Blue2thprinting: {blue-[tooth}-printing]

Answering the question "WTF am I even looking at?!"

Xeno Kovah
OpenSecurityTraining2 (ost2.fyi)
& Dark Mentor LLC (darkmentor.com)

About Me

- 75% of my time is spent making free (as in beer), open access, and *open source* (CreativeCommons licensed) classes for a non-profit I started, **OpenSecurityTraining2 (ost2.fyi)**

About Me

- 75% of my time is spent making free (as in beer), open access, and *open source* (CreativeCommons licensed) classes for a non-profit I started, **OpenSecurityTraining2 (ost2.fyi)**

- 25% of my time doing consulting and research for **Dark Mentor LLC**
  - The research is for fun, but is *also a trojan horse* to get me into conferences to tell you about OST2 ;)

What I Want To Know:

What Bluetooth Chip Is Inside Any Device


DARK MENTOR


nest

Texas Instruments

Silicon Labs

Broadcom

?

Why I Want To Know It:

So I Know if it's Vulnerable To a Firmware-Level Exploit

TEXAS INSTRUMENTS

SILICON LABS

BROADCOM®

ARMIS®

DST2.FYI

TEXAS INSTRUMENTS

SILICON LABS®

BROADCOM®

ARMIS®

DST2.FYI

TEXAS INSTRUMENTS

SEMC
SECURE MOBILE NETWORKING

SILICON LABS®

BROADCOM®

ARMIS®

DARK MENTOR

TEXAS INSTRUMENTS

SEEMO

SECURE MOBILE NETWORKING

SILICON LABS®

BROADCOM®

ARMIS®

DARK MENTOR

TEXAS INSTRUMENTS

SEEMO

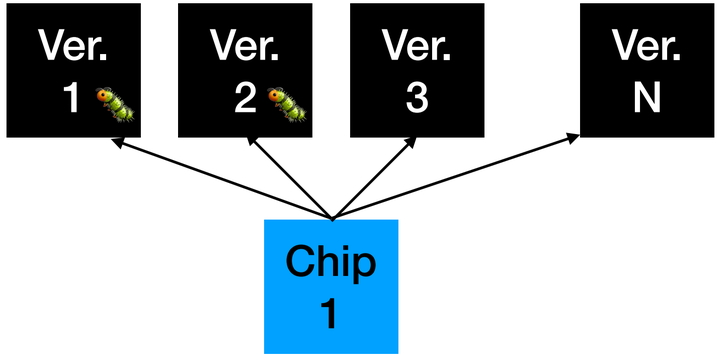
SECURE MOBILE NETWORKING

BROADCOM®

DARK MENTOR

SILICON LABS®

VersionPrint

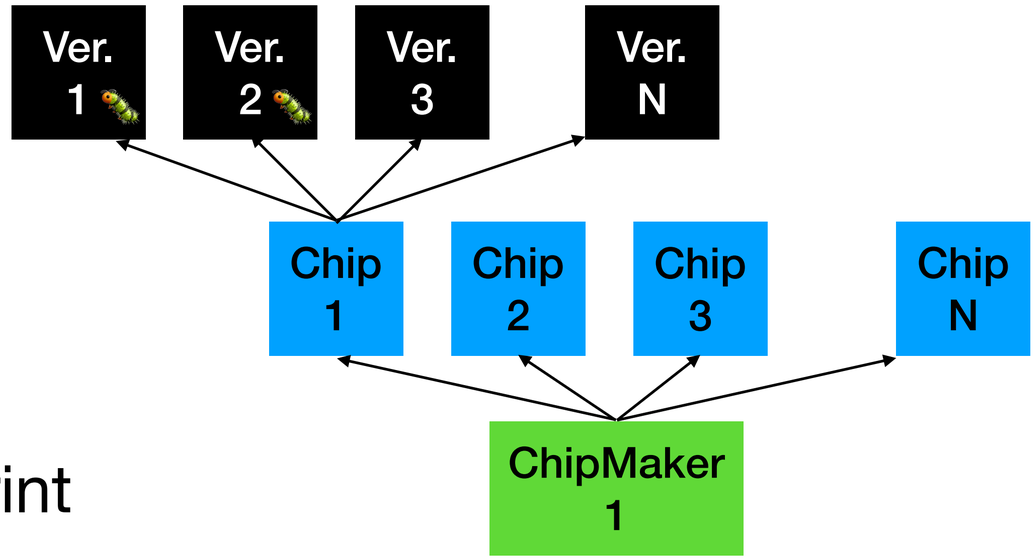


ChipPrint

VersionPrint

ChipPrint

ChipMakerPrint

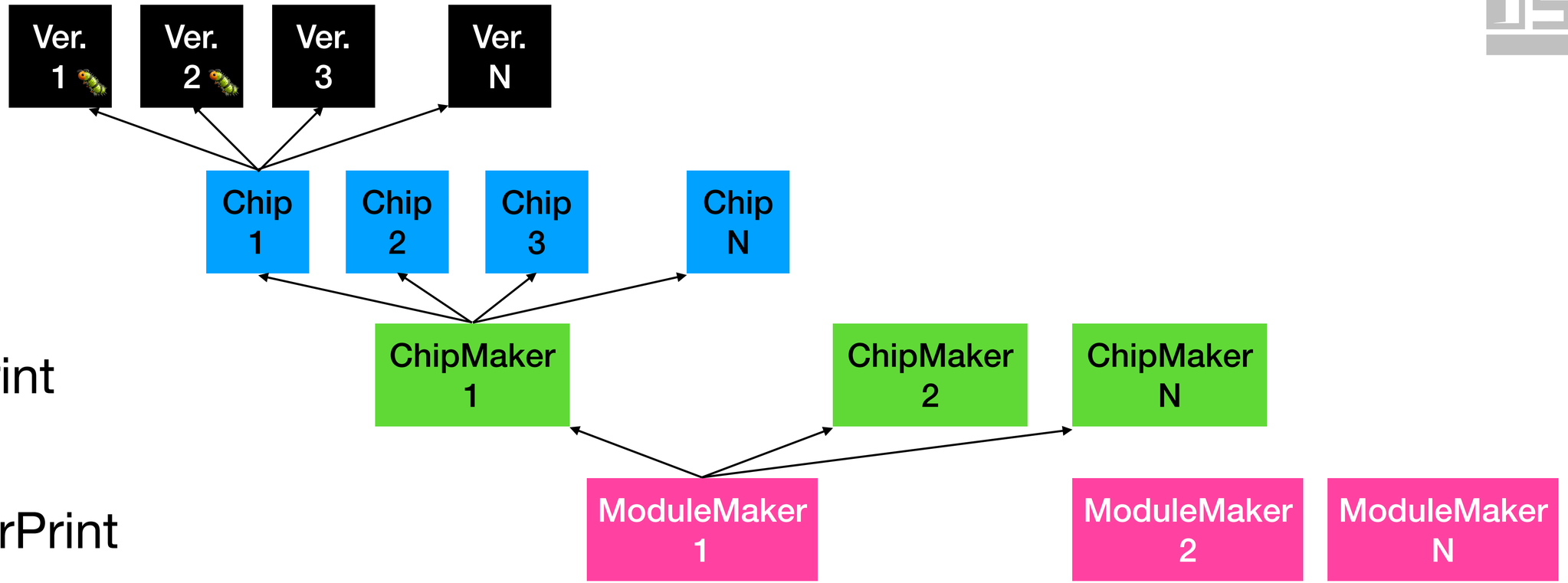


VersionPrint

ChipPrint

ChipMakerPrint

ModuleMakerPrint



Realtek

ChipMaker
1

From
https://docs.ai-thinker.com/en/rtl87xx

REALTEK

ChipMaker
1

Ai-Thinker Technology

ModuleMaker
1

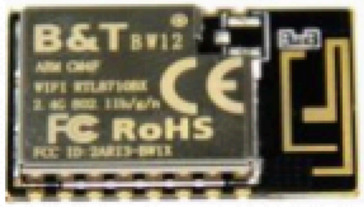
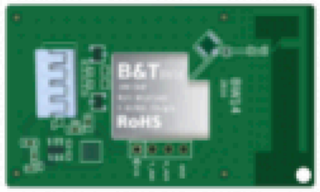
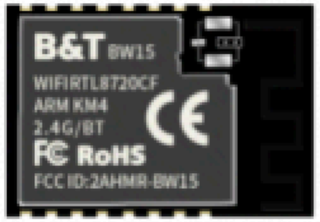
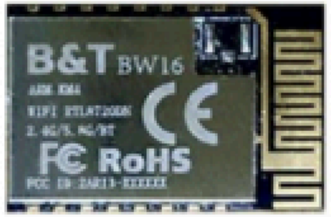
From
https://docs.ai-thinker.com/en/rtl87xx

REALTEK

ChipMaker 1

Ai-Thinker Technology

ModuleMaker 1

Model	BW12		BW15	BW16（hot）
Picture				
Chip	RTL8710BX	RTL8710BX	RTL8720CF	RTL8720DN
Package	SMT-16	/	SMD-16	SMD-16
Size	24 x16x 3mm (LxWxH) ±0.2mm	50.5*29.2*3.3（±0.2） mm	24*16*3(±0.2)MM	24*16*3(±0.2)MM
Antenna	on-board PCB/ IPEX antenna	on-board PCB/ IPEX antenna	on-board PCB/ IPEX antenna	on-board PCB/ IPEX antenna
Frequency range	24 Module 1 lz	240 Module 2 Hz	2.40 Module 3 GHz	2400-248 Module 4 180-5825MHz
Bluetooth			Bl LE	5.0
Operating temperature	-20~+85° C	-20℃~70℃	-40 ℃ ~ 85 ℃	-20 ℃ ~ 70 ℃
Storage temperature	-40 ~125°C	-40℃~125℃	-40 ℃ ~ 125 ℃ , < 90%RH	-40 ℃ ~ 125 ℃ , < 90%RH
Power supply	3.3±10%V	5V ~ 12V	Voltage 3.0 V ~3.6 V, current >500 mA	Voltage 3.0V ~ 3.6V，Typical 3.3V, Current >450mA
Interface	UART,I2C, SPI, GPIO, SWD, PWM	UART	UART/GPIO/ADC/PWM /IIC /SPI	UART/GPIO/ADC/PWM/IIC/SPI/SWD

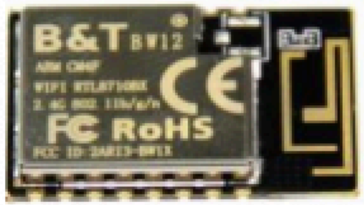
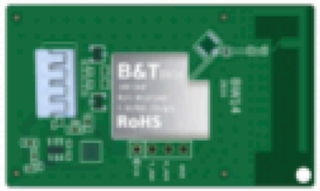
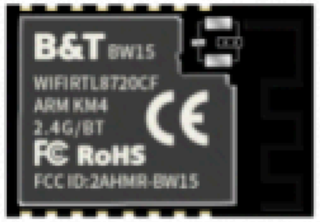
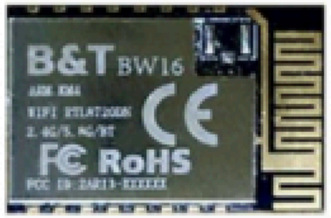
From
https://docs.ai-thinker.com/en/rtl87xx

REALTEK

ChipMaker 1

Ai-Thinker Technology

ModuleMaker 1

Model	BW12		BW15	BW16（hot）
Picture				
Chip	RTL8710BX	RTL8710BX	RTL8720CF	RTL8720DN
Package	SMT-16	/	SMD-16	SMD-16
Size	24 x16x 3mm (LxWxH) ±0.2mm	50.5*29.2*3.3（±0.2） mm	24*16*3(±0.2)MM	24*16*3(±0.2)MM
Antenna	on-board PCB/ IPEX antenna	on-board PCB/ IPEX antenna	on-board PCB/ IPEX antenna	on-board PCB/ IPEX antenna
Frequency range	24 Module 1 lz	240 Module 2 Hz	2.40 Module 3 GHz	2400-248 Module 4 180-5825MHz
Bluetooth			Bl LE	5.0
Operating temperature	-20~+85° C	-20℃~70℃	-40 ℃ ~ 85 ℃	-20 ℃ ~ 70 ℃
Storage temperature	-40 ~125°C	-40℃~125℃	-40 ℃ ~ 125 ℃ , < 90%RH	-40 ℃ ~ 125 ℃ , < 90%RH
Power supply	3.3±10%V	5V ~ 12V	Voltage 3.0 V ~3.6 V, current >500 mA	Voltage 3.0V ~ 3.6V，Typical 3.3V, Current >450mA
Interface	UART,I2C, SPI, GPIO, SWD, PWM	UART	UART/GPIO/ADC/PWM /IIC /SPI	UART/GPIO/ADC/PWM/IIC/SPI/SWD

???

From
https://docs.ai-thinker.com/en/rtl87xx

3330 *Product Makers registered* with Bluetooth SIG as of the time of writing!

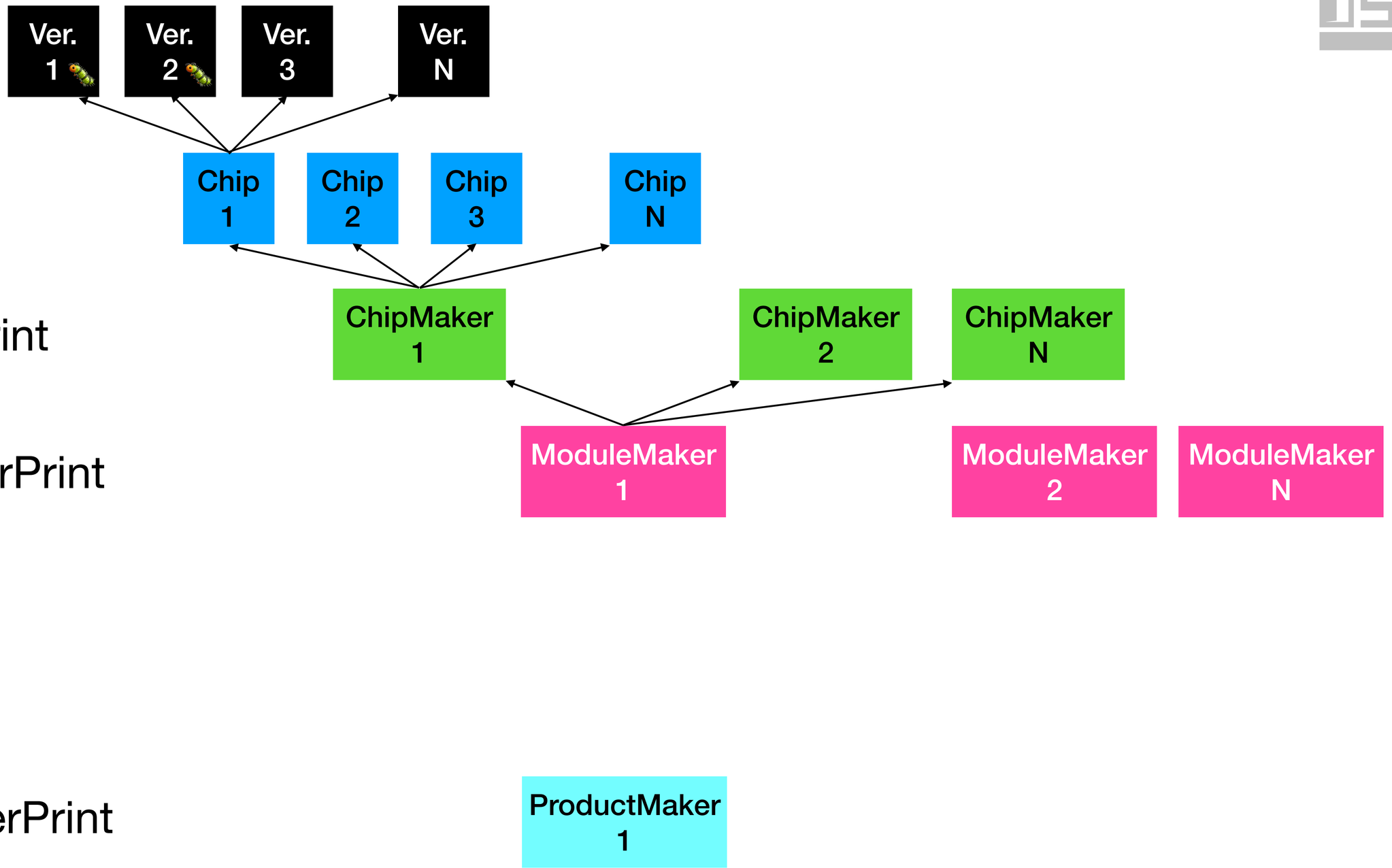
VersionPrint

ChipPrint

ChipMakerPrint

ModuleMakerPrint

ProductMakerPrint



3330 *Product Makers registered* with Bluetooth SIG as of the time of writing!

VersionPrint

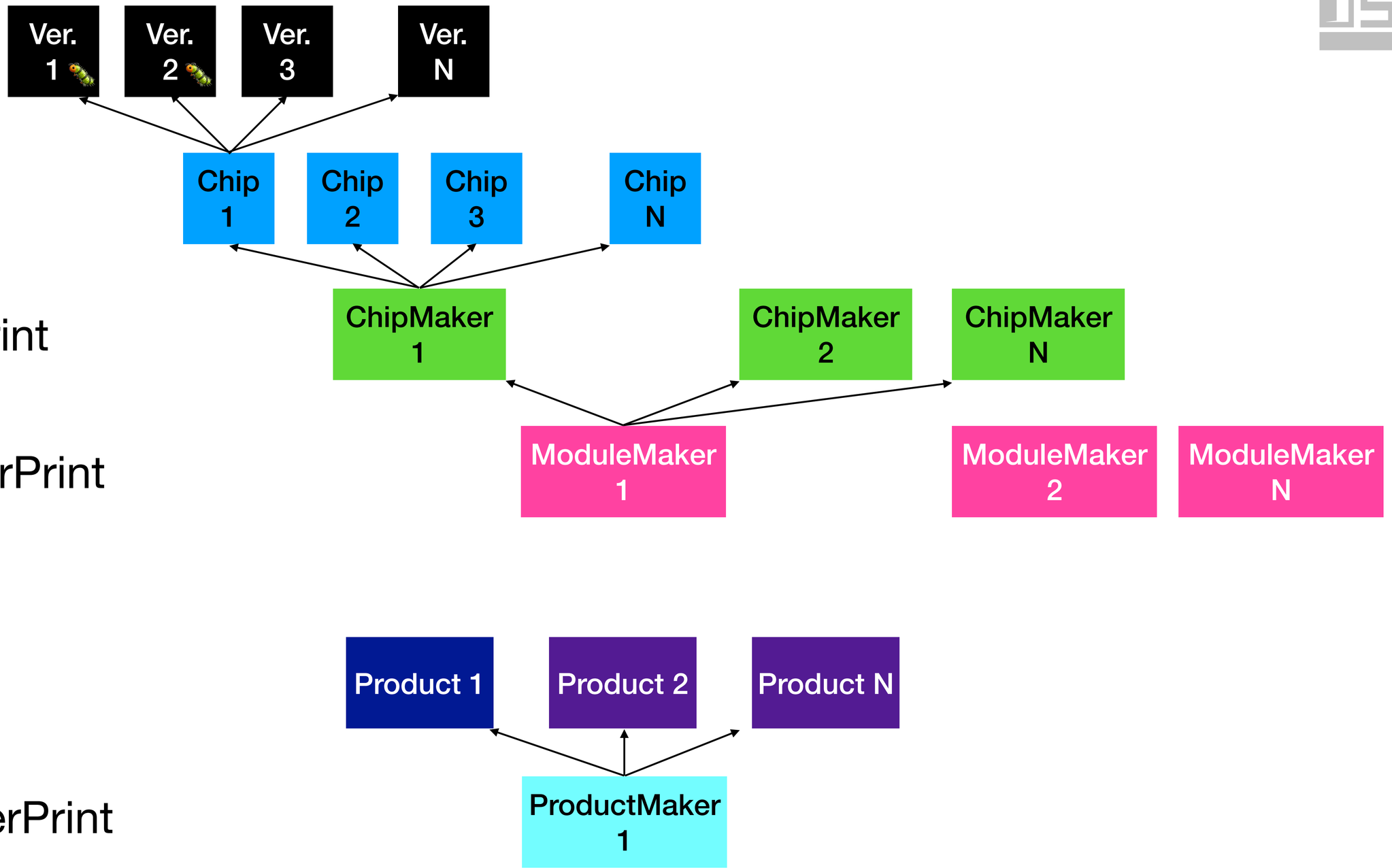
ChipPrint

ChipMakerPrint

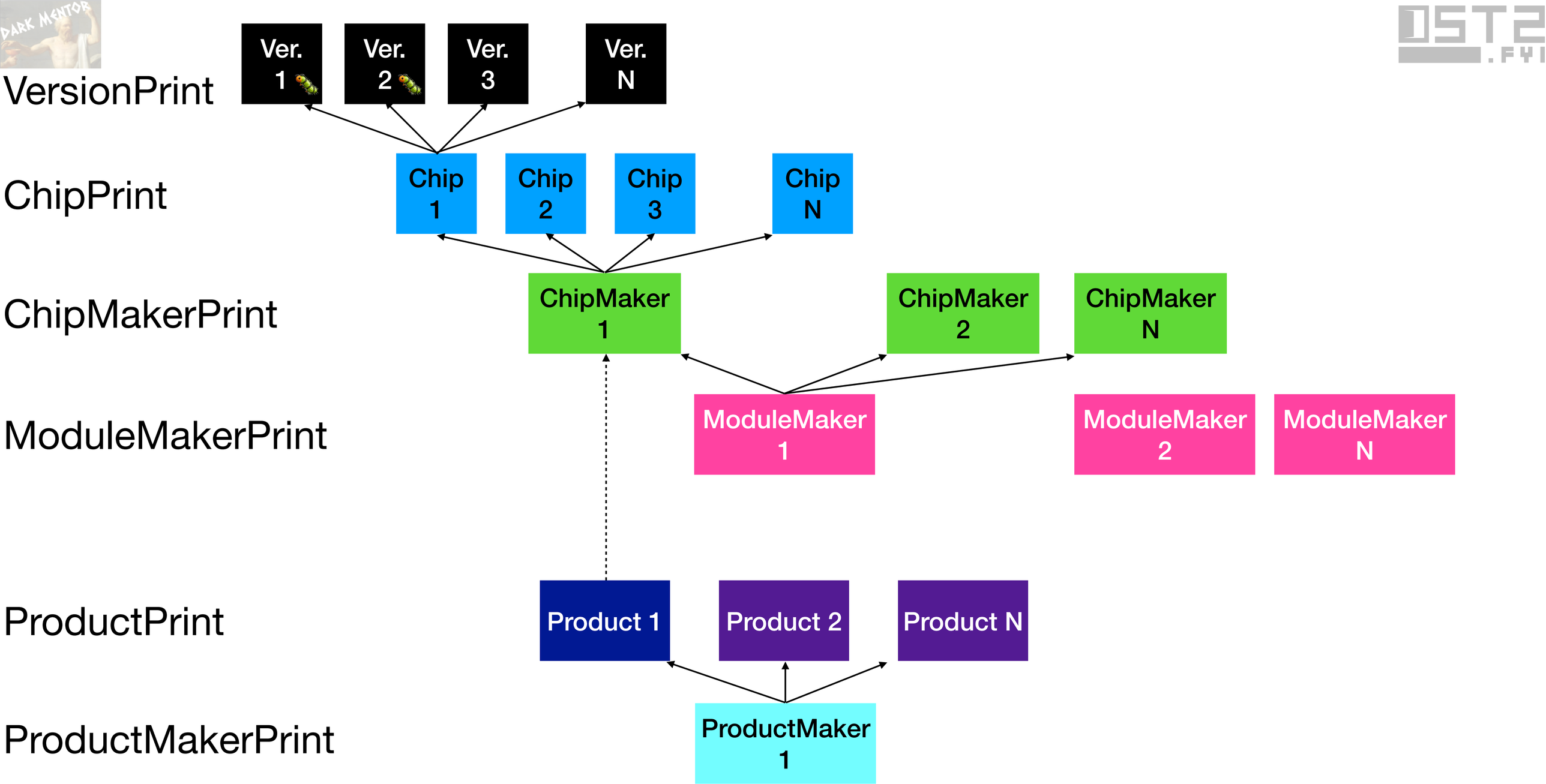
ModuleMakerPrint

ProductPrint

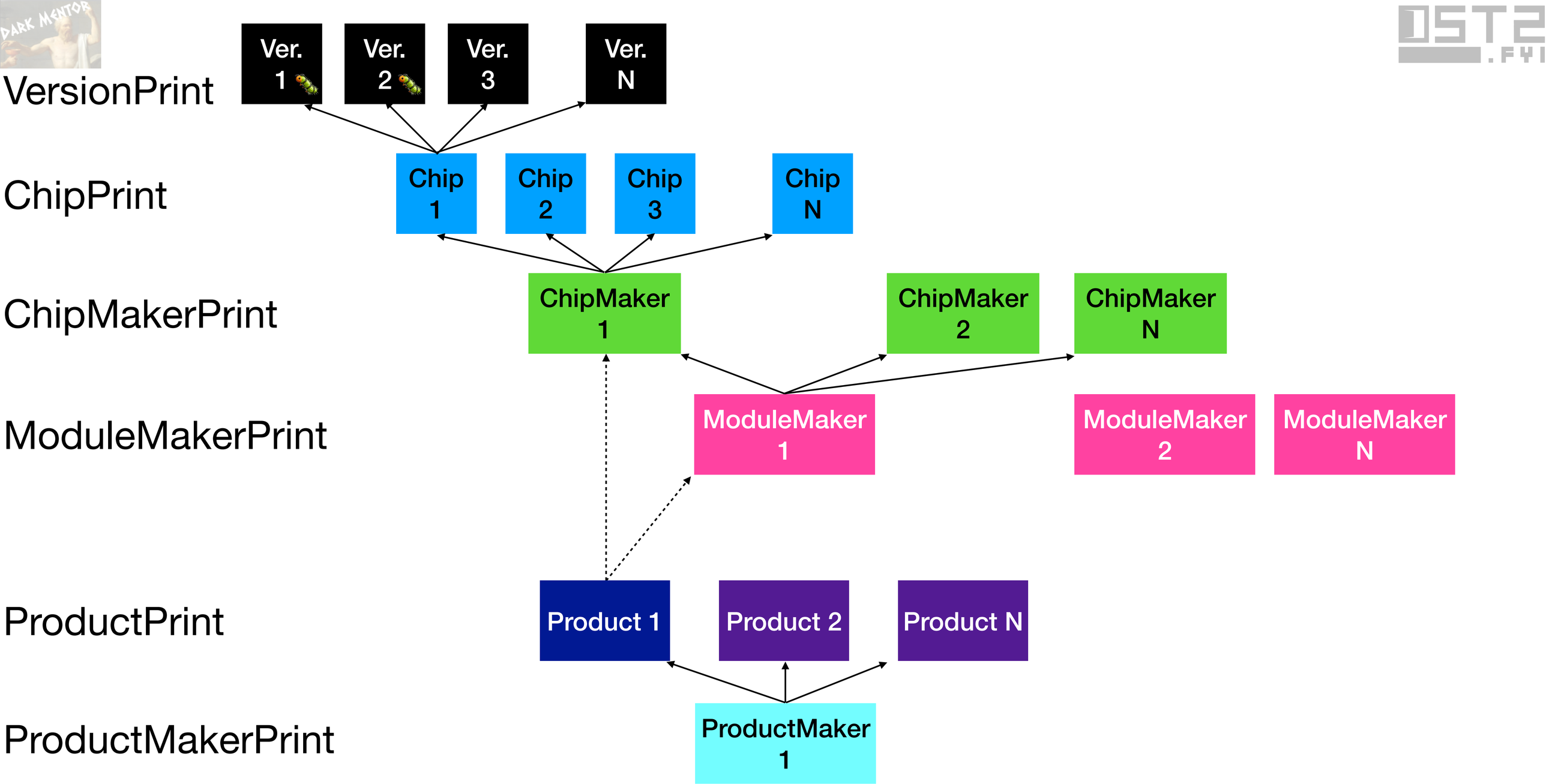
ProductMakerPrint



3330 *Product Makers registered* with Bluetooth SIG as of the time of writing!



3330 *Product Makers registered* with Bluetooth SIG as of the time of writing!



3330 *Product Makers registered* with Bluetooth SIG as of the time of writing!

There is almost always a 1:1 relationship from Products to Chips

We need to discover it

3330 *Product Makers registered* with Bluetooth SIG as of the time of writing!

VersionPrint

ChipPrint

ChipMakerPrint

ModuleMakerPrint

ProductPrint

ProductMakerPrint

Ver. 1

Ver. 2

Ver. 3

Ver. N

Chip 1

Chip 2

Chip 3

Chip N

ChipMaker

ChipMaker 2

ChipMaker N

ModuleMaker 1

ModuleMaker 2

ModuleMaker N

Product 1

Product 2

Product N

ProductMaker 1

There is almost always a 1:1 relationship from Products to Chips

We need to discover it

3330 *Product Makers registered* with Bluetooth SIG as of the time of writing!

VersionPrint

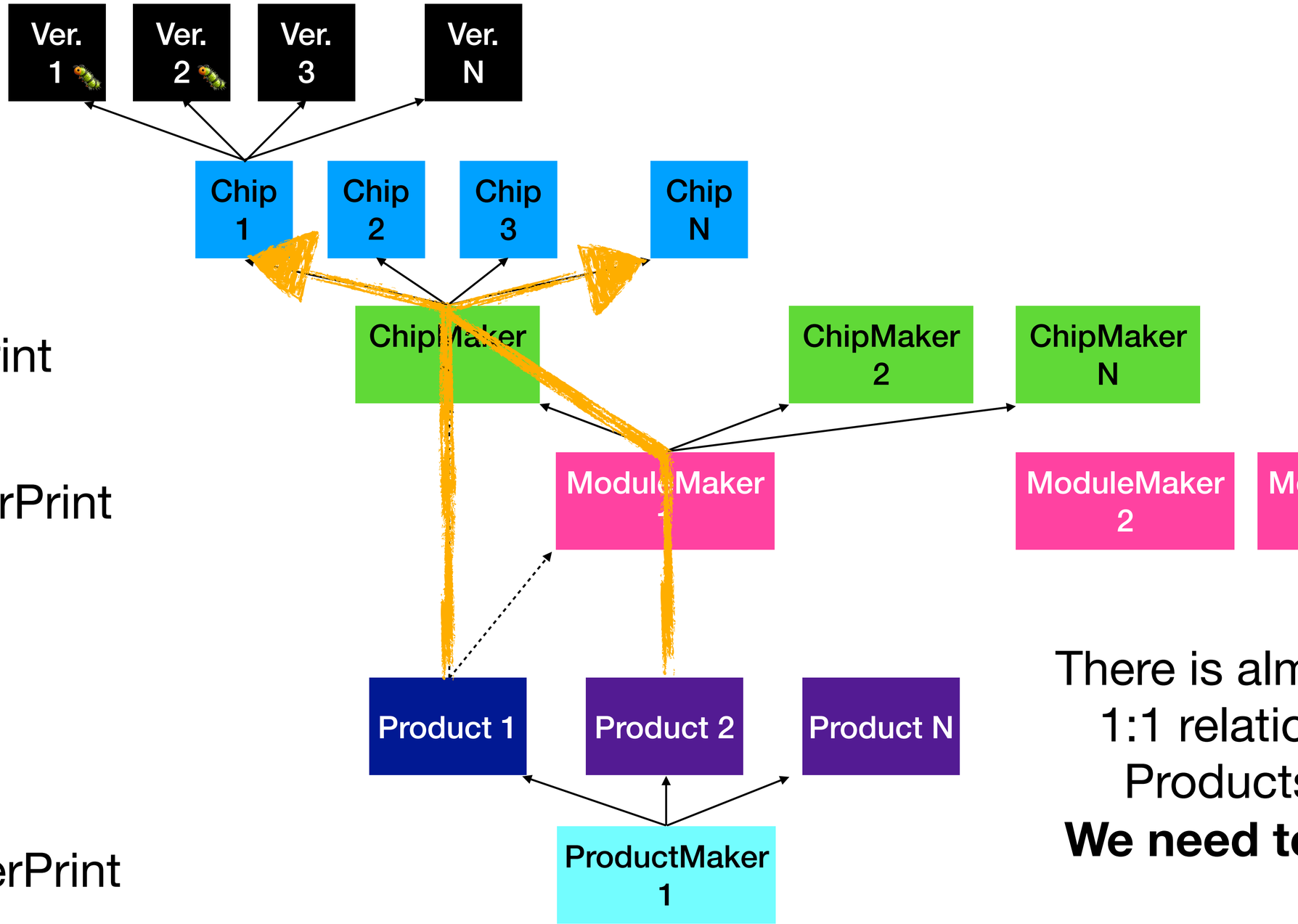
ChipPrint

ChipMakerPrint

ModuleMakerPrint

ProductPrint

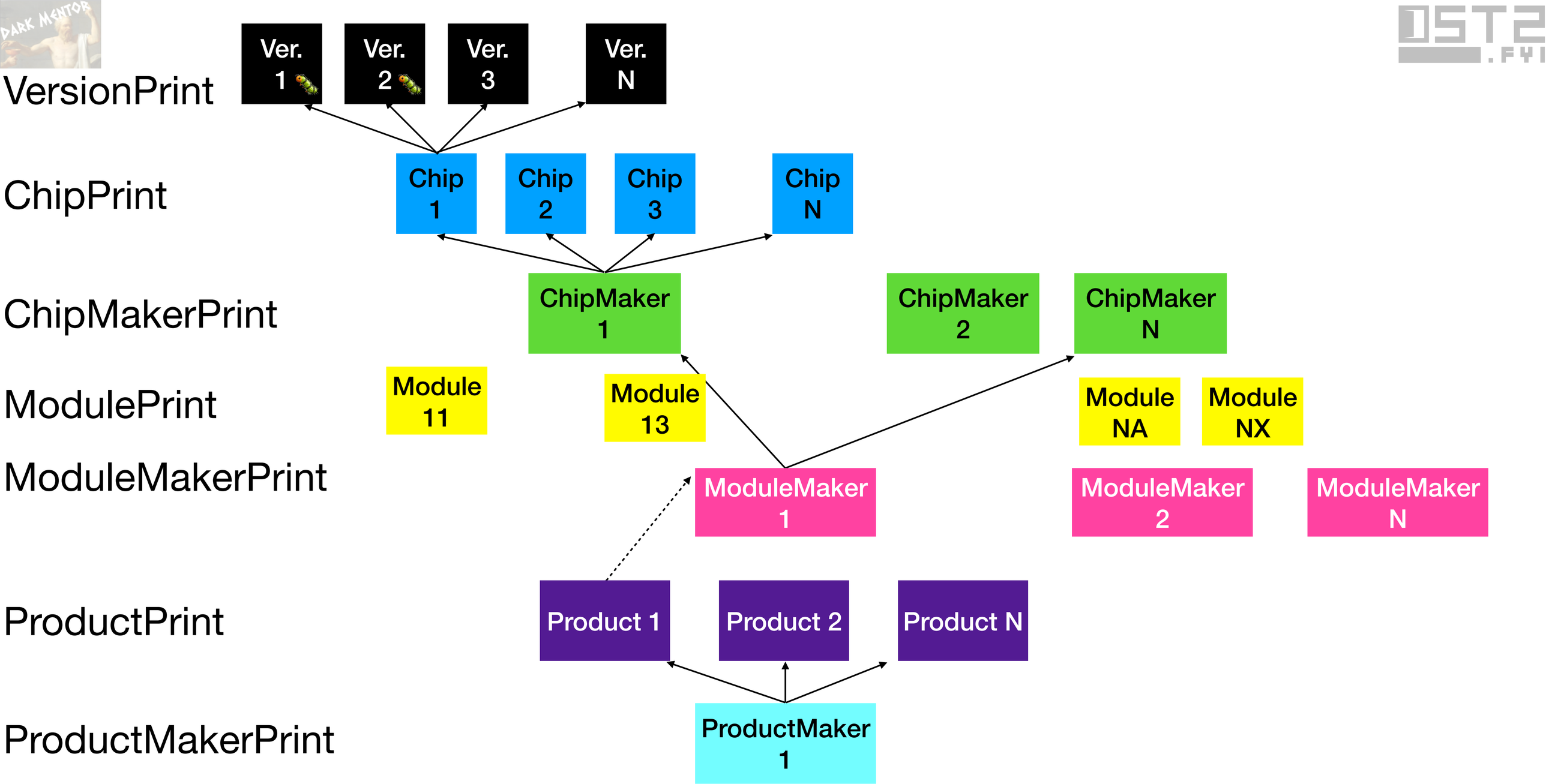
ProductMakerPrint



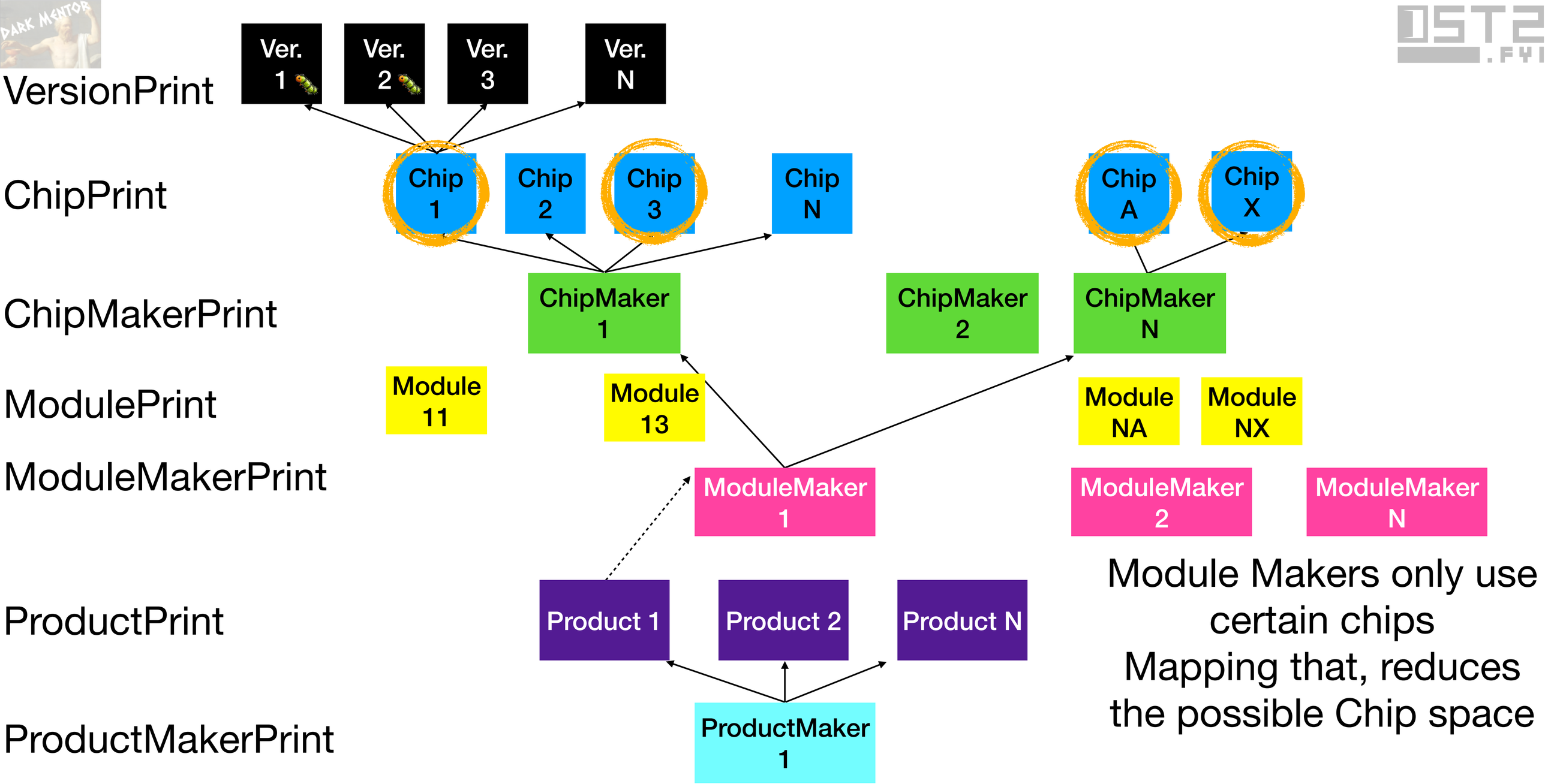
There is almost always a 1:1 relationship from Products to Chips

We need to discover it

3330 *Product Makers registered* with Bluetooth SIG as of the time of writing!

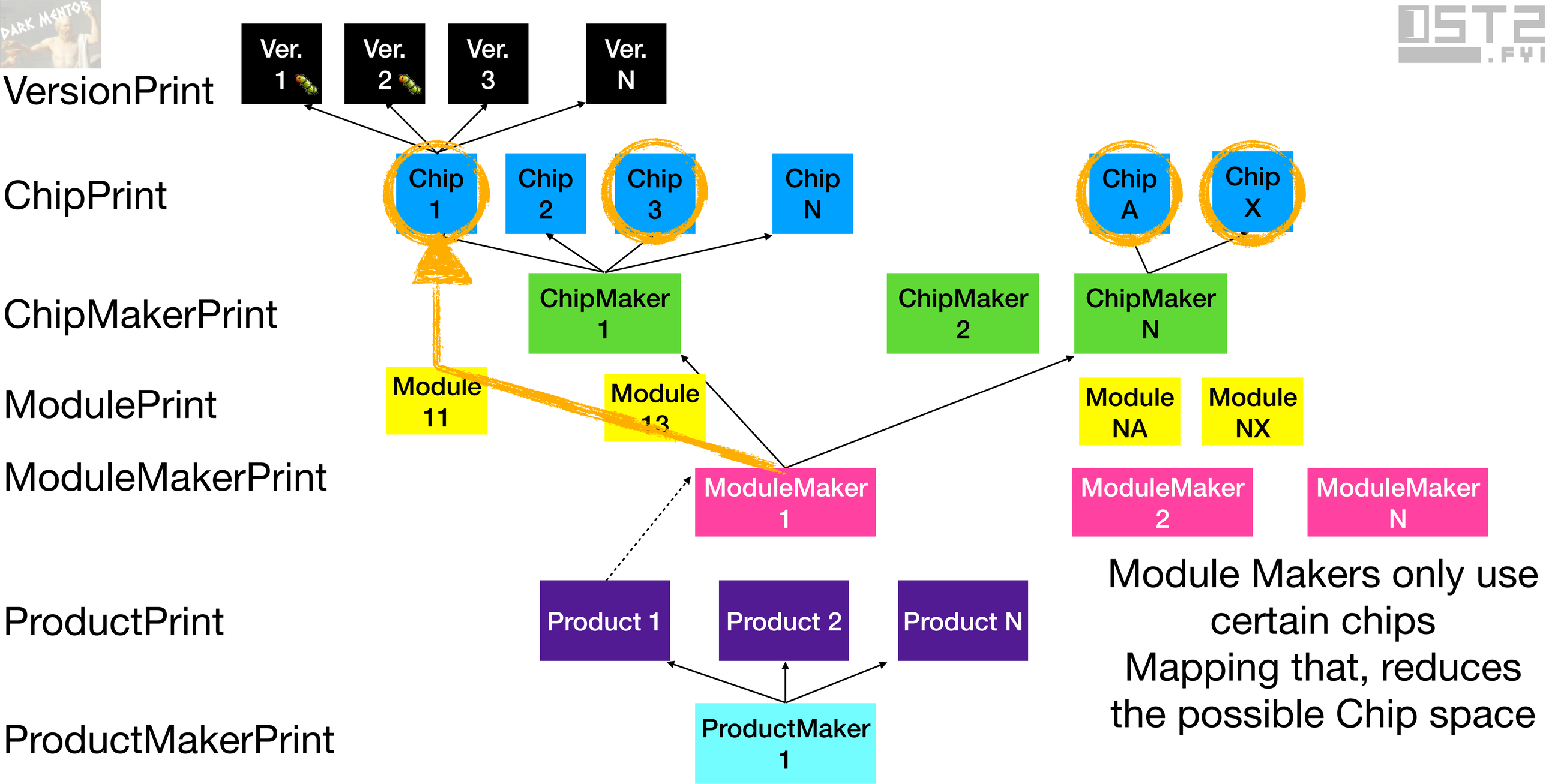


3330 *Product Makers registered* with Bluetooth SIG as of the time of writing!



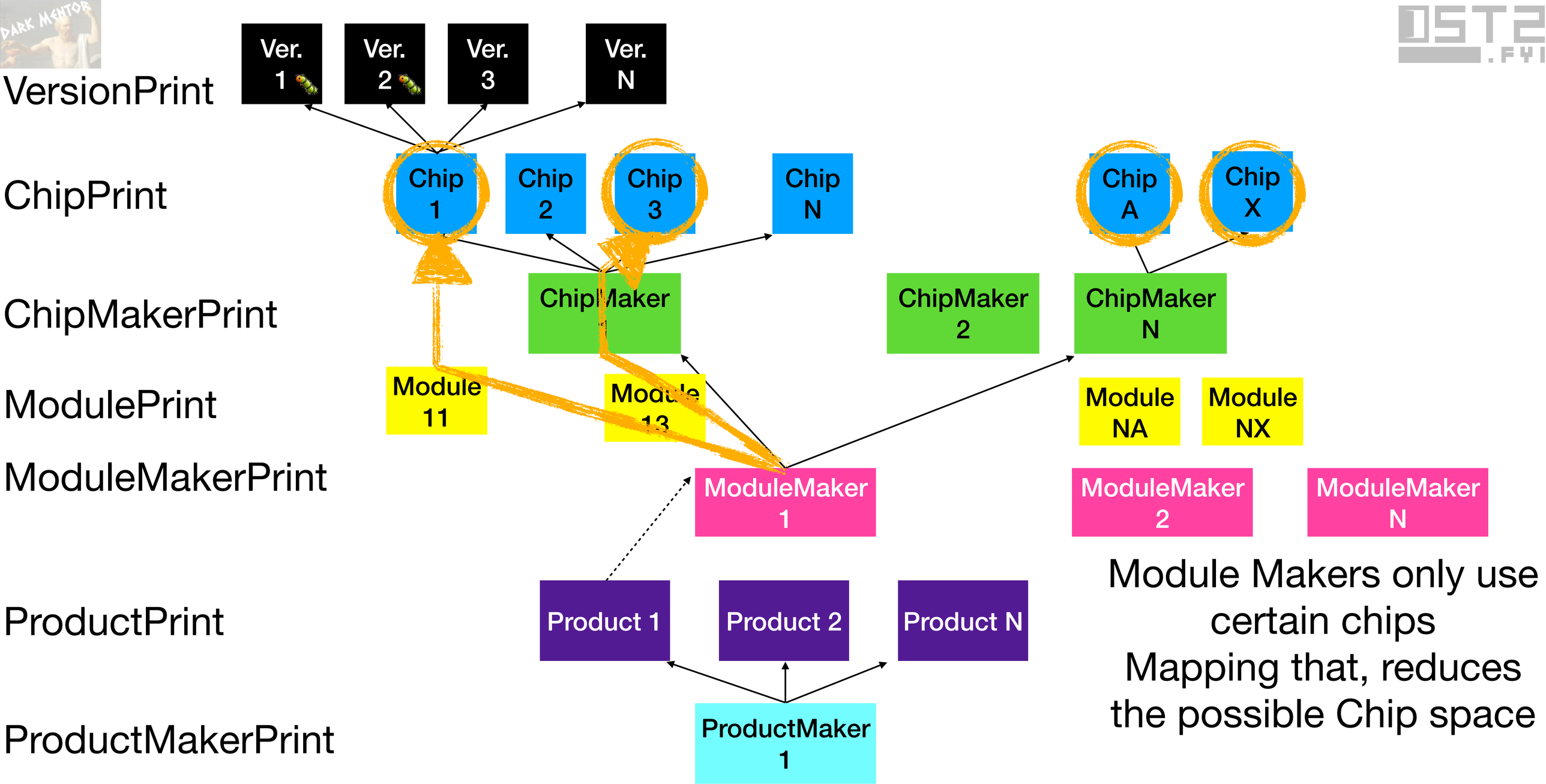
Module Makers only use certain chips
Mapping that, reduces the possible Chip space

3330 *Product Makers registered* with Bluetooth SIG as of the time of writing!

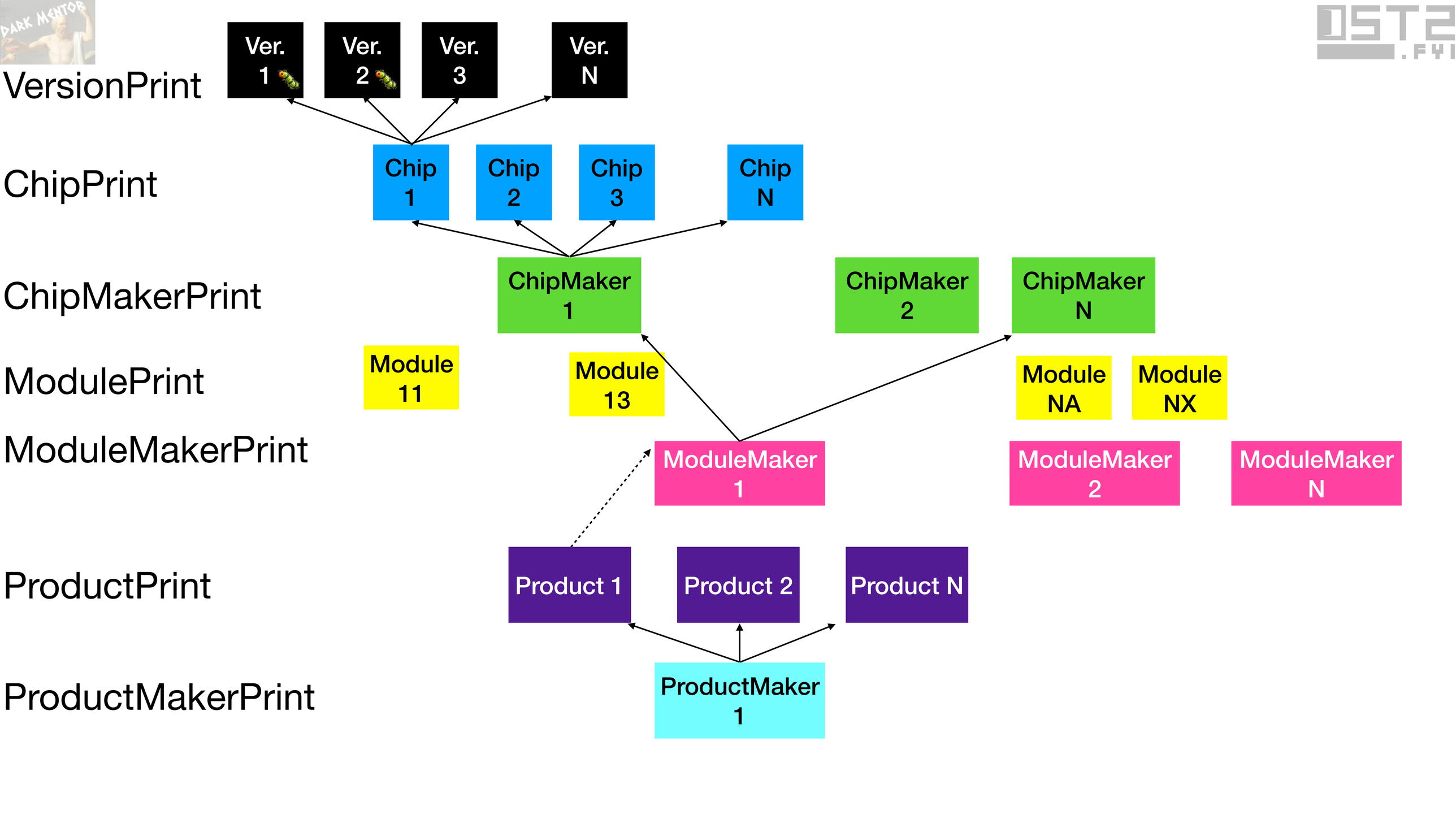


Module Makers only use certain chips
Mapping that, reduces the possible Chip space

3330 *Product Makers registered* with Bluetooth SIG as of the time of writing!



3330 *Product Makers registered* with Bluetooth SIG as of the time of writing!


VersionPrint
ChipPrint
ChipMakerPrint
ModulePrint
ModuleMakerPrint
ProductPrint
ProductMakerPrint
Ver. 1
Ver. 2
Ver. 3
Ver. N
Chip 1
Chip 2
Chip 3
Chip N
ChipMaker 1
ChipMaker 2
ChipMaker N
Module 11
Module 13
Module NA
Module NX
ModuleMaker 1
ModuleMaker 2
ModuleMaker N
Product 1
Product 2
Product N
ProductMaker 1

WHAT I WANT!

VersionPrint

Ver. 1

Ver. 2

Ver. 3

Ver. N

ChipPrint

Chip 1

Chip 2

Chip 3

Chip N

ChipMakerPrint

ChipMaker 1

ChipMaker 2

ChipMaker N

ModulePrint

Module 11

Module 13

Module NA

Module NX

ModuleMakerPrint

ModuleMaker 1

ModuleMaker 2

ModuleMaker N

ProductPrint

Product 1

Product 2

Product N

ProductMakerPrint

ProductMaker 1

VersionPrint

Ver. 1

Ver. 2

Ver. 3

Ver. N

WHAT I WANT!

ChipPrint

Chip 1

Chip 2

Chip 3

Chip N

WHAT I MOSTLY GET 😔

ChipMakerPrint

ChipMaker 1

ChipMaker 2

ChipMaker N

ModulePrint

Module 11

Module 13

Module NA

Module NX

ModuleMakerPrint

ModuleMaker 1

ModuleMaker 2

ModuleMaker N

ProductPrint

Product 1

Product 2

Product N

ProductMakerPrint

ProductMaker 1

My Terminology

- BTC = Bluetooth Classic 
- BLE = Bluetooth Low Energy
- BDADDR = Bluetooth Device Address (like MAC address)

So you've millions of datapoints...

Is any of it useful to find a VersionPrint?

- I started doing basic naïve BT data collection as a hobby during the pandemic as a way to get out of the house and drive around
  - See "It was harder to sniff Bluetooth through my mask during the pandemic" talk from summer 2023

So you've millions of datapoints...

Is any of it useful to find a VersionPrint?

- I started doing basic naïve BT data collection as a hobby during the pandemic as a way to get out of the house and drive around
  - See "It was harder to sniff Bluetooth through my mask during the pandemic" talk from summer 2023
- The majority of my data is Linux "HCI" logs
  - HCI is the Host-Controller-Interface, between Linux, and the BT chip on my logging platform (mostly Raspberry Pi Zeros or 4Bs)

So you've millions of datapoints...

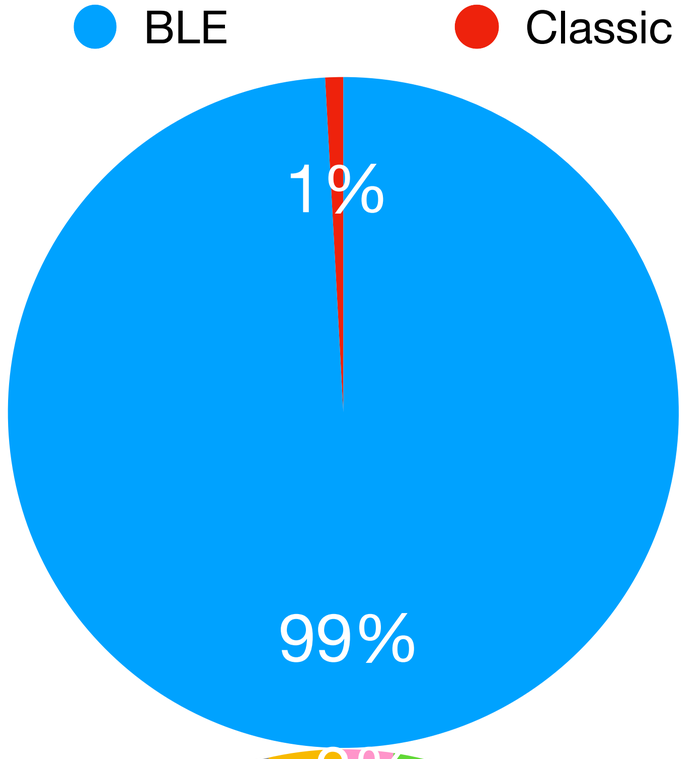
Is any of it useful to find a VersionPrint?

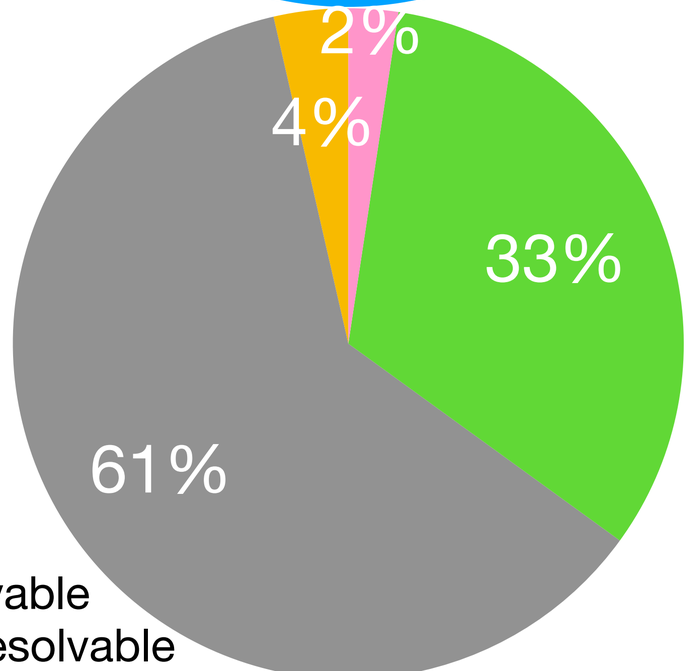
- I started doing basic naïve BT data collection as a hobby during the pandemic as a way to get out of the house and drive around
  - See "It was harder to sniff Bluetooth through my mask during the pandemic" talk from summer 2023
- The majority of my data is Linux "HCI" logs
  - HCI is the Host-Controller-Interface, between Linux, and the BT chip on my logging platform (mostly Raspberry Pi Zeros or 4Bs)
- I started work on customized 2thprinting in May 2023, once I had a chance to start looking at what the HCI logs could, and couldn't, provide for 2thprinting

Overall BDADDR Data

My data as of 2024-01-12

- 74,934 *unique* BT Classic BDADDRs
- 8,569,483 *unique* BLE BDADDRs
  - 204,708 "public" BDADDRs
  - 2,793,274 "random static" BDADDRs
  - 5,264,247 "random resolvable" BDADDRs
  - 307,030 "random non-resolvable" BDADDRs





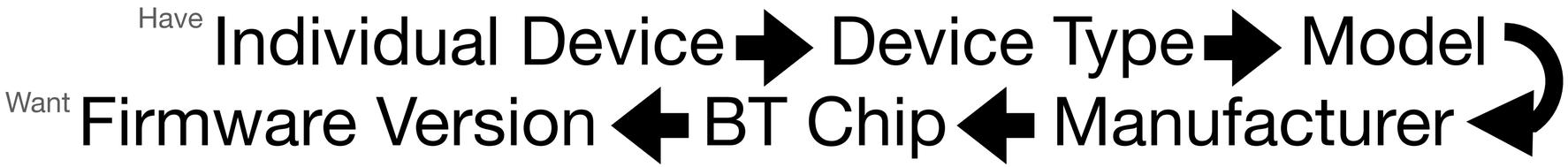
What I Want To Know:

What Bluetooth Chip Is Inside Any Device

Why I Want To Know It:

So I Know if it's Vulnerable To a Firmware-Level Exploit

Some Possible Information Relationships

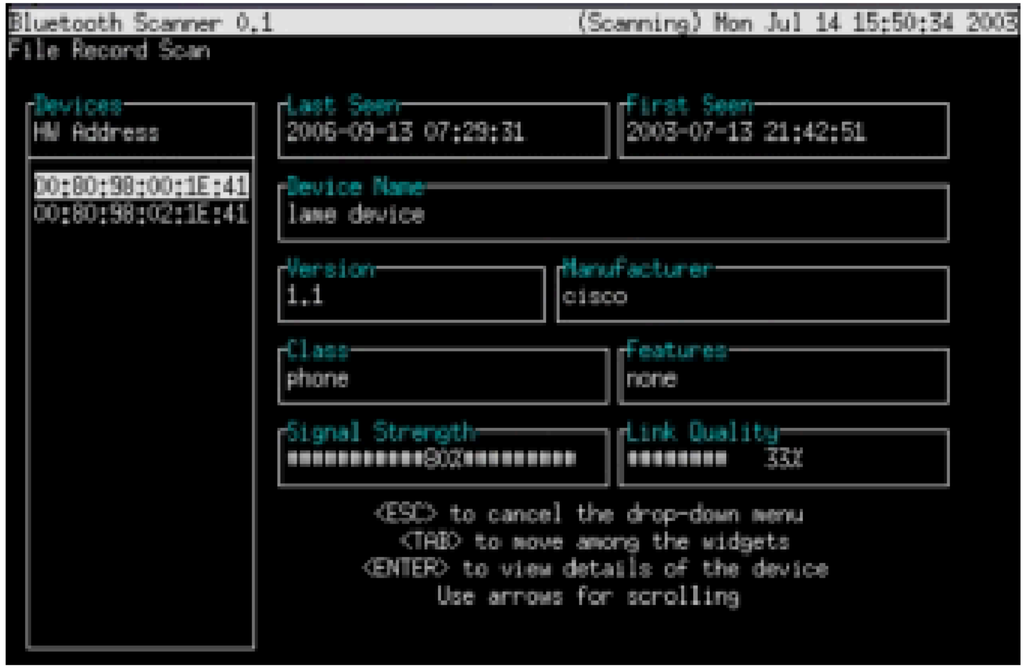


Prior Work

"Bluesniff - The Next Wardriving Frontier"

- [1] by Potter from 2003 "Focused on providing a UI", provided information about discoverable BTC devices

Exhibit G: Bluesniff



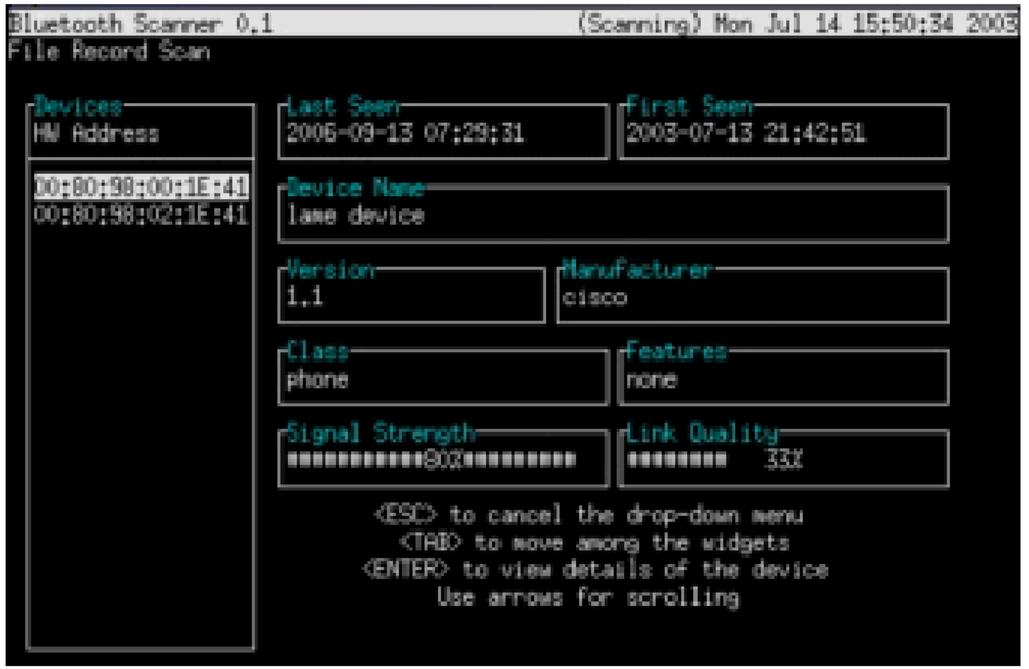
[1] https://web.archive.org/web/20031115220513/http://www.shmoo.com/~gdead/dc-11-brucepotter.ppt
Image from https://web.archive.org/web/20040303230609/http://www.atstake.com/research/reports/acrobat/atstake_war_nibbling.pdf

Prior Work

"Bluesniff - The Next Wardriving Frontier"

- [1] by Potter from 2003 "Focused on providing a UI", provided information about discoverable BTC devices

Exhibit G: Bluesniff



Individual Device → Device Type → Model → Manufacturer → BT Chip → Firmware Version

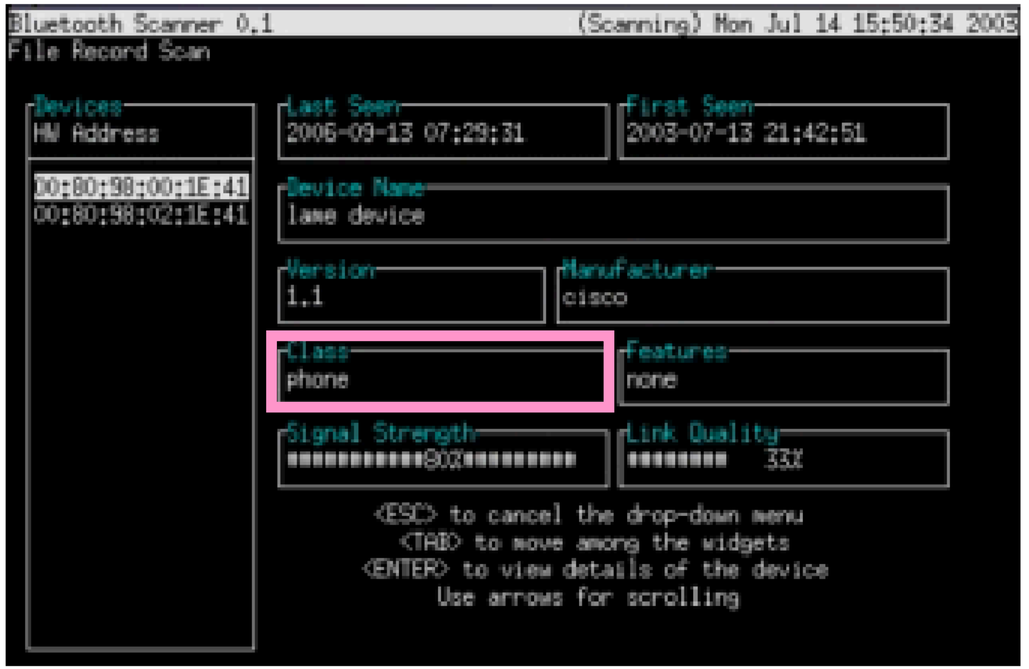
[1] https://web.archive.org/web/20031115220513/http://www.shmoo.com/~gdead/dc-11-brucepotter.ppt
Image from https://web.archive.org/web/20040303230609/http://www.atstake.com/research/reports/acrobat/atstake_war_nibbling.pdf

Prior Work

"Bluesniff - The Next Wardriving Frontier"

- [1] by Potter from 2003 "Focused on providing a UI", provided information about discoverable BTC devices

Exhibit G: Bluesniff



Individual Device → Device Type → Model

Firmware Version ← BT Chip ← Manufacturer

[1] https://web.archive.org/web/20031115220513/http://www.shmoo.com/~gdead/dc-11-brucepotter.ppt

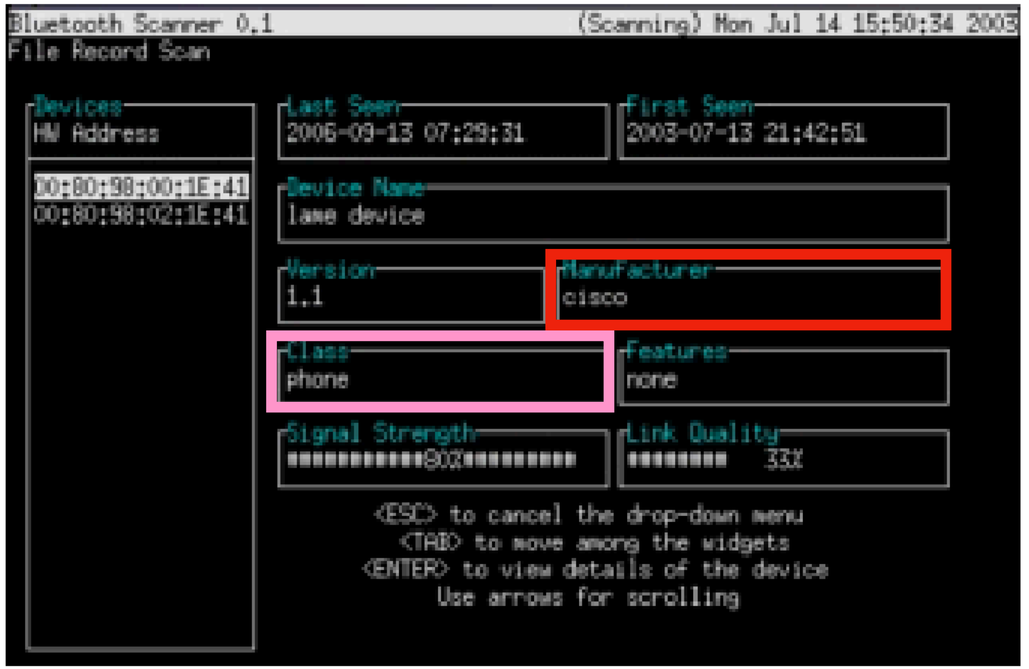
Image from https://web.archive.org/web/20040303230609/http://www.atstake.com/research/reports/acrobat/atstake_war_nibbling.pdf

Prior Work

"Bluesniff - The Next Wardriving Frontier"

- [1] by Potter from 2003 "Focused on providing a UI", provided information about discoverable BTC devices

Exhibit G: Bluesniff



Individual Device → Device Type → Model

Firmware Version ← BT Chip ← Manufacturer

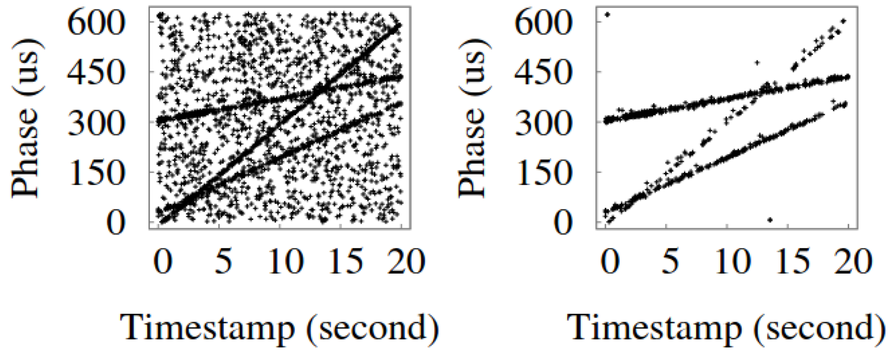
[1] https://web.archive.org/web/20031115220513/http://www.shmoo.com/~gdead/dc-11-brucepotter.ppt

Image from https://web.archive.org/web/20040303230609/http://www.atstake.com/research/reports/acrobat/atstake_war_nibbling.pdf

Prior Work

"BlueID: A Practical System for Bluetooth Device Identification"

- [1] by Jun Huang et al. from 2014 is focused on identifying individual devices, within a collection of potentially address-randomizing devices, based on clock skew over time



(a) Before noise filtering. (b) After noise filtering.

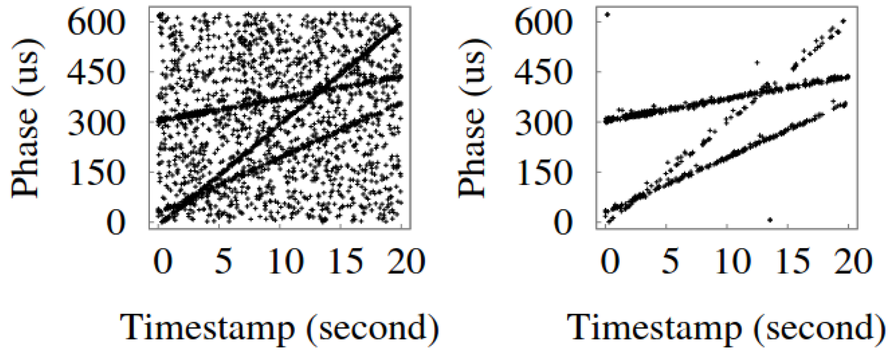
Fig. 2. Effect of noise filtering on Bluetooth preamble detections.

[1] https://www.cse.msu.edu/~huangjun/docs/blueid_infocom14.pdf

Prior Work

"BlueID: A Practical System for Bluetooth Device Identification"

- [1] by Jun Huang et al. from 2014 is focused on identifying individual devices, within a collection of potentially address-randomizing devices, based on clock skew over time



(a) Before noise filtering. (b) After noise filtering.

Fig. 2. Effect of noise filtering on Bluetooth preamble detections.

Individual Device → Device Type → Model → Manufacturer → BT Chip → Firmware Version

[1] https://www.cse.msu.edu/~huangjun/docs/blueid_infocom14.pdf

BT Timeline wiki plug!: https://darkmentor.com/bt.html

Bluetooth Security Timeline

24th March 2024 at 10:57am

Submit additions or corrections via Merge Requests at https://gitlab.com/XenoKovah/bluetooth-security-timeline

Key:
⬆️🥊 = High Impact!
🥷 = PoC exploit available
🛠️ = Tool

2024

03

BlueSpy – Spying on Bluetooth conversations🛠️

OOB-Write in Android ATT

Use-after-free in Android BLE audio

RattaGATTa: Scalable Bluetooth Low-Energy Survey🛠️

02

Commercial Vehicle Electronic Logging Device Security: Unmasking the Risk of Truck-to-Truck Cyber Worms

01

Reverse Engineering Husqvarna Automower BLE Commands🛠️

2023

Bluetooth Security Timeline

By @XenoKovah of @DarkMentorLLC

fingerprint 16 matches

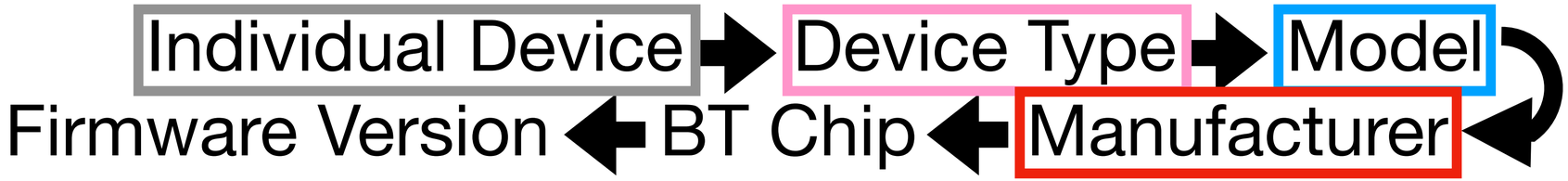
Title matches:

A PSD-based fingerprinting approach to detect IoT device spoofing
An overview of bluetooth device discovery and fingerprinting techniques – assessing the local context
Automatic Fingerprinting of Vulnerable BLE IoT Devices with Static UUIDs from Mobile Apps
Blueprinting - Remote Device Identification based on Bluetooth Fingerprinting Techniques
Fingerprinting and analysis of Bluetooth devices with automata learning
Fingerprinting Bluetooth-Low-Energy Devices Based on the Generic Attribute Profile
Reverse Engineering Apple's BLE Continuity Protocol for Tracking, OS Fingerprinting, and Behavioral Profiling
Tech: Fingerprinting

All matches:

A PSD-based fingerprinting approach to detect IoT device spoofing
An overview of bluetooth device discovery and fingerprinting techniques – assessing the local context
Automatic Fingerprinting of Vulnerable BLE IoT Devices with Static UUIDs from Mobile Apps
Blue2thprinting (blue-[tooth)-printing]: answering the question of 'WTF am I even looking at?!'
BlueID: A Practical System for Bluetooth Device Identification
Blueprinting - Remote Device Identification based on Bluetooth Fingerprinting Techniques
Bluetooth Security Timeline
Evaluating Physical-Layer BLE Location Tracking Attacks on Mobile Devices
Every Byte Matters: Traffic Analysis of Bluetooth Wearable Devices
Fingerprinting and analysis of Bluetooth devices with automata learning
Fingerprinting Bluetooth-Low-Energy Devices Based on the Generic Attribute Profile
It Was Harder to Sniff Bluetooth Through My Mask During the Pandemic...
Mass-pwning with a small IoT spy bug
RattaGATTa: Scalable Bluetooth Low-Energy Survey
Reverse Engineering Apple's BLE Continuity Protocol for Tracking, OS Fingerprinting, and Behavioral Profiling
Tech: Fingerprinting

Prior Work - What I Mostly Get




DARK MENTOR

What I Want


Individual Device
Device Type
Model
Firmware Version
BT Chip
Manufacturer

🧘 Passive

2thprinting Approaches

🚶 Mostly-Passive

🤾 Active

Bluetooth: The Gathering: 🧘Passive

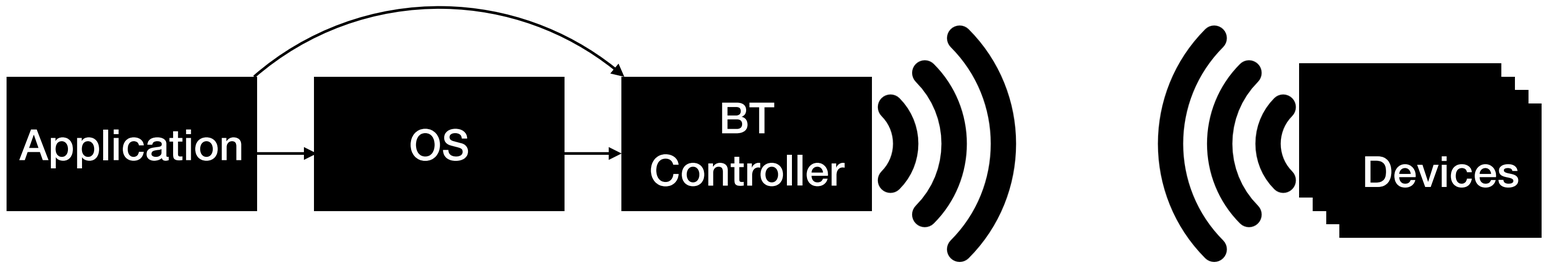
- Run a sniffer, never send *any* packets
- **BLE:** Sniffle, Ice9 Sniffer, **BTC:** Ubertooth
- BLE ADV_IND, NONCONN_ADV_IND

Bluetooth: The Gathering: 🚶 *Mostly*-Passive

- Ask your OS "What Bluetooth devices are currently visible?"
- It will scan for any advertisements, and *potentially,* autonomously, query some limited information about devices it finds, such as device name, class of device, etc (depends on OS & Bluetooth stack version)
  - This is most of my data

Bluetooth: The Gathering: 🤾Active

- Send custom BLE LL / BTC LMP packets (requires custom controller firmware)
- Connect to all connectable interfaces, query all queryable information

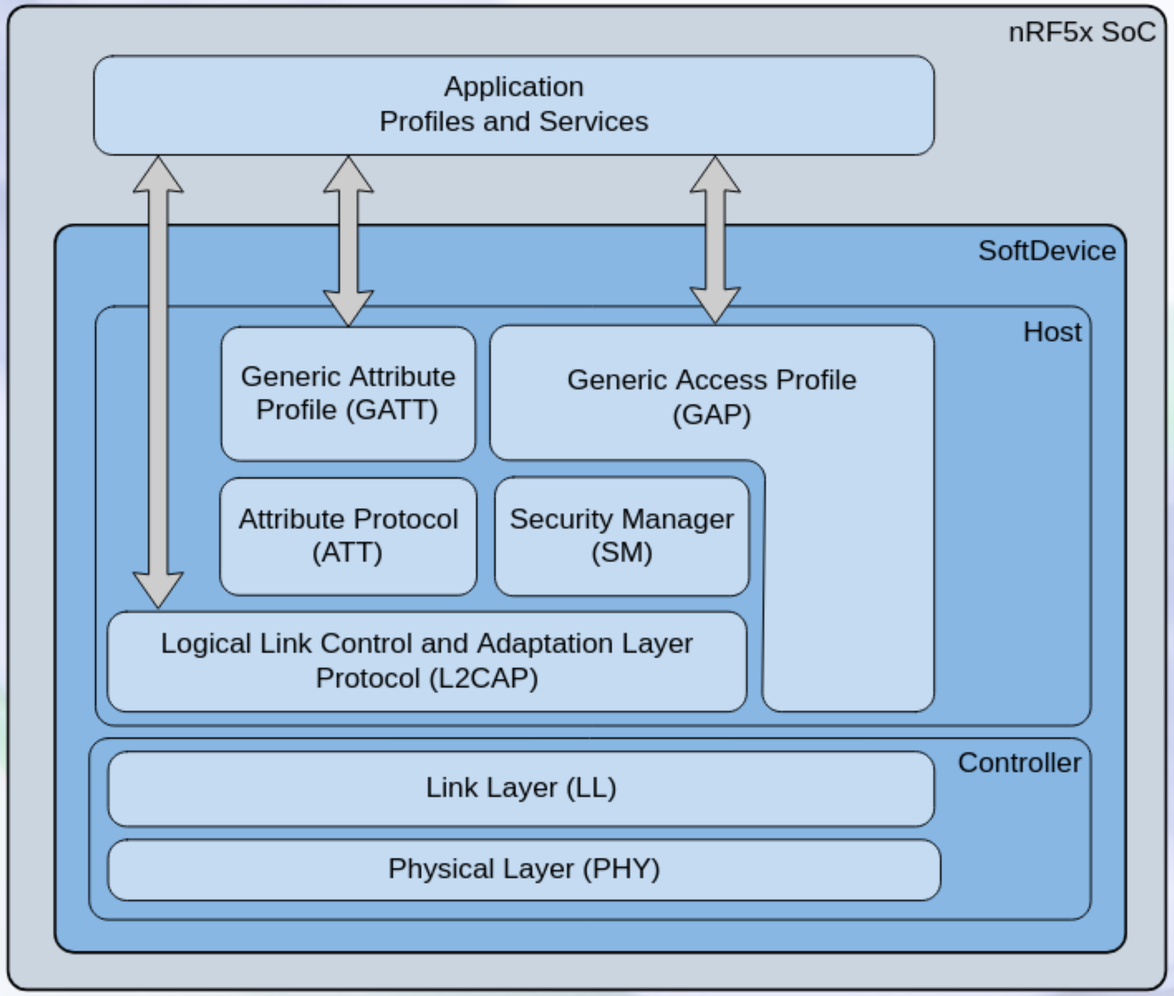


2thprint by BDADDR OUI 🧘

2thprint by BDADDR OUI 🧘

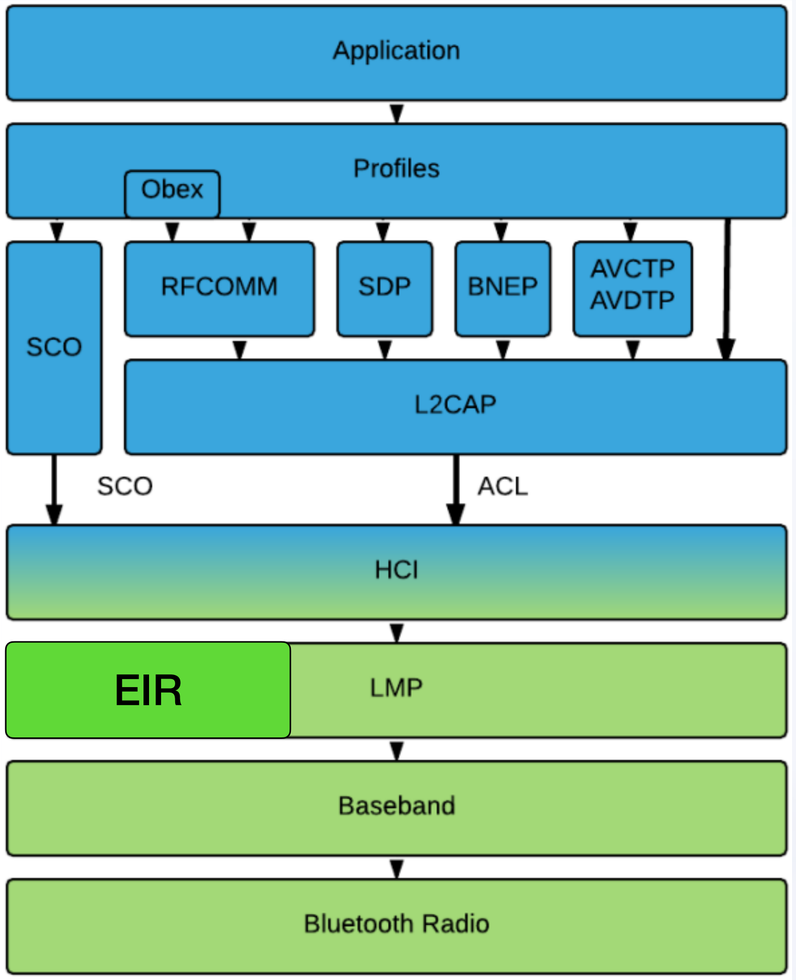
BLE

[1]



BTC

[2]

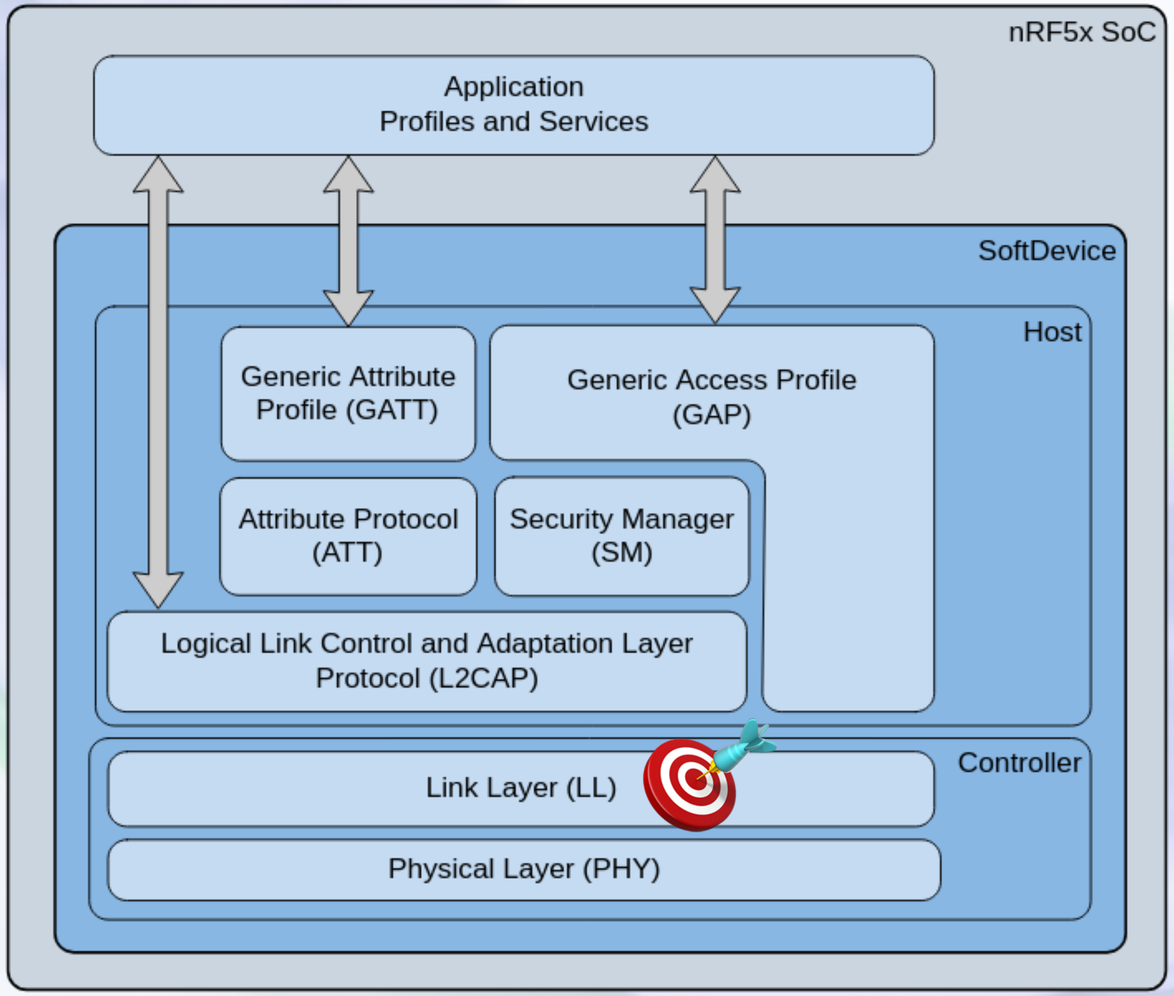


[1] https://infocenter.nordicsemi.com/index.jsp?topic=%2Fsds_s140%2FSDS%2Fs1xx%2Fble_protocol_stack%2Fble_protocol_stack.html
[2] https://crosscontrol.com/manual/Bluetooth%20Documentation/content/bluetooth.html

