Hacking Sony Camera's for fun and profit

Rahul Ravikumar

@tikurahul

The Camera

Sony A7R Mark V
Supports BLE, WiFi Direct

Why?

Why?

Imaging Edge Mobile

1.9 ★ | 10M+ Downloads

Why?

Why?

Imaging Edge Mobile

1.9 ★ | 10M+ Downloads

Creator's App

3.3 ★ | 500K+ Downloads

App Features

- Sony Cloud Storage & Sync
- Community
- Preview
- Remote Control
- Transfer Photos

App Features

- Sony Cloud Storage & Sync
- Community
- Preview
- Remote Control
- Transfer Photos

Agenda

1. Reverse Engineer the BLE Remote Protocol
2. Build a Compose Multiplatform App (that uses the protocol)
3. Profit ?

Basics

Basics

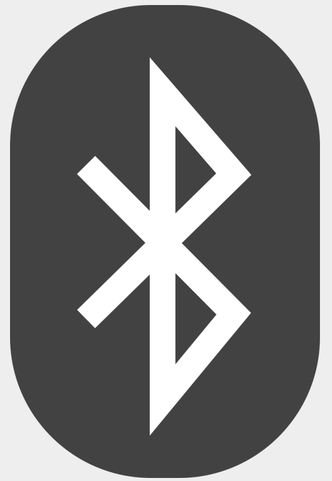
- GAP (Generic Access Profile)
  - Used in device discovery

Basics

- GAP (Generic Access Profile)
  - Used in device discovery
- GATT(Generic Attribute Profile)
  - Used to dispatch commands & receive notifications

GAP

Generic Access Profile



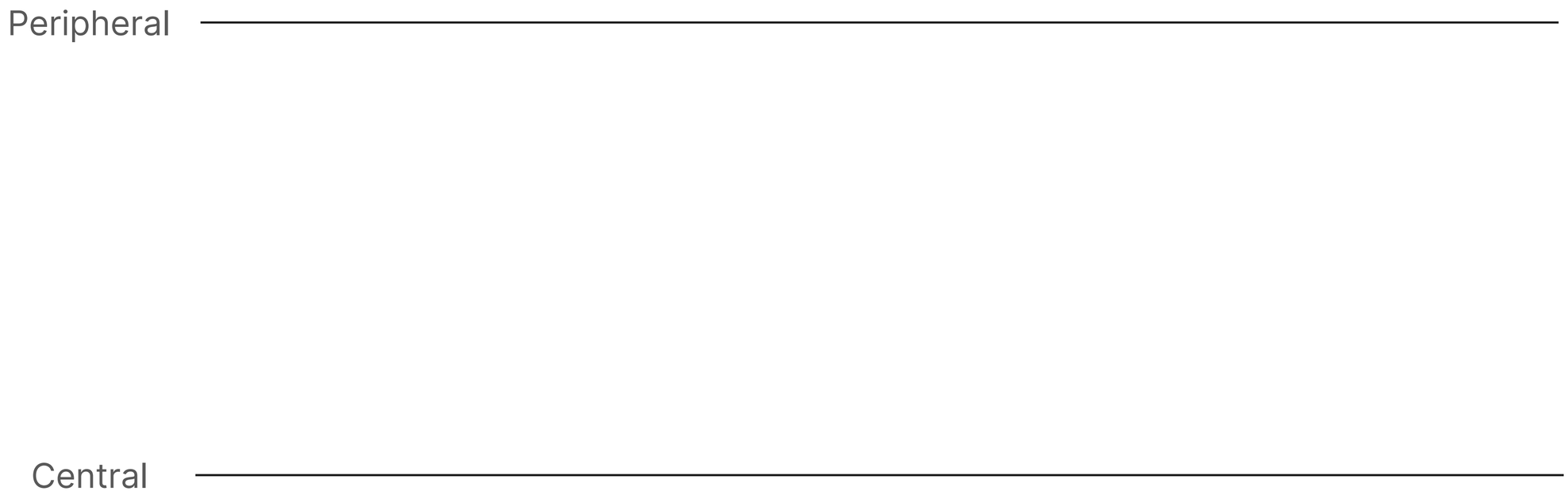
GAP Device Roles

- Peripheral
  - A device that can be controlled (a.k.a. Camera)
- Central
  - The controller (Smartphone)

GAP Discovery

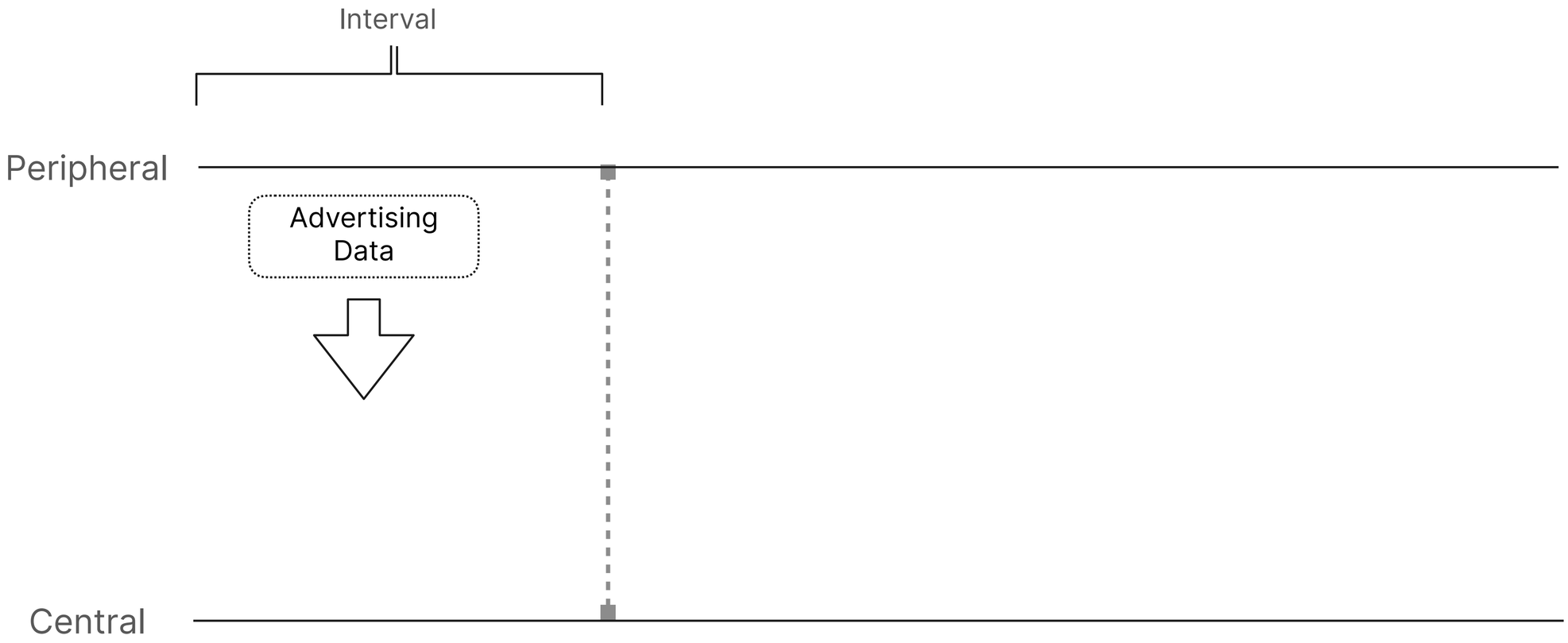
- Peripherals broadcast advertising packets at regular intervals
- Allows up 31 bytes of custom payload (Manufacturer specific)
- Typically stops after pairing / bonding is complete

