

KotlinConf

Copenhagen

2024

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?

Imaging Edge Mobile



Why?

Imaging Edge Mobile



1.9 ★

10M+
Downloads

Creator's App



3.3 ★

500K+
Downloads

App Features

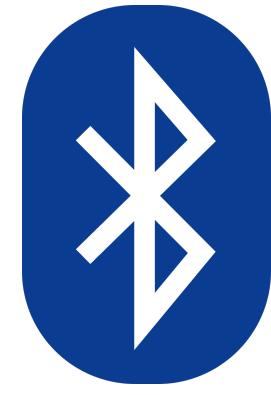
- Sony Cloud Storage & Sync
- Community
- Preview
- Remote Control
- Transfer Photos

App Features

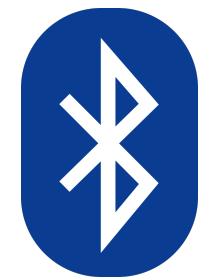
- Sony Cloud Storage & Sync 
- Community 
- Preview 
- Remote Control 
- Transfer Photos 

Agenda

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

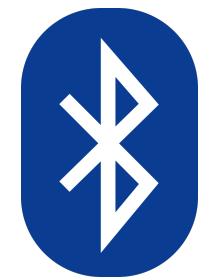


Basics



Basics

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

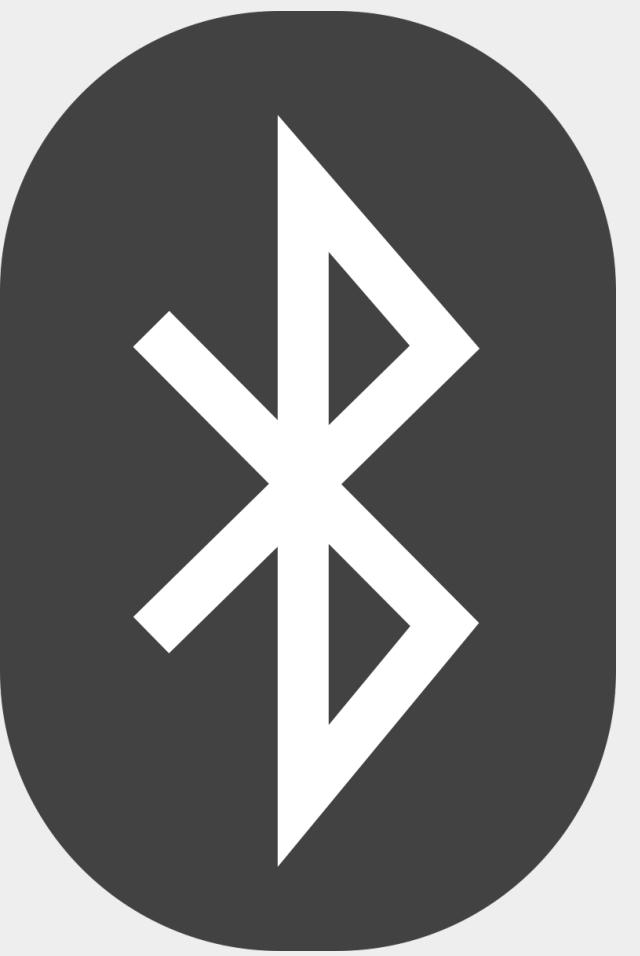


Basics

- 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

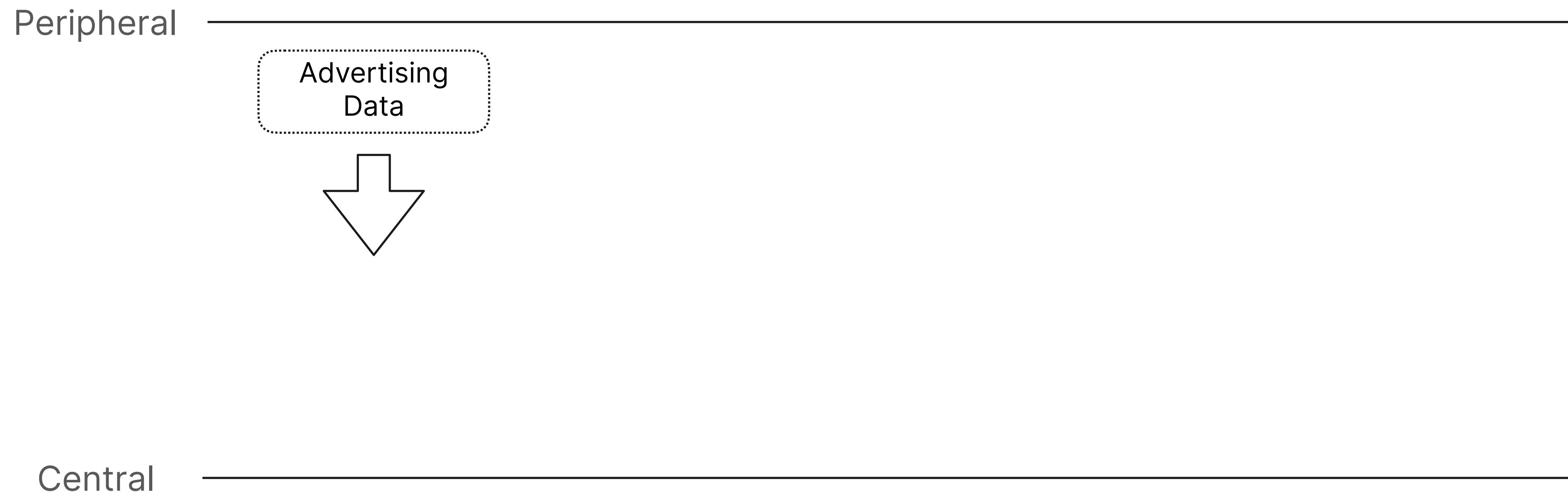
- Peripherals broadcast advertising packets at regular intervals
- Allows up 31 bytes of custom payload (Manufacturer specific)
- Typically stops after pairing / bonding is complete

