Understanding the BLEEP-ing Wildlife and Identifying their Ble-S

Paul A. Wortman, PhD
Mauddib28

May 18, 2025

Table of contents

Whoami

- PhD
- Bluetooth Security Researcher
- Research Scientist

Contact Info:
https://www.linkedin.com/in/dr-paul-wortman-37200571/

Whatisthis?

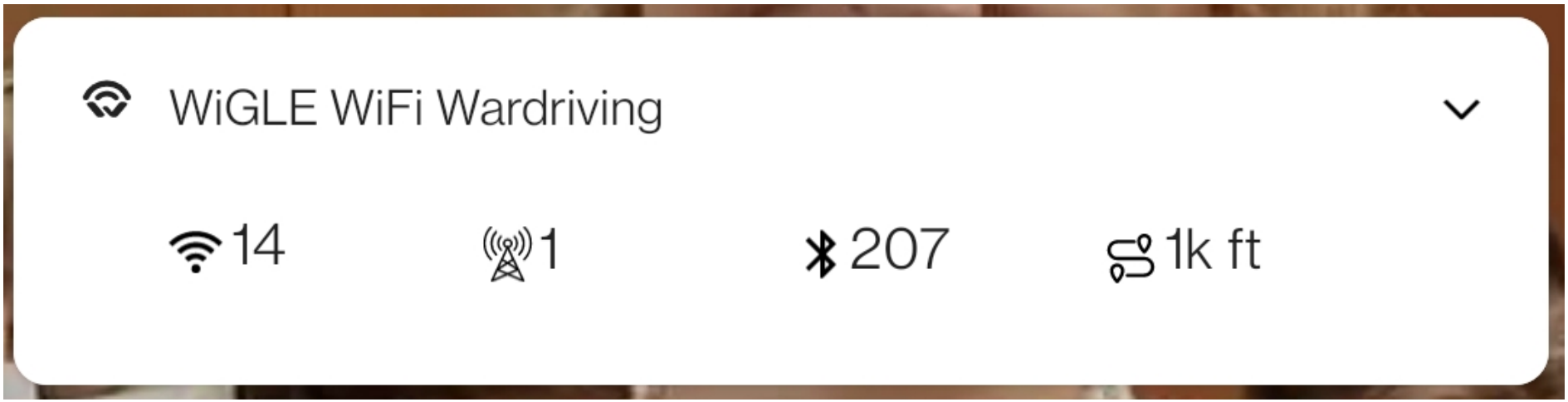


Figure 1: Wiggle War Drive - Landing Strip

Intent of Research - Present and Counting

BLEEP:

- Swiss-army knife tool
- Map the existing Bluetooth landscape
- Retain low-level granularity for I/O

Observations:

- Establish trends in Bluetooth deployments
- Obtain swath of information presented by BLE devices over time
- Improve base-rock of knowledge for Cyber Security Community and Researchers

BR/ED vs BLE

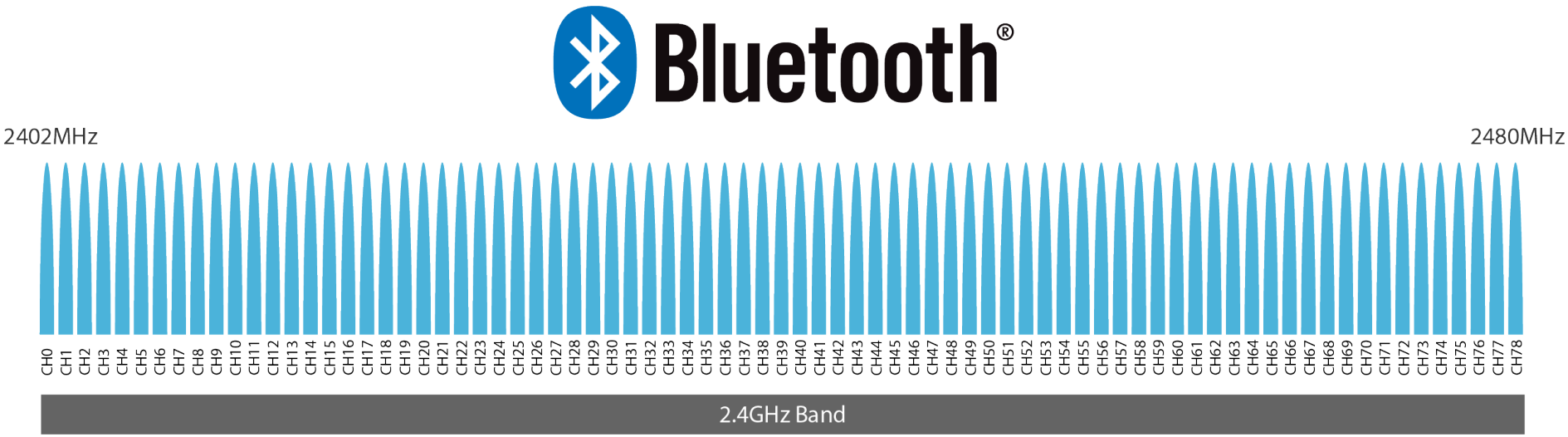


Figure 2: Bluetooth Classic Spectrum

- 79 number of (pairing) channels
- Freq. hoping to minimize interference
  - Defense in depth
- Larger power requirements minimize effectiveness for embedded systems

BR/ED vs BLE

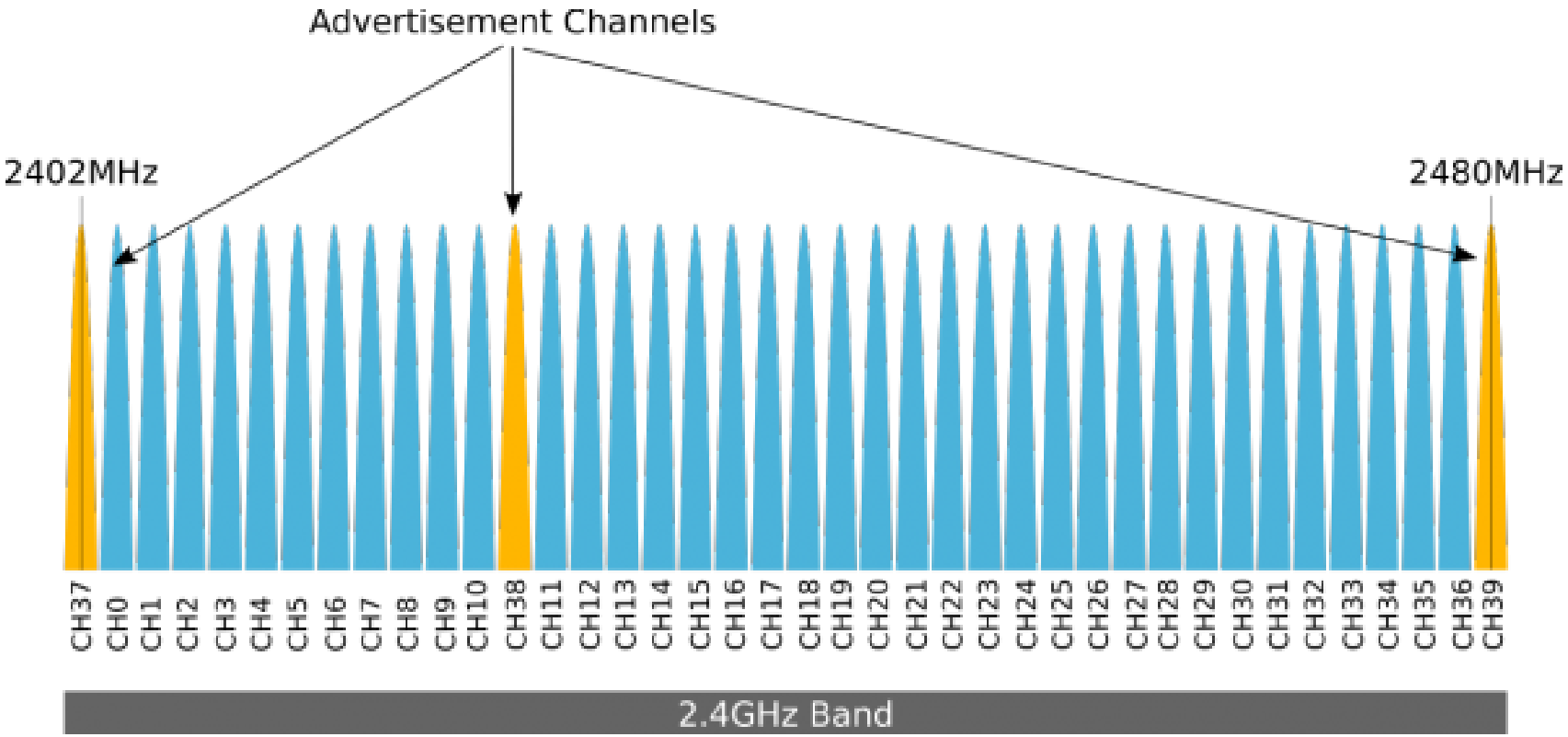


Figure 3: Bluetooth Low Energy Spectrum

- Three pairing channels; simplified sniffing of pairing
- Post connection return to classic frequency hopping
  - Capture of handshake provides easier eavesdropping
- Lower power requirements; ideal for embedded systems

BLE - Must Know Basics

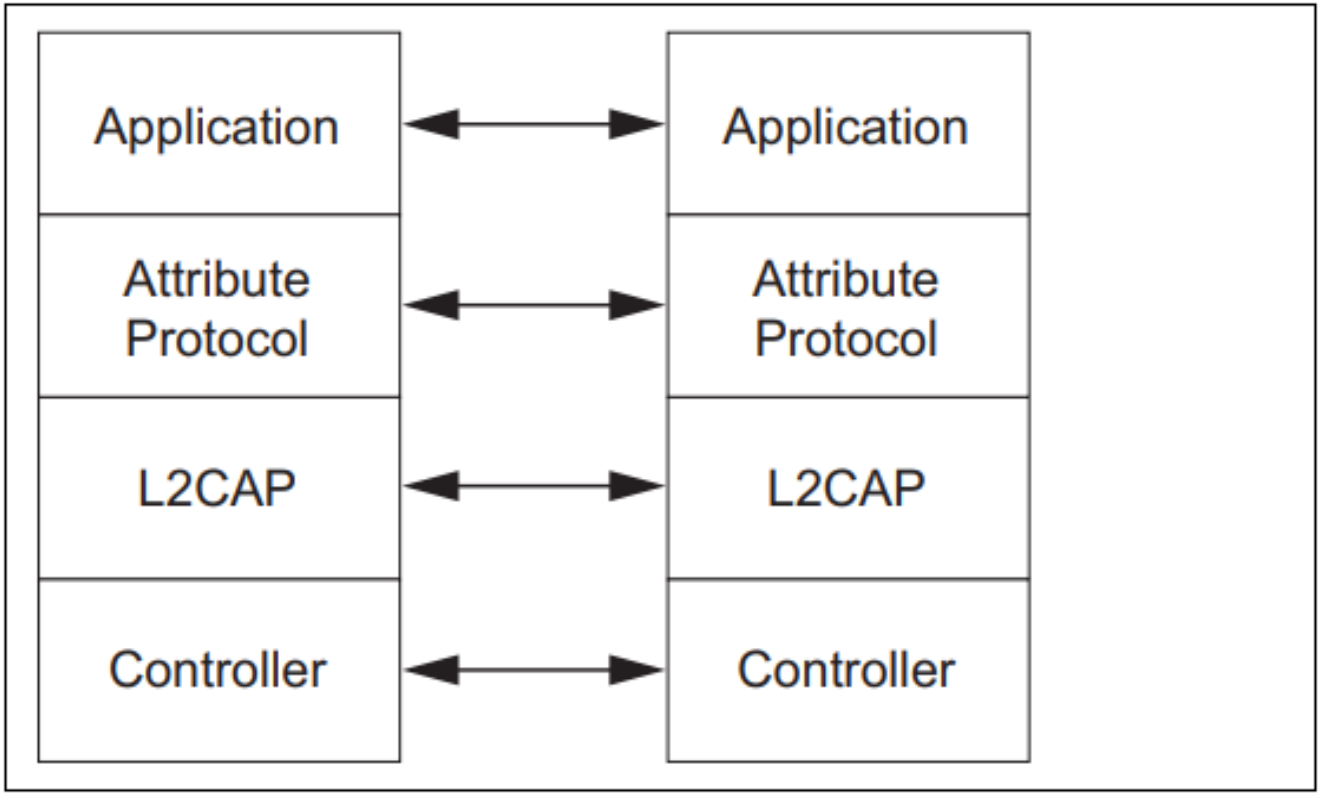


Figure 4: Protocol model [**?**]

- GATT Server
  - Inability to “change” a GATT server once initialized
  - Flavor differences; Arduino will not allow writing to Descriptors

BLE - Must Know Basics - High-level BLE Structure

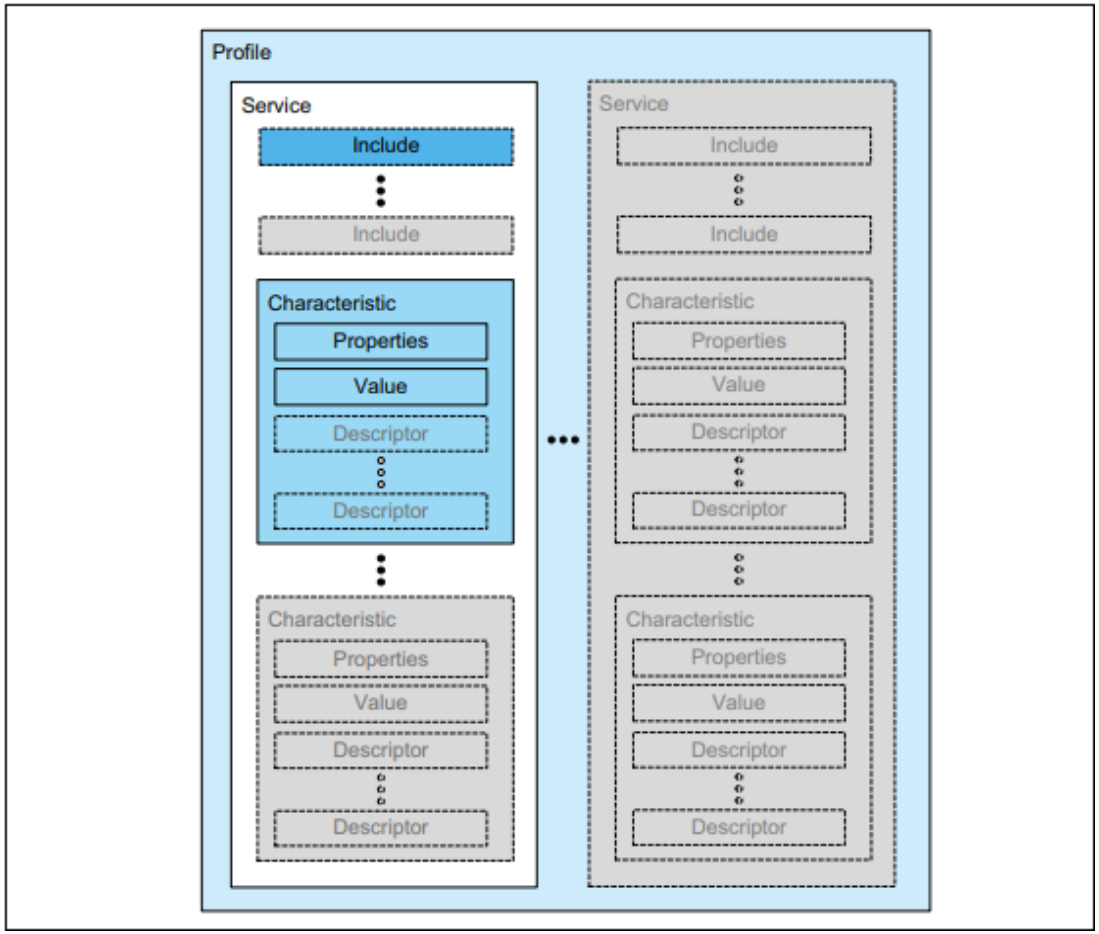


Figure 5: GATT-Based Profile hierarchy [?]

- Device, Services, Characteristics, Descriptors
- Characteristics have to be read once to populate data
  - Second read allows determining the data

Operational Model

BT SIG LE Primer - BLE SM

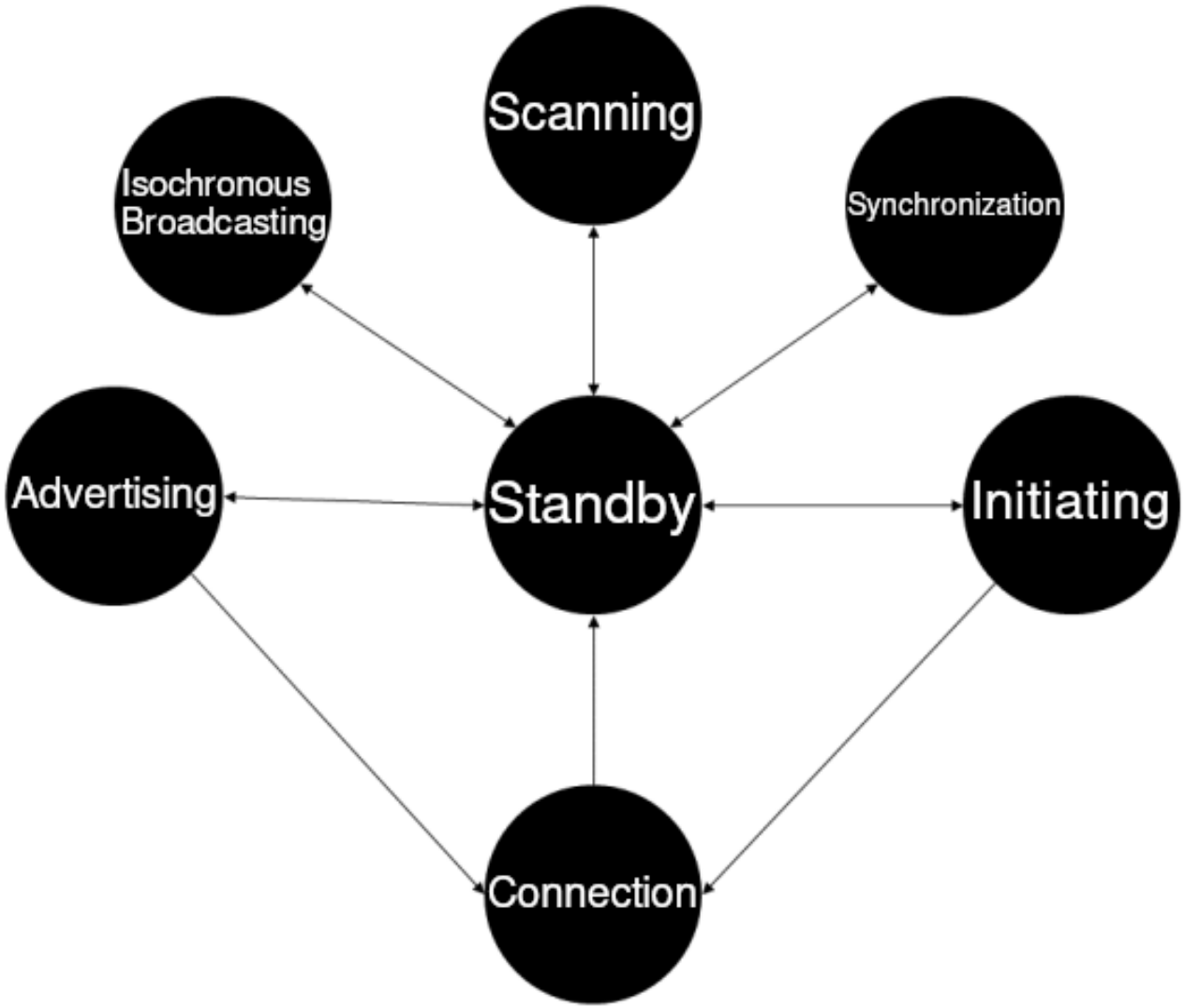


Figure 9 - The Link Layer State Machine

BLE SM - Constraints

Embedded Bluetooth devices essentially run under the following constraints:

- BLE device acts as a single processor device
- Multiplexing is the “workaround” for parallelism / threading
- Precognition of what is being searched for

BLE SM - Specifics

Method of Examining BLE Devices as a State Machine:

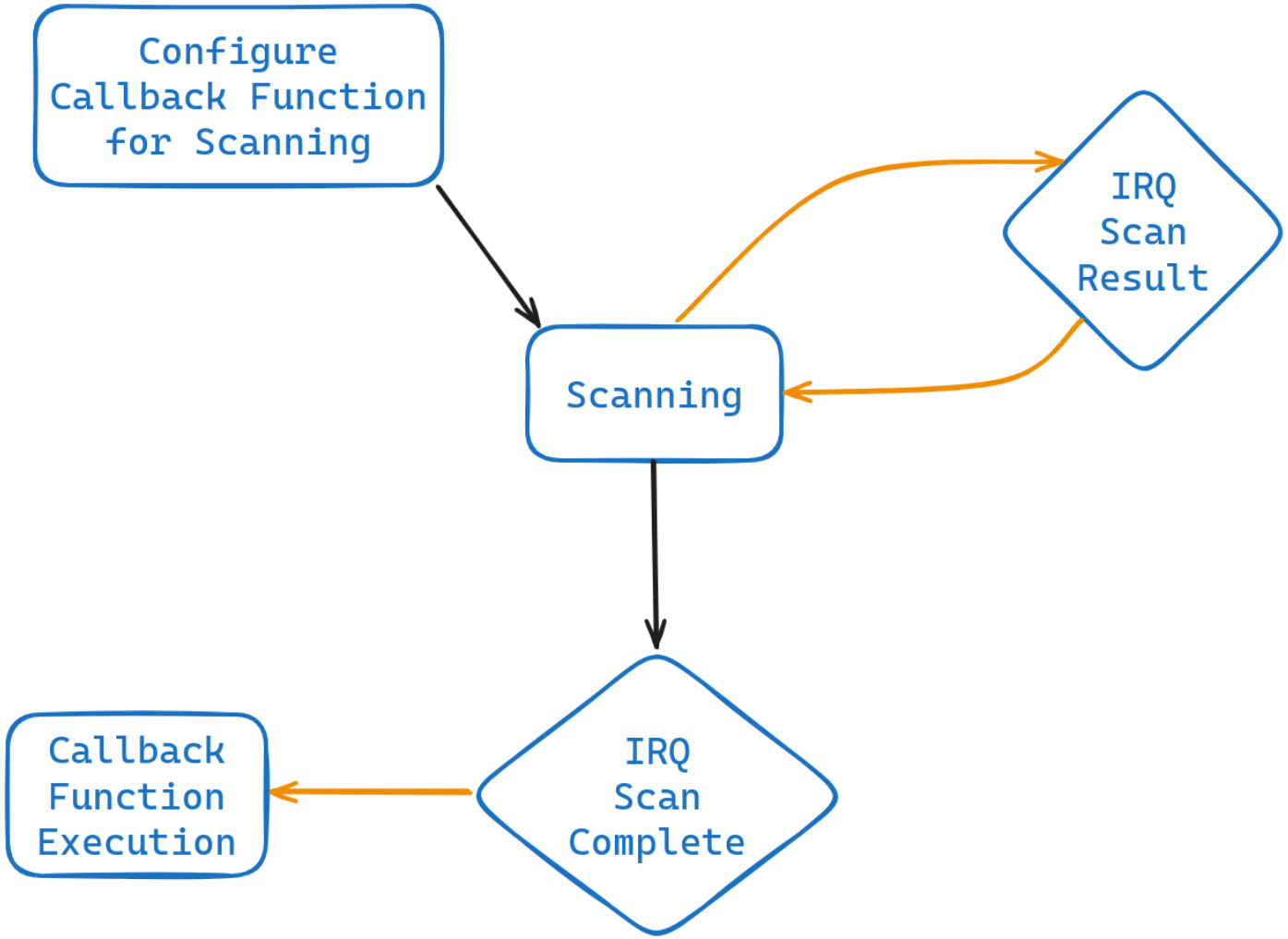
- Tasks must be performed in a specific order
- Too much nesting leads to stalling/loss
- Memory access is a tricky process....
  - May require creating copies of data
  - Leads to potential resource limits / hanging

Note: There is a notable difference between a *Central* and *Peripheral* device

- E.g. GATTC, GATTS
- Negligible for higher level review

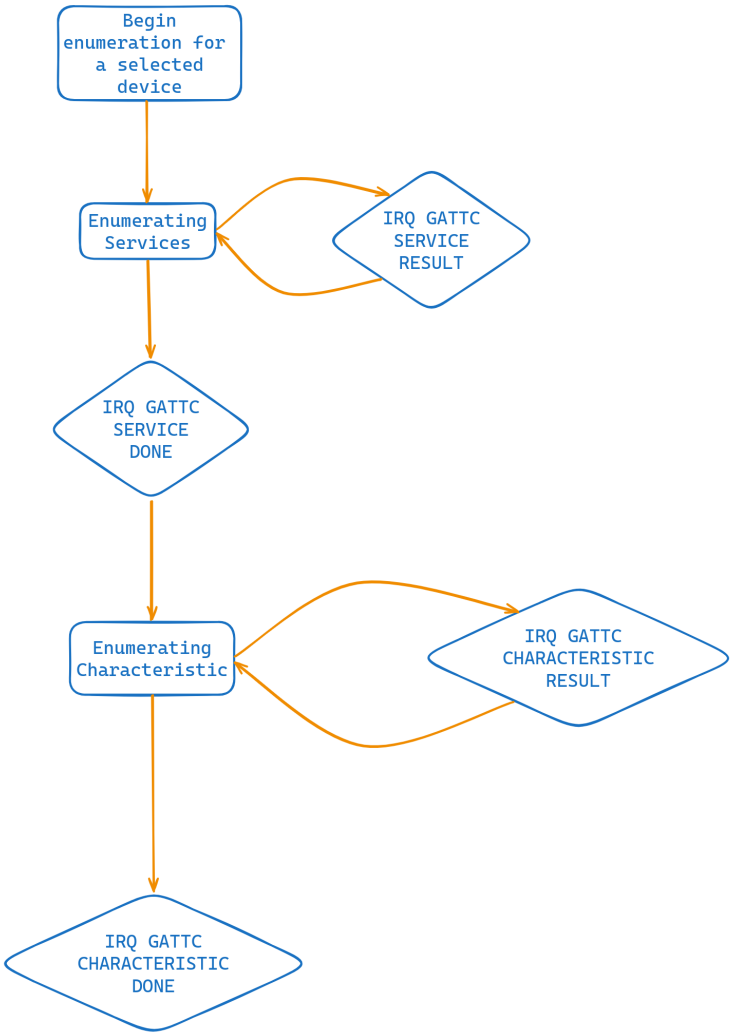
BLE SM - Scanning

Scanning State Machine:



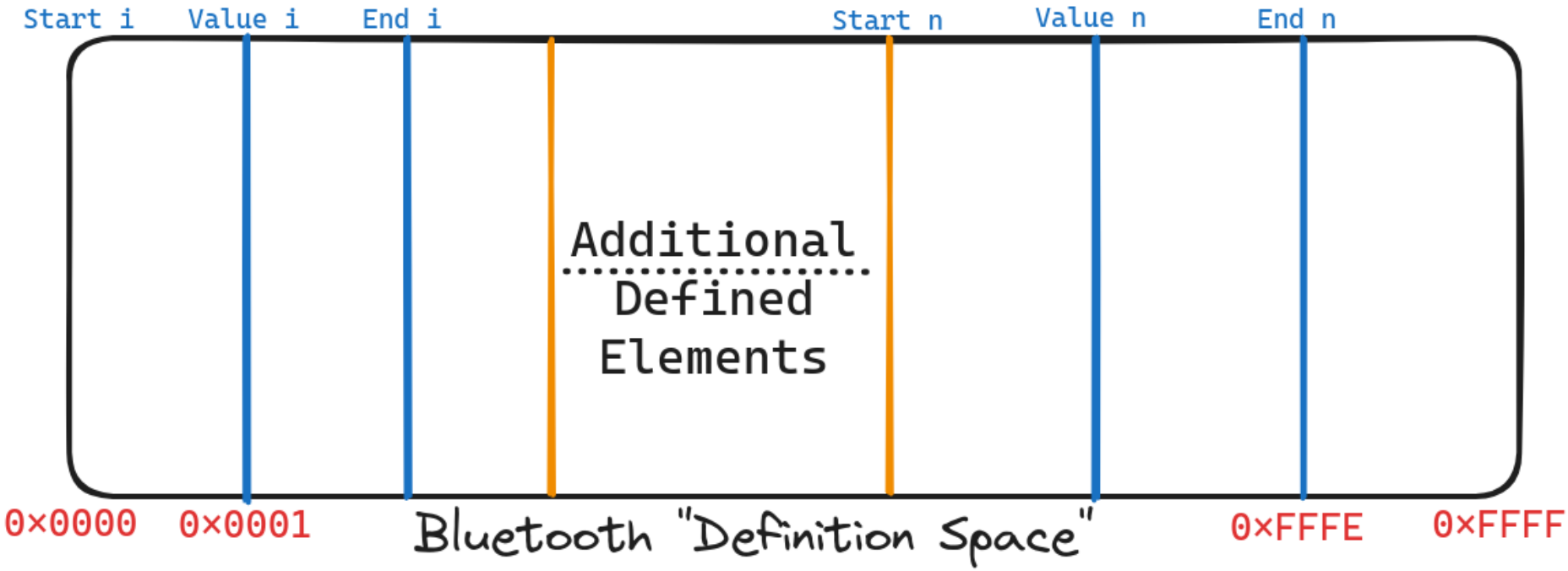
BLE SM - Enumeration

Enumeration State Machine:



BLE SM - Memories.....

BUT WAIT!! How do we visualize the mystery device???



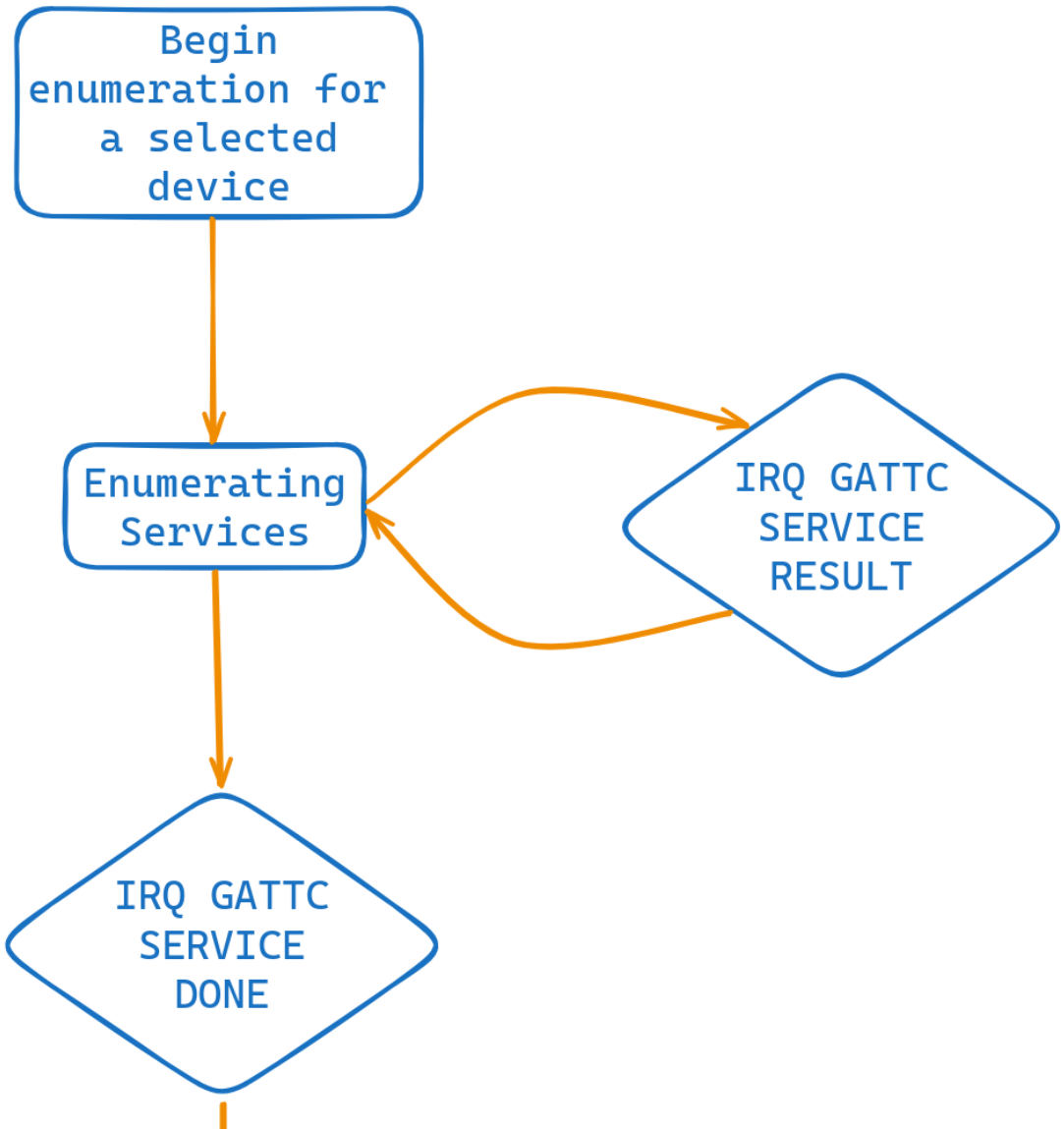
Handles Handles Everywhere

Handles vs. UUIDs vs. Short UUIDs Multiple ways of referencing the same Service/Characteristic/Descriptor:

- UUID
  - Short (0x5678)
  - Long (12345678-0000-1111-2222-4444-55555)
- Handles
  - Start, End, Value
  - Note: Value is within the Start - End range
- Handles are a representation of the UUIDs; although Handles can appear differently between CLI tools and D-Bus structure returns

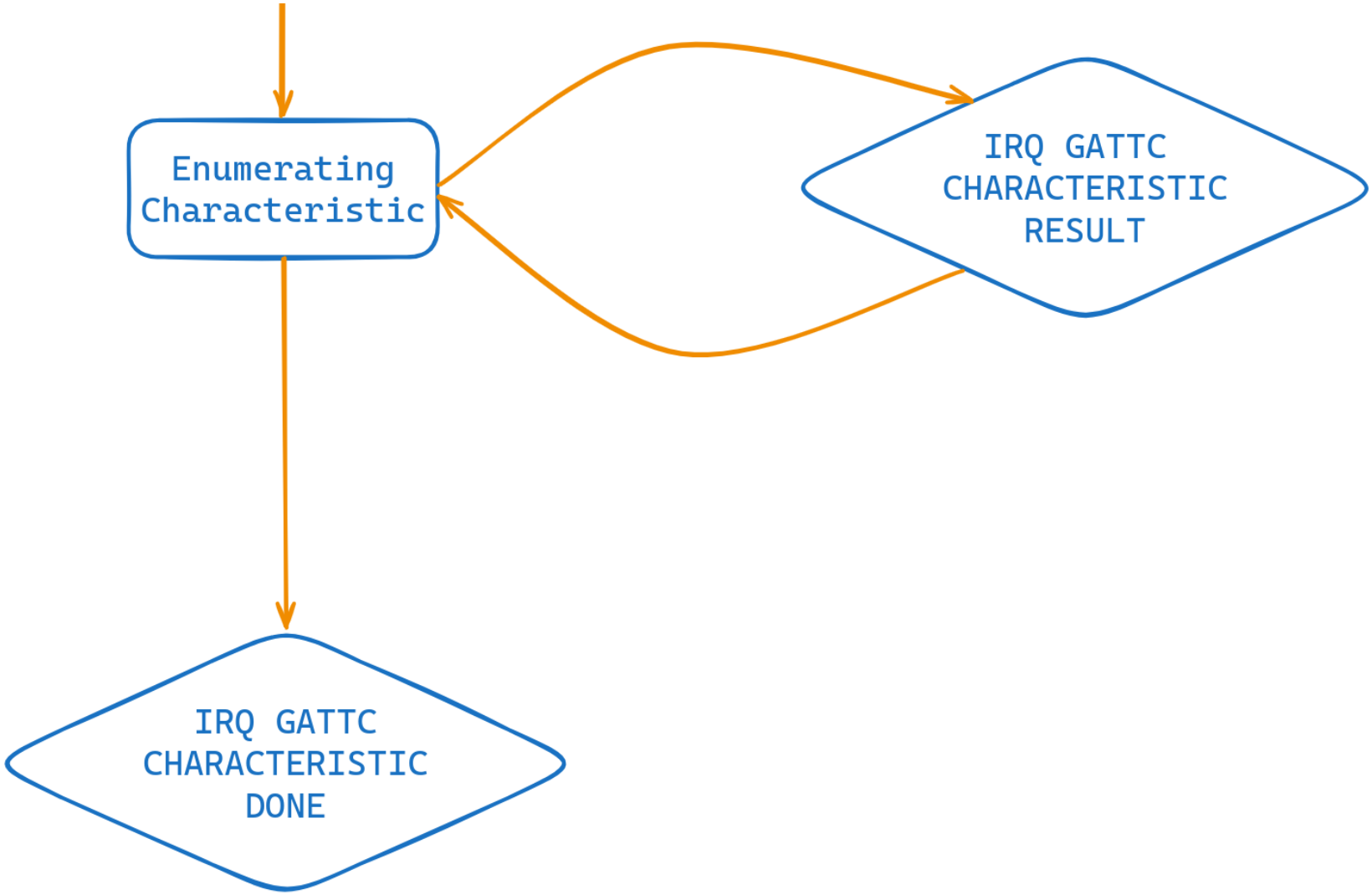
BLE SM - Enumeration - Services

Enumeration of Services:

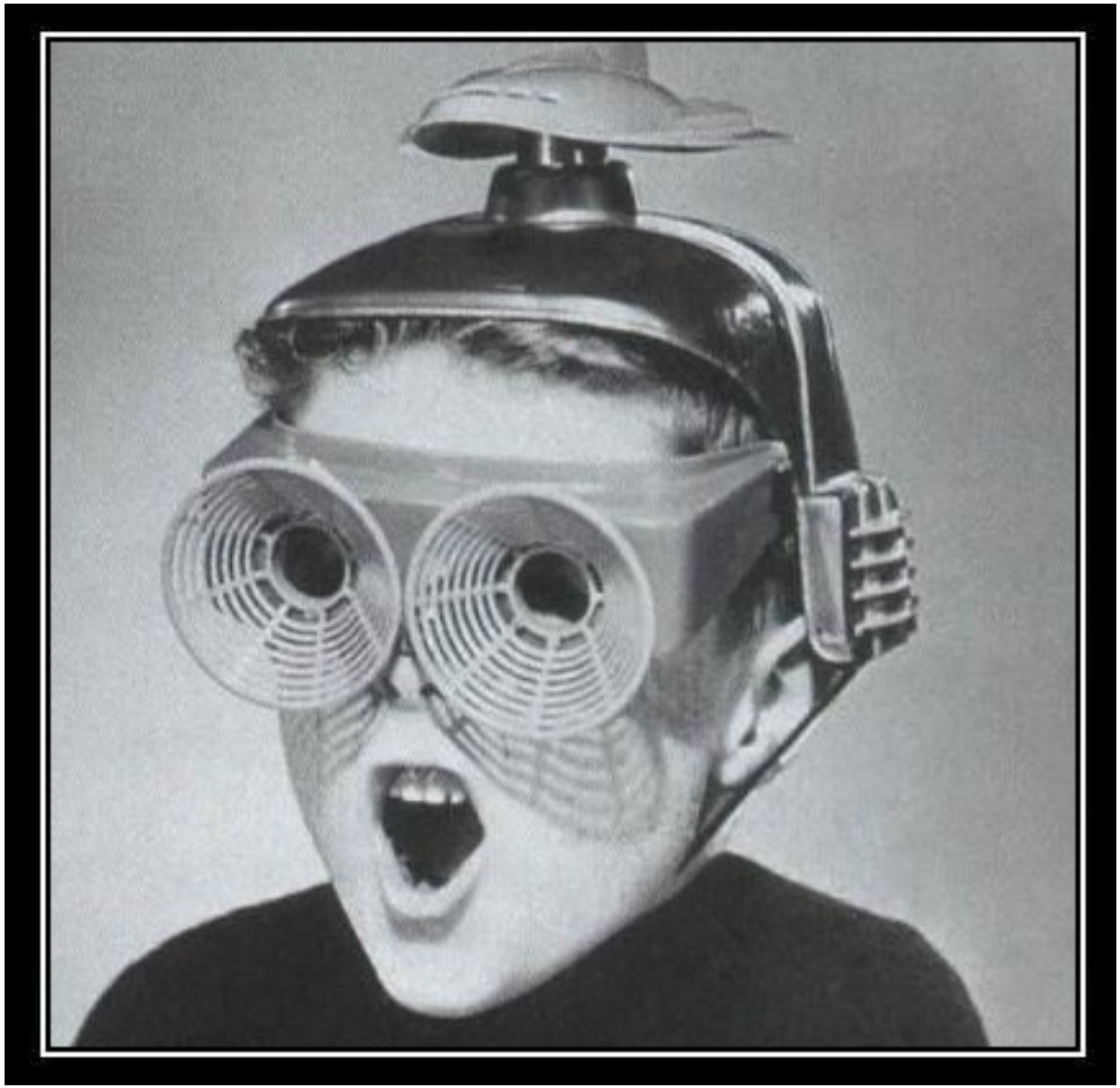


BLE SM - Enumeration - Characteristics

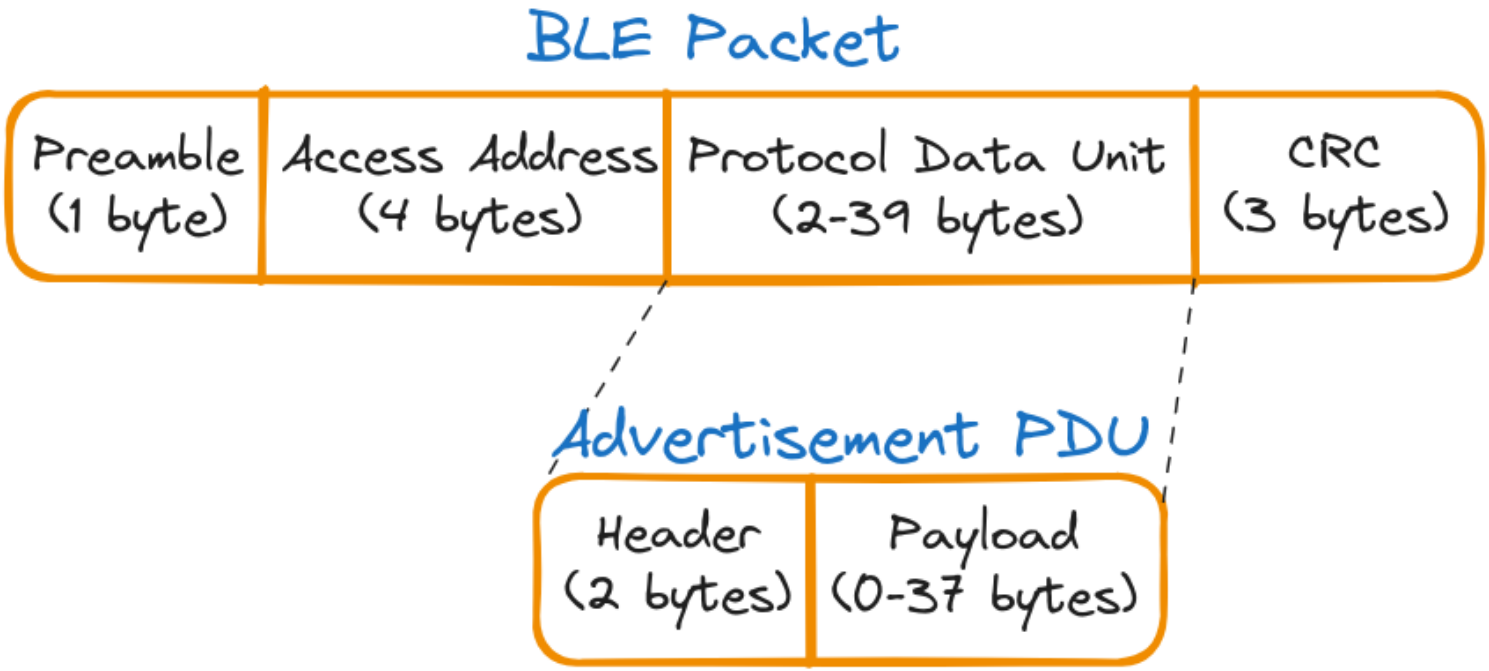
Enumeration of Characteristics:



Basics of Advertisement



BLE - Must Know Basics - Time to Advertise



Purpose of Device's Advertisement Packet

- Make self known to nearby devices
- Pass device address DE:AD:BE:EF:00 for identification
- Additional Services information

But What About Real Life?

```
/**
 * @brief Parse the advertising pay load.
 *
 * The pay load is a buffer of bytes that is either 31 bytes long or terminated by
 * a 0 length value.  Each entry in the buffer has the format:
 * [length][type][data...]
 *
 * The length does not include itself but does include everything after it until the next record.  A record
 * with a length value of 0 indicates a terminator.
 *
 * https://www.bluetooth.com/specifications/assigned-numbers/generic-access-profile
 */
void BLEAdvertisedDevice::parseAdvertisement(uint8_t *payload, size_t total_len) {
  uint8_t length;
  uint8_t ad_type;
  uint8_t sizeConsumed = 0;
  bool finished = false;
  m_payload = payload;
  m_payloadLength = total_len;
```

Figure 7: Documentation in BLE Advertised Device Code [?]

Moar Restrictions?!?!

Larger Limitations:

- Only a small space of UUIDs is standardized
  - Specific format for Bluetooth SIG (`XXXXXXXX-0000-1000-8000-00805f9b34fb`)
  - Some "provided" as vendor specific
  - Wild West
- ABSTRACTIONS!?!?!!!
  - Always abstractions of something lower
  - Eventually hit H-File bedrock....
  - Keeping the secrets

Why are you doing this?

-=[Enumerate the Wild Life]=-

- BLE War Driver
- Development Boards
- Phones
- Toys
- Audio Equipment

What Parts To Examine

Displays of Information:

- Advertisement Packets
- Device Information / Appearance(s)
- Behavioral Interactions

War Driver - Data Observations

Straight Outta Github

```
BLEAdvertisedDevice::BLEAdvertisedDevice() {
  m_adFlag = 0;
  m_appearance = 0;
  m_deviceType = 0;
  m_manufacturerData = "";
  m_name = "";
  m_rssi = -9999;
  m_serviceUUIDs = {};
  m_serviceData = {};
  m_serviceDataUUIDs = {};
  m_txPower = 0;
  m_pScan = nullptr;

  m_haveAppearance = false;
  m_haveManufacturerData = false;
  m_haveName = false;
  m_haveRSSI = false;
  m_haveTXPower = false;

}  // BLEAdvertisedDevice
```

Figure 8: Arduino ESP32 BLEAdvertisedDevice Constructor [**?**]

Straight Outta Github

```
BLEAdvertisedDevice::BLEAdvertisedDevice() {
  m_adFlag = 0;
  m_appearance = 0;
  m_deviceType = 0;
  m_manufacturerData = "";
  m_name = "";
  m_rssi = -9999;
  m_serviceUUIDs = {};
  m_serviceData = {};
  m_serviceDataUUIDs = {};
  m_haveAppearance = false;
  m_haveManufacturerData = false;
  m_haveName = false;
  m_haveRSSI = false;
  m_haveTXPower = false;

}  // BLEAdvertisedDevice
```

Figure 8: Arduino ESP32 BLEAdvertisedDevice Constructor [**?**]

I'm seeing triple???

"Service UUID", "Service Data UUID", "Service Data"

- Use Arduino ESP32 Github Repository as reference material
  - Definition in the BLEAdvertisedDevice.h shows a series of `std::vectors`
- A series of `m_<name>` type variables
  - Two `std::vector<BLEUUID>` (`m_serviceUUIDs`, `m_serviceDataUUIDs`)
  - One `std::vector<String>` (`m_serviceData`)
- Service UUID points to Service Data can contains Service Data UUIDs??
  - Service → Characteristic → Descriptor nesting??

Service UUID Data - Dissection

b'0000febe-0000-1000-8000-00805f9b34fb'

Service UUID Data - Dissection

`b'0000febe-0000-1000-8000-00805f9b34fb'`

- Short UUID (i.e. `16bit`)

Service UUID Data - Dissection

`b'0000febe-0000-1000-8000-00805f9b34fb'`

- Short UUID (i.e. `16bit`)
- Following BT SIG format (`0000` `-0000-1000-8000-00805f9b34fb`)

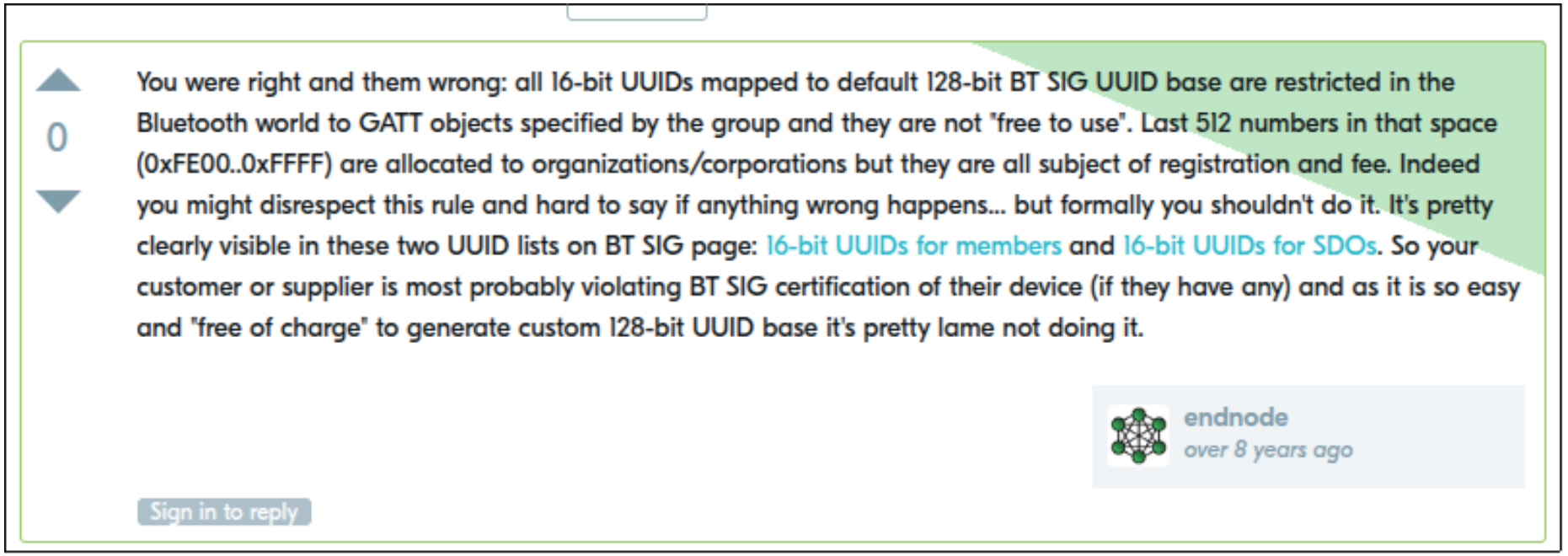


Figure 9: Nordic DevZone Forum Question [?]

Can One Learn These UUIDs....?

```
b'0000febe-0000-1000-8000-00805f9b34fb'
```

Can One Learn These UUIDs....?

```
b'0000fe0d-0000-1000-8000-00805f9b34fb'
b'0000fe0f-0000-1000-8000-00805f9b34fb'
b'0000fe61-0000-1000-8000-00805f9b34fb'
b'0000feb8-0000-1000-8000-00805f9b34fb'
b'0000febe-0000-1000-8000-00805f9b34fb'
b'0000fef3-0000-1000-8000-00805f9b34fb'
b'0000ffe1-0000-1000-8000-00805f9b34fb'
b'0000fff0-0000-1000-8000-00805f9b34fb'
```

Can One Learn These UUIDs....?

b'0000fe0d-0000-1000-8000-00805f9b34fb'
b'0000fe0f-0000-1000-8000-00805f9b34fb'
b'0000fe61-0000-1000-8000-00805f9b34fb'
b'0000feb8-0000-1000-8000-00805f9b34fb'
b'0000febe-0000-1000-8000-00805f9b34fb'
b'0000fef3-0000-1000-8000-00805f9b34fb'
b'0000ffe1-0000-1000-8000-00805f9b34fb'
b'0000fff0-0000-1000-8000-00805f9b34fb'

Not with logic....Top Tier DGAF

```
b'0000fe0d-0000-1000-8000-00805f9b34fb'
b'0000fe0f-0000-1000-8000-00805f9b34fb'
b'0000fe61-0000-1000-8000-00805f9b34fb'
b'0000feb8-0000-1000-8000-00805f9b34fb'
b'0000febe-0000-1000-8000-00805f9b34fb'
b'0000fef3-0000-1000-8000-00805f9b34fb'
b'0000ffe1-0000-1000-8000-00805f9b34fb'
b'0000fff0-0000-1000-8000-00805f9b34fb'
b'1b19b844-038f-11e5-8418-1697f925ec7b'
b'3e1d50cd-7e3e-427d-8e1c-b78aa87fe624'
```

Address this!

```
b'42:1a:b8:c8:c8:5e\x00xVx\x18?{\x00\x00\x00dC?dC?'
b'48:90:c7:90:4c:50\x00xVp%?{\x00\x00\x00dC?dC?'
b'4b:aa:6a:01:44:05\x00xVx\x18?{\x00\x00\x00dC?dC?'
b'4b:e7:41:ff:6a:cf\x00xV%?+\x00\x00\x004\x12\x12\x00\x00\x00'
b'4c:f6:5f:35:1d:c9\x00xV\x08,?5\x00\x00\x00dC?dC?'
b'4d:66:bb:cc:a9:72\x00xV \x19?#\x00\x00\x004\x12\x12\x00\x00\x00'
b'4e:03:00:14:ba:6f\x00xVh\x19?\x00\x00\x00dC?dC?'
b'51:42:19:2d:d8:6c\x00xV,?\x17\x00\x00\x00`\x0c?dC?'
b'5a:2d:42:c6:26:5d\x00xV\x13?G\x01\x00\x00dC?dC?'
b'5a:32:66:2f:bf:6e\x00xV\x18?{\x00\x00\x00dC?dC?'
b'61:56:0c:96:53:41\x00xV%?+\x00\x00\x004\x12\x12\x00\x00\x00'
b'61:fe:cb:83:d7:1a\x00xV\x18?{\x00\x00\x00dC?dC?'
b'67:ea:f4:d9:64:9a\x00xV,?\x13\x00\x00\x00\x1e?dC?'
b'68:3f:3d:39:68:54\x00xV\x00\x18?/\x00\x00\x00dC?dC?'
b'6b:04:8e:08:29:46\x00xVp%?\x00\x00\x00dC?dC?'
b'70:b6:98:8f:84:38\x00xV\x00\x18?/\x00\x00\x00dC?dC?'
b'75:cf:6b:b5:24:54\x00xV\x19?c\x00\x00\x00dC?dC?'
b'76:be:5d:c2:cc:fa\x00xVx\x18?/\x00\x00\x00dC?dC?'
b'76:d9:4c:41:b8:4c\x00xV\x19?c\x00\x00\x00dC?dC?'
b'78:ff:0c:61:64:0b\x00xV\\\x19?\x00\x00\x00dC?dC?'
b'79:03:ac:9e:bc:86\x00xV,?#\x00\x00\x00dC?dC?'
b"7a:10:f5:57:c3:8e\x00xV'?+\x00\x00\x004\x12\x12\x00\x00\x00"
b'7c:bb:ed:98:98:8c\x00xVh\x19?\x00\x00\x00dC?dC?'
b'7c:e9:c1:97:df:13\x00xV\\\x12?+\x00\x00\x004\x12\x12\x00\x00\x00'
b'90:7b:c6:e4:29:14\x00xV%?w\x00\x00\x00dC?dC?'
```

Address this!

```
b'42:1a:b8:c8:c8:5e\x00xVx\x18?{\x00\x00\x00dC?dC?'
b'48:90:c7:90:4c:50\x00xVp%?{\x00\x00\x00dC?dC?'
b'4b:aa:6a:01:44:05\x00xVx\x18?{\x00\x00\x00dC?dC?'
b'4b:e7:41:ff:6a:cf\x00xV%?+\x00\x00\x004\x12\x12\x00\x00\x00'
b'4c:f6:5f:35:1d:c9\x00xV\x08,?S\x00\x00\x00dC?dC?'
b'4d:66:bb:cc:a9:72\x00xV \x19?#\x00\x00\x004\x12\x12\x00\x00\x00'
b'4e:03:00:14:ba:6f\x00xVh\x19?\x00\x00\x00dC?dC?'
b'51:42:19:2d:d8:6c\x00xV,?\x17\x00\x00\x00`\x0c?dC?'
b'5a:2d:42:c6:26:5d\x00xV\x13?G\x01\x00\x00dC?dC?'
b'5a:32:66:2f:bf:6e\x00xV\x18?{\x00\x00\x00dC?dC?'
b'61:56:0c:96:53:41\x00xV%?+\x00\x00\x004\x12\x12\x00\x00\x00'
b'61:fe:cb:83:d7:1a\x00xV\x18?{\x00\x00\x00dC?dC?'
b'67:ea:f4:d9:64:9a\x00xV,?\x13\x00\x00\x00\x1e?dC?'
b'68:3f:3d:39:68:54\x00xV\x00\x18?/\x00\x00\x00dC?dC?'
b'6b:04:8e:08:29:46\x00xVp%?\x00\x00\x00dC?dC?'
b'70:b6:98:8f:84:38\x00xV\x00\x18?/\x00\x00\x00dC?dC?'
b'75:cf:6b:b5:24:54\x00xV\x19?c\x00\x00\x00dC?dC?'
b'76:be:5d:c2:cc:fa\x00xVx\x18?/\x00\x00\x00dC?dC?'
b'76:d9:4c:41:b8:4c\x00xV\x19?c\x00\x00\x00dC?dC?'
b'78:ff:0c:61:64:0b\x00xV\\\x19?\x00\x00\x00dC?dC?'
b'79:03:ac:9e:bc:86\x00xV,?#\x00\x00\x00dC?dC?'
b"7a:10:f5:57:c3:8e\x00xV'?+\x00\x00\x004\x12\x12\x00\x00\x00"
b'7c:bb:ed:98:98:8c\x00xVh\x19?\x00\x00\x00dC?dC?'
b'7c:e9:c1:97:df:13\x00xV\\\x12?+\x00\x00\x004\x12\x12\x00\x00\x00'
b'90:7b:c6:e4:29:14\x00xV%?w\x00\x00\x00dC?dC?'
```

Address this!

```
b'42:1a:b8:c8:c8:5e\x00xVx\x18?{\x00\x00\x00dC?dC?'
b'48:90:c7:90:4c:50\x00xVp%?{\x00\x00\x00dC?dC?'
b'4b:aa:6a:01:44:05\x00xVx\x18?{\x00\x00\x00dC?dC?'
b'4b:e7:41:ff:6a:cf\x00xV%?+\x00\x00\x004\x12\x12\x00\x00\x00'
b'4c:f6:5f:35:1d:c9\x00xV\x08,?5\x00\x00\x00dC?dC?'
b'4d:66:bb:cc:a9:72\x00xV \x19?#\x00\x00\x004\x12\x12\x00\x00\x00'
b'4e:03:00:14:ba:6f\x00xVh\x19?\x00\x00\x00dC?dC?'
b'51:42:19:2d:d8:6c\x00xV,?\x17\x00\x00\x00`\x0c?dC?'
b'5a:2d:42:c6:26:5d\x00xV\x13?G\x01\x00\x00dC?dC?'
b'5a:32:66:2f:bf:6e\x00xV\x18?{\x00\x00\x00dC?dC?'
b'61:56:0c:96:53:41\x00xV%?+\x00\x00\x004\x12\x12\x00\x00\x00'
b'61:fe:cb:83:d7:1a\x00xV\x18?{\x00\x00\x00dC?dC?'
b'67:ea:f4:d9:64:9a\x00xV,?\x13\x00\x00\x00\x1e?dC?'
b'68:3f:3d:39:68:54\x00xV\x00\x18?/\x00\x00\x00dC?dC?'
b'6b:04:8e:08:29:46\x00xVp%?\x00\x00\x00dC?dC?'
b'70:b6:98:8f:84:38\x00xV\x00\x18?/\x00\x00\x00dC?dC?'
b'75:cf:6b:b5:24:54\x00xV\x19?c\x00\x00\x00dC?dC?'
b'76:be:5d:c2:cc:fa\x00xVx\x18?/\x00\x00\x00dC?dC?'
b'76:d9:4c:41:b8:4c\x00xV\x19?c\x00\x00\x00dC?dC?'
b'78:ff:0c:61:64:0b\x00xV\\\x19?\x00\x00\x00dC?dC?'
b'79:03:ac:9e:bc:86\x00xV,?#\x00\x00\x00dC?dC?'
b"7a:10:f5:57:c3:8e\x00xV'?+\x00\x00\x004\x12\x12\x00\x00\x00"
b'7c:bb:ed:98:98:8c\x00xVh\x19?\x00\x00\x00dC?dC?'
b'7c:e9:c1:97:df:13\x00xV\\\x12?+\x00\x00\x004\x12\x12\x00\x00\x00'
b'90:7b:c6:e4:29:14\x00xV%?w\x00\x00\x00dC?dC?'
```

Junk like that....

b'J\x17#LUYC\x112 N\x0cP44\x009?s\x00\x00\x00'