2thprint by BDADDR OUI 🧘

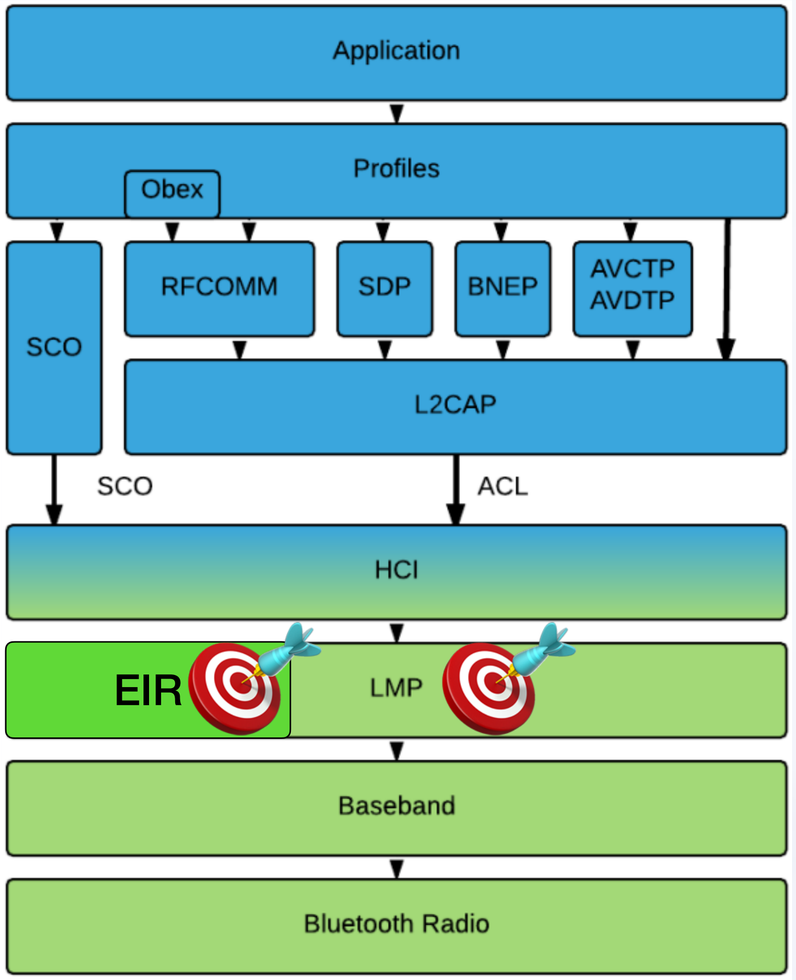
BLE

[1]



BTC

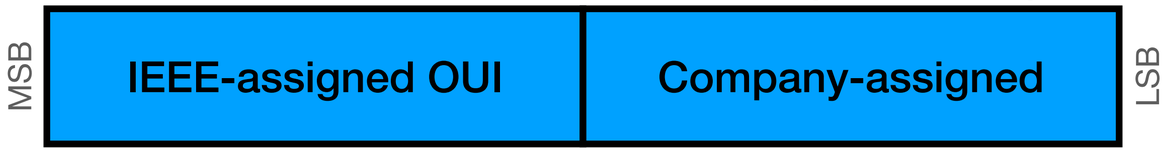
[2]



[1] https://infocenter.nordicsemi.com/index.jsp?topic=%2Fsds_s140%2FSDS%2Fs1xx%2Fble_protocol_stack%2Fble_protocol_stack.html
[2] https://crosscontrol.com/manual/Bluetooth%20Documentation/content/bluetooth.html

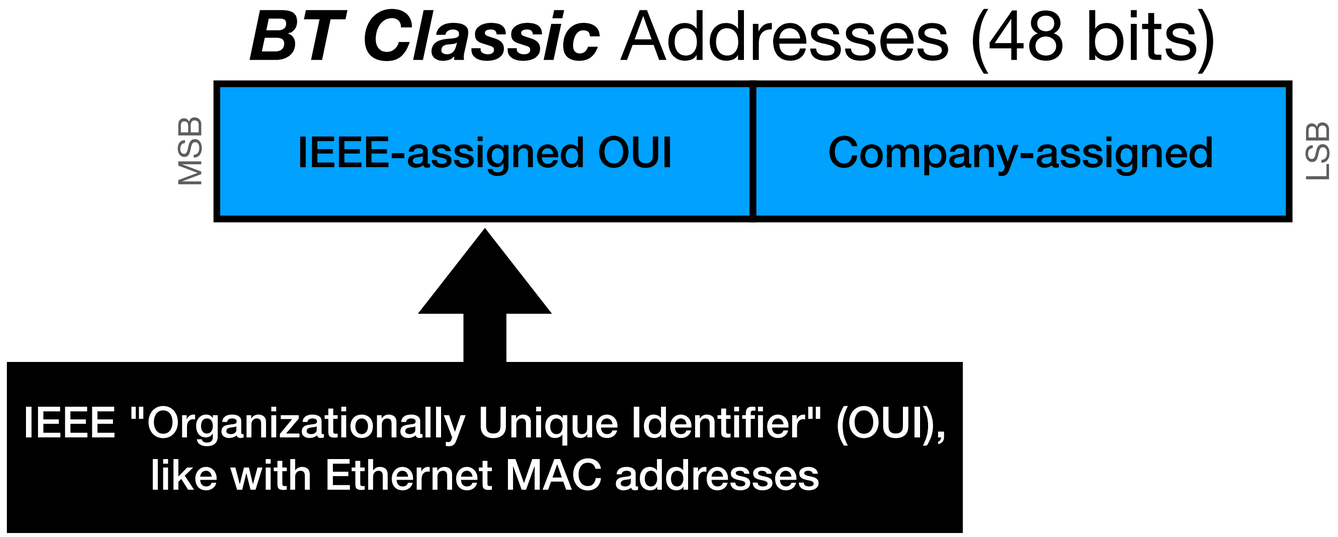
Background - BTC *BT Device Address (BDADDR)*

BT Classic Addresses (48 bits)



https://standards.ieee.org/faqs/regauth

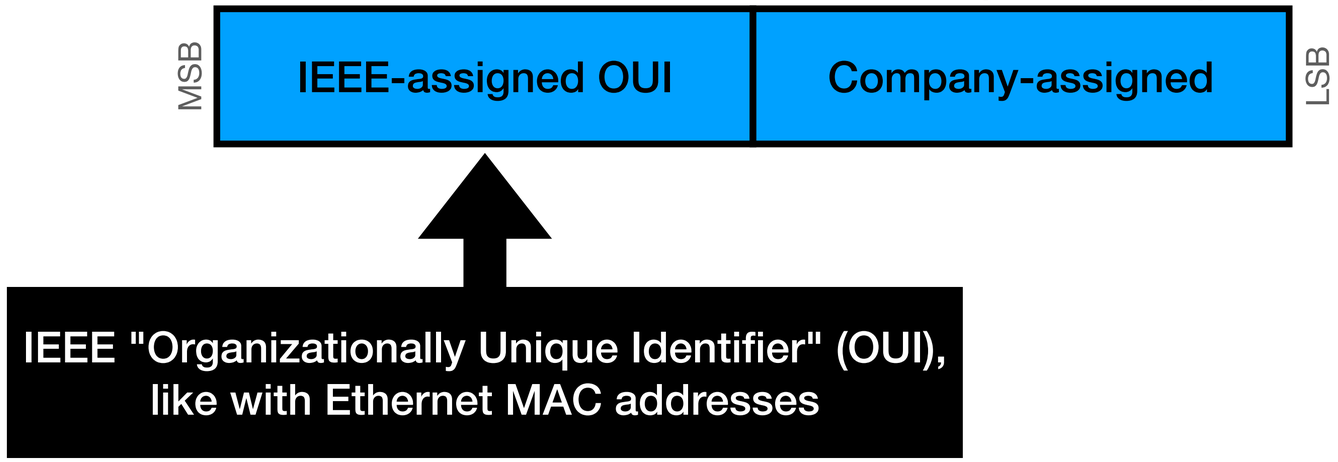
Background - BTC *BT Device Address (BDADDR)*



https://standards.ieee.org/faqs/regauth

Background - BTC *BT Device Address (BDADDR)*

BT Classic Addresses (48 bits)

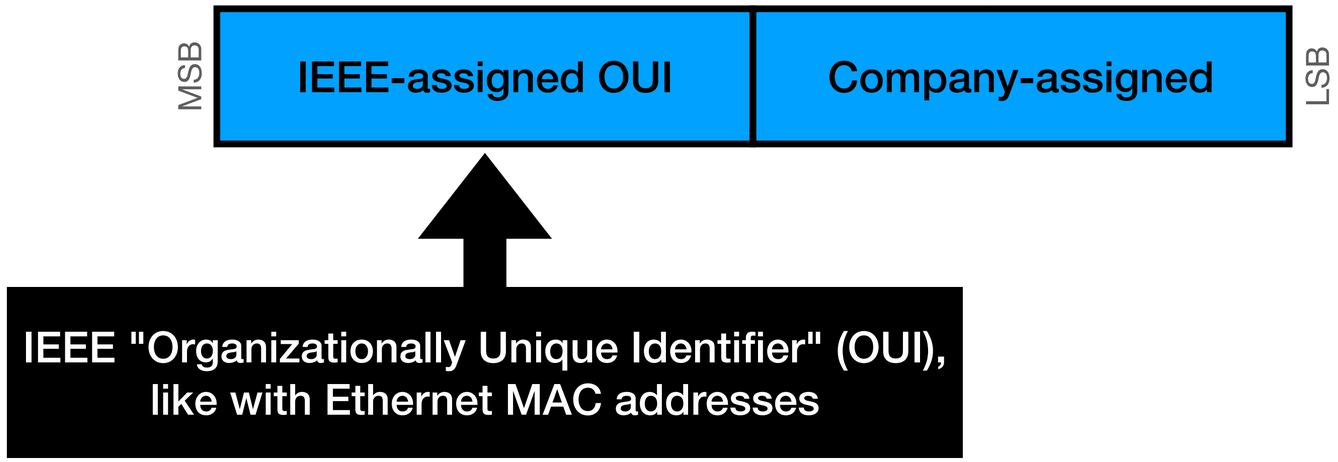


24 bits ("MA-L") - Most common case

https://standards.ieee.org/faqs/regauth

Background - BTC *BT Device Address (BDADDR)*

BT Classic Addresses (48 bits)

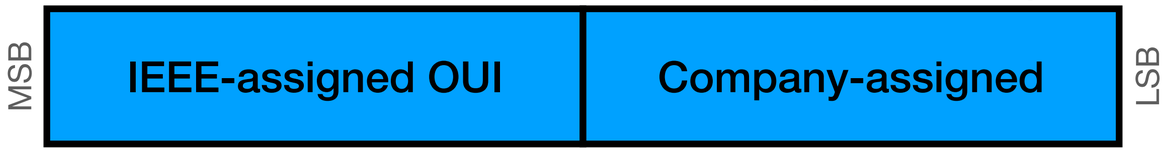


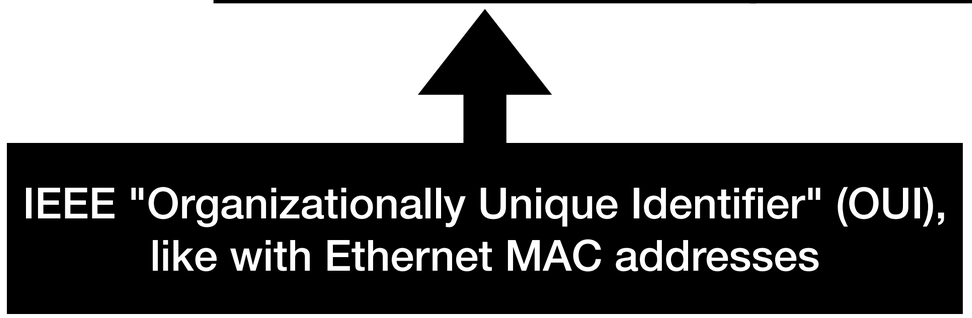
24 bits ("MA-L") - Most common case
20 bits ("MA-M")

https://standards.ieee.org/faqs/regauth

Background - BTC *BT Device Address (BDADDR)*

BT Classic Addresses (48 bits)





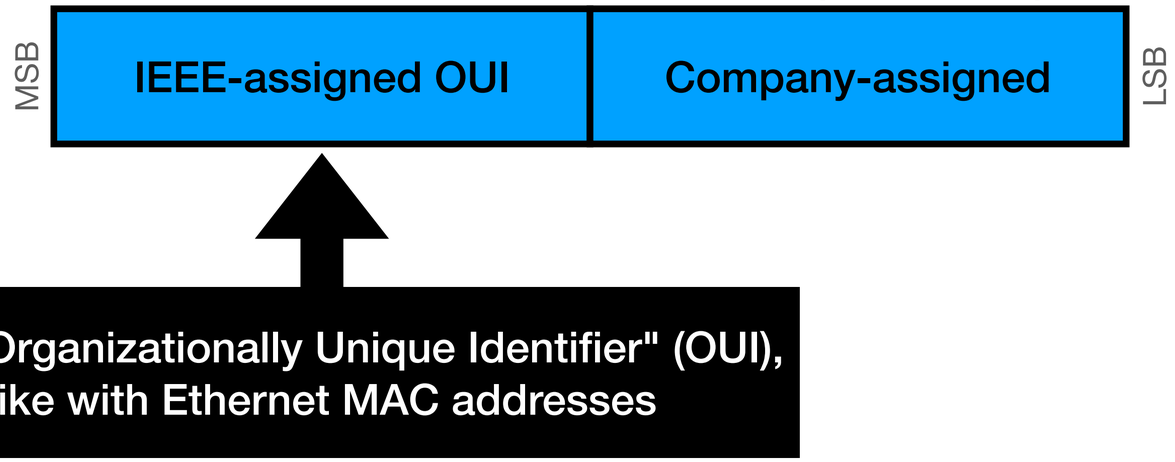
24 bits ("MA-L") - Most common case
20 bits ("MA-M")
12 bits ("MA-S")

https://standards.ieee.org/faqs/regauth

Background - BTC *BT Device Address (BDADDR)*

00:1f:ff:5f:0d:5a

BT Classic Addresses (48 bits)



24 bits ("MA-L") - Most common case
20 bits ("MA-M")
12 bits ("MA-S")

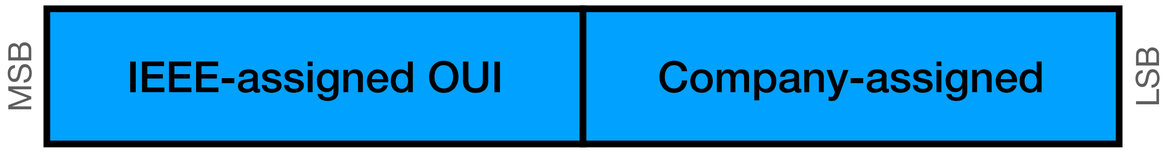
https://standards.ieee.org/faqs/regauth

Background - BTC *BT Device Address (BDADDR)*

(00:1f:ff) == Respironics, Inc.

00:1f:ff:5f:0d:5a

BT Classic Addresses (48 bits)



IEEE "Organizationally Unique Identifier" (OUI), like with Ethernet MAC addresses

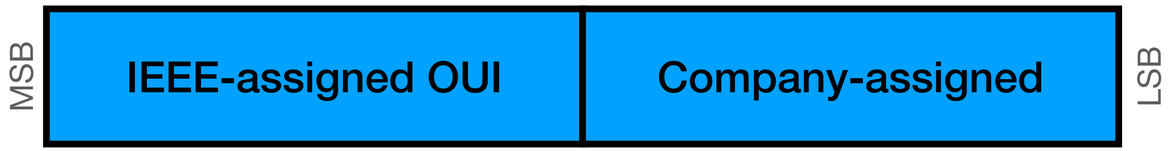
24 bits ("MA-L") - Most common case
20 bits ("MA-M")
12 bits ("MA-S")

https://standards.ieee.org/faqs/regauth

Background - BLE *BT Device Address (BDADDR)*

👋 *There*'s *a bit* in BLE packet headers that says whether a BDADDR is "public" or "random" 👋

BLE Public Addresses (48 bits)

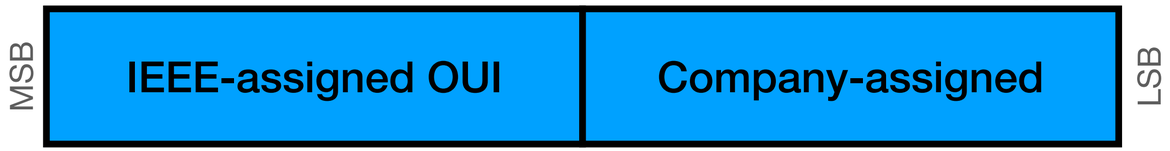


BLE Random Addresses

Background - BLE *BT Device Address (BDADDR)*

👋 *There's a bit* in BLE packet headers that says whether a BDADDR is "public" or "random" 👋

BLE Public Addresses (48 bits)



BLE Random Addresses

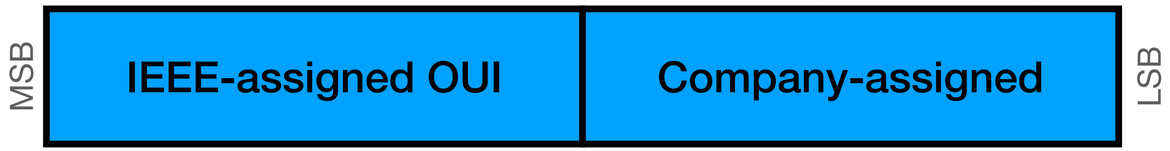
BLE Random

Static (48 bits)

Background - BLE *BT Device Address (BDADDR)*

👋 *There's a bit* in BLE packet headers that says whether a BDADDR is "public" or "random" 👋

BLE Public Addresses (48 bits)

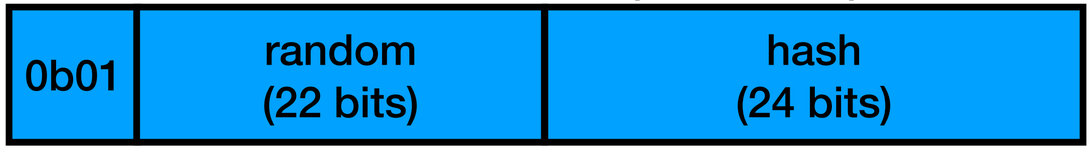


BLE Random Addresses

BLE Random
Static (48 bits)

BLE Random
Private

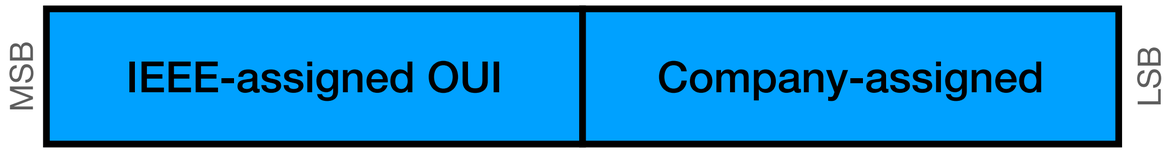
BLE Random Private
Resolvable (48 bits)



Background - BLE *BT Device Address (BDADDR)*

👋 *There's a bit* in BLE packet headers that says whether a BDADDR is "public" or "random" 👋

BLE Public Addresses (48 bits)

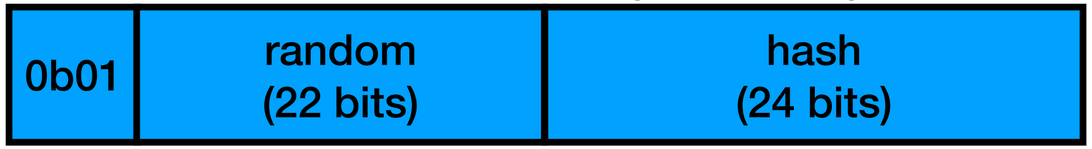


BLE Random Addresses

BLE Random
Static (48 bits)

BLE Random
Private

BLE Random Private
Resolvable (48 bits)



BLE Random Private
Non-resolvable (48 bits)

Random address bit(s)

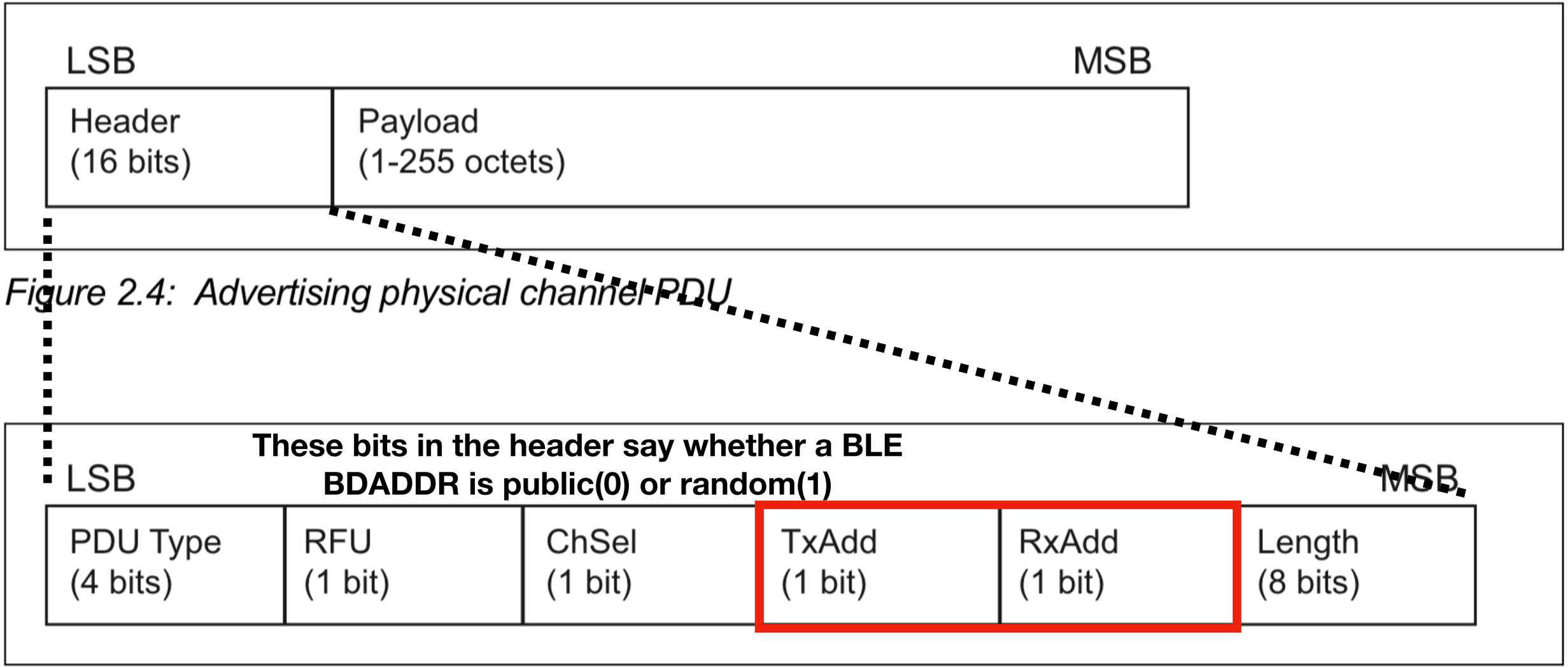


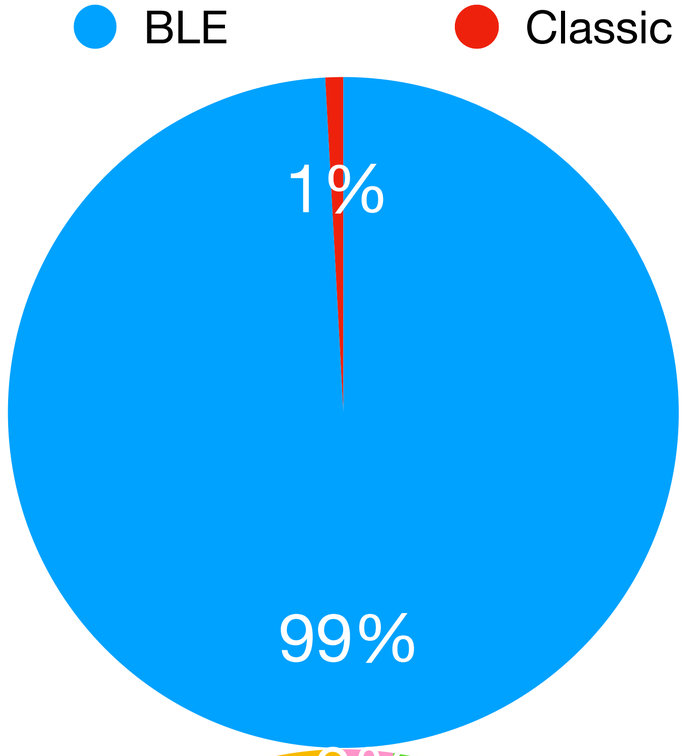
Figure 2.4: Advertising physical channel PDU

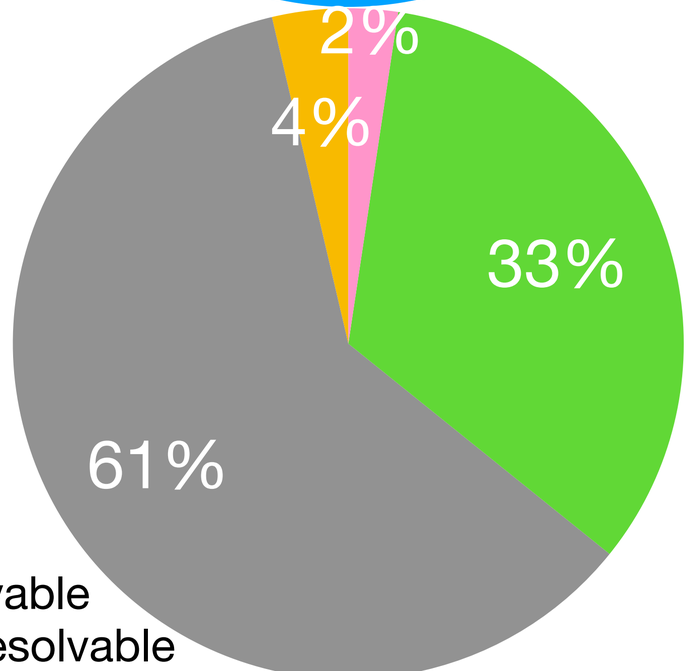
Figure 2.5: Advertising physical channel PDU header

Overall BDADDR Data

IEEE OUI Applicability

- **74,934 *unique* BT Classic BDADDRs**👍
- 8,569,483 *unique* BLE BDADDRs
  - **204,708 "public" BDADDRs**👍
  - ~~2,793,274 "random static" BDADDRs~~
  - ~~5,264,247 "random resolvable" BDADDRs~~
  - ~~307,030 "random non-resolvable" BDADDRs~~
- So OUIPrints applicable to only ~3.2% of the BDADDRs (74,934+ 204,708)/(74,934+8,569,483)





📱 = phone-related, 🚗 = car-related, 🎶 = audio-related, 🍪 = chip-related, 🧩 = module-related

BTC Data (top 20 of 604 companies seen)

	company_by_bdaddr		found
GPS/Watches/etc	Garmin International		10454
📱📺	Samsung Electronics Co.,Ltd	*Qualcomm, Broadcom, MediaTek, Samsung* 🍪	7057
📱	OnePlus Technology (Shenzhen) Co., Ltd		3757
🍪	Actions Semiconductor Co.,Ltd.(Cayman Islands)		3054
📱	Apple, Inc.	*Mostly Broadcom, Sometimes Apple (e.g. AirPods)* 🍪	2697
🎶🚗🧩	Panasonic Automotive Systems Co.,Ltd		2499
🎶🚗🧩	Laird Connectivity		2244
🍪	Intel Corporate		2042
🎶🚗🧩	PIONEER CORPORATION		1992
🚗	ALPSALPINE CO,.LTD		1944
📱	GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP.,LTD		1696
🧩🍪	AzureWave Technology Inc.	*NXP, Cypress, MediaTek* 🍪	1378
🍪	Texas Instruments		995
📱	Wistron Neweb Corporation		932
🧩	silex technology, Inc.	*Qualcomm* 🍪	893
🎶🚗🧩	Shinwa Industries(China) Ltd.	*Qualcomm/CSR, TI, Cypress, Sunplus* 🍪	861
🎶🚗🧩	MITSUMI ELECTRIC CO.,LTD.	*CSR->Qualcomm* 🍪	849
🎶🚗🧩	PARROT SA	*TI* 🍪	749
📱 integrator?	Wingtech Mobile Communications Co., Ltd.	*MediaTek?* 🍪	692
🎶🚗🍪	Sunplus Technology Co., Ltd.		608

📱 = phone-related, 🚗 = car-related, 🎶 = audio-related, 🍪 = chip-related, 🧩 = module-related

BTC Data (top 20 of 604 companies seen)

	company_by_bdaddr		found
GPS/Watches/etc	Garmin International		10454
📱📺	Samsung Electronics Co.,Ltd	*Qualcomm, Broadcom, MediaTek, Samsung* 🍪	7057
📱	OnePlus Technology (Shenzhen) Co., Ltd		3757
🍪	Actions Semiconductor Co.,Ltd.(Cayman Islands)		3054
📱	Apple, Inc.	*Mostly Broadcom, Sometimes Apple (e.g. AirPods)* 🍪	2697
🎶🚗🧩	Panasonic Automotive Systems Co.,Ltd		2499
🎶🚗🧩	Laird Connectivity		2244
🍪	Intel Corporate		
🎶🚗🧩	PIONEER CORPORATION		
🚗	ALPSALPINE CO,.LTD		
📱	GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP.,LTD		1696
🧩🍪	AzureWave Technology Inc.	*NXP, Cypress, MediaTek* 🍪	1378
🍪	Texas Instruments		995
📱	Wistron Neweb Corporation		932
🧩	silex technology, Inc.	*Qualcomm* 🍪	893
🎶🚗🧩	Shinwa Industries(China) Ltd.	*Qualcomm/CSR, TI, Cypress, Sunplus* 🍪	861
🎶🚗🧩	MITSUMI ELECTRIC CO.,LTD.	*CSR->Qualcomm* 🍪	849
🎶🚗🧩	PARROT SA	*TI* 🍪	749
📱 integrator?	Wingtech Mobile Communications Co., Ltd.	*MediaTek?* 🍪	692
🎶🚗🍪	Sunplus Technology Co., Ltd.		608

Note! My data is skewed towards vehicles, because I like to put my sniffers over freeways!

📱 = phone-related, 🚗 = car-related, 🎶 = audio-related, 🍪 = chip-related, 🧩 = module-related

BLE Data (top 20 of 631 companies seen)

	company_by_bdaddr		found	
🍪	Texas Instruments		32252	
🎶	VXi Corporation		25243	
📱🖥️	Samsung Electronics Co.,Ltd	*Qualcomm, Broadcom, MediaTek, Samsung* 🍪	13165	
🎶	Bose Corporation		8584	
🐀⌨️	Logitech, Inc		5031	
🚗	Cambridge Mobile Telematics, Inc.	*CSR->Qualcomm* 🍪	5024	
📱	Apple, Inc.	*Mostly Broadcom, Sometimes Apple (e.g. AirPods)* 🍪	4970	
🍪	Silicon Laboratories		3849	
🍪	Espressif Inc.		3027	
BLE beacons	Shenzhen Minew Technologies Co., Ltd.		2609	
🧩	Murata Manufacturing Co., Ltd.	*Nordic, Cypress, CSR, Onsemi, Dialog* 🍪	2288	
🍪	Telink Semiconductor (Taipei) Co. Ltd.		1965	
🍪🧩 + 🍪?	Shenzhen Jingxun Software Telecommunication Technology Co.,Ltd		1891	*RealTek, Airoha* 🍪
GPS/Watches/etc	Garmin International		1740	
🧩	Sunitec Enterprise Co.,Ltd	*Broadcom* 🍪	1442	
BLE beacons	Aruba, a Hewlett Packard Enterprise Company		1409	
LED lights & sensors	Shenzhen Intellirocks Tech co.,ltd	*Telink* 🍪	1164	
Teslas	Shanghai Rui Rui Communication Technology Co.Ltd.		1073	(TI bought OUI?)
🎶🚗🧩	ALPSALPINE CO,.LTD		979	
🎶 Hearing aids	Starkey Labs Inc.		956	

Of what I want to know

- If the BDADDR maps to a *chip-maker*, we have an idea of what chip maker is being used with high probability

"Texas Instruments"	"Silicon Laboratories"	"Intel Corporate"
"Telink Semiconductor (Taipei) Co. Ltd."	"Cambridge Silicon Radio"	"Espressif Inc."
"Nordic Semiconductor ASA"	"NXP Semiconductors"	"NXP France Semiconductors France"
"NXP Semiconductor (Tianjin) LTD."	"NXP (China) Management Ltd."	"Microchip Technology Inc."
"Broadcom"	"Qualcomm Technologies International, Ltd. (QTIL)"	"REALTEK SEMICONDUCTOR CORP."

- For some other names (like *module-makers*), we might know that there's only 1 or 2 chips they ever use, though of course that can change
  - Need to collect that data over time

The First Traces

Of what I want to know

- If the BDADDR maps to a *chip-maker*, we have an idea of what chip maker is being used with high probability

"Texas Instruments"	"Silicon Laboratories"	"Intel Corporate"
"Telink Semiconductor (Taipei) Co. Ltd."	"Cambridge Silicon Radio"	"Espressif Inc."
"Nordic Semiconductor ASA"	"NXP Semiconductors"	"NXP France Semiconductors France"
"NXP Semiconductor (Tianjin) LTD."	"NXP (China) Management Ltd."	"Microchip Technology Inc."
"Broadcom"	"Qualcomm Technologies International, Ltd. (QTIL)"	"REALTEK SEMICONDUCTOR CORP."

- For some other names (like *module-makers*), we might know that there's only 1 or 2 chips they ever use, though of course that can change
  - Need to collect that data over time

What I Want

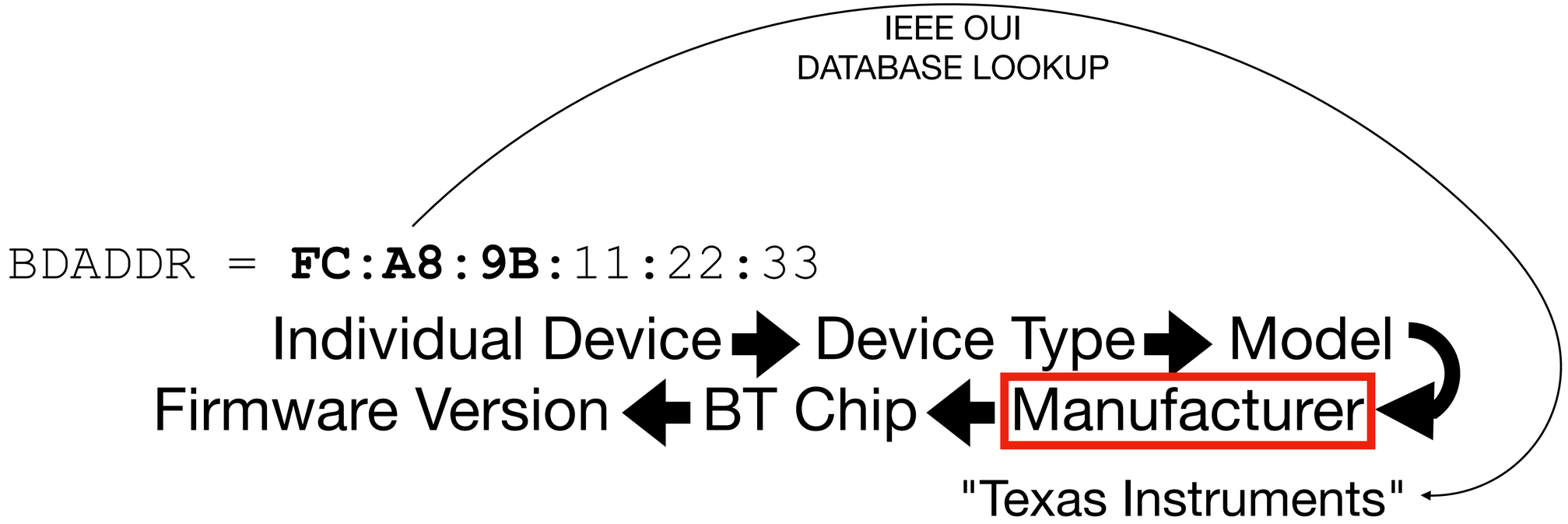
Individual Device → Device Type → Model ↷
Firmware Version ← BT Chip ← Manufacturer

What I Want

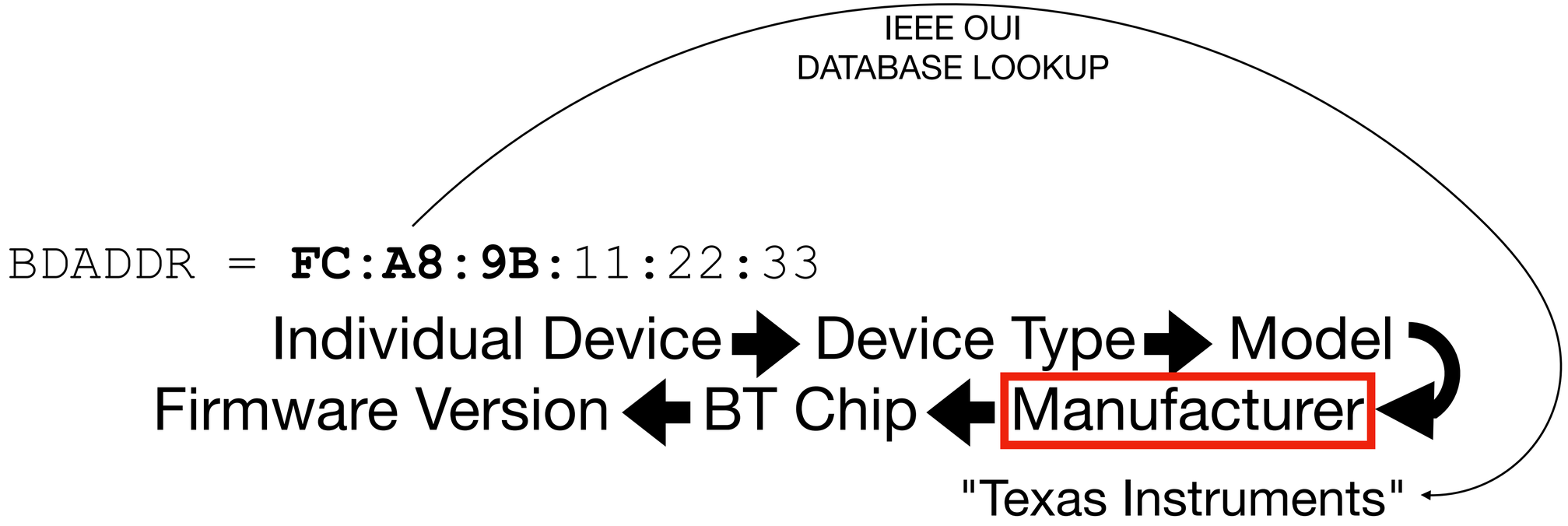
`BDADDR = FC:A8:9B:11:22:33`

Individual Device → Device Type → Model ↷
Firmware Version ← BT Chip ← Manufacturer ↶

What I Want

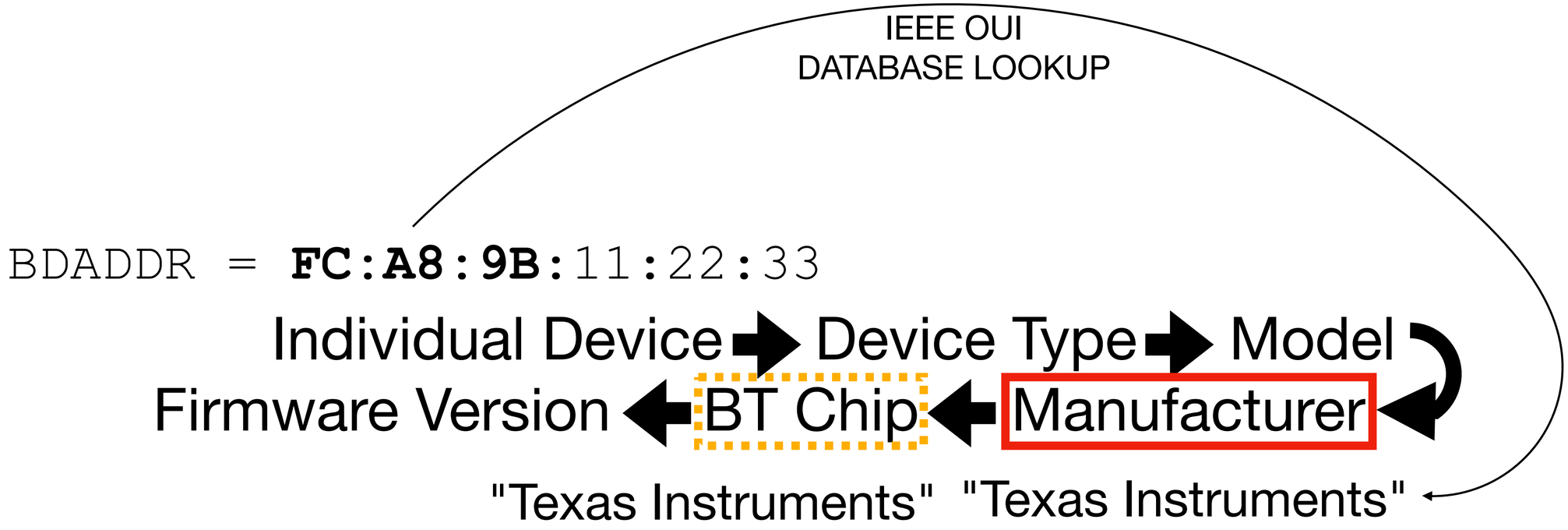

IEEE OUI
DATABASE LOOKUP
BDADDR = FC:A8:9B:11:22:33
Individual Device
Device Type
Model
Firmware Version
BT Chip
Manufacturer
"Texas Instruments"

What I Want



ASSUMPTION:
OUIPrint == ChipPrint, for OUI == {Silicon Vendor OUIs}

What I Want



ASSUMPTION:

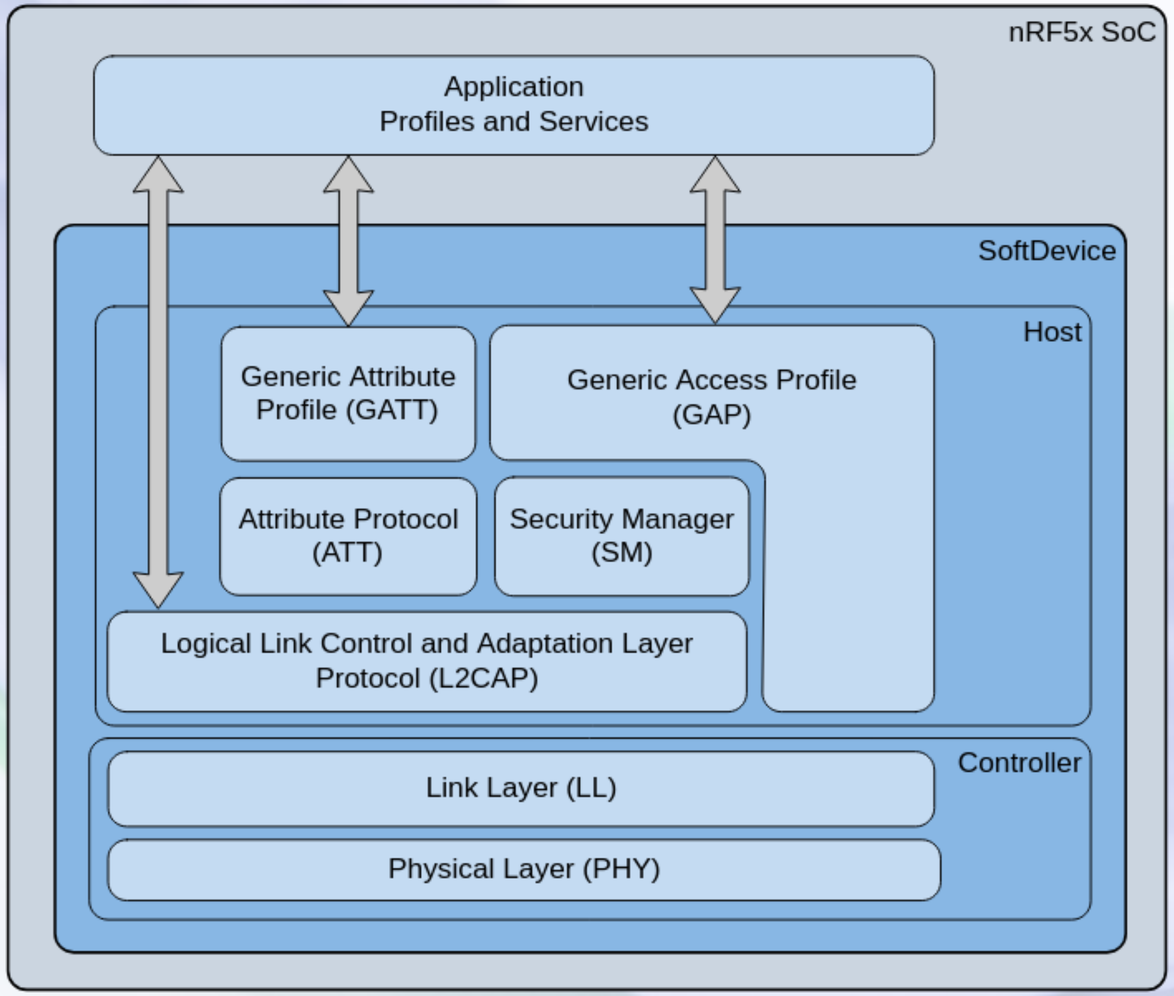
OUIPrint == ChipPrint, for OUI == {Silicon Vendor OUIs}

2thprint by Link Layer Version Info 🚶 or 🤾

2thprint by Link Layer Version Info 🚶 or 🤾

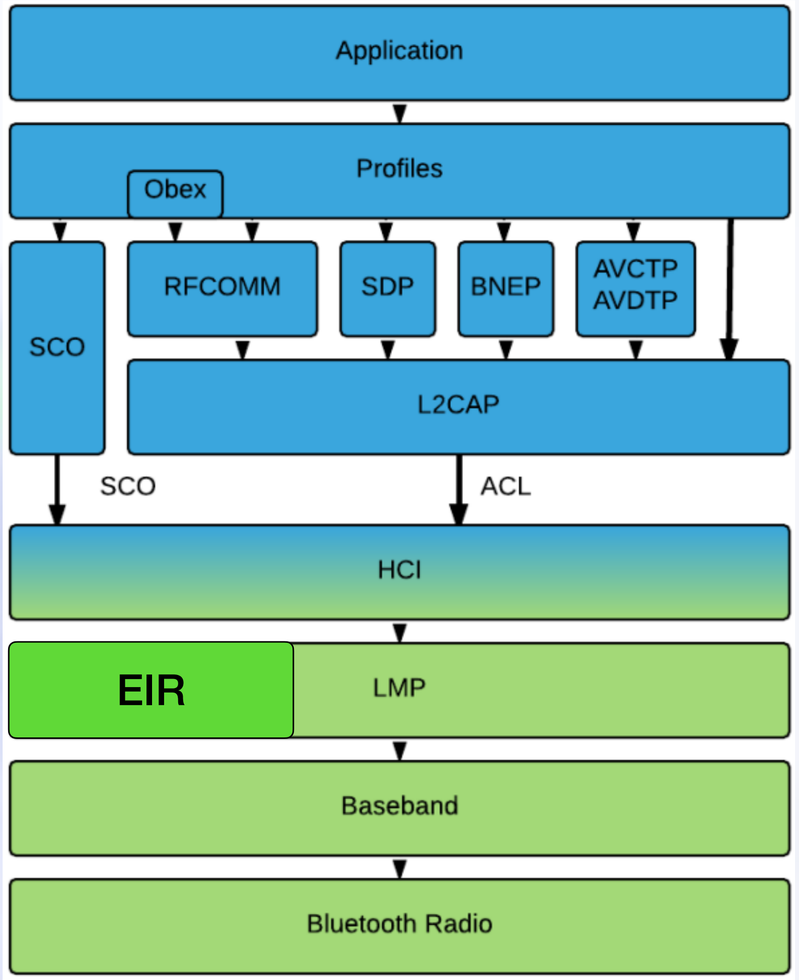
BLE

[1]



BTC

[2]

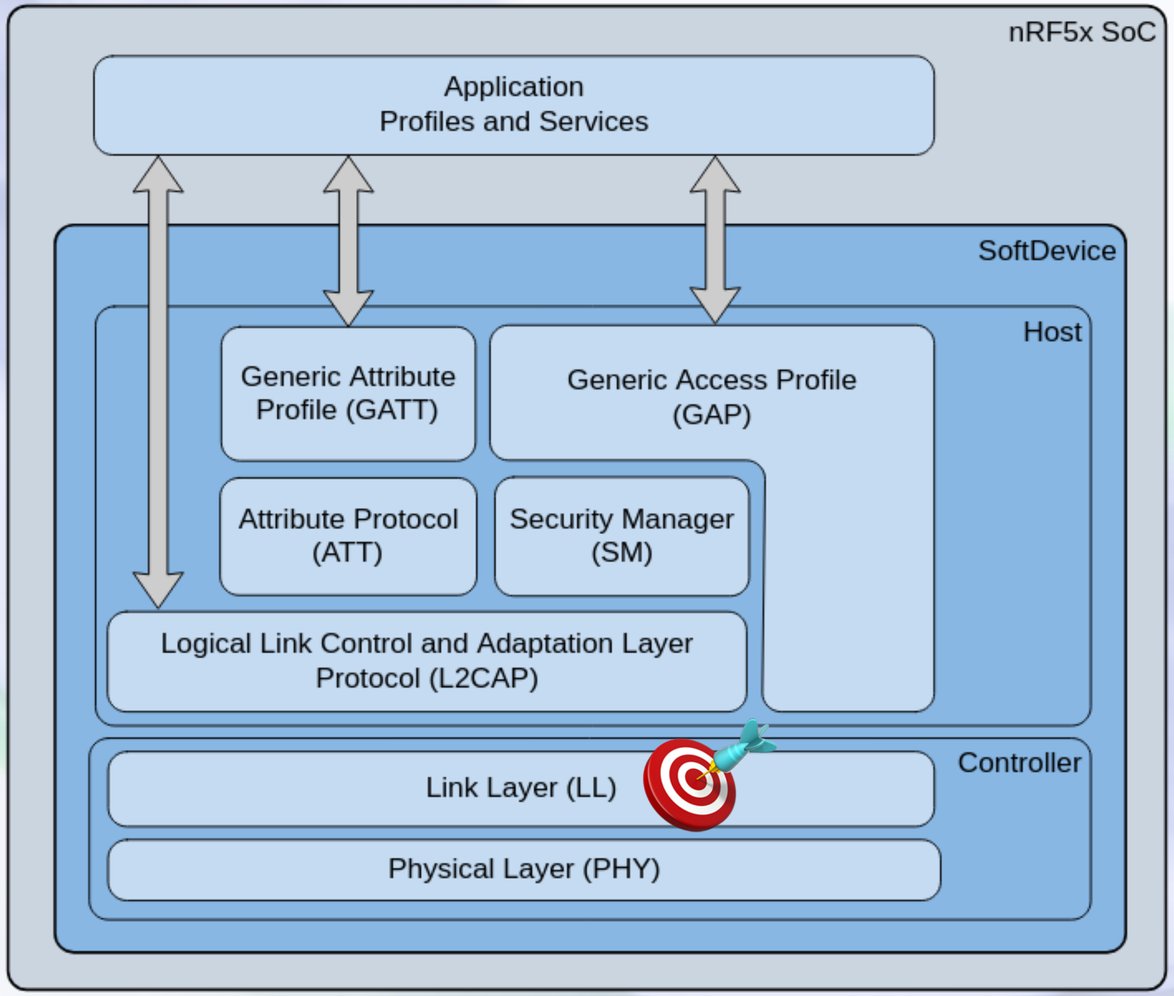


[1] https://infocenter.nordicsemi.com/index.jsp?topic=%2Fsds_s140%2FSDS%2Fs1xx%2Fble_protocol_stack%2Fble_protocol_stack.html
[2] https://crosscontrol.com/manual/Bluetooth%20Documentation/content/bluetooth.html

2thprint by Link Layer Version Info 🚶 or 🤾

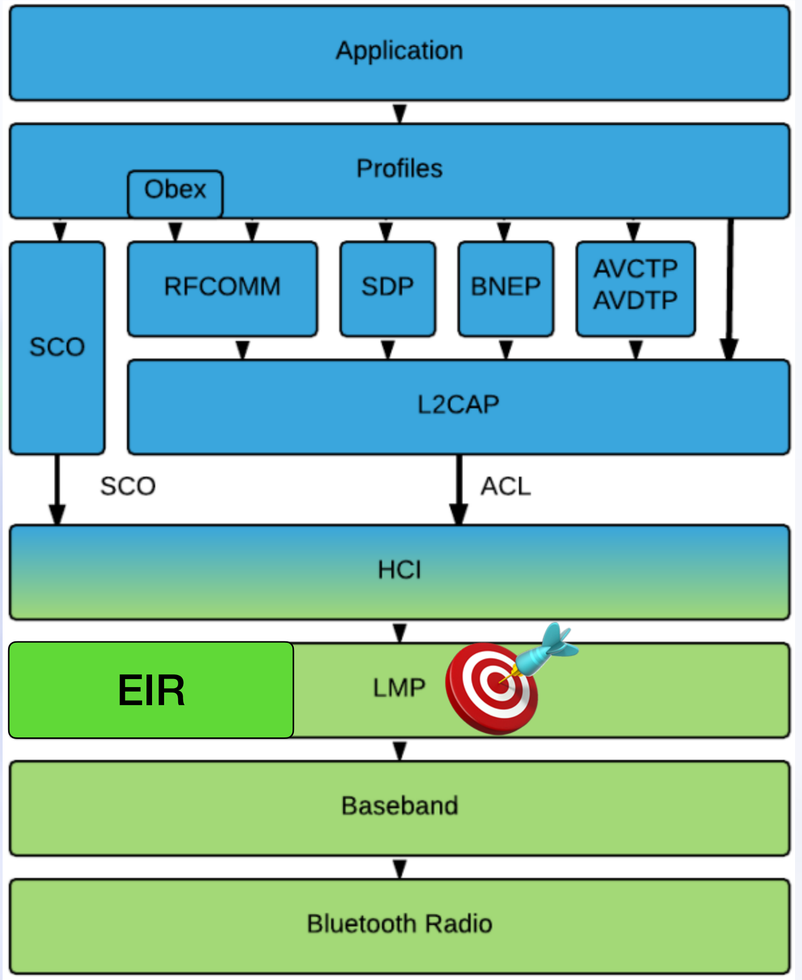
BLE

[1]



BTC

[2]

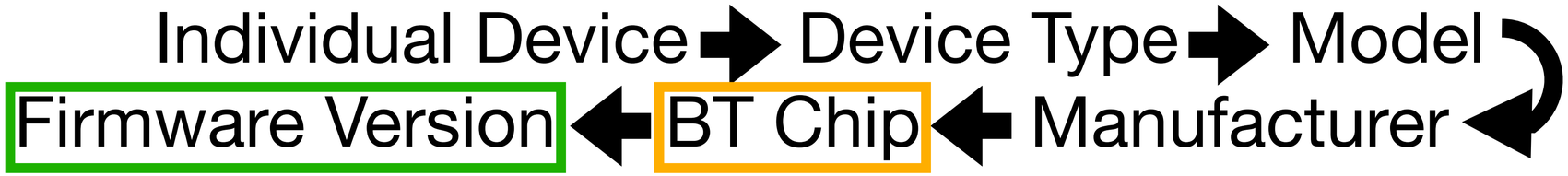


[1] https://infocenter.nordicsemi.com/index.jsp?topic=%2Fsds_s140%2FSDS%2Fs1xx%2Fble_protocol_stack%2Fble_protocol_stack.html
[2] https://crosscontrol.com/manual/Bluetooth%20Documentation/content/bluetooth.html

2thprint by Link Layer Version Information

LL_VERSION_IND (BLE), LMP_version_res (BTC)

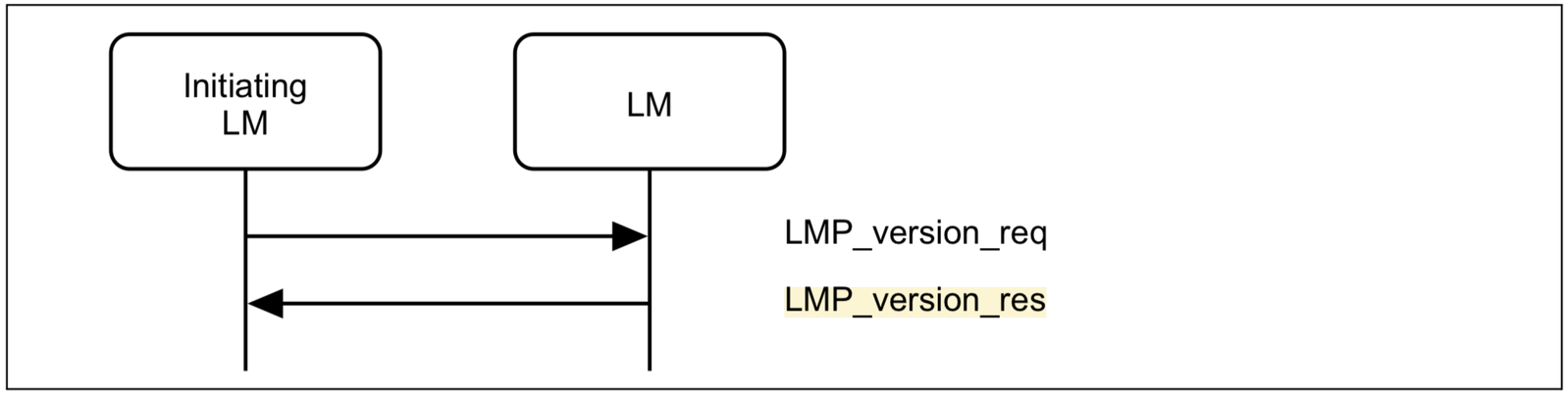
- BTC has Link Management Protocol (LMP) and BLE has Link-Layer (LL) Control packets, that can be sent to request some chip and firmware version information
- These can be sent/received *without* any sort of BT pairing/bonding!



2thprint by
LMP_version_res (BTC)

M/O	PDU	Contents
M	LMP_version_req	VersNr CompId SubVersNr
M	LMP_version_res	VersNr CompId SubVersNr

Table 4.26: PDUs used for LMP version request



Sequence 77: Request for LMP version

From BT
Core Spec v4.2

2thprint by
LL_VERSION_IND (BLE)

2.4.2.13 LL_VERSION_IND

The format of the CtrData field is shown in Figure 2.23.

CtrData		
VersNr (1 octet)	CompId (2 octets)	SubVersNr (2 octets)

Figure 2.23: CtrData field of the LL_VERSION_IND PDU

The LL_VERSION_IND CtrData consists of three fields:

- VersNr field shall contain the version of the Bluetooth Controller specification (see Bluetooth Assigned Numbers).
- CompId field shall contain the company identifier of the manufacturer of the Bluetooth Controller (see Bluetooth Assigned Numbers).
- SubVersNr field shall contain a unique value for each implementation or revision of an implementation of the Bluetooth Controller.

From BT
Core Spec v4.2

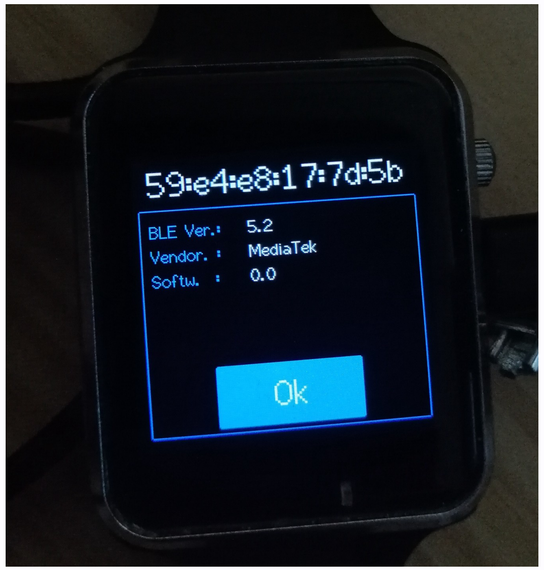
Prior Work

"ESPwn32: Hacking with ESP32 System-on-Chips"

- Oh no! I got scooped! (Or did I?)
- [1] by Cayre et al. from May 2023 recognized that LL_VERSION_IND packets contains useful information
- But it subsequently *assumes* this information is *sufficient* for vulnerability applicability assessment, without offering any proof / data analysis

Remote BLE stack fingerprinting !

EURECOM Quarkslab



[1] https://wootconference.org/papers/woot23-paper22.pdf

Prior Work

"ESPwn32: Hacking with ESP32 System-on-Chips"

- Oh no! I got scooped! (Or did I?)
- [1] by Cayre et al. from May 2023 recognized that LL_VERSION_IND packets contains useful information
- But it subsequently *assumes* this information is *sufficient* for vulnerability applicability assessment, without offering any proof / data analysis

[1] https://wootconference.org/papers/woot23-paper22.pdf

LMP/LL 2thprints useful, but not definitive

- It turns out that for MediaTek (CID = 70), the most common value for the sub version is 0

device_BT_CID	lmp_sub_version	frequency
70	0	774
70	288	189
70	4648	86
70	4101	62
70	2051	15
70	1571	14
70	613	11
70	533	10
70	2344	10
70	1030	9
70	4391	8
70	1797	7
70	4135	5
70	304	4
70	726	4
70	791	4
70	1560	4
70	1817	4

...

device_BT_CID	ll_sub_version	frequency
70	0	36
70	534	8
70	4101	8
70	4648	6
70	2051	5
70	4355	3
70	4373	2
70	288	1
70	304	1
70	546	1
70	776	1
70	791	1
70	1033	1
70	1042	1
70	1045	1
70	1568	1
70	4097	1
70	4116	1

LMP/LL 2thprints useful, but not definitive

- It turns out that for MediaTek (CID = 70), the most common value for the sub version is 0

device_BT_CID	lmp_sub_version	frequency
70	0	774
70	288	189
70	4648	86
70	4101	62
70	2051	15
70	1571	14
70	613	11
70	533	10
70	2344	10
70	1030	9
70	4391	8
70	1797	7
70	4135	5
70	304	4
70	726	4
70	791	4
70	1560	4
70	1817	4

...

device_BT_CID	ll_sub_version	frequency
70	0	36
70	534	8
70	4101	8
70	4648	6
70	2051	5
70	4355	3
70	4373	2
70	288	1
70	304	1
70	546	1
70	776	1
70	791	1
70	1033	1
70	1042	1
70	1045	1
70	1568	1
70	4097	1
70	4116	1

LMP/LL 2thprints useful, but not definitive

- It turns out that for MediaTek (CID = 70), the most common value for the sub version is 0

device_BT_CID	lmp_sub_version	frequency
70	0	774
70	288	189
70	4648	86
70	4101	62
70	2051	15
70	1571	14
70	613	11
70	533	10
70	2344	10
70	1030	9
70	4391	8
70	1797	7
70	4135	5
70	304	4
70	726	4
70	791	4
70	1560	4
70	1817	4

...

device_BT_CID	ll_sub_version	frequency
70	0	36
70	534	8
70	4101	8
70	4648	6
70	2051	5
70	4355	3
70	4373	2
70	288	1
70	304	1
70	546	1
70	776	1
70	791	1
70	1033	1
70	1042	1
70	1045	1
70	1568	1
70	4097	1
70	4116	1

OnePlus Pad

Halo Green | 8 GB RAM + 128 GB Storage

CA$649.99

Color: Halo Green

ROM

8 GB RAM + 128 GB Storage

...but not definitive

...most common value for the sub

device_BT_CID	ll_sub_version	frequency
70	0	36
70	534	8
70	4101	8
70	4648	6
70	2051	5
70	4355	3
70	4373	2
70	288	1
70	304	1
70	546	1
70	776	1
70	791	1
70	1033	1
70	1042	1
70	1045	1
70	1568	1
70	4097	1
70	4116	1

70	4101	62
70	2051	15
70	1571	14
70	613	11
70	533	10
70	2344	10
70	1030	9
70	4391	8
70	1797	7
70	4135	5
70	304	4
70	726	4
70	791	4
70	1560	4
70	1817	4

...

OnePlus Pad

Halo Green | 8 GB RAM + 128 GB Storage

CA$649.99

Color: Halo Green

ROM

8 GB RAM + 128 GB Storage

OnePlus Trade-In Open for Every

70	4101	62
70	2051	15
70	1571	14
70	613	11
70	533	10
70	2344	10
70	1030	9
70	4391	8
70	1797	7
70	4135	5
70	304	4
70	726	4
70	791	4
70	1560	4
70	1817	4

...

OnePlus Pad

Halo Green | 8 GB RAM + 128 GB Storage

CA$649.99

Color: Halo Green

ROM

8 GB RAM + 128 GB Storage

62
15
14
11
10
10
9
8
7
5
4
4
4
4
4

OnePlus Pad

Halo Green | 8 GB RAM + 128 GB Storage

CA$649.99

Color: Halo Green

ROM

8 GB RAM + 128 GB Storage

OnePlus Trade-In Open for Every

62
15
14
11
10
10
9
8
7
5
4
4
4
4
4

(Link Layer) Version Number

VersNr (1 byte)

CtrData		
VersNr (1 octet)	CompId (2 octets)	SubVersNr (2 octets)

Figure 2.[illegible]: CtrData field of the LL_VERSION_IND PDU

Last Modified: 2023-02-21

Core Specification Name	Version
Bluetooth® Core Specification 1.0b (Withdrawn)	0x00
Bluetooth® Core Specification 1.1 (Withdrawn)	0x01
Bluetooth® Core Specification 1.2 (Withdrawn)	0x02
Bluetooth® Core Specification 2.0+EDR (Withdrawn)	0x03
Bluetooth® Core Specification 2.1+EDR (Withdrawn)	0x04
Bluetooth® Core Specification 3.0+HS (Withdrawn)	0x05
Bluetooth® Core Specification 4.0 (Withdrawn)	0x06
Bluetooth® Core Specification 4.1 (Deprecated)	0x07
Bluetooth® Core Specification 4.2	0x08
Bluetooth® Core Specification 5.0	0x09
Bluetooth® Core Specification 5.1	0x0A
Bluetooth® Core Specification 5.2	0x0B
Bluetooth® Core Specification 5.3	0x0C
Bluetooth® Core Specification 5.4	0x0D

From BT
Assigned Numbers document

(Link Layer) Company Identifier

CompId (2 bytes) - 3330 defined at time of writing

CtrData		
VersNr (1 octet)	CompId (2 octets)	SubVersNr (2 octets)

Figure 2.23: CtrData field of the LL_VERSION_IND PDU

```
company_identifiers:

  - value: 0x0CA5
    name: 'Princess Cruise Lines, Ltd.'

  - value: 0x0CA4
    name: 'MITSUBISHI ELECTRIC LIGHTING CO, LTD'

  - value: 0x0CA3
    name: 'MAQUET GmbH'

  - value: 0x0CA2
    name: 'XSENSE LTD'

  - value: 0x0CA1
    name: 'YAMAHA MOTOR CO.,LTD.'

  - value: 0x0CA0
    name: 'BIGBEN'

  - value: 0x0C9F
    name: 'Dragonfly Energy Corp.'

  - value: 0x0C9E
```

From htt

```
  name: 'H+B Hightech GmbH'

- value: 0x0C95
  name: 'Gemstone Lights Canada Ltd.'

- value: 0x0C94
  name: 'Baxter Healthcare Corporation'

- value: 0x0C93
  name: 'Movesense Oy'

- value: 0x0C92
  name: 'Kesseböhmer Ergonomietechnik GmbH'

- value: 0x0C91
  name: 'Yashu Systems'

- value: 0x0C90
  name: 'WESCO AG'

- value: 0x0C8F
  name: 'Radar Automobile Sales(Shandong)Co.,Ltd.'

- value: 0x0C8E
  name: 'Technocon Engineering Ltd.'

- value: 0x0C8D
  name: 'tonies GmbH'

- value: 0x0C8C
  name: 'T-Mobile USA'
```

From https://bitbucket.org/bluetooth-SIG/public/src/main/company_identifiers/company_identifiers.yaml, updated very frequently!

CtrData		
VersNr (1 octet)	CompId (2 octets)	SubVersNr (2 octets)

Figure 2.23: CtrData field of the LL_VERSION_IND PDU

(Link Layer) Company Identifier

CompId (2 bytes) - 3330 defined at time of writing

```
company_identifiers:

  - value: 0x0CA5
    name: 'Princess Cruise Lines, Ltd.'

  - value: 0x0CA4
    name: 'MITSUBISHI ELECTRIC LIGHTING CO, LTD'

  - value: 0x0CA3
    name: 'MAQUET GmbH'

  - value: 0x0CA2
    name: 'XSENSE LTD'

  - value: 0x0CA1
    name: 'YAMAHA MOTOR CO.,LTD.'

  - value: 0x0CA0
    name: 'BIGBEN'

  - value: 0x0C9F
    name: 'Dragonfly Energy Corp.'

  - value: 0x0C9E
```

From htt y!

(Link Layer) Company Identifier

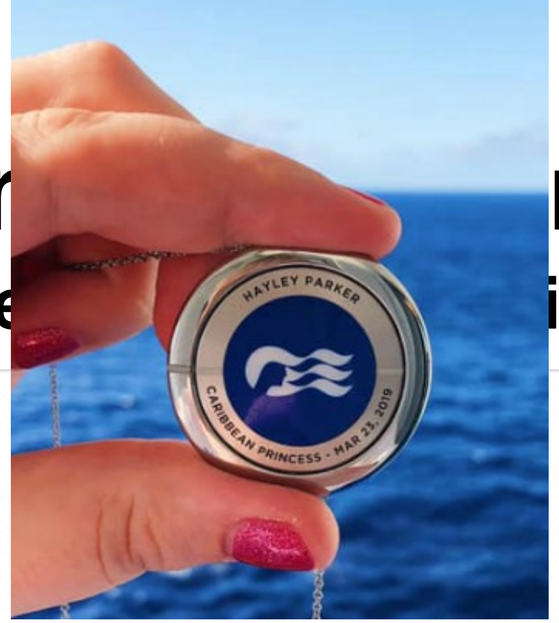
CompId (2 bytes) - 3330 defined at time of writing

```
company_identifiers:

- value: 0x0CA5
  name: 'Princess Cruise Lines, Ltd.'

- value: 0x0CA4
  name: 'MITSUBISHI ELECTRIC LIGHTING CO, LTD'

- value: 0x0CA3
  name: 'MAQUET GmbH'

- value: 0x0CA2
  name: 'XSENSE LTD'

- value: 0x0CA1
  name: 'YAMAHA MOTOR CO.,LTD.'

- value: 0x0CA0
  name: 'BIGBEN'

- value: 0x0C9F
  name: 'Dragonfly Energy Corp.'

- value: 0x0C9E
```

From htt y!

(Link Layer) Compar r

CompId (2 bytes) - 3330 define iting

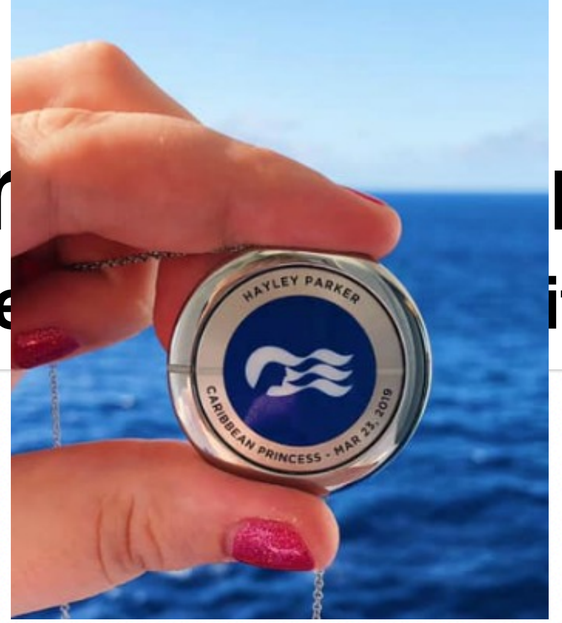



```
company_identifiers:

  - value: 0x0CA5
    name: 'Princess Cruise Lines, Ltd.'

  - value: 0x0CA4
    name: 'MITSUBISHI ELECTRIC LIGHTING CO, LTD'

  - value: 0x0CA3
    name: 'MAQUET GmbH'

  - value: 0x0CA2
    name: 'XSENSE LTD'

  - value: 0x0CA1
    name: 'YAMAHA MOTOR CO.,LTD.'

  - value: 0x0CA0
    name: 'BIGBEN'

  - value: 0x0C9F
    name: 'Dragonfly Energy Corp.'

  - value: 0x0C9E
```

From htt y!

(Link Layer) Compar r

CompId (2 bytes) - 3330 define iting



Top Side of PCB View

```
company_identifiers:

  - value: 0x0CA5
    name: 'Princess Cruise Lines, Ltd.'

  - value: 0x0CA4
    name: 'MITSUBISHI ELECTRIC LIGHTING CO, LTD'

  - value: 0x0CA3
    name: 'MAQUET GmbH'

  - value: 0x0CA2
    name: 'XSENSE LTD'

  - value: 0x0CA1
    name: 'YAMAHA MOTOR CO.,LTD.'

  - value: 0x0CA0
    name: 'BIGBEN'

  - value: 0x0C9F
    name: 'Dragonfly Energy Corp.'

  - value: 0x0C9E
```

From htt y!

(Link Layer) Compar r

CompId (2 bytes) - 3330 define iting

`company_identifiers:`

Hands Full? No Problem

You walk along the corridor and voila! Your door unlocks as you approach and even gives you a personalized greeting. You'll enjoy keyless entry with automatic door locks every time you enter your stateroom.