GAP Discovery

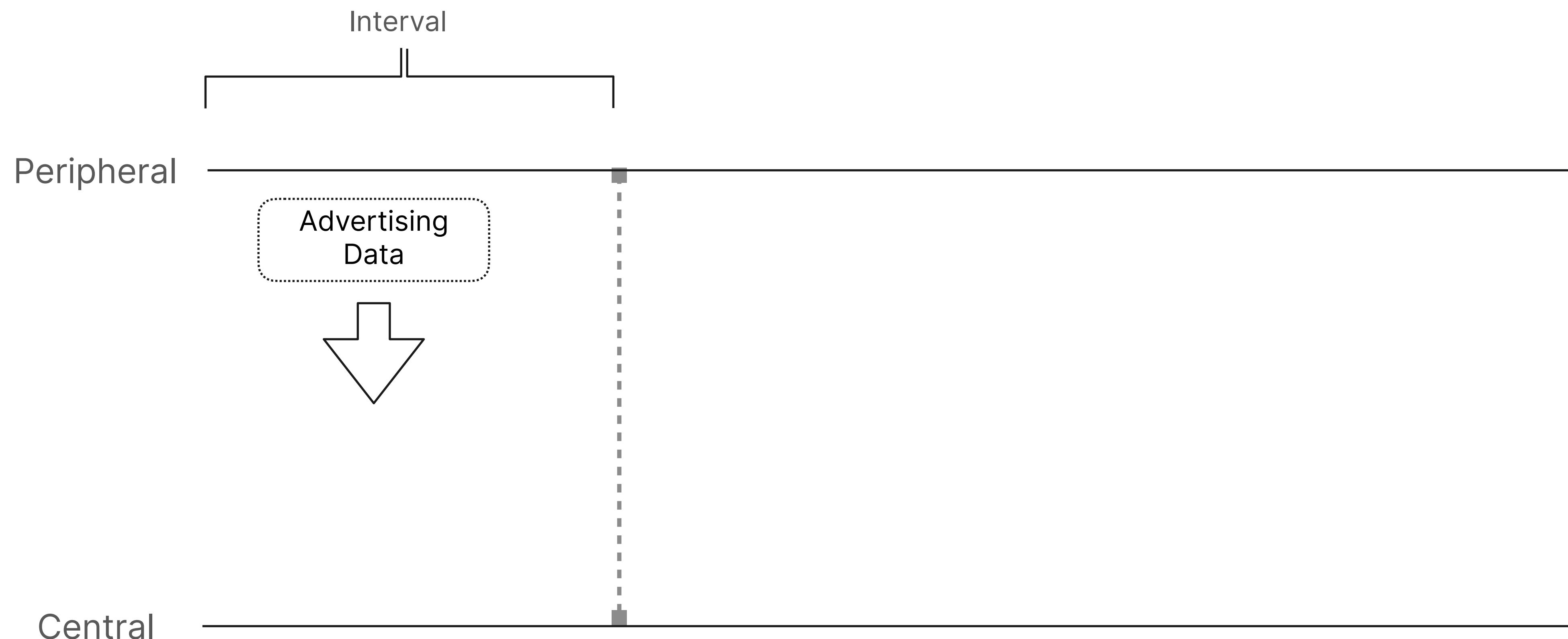
Peripheral —————

Central —————

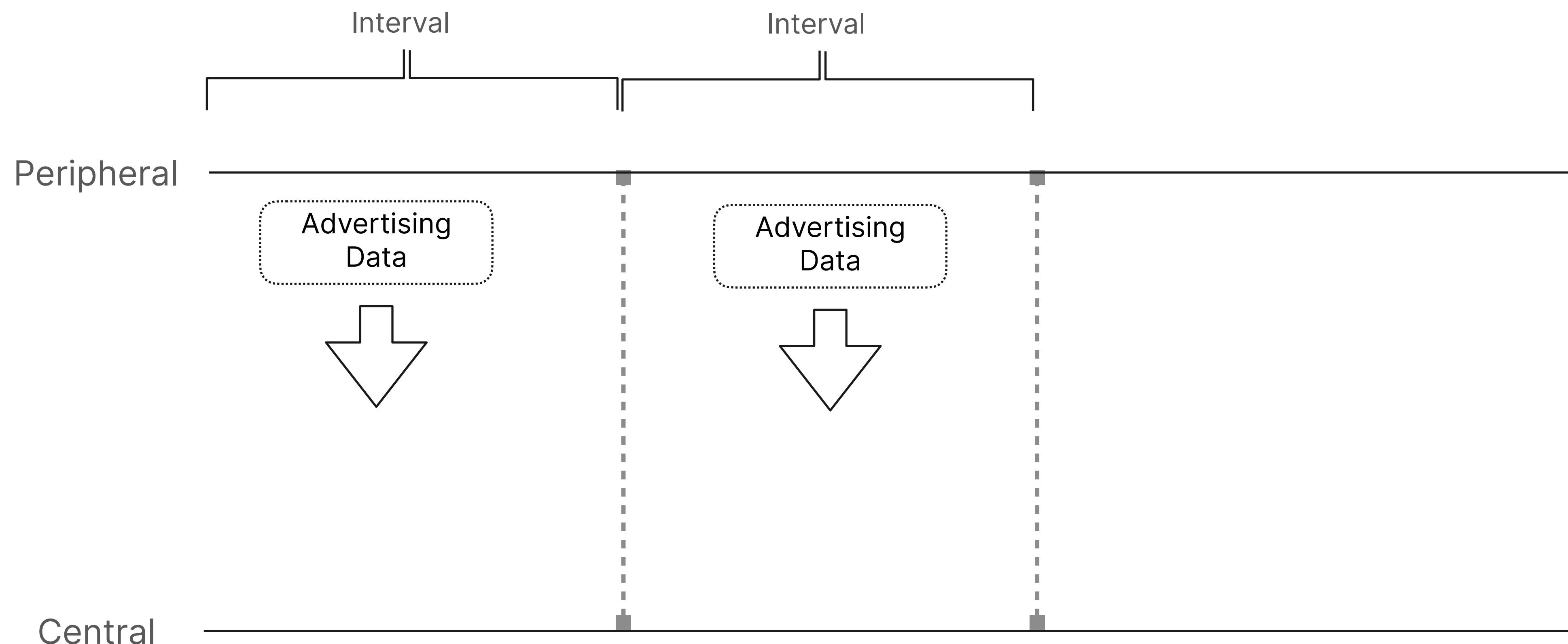
GAP Discovery



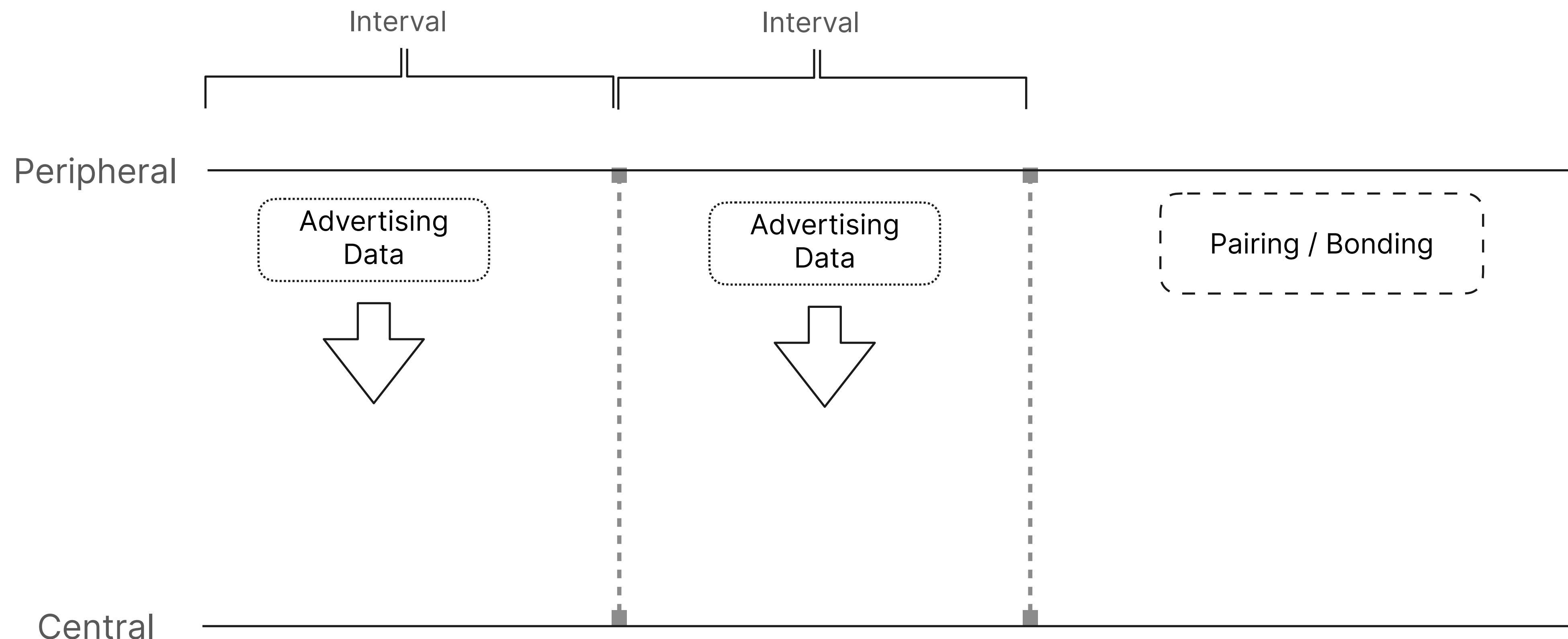
GAP Discovery



GAP Discovery



GAP Discovery



GATT

Generic Attribute Profile

Profile

Service

Characteristic

Characteristic

Characteristic

Service

Characteristic

A collection of services

.....

Profile

Service

Characteristic

Characteristic

Characteristic

Service

Characteristic

A collection of services

.....

Logical grouping of APIs

.....