GAP Discovery

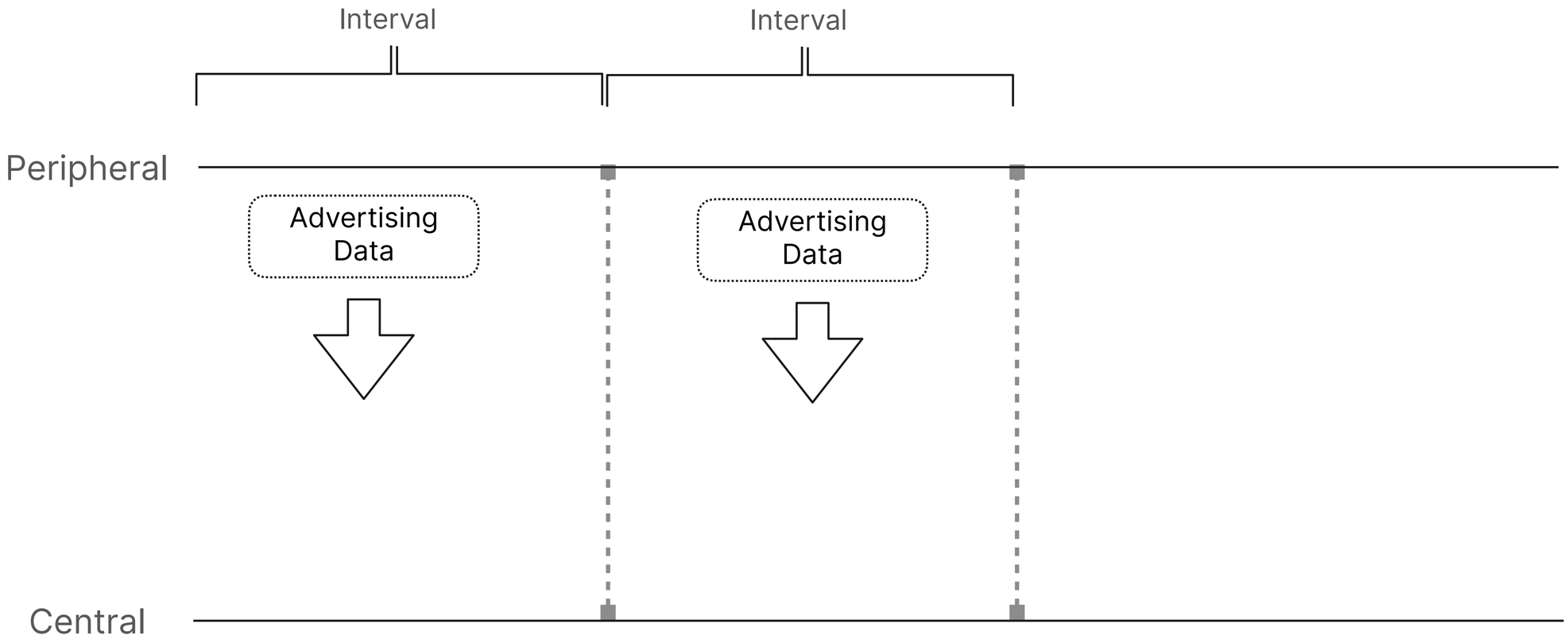


GAP Discovery

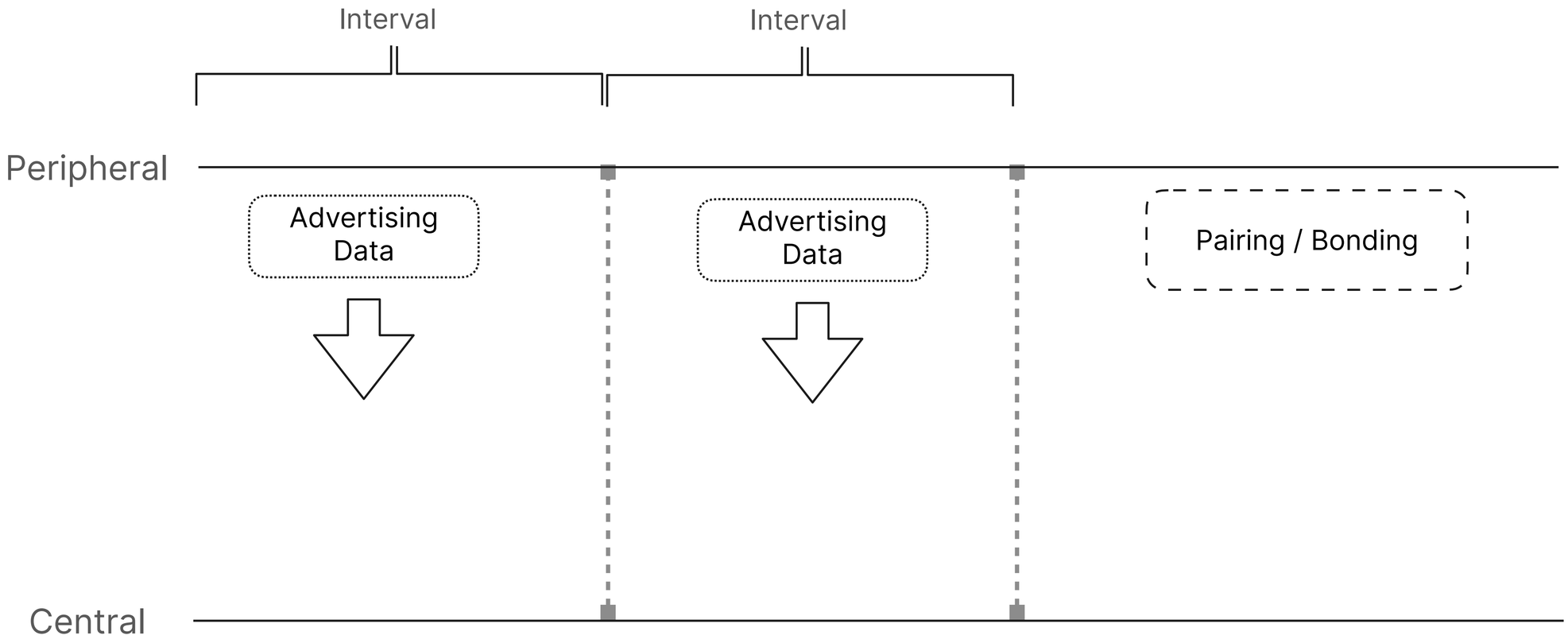
GAP Discovery



GAP Discovery

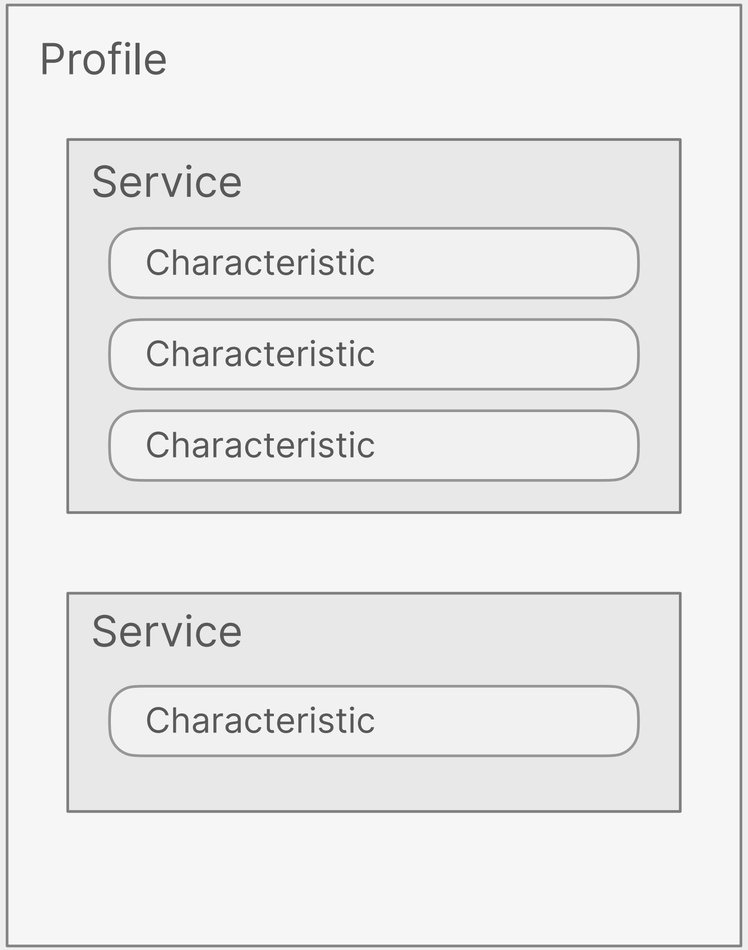


GAP Discovery

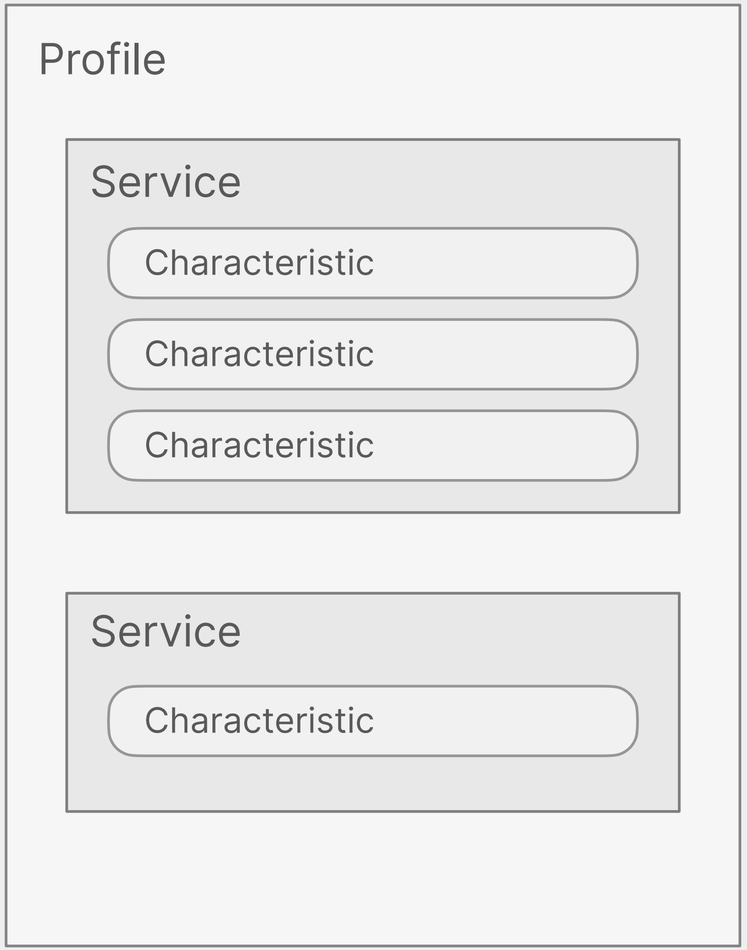


GATT

Generic Attribute Profile

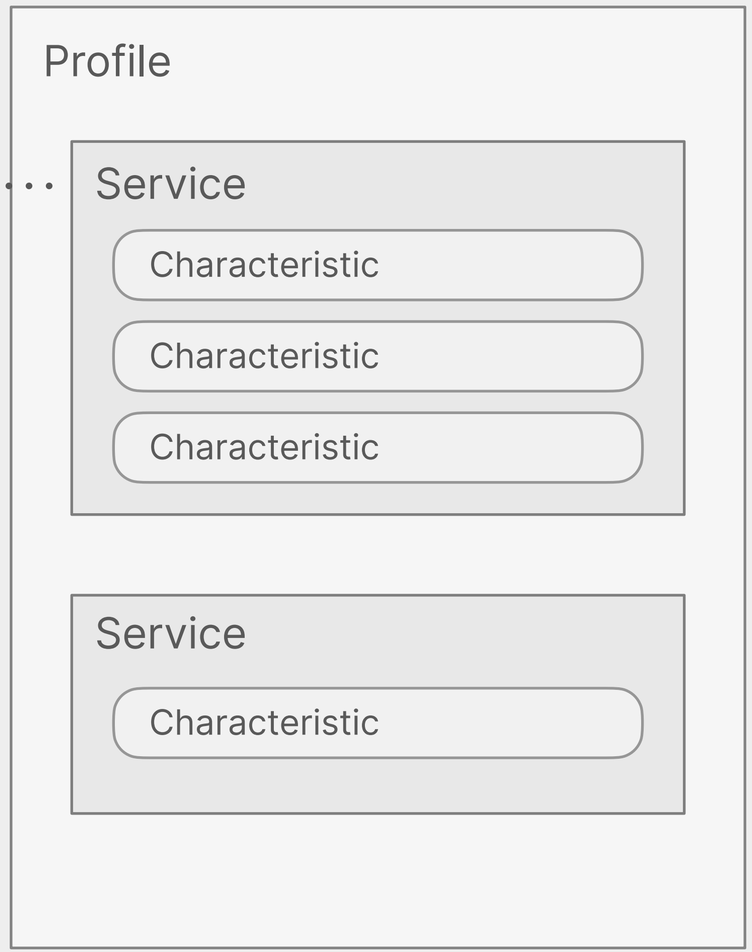


A collection of services