(Link Layer) Compar r

CompId (2 bytes) - 3330 define iting

`company_identifiers:`

Hands Full? No Problem

You walk along the corridor and voila! Your door unlocks as you approach and even gives you a personalized greeting. You'll enjoy keyless entry with automatic door locks every time you enter your stateroom.

https://hardwear.io/netherlands-2022/speakers/sultan-khan.php

(Link Layer) Compar r

CompId (2 bytes) - 3330 define iting

`company_identifiers:`

Hands Full? No Problem

You walk along the corridor and voila! Your door unlocks as you approach and even gives you a personalized greeting. You'll enjoy keyless entry with automatic door locks every time you enter your stateroom.

https://hardwear.io/netherlands-2022/speakers/sultan-khan.php

Vendor Prevalence

BLE - 2024-01-12

- In general though this seems to have a higher prevalence of silicon makers than other BT company/vendor ID fields, so a better S/N ratio for what I want to know
- I have only seen ~ 11466 / 92854 (12.3%) success in my LL 2thprint log
  - Future work will take RSSI into account

CtrData		
VersNr (1 octet)	CompId (2 octets)	SubVersNr (2 octets)

Figure 2.23: CtrData field of the LL_VERSION_IND PDU

comp_by_CompId	count
Broadcom Corporation	8108
Apple, Inc.	1466
Nordic Semiconductor ASA	163
Qualcomm Technologies International, Ltd. (QTIL)	121
MediaTek, Inc.	119
Qualcomm	114
Cypress Semiconductor	85
Texas Instruments Inc.	83
Samsung Electronics Co. Ltd.	60
Dialog Semiconductor B.V.	41
RivieraWaves S.A.S	32
Telink Semiconductor Co. Ltd	29
Bestechnic(Shanghai),Ltd	28
Realtek Semiconductor Corporation	28
ST Microelectronics	26
Marvell Technology Group Ltd.	19
Casambi Technologies Oy	15
Zhuhai Jieli technology Co.,Ltd	15
Airoha Technology Corp.	14
Silicon Laboratories	13
Ambiq	11
Atheros Communications, Inc.	10
Universal Electronics, Inc.	8
Shenzhen Goodix Technology Co., Ltd	6

Vendor Prevalence

BLE - 2024-01-12

- In general though this seems to have a higher prevalence of silicon makers than other BT company/vendor ID fields, so a better S/N ratio for what I want to know
- I have only seen ~ 11466 / 92854 (12.3%) success in my LL 2thprint log
  - Future work will take RSSI into account

comp_by_CompId	count
Broadcom Corporation	8108
Apple, Inc.	1466
Nordic Semiconductor ASA	163
Qualcomm Technologies International, Ltd. (QTIL)	121
MediaTek, Inc.	119
Qualcomm	114
Cypress Semiconductor	85
Texas Instruments Inc.	83
Samsung Electronics Co. Ltd.	60
Dialog Semiconductor B.V.	41
RivieraWaves S.A.S	32
Telink Semiconductor Co. Ltd	29
Bestechnic(Shanghai),Ltd	28
Realtek Semiconductor Corporation	28
ST Microelectronics	26
Marvell Technology Group Ltd.	19
Casambi Technologies Oy	15
Zhuhai Jieli technology Co.,Ltd	15
Airoha Technology Corp.	14
Silicon Laboratories	13
Ambiq	11
Atheros Communications, Inc.	10
Universal Electronics, Inc.	8
Shenzhen Goodix Technology Co., Ltd	6
Yichip Microelectronics (Hangzhou) Co.,Ltd.	5
UNKNOWN_COMP_BY_BT_CID	5
beken	5
Actions (Zhuhai) Technology Co., Limited	5
PHYPLUS Inc	4
Intel Corp.	4
Toshiba Corp.	3
Shanghai wuqi microelectronics Co.,Ltd	2
Barrot Technology Co.,Ltd.	2
Hong Kong HunterSun Electronic Limited	2
WuXi Vimicro	2
NXP B.V.	2
Ingchips Technology Co., Ltd.	2
LAPIS Semiconductor Co.,Ltd	2
Bluetrum Technology Co.,Ltd	2
ON Semiconductor	1
MindTree Ltd.	1

Vendor Prevalence

BTC - 2024-01-12

- In general though this seems to have a higher prevalence of silicon makers than other BT company/vendor ID fields, so a better S/N ratio for what I want to know
- I have only seen ~ 7916 / 25125 (31.5%) success in my LMP 2thprint log
  - Future work will take RSSI into account

CtrData		
VersNr (1 octet)	CompId (2 octets)	SubVersNr (2 octets)

Figure 2.23: CtrData field of the LL_VERSION_IND PDU

comp_by_CompId	count
Qualcomm	35
MediaTek, Inc.	26
Broadcom Corporation	25
Intel Corp.	8
Qualcomm Technologies International, Ltd. (QTIL)	7
Zhuhai Jieli technology Co.,Ltd	7
Realtek Semiconductor Corporation	6
Cypress Semiconductor	3
Marvell Technology Group Ltd.	2
Samsung Electronics Co. Ltd.	2
RivieraWaves S.A.S	2
Bluegiga	1
Equinux AG	1
G-wearables inc.	1
Anova Applied Electronics	1
Toshiba Corp.	1
Texas Instruments Inc.	1
Lumens For Less, Inc	1
Nokia Mobile Phones	1
Actions (Zhuhai) Technology Co., Limited	1
Shenzhen Feasycom Technology Co., Ltd.	1

Vendor Prevalence

BTC - 2024-01-12

CtrData		
VersNr (1 octet)	CompId (2 octets)	SubVersNr (2 octets)

Figure 2.23: CtrData field of the LL_VERSION_IND PDU

- In general though this seems to have a higher prevalence of silicon makers than other BT company/vendor ID fields, so a better S/N ratio for what I want to know
- I have only seen ~ 7916 / 25125 (31.5%) success in my LMP 2thprint log
  - Future work will take RSSI into account

Bitflip!

comp_by_CompId	count
Qualcomm	35
MediaTek, Inc.	26
Broadcom Corporation	25
Intel Corp.	8
Qualcomm Technologies International, Ltd. (QTIL)	7
Zhuhai Jieli technology Co.,Ltd	7
Realtek Semiconductor Corporation	6
Cypress Semiconductor	3
Marvell Technology Group Ltd.	2
Samsung Electronics Co. Ltd.	2
RivieraWaves S.A.S	2
Bluegiga	1
Equinux AG	1
G-wearables inc.	1
Anova Applied Electronics	1
Toshiba Corp.	1
Texas Instruments Inc.	1
Lumens For Less, Inc	1
Nokia Mobile Phones	1
Actions (Zhuhai) Technology Co., Limited	1
Shenzhen Feasycom Technology Co., Ltd.	1

device_bdaddr	comp_by_bdaddr	VersNr	SubVersNr	CompId	comp_by_CompId	device_name
FE:86:B6:4F:FC:0D	UNKNOWN_COMP_BY_BDADDR	8	3120	5D0	Anova Applied Electronics	BT201-AUDIO
70:09:71:69:80:D1	Samsung Electronics Co.,Ltd	9	1005	47	Bluegiga	[TV] Samsung TU7000 50 TV
10:2C:6B:91:A8:F5	AMPAK Technology, Inc.	A	2306	F	Broadcom Corporation	Stream TV
10:2C:6B:99:75:63	AMPAK Technology, Inc.	A	6B06	F	Broadcom Corporation	Living Room
14:7D:DA:0F:66:E8	Apple, Inc.	9	4406	F	Broadcom Corporation	mbp
C0:97:27:1C:2C:6B	SAMSUNG ELECTRO-MECHANICS(THAILAND)	7	2304	F	Broadcom Corporation	[TV] Samsung 8 Series (65)
F8:04:2E:81:2F:33	SAMSUNG ELECTRO-MECHANICS(THAILAND)	7	2304	F	Broadcom Corporation	[TV] UN55JU650D
84:A4:66:BA:96:6D	Samsung Electronics Co.,Ltd	6	410E	F	Broadcom Corporation	[TV]Samsung LED55
6C:56:97:31:8E:DA	Amazon Technologies Inc.	8	2304	131	Cypress Semiconductor	Echo Show-2N2
2C:33:61:E6:E2:07	Apple, Inc.	B	240C	131	Cypress Semiconductor	apple’s Keyboard
2C:33:61:E6:E2:07	Apple, Inc.	B	240C	131	Cypress Semiconductor	wkeybd_KPAL
FE:86:B6:4F:FC:0D	UNKNOWN_COMP_BY_BDADDR	8	3120	1D6	G-wearables inc.	BT201-AUDIO
AC:67:5D:CA:0A:8E	Intel Corporate	9	100	2	Intel Corp.	EXPCQ6092
C8:B2:9B:B0:25:83	Intel Corporate	B	216E	2	Intel Corp.	DESKTOP-EC66KUJ
00:42:38:F7:73:8E	Intel Corporate	B	2237	2	Intel Corp.	CVLAPTOP07
34:C9:3D:2D:B5:B2	Intel Corporate	B	226A	2	Intel Corp.	FCS00200079
AC:3F:A4:D2:3F:65	TAIYO YUDEN CO.,LTD	5	4633	48	Marvell Technology Group Ltd.	TJQLJ175205968
10:4E:89:69:FD:70	Garmin International	7	0	46	MediaTek, Inc.	BT_Garmin DriveSmart #3972245662
E8:9E:B4:18:AE:70	Hon Hai Precision Ind. Co.,Ltd.	6	928	46	MediaTek, Inc.	XBR-75X850E
E8:51:77:E8:C6:B9	Qingdao Intelligent&Precise Electronics Co.,Ltd.	A	12E4	46	MediaTek, Inc.	SmartTV 4K
70:09:71:34:21:95	Samsung Electronics Co.,Ltd	9	1005	46	MediaTek, Inc.	[TV] Samsung TU700D 50 TV
70:09:71:69:80:D1	Samsung Electronics Co.,Ltd	9	1005	46	MediaTek, Inc.	[TV] Samsung TU7000 50 TV
C0:23:8D:74:A2:EF	Samsung Electronics Co.,Ltd	9	1005	46	MediaTek, Inc.	[TV] Samsung Q60AA 65 TV
BC:7E:8B:2B:13:0D	Samsung Electronics Co.,Ltd	9	1228	46	MediaTek, Inc.	[TV] Samsung 7 Series (55)
00:7C:2D:29:B2:86	Samsung Electronics Co.,Ltd	9	308	46	MediaTek, Inc.	[TV] Samsung 7 Series (55)
D0:03:DF:D1:30:EF	Samsung Electronics Co.,Ltd	9	308	46	MediaTek, Inc.	[TV] Samsung 7 Series (43)
D4:9D:C0:96:1C:EF	Samsung Electronics Co.,Ltd	9	317	46	MediaTek, Inc.	[TV] Samsung 7 Series (50)
70:09:71:69:80:D1	Samsung Electronics Co.,Ltd	9	7003	46	MediaTek, Inc.	[TV] Samsung TU7000 50 TV
70:09:71:34:21:95	Samsung Electronics Co.,Ltd	9	7005	46	MediaTek, Inc.	[TV] Samsung TU700D 50 TV
4C:C9:5E:72:FE:93	Samsung Electronics Co.,Ltd	9	803	46	MediaTek, Inc.	[TV] Samsung 7 Series (43)
AC:67:5D:CA:0A:8E	Intel Corporate	9	100	1	Nokia Mobile Phones	EXPCQ6092
4C:CE:2D:1C:A7:BB	Danlaw Inc	7	25A	1D	Qualcomm	DL-2233301744
0C:02:BD:D3:05:67	Samsung Electronics Co.,Ltd	9	2BE	1D	Qualcomm	NULL
5C:C1:D7:3F:57:1B	Samsung Electronics Co.,Ltd	8	321	1D	Qualcomm	[TV] Samsung 6 Series (43)
5C:C1:D7:3F:5A:01	Samsung Electronics Co.,Ltd	8	321	1D	Qualcomm	[TV] Samsung 6 Series (43)
7C:64:56:B6:44:6F	Samsung Electronics Co.,Ltd	8	321	1D	Qualcomm	[TV] Samsung 6 Series (43)
7C:64:56:B6:44:75	Samsung Electronics Co.,Ltd	8	321	1D	Qualcomm	[TV] Samsung 6 Series (43)
D0:03:DF:EF:3A:CB	Samsung Electronics Co.,Ltd	8	321	1D	Qualcomm	[Refrigerator] Samsung
00:06:66:0B:E4:1D	Roving Networks	5	1A31	A	Qualcomm Technologies International, Ltd. (QTIL)	PLREP-E41D
88:E0:34:08:DF:FA	Shinwa industries(China) ltd.	8	2918	A	Qualcomm Technologies International, Ltd. (QTIL)	NULL
80:5E:0C:CC:1C:F8	YEALINK(XIAMEN) NETWORK TECHNOLOGY CO.,LTD.	8	2918	A	Qualcomm Technologies International, Ltd. (QTIL)	Yealink MP50
EC:9C:32:4F:A0:A2	Sichuan AI-Link Technology Co., Ltd.	7	7E1C	5D	Realtek Semiconductor Corporation	rk3328
C9:5C:04:77:9A:DD	UNKNOWN_COMP_BY_BDADDR	7	6AE6	5D	Realtek Semiconductor Corporation	BOOMBOX
DC:0D:30:F2:59:99	Shenzhen Feasycom Technology Co., Ltd.	9	6	A2D	Shenzhen Feasycom Technology Co., Ltd.	979869022455
14:8F:21:50:AB:18	Garmin International	6	1B5D	D	Texas Instruments Inc.	BT_nuvi #3912042869
7C:64:56:B6:44:6F	Samsung Electronics Co.,Ltd	8	6321	801D	UNKNOWN_COMP_BY_BT_CID	[TV] Samsung 6 Series (43)
BD:94:2C:C6:2D:74	UNKNOWN_COMP_BY_BDADDR	9	3520	39D6	UNKNOWN_COMP_BY_BT_CID	CAD-4057
B7:89:B9:E1:05:00	UNKNOWN_COMP_BY_BDADDR	9	3120	5D6	Zhuhai Jieli technology Co.,Ltd	CAD-6057
FE:86:B6:4F:FC:0D	UNKNOWN_COMP_BY_BDADDR	3	3120	5D6	Zhuhai Jieli technology Co.,Ltd	BT201-AUDIO
FE:86:B6:4F:FC:0D	UNKNOWN_COMP_BY_BDADDR	8	3120	5D6	Zhuhai Jieli technology Co.,Ltd	BT201-AUDIO

Example Data

device_bdaddr	comp_by_bdaddr	VersNr	SubVersNr	CompId	comp_by_CompId	device_name
FE:86:B6:4F:FC:0D	UNKNOWN_COMP_BY_BDADDR	8	3120	5D0	Anova Applied Electronics	BT201-AUDIO
70:09:71:69:80:D1	Samsung Electronics Co.,Ltd	9	1005	47	Bluegiga	[TV] Samsung TU7000 50 TV
10:2C:6B:91:A8:F5	AMPAK Technology, Inc.	A	2306	F	Broadcom Corporation	Stream TV
10:2C:6B:99:75:63	AMPAK Technology, Inc.	A	6B06	F	Broadcom Corporation	Living Room
14:7D:DA:0F:66:E8	Apple, Inc.	9	4406	F	Broadcom Corporation	mbp
C0:97:27:1C:2C:6B	SAMSUNG ELECTRO-MECHANICS(THAILAND)	7	2304	F	Broadcom Corporation	[TV] Samsung 8 Series (65)
F8:04:2E:81:2F:33	SAMSUNG ELECTRO-MECHANICS(THAILAND)	7	2304	F	Broadcom Corporation	[TV] UN55JU650D
84:A4:66:BA:96:6D	Samsung Electronics Co.,Ltd	6	410E	F	Broadcom Corporation	[TV]Samsung LED55
6C:56:97:31:8E:DA	Amazon Technologies Inc.	8	2304	131	Cypress Semiconductor	Echo Show-2N2
2C:33:61:E6:E2:07	Apple, Inc.	B	240C	131	Cypress Semiconductor	apple’s Keyboard
2C:33:61:E6:E2:07	Apple, Inc.	B	240C	131	Cypress Semiconductor	wkeybd_KPAL
FE:86:B6:4F:FC:0D	UNKNOWN_COMP_BY_BDADDR	8	3120	1D6	G-wearables inc.	BT201-AUDIO
AC:67:5D:CA:0A:8E	Intel Corporate	9	100	2	Intel Corp.	EXPCQ6092
C8:B2:9B:B0:25:83	Intel Corporate	B	216E	2	Intel Corp.	DESKTOP-EC66KUJ
00:42:38:F7:73:8E	Intel Corporate	B	2237	2	Intel Corp.	CVLAPTOP07
34:C9:3D:2D:B5:B2	Intel Corporate	B	226A	2	Intel Corp.	FCS00200079
AC:3F:A4:D2:3F:65	TAIYO YUDEN CO.,LTD	5	4633	48	Marvell Technology Group Ltd.	TJQLJ175205968
10:4E:89:69:FD:70	Garmin International	7	0	46	MediaTek, Inc.	BT_Garmin DriveSmart #3972245662
E8:9E:B4:18:AE:70	Hon Hai Precision Ind. Co.,Ltd.	6	928	46	MediaTek, Inc.	XBR-75X850E
E8:51:77:E8:C6:B9	Qingdao Intelligent&Precise Electronics Co.,Ltd.	A	12E4	46	MediaTek, Inc.	SmartTV 4K
70:09:71:34:21:95	Samsung Electronics Co.,Ltd	9	1005	46	MediaTek, Inc.	[TV] Samsung TU700D 50 TV
70:09:71:69:80:D1	Samsung Electronics Co.,Ltd	9	1005	46	MediaTek, Inc.	[TV] Samsung TU7000 50 TV
C0:23:8D:74:A2:EF	Samsung Electronics Co.,Ltd	9	1005	46	MediaTek, Inc.	[TV] Samsung Q60AA 65 TV
BC:7E:8B:2B:13:0D	Samsung Electronics Co.,Ltd	9	1228	46	MediaTek, Inc.	[TV] Samsung 7 Series (55)
00:7C:2D:29:B2:86	Samsung Electronics Co.,Ltd	9	308	46	MediaTek, Inc.	[TV] Samsung 7 Series (55)
D0:03:DF:D1:30:EF	Samsung Electronics Co.,Ltd	9	308	46	MediaTek, Inc.	[TV] Samsung 7 Series (43)
D4:9D:C0:96:1C:EF	Samsung Electronics Co.,Ltd	9	317	46	MediaTek, Inc.	[TV] Samsung 7 Series (50)
70:09:71:69:80:D1	Samsung Electronics Co.,Ltd	9	7003	46	MediaTek, Inc.	[TV] Samsung TU7000 50 TV
70:09:71:34:21:95	Samsung Electronics Co.,Ltd	9	7005	46	MediaTek, Inc.	[TV] Samsung TU700D 50 TV
4C:C9:5E:72:FE:93	Samsung Electronics Co.,Ltd	9	803	46	MediaTek, Inc.	[TV] Samsung 7 Series (43)
AC:67:5D:CA:0A:8E	Intel Corporate	9	100	1	Nokia Mobile Phones	EXPCQ6092
4C:CE:2D:1C:A7:BB	Danlaw Inc	7	25A	1D	Qualcomm	DL-2233301744
0C:02:BD:D3:05:67	Samsung Electronics Co.,Ltd	9	2BE	1D	Qualcomm	NULL
5C:C1:D7:3F:57:1B	Samsung Electronics Co.,Ltd	8	321	1D	Qualcomm	[TV] Samsung 6 Series (43)
5C:C1:D7:3F:5A:01	Samsung Electronics Co.,Ltd	8	321	1D	Qualcomm	[TV] Samsung 6 Series (43)
7C:64:56:B6:44:6F	Samsung Electronics Co.,Ltd	8	321	1D	Qualcomm	[TV] Samsung 6 Series (43)
7C:64:56:B6:44:75	Samsung Electronics Co.,Ltd	8	321	1D	Qualcomm	[TV] Samsung 6 Series (43)
D0:03:DF:EF:3A:CB	Samsung Electronics Co.,Ltd	8	321	1D	Qualcomm	[Refrigerator] Samsung
00:06:66:0B:E4:1D	Roving Networks	5	1A31	A	Qualcomm Technologies International, Ltd. (QTIL)	PLREP-E41D
88:E0:34:08:DF:FA	Shinwa industries(China) ltd.	8	2918	A	Qualcomm Technologies International, Ltd. (QTIL)	NULL
80:5E:0C:CC:1C:F8	YEALINK(XIAMEN) NETWORK TECHNOLOGY CO.,LTD.	8	2918	A	Qualcomm Technologies International, Ltd. (QTIL)	Yealink MP50
EC:9C:32:4F:A0:A2	Sichuan AI-Link Technology Co., Ltd.	7	7E1C	5D	Realtek Semiconductor Corporation	rk3328
C9:5C:04:77:9A:DD	UNKNOWN_COMP_BY_BDADDR	7	6AE6	5D	Realtek Semiconductor Corporation	BOOMBOX
DC:0D:30:F2:59:99	Shenzhen Feasycom Technology Co., Ltd.	9	6	A2D	Shenzhen Feasycom Technology Co., Ltd.	979869022455
14:8F:21:50:AB:18	Garmin International	6	1B5D	D	Texas Instruments Inc.	BT_nuvi #3912042869
7C:64:56:B6:44:6F	Samsung Electronics Co.,Ltd	8	6321	801D	UNKNOWN_COMP_BY_BT_CID	[TV] Samsung 6 Series (43)
BD:94:2C:C6:2D:74	UNKNOWN_COMP_BY_BDADDR	9	3520	39D6	UNKNOWN_COMP_BY_BT_CID	CAD-4057
B7:89:B9:E1:05:00	UNKNOWN_COMP_BY_BDADDR	9	3120	5D6	Zhuhai Jieli technology Co.,Ltd	CAD-6057
FE:86:B6:4F:FC:0D	UNKNOWN_COMP_BY_BDADDR	3	3120	5D6	Zhuhai Jieli technology Co.,Ltd	BT201-AUDIO
FE:86:B6:4F:FC:0D	UNKNOWN_COMP_BY_BDADDR	8	3120	5D6	Zhuhai Jieli technology Co.,Ltd	BT201-AUDIO

Example Data

device_bdaddr	comp_by_bdaddr	VersNr	SubVersNr	CompId	comp_by_CompId	device_name
FE:86:B6:4F:FC:0D	UNKNOWN_COMP_BY_BDADDR	8	3120	5D0	Anova Applied Electronics	BT201-AUDIO
70:09:71:69:80:D1	Samsung Electronics Co.,Ltd	9	1005	47	Bluegiga	[TV] Samsung TU7000 50 TV
10:2C:6B:91:A8:F5	AMPAK Technology, Inc.	A	2306	F	Broadcom Corporation	Stream TV
10:2C:6B:99:75:63	AMPAK Technology, Inc.	A	6B06	F	Broadcom Corporation	Living Room
14:7D:DA:0F:66:E8	Apple, Inc.	9	4406	F	Broadcom Corporation	mbp
C0:97:27:1C:2C:6B	SAMSUNG ELECTRO-MECHANICS(THAILAND)	7	2304	F	Broadcom Corporation	[TV] Samsung 8 Series (65)
F8:04:2E:81:2F:33	SAMSUNG ELECTRO-MECHANICS(THAILAND)	7	2304	F	Broadcom Corporation	[TV] UN55JU650D
84:A4:66:BA:96:6D	Samsung Electronics Co.,Ltd	6	410E	F	Broadcom Corporation	[TV]Samsung LED55
6C:56:97:31:8E:DA	Amazon Technologies Inc.	8	2304	131	Cypress Semiconductor	Echo Show-2N2
2C:33:61:E6:E2:07	Apple, Inc.	B	240C	131	Cypress Semiconductor	apple's Keyboard
2C:33:61:E6:E2:07	Apple, Inc.	B	240C	131	Cypress Semiconductor	wkeybd_KBAL
FE:86:B6:4F:FC:0D	UNKNOWN_COMP_BY_BDADDR	8	3120	1D6	G-wearables inc.	BT201-AUDIO
AC:67:5D:CA:0A:8E	Intel Corporate	9	100	2	Intel Corp.	EXPCQ6092
C8:B2:9B:B0:25:83	Intel Corporate	B	216E	2	Intel Corp.	DESKTOP-EC66KUJ
00:42:38:F7:73:8E	Intel Corporate	B	2237	2	Intel Corp.	CVLAPTOP07
34:C9:3D:2D:B5:B2	Intel Corporate	B	226A	2	Intel Corp.	FCS00200079
AC:3F:A4:D2:3F:65	TAIYO YUDEN CO.,LTD	5	4633	48	Marvell Technology Group Ltd.	TJQLJ175205968
10:4E:89:69:FD:70	Garmin International	7	0	46	MediaTek, Inc.	BT_Garmin DriveSmart #3972245662
E8:9E:B4:18:AE:70	Hon Hai Precision Ind. Co.,Ltd.	6	928	46	MediaTek, Inc.	XBR-75X850E
E8:51:77:E8:C6:B9	Qingdao Intelligent&Precise Electronics Co.,Ltd.	A	12E4	46	MediaTek, Inc.	SmartTV 4K
70:09:71:34:21:95	Samsung Electronics Co.,Ltd	9	1005	46	MediaTek, Inc.	[TV] Samsung TU700D 50 TV
70:09:71:69:80:D1	Samsung Electronics Co.,Ltd	9	1005	46	MediaTek, Inc.	[TV] Samsung TU7000 50 TV
C0:23:8D:74:A2:EF	Samsung Electronics Co.,Ltd	9	1005	46	MediaTek, Inc.	[TV] Samsung Q60AA 65 TV
BC:7E:8B:2B:13:0D	Samsung Electronics Co.,Ltd	9	1228	46	MediaTek, Inc.	[TV] Samsung 7 Series (55)
00:7C:2D:29:B2:86	Samsung Electronics Co.,Ltd	9	308	46	MediaTek, Inc.	[TV] Samsung 7 Series (55)
D0:03:DF:D1:30:EF	Samsung Electronics Co.,Ltd	9	308	46	MediaTek, Inc.	[TV] Samsung 7 Series (43)
D4:9D:C0:96:1C:EF	Samsung Electronics Co.,Ltd	9	317	46	MediaTek, Inc.	[TV] Samsung 7 Series (50)
70:09:71:69:80:D1	Samsung Electronics Co.,Ltd	9	7003	46	MediaTek, Inc.	[TV] Samsung TU7000 50 TV
70:09:71:34:21:95	Samsung Electronics Co.,Ltd	9	7005	46	MediaTek, Inc.	[TV] Samsung TU700D 50 TV
4C:C9:5E:72:FE:93	Samsung Electronics Co.,Ltd	9	803	46	MediaTek, Inc.	[TV] Samsung 7 Series (43)
AC:67:5D:CA:0A:8E	Intel Corporate	9	100	1	Nokia Mobile Phones	EXPCQ6092
4C:CE:2D:1C:A7:BB	Danlaw Inc	7	25A	1D	Qualcomm	DL-2233301744
0C:02:BD:D3:05:67	Samsung Electronics Co.,Ltd	9	2BE	1D	Qualcomm	NULL
5C:C1:D7:3F:57:1B	Samsung Electronics Co.,Ltd	8	321	1D	Qualcomm	[TV] Samsung 6 Series (43)
5C:C1:D7:3F:5A:01	Samsung Electronics Co.,Ltd	8	321	1D	Qualcomm	[TV] Samsung 6 Series (43)
7C:64:56:B6:44:6F	Samsung Electronics Co.,Ltd	8	321	1D	Qualcomm	[TV] Samsung 6 Series (43)
7C:64:56:B6:44:75	Samsung Electronics Co.,Ltd	8	321	1D	Qualcomm	[TV] Samsung 6 Series (43)
D0:03:DF:EF:3A:CB	Samsung Electronics Co.,Ltd	8	321	1D	Qualcomm	[Refrigerator] Samsung
00:06:66:0B:E4:1D	Roving Networks	5	1A31	A	Qualcomm Technologies International, Ltd. (QTIL)	PLREP-E41D
88:E0:34:08:DF:FA	Shinwa industries(China) ltd.	8	2918	A	Qualcomm Technologies International, Ltd. (QTIL)	NULL
80:5E:0C:CC:1C:F8	YEALINK(XIAMEN) NETWORK TECHNOLOGY CO.,LTD.	8	2918	A	Qualcomm Technologies International, Ltd. (QTIL)	Yealink MP50
EC:9C:32:4F:A0:A2	Sichuan AI-Link Technology Co., Ltd.	7	7E1C	5D	Realtek Semiconductor Corporation	rk3328
C9:5C:04:77:9A:DD	UNKNOWN_COMP_BY_BDADDR	7	6AE6	5D	Realtek Semiconductor Corporation	BOOMBOX
DC:0D:30:F2:59:99	Shenzhen Feasycom Technology Co., Ltd.	9	6	A2D	Shenzhen Feasycom Technology Co., Ltd.	979869022455
14:8F:21:50:AB:18	Garmin International	6	1B5D	D	Texas Instruments Inc.	BT_nuvi #3912042869
7C:64:56:B6:44:6F	Samsung Electronics Co.,Ltd	8	6321	801D	UNKNOWN_COMP_BY_BT_CID	[TV] Samsung 6 Series (43)
BD:94:2C:C6:2D:74	UNKNOWN_COMP_BY_BDADDR	9	3520	39D6	UNKNOWN_COMP_BY_BT_CID	CAD-4057
B7:89:B9:E1:05:00	UNKNOWN_COMP_BY_BDADDR	9	3120	5D6	Zhuhai Jieli technology Co.,Ltd	CAD-6057
FE:86:B6:4F:FC:0D	UNKNOWN_COMP_BY_BDADDR	3	3120	5D6	Zhuhai Jieli technology Co.,Ltd	BT201-AUDIO
FE:86:B6:4F:FC:0D	UNKNOWN_COMP_BY_BDADDR	8	3120	5D6	Zhuhai Jieli technology Co.,Ltd	BT201-AUDIO

Example Data

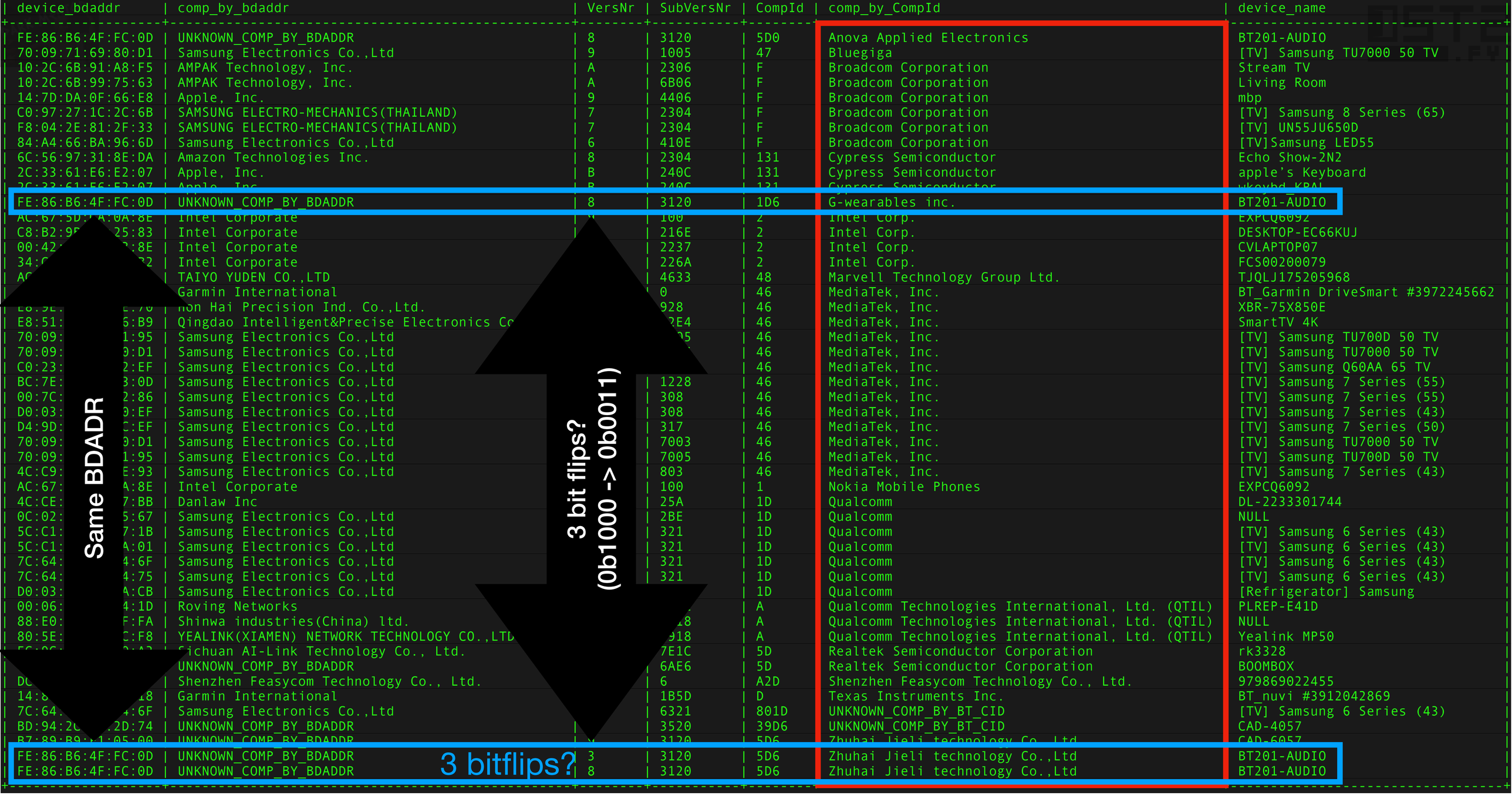
device_bdaddr	comp_by_bdaddr	VersNr	SubVersNr	CompId	comp_by_CompId	device_name
FE:86:B6:4F:FC:0D	UNKNOWN_COMP_BY_BDADDR	8	3120	5D0	Anova Applied Electronics	BT201-AUDIO
70:09:71:69:80:D1	Samsung Electronics Co.,Ltd	9	1005	47	Bluegiga	[TV] Samsung TU7000 50 TV
10:2C:6B:91:A8:F5	AMPAK Technology, Inc.	A	2306	F	Broadcom Corporation	Stream TV
10:2C:6B:99:75:63	AMPAK Technology, Inc.	A	6B06	F	Broadcom Corporation	Living Room
14:7D:DA:0F:66:E8	Apple, Inc.	9	4406	F	Broadcom Corporation	mbp
C0:97:27:1C:2C:6B	SAMSUNG ELECTRO-MECHANICS(THAILAND)	7	2304	F	Broadcom Corporation	[TV] Samsung 8 Series (65)
F8:04:2E:81:2F:33	SAMSUNG ELECTRO-MECHANICS(THAILAND)	7	2304	F	Broadcom Corporation	[TV] UN55JU650D
84:A4:66:BA:96:6D	Samsung Electronics Co.,Ltd	6	410E	F	Broadcom Corporation	[TV]Samsung LED55
6C:56:97:31:8E:DA	Amazon Technologies Inc.	8	2304	131	Cypress Semiconductor	Echo Show-2N2
2C:33:61:E6:E2:07	Apple, Inc.	B	240C	131	Cypress Semiconductor	apple's Keyboard
2C:33:61:E6:E2:07	Apple, Inc.	B	240C	131	Cypress Semiconductor	wkeybd-KBAL
FE:86:B6:4F:FC:0D	UNKNOWN_COMP_BY_BDADDR	8	3120	1D6	G-wearables inc.	BT201-AUDIO
AC:67:5D:CA:0A:8E	Intel Corporate	9	100	2	Intel Corp.	EXPCQ6092
C8:B2:9B:B0:25:83	Intel Corporate	B	216E	2	Intel Corp.	DESKTOP-EC66KUJ
00:42:38:F7:73:8E	Intel Corporate	B	2237	2	Intel Corp.	CVLAPTOP07
34:C9:3D:2D:B5:B2	Intel Corporate	B	226A	2	Intel Corp.	FCS00200079
AC:3F:A4:D2:3F:65	TAIYO YUDEN CO.,LTD	5	4633	48	Marvell Technology Group Ltd.	TJQLJ175205968
10:4E:89:69:FD:70	Garmin International	7	0	46	MediaTek, Inc.	BT_Garmin DriveSmart #3972245662
E8:9E:B4:18:AE:70	Hon Hai Precision Ind. Co.,Ltd.	6	928	46	MediaTek, Inc.	XBR-75X850E
E8:51:77:E8:C6:B9	Qingdao Intelligent&Precise Electronics Co.,Ltd.	A	12E4	46	MediaTek, Inc.	SmartTV 4K
70:09:71:34:21:95	Samsung Electronics Co.,Ltd	9	1005	46	MediaTek, Inc.	[TV] Samsung TU700D 50 TV
70:09:71:69:80:D1	Samsung Electronics Co.,Ltd	9	1005	46	MediaTek, Inc.	[TV] Samsung TU7000 50 TV
C0:23:8D:74:A2:EF	Samsung Electronics Co.,Ltd	9	1005	46	MediaTek, Inc.	[TV] Samsung Q60AA 65 TV
BC:7E:8B:2B:13:0D	Samsung Electronics Co.,Ltd	9	1228	46	MediaTek, Inc.	[TV] Samsung 7 Series (55)
00:7C:2D:29:B2:86	Samsung Electronics Co.,Ltd	9	308	46	MediaTek, Inc.	[TV] Samsung 7 Series (55)
D0:03:DF:D1:30:EF	Samsung Electronics Co.,Ltd	9	308	46	MediaTek, Inc.	[TV] Samsung 7 Series (43)
D4:9D:C0:96:1C:EF	Samsung Electronics Co.,Ltd	9	317	46	MediaTek, Inc.	[TV] Samsung 7 Series (50)
70:09:71:69:80:D1	Samsung Electronics Co.,Ltd	9	7003	46	MediaTek, Inc.	[TV] Samsung TU7000 50 TV
70:09:71:34:21:95	Samsung Electronics Co.,Ltd	9	7005	46	MediaTek, Inc.	[TV] Samsung TU700D 50 TV
4C:C9:5E:72:FE:93	Samsung Electronics Co.,Ltd	9	803	46	MediaTek, Inc.	[TV] Samsung 7 Series (43)
AC:67:5D:CA:0A:8E	Intel Corporate	9	100	1	Nokia Mobile Phones	EXPCQ6092
4C:CE:2D:1C:A7:BB	Danlaw Inc	7	25A	1D	Qualcomm	DL-2233301744
0C:02:BD:D3:05:67	Samsung Electronics Co.,Ltd	9	2BE	1D	Qualcomm	NULL
5C:C1:D7:3F:57:1B	Samsung Electronics Co.,Ltd	8	321	1D	Qualcomm	[TV] Samsung 6 Series (43)
5C:C1:D7:3F:5A:01	Samsung Electronics Co.,Ltd	8	321	1D	Qualcomm	[TV] Samsung 6 Series (43)
7C:64:56:B6:44:6F	Samsung Electronics Co.,Ltd	8	321	1D	Qualcomm	[TV] Samsung 6 Series (43)
7C:64:56:B6:44:75	Samsung Electronics Co.,Ltd	8	321	1D	Qualcomm	[TV] Samsung 6 Series (43)
D0:03:DF:EF:3A:CB	Samsung Electronics Co.,Ltd	8	321	1D	Qualcomm	[Refrigerator] Samsung
00:06:66:0B:E4:1D	Roving Networks	5	1A31	A	Qualcomm Technologies International, Ltd. (QTIL)	PLREP-E41D
88:E0:34:08:DF:FA	Shinwa industries(China) ltd.	8	2918	A	Qualcomm Technologies International, Ltd. (QTIL)	NULL
80:5E:0C:CC:1C:F8	YEALINK(XIAMEN) NETWORK TECHNOLOGY CO.,LTD.	8	2918	A	Qualcomm Technologies International, Ltd. (QTIL)	Yealink MP50
EC:9C:32:4F:A0:A2	Sichuan AI-Link Technology Co., Ltd.	7	7E1C	5D	Realtek Semiconductor Corporation	rk3328
C9:5C:04:77:9A:DD	UNKNOWN_COMP_BY_BDADDR	7	6AE6	5D	Realtek Semiconductor Corporation	BOOMBOX
DC:0D:30:F2:59:99	Shenzhen Feasycom Technology Co., Ltd.	9	6	A2D	Shenzhen Feasycom Technology Co., Ltd.	979869022455
14:8F:21:50:AB:18	Garmin International	6	1B5D	D	Texas Instruments Inc.	BT_nuvi #3912042869
7C:64:56:B6:44:6F	Samsung Electronics Co.,Ltd	8	6321	801D	UNKNOWN_COMP_BY_BT_CID	[TV] Samsung 6 Series (43)
BD:94:2C:C6:2D:74	UNKNOWN_COMP_BY_BDADDR	9	3520	39D6	UNKNOWN_COMP_BY_BT_CID	CAD-4057
B7:89:B9:E1:05:00	UNKNOWN_COMP_BY_BDADDR	9	3120	5D6	Zhuhai Jieli technology Co.,Ltd	CAD-6057
FE:86:B6:4F:FC:0D	UNKNOWN_COMP_BY_BDADDR	3	3120	5D6	Zhuhai Jieli technology Co.,Ltd	BT201-AUDIO
FE:86:B6:4F:FC:0D	UNKNOWN_COMP_BY_BDADDR	8	3120	5D6	Zhuhai Jieli technology Co.,Ltd	BT201-AUDIO

Example Data

device_bdaddr	comp_by_bdaddr	VersNr	SubVersNr	CompId	comp_by_CompId	device_name
FE:86:B6:4F:FC:0D	UNKNOWN_COMP_BY_BDADDR	8	3120	5D0	Anova Applied Electronics	BT201-AUDIO
70:09:71:69:80:D1	Samsung Electronics Co.,Ltd	9	1005	47	Bluegiga	[TV] Samsung TU7000 50 TV
10:2C:6B:91:A8:F5	AMPAK Technology, Inc.	A	2306	F	Broadcom Corporation	Stream TV
10:2C:6B:99:75:63	AMPAK Technology, Inc.	A	6B06	F	Broadcom Corporation	Living Room
14:7D:DA:0F:66:E8	Apple, Inc.	9	4406	F	Broadcom Corporation	mbp
C0:97:27:1C:2C:6B	SAMSUNG ELECTRO-MECHANICS(THAILAND)	7	2304	F	Broadcom Corporation	[TV] Samsung 8 Series (65)
F8:04:2E:81:2F:33	SAMSUNG ELECTRO-MECHANICS(THAILAND)	7	2304	F	Broadcom Corporation	[TV] UN55JU650D
84:A4:66:BA:96:6D	Samsung Electronics Co.,Ltd	6	410E	F	Broadcom Corporation	[TV]Samsung LED55
6C:56:97:31:8E:DA	Amazon Technologies Inc.	8	2304	131	Cypress Semiconductor	Echo Show-2N2
2C:33:61:E6:E2:07	Apple, Inc.	B	240C	131	Cypress Semiconductor	apple's Keyboard
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
FE:86:B6:4F:FC:0D	UNKNOWN_COMP_BY_BDADDR	8	3120	1D6	G-wearables inc.	BT201-AUDIO
AC:67:5D:[illegible]	Intel Corporate	9	100	2	Intel Corp.	EXPCQ6092
C8:B2:9[illegible]	Intel Corporate	B	216E	2	Intel Corp.	DESKTOP-EC66KUJ
00:42:[illegible]	Intel Corporate	B	2237	2	Intel Corp.	CVLAPTOP07
34:C[illegible]	Intel Corporate	B	226A	2	Intel Corp.	FCS00200079
AC[illegible]	TAIYO YUDEN CO.,LTD	5	4633	48	Marvell Technology Group Ltd.	TJQLJ175205968
[illegible]	Garmin International	7	0	46	MediaTek, Inc.	BT_Garmin DriveSmart #3972245662
E8:9E:[illegible]	Hon Hai Precision Ind. Co.,Ltd.	6	928	46	MediaTek, Inc.	XBR-75X850E
E8:51:[illegible]	Qingdao Intelligent&Precise Electronics Co.,Ltd.	A	12E4	46	MediaTek, Inc.	SmartTV 4K
70:09:[illegible]	Samsung Electronics Co.,Ltd	9	1005	46	MediaTek, Inc.	[TV] Samsung TU700D 50 TV
70:09:[illegible]	Samsung Electronics Co.,Ltd	9	1005	46	MediaTek, Inc.	[TV] Samsung TU7000 50 TV
C0:23:[illegible]	Samsung Electronics Co.,Ltd	9	1005	46	MediaTek, Inc.	[TV] Samsung Q60AA 65 TV
BC:7E:[illegible]	Samsung Electronics Co.,Ltd	9	1228	46	MediaTek, Inc.	[TV] Samsung 7 Series (55)
00:7C:[illegible]	Samsung Electronics Co.,Ltd	9	308	46	MediaTek, Inc.	[TV] Samsung 7 Series (55)
D0:03:[illegible]	Samsung Electronics Co.,Ltd	9	308	46	MediaTek, Inc.	[TV] Samsung 7 Series (43)
D4:9D:[illegible]	Samsung Electronics Co.,Ltd	9	317	46	MediaTek, Inc.	[TV] Samsung 7 Series (50)
70:09:[illegible]	Samsung Electronics Co.,Ltd	9	7003	46	MediaTek, Inc.	[TV] Samsung TU7000 50 TV
70:09:[illegible]	Samsung Electronics Co.,Ltd	9	7005	46	MediaTek, Inc.	[TV] Samsung TU700D 50 TV
4C:C9:[illegible]	Samsung Electronics Co.,Ltd	9	803	46	MediaTek, Inc.	[TV] Samsung 7 Series (43)
AC:67:[illegible]	Intel Corporate	9	100	1	Nokia Mobile Phones	EXPCQ6092
4C:CE:[illegible]	Danlaw Inc	7	25A	1D	Qualcomm	DL-2233301744
0C:02:[illegible]	Samsung Electronics Co.,Ltd	9	2BE	1D	Qualcomm	NULL
5C:C1:[illegible]	Samsung Electronics Co.,Ltd	8	321	1D	Qualcomm	[TV] Samsung 6 Series (43)
5C:C1:[illegible]	Samsung Electronics Co.,Ltd	8	321	1D	Qualcomm	[TV] Samsung 6 Series (43)
7C:64:[illegible]	Samsung Electronics Co.,Ltd	8	321	1D	Qualcomm	[TV] Samsung 6 Series (43)
7C:64:[illegible]	Samsung Electronics Co.,Ltd	8	321	1D	Qualcomm	[TV] Samsung 6 Series (43)
D0:03:[illegible]	Samsung Electronics Co.,Ltd	8	321	1D	Qualcomm	[Refrigerator] Samsung
00:06:[illegible]	Roving Networks	5	1A31	A	Qualcomm Technologies International, Ltd. (QTIL)	PLREP-E41D
88:E0:[illegible]	Shinwa industries(China) ltd.	8	2918	A	Qualcomm Technologies International, Ltd. (QTIL)	NULL
80:5E:[illegible]	YEALINK(XIAMEN) NETWORK TECHNOLOGY CO.,LTD.	8	2918	A	Qualcomm Technologies International, Ltd. (QTIL)	Yealink MP50
[illegible]	Sichuan AI-Link Technology Co., Ltd.	7	7E1C	5D	Realtek Semiconductor Corporation	rk3328
[illegible]	UNKNOWN_COMP_BY_BDADDR	7	6AE6	5D	Realtek Semiconductor Corporation	BOOMBOX
DC[illegible]	Shenzhen Feasycom Technology Co., Ltd.	9	6	A2D	Shenzhen Feasycom Technology Co., Ltd.	979869022455
14:8[illegible]	Garmin International	6	1B5D	D	Texas Instruments Inc.	BT_nuvi #3912042869
7C:64:[illegible]	Samsung Electronics Co.,Ltd	8	6321	801D	UNKNOWN_COMP_BY_BT_CID	[TV] Samsung 6 Series (43)
BD:94:2C:[illegible]	UNKNOWN_COMP_BY_BDADDR	9	3520	39D6	UNKNOWN_COMP_BY_BT_CID	CAD-4057
B7:89:B9:[illegible]	UNKNOWN_COMP_BY_BDADDR	9	3120	5D6	Zhuhai Jieli technology Co.,Ltd	CAD-6057
FE:86:B6:4F:FC:0D	UNKNOWN_COMP_BY_BDADDR	3	3120	5D6	Zhuhai Jieli technology Co.,Ltd	BT201-AUDIO
FE:86:B6:4F:FC:0D	UNKNOWN_COMP_BY_BDADDR	8	3120	5D6	Zhuhai Jieli technology Co.,Ltd	BT201-AUDIO

Same BDADR

Example Data



Example Data

device_bdaddr	comp_by_bdaddr	VersNr	SubVersNr	CompId	comp_by_CompId	device_name
FE:86:B6:4F:FC:0D	UNKNOWN_COMP_BY_BDADDR	8	3120	5D0	Anova Applied Electronics	BT201-AUDIO
70:09:71:69:80:D1	Samsung Electronics Co.,Ltd	9	1005	47	Bluegiga	[TV] Samsung TU7000 50 TV
10:2C:6B:91:A8:F5	AMPAK Technology, Inc.	A	2306	F	Broadcom Corporation	Stream TV
10:2C:6B:99:75:63	AMPAK Technology, Inc.	A	6B06	F	Broadcom Corporation	Living Room
14:7D:DA:0F:66:E8	Apple, Inc.	9	4406	F	Broadcom Corporation	mbp
C0:97:27:1C:2C:6B	SAMSUNG ELECTRO-MECHANICS(THAILAND)	7	2304	F	Broadcom Corporation	[TV] Samsung 8 Series (65)
F8:04:2E:81:2F:33	SAMSUNG ELECTRO-MECHANICS(THAILAND)	7	2304	F	Broadcom Corporation	[TV] UN55JU650D
84:A4:66:BA:96:6D	Samsung Electronics Co.,Ltd	6	410E	F	Broadcom Corporation	[TV]Samsung LED55
6C:56:97:31:8E:DA	Amazon Technologies Inc.	8	2304	131	Cypress Semiconductor	Echo Show-2N2
2C:33:61:E6:E2:07	Apple, Inc.	B	240C	131	Cypress Semiconductor	apple's Keyboard
2C:33:61:E6:E2:07	Apple, Inc.	B	240C	131	Cypress Semiconductor	wkeybd-KBAL
FE:86:B6:4F:FC:0D	UNKNOWN_COMP_BY_BDADDR	8	3120	1D6	G-wearables inc.	BT201-AUDIO
AC:67:5D:[illegible]	Intel Corporate	[illegible]	100	[illegible]	Intel Corp.	EXPCQ6092
C8:B2:9[illegible]	Intel Corporate	[illegible]	216E	[illegible]	Intel Corp.	DESKTOP-EC66KUJ
00:42:[illegible]	Intel Corporate	[illegible]	2237	[illegible]	Intel Corp.	CVLAPTOP07
34:C[illegible]	Intel Corporate	[illegible]	226A	[illegible]	Intel Corp.	FCS00200079
AC[illegible]	TAIYO YUDEN CO.,LTD	[illegible]	4633	[illegible]	Marvell Technology Group Ltd.	TJQLJ175205968
[illegible]	Garmin International	[illegible]	0	[illegible]	MediaTek, Inc.	BT_Garmin DriveSmart #3972245662
E8:9E:[illegible]	Hon Hai Precision Ind. Co.,Ltd.	[illegible]	928	[illegible]	MediaTek, Inc.	XBR-75X850E
E8:51:[illegible]	Qingdao Intelligent&Precise Electronics Co	[illegible]	[illegible]	[illegible]	MediaTek, Inc.	SmartTV 4K
70:09:[illegible]	Samsung Electronics Co.,Ltd	[illegible]	[illegible]	[illegible]	MediaTek, Inc.	[TV] Samsung TU700D 50 TV
70:09:[illegible]	Samsung Electronics Co.,Ltd	[illegible]	[illegible]	[illegible]	MediaTek, Inc.	[TV] Samsung TU7000 50 TV
C0:23:[illegible]	Samsung Electronics Co.,Ltd	[illegible]	[illegible]	[illegible]	MediaTek, Inc.	[TV] Samsung Q60AA 65 TV
BC:7E:[illegible]	Samsung Electronics Co.,Ltd	[illegible]	1228	[illegible]	MediaTek, Inc.	[TV] Samsung 7 Series (55)
00:7C:[illegible]	Samsung Electronics Co.,Ltd	[illegible]	308	[illegible]	MediaTek, Inc.	[TV] Samsung 7 Series (55)
D0:03:[illegible]	Samsung Electronics Co.,Ltd	[illegible]	308	[illegible]	MediaTek, Inc.	[TV] Samsung 7 Series (43)
D4:9D:[illegible]	Samsung Electronics Co.,Ltd	[illegible]	317	[illegible]	MediaTek, Inc.	[TV] Samsung 7 Series (50)
70:09:[illegible]	Samsung Electronics Co.,Ltd	[illegible]	7003	[illegible]	MediaTek, Inc.	[TV] Samsung TU7000 50 TV
70:09:[illegible]	Samsung Electronics Co.,Ltd	[illegible]	7005	[illegible]	MediaTek, Inc.	[TV] Samsung TU700D 50 TV
4C:C9:[illegible]	Samsung Electronics Co.,Ltd	[illegible]	803	[illegible]	MediaTek, Inc.	[TV] Samsung 7 Series (43)
AC:67:[illegible]	Intel Corporate	[illegible]	100	[illegible]	Nokia Mobile Phones	EXPCQ6092
4C:CE:[illegible]	Danlaw Inc	[illegible]	25A	[illegible]	Qualcomm	DL-2233301744
0C:02:[illegible]	Samsung Electronics Co.,Ltd	[illegible]	2BE	[illegible]	Qualcomm	NULL
5C:C1:[illegible]	Samsung Electronics Co.,Ltd	[illegible]	321	[illegible]	Qualcomm	[TV] Samsung 6 Series (43)
5C:C1:[illegible]	Samsung Electronics Co.,Ltd	[illegible]	321	[illegible]	Qualcomm	[TV] Samsung 6 Series (43)
7C:64:[illegible]	Samsung Electronics Co.,Ltd	[illegible]	321	[illegible]	Qualcomm	[TV] Samsung 6 Series (43)
7C:64:[illegible]	Samsung Electronics Co.,Ltd	[illegible]	321	[illegible]	Qualcomm	[TV] Samsung 6 Series (43)
D0:03:[illegible]	Samsung Electronics Co.,Ltd	[illegible]	[illegible]	[illegible]	[illegible]omm	[Refrigerator] Samsung
00:06:[illegible]	Roving Networks	[illegible]	[illegible]	[illegible]	[illegible]comm Technologies International, Ltd. (QTIL)	PLREP-E41D
88:E0:[illegible]	Shinwa industries(China) ltd.	[illegible]	[illegible]	[illegible]	[illegible]alcomm Technologies International, Ltd. (QTIL)	NULL
80:5E:[illegible]	YEALINK(XIAMEN) NETWORK TECHNOLOGY CO.,LTD	[illegible]	[illegible]91	[illegible]	[illegible]ualcomm Technologies International, Ltd. (QTIL)	Yealink MP50
[illegible]	Sichuan AI-Link Technology Co., Ltd.	[illegible]	7E1C	[illegible]	Realtek Semiconductor Corporation	rk3328
[illegible]	UNKNOWN_COMP_BY_BDADDR	[illegible]	6AE6	[illegible]	Realtek Semiconductor Corporation	BOOMBOX
DC[illegible]	Shenzhen Feasycom Technology Co., Ltd.	[illegible]	6	[illegible]	Shenzhen Feasycom Technology Co., Ltd.	979869022455
14:8[illegible]	Garmin International	[illegible]	1B5D	[illegible]	Texas Instruments Inc.	BT_nuvi #3912042869
7C:64:[illegible]	Samsung Electronics Co.,Ltd	[illegible]	6321	[illegible]	UNKNOWN_COMP_BY_BT_CID	[TV] Samsung 6 Series (43)
BD:94:2[illegible]	UNKNOWN_COMP_BY_BDADDR	[illegible]	3520	[illegible]	UNKNOWN_COMP_BY_BT_CID	CAD-4057
B7:89:B9:[illegible]	UNKNOWN_COMP_BY_BDADDR	[illegible]	3120	[illegible]	Zhuhai Jieli technology Co.,Ltd	CAD-6057
FE:86:B6:4F:FC:0D	UNKNOWN_COMP_BY_BDADDR	3	3120	5D6	Zhuhai Jieli technology Co.,Ltd	BT201-AUDIO
FE:86:B6:4F:FC:0D	UNKNOWN_COMP_BY_BDADDR	8	3120	5D6	Zhuhai Jieli technology Co.,Ltd	BT201-AUDIO

Example Data

(Link Layer) Sub-Version Number

SubVersNr (2 bytes)

- The vendor gets to make up whatever value they want here!

From BT
Assigned Numbers document

(Link I

SubVersI

- The venc

2.4.2.13 LL_VERSION_IND

The format of the CtrData field is shown in Figure 2.23.

CtrData		
VersNr (1 octet)	CompId (2 octets)	SubVersNr (2 octets)

Figure 2.23: CtrData field of the LL_VERSION_IND PDU

The LL_VERSION_IND CtrData consists of three fields:

- VersNr field shall contain the version of the Bluetooth Controller specification (see Bluetooth Assigned Numbers).
- CompId field shall contain the company identifier of the manufacturer of the Bluetooth Controller (see Bluetooth Assigned Numbers).

SubVersNr field shall contain a unique value for each implementation or revision of an implementation of the Bluetooth Controller.

From BT
Assigned Numbers document

Does SubVersNr Imply OS/Firmware Version?

- **Hypothesis:** SubVersNr will increment per OS/firmware update, and thus can be used to infer the OS/firmware version
  - Conclusion:
    - **Rejected** for Broadcom

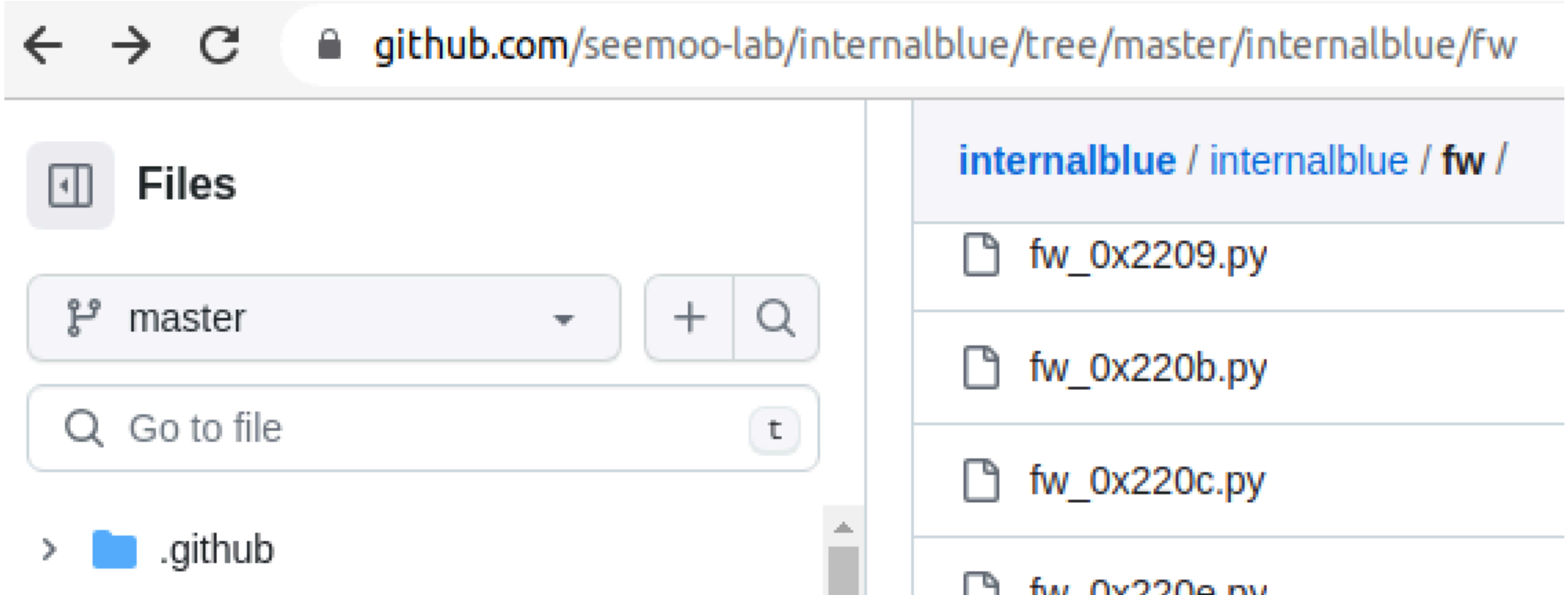
Does SubVersNr Imply OS/Firmware Version?

- From BlueZ 5.66 monitor/packet.c

```
} broadcom_usb_subversion_table[] = {
  { 0x210b, "BCM43142A0" },  /* 001.001.011 */
  { 0x2112, "BCM4314A0"},  /* 001.001.018 */
  { 0x2118, "BCM20702A0" },  /* 001.001.024 */
  { 0x2126, "BCM4335A0"},  /* 001.001.038 */
  { 0x220e, "BCM20702A1" },  /* 001.002.014 */
  { 0x230f, "BCM4354A2"},  /* 001.003.015 */
  { 0x4106, "BCM4335B0"},  /* 002.001.006 */
  { 0x410e, "BCM20702B0" },  /* 002.001.014 */
  { 0x6109, "BCM4335C0"},  /* 003.001.009 */
  { 0x610c, "BCM4354"},  /* 003.001.012 */
```

Oh right...I remember something now...

- InternalBlue has firmware files per Broadcom chip, and they're ordered by numbers that look like those SubVersions!



C

•

fw_0x2033.py

fw_0x203a.py

fw_0x2056.py

fw_0x21a9.py

fw_0x21d0.py

fw_0x2209.py

fw_0x220b.py

fw_0x220c.py

fw_0x220e.py

fw_0x2230.py

fw_0x240f.py

fw_0x3032.py

fw_0x4196.py

fw_0x4208.py

fw_0x420e.py

fw_0x420e_iphone.py

fw_0x4228.py

fw_0x422a.py

fw_0x6103.py

fw_0x6109.py

fw_0x6119.py

C

- fw_0x2033.py
- fw_0x203a.py
- fw_0x2056.py
- fw_0x21a9.py
- fw_0x21d0.py
- fw_0x2209.py

```
} broadcom_usb_subversion_table[] = {
  { 0x210b, "BCM43142A0" }, /* 001.001.011 */
  { 0x2112, "BCM4314A0"  }, /* 001.001.018 */
  { 0x2118, "BCM20702A0" }, /* 001.001.024 */
  { 0x2126, "BCM4335A0"  }, /* 001.001.038 */
  { 0x220e, "BCM20702A1" }, /* 001.002.014 */
  { 0x230f, "BCM4354A2"  }, /* 001.003.015 */
  { 0x4106, "BCM4335B0"  }, /* 002.001.006 */
  { 0x410e, "BCM20702B0" }, /* 002.001.014 */
  { 0x6109, "BCM4335C0"  }, /* 003.001.009 */
  { 0x610c, "BCM4354"    }, /* 003.001.012 */
```

- fw_0x4196.py
- fw_0x4208.py
- fw_0x420e.py
- fw_0x420e_iphone.py
- fw_0x4228.py
- fw_0x422a.py
- fw_0x6103.py
- fw_0x6109.py
- fw_0x6119.py

Broadcom

- So at least for Broadcom, the SubVersion is used to store a specific silicon chip *(& stepping revision)* information!
- ***The ideal ChipPrint!*** 🥳
- (I would have preferred a VersionPrint, but oh well...)

VersionPrint

Ver. 1 | Ver. 2 | Ver. 3 | Ver. N

WHAT I WANT!

ChipPrint

Chip 1 | Chip 2 | Chip 3 | Chip N

WHAT I MOSTLY GET 😔

ChipMakerPrint

ChipMaker 1 | ChipMaker 2 | ChipMaker N

ModulePrint

Module 11 | Module 13 | Module NA | Module NX

ModuleMakerPrint

ModuleMaker 1 | ModuleMaker 2 | ModuleMaker N

ProductPrint

Product 1 | Product 2 | Product N

ProductMakerPrint

ProductMaker 1

Does SubVersNr Imply OS/Firmware Version?

- **Hypothesis:** SubVersNr will increment per OS/firmware update, and thus can be used to infer the OS/firmware version
  - Conclusion:
    - Weak reject for MediaTek, which seems to default to SubVersNr == 0, but where there are a range of versions seen, which probably then depends on the device maker's behavior
    - *Requires more investigation*

Does SubVersNr Imply OS/Firmware Version?

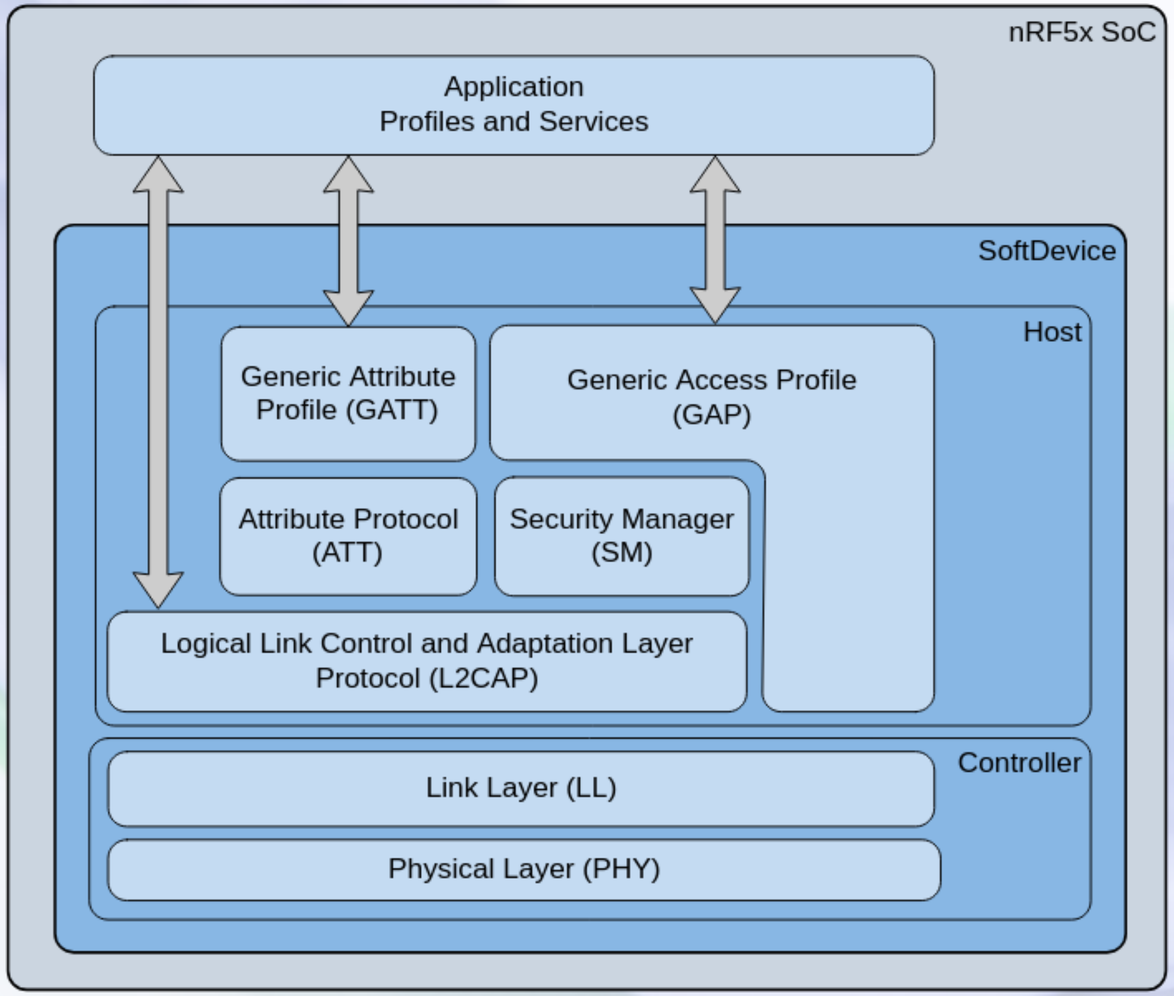
- **Hypothesis:** SubVersNr will increment per OS/firmware update, and thus can be used to infer the OS/firmware version
  - Overall Conclusion:
    - Requires more investigation!
      - Fundamentally requires hands on with a device + manually updating firmware and observing how the sub-version-number changes

2thprint by Link Layer Packet Combinations 🤾

2thprint by Link Layer Packet Combinations

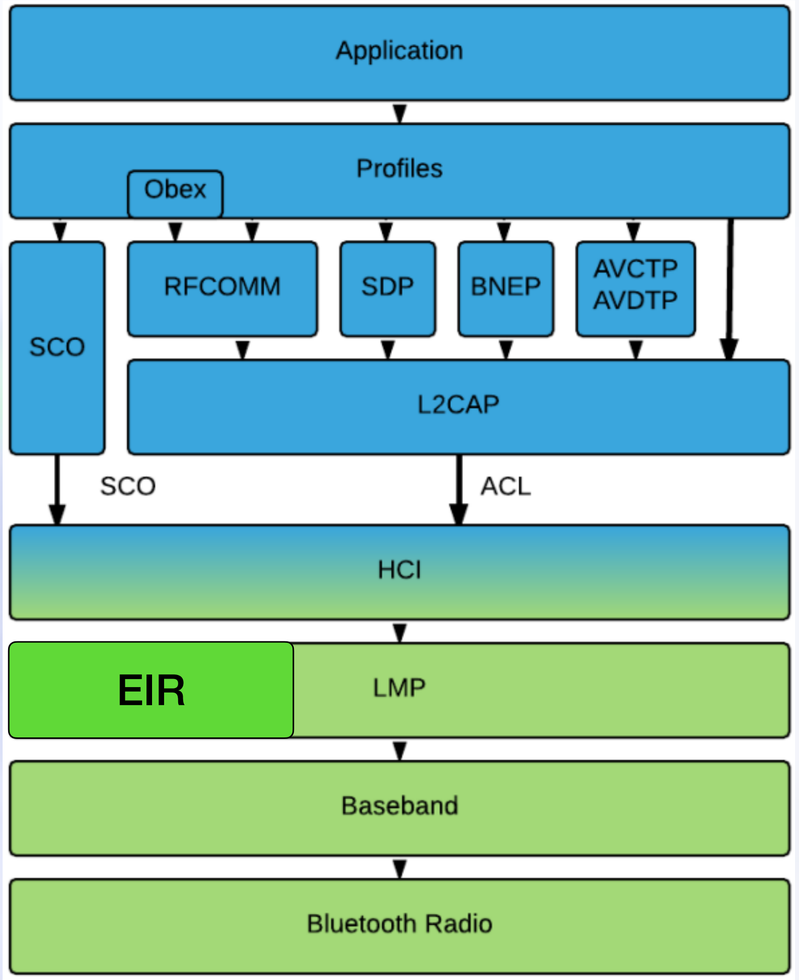
BLE

[1]



BTC

[2]

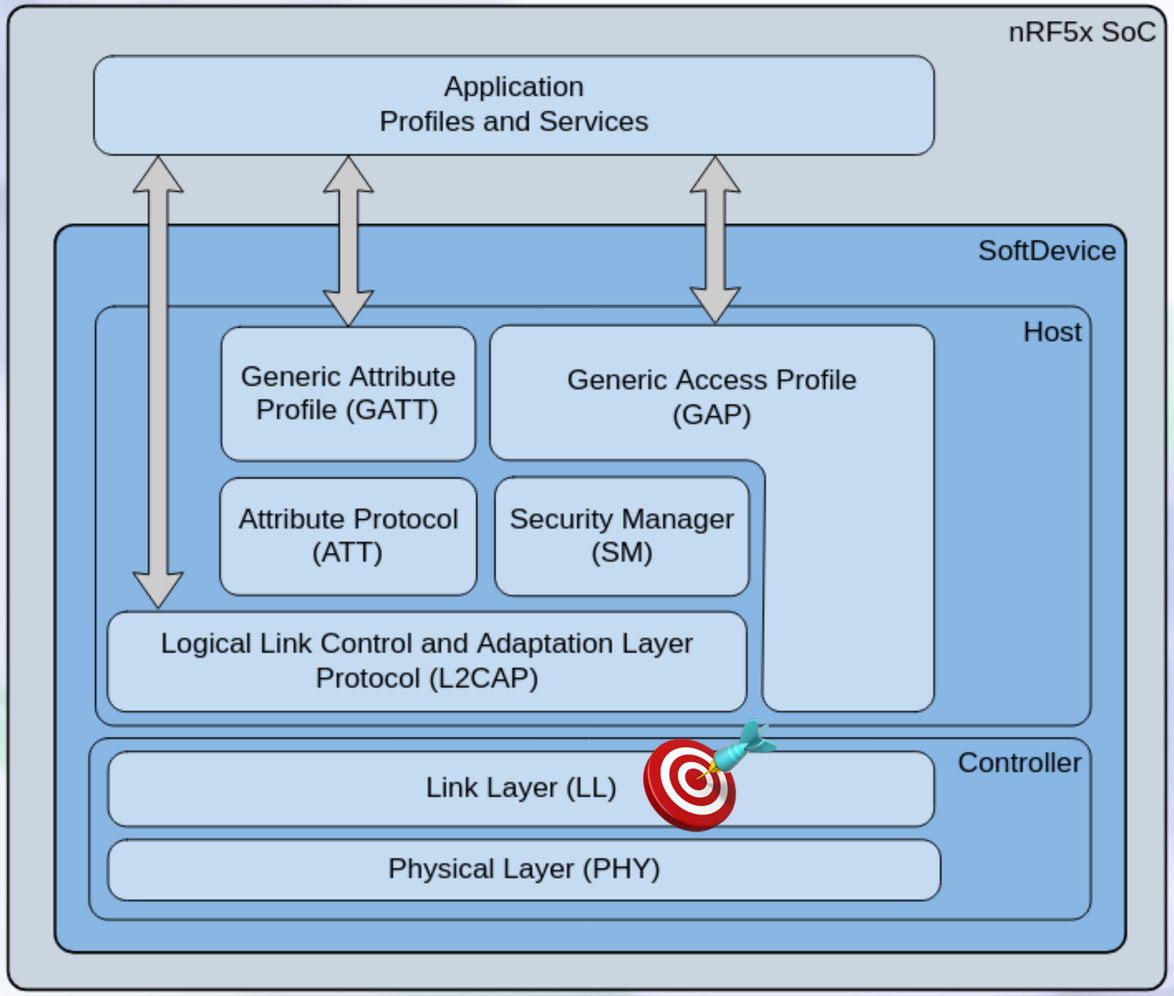


[1] https://infocenter.nordicsemi.com/index.jsp?topic=%2Fsds_s140%2FSDS%2Fs1xx%2Fble_protocol_stack%2Fble_protocol_stack.html
[2] https://crosscontrol.com/manual/Bluetooth%20Documentation/content/bluetooth.html

2thprint by Link Layer Packet Combinations

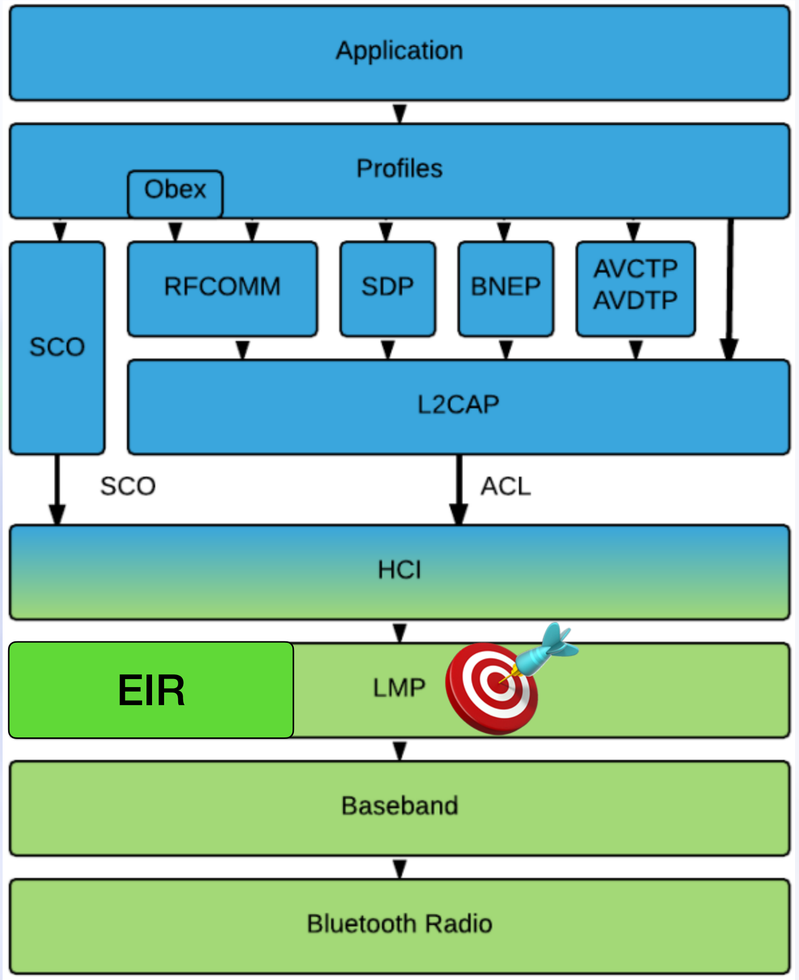
BLE

[1]



BTC

[2]

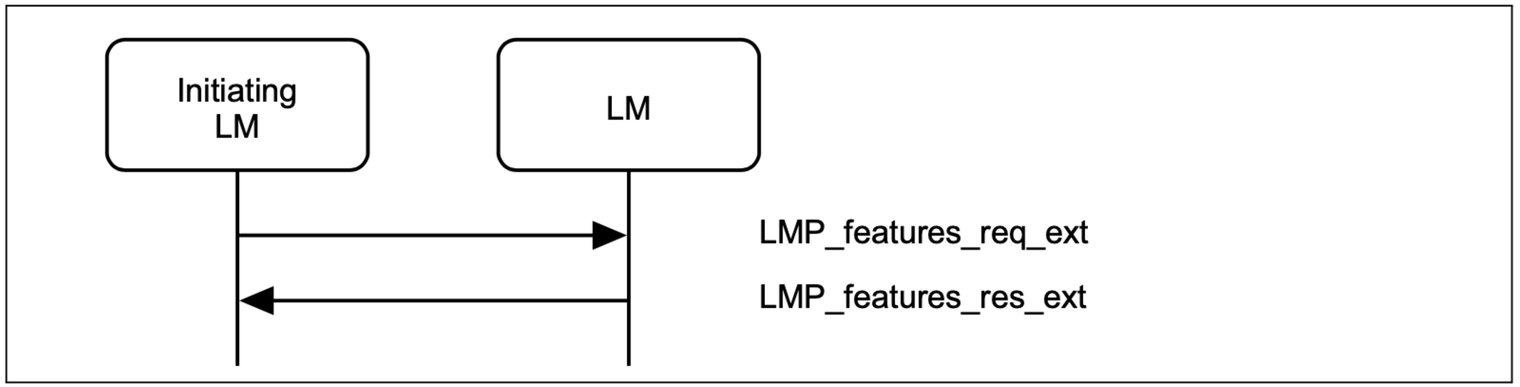


[1] https://infocenter.nordicsemi.com/index.jsp?topic=%2Fsds_s140%2FSDS%2Fs1xx%2Fble_protocol_stack%2Fble_protocol_stack.html
[2] https://crosscontrol.com/manual/Bluetooth%20Documentation/content/bluetooth.html

Version Information is not the only game in town

- If we want to be more nmap-OS-fingerprint-like, it makes sense to hit the target with multiple packet types, potentially in different orders, and see how it responds
- **LMP packet types:** LMP_features_req, LMP_features_req_ext, LMP_version_req, LMP_name_req, LMP_switch_req, LMP_ping_req, LMP_encryption_key_size_req, *malformed* LMP_features_req, *malformed* LMP_features_req_ext
- **BLE LL packet types:** LL_VERSION_IND, LL_LENGTH_REQ, LL_PING_REQ, LL_FEATURE_REQ

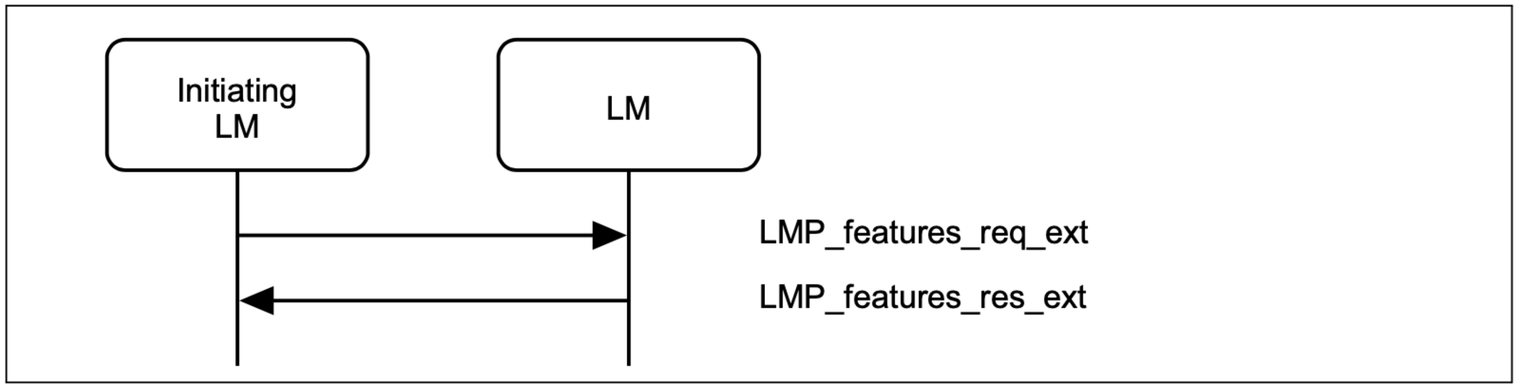
"*malformed*" LMP_features_ext_req?



Sequence 79: Request for extended features

From BT
Core Spec v4.2

"*malformed*" LMP_features_ext_req?



Sequence 79: Request for extended features

3.3 FEATURE MASK DEFINITION

The features are represented as a bit mask when they are transferred in LMP messages. For each feature a single bit is specified which shall be set to 1 if the feature is supported and set to 0 otherwise. The single exception is the flow control lag which is coded as a 3 bit field with the least significant bit in byte 2 bit 4 and the most significant bit in byte 2 bit 6. All removed, unknown, or unassigned feature bits shall be set to 0 and ignored upon receipt.

No.	Supported feature	Byte	Bit
0	3 slot packets	0	0
1	5 slot packets	0	1
2	Encryption	0	2

From BT Core Spec v4.2

"malform ?

3	Slot offset	0	3
4	Timing accuracy	0	4
5	Role switch	0	5
6	Hold mode	0	6
7	Sniff mode	0	7
8	Park state	1	0
9	Power control requests	1	1
10	Channel quality driven data rate (CQDDR)	1	2
11	SCO link	1	3

...

No.	Supported feature	Byte	Bit
57	Inquiry TX Power Level	7	1
58	Enhanced Power Control	7	2
59	Reserved	7	3
60	Reserved	7	4
61	Reserved	7	5
62	Reserved	7	6
63	Extended features	7	7

Table 3.2: Feature mask definitions (page 0)

From BT
Core Spec v4.2

"malform ?

3	Slot offset	0	3
4	Timing accuracy	0	4
5	Role switch	0	5
6	Hold mode	0	6
7	Sniff mode	0	7
8	Park state	1	0
9	Power control requests	1	1
10	Channel quality driven data rate (CQDDR)	1	2
11	SCO link	1	3

...

No.	Supported feature	Byte	Bit
57	Inquiry TX Power Level	7	1
58	Enhanced Power Control	7	2
59	Reserved	7	3
60	Reserved	7	4
61	Reserved	7	5
62	Reserved	7	6
63	Extended features	7	7

Table 3.2: Feature mask definitions (page 0)

From BT
Core Spec v4.2

No.	Supported Feature	Byte	Bit
64	Secure Simple Pairing (Host Support)	0	0
65	LE Supported (Host)	0	1
66	Simultaneous LE and BR/EDR to Same Device Capable (Host)	0	2
67	Secure Connections (Host Support)	0	3

Table 3.3: Extended feature mask definition (page 1)

No.	Supported Feature	Byte	Bit
128	Connectionless Slave Broadcast – Master Operation	0	0
129	Connectionless Slave Broadcast – Slave Operation	0	1
130	Synchronization Train	0	2
131	Synchronization Scan	0	3
132	Inquiry Response Notification Event	0	4
133	Generalized interlaced scan	0	5
134	Coarse Clock Adjustment	0	6
135	Reserved	0	7
136	Secure Connections (Controller Support)	1	0
137	Ping	1	1
138	Reserved	1	2
139	Train nudging	1	3

Table 3.4: Extended feature mask definition (page 2)

From BT
Core Spec v4.2

No.	Supported Feature	Byte	Bit
64	Secure Simple Pairing (Host Support)	0	0
65	LE Supported (Host)	0	1
66	Simultaneous LE and BR/EDR to Same Device Capable (Host)	0	2
67	Secure Connections (Host Support)	0	3

Table 3.3: Extended feature mask definitio (page 1)

No.	Supported Feature	Byte	Bit
128	Connectionless Slave Broadcast – Master Operation	0	0
129	Connectionless Slave Broadcast – Slave Operation	0	1
130	Synchronization Train	0	2
131	Synchronization Scan	0	3
132	Inquiry Response Notification Event	0	4
133	Generalized interlaced scan	0	5
134	Coarse Clock Adjustment	0	6
135	Reserved	0	7
136	Secure Connections (Controller Support)	1	0
137	Ping	1	1
138	Reserved	1	2
139	Train nudging	1	3

Table 3.4: Extended feature mask definitio (page 2)

From BT
Core Spec v4.2

Pick a page, any page...

M/O	PDU	Contents
M	LMP_features_req	features
M	LMP_features_res	features
O(63)	LMP_features_req_ext	features page max supported page extended features
O(63)	LMP_features_res_ext	features page max supported page extended features

Table 4.27: PDUs used for features request

"The LMP_features_req_ext PDU contains a feature page index that specifies which page is requested and the contents of that page for the requesting device. Pages are numbered from 0-255 with page 0 corresponding to the normal features mask. "

From BT
Core Spec v4.2

Pick a page, any pag

You should *never* request a feature page > their max supported page OR the max page in the version of the spec that they conform to.
E.g. Spec 4.2 only has pages 0, 1, 2.
So what happens if you request 3...or 255?

M/O	PDU	Contents
M	LMP_features_req	features
M	LMP_features_res	features
O(63)	LMP_features_req_ext	features page max supported page extended features
O(63)	LMP_features_res_ext	features page max supported page extended features

Table 4.27: PDUs used for features request

"The LMP_features_req_ext PDU contains a feature page index that specifies which page is requested and the contents of that page for the requesting device. Pages are numbered from 0-255 with page 0 corresponding to the normal features mask. "

From BT
Core Spec v4.2

How to Send Packets?

- Sweyntooth[1] (2020, BLE-only) & Braktooth[2] (2022, BTC-only)
  - Provide a way in Python and C respectively to create & send arbitrary link-layer packets in an arbitrary order

[1] https://asset-group.github.io/disclosures/sweyntooth/
[2] https://asset-group.github.io/disclosures/braktooth/

DATA ANALYSIS ETA WEN?

- Finding "weird packets/combinations" was the original idea for 2thprinting...and yet...I haven't actually analyzed this data yet ¯_(ツ)_/¯. Why tho?

DATA ANALYSIS ETA WEN?

- Finding "weird packets/combinations" was the original idea for 2thprinting...and yet...I haven't actually analyzed this data yet ¯_(ツ)_/¯. Why tho?
- 1) it *feels* like I haven't found the right balance yet between speed and useful signal
  - I'm prioritizing 2thprinting mechanisms that are as fast as possible, so they can be used against moving targets
    - Reinvocation of Braktooth/Sweyntooth adds 5+ seconds of overhead to every 2thprinting attempt

DATA ANALYSIS ETA WEN?

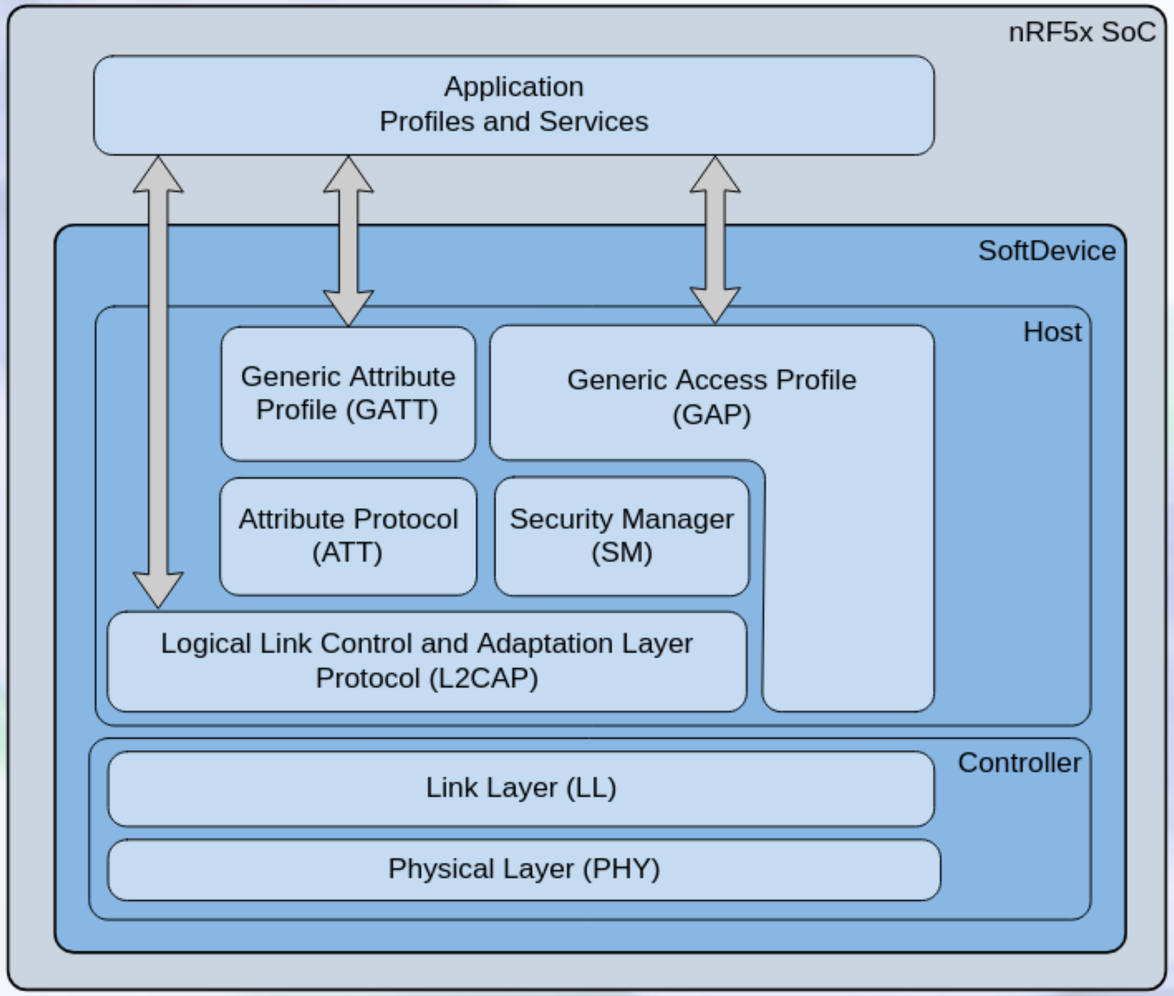
- Finding "weird packets/combinations" was the original idea for 2thprinting...and yet...I haven't actually analyzed this data yet ¯_(ツ)_/¯. Why tho?
- 1) it *feels* like I haven't found the right balance yet between speed and useful signal
  - I'm prioritizing 2thprinting mechanisms that are as fast as possible, so they can be used against moving targets
    - Reinvocation of Braktooth/Sweyntooth adds 5+ seconds of overhead to every 2thprinting attempt
- 2) I want known *reference chips* to compare this data to before I start asserting "this packet combination result is indicative of vendor X"
  - Current research intern project

2thprint by Manufacturer Specific Data 🧘 or 🚶

2thprint by Manufacturer Specific Data 🧘 or 🚶

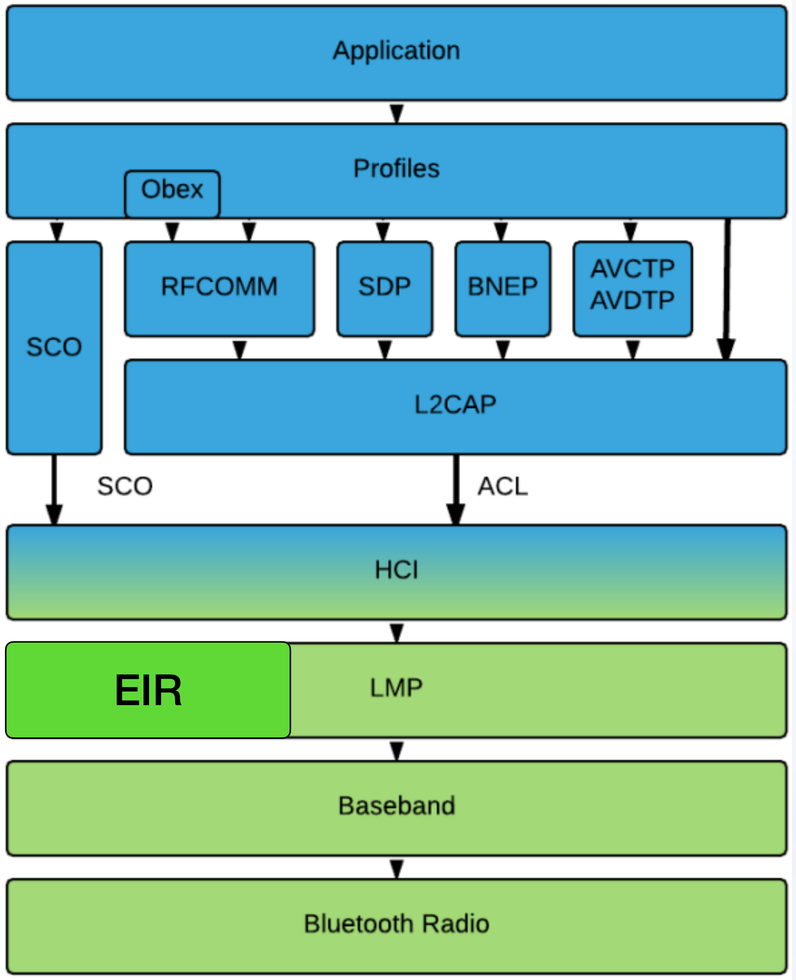
BLE

[1]



BTC

[2]

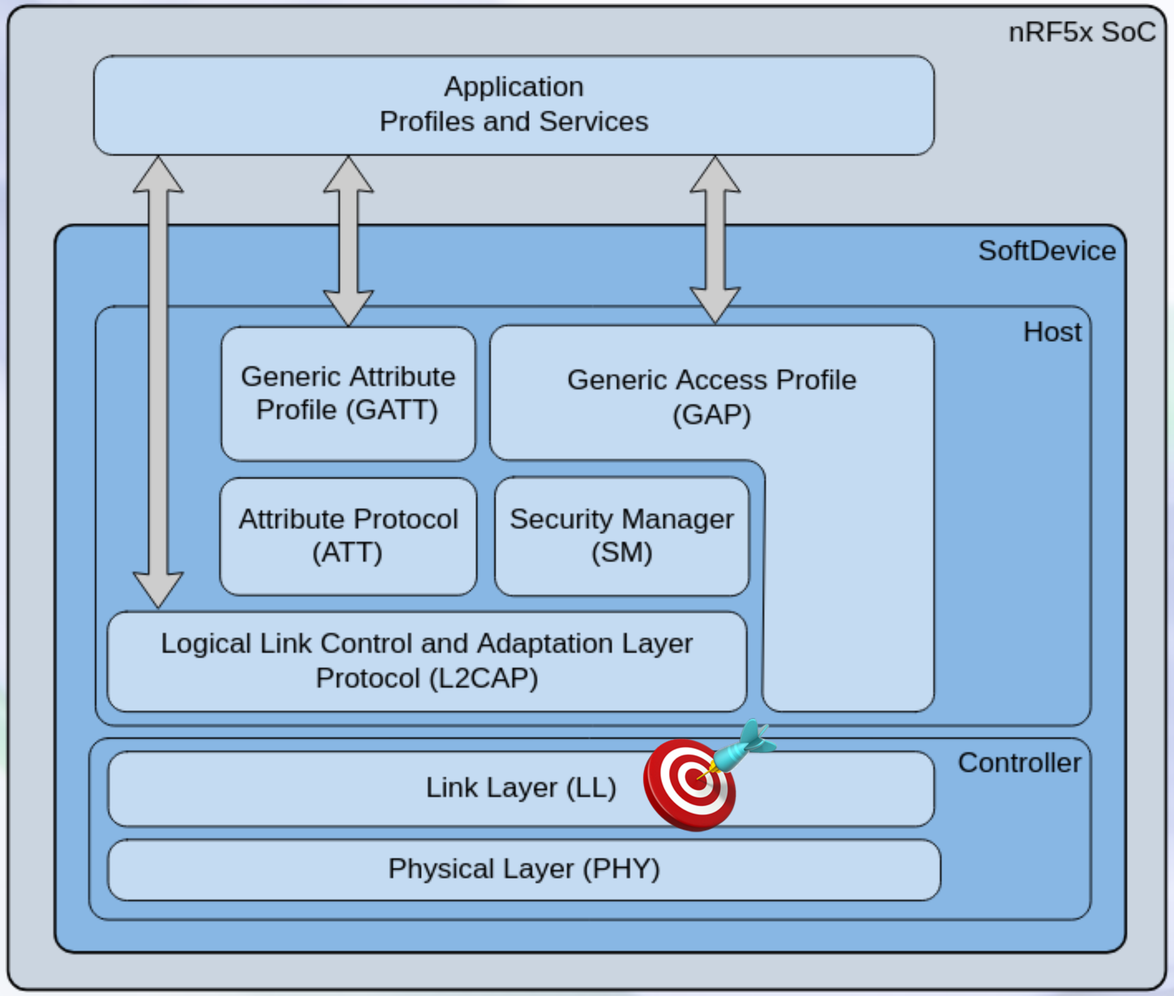


[1] https://infocenter.nordicsemi.com/index.jsp?topic=%2Fsds_s140%2FSDS%2Fs1xx%2Fble_protocol_stack%2Fble_protocol_stack.html
[2] https://crosscontrol.com/manual/Bluetooth%20Documentation/content/bluetooth.html

2thprint by Manufacturer Specific Data 🧘 or 🚶

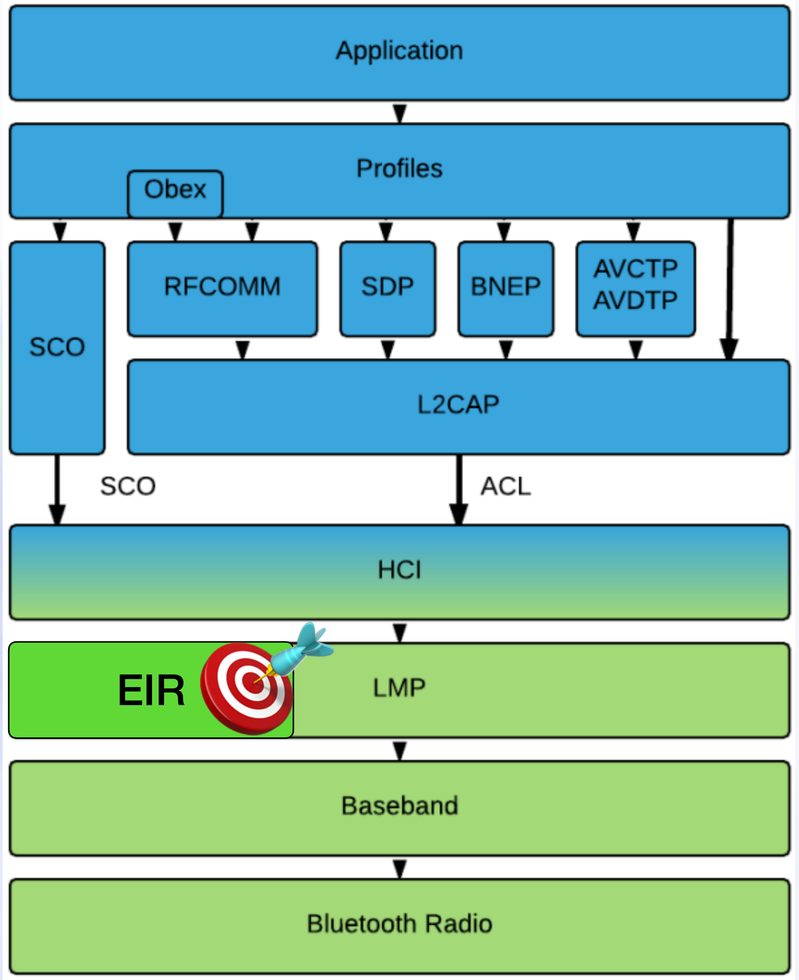
BLE

[1]



BTC

[2]



[1] https://infocenter.nordicsemi.com/index.jsp?topic=%2Fsds_s140%2FSDS%2Fs1xx%2Fble_protocol_stack%2Fble_protocol_stack.html
[2] https://crosscontrol.com/manual/Bluetooth%20Documentation/content/bluetooth.html

2thprint by Manufacturer-Specific Data (MSD):

Company ID (CID)

- BLE Advertisements and BTC Extended Inquiry Response packets can include MSD data where the manufacturer can *mostly* put whatever they want

Data Types Specification

Bluetooth®

1 DATA TYPES DEFINITIONS AND FORMATS

This part defines the basic data types used for Extended Inquiry Response (EIR), Advertising Data (AD), Scan Response Data (SRD), Additional Controller Advertising Data (ACAD), and OOB data blocks. Additional data types may be defined in profile specifications.

