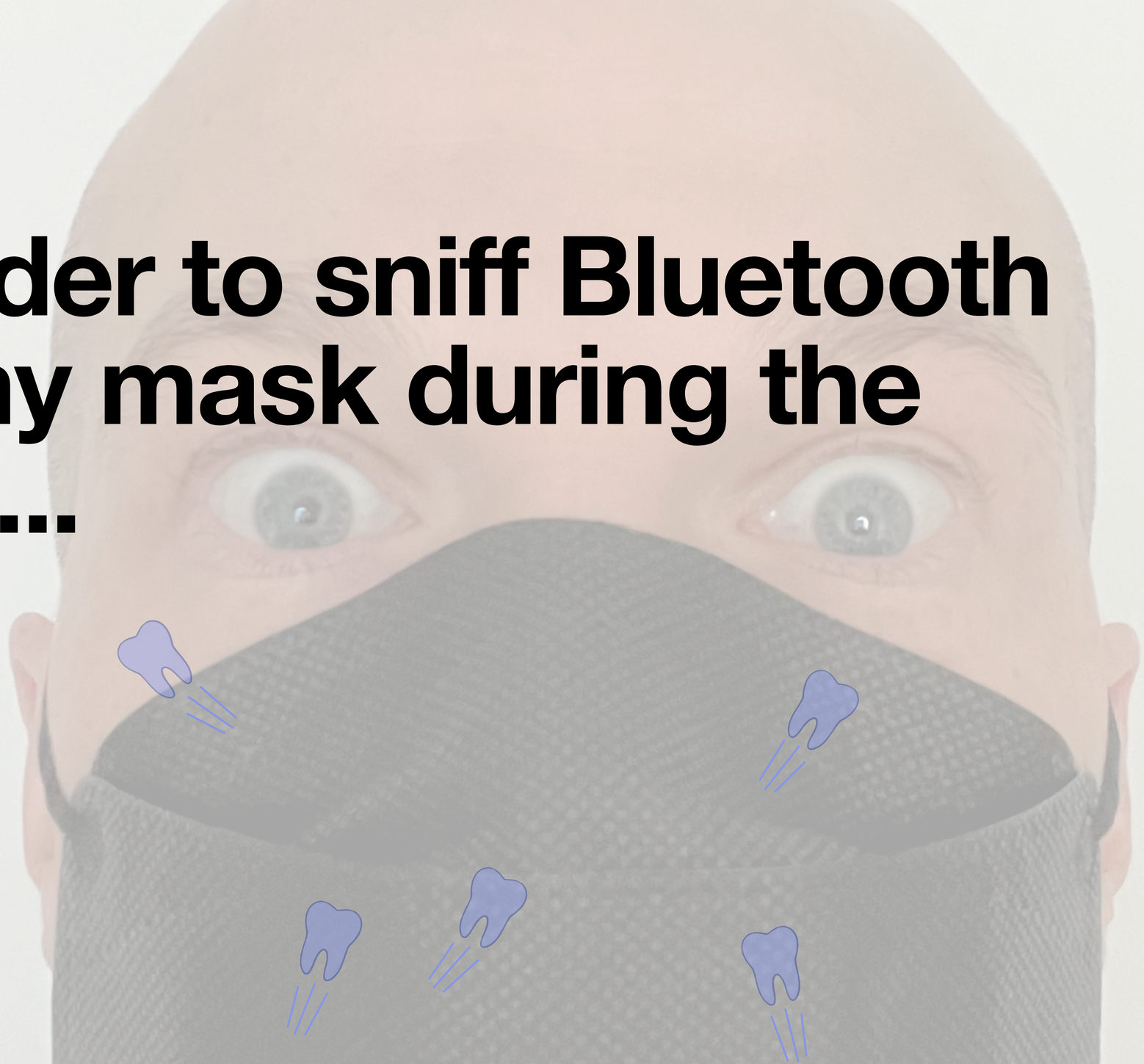
It was harder to sniff Bluetooth through my mask during the pandemic...



