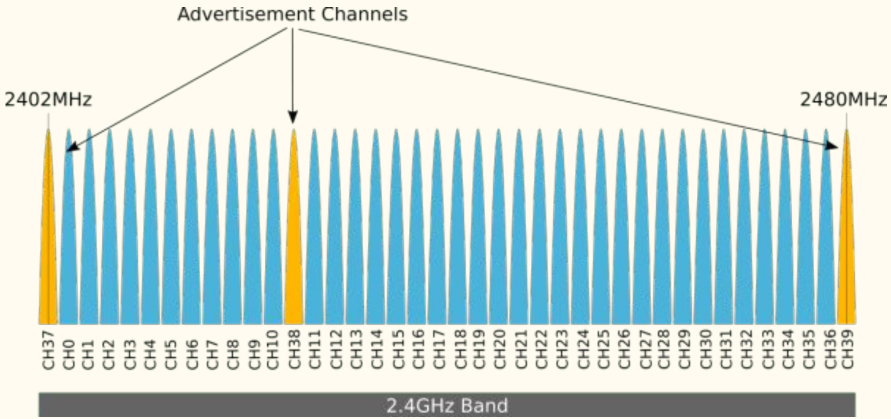
Open Bar at the Playground: Condensed Edition

Black Alps 2023 | @SamZorSec

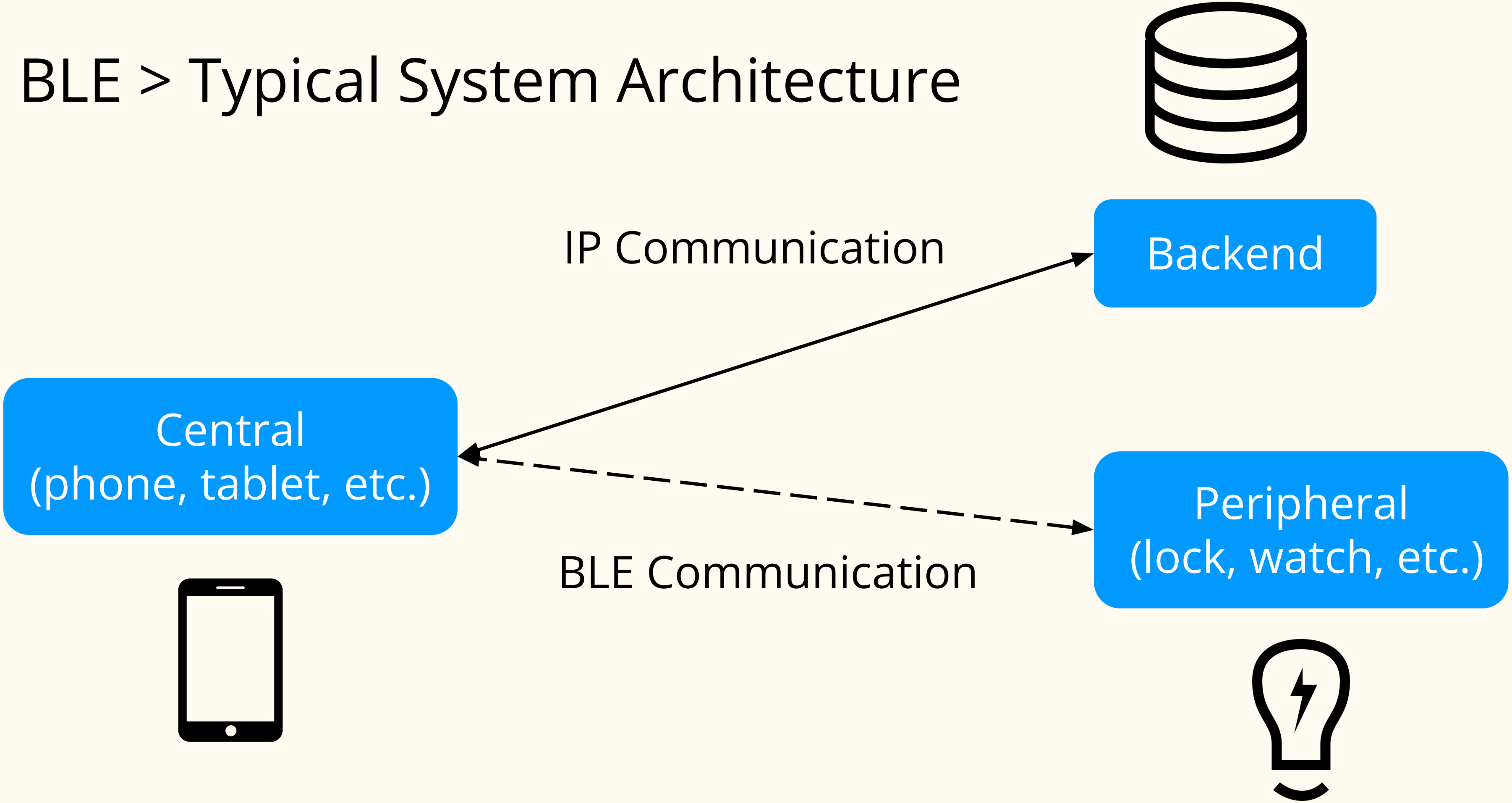
What is BLE and how it works?