Each data type shall only be used in accordance with the requirements specified in Table 1.1.

	Context				
Data type	**EIR**	**AD**	**SRD**	**ACAD**	**OOB**
Service UUID	O	O	O	O	O
Local Name	C.1	C.1	C.1	X	C.1
Flags	C.1	C.1	X	X	C.1
Manufacturer Specific Data	O	O	O	O	O

2thprint by Manufacturer-Specific Data (MSD):

Company ID (CID)

- BLE Advertisements and BTC Extended Inquiry Response packets can include MSD data where the manufacturer can *mostly* put whatever they want

Data Types Specification

Bluetooth®

1 DATA TYPES DEFINITIONS AND FORMATS

This part defines the basic data types used for Extended Inquiry Response (EIR), Advertising Data (AD), Scan Response Data (SRD), Additional Controller Advertising Data (ACAD), and OOB data blocks. Additional data types may be defined in profile specifications.

Each data type shall only be used in accordance with the requirements specified in Table 1.1.

Data type	Context				
	EIR	AD	SRD	ACAD	OOB
Service UUID	O	O	O	O	O
Local Name	C.1	C.1	C.1	X	C.1
Flags	C.1	C.1	X	X	C.1
Manufacturer Specific Data	O	O	O	O	O

2thprint by Manufacturer-Specific Data (MSD):

Company ID (CID)

- They's *supposed* to put their company's assigned number in the first 2 bytes, but not everyone does...

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

2thprint by Manufacturer-Specific Data (MSD):

Company ID (CID)

- They's *supposed* to put their company's assigned number in the first 2 bytes, but not everyone does...

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

2thprint by Manufacturer-Specific Data (MSD):

Company ID (CID)

- They's *supposed* to put their company's assigned number in the first 2 bytes, but not everyone does...
- Also, some put the company ID as little-endian, and some as big-endian, and some use both!

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 Ass Numbers. The interpretation of any other octets within the data shall d by the manufacturer specified by the company identifier.

It doesn't say what endianness it should use!

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

Endianness info from BT Spec 4.0!

Lost in BT Spec 4.2 when they created the Core Specification Supplement doc?

8.1 EIR DATA TYPE DEFINITIONS

This section defines the basic EIR data types. Additional EIR data types may be defined in profile specifications.

All EIR data type values are listed in the Bluetooth Assigned Numbers document.

All numerical multi-byte entities and values associated with the following data types shall use little-endian byte order.

Top 20 Vendors for BTC MSD data

BTC - 2024-01-12

device_BT_CID	company_name	frequency	
0x8700	Garmin International (wrong-endian)	5942	❌
0x4C00	Apple, Inc. (wrong-endian)	2487	🍪
0x1D	Qualcomm	2437	🍪
0xFF19	Samsung Electronics Co. Ltd. (just wacky)	1938	🍪
0xF	Broadcom Corporation	950	🍪
0x75	Samsung Electronics Co. Ltd.	879	🍪
0x7500	Samsung Electronics Co.,Ltd (wrong-endian)	278	🍪
0xD906	Shanghai Mountain View Silicon Co.,Ltd. (wrong-endian)	274	🍪
0x3E0	Actions (Zhuhai) Technology Co., Limited	97	🍪
0x4C	Apple, Inc.	45	🍪
0x27D	HUAWEI Technologies Co., Ltd.	43	❌
0xA	Qualcomm Technologies International, Ltd. (QTIL)	32	🍪
0xA02	Ayxon-Dynamics GmbH	14	❌
0x200	Verifone Systems Pte Ltd. Taiwan Branch	7	❌
0x0	Ericsson AB	7	❌
0xA00	Ampler Bikes OU (wrong-endian Qualcomm?)	6	❌
0x5F0	beken	6	🍪
0x850	Yealink (Xiamen) Network Technology Co.,LTD	5	❌
0x18C	Wilo SE	3	❌
0x67	GN Audio A/S	3	❌

...

Top 20 Vendors for BLE MSD data

BLE - 2024-01-12

device_BT_CID	company_name		frequency
0x4C	Apple, Inc.	🍪	9503999
0x6	Microsoft	❌	94967
0x75	Samsung Electronics Co. Ltd.	🍪	83182
0x11B	Hewlett Packard Enterprise	❌	18899
0x183	Walt Disney	❌	14073
0x3	IBM Corp.	❌	11937
0x87	Garmin International, Inc.	❌	10150
0x131	Cypress Semiconductor	🍪	7872
0x0	Ericsson AB	❌	7547
0x171	Amazon.com Services LLC	❌	6926
0x57	Harman International Industries, Inc.	❌	6424
0x87F	Phillips Connect Technologies LLC	❌	5735
0x12D	Sony Corporation	❌	5265
0xE0	Google	❌	4370
0x310	SGL Italia S.r.l.	❌	3730
0xB01	RESIDEO TECHNOLOGIES, INC.	❌	3608
0xA01	Cleveron AS	❌	3139
0x157	Anhui Huami Information Technology Co., Ltd.	❌	2657
0x65	HP, Inc.	❌	2412
0x4C00	Apple, Inc. (wrong-endian)	🍪	1946

...

2thprint by GATT 🤾*

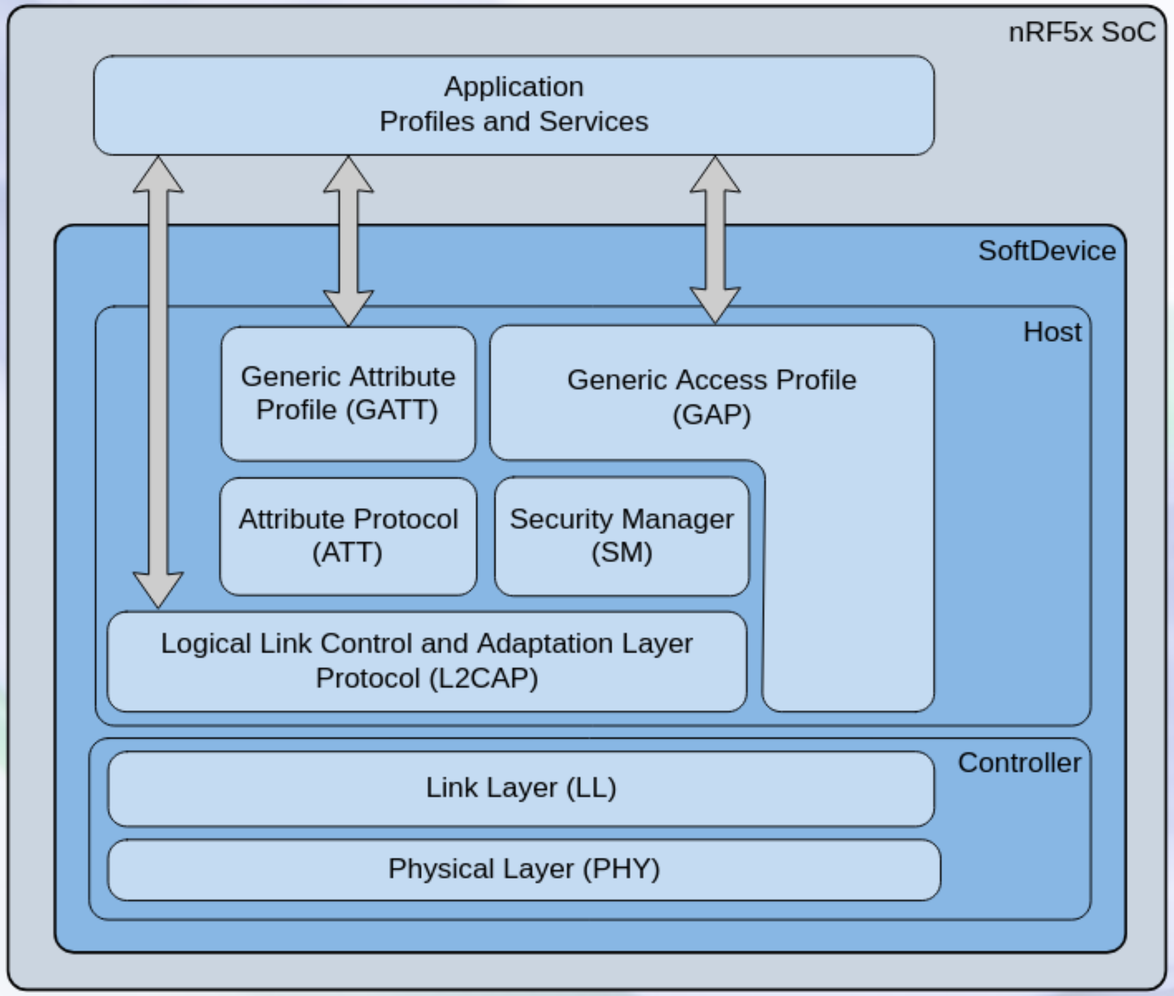
* I would tend to argue though that GATT UUID16/UUID128s included in ADV_IND or SCAN_RSP are passive and semi-passive respectively

2thprint by GATT  *

* I would tend to argue though that GATT UUID16/UUID128s included in ADV_IND or SCAN_RSP are passive and semi-passive respectively

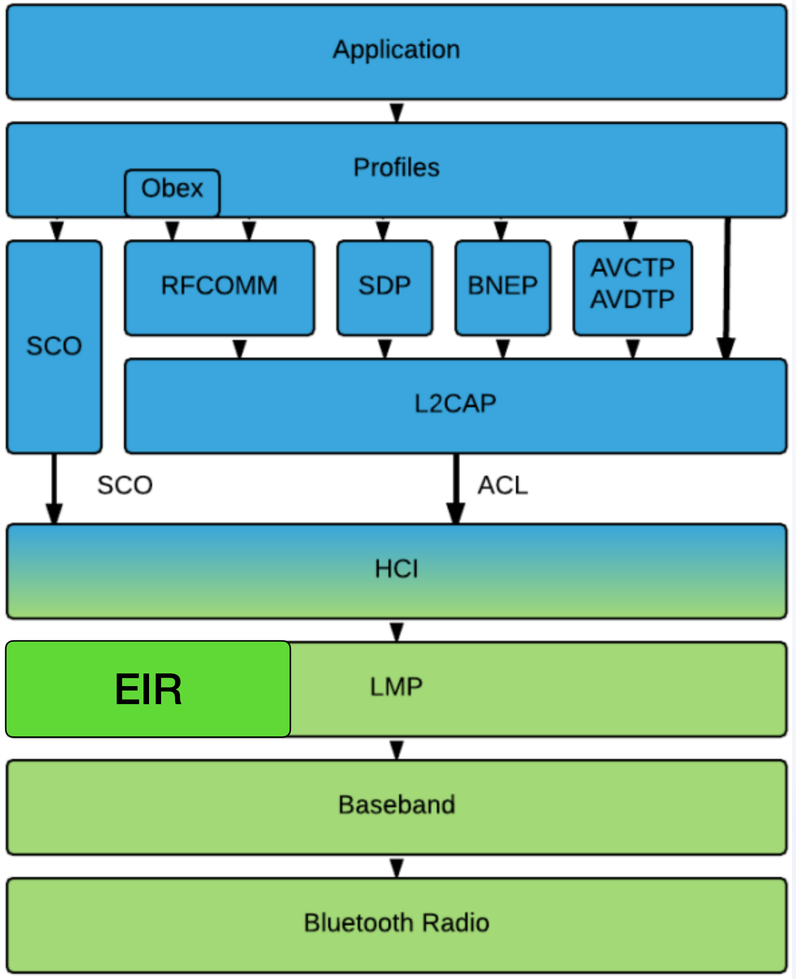
BLE

[1]



BTC

[2]



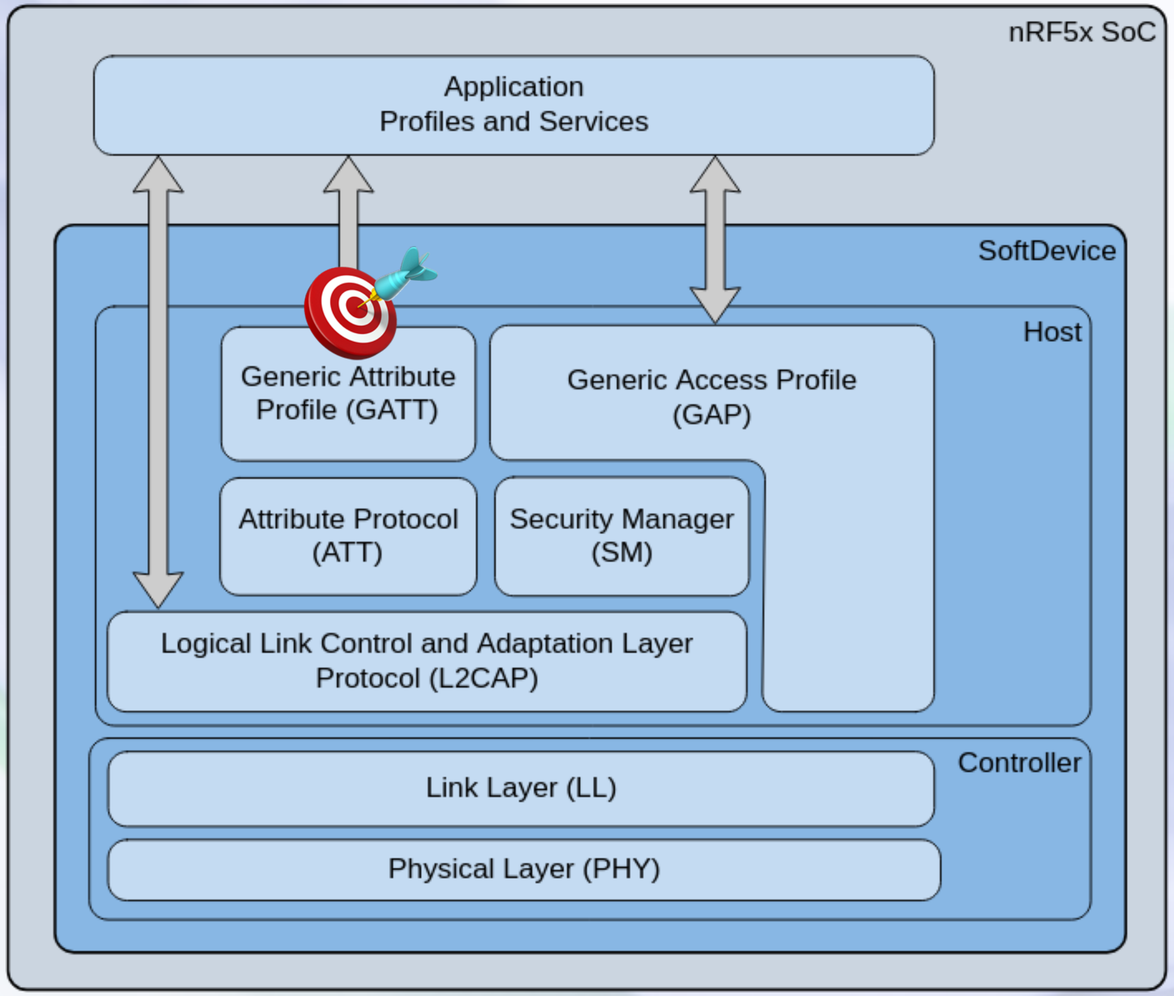
[1] https://infocenter.nordicsemi.com/index.jsp?topic=%2Fsds_s140%2FSDS%2Fs1xx%2Fble_protocol_stack%2Fble_protocol_stack.html
[2] https://crosscontrol.com/manual/Bluetooth%20Documentation/content/bluetooth.html

2thprint by GATT  *

* I would tend to argue though that GATT UUID16/UUID128s included in ADV_IND or SCAN_RSP are passive and semi-passive respectively

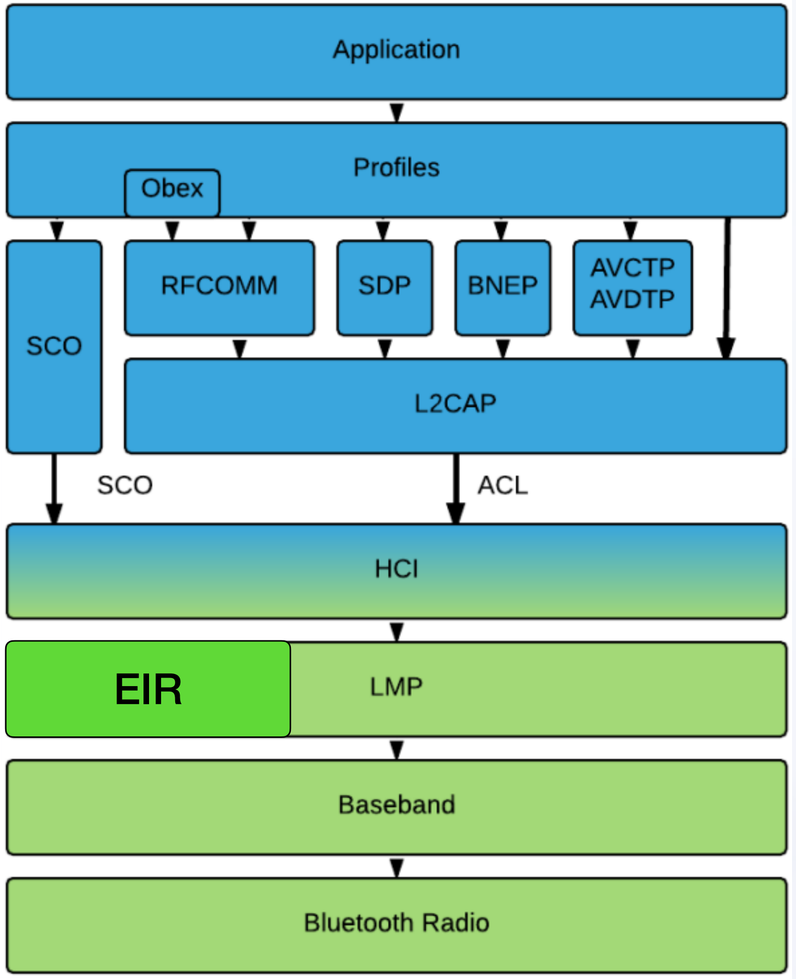
BLE

[1]



BTC

[2]

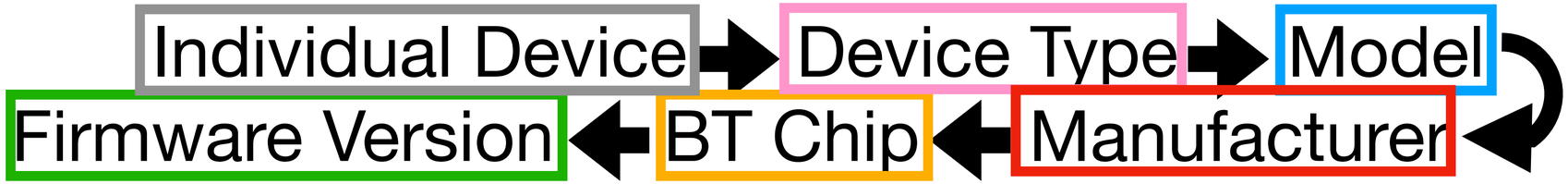


[1] https://infocenter.nordicsemi.com/index.jsp?topic=%2Fsds_s140%2FSDS%2Fs1xx%2Fble_protocol_stack%2Fble_protocol_stack.html
[2] https://crosscontrol.com/manual/Bluetooth%20Documentation/content/bluetooth.html

2thprint by GATT

GATTPrint

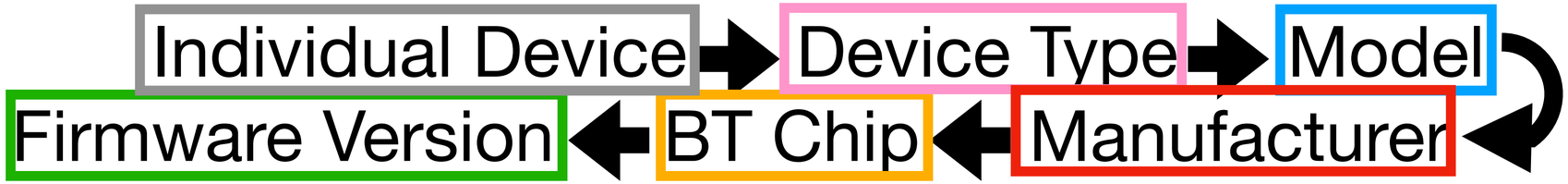
- **G**eneric **Att**ribute *Profile* (GATT) is a sort of weird thing that's built on top of Attribute Protocol (ATT), which is the actual protocol for sending & receiving data
- Mostly used on BLE, though it can technically be used on BTC devices too
- You can *theoretically* get ALL the types of information through GATT!



2thprint by GATT

GATTPrint

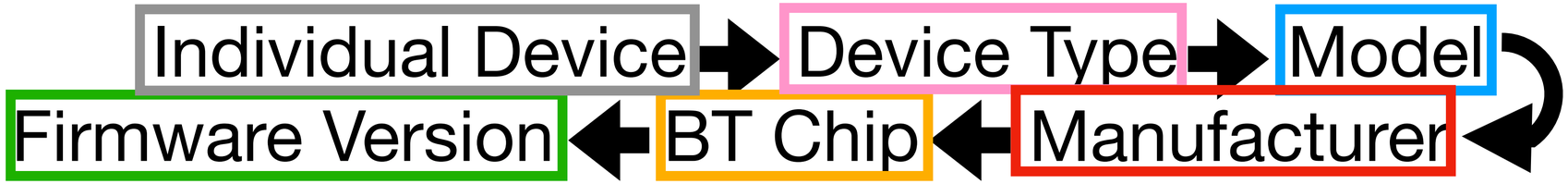
- **G**eneric **Att**ribute *Profile* (GATT) is a sort of weird thing that's built on top of Attribute Protocol (ATT), which is the actual protocol for sending & receiving data
- Mostly used on BLE, though it can technically be used on BTC devices too
- You can *theoretically* get ALL the types of information through GATT!



2thprint by GATT

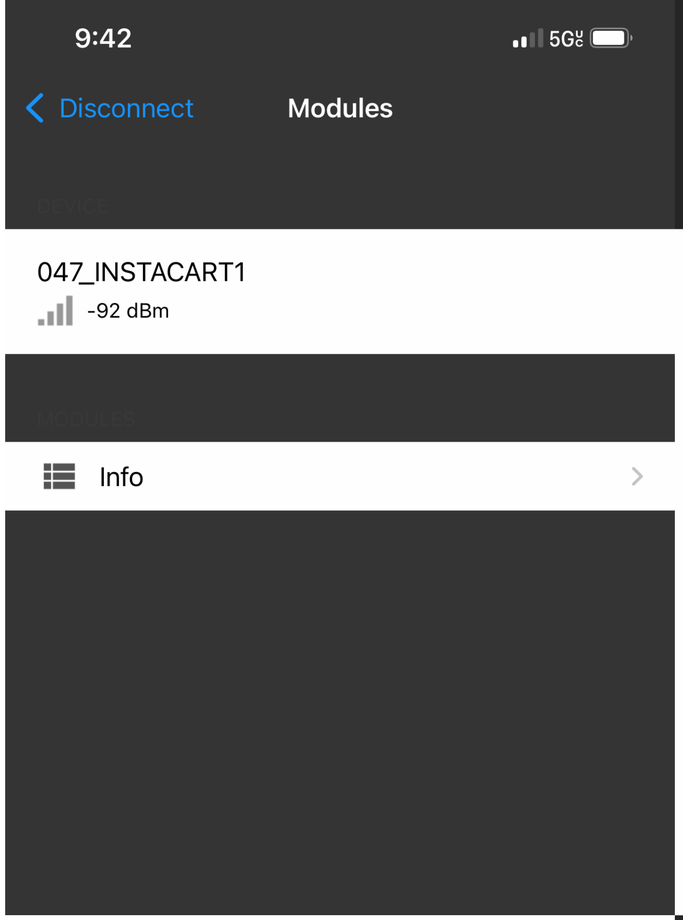
GATTPrint

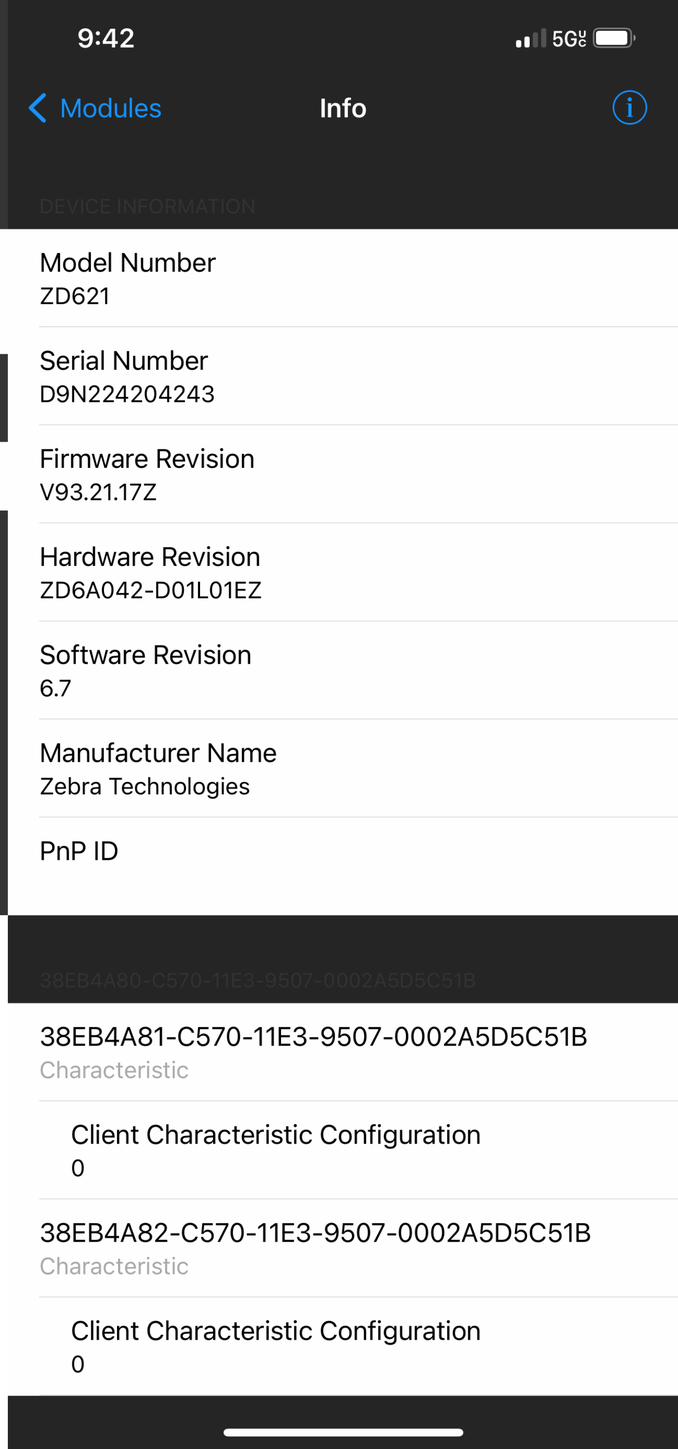
- **G**eneric **Att**ribute *Profile* (GATT) is a sort of weird thing that's built on top of Attribute Protocol (ATT), which is the actual protocol for sending & receiving data
- Mostly used on BLE, though it can technically be used on BTC devices too
- You can *theoretically* get ALL the types of information through GATT!



GATT on Phones

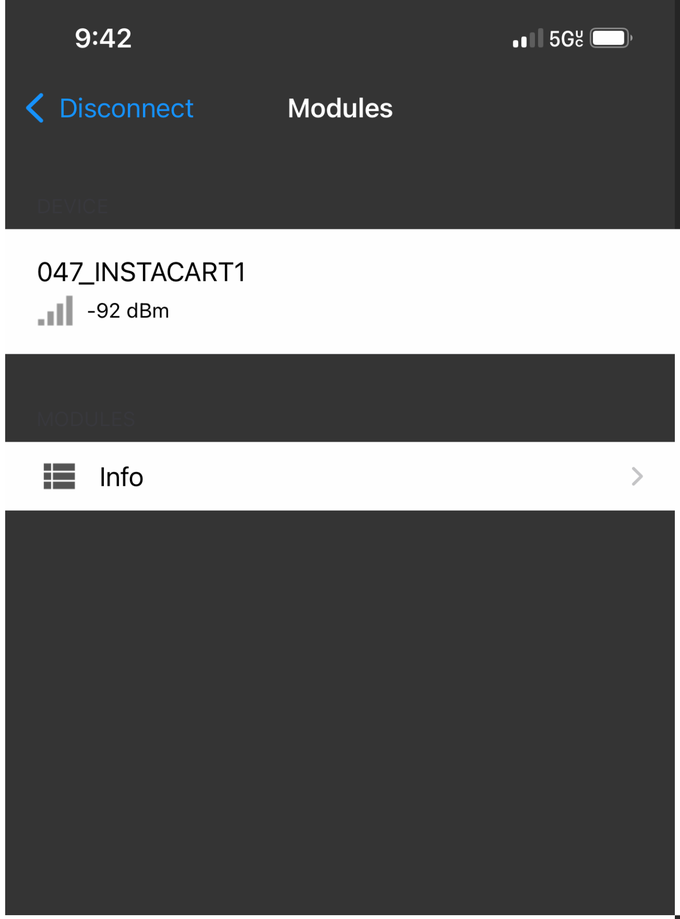
- When you open a Bluetooth scanner app like LightBlue or BluefruitConnect on your phone, and they show you information, usually that is GATT information
- This is from BluefruitConnect

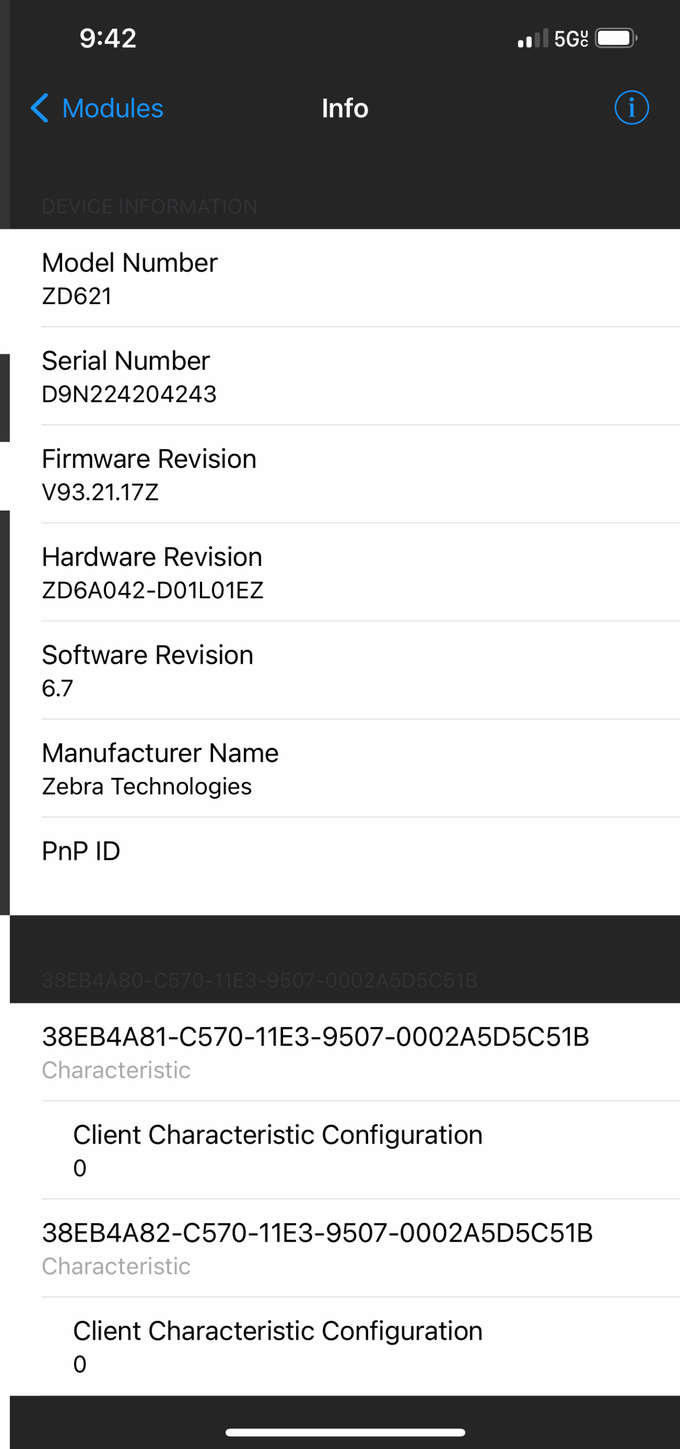




GATT on Phones

- When you open a Bluetooth scanner app like LightBlue or BluefruitConnect on your phone, and they show you information, usually that is GATT information
- This is from BluefruitConnect

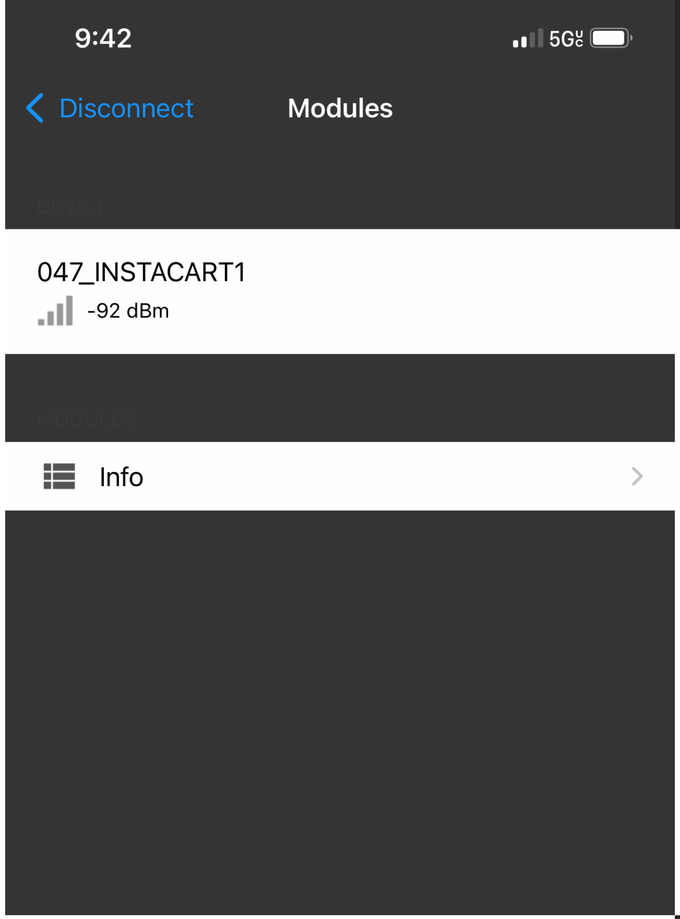


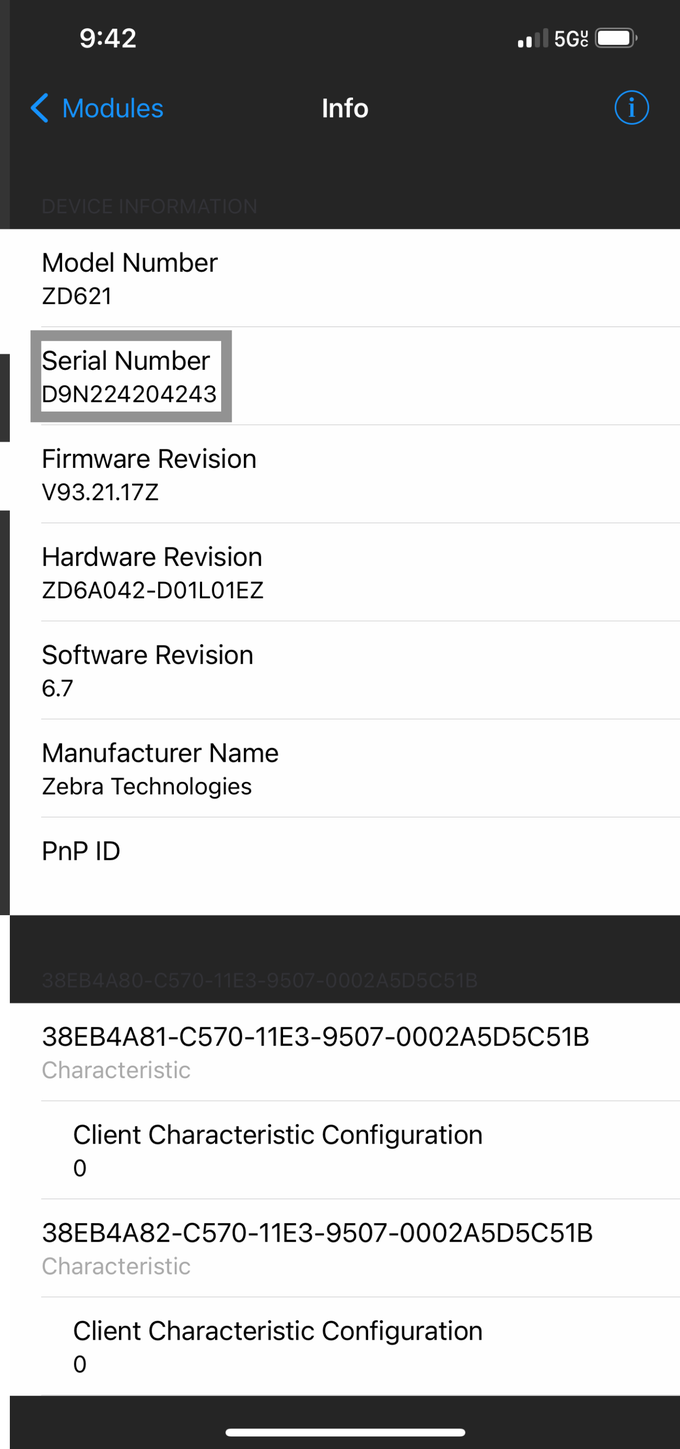


Individual Device → Device Type → Model → Manufacturer → BT Chip → Firmware Version

GATT on Phones

- When you open a Bluetooth scanner app like LightBlue or BluefruitConnect on your phone, and they show you information, usually that is GATT information
- This is from BluefruitConnect

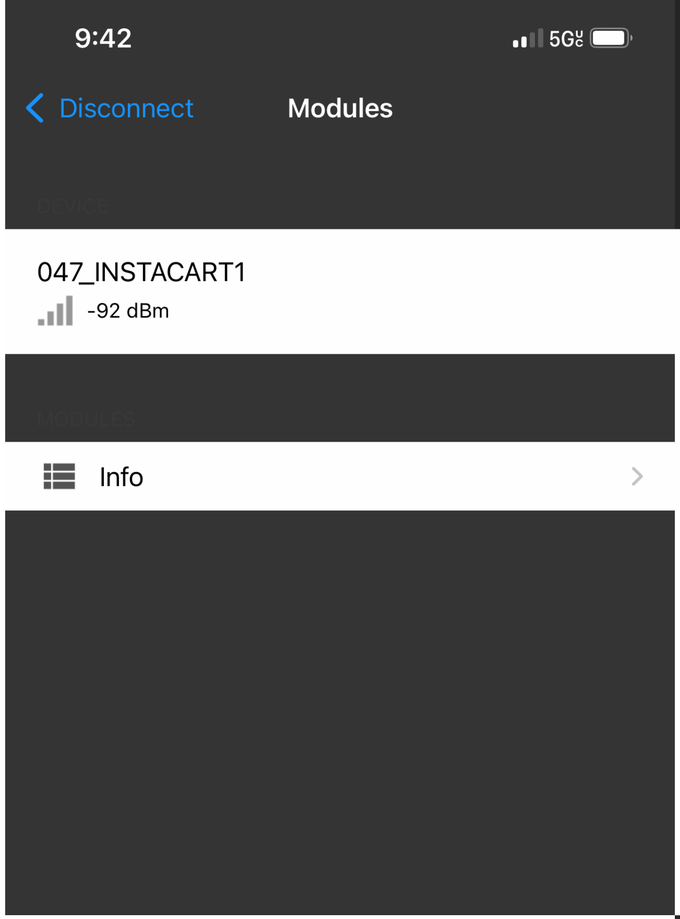


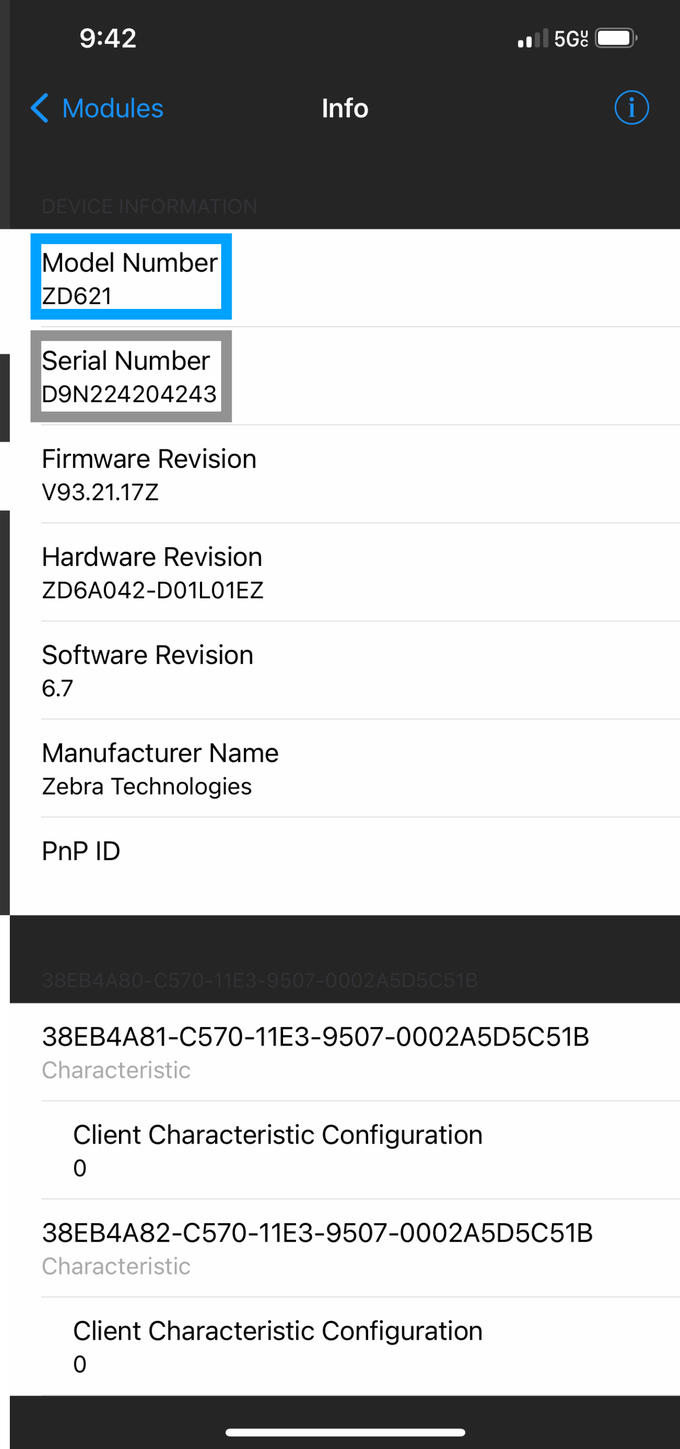


Individual Device → Device Type → Model → Manufacturer → BT Chip → Firmware Version

GATT on Phones

- When you open a Bluetooth scanner app like LightBlue or BluefruitConnect on your phone, and they show you information, usually that is GATT information
- This is from BluefruitConnect

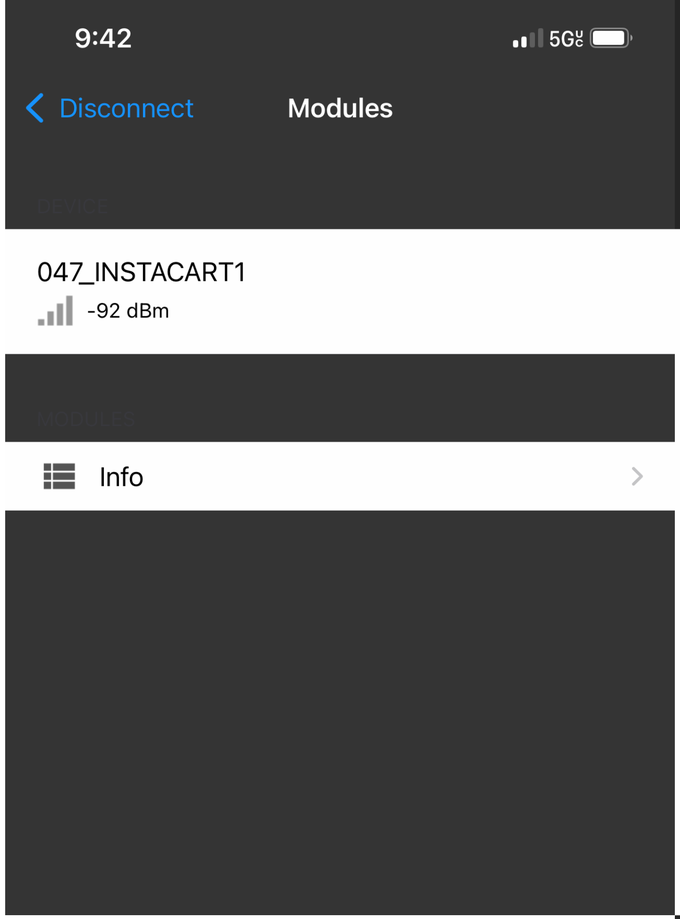


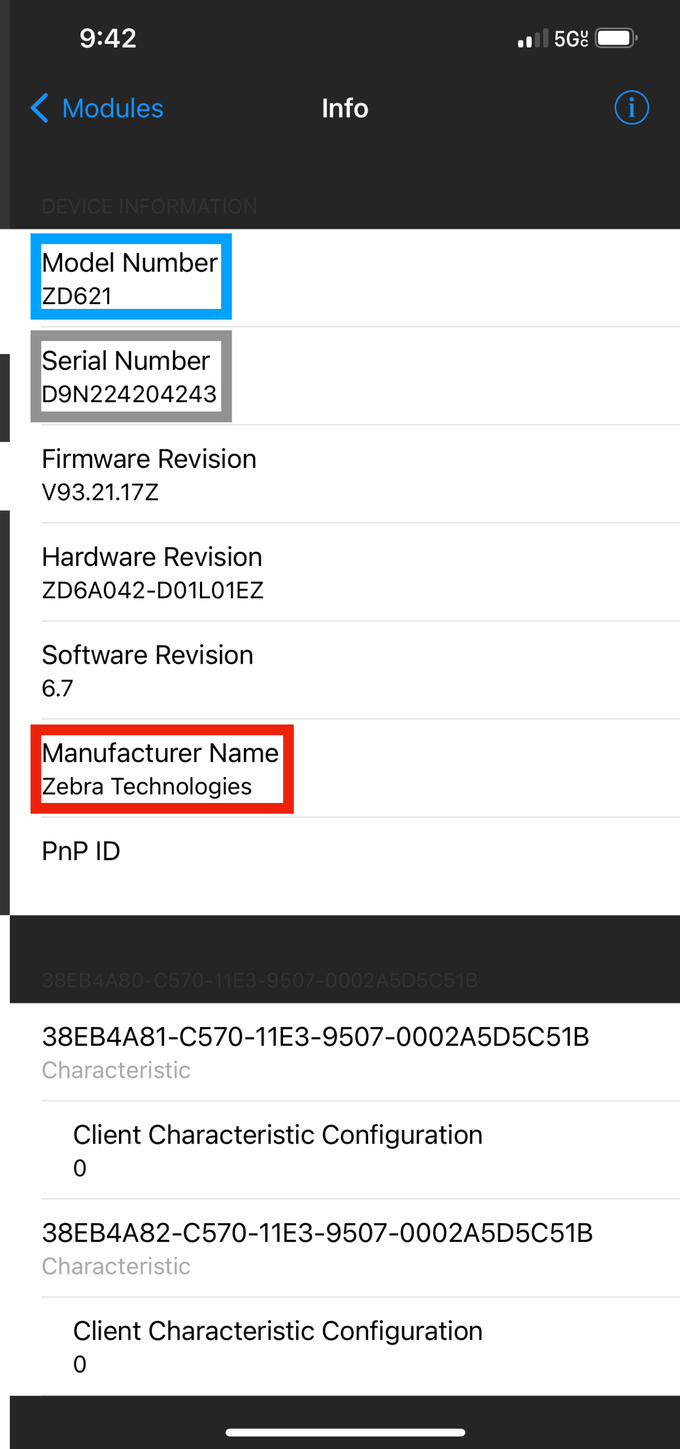


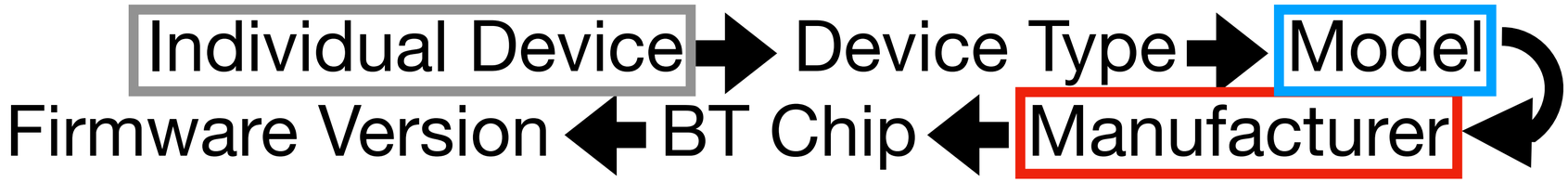
Individual Device → Device Type → Model → Manufacturer → BT Chip → Firmware Version

GATT on Phones

- When you open a Bluetooth scanner app like LightBlue or BluefruitConnect on your phone, and they show you information, usually that is GATT information
- This is from BluefruitConnect

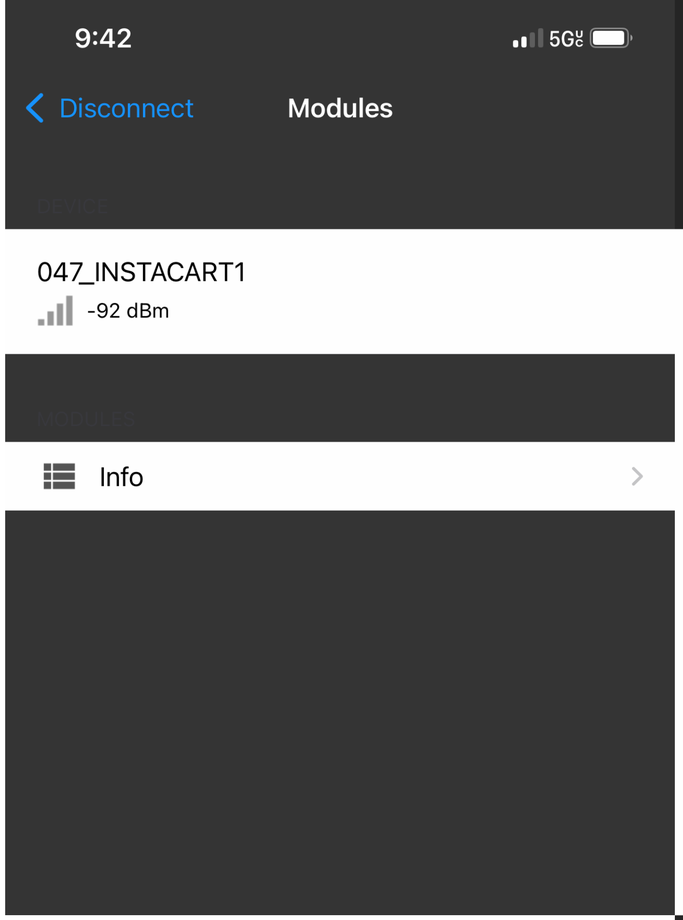


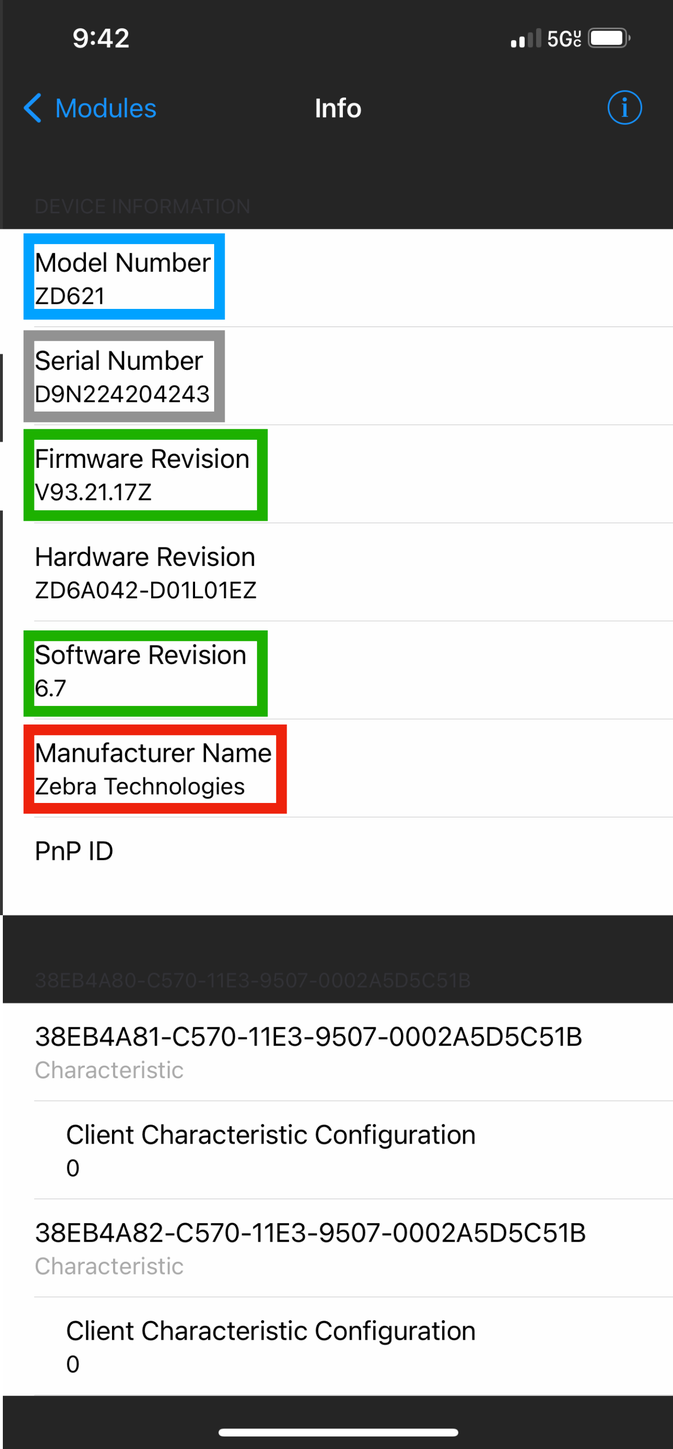


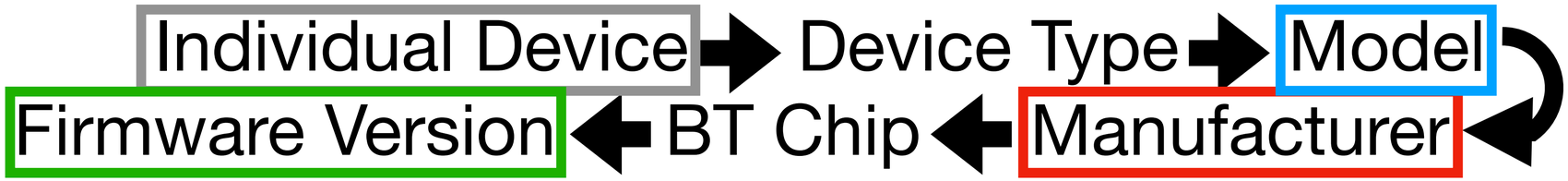


GATT on Phones

- When you open a Bluetooth scanner app like LightBlue or BluefruitConnect on your phone, and they show you information, usually that is GATT information
- This is from BluefruitConnect

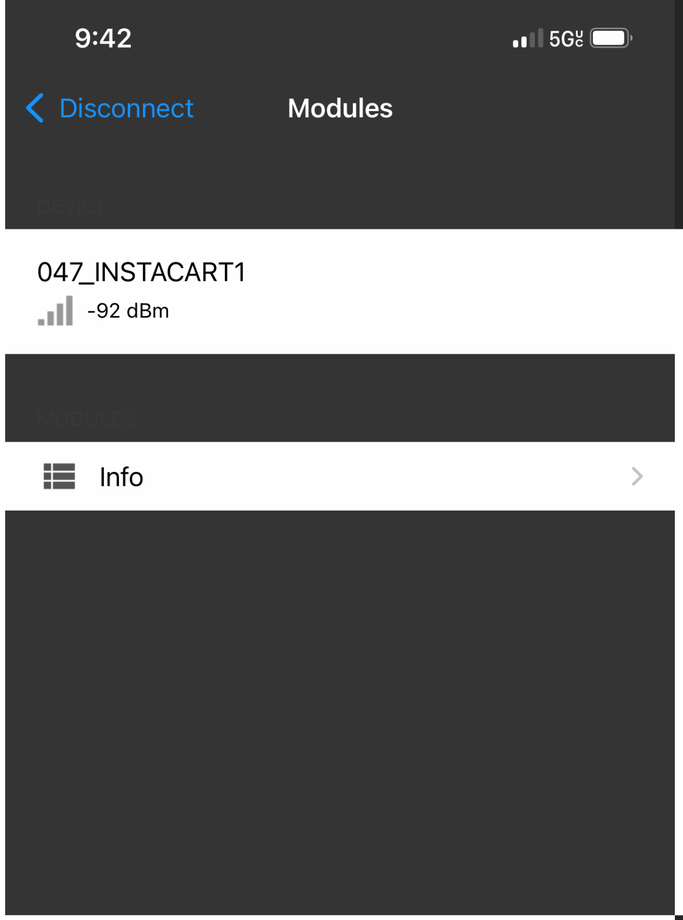


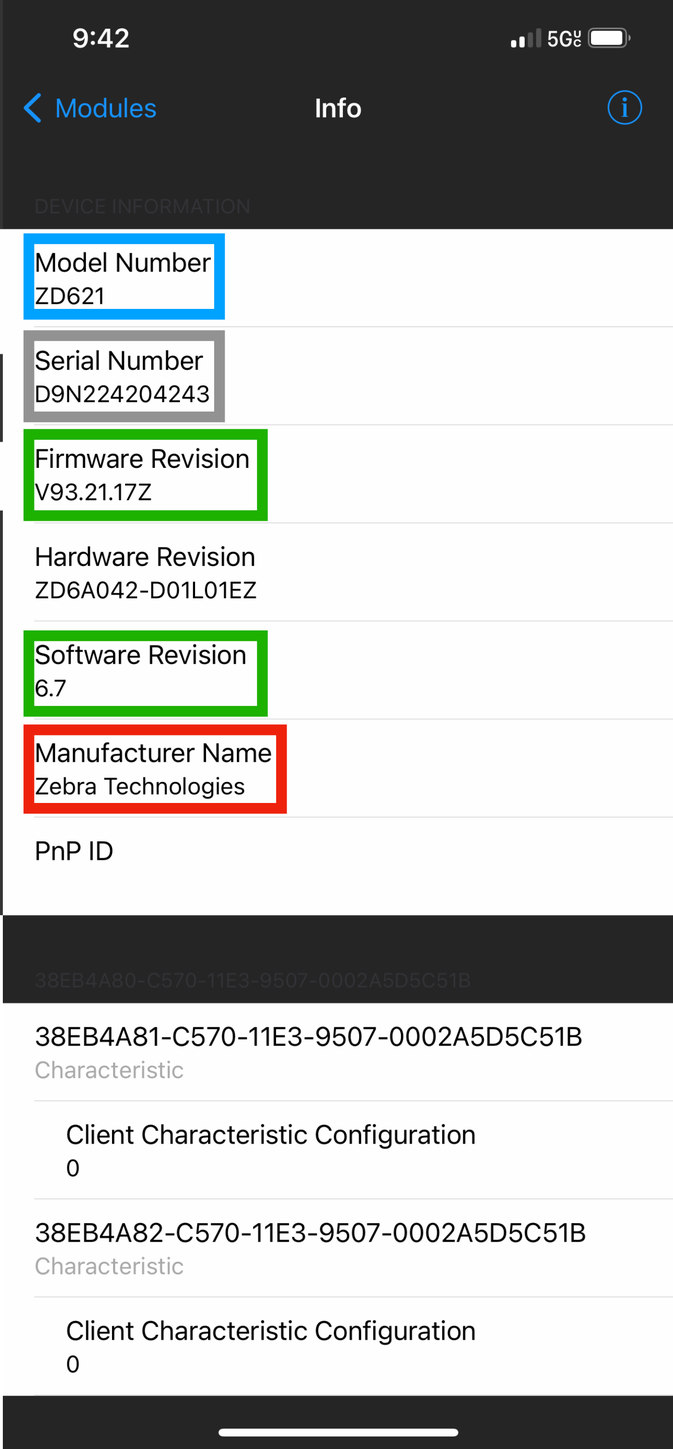


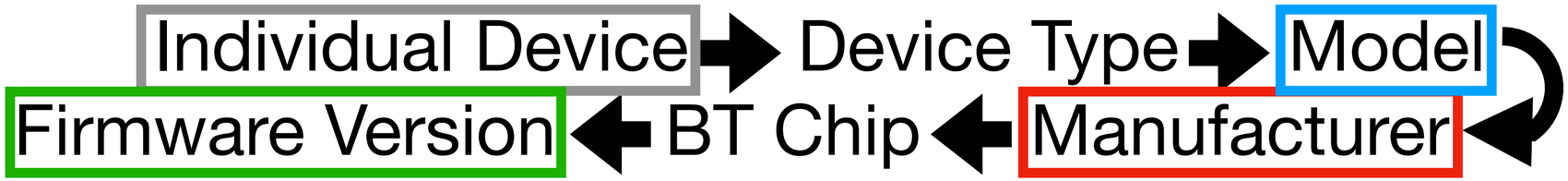


GATT on Phones

- When you open a Bluetooth scanner app like LightBlue or BluefruitConnect on your phone, and they show you information, usually that is GATT information
- This is from BluefruitConnect

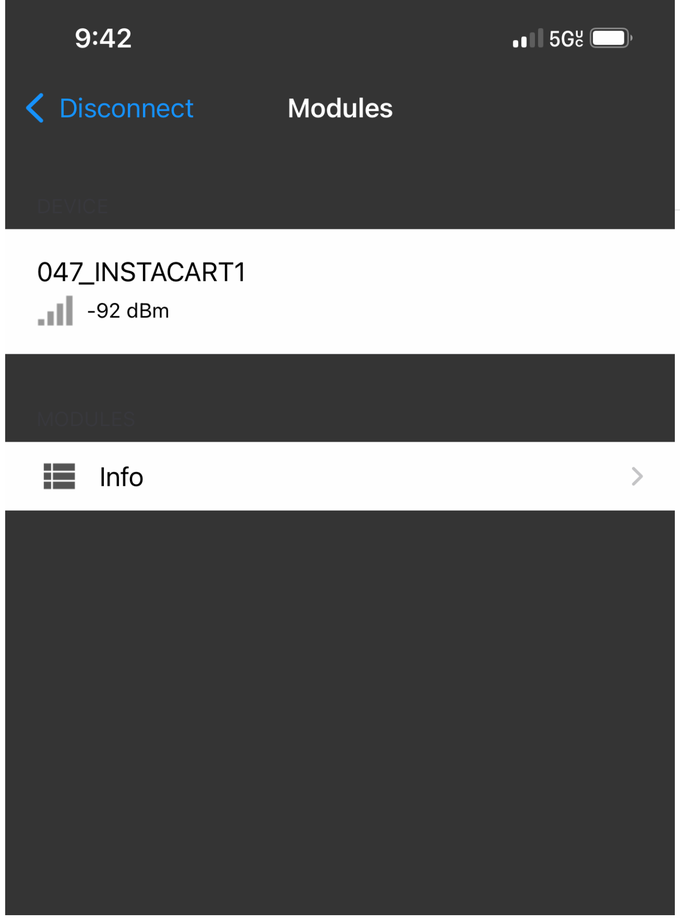


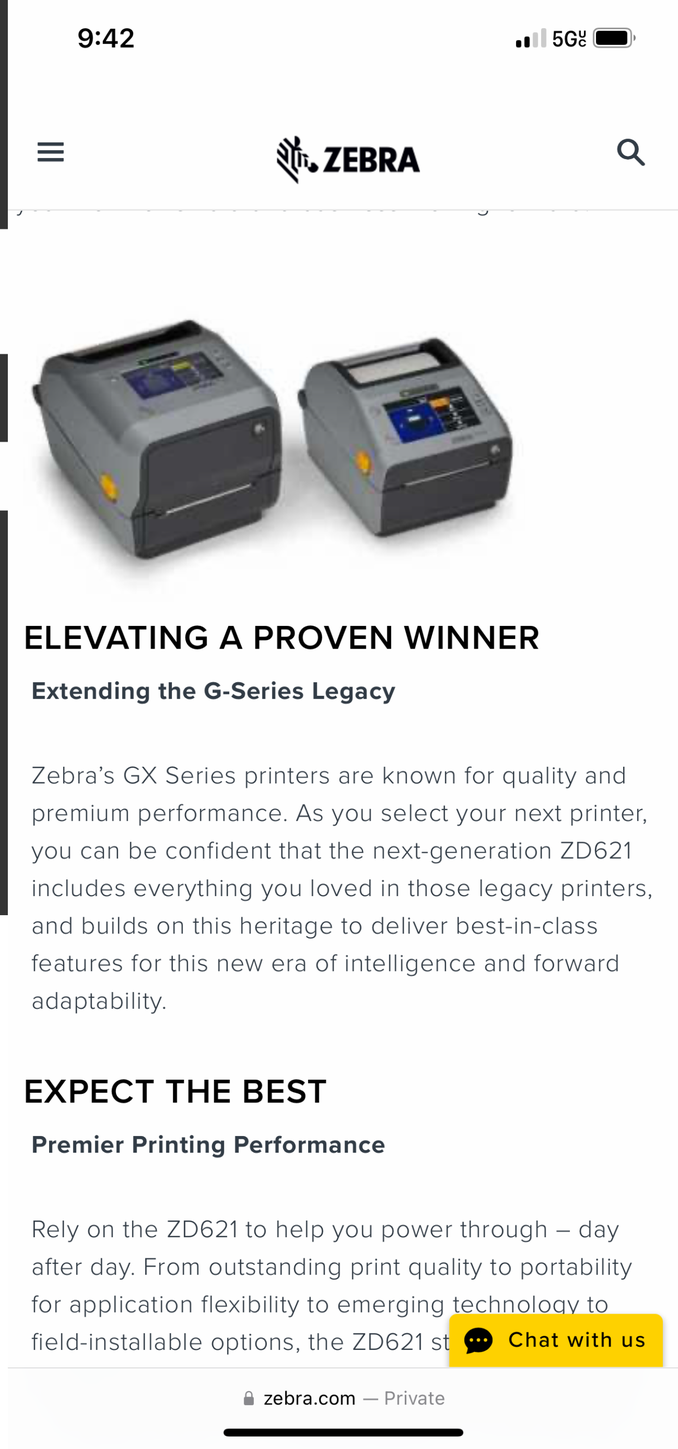


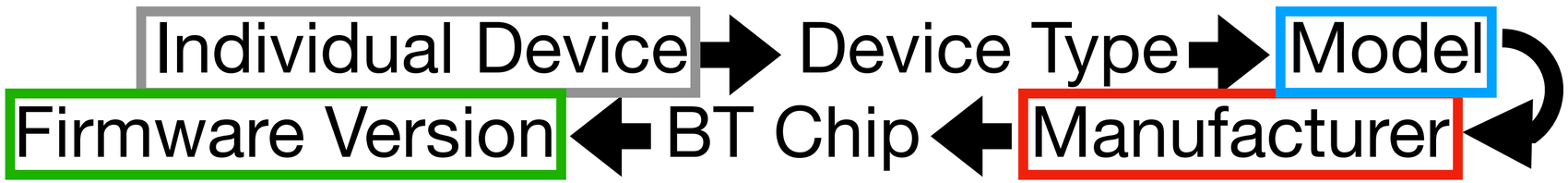


GATT on Phones

- When you open a Bluetooth scanner app like LightBlue or BluefruitConnect on your phone, and they show you information, usually that is GATT information
- This is from BluefruitConnect

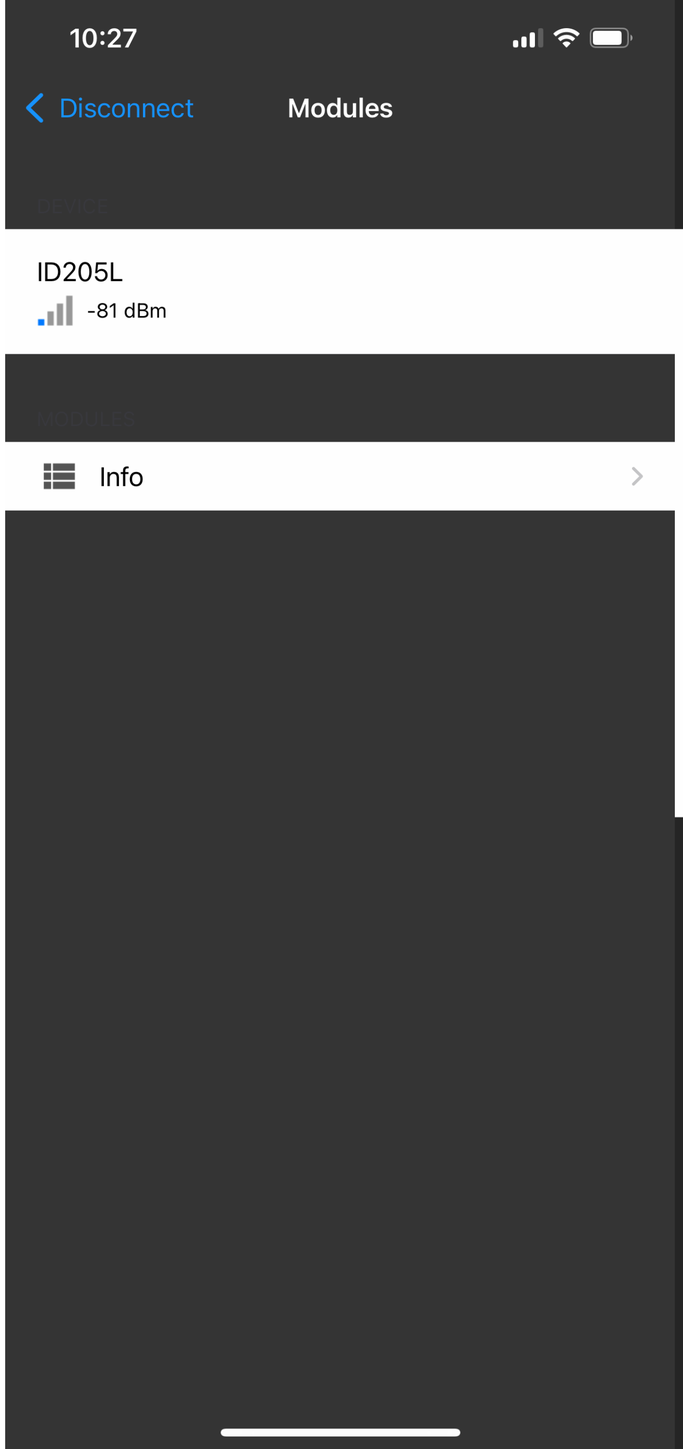


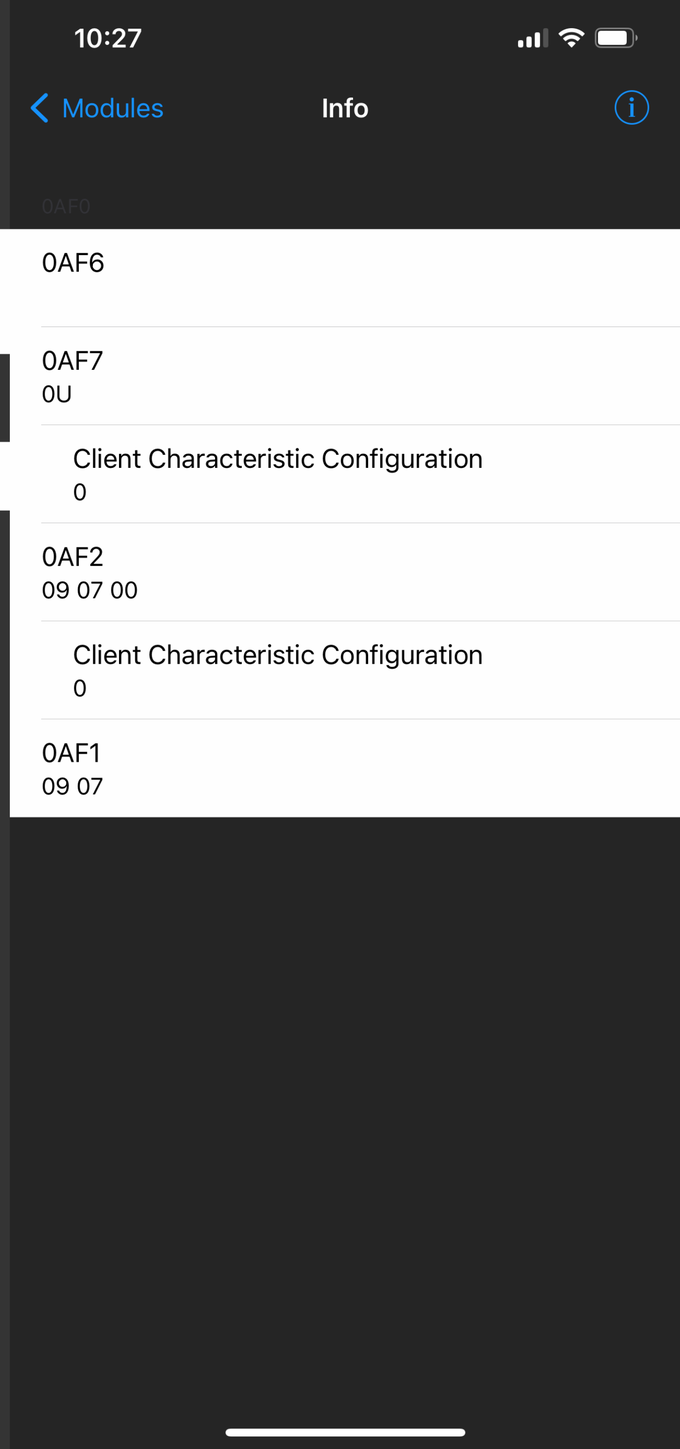




GATT in General

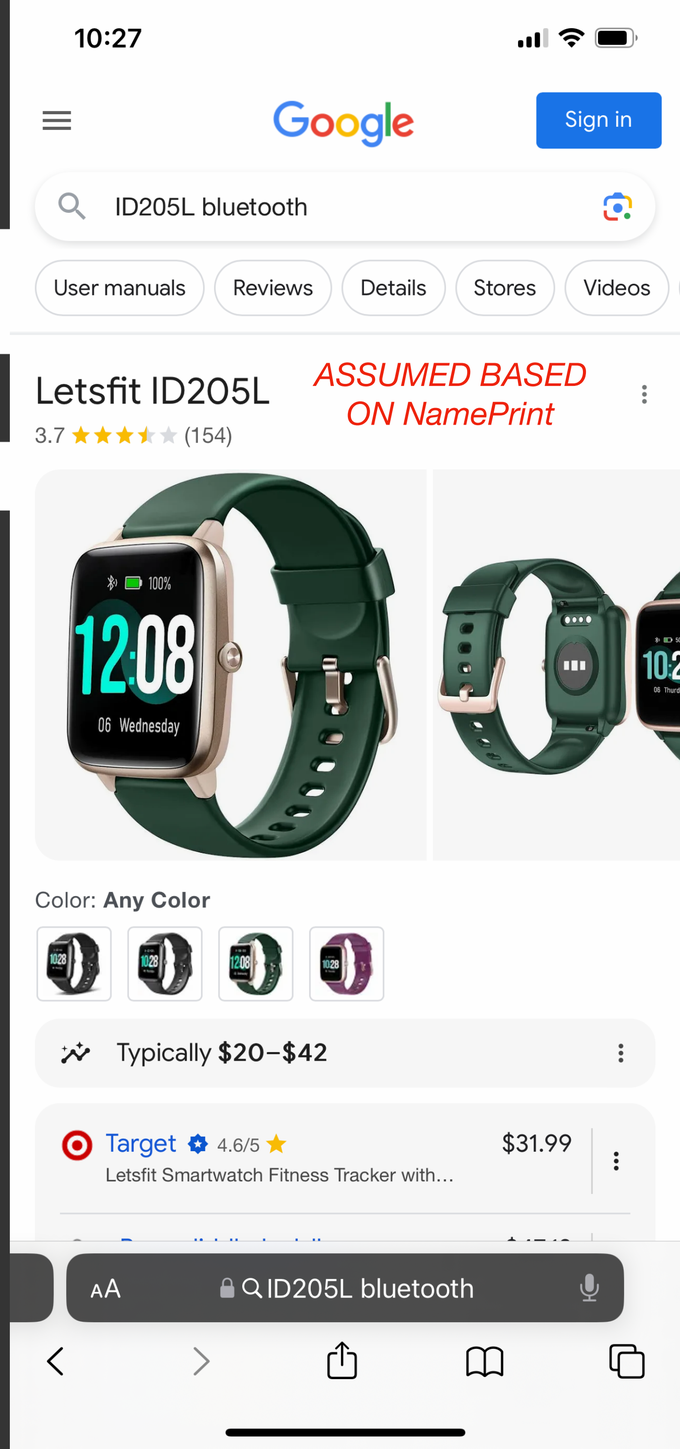
- On the *OTHER* hand...we may instead get a whole bunch of *nothing useful* from GATT
- Devices may not respond to GATT requests, and when they do, we're in no way guaranteed to get "characteristics" which contain the kind of information we want
  - GATT inquiries can take a few seconds. For moving targets, there is a low probability of success to perform a full information collection without a strong transmitter and good antenna





GATT in General

- On the *OTHER* hand...we may instead get a whole bunch of *nothing useful* from GATT
- Devices may not respond to GATT requests, and when they do, we're in no way guaranteed to get "characteristics" which contain the kind of information we want
  - GATT inquiries can take a few seconds. For moving targets, there is a low probability of success to perform a full information collection without a strong transmitter and good antenna



Prior Work

"Fingerprinting Bluetooth-Low-Energy Devices Based on the Generic Attribute Profile"

- [1] by Celosia & Cunche from 2019 connected 🤸 to BLE devices via GATT and just called *all the returned information* the fingerprint
  - Noteworthy, in my mind, for the different threat model (user privacy), that called out basically everything *except* firmware revision string as interesting

> We identified that information found in GATT profiles can be used to infer the following information: **device type**, **device model**, **device manufacturer** and **user's name**. All this information can threaten the privacy of the device owner.

[1] https://inria.hal.science/hal-02359914/file/paper.pdf

Prior Work

"Fingerprinting Bluetooth-Low-Energy De **Prof**

- [1] by Celosia & Cunche from 2019 connected 🕺 to BLE devices via GATT and just called *all the returned information* the fingerprint
  - Noteworthy, in my mind, for the different threat model (user privacy), that called out basically everything *except* firmware revision string as interesting

> We identified that information found in GATT profiles can be used to infer the following information: **device type**, **device model**, **device manufacturer** and **user's name**. All this information can threaten the privacy of the device owner.

[1] https://inria.hal.science/hal-02359914/file/paper.pdf

Table 4: Average time to collect a GATT profile among different devices.

Device type	Device	Time (sec)
Lightbulb	Osram Smart+	6.531
Motion sensor	Eve Motion	6.468
Socket outlet	Eve Energy	5.919
Smartphone	Apple iPhone 8	4.354
Smartphone	Apple iPhone 6	4.259
Keyring	Nut	4.148
TV dongle	Google Chromecast	3.660
Fitness wristband	Fitbit Inspire	3.231
Presentation remote	Logitech Spotlight	2.860
Smartwatch	Apple Watch Series 3	2.853
Heart rate monitor	Polar H7	2.751
Fitness wristband	Fitbit Flex	2.552
Headset	Bose SoundLink Around-Ear II	2.181
Speaker	Divacore Ktulu2+	1.742
Keyring	Chipolo	1.426
	Average	3.662

[1] https://inria.hal.science/hal-02359914/file/paper.pdf

Table 4: Average time to collect a GATT profile among different devices.

Device type	Device	Time (sec)
Lightbulb	Osram Smart+	6.531
Motion sensor	Eve Motion	6.468
Socket outlet	Eve Energy	5.919
Smartphone	Apple iPhone 8	4.354
Smartphone	Apple iPhone 6	4.259
Keyring	Nut	4.148
TV dongle	Google Chromecast	3.660
Fitness wristband	Fitbit Inspire	3.231
Presentation remote	Logitech Spotlight	2.860
Smartwatch	Apple Watch Series 3	2.853
Heart rate monitor	Polar H7	2.751
Fitness wristband	Fitbit Flex	2.552
	ound-Ear II	2.181
		1.742
		1.426
		3.662

I've seen things take up to 24 seconds to reply to GATTprinting...

[1] https://inria.hal.science/hal-02359914/file/paper.pdf

Table 4: Average time to collect a GATT profile among different devices.

Device type	Device	Time (sec)
Lightbulb	Osram Smart+	6.531
Motion sensor	Eve Motion	6.468
Socket outlet	Eve Energy	5.919
Smartphone	Apple iPhone 8	4.354
Smartphone	Apple iPhone 6	4.259
Keyring	Nut	4.148
TV dongle	Google Chromecast	3.660
Fitness wristband	Fitbit Inspire	3.231
Presentation remote	Logitech Spotlight	2.860
Smartwatch	Apple Watch Series 3	2.853
Heart rate monitor	Polar H7	2.751
Fitness wristband	Fitbit Flex	2.552
	ound-Ear II	2.181
		1.742
		1.426
		3.662

I've seen things take up to 24 seconds to reply to GATTprinting...