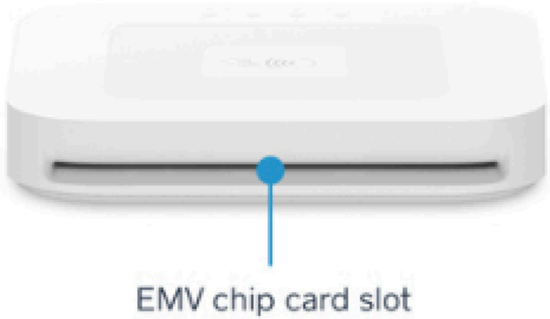
Xeno Kovah
OpenSecurityTraining2 &
Dark Mentor LLC

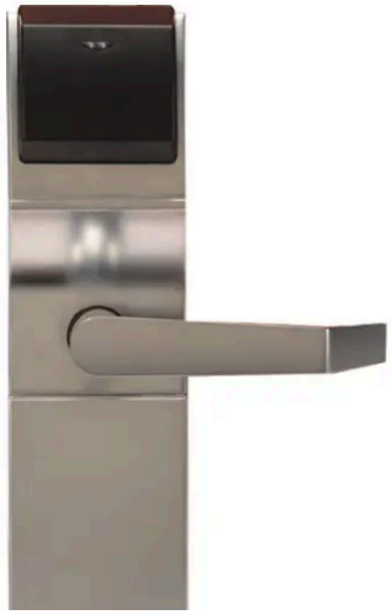
Begin - Prelude

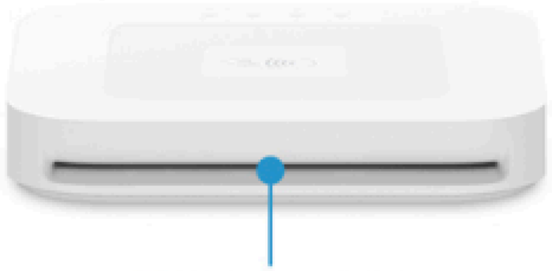
What I Want To Know:

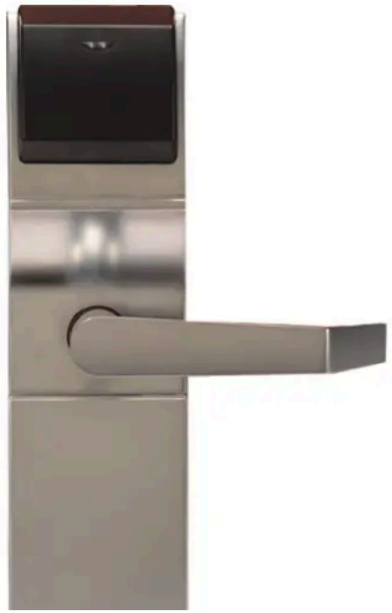
What Bluetooth Chip Is Inside Any Device

DARK MENTOR


EMV chip card slot







TEXAS INSTRUMENTS

BROADCOM®

SILICON LABS

?

Why I Want To Know It:

So I Know If It's Vulnerable To A Firmware-Level Exploit

DST2.FYI

TEXAS INSTRUMENTS

SILICON LABS

BROADCOM®

ARMIS®

DST2.FYI

Texas Instruments

SILICON LABS®

BROADCOM®

ARMIS®

DARK MENTOR

TEXAS INSTRUMENTS

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

How Am I Going To Figure It Out?

1) Know That I Know Nothing 😏
2) Do A Bunch Of Naive BT Data Collection
3) Find Out What I Don't Know

Takeaways 1

- *Bluetooth sniffing goals are different from WiFi goals*, and consequently the sniffing tech is under-developed to help with those goals
- When there's a BT FW bug, **no one knows what all it affects**

Takeaways 2

- There are lots of devices that do not have human-readable names, so it's not clear what they are
  - *Somebody (/me!)* ought to start learning to *toothprint* BT devices!
- There are lots of devices that are advertising names, but it's not clear what they are
  - I'm looking at you "***BLE003U***"
  - Somebody ought to start a database! Or at least a wiki?!

Goals

WiFi

- **I assert that the goals of Bluetooth monitoring are different from WiFi**
- WiFi (historically)
  - Find open networks for free access
    - Find unexpected entry points to corporate networks
  - Study the distribution of WiFi security protocols like WEP, WPA, WPA2, etc

Goals

Bluetooth

- **I assert that the goals of Bluetooth monitoring are different from WiFi**
- Bluetooth (ideally)
  - Should determine whether an observed device location is *static* or *mobile* (through multiple scans over time)
  - Should understand the potential of individuals to be *tracked* via their mobile Bluetooth devices
  - Should include information necessary to know whether a Bluetooth device is running vulnerable firmware