Profile

Service

Characteristic

Characteristic

Characteristic

Service

Characteristic

A collection of services

.....

Logical grouping of APIs

.....

Endpoint

.....

Profile

Service

Characteristic

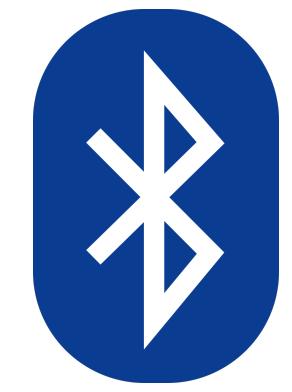
Service

Characteristic

Service

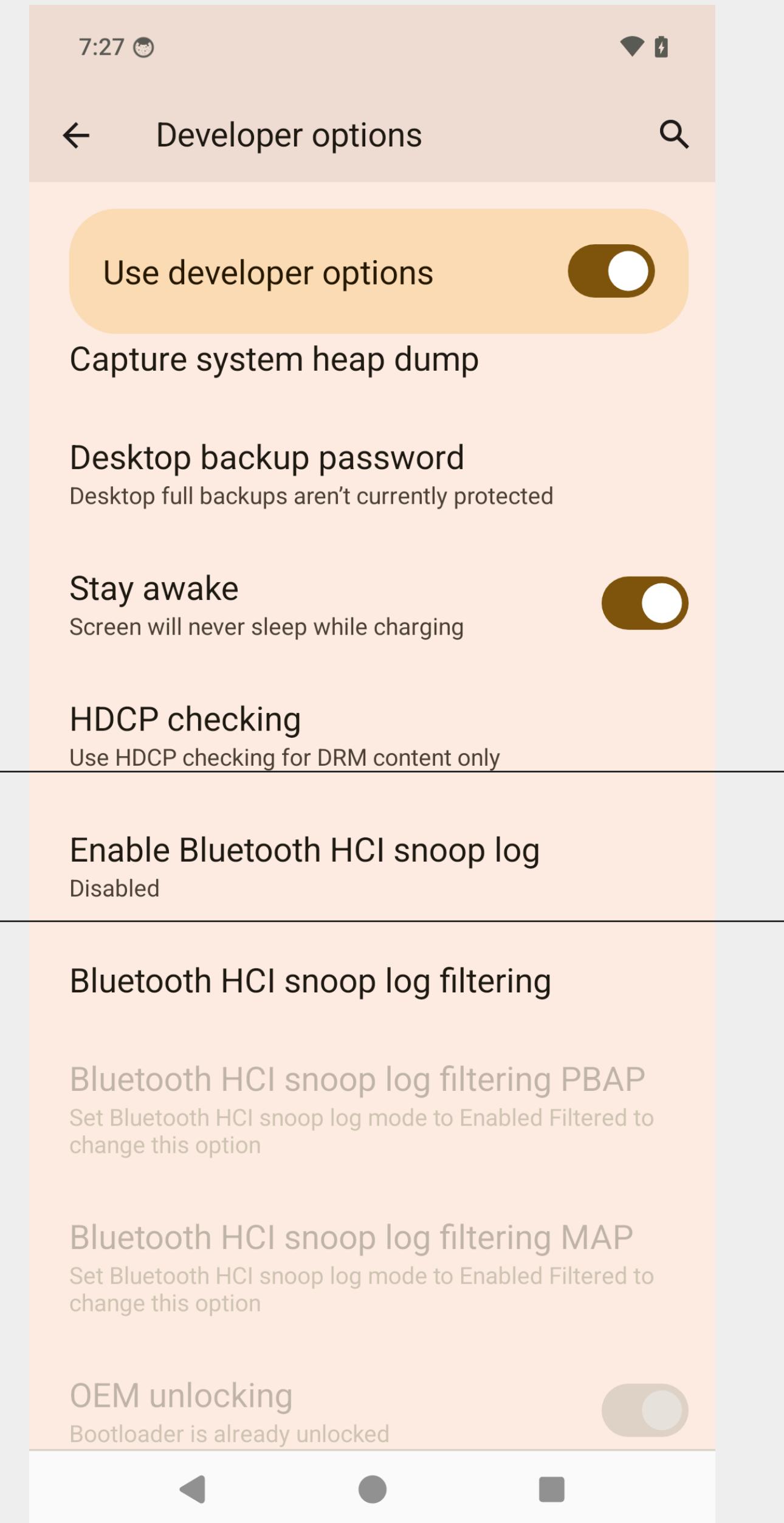
Characteristic

Tools



Logs

Open in Wireshark





BlueSee

- Used to explore profiles + services available

BlueSee

Connected?	UUID or Device Info	RSSI	Name	Manufacturer	Manufacturer Data
	C5E78F17-16D5-48FA-DFCF-EE360C908F58	-63	BlazePod		
	172CA71D-EBA8-C309-C2B3-EB8A2795C3BB	-69	S8edaab976f...	Apple, Inc.	Apple iBeacon: 74278BDA-B644-4520-8F0C-720EAF059935 (Maj 0, Min 0, TxP 128)
	BDD57680-FF96-E831-B92E-F00C07FD3B85	-52	BlazePod		d709740100c5fb8
	4F6FD223-F87E-B62D-DEEE-BA12A2864E0B	-44	rahulrav-a7r5	Sony Corporation	2d0103006500553122bf0023b70c2160000000000000
	91901777-BC53-7977-97BD-7ABF23DCE307	-85	D1538633		
	85E739B9-F69D-0EFD-9433-4F2DBC1196A5	-83		Apple, Inc.	Apple (unknown): 3f1e78cca78c
	B5979CD8-21D9-E400-2250-71802842EFE4	-65	BlazePod		d7096e01a24688bf
