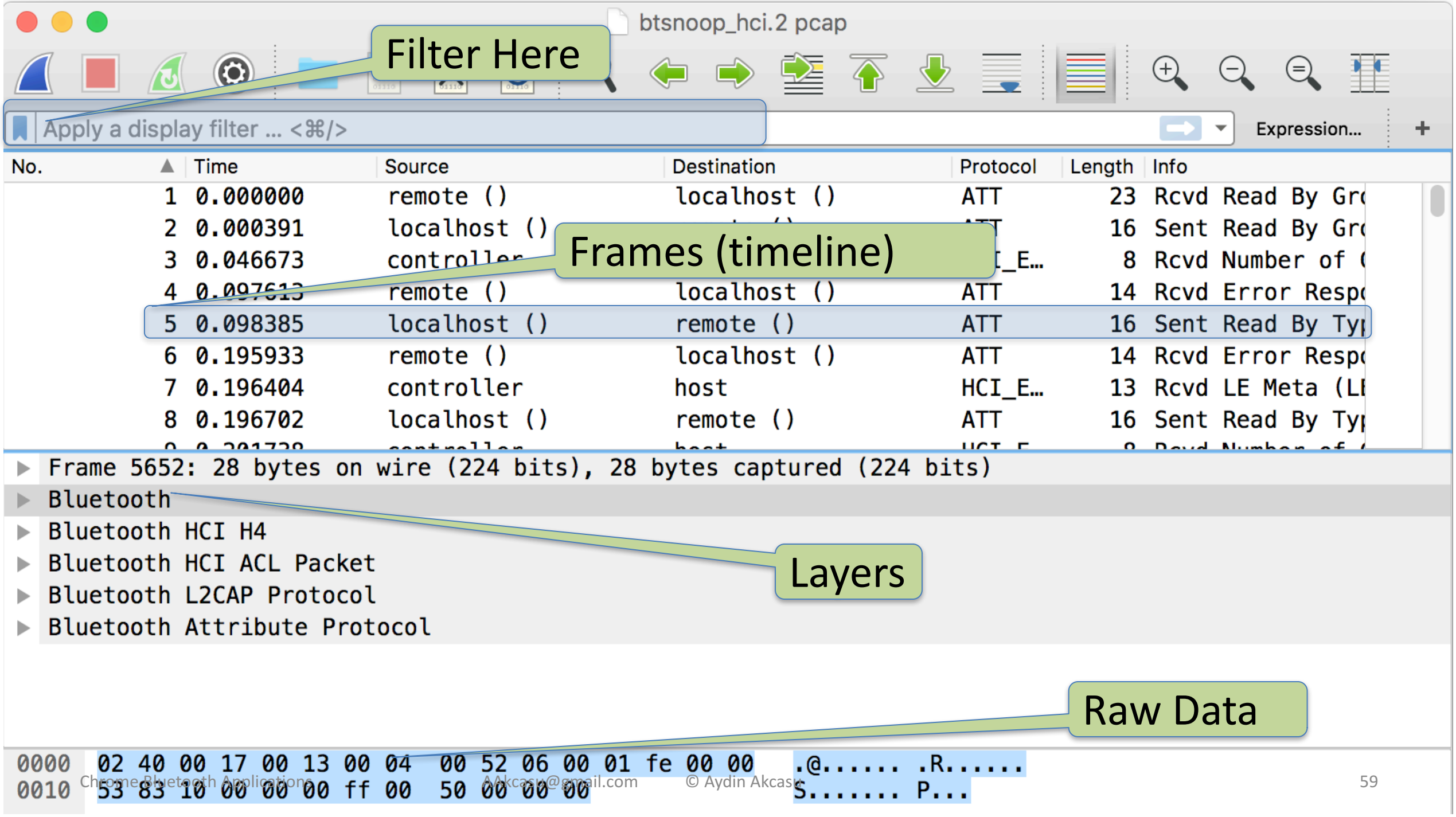


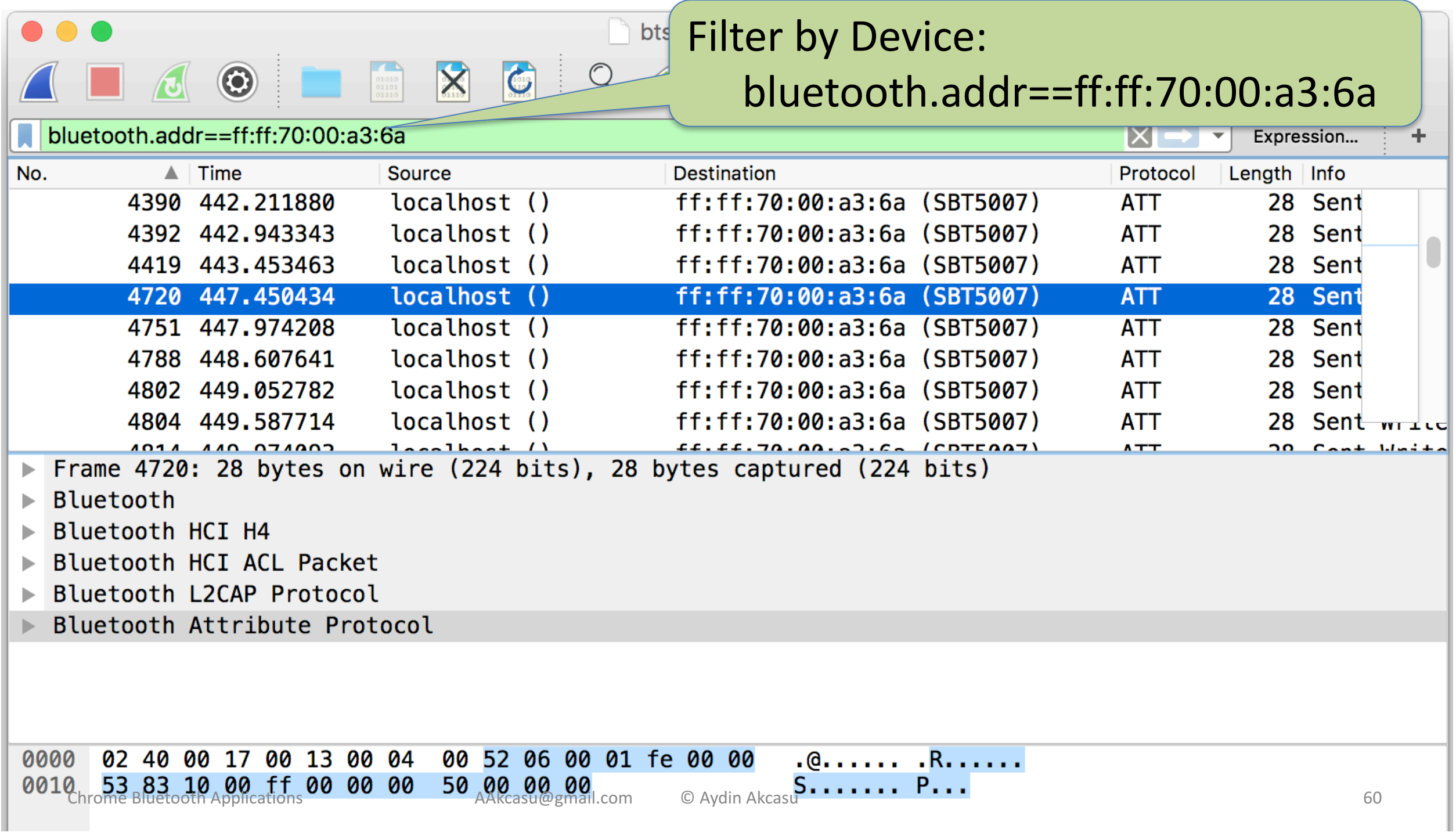
ANALYZE PACKETS FOR THIS IDENTIFIABLE COLOR PATTERN

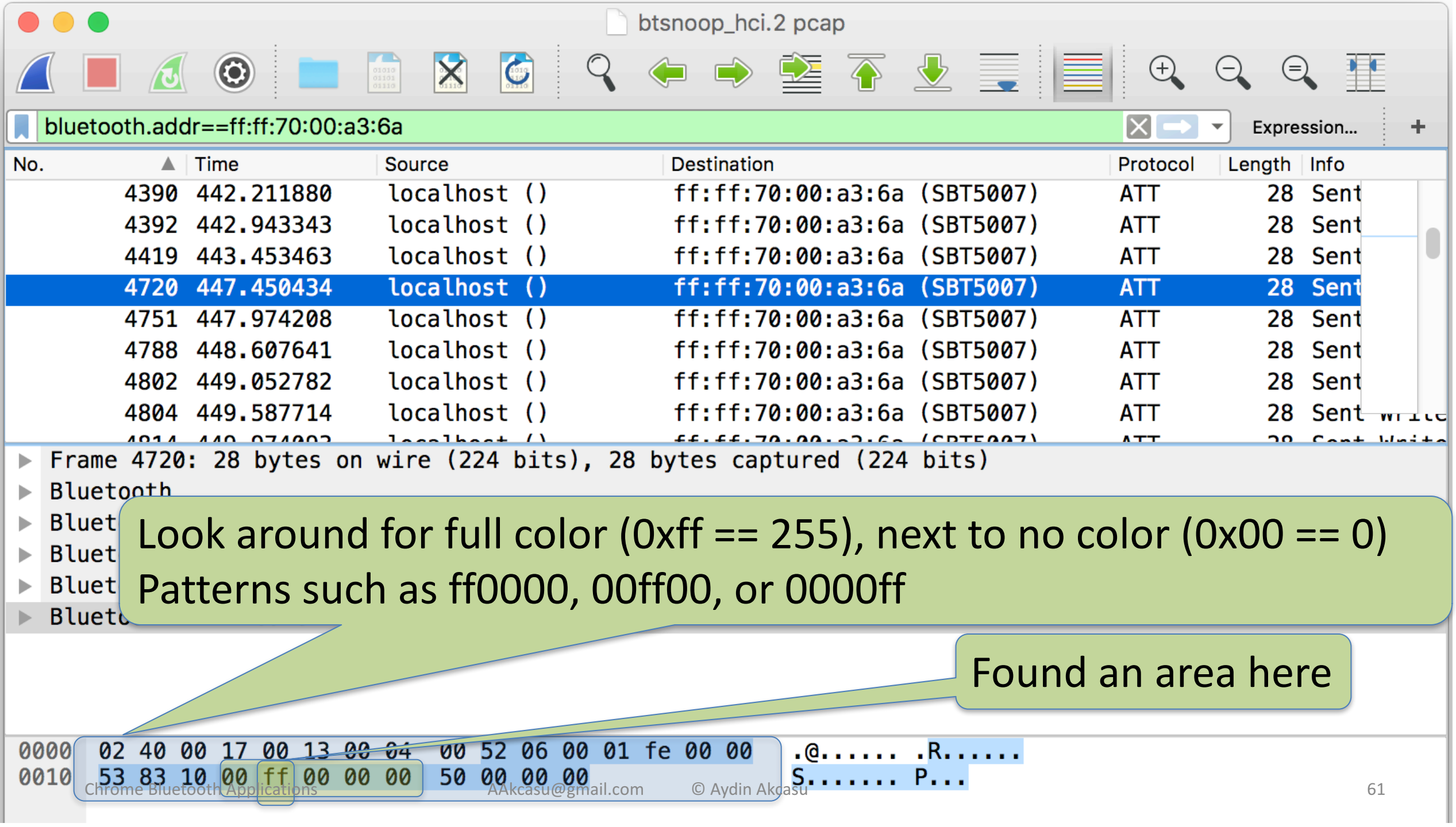
Wireshark

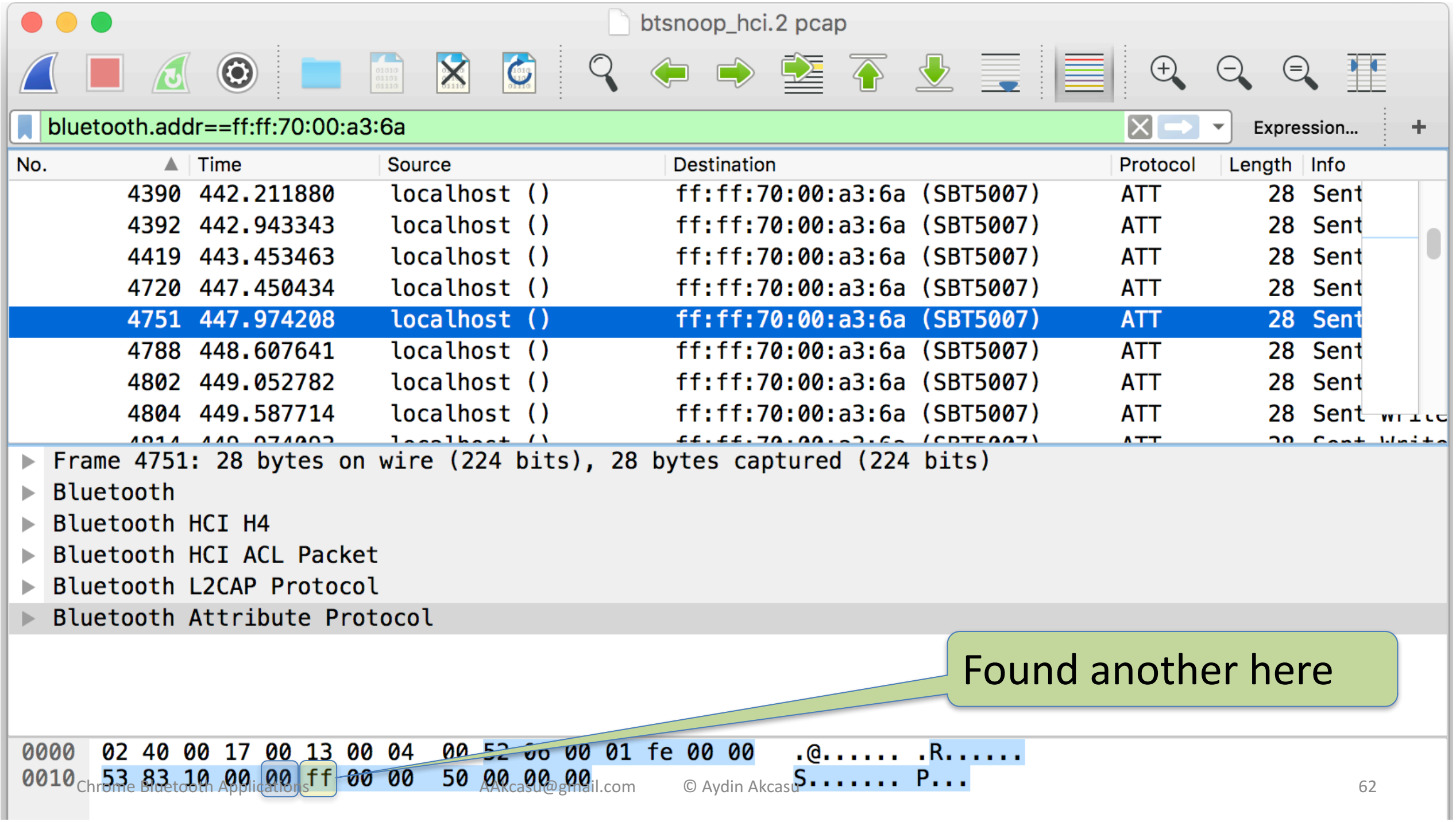
- **Wireshark is the world's foremost and widely-used network protocol analyzer.**