Goals

Bluetooth

- **I assert that the goals of Bluetooth monitoring are different from WiFi**
- Bluetooth (ideally)
  - Should determine whether an observed device location is *static* or *mobile* (through multiple scans over time)
    - Should understand the potential of individuals to be *tracked* via their mobile Bluetooth devices
    - Should include information necessary to know whether a Bluetooth device is running vulnerable firmware

Goals

Bluetooth

- **I assert that the goals of Bluetooth monitoring are different from WiFi**
- Bluetooth (ideally)
  - Should determine whether an observed device location is *static* or *mobile* (through multiple scans over time)
  - Should understand the potential of individuals to be *tracked* via their mobile Bluetooth devices
    - Should include information necessary to know whether a Bluetooth device is running vulnerable firmware

Goals

Bluetooth

- **I assert that the goals of Bluetooth monitoring are different from WiFi**
- Bluetooth (ideally)
  - Should determine whether an observed device location is *static* or *mobile* (through multiple scans over time)
  - Should understand the potential of individuals to be *tracked* via their mobile Bluetooth devices
    - Should include information necessary to know whether a Bluetooth device is running vulnerable firmware

Goals

Bluetooth

- **I assert that the goals of Bluetooth monitoring are different from WiFi**
- Bluetooth (ideally)
  - Should determine whether an observed device location is *static* or *mobile* (through multiple scans over time)
  - Should understand the potential of individuals to be *tracked* via their mobile Bluetooth devices
    - Should include information necessary to know whether a Bluetooth device is running vulnerable firmware

UPCOMING WORK! STAY TUNED!

Goals

WiFi

- **WiFi scanning can adopt the Bluetooth goals too!**
- WiFi (ideally)
  - Should include information necessary to know whether a WiFi access point is running vulnerable firmware
  - Should determine whether an observed device location is *static* or *mobile* (through multiple scans over time)

Goals

WiFi

- **WiFi scanning can adopt the Bluetooth goals too!**
- WiFi (ideally)
  - Should include information necessary to know whether a WiFi access point is running vulnerable firmware https://blog.exodusintel.com/2017/07/26/broadpwn/
  - Should determine whether an observed device location is *static* or *mobile* (through multiple scans over time)

What Hardware Should I Use To Scan For BT?

What Hardware Should I Use To Scan For BT?