BLE > Introduction

- BLE → Bluetooth Low Energy
- **Short range** wireless protocol
  - 2.4 GHz ISM band
  - 40x 2 MHz channels
- **Low power** consumption
- Use-cases
  - Wearable fitness trackers
  - Lightbulbs
  - Beacons
  - Etc.



BLE > Typical System Architecture



IP Communication

Backend

Central
(phone, tablet, etc.)

Peripheral
(lock, watch, etc.)

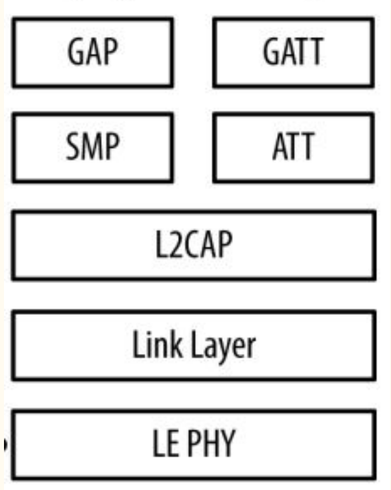
BLE Communication

BLE > Stack

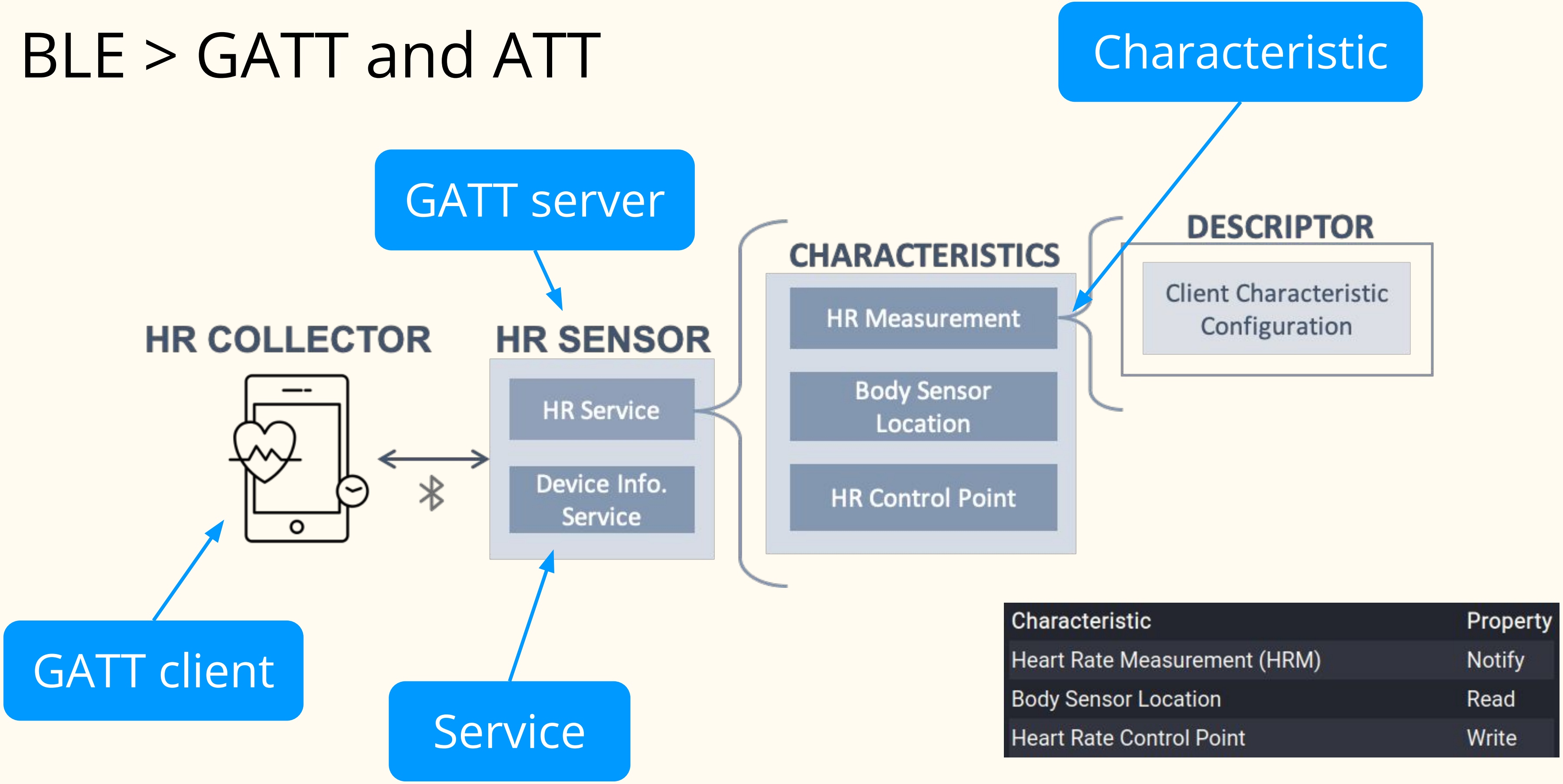
- Generic Attribute Profile (GATT)
  - Defines how data is **organized and exchanged**
  - Establishes a **hierarchy of services** and **characteristics**
- Attribute Protocol (ATT)
  - Defines the **format** and **rules** for reading and writing attributes
  - Common properties
    - Read
    - Write
    - Notify
    - Indicate