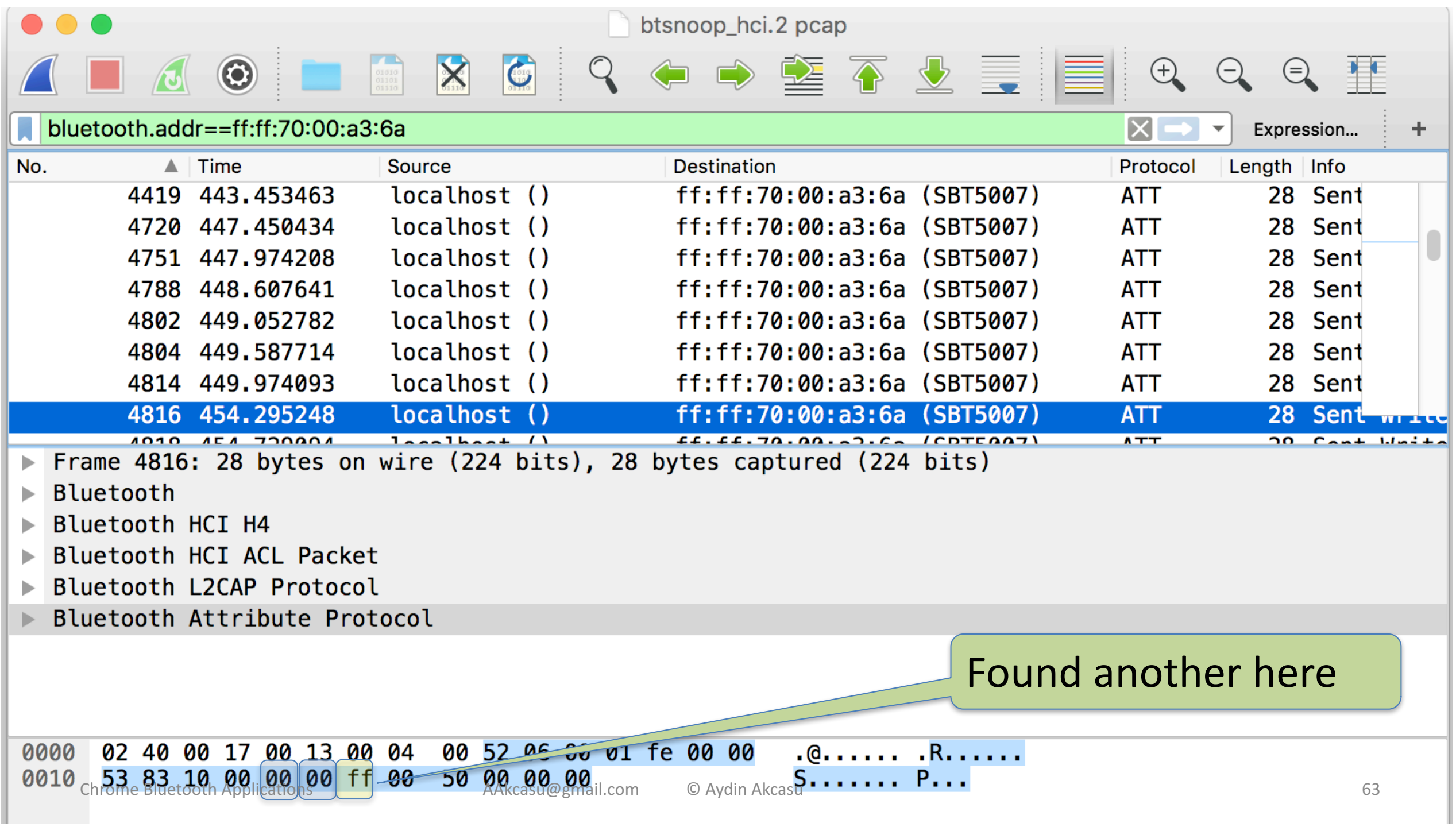


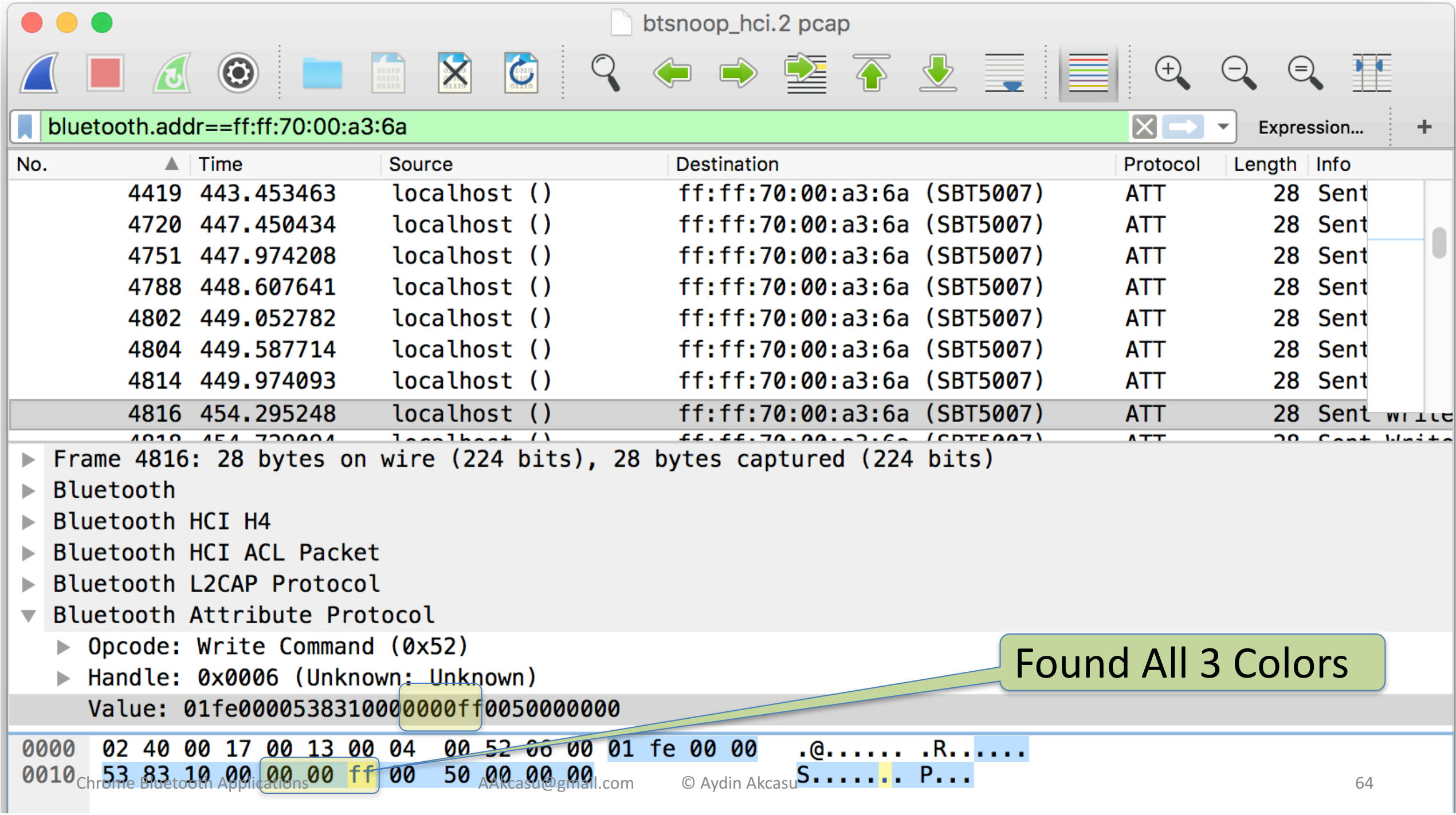

btsnoop_hci.2 pcap
Filter Here
Apply a display filter ... <⌘/>
Expression...
Frames (timeline)
No. Time Source Destination Protocol Length Info
1 0.000000 remote () localhost () ATT 23 Rcvd Read By Gr
2 0.000391 localhost () 16 Sent Read By Gr
3 0.046673 8 Rcvd Number of
4 0.097613 remote () localhost () ATT 14 Rcvd Error Resp
5 0.098385 localhost () remote () ATT 16 Sent Read By Ty
6 0.195933 remote () localhost () ATT 14 Rcvd Error Resp
7 0.196404 controller host HCI_E… 13 Rcvd LE Meta (LE
8 0.196702 localhost () remote () ATT 16 Sent Read By Ty
Frame 5652: 28 bytes on wire (224 bits), 28 bytes captured (224 bits)
Bluetooth
Bluetooth HCI H4
Bluetooth HCI ACL Packet
Bluetooth L2CAP Protocol
Bluetooth Attribute Protocol
Layers
Raw Data
0000 02 40 00 17 00 13 00 04 00 52 06 00 01 fe 00 00 .@..... .R.....
0010 53 83 10 00 00 00 ff 00 50 00 00 00 S..... P...

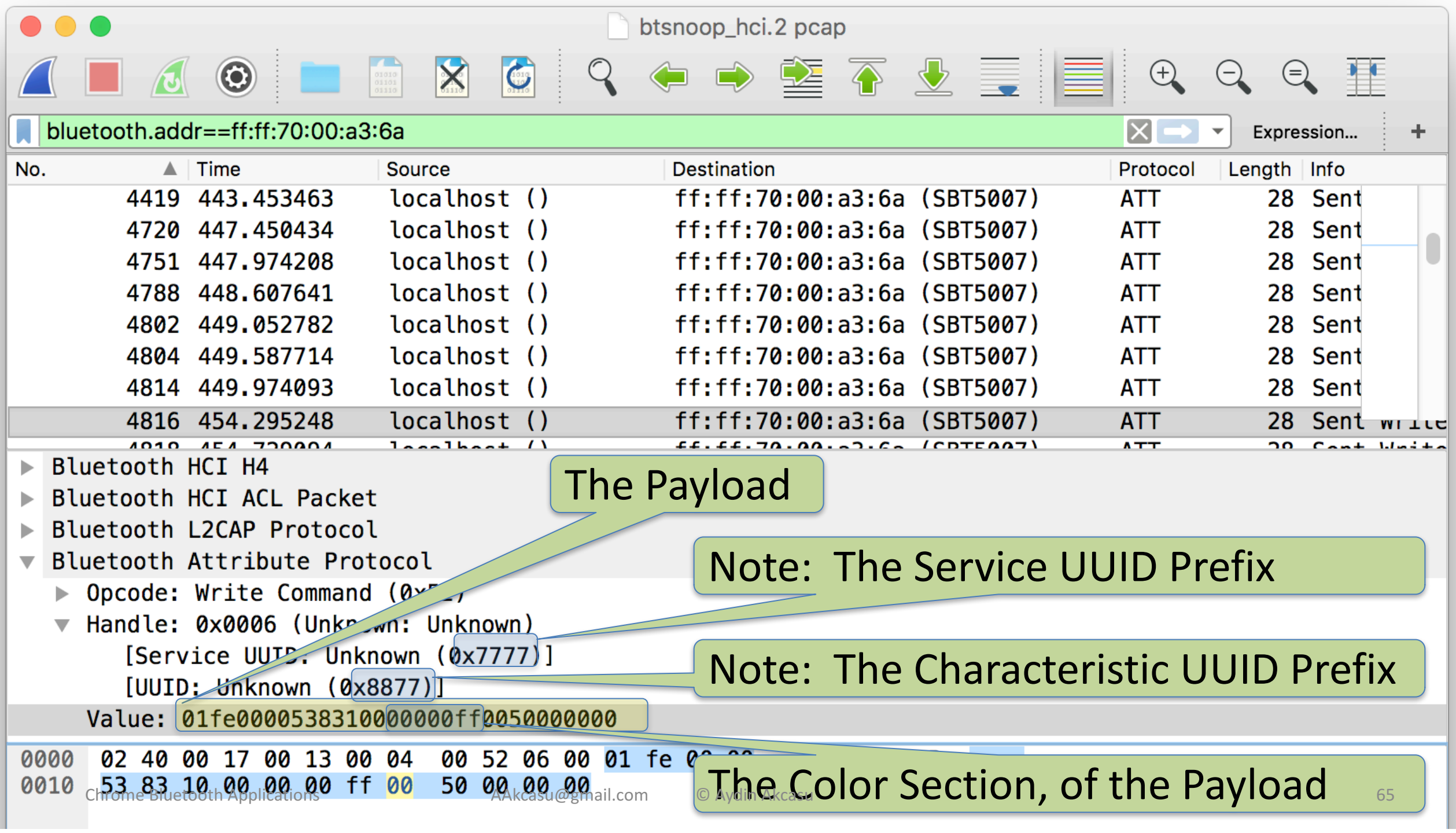

Filter by Device:
bluetooth.addr==ff:ff:70:00:a3:6a
bluetooth.addr==ff:ff:70:00:a3:6a
Expression...
No. Time Source Destination Protocol Length Info
4390 442.211880 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4392 442.943343 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4419 443.453463 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4720 447.450434 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4751 447.974208 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4788 448.607641 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4802 449.052782 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4804 449.587714 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
Frame 4720: 28 bytes on wire (224 bits), 28 bytes captured (224 bits)
Bluetooth
Bluetooth HCI H4
Bluetooth HCI ACL Packet
Bluetooth L2CAP Protocol
Bluetooth Attribute Protocol
0000 02 40 00 17 00 13 00 04 00 52 06 00 01 fe 00 00 .@..... .R.....
0010 53 83 10 00 ff 00 00 00 50 00 00 00 S..... P...


btsnoop_hci.2 pcap
bluetooth.addr==ff:ff:70:00:a3:6a
Expression...
No. Time Source Destination Protocol Length Info
4390 442.211880 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4392 442.943343 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4419 443.453463 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4720 447.450434 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4751 447.974208 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4788 448.607641 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4802 449.052782 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4804 449.587714 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