[1] https://inria.hal.science/hal-02359914/file/paper.pdf

	All	
	%	#
Device Name	99.49	13182
Appearance	99.48	13082
Service Changed	0.02	2
Manufacturer Name String	99.48	9177
Model Number String	99.36	9158
Battery Level	2.45	191
Current Time	0.41	31
Peripheral Preferred Connection Parameters	99.90	1051
Software Revision String	97.04	1017
Hardware Revision String	95.95	996
Serial Number String	97.12	979
Firmware Revision String	94.99	835

[1] https://inria.hal.science/hal-02359914/file/paper.pdf

	All	
	%	#
Device Name	99.49	13182
Appearance	99.48	13082
Service Changed	0.02	2
Manufacturer Name String	99.48	9177
Model Number String	99.36	9158
Battery Level	2.45	191
Current Time	0.41	31
Peripheral Preferred Connection Parameters	99.90	1051
Software Revision String	97.04	1017
Hardware Revision String	95.95	996
Serial Number String	97.12	979
Firmware Revision String	94.99	835

At least 13182 devices reported a Name (and it was readable 99.49% of the time)

[1] https://inria.hal.science/hal-02359914/file/paper.pdf

	All	
	%	#
Device Name	99.49	13182
Appearance	99.48	13082
Service Changed	0.02	2
Manufacturer Name String	99.48	9177
Model Number String	99.36	9158
Battery Level	2.45	191
Current Time	0.41	31
Peripheral Preferred Connection Parameters	99.90	1051
Software Revision String	97.04	1017
Hardware Revision String	95.95	996
Serial Number String	97.12	979
Firmware Revision String	94.99	835

At least 13182 devices reported a Name (and it was readable 99.49% of the time)

Only 835 devices reported a Firmware Revision String! (and it was readable 94.49% of the time)

[1] https://inria.hal.science/hal-02359914/file/paper.pdf

	All	
	%	#
Device Name	99.49	13182
Appearance	99.48	13082
Service Changed	0.02	2
Manufacturer Name String	99.48	9177
Model Number String	99.36	9158
Battery Level	2.45	191
Current Time	0.41	31
Peripheral Preferred Connection Parameters	99.90	1051
Software Revision String	97.04	1017
Hardware Revision String	95.95	996
Serial Number String	97.12	979
Firmware Revision String	94.99	835

At least 13182 devices reported a Name (and it was readable 99.49% of the time)

Only 835 devices reported a Firmware Revision String! (and it was readable 94.49% of the time)

Note: Their dataset is heavily skewed by containing at least 9924 iPhones, and iPhones don't report a Firmware Revision String

[1] https://inria.hal.science/hal-02359914/file/paper.pdf

	All	
	%	#
Device Name	99.49	13182
Appearance	99.48	13082
Service Changed	0.02	2
Manufacturer Name String	99.48	9177
Model Number String	99.36	9158
Battery Level	2.45	191
Current Time	0.41	31
Peripheral Preferred Connection Parameters	99.90	1051
Software Revision String	97.04	1017
Hardware Revision String	95.95	996
Serial Number String	97.12	979
Firmware Revision String	94.99	835

At least 13182 devices reported a Name (and it was readable 99.49% of the time)

Only 835 devices reported a Firmware Revision String! (and it was readable 94.49% of the time)

Note: Their dataset is heavily skewed by containing at least 9924 iPhones, and iPhones don't report a Firmware Revision String

[1] https://inria.hal.science/hal-02359914/file/paper.pdf

	All	
	%	#
Device Name	99.49	13182
Appearance	99.48	13082
Service Changed	0.02	2
Manufacturer Name String	99.48	9177
Model Number String	99.36	9158
Battery Level	2.45	191
Current Time	0.41	31
Peripheral Preferred Connection Parameters	99.90	1051
Software Revision String	97.04	1017
Hardware Revision String	95.95	996
Serial Number String	97.12	979
Firmware Revision String	94.99	835

At least 13182 devices reported a Name (and it was readable 99.49% of the time)

Only 835 devices reported a Firmware Revision String! (and it was readable 94.49% of the time)

Note: Their dataset is heavily skewed by containing at least 9924 iPhones, and iPhones don't report a Firmware Revision String

[1] https://inria.hal.science/hal-02359914/file/paper.pdf

Prior Work

"Automatic Fingerprinting of Vulnerable BLE IoT Devices with Static UUIDs from Mobile Apps"

- [1] by Zuo et al. from 2019 scanned 🚶 BLE devices via Generic Attribute Profile (GATT) and just called all the top level UUID128s the fingerprint
  - Here they were referring to more like a "device-*model*" fingerprint, not "individual-device" fingerprint
  - Same basic idea as Celosia & Cunche 2019, but they claimed they only did passive scanning for what was advertised, and they didn't connect ❌ to devices and request the GATT information for "ethical reasons" (Which I don't buy. More like CYA.)
  - Most interestingly, they scraped a bunch of Android applications to attempt to extract GATT-related UUID128s via static analysis

[1] https://web.cse.ohio-state.edu/~lin.3021/file/CCS19a.pdf

My GATTPrint-er

- The BlueZ *(deprecated)* "gatttool" seemed to already do a good job of collecting this information. But the output wasn't easily machine-parsable. So I modified the source to store info to a more easily machine-parsable log file
  - Pro tip: If you try to use the higher-layer BT APIs (such as those available via most Python->BT libraries), you will not be able to collect this info without first pairing. But pairing isn't actually necessary for most characteristics of most devices!
    - Some devices though may refuse read/write requests on access control grounds, due to lack of the encryption/authentication that comes as a result of pairing

Vendor-specific 128-bit UUIDs

🍪Silicon-specific examples: Texas Instruments

- f000ffc**0**-0451-4000-b000-000000000000 - **OTA Firmware update** GATT Service
  - f000ffc**1**-0451-4000-b000-000000000000, f000ffc**2**-0451-4000-b000-000000000000, f000ffc**3**-0451-4000-b000-000000000000, f000ffc**4**-0451-4000-b000-000000000000 - Associated GATT Characteristics
- BleedingBit exploited an Aruba-customized TI OTA firmware update service (that just added some security-by-obscurity magic unlock code)

https://software-dl.ti.com/lprf/simplelink_cc2640r2_sdk/1.35.00.33/exports/docs/ble5stack/ble_user_guide/html/oad/oad_concepts.html#oad-service-0xffc0

Vendor-specific 128-bit UUIDs

🍪Silicon-specific examples: Nordic

- 6e400001-b5a3-f393-e0a9-e50e24dcca9e - **UART** GATT Service (advertised in SCAN_RSP as well as GATT)
  - 6e400002-b5a3-f393-e0a9-e50e24dcca9e - UART RX GATT Characteristic
  - 6e400003-b5a3-f393-e0a9-e50e24dcca9e - UART TX GATT Characteristic
- 00001530-1212-efde-1523-785feabcd123 - **"Legacy" (Insecure) Device Firmware Update (DFU)** GATT Service
  - 00001531-1212-efde-1523-785feabcd123, 00001532-1212-efde-1523-785feabcd123, 0000153-1212-efde-1523-785feabcd123 - Associated GATT Characteristics
- 0000fe59-0000-1000-8000-00805f9b34fb - **Secure Device Firmware Update (DFU)** GATT Service
  - 8EC90001-F315-4F60-9FB8-838830DAEA50, 8EC90002-F315-4F60-9FB8-838830DAEA50 - Associated GATT Characteristics

https://developer.nordicsemi.com/nRF_Connect_SDK/doc/latest/nrf/libraries/bluetooth_services/services/nus.html
https://nordicsemiconductor.github.io/IOSnRFConnect/assets/files/UserManual.pdf
https://github.com/adafruit/Bluefruit_LE_Connect_Android/blob/master/app/src/main/java/com/adafruit/bluefruit/le/connect/ble/KnownUUIDs.java

Vendor-specific 128-bit UUIDs

🍪**Silicon-specific examples: Cambridge Silicon Radio (bought by Qualcomm)**

- 0000110**0**-d102-11e1-9b23-00025b00a5a5 - **GAIA (Over The Air update protocol)** GATT service
  - 0000110**1**-d102-11e1-9b23-00025b00a5a5, 0000110**2**-d102-11e1-9b23-00025b00a5a5, 0000110**3**-d102-11e1-9b23-00025b00a5a5 - Associated GATT characteristics

https://developer.qualcomm.com/qfile/34081/csr102x_otau_overview.pdf

Vendor-specific 128-bit UUIDs

🍪Silicon-specific examples: Silicon Labs

- 331a36f5-2459-45ea-9d95-6142f0c4b307 - **BGX Xpress Streaming (arbitrary data)** GATT Service
  - a9da6040-0823-4995-94ec-9ce41ca28833, a73e9a10-628f-4494-a099-12efaf72258f, 75a9f022-af03-4e41-b4bc-9de90a47d50b - Associated GATT characteristics

https://docs.silabs.com/gecko-os/1/bgx/latest/ble-services

Vendor-specific 128-bit UUIDs

🧩Module-specific examples: Laird

- 569a1101-b87f-490c-92cb-11ba5ea5167c - **Virtual Serial Port** Service (GATT & ADV_IND)
  - 569a2000-b87f-490c-92cb-11ba5ea5167c - TX GATT Characteristic
  - 569a2001-b87f-490c-92cb-11ba5ea5167c - RX GATT Characteristic

https://www.mouser.com/pdfDocs/ApplicationNoteLairdBLESerialPortServicev1_0_0.pdf

What I Want

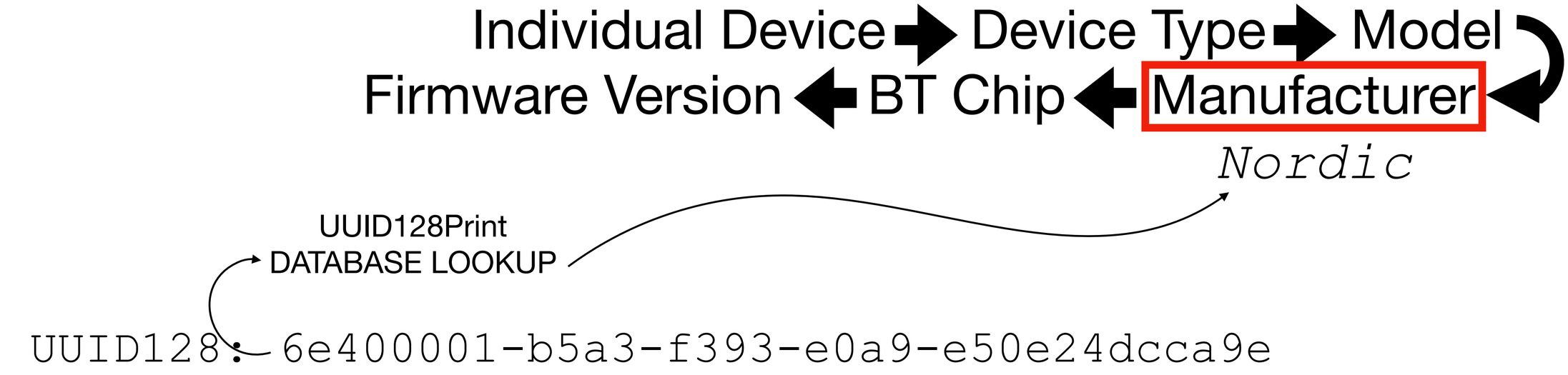
Individual Device → Device Type → Model ↷
Firmware Version ← BT Chip ← Manufacturer

What I Want

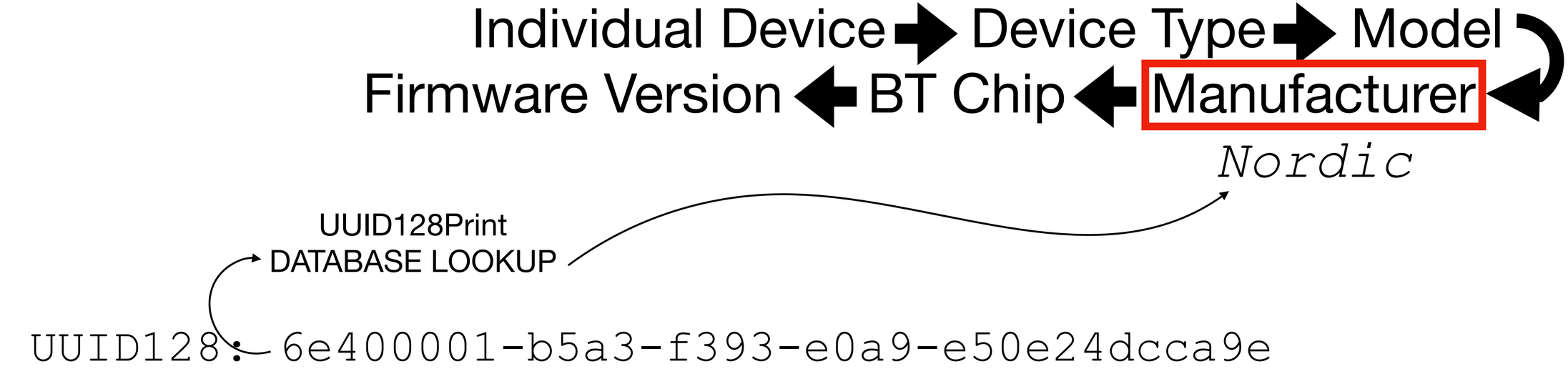

```
UUID128: 6e400001-b5a3-f393-e0a9-e50e24dcca9e
```


DARK MENTOR

What I Want

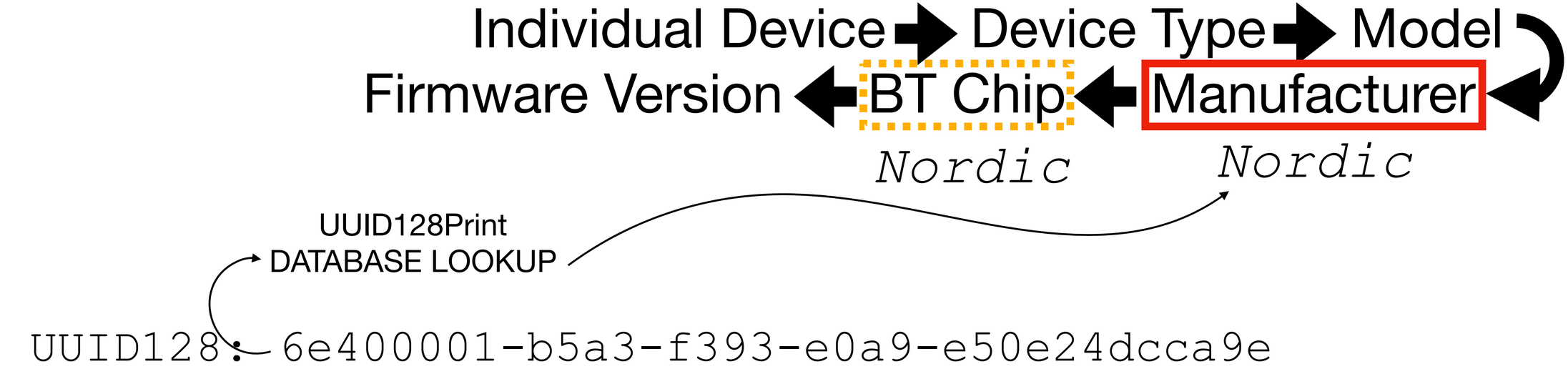

Individual Device
Device Type
Model
Firmware Version
BT Chip
Manufacturer
Nordic
UUID128Print
DATABASE LOOKUP
UUID128: 6e400001-b5a3-f393-e0a9-e50e24dcca9e

What I Want



ASSUMPTION:
UUID128Prints can be reused *within* Manufacturers,
but not reused *between* Manufacturers

What I Want



ASSUMPTION:
UUID128Prints can be reused *within* Manufacturers,
but not reused *between* Manufacturers

Top 20 GATT Services in my data FWIW

2024-01-12

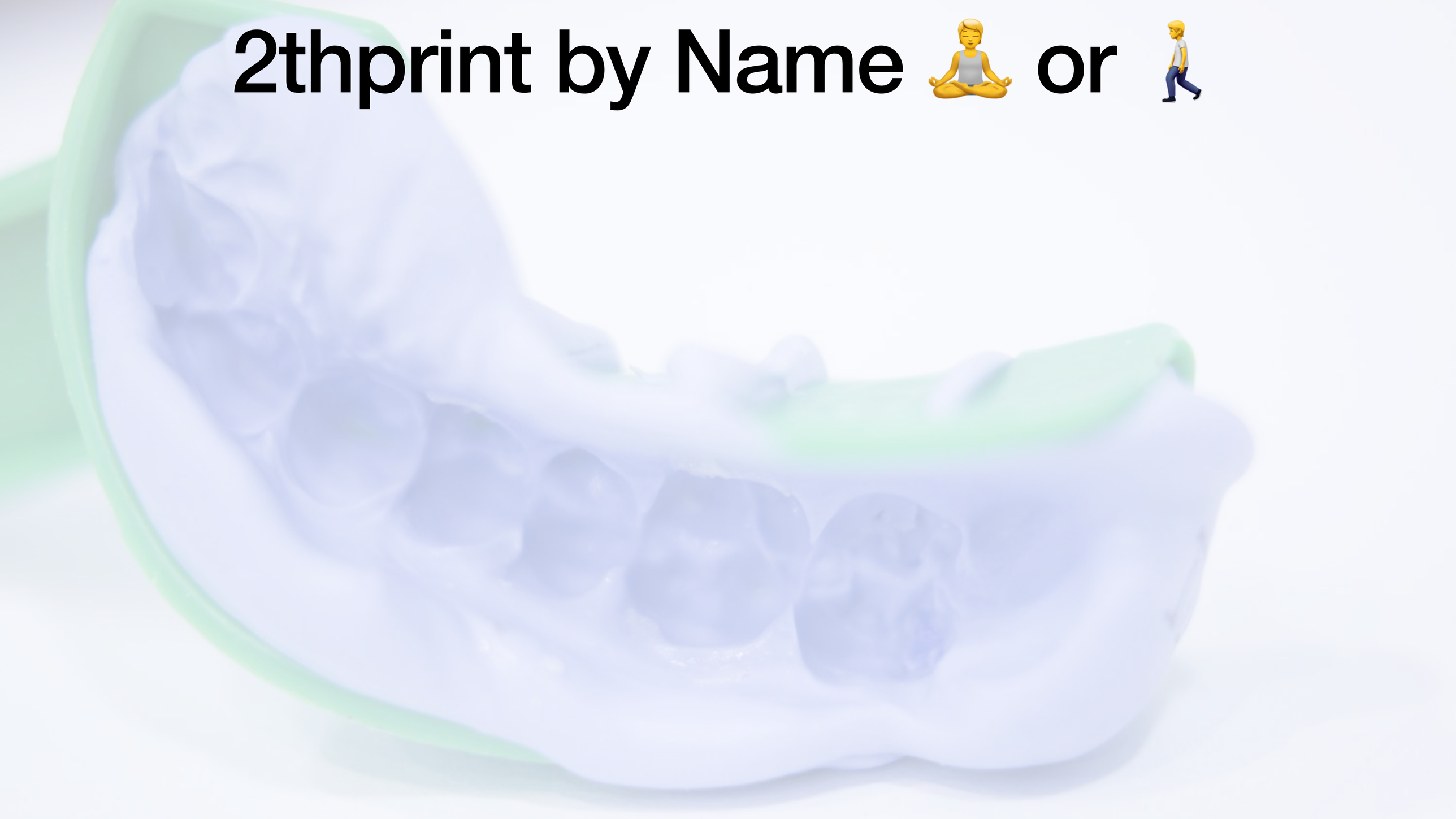
UUID128	Count	
00001800-0000-1000-8000-00805f9b34fb	21127	-> "Generic Access" (GAP)
00001801-0000-1000-8000-00805f9b34fb	20675	-> Generic Attribute (GATT)
0000180a-0000-1000-8000-00805f9b34fb	18044	-> Device Information
9fa480e0-4967-4542-9390-d343dc5d04ae	15738	-> Apple Nearby
d0611e78-bbb4-4591-a5f8-487910ae4366	15737	-> Apple Continuity
0000180f-0000-1000-8000-00805f9b34fb	11284	-> Battery
00001805-0000-1000-8000-00805f9b34fb	10641	-> Current Time
89d3502b-0f36-433a-8ef4-c502ad55f8dc	10636	-> Apple Media Service
7905f431-b5ce-4e99-a40f-4b1e122d00d0	10636	-> Apple Notification Center Service
0000febe-0000-1000-8000-00805f9b34fb	843	-> Bose
0000fe03-0000-1000-8000-00805f9b34fb	598	-> Amazon Alexa
0000fe2c-0000-1000-8000-00805f9b34fb	421	-> Google Fast Pair
9aa4730f-b25c-4cc3-b821-c931559fc196	359	-> Apple Watch? (my data seems to support)
eedd5e73-6aa8-4673-8219-398a489da87c	280	-> Samsung SmartTag Authentication Service
0000fd69-0000-1000-8000-00805f9b34fb	246	-> Samsung SmartTag Offline Finding Advertisement
0000feed-0000-1000-8000-00805f9b34fb	234	-> Tile
0000180d-0000-1000-8000-00805f9b34fb	222	-> Heart Rate
eed6d5cc-c3b2-4d7b-8c6b-7acbf7965bb6	204	-> Samsung Galaxy Watch (based on my data)
00001855-0000-1000-8000-00805f9b34fb	202	-> Telephony and Media Audio
0000184c-0000-1000-8000-00805f9b34fb	196	-> Generic Telephone Bearer

Top 20 GATT Characteristics in my data FWIW

2024-01-12

char_UUID128	Count	
00002a00-0000-1000-8000-00805f9b34fb	19592	-> Device Name
00002a01-0000-1000-8000-00805f9b34fb	19205	-> Appearance
00002a05-0000-1000-8000-00805f9b34fb	18443	-> Service Changed
00002a29-0000-1000-8000-00805f9b34fb	16776	-> Manufacturer Name String
00002a24-0000-1000-8000-00805f9b34fb	16650	-> Model Number String
af0badb1-5b99-43cd-917a-a77bc549e3cc	15194	-> Apple Nearby Characteristic
8667556c-9a37-4c91-84ed-54ee27d90049	15193	-> Apple Continuity Characteristic
00002a19-0000-1000-8000-00805f9b34fb	10632	-> Battery Level
00002a2b-0000-1000-8000-00805f9b34fb	10245	-> Current Time
9fbf120d-6301-42d9-8c58-25e699a21dbd	10194	-> Apple Notification Center Notification Source
69d1d8f3-45e1-49a8-9821-9bbdfdaad9d9	10194	-> Apple Notification Center Control Point
22eac6e9-24d6-4bb5-be44-b36ace7c7bfb	10192	-> Apple Notification Center Data Source
9b3c81d8-57b1-4a8a-b8df-0e56f7ca51c2	10185	-> Apple Media Center Remote Command
2f7cabce-808d-411f-9a0c-bb92ba96c102	10183	-> Apple Media Center Entity Update
c6b2f38c-23ab-46d8-a6ab-a3a870bbd5d7	10183	-> Apple Media Center Entity Attribute
00002a0f-0000-1000-8000-00805f9b34fb	10176	-> Local Time Information
00002a26-0000-1000-8000-00805f9b34fb	1682	-> Firmware Revision String
00002aa6-0000-1000-8000-00805f9b34fb	1655	-> Central Address Resolution
00002a04-0000-1000-8000-00805f9b34fb	1644	-> Peripheral Preferred Connection Parameters
00002a28-0000-1000-8000-00805f9b34fb	1563	-> Software Revision String

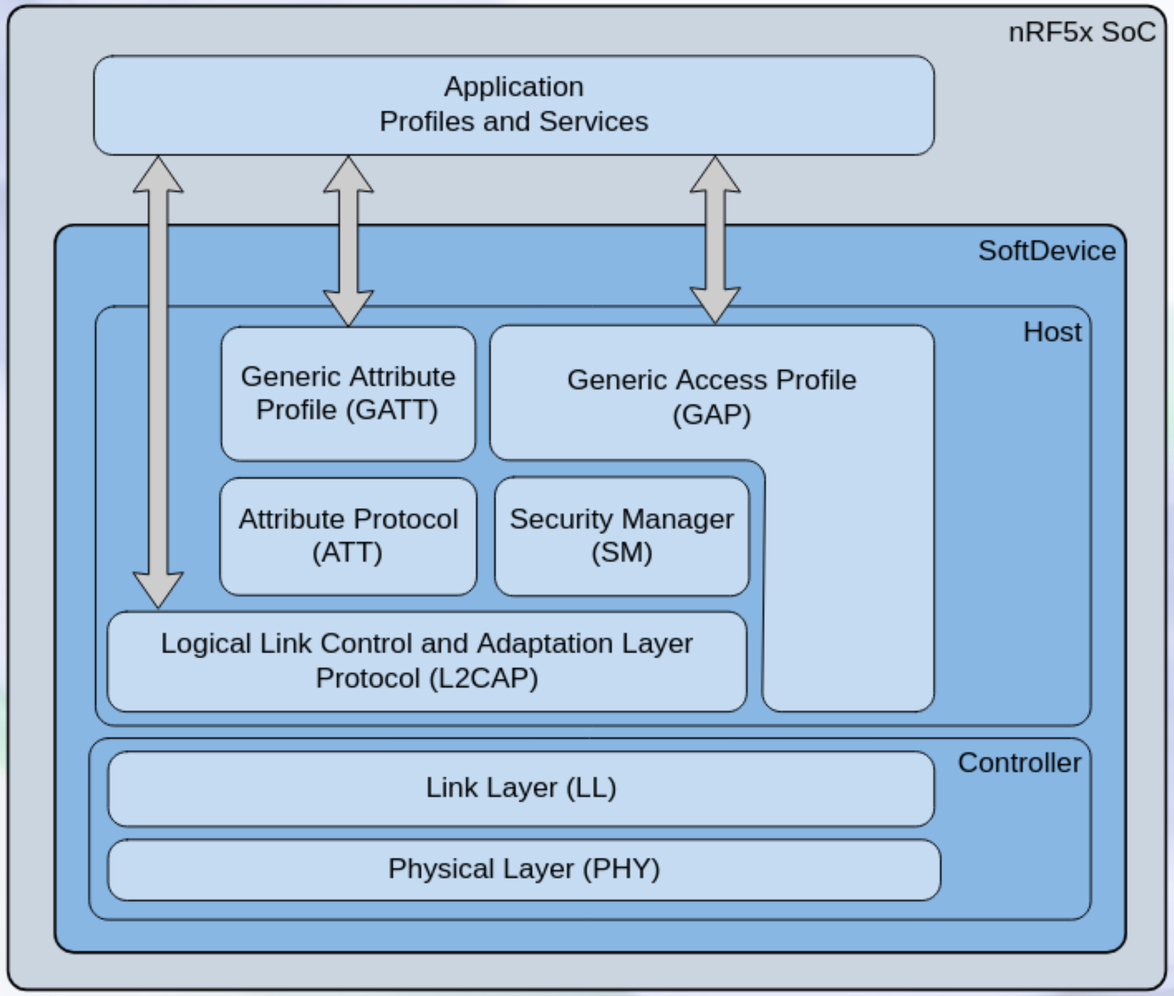
2thprint by Name 🧘‍♂️ or 🚶‍♂️



2thprint by Name 🧘 or 🚶

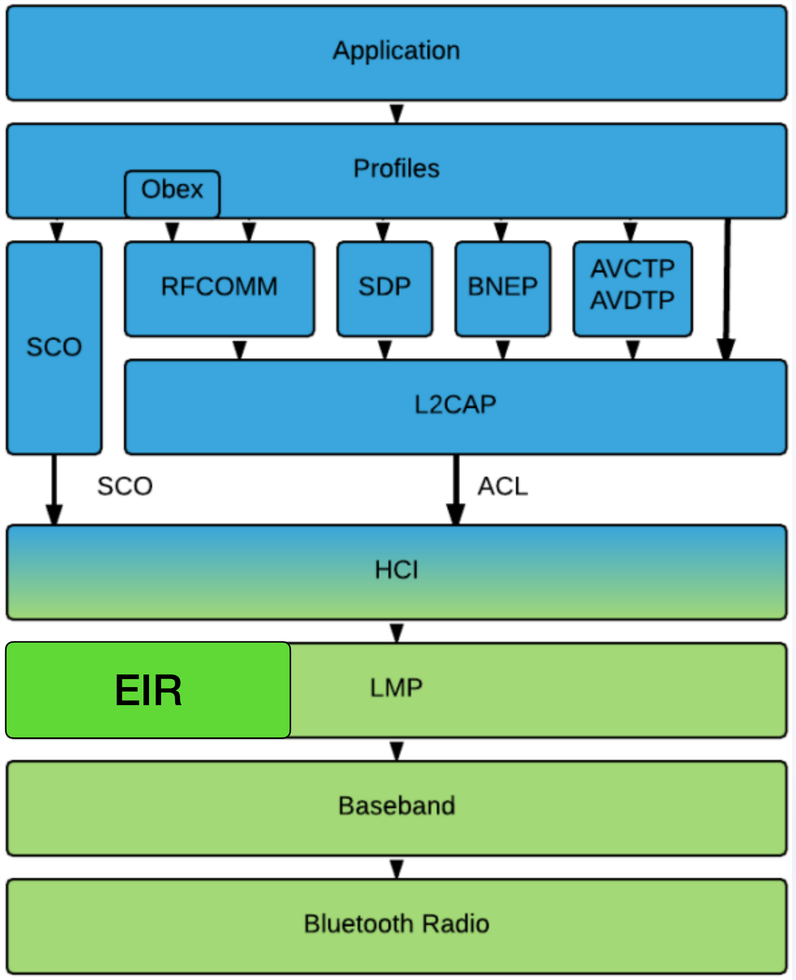
BLE

[1]



BTC

[2]

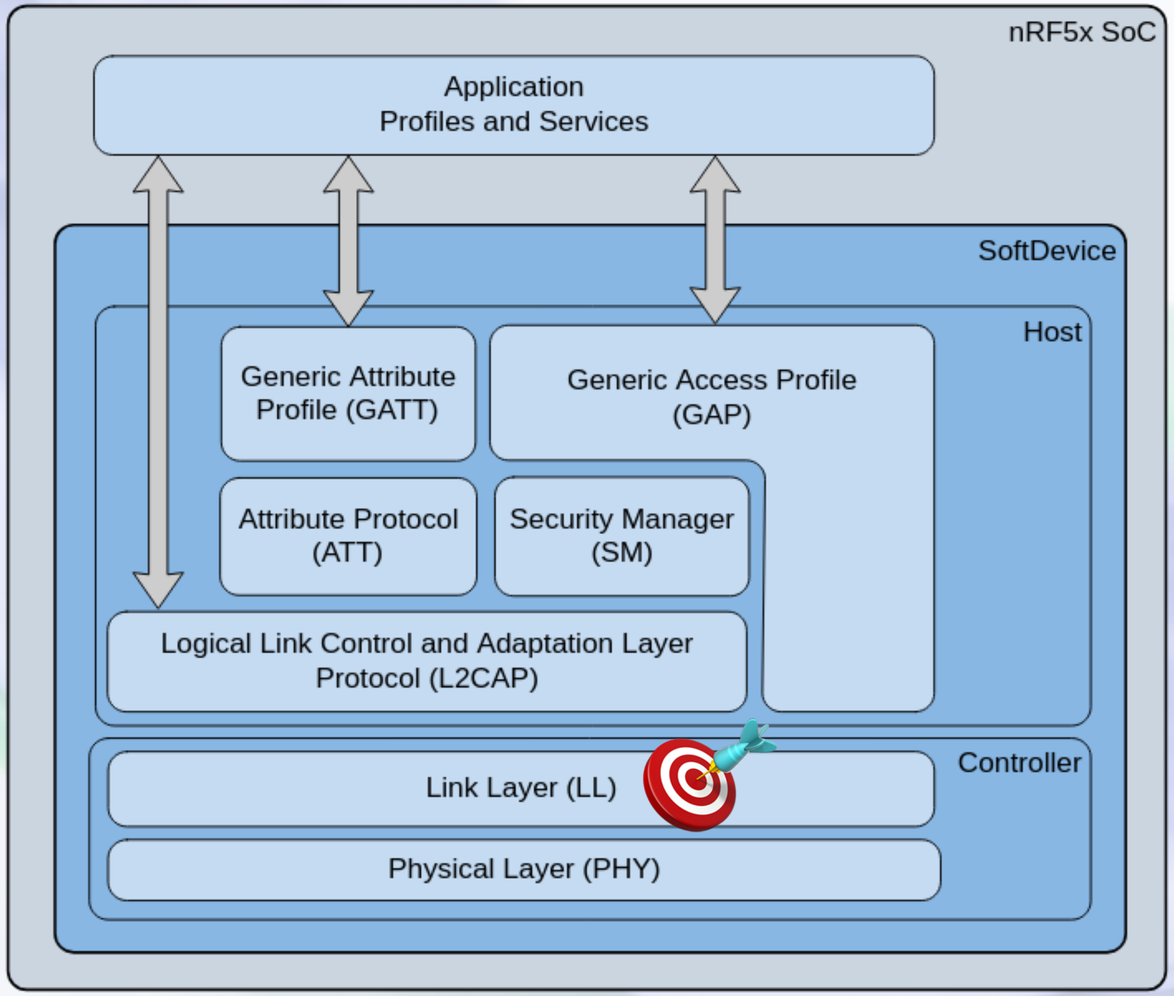


[1] https://infocenter.nordicsemi.com/index.jsp?topic=%2Fsds_s140%2FSDS%2Fs1xx%2Fble_protocol_stack%2Fble_protocol_stack.html
[2] https://crosscontrol.com/manual/Bluetooth%20Documentation/content/bluetooth.html

2thprint by Name 🧘 or 🚶

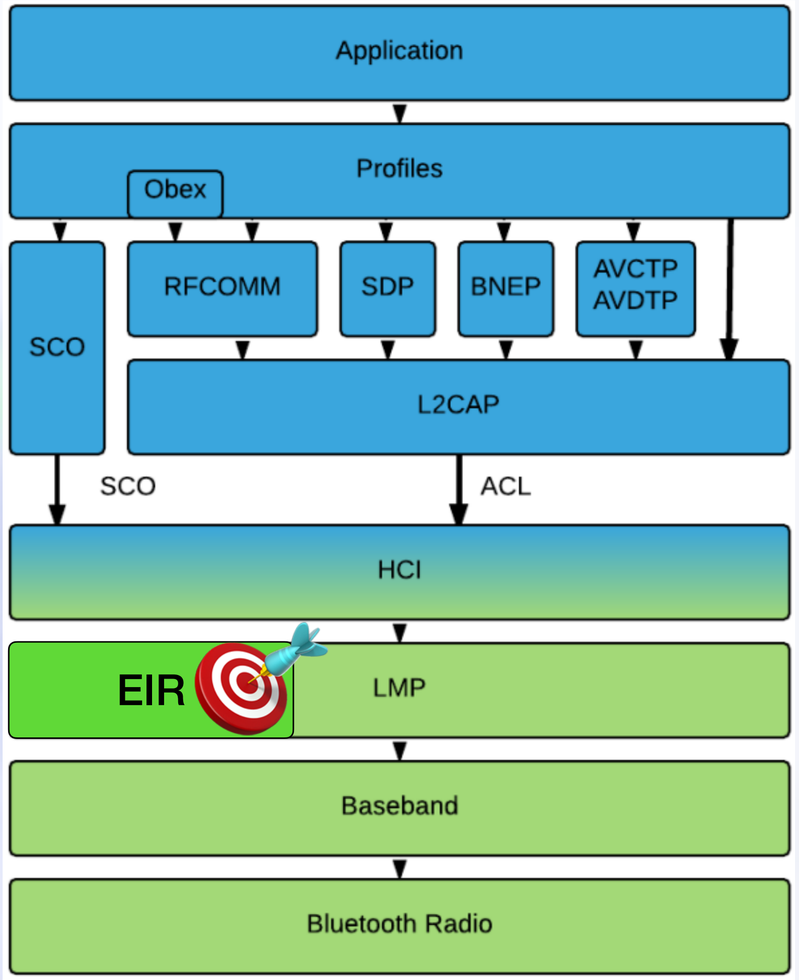
BLE

[1]



BTC

[2]



[1] https://infocenter.nordicsemi.com/index.jsp?topic=%2Fsds_s140%2FSDS%2Fs1xx%2Fble_protocol_stack%2Fble_protocol_stack.html
[2] https://crosscontrol.com/manual/Bluetooth%20Documentation/content/bluetooth.html

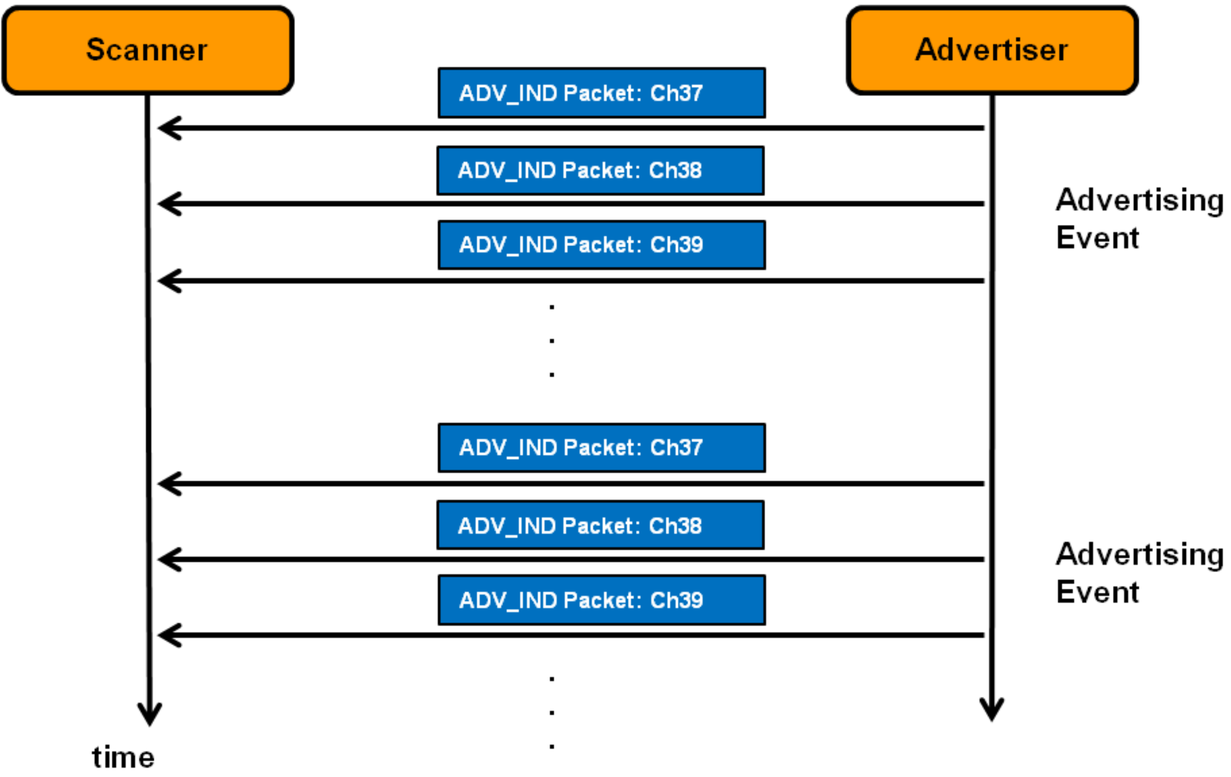
2thprint by Name

aka "*NamePrint*"

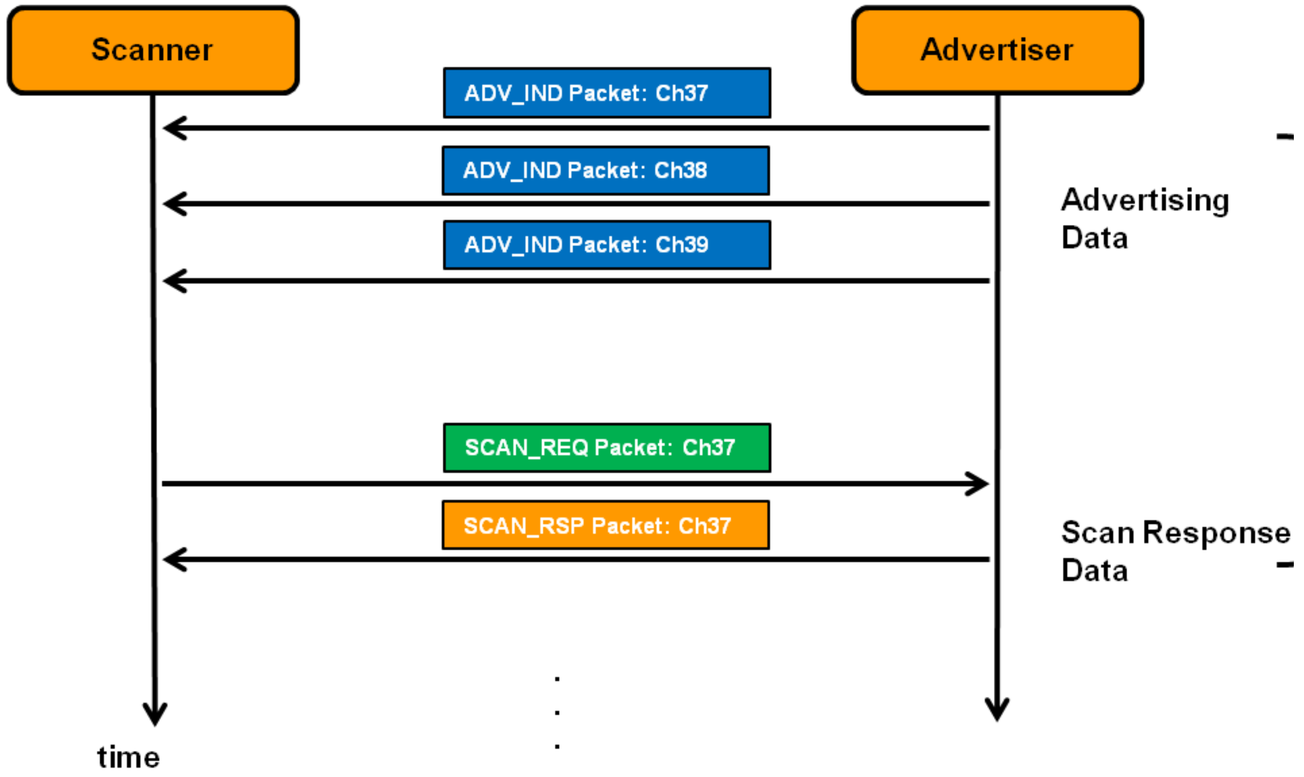
- Let's start with the easy situation, where a device more or less literally tells you what it is, based on its name
  - "Ember Ceramic Mug"
  - "Nest Cam"
  - "Versa 4"
  - "User’s MacBook Pro"

Background

Passive Scanning 🧘



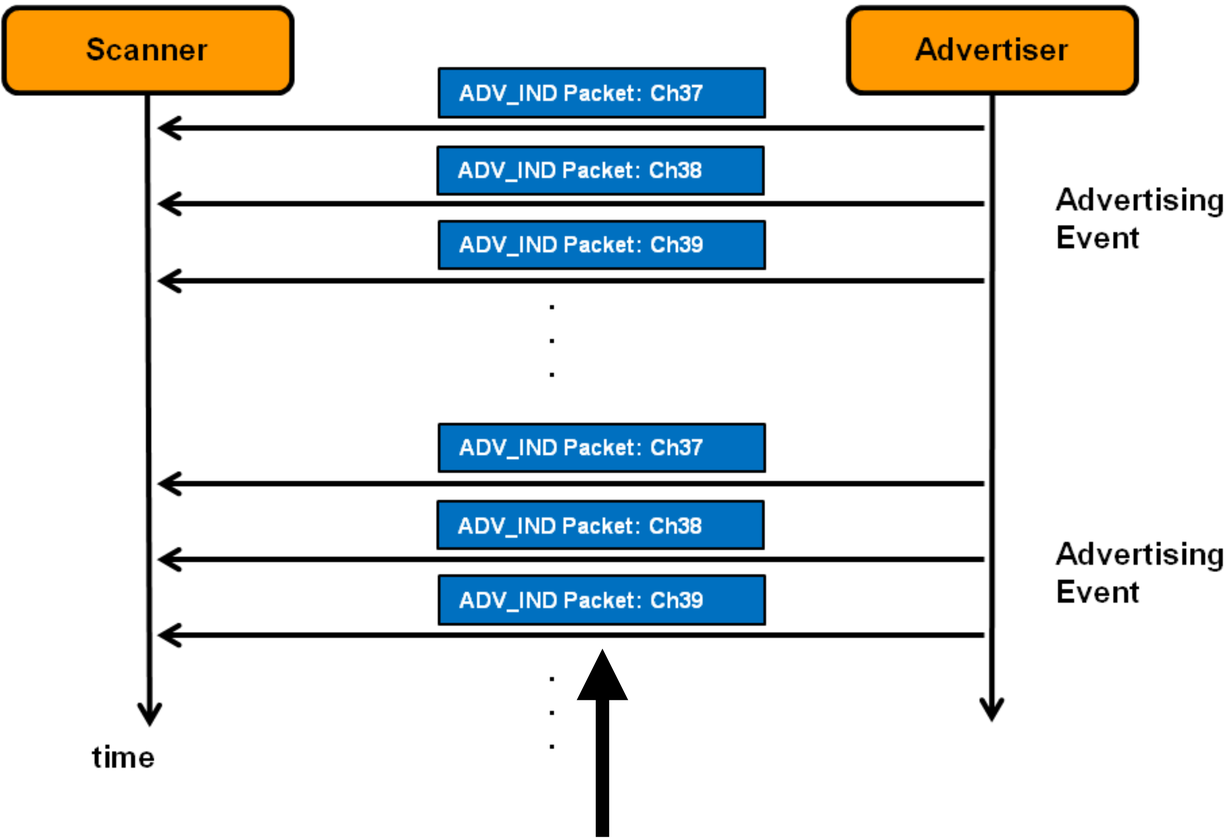
"Mostly-passive" 🚶 Scanning



Images from https://microchipdeveloper.com/wireless:ble-link-layer-discovery

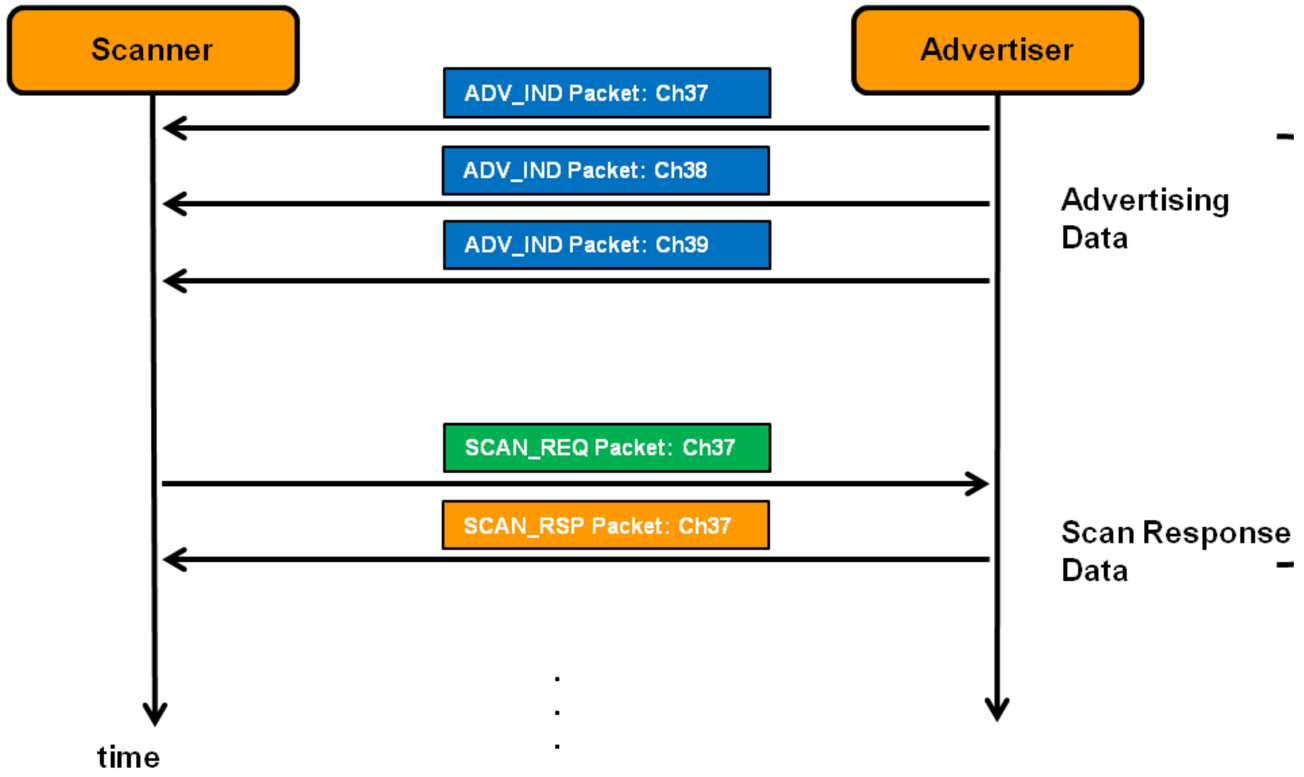
Background

Passive Scanning 🧘



Sometimes the name will be here 🧘

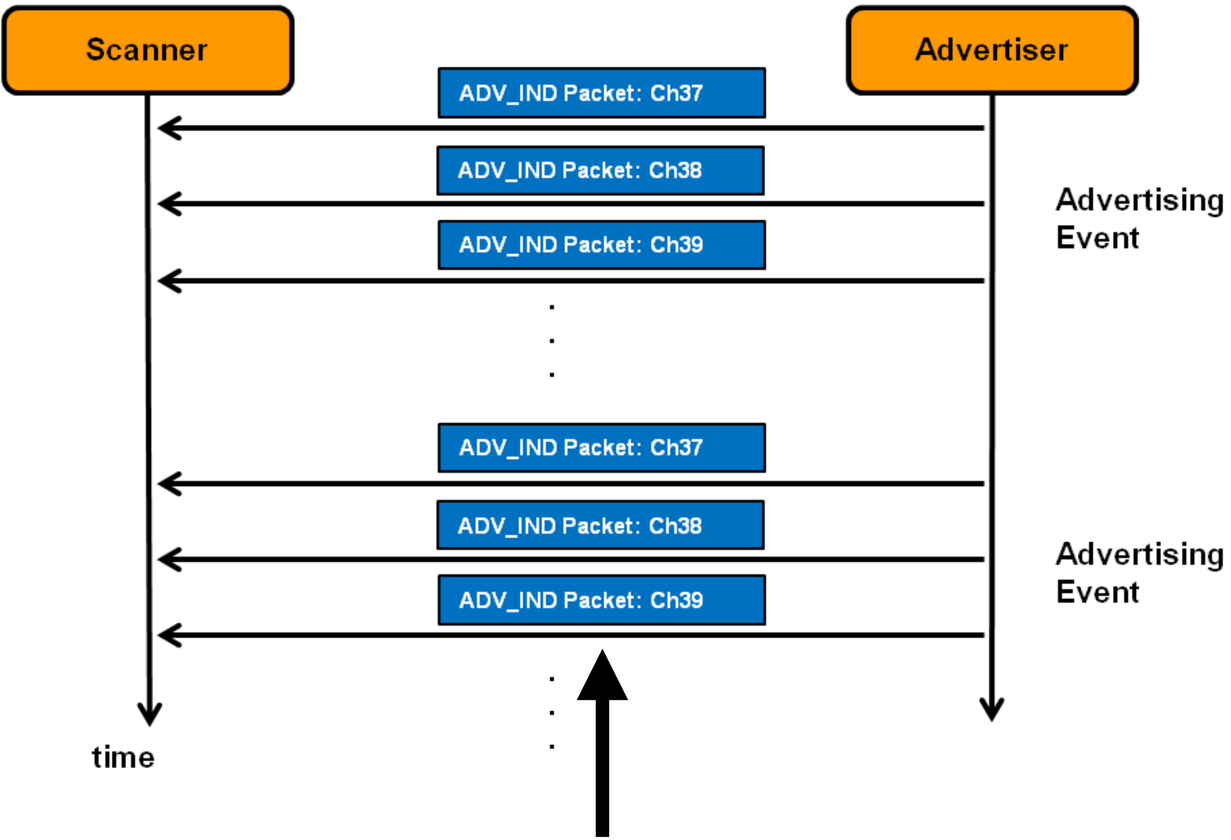
"Mostly-passive" 🚶 Scanning



Images from https://microchipdeveloper.com/wireless:ble-link-layer-discovery

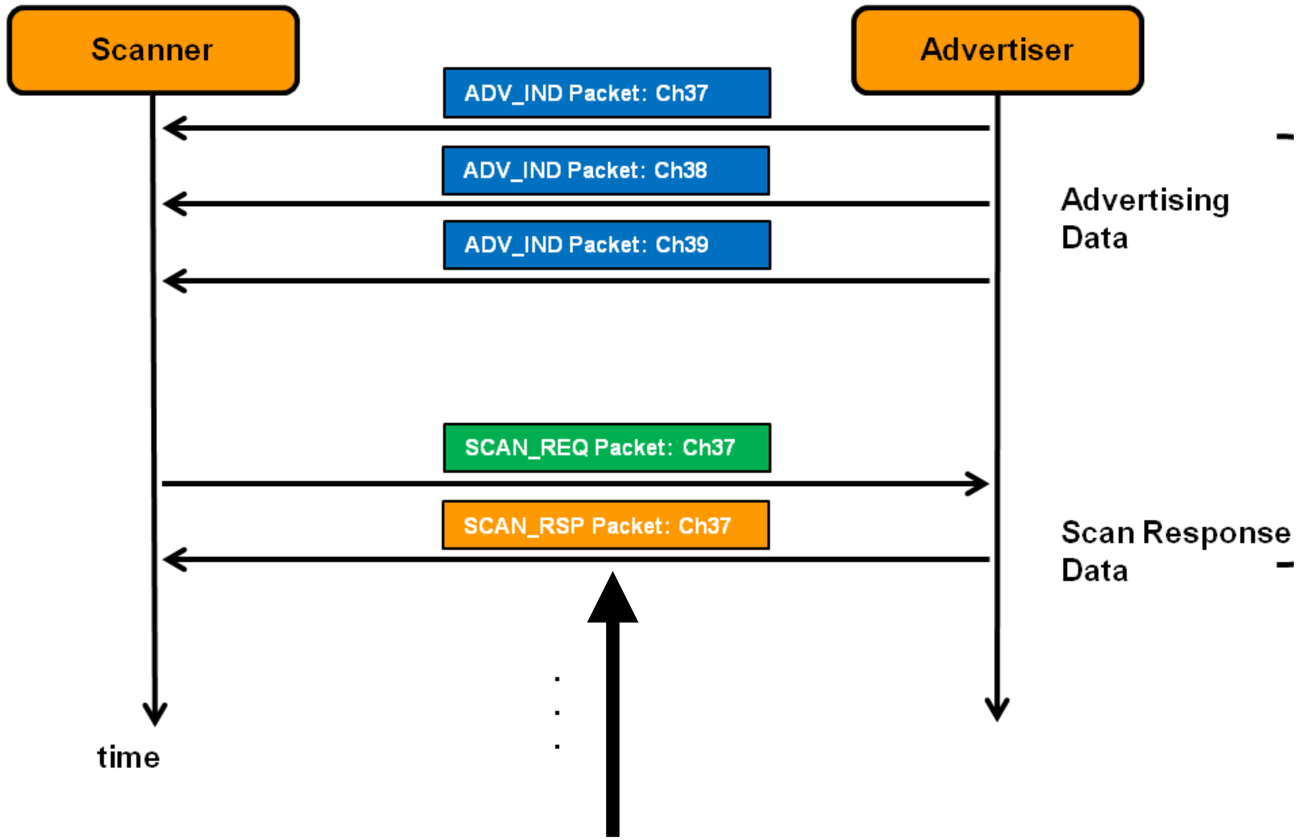
Background

Passive Scanning 🧘



Sometimes the name will be here 🧘

"Mostly-passive" 🚶 Scanning



Other times the OS will ask for it 🚶, and it comes back in a SCAN_RSP

Images from https://microchipdeveloper.com/wireless:ble-link-layer-discovery

BT Name Behavior: One-to-One

One device == one *unique* name && one *unique* BDADDR

BT Name Behavior: One-to-One

One device == one *unique* name && one *unique* BDADDR

***Complete* BDADDR inclusion:**

`oura_A038F8445ED7` → `a0:38:f8:44:5e:d7` (public address)

`NOKE3K_C8D8DCF760F6` → `c8:d8:dc:f7:60:f6` (random static)

BT Name Behavior: One-to-One

One device == one *unique* name && one *unique* BDADDR

Complete **BDADDR inclusion:**

`oura_A038F8445ED7` → `a0:38:f8:44:5e:d7 (public address)`

`NOKE3K_C8D8DCF760F6` → `c8:d8:dc:f7:60:f6 (random static)`

Partial **BDADDR inclusion:**

`Galaxy Fit2 (987C)` → `10:39:17:36:98:7c (public address)`

`Xiaomi Smart Band 7 34C1` → `c6:05:ea:95:34:c1 (random static)`

BT Name Behavior: One-to-One

One device == one *unique* name && one *unique* BDADDR

Complete **BDADDR inclusion:**

oura_A038F8445ED7 → a0:38:f8:44:5e:d7 (public address)

NOKE3K_C8D8DCF760F6 → c8:d8:dc:f7:60:f6 (random static)

Partial **BDADDR inclusion:**

Galaxy Fit2 (987C) → 10:39:17:36:98:7c (public address)

Xiaomi Smart Band 7 34C1 → c6:05:ea:95:34:c1 (random static)

(Presumed) serial number inclusion

TW370_TIA00414 → 4c:36:4e:4c:57:2a (public address)

CATBTNT-04 DKS02390 → 00:81:f9:7e:37:a6 (public address)

BT Name Behavior: One-to-One

One device == one *unique* name && one *unique* BDADDR

BT Name Behavior: One-to-One

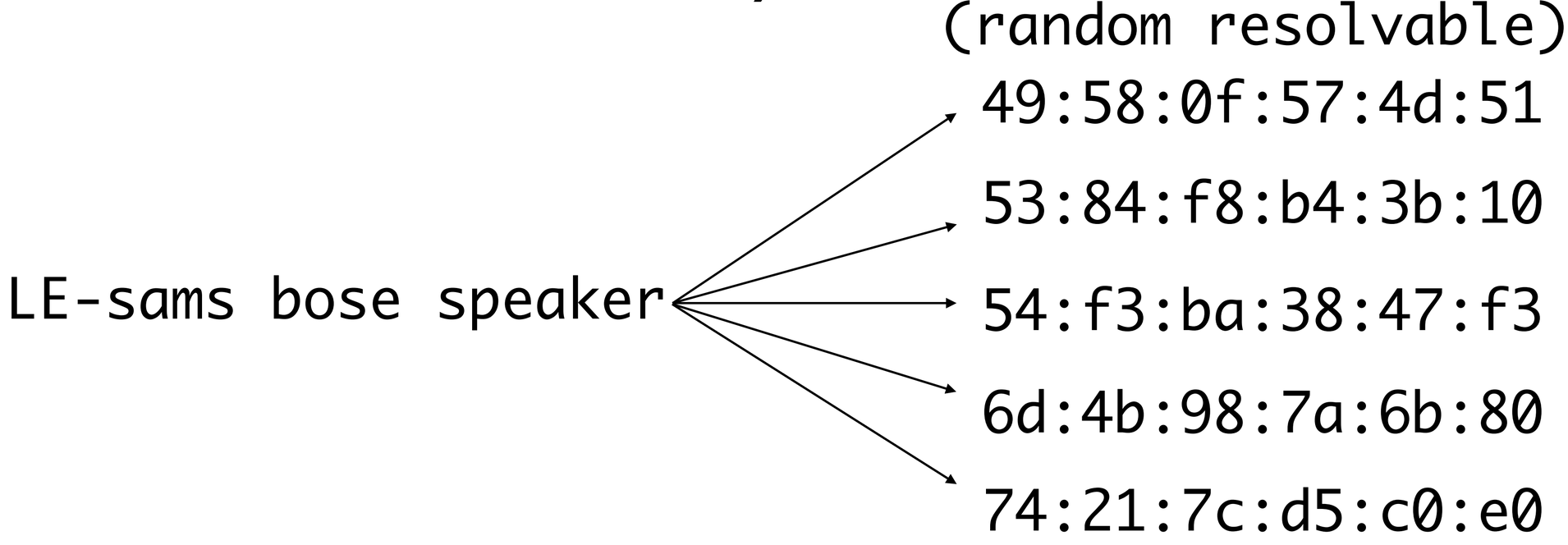
One device == one *unique* name && one *unique* BDADDR

Possible **partial BDADDR disclosure?:**

```
Galaxy Watch Active2(C898) LE→c0:b9:b5:02:10:31 (random static)
```

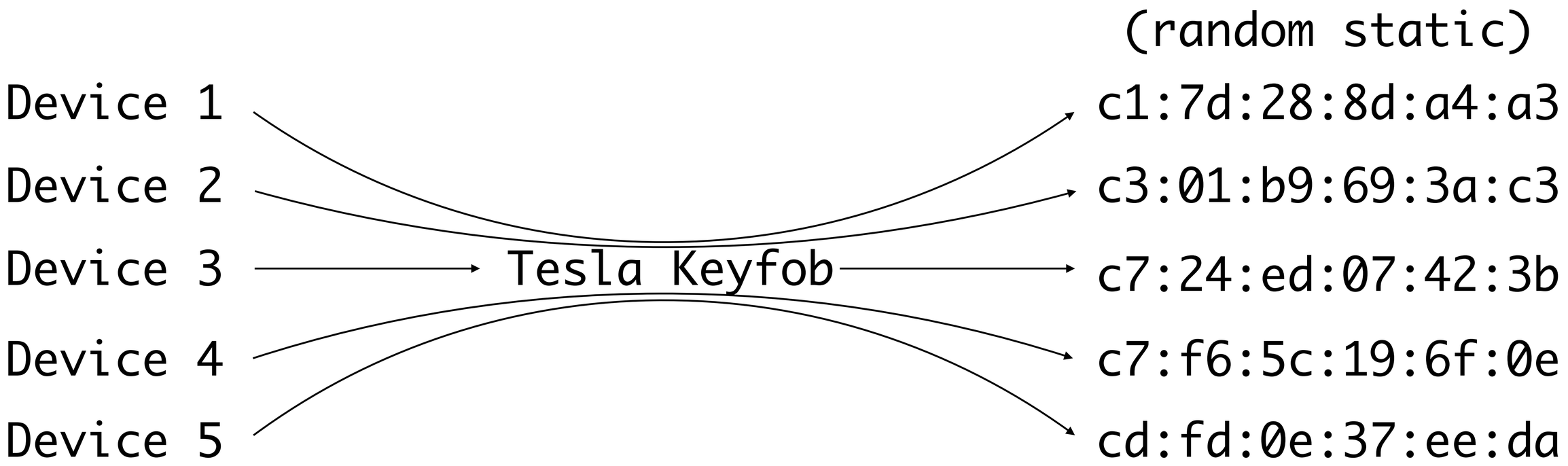
BT Name Behavior: One-to-Many

One device == one *unique* name && many BDADDRs (exclusive to BLE random addresses)



BT Name Behavior: Many-to-Many v1

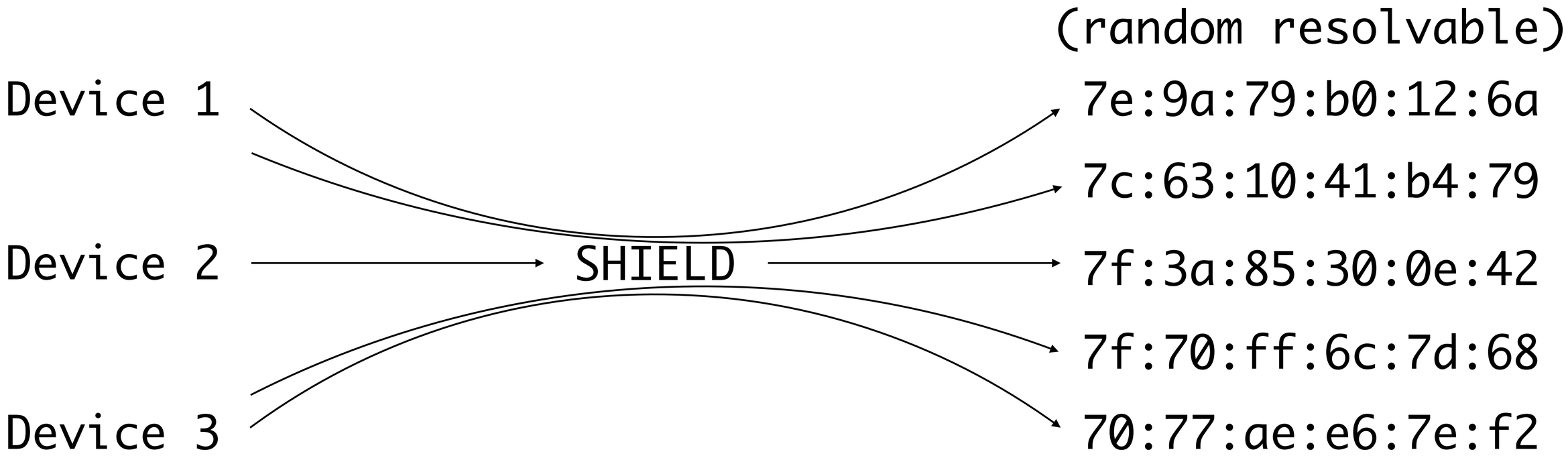
Many devices, one *shared* name, one *unique* BDADDR per device



Example: Tesla Keyfob

BT Name Behavior: Many-to-Many v2

Many devices, one *shared* name, *many* BDADDR per device

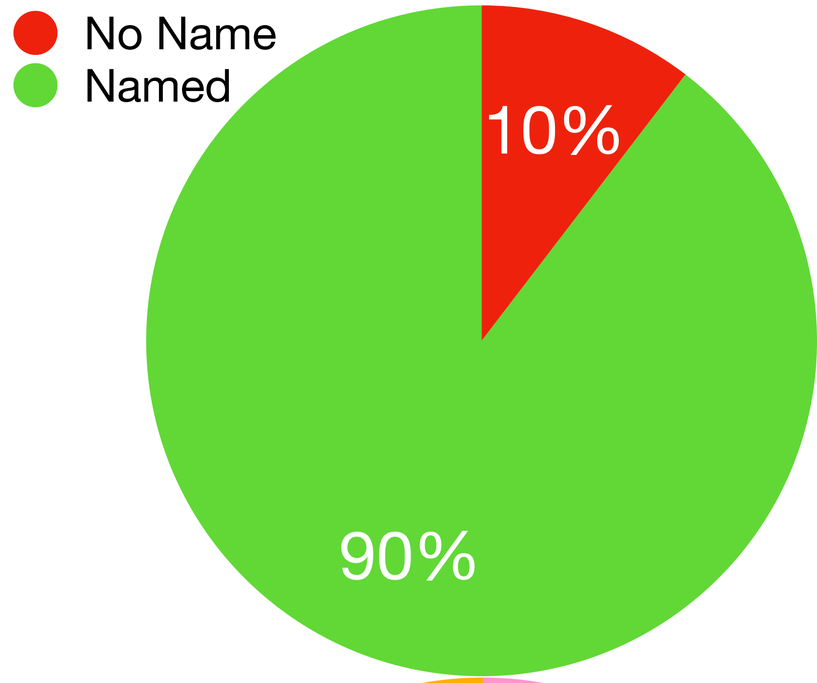


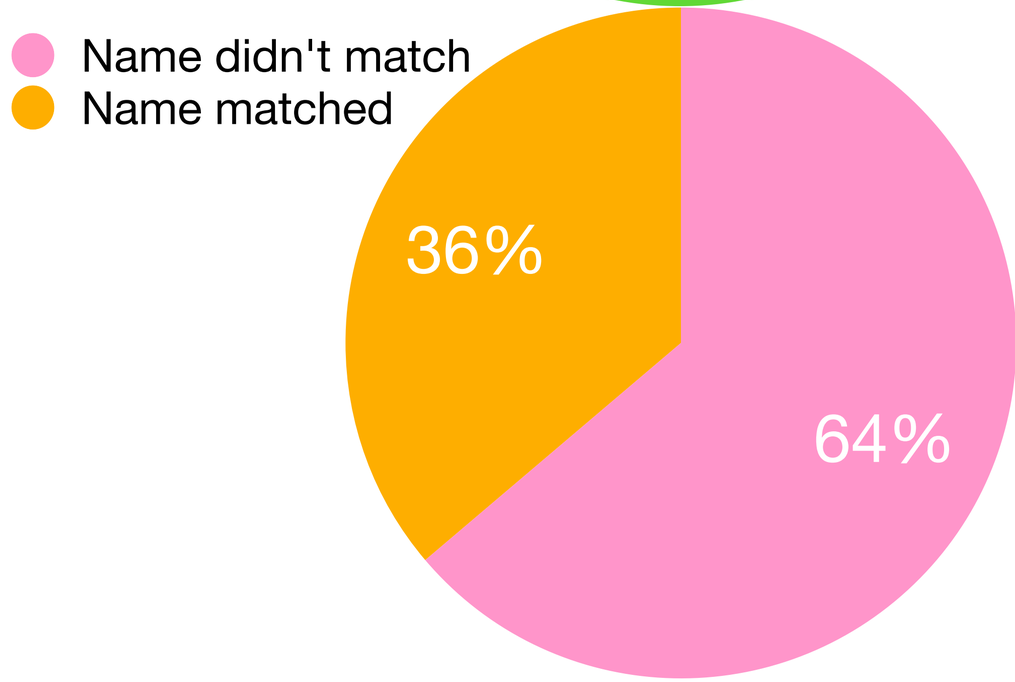
Example: Nvidia SHIELD

NamePrint Data

BTC as of 2024-01-12

- **I wrote 1,447 regex "NamePrints"**
  - 557 NamePrints matched on BTC data
- 65,451 *unique* BT Classic BDADDRs with a name
  - 65,744 *unique* {name:BDADDR} pairs[1]
    - 23,803 NamePrint matches
      - 23,803 / 65,744 = 36% of all BTC data
  - 33,368 *unique names* in BTC data[2]

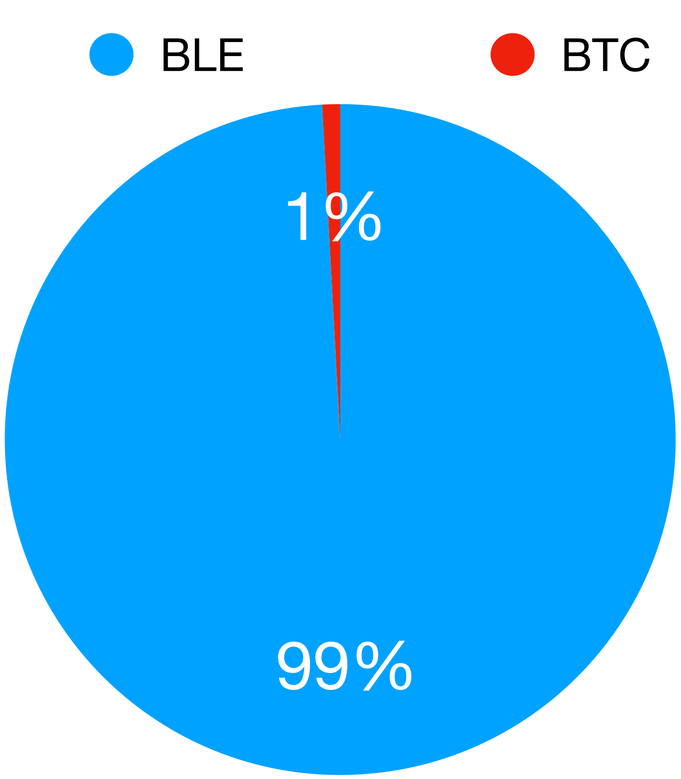


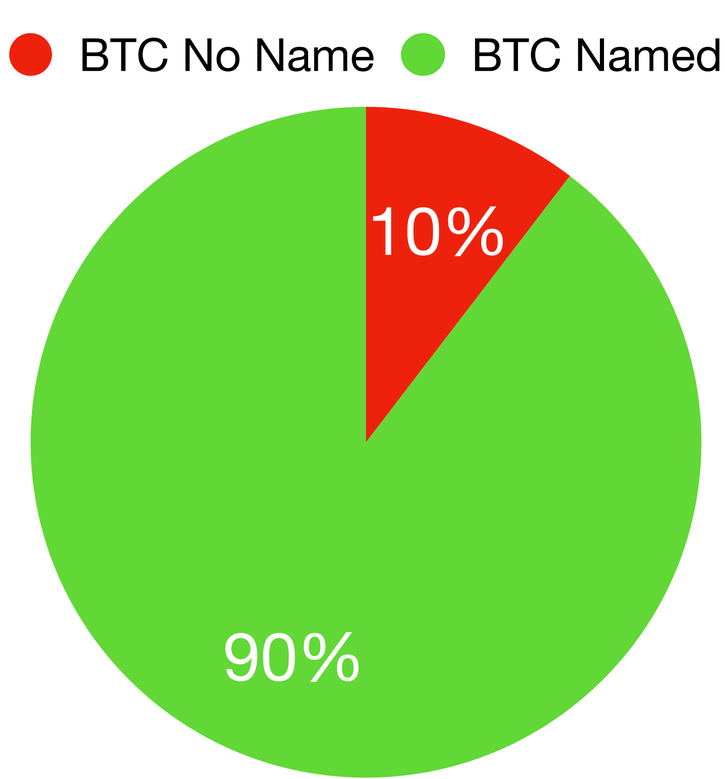


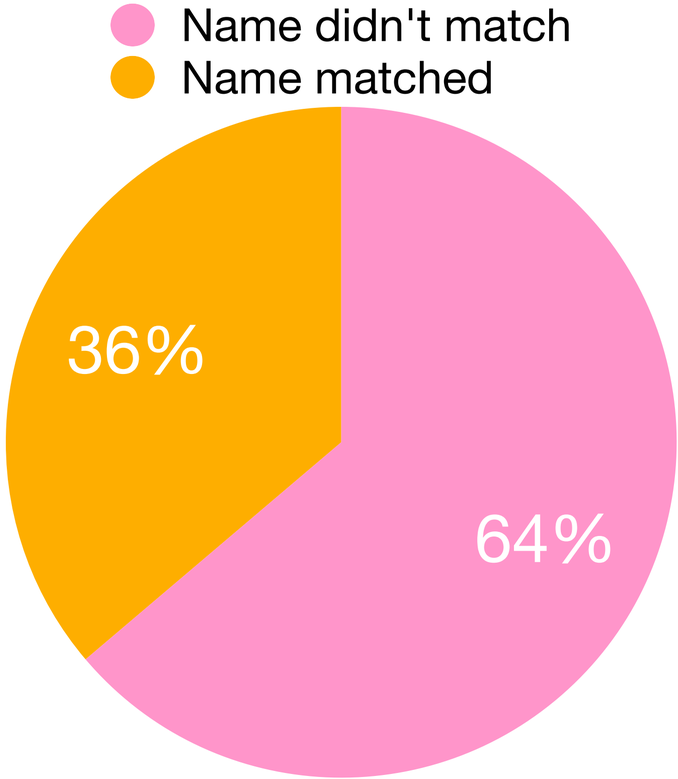
[1]How can there be more bdaddr:name pairs than bdaddrs? Multiple names per bdaddr! (Often due to receiving corrupt name data.)
[2]How can there be more names than matches? Because NamePrints are regexes, one NamePrint matches multiple names

Summary of BTC NamePrint % applicability

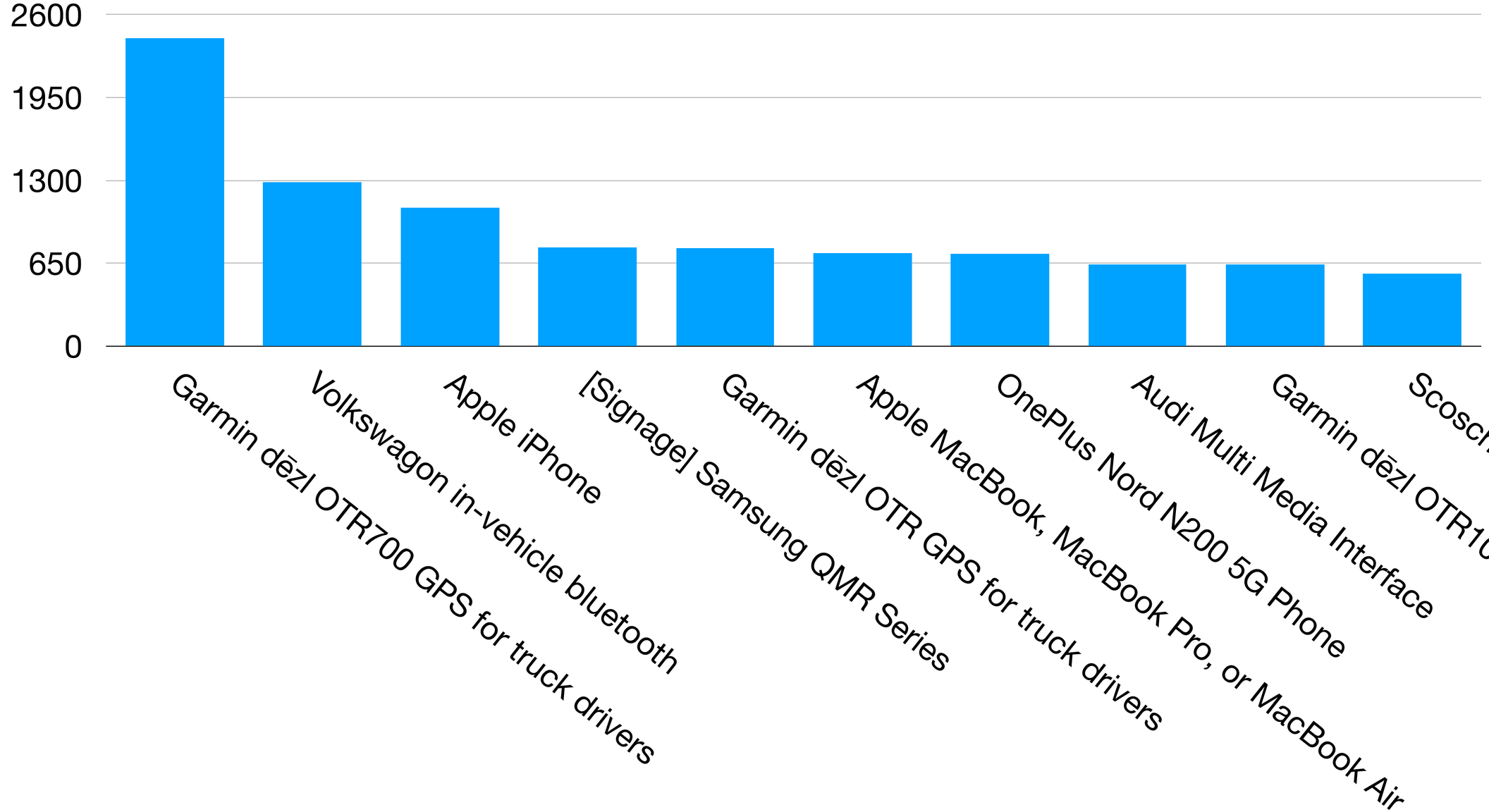
- 36% of 90% of 1% (.324%) of all my data is BTC with a name that matches a NamePrint





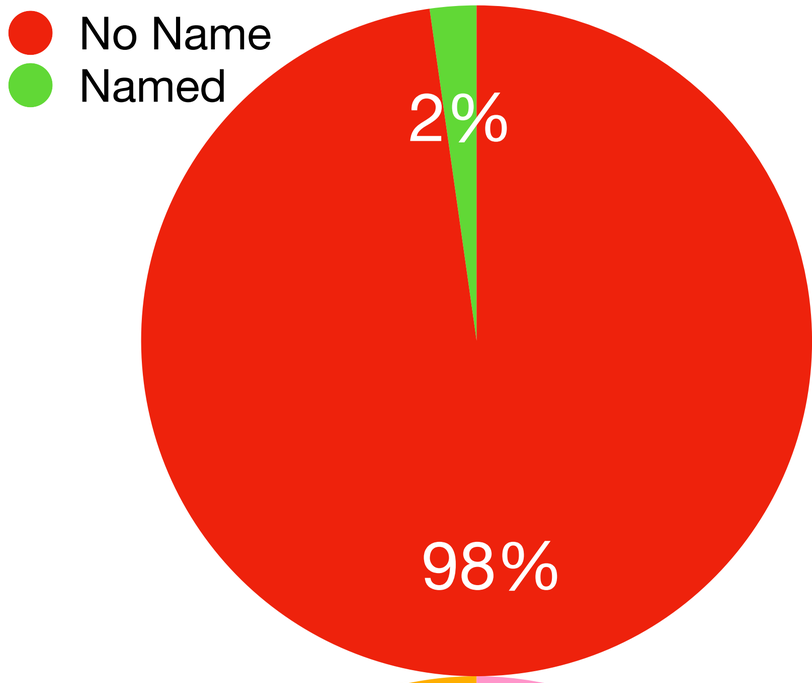


Top 10 BTC Matches

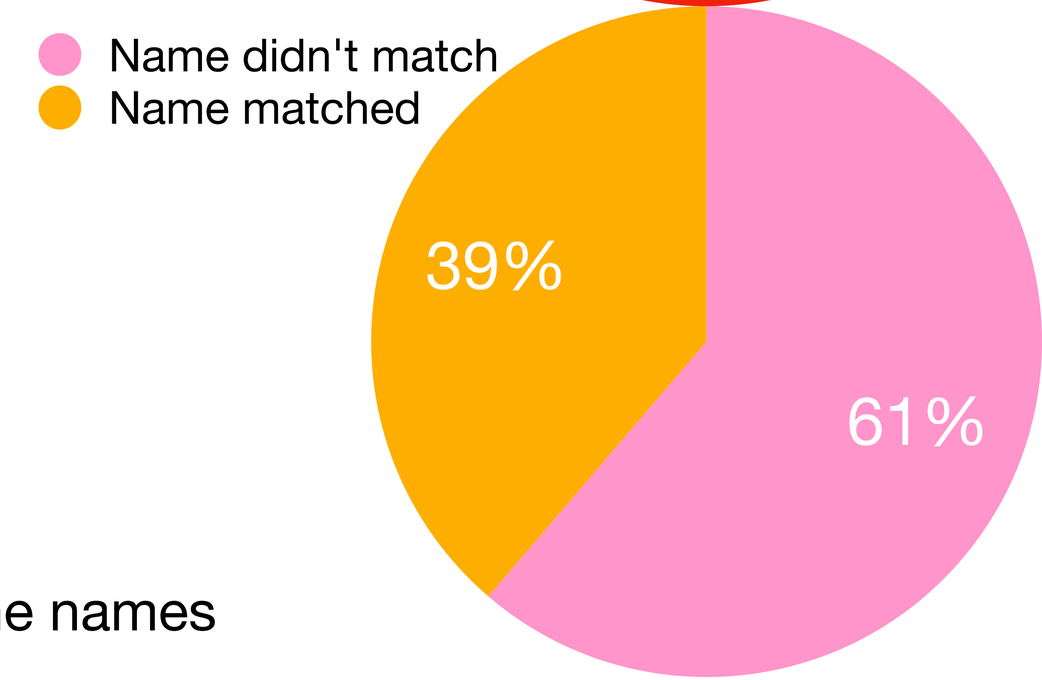


NamePrint Data

BLE as of 2024-01-12



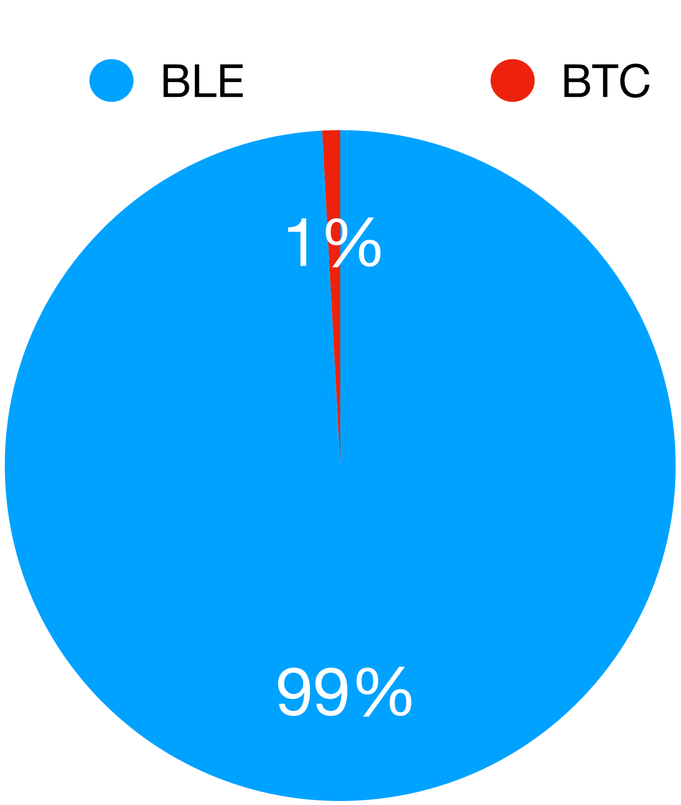
- **Made 1447 regex "NamePrints"**
  - 912 NamePrints matched on BLE data
- 188,059 *unique* BLE BDADDRs with a name
  - 195,954 *unique* name:BDADDR pairs[1]
    - 123,865 matches
      - 39% of named data, 1.7% of all BTC data
  - 18,959 *unique names*[2]
    - So 540 regexes match 18959/37939 ~ 50% of the names

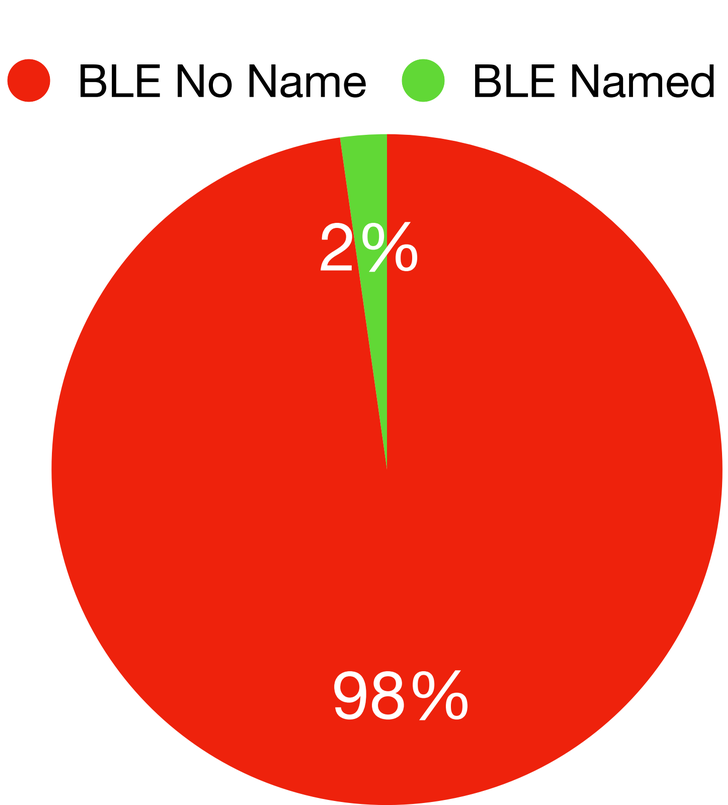


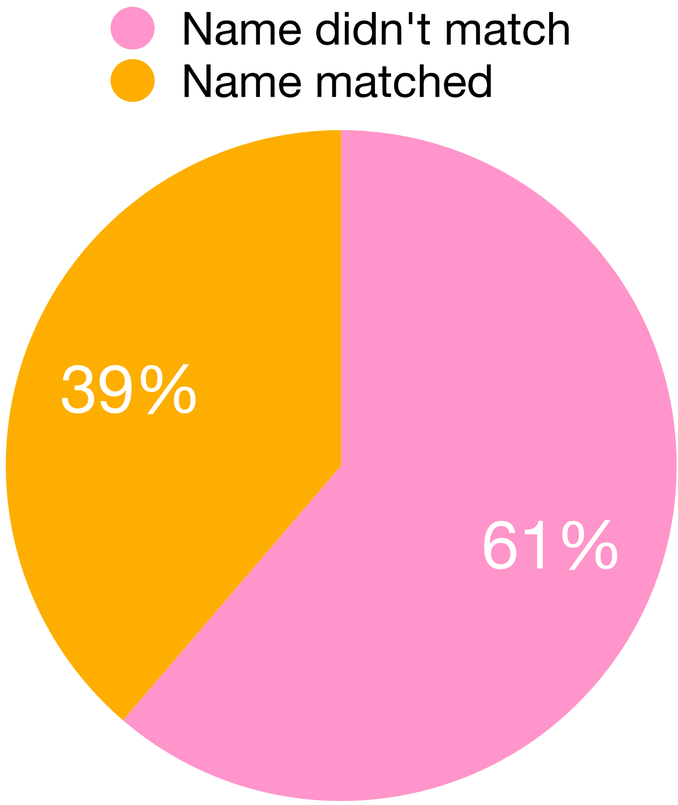
[1]How can there be more bdaddr:name pairs than bdaddrs? Multiple names per bdaddr! (Often due to receiving corrupt name data.)
[2]How can there be less names than name:BDADDR pairs? BDADDR randomization

Summary of BTC NamePrint % applicability

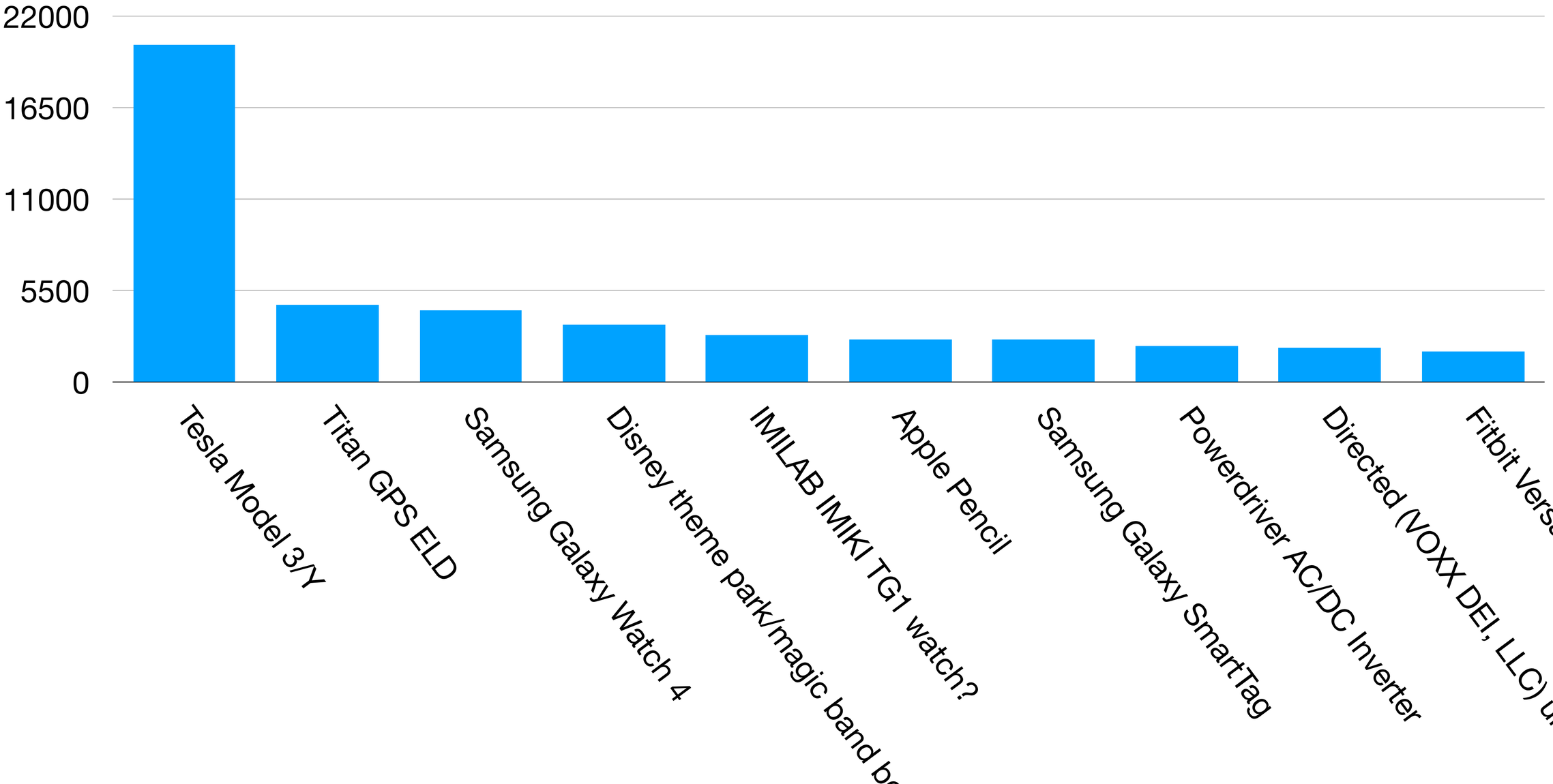
- 39% of 2% of 99% (7.128%) of all my data is BLE with a name that matches a NamePrint







Top 10 BLE Matches



Occasionally NamePrint -> ChipPrint

- *Very rarely (as in, I've only seen this once so far ;))*, the vendor will make a big deal out of what chip it uses, and then you can quickly get a ChipPrint directly from the NamePrint!