	64D5E3CB-B24D-2EC1-9511-79A3202F7A12	-83		Apple, Inc.	Apple (unknown): 051d82ecf248
	3EFA2692-ED40-A04A-6367-40D38699286D	-79		Apple, Inc.	Apple (unknown): 051c71869e
	AC254670-40FF-EA06-BF44-D9B97A91AB09	-78		Apple, Inc.	Apple (unknown): 391f9d9c691778
	6D4255AD-AAF5-CB98-D8EE-1DCC242F1788	-74		Apple, Inc.	Apple (unknown): c00a78ec1400400c10

Scan

Automatically Subscribe

Disconnect from all devices

Filters

Only show connectable devices

Filter by minimum RSSI: minrss

Filter by device name

name

Apply Advertised Service Filters

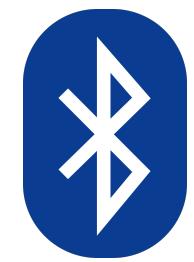
50C928BD-4CB8-4C84-B745...

1122

Generic Access

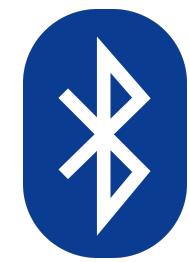
00035B03-58E6-07DD-021A...

+ -



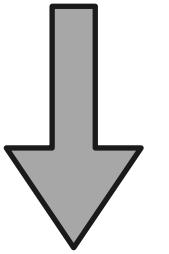
Manufacturer Specific Data

0x2D01 0300 6500 4531 ...

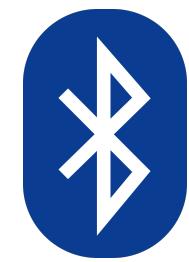


Manufacturer Specific Data

0x[2D01]0300 6500 4531 ...

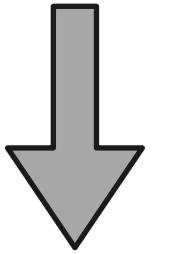


Sony Company Identifier

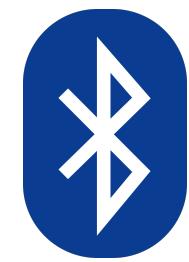


Manufacturer Specific Data

0x2D01[0300]6500 4531 ...