Frame 4720: 28 bytes on wire (224 bits), 28 bytes captured (224 bits)
Bluetooth
Look around for full color (0xff == 255), next to no color (0x00 == 0)
Patterns such as ff0000, 00ff00, or 0000ff
Found an area here
0000 02 40 00 17 00 13 00 04 00 52 06 00 01 fe 00 00 .@..... .R.....
0010 53 83 10 00 ff 00 00 00 50 00 00 00 S..... P...


btsnoop_hci.2 pcap
bluetooth.addr==ff:ff:70:00:a3:6a
Expression...
No. Time Source Destination Protocol Length Info
4390 442.211880 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4392 442.943343 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4419 443.453463 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4720 447.450434 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4751 447.974208 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4788 448.607641 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4802 449.052782 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4804 449.587714 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
Frame 4751: 28 bytes on wire (224 bits), 28 bytes captured (224 bits)
Bluetooth
Bluetooth HCI H4
Bluetooth HCI ACL Packet
Bluetooth L2CAP Protocol
Bluetooth Attribute Protocol
0000 02 40 00 17 00 13 00 04 00 52 00 00 01 fe 00 00 .@..... .R.....
0010 53 83 10 00 00 ff 00 00 50 00 00 00 S..... P...
Found another here

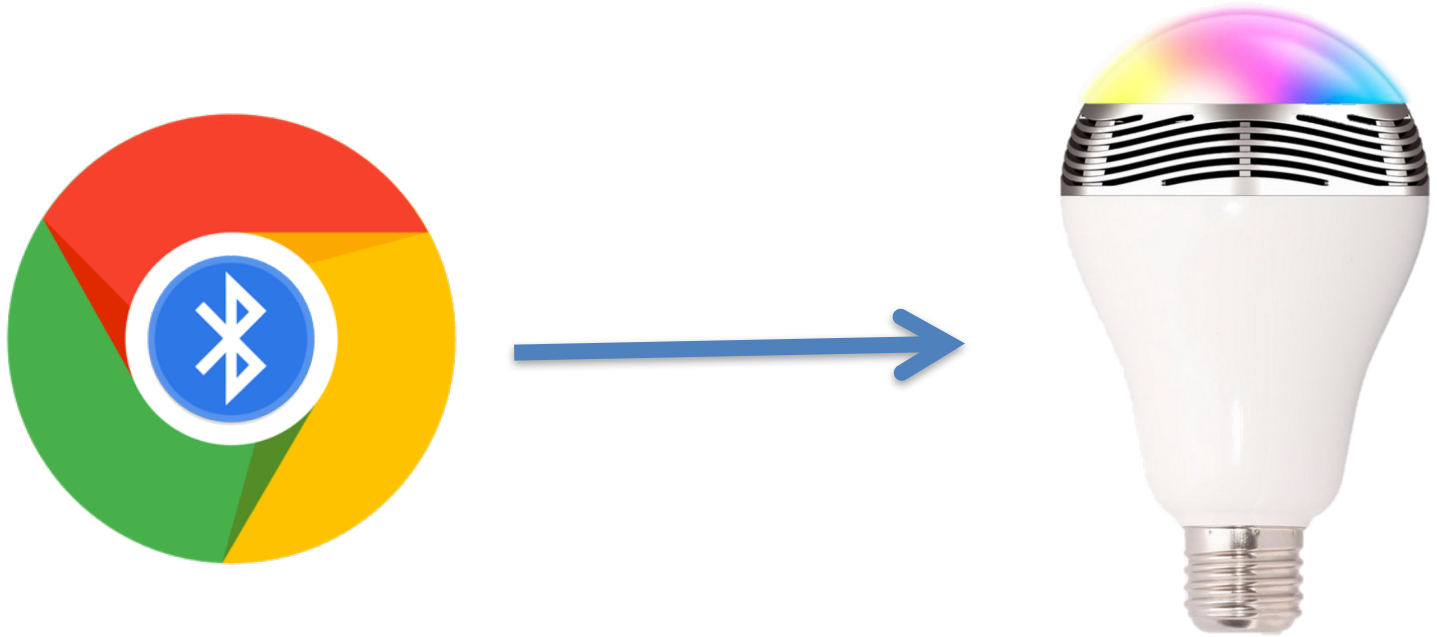

btsnoop_hci.2 pcap
bluetooth.addr==ff:ff:70:00:a3:6a
Expression...
No. Time Source Destination Protocol Length Info
4419 443.453463 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4720 447.450434 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4751 447.974208 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4788 448.607641 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4802 449.052782 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4804 449.587714 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4814 449.974093 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4816 454.295248 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
Frame 4816: 28 bytes on wire (224 bits), 28 bytes captured (224 bits)
Bluetooth
Bluetooth HCI H4
Bluetooth HCI ACL Packet
Bluetooth L2CAP Protocol
Bluetooth Attribute Protocol
0000 02 40 00 17 00 13 00 04 00 52 06 00 01 fe 00 00 .@..... .R.....
0010 53 83 10 00 00 00 ff 00 50 00 00 00 S..... P...
Found another here