Junk like that....

```
b'J\x17#LUYC\x112 N\x0cP44\x0097?s\x00\x00\x00'
```

Junk like that....

```
b'J\x17#LUYC\x112 N\x0cP44\x009?s\x00\x00\x00'
```

Junk yard dumps

```
b'J\x17#LUYC\x112 N\x0cP44\x009?s\x00\x00\x00'
b'J\x17#LUYC\x112 N\x0cP44\x00\x1f?7\x00\x00\x00'
b'J\x17#M3XL\x1120!t\x1aX\x1fa>\r [\x00\x14\x19?K\x00\x00\x00'
b'J\x17#N005\x112iXA\r(Z\x17&xn\x14d\x00t\x1d?s\x00\x00\x00'
b'J\x17#NFO1\x112(Q;)) i^QT\x00\x0c ?#\x00\x00\x00'
b'J\x17#NFO1\x112(Q;)) i^QT\x00\x14 ?\x1b\x00\x00\x00'
b'J\x17#NFO1\x112(Q;)) i^QT\x00(6?\x02\x00\x00'
b'J\x17#NFO1\x112(Q;)) i^QT\x004<?#\x00\x00\x00'
```

Junk yard dumps

```
b'J\x17#LUYC\x112 N\x0cP44\x009?s\x00\x00\x00'
b'J\x17#LUYC\x112 N\x0cP44\x00\x1f?7\x00\x00\x00'
b'J\x17#M3XL\x1120!t\x1aX\x1fa>\r [\x00\x14\x19?K\x00\x00\x00'
b'J\x17#NOO5\x112iXA\r(Z\x17&xn\x14d\x00t\x1d?s\x00\x00\x00'
b'J\x17#NFO1\x112(Q;)) i^QT\x00\x0c ?#\x00\x00\x00'
b'J\x17#NFO1\x112(Q;)) i^QT\x00\x14 ?\x1b\x00\x00\x00'
b'J\x17#NFO1\x112(Q;)) i^QT\x00(6?\x02\x00\x00'
b'J\x17#NFO1\x112(Q;)) i^QT\x004<?#\x00\x00\x00'
```

Junk yard dumps

```
b'J\x17#LUYC\x112 N\x0cP44\x009?s\x00\x00\x00'
b'J\x17#LUYC\x112 N\x0cP44\x00\x1f?7\x00\x00\x00'
b'J\x17#M3XL\x1120lt\x1aX\x1fa>\r [\x00\x14\x19?K\x00\x00\x00'
b'J\x17#N005\x112iXA\r(Z\x17&xn\x14d\x00t\x1d?s\x00\x00\x00'
b'J\x17#NFO1\x112(Q;)) i^QT\x00\x0c ?#\x00\x00\x00'
b'J\x17#NFO1\x112(Q;)) i^QT\x00\x14 ?\x1b\x00\x00\x00'
b'J\x17#NFO1\x112(Q;)) i^QT\x00(6?\x02\x00\x00'
b'J\x17#NFO1\x112(Q;)) i^QT\x004<?#\x00\x00\x00'
```

All together - Now with Counts

```
1   :  b'\x04\xd2\x89\x0eS\x13<i[rM\x0f\xca\x80\x00xV|,?g\x00\x00\x00dC?'
1   :  b"\x04\x14`\x01\x1f%\x02`\x00xV@'?w\x00\x00\x00dC?"
74  :  b'\x11\x00\x00\x00L>'
2   :  b'0000fe0f-0000-1000-8000-00805f9b34fb'
1   :  b'0000fe2c-0000-1000-8000-00805f9b34fb'
1   :  b'0000feb8-0000-1000-8000-00805f9b34fb'
18  :  b'0000fef3-0000-1000-8000-00805f9b34fb'
1   :  b'0000ffe1-0000-1000-8000-00805f9b34fb'
1   :  b'42:1a:b8:c8:c8:5e\x00xVx\x18?{\x00\x00\x00dC?dC?'
1   :  b'48:90:c7:90:4c:50\x00xVp%?{\x00\x00\x00dC?dC?'
1   :  b'4b:aa:6a:01:44:05\x00xVx\x18?{\x00\x00\x00dC?dC?'
1   :  b'4b:e7:41:ff:6a:cf\x00xV%?+\x00\x00\x004\x12\x12\x00\x00\x00'
1   :  b'4d:66:bb:cc:a9:72\x00xV \x19?#\x00\x00\x004\x12\x12\x00\x00\x00'
```

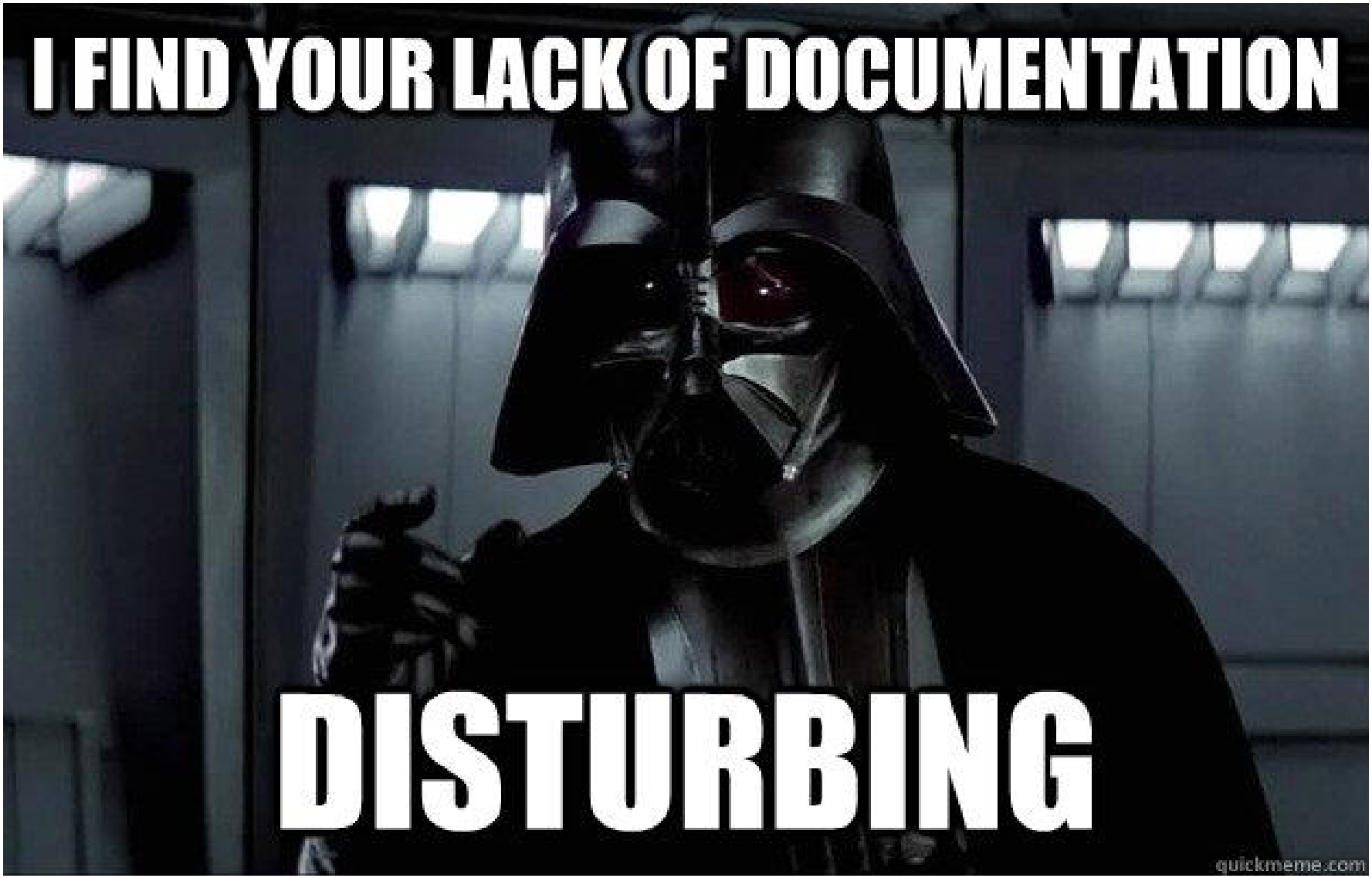
Figure 10: Excerpt of Service Data UUID Data

Summary of the Triplets

Summary on observations

- Interesting range of patterns and information
- UUIDs, Addresses, Junk??, Manufacturer Specific Data???
- “Engineers just want to have fun”

Manufacturer Data



Bluetooth Spec - Manufacturer Data

Data Types Specification

1.4 MANUFACTURER SPECIFIC DATA

1.4.1 Description

The Manufacturer Specific data type is used for manufacturer specific data. The first two data octets shall contain a company identifier from Assigned Numbers. The interpretation of any other octets within the data shall be defined by the manufacturer specified by the company identifier.

1.4.2 Format

Data Type	Description
«Manufacturer Specific Data» *uint16*, which may be followed by *struct*	The first value contains the Company Identifier Code. Any remainder contains manufacturer specific data.

Table 1.5: Manufacturer Specific data type

Bluetooth Spec - Manufacturer Data

HCI_Subversion: *Size: 2 octets*

Value	Parameter Description
0xXXXX	Revision of the HCI implementation in the Controller. This value is vendor-specific.

LMP_Version: *Size: 1 octet*

Value	Parameter Description
0xXX	Version of the Current LMP supported by the Controller. See Assigned Numbers

Company_Identifier: *Size: 2 octets*

Value	Parameter Description
0xXXXX	Company identifier for the manufacturer of the Controller. See Assigned Numbers

LMP_Subversion: *Size: 2 octets*

Value	Parameter Description

Bluetooth Spec - Manufacturer Data

7 Company Identifiers

Company identifiers are unique numbers assigned by the Bluetooth SIG to member companies requesting one.

To request a new Company Identifier, please submit a ticket to Bluetooth Support and select the Assigned Numbers category (login required). For those not familiar with the assignment process, please refer to Section 2.3 of the Assigned Numbers Process Document which is available on the Templates and Documents page.

Please allow five business days for your request to be fulfilled, and another five business days from the time your request is fulfilled to view your Company Identifier on this page.

Referenced from the following:

- Bluetooth Core Specification [Vol 4] Part E, Section 7.1.45 [4].
- Bluetooth Core Specification [Vol 4] Part E, Section 7.4.1 [4].
- Bluetooth Core Specification [Vol 4] Part E, Section 7.4.8 [4].
- Bluetooth Core Specification [Vol 4] Part E, Section 7.4.10 [4].
- Bluetooth Core Specification [Vol 4] Part E, Section 7.7.12 [4].
- Bluetooth Core Specification [Vol 4] Part E, Section 7.8.109 [4].
- Bluetooth Core Specification [Vol 6] Part B, Section 2.4.2.13 [4].
- Supplement to the Bluetooth Core Specification Part A, Section 1.4.1 [22].

7.1 Company Identifiers by Value

Last Modified: 2023-12-15

Filename: company_identifiers.yaml

Value	Name
0x0000	Ericsson AB
0x0001	Nokia Mobile Phones
0x0002	Intel Corp.

Bluetooth Spec - What Rulez?

0x29	PB-ADV	Mesh Profile Specification, Section 5.2.1
0x2A	Mesh Message	Mesh Profile Specification, Section 3.3.1
0x2B	Mesh Beacon	Mesh Profile Specification, Section 3.9
0x2C	BIGInfo	Core Specification Supplement, Part A, Section 1.21
0x2D	Broadcast_Code	Core Specification Supplement, Part A, Section 1.22
0x2E	Resolvable Set Identifier	Coordinated Set Identification Profile v1.0 or later
0x2F	Advertising Interval - long	Core Specification Supplement, Part A, Section 1.15
0x30	Broadcast_Name	Public Broadcast Profile v1.0 or later
0x31	Encrypted Advertising Data	Core Specification Supplement, Part A, Section 1.23
0x32	Periodic Advertising Response Timing Information	Core Specification Supplement, Part A, Section 1.24
0x34	Electronic Shelf Label	ESL Profile
0x3D	3D Information Data	3D Synchronization Profile
0xFF	Manufacturer Specific Data	Core Specification Supplement, Part A, Section 1.4

Bluetooth Spec - What Rulez?

0x29	PB-ADV	Mesh Profile Specification, Section 5.2.1
0x2A	Mesh Message	Mesh Profile Specification, Section 3.3.1
0x2B	Mesh Beacon	Mesh Profile Specification, Section 3.9
0x2C	BIGInfo	Core Specification Supplement, Part A, Section 1.21
0x2D	Broadcast Code	Core Specification Supplement, Part

0xFF	Manufacturer Specific Data	Core Specification Supplement, Part A, Section 1.4

0x31	Encrypted Advertising Data	Core Specification Supplement, Part A, Section 1.23
0x32	Periodic Advertising Response Timing Information	Core Specification Supplement, Part A, Section 1.24
0x34	Electronic Shelf Label	ESL Profile
0x3D	3D Information Data	3D Synchronization Profile
0xFF	Manufacturer Specific Data	Core Specification Supplement, Part A, Section 1.4

Data Types Specification

1.4 MANUFACTURER SPECIFIC DATA

1.4.1 Description

The Manufacturer Specific data type is used for manufacturer specific data. The first two data octets shall contain a company identifier from Assigned Numbers. The interpretation of any other octets within the data shall be defined by the manufacturer specified by the company identifier.

1.4.2 Format

Data Type	Description
«Manufacturer Specific Data» *uint16*, which may be followed by *struct*	The first value contains the Company Identifier Code. Any remainder contains manufacturer specific data.

Table 1.5: Manufacturer Specific data type

Bluetooth Spec - What Rulez?

Generic Attribute Profile (GATT)

APPENDIX A EXAMPLE ATT SERVER CONTENTS

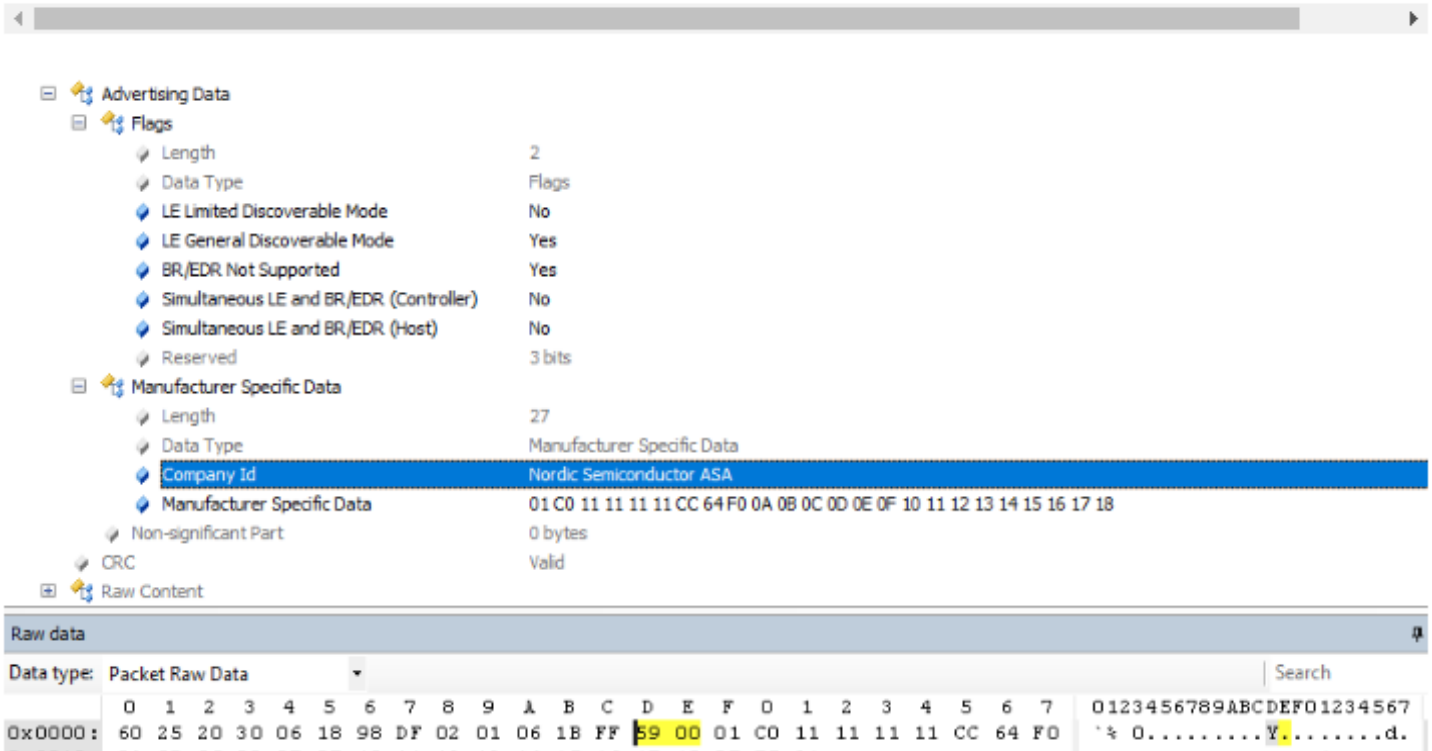
Table A.1 shows an example ATT Server and the attributes contained on the server.

Note: This example does not necessarily use UUIDs or services defined by the Bluetooth SIG or in adopted profiles.

Handle	Attribute Type	Attribute Value
0x0001	«Primary Service»	«GAP Service»
0x0004	«Characteristic»	{0x02, 0x0006, «Device Name»}
0x0006	«Device Name»	“Example Device”
0x0010	«Primary Service»	«GATT Service»
0x0011	«Characteristic»	{0x26, 0x0012, «Service Changed»}
0x0012	«Service Changed»	0x0000, 0x0000
0x0100	«Primary Service»	«Battery State Service»
0x0106	«Characteristic»	{0x02, 0x0110, «Battery State»}
0x0110	«Battery State»	0x04

Manufacturer Specify Data

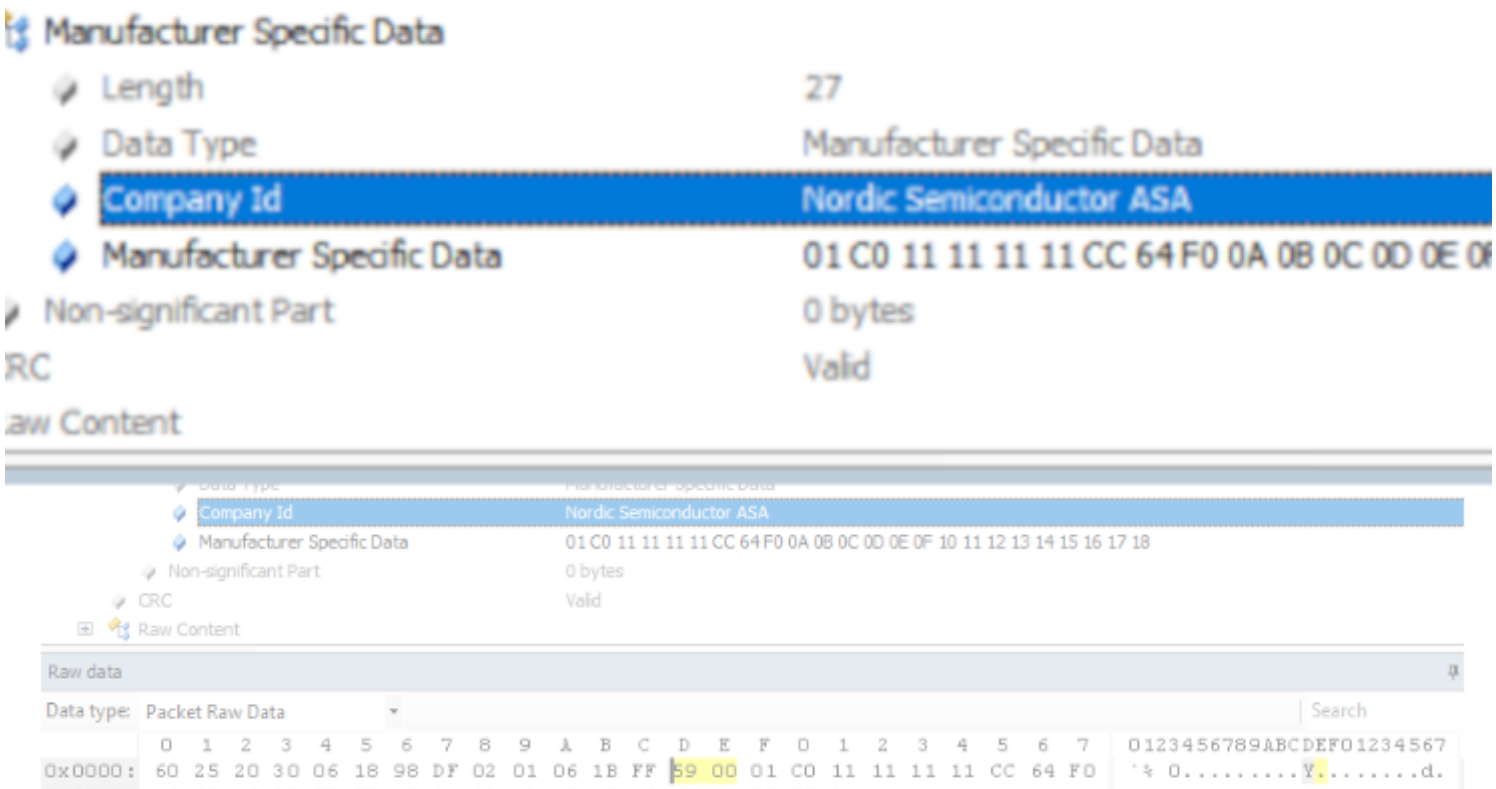
Length	Data Type	Company ID	Manufacturer Specific Data
0x1B (27)	0xFF	0x0059	0x0001C0111111CC64F00A0B0C0D0E0F1011121314151



Manufacturer Data - Jimmy Wong

Manufacturer Specify Data

Length	Data Type	Company ID	Manufacturer Specific Data
0x1B (27)	0xFF	0x0059	0x0001C0111111CC64F00A0B0C0D0E0F1011121314151



Manufacturer Data - Jimmy Wong

Manufacturer Specific Data (offset)	Type	Value / Data
0	Header of Manufacturer Payload	0x01
1-7	MAC Address	0xCC, 0x11, 0x11, 0x11, 0x11, 0xC0
8	Battery Value in %	0x64 (100%)
9	Measured RSSI Value	0xF0
10 – 24	Other Value	0x0A, 0x0B, 0x0C, 0x0D, 0x0E, 0x0F, 0x10, 0x11, 0x12, 0x13, 0x14, 0x15, 0x16, 0x17, 0x18

D.I.Y. Headache

Original Manufacturer Data: `dbus.UInt16(76):`
`[16,7,49,31,116,142,223,166,88]`

- `dbus.UInt16(76)` == `Apple, Inc.  (76)`
- First following number (16) corresponds to `type:  Unknown (16)` (as observed with `btmon`)
- The `07` might indicate the length of data to follow??
  - No 49 (e.g. `0x31`) in known format types
- Converting the remainder of the string to ASCii presents `b'1\x1ft\x8e\xdf\xa6X'`

`dbus.UInt16(76):`
`[12,14,0,255,10,36,134,73,211,168,216,43,215,`
`196,251,132,16,6,120,29,225,79,178,72]`

- According to formattypes.yaml `d'14'` == `0x0E` == `sint16`
  - Format type `0x07` converts to `uint24`??