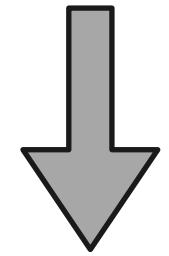


A Camera

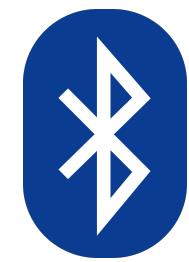


Manufacturer Specific Data

0x2D01 0300[6500]4531 ...

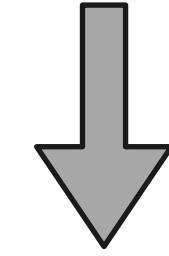


Protocol Version

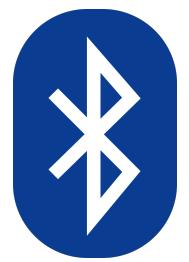


Manufacturer Specific Data

0x2D01 0300 6500 (4531)...

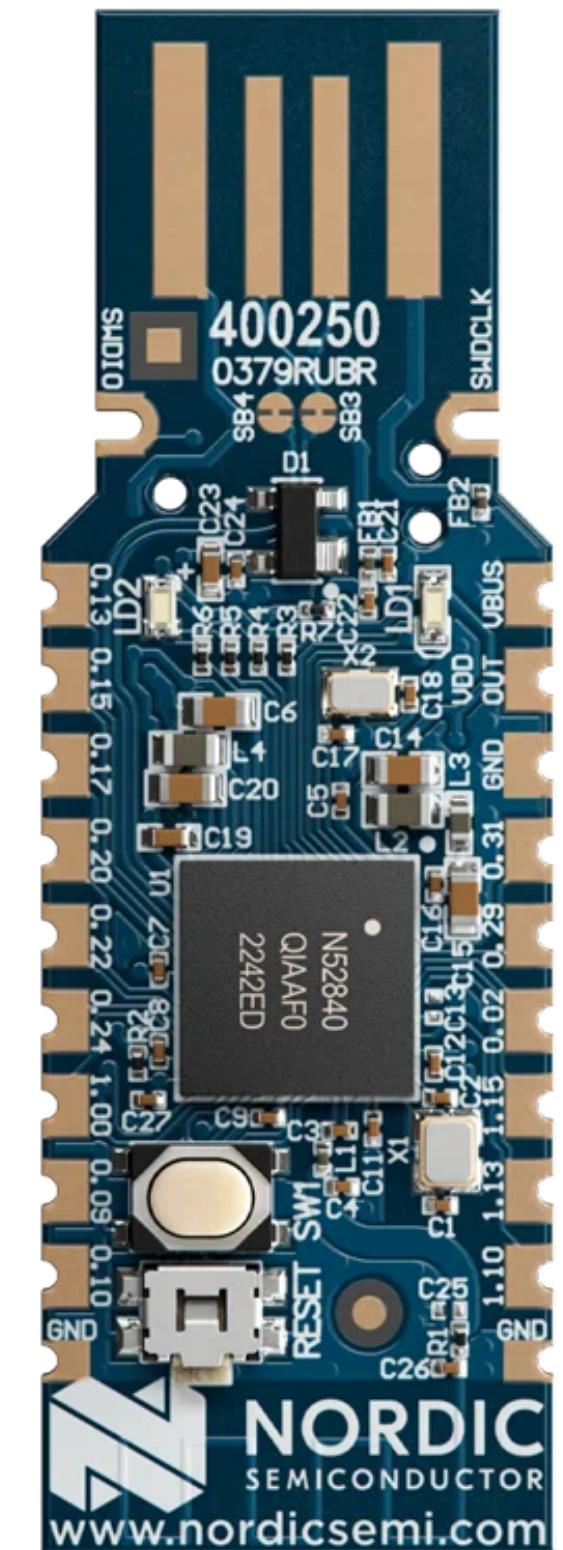


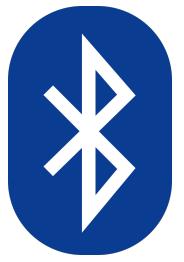
ASCII Model Code ([E1](#))



Wireshark

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





Wireshark

ble-protocol.pcapng

_ws.col.protocol == "ATT"

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, Han...
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, Han...
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, Han...
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, Han...
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, Han...
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, Han...
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, Han...
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, Han...
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, Han...