btsnoop_hci.2 pcap
bluetooth.addr==ff:ff:70:00:a3:6a
Expression...
No. Time Source Destination Protocol Length Info
4419 443.453463 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4720 447.450434 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4751 447.974208 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4788 448.607641 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4802 449.052782 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4804 449.587714 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4814 449.974093 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4816 454.295248 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
Frame 4816: 28 bytes on wire (224 bits), 28 bytes captured (224 bits)
Bluetooth
Bluetooth HCI H4
Bluetooth HCI ACL Packet
Bluetooth L2CAP Protocol
Bluetooth Attribute Protocol
Opcode: Write Command (0x52)
Handle: 0x0006 (Unknown: Unknown)
Value: 01fe000053831000 0000ff 0050000000
0000 02 40 00 17 00 13 00 04 00 52 06 00 01 fe 00 00 .@..... .R.....
0010 53 83 10 00 00 00 ff 00 50 00 00 00 S..... P...
Found All 3 Colors


btsnoop_hci.2 pcap
bluetooth.addr==ff:ff:70:00:a3:6a
Expression...
No. Time Source Destination Protocol Length Info
4419 443.453463 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4720 447.450434 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4751 447.974208 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4788 448.607641 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4802 449.052782 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4804 449.587714 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4814 449.974093 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
4816 454.295248 localhost () ff:ff:70:00:a3:6a (SBT5007) ATT 28 Sent
Bluetooth HCI H4
Bluetooth HCI ACL Packet
Bluetooth L2CAP Protocol
Bluetooth Attribute Protocol
Opcode: Write Command
Handle: 0x0006 (Unknown: Unknown)
[Service UUID: Unknown (0x7777)]
[UUID: Unknown (0x8877)]
Value: 01fe00005383100000ff0050000000
0000 02 40 00 17 00 13 00 04 00 52 06 00 01 fe
0010 53 83 10 00 00 00 ff 00 50 00 00 00
The Payload
Note: The Service UUID Prefix
Note: The Characteristic UUID Prefix
The Color Section, of the Payload

Current Conclusions:

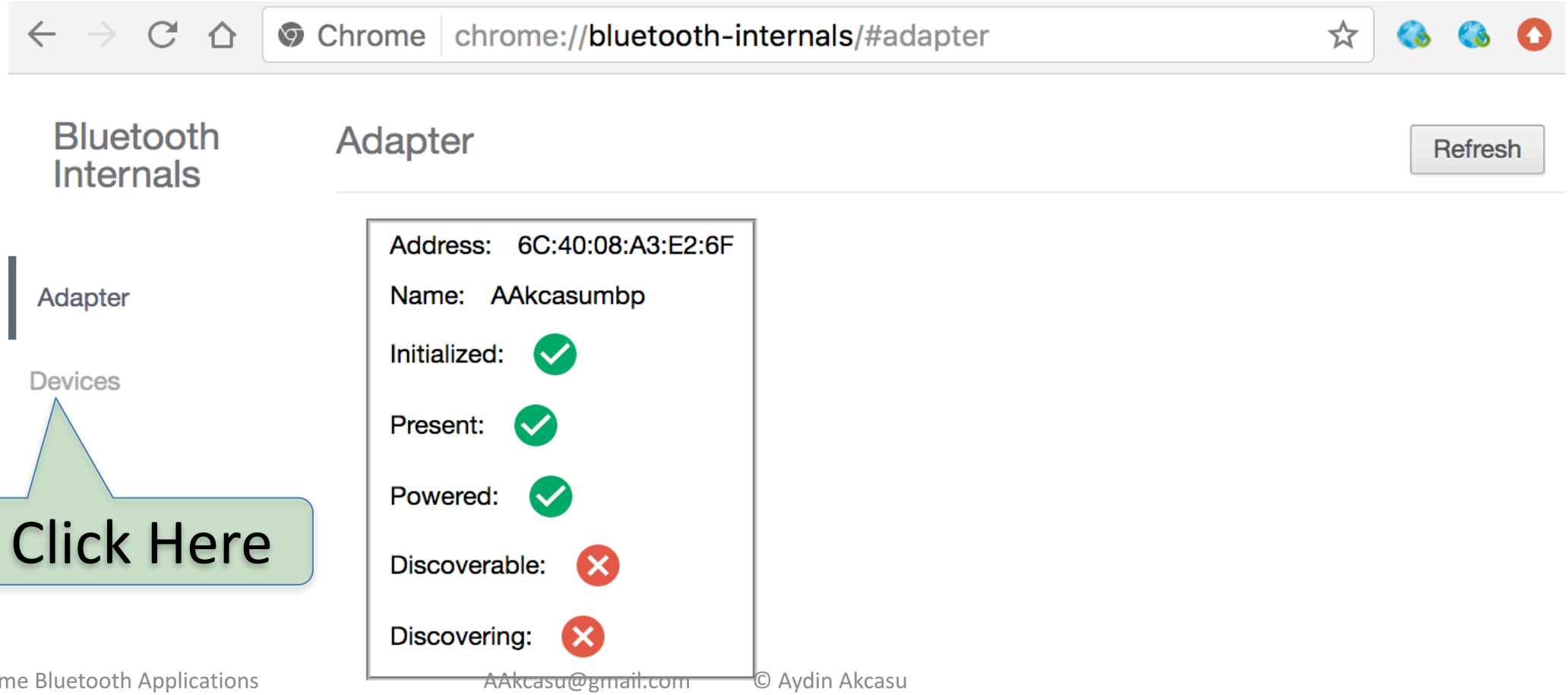
- **ServiceUUID:**
  - **0x7777…**
- **CharacteristicUUID:**
  - **0x 8877…**
- **Send Payload:**
  - **01fe000053831000xxyyzz0050000000**
  - Where xx,yy,zz each represent one of the following:
    - Red, Green, Blue (we don't know the order yet)