A collection of services

Logical grouping of APIs

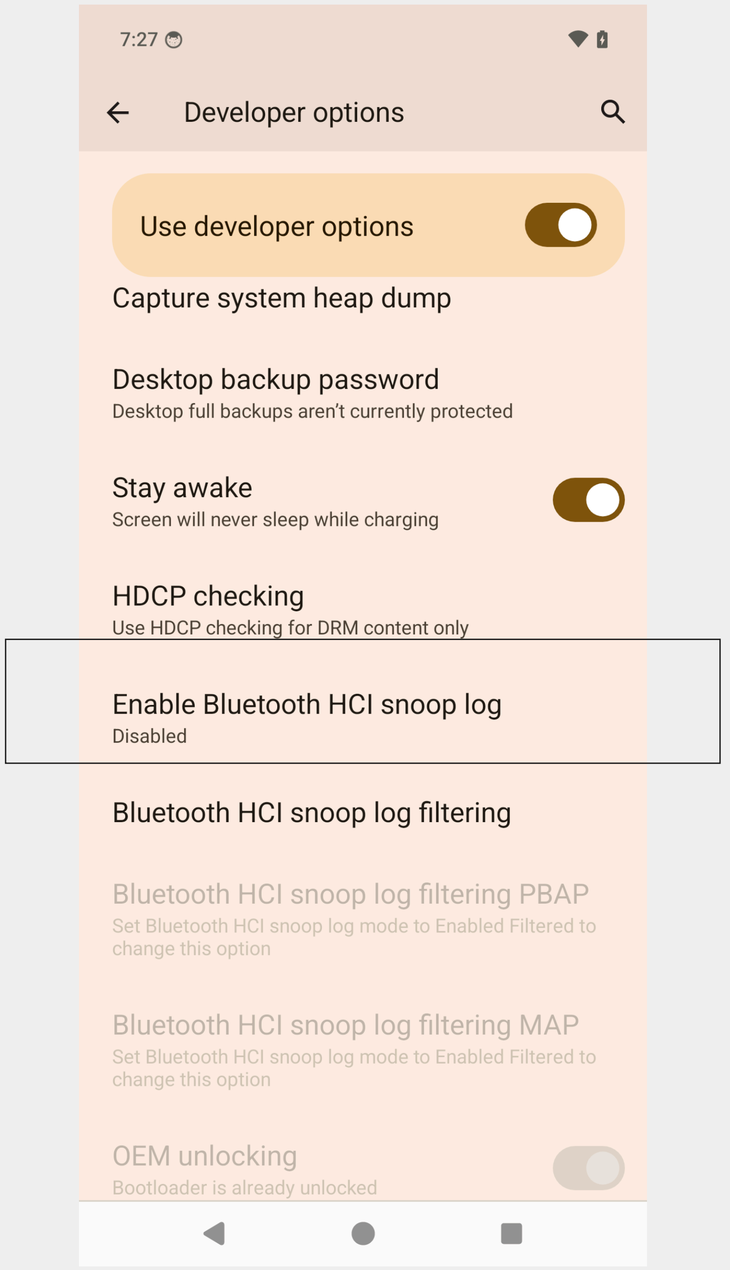



A collection of services
Logical grouping of APIs
Endpoint
Profile
Service
Characteristic
Characteristic
Characteristic
Service
Characteristic

Tools

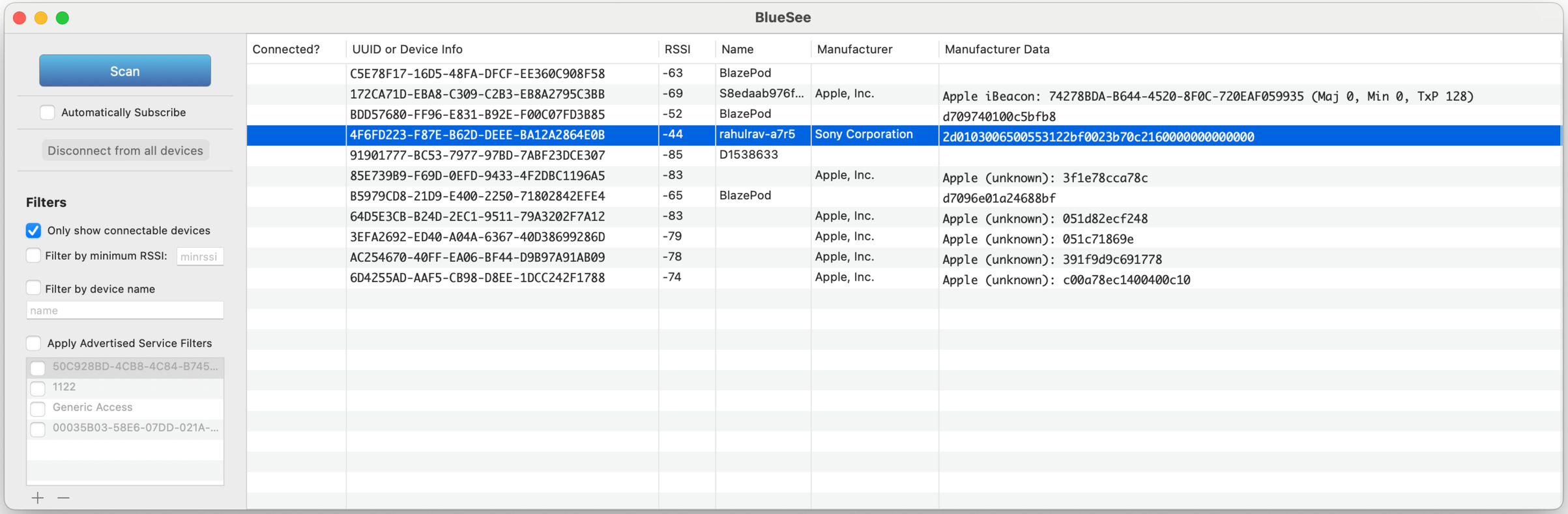
Logs

Open in Wireshark



BlueSee