Table 1

Board	Antenna connector?	link	BT chip	datasheet / description link(s)	Spec supported	TX power		OTA Firmware Update	Secure Boot
Raspberry Pi 4B	no (PCB only), but you can hack one in if you're gutsy/a hare https://www.youtube.com/watch?v=MTeWm2GBwU7	https://www.raspberrypi.com/products/raspberry-pi-4-model-b/	Cypress 43455	https://www.cypress.com/file/335970/download	5.0	BR TX: +8.12 dBm BLE TX: +8.5 dBm Table 6-1: Bluetooth Transmitter RF Specifications Parameter | Conditions | Minimum | Typical | Maximum | Unit Note: The specification in this table are measured at the Bluetooth chip pin output, unless otherwise defined.			
Raspberry Pi Zero W	no (PCB only), but you can hack one in if you're gutsy/a hare https://www.raspberrypi.com/products/raspberry-pi-zero-w/ external antenna mod And FW09 here's how to change default antenna, analysis: https://www.tomshardware.com/reviews/raspberry-pi-wireless-charging-antenna-range-engineering,6014.html	https://www.raspberrypi.org/blog/raspberry-pi-zero-w-joins-family/	CYW43438	https://www.cypress.com/file/298376/download https://infocenter.nordicsemi.com/pdf/nRF52832_PS_v1.4.pdf#secure boot	4.2 (Now they claim 5 compat?)	BR TX: 8-12 dBm (depending on encoding) BR RX: -92 to -86 dBm (depending on encoding) BLE TX: 8.5 dBm BLE RX: -97 dBm		Yes	No mention
Carbon	yes	https://www.96boards.org/product/carbon/	Nordic nRF91622	no 4 (BLE) Doesn't say explicitly	https://www.nordicsemi.com/eng/Products/Low-power-short-range-wireless/nRF91622 https://infocenter.nordicsemi.com/pdf/nRF91_PS_1.1.pdf	TX: +4dBm RX: -93dBm		Yes	No mention
Orange Pi 0IE	yes	https://www.96boards.org/product/orangepi-0ie/	RDA RDA5991	BT 2.1	https://www.rda.ac.cn/soft/comercial/RDA5991H%20Datasheet_V1.0.pdf https://forum.hackaday.com/uploads/default/original/3X/0/4/04d4d4d0f4f4f4f4f4f4f4f4f4f4f4f4f4f4f4f4.pdf	TX: +20dBm RX: -90dBm "easy" it does +20dBm, but who cares if it's 2.1		No mention	No mention
Wireshare SDBT Development Bluetooth 5IoT for Raspberry Pi	yes	https://www.amazon.com/SDBT-Development-Compatible-Raspberry-Pi/dp/B07SMMWNHL	SimCom B68	https://simcom.ae/module/SIM68M-gps-protected.html https://download.mikroe.com/documents/datasheets/click_nfc_hardware_design_v1.00.pdf	Doesn't say	Doesn't say anything about dBm for Bluetooth, only GPS.		No mention	No mention
Red Bear IoT BMD-300 for Raspberry Pi	yes	https://redbear.cn/product/bmd-300/	Broadcom 43430	https://www.cypress.com/file/298876/download	4.2	4dBm	Table 6: Bluetooth Radiated RF Specifications General Parameter | Conditions | Minimum | Typical | Maximum | Unit Frequency range | | 2400 | | 2483 | MHz TX power in Bluetooth classic | | | 10 | | dBm TX power in Bluetooth | | | 10 | | dBm Power control step | | | 4 | | dB	No mention	No mention
tsy5881	yes	https://www.speedyboard.xyz/product/tsy5881-wi-fi-and-Bluetooth-soc-with-ARM-CPU-(ARM-Cortex-M0-a-DSP-core/ Out of stock everywhere. Probably not likely to be web purchasable	UniSoC UWP5661	https://github.com/unisoc-github-io/unisoc-github-io/tree/master/UWP5661	5.0	10dBm bla; 20dBm classic		No mention	No mention
nRF52840 Micro Development Kit V already has the full sized dev kit, but this one is narrowed to NFC, not BT	yes	https://www.speedyboard.xyz/product/nrf52840-Micro-Development-Kit-p-3070.html	nRF52840	https://www.nordicsemi.com/Software-and-tools/Software/nRF52840-SDK/Download?lb_docid=DITA-nRF52840-SDK_v15.0.0%2Fnrf52840%2Fdita%2Fnrf52840%2Fsoftware_setup%2Fsdk_overview.html&lang=en-GB# https://infocenter.nordicsemi.com/pdf/nRF52840_PS_v1.1.pdf	4.2	TX: +8dBm RX BLE ind: -95 dBm RX BLE long range: ~100 dBm	3.2 supports? Bottom of the page: https://www.nordicsemi.com/Software-and-tools/Development-Kits/nRF52840-DK nRF52840 SoC Bluetooth 5.2 SoC supporting Bluetooth Low Energy, Bluetooth mesh, NFC, Thread and Zigbee	No mention	yes!
CYW9SBT1DKHBY B-01 V already has link	Yes, but must move a capacitor (same thing) up the board	https://www.cypress.com/documentation/development-kitsboards/cyw9sbt1dkhbyb-01-evaluation-kit	CYW20719B1	https://www.cypress.com/file/298626/download	5.0 BR (only? not EDR?) + BLE	TX: +12 dBm RX BLE: -94.5 dBm		No mention	No mention
CYW9SBT1DKHBY B-01 Evaluation Kit (purchased 1x)	Yes, but must move a capacitor https://community.cypress.com/message/36324#36324	https://www.cypress.com/documentation/development-kitsboards/cyw9sbt1dkhbyb-01-evaluation-kit	CY8D14B2B-S2 CY8D14B2B-S3 CY8D14B2B-S4 CY8D2719	https://www.cypress.com/file/278751/download	5.0 SR, EDR, BLE	TX BR: +20 dBm TX BLE: +20 dBm RX BLE: -95 dBm	OTA Update	No mention	No mention
Beaglebone Green Wireless	yes	https://www.seeedstudio.com/product/1653-Blue---BT-p-2455.html https://www.seeedstudio.com/Beaglebone-Green-Wireless-Base-Kit-p-2504.html Blue - $70 https://www.seeedstudio.com/Beaglebone-Blue---BT-p-2455.html https://www.seeedstudio.com/Beaglebone-Green-Wireless-Base-Kit-p-2504.html black - $60 https://www.ezone.com/product/Beaglebone-Black-BT/	R-WL1866 (Combo)	https://github.com/Murata-Wireless/Documentation/blob/master/Datasheets/Bluetooth/Bluetooth_Module_Wireless_SCI.pdf https://www.ti.com/lit/ds/symlink/wl1866mod.pdf http://www.ti.com/lit/ds/symlink/wl1835mod.pdf	4.2	7 dBm BLE, 7.2dBm EDR, 11.7 BR			
Parallel Corporation EV Board Development board	yes	https://www.ezone.com/product/Parallel-Corporation-EV-Board-Development-Board-p-4435?cs=en_US&sc=shopping&kpid=4435&gclid=EAIaIQobChMIqfLzKeuO4AIVkJ7ICh2_DwEEAQYASABEgKNZfD_BwE $49	nRF52832	https://static.squarespace.com/static/5b1c5062e2ccd1b2cb4ab6c8/t/5b1c5b2ce2ccd1b2cb4b0b97/1528299820000/nRF52832_PS_v1.1.pdf https://www.nordicsemi.com/eng/content/download/2726/34743/file/nRF52832_Errata_v1.0.pdf	4.2; nRF = 4dB, but this module is claimed as 20dBm, and is apparently +-18.75dBm according to the FCC tests (https://fccid.io/2ABWB7302SB/) Is that a power amplifier under the shield? https://fccid.io/2ABWB-BT302/Internal-Photos/Internal-Photos-3484127 Seems to be a SKY66112-11 based on the logo and guessing the writing: https://store.skyworksinc.com/products/sky66112-11-qfn-skyfive-lga-5?t=66&l=https://www.skyworksinc.com/-/media/SkyWorks/Documents/Products/3201-3300/SKY66112_11_20202004.pdf			https://www.amzn.com/gp/product/e/b/B0DwTpmdst-corporation?ie=UTF8&ASIN=B0DwTpmdst&linkCode=ll1&tag=&linkId=&ref_=as_li_ss_tl	$49 before shipping
Arduino BT	no	https://store.arduino.cc/usa/nano-ble-sense	Bluetooth 5	https://www.u-blox.com/sites/default/files/NINA-B1_DataSheet_UBX-19017337_C1-Public.pdf	BT 2.1 + EDR	11dBm / -96dBm			
nRF52 DP Wireless Battery Nano Node Board (purchased 1x)	Yes, but must move a capacitor (same thing) up the board (I bought it)	https://www.seeedstudio.com/product/development-tools/development-tools/wireless/nrf52dp-nrf52-development-board-wireless-battery-nano-node-p-4106.html	TLSR8410B4 QFN32MQ1						
SVK-ANNA-B112 Evaluation kits for ANNA-B112 Bluetooth 5 module with Bluetooth 5 low energy and NFC	yes	https://www.u-blox.com/en/product/anna-b112#tab-documentation-resources https://www.u-blox.com/sites/default/files/ANNA-B112_UserGuide_UBX-18018358_C1-Public.pdf	u-Blox ANNA-B112	https://www.u-blox.com/sites/default/files/ANNA-B112_DataSheet_UBX-18012337_C1-Public.pdf	BT 5 BLE, v Mesh (no classic?)	Typical +4 dBM, max w/ Antenna +3 dBm			