Represent a functionality

Represent a data element

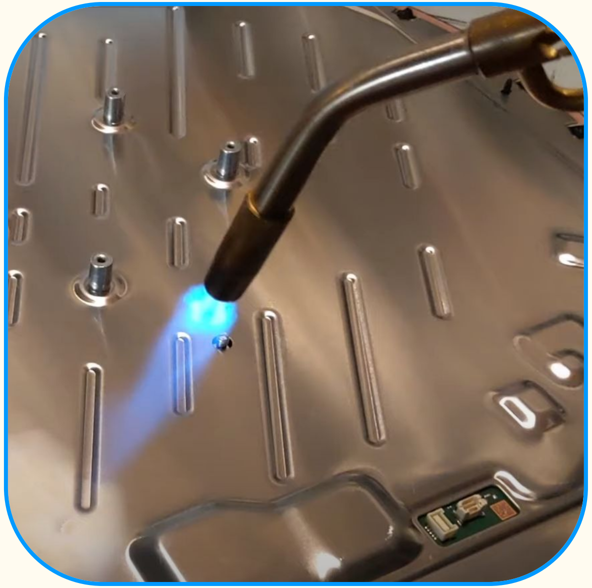


BLE > GATT and ATT

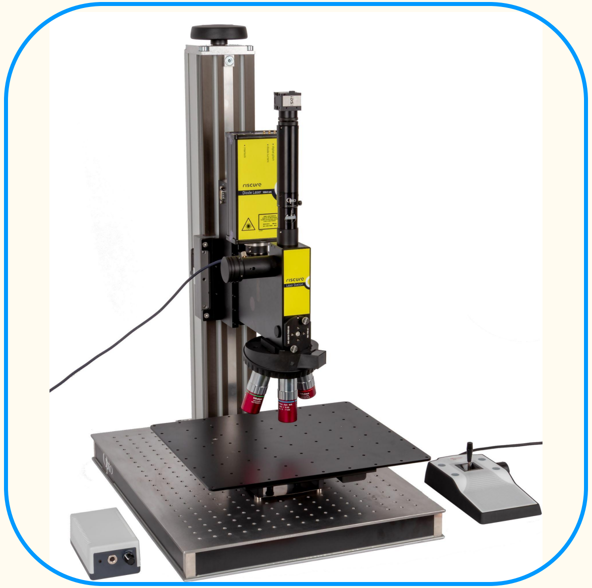


Characteristic	Property
Heart Rate Measurement (HRM)	Notify
Body Sensor Location	Read
Heart Rate Control Point	Write

What tools can I use to target a BLE device?

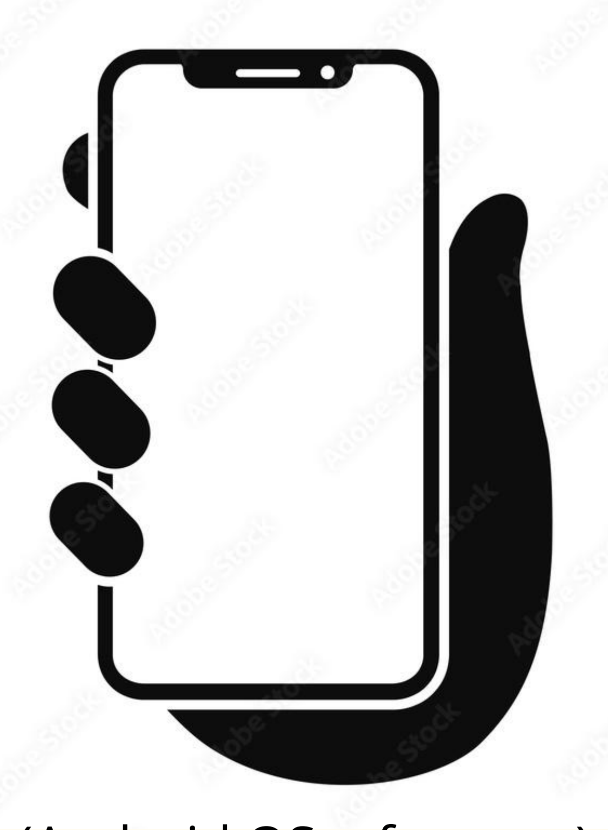


~~Blowtorch~~



~~Laser Station~~

~~Ground Antenna~~

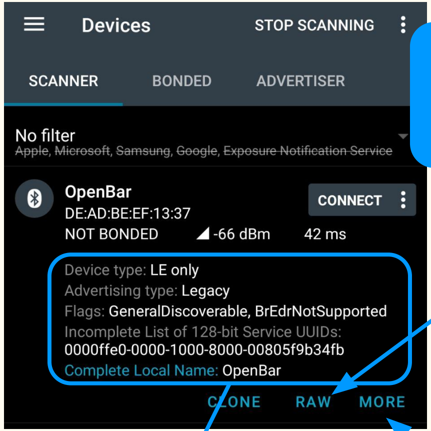


(Android OS, of course)