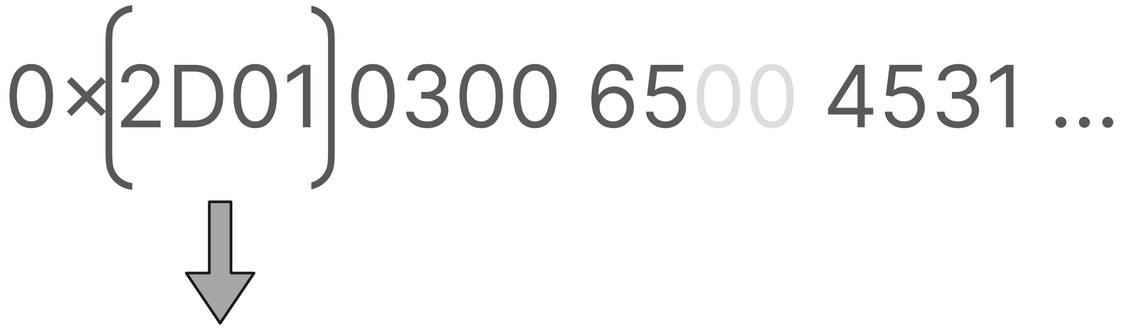
- Used to explore profiles + services available



Manufacturer Specific Data

0×2D01 0300 6500 4531 …

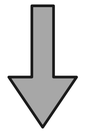
Manufacturer Specific Data



Sony Company Identifier

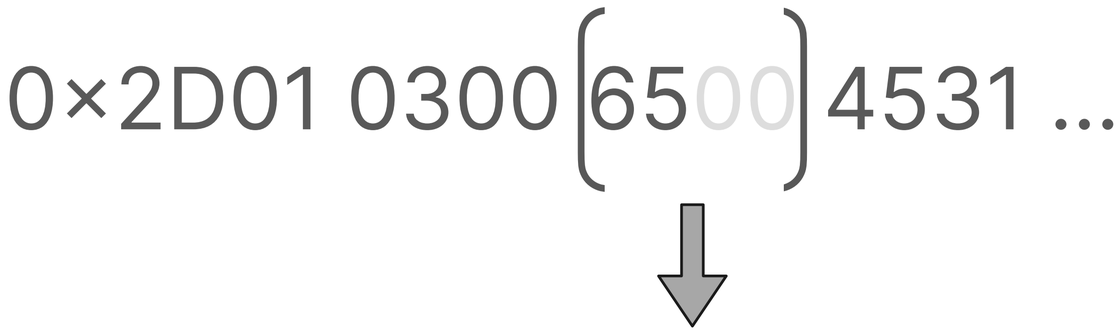
Manufacturer Specific Data

0×2D01 0300 6500 4531 ...