> 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: 8000ff00ff00ffffffffffff]
[UUID: Unknown (0xffff)]
Value: 0107

Packets: 44462 · Displayed: 388 (0.9%) · Comments: 1 · Profile: nRF-Sniffer-BLE

ble-protocol.pcapng

_ws.col.protocol == "ATT"

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: 8000ff00ff00ffffffffff]
    [UUID: Unknown (0xff01)]
  Value: 0107
```

Packets: 44462 · Displayed: 388 (0.9%) · Comments: 1 · Profile: nRF-Sniffer-BLE

Filter for GATT

ble-protocol.pcapng

_ws.col.protocol == "ATT"

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: 8000ff00ff00ffffffffffff]
    [UUID: Unknown (0xff01)]
  Value: 0107
```

Packets: 44462 · Displayed: 388 (0.9%) · Comments: 1 · Profile: nRF-Sniffer-BLE

Can decrypt traffic

ble-protocol.pcapng

_ws.col.protocol == "ATT"

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: 8000ff00ff00ffffffffffff]
    [UUID: Unknown (0xff01)]
  Value: 0107

```

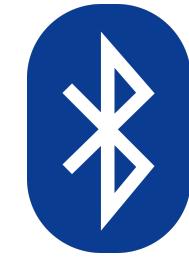
Packets: 44462 · Displayed: 388 (0.9%) · Comments: 1 · Profile: nRF-Sniffer-BLE

GATT Request

> Frame 281981: 55 bytes on wire (280 bits), 55 bytes captured (280 bits) on interface ens3s102, id = 0
> nRF Sniffer for Bluetooth LE
v 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
v Bluetooth L2CAP Protocol
 Length: 5
 CID: Attribute Protocol (0x0004)
v Bluetooth Attribute Protocol
 > Opcode: Write Request (0x12)
 v Handle: 0x002d (Unknown: Unknown)
 [Service UUID: 8000ff00ff00ffffffffffff]
 [UUID: Unknown (0xff01)]
 Value: 0107

> Frame 281981: 33 bytes on wire (260 bits), 33 bytes captured (260 bits) on interface ens3s102, 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: 8000ff00ff00ffffffffffff]
 [UUID: Unknown (0xff01)]
 Value: 0107

GATT Payload



Camera Protocol

Camera Control Service UUID

[8000FF00-FF00-FFFF-FFFF-FFFFFFFFFFFF](#)

REMOTE_COMMAND

[0000FF01-0000-1000-8000-00805F9B34FB](#)

REMOTE_NOTIFY

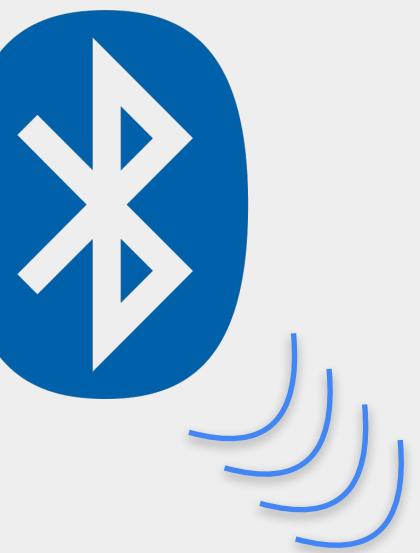
[0000FF02-0000-1000-8000-00805F9B34FB](#)



Taking a picture

- 0xFF01, 0x0106 (RESET)
- 0xFF01, 0x0107 (FOCUS_REQUEST)
- Wait for notification on 0xFF02 with payload (0x02, 0x3F, 0x20)
- 0xFF01, 0x0109 (TAKE_PICTURE)
- Wait for notification on 0xFF02 with payload (0x02, 0xA0, 0x20)
- 0xFF01, 0x0108 (SHUTTER_UP)
- 0xFF01, 0x0106 (RESET)

Demo



@tikurahul

Thank you,
and don't forget
to vote