DISCOVER AND TEST SERVICE, CHARACTERISTIC AND PAYLOAD INFORMATION

Open Chromes' Internal Bluetooth Tools

- Open "chrome://bluetooth-internals" in Chrome



Bluetooth Internals

Adapter

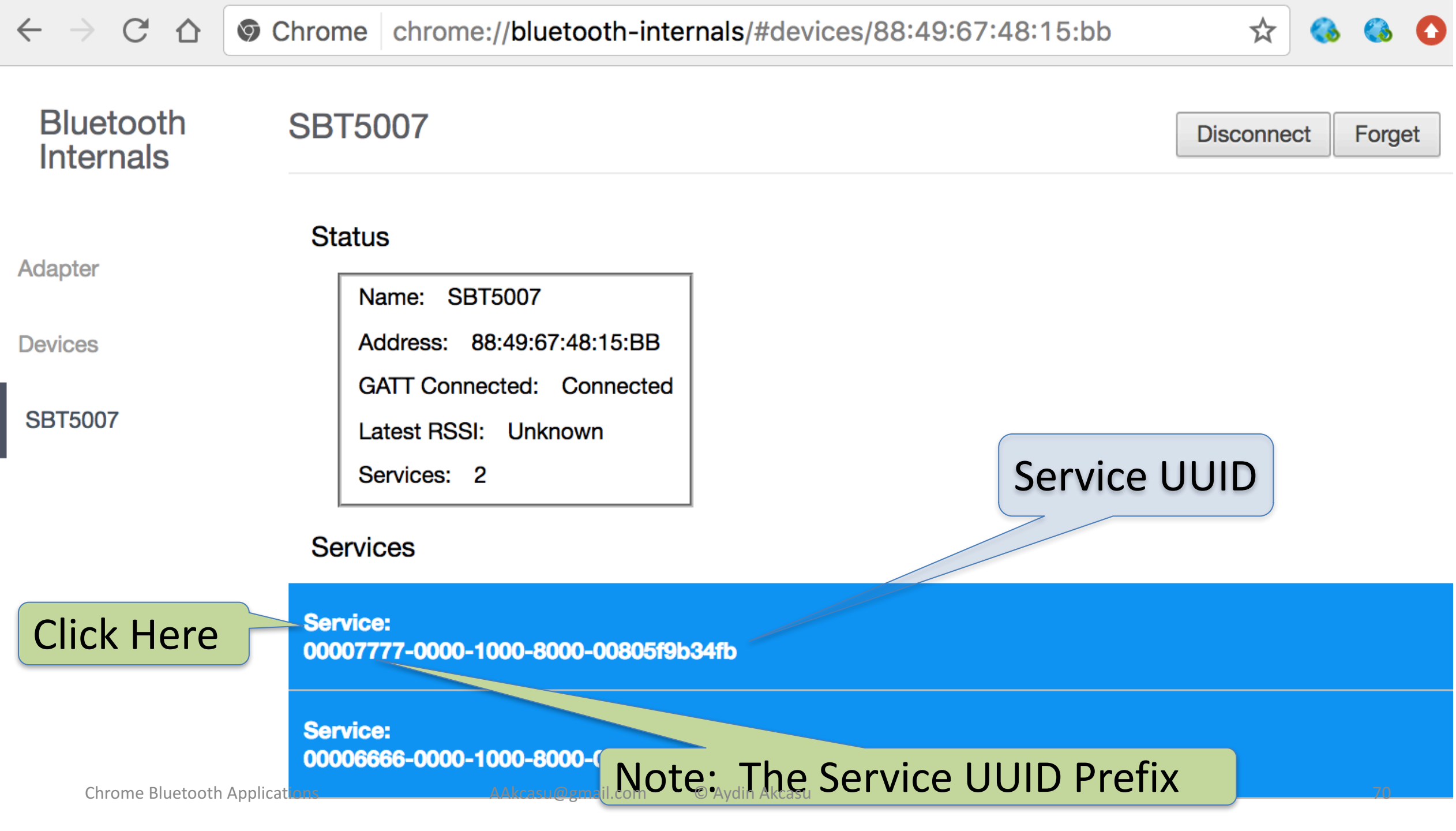
Devices

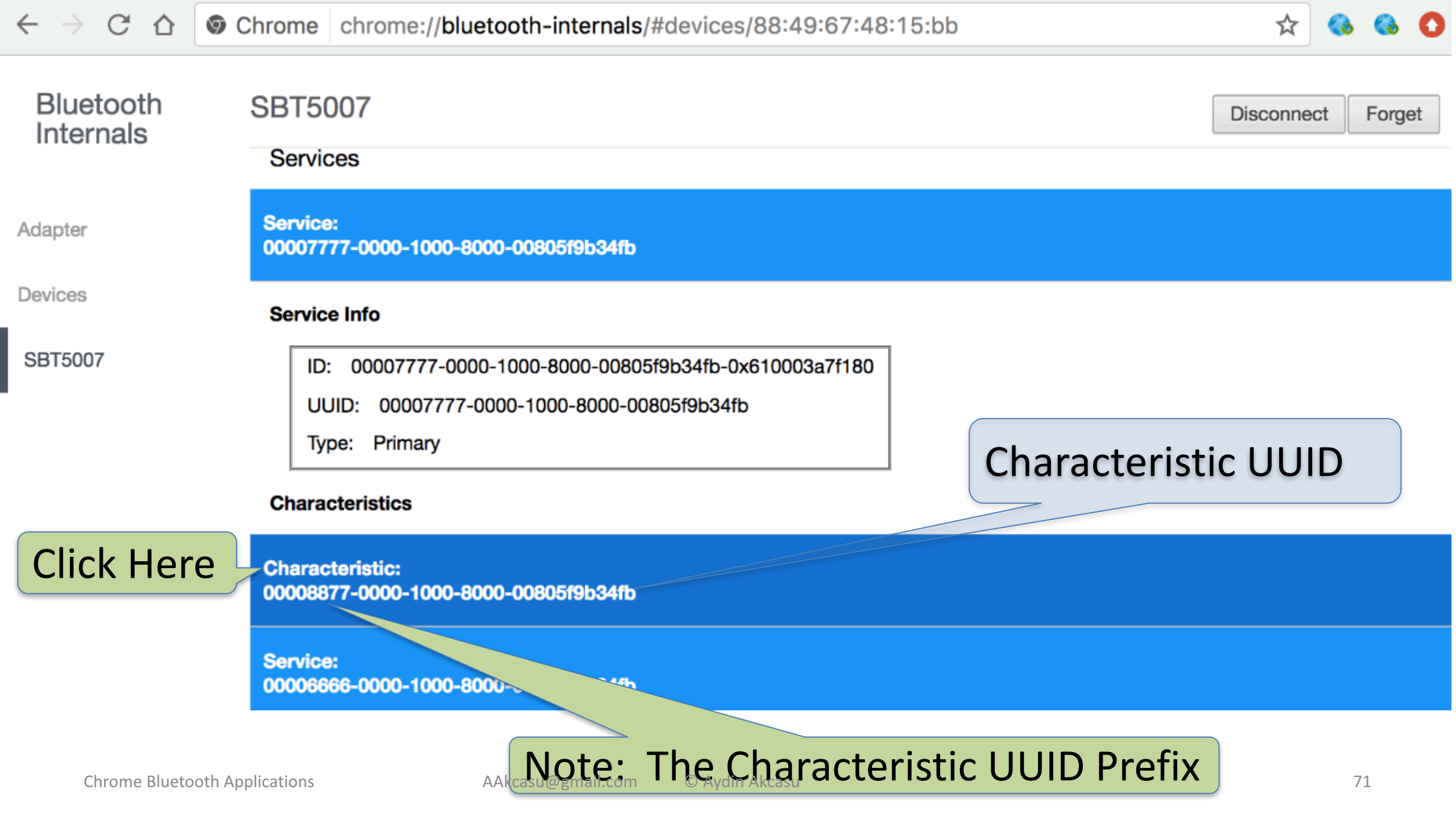
Devices

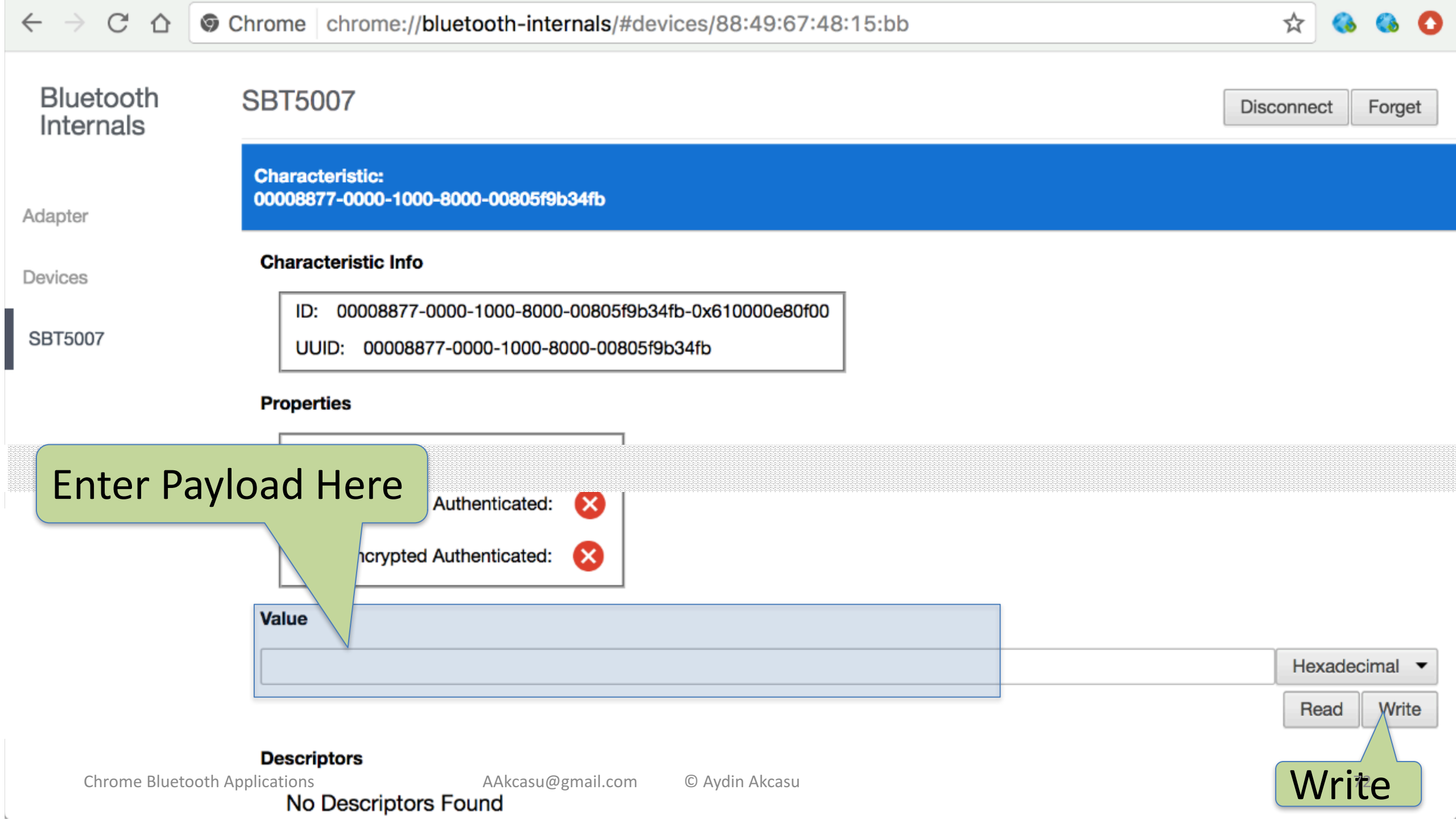
Click Here

Start Scan

Name	Address	Latest RSSI	Services	GATT Connection	
Unknown or Unsupported Device (74:92:F9:38:91:FD)	74:92:F9:38:91:FD	Unknown	Unknown	Not Connected	Inspect Forget
Unknown or Unsupported Device (A9:A5:90:36:B1:A0)	A9:A5:90:36:B1:A0	Unknown	Unknown	Not Connected	Inspect Forget
SBT5007	88:49:67:48:15:BB	Unknown	Unknown	Connected	Inspect Forget
SBT5007	AF:67:5E:97:EE:65	Unknown	Unknown	Not Connected	Inspect Forget
dogmeat tackpad 2	84:38:35:37:E4:E4	Unknown	Unknown	Not Connected	Inspect Forget
XT1028	EC:88:92:55:07:4C	Unknown	Unknown	Not Connected	Inspect Forget
Classic	C5:F4:F5:EF:47:5B	Unknown	Unknown	Not Connected	Inspect Forget
Q29_R	1C:52:16:00:D4:A6	Unknown	Unknown	Not Connected	Inspect Forget
Aydin Akcasu's Mouse	48:4B:AA:ED:68:C3	Unknown	Unknown	Not Connected	Inspect Forget


Chrome
chrome://bluetooth-internals/#devices/88:49:67:48:15:bb
Bluetooth Internals
SBT5007
Disconnect
Forget
Adapter
Devices
SBT5007
Status
Name: SBT5007
Address: 88:49:67:48:15:BB
GATT Connected: Connected
Latest RSSI: Unknown
Services: 2
Services
Service:
00007777-0000-1000-8000-00805f9b34fb
Service:
00006666-0000-1000-8000-
Service UUID
Click Here
Note: The Service UUID Prefix


Chrome
chrome://bluetooth-internals/#devices/88:49:67:48:15:bb
Bluetooth Internals
SBT5007
Disconnect
Forget
Services
Adapter
Devices
SBT5007
Service:
00007777-0000-1000-8000-00805f9b34fb
Service Info
ID: 00007777-0000-1000-8000-00805f9b34fb-0x610003a7f180
UUID: 00007777-0000-1000-8000-00805f9b34fb
Type: Primary
Characteristics
Characteristic UUID
Click Here
Characteristic:
00008877-0000-1000-8000-00805f9b34fb
Service:
00006666-0000-1000-8000
Note: The Characteristic UUID Prefix


Chrome
chrome://bluetooth-internals/#devices/88:49:67:48:15:bb
Bluetooth Internals
SBT5007
Disconnect
Forget
Adapter
Devices
SBT5007
Characteristic:
00008877-0000-1000-8000-00805f9b34fb
Characteristic Info
ID: 00008877-0000-1000-8000-00805f9b34fb-0x610000e80f00
UUID: 00008877-0000-1000-8000-00805f9b34fb
Properties
Authenticated:
ncrypted Authenticated:
Enter Payload Here
Value
Hexadecimal
Read
Write
Write
Descriptors
No Descriptors Found

1

Chrome chrome://bluetooth-internals/#devices/88:49:67:48:15:bb

Test with these values, and note the resulting colors:

A: 0x01fe000053831000000ff0050000000

B: 0x01fe00005383100000ff000050000000

C: 0x01fe0000538310000ff0000050000000

Disconnect Forget

Devices

SBT5007

-8000-00805f9b34fb-0x610000e80f00

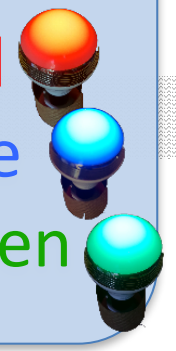
4

Findings from the bulb color:

A: 0x01fe000053831000**0000ff**0050000000 - Red

B: 0x01fe000053831000**00ff00**0050000000 - Blue

C: 0x01fe000053831000**ff0000**0050000000 - Green



Value

2

0x01fe000053831000000ff0050000000

Hexadecimal

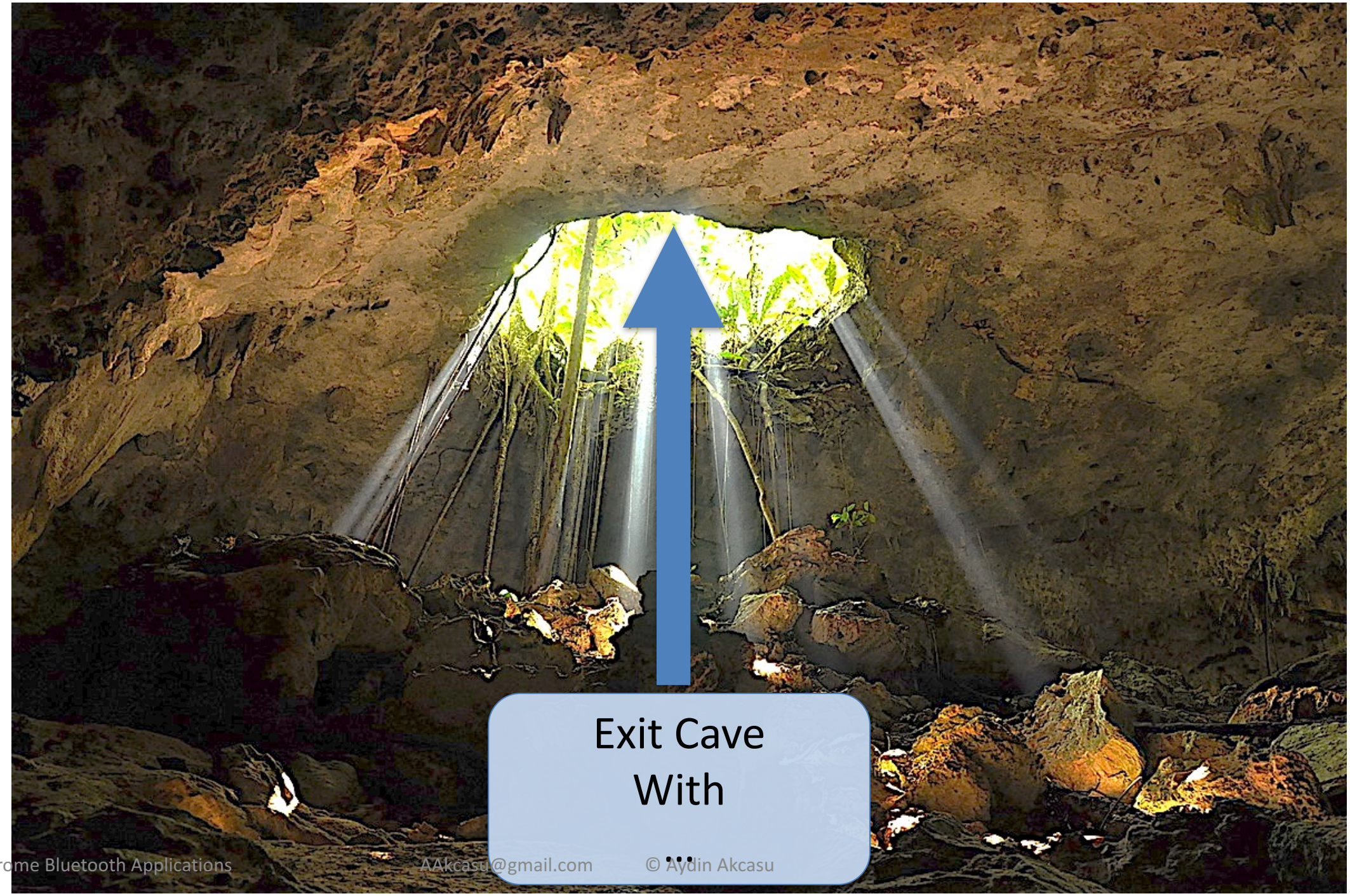
Read Write

5

0x01fe000053831000GGBBRR0050000000 - Summary

3 Write

No Descriptors Found


Exit Cave
With
...

Conclusions:

- **ServiceUUID:**
  - **00007777-0000-1000-8000-00805f9b34fb**
- **CharacteristicUUID:**
  - **00008877-0000-1000-8000-00805f9b34fb**
- **Send Payload:**
  - **01fe000053831000GGBBRR0050000000**

CREATE THE BLUETOOTH BULB WEB APP

```
6       let serviceUuid = '00007777-0000-1000-8000-00805f9b34fb';
7       let characteristicUuid = '00008877-0000-1000-8000-00805f9b34fb';
8
9       navigator.bluetooth.requestDevice
10          ({…
13          })
14          .then(device => {…
17          })
18          .then(server => { return server.getPrimaryService(serviceUuid); }
19          .then(service => { return service.getCharacteristic(characteristi
20
21          .then(characteristic => {   // Save characteristic…
24          })
25          .then(characteristic => {   // Set colors…
28          })
29          .catch(error => {   // Handle Errors…
31          });
32  }
```

```
24          .then(service => { return service.getCharacteristic(characteristicUuid); })
25
26          .then(characteristic => {   // Save characteristic…
29          })
30          .then(characteristic => {   // Set colors
31              lightBulb_traffic(characteristic);
32              return characteristic;
33          })

50  function lightBulb_traffic(characteristic) {   // Set a traffic light pattern
51      characteristic = characteristic || lightBulb_C
52
53      var send = getPayload(0x00, 0xff, 0x00);    // Green
54      characteristic.writeValue(send);
55      sleep(2000);
56
```

Function Call

Get the Payload

Write this value to the characteristic

```
39  function getPayload(r, g, b) {   // Create the payload
40      var data = [
41          0x01, 0xfe, 0x00, 0x00, 0x53, 0x83, 0x10, 0x00,
42          g, // Green
43          b, // Blue
44          r, // Red
45          0x00, 0x50, 0x00, 0x00, 0x00
46      ];
47      return Uint8Array.from(data);
```

1

2

Remember this?

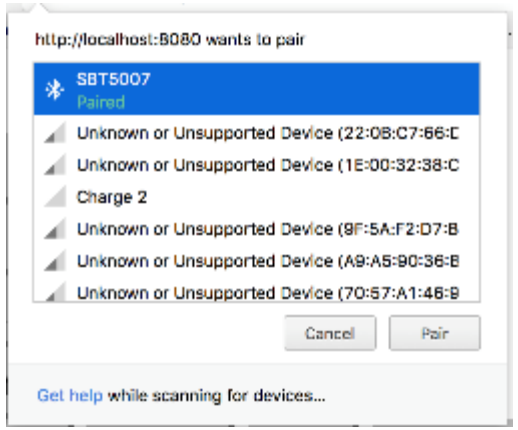
0x01fe000053831000GGBBRR0050000000 - Summary

3

0x01 fe 00 00 53 83 10 00 GG BB RR 00 50 00 00 00

Results

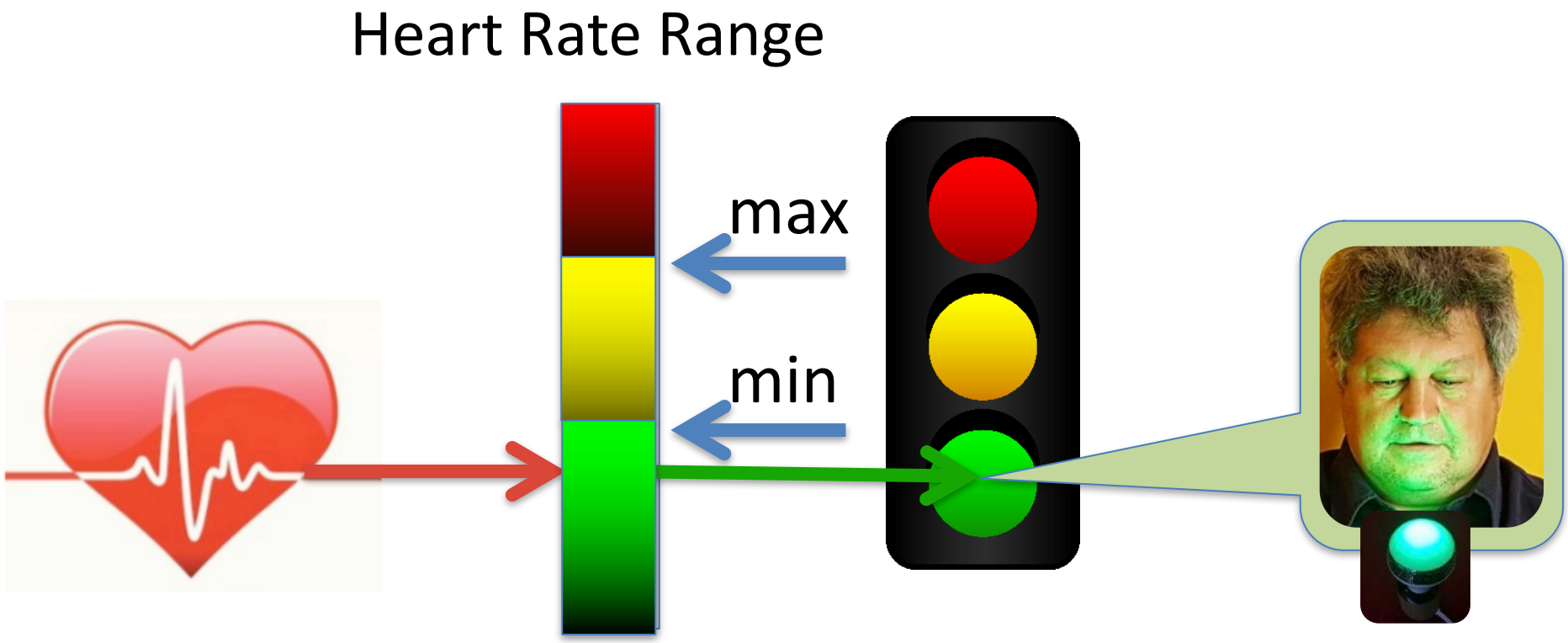
Light Bulb | Traffic | Red | Yellow | Green | Blue | Stop



+

PUTTING IT ALL TOGETHER WITH A “STRESS DISPLAY”

“Stress Display” Process



THE DEMO

Chrome Bluetooth Demo:

Basic:

Device Information | Battery Information | % |

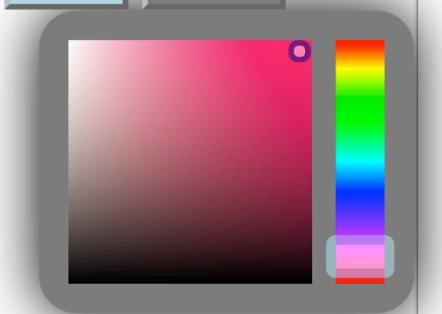
Heart Rate:

Start | 0 | Stop

Light Bulb:

Start | Traffic | Red | Yellow | Green | Blue | Black

Stop | RGB: (0xf2,0x0c,0x6a)



Stress Display:

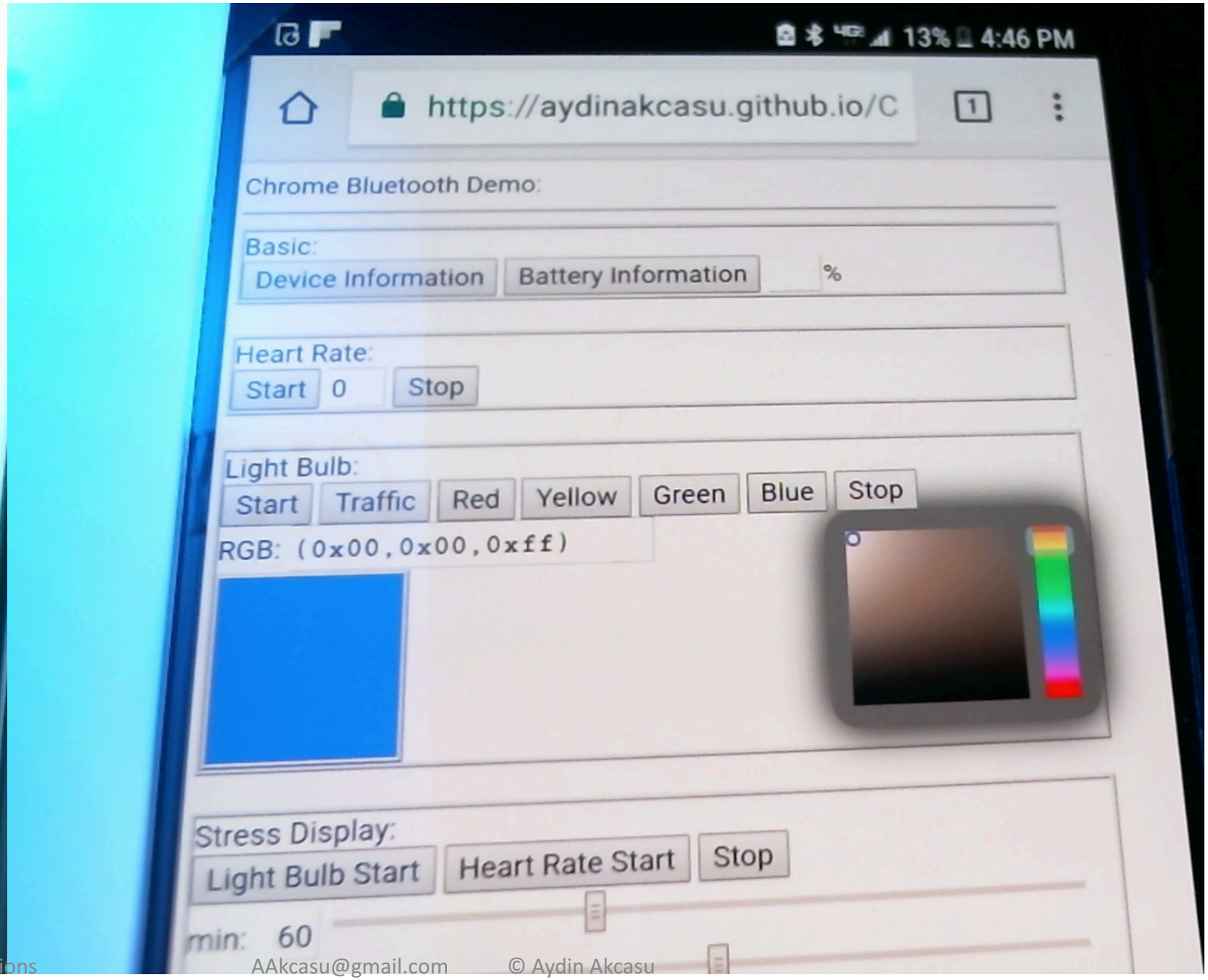
Light Bulb Start | Heart Rate Start | Stop

min: 60

max: 70

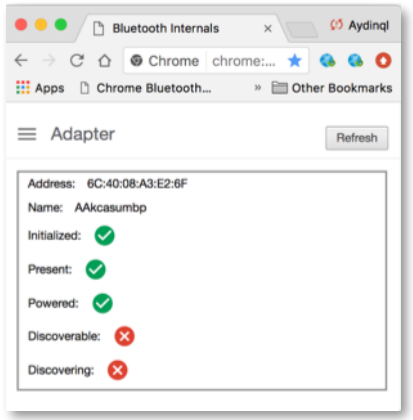
Results:

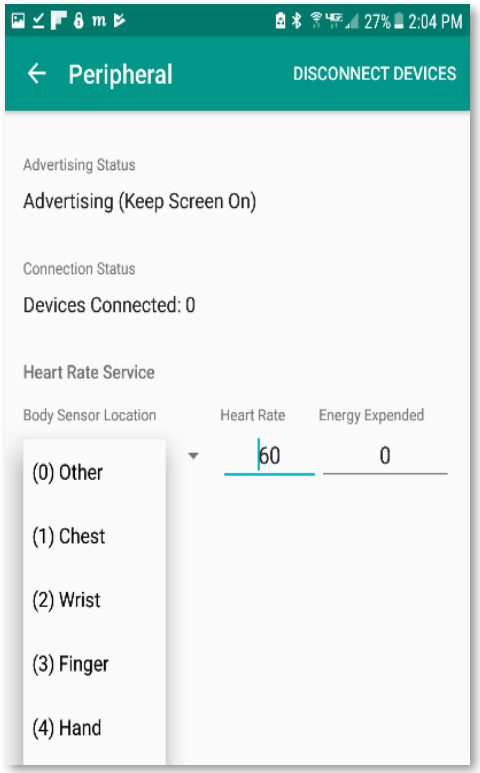
```
72|------------------------------>
72|------------------------------>
72|------------------------------>
```


13% 4:46 PM
https://aydinakcasu.github.io/C
1
Chrome Bluetooth Demo:
Basic:
Device Information
Battery Information
%
Heart Rate:
Start
0
Stop
Light Bulb:
Start
Traffic
Red
Yellow
Green
Blue
Stop
RGB: (0x00,0x00,0xff)
Stress Display:
Light Bulb Start
Heart Rate Start
Stop
min:
60

Software

- **Get Bluetooth information using Chrome:**
  - chrome://bluetooth-internals
- **Wireshark (to analyze packets)**
  - https://www.wireshark.org/
- **Bluetooth Simulator App:**
  - BLE Peripheral Simulator App
  - Google Play Store