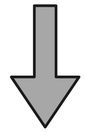
A Camera

Manufacturer Specific Data



Manufacturer Specific Data

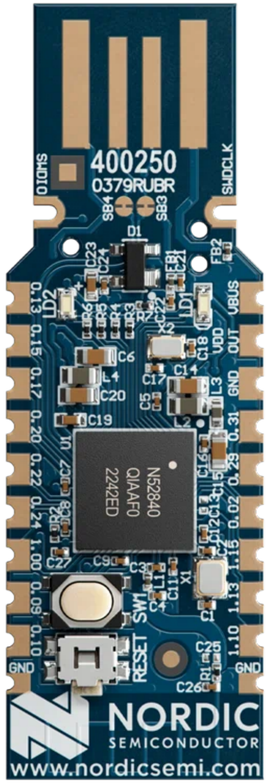
0×2D01 0300 6500 4531 ...



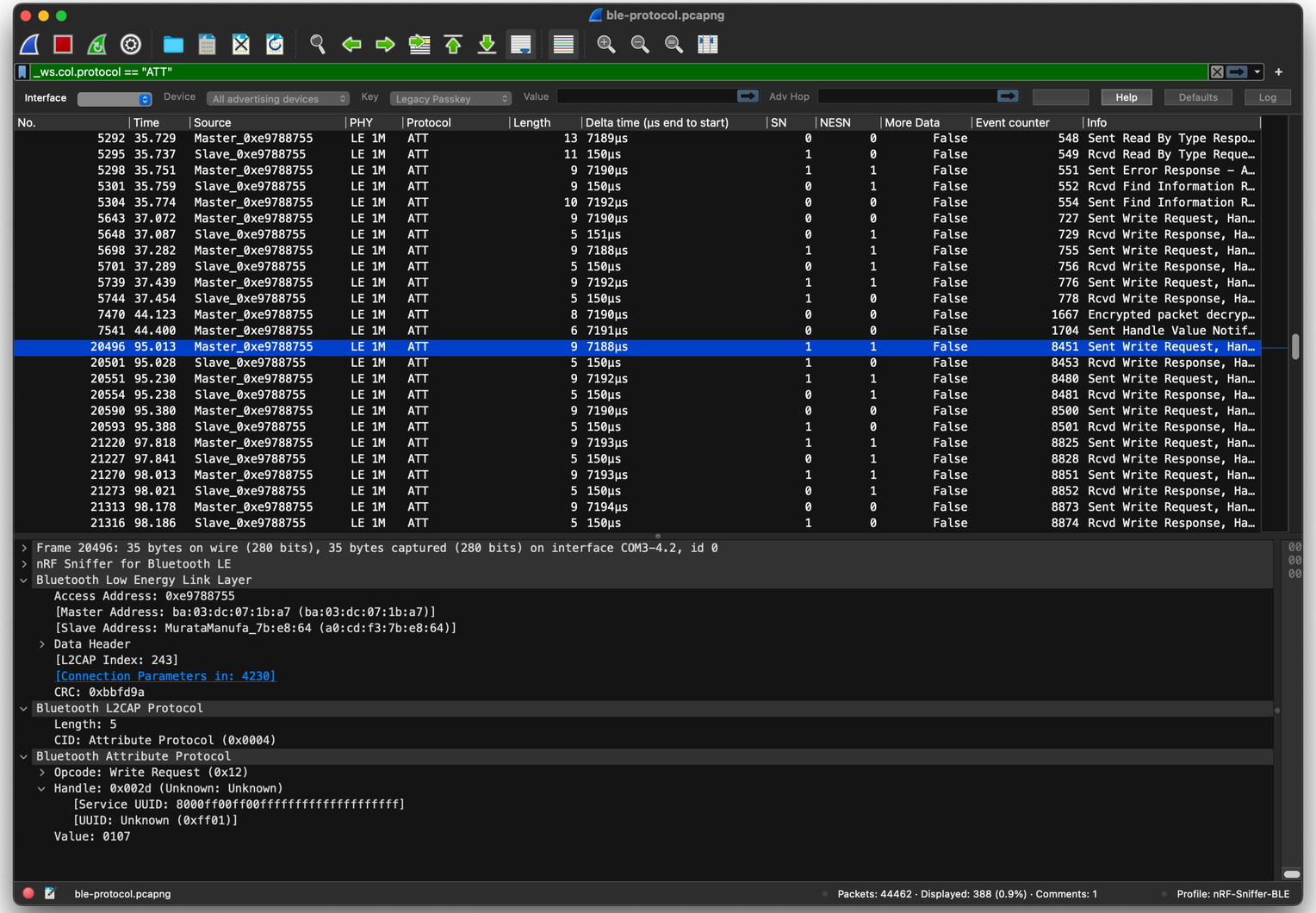
ASCII Model Code (E1)