Development Boards - What the Dev?

Development Boards - What the Dev?

```
Device  D8:3A:DD:2D:9D:66
        Properties:             {dbus.String('Address'): 'D8:3A:DD:2D:9D:66', dbu
rusted'): False, dbus.String('Blocked'): False, dbus.String('LegacyPairing'): Fal
.String('Adapter'): '/org/bluez/hci0', dbus.String('ServicesResolved'): True, dbu
        Address         -       Value:  D8:3A:DD:2D:9D:66
        AddressType             -       Value:  public
        Name            -       Value:  eink-display
        Alias           -       Value:  eink-display
        Paired          -       Value:  False
        Bonded          -       Value:  False
        Trusted         -       Value:  False
        Blocked         -       Value:  False
        LegacyPairing           -       Value:  False
        Connected               -       Value:  True
        UUIDs           -       Value:  ['00001800-0000-1000-8000-00805f9b34fb',
        Adapter         -       Value:  /org/bluez/hci0
        ServicesResolved                -       Value:  True
        AdvertisingFlags                -       Value:  [6]             [ Incompl
```

Development Boards - What the Dev?

```
Device  D8:3A:DD:1F:D0:BC
        Properties:             {dbus.String('Address'): 'D8:3A:DD:1F:D0:BC', dbu
False, dbus.String('Blocked'): False, dbus.String('LegacyPairing'): False, dbus.S
dapter'): '/org/bluez/hci0', dbus.String('ServicesResolved'): True, dbus.String('
        Address         -       Value:  D8:3A:DD:1F:D0:BC
        AddressType             -       Value:  public
        Name            -       Value:  BLE-LED
        Alias           -       Value:  BLE-LED
        Paired          -       Value:  False
        Bonded          -       Value:  False
        Trusted         -       Value:  False
        Blocked         -       Value:  False
        LegacyPairing           -       Value:  False
        Connected               -       Value:  True
        UUIDs           -       Value:  ['00001800-0000-1000-8000-00805f9b34fb',
        Adapter         -       Value:  /org/bluez/hci0
        ServicesResolved                -       Value:  True
        AdvertisingFlags                -       Value:  [6]             [ Incompl
```

Development Boards - What the Dev?

```
Device  D8:3A:DD:1F:D0:BC
        Properties:             {dbus.String('Address'): 'D8:3A:DD:1F:D0:BC', dbu
sted'): False, dbus.String('Blocked'): False, dbus.String('LegacyPairing'): False
tring('Adapter'): '/org/bluez/hci0', dbus.String('ServicesResolved'): True, dbus.
        Address         -       Value:  D8:3A:DD:1F:D0:BC
        AddressType             -       Value:  public
        Name            -       Value:  MPY BTSTACK
        Alias           -       Value:  MPY BTSTACK
        Paired          -       Value:  False
        Bonded          -       Value:  False
        Trusted         -       Value:  False
        Blocked         -       Value:  False
        LegacyPairing           -       Value:  False
        Connected               -       Value:  True
        UUIDs           -       Value:  ['00001800-0000-1000-8000-00805f9b34fb',
        Adapter         -       Value:  /org/bluez/hci0
        ServicesResolved                -       Value:  True
        AdvertisingFlags                -       Value:  [6]             [ Incompl
```

Development Boards - What the Dev?

```
Device  94:C9:60:AE:2D:41
        Properties:             {dbus.String('Address'): '94:C9:60:AE:2D:41', dbu
tring('Trusted'): False, dbus.String('Blocked'): False, dbus.String('LegacyPairin
', '00001819-0000-1000-8000-00805f9b34fb', '0000a7e6-0000-1000-8000-00805f9b34fb'
        Address         -       Value:  94:C9:60:AE:2D:41
        AddressType             -       Value:  public
        Name            -       Value:  BLE GPS Reporter
        Alias           -       Value:  BLE GPS Reporter
        Paired          -       Value:  False
        Bonded          -       Value:  False
        Trusted         -       Value:  False
        Blocked         -       Value:  False
        LegacyPairing           -       Value:  False
        Connected               -       Value:  True
        UUIDs           -       Value:  ['00001800-0000-1000-8000-00805f9b34fb',
        Adapter         -       Value:  /org/bluez/hci0
        ServicesResolved                -       Value:  True
        AdvertisingFlags                -       Value:  [6]             [ Incompl
```

Development Boards - What the Dev?

```
[*] Providing List of All Read Values Associated to known Charact
        [ Char Handle ] -       [ Value (ASCii) ]
        char0002        -       MPY BTSTACK
        char0005        -       -=!=- UNKNOWN -=!=-
        char0008        -       Display:
        char000b        -       Connected
[!] Error: May not have permission for R/W; perhaps need more tha
        org.bluez.Error.NotPermitted: Read not permitted
        Error Value Generated:          [ 13 ]
        char000d        -       None
[!] Error: May not have permission for R/W; perhaps need more tha
        org.bluez.Error.NotPermitted: Read not permitted
        Error Value Generated:          [ 13 ]
        char000f        -       None
```

Development Boards - What the Dev?

```
Select an Action to Take: read-all
[*] Providing List of All Read Values Associated to kno
        [ Char Handle ] -        [ Value (ASCii) ]
        char0002        -        MPY BTSTACK
        char0005        -        -=!=- UNKNOWN -=!=-
        char0008        -
        char000a        -        Connected
```

Development Boards - What the Dev?

```
Select an Action to Take: read-all
[*] Providing List of All Read Values Associated to known
        [ Char Handle ] -       [ Value (ASCii) ]
[!] Error: May not have permission for R/W; perhaps need
        org.bluez.Error.NotPermitted: Read not permitted
        Error Value Generated:          [ 13 ]
        char0002        -       None
        char0006        -       BLE GPS Reporter
        char0008        -
        char000a        -
        char000d        -       -=!=- UNKNOWN -=!=-
        char000f        -       -=!=- UNKNOWN -=!=-
        char0013        -       -=!=- UNKNOWN -=!=-
        char0017        -       Low Memory
Select an Action to Take:
```

Toys - Just for Kids?

What did you do to BB-8??

```
Device  EC:04:28:42:18:4E
        Properties:             {dbus.String('Address'): 'EC:04:28:42:18:4E', dbus.String('AddressType'
False, dbus.String('Blocked'): False, dbus.String('LegacyPairing'): False, dbus.String('Connected'): Tru
1000-8000-00805f9b34fb', '22bb746f-2ba0-7554-2d6f-726568705327', '22bb746f-2bb0-7554-2d6f-726568705327'
tisingFlags'): [6]}     -       Value:  BB-184E
        Alias           -       Value:  BB-184E
        Paired          -       Value:  False
        Bonded          -       Value:  False
        Trusted         -       Value:  False
        Blocked         -       Value:  False
        LegacyPairing           -       Value:  False
        Connected               -       Value:  True
        UUIDs           -       Value:  ['00001016-d102-11e1-9b23-00025b00a5a5', '00001800-0000-1000-800
-726568705327']         -       Value:  /org/bluez/hci0
        ManufacturerData                -       Value:  {dbus.UInt16(12339): []}                [ -=UNK
        ServicesResolved                -       Value:  True
        AdvertisingFlags                -       Value:  [6]             [ Incomplete List of 128-bit Ser
[!] Error: May not have permission for R/W; perhaps need more than just connection to device? OR the 're
        org.bluez.Error.NotPermitted: Read not permitted
        Error Value Generated:          [ 13 ]
[!] Error: May not have permission for R/W; perhaps need more than just connection to device? OR the 're
        org.bluez.Error.NotPermitted: Read not permitted
        Error Value Generated:          [ 13 ]
```

What did you do to BB-8??

```
[+] Returning Found List of Descriptors
Select an Action to Take: read-all
[*] Providing List of All Read Values Associated to known Characteristics
        [ Char Handle ] -       [ Value (ASCii) ]
        char0002        -       BB-184E
        char0004        -       b'\x80\x00'
        char0006        -       b'\x08\x00\x10\x00\x00\x00\xaf\x00'
        char0009        -       b'\x05\xff\xff'
[!] Error: May not have permission for R/W; perhaps need more than just connection to device? OR th
        [ ... ]
        char0016        -       None
        char0019        -       b'\xe0'
[!] Error: May not have permission for R/W; perhaps need more than just connection to device? OR th
        org.bluez.Error.NotPermitted: Read not permitted
        Error Value Generated:          [ 13 ]
        char001d        -       None
        char0020        -
        char0026        -       b'\xaf\x00'
        [ ... ]
        char0037        -       None
        char0039        -       -=!=- UNKNOWN -=!=-
        char003f        -       EC:04:28:42:18:4E
        char0044        -       Sphero
        char0046        -       1.47
Select an Action to Take: quit
```

What did you do to BB-8??

```
[+] Returning Found List of Descriptors
Select an Action to Take: read-all
[*] Providing List of All Read Values Associated to known Characteristics
        [ Char Handle ] -       [ Value (ASCii) ]
        char0002        -       BB-184E
        char0004        -       b'\x80\x00'
        char0006        -       b'\x08\x00\x10\x00\x00\x00\xaf\x00'
        char0009        -       b'\x05\xff\xff'
[!] Error: May not have permission for R/W; perhaps need more than just connection to device? OR th
char0037                -       None
char0039                -       -=!=- UNKNOWN -=!=-
char003f                -       EC:04:28:42:18:4E                                    OR th
char0044                -       Sphero
char0046                -       1.47
        [ ... ]
        char0037        -       None
        char0039        -       -=!=- UNKNOWN -=!=-
        char003f        -       EC:04:28:42:18:4E
        char0044        -       Sphero
        char0046        -       1.47
Select an Action to Take: quit
```

Toys - PokeBall

```
Device  58:2F:40:8A:45:1B
        Properties:             {dbus.String('Address'): '58:2F:40:8A:45:1B', dbus.String('AddressType'): 'public
sted'): False, dbus.String('Blocked'): False, dbus.String('LegacyPairing'): False, dbus.String('Connected'): True
0f-0000-1000-8000-00805f9b34fb', '21c50462-0000-1000-8000-00805f9b34fb', '21c50462-67cb-63a3-5c4c-82b5b9939aeb',
d8e37', 'c7261110-f425-447a-a1bd-9d7246768bd8'], dbus.String('Adapter'): '/org/bluez/hci0', dbus.String('Manufact
00-1000-8000-00805f9b34fb'): [0]}, dbus.String('ServicesResolved'): True, dbus.String('AdvertisingFlags'): [6]}
        Address         -       Value:  58:2F:40:8A:45:1B
        AddressType             -       Value:  public
        Name            -       Value:  Pokemon PBP
        Alias           -       Value:  Pokemon PBP
        Paired          -       Value:  False
        Bonded          -       Value:  False
        Trusted         -       Value:  False
        Blocked         -       Value:  False
        LegacyPairing           -       Value:  False
        LegacyPairing           -       Value:  False
        Connected               -       Value:  True
        UUIDs           -       Value:  ['00001800-0000-1000-8000-00805f9b34fb', '00001801-0000-1000-8000-00805f9
-82b5b9939aeb', '2bbe7f7c-7304-4466-8407-8eaf89f8ce45', '6675e16c-f36d-4567-bb55-6b51e27a23e5', 'addc3e26-4aa5-4c
        Adapter         -       Value:  /org/bluez/hci0
        ManufacturerData                -       Value:  {dbus.UInt16(1363): [1, 173, 222, 0, 239, 190, 0, 0, 220,
        ServiceData             -       Value:  {dbus.String('21c50462-0000-1000-8000-00805f9b34fb'): [0]}
        ServicesResolved                -       Value:  True
        AdvertisingFlags                -       Value:  [6]             [ Incomplete List of 128-bit Service or S
[!] Unrecognized ATT error seen
        org.bluez.Error.Failed: Operation failed with ATT error: 0x01
        Error Value Generated:          [ None ]
[!] Error: May not have permission for R/W; perhaps need more than just connection to device? OR the 'read' capab
        org.bluez.Error.NotPermitted: Read not permitted
        Error Value Generated:          [ 13 ]
```

Toys - PokeBall

```
[+] Returning Found List of Descriptors
Select an Action to Take: read-all
[*] Providing List of All Read Values Associated to known Characteri
        [ Char Handle ] -       [ Value (ASCii) ]
        char0002        -       Pokemon PBP
        char0004        -       b'\xc0\x03'
[!] Unrecognized ATT error seen
        org.bluez.Error.Failed: Operation failed with ATT error: 0x0
        Error Value Generated:          [ None ]
        char0011        -       None
        char0021        -       d
        char0031        -       Nintendo
        char0033        -       18.0    EC5A2BF1
        char0041        -       b'd\x00\xf9wx\xc3\xfcj\xfc\xa0\x0f\x
[!] Error: May not have permission for R/W; perhaps need more than j
        org.bluez.Error.NotPermitted: Read not permitted
        Error Value Generated:          [ 13 ]
        char0045        -       None
```

Do you guys not have phones?

Samsung Z Fold

```
Device  84:5F:04:45:36:12
        Properties:             {dbus.String('Address'): '84:5F:04:45:36:12', dbus.String('AddressType
s.String('Icon'): 'phone', dbus.String('Paired'): True, dbus.String('Bonded'): False, dbus.String('Tru
00805f9b34fb', '0000110a-0000-1000-8000-00805f9b34fb', '0000110c-0000-1000-8000-00805f9b34fb', '000011
0000-1000-8000-00805f9b34fb', '0000112f-0000-1000-8000-00805f9b34fb', '00001132-0000-1000-8000-00805f9
5a'], dbus.String('Modalias'): 'bluetooth:v0075p0100d0201', dbus.String('Adapter'): '/org/bluez/hci0',
10, 101, 93, 32, 0]}, dbus.String('ServicesResolved'): True}
        Address         -       Value:  84:5F:04:45:36:12
        AddressType             -       Value:  public
        Name            -       Value:  Galaxy Z Fold3 5G
        Alias           -       Value:  Galaxy Z Fold3 5G
        Class           -       Value:  5898764         [ Phone : Smartphone - Networking,Capturing,Ob
        Icon            -       Value:  phone
        Paired          -       Value:  True
        Bonded          -       Value:  False
        Trusted         -       Value:  False
        Blocked         -       Value:  False
        LegacyPairing           -       Value:  False
        Connected               -       Value:  True
        UUIDs           -       Value:  ['00001105-0000-1000-8000-00805f9b34fb', '0000110a-0000-1000-8
-00805f9b34fb', '00001116-0000-1000-8000-00805f9b34fb', '0000111f-0000-1000-8000-00805f9b34fb', '0000
-0000-1000-8000-00805f9b34fb', 'a82efa21-ae5c-3dde-9bbc-f16da7b16c5a']
        Modalias                -       Value:  bluetooth:v0075p0100d0201
        Adapter         -       Value:  /org/bluez/hci0
        ManufacturerData                -       Value:  {dbus.UInt16(117): [2, 9, 1, 0, 0, 0, 1, 1, 0,
        ServicesResolved                -       Value:  True
[+] Exploration Basics Successfully Created
```

Samsung Z Fold

```
[*] User Interactive Exploration Tool - Select Action
        - 'print' to Pretty Print the known user device internals map
        - 'info' to print device information
        - 'tools' to Access the Tools Sub-Menu
        - 'signals' to configure emission capture
        - 'generate' to Access the Generation Sub-Menu
        - 'explore' to Access the Exploration Sub-Menu
        - 'read' to Access the Reading Sub-Menu
        - 'write' to Access the Writing Sub-Menu
        - 'help' to print this information
        - 'quit' to exit user exploration
        - 'reconnect' to reconnect to the current target device
        Nota Bene:      Complete Re-Read of the Device may be required to update the Device Internals
        Ssh.....
Select an Action to Take: generate-all
[*] Generating all internal lists
[*] Finding and Returing the List of Services from Internals Map
[+] Returing Found List of Services
[*] Finding and Returning the List of Characteristics from Internals Map
[+] Returning Found List of Characteristics
[*] Finding and Returning the List of Descriptors from Intnernals Map
[+] Returning Found List of Descriptors
Select an Action to Take: read-all
[*] Providing List of All Read Values Associated to known Characteristics
        [ Char Handle ] -       [ Value (ASCii) ]
ERROR: The required list has not been generated
Select an Action to Take: quit
```

OnePlus 6T

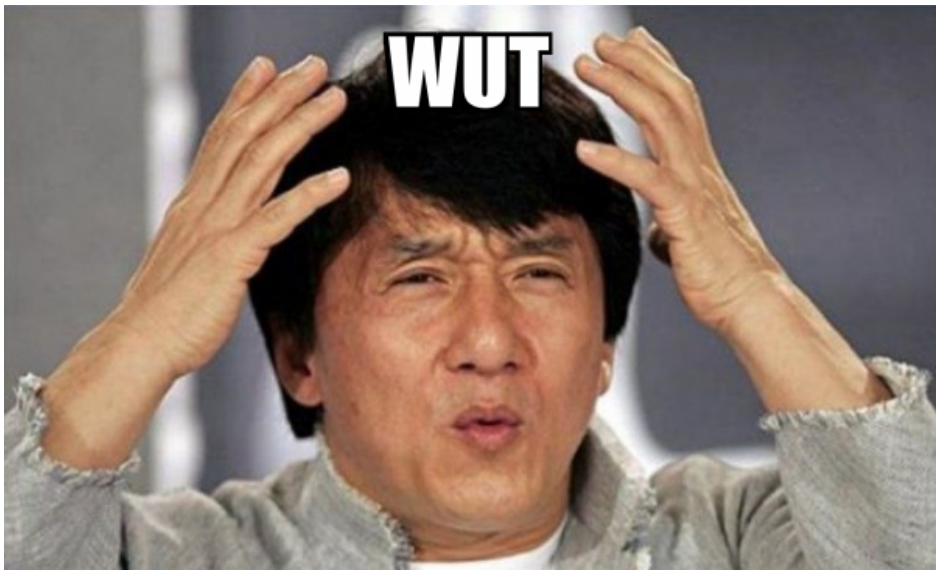
```
Device  64:A2:F9:BC:8E:95
        Properties:             {dbus.String('Address'): '64:A2:F9:BC:8E:95', dbus.String('Address
'): 'phone', dbus.String('Paired'): True, dbus.String('Bonded'): True, dbus.String('Trusted'): Fal
'00001105-0000-1000-8000-00805f9b34fb', '0000110a-0000-1000-8000-00805f9b34fb', '0000110c-0000-100
00805f9b34fb', '0000111f-0000-1000-8000-00805f9b34fb', '0000112d-0000-1000-8000-00805f9b34fb', '00
0000-1000-8000-00805f9b34fb', '0000c103-0000-1000-8000-00805f9b34fb', '0000c104-0000-1000-8000-008
'): '/org/bluez/hci0', dbus.String('ServicesResolved'): True}
        Address         -       Value:  64:A2:F9:BC:8E:95
        AddressType             -       Value:  public
        Name            -       Value:  OnePlus 6T
        Alias           -       Value:  OnePlus 6T
        Class           -       Value:  5898764         [ Phone : Smartphone - Networking,Capturir
        Icon            -       Value:  phone
        Paired          -       Value:  True
        Bonded          -       Value:  True
        Trusted         -       Value:  False
        Blocked         -       Value:  False
        LegacyPairing           -       Value:  False
        Connected               -       Value:  True
        UUIDs           -       Value:  ['00000000-0000-0000-0000-000000000000', '00001105-0000-10
-00805f9b34fb', '00001115-0000-1000-8000-00805f9b34fb', '00001116-0000-1000-8000-00805f9b34fb', '0
-0000-1000-8000-00805f9b34fb', '00001800-0000-1000-8000-00805f9b34fb', '00001801-0000-1000-8000-00
c5a']
        Modalias                -       Value:  bluetooth:v001Dp1200d1436
        Adapter         -       Value:  /org/bluez/hci0
        ServicesResolved                -       Value:  True
```

OnePlus 6T

```
[!] Error occurred while connecting to the device
[!] check_and_explore__bluetooth_device__user_selected::Unknown D-Bu
        Error:  org.freedesktop.DBus.Error.InvalidArgs: No such inte
        D-Bus Name:     <bound method DBusException.get_dbus_name of
        All Error Args: ("No such interface 'org.bluez.GattService1'
[+] Finished Main()
```

OnePlus 6T

```
[!] Error occurred while connecting to the device
[!] check_and_explore__bluetooth_device__user_selected::Unknown D-Bu
        Error:  org.freedesktop.DBus.Error.InvalidArgs: No such inte
        D-Bus Name:     <bound method DBusException.get_dbus_name of
        All Error Args: ("No such interface 'org.bluez.GattService1'
[+] Finished Main()
```



OnePlus 6T

```
: ['org.freedesktop.DBus.Introspectable', 'org.bluez.Device1', 'org.fr
rate a list of device services
 at 0x7fcc707525c0>
trib:    [ {} ]
 Child Attrib:   [ {'name': 'org.freedesktop.DBus.Introspectable'} ]
 Child Attrib:   [ {'name': 'org.bluez.Device1'} ]
 Child Attrib:   [ {'name': 'org.freedesktop.DBus.Properties'} ]
 Child Attrib:   [ {'name': 'org.bluez.Network1'} ]
 Child Attrib:   [ {'name': 'org.bluez.MediaControl1'} ]
 Child Attrib:   [ {'name': 'player0'} ]
 Child Attrib:   [ {'name': 'sep1'} ]
nt resolved without raising an exception
d to generate list of device services
         [ ['player0', 'sep1'] ]
```

Audio Equipment - Hear me Out

Wait.... I remember!