+
nRF Connect for Mobile

+
Android Bluetooth HCI snoop log

[Bonus] BLE > Tools > nRF Connect for Mobile



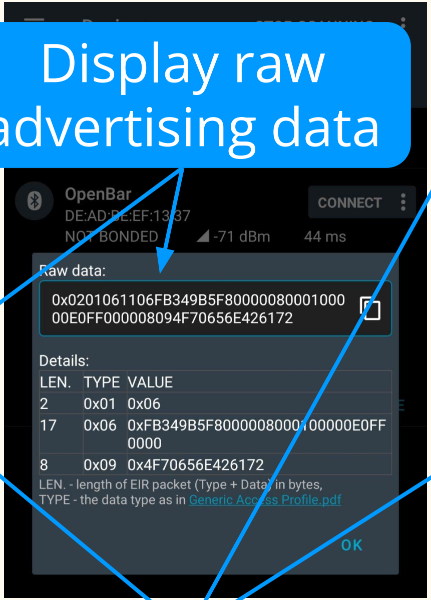
No filter
~~Apple, Microsoft, Samsung, Google, Exposure Notification Service~~

OpenBar
DE:AD:BE:EF:13:37
NOT BONDED -66 dBm 42 ms

Device type: LE only
Advertising type: Legacy
Flags: GeneralDiscoverable, BrEdrNotSupported
Incomplete List of 128-bit Service UUIDs:
0000ffe0-0000-1000-8000-00805f9b34fb
Complete Local Name: OpenBar

Advertising data

Display raw advertising data



OpenBar
DE:AD:BE:EF:13:37
NOT BONDED -71 dBm 44 ms

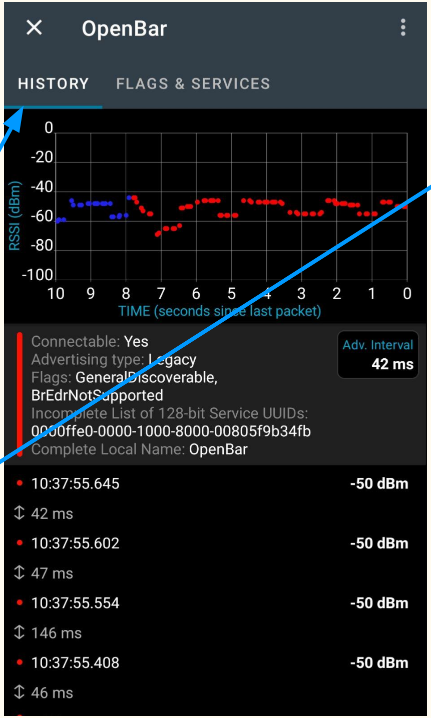
Raw data:

0x0201061106FB349B5F80000080001000
00E0FF000008094F70656E426172

Details:

LEN.	TYPE	VALUE
2	0x01	0x06
17	0x06	0xFB349B5F8000008000100000E0FF 0000
8	0x09	0x4F70656E426172

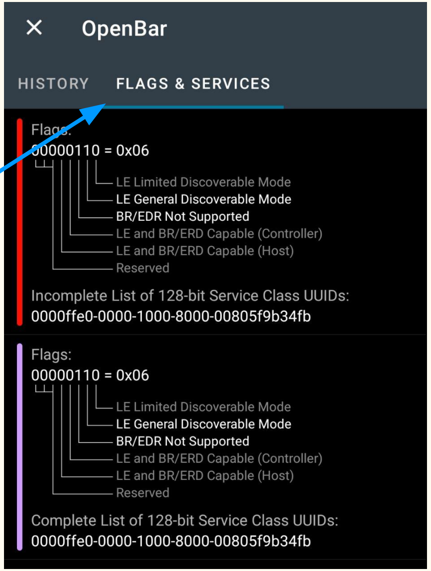
LEN. - length of EIR packet (Type + Data) in bytes,
TYPE - the data type as in Generic Access Profile.pdf



Connectable: Yes
Advertising type: Legacy
Flags: GeneralDiscoverable,
BrEdrNotSupported
Incomplete List of 128-bit Service UUIDs:
0000ffe0-0000-1000-8000-00805f9b34fb
Complete Local Name: OpenBar

Adv. Interval
42 ms

10:37:55.645	-50 dBm
↕ 42 ms	
10:37:55.602	-50 dBm
↕ 47 ms	
10:37:55.554	-50 dBm
↕ 146 ms	
10:37:55.408	-50 dBm
↕ 46 ms	