Wireshark

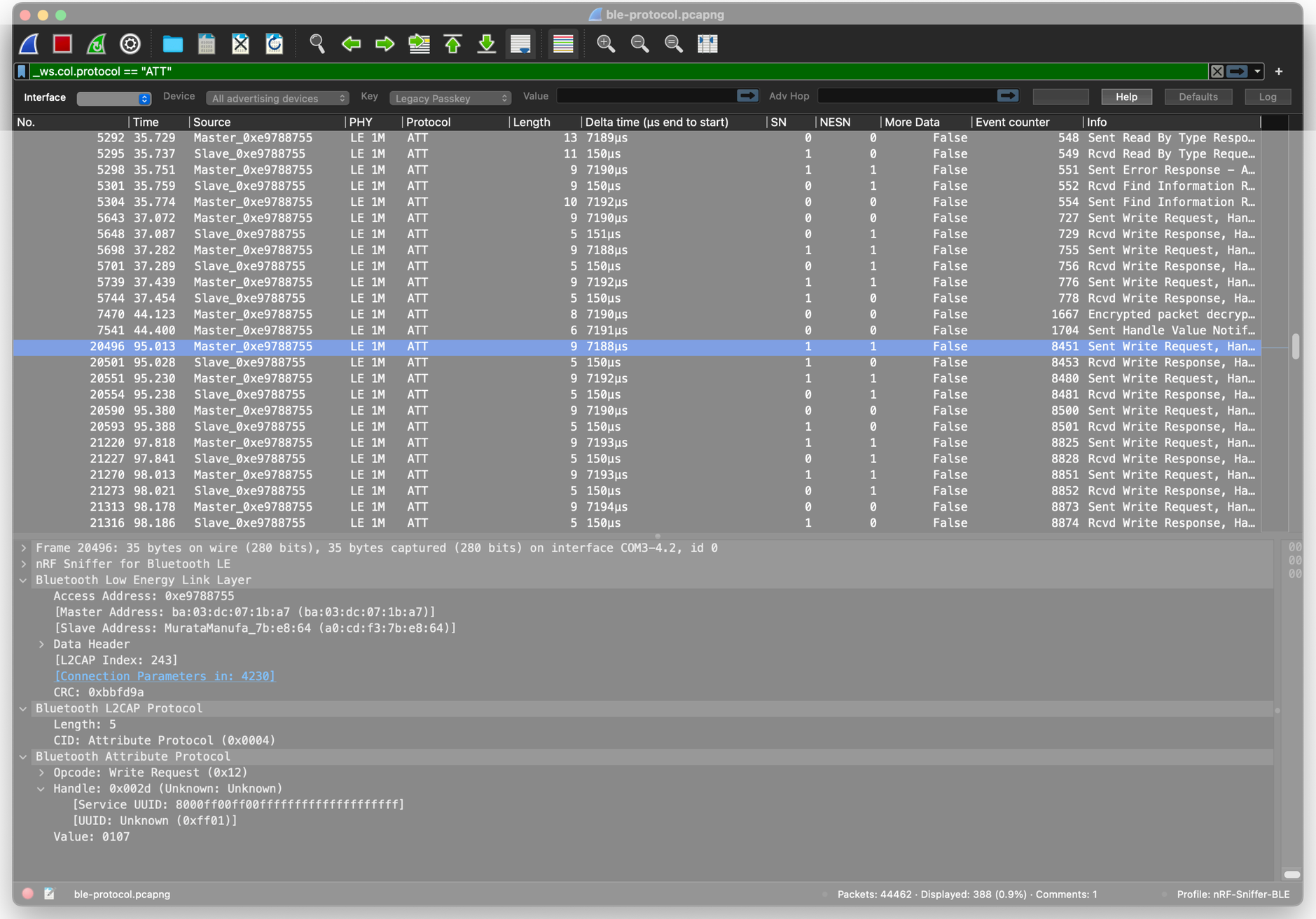
- Using a BLE Sniffer
  - Nordic NRF52840 Dongle
  - Adafruit BLE Sniffer