goo.gl/VnyPdX

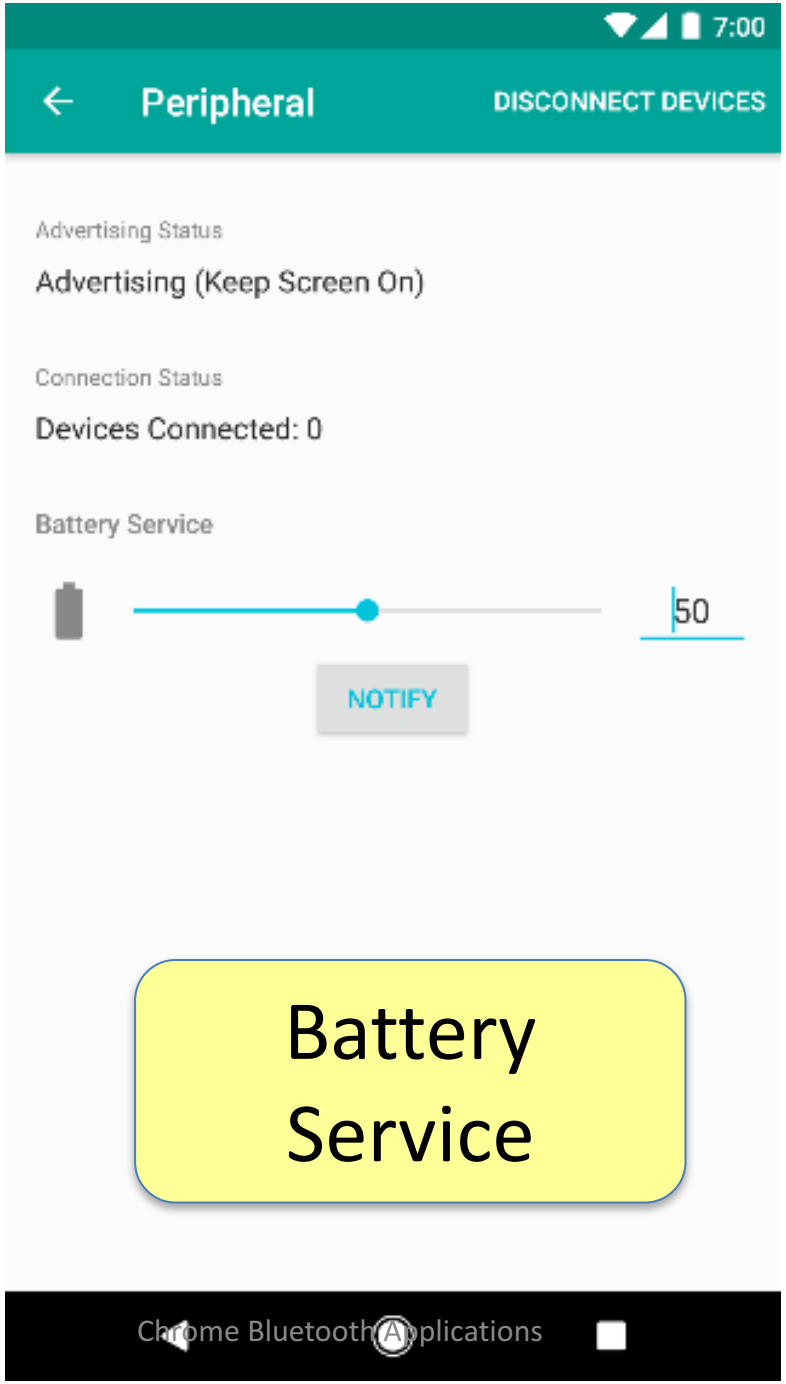
BLE Peripheral Simulator

WebBluetoothCG Libraries & Demo

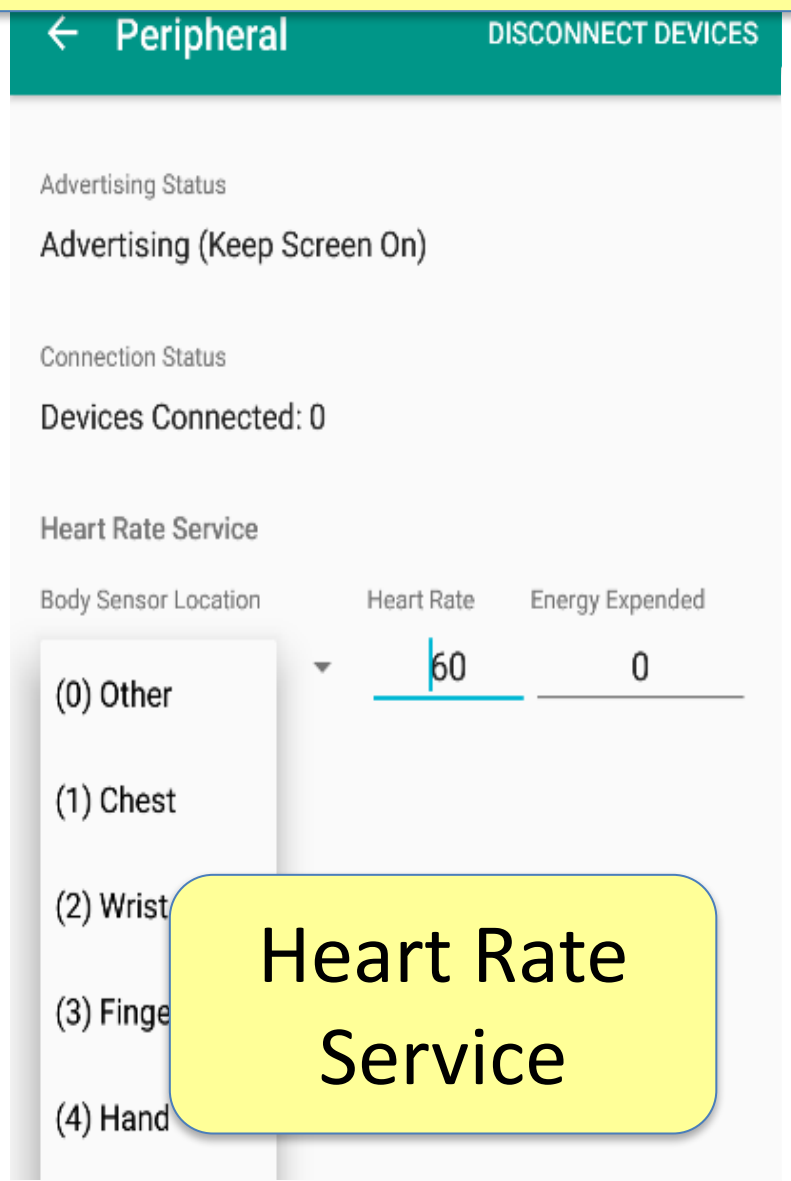
E Everyone

CONNECT USING A BLUETOOTH SIMULATOR

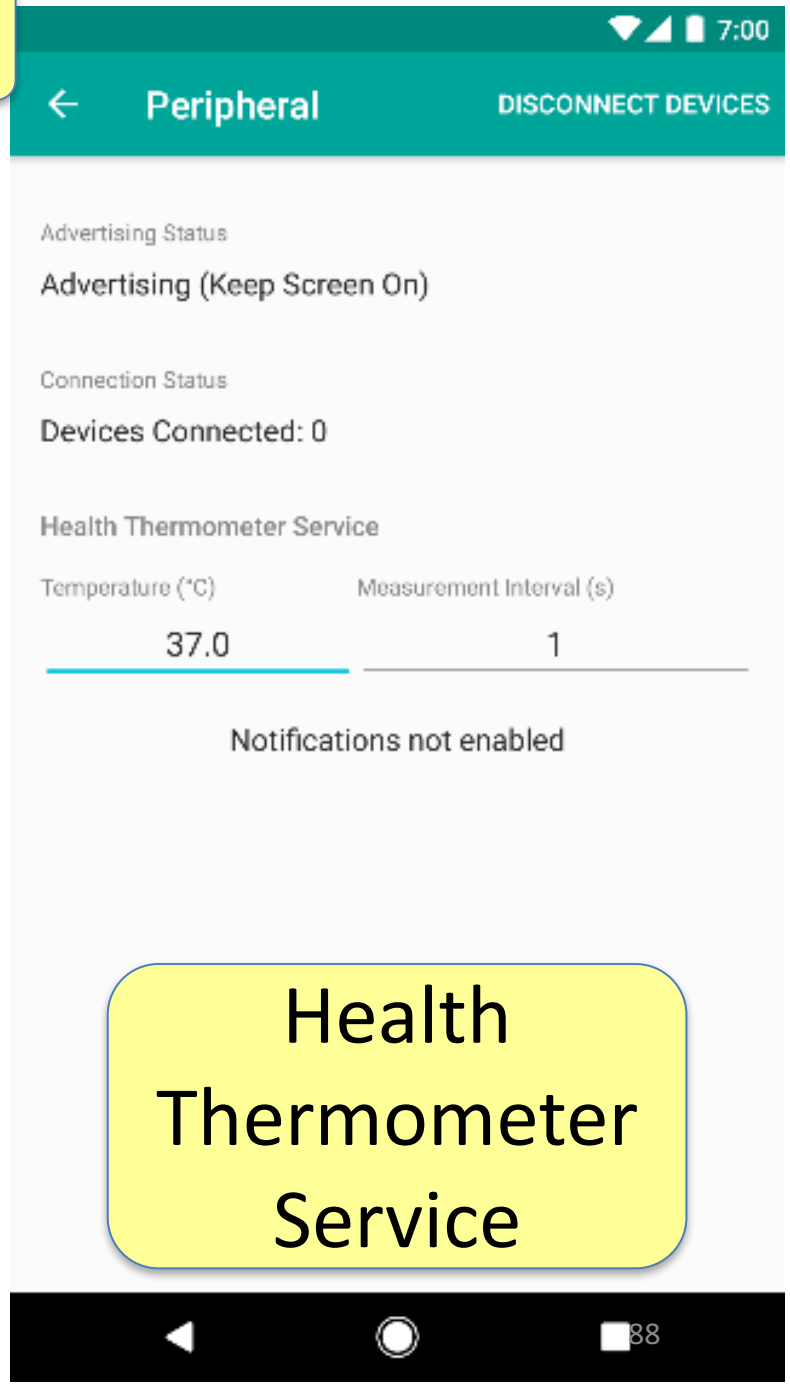
BLE Peripheral Simulator



Battery Service



Heart Rate Service



Health Thermometer Service

Helpful Links:

- **Web Bluetooth (100 Days of Google Dev)**
  - https://www.youtube.com/watch?v=I3obFcCw8mk
- **Interact with Bluetooth devices on the Web**
  - https://developers.google.com/web/updates/2015/07/interact-with-ble-devices-on-the-web
- **Reverse Engineering a Bluetooth Lightbulb**
  - https://medium.com/@urish/reverse-engineering-a-bluetooth-lightbulb-56580fcb7546

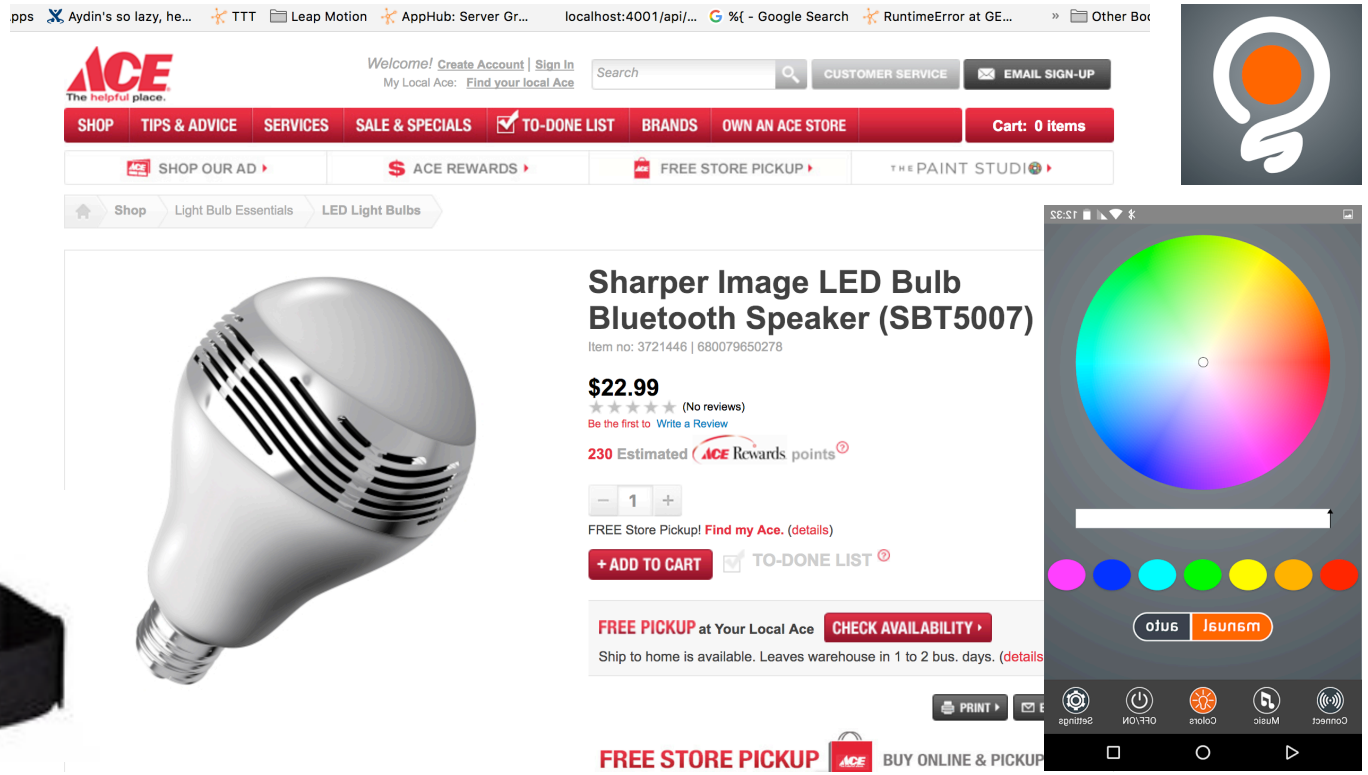
goo.gl/VnyPdX

Hardware Used:

Sharper Image LED Bulb Bluetooth Speaker (SBT5007)

- *Ace Hardware:* ***$22.99***
- *Menards – Online ($11)*

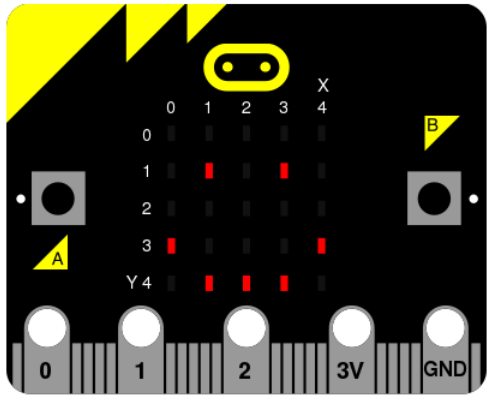
- **Crane Heart Rate Monitor**
  - *About $15 at Aldi*
  - *Just about anywhere ($20+)*

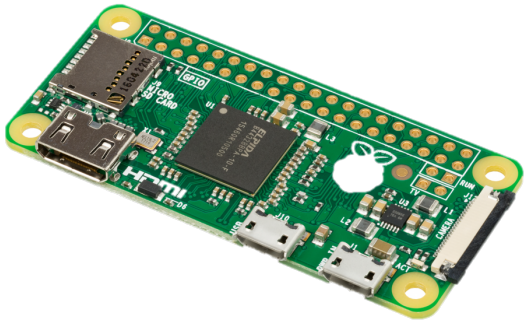


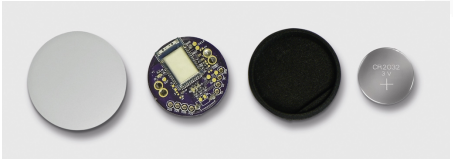
goo.gl/VnyPdX

Other Hardware for Bluetooth

- Micro:bit
- Raspberry PI
- BB-8 (Star Wars)
- Drone (Parrot Mini Drone Rolling Spider)
- Thermometer
- Puck.js







goo.gl/VnyPdX

Demo and Code

- **Live Demo:**
  - https://AydinAkcasu.github.io/ChromeBluetooth/
  - goo.gl/b3Wzv5
- **Source Code:**
  - https://github.com/AydinAkcasu/ChromeBluetooth
  - goo.gl/VnyPdX

goo.gl/VnyPdX

Aydin Akcasu

Email: AydinAkcasu@QuickenLoans.com

AAkcasu@gmail.com

LinkedIn: Linkedin.com/in/aydin-akcasu-51063

Twitter: @AAkcasu

Trip Info: RidinWithAydin.com

goo.gl/VnyPdX