- Have to present yourself correctly (Alsa)
- Caused hijacked headphones audio stream

Fudo Speaker

```
Device  F7:A2:CE:18:37:42
        Properties:             {dbus.String('Address'): 'F7:A2:CE:18:37:42', dbus.String('AddressType'): 'public
('Icon'): 'audio-headset', dbus.String('Paired'): True, dbus.String('Bonded'): False, dbus.String('Trusted'): Fal
00805f9b34fb', '0000110e-0000-1000-8000-00805f9b34fb', '0000111e-0000-1000-8000-00805f9b34fb', '00001200-0000-100
 {dbus.UInt16(29282): [50, 50, 120, 120, 17, 34, 51, 68, 85, 102, 170, 187, 0, 0]}, dbus.String('ServicesResolved
 192]}}
        Address         -       Value:  F7:A2:CE:18:37:42
        AddressType             -       Value:  public
        Name            -       Value:  25603 speaker
        Alias           -       Value:  25603 speaker
        Class           -       Value:  2360324         [ Audio/Video : Wearable Headset Device - Rendering,Audio
        Icon            -       Value:  audio-headset
        Paired          -       Value:  True
        Bonded          -       Value:  False
        Trusted         -       Value:  False
        Blocked         -       Value:  False
        LegacyPairing           -       Value:  False
        Connected               -       Value:  True
        UUIDs           -       Value:  ['0000110b-0000-1000-8000-00805f9b34fb', '0000110e-0000-1000-8000-00805f9
        Modalias                -       Value:  bluetooth:v05D6p000Ad0240
        Adapter         -       Value:  /org/bluez/hci0
        ManufacturerData                -       Value:  {dbus.UInt16(29282): [50, 50, 120, 120, 17, 34, 51, 68, 8
        ServicesResolved                -       Value:  True
        AdvertisingData         -       Value:  {dbus.Byte(254): [15, 27, 52, 140, 1, 0, 64, 32, 129, 71, 4, 143,
[!] Error occurred while connecting to the device
                [!] check_and_explore__bluetooth_device__user_selected::Unknown D-Bus Error has Occured when Atte
        Error:  org.freedesktop.DBus.Error.InvalidArgs: No such interface 'org.bluez.GattService1'
        D-Bus Name:     <bound method DBusException.get_dbus_name of DBusException("No such interface 'org.bluez.
        All Error Args: ("No such interface 'org.bluez.GattService1'",)
[+] Finished Main()
```

```
Device  41:42:C8:7B:71:5C
        Properties:             {dbus.String('Address'): '41:42:C8:7B:71:5C', dbus.String('Add
-headphones', dbus.String('Paired'): True, dbus.String('Bonded'): False, dbus.String('Trusted'
, '0000110c-0000-1000-8000-00805f9b34fb', '0000110e-0000-1000-8000-00805f9b34fb', '0000111e-00
        Address         -       Value:  41:42:C8:7B:71:5C
        AddressType             -       Value:  public
        Name            -       Value:  EGC07
        Alias           -       Value:  EGC07
        Class           -       Value:  2360344         [ Audio/Video : Headphones - Rendering
        Icon            -       Value:  audio-headphones
        Paired          -       Value:  True
        Bonded          -       Value:  False
        Trusted         -       Value:  False
        Blocked         -       Value:  False
        LegacyPairing           -       Value:  False
        Connected               -       Value:  True
        UUIDs           -       Value:  ['0000110b-0000-1000-8000-00805f9b34fb', '0000110c-000
        Adapter         -       Value:  /org/bluez/hci0
        ServicesResolved                        -       Value:  True
[!] Error occurred while connecting to the device
[!] check_and_explore__bluetooth_device__user_selected::Unknown D-Bus Error has Occured when A
        Error:  org.freedesktop.DBus.Error.InvalidArgs: No such interface 'org.bluez.GattServi
        D-Bus Name:     <bound method DBusException.get_dbus_name of DBusException("No such in
        All Error Args: ("No such interface 'org.bluez.GattService1'",)
[+] Finished Main()
```

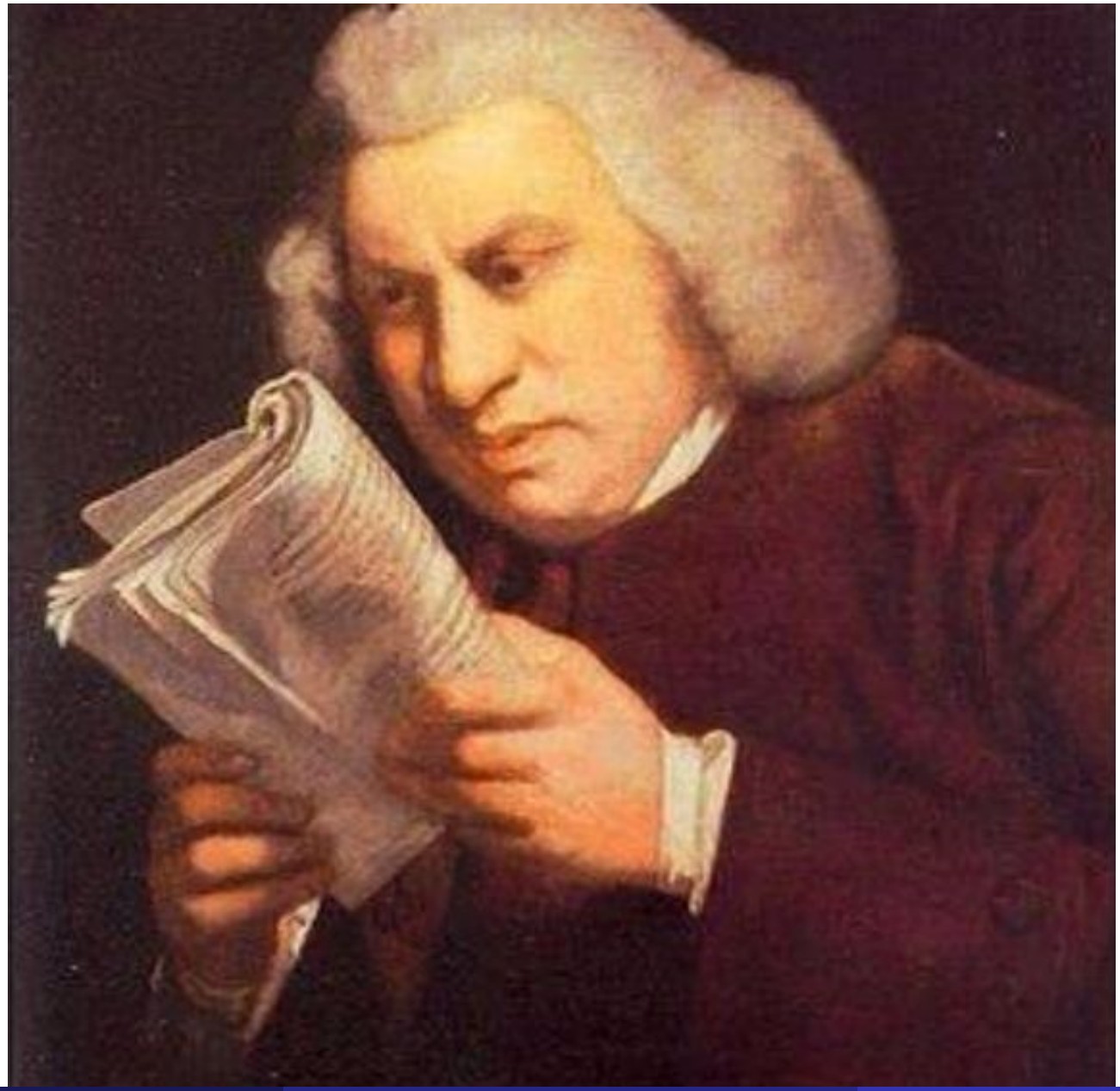
Razer BlackShark

```
Device  44:5E:CD:39:12:F9
        Properties:             {dbus.String('Address'): '44:5E:CD:39:12:F9', dbus.String('AddressType'):
iant_level=1), dbus.String('Icon'): 'audio-headset', dbus.String('Paired'): True, dbus.String('Bonded'):
'00001101-0000-1000-8000-00805f9b34fb', '00001108-0000-1000-8000-00805f9b34fb', '0000110b-0000-1000-8000-
00805f9b34fb'], dbus.String('Adapter'): '/org/bluez/hci0', dbus.String('ManufacturerData'): {dbus.UInt16(
        Address         -       Value:  44:5E:CD:39:12:F9
        AddressType             -       Value:  public
        Name            -       Value:  Razer BlackShark V2 Pro BT
        Alias           -       Value:  Razer BlackShark V2 Pro BT
        Class           -       Value:  2360324         [ Audio/Video : Wearable Headset Device - Renderi
        Icon            -       Value:  audio-headset
        Paired          -       Value:  True
        Bonded          -       Value:  False
        Trusted         -       Value:  False
        Blocked         -       Value:  False
        LegacyPairing           -       Value:  True
        Connected               -       Value:  True
        UUIDs           -       Value:  ['00001101-0000-1000-8000-00805f9b34fb', '00001108-0000-1000-8000
-00805f9b34fb', '00001200-0000-1000-8000-00805f9b34fb']
        Adapter         -       Value:  /org/bluez/hci0
        ManufacturerData                -       Value:  {dbus.UInt16(30017): [100, 105, 111, 87, 105, 115
        ServicesResolved                -       Value:  True
[!] Error occurred while connecting to the device
[!] check_and_explore__bluetooth_device__user_selected::Unknown D-Bus Error has Occured when Attempting a
        Error:  org.freedesktop.DBus.Error.InvalidArgs: No such interface 'org.bluez.GattService1'
        D-Bus Name:     <bound method DBusException.get_dbus_name of DBusException("No such interface 'or
        All Error Args: ("No such interface 'org.bluez.GattService1'",)
[+] Finished Main()
```

DS220 Audio Adapter

```
Device  53:4A:52:FE:01:38
        Properties:             {dbus.String('Address'): '53:4A:52:FE:01:38', dbus.String('AddressType'): 'pu
-headphones', dbus.String('Paired'): True, dbus.String('Bonded'): True, dbus.String('Trusted'): False, dbus.S
0-1000-8000-00805f9b34fb', '0000110c-0000-1000-8000-00805f9b34fb', '0000110d-0000-1000-8000-00805f9b34fb', '0
ring('ServicesResolved'): True}
        Address         -       Value:  53:4A:52:FE:01:38
        AddressType             -       Value:  public
        Name            -       Value:  DS220
        Alias           -       Value:  DS220
        Class           -       Value:  2360344         [ Audio/Video : Headphones - Rendering,Audio ]
        Icon            -       Value:  audio-headphones
        Paired          -       Value:  True
        Bonded          -       Value:  True
        Trusted         -       Value:  False
        Blocked         -       Value:  False
        LegacyPairing           -       Value:  False
        RSSI            -       Value:  -20
        Connected               -       Value:  True
        UUIDs           -       Value:  ['0000110b-0000-1000-8000-00805f9b34fb', '0000110c-0000-1000-8000-008
        Adapter         -       Value:  /org/bluez/hci0
        TxPower         -       Value:  4
        ServicesResolved                -       Value:  True
DO STUFF!!!
[!] Error occurred while connecting to the device
[!] check_and_explore__bluetooth_device__user_selected::Unknown D-Bus Error has Occured when Attempting a Con
        Error:  org.freedesktop.DBus.Error.InvalidArgs: No such interface 'org.bluez.GattService1'
        D-Bus Name:     <bound method DBusException.get_dbus_name of DBusException("No such interface 'org.bl
        All Error Args: ("No such interface 'org.bluez.GattService1'",)
[+] Finished Main()
```

DS220 Audio Adapter - WTH?



BLE Audio - BLEEP Debugging Comparison

```
n
nt resolved without raising an exception
to enumerate device object
mpting to generate a list of device services
:Attempting to Generate Introspection Interface
Element 'node' at 0x7dd5f7f53bf0>
       Root Attrib:    [ {} ]
               Child Attrib:   [ {'name': 'org.freedesktop.DBus.Introspectable'} ]
               Child Attrib:   [ {'name': 'org.bluez.Device1'} ]
               Child Attrib:   [ {'name': 'org.freedesktop.DBus.Properties'} ]
               Child Attrib:   [ {'name': 'org.bluez.MediaControl1'} ]
               Child Attrib:   [ {'name': 'org.bluez.Battery1'} ]
               Child Attrib:   [ {'name': 'sep1'} ]
               Child Attrib:   [ {'name': 'sep2'} ]
t! Try statement resolved without raising an exception
leted attempted to generate list of device services
rated List:             [ ['sep1', 'sep2'] ]
:BLE service   -        sep1
```

BLE Audio - BLEEP Debugging Comparison

```
resolved without raising an exception
enumerate device object
ng to generate a list of device services
tempting to Generate Introspection Interface
ment 'node' at 0x7560f4957d80>
    Root Attrib:    [ {} ]
        Child Attrib:   [ {'name': 'org.freedesktop.DBus.Introspectable'} ]
        Child Attrib:   [ {'name': 'org.bluez.Device1'} ]
        Child Attrib:   [ {'name': 'org.freedesktop.DBus.Properties'} ]
        Child Attrib:   [ {'name': 'org.bluez.MediaControl1'} ]
        Child Attrib:   [ {'name': 'org.bluez.Battery1'} ]
        Child Attrib:   [ {'name': 'sep1'} ]
Try statement resolved without raising an exception
ed attempted to generate list of device services
ed List:            [ ['sep1'] ]
[ service   -       sep1
```

BLE Audio - BLEEP Debugging Comparison

```
rate device object
empting to generatea dictionary of device enumeration
 Attempting to Generate Introspection Interface
 node' at 0x7f547014f970>
ot Attrib:    [ {} ]
        Child Attrib:   [ {'name': 'org.freedesktop.DBus.Introspectable'} ]
        Child Attrib:   [ {'name': 'org.bluez.Device1'} ]
        Child Attrib:   [ {'name': 'org.freedesktop.DBus.Properties'} ]
        Child Attrib:   [ {'name': 'org.bluez.MediaControl1'} ]
        Child Attrib:   [ {'name': 'org.bluez.Battery1'} ]
        Child Attrib:   [ {'name': 'sep1'} ]
        Child Attrib:   [ {'name': 'sep16'} ]
        Child Attrib:   [ {'name': 'sep2'} ]
t! Try statement resolved without raising an exception
leted attempted to generate dictionary of device information
erated Dictionary:              [ {'interfaces': ['org.freedesktop.DBus.Intro
```

BLE Audio - BLEEP Debugging Comparison

```
merate device object
ttempting to generatea dictionary of device enumeration
n::Attempting to Generate Introspection Interface
t 'node' at 0x733896347920>
 Root Attrib:    [ {} ]
         Child Attrib:   [ {'name': 'org.freedesktop.DBus.Introspectable'} ]
         Child Attrib:   [ {'name': 'org.bluez.Device1'} ]
         Child Attrib:   [ {'name': 'org.freedesktop.DBus.Properties'} ]
         Child Attrib:   [ {'name': 'org.bluez.MediaControl1'} ]
         Child Attrib:   [ {'name': 'sep1'} ]
         Child Attrib:   [ {'name': 'sep10'} ]
         Child Attrib:   [ {'name': 'sep3'} ]
         Child Attrib:   [ {'name': 'sep5'} ]
         Child Attrib:   [ {'name': 'sep6'} ]
         Child Attrib:   [ {'name': 'sep7'} ]
         Child Attrib:   [ {'name': 'sep8'} ]
lert! Try statement resolved without raising an exception
ompleted attempted to generate dictionary of device information
enerated Dictionary:              [ {'interfaces': ['org.freedesktop.DBus.Intro
```

DS220 Audio Adapter - bluetoothctl

```
[NEW] Device 53:4A:52:FE:01:38 DS220
[CHG] Device 53:4A:52:FE:01:38 Connected: yes
[CHG] Device 53:4A:52:FE:01:38 UUIDs: 0000110b-0000-1000-8000-00805f9b34fb
[CHG] Device 53:4A:52:FE:01:38 UUIDs: 0000110c-0000-1000-8000-00805f9b34fb
[CHG] Device 53:4A:52:FE:01:38 UUIDs: 0000110d-0000-1000-8000-00805f9b34fb
[CHG] Device 53:4A:52:FE:01:38 UUIDs: 0000110e-0000-1000-8000-00805f9b34fb
[CHG] Device 53:4A:52:FE:01:38 UUIDs: 0000110f-0000-1000-8000-00805f9b34fb
[CHG] Device 53:4A:52:FE:01:38 ServicesResolved: yes
[CHG] Device 53:4A:52:FE:01:38 Bonded: yes
[CHG] Device 53:4A:52:FE:01:38 Paired: yes
[NEW] Endpoint /org/bluez/hci0/dev_53_4A_52_FE_01_38/sep10
[NEW] Endpoint /org/bluez/hci0/dev_53_4A_52_FE_01_38/sep8
[NEW] Endpoint /org/bluez/hci0/dev_53_4A_52_FE_01_38/sep6
[NEW] Endpoint /org/bluez/hci0/dev_53_4A_52_FE_01_38/sep7
[NEW] Endpoint /org/bluez/hci0/dev_53_4A_52_FE_01_38/sep5
[NEW] Endpoint /org/bluez/hci0/dev_53_4A_52_FE_01_38/sep3
[NEW] Endpoint /org/bluez/hci0/dev_53_4A_52_FE_01_38/sep1
[NEW] Transport /org/bluez/hci0/dev_53_4A_52_FE_01_38/sep1/fd3
[CHG] Transport /org/bluez/hci0/dev_53_4A_52_FE_01_38/sep1/fd3 State: active
[CHG] Controller 00:01:95:4B:48:0F Discovering: no
[CHG] Transport /org/bluez/hci0/dev_53_4A_52_FE_01_38/sep1/fd3 Volume: 0x0054 (84)
[CHG] Transport /org/bluez/hci0/dev_53_4A_52_FE_01_38/sep1/fd3 State: idle
[CHG] Controller 00:01:95:4B:48:0F Discovering: yes
```

BlueZ Documentation - Media Control

```
======================
org.bluez.MediaControl
======================

----------------------------------------
BlueZ D-Bus MediaControl API documentation
----------------------------------------

:Version: BlueZ
:Date: September 2023
:Manual section: 5
:Manual group: Linux System Administration

Interface
=========

:Service:       org.bluez
:Interface:     org.bluez.MediaControl1
:Object path:   [variable prefix]/{hci0,hci1,...}/dev_XX_XX_XX_XX_XX_XX

Methods
-------

void Play() [Deprecated]
````````````````````````