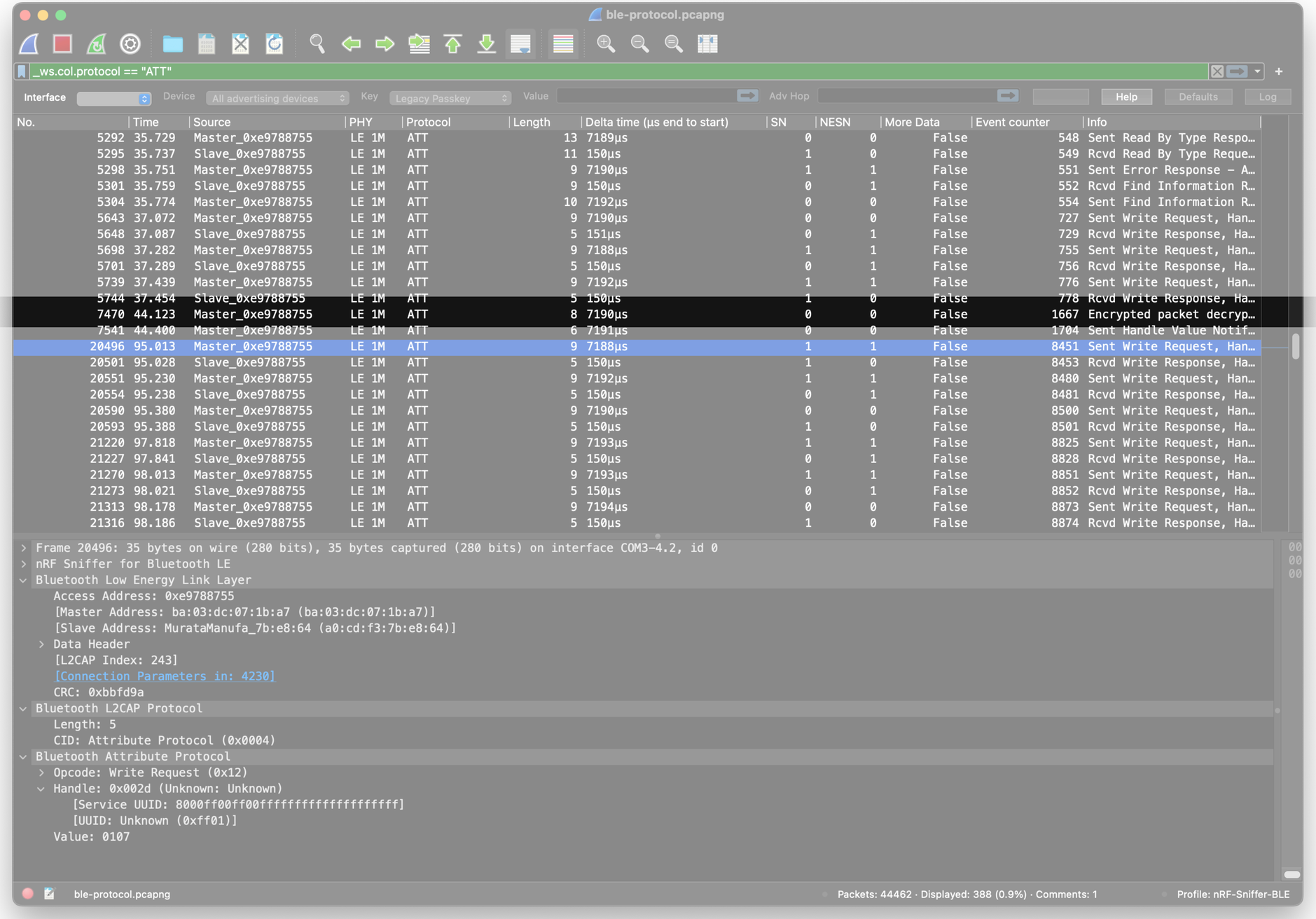


Wireshark

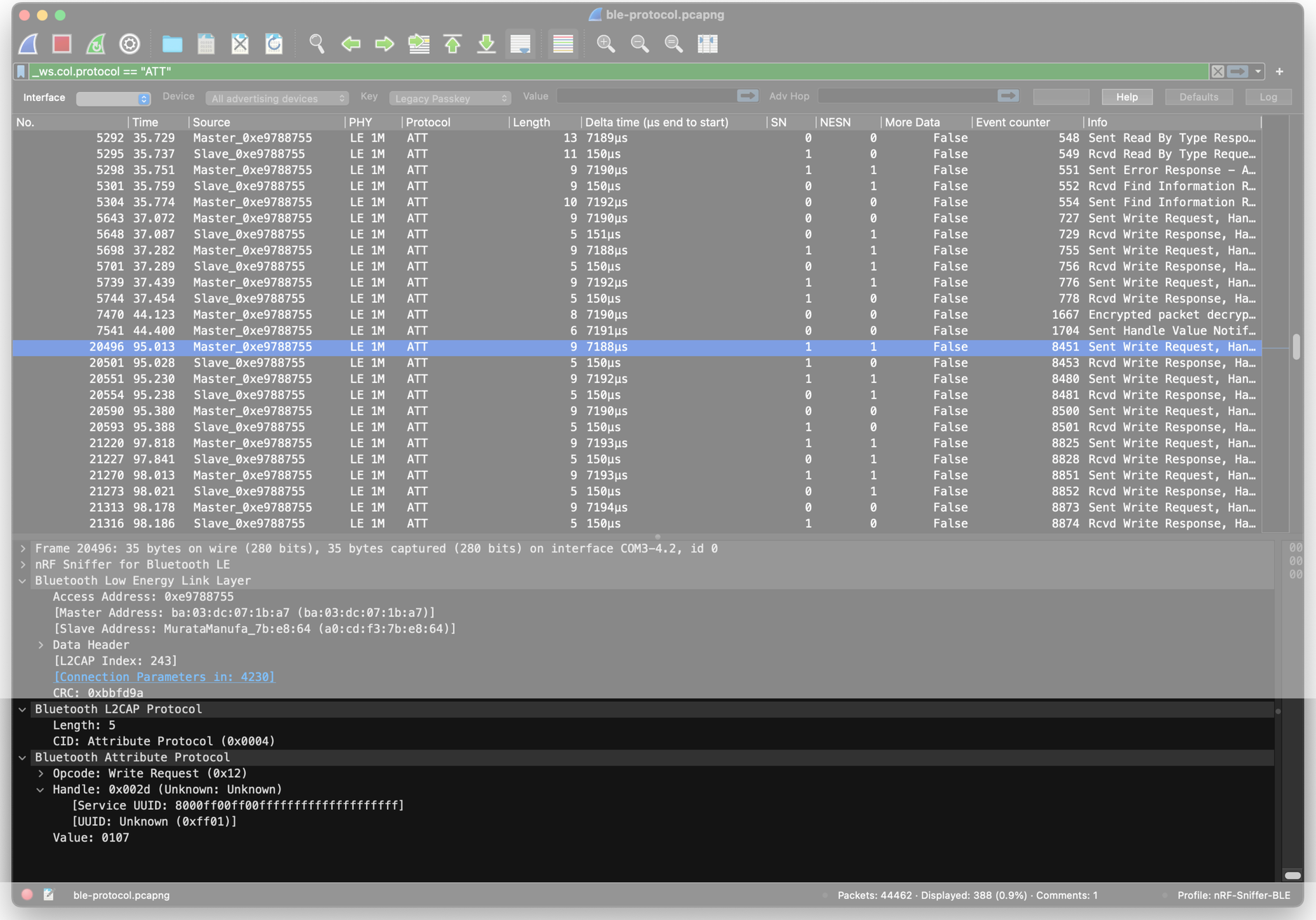

ble-protocol.pcapng
_ws.col.protocol == "ATT"
Interface
Device
All advertising devices
Key
Legacy Passkey
Value
Adv Hop
Help
Defaults
Log
No. | Time | Source | PHY | Protocol | Length | Delta time (µs end to start) | SN | NESN | More Data | Event counter | Info
5292 35.729 Master_0xe9788755 LE 1M ATT 13 7189µs 0 0 False 548 Sent Read By Type Respo…
5295 35.737 Slave_0xe9788755 LE 1M ATT 11 150µs 1 0 False 549 Rcvd Read By Type Reque…
5298 35.751 Master_0xe9788755 LE 1M ATT 9 7190µs 1 1 False 551 Sent Error Response - A…
5301 35.759 Slave_0xe9788755 LE 1M ATT 9 150µs 0 1 False 552 Rcvd Find Information R…
5304 35.774 Master_0xe9788755 LE 1M ATT 10 7192µs 0 0 False 554 Sent Find Information R…
5643 37.072 Master_0xe9788755 LE 1M ATT 9 7190µs 0 0 False 727 Sent Write Request, Han…
5648 37.087 Slave_0xe9788755 LE 1M ATT 5 151µs 0 1 False 729 Rcvd Write Response, Ha…
5698 37.282 Master_0xe9788755 LE 1M ATT 9 7188µs 1 1 False 755 Sent Write Request, Han…
5701 37.289 Slave_0xe9788755 LE 1M ATT 5 150µs 0 1 False 756 Rcvd Write Response, Ha…
5739 37.439 Master_0xe9788755 LE 1M ATT 9 7192µs 1 1 False 776 Sent Write Request, Han…
5744 37.454 Slave_0xe9788755 LE 1M ATT 5 150µs 1 0 False 778 Rcvd Write Response, Ha…
7470 44.123 Master_0xe9788755 LE 1M ATT 8 7190µs 0 0 False 1667 Encrypted packet decryp…
7541 44.400 Master_0xe9788755 LE 1M ATT 6 7191µs 0 0 False 1704 Sent Handle Value Notif…
20496 95.013 Master_0xe9788755 LE 1M ATT 9 7188µs 1 1 False 8451 Sent Write Request, Han…
20501 95.028 Slave_0xe9788755 LE 1M ATT 5 150µs 1 0 False 8453 Rcvd Write Response, Ha…
20551 95.230 Master_0xe9788755 LE 1M ATT 9 7192µs 1 1 False 8480 Sent Write Request, Han…
20554 95.238 Slave_0xe9788755 LE 1M ATT 5 150µs 0 1 False 8481 Rcvd Write Response, Ha…
20590 95.380 Master_0xe9788755 LE 1M ATT 9 7190µs 0 0 False 8500 Sent Write Request, Han…
20593 95.388 Slave_0xe9788755 LE 1M ATT 5 150µs 1 0 False 8501 Rcvd Write Response, Ha…
21220 97.818 Master_0xe9788755 LE 1M ATT 9 7193µs 1 1 False 8825 Sent Write Request, Han…
21227 97.841 Slave_0xe9788755 LE 1M ATT 5 150µs 0 1 False 8828 Rcvd Write Response, Ha…
21270 98.013 Master_0xe9788755 LE 1M ATT 9 7193µs 1 1 False 8851 Sent Write Request, Han…
21273 98.021 Slave_0xe9788755 LE 1M ATT 5 150µs 0 1 False 8852 Rcvd Write Response, Ha…
21313 98.178 Master_0xe9788755 LE 1M ATT 9 7194µs 0 0 False 8873 Sent Write Request, Han…
21316 98.186 Slave_0xe9788755 LE 1M ATT 5 150µs 1 0 False 8874 Rcvd Write Response, Ha…
Frame 20496: 35 bytes on wire (280 bits), 35 bytes captured (280 bits) on interface COM3-4.2, id 0
nRF Sniffer for Bluetooth LE
Bluetooth Low Energy Link Layer
Access Address: 0xe9788755
[Master Address: ba:03:dc:07:1b:a7 (ba:03:dc:07:1b:a7)]
[Slave Address: MurataManufa_7b:e8:64 (a0:cd:f3:7b:e8:64)]
Data Header
[L2CAP Index: 243]
[Connection Parameters in: 4230]
CRC: 0xbbfd9a
Bluetooth L2CAP Protocol
Length: 5
CID: Attribute Protocol (0x0004)
Bluetooth Attribute Protocol
Opcode: Write Request (0x12)
Handle: 0x002d (Unknown: Unknown)
[Service UUID: 8000ff00ff00ffffffffffffffffffff]
[UUID: Unknown (0xff01)]
Value: 0107
ble-protocol.pcapng
Packets: 44462 · Displayed: 388 (0.9%) · Comments: 1
Profile: nRF-Sniffer-BLE