- NamePrint="^FiiO BTR5$",ChipPrint="CSR8675"

BTR5

Flagship Portable High-Fidelity Bluetooth Amplifier

- High Performance DAC ES9218P*2
- Flagship Bluetooth chip CSR8675
- FPGA clock management，dual independent crystal oscillators
- Bluetooth 5.0 with full format support
- Independent control chip XMOS XUF208
- USB DAC supporting up to 384kHz/DSD256 native
- Double-sided 2.5D glass with OLED display
- 3.5mm+2.5mm headphone outputs
- Intelligent control with FiiO Music app
- One-touch NFC pairing

VGP 2021 受賞 | VGP 2020 SUMMER 受賞

XMOS | DAC | 8675

BTR5

Flagship Portable High-Fidelity Bluetooth Amplifier

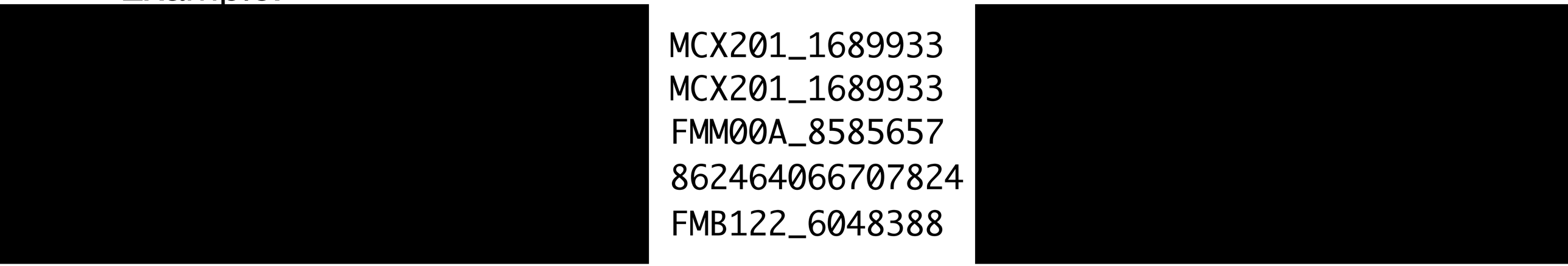
- High Performance DAC ES9218P*2
- Flagship Bluetooth chip CSR8675
- FPGA clock management，dual independent crystal oscillators
- Bluetooth 5.0 with full format support
- Independent control chip XMOS XUF208
- USB DAC supporting up to 384kHz/DSD256 native
- Double-sided 2.5D glass with OLED display
- 3.5mm+2.5mm headphone outputs
- Intelligent control with FiiO Music app
- One-touch NFC pairing

VGP 2021 受賞 | VGP 2020 SUMMER 受賞

XMOS | DAC | 8675

OUIPrints Beget NamePrints

- If we have the company name from a BDADDR, it may help us track down model names from a company, and consequently create more 2thprints-by-name.
- Example:



OUIPrints Beget NamePrints

- If we have the company name from a BDADDR, it may help us track down model names from a company, and consequently create more 2thprints-by-name.
- Example:

```
| 00:1e:42:33:59:e5 | Teltonika | MCX201_1689933
| 00:1e:42:35:51:64 | Teltonika | MCX201_1689933
| 00:1e:42:50:9f:ea | Teltonika | FMM00A_8585657
| 00:1e:42:58:15:df | Teltonika | 862464066707824
| 00:1e:42:a7:bd:49 | Teltonika | FMB122_6048388
```

OUIPrints Beget NamePrints

- If we have the company name from a BDADDR, it may help us track down model names from a company, and consequently create more 2thprints-by-name.
- Example:

| 00:1e:42:33:59:e5 | Teltonika | MCX201_1689933 | https://www.moreycorp.com/products/mcx201/
| 00:1e:42:35:51:64 | Teltonika | MCX201_1689933 |
| 00:1e:42:50:9f:ea | Teltonika | FMM00A_8585657 |
| 00:1e:42:58:15:df | Teltonika | 862464066707824 | ¯_(ツ)_/¯
| 00:1e:42:a7:bd:49 | Teltonika | FMB122_6048388 |

OUIPrints Beget NamePrints

- If we have the company name from a BDADDR, it may h
  model names from a company, and consequently create
  name.
- Example:

| 00:1e:42:33:59:e5 | Teltonika | MCX201_1689933 | https://www.moreycorp.com/products/mcx201/
| 00:1e:42:35:51:64 | Teltonika | MCX201_1689933 |
| 00:1e:42:50:9f:ea | Teltonika | FMM00A_8585657 |
| 00:1e:42:58:15:df | Teltonika | 862464066707824 | ¯_(ツ)_/¯
| 00:1e:42:a7:bd:49 | Teltonika | FMB122_6048388 |

OUIPrints Beget NamePrints

- If we have the company name from a BDADDR, it may h
  model names from a company, and consequently create
  name.

- Example:

| 00:1e:42:33:59:e5 | Teltonika | MCX201_1689933 | https://www.moreycorp.com/products/mcx201/
| 00:1e:42:35:51:64 | Teltonika | MCX201_1689933 |
| 00:1e:42:50:9f:ea | Teltonika | FMM00A_8585657 |
| 00:1e:42:58:15:df | Teltonika | 862464066707824 | ¯_(ツ)_/¯
| 00:1e:42:a7:bd:49 | Teltonika | FMB122_6048388 |

OUIPrints Beget NamePrints

- If we have the company name from a BDADDR, it may help us track down model names from a company, and consequently create more 2thprints-by-name.
- Example:

| 00:1e:42:33:59:e5 | Teltonika | MCX201_1689933 | https://www.moreycorp.com/products/mcx201/
| 00:1e:42:35:51:64 | Teltonika | MCX201_1689933 |
| 00:1e:42:50:9f:ea | Teltonika | FMM00A_8585657 |
| 00:1e:42:58:15:df | Teltonika | 862464066707824 | ¯_(ツ)_/¯
| 00:1e:42:a7:bd:49 | Teltonika | FMB122_6048388 |

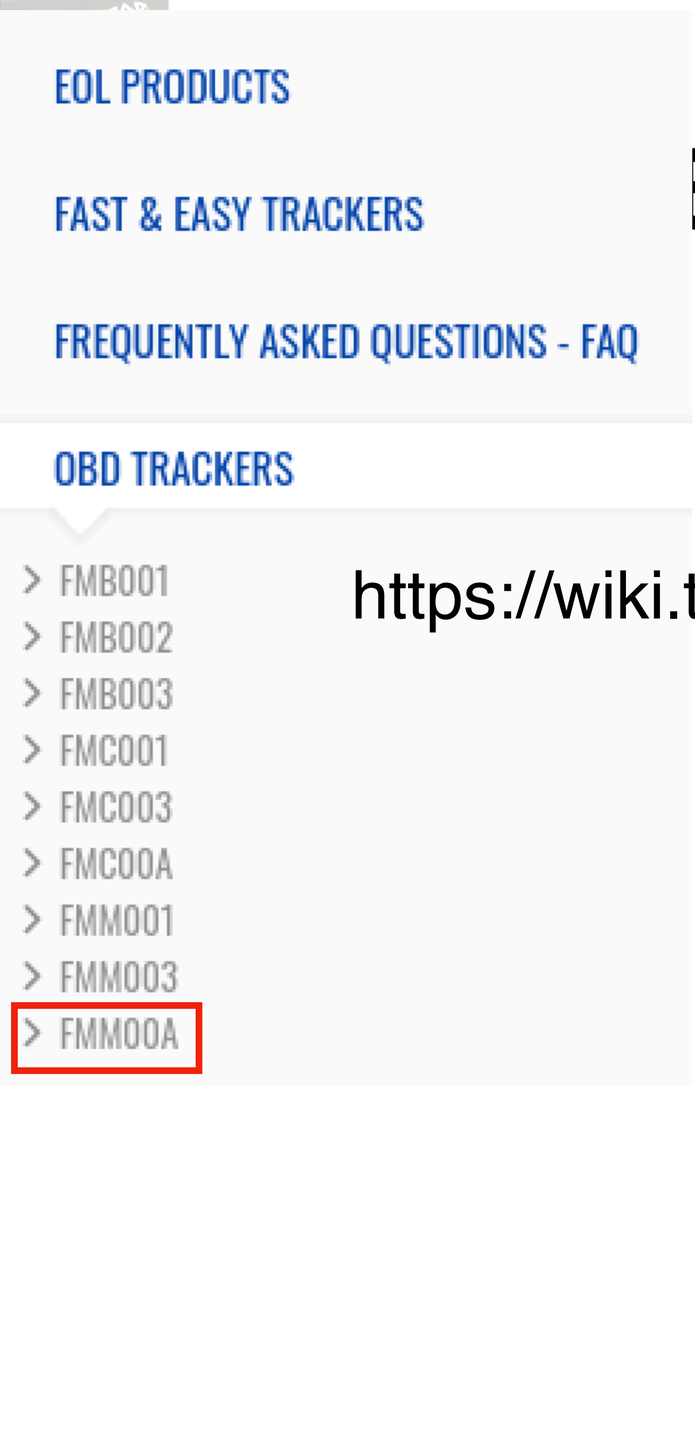
OUIPrints Beget Names

- If we have the company name from a BDADDR, it may help us track down model names from a company, and consequently create more 2thprints-by-name.
- Example:

| 00:1e:42:33:59:e5 | Teltonika | MCX201_1689933 | https://www.moreycorp.com/products/mcx201/
| 00:1e:42:35:51:64 | Teltonika | MCX201_1689933 |
| 00:1e:42:50:9f:ea | Teltonika | FMM00A_8585657 | https://wiki.teltonika-gps.com/view/FMM00A_Bluetooth_settings
| 00:1e:42:58:15:df | Teltonika | 862464066707824 | ¯_(ツ)_/¯
| 00:1e:42:a7:bd:49 | Teltonika | FMB122_6048388 | https://wiki.teltonika-gps.com/view/FMB122_Bluetooth_settings

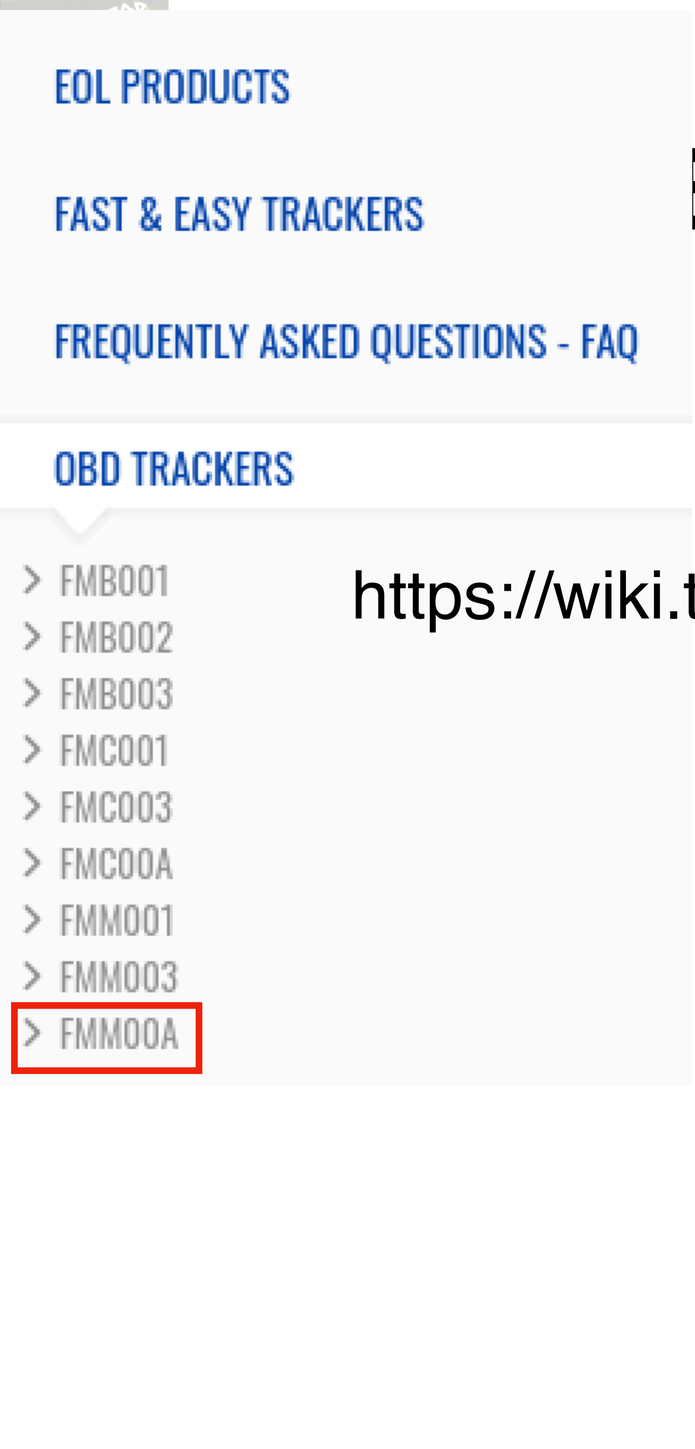
OUIPrints Beget Names

https://wiki.teltonika-gps.com/view/FMM00A_Bluetooth_settings



Beget Names

https://wiki.teltonika-gps.com/view/FMM00A_Bluetooth_settings



Beget Names

https://wiki.teltonika-gps.com/view/FMM00A_Bluetooth_settings

search for networks

WiFi | Cell | BT

Lat: 13.0374 to: 48.291

Lon: -112.87 to: -75.077

Last Updated: 20010925174546

BSSID/MAC: 0A:2C:EF:3D:25:1B or 0A:2C

Network Name (wildcards[1]: % and _):

FMM00A%

☐ Only Nets I Was the First to See

Query

[1]'%': 0-or-more characters, '_': a single character.

- FMM001
- FMM003
- FMM00A

FMM00A_8488746 QoS: **0** type: **BT**
00:1e:42:50:26:98 ? 2023-04-13 - 2023-04-13

FMM00A_8585657 QoS: **0** type: **BT**
00:1e:42:51:77:e9 ? 2023-06-01 - 2023-06-01

FMM00A_8682488 QoS: **0** type: **BT**
00:1e:42:52:72:6c ? 2023-04-22 - 2023-04-24

FMM00A_3268558 QoS: **0** type: **BT**
00:1e:42:55:0b:22 ? 2023-04-25 - 2023-04-25

FMM00A_8585657 QoS: **0** type: **BT**
00:1e:42:56:92:a9 ? 2023-05-27 - 2023-05-30

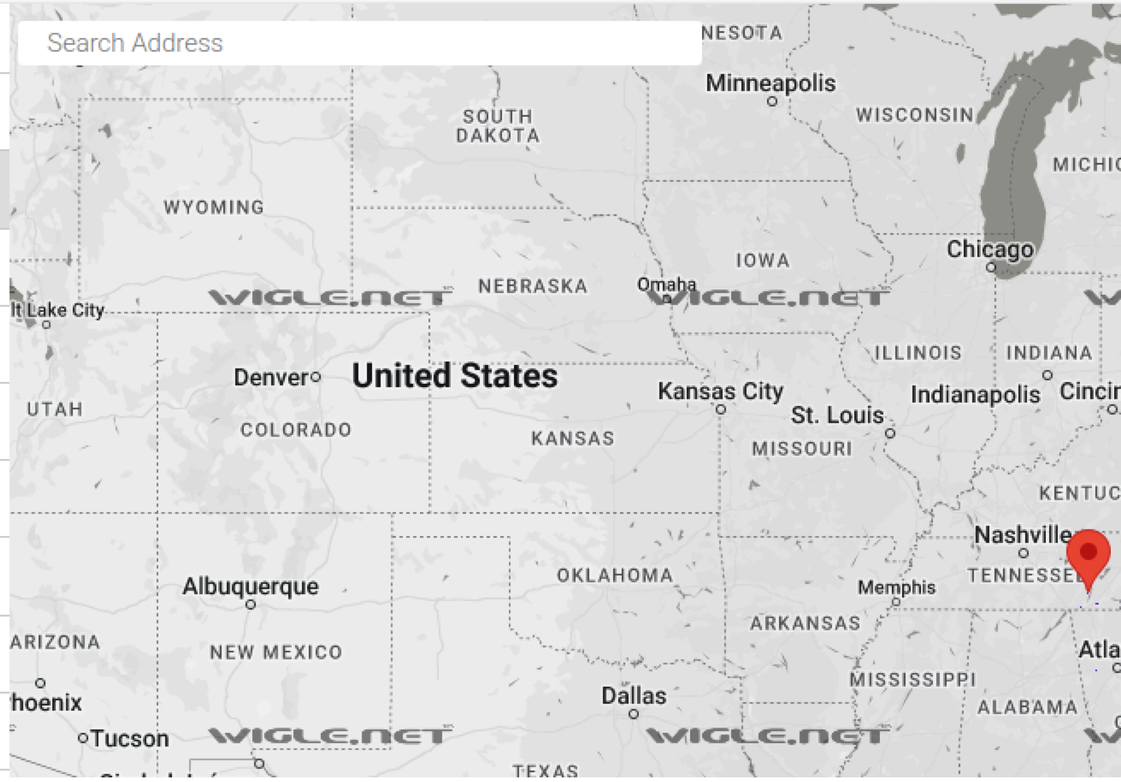
FMM00A_8585657 QoS: **0** type: **BT**
00:1e:42:58:23:6f ? 2023-04-19 - 2023-04-19

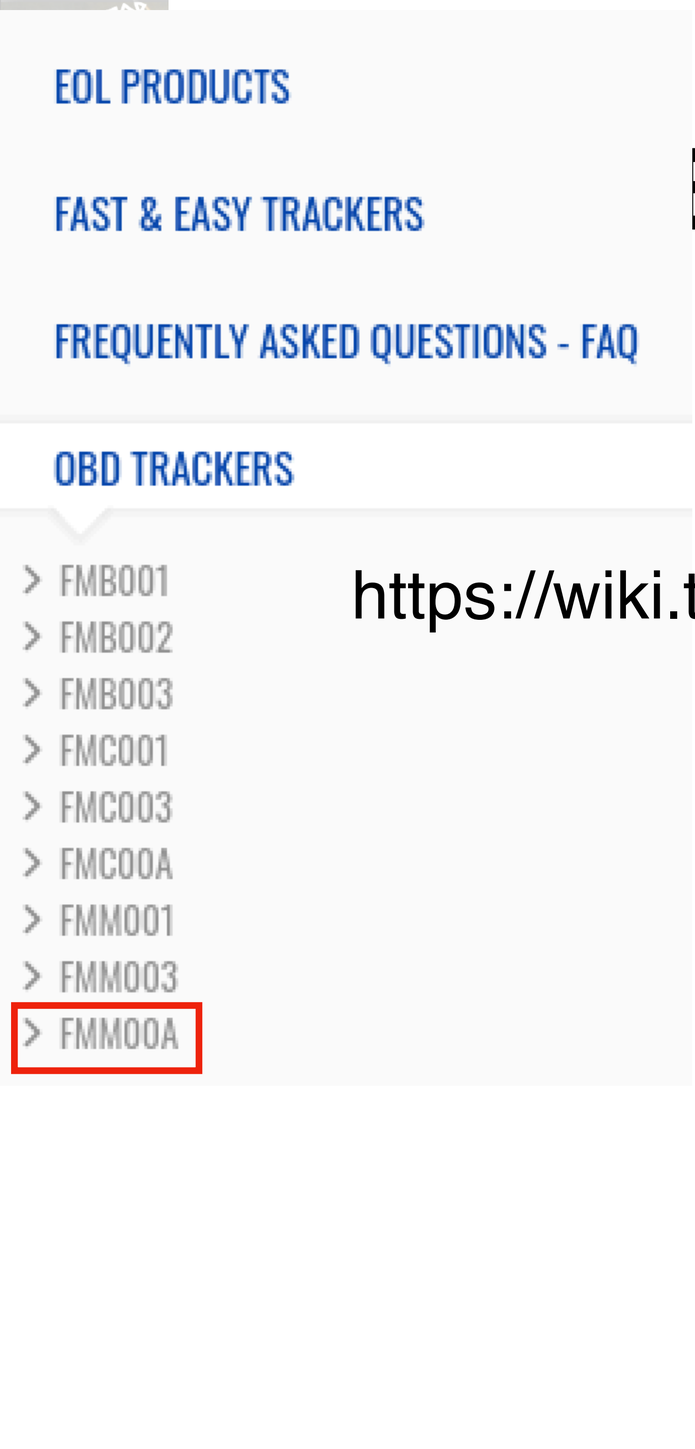
FMM00A_8682488 QoS: **0** type: **BT**
00:1e:42:58:a8:0f ? 2023-05-09 - 2023-05-09

FMM00A_8682488 QoS: **0** type: **BT**
00:1e:42:59:88:4e ? 2023-05-23 - 2023-05-23

FMM00A_8585657 QoS: **0** type: **BT**
00:1e:42:5a:1c:07 ? 2023-06-06 - 2023-06-06

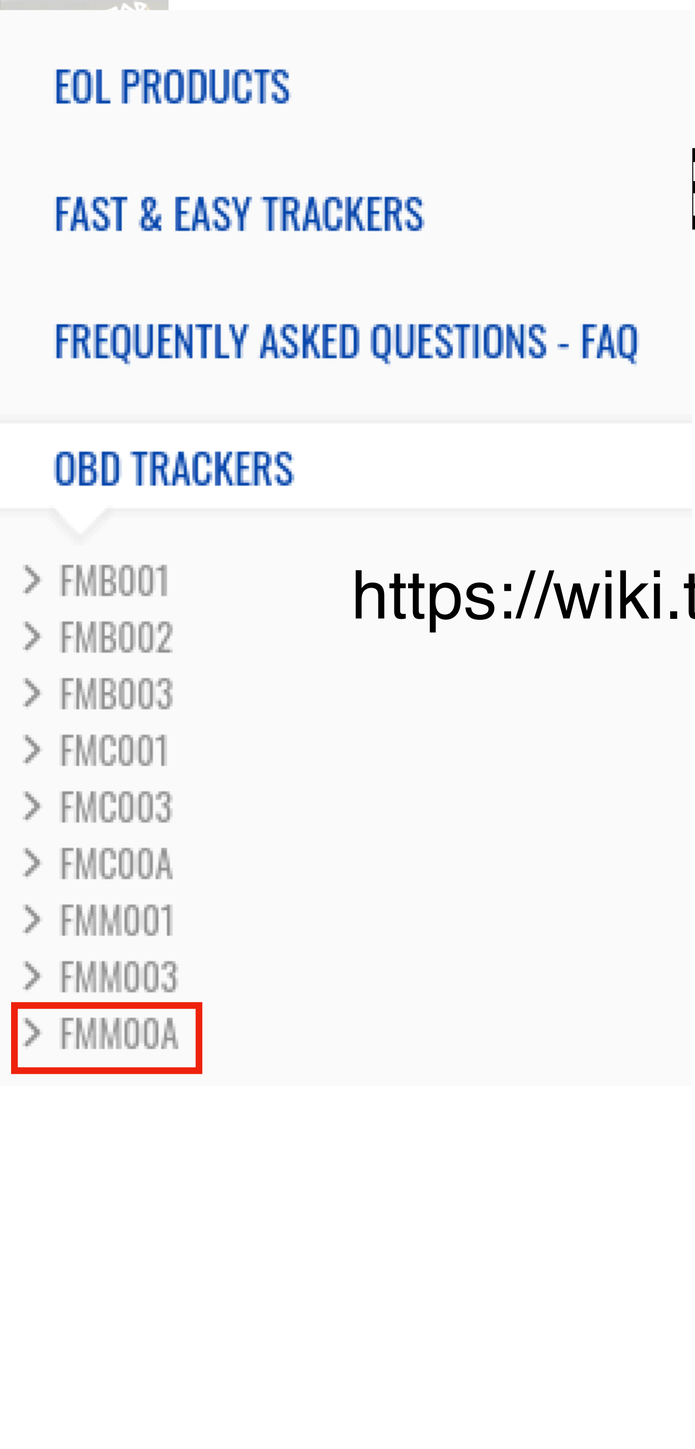
FMM00A_8585657 QoS: **0** type: **BT**
00:1e:42:5b:07:a8 ? 2023-04-30 - 2023-04-30





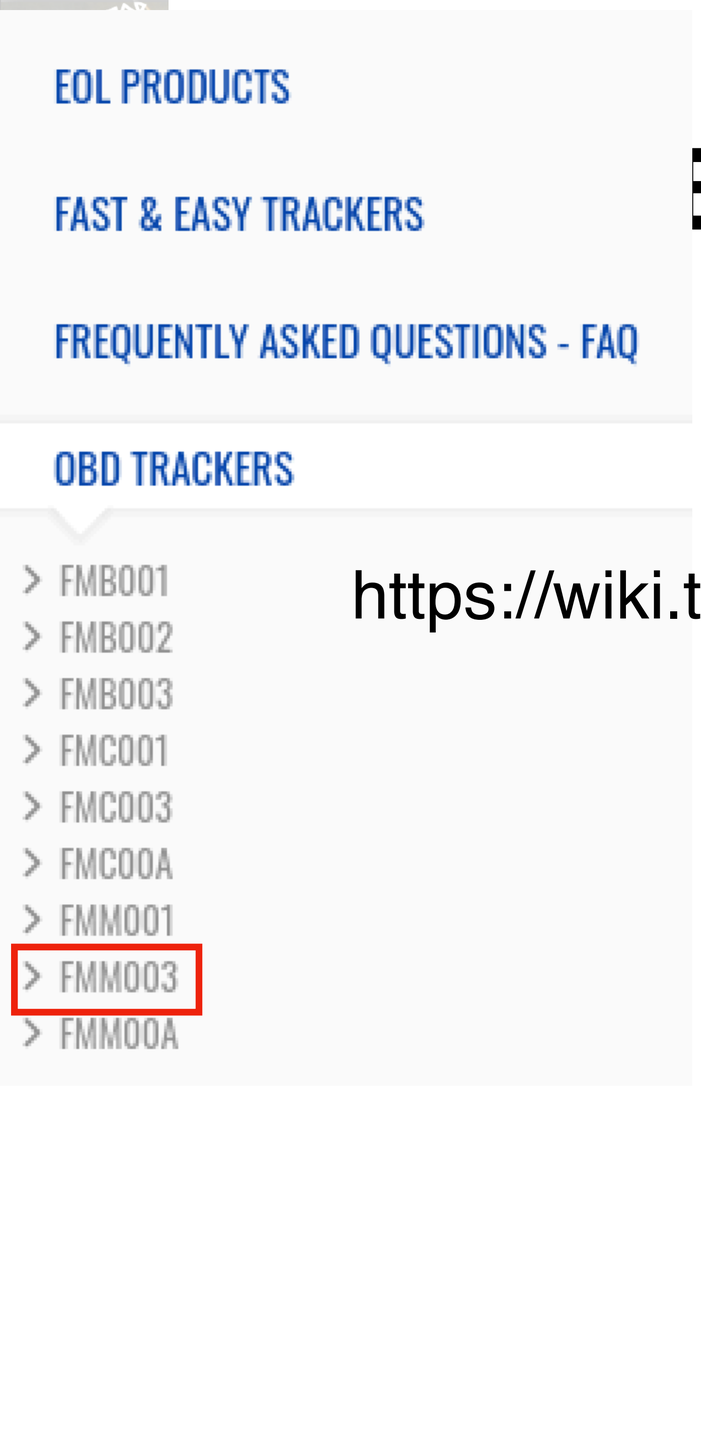
Beget Names

https://wiki.teltonika-gps.com/view/FMM00A_Bluetooth_settings



Beget Names

https://wiki.teltonika-gps.com/view/FMM00A_Bluetooth_settings



Beget Names

https://wiki.teltonika-gps.com/view/FMM00A_Bluetooth_settings

search for networks

WiFi | Cell | BT

Lat: 36.4227 to: 62.7957

Lon: -12.8051 to: 24.9878

Last Updated: 20010925174546

BSSID/MAC: 0A:2C:EF:3D:25:1B or 0A:2C

Network Name (wildcards[1]: % and _):

FMM003%

Only Nets I Was the First to See

- FMC001
- FMC003
- FMC00A
- FMM001
- FMM003
- FMM00A

FMM003_2524025 QoS: **2** type: **BT**
00:1e:42:2c:b1:10 ? 2022-09-25 - 2022-12-03

FMM003_2524025 QoS: **0** type: **BT**
00:1e:42:2d:8f:f0 ? 2022-12-03 - 2022-12-02

FMM003_2524025 QoS: **0** type: **BT**
00:1e:42:32:92:03 ? 2022-10-30 - 2022-10-29

FMM003_2524025 QoS: **0** type: **BT**
00:1e:42:32:c6:73 ? 2022-10-08 - 2022-10-08

FMM003_6805451 QoS: **0** type: **BT**
00:1e:42:5b:c0:4d ? 2023-05-01 - 2023-05-01

FMM003_DTM449 QoS: **0** type: **BT**
00:1e:42:5c:dc:68 ? 2023-05-23 - 2023-05-23

FMM003_6805451 QoS: **0** type: **BT**
00:1e:42:5e:db:6b ? 2023-02-20 - 2023-02-20

FMM003_6735591 QoS: **0** type: **BT**
4d:05:95:2b:62:61 ? 2019-01-15 - 2023-05-05

View | Uploads | Info | Stats | Tools

search for networks

WiFi | Cell | BT

Lat: 36.4227 **to:** 62.7957

Lon: -12.8051 **to:** 24.9878

Last Updated: 20010925174546

BSSID/MAC: 0A:2C:EF:3D:25:1B or 0A:2C

Network Name (wildcards[1]: % and _):

FMM003%

☐ **Only Nets I Was the First to See**

> FMC001

> FMC003

FMM003_2524025 QoS: **2** type: **BT**
00:1e:42:2c:b1:10 ? 2022-09-25 - 2022-12-03

FMM003_2524025 QoS: **0** type: **BT**
00:1e:42:2d:8f:f0 ? 2022-12-03 - 2022-12-02

FMM003_2524025 QoS: **0** type: **BT**
00:1e:42:32:92:03 ? 2022-10-30 - 2022-10-29

FMM003_2524025 QoS: **0** type: **BT**
00:1e:42:32:c6:73 ? 2022-10-08 - 2022-10-08

FMM003_6805451 QoS: **0** type: **BT**
00:1e:42:5b:c0:4d ? 2023-05-01 - 2023-05-01

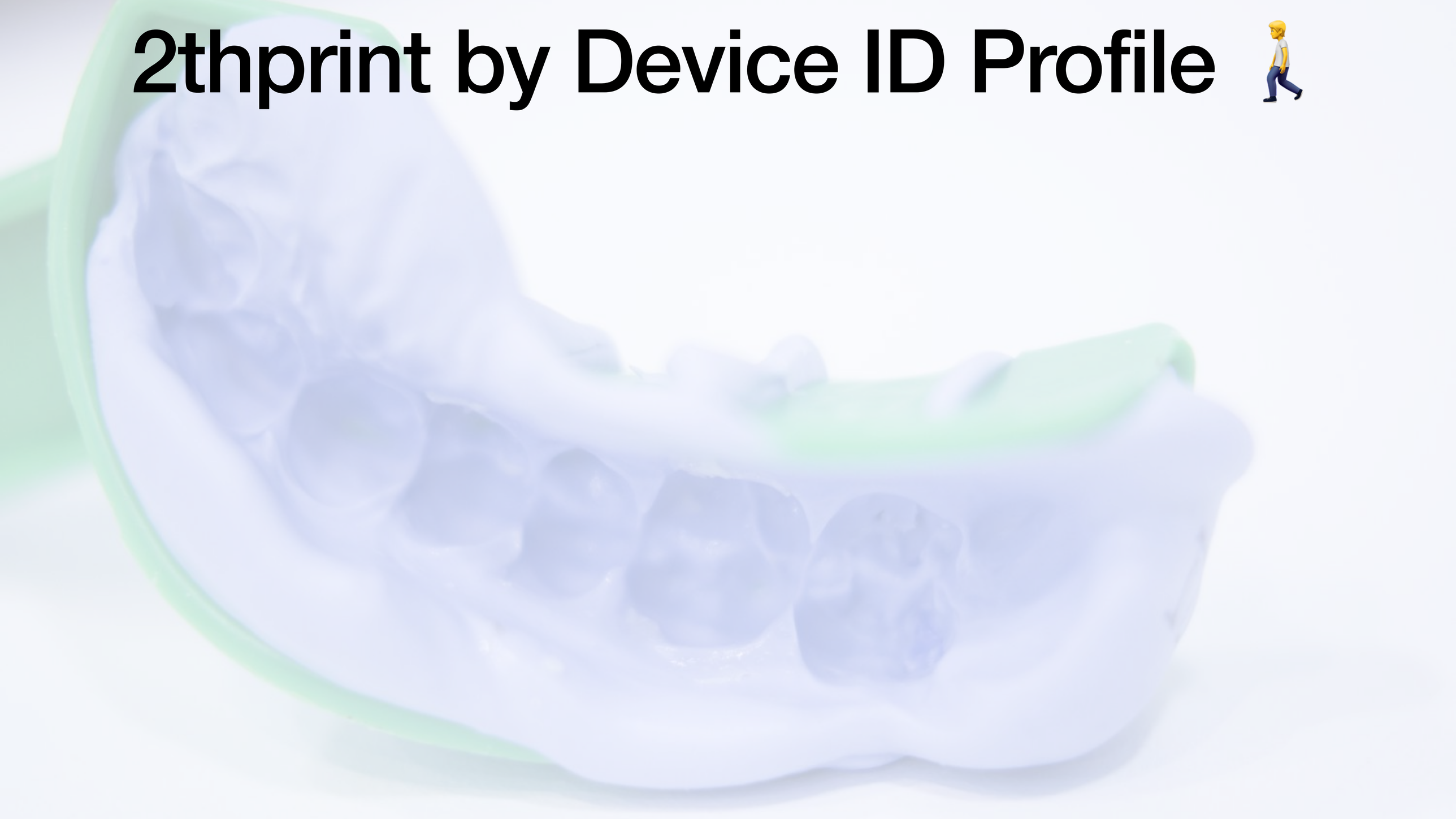
FMM003_DTM449 QoS: **0** type: **BT**
00:1e:42:5c:dc:68 ? 2023-05-23 - 2023-05-23

FMM003_6805451 QoS: **0** type: **BT**
00:1e:42:5e:db:6b ? 2023-02-20 - 2023-02-20

FMM003_6735591 QoS: **0** type: **BT**
4d:05:95:2b:62:61 ? 2019-01-15 - 2023-05-05


```
"Morey (Teltonika by BDADDR) MCX201 telematics LTE/GNSS/BLE tracker (https://www.moreycorp.com/products/mcx201/, http://3.126.97.106/view/MCX201_First_Start, saw two different BDADDRs with the same last 7...)","^MCX201_[0-9]{7}$"
"Teltonika FMM00A telematics tracker (https://wiki.teltonika-gps.com/view/FMM00A_Bluetooth_settings)","^FMM00A_[0-9]{7}$"
"Teltonika FMB122 telematics tracker (https://wiki.teltonika-gps.com/view/FMB122_Bluetooth_settings)","^FMB122_[0-9]{7}$"
"Teltonika FMB110 telematics tracker (Based on naming convention, and model list here: https://wiki.teltonika-gps.com/view/FMB122_Bluetooth_settings, plus sightings in WiGLE data)","^FMB110_[0-9]{7}$"
"Teltonika FMB120 telematics tracker (Based on naming convention, and model list here: https://wiki.teltonika-gps.com/view/FMB122_Bluetooth_settings, plus sightings in WiGLE data)","^FMB120_[0-9]{7}$"
"Teltonika FMB125 telematics tracker (Based on naming convention, and model list here: https://wiki.teltonika-gps.com/view/FMB122_Bluetooth_settings, plus sightings in WiGLE data)","^FMB125_[0-9]{7}$"
"Teltonika FMB130 telematics tracker (Based on naming convention, and model list here: https://wiki.teltonika-gps.com/view/FMB122_Bluetooth_settings, plus sightings in WiGLE data)","^FMB130_[0-9]{7}$"
"Teltonika FMB202 telematics tracker (Based on naming convention, and model list here: https://wiki.teltonika-gps.com/view/FMB122_Bluetooth_settings, plus sightings in WiGLE data)","^FMB202_[0-9]{7}$"
"Teltonika FMB204 telematics tracker (Based on naming convention, and model list here: https://wiki.teltonika-gps.com/view/FMB122_Bluetooth_settings, plus sightings in WiGLE data)","^FMB204_[0-9]{7}$"
"Teltonika FMB208 telematics tracker (Based on naming convention, and model list here: https://wiki.teltonika-gps.com/view/FMB122_Bluetooth_settings, plus sightings in WiGLE data)","^FMB208_[0-9]{7}$"
"Teltonika FMB209 telematics tracker (Based on naming convention, and model list here: https://wiki.teltonika-gps.com/view/FMB122_Bluetooth_settings, plus sightings in WiGLE data)","^FMB209_[0-9]{7}$"
"Teltonika FMB225 telematics tracker (Based on naming convention, and model list here: https://wiki.teltonika-gps.com/view/FMB122_Bluetooth_settings, plus sightings in WiGLE data)","^FMB225_[0-9]{7}$"
"Teltonika FMB230 telematics tracker (Based on naming convention, and model list here: https://wiki.teltonika-gps.com/view/FMB122_Bluetooth_settings, plus sightings in WiGLE data)","^FMB230_[0-9]{7}$"
"Teltonika FMC125 telematics tracker (Based on naming convention, and model list here: https://wiki.teltonika-gps.com/view/FMB122_Bluetooth_settings, plus sightings in WiGLE data)","^FMC125_[0-9]{7}$"
"Teltonika FMC130 telematics tracker (Based on naming convention, and model list here: https://wiki.teltonika-gps.com/view/FMB122_Bluetooth_settings, plus sightings in WiGLE data)","^FMC130_[0-9]{7}$"
"Teltonika FMC13A telematics tracker (Based on naming convention, and model list here: https://wiki.teltonika-gps.com/view/FMB122_Bluetooth_settings, plus sightings in WiGLE data)","^FMC13A_[0-9]{7}$"
"Teltonika FMC225 telematics tracker (Based on naming convention, and model list here: https://wiki.teltonika-gps.com/view/FMB122_Bluetooth_settings, plus sightings in WiGLE data)","^FMC225_[0-9]{7}$"
"Teltonika FMC230 telematics tracker (Based on naming convention, and model list here: https://wiki.teltonika-gps.com/view/FMB122_Bluetooth_settings, plus sightings in WiGLE data)","^FMC230_[0-9]{7}$"
"Teltonika FMM125 telematics tracker (Based on naming convention, and model list here: https://wiki.teltonika-gps.com/view/FMB122_Bluetooth_settings, plus sightings in WiGLE data)","^FMM125_[0-9]{7}$"
"Teltonika FMM130 telematics tracker (Based on naming convention, and model list here: https://wiki.teltonika-gps.com/view/FMB122_Bluetooth_settings, plus sightings in WiGLE data)","^FMM130_[0-9]{7}$"
"Teltonika FMM13A telematics tracker (Based on naming convention, and model list here: https://wiki.teltonika-gps.com/view/FMB122_Bluetooth_settings, plus sightings in WiGLE data)","^FMM13A_[0-9]{7}$"
"Teltonika FMM230 telematics tracker (Based on naming convention, and model list here: https://wiki.teltonika-gps.com/view/FMB122_Bluetooth_settings, plus sightings in WiGLE data)","^FMM230_[0-9]{7}$"
"Teltonika FMB001 telematics tracker (Based on naming convention, and model list here: https://wiki.teltonika-gps.com/view/FMM00A_Bluetooth_settings, plus sightings in WiGLE data)","^FMB001_[0-9]{7}$"
"Teltonika FMB002 telematics tracker (Based on naming convention, and model list here: https://wiki.teltonika-gps.com/view/FMM00A_Bluetooth_settings, plus sightings in WiGLE data)","^FMB002_[0-9]{7}$"
"Teltonika FMB003 telematics tracker (Based on naming convention, and model list here: https://wiki.teltonika-gps.com/view/FMM00A_Bluetooth_settings, plus sightings in WiGLE data)","^FMB003_[0-9]{7}$"
"Teltonika FMM001 telematics tracker (Based on naming convention, and model list here: https://wiki.teltonika-gps.com/view/FMM00A_Bluetooth_settings, plus sightings in WiGLE data)","^FMM001_[0-9]{7}$"
"Teltonika FMM003 telematics tracker (Based on naming convention, and model list here: https://wiki.teltonika-gps.com/view/FMM00A_Bluetooth_settings, plus sightings in WiGLE data)","^FMM003_[0-9]{7}$"
"Teltonika FMM00A telematics tracker (Based on naming convention, and model list here: https://wiki.teltonika-gps.com/view/FMM00A_Bluetooth_settings, plus sightings in WiGLE data)","^FMM00A_[0-9]{7}$"
```

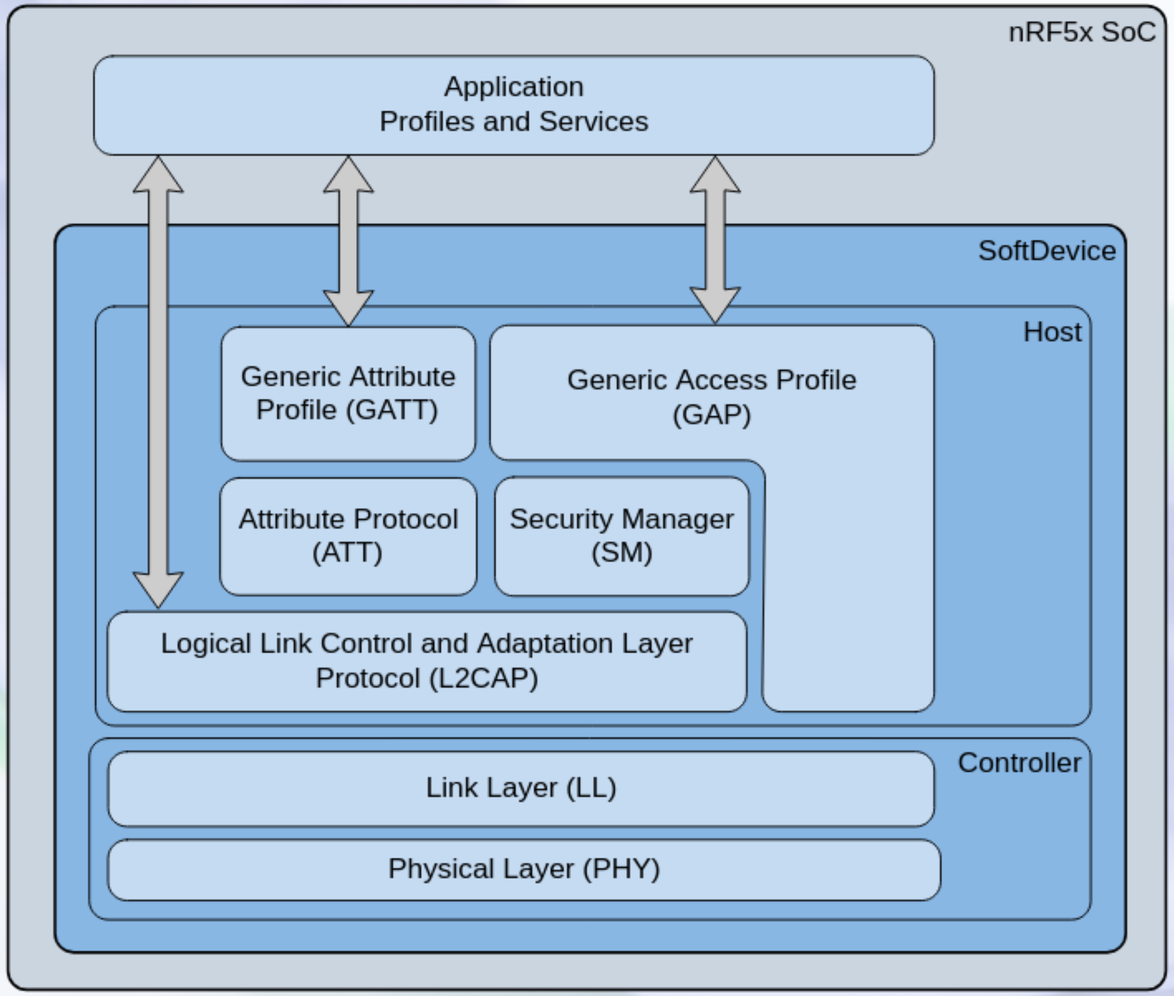
2thprint by Device ID Profile 🚶



2thprint by Device ID Profile

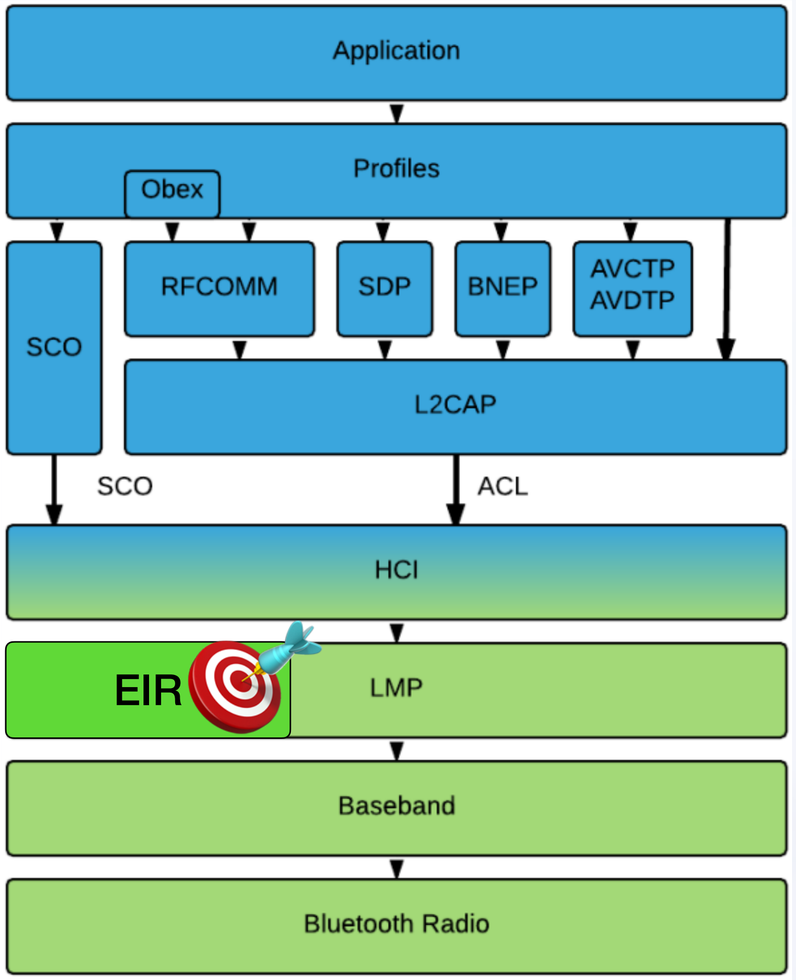
BLE

[1]



BTC

[2]



[1] https://infocenter.nordicsemi.com/index.jsp?topic=%2Fsds_s140%2FSDS%2Fs1xx%2Fble_protocol_stack%2Fble_protocol_stack.html
[2] https://crosscontrol.com/manual/Bluetooth%20Documentation/content/bluetooth.html

BTC EIR Device ID

- Some devices seem to include Device ID information as shown here in BTC Extended Inquiry Response packets

5.1.10 Device Identification Profile (DID)

Applicable to Service Class UUIDs:

- PnPInformation: 0x1200

Last Modified: 2023-02-02

Attribute ID	Attribute Name
0x0200	SpecificationID
0x0201	VendorID
0x0202	ProductID
0x0203	Version
0x0204	PrimaryRecord
0x0205	VendorIDSource

First screenshot from BT Assigned Numbers document, 2nd from Wireshark
3rd from https://www.t-mobile.com/support/public-files/attachments/syncup-drive/SyncUP%20DRIVE%207000T1%20User%20Manual_%20EN.pdf

BTC EIR Device ID

- Some devices seem to include Device ID information as shown here in BTC Extended Inquiry Response packets
  - Despite the fact that I can't find anything in the spec saying that's supposed to be a thing? (The "Supplement to the Bluetooth Core Specification" doesn't list it as valid...)

5.1.10 Device Identification Profile (DID)

Applicable to Service Class UUIDs:

- PnPInformation: 0x1200

Last Modified: 2023-02-02

Attribute ID	Attribute Name
0x0200	SpecificationID
0x0201	VendorID
0x0202	ProductID
0x0203	Version
0x0204	PrimaryRecord
0x0205	VendorIDSource

First screenshot from BT Assigned Numbers document, 2nd from Wireshark
3rd from https://www.t-mobile.com/support/public-files/attachments/syncup-drive/SyncUP%20DRIVE%207000T1%20User%20Manual_%20EN.pdf

BTC EIR Device ID

- Some devices seem to include Device ID information as shown here in BTC Extended Inquiry Response packets
  - Despite the fact that I can't find anything in the spec saying that's supposed to be a thing? (The "Supplement to the Bluetooth Core Specification" doesn't list it as valid...)
- If VendorIDSource = 1, the VendorID is looked up in the Bluetooth assigned company IDs. If it's 2, it's looked up in the USB assigned company IDs

5.1.10 Device Identification Profile (DID)

Applicable to Service Class UUIDs:

- PnPInformation: 0x1200

Last Modified: 2023-02-02

Attribute ID	Attribute Name
0x0200	SpecificationID
0x0201	VendorID
0x0202	ProductID
0x0203	Version
0x0204	PrimaryRecord
0x0205	VendorIDSource

First screenshot from BT Assigned Numbers document, 2nd from Wireshark
3rd from https://www.t-mobile.com/support/public-files/attachments/syncup-drive/SyncUP%20DRIVE%207000T1%20User%20Manual_%20EN.pdf

BTC EIR Device ID

- Some devices seem to include Device ID information as shown here in BTC Extended Inquiry Response packets
  - Despite the fact that I can't find anything in the spec saying that's supposed to be a thing? (The "Supplement to the Bluetooth Core Specification" doesn't list it as valid...)
- If VendorIDSource = 1, the VendorID is looked up in the Bluetooth assigned company IDs. If it's 2, it's looked up in the USB assigned company IDs

5.1.10 Device Identification Profile (DID)

Applicable to Service Class UUIDs:

- PnPInformation: 0x1200

Last Modified: 2023-02-02

Attribute ID	Attribute Name
0x0200	SpecificationID
0x0201	VendorID
0x0202	ProductID
0x0203	Version
0x0204	PrimaryRecord
0x0205	VendorIDSource

First screenshot from BT Assigned Numbers document, 2nd from Wireshark
3rd from https://www.t-mobile.com/support/public-files/attachments/syncup-drive/SyncUP%20DRIVE%207000T1%20User%20Manual_%20EN.pdf

BTC EIR Device ID

- Some devices seem to include Device ID information as shown here in BTC Extended Inquiry Response packets
  - Despite the fact that I can't find anything in the spec saying that's supposed to be a thing? (The "Supplement to the Bluetooth Core Specification" doesn't list it as valid...)
- If VendorIDSource = 1, the VendorID is looked up in the Bluetooth assigned company IDs. If it's 2, it's looked up in the USB assigned company IDs

5.1.10 Device Identification Profile (DID)

Applicable to Service Class UUIDs:

- PnPInformation: 0x1200

Last Modified: 2023-02-02

Attribute ID	Attribute Name
0x0200	SpecificationID
0x0201	VendorID
0x0202	ProductID
0x0203	Version
0x0204	PrimaryRecord
0x0205	VendorIDSource

First screenshot from BT Assigned Numbers document, 2nd from Wireshark
3rd from https://www.t-mobile.com/support/public-files/attachments/syncup-drive/SyncUP%20DRIVE%207000T1%20User%20Manual_%20EN.pdf

BTC EIR Device ID

- Some devices seem to include Device ID information as shown here in BTC Extended Inquiry Response packets
  - Despite the fact that I can't find anything in the spec saying that's supposed to be a thing? (The "Supplement to the Bluetooth Core Specification" doesn't list it as valid...)
- If VendorIDSource = 1, the VendorID is looked up in the Bluetooth assigned company IDs. If it's 2, it's looked up in the USB assigned company IDs

```
Extended Inquiry Response Data
  Device Name: SD-7000T_96
    Length: 12
    Type: Device Name (0x09)
    Device Name: SD-7000T_96
  Tx Power Level
    Length: 2
    Type: Tx Power Level (0x0a)
    Power Level (dBm): 6
  Device ID / Security Manager TK Value
    Length: 9
    Type: Device ID / Security Manager TK Value (0x10)
    Vendor ID Source: USB Implementer's Forum (0x0002)
    Vendor ID: Linux Foundation (0x1d6b)
    Product ID: 0x0246 (Unknown)
    Version: 0x053c
```

Last Modified: 2023-02-02

Attribute ID	Attribute Name
0x0200	SpecificationID
0x0201	VendorID
0x0202	ProductID
0x0203	Version
0x0204	PrimaryRecord
0x0205	VendorIDSource

First screenshot from BT Assigned Numbers document, 2nd from Wireshark
3rd from https://www.t-mobile.com/support/public-files/attachments/syncup-drive/SyncUP%20DRIVE%207000T1%20User%20Manual_%20EN.pdf

BTC EIR Device ID

SyncUP DRIVE connected by T-Mobile

Product: SD-7000T1

User Manual

```
Extended Inquiry Response Data
  Device Name: SD-7000T_96
      Length: 12
      Type: Device Name (0x09)
      Device Name: SD-7000T_96
  Tx Power Level
      Length: 2
      Type: Tx Power Level (0x0a)
      Power Level (dBm): 6
  Device ID / Security Manager TK Value
      Length: 9
      Type: Device ID / Security Manager TK Value (0x10)
      Vendor ID Source: USB Implementer's Forum (0x0002)
      Vendor ID: Linux Foundation (0x1d6b)
      Product ID: 0x0246 (Unknown)
      Version: 0x053c
```

- Some devices seem to include Device ID information as shown here in BTC Extended Inquiry Response packets
  - Despite the fact that I can't find anything in the spec saying that's supposed to be a thing? (The "Supplement to the Bluetooth Core Specification" doesn't list it as valid...)
- If VendorIDSource = 1, the VendorID is looked up in the Bluetooth assigned company IDs. If it's 2, it's looked up in the USB assigned company IDs

Last Modified: 2023-02-02

Attribute ID	Attribute Name
0x0200	SpecificationID
0x0201	VendorID
0x0202	ProductID
0x0203	Version
0x0204	PrimaryRecord
0x0205	VendorIDSource

First screenshot from BT Assigned Numbers document, 2nd from Wireshark
3rd from https://www.t-mobile.com/support/public-files/attachments/syncup-drive/SyncUP%20DRIVE%207000T1%20User%20Manual_%20EN.pdf

Top 20 Vendors for BTC Device ID data

BTC - 2024-01-12

vendor_source	vendor_id_hex	company_name	frequency	
Bluetooth	0x4E8	STABILO International	4462	<- actually Samsung
USB	0x1D6B	Linux Foundation	433	
Bluetooth	0x0	Ericsson AB	95	
USB	0x44E	Alps Electric Co., Ltd	85	
Bluetooth	0xA	Qualcomm Technologies International, Ltd. (QTIL)	62	
Bluetooth	0x75	Samsung Electronics Co. Ltd.	60	
USB	0xA12	Cambridge Silicon Radio, Ltd	58	
Bluetooth	0x4C	Apple, Inc.	23	
Bluetooth	0x3E0	Actions (Zhuhai) Technology Co., Limited	21	
USB	0x108C	Robert Bosch GmbH	16	
992	0xFFFF	NULL	15	
Bluetooth	0x9E	Bose Corporation	12	
Bluetooth	0x474C	NULL	12	
USB	0x54C	Sony Corp.	5	
Bluetooth	0x850	Yealink (Xiamen) Network Technology Co.,LTD	5	
256	0x4E8	NULL	5	
USB	0xA9	NULL	4	
Bluetooth	0x418	Reserved	4	
USB	0xA	NULL	4	
Bluetooth	0x103	Bang & Olufsen A/S	4	

Top 20 Vendors for BTC Device ID data

BTC - 2024-01-12

Samsung's setting their vendor source to Bluetooth but then using their USB ID

vendor_source	vendor_id_hex	company_name	frequency	
Bluetooth	0x4E8	STABILO International	4462	<- actually Samsung
USB	0x1D6B	Linux Foundation	433	
Bluetooth	0x0	Ericsson AB	95	
USB	0x44E	Alps Electric Co., Ltd	85	
Bluetooth	0xA	Qualcomm Technologies International, Ltd. (QTIL)	62	
Bluetooth	0x75	Samsung Electronics Co. Ltd.	60	
USB	0xA12	Cambridge Silicon Radio, Ltd	58	
Bluetooth	0x4C	Apple, Inc.	23	
Bluetooth	0x3E0	Actions (Zhuhai) Technology Co., Limited	21	
USB	0x108C	Robert Bosch GmbH	16	
992	0xFFFF	NULL	15	
Bluetooth	0x9E	Bose Corporation	12	
Bluetooth	0x474C	NULL	12	
USB	0x54C	Sony Corp.	5	
Bluetooth	0x850	Yealink (Xiamen) Network Technology Co.,LTD	5	
256	0x4E8	NULL	5	
USB	0xA9	NULL	4	
Bluetooth	0x418	Reserved	4	
USB	0xA	NULL	4	
Bluetooth	0x103	Bang & Olufsen A/S	4	

- This snippet from the 4.0 spec (before they started using the Core Spec Supplement) suggests that Device ID profile information can be included in EIR

8.1 EIR DATA TYPE DEFINITIONS

This section defines the basic EIR data types. Additional EIR data types may be defined in profile specifications.

- Basically all the other data types made their way into the CSS but not this...

7 EIR Transactions to Obtain Device ID Information

If Extended Inquiry Response is supported by a given device that supports the Device ID Profile, then the device may expose the Device ID information in the Extended Inquiry Response when discoverable.

If an implementer chooses to expose a Device ID EIR record, the following Device ID attribute values shall be exposed:

Attribute	Attribute Value Type
VendorIDSource	Uint16
VendorID	Uint16
ProductID	Uint16
Version	Uint16

See section 8.2 for details on the format of the Device ID EIR Record.

From Device Identification Profile 1.3

8.2 Device ID Extended Inquiry Response

The inclusion of the Device ID EIR Record is optional. However, for each Device ID EIR Record that is included in the EIR record, a corresponding Device ID Service Record (meaning that all attributes that appear in both the Service Record and the EIR Record shall be equal) shall be included in the SDP database. The format of the Device ID EIR Record shall be as shown in Table 8.2.

Value	Notes
0x09	Length of this Data
0xTT	Device ID EIR Tag
0xYYYY	Uint16 Vendor ID Source
0xYYYY	Uint16 VendorID
0xYYYY	Uint16 ProductID
0xYYYY	Uint16 Version

Table 8.2: Device ID Extended Inquiry Response Tags

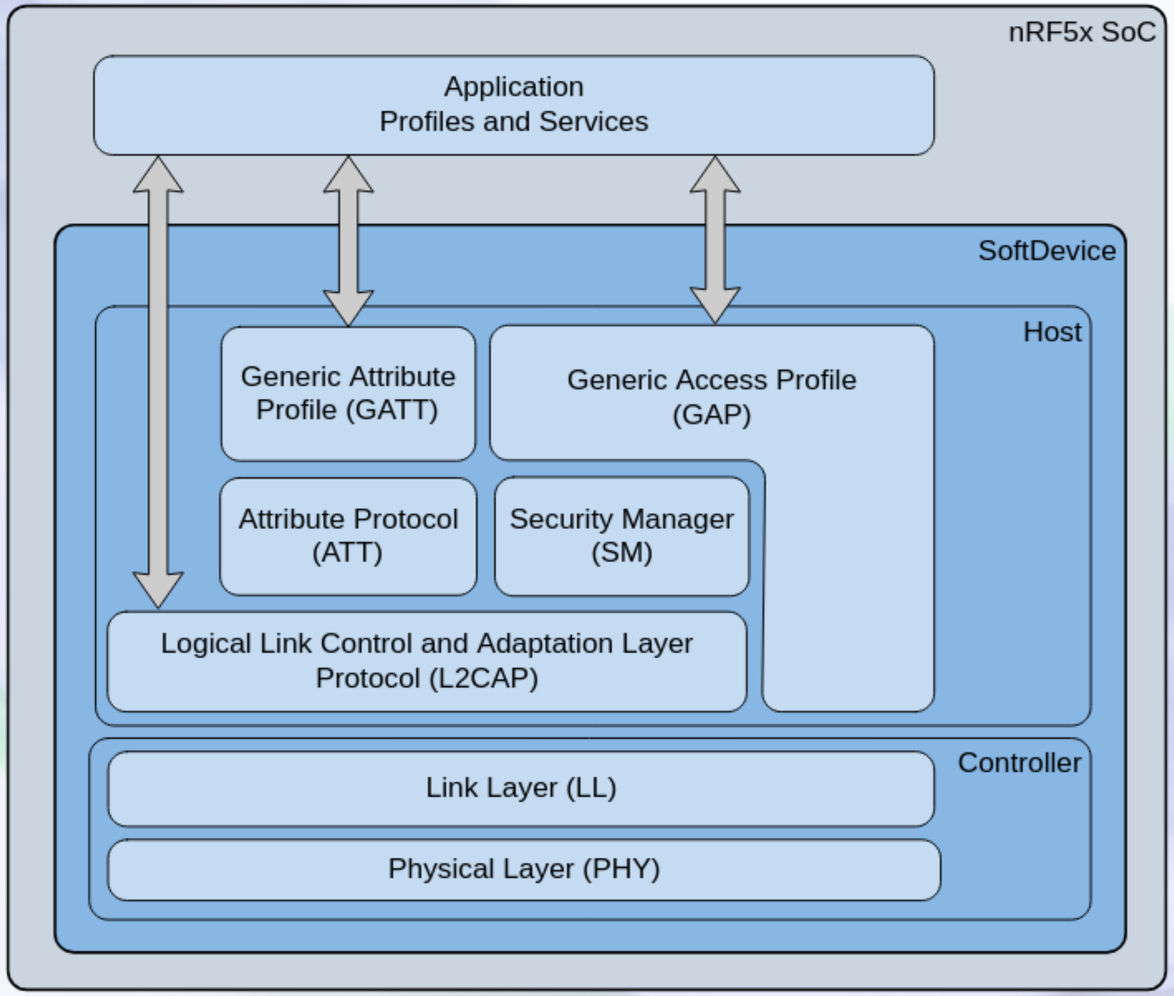
From Device Identification Profile 1.3

2thprint by UUID16 🧘‍♂️ or 🚶‍♂️

2thprint by UUID16 🧘 or 🚶

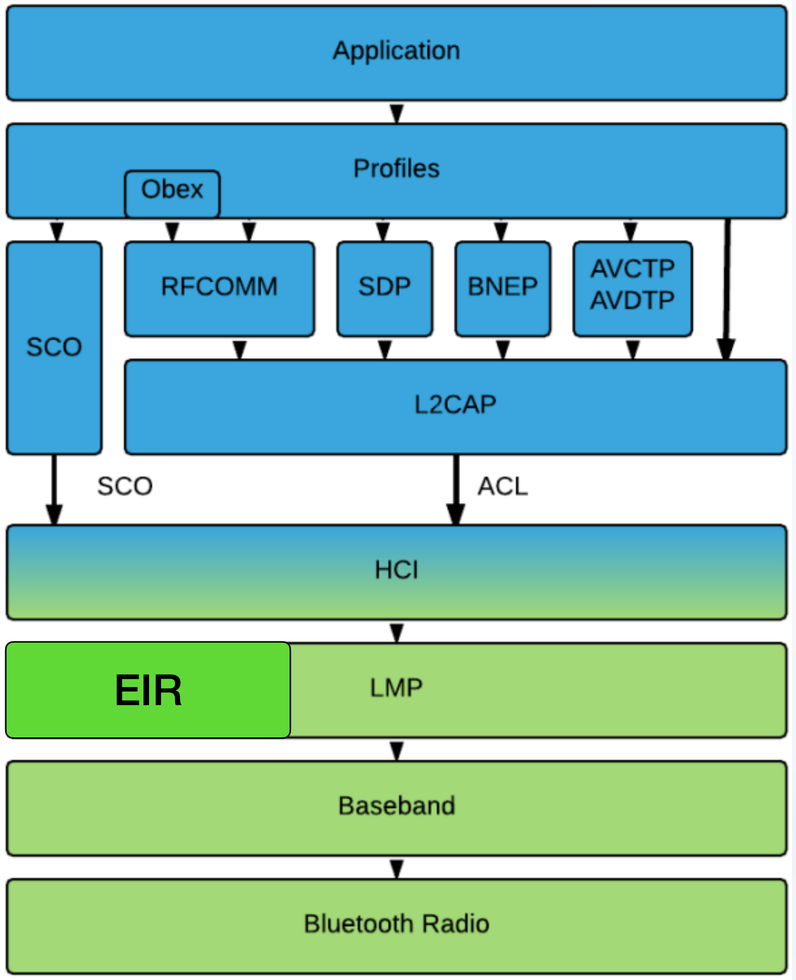
BLE

[1]



BTC

[2]

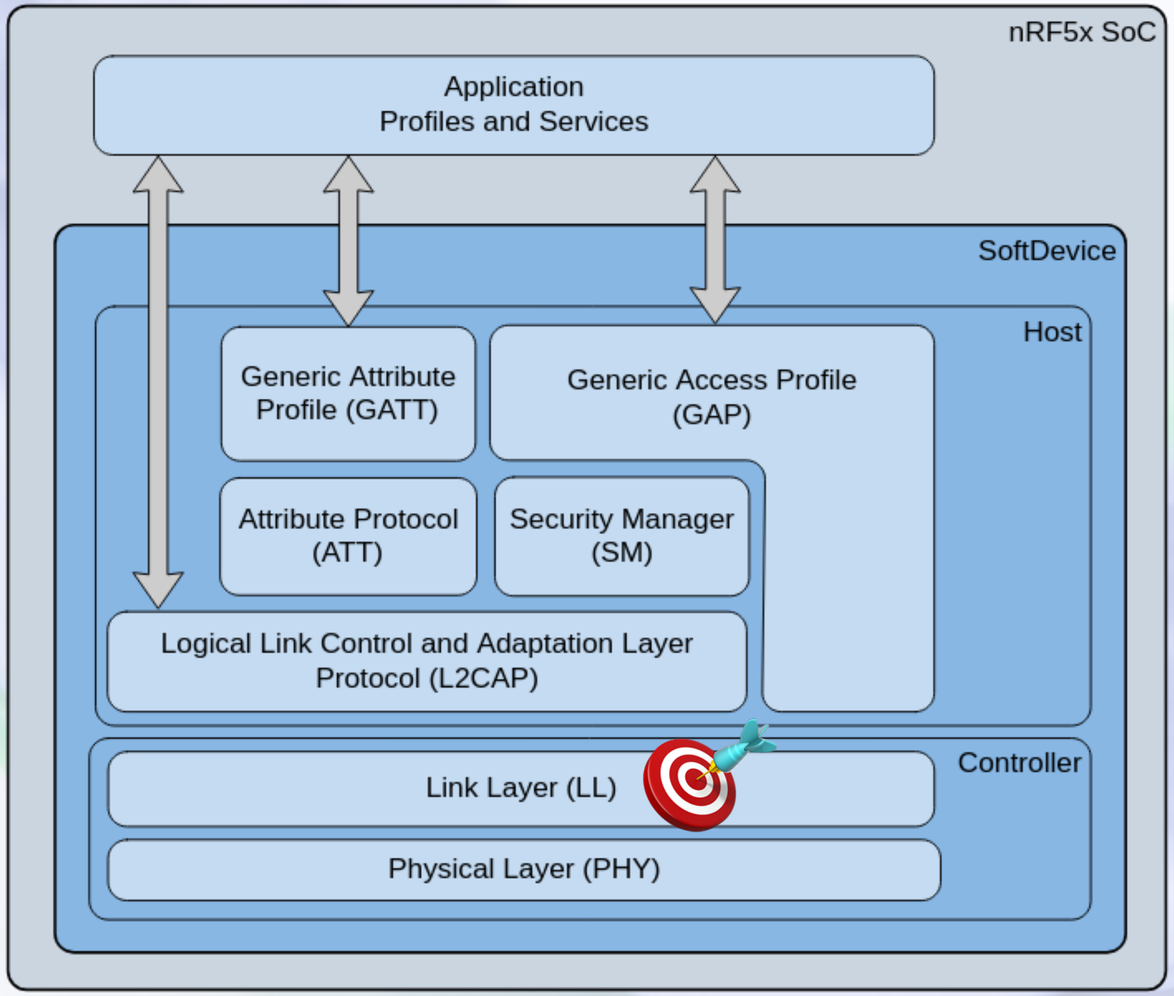


[1] https://infocenter.nordicsemi.com/index.jsp?topic=%2Fsds_s140%2FSDS%2Fs1xx%2Fble_protocol_stack%2Fble_protocol_stack.html
[2] https://crosscontrol.com/manual/Bluetooth%20Documentation/content/bluetooth.html

2thprint by UUID16 🧘 or 🚶

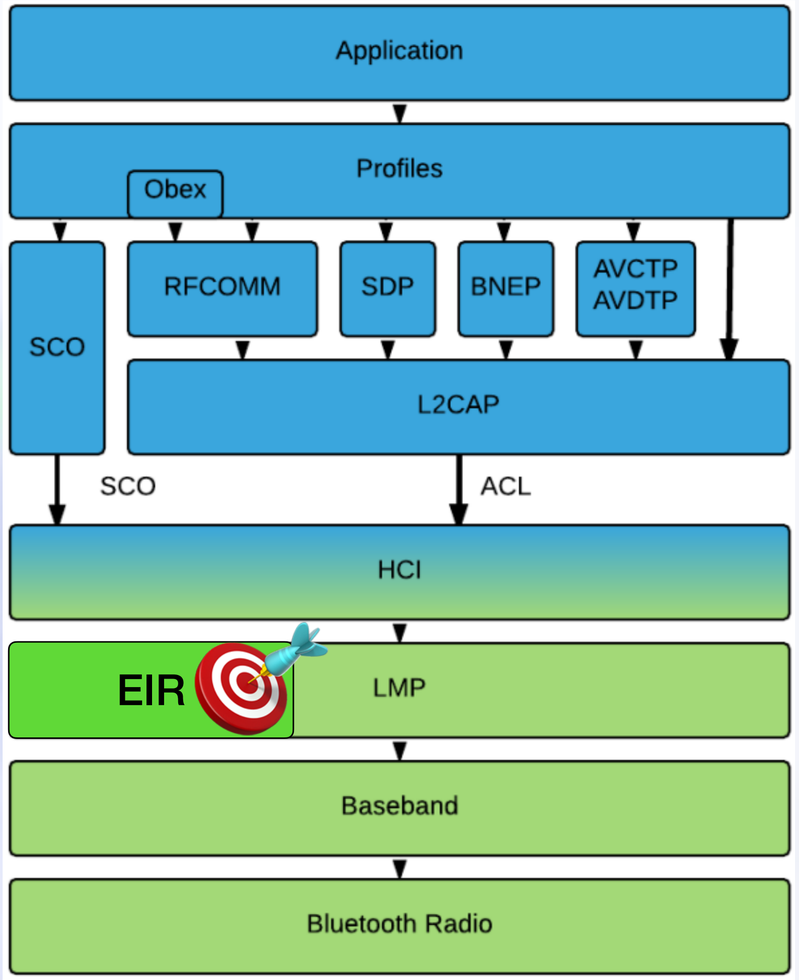
BLE

[1]



BTC

[2]



[1] https://infocenter.nordicsemi.com/index.jsp?topic=%2Fsds_s140%2FSDS%2Fs1xx%2Fble_protocol_stack%2Fble_protocol_stack.html
[2] https://crosscontrol.com/manual/Bluetooth%20Documentation/content/bluetooth.html

2thprint by UUID16

UUID16Print

- 16-bit UUIDs can be optionally included in BTC EIR packets or BLE Advertisements
- They are frequently used to advertise company-specific *services* (usually served over GATT)

```
./TellMeEverything.py --UUID16stats=quiet
----= BLUETOOTH CLASSIC RESULTS =----
count   uuid16  company
❌254   0xfe4c  Volkswagen AG
❌57    0xfe31  Volkswagen AG
❌31    0xfe35  HUAWEI Technologies Co., Ltd
❌24    0xfdd1  Huawei Technologies Co., Ltd
🍪12    0xfd69  Samsung Electronics Co., Ltd
❌1     0xfeea  Swirl Networks, Inc.

----= BLUETOOTH LOW ENERGY RESULTS =----
count   uuid16  company
❌109258   0xfef3  Google LLC
🍪108953   0xfd6f  Apple, Inc.
🍪44895    0xfd69  Samsung Electronics Co., Ltd
❌29877    0xfeed  Tile, Inc.
❌29059    0xfebe  Bose Corporation
❌13392    0xfeaa  Google LLC
❌13184    0xfe9f  Google LLC
❌12533    0xfe03  Amazon.com Services, Inc.
❌9450     0xfd5a  Samsung Electronics Co., Ltd.
❌8922     0xfe50  Google LLC
❌6642     0xfe1f  Garmin International, Inc.
❌5107     0xfe2c  Google LLC
❌4686     0xfe61  Logitech International SA
❌3903     0xfe4c  Volkswagen AG
❌3801     0xfe26  Google LLC
❌2663     0xfea0  Google LLC
❌2451     0xfd82  Sony Corporation
❌2420     0xfe78  Hewlett-Packard Company
❌2353     0xfee7  Tencent Holdings Limited.
❌2018     0xfe48  General Motors
...
```

2thprint by UUID16

UUID16Print

- 16-bit UUIDs can be optionally included in BTC EIR packets or BLE Advertisements
- They are frequently used to advertise company-specific *services* (usually served over GATT)
- Silicon vendors are *present*, but not *prevalent*

```
./TellMeEverything.py --UUID16stats=quiet
----= BLUETOOTH CLASSIC RESULTS =----
count   uuid16  company
❌254    0xfe4c  Volkswagen AG
❌57   0xfe31  Volkswagen AG
❌31   0xfe35  HUAWEI Technologies Co., Ltd
❌24   0xfdd1  Huawei Technologies Co., Ltd
🍪12   0xfd69  Samsung Electronics Co., Ltd
❌1    0xfeea  Swirl Networks, Inc.

----= BLUETOOTH LOW ENERGY RESULTS =----
count   uuid16  company
❌109258    0xfef3  Google LLC
🍪108953    0xfd6f  Apple, Inc.
🍪44895   0xfd69  Samsung Electronics Co., Ltd
❌29877   0xfeed  Tile, Inc.
❌29059   0xfebe  Bose Corporation
❌13392   0xfeaa  Google LLC
❌13184   0xfe9f  Google LLC
❌12533   0xfe03  Amazon.com Services, Inc.
❌9450    0xfd5a  Samsung Electronics Co., Ltd.
❌8922    0xfe50  Google LLC
❌6642    0xfe1f  Garmin International, Inc.
❌5107    0xfe2c  Google LLC
❌4686    0xfe61  Logitech International SA
❌3903    0xfe4c  Volkswagen AG
❌3801    0xfe26  Google LLC
❌2663    0xfea0  Google LLC
❌2451    0xfd82  Sony Corporation
❌2420    0xfe78  Hewlett-Packard Company
❌2353    0xfee7  Tencent Holdings Limited.
❌2018    0xfe48  General Motors
...
```

2thprint by UUID16

UUID16Print

- 16-bit UUIDs can be optionally included in BTC EIR packets or BLE Advertisements
- They are frequently used to advertise company-specific *services* (usually served over GATT)
- Silicon vendors are *present*, but not *prevalent*

```
./TellMeEverything.py --UUID16stats=quiet
----= BLUETOOTH CLASSIC RESULTS =----
count   uuid16  company
❌254   0xfe4c  Volkswagen AG
❌57    0xfe31  Volkswagen AG
❌31    0xfe35  HUAWEI Technologies Co., Ltd
❌24    0xfdd1  Huawei Technologies Co., Ltd
🍪12    0xfd69  Samsung Electronics Co., Ltd
❌1     0xfeea  Swirl Networks, Inc.

----= BLUETOOTH LOW ENERGY RESULTS =----
count   uuid16  company
❌109258   0xfef3  Google LLC
🍪108953   0xfd6f  Apple, Inc.
🍪44895    0xfd69  Samsung Electronics Co., Ltd
❌29877    0xfeed  Tile, Inc.
❌29059    0xfebe  Bose Corporation
❌13392    0xfeaa  Google LLC
❌13184    0xfe9f  Google LLC
❌12533    0xfe03  Amazon.com Services, Inc.
❌9450     0xfd5a  Samsung Electronics Co., Ltd.
❌8922     0xfe50  Google LLC
❌6642     0xfe1f  Garmin International, Inc.
❌5107     0xfe2c  Google LLC
❌4686     0xfe61  Logitech International SA
           0xfe4c  Volkswagen AG
           0xfe26  Google LLC
           0xfea0  Google LLC
           0xfd82  Sony Corporation
           0xfe78  Hewlett-Packard Company
           0xfee7  Tencent Holdings Limited.
           0xfe48  General Motors
...
```

```
1740   0xfee0 🍪 Anhui Huami Information Technology Co., Ltd.
1558   0xfd92 🍪 Qualcomm Technologies International, Ltd. (QTIL)
749    0xfef5 🍪 Dialog Semiconductor GmbH
216    0xfe8f 🍪 CSR
189    0xfefb 🍪 Telit Wireless Solutions (Formerly Stollmann E+V GmbH)
136    0xfef1 🍪 CSR
74     0xfe59 🍪 Nordic Semiconductor ASA
```

What I Want

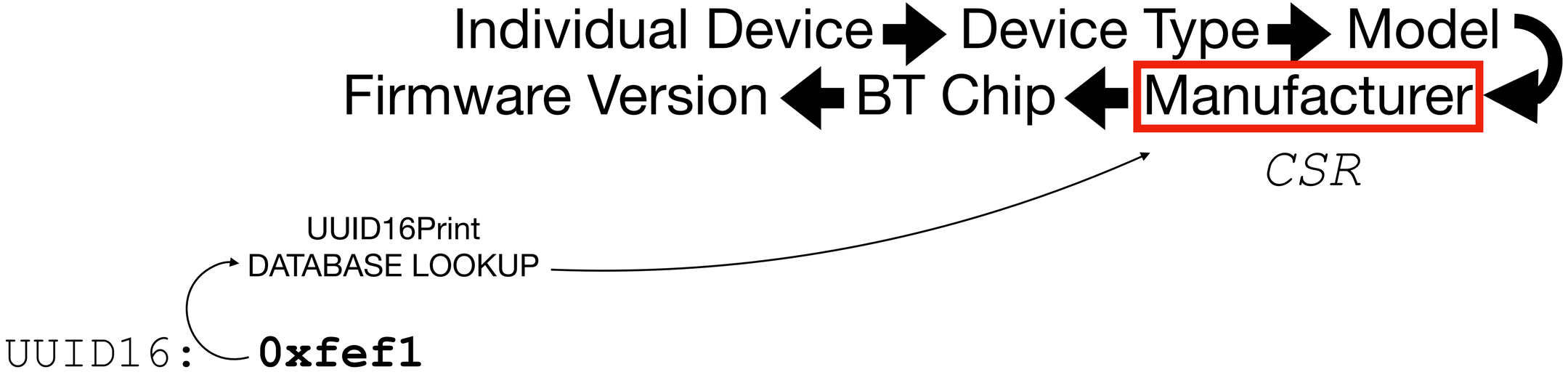
Individual Device → Device Type → Model ↷
Firmware Version ← BT Chip ← Manufacturer

What I Want

UUID16: **0xfef1**

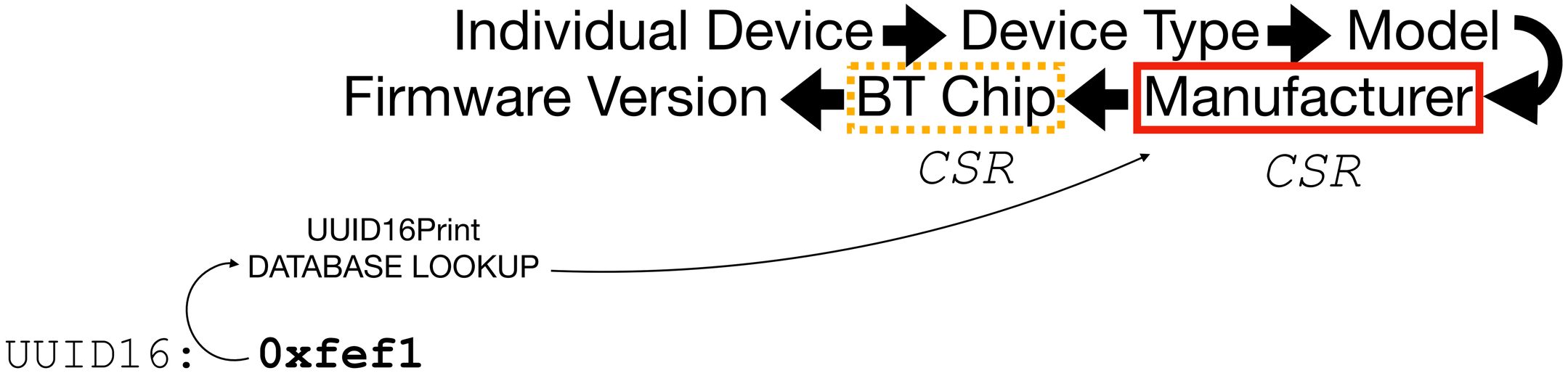

DARK MENTOR

What I Want

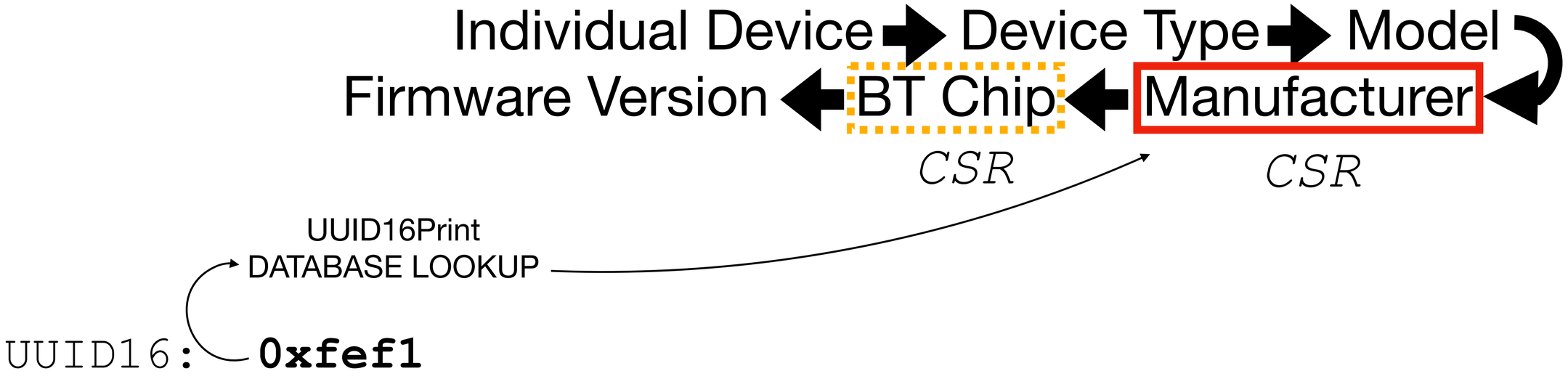

Individual Device
Device Type
Model
Firmware Version
BT Chip
Manufacturer
CSR
UUID16Print
DATABASE LOOKUP
UUID16:
0xfef1


DARK MENTOR

What I Want


Individual Device
Device Type
Model
Firmware Version
BT Chip
Manufacturer
CSR
CSR
UUID16Print
DATABASE LOOKUP
UUID16:
0xfef1

What I Want



ASSUMPTION:

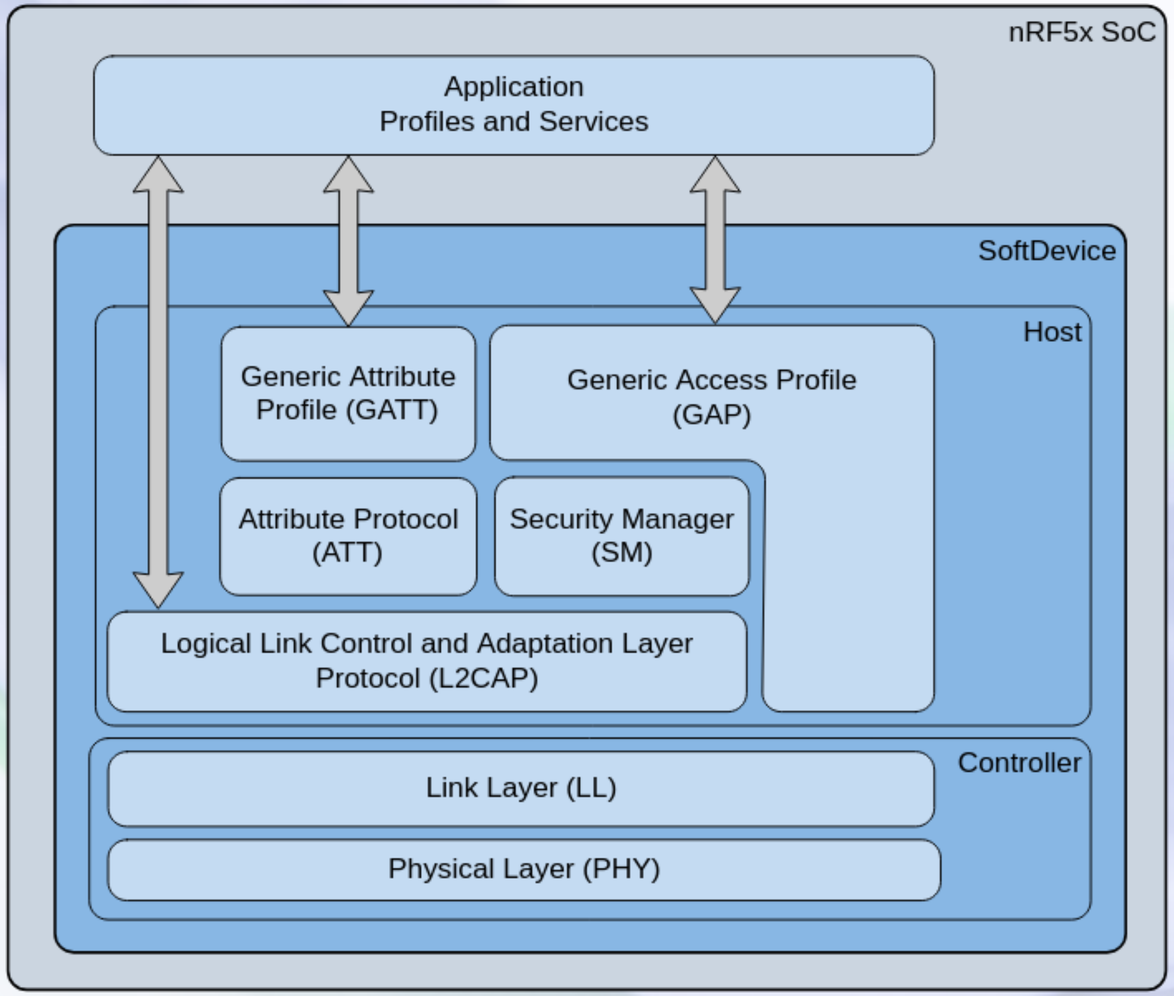
UUID16Prints are just the assigned values from the BT public/assigned_numbers/uuids/member_uuids.yaml

2thprint by UUID128 🧘‍♂️ or 🚶‍♂️

2thprint by UUID128 🧘 or 🚶

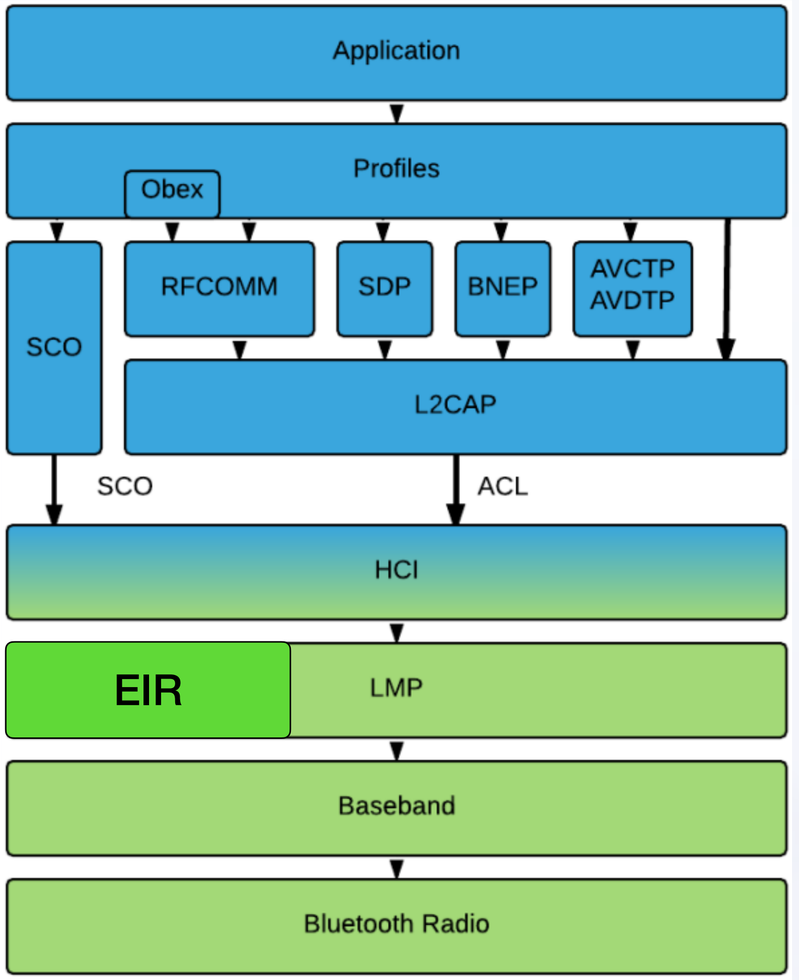
BLE

[1]



BTC

[2]

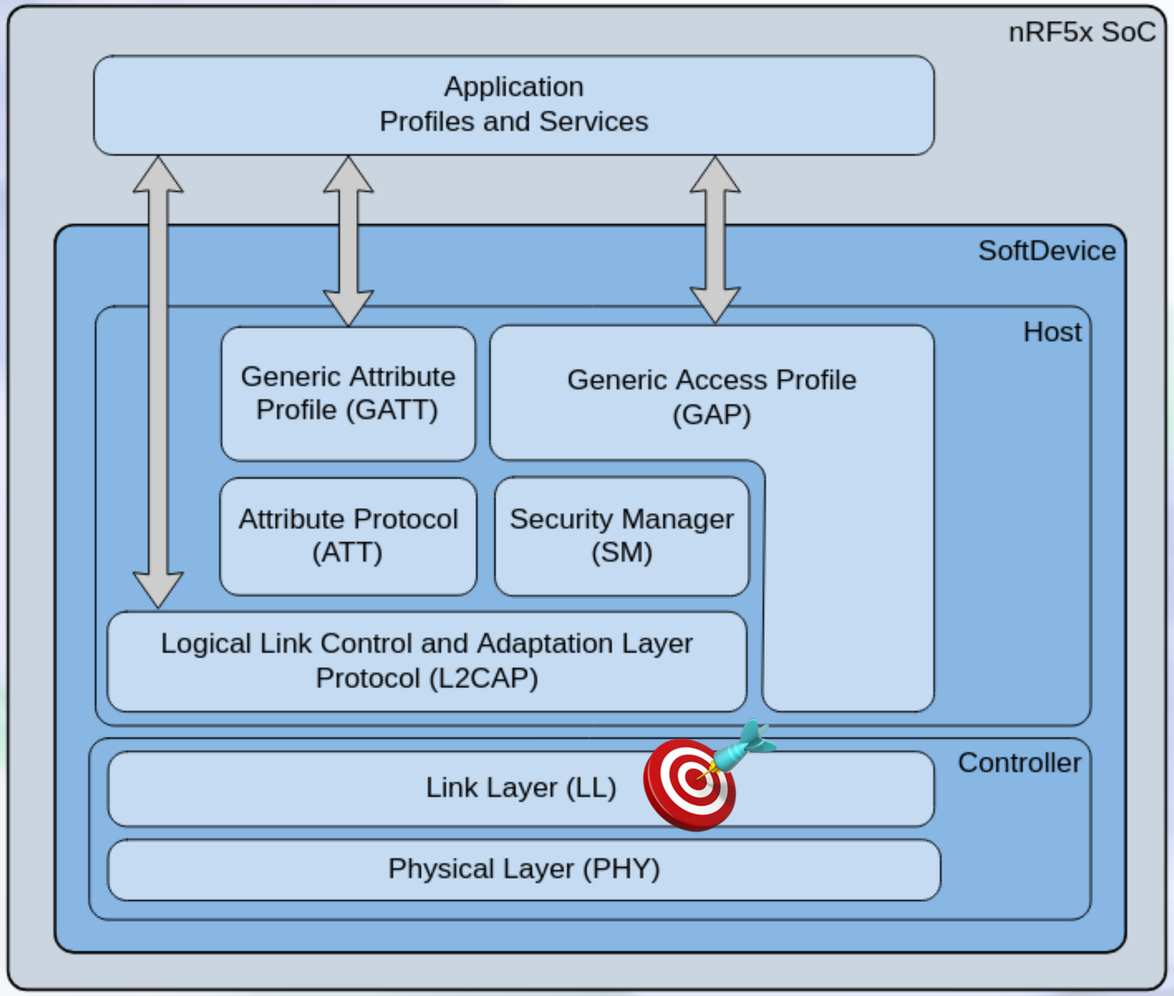


[1] https://infocenter.nordicsemi.com/index.jsp?topic=%2Fsds_s140%2FSDS%2Fs1xx%2Fble_protocol_stack%2Fble_protocol_stack.html
[2] https://crosscontrol.com/manual/Bluetooth%20Documentation/content/bluetooth.html

2thprint by UUID128 🧘 or 🚶

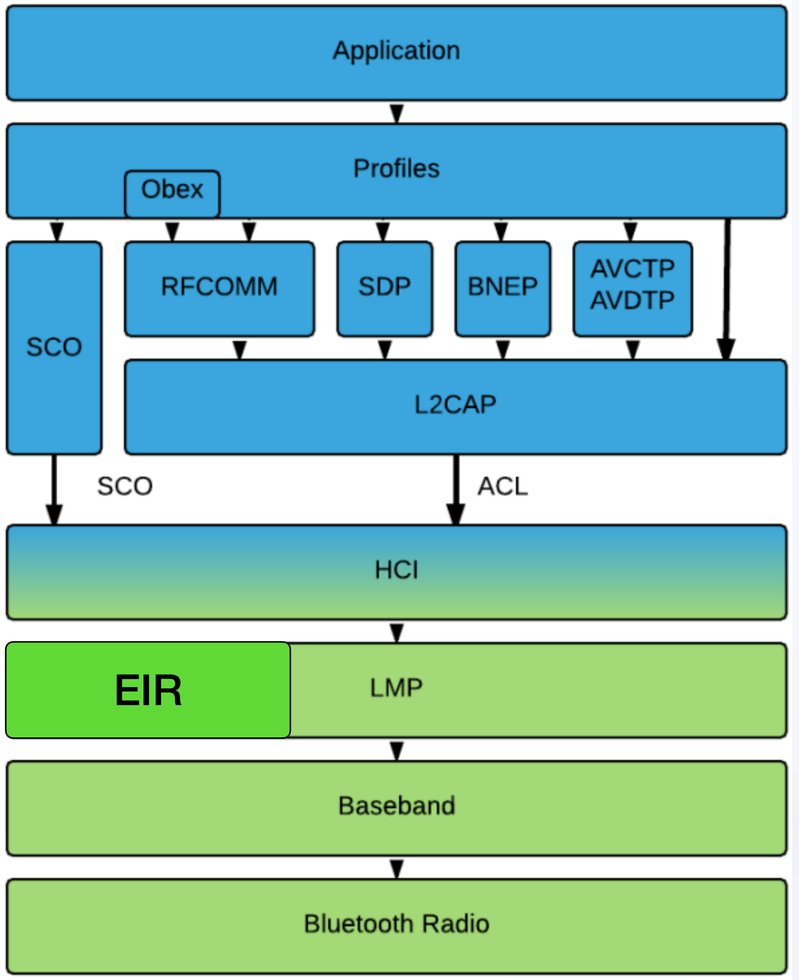
BLE

[1]



BTC

[2]

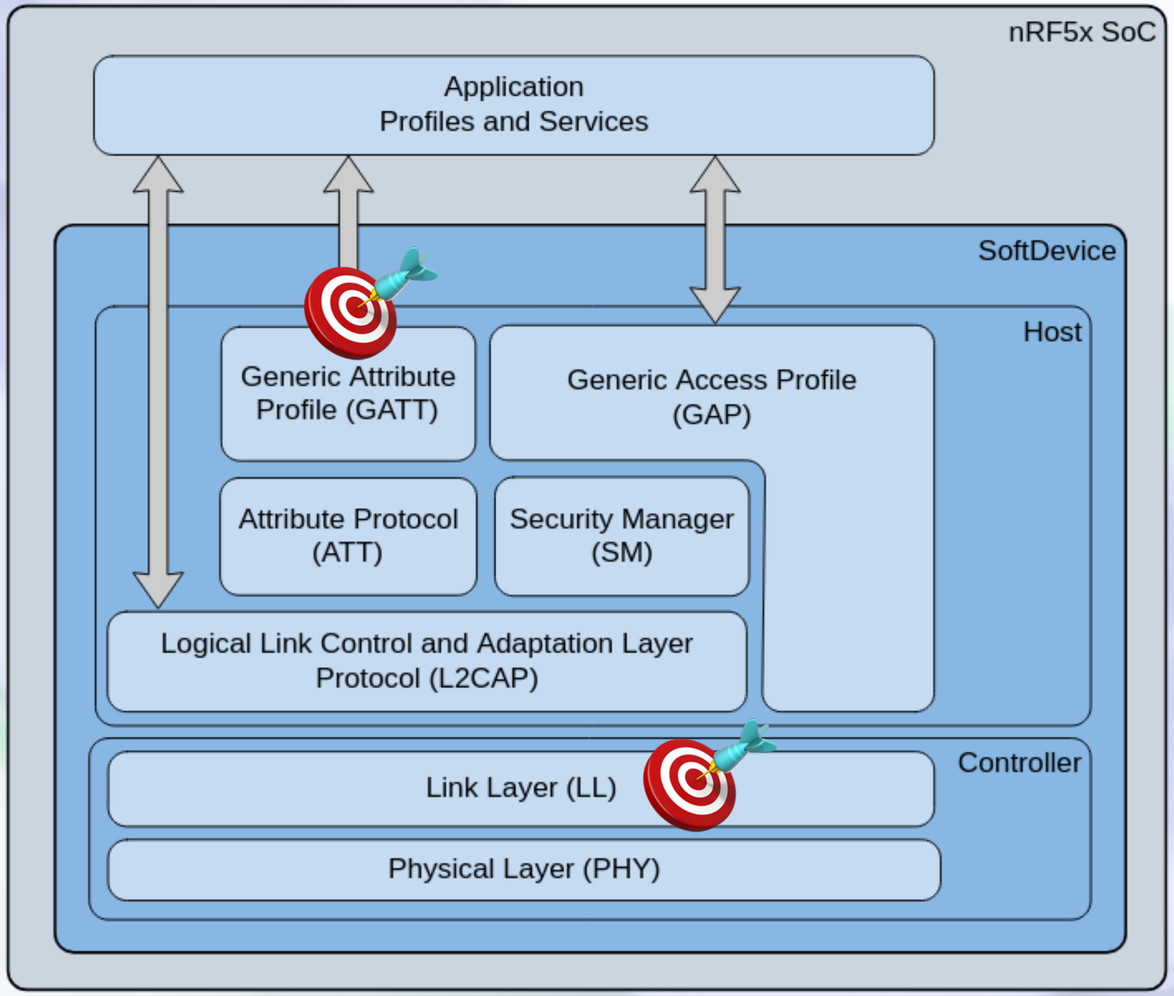


[1] https://infocenter.nordicsemi.com/index.jsp?topic=%2Fsds_s140%2FSDS%2Fs1xx%2Fble_protocol_stack%2Fble_protocol_stack.html
[2] https://crosscontrol.com/manual/Bluetooth%20Documentation/content/bluetooth.html

2thprint by UUID128 🧘 or 🚶

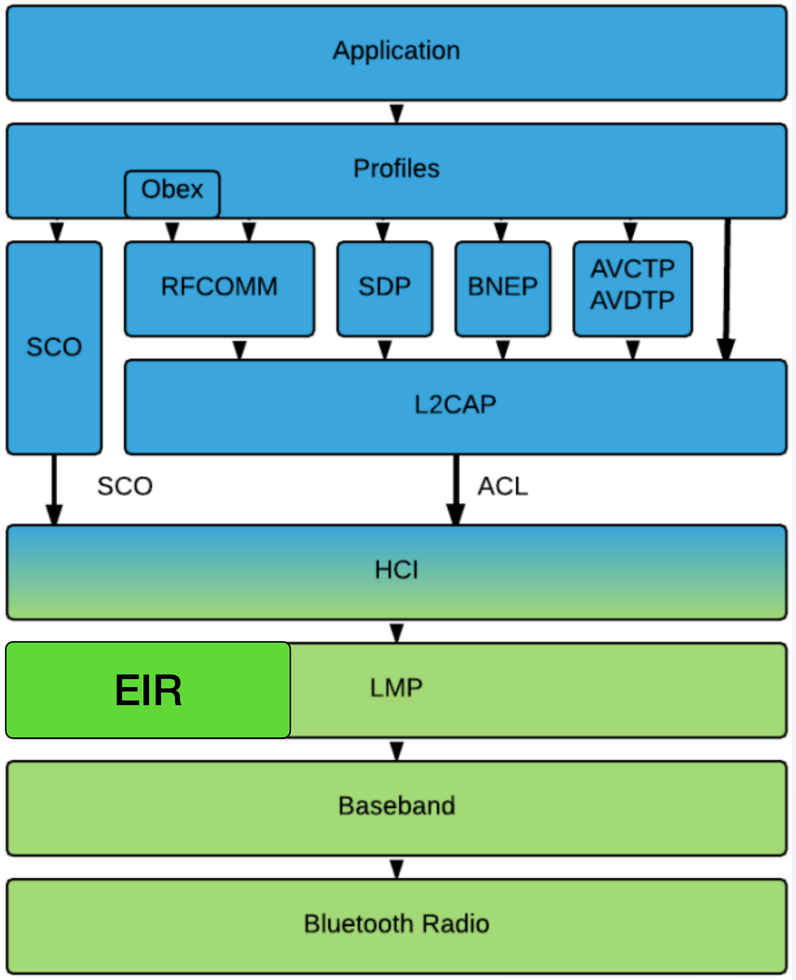
BLE

[1]



BTC

[2]



[1] https://infocenter.nordicsemi.com/index.jsp?topic=%2Fsds_s140%2FSDS%2Fs1xx%2Fble_protocol_stack%2Fble_protocol_stack.html
[2] https://crosscontrol.com/manual/Bluetooth%20Documentation/content/bluetooth.html

2thprint by UUID128

UUID128Print

- Detective Work🕵️: UUID128Print -> NamePrint

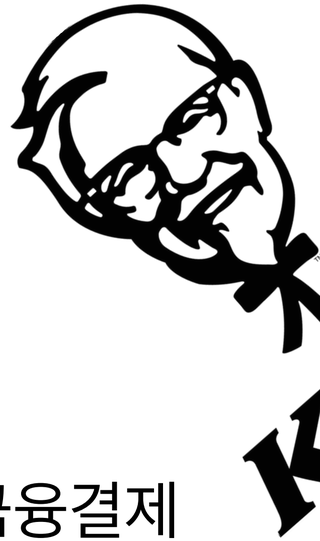
KFTC BANKPOS

Point of Sale terminal

- Regex: ^KFTC BANKPOS$
- "Korea Financial Telecommunications and Clearings Institute (Korean: 금융결제원, KFTC) is a non-profit organization which manages several inter-bank payment systems in South Korea."
  - https://en.wikipedia.org/wiki/Korea_Financial_Telecommunications_%26_Clearings_Institute

KFTC BANKPOS

Point of Sale terminal



- Regex: ^KFTC BANKPOS$
- "Korea Financial Telecommunications and Clearings Institute (Korean: 금융결제원, KFTC) is a non-profit organization which manages several inter-bank payment systems in South Korea."
  - https://en.wikipedia.org/wiki/Korea_Financial_Telecommunications_%26_Clearings_Institute

KFTC BANKPOS

Point of Sale terminal

```
For bdaddr = 04:32:f4:18:2e:d8:
        Company Name by IEEE OUI (04:32:f4): Partron

        No BTC Extended Inquiry Result Device info.

        DeviceName: KFTC BANKPOS
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        No UUID16s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x004c (Apple, Inc.) - take with a grain of salt, not all companies populate this accurately!
                         Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x4c00 (No Match)
                Raw Data: 0215585cde931b0142cc9a1325009bedc65e00010002c5
                Apple iBeacon:
                        UUID128: 585cde93-1b01-42cc-9a13-25009bedc65e
                        Major ID: 0001
                        Minor ID: 0002
                        RSSI at 1 meter: -59dBm
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
                        This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
```

KFTC BANKPOS

Point of Sale terminal

```
For bdaddr = 04:32:f4:18:48:d7:
        Company Name by IEEE OUI (04:32:f4): Partron

        No BTC Extended Inquiry Result Device info.

        No Names found.

        No UUID16s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x004c (Apple, Inc.) - take with a grain of salt, not all companies populate this accurately!
                         Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x4c00 (No Match)
                Raw Data: 0215585cde931b0142cc9a1325009bedc65e00010002c5
                Apple iBeacon:
                        UUID128: 585cde93-1b01-42cc-9a13-25009bedc65e
                        Major ID: 0001
                        Minor ID: 0002
                        RSSI at 1 meter: -59dBm
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
                        This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
```

What I Want

Individual Device → Device Type → Model ↷
Firmware Version ← BT Chip ← Manufacturer

What I Want

UUID128: **585cde93-1b01-42cc-9a13-25009bedc65e**

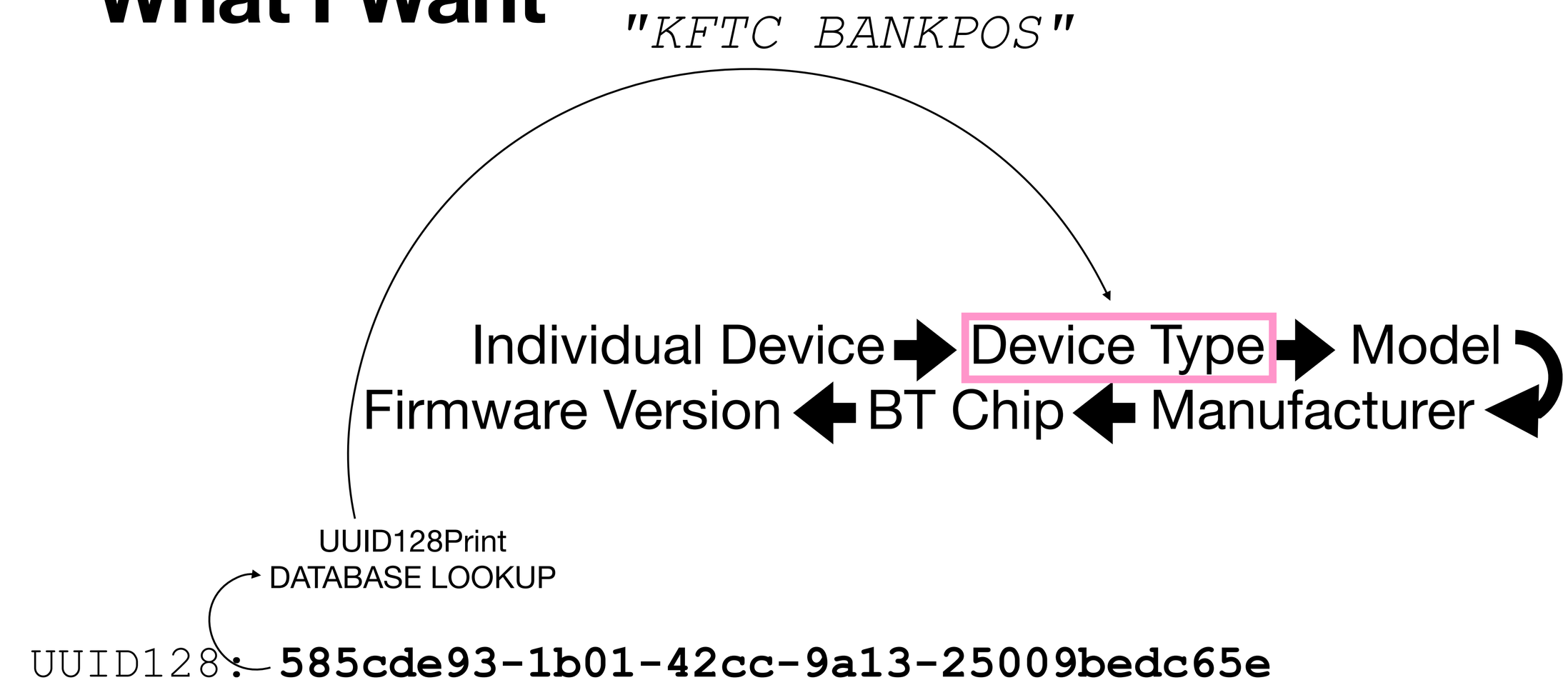
What I Want

UUID128Print
DATABASE LOOKUP

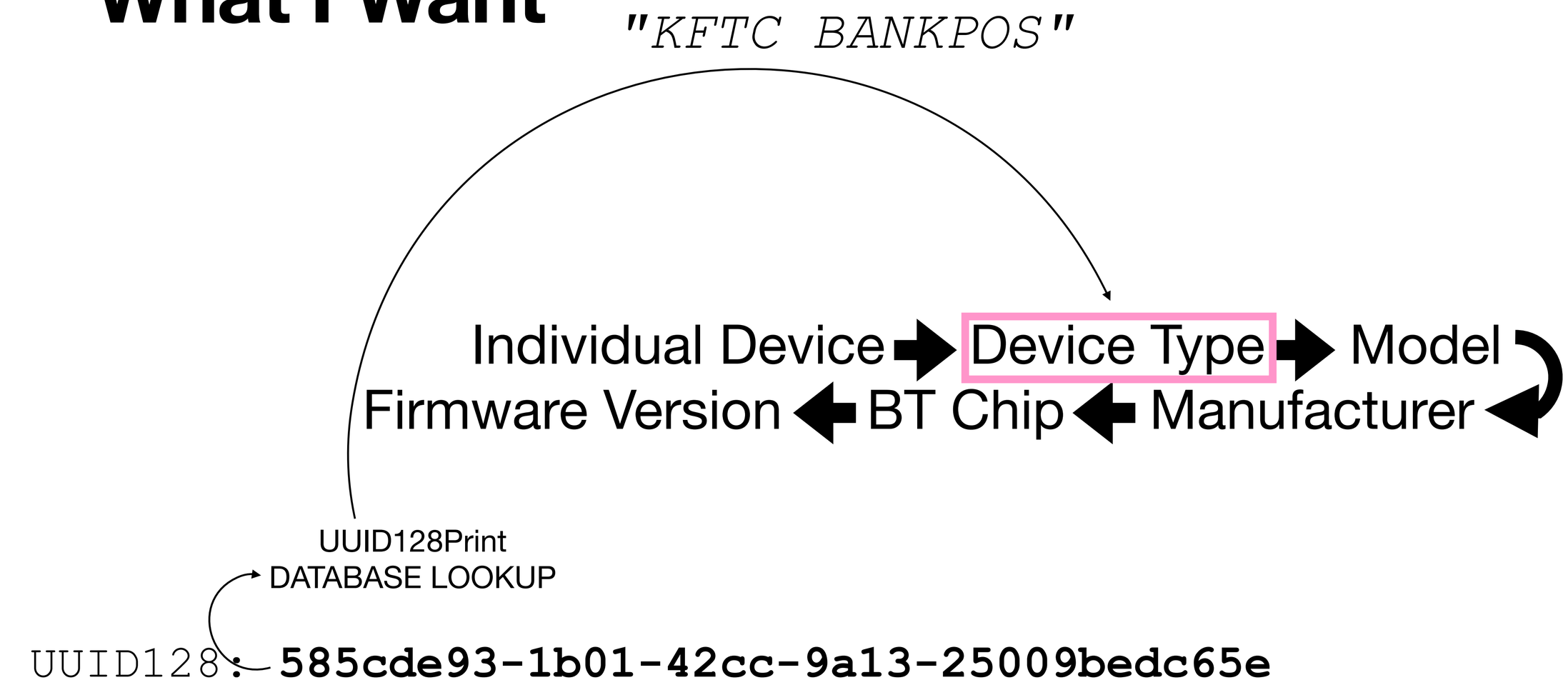
UUID128: **585cde93-1b01-42cc-9a13-25009bedc65e**


DARK MENTOR

What I Want


"KFTC BANKPOS"
Individual Device
Device Type
Model
Manufacturer
BT Chip
Firmware Version
UUID128Print
DATABASE LOOKUP
UUID128: 585cde93-1b01-42cc-9a13-25009bedc65e

What I Want



ASSUMPTION:
UUID128Prints can be reused *within* Manufacturers,
but not reused *between* Manufacturers

Vendor-specific 128-bit UUIDs

- abbaff00-e56a-484c-b832-8b17cf6cbfe8
  - Versa (|2|Lite), Ionic
- adab*fb00*-6e7d-4601-bda2-bffaa68956ba
  - Inspire HR, Flex 2
- adab*0d57*-6e7d-4601-bda2-bffaa68956ba
- adab*6552*-6e7d-4601-bda2-bffaa68956ba
  - One
- adab*5b8c*-6e7d-4601-bda2-bffaa68956ba
  - Flex

Vendor-specific 128-bit UUIDs

- abbaff00-e56a-484c-b832-8b17cf6cbfe8
  - Versa (|2|Lite), Ionic
- adab*fb00*-6e7d-4601-bda2-bffaa68956ba
  - Inspire HR, Flex 2
- adab*0d57*-6e7d-4601-bda2-bffaa68956ba
- adab*6552*-6e7d-4601-bda2-bffaa68956ba
  - One
- adab*5b8c*-6e7d-4601-bda2-bffaa68956ba
  - Flex

```
> HCI Event: LE Meta Event (0x3e) plen 42
    LE Advertising Report (0x02)
      Num reports: 1
      Event type: Connectable undirected - ADV_IND (0x00)
      Address type: Random (0x01)
      Address: F5:6E:B2:C3:73:D2 (Static)
      Data length: 30
      Flags: 0x06
        LE General Discoverable Mode
        BR/EDR Not Supported
      128-bit Service UUIDs (partial): 1 entry
        Vendor specific (abbaff00-e56a-484c-b832-8b17cf6cbfe8)
      Service Data (UUID 0x180a): 2604329303
      RSSI: -93 dBm (0xa3)
```

Vendor-specific 128-bit UUIDs

- abbaff00-e56a-484c-b832-8b17cf6cbfe8
  - Versa (|2|Lite), Ionic
- adab*fb00*-6e7d-4601-bda2-bffaa68956ba
  - Inspire HR, Flex 2
- adab*0d57*-6e7d-4601-bda2-bffaa68956ba
- adab*6552*-6e7d-4601-bda2-bffaa68956ba
  - One
- adab*5b8c*-6e7d-4601-bda2-bffaa68956ba
  - Flex

> HCI Event: LE Meta Event (0x3e) plen 42
  LE Advertising Report (0x02)
    Num reports: 1
    Event type: Connectable undirected - **ADV_IND** (0x00)
    Address type: Random (0x01)
    Address: F5:6E:B2:C3:73:D2 (Static)
    Data length: 30
    Flags: 0x06
      LE General Discoverable Mode
      BR/EDR Not Supported
    128-bit Service UUIDs (partial): 1 entry
      Vendor specific (**abbaff00-e56a-484c-b832-8b17cf6cbfe8**)
    Service Data (UUID 0x180a): 2604329303
    RSSI: -93 dBm (0xa3)

What I Want

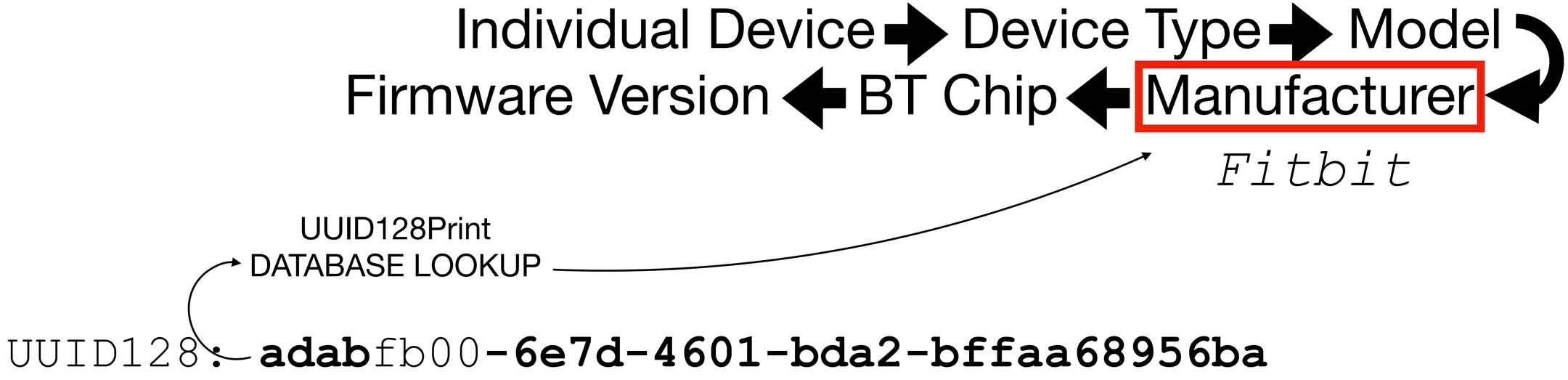
Individual Device → Device Type → Model ↷
Firmware Version ← BT Chip ← Manufacturer

What I Want

UUID128: **adab**fb00**-6e7d-4601-bda2-bffaa68956ba**

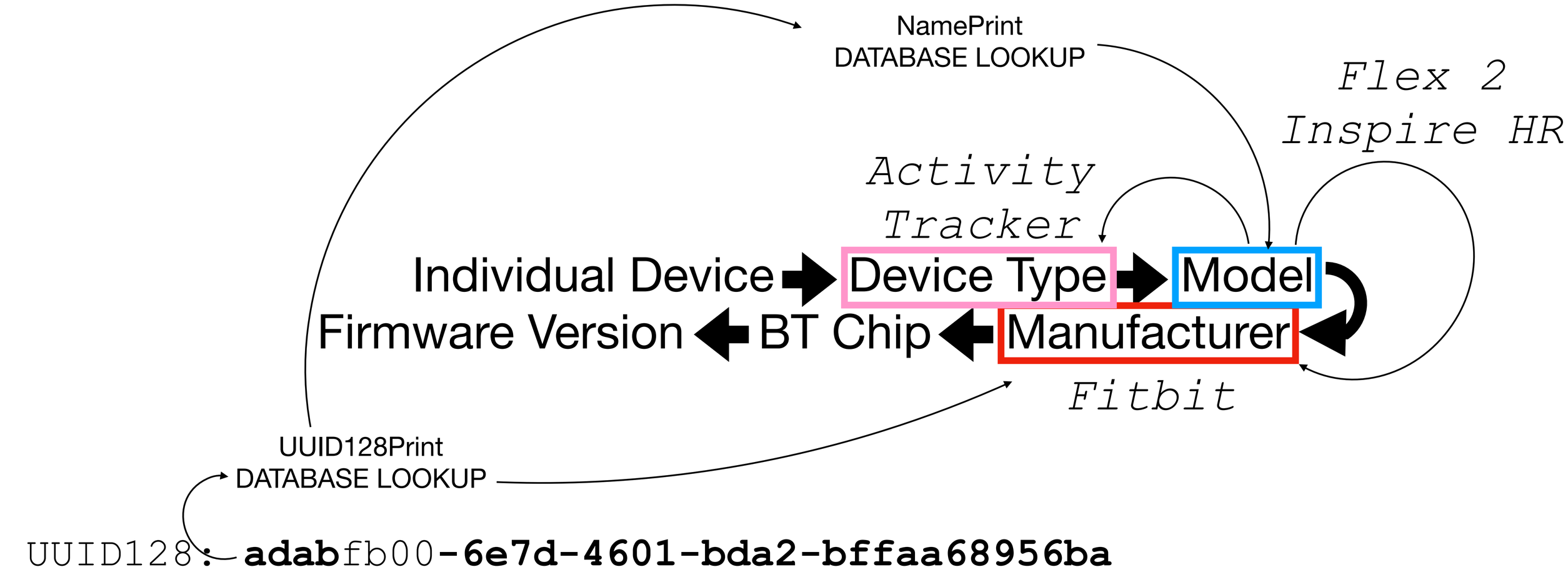

DARK MENTOR

What I Want

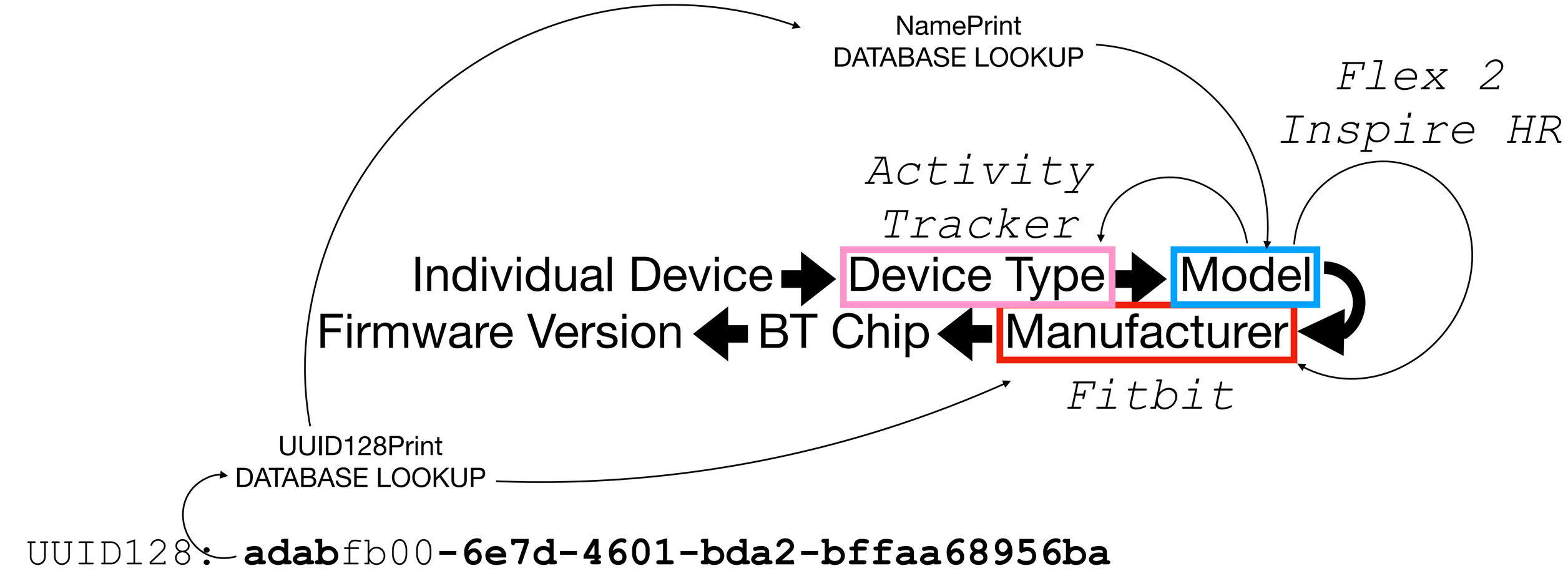

Individual Device
Device Type
Model
Firmware Version
BT Chip
Manufacturer
Fitbit
UUID128Print
DATABASE LOOKUP
UUID128:
adabfb00-6e7d-4601-bda2-bffaa68956ba


DARK MENTOR

What I Want


NamePrint
DATABASE LOOKUP
Flex 2
Inspire HR
Activity
Tracker
Individual Device
Device Type
Model
Firmware Version
BT Chip
Manufacturer
Fitbit
UUID128Print
DATABASE LOOKUP
UUID128:
adabfb00-6e7d-4601-bda2-bffaa68956ba

What I Want



ASSUMPTION:
UUID128Prints can be reused *within* Manufacturers,
but not reused *between* Manufacturers

What I Want

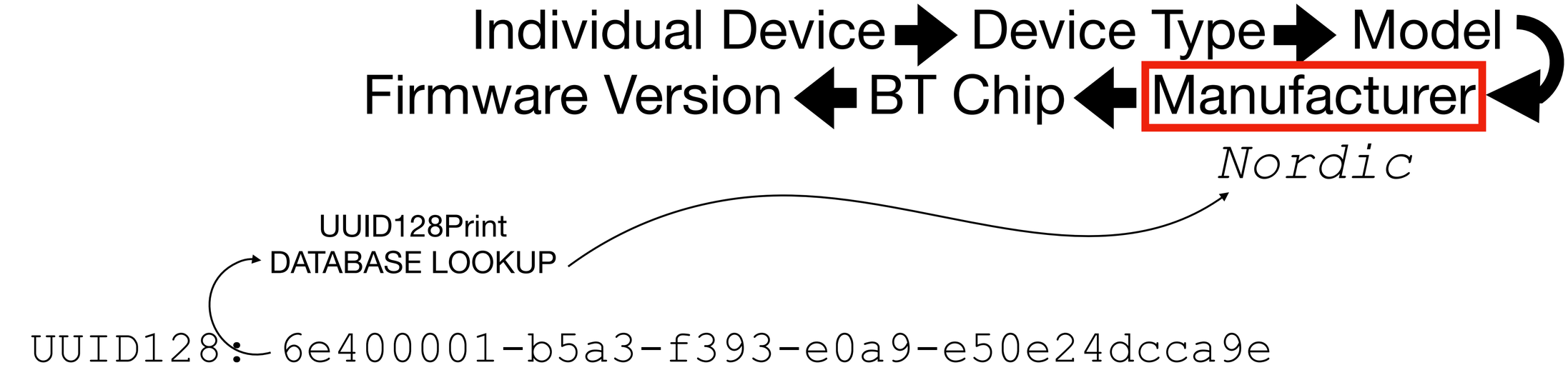
Individual Device → Device Type → Model ↷
Firmware Version ← BT Chip ← Manufacturer

What I Want

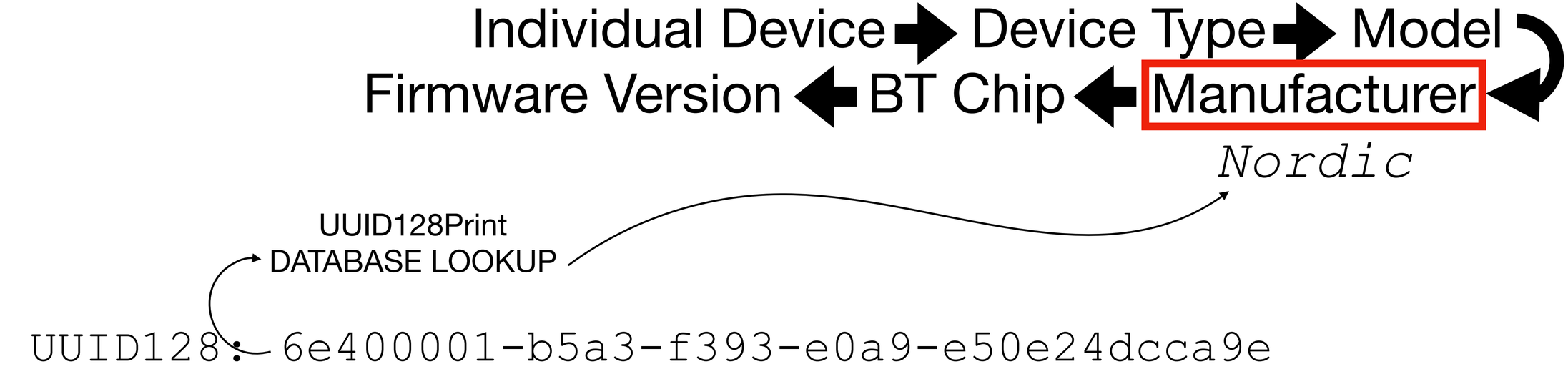

```
UUID128: 6e400001-b5a3-f393-e0a9-e50e24dcca9e
```


DARK MENTOR

What I Want

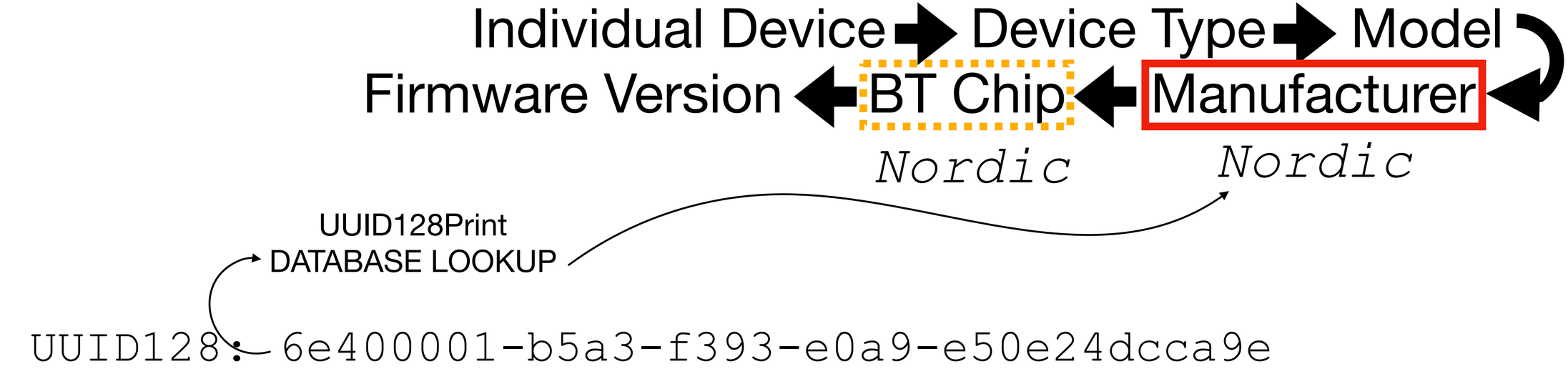

Individual Device
Device Type
Model
Firmware Version
BT Chip
Manufacturer
Nordic
UUID128Print
DATABASE LOOKUP
UUID128: 6e400001-b5a3-f393-e0a9-e50e24dcca9e

What I Want



ASSUMPTION:
UUID128Prints can be reused *within* Manufacturers,
but not reused *between* Manufacturers

What I Want



ASSUMPTION:
UUID128Prints can be reused *within* Manufacturers,
but not reused *between* Manufacturers

iBeacon: "The other UUID128!"

UUID128Print

- One of the most common types of "Manufacturer-Specific Data" (MSD) is the Apple-specified iBeacon (https://developer.apple.com/ibeacon/)
- It contains a UUID128 that beacon-deployers are supposed to associate with themselves, a Major ID and Minor ID that they're supposed to associate with individual beacons (e.g. Major ID for a country/store, and minor ID for an individual beacon)

```
Device Company ID: 0x004c (Apple, Inc.) - take with a grain of salt, not all companies populate this accurately!
        Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x4c00 (No Match)
Raw Data: 0215f34ebac47cd74027878e55f4e71d03090000000088
Apple iBeacon:
        UUID128: f34ebac4-7cd7-4027-878e-55f4e71d0309
        Major ID: 0000
        Minor ID: 0000
        RSSI at 1 meter: -120dBm
        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
        This was found in an event of type 3 which corresponds to Non-Connectable Undirected Advertising (ADV_NONCONN_IND)
```

iBeacon: "The other UUID128!"

UUID128Print

- Detective Work🕵️: GATT -> Google Search

```
        GATT Characteristic: 00002a29-0000-1000-8000-00805f9b34fb (Manufacturer Name String), Properties: 2 ('Readable' )
        GATT Characteristic value read as b'MILWAUKEE TOOL'
GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 9
GATT Descriptor: 00002a24-0000-1000-8000-00805f9b34fb, Descriptor Handle: 10
        GATT Characteristic: 00002a24-0000-1000-8000-00805f9b34fb (Model Number String), Properties: 2 ('Readable' )
        GATT Characteristic value read as b'BLE112'
GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 11
GATT Descriptor: 00002a25-0000-1000-8000-00805f9b34fb, Descriptor Handle: 12
        GATT Characteristic: 00002a25-0000-1000-8000-00805f9b34fb (Serial Number String), Properties: 2 ('Readable' )
        GATT Characteristic value read as b'123456789'
```

iBeacon: "The other UUID128!"

UUID128Print

- Detective Work🕵️: GATT -> Google Search

```
istic: 00002a29-0000-1000-8000-00805f9b34fb (Manufacturer
istic value read as b'MILWAUKEE TOOL'
803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 9
a24-0000-1000-8000-00805f9b34fb, Descriptor Handle: 10
istic: 00002a24-0000-1000-8000-00805f9b34fb (Model Number
istic value read as b'BLE112'
803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 11
a25-0000-1000-8000-00805f9b34fb, Descriptor Handle: 12
istic: 00002a25-0000-1000-8000-00805f9b34fb (Serial Number
istic value read as b'123456789'
```

iBeacon: "The other UUID128!"

UUID128Print

- Detective Work🕵️: GATT -> Google Search

```
istic: 00002a29-0000-1000-8000-00805f9b34fb (Manufacturer
istic value read as b MILWAUKEE TOOL
803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 9
a24-0000-1000-8000-00805f9b34fb, Descriptor Handle: 10
istic: 00002a24-0000-1000-8000-00805f9b34fb (Model Number
istic value read as b'BLE112'
803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 11
a25-0000-1000-8000-00805f9b34fb, Descriptor Handle: 12
istic: 00002a25-0000-1000-8000-00805f9b34fb (Serial Number
istic value read as b'123456789'
```

iBeacon: "The other UUID128

UUID128Print

- Detective Work🕵️: GATT -> Google Search

```
istic: 00002a29-0000-1000-8000-00805f9b34fb (Manufacturer
istic value read as b MILWAUKEE TOOL
803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 9
a24-0000-1000-8000-00805f9b34fb, Descriptor Handle: 10
istic: 00002a24-0000-1000-8000-00805f9b34fb (Model Number
istic value read as b'BLE112'
803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 11
a25-0000-1000-8000-00805f9b34fb, Descriptor Handle: 12
istic: 00002a25-0000-1000-8000-00805f9b34fb (Serial Number
istic value read as b'123456789'
```

iBeacon: "The other UUID128!"

UUID128Print

- Detective Work🕵️: GATT -> Google Search

```
istic: 00002a29-0000-1000-8000-00805f9b34fb (Manufacturer
istic value read as b MILWAUKEE TOOL
803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 9
a24-0000-1000-8000-00805f9b34fb, Descriptor Handle: 10
istic: 00002a24-0000-1000-8000-00805f9b34fb (Model Number
istic value read as b'BLE112'
803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 11
a25-0000-1000-8000-00805f9b34fb, Descriptor Handle: 12
istic: 00002a25-0000-1000-8000-00805f9b34fb (Serial Number
istic value read as b'123456789'
```

iBeacon: "The other UUID128!"

UUID128Print

- Detective Work🕵️: GATT -> Google Search

```
istic: 00002a29-0000-1000-8000-00805f9b34fb (Manufacturer
istic value read as b MILWAUKEE TOOL
803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 9
a24-0000-1000-8000-00805f9b34fb, Descriptor Handle: 10
istic: 00002a24-0000-1000-8000-00805f9b34fb (Model Number
istic value read as b BLE112
803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 11
a25-0000-1000-8000-00805f9b34fb, Descriptor Handle: 12
istic: 00002a25-0000-1000-8000-00805f9b34fb (Serial Number
istic value read as b'123456789'
```

Milwaukee tool BLE112 bluetooth

Shopping | Images | Videos | App | News | Maps | Books | Flights | Finance

Milwaukee Tool
https://www.milwaukeetool.com › Products

TICK Tool and Equipment Tracker

Bluetooth tracker for **tools** and **equipment** offers multiple attachment options and a low profile design - users can glue, screw, rivet or strap the TICK™…

★★★★½ Rating: 4.7 · 901 reviews

Missing: ~~BLE112~~ | Show results with: BLE112

Milwaukee Tool
https://www.milwaukeetool.com › Products

Milwaukee tool BLE112 bluetooth

Shopping | Images | Videos | App | News | Maps | Books | Flights | Finance

They make an AirTag "for tools"!

Where's your anti-stalking defense now?

and a low profile design - users can glue, screw, rivet or strap the TICK™

★★★★½ Rating: 4.7 · 901 reviews

Missing: ~~BLE112~~ | Show results with: BLE112

Milwaukee Tool

https://www.milwaukeetool.com › Products

Milwaukee tool BLE112 bluetooth

Shopping | Images | Videos | App | News | Maps | Books | Flights | Finance

Milwaukee Tool
https://www.milwaukeetool.com › Products

TICK Tool and Equipment Tracker

Bluetooth tracker for **tools** and **equipment** offers multiple attachment options and a low profile design - users can glue, screw, rivet or strap the TICK™…

★★★★½ Rating: 4.7 · 901 reviews

Missing: ~~BLE112~~ | Show results with: BLE112

Milwaukee Tool
https://www.milwaukeetool.com › Products

Can Milwaukee tools be traced?

Does Milwaukee have Bluetooth?

Feedback

Silicon Labs
https://www.silabs.com › bluetooth › device.bled112

BLED112

The **BLED112 Bluetooth** Low Energy Dongle integrates all **Bluetooth** LE features. The USB dongle has a virtual COM port that enables seamless ho…

BLE112 bluetooth -"BLED112"

Images | Videos | Manual | Shopping | News | Maps | Books | Flights | Finan

Sponsored

Mouser Electronics
https://www.mouser.com

BLED112 Bluetooth Smart Dongle - Silicon Labs | Mouser

Mouser is an Authorized Silicon Labs Distributor with Inventory, Prices & Datasheets. Huge Selection of Silicon Labs In Stock with No Minimum Orders & Fast Delivery! Fast Delivery. AS6496 Certified. Authorized Distributor. ISO 9001:2015. Order by 8PM CST.

Get phone number

Selection of Silicon Labs In Stock with No Minimum Orders & Fast Delivery! Fast Delivery. AS6496 Certified. Authorized Distributor. ISO 9001:2015. Order by 8PM CST.

Get phone number

Silicon Labs
https://www.silabs.com › public › data-sheets

BLE112 Datasheet

BLE112 offers all **Bluetooth** Low Energy features: radio, stack, profiles and application space for customer applications, so no external processor is needed. The ...

36 pages

Digikey
https://forum.digikey.com › getting-started-with-the-bl...

Getting Started with the BlueGiga BLE112 Bluetooth Low ...

Mar 9, 2021 — Purpose. This page explains how to set up the Silicon Labs **BLE112** **Bluetooth** Low Energy module to communicate with a microcontroller via UART.

BLE112

DATA SHEET

Wednesday, 02 December 2020

Version 1.8

SILICON LABS

Selection of Silicon Labs In Stock with No Minimum Orders & Fast Delivery! Fast Delivery. AS6496 Certified. Authorized Distributor. ISO 9001:2015. Order by 8PM CST.

Get phone number

Silicon Labs
https://www.silabs.com › public › data-sheets

BLE112 Datasheet

BLE112 offers all **Bluetooth** Low Energy features: radio, stack, profiles and application space for customer applications, so no external processor is needed. The ...

36 pages

Digikey
https://forum.digikey.com › getting-started-with-the-bl...

Getting Started with the BlueGiga BLE112 Bluetooth Low ...

Mar 9, 2021 — Purpose. This page explains how to set up the Silicon Labs **BLE112** **Bluetooth** Low Energy module to communicate with a microcontroller via UART.

Selection of Silicon Labs In Stock with No Minimum Orders & Fast Delivery! Fast Delivery. AS6496 Certified. Authorized Distributor. ISO 9001:2015. Order by 8PM CST.

Get phone number

Silicon Labs
https://www.silabs.com › public › data-sheets

BLE112 Datasheet

BLE112 offers all **Bluetooth** Low Energy features: radio, stack, profiles and application space for customer applications, so no external processor is needed. The ...

36 pages

Digikey
https://forum.digikey.com › getting-started-with-the-bl...

Getting Started with the BlueGiga BLE112 Bluetooth Low ...

Mar 9, 2021 — Purpose. This page explains how to set up the Silicon Labs **BLE112** **Bluetooth** Low Energy module to communicate with a microcontroller via UART

iBeacon: "The other UUID128!"

UUID128Print

- Detective Work🕵: GATT -> Google Search -> **BLE112 == Bluegiga module**

```
n:
rvice: Begin Handle: 1   End Handle: 5          UUID128: 00001800-0000-1000-8000-00805f9b34fb (Generic Access)
 GATT Descriptor: 00002800-0000-1000-8000-00805f9b34fb, Descriptor Handle: 1
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 2
 GATT Descriptor: 00002a00-0000-1000-8000-00805f9b34fb, Descriptor Handle: 3
        GATT Characteristic: 00002a00-0000-1000-8000-00805f9b34fb (Device Name), Properties: 10 ('Readable' 'Writable' )
        GATT Characteristic value read as b'000C007771MKE  '
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 4
 GATT Descriptor: 00002a01-0000-1000-8000-00805f9b34fb, Descriptor Handle: 5
        GATT Characteristic: 00002a01-0000-1000-8000-00805f9b34fb (Appearance), Properties: 2 ('Readable' )
        GATT Characteristic value read as b'\x00\x01'
                Appearance decodes as: Category (8): Tag, Sub-Category (0): Generic
rvice: Begin Handle: 6   End Handle: 12         UUID128: 0000180a-0000-1000-8000-00805f9b34fb (Device Information)
 GATT Descriptor: 00002800-0000-1000-8000-00805f9b34fb, Descriptor Handle: 6
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 7
 GATT Descriptor: 00002a29-0000-1000-8000-00805f9b34fb, Descriptor Handle: 8
        GATT Characteristic: 00002a29-0000-1000-8000-00805f9b34fb (Manufacturer Name String), Properties: 2 ('Readable' )
        GATT Characteristic value read as b'MILWAUKEE TOOL'
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 9
 GATT Descriptor: 00002a24-0000-1000-8000-00805f9b34fb, Descriptor Handle: 10
        GATT Characteristic: 00002a24-0000-1000-8000-00805f9b34fb (Model Number String), Properties: 2 ('Readable' )
        GATT Characteristic value read as b'BLE112'
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 11
 GATT Descriptor: 00002a25-0000-1000-8000-00805f9b34fb, Descriptor Handle: 12
        GATT Characteristic: 00002a25-0000-1000-8000-00805f9b34fb (Serial Number String), Properties: 2 ('Readable' )
        GATT Characteristic value read as b'123456789'
```

```
p:c4:7a:
 IEEE OUI (00:07:80): Bluegiga Technologies OY

 Inquiry Result Device info.



d.

er found.

ata found.

ecific Data:
Company ID: 0x6501 (No Match) - take with a grain of salt, not all companies pop
  Endianness-flipped device company ID (in case the vendor used the wrong endian
a: 000c00777100
 In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
 This was found in an event of type 0 which corresponds to Connectable Undirecte

ice Data found.

n:
```

IEEE OUI (00:07:80): Bluegiga Technologies OY

Inquiry Result Device info.

d.

er found.

ata found.

ecific Data:
Company ID: 0x6501 (No Match) - take with a grain of salt, not all companies pop
Endianness-flipped device company ID (in case the vendor used the wrong endian
a: 000c00777100
In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
This was found in an event of type 0 which corresponds to Connectable Undirecte

ice Data found.

n:

bluegiga silicon labs

Images | Bluetooth | App | Videos | BLED112 | BLE GUI tool | UART demo | Shopp

Silicon Labs
https://www.silabs.com › developers › bluegiga-blueto...

Bluegiga Bluetooth Smart Software Development Kit (SDK)

Bluegiga Bluetooth Smart Software is a complete Bluetooth Smart software stack for **Bluegiga** Legacy Bluetooth Smart products, such as BLE112, BLE113, ...

People also ask

Is Silicon Labs safe?

Bluegiga Legacy Modules (BLE)

The **Bluegiga** Legacy Bluetooth 4.0 Low Energy (BLE) Modules were launched in 2011. For new Bluetooth 5 designs, we recommend our latest Bluetooth modules.

Silicon Labs Newsroom
https://news.silabs.com › 2015-02-03-Silicon-Labs-Ac...

Silicon Labs Acquires Bluegiga, a Leader in Bluetooth and ...

Feb 3, 2015 — **Silicon Labs** completed the acquisition of **Bluegiga** Technologies Oy on January 30, 2015. Under the agreement, **Bluegiga** investors received ...

Bluegiga Legacy Modules (BLE)

The **Bluegiga** Legacy Bluetooth 4.0 Low Energy (BLE) Modules were launched in 2011. For new Bluetooth 5 designs, we recommend our latest Bluetooth modules.

Silicon Labs Newsroom

https://news.silabs.com › 2015-02-03-Silicon-Labs-Ac

Silicon Labs Acquires Bluegiga, a Leader in Bluetooth and ...

Feb 3, 2015 — **Silicon Labs** completed the acquisition of **Bluegiga** Technologies Oy on January 30, 2015. Under the agreement, **Bluegiga** investors received ...

iBeacon: "The other UUID128!"

UUID128Print

- Detective Work🕵️: GATT -> Google Search -> BLE112 == Bluegiga module -> Google Search **-> Bluegiga == Silicon Labs**

iBeacon: "The other UUID128!"

UUID128Print

- Detective Work🕵️: GATT -> Google Search -> BLE112 == Bluegiga module -> Google Search -> Bluegiga == Silicon Labs

```
istic: 00002a29-0000-1000-8000-00805f9b34fb (Manufacturer
istic value read as b'MILWAUKEE TOOL'
803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 9
a24-0000-1000-8000-00805f9b34fb, Descriptor Handle: 10
istic: 00002a24-0000-1000-8000-00805f9b34fb (Model Number
istic value read as b BLE112
803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 11
a25-0000-1000-8000-00805f9b34fb, Descriptor Handle: 12
istic: 00002a25-0000-1000-8000-00805f9b34fb  Serial Number
istic value read as b 123456789
```

iBeacon: "The other UUID128!"

UUID128Print

- Detective Work🕵️: GATT -> Google Search -> BLE112 == Bluegiga module -> Google Search -> Bluegiga == Silicon Labs

```
istic: 00002a29-0000-1000-8000-00805f9b34fb (Manufacturer
istic value read as b'MILWAUKEE TOOL'
803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 9
a24-0000-1000-8000-00805f9b34fb, Descriptor Handle: 10
istic: 00002a24-0000-1000-8000-00805f9b34fb (Model Number
istic value read as b BLE112
000-1000-8000-00805f9b34fb, Descriptor Handle: 11
805f9b34fb, Descriptor Handle: 12
1000-8000-00805f9b34fb  Serial Number
123456789
```

Kinda seems *uninitialized*

iBeacon: "The other UUID128!"

UUID128Print

```
turer-specific Data:
 Device Company ID: 0x6501 (No Match) - take with a grain of salt, not all companies populate
          Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x0165 (Milwaukee Electric
 Raw Data: 000c00777100
        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
        This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

s of Device Data found.

formation:
 GATT Service: Begin Handle: 1   End Handle: 5          UUID128: 00001800-0000-1000-8000-00805f9b34fb (Generic Access)
        GATT Descriptor: 00002800-0000-1000-8000-00805f9b34fb, Descriptor Handle: 1
        GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 2
        GATT Descriptor: 00002a00-0000-1000-8000-00805f9b34fb, Descriptor Handle: 3
                GATT Characteristic: 00002a00-0000-1000-8000-00805f9b34fb (Device Name), Properties: 10 ('Readable' 'Writa
                GATT Characteristic value read as b'000C007771MKE  '
        GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 4
        GATT Descriptor: 00002a01-0000-1000-8000-00805f9b34fb, Descriptor Handle: 5
                GATT Characteristic: 00002a01-0000-1000-8000-00805f9b34fb (Appearance), Properties: 2 ('Readable' )
                GATT Characteristic value read as b'\x00\x01'
                        Appearance decodes as: Category (8): Tag, Sub-Category (0): Generic
 GATT Service: Begin Handle: 6   End Handle: 12         UUID128: 0000180a-0000-1000-8000-00805f9b34fb (Device Information)
        GATT Descriptor: 00002800-0000-1000-8000-00805f9b34fb, Descriptor Handle: 6
        GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 7
        GATT Descriptor: 00002a29-0000-1000-8000-00805f9b34fb, Descriptor Handle: 8
                GATT Characteristic: 00002a29-0000-1000-8000-00805f9b34fb (Manufacturer Name String), Properties: 2 ('Read
                GATT Characteristic value read as b'MILWAUKEE TOOL'
        GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 9
```

iBeacon: "The other UUID128!"

UUID128Print

```
turer-specific Data:
 Device Company ID: 0x6501 (No Match) - take with a grain of salt, not all companies populate
          Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x0165 (Milwaukee Electric
 Raw Data: 000c00777100
         In BT LE Data (LE_bdaddr_to_mf_specific), h                ndom = 0 (Public)
         This was found in an event of type 0 which                 s to Connectable Undirected Advertising (ADV_IND)

s of Device Data found.

formation:
 GATT Service: Begin Handle: 1   End Handle: 5                 UID128:
         GATT Descriptor: 00002800-0000-1000-800                34fb, Desc
         GATT Descriptor: 00002803-0000-1000-80                 fb, Desc
         GATT Descriptor: 00002a00-0000-1000-8                  , Desc
                 GATT Characteristic: 00002a0                   00805f
                 GATT Characteristic value read as b'000C00777 1MKE   '
         GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 4
         GATT Descriptor: 00002a01-0000-1000-8000-00805f9b34fb, Descriptor Handle: 5
                 GATT Characteristic: 00002a01-0000-1000-8000-00805f9b34fb (Appearance), Properties: 2 ('Readable' )
                 GATT Characteristic value read as b'\x00\x01'
                         Appearance decodes as: Category (8): Tag, Sub-Category (0): Generic
 GATT Service: Begin Handle: 6   End Handle: 12          UUID128: 0000180a-0000-1000-8000-00805f9b34fb (Device Information)
         GATT Descriptor: 00002800-0000-1000-8000-00805f9b34fb, Descriptor Handle: 6
         GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 7
         GATT Descriptor: 00002a29-0000-1000-8000-00805f9b34fb, Descriptor Handle: 8
                 GATT Characteristic: 00002a29-0000-1000-8000-00805f9b34fb (Manufacturer Name String), Properties: 2 ('Read
                 GATT Characteristic value read as b'MILWAUKEE TOOL'
         GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 9
```

They seem to be using a big-endian BT CID, rather than the more common little-endian

iBeacon: "The other UUID128!"

UUID128Print

- Detective Work🕵️: GATT -> Google Search -> BLE112 == Bluegiga module -> Google Search -> Bluegiga == Silicon Labs -> iBeacons

```
turer-specific Data:
 Device Company ID: 0x6501 (No Match) - take with a grain of salt, not all companies populate this accurately!
          Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x0165 (Milwaukee Electric T
 Raw Data: 000c03249000
         In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
         This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
 Device Company ID: 0x004c (Apple, Inc.) - take with a grain of salt, not all companies populate this accurately!
          Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x4c00 (No Match)
 Raw Data: 0215f34ebac47cd74027878e55f4e71d03090000000088
 Apple iBeacon:
         UUID128: f34ebac4-7cd7-4027-878e-55f4e71d0309
         Major ID: 0000
         Minor ID: 0000
         RSSI at 1 meter: -120dBm
         In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
         This was found in an event of type 3 which corresponds to Non-Connectable Undirected Advertising (ADV_NONCONN_IND)
```

iBeacon: "The other UUID128!"

UUID128Print

- Detective Work🕵️: GATT -> Google Search -> BLE112 == Bluegiga module -> Google Search -> Bluegiga == Silicon Labs -> iBeacons

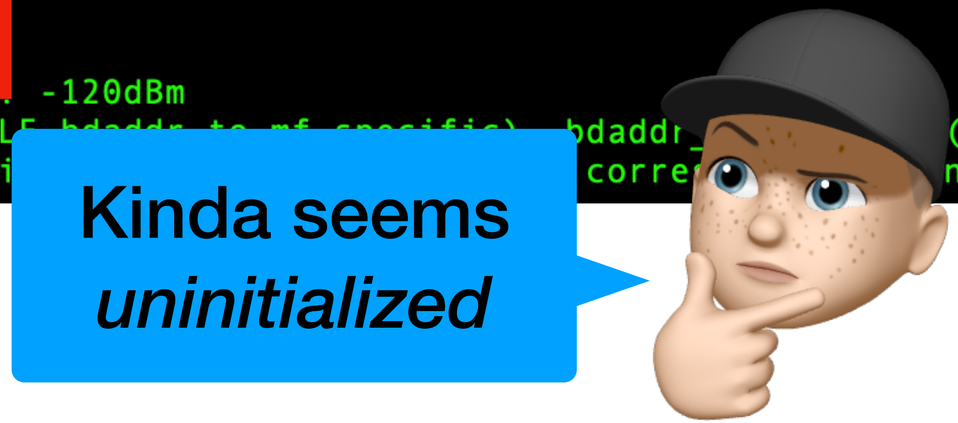
```
turer-specific Data:
 Device Company ID: 0x6501 (No Match) - take with a grain of salt, not all companies populate this accurately!
          Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x0165 (Milwaukee Electric T
 Raw Data: 000c03249000
         In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
         This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
 Device Company ID: 0x004c (Apple, Inc.) - take with a grain of salt, not all companies populate this accurately!
          Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x4c00 (No Match)
 Raw Data: 0215f34ebac47cd74027878e55f4e71d03090000000088
 Apple iBeacon:
         [illegible]4-7cd7-4027-878e-55f4e71d0309
         Major ID: 0000
         Minor ID: 0000
         [illegible] -120dBm
         In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
         This was found in an event of type 3 which corresponds to Non-Connectable Undirected Advertising (ADV_NONCONN_IND)
```

iBeacon: "The other UUID128!"

UUID128Print

- Detective Work🕵️: GATT -> Google Search -> BLE112 == Bluegiga module -> Google Search -> Bluegiga == Silicon Labs -> iBeacons

```
turer-specific Data:
 Device Company ID: 0x6501 (No Match) - take with a grain of salt, not all companies populate this accurately!
          Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x0165 (Milwaukee Electric T
 Raw Data: 000c03249000
         In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
         This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
 Device Company ID: 0x004c (Apple, Inc.) - take with a grain of salt, not all companies populate this accurately!
          Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x4c00 (No Match)
 Raw Data: 0215f34ebac47cd74027878e55f4e71d03090000000088
 Apple iBeacon:
         UUID128: f34e[illegible]4-7cd7-4027-878e-55f4e71d0309
         Major ID: 0000
         Minor ID: 0000
         RSSI at 1 meter: -120dBm
         In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
         This was found in an event of type 3 which corresponds to Non-Connectable Undirected Advertising (ADV_NONCONN_IND)
```



iBeacon: "The other UUID128!"

UUID128Print

- Detective Work🕵️: GATT -> Google Search -> BLE112 == Bluegiga module -> Google Search -> Bluegiga == Silicon Labs -> iBeacons -> UUID128

```
turer-specific Data:
 Device Company ID: 0x6501 (No Match) - take with a grain of salt, not all companies populate this accurately!
          Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x0165 (Milwaukee Electric T
 Raw Data: 000c03249000
         In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
         This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
 Device Company ID: 0x004c (Apple, Inc.) - take with a grain of salt, not all companies populate this accurately!
          Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x4c00 (No Match)
 Raw Data: 0215f34ebac47cd74027878e55f4e71d03090000000088
 Apple iBeacon:
         UUID128: f34ebac4-7cd7-4027-878e-55f4e71d0309
         Major ID: 0000
         Minor ID: 0000
         RSSI at 1 meter: -120dBm
         In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_                    (Public)
         This was found in an event of type 3 which corre                    n-Connectable Undirected Advertising (ADV_NONCONN_IND)
```

iBeacon: "The other UUID128!"

UUID128Print

- Detective Work🕵️: GATT -> Google Search -> BLE112 == Bluegiga module -> Google Search -> Bluegiga == Silicon Labs -> iBeacons -> UUID128

```
turer-specific Data:
 Device Company ID: 0x6501 (No Match) - take with a grain of salt, not all companies populate this accurately!
          Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x0165 (Milwaukee Electric T
 Raw Data: 000c03249000
         In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
         This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
 Device Company ID: 0x004c (Apple, Inc.) - take with a grain of salt, not all companies populate this accurately!
          Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x4c00 (No Match)
 Raw Data: 0215f34ebac47cd74027878e55f4e71d03090000000088
 Apple i
         UUID128: f34ebac4-7cd7-4027-878e-55f4e71d0309
         Minor ID: 0000
         RSSI at 1 meter: -120dBm
         In BT LE D                                                    (Public)
         This was f                                                    n-Connectable Undirected Advertising (ADV_NONCONN_IND)
```

Where else does this UUID128 appear?

iBeacon: "The other UUID128!"

UUID128Print

- Detective Work🕵️: GATT -> Google Search -> BLE112 == Bluegiga module -> Google Search -> Bluegiga == Silicon Labs -> iBeacons -> UUID128

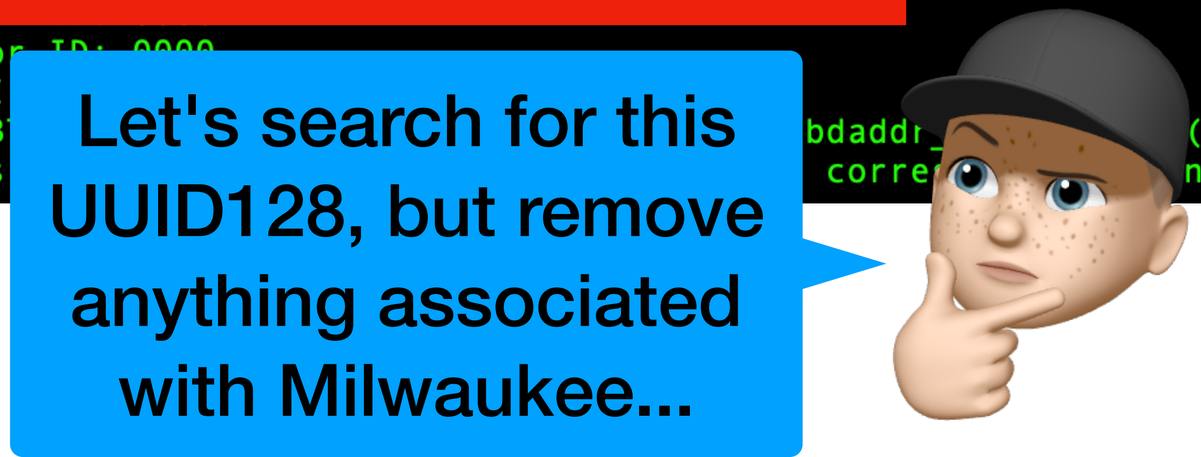
```
turer-specific Data:
 Device Company ID: 0x6501 (No Match) - take with a grain of salt, not all companies populate this accurately!
          Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x0165 (Milwaukee Electric T
 Raw Data: 000c03249000
         In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
         This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
 Device Company ID: 0x004c (Apple, Inc.) - take with a grain of salt, not all companies populate this accurately!
          Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x4c00 (No Match)
 Raw Data: 0215f34ebac47cd74027878e55f4e71d03090000000088
 Apple i
         UUID128: f34ebac4-7cd7-4027-878e-55f4e71d0309
         Minor ID: 0000
         RSSI at 1 meter: -120dBm
         In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr                (Public)
         This was found in an event of type 3 which corre                n-Connectable Undirected Advertising (ADV_NONCONN_IND)
```

iBeacon: "The other UUID128!"

UUID128Print

- Detective Work🕵️: GATT -> Google Search -> BLE112 == Bluegiga module -> Google Search -> Bluegiga == Silicon Labs -> iBeacons -> UUID128

```
turer-specific Data:
 Device Company ID: 0x6501 (No Match) - take with a grain of salt, not all companies populate this accurately!
          Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x0165 (Milwaukee Electric T
 Raw Data: 000c03249000
         In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
         This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
 Device Company ID: 0x004c (Apple, Inc.) - take with a grain of salt, not all companies populate this accurately!
          Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x4c00 (No Match)
 Raw Data: 0215f34ebac47cd74027878e55f4e71d03090000000088
 Apple i
         UUID128: f34ebac4-7cd7-4027-878e-55f4e71d0309
         Minor
         RSSI
         In B                                    bdaddr                  (Public)
         This                                     corre                  n-Connectable Undirected Advertising (ADV_NONCONN_IND)
```



```
================================================================================
For bdaddr = 84:71:27:69:c3:dc:
        Company Name by IEEE OUI (84:71:27): Silicon Laboratories

        No BTC Extended Inquiry Result Device info.

        No Names found.

        No UUID16s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x004c (Apple, Inc.) - take with a grain of salt, not all companies populate this accurately!
                         Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x4c00 (No Match)
                Raw Data: 0215f34ebac47cd74027878e55f4e71d03090000000088
                Apple iBeacon:
                        UUID128: f34ebac4-7cd7-4027-878e-55f4e71d0309
                        Major ID: 0000
                        Minor ID: 0000
                        RSSI at 1 meter: -120dBm
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
                        This was found in an event of type 3 which corresponds to Non-Connectable Undirected Advertising (ADV_NONCONN_IND)

        No Class of Device Data found.

        No GATT Information found.

        No BLE 2thprint Info found.

        No BTC 2thprint Info found.

================================================================================
For bdaddr = 84:fd:27:34:d2:62:
        Company Name by IEEE OUI (84:fd:27): Silicon Laboratories

        No BTC Extended Inquiry Result Device info.

        No Names found.
```

```
================================================================================
For bdaddr = 84:71:27:69:c3:dc:
        Company Name by IEEE OUI (84:71:27): Silicon Laboratories

        No BTC Extended Inquiry Result Device info.

        No Names found.

        No UUID16s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x004c (Apple, Inc.) - take with a grain of salt, not all companies populate this accurately!
                         Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x4c00 (No Match)
                Raw Data: 0215f34ebac47cd74027878e55f4e71d03090000000088
                Apple iBeacon:
                        UUID128: f34ebac4-7cd7-4027-878e-55f4e71d0309
                        Major ID: 0000
                        Minor ID: 0000
                        RSSI at 1 meter: -120dBm
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
                        This was found in an event of type 3 which corresponds to Non-Connectable Undirected Advertising (ADV_NONCONN_IND)

        No Class of Device Data found.

        No GATT Information found.

        No BLE 2thprint Info found.

        No BTC 2thprint Info found.

================================================================================
For bdaddr = 84:fd:27:34:d2:62:
        Company Name by IEEE OUI (84:fd:27): Silicon Laboratories

        No BTC Extended Inquiry Result Device info.

        No Names found.
```

```
                    This was found in an event of type 3 which corresponds to Non-Connectable Undirected Advertising (ADV_NONCONN_IND)

        No Class of Device Data found.

        No GATT Information found.

        No BLE 2thprint Info found.

================================================================================
For bdaddr = 88:6b:0f:0e:22:f0:
        Company Name by IEEE OUI (88:6b:0f) Bluegiga Technologies OY

        No BTC Extended Inquiry Result Device info.

        No Names found.

        No UUID16s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x004c (Apple, Inc.) - take with a grain of salt, not all companies populate this accurately!
                         Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x4c00 (No Match)
                Raw Data: 0215f34ebac47cd74027878e55f4e71d03090000000088
                Apple iBeacon:
                        UUID128: f34ebac4-7cd7-4027-878e-55f4e71d0309
                        Major ID: 0000
                        Minor ID: 0000
                        RSSI at 1 meter: -120dBm
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
                        This was found in an event of type 3 which corresponds to Non-Connectable Undirected Advertising (ADV_NONCONN_IND)

        No Class of Device Data found.

        No GATT Information found.

        No BLE 2thprint Info found.

        No BTC 2thprint Info found.
```

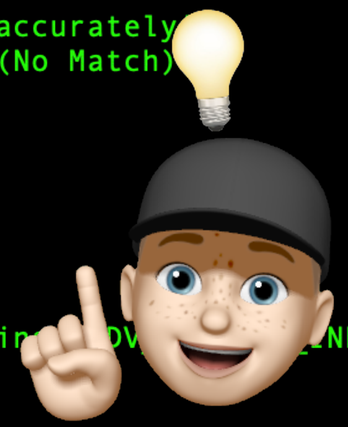
```
                    This was found in an event of type 3 which corresponds to Non-Connectable Undirected Advertising (ADV_NONCONN_IND)

        No Class of Device Data found.

        No GATT Information found.

        No BLE 2thprint Info found.

================================================================================
For bdaddr = 88:6b:0f:0e:22:f0:
        Company Name by IEEE OUI (88:6b:0f) Bluegiga Technologies OY

        No BTC Extended Inquiry Result Device info.

        No Names found.

        No UUID16s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x004c (Apple, Inc.) - take with a grain of                accurately!
                         Endianness-flipped device company ID (in case the vend               (No Match)
                Raw Data: 0215f34ebac47cd74027878e55f4e71d03090000000088
                Apple iBeacon:
                        UUID128: f34ebac4-7cd7-4027-878e-55f4e71d0309
                        Major ID: 0000
                        Minor ID: 0000
                        RSSI at 1 meter: -120dBm
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random
                        This was found in an event of type 3 which corresponds                ing (A          N_IND)

        No Class of Device Data found.

        No GATT Information found.

        No BLE 2thprint Info found.

        No BTC 2thprint Info found.
```

Does this UUID128, ever appear with any device NOT associated with Silicon Labs or Bluegiga based on the OUI?

```
                        This was found in an event of type 3 which corresponds to Non-Connectable Undirected Advertising (ADV_NONCONN_IND)

        No Class of Device Data found.

        No GATT Information found.

        No BLE 2thprint Info found.

================================================================================
For bdaddr = 88:6b:0f:0e:22:f0:
        Company Name by IEEE OUI (88:6b:0f): Bluegiga Technologies OY

        No BTC Extended Inquiry Result Device info.

        No Names found.

        No UUID16s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x004c (Apple, Inc.) - take with a grain of salt, not all companies populate this accurately!
                         Endianness-flipped device company ID (in case the vendor used the wrong endianness): 0x4c00 (No Match)
                Raw Data: 0215f34ebac47cd74027878e55f4e71d03090000000088
                Apple iBeacon:
                        UUID128: f34ebac4-7cd7-4027-878e-55f4e71d0309
                        Major ID: 0000
                        Minor ID: 0000
                        RSSI at 1 meter: -120dBm
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
                        This was found in an event of type 3 which corresponds to Non-Connectable Undirected Advertising (ADV_NONCONN_IND)

        No Class of Device Data found.

        No GATT Information found.

        No BLE 2thprint Info found.

        No BTC 2thprint Info found.
```

```
                    This was found in an event of type 3 which corresponds to Non-Connectable Undirected Advertising (ADV_NONCONN_IND)

        No Class of Device Data found.

        No GATT Information found.

        No BLE 2thprint Info found.

================================================================================
For bdaddr = 88:6b:0f:0e:22:f0:
        Company Name by IEEE OUI (88:6b:0f): Bluegiga Technologies OY

        No BTC Extended Inquiry Result Device info.

        No Names found.

        No UUID16s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x004c (Apple, Inc.) - take with a grain o                s accurately
                         Endianness-flipped device company ID (in case the ve               00 (No Match)
                Raw Data: 0215f34ebac47cd74027878e55f4e71d03090000000088
                Apple iBeacon:
                        UUID128: f34ebac4-7cd7-4027-878e-55f4e71d0309
                        Major ID: 0000
                        Minor ID: 0000
                        RSSI at 1 meter: -120dBm
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_rand
                        This was found in an event of type 3 which correspond                isin       OV       IND)

        No Class of Device Data found.

        No GATT Information found.

        No BLE 2thprint Info found.

        No BTC 2thprint Info found.
```

No! Therefore, there is a high probability that this UUID128, if present, is strongly indicative of Bluegiga/SiLabs chips!



iBeacon: "The other UUID128!"

UUID128Print

- Detective Work🕵: GATT -> Google Search -> BLE112 == Bluegiga module -> Google Search -> Bluegiga == Silicon Labs -> iBeacons -> UUID128
- UUID128 **f34ebac4-7cd7-4027-878e-55f4e71d0309** == Bluegiga/ Silicon chips!
  - It doesn't hurt that the OUIPrint is corroborating ;)
- Note: I could be wrong, and it could be that this UUID128 is actually all Milwaukee equipment that is missing the other IDs like UUID16 or Milwaukee MSD or GATT info
- This is why we need more crowdsourced data!

iBeacon: "The other UUID128!"

UUID128Print

iBeacon: "The other UUID128!"

UUID128Print

- Plot Twist! The Bluegiga *module* was based on a TI *chip*!

iBeacon: "The other UUID128!"

UUID128Print

- Plot Twist! The Bluegiga *module* was based on a TI *chip*!

7 Block diagram

BLE112 is based on TI's CC2540 chip. Embedded 32 MHz and 32.678 kHz crystals are used for clock generation. Matched balun and low pass filter provide optimal radio performance with extremely low spurious emissions. Small ceramic chip antenna gives good radiation efficiency even when the module is used in layouts with very limited space. https://www.silabs.com/documents/public/data-sheets/BLE112-DataSheet.pdf

iBeacon: "The other UUID128!"

UUID128Print

- Plot Twist! The Bluegiga *module* was based on a TI *chip*!

7 Block diagram

BLE112 is based on TI's CC2540 chip Embedded 32 MHz and 32.678 kHz crystals are used for clock generation. Matched balun and low pass filter provide optimal radio performance with extremely low spurious emissions. Small ceramic chip antenna gives good radiation efficiency even when the module is used in layouts with very limited space. https://www.silabs.com/documents/public/data-sheets/BLE112-DataSheet.pdf

But sometimes...

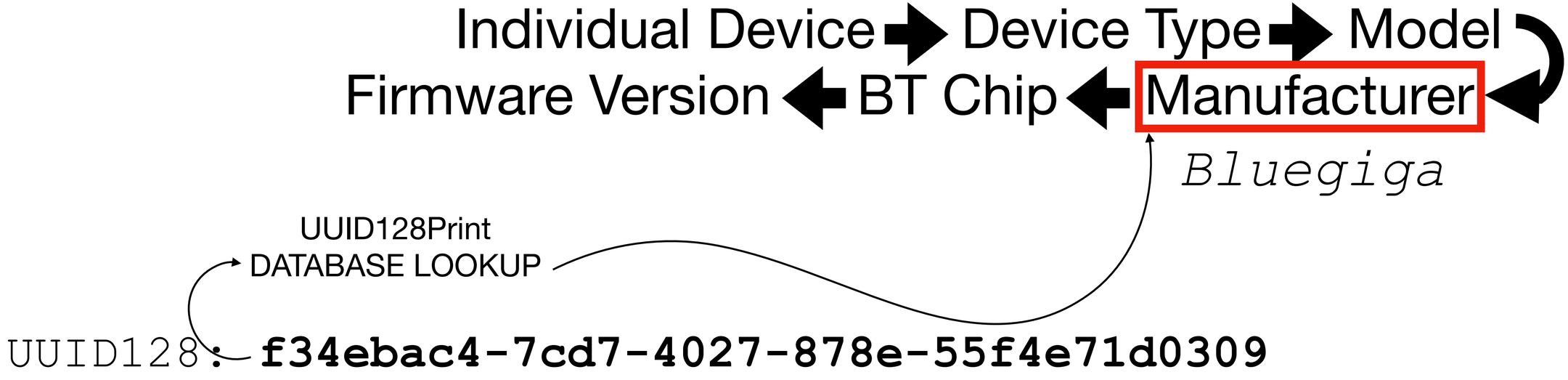
Individual Device → Device Type → Model ↷
Firmware Version ← BT Chip ← Manufacturer

But sometimes...