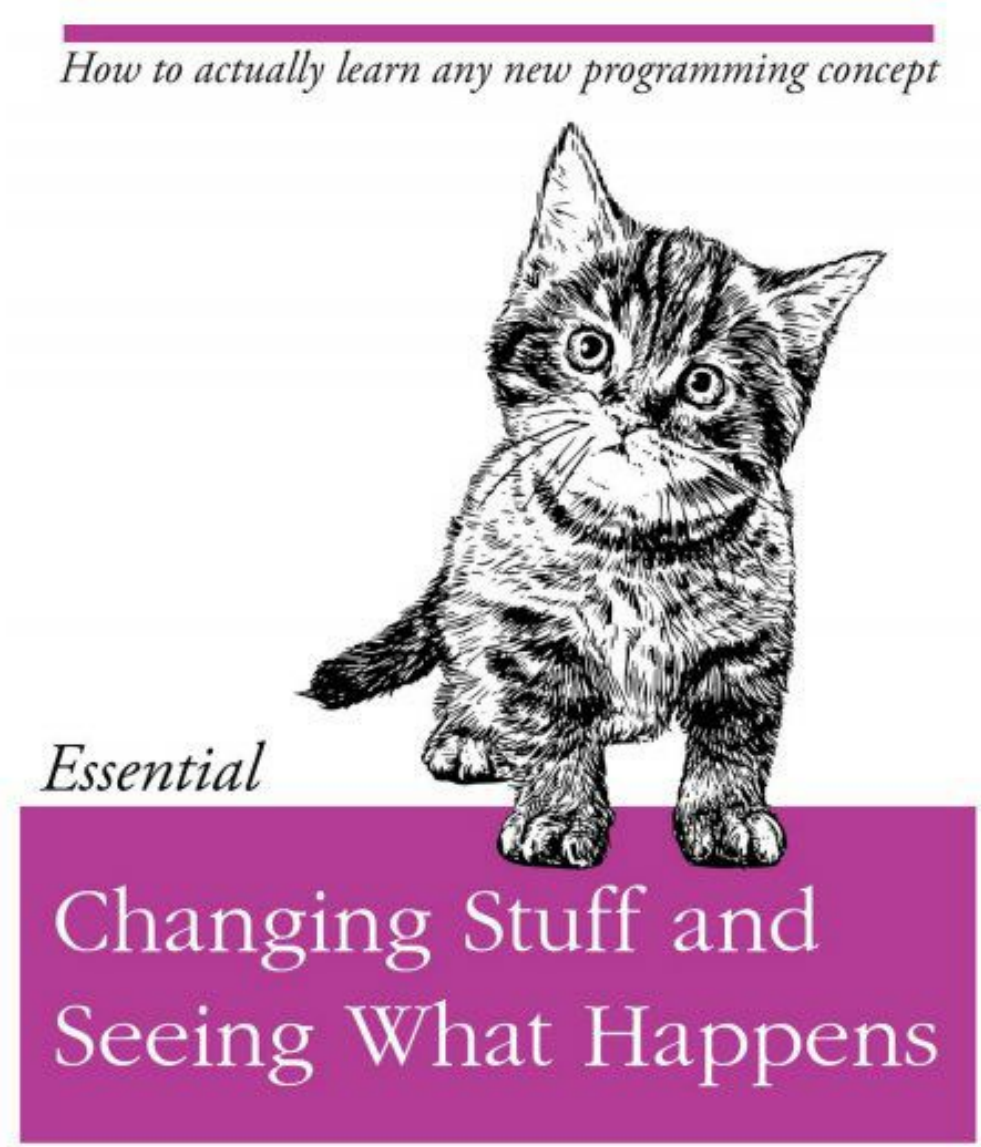
        Resume playback.

void Pause() [Deprecated]
`````````````````````````
```

# DS220 Audio Adapter - `busctl` Media Control

| | | | | |
|---|---|---|---|---|
| **org.bluez.MediaControl1** | interface | - | - | - |
| .FastForward | method | - | - | deprecated |
| .Next | method | - | - | deprecated |
| .Pause | method | - | - | deprecated |
| .Play | method | - | - | deprecated |
| .Previous | method | - | - | deprecated |
| .Rewind | method | - | - | deprecated |
| .Stop | method | - | - | deprecated |
| .VolumeDown | method | - | - | deprecated |
| .VolumeUp | method | - | - | deprecated |
| .Connected | property | b | true | emits-change |
| .Player | property | o | - | emits-change |
| **org.freedesktop.DBus.Introspectable** | interface | - | - | - |
| .Introspect | method | - | s | - |
| **org.freedesktop.DBus.Properties** | interface | - | - | - |
| .Get | method | ss | v | - |
| .GetAll | method | s | a{sv} | - |
| .Set | method | ssv | - | - |
| .PropertiesChanged | signal | sa{sv}as | - | - |

# BlueZ Documentation - Media Endpoint

```
----------------------------------------
BlueZ D-Bus MediaEndpoint API documentation
----------------------------------------

:Version: BlueZ
:Date: September 2023
:Manual section: 5
:Manual group: Linux System Administration

Interface
=========

:Service:         unique name (Server role)
                  org.bluez (Client role)
:Interface:       org.bluez.MediaEndpoint1
:Object path:     freely definable (Server role)
                  [variable prefix]/{hci0,hci1,...}/dev_XX_XX_XX_XX_XX_XX/sepX
                  (Client role)
```

# DS220 Audio Adapter - `busctl` Media Endpoint

```
[duncan@ArtII 2025--CackalackyCon]$ busctl tree org.bluez
└─ /org
  └─ /org/bluez
    └─ /org/bluez/hci0
      ├─ /org/bluez/hci0/dev_53_4A_52_FE_01_38
      │ ├─ /org/bluez/hci0/dev_53_4A_52_FE_01_38/sep1
      │ │ └─ /org/bluez/hci0/dev_53_4A_52_FE_01_38/sep1/fd5
      │ ├─ /org/bluez/hci0/dev_53_4A_52_FE_01_38/sep10
      │ ├─ /org/bluez/hci0/dev_53_4A_52_FE_01_38/sep3
      │ ├─ /org/bluez/hci0/dev_53_4A_52_FE_01_38/sep5
      │ ├─ /org/bluez/hci0/dev_53_4A_52_FE_01_38/sep6
      │ ├─ /org/bluez/hci0/dev_53_4A_52_FE_01_38/sep7
      │ └─ /org/bluez/hci0/dev_53_4A_52_FE_01_38/sep8
      ├─ /org/bluez/hci0/dev_58_2F_40_8A_45_1B
      ├─ /org/bluez/hci0/dev_64_A2_F9_BC_8E_95
      ├─ /org/bluez/hci0/dev_94_C9_60_AE_2D_41
      └─ /org/bluez/hci0/dev_E2_73_E7_F7_7B_05
[duncan@ArtII 2025--CackalackyCon]$ busctl introspect org.bluez /org/bluez/hci0/dev_53_4A_52_FE_01_38/sep1
NAME                                TYPE      SIGNATURE RESULT/VALUE                                FLAGS
org.bluez.MediaEndpoint1            interface -         -                                           -
.SetConfiguration                   method    oa{sv}    -                                           -
.Capabilities                       property  ay        4 255 255 2 53                            emits-change
.Codec                              property  y         0                                         emits-change
.DelayReporting                     property  b         false                                     emits-change
.Device                             property  o         "/org/bluez/hci0/dev_53_4A_52_FE_01_38"   emits-change
.UUID                               property  s         "0000110b-0000-1000-8000-00805f9b34fb"    emits-change
org.freedesktop.DBus.Introspectable interface -         -                                           -
.Introspect                         method    -         s                                         -
org.freedesktop.DBus.Properties     interface -         -                                           -
.Get                                method    ss        v                                         -
.GetAll                             method    s         a{sv}                                     -
```

# BlueZ Documentation - Media Transport

```
========================
org.bluez.MediaTransport
========================

-----------------------------------------
BlueZ D-Bus MediaTransport API documentation
-----------------------------------------

:Version: BlueZ
:Date: July 2024
:Manual section: 5
:Manual group: Linux System Administration

Interface
=========

:Service:         org.bluez
:Interface:       org.bluez.MediaTransport1
:Object path:     [variable prefix]/{hci0,hci1,...}/dev_XX_XX_XX_XX_XX_XX/fdX

Methods
-------

fd, uint16, uint16 Acquire()
````````````````````````````
```
```

DS220 Audio Adapter - `busctl` Media Transport

```
[duncan@ArtII 2025--CackalackyCon]$ busctl introspect org.bluez /org/bluez/hci0/dev_53_4A_52_FE_01_38/sep1/fd5
NAME                                TYPE      SIGNATURE RESULT/VALUE                              FLAGS
org.bluez.MediaTransport1           interface -         -                                         -
.Acquire                            method    -         hqq                                       -
.Release                            method    -         -                                         -
.Select                             method    -         -                                         -
.TryAcquire                         method    -         hqq                                       -
.Unselect                           method    -         -                                         -
.Codec                              property  y         0                                         emits-change
.Configuration                      property  ay        4 33 21 2 53                              emits-change
.Delay                              property  q         -                                         emits-change writable
.Device                             property  o         "/org/bluez/hci0/dev_53_4A_52_FE_01_38"   emits-change
.State                              property  s         "idle"                                    emits-change
.UUID                               property  s         "0000110a-0000-1000-8000-00805f9b34fb"    emits-change
.Volume                             property  q         84                                        emits-change writable
org.freedesktop.DBus.Introspectable interface -         -                                         -
.Introspect                         method    -         s                                         -
org.freedesktop.DBus.Properties     interface -         -                                         -
.Get                                method    ss        v                                         -
.GetAll                             method    s         a{sv}                                     -
.Set                                method    ssv       -                                         -
.PropertiesChanged                  signal    sa{sv}as  -                                         -
```

How To Develop



BLEEP-ing Improvements

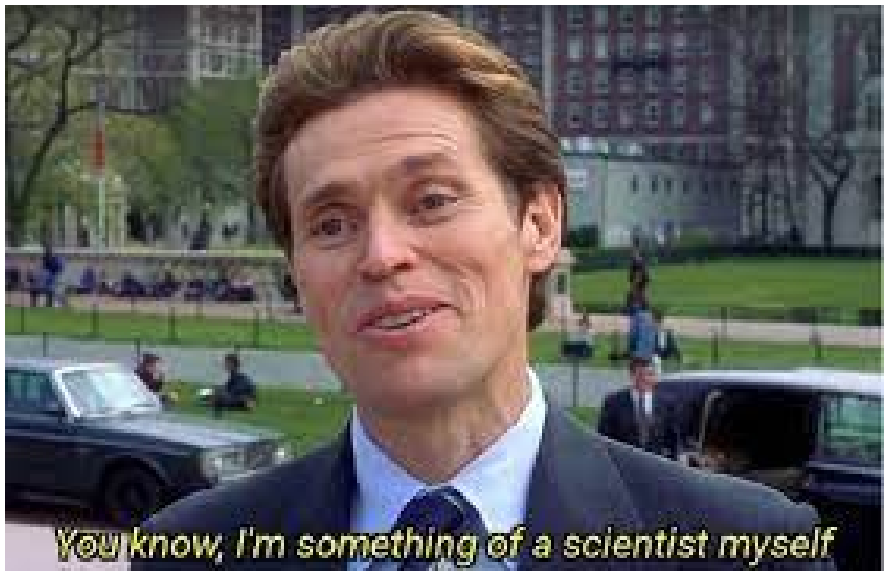
```
Media Control Properties:
        Connected:                  True

[*] Generating Media Endpoit Inspection Structures
[+] Completed Generating Media Endpoint Inspection Structures
Media Endpoint Properties:
        UUID:               0000110b-0000-1000-8000-00805f9b34fb
        Codec:              0
        Capabilities:               [255, 255, 2, 53]
        Device:             /org/bluez/hci0/dev_53_4A_52_FE_01_38
        DelayReporting:             False

Media Endpoint Properties:
        UUID:               0000110b-0000-1000-8000-00805f9b34fb
        Codec:              0
        Capabilities:               [255, 255, 2, 53]
        Device:             /org/bluez/hci0/dev_53_4A_52_FE_01_38
        DelayReporting:             False
```

BLEEP-ing Improvements

```
Media Endpoint Properties:
        UUID:           0000110b-0000-1000-8000-00805f9b34fb
        Codec:          0
        Capabilities:           [255, 255, 2, 53]
        Device:         /org/bluez/hci0/dev_53_4A_52_FE_01_38
        DelayReporting:         False

[*] find_and_get__interface_introspection__full_enumeration::Extracting E-Tree Details from Target Introspection
[!] Introspection E-Tree Information:           <Element 'node' at 0x75f41a788860>
Root Tag:       [ node ]                -               Root Attrib:    [ {} ]
        Child Tag:      [ interface ]           -               Child Attrib:   [ {'name': 'org.freedesktop.DBus.Introspectable'
        Child Tag:      [ interface ]           -               Child Attrib:   [ {'name': 'org.bluez.Device1'} ]
        Child Tag:      [ interface ]           -               Child Attrib:   [ {'name': 'org.freedesktop.DBus.Properties'} ]
        Child Tag:      [ interface ]           -               Child Attrib:   [ {'name': 'org.bluez.MediaControl1'} ]
        Child Tag:      [ node ]                -               Child Attrib:   [ {'name': 'sep1'} ]
        Child Tag:      [ node ]                -               Child Attrib:   [ {'name': 'sep10'} ]
        Child Tag:      [ node ]                -               Child Attrib:   [ {'name': 'sep3'} ]
        Child Tag:      [ node ]                -               Child Attrib:   [ {'name': 'sep5'} ]
        Child Tag:      [ node ]                -               Child Attrib:   [ {'name': 'sep6'} ]
        Child Tag:      [ node ]                -               Child Attrib:   [ {'name': 'sep7'} ]
        Child Tag:      [ node ]                -               Child Attrib:   [ {'name': 'sep8'} ]
[*] find_and_get__interface_introspection__full_enumeration::Extracting E-Tree Details from Target Introspection
[!] Introspection E-Tree Information:           <Element 'node' at 0x75f41a78a6b0>
Root Tag:       [ node ]                -               Root Attrib:    [ {} ]
        Child Tag:      [ interface ]           -               Child Attrib:   [ {'name': 'org.freedesktop.DBus.Introspectable'
        Child Tag:      [ interface ]           -               Child Attrib:   [ {'name': 'org.bluez.MediaEndpoint1'} ]
        Child Tag:      [ interface ]           -               Child Attrib:   [ {'name': 'org.freedesktop.DBus.Properties'} ]
        Child Tag:      [ node ]                -               Child Attrib:   [ {'name': 'fd7'} ]
```

Lessons Learned

- Variety of Wildlife Implementations
  - Multi-Descriptors per Characteristic, Canaries
- Vendor Specific Operations + Behavior
  - Manufacturer Data, Vendor Specific Codes
- Fake it or just have fun with it
  - Audio - Whateva' whateva' I do what I want!



Pain Points

Pain Points #001

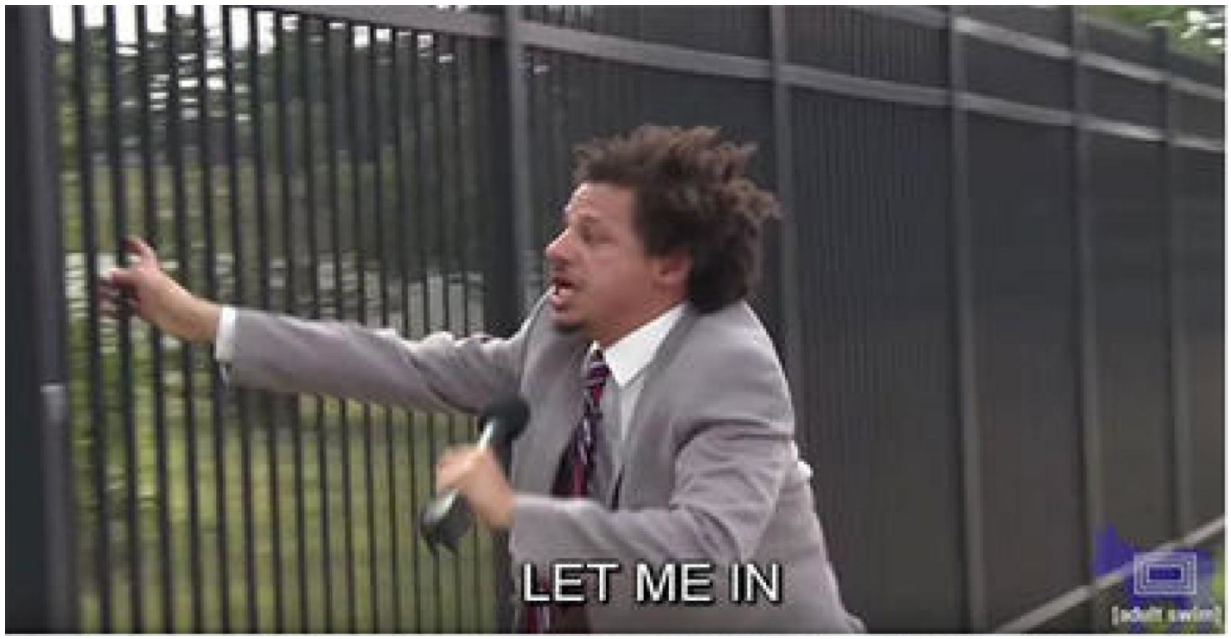
Why all the secrets?

- Hard to find good examples
  - Intended operation
  - Security is **Magical** and etherial
- If **ANYONE** find a good security/pairing example, *PLEASE* tell me!!!

Pain Points #002

Abstract this!

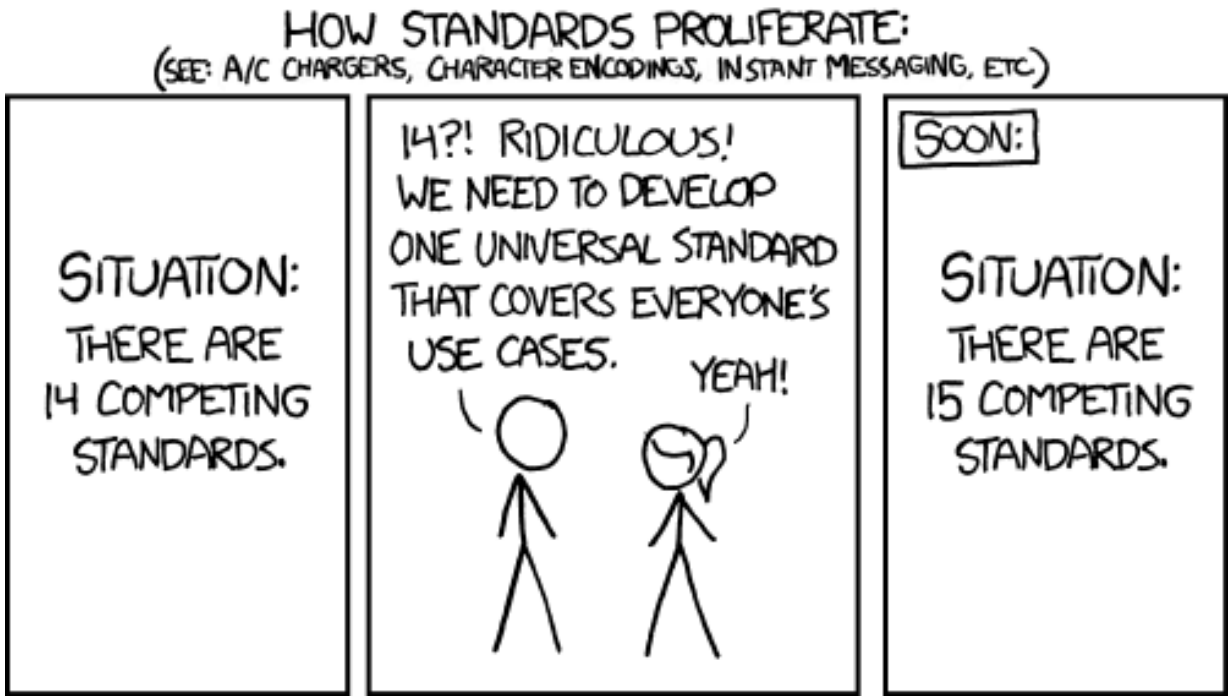
- Eventually hit bedrock
  - The rabbit hole has a wall in it
  - Lack of transparency in lower-levels
- Time for more Reverse Engineering!



Pain Points #003

Everyone is the cutting edge developer?

- Everyone can do whatever they want
- Even `btmon` returns Vendor Specific or Unknown
- Time to start cataloging...



Fantastic Bluetooth Talks and Where to Find Them

Bluetooth Landscape Exploration & Enumeration Platform (BLEEP)

- CackalackyCon 2024 [S + V]
- BSidesLV 2024 [S + V]
- DefCon 32 Demo Labs [S]

General Background and Development:

- Null404 Talk 1 [S + V]
- Null404 Talk 2 [S + V]

Key Wildlife Observation Tools and How to Build Them

Projects and Documentation for Development Work

- RealTek BW-16
- Pico WH Development
- Bletsubushi

Warning: Quality of Documentation may Vary.....