Filter for GATT

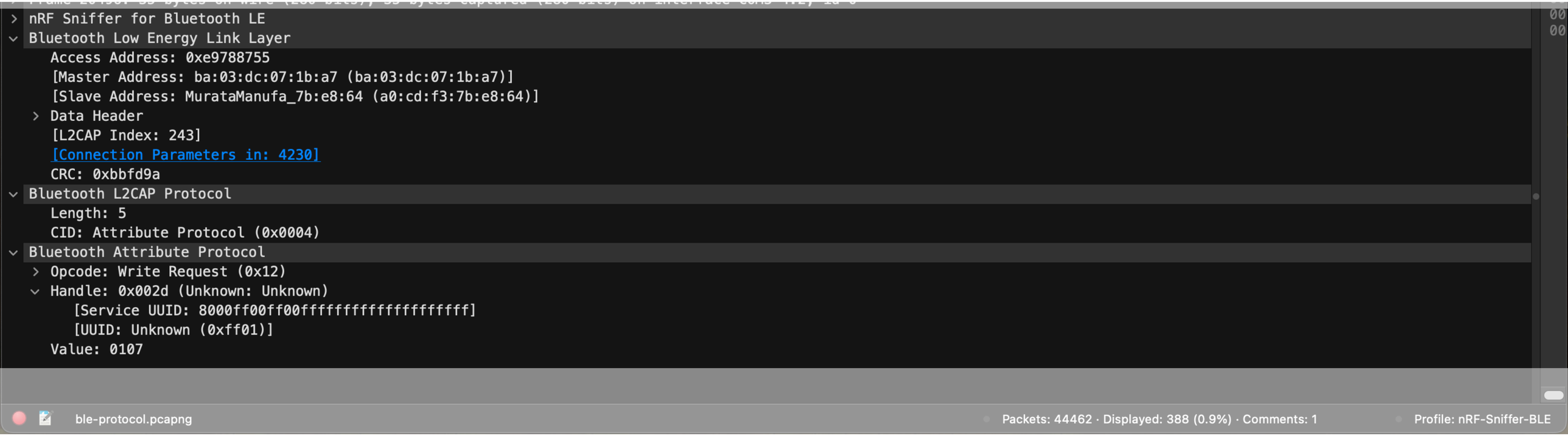


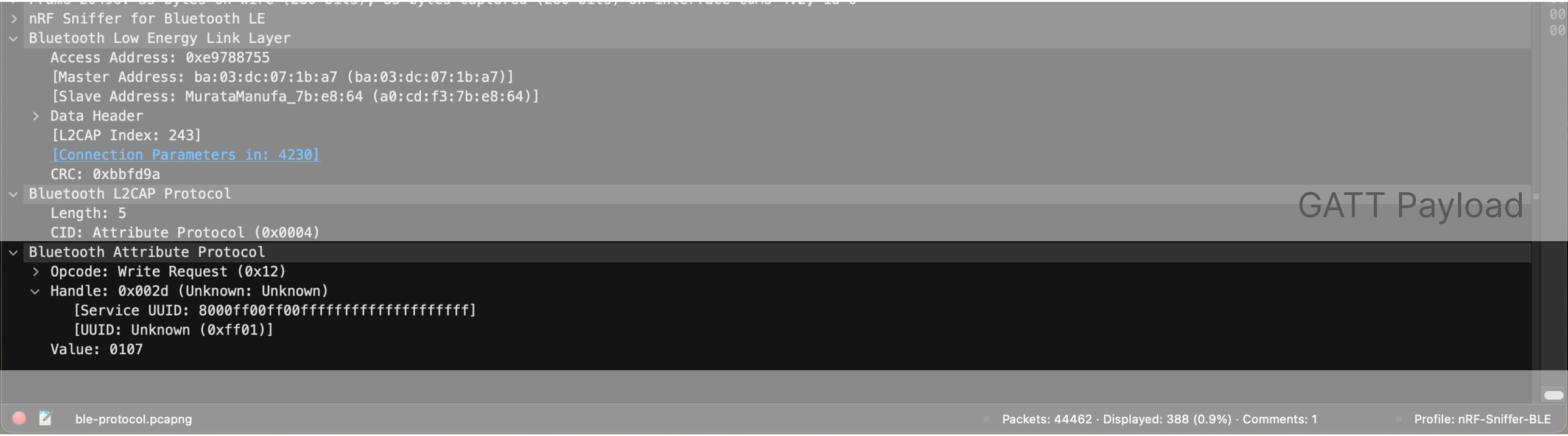


Can decrypt traffic



GATT Request


nRF Sniffer for Bluetooth LE
Bluetooth Low Energy Link Layer
Access Address: 0xe9788755
[Master Address: ba:03:dc:07:1b:a7 (ba:03:dc:07:1b:a7)]
[Slave Address: MurataManufa_7b:e8:64 (a0:cd:f3:7b:e8:64)]
Data Header
[L2CAP Index: 243]
[Connection Parameters in: 4230]
CRC: 0xbbfd9a
Bluetooth L2CAP Protocol
Length: 5
CID: Attribute Protocol (0x0004)
Bluetooth Attribute Protocol
Opcode: Write Request (0x12)
Handle: 0x002d (Unknown: Unknown)
[Service UUID: 8000ff00ff00ffffffffffffffffffff]
[UUID: Unknown (0xff01)]
Value: 0107
ble-protocol.pcapng
Packets: 44462 · Displayed: 388 (0.9%) · Comments: 1
Profile: nRF-Sniffer-BLE


nRF Sniffer for Bluetooth LE
Bluetooth Low Energy Link Layer
Access Address: 0xe9788755
[Master Address: ba:03:dc:07:1b:a7 (ba:03:dc:07:1b:a7)]
[Slave Address: MurataManufa_7b:e8:64 (a0:cd:f3:7b:e8:64)]
Data Header
[L2CAP Index: 243]
[Connection Parameters in: 4230]
CRC: 0xbbfd9a
Bluetooth L2CAP Protocol
Length: 5
CID: Attribute Protocol (0x0004)
Bluetooth Attribute Protocol
Opcode: Write Request (0x12)
Handle: 0x002d (Unknown: Unknown)
[Service UUID: 8000ff00ff00ffffffffffffffffffff]
[UUID: Unknown (0xff01)]
Value: 0107
GATT Payload
ble-protocol.pcapng
Packets: 44462 · Displayed: 388 (0.9%) · Comments: 1
Profile: nRF-Sniffer-BLE

Camera Protocol

Camera Control Service UUID

8000FF00-FF00-FFFF-FFFF-FFFFFFFFFFFF

REMOTE_COMMAND

0000FF01-0000-1000-8000-00805F9B34FB

REMOTE_NOTIFY

0000FF02-0000-1000-8000-00805F9B34FB

Taking a picture

- 0xFF01, 0×0106 (RESET)
- 0xFF01, 0×0107 (FOCUS_REQUEST)
- Wait for notification on 0xFF02 with payload (0×02, 0×3F, 0×20)
- 0xFF01, 0×0109 (TAKE_PICTURE)
- Wait for notification on 0xFF02 with payload (0×02, 0xA0, 0×20)
- 0xFF01, 0×0108 (SHUTTER_UP)
- 0xFF01, 0×0106 (RESET)

Demo

@tikurahul

Thank you, and don’t forget to vote