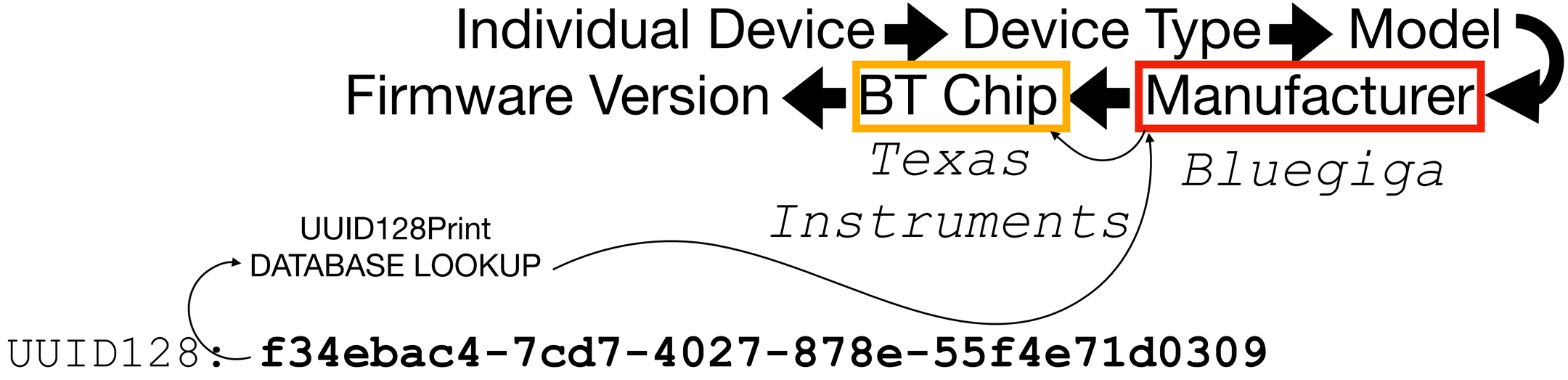
Individual Device → Device Type → Model ↷
Firmware Version ← BT Chip ← Manufacturer ↶

`UUID128:` **`f34ebac4-7cd7-4027-878e-55f4e71d0309`**

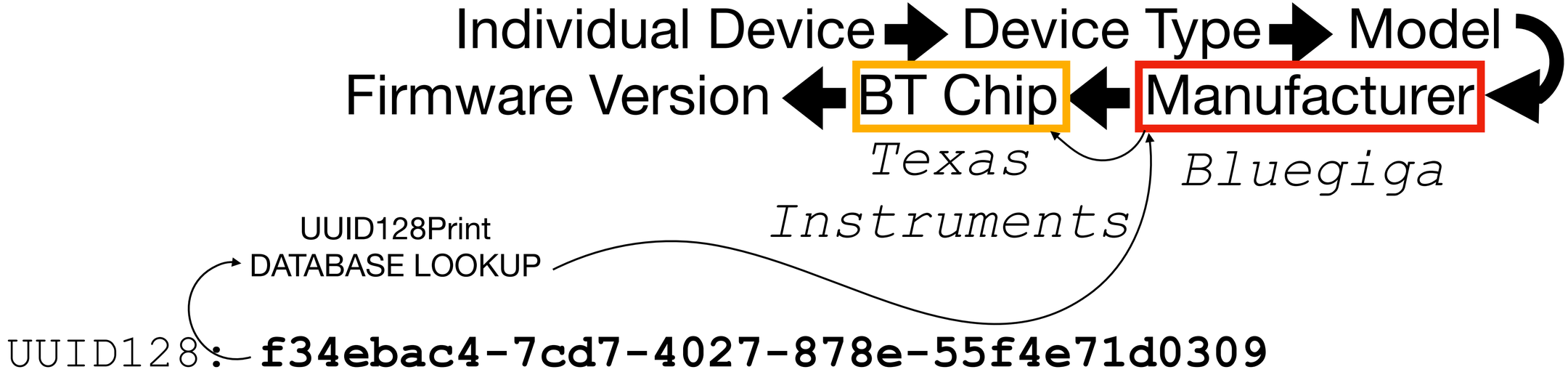
But sometimes...



But sometimes...

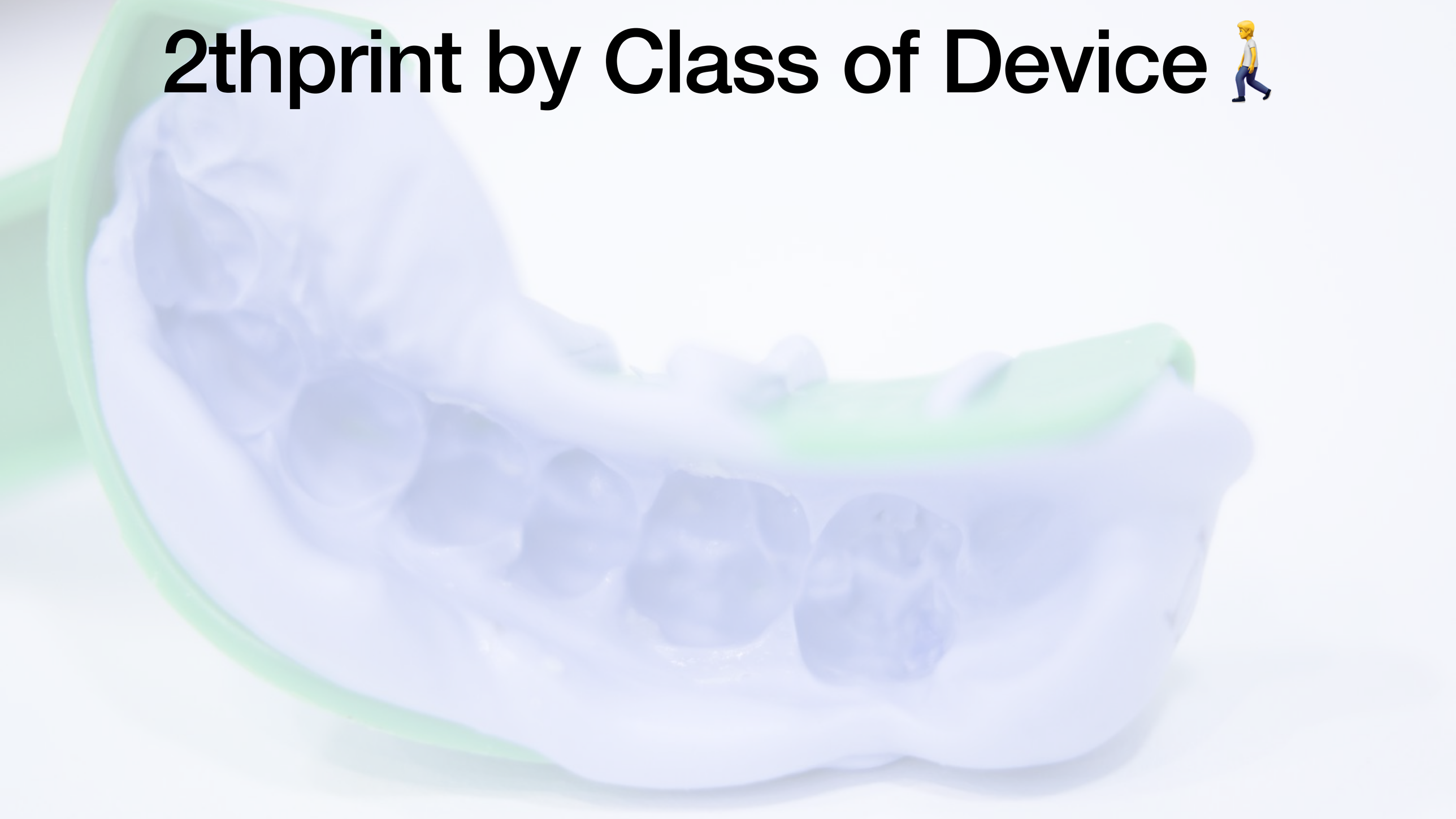


But sometimes...



ASSUMPTION:
UUID128Prints can be reused *within* Manufacturers,
but not reused *between* Manufacturers

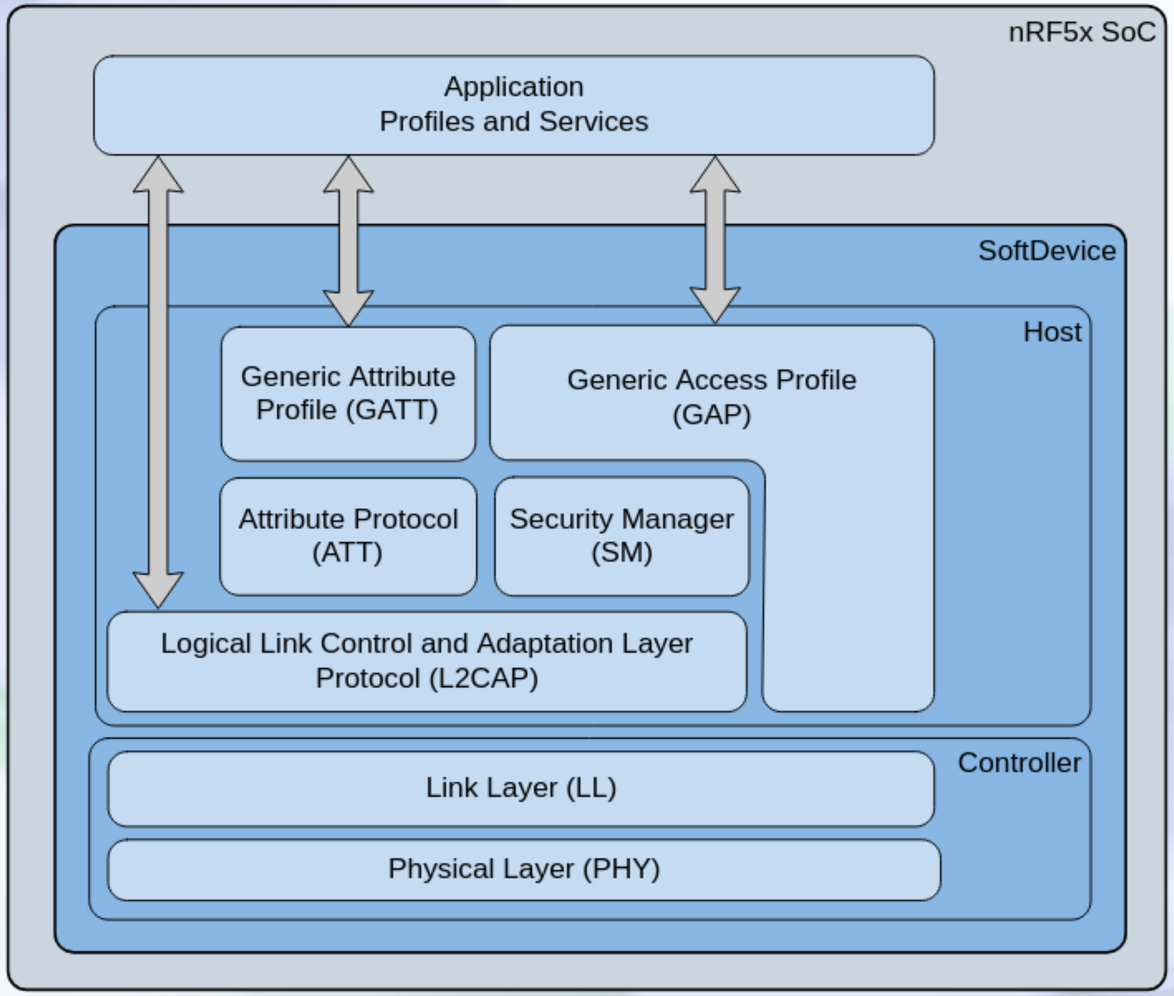
2thprint by Class of Device 🚶



2thprint by Class of Device 🚶

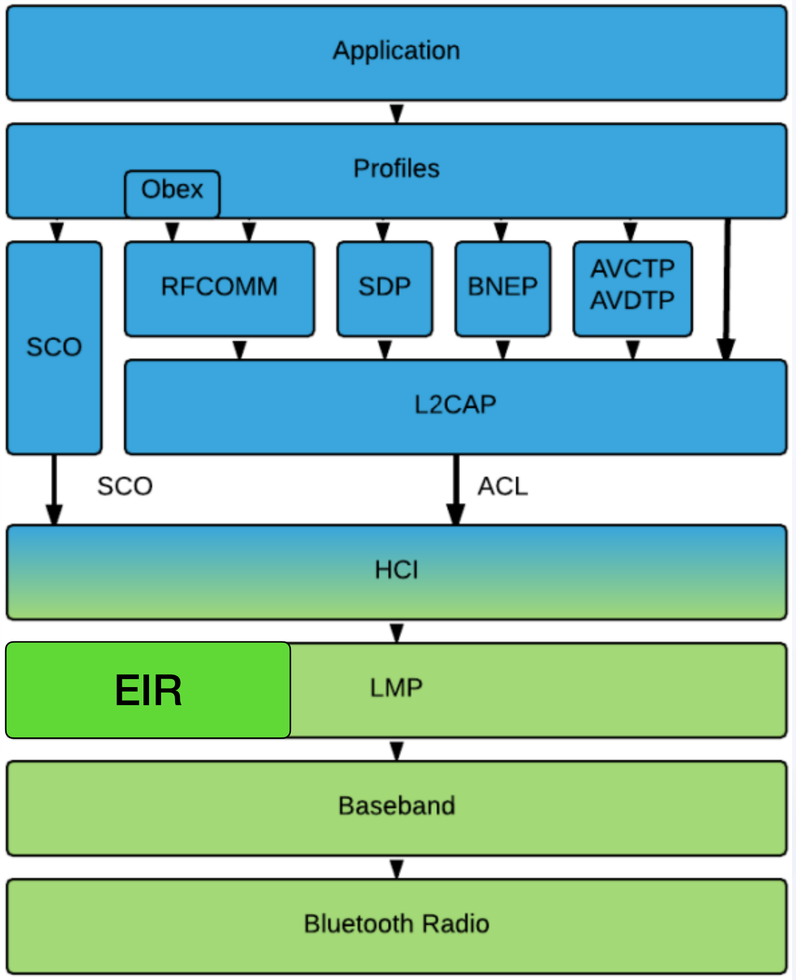
BLE

[1]



BTC

[2]

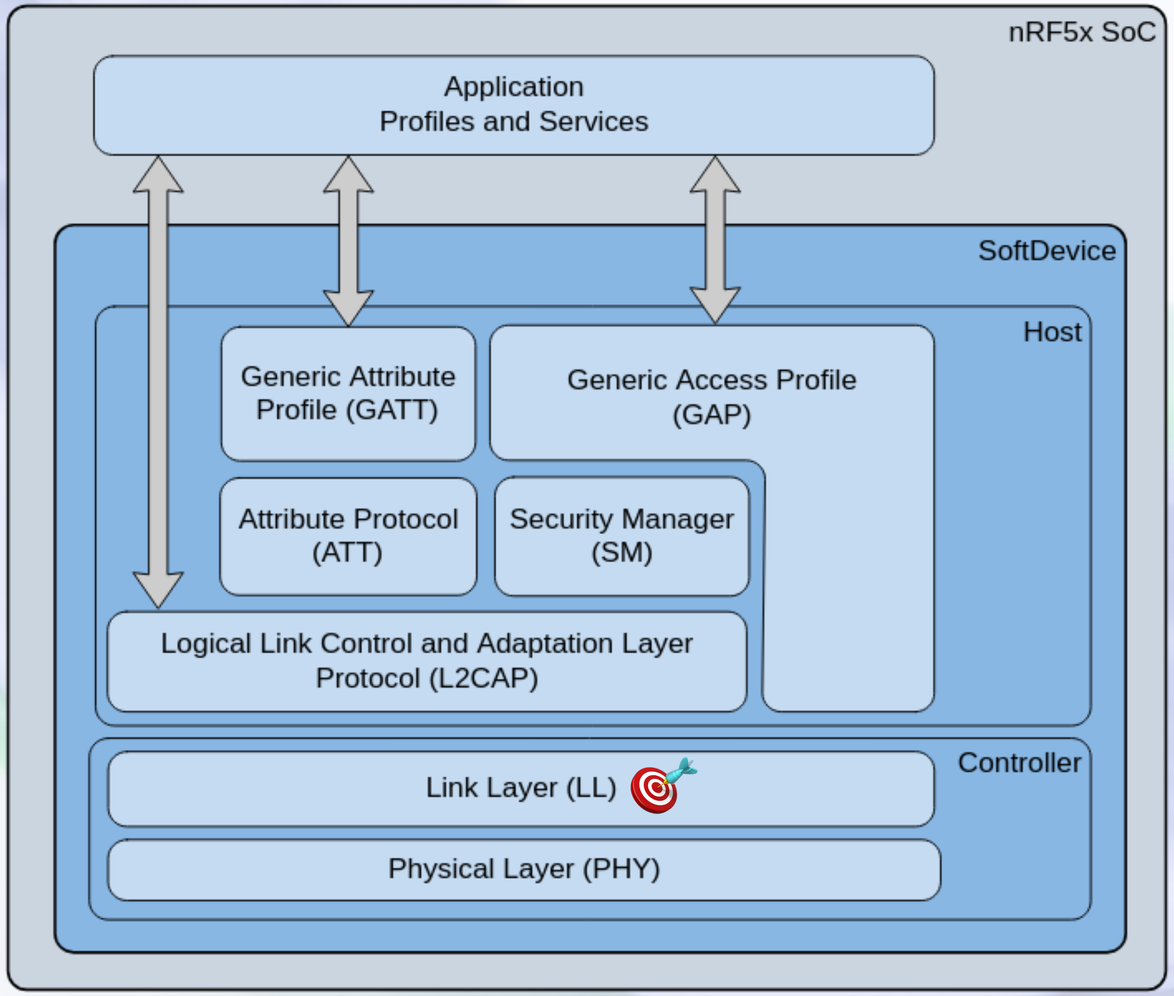


[1] https://infocenter.nordicsemi.com/index.jsp?topic=%2Fsds_s140%2FSDS%2Fs1xx%2Fble_protocol_stack%2Fble_protocol_stack.html
[2] https://crosscontrol.com/manual/Bluetooth%20Documentation/content/bluetooth.html

2thprint by Class of Device 🚶

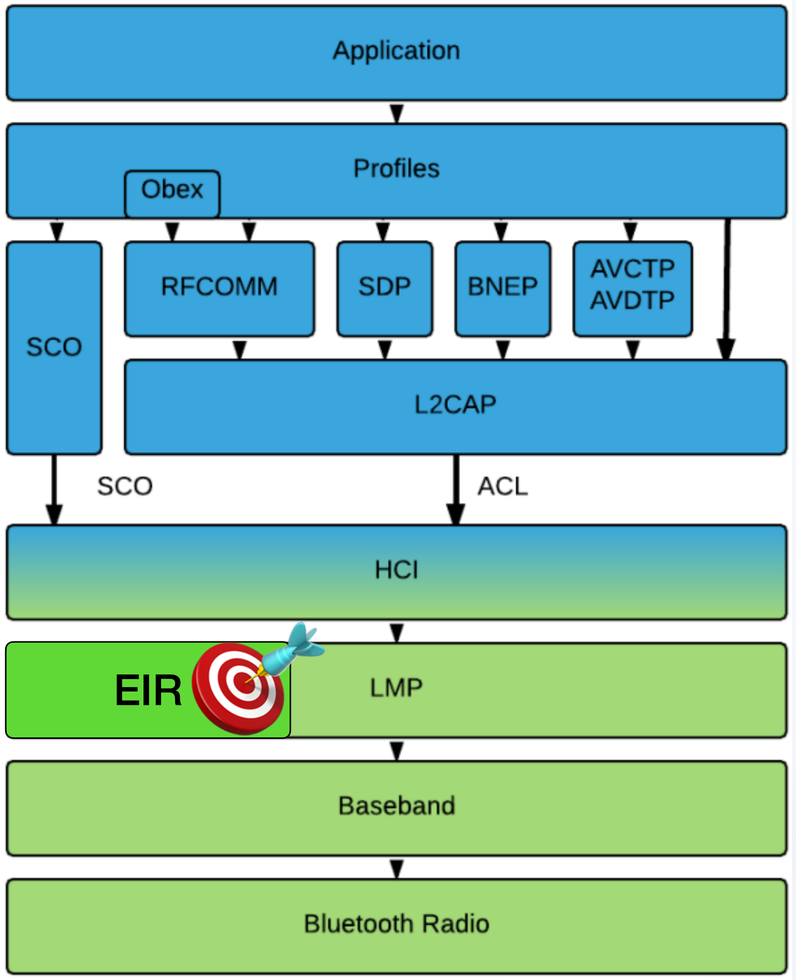
BLE

[1]



BTC

[2]



[1] https://infocenter.nordicsemi.com/index.jsp?topic=%2Fsds_s140%2FSDS%2Fs1xx%2Fble_protocol_stack%2Fble_protocol_stack.html
[2] https://crosscontrol.com/manual/Bluetooth%20Documentation/content/bluetooth.html

2thprint by Class of Device (CoD)

Primarily applicable to BTC (but some rare BLE devices use it too)

- BTC Extended Inquiry Response (EIR) packets contain a 24-bit CoD value

2.8 Class of Device

Referenced from the following:

- Bluetooth Core Specification [Vol 2] Part B, Section 6.5.1.4 [4].
- Supplement to the Bluetooth Core Specification Part A, Section 1.6.2 [22].

The Class of Device is composed of four fields: A Major Service Classes bitfield, a Major Device Class enumerated value, the Minor Device Classes, and a fixed value of 0b00 in the two least significant bits. The format of the Minor Device Class is determined by the Major Device Class value. The structure of the Class of Device is defined below:

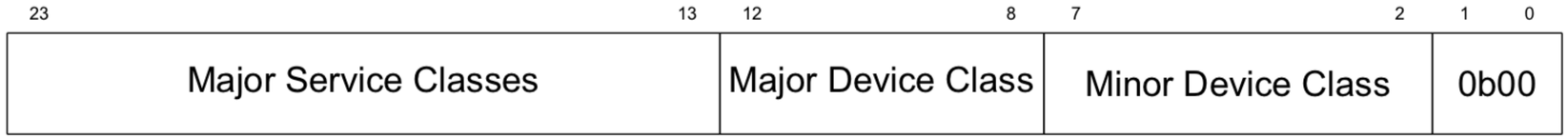


Figure 2.2: Class of Device format

2.8.2 Major Device Classes

The Miscellaneous major device class is used where a more specific Major Device Class code is not suitable. A device that does not have a major class code assigned can use the Uncategorizied: device code not specified until ”classified.”

Last Modified: 2022-05-25

12	11	10	9	8	Major Device Class
0	0	0	0	0	Miscellaneous
0	0	0	0	1	Computer (desktop, notebook, PDA, organizer, ...)
0	0	0	1	0	Phone (cellular, cordless, pay phone, modem, ...)
0	0	0	1	1	LAN/Network Access point
0	0	1	0	0	Audio/Video (headset, speaker, stereo, video display, VCR, ...)
0	0	1	0	1	Peripheral (mouse, joystick, keyboard, ...)
0	0	1	1	0	Imaging (printer, scanner, camera, display, ...)
0	0	1	1	1	Wearable
0	1	0	0	0	Toy
0	1	0	0	1	Health
1	1	1	1	1	Uncategorized: device code not specified

2.8.1 Major Service Classes

Last Modified: 2022-05-25

Bit	Class of Device Major Service Class
13	Limited Discoverable Mode
14	LE audio
15	Reserved for future use
16	Positioning (Location identification)
17	Networking (LAN, Ad hoc, ...)
18	Rendering (Printing, Speakers, ...)
19	Capturing (Scanner, Microphone, ...)
20	Object Transfer (v-Inbox, v-Folder, ...)
21	Audio (Speaker, Microphone, Headset service, ...)
22	Telephony (Cordless telephony, Modem, Headset service, ...)
23	Information (WEB-server, WAP-server, ...)

Individual Device → Device Type → Model → Manufacturer → BT Chip → Firmware Version

2.8.2 Major Device Classes

The Miscellaneous major device class is used where a more specific Major Device Class code is not suitable. A device that does not have a major class code assigned can use the Uncategorizied: device code not specified until ”classified.”

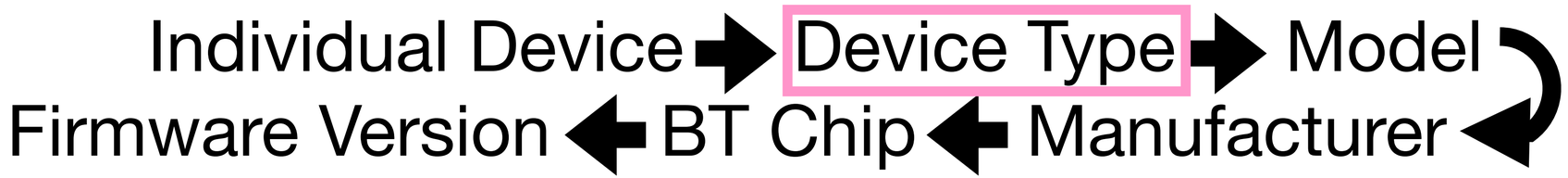
Last Modified: 2022-05-25

12	11	10	9	8	Major Device Class
0	0	0	0	0	Miscellaneous
0	0	0	0	1	Computer (desktop, notebook, PDA, organizer, ...)
0	0	0	1	0	Phone (cellular, cordless, pay phone, modem, ...)
0	0	0	1	1	LAN/Network Access point
0	0	1	0	0	Audio/Video (headset, speaker, stereo, video display, VCR, ...)
0	0	1	0	1	Peripheral (mouse, joystick, keyboard, ...)
0	0	1	1	0	Imaging (printer, scanner, camera, display, ...)
0	0	1	1	1	Wearable
0	1	0	0	0	Toy
0	1	0	0	1	Health
1	1	1	1	1	Uncategorized: device code not specified

2.8.1 Major Service Classes

Last Modified: 2022-05-25

Bit	Class of Device Major Service Class
13	Limited Discoverable Mode
14	LE audio
15	Reserved for future use
16	Positioning (Location identification)
17	Networking (LAN, Ad hoc, ...)
18	Rendering (Printing, Speakers, ...)
19	Capturing (Scanner, Microphone, ...)
20	Object Transfer (v-Inbox, v-Folder, ...)
21	Audio (Speaker, Microphone, Headset service, ...)
22	Telephony (Cordless telephony, Modem, Headset service, ...)
23	Information (WEB-server, WAP-server, ...)

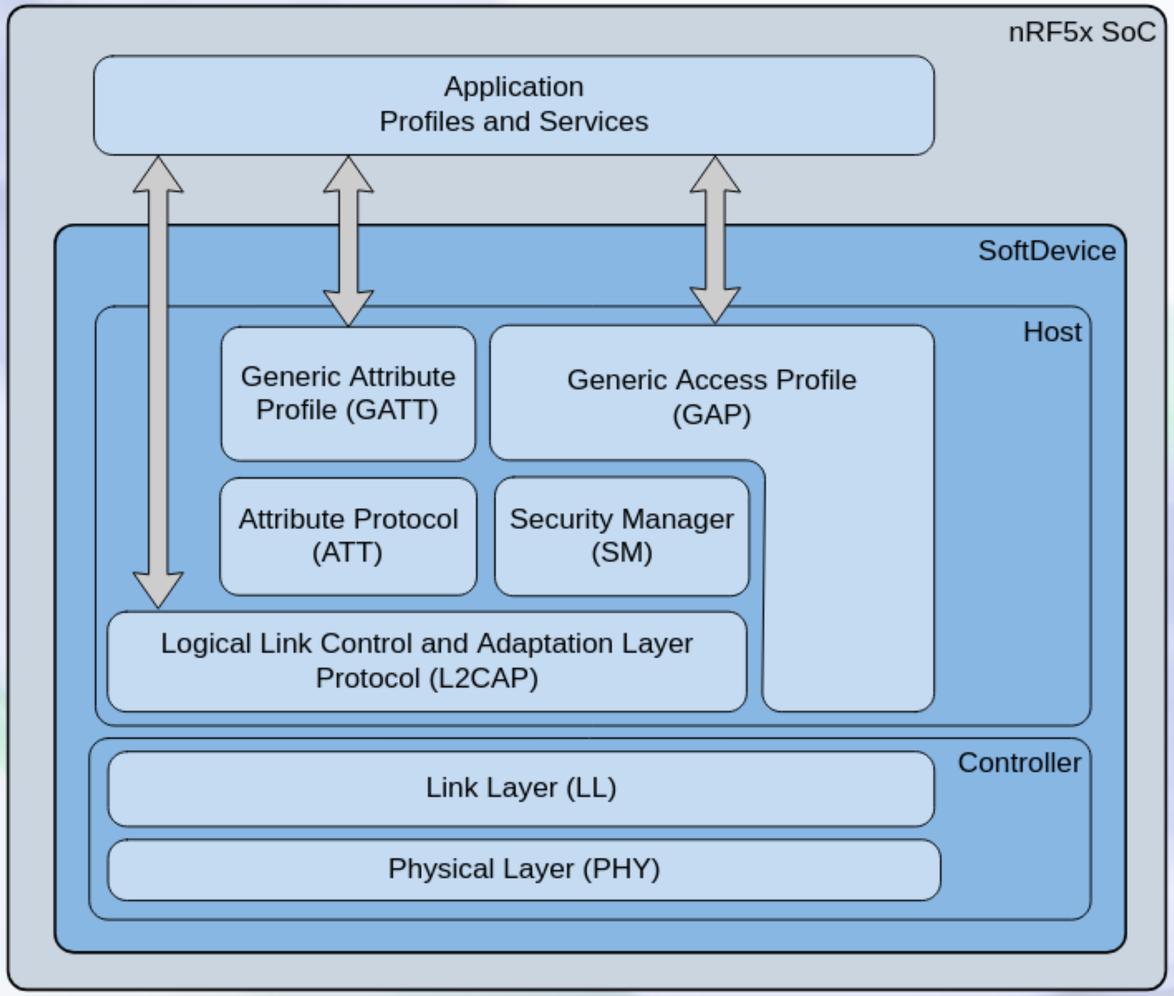


2thprint by SDP 🤾

2thprint by SDP

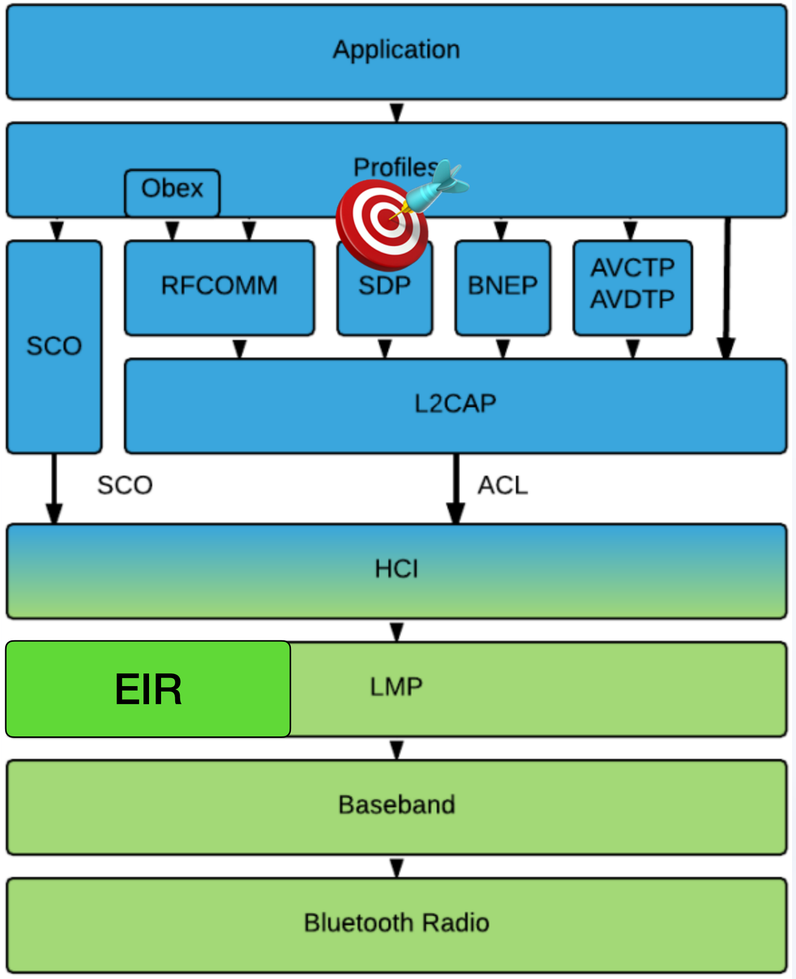
BLE

[1]



BTC

[2]



[1] https://infocenter.nordicsemi.com/index.jsp?topic=%2Fsds_s140%2FSDS%2Fs1xx%2Fble_protocol_stack%2Fble_protocol_stack.html
[2] https://crosscontrol.com/manual/Bluetooth%20Documentation/content/bluetooth.html

Prior Work

"Blueprinting - Remote Device Identification based on Bluetooth Fingerprinting Techniques"

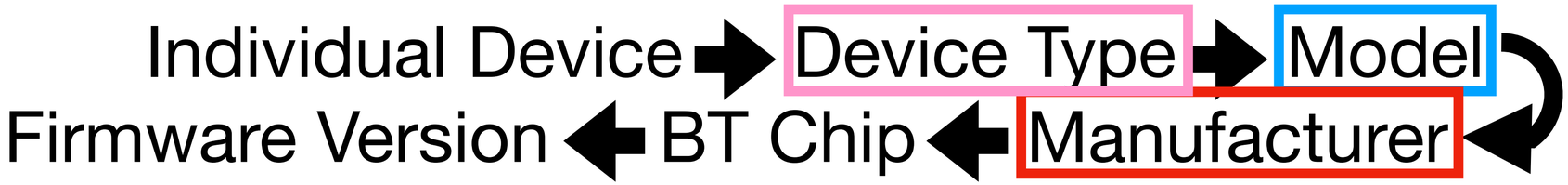
- [1] by Herfurt & Mulliner from 2004 connected to BTC devices via Service Discovery Protocol (SDP) and created a hash from selected data within the available profiles
  - I'm simply using the deprecated "sdptool" from BlueZ with its existing XML output option. *But I haven't decided how to process the data yet!*

[1] http://www.mulliner.org/collin/publications/Blueprinting.pdf

Prior Work

"Blueprinting - Remote Device Identification based on Bluetooth Fingerprinting Techniques"

- [1] by Herfurt & Mulliner from 2004 connected to BTC devices via Service Discovery Protocol (SDP) and created a hash from selected data within the available profiles
  - I'm simply using the deprecated "sdptool" from BlueZ with its existing XML output option. *But I haven't decided how to process the data yet!*

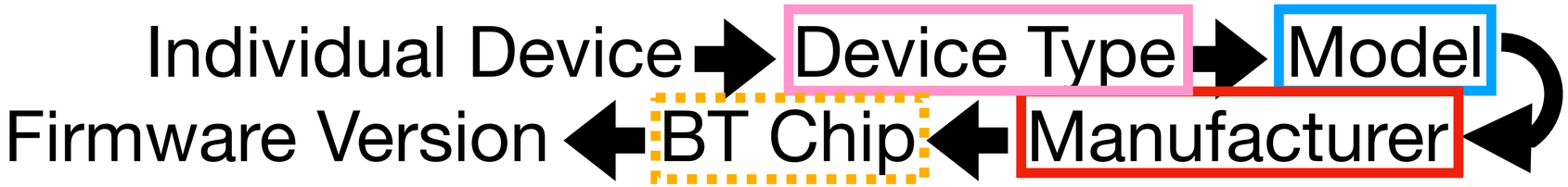


[1] http://www.mulliner.org/collin/publications/Blueprinting.pdf

Prior Work

"Blueprinting - Remote Device Identification based on Bluetooth Fingerprinting Techniques"

- [1] by Herfurt & Mulliner from 2004 connected to BTC devices via Service Discovery Protocol (SDP) and created a hash from selected data within the available profiles
  - I'm simply using the deprecated "sdptool" from BlueZ with its existing XML output option. *But I haven't decided how to process the data yet!*



[1] http://www.mulliner.org/collin/publications/Blueprinting.pdf

2thprint by "Pics or it didn't happen" 📸

2thprint by looking up teardown pictures :P

This is not scalable...unless we crowdsource it!

- When one wants to know the ChipPrint for a very specific device, one can just search for teardown pictures!
- Sometimes the FCC (or other wireless regulatory authorities') database "internal photos" are useful in this regard

E Tu Rivian?

- Regex: ^Rivian Sensor [1234]$ e.g. Rivian Sensor 1
- Regex: ^Rivian Phone Key$
- Regex: ^Rivian Camp Speaker$

https://apps.fcc.gov/eas/GetApplicationAttachment.html?id=5383917

E Tu Rivian?

- Regex: ^Rivian Sensor [1234]$ e.g. Rivian Sensor 1
- Regex: ^Rivian Phone Key$
- Regex: ^Rivian Camp Speaker$

Address type: **Public** (0x00)
Address: AC:4D:16:FD:40:93 (OUI AC-4D-16)
Name (complete): Rivian Sensor 3

https://apps.fcc.gov/eas/GetApplicationAttachment.html?id=5383917

E Tu Rivian?

- Regex: ^Rivian Sensor [1234]$ e.g. Rivian Sensor 1
- Regex: ^Rivian Phone Key$
- Regex: ^Rivian Camp Speaker$

Address type: **Public** (0x00)
Address: AC:4D:16:FD:40:93 (OUI AC-4D-16) ← Actually Texas Instruments btmon just didn't have it in its vendor database
Name (complete): Rivian Sensor 3

```
For bdaddr = AC:4D:16:FD:40:93:
        Company Name by IEEE OUI (AC:4D:16): Texas Instruments

        No BTC Extended Inquiry Result Device info.

        DeviceName: Rivian Sensor 3
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
```

https://apps.fcc.gov/eas/GetApplicationAttachment.html?id=5383917

E Tu

- Rege
- Rege
- Rege

Address
Address
Name (c

```
For bdaddr = A
        Compan

        No BTC

        Device
```

https://apps.fcc.gov/e

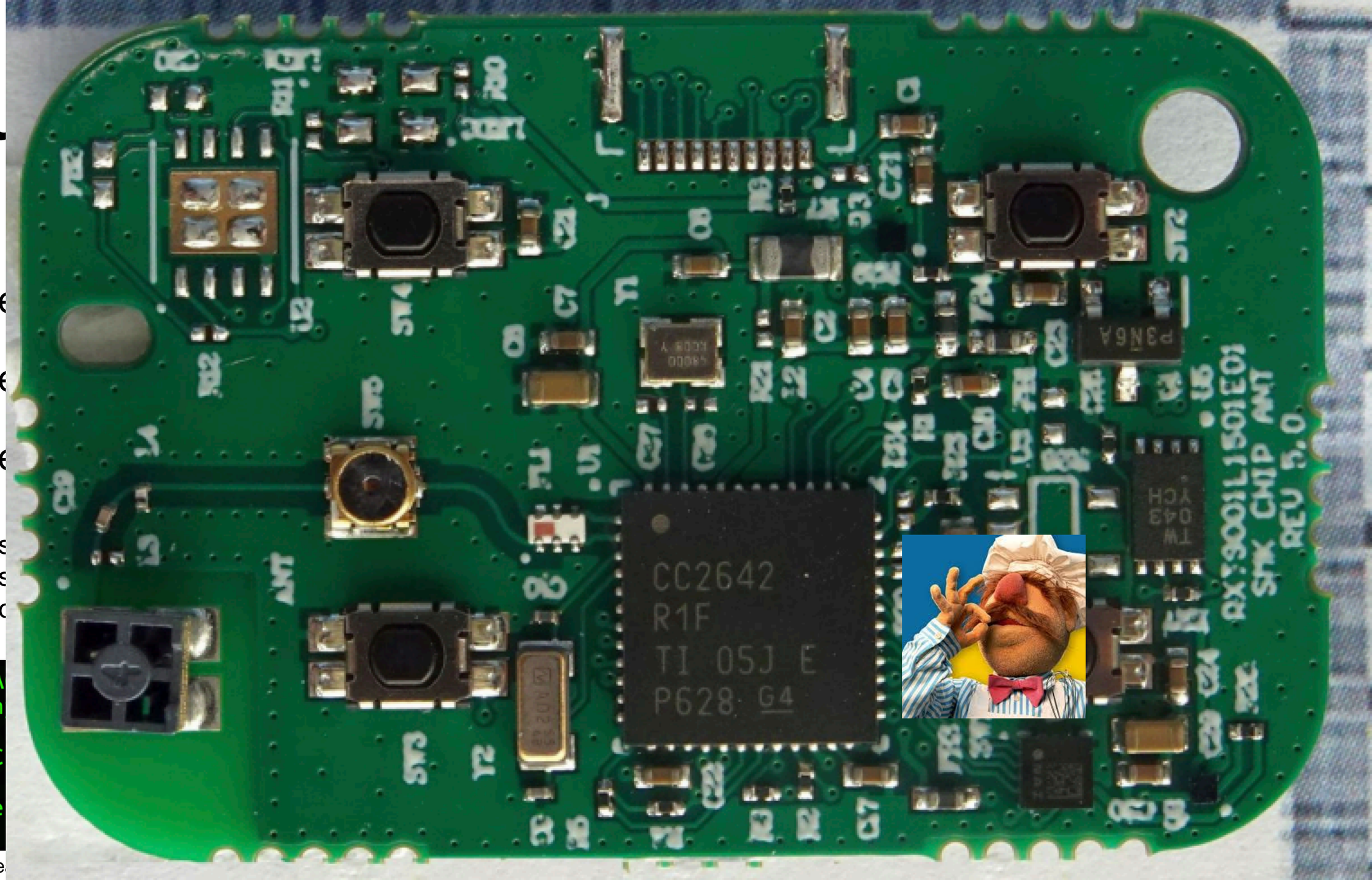
E Tu

- Rege
- Rege
- Rege

Address
Address
Name (c

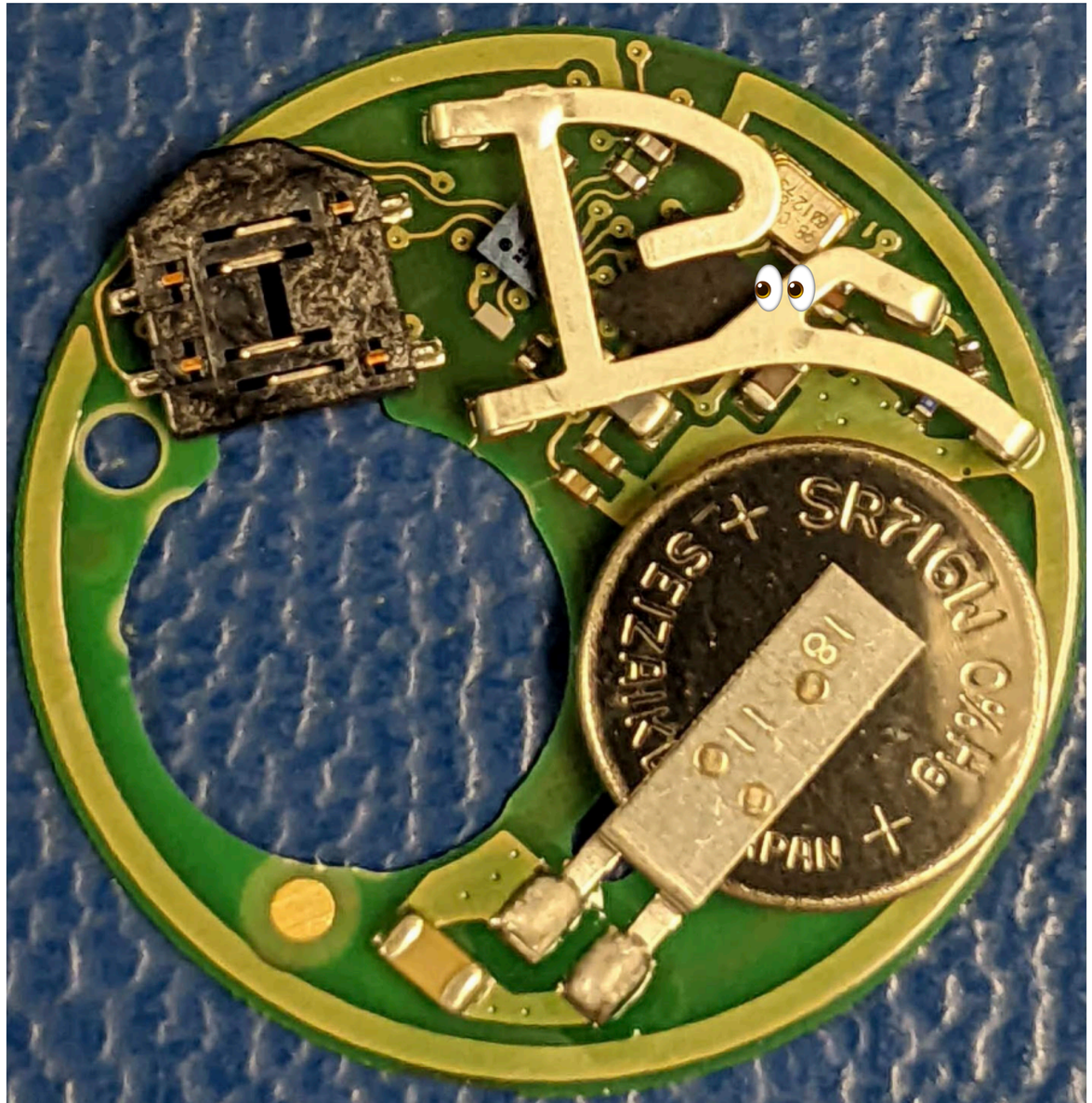
```
For bdaddr = A
        Compan

        No BTC

        Device
```

https://apps.fcc.gov/e

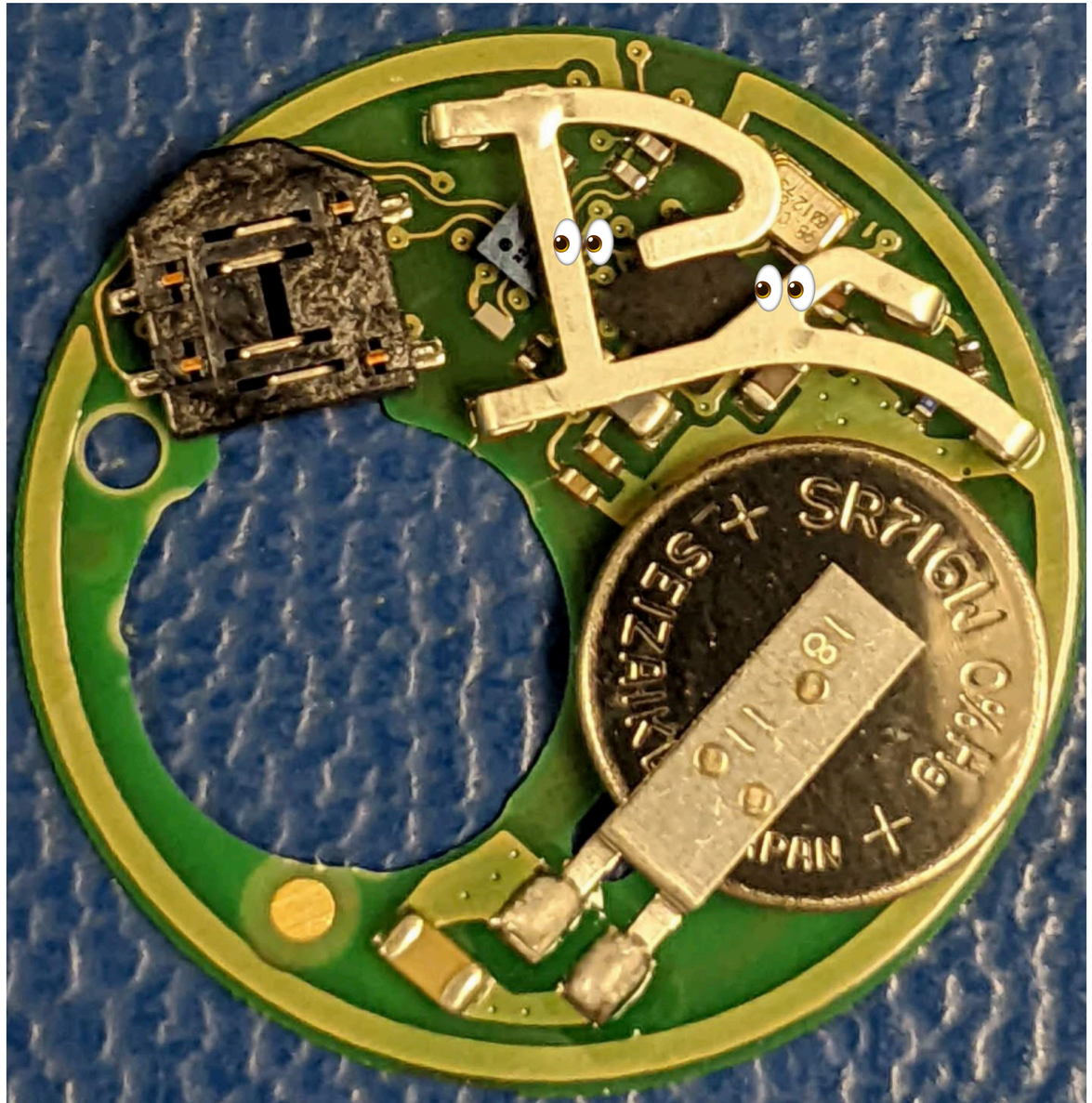


Common Case

Common Case

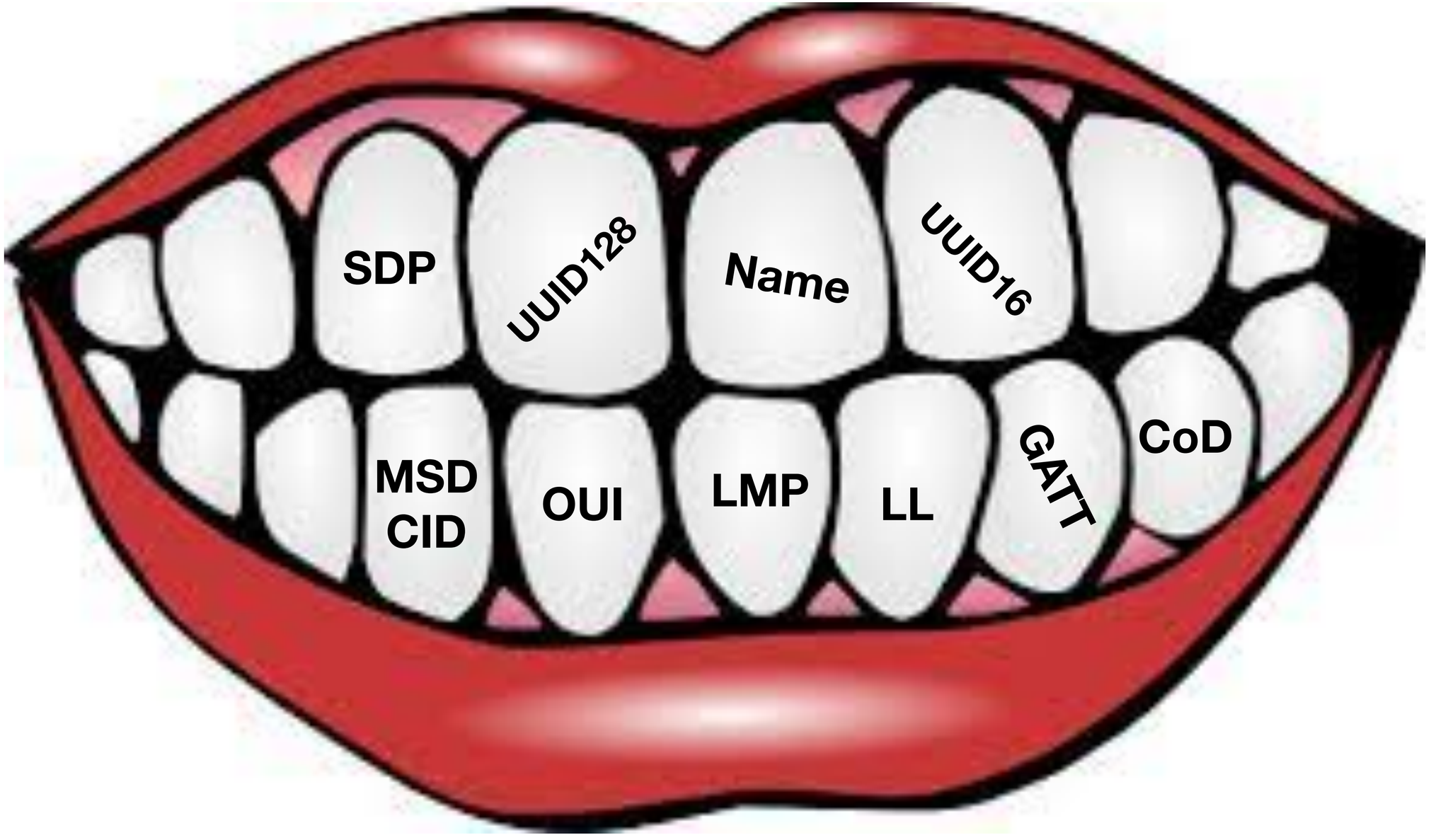


Common Case

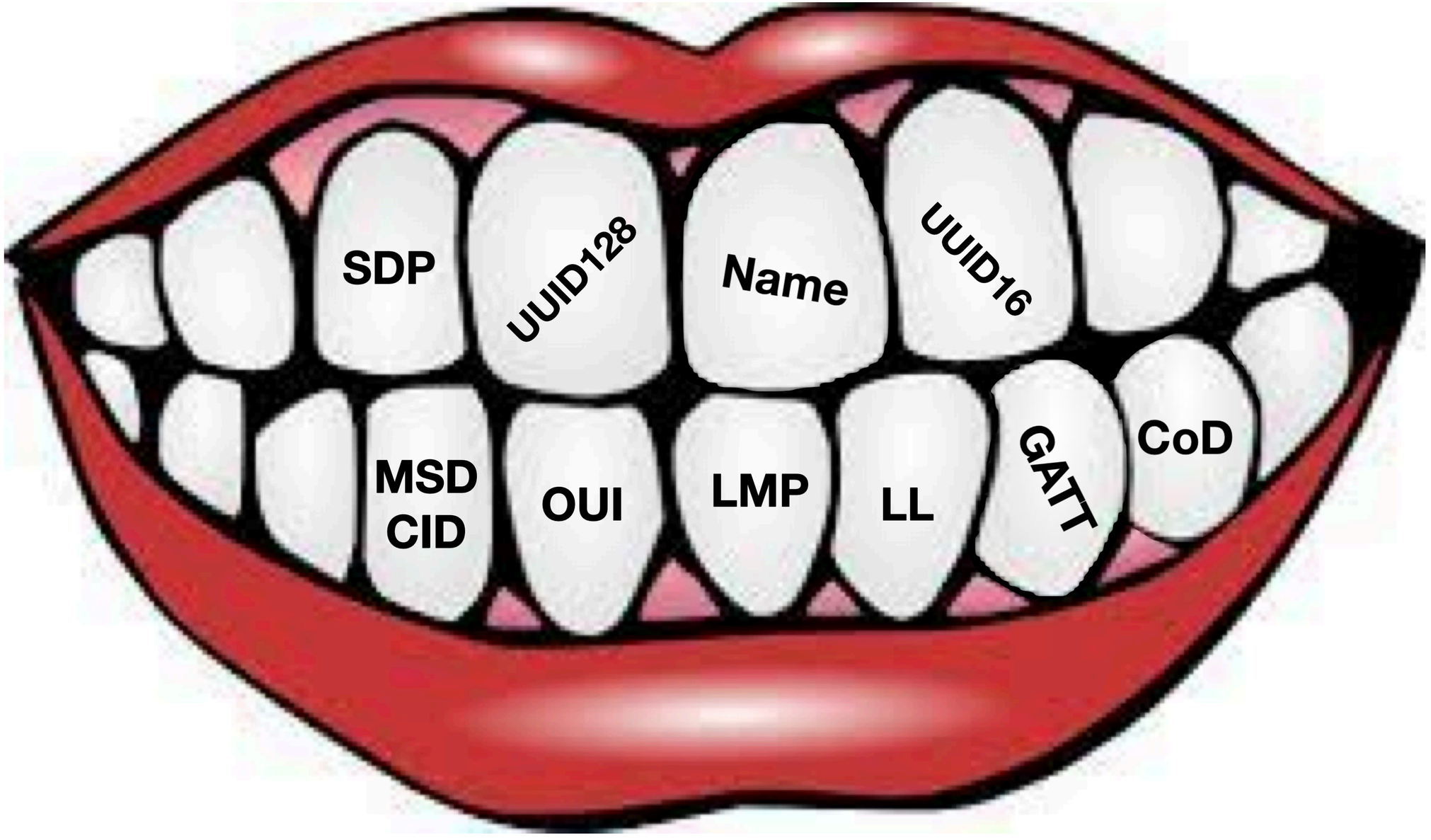


Putting It All *Toothgether* 😜

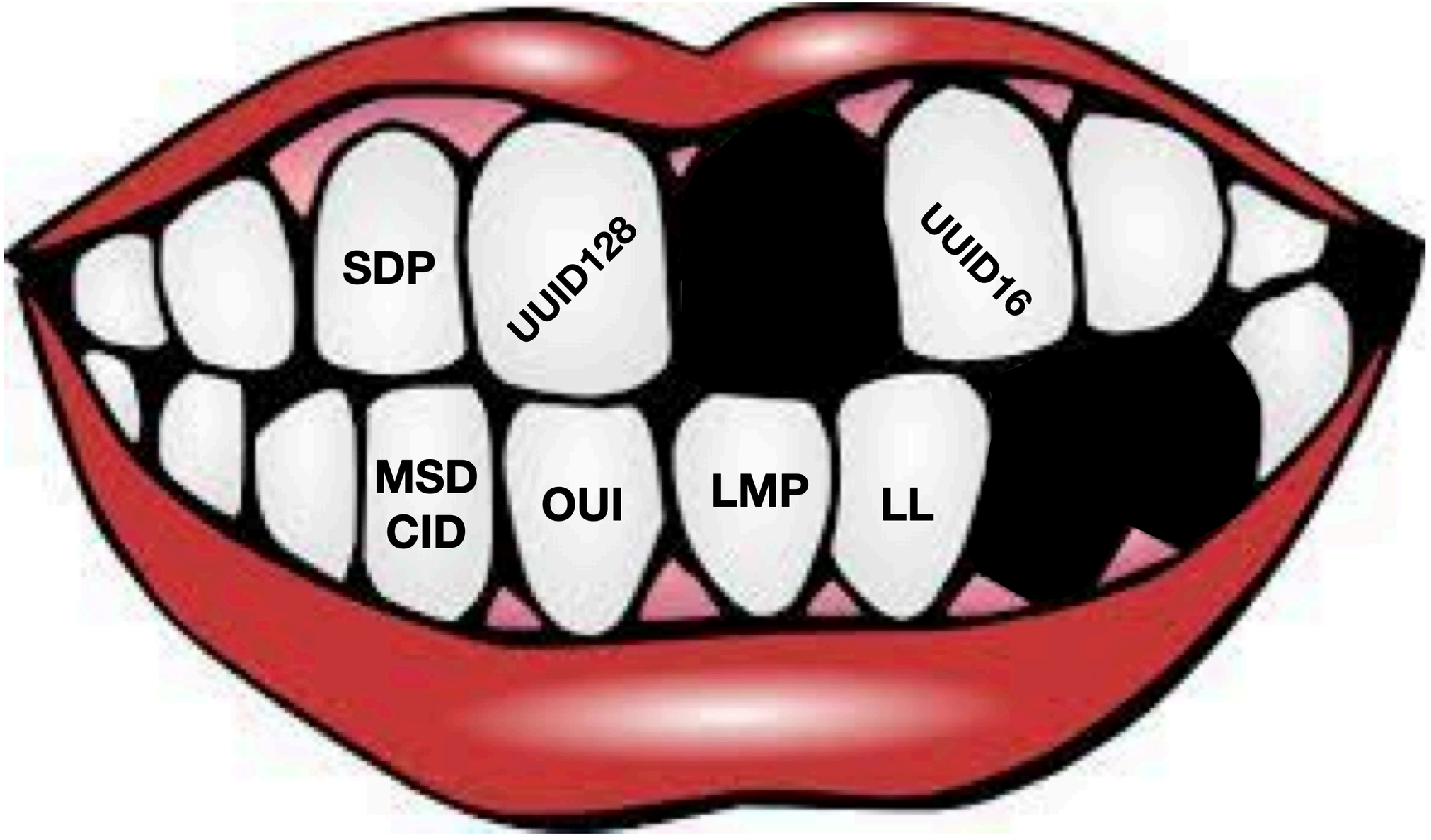
Putting It All *Toothgether* 😜

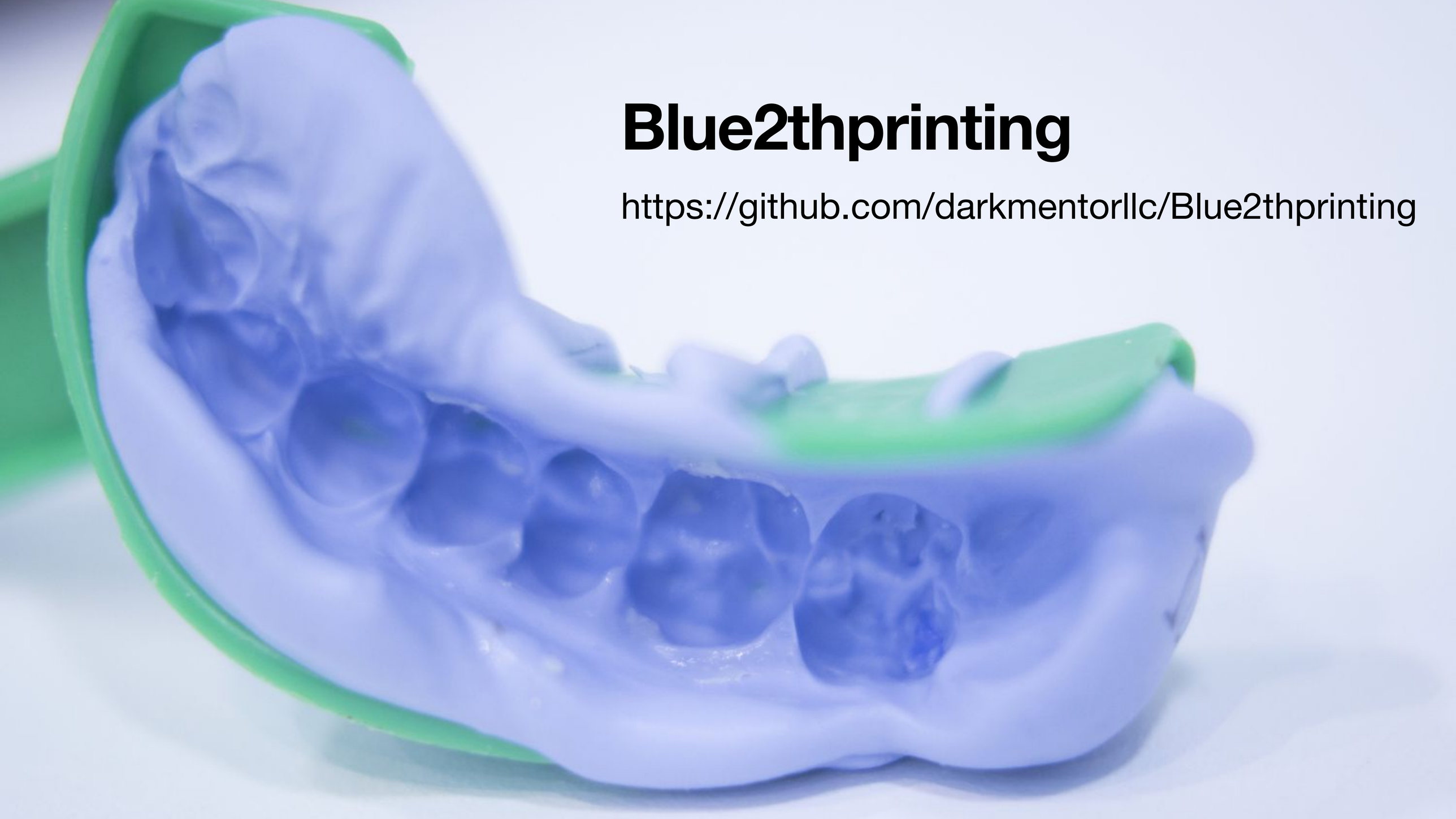


Reminder, even if wireless links weren't *lossy*, you're not generally going to have all the data for every device



Reminder, even if wireless links weren't *lossy*, you're not generally going to have all the data for every device





Blue2thprinting

https://github.com/darkmentorllc/Blue2thprinting

Call To Action!

Conclusion

- Bluetooth *vulnerability assessment* **is not yet a thing you can really do**!
- This is an active research topic I'm working on, but it needs more researchers working on it (because this is only 25% of my time ;))
  - "I'm puttin' together a (Blue)crew..."
- The starting point, as always, is to read related work
- I've organized the related work into a TiddlyWiki that I will continue to update over the coming years, and which others can contribute to via github PRs
  - https://darkmentor.com/bt.html

Fin

- BT research is cool
- But *OpenSecurityTraining2 (https://ost2.fyi , @OpenSecTraining) is cooler!*
  - We'll have BT classes eventually, but in the meantime there's so much other stuff to learn! Reverse Engineering, Vulnerabilities, Firmware, System Architecture!
- You should take a class, or *teach* a class!

Backup

Ongoing work

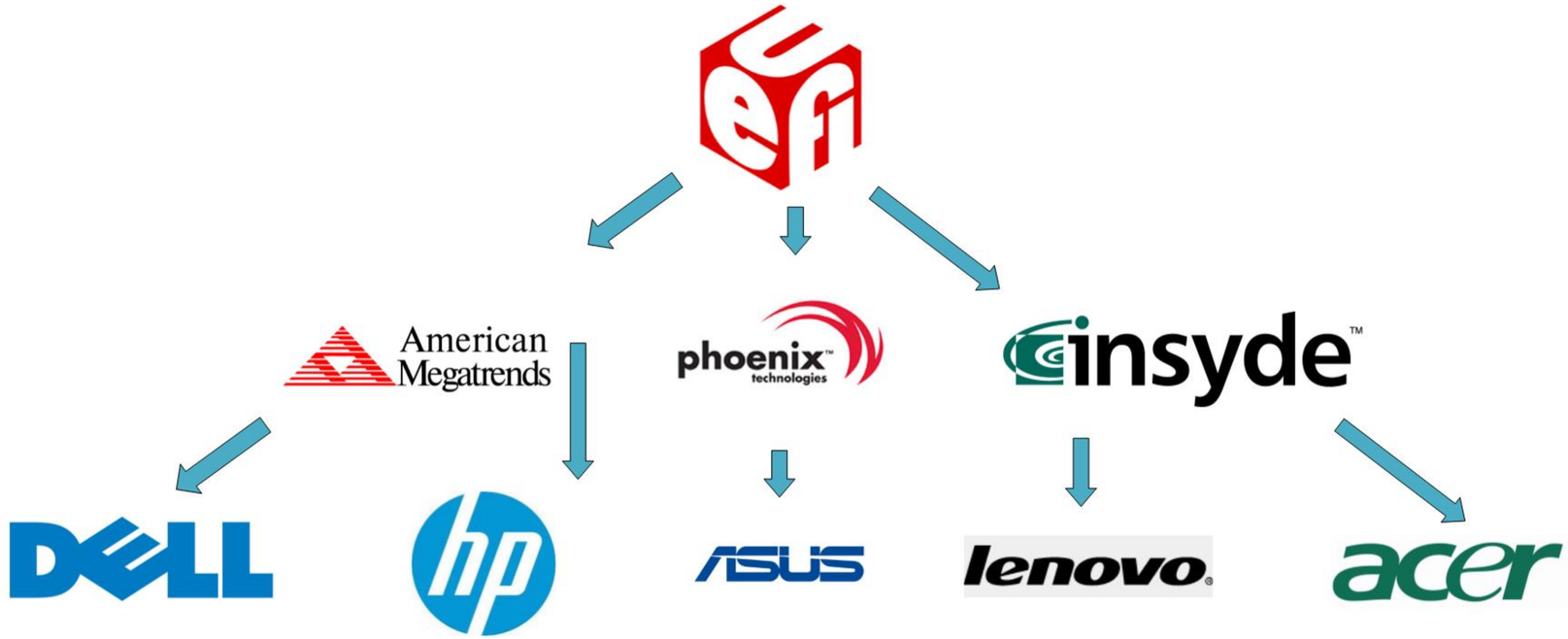
- How should I structure the 2thprints data?!
- What % of devices respond to GATT/SDP/LMP2th/LL2th/etc requests?
  - Working with a student on a research project to investigate more rigorously
- What other packet types (teef!) can we add to improve the 2thprint? (e.g. L2CAP? RFCOMM?) What about behaviors? (E.g. beaconing frequency.)
  - Also need to include vendor-specific overlay protocols like Apple Continuity
- Can we do the work they didn't do in [1] to *automatically* generate minimal chip-model-differentiation packet sequences from existing learned state machines?

[1] "Fingerprinting and analysis of Bluetooth devices with automata learning", Pferscher & Aichernig, https://link.springer.com/article/10.1007/s10703-023-00425-y

BTW

Did I mention the Bluetooth *ecosystem* is ***ARCHITECTURALLY UNSECURABLE***

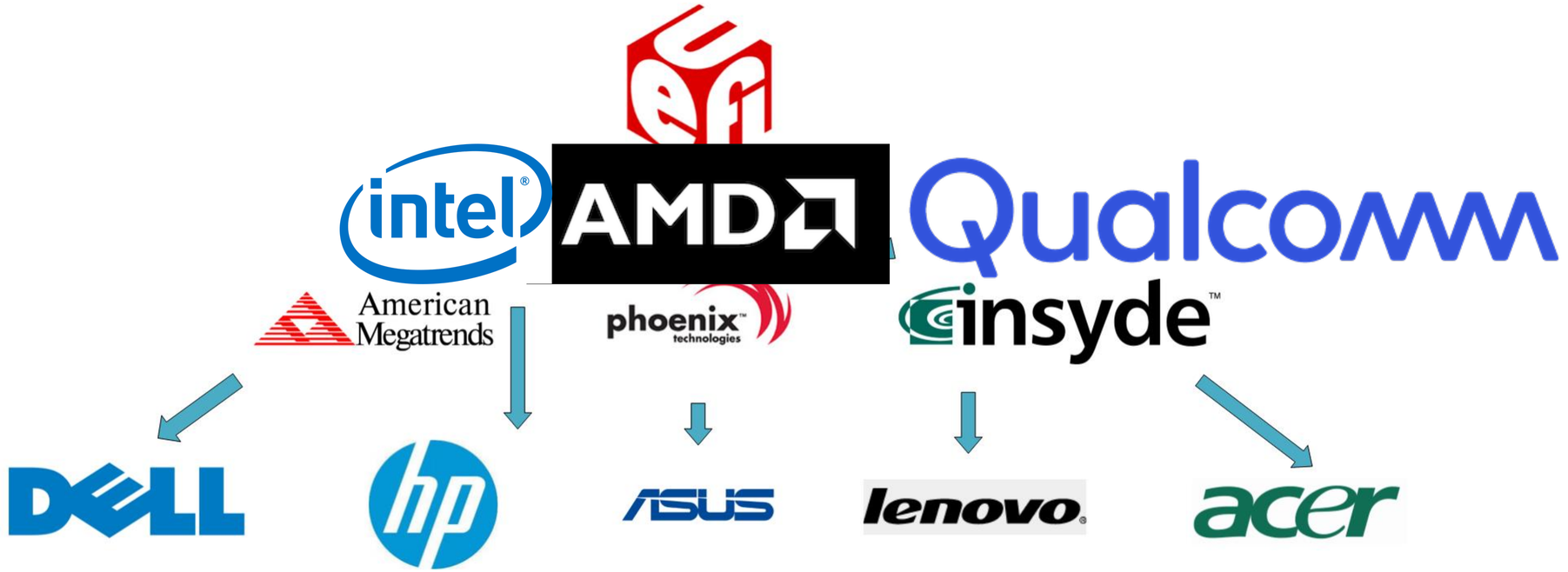
UEFI Vulnerability Proliferation



- **If an attacker finds a vulnerability in the UEFI "reference implementation," its proliferation across IBVs and OEMs would potentially be wide spread.**
  - More on how this theory works "in practice" later…

https://www.blackhat.com/docs/us-14/materials/us-14-Kallenberg-Extreme-Privilege-Escalation-On-Windows8-UEFI-Systems.pdf

UEFI Vulnerability Proliferation

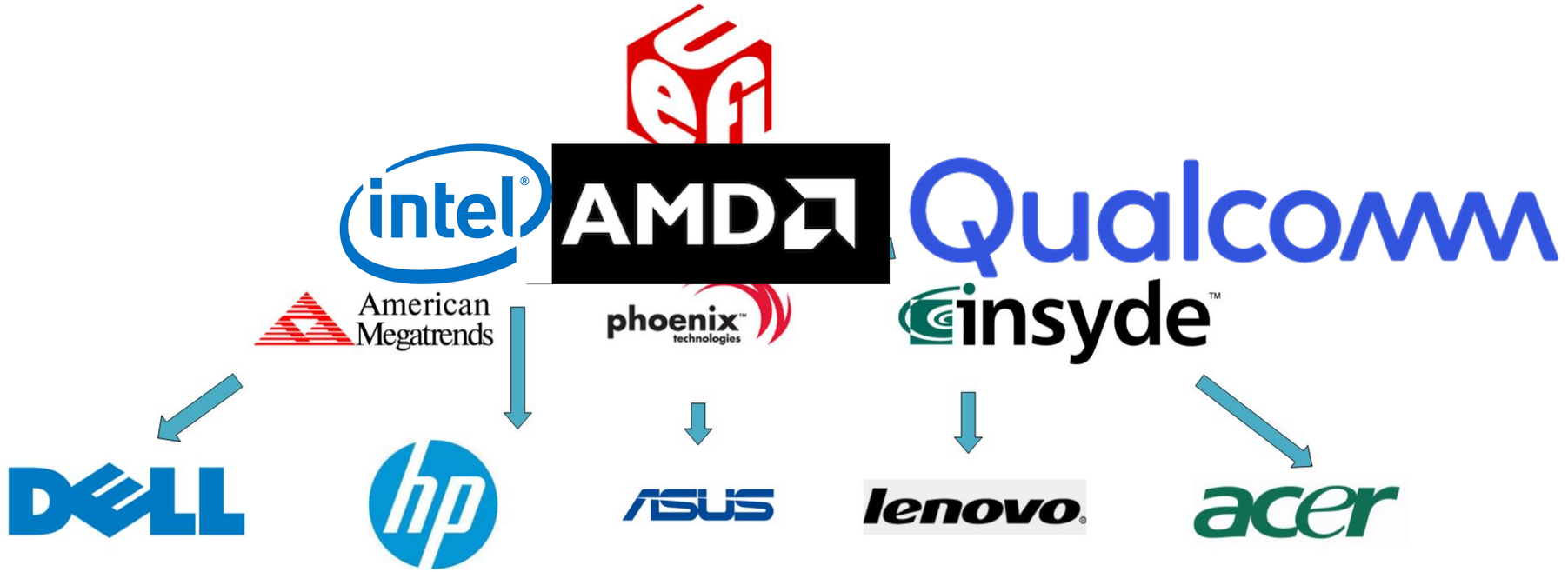


- **If an attacker finds a vulnerability in the UEFI "reference implementation," its proliferation across IBVs and OEMs would potentially be wide spread.**
  - More on how this theory works "in practice" later…

https://www.blackhat.com/docs/us-14/materials/us-14-Kallenberg-Extreme-Privilege-Escalation-On-Windows8-UEFI-Systems.pdf

UEFI Vulnerability Proliferation

SIG

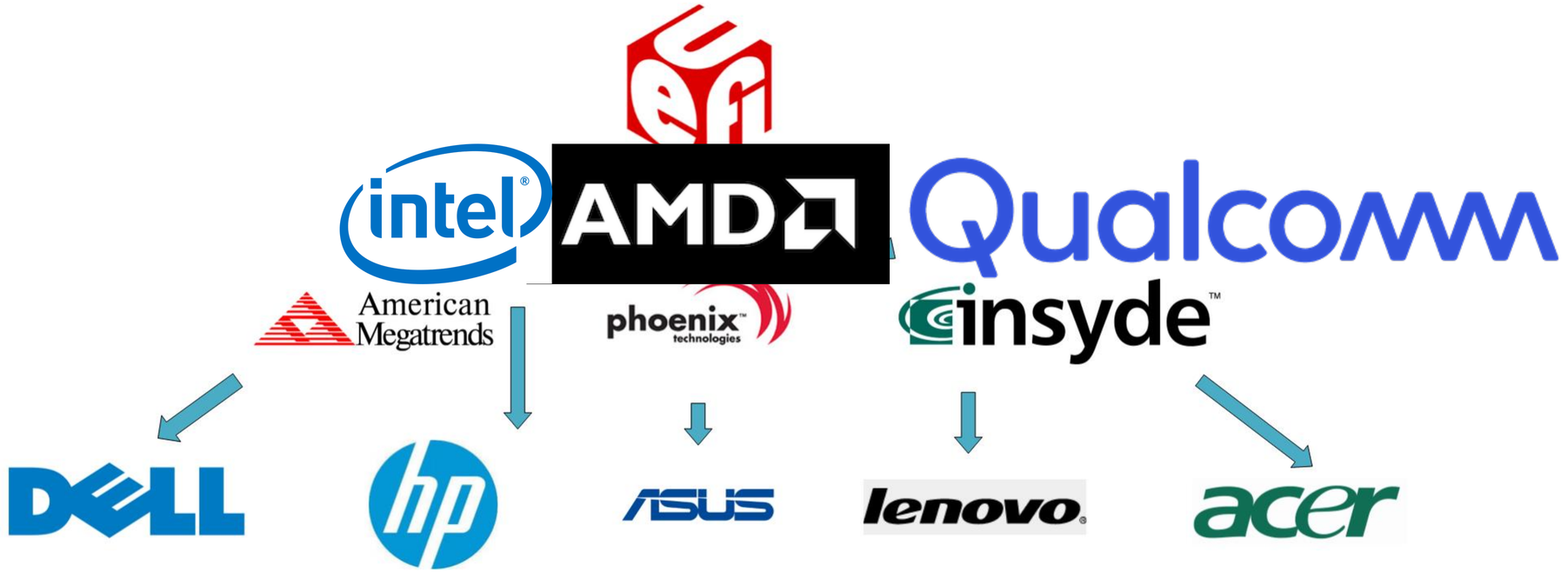


- **If an attacker finds a vulnerability in the UEFI "reference implementation," its proliferation across IBVs and OEMs would potentially be wide spread.**
  - More on how this theory works "in practice" later…

https://www.blackhat.com/docs/us-14/materials/us-14-Kallenberg-Extreme-Privilege-Escalation-On-Windows8-UEFI-Systems.pdf

UEFI Vulnerability Proliferation

SIG Silicon

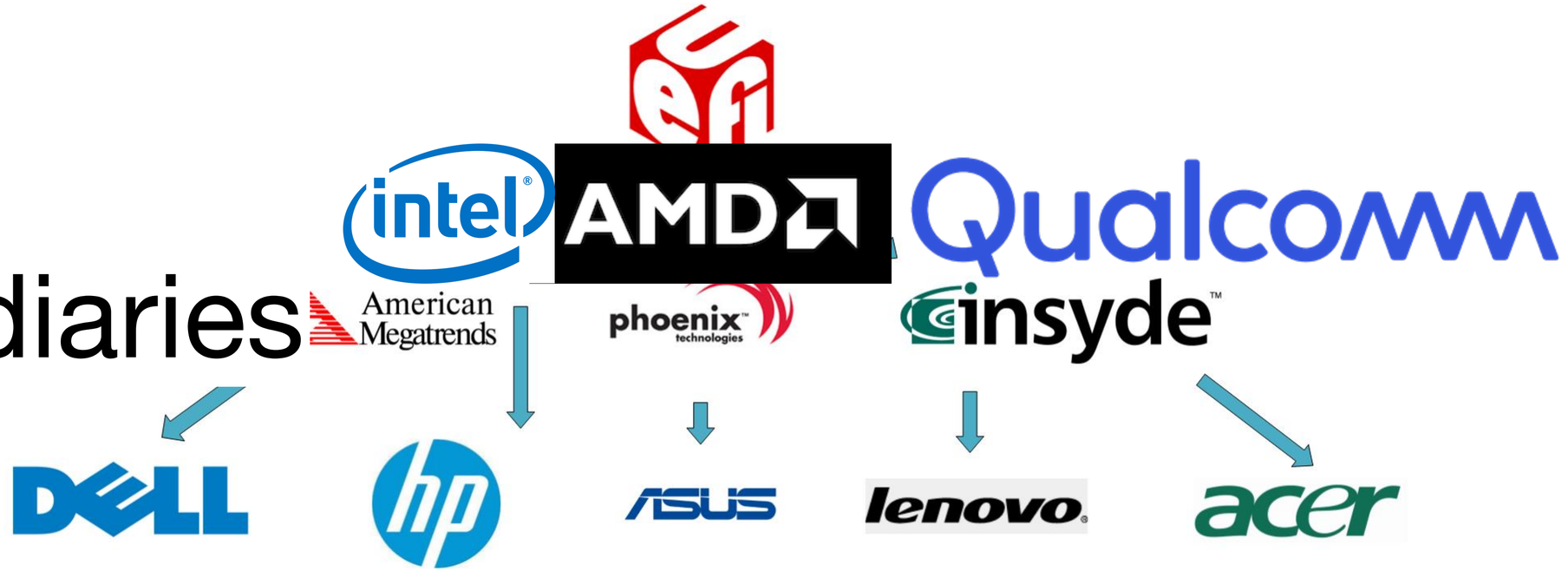


- **If an attacker finds a vulnerability in the UEFI "reference implementation," its proliferation across IBVs and OEMs would potentially be wide spread.**
  - More on how this theory works "in practice" later…

https://www.blackhat.com/docs/us-14/materials/us-14-Kallenberg-Extreme-Privilege-Escalation-On-Windows8-UEFI-Systems.pdf

UEFI Vulnerability Proliferation

SIG Silicon Intermediaries

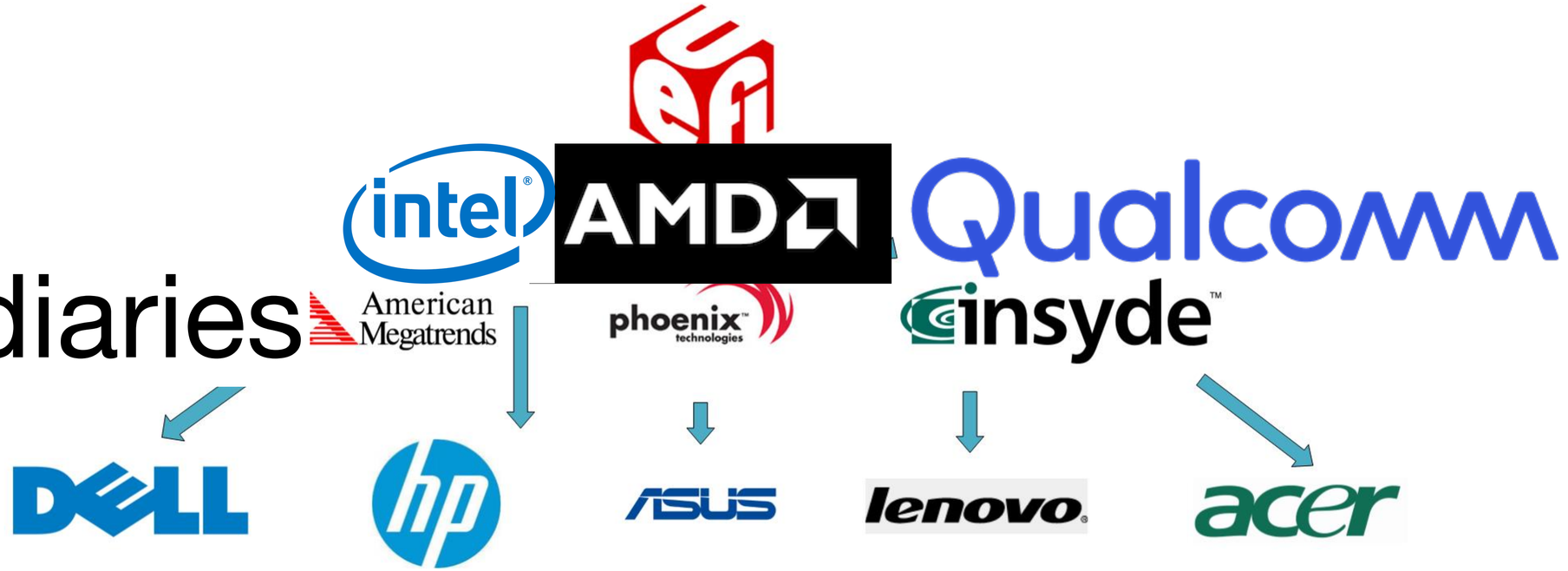


- **If an attacker finds a vulnerability in the UEFI "reference implementation," its proliferation across IBVs and OEMs would potentially be wide spread.**
  - More on how this theory works "in practice" later…

https://www.blackhat.com/docs/us-14/materials/us-14-Kallenberg-Extreme-Privilege-Escalation-On-Windows8-UEFI-Systems.pdf

UEFI Vulnerability Proliferation

SIG Silicon Intermediaries Device Makers



- **If an attacker finds a vulnerability in the UEFI "reference implementation," its proliferation across IBVs and OEMs would potentially be wide spread.**
  - More on how this theory works "in practice" later…

https://www.blackhat.com/docs/us-14/materials/us-14-Kallenberg-Extreme-Privilege-Escalation-On-Windows8-UEFI-Systems.pdf

Bluetooth®

DST2.FYI

SIG

SIG

Bluetooth®

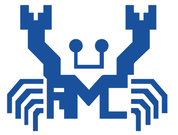
Silicon Vendors (>20)

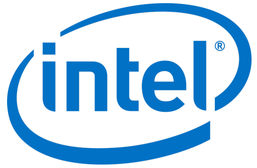
SIG

Bluetooth®

Silicon Vendors (>20)

Silicon





SIG

Bluetooth®

Silicon Vendors (>20)

Silicon

Module-Makers (IDEK how many)

SIG

Bluetooth®

Silicon Vendors (>20)

Silicon

Module-Makers (IDEK how many)

Intermediaries

SIG

Bluetooth®

Silicon Vendors (>20)

Silicon

Module-Makers (IDEK how many)

Intermediaries

Product-Makers

3330 *registered* with Bluetooth SIG as of the time of writing!

SIG

Bluetooth®

Silicon Vendors (>20)

Silicon

Module-Makers (IDEK how many)

Intermediaries

Device

Product-Makers

Makers ***3330*** *registered* with Bluetooth SIG as of the time of writing!

SIG

Bluetooth®

Silicon Vendors (>20)

Silicon

Module-Makers (IDEK how many)

Intermediaries

Device

Product-Makers

Makers ***3330*** *registered* with Bluetooth SIG as of the time of writing!

SIG

FOR SECURITY

Silicon

Module-Makers (IDEK how many)

Intermediaries

Device Makers

Product-Makers

3330 *registered* with Bluetooth SIG as of the time of writing!