Future Work

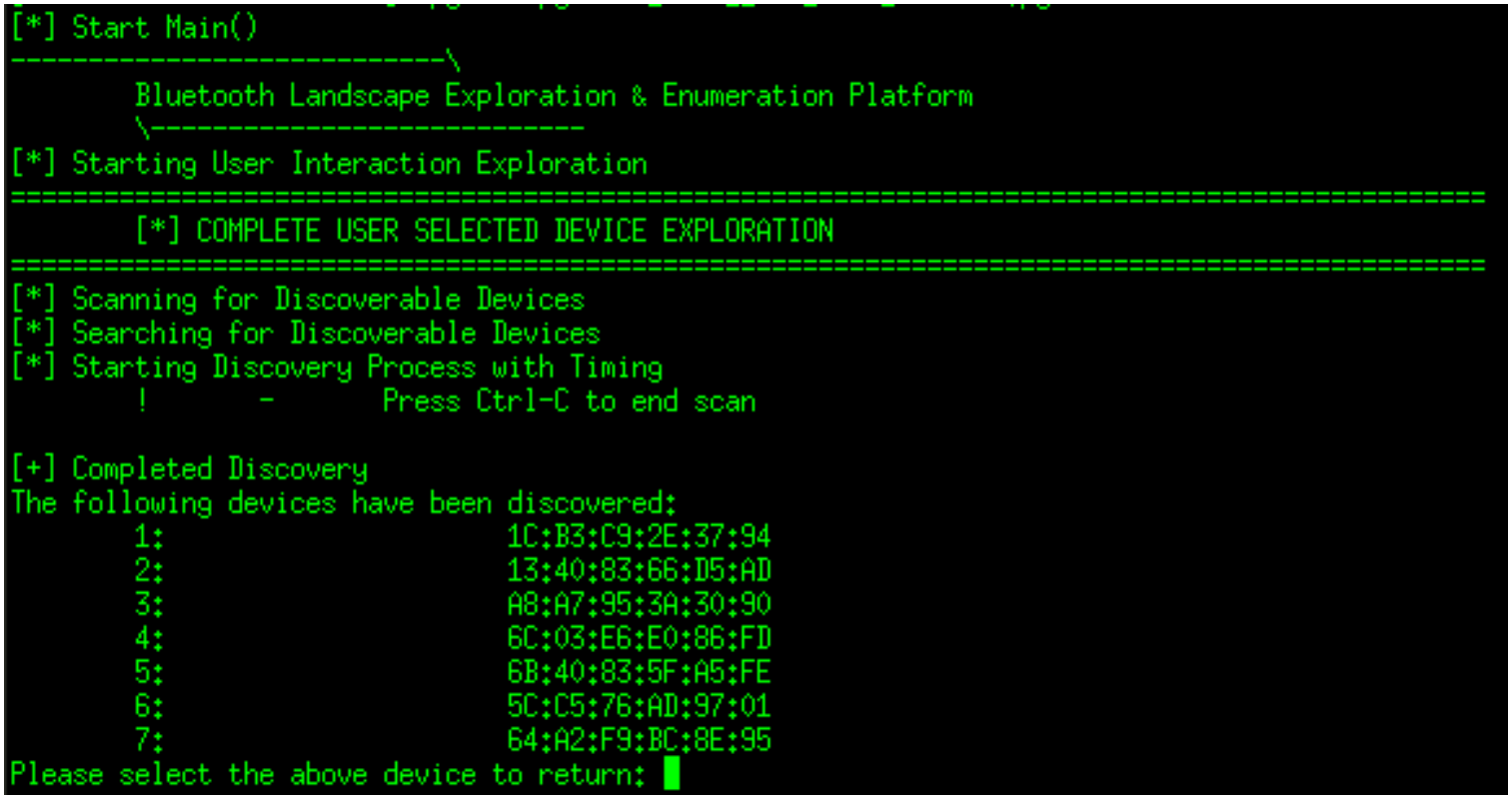
- Continue to dissect and explore the information that BLE devices transmit
  - All manufacturer/vendor specific
  - Who does not love a good information leak?
  - Git gud at Reverse Engineering!!
- Develop more things to learn what is out there!
  - Expand knowledge of the limitations
  - Hardware specific constrains and capabilities
- Expand further into Bluetooth Classic (BD/EDR)
  - BLE has been the embedded system/IoT bed rock
  - BD/EDR appears to be the audio development + casting bed rock

Questions

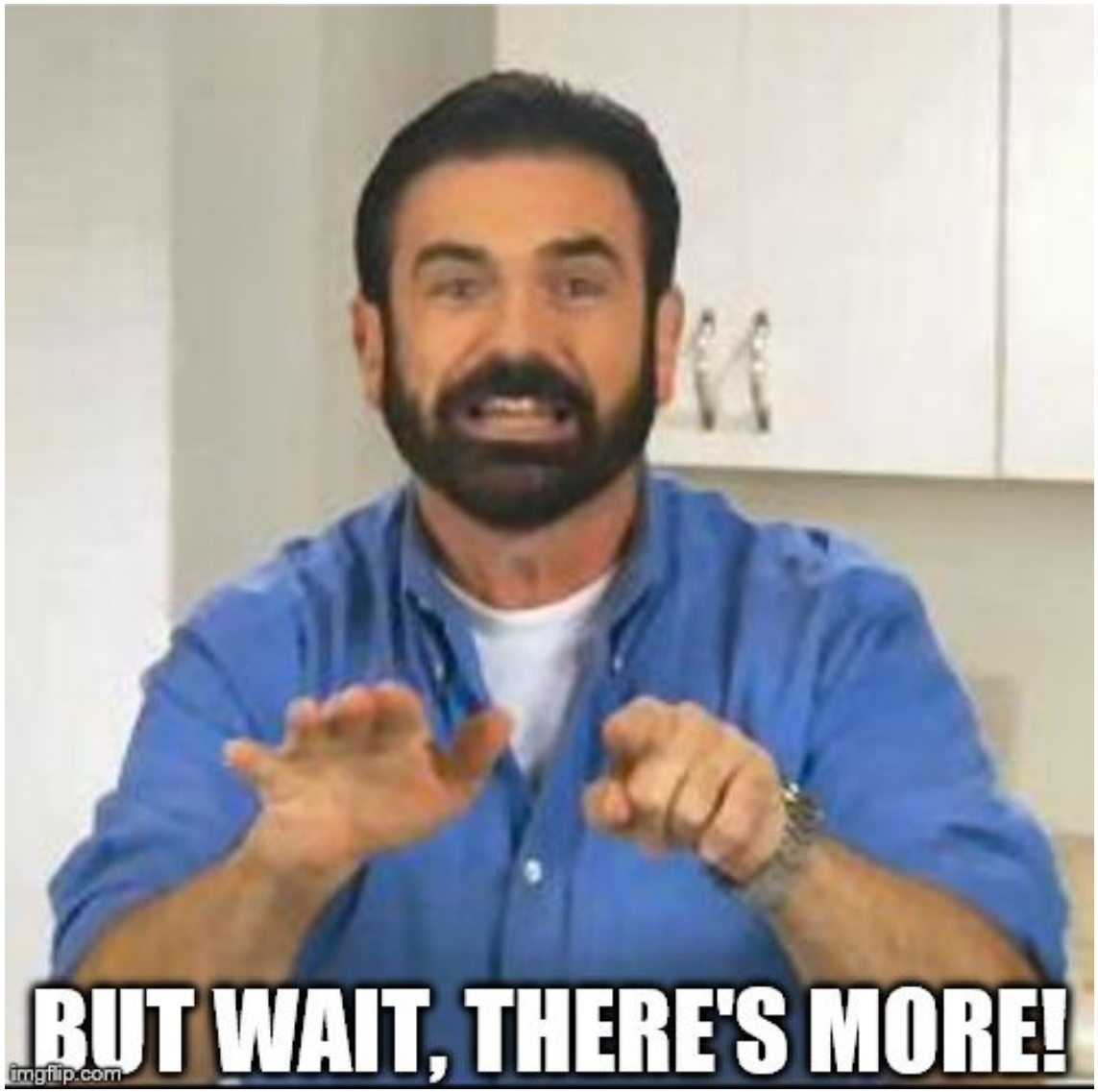
Questions?

Research Details

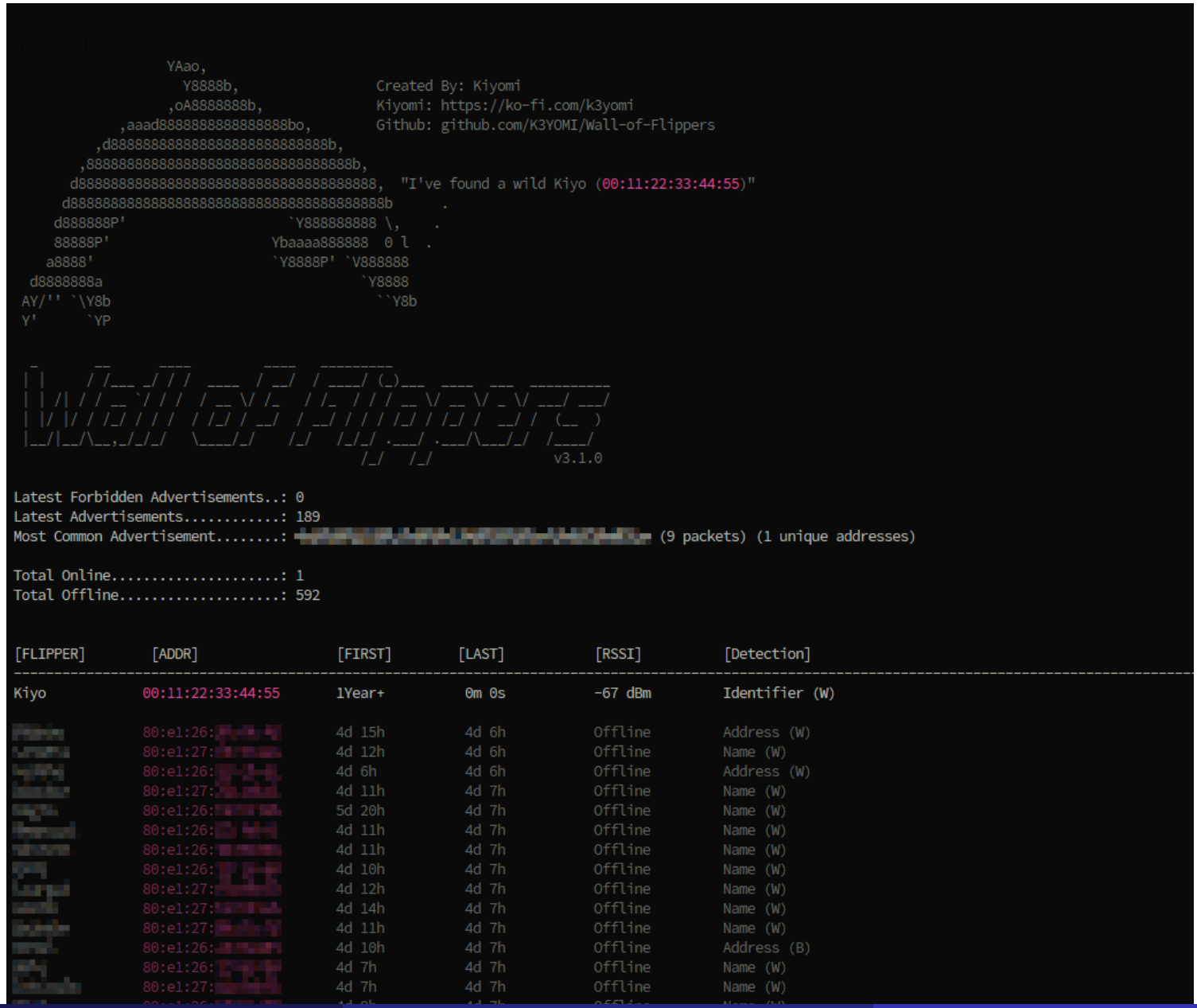
- Git Repo: https://github.com/Mauddib28/bleep-tool



What About the Hackers?



Wall of Flippers



Wall of Flippers

Identifies Flipper Devices

- Examines the Advertisement Packets
- Extracts the Device Address to determine if a now Flipper MAC

BLE Nano Shark

This project successfully funded on December 19, but you can still Late Pledge for available rewards.

BLEShark Nano: A Compact Wireless Multi-Tool for Hackers

A portable device for testing Bluetooth and Wi-Fi vulnerabilities—including games, apps, auto updates, and a smooth interface.

$81,540

pledged of **$3,482 goal**

1,709

backers

Back th

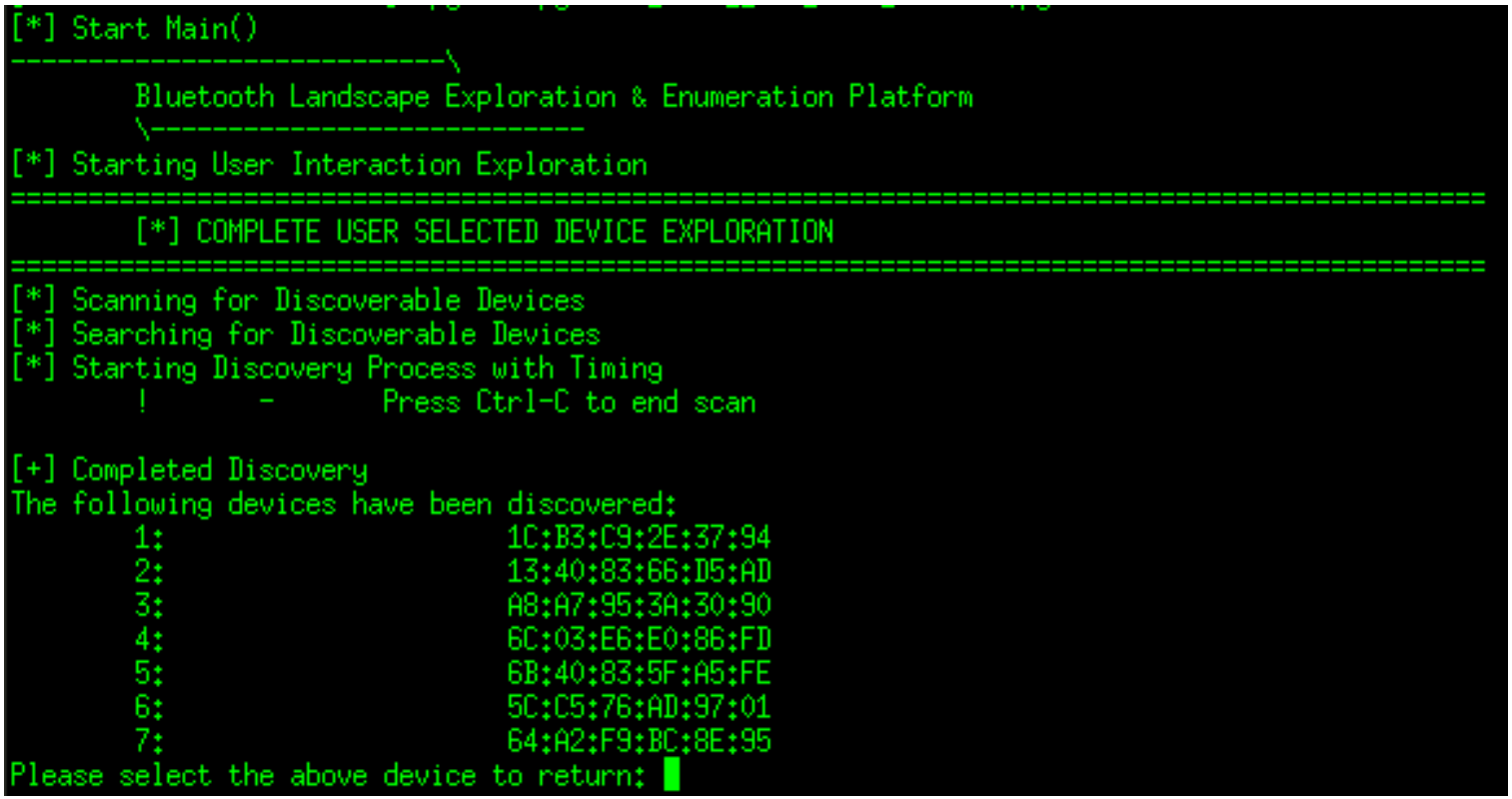
Save

BLE Nano Shark

- Combines several existing tools into one toy
- Leverages pairing capability to display requests
  - Most likely due to secondary or tertiary thread/process to handle pairing
  - Agent? Agent Manager?
  - Note: MOST interested in dissecting how this was done

Bluetooth Landscape Exploration & Enumeration Platform

- Git Repo: https://github.com/Mauddib28/bleep-tool



Bibliography References I

Freedesktop

What is D-Bus, Published 2022

https://www.freedesktop.org/wiki/Software/dbus/

Last Accessed: 2024-03-28 22:43:19 EST

GNU

Knowing the Details of D-Bus Services

https://www.gnu.org/software/emacs/manual/html_node/dbus/Introspection.html

Last Accessed: 2024-04-01 19:48:34 EST

Programiz

Python Decorators

https://www.programiz.com/python-programming/decorator

Last Accessed: 2024-04-01 19:52:34 EST

Bibliography References II

hbldh

characteristic.py

https://github.com/hbldh/bleak/blob/63adefa24cb6ed11c8cf154fa41f51ecff1df98c/bleak/backends/characteristic.py

Last Accessed: 2024-04-01 19:56:34 EST

elsampsa

Bluetooth + DBus + gobject demo

https://github.com/elsampsa/btdemo

Last Accessed: 2024-04-01 19:54:52 EST

Freedesktop

DbusTools, Published May 07 2021

https://www.freedesktop.org/wiki/Software/DbusTools/

Last Accessed: 2024-03-28 22:57:29 EST

Bibliography References III


Bluetooth SIG
assigned_numbers
https://bitbucket.org/bluetooth-SIG/public/src/main/assigned_numbers/
Last Accessed: 2024-04-01 21:00:29 EST


Bluetooth SIG
public bitbucket
https://bitbucket.org/bluetooth-SIG/public/src/main/
Last Accessed: 2024-04-02 15:13:33 EST


Archlinux Forum
Activation via systemd failed for unit dbus-org.bluez.service
https://bbs.archlinux.org/viewtopic.php?id=155714
Last Accessed: 2024-04-02 15:09:42 EST

Bibliography References IV

oscaracena

gattlib.h

https://github.com/oscaracena/pygattlib/blob/7d08c0805313201b2ab12628e19544bb180218a8/src/gattlib.h

Last Accessed: 2024-04-02 15:09:42 EST

Bluetooth SIG

Bluetooth for Linux Developers Study Guide - Versions 1.0, 1.0.1

https://www.bluetooth.com/bluetooth-resources/bluetooth-for-linux/

Last Accessed: 2021-12-29 10:26:27 EST, 2022-10-18 18:54:02 EST

Bibliography References V


Bluetooth SIG
Developer Study Guide Bluetooth Internet Gateways - Version 2.0.0
https://www.bluetooth.com/blog/the-bluetooth-internet-gateway-study-guide/
Last Accessed: 2021-07-21 14:46:56 EST


Bluetooth SIG
Bluetooth LE Developer Study Guide - Version 5.2.0
https://www.bluetooth.com/bluetooth-resources/bluetooth-le-developer-starter-kit/
Last Accessed: 2023-02-16 11:36:57 EST

Bibliography References VI

Bluetooth SIG

Bluetooth Core Specification - Versions 5.3, 5.4

https://www.bluetooth.com/specifications/specs/core-specification-5-[3—4]/

Last Accessed: 2023-12-19 13:24:22 EST, 2023-12-16 11:33:37 EST

Bluetooth SIG

Generic Attribute Profile (GATT)

https://www.bluetooth.com/wp-content/uploads/Files/Specification/HTML/Core-54/out/en/host/generic-attribute-profile–gatt-.html

Last Accessed: 2023-12-16 11:22:03 EST

Marcel Holtmann, Maxim Krasnyansky, Qualcomm

BlueZ - Bluetooth protocol stack for Linux

https://git.kernel.org/pub/scm/bluetooth/bluez.git/tree/doc

Last Accessed: 2024-04-11 10:39:23 EST

Bibliography References VII

Espressif

Arduino Core for the ESP32

https://github.com/espressif/arduino-esp32/tree/master

Last Accessed: 2025-04-24 11:32:28 EST

Nordic DevZone Forum

Available 16-bit UUIDs

https://devzone.nordicsemi.com/f/nordic-q-a/26248/available-16-bit-uuids#:~:text=I%20found%20a%20case%20of,Best%20regards!

Last Accessed: 2025-04-26 12:47:23 EST

Jimmywong

Advertising Payload format on BLE

https://jimmywongiot.com/2019/08/13/advertising-payload-format-on-ble/

Last Accessed: 2025-04-28 19:38:44 EST