Flags:
00000110 = 0x06
LE Limited Discoverable Mode
LE General Discoverable Mode
BR/EDR Not Supported
LE and BR/ERD Capable (Controller)
LE and BR/ERD Capable (Host)
Reserved

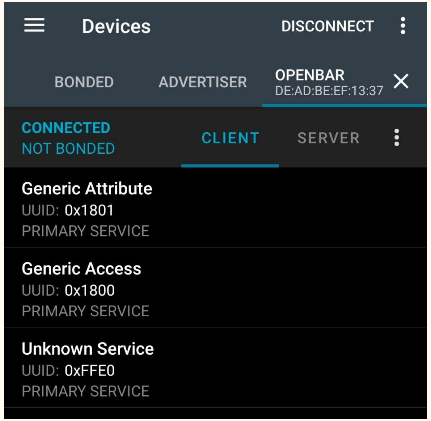
Incomplete List of 128-bit Service Class UUIDs:
0000ffe0-0000-1000-8000-00805f9b34fb

Flags:
00000110 = 0x06
LE Limited Discoverable Mode
LE General Discoverable Mode
BR/EDR Not Supported
LE and BR/ERD Capable (Controller)
LE and BR/ERD Capable (Host)
Reserved

Complete List of 128-bit Service Class UUIDs:
0000ffe0-0000-1000-8000-00805f9b34fb

Display history, flags and services

[Bonus] BLE > Tools > nRF Connect for Mobile



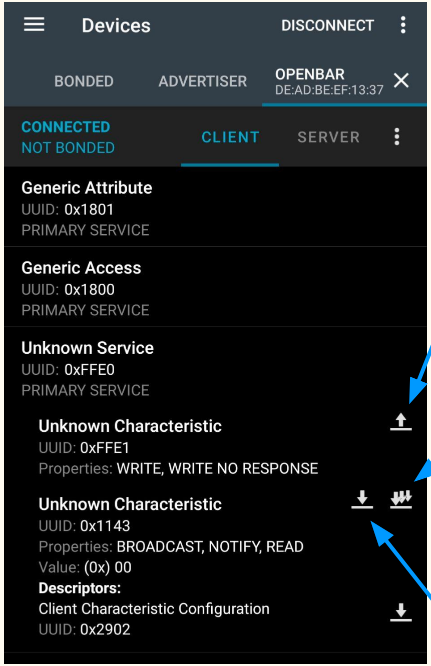
DE:AD:BE:EF:13:37

CONNECTED
NOT BONDED

Generic Attribute
UUID: 0x1801
PRIMARY SERVICE

Generic Access
UUID: 0x1800
PRIMARY SERVICE

Unknown Service
UUID: 0xFFE0
PRIMARY SERVICE



DE:AD:BE:EF:13:37

CONNECTED
NOT BONDED

Generic Attribute
UUID: 0x1801
PRIMARY SERVICE

Generic Access
UUID: 0x1800
PRIMARY SERVICE

Unknown Service
UUID: 0xFFE0
PRIMARY SERVICE

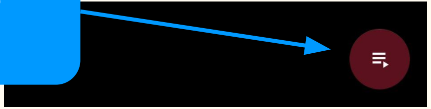
Unknown Characteristic
UUID: 0xFFE1
Properties: WRITE, WRITE NO RESPONSE

Unknown Characteristic
UUID: 0x1143
Properties: BROADCAST, NOTIFY, READ
Value: (0x) 00
Descriptors:
Client Characteristic Configuration
UUID: 0x2902

Write to the characteristic

Subscribe to notifications

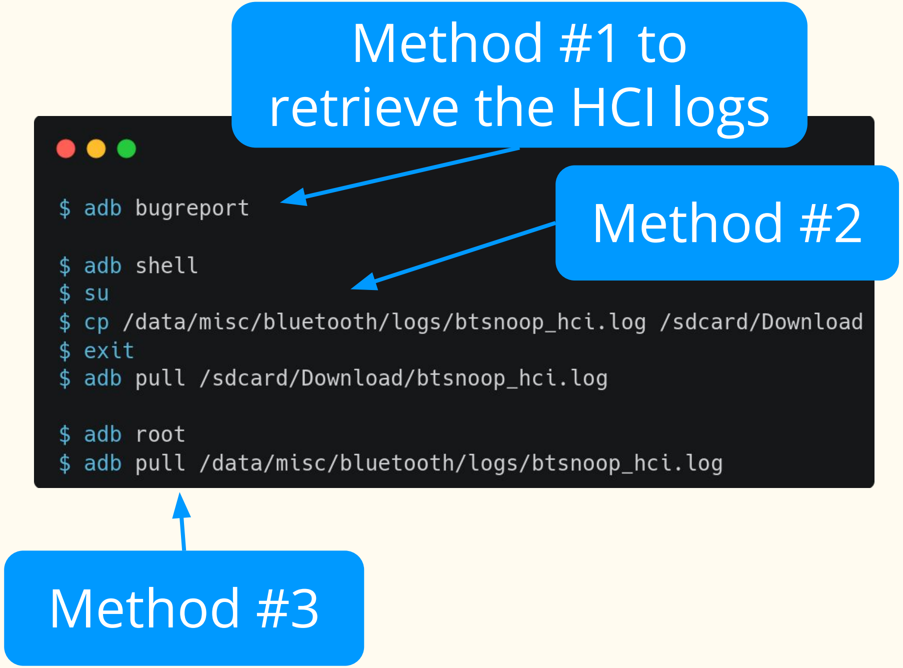
Read the characteristic



Create or trigger a macro

[Bonus] BLE > Tools > Bluetooth HCI snoop log

- Allows to retrieve all **Bluetooth** Host Controller Host interface (HCI) **logs into a single file**
- Features
  - Available by default
    - Settings > System > Developer options > Enable Bluetooth HCI snoop log
  - Logging happens before the BLE Link Layer encryption (if any)
- HCI logs are generally stored in /data/misc/bluetooth/logs



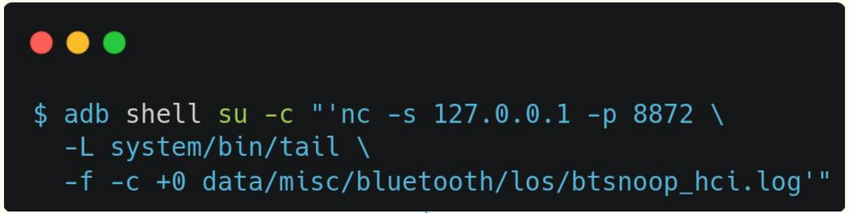
Method #1 to retrieve the HCI logs

Method #2

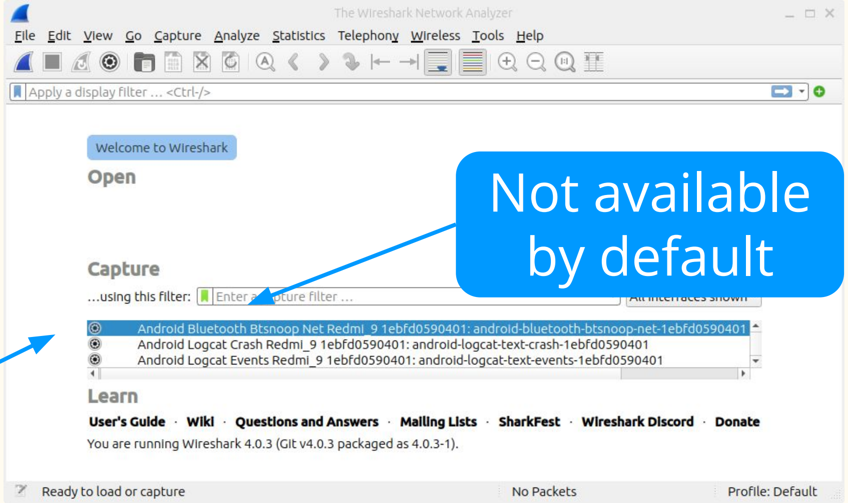
Method #3

```
$ adb bugreport

$ adb shell
$ su
$ cp /data/misc/bluetooth/logs/btsnoop_hci.log /sdcard/Download
$ exit
$ adb pull /sdcard/Download/btsnoop_hci.log

$ adb root
$ adb pull /data/misc/bluetooth/logs/btsnoop_hci.log
```

[Bonus] BLE > Tools > Bluetooth HCI snoop log



```
$ adb shell su -c "'nc -s 127.0.0.1 -p 8872 \
  -L system/bin/tail \
  -f -c +0 data/misc/bluetooth/los/btsnoop_hci.log'"
```



The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Open
Capture
…using this filter:
Enter a capture filter …
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

Android Bluetooth Btsnoop Net Redmi_9 1ebfd0590401: android-bluetooth-btsnoop-net-1ebfd0590401
Android Logcat Crash Redmi_9 1ebfd0590401: android-logcat-text-crash-1ebfd0590401
Android Logcat Events Redmi_9 1ebfd0590401: android-logcat-text-events-1ebfd0590401

You are running Wireshark 4.0.3 (Git v4.0.3 packaged as 4.0.3-1).

Ready to load or capture
No Packets
Profile: Default

Not available by default

Allows to capture HCI logs in realtime

Demo #1

What tools can I use to target a (more secure) BLE device?

BLE > Tools

- Mirage
    - Swiss army knife to interact with BLE devices (also ZigBee, Wi-Fi, etc.)
        - MITM
        - Jamming / hijacking
        - Scenarios
- Sniffle
    - Sniffer for BLE 4.0 and 5.0
- Bleak
    - Multi-platform python library to interact with a BLE Server
- Bless
    - Multi-platform python library to implement a BLE Server

[Bonus] BLE > Tools > Mirage

- Scan for BLE devices
    - `mirage ble_scan`
- Connect to a device and discover its services and characteristics
    - `mirage ble_master`
    - `connect <MAC> [<connection type>]`
    - `discover`
- Perform a MITM
    - `mirage ble_mitm TARGET=<MAC>`
- Monitor BLE communications from an ADB interface
    - `mirage ble_monitor`

[Bonus] BLE > Tools > EXPLIoT

- Scan for BLE devices

  -
    ```
    run ble.generic.scan --timeout <timeout>
    ```
- Connect to a device and discover its services and characteristics

  -
    ```
    run ble.generic.enum --addr <MAC> --randaddrtype --services --chars
    ```
- Fuzz a specific characteristic

  -
    ```
    run ble.generic.fuzzchar --addr <MAC> --handle <handle> --value <x>
    ```

Demo #2

Conclusion

- Both companies behind the two demonstrations have been contacted
- Both companies should apply patches until the end of the year
- None of the companies has a solution called **OpenBar** ;-)

BLE > Additional Learning Resources

- BLE HackMe
  - https://smartlockpicking.com/ble_hackme/
- BLE CTF
  - https://github.com/hackgnar/ble_ctf
- BLE CTF 2.0
  - https://github.com/hackgnar/ble_ctf_infinity

References

- https://i0.wp.com/embeddedcentric.com/wp-content/uploads/2019/03/bluetooth_ble_spectrum.png
- https://atadiat.com/wp-content/uploads/2018/09/BLE-Stack.png
- https://getquote.riscure.com/media/24970/ls2-complete-fr.jpg
- https://www.youtube.com/watch?v=omScudUro3s
- https://www.viasat.com/content/dam/us-site/antenna-systems/images/1112362_WebCon_Ground_Antennas_AS_Inset_Image4_001.jpg.transform/medium/img.jpeg
- https://as1.ftcdn.net/v2/jpg/02/72/17/48/1000_F_272174843_qMXMxCOzFlNST6AMjDqBQFyjWEUZfqoL.jpg