What Hardware Should I Use To Scan For BT?

They call me the king of the spreadsheets,
Got 'em all printed out on my bedsheets
- Weird Al, "*It's All About the Pentiums*"

Table 1

Board	Antenna connector?	link	BT chip	datasheet / description link(s)	Spec supported	TX power		OTA Firmware Update	Secure Boot
Raspberry Pi 4B	no (PCB only), but you can hack one in with a little guidance here: https://www.youtube.com/watch?v=MTeWm2GBwA7I	https://www.raspberrypi.com/products/raspberry-pi-4-model-b/	Cypress 43455	https://www.cypress.com/file/335970/download	5.0	BR TX: -6-12 dBm BLE TX: +8.5 dBm Table 1 Bluetooth Transmitter RF Specifications			
Raspberry Pi Zero W	no (PCB only), but you can hack one in with an external antenna if you're willing to do it this way: raspunzel.com/2018/04/04/how-to-add-an-external-antenna-to-your-raspberry-pi-zero-w-external-antenna-mod/ And FWIW here's the schematic for the default antenna, in analysis: https://learn.sparkfun.com/tutorials/hookup-guide-for-the-sparkfun-wireless-combo-dev-board---esp32-(qca6174)/hardware-overview-the-raspberry-pi	https://raspberrypi.stackexchange.com/questions/41776/what-is-the-default-antenna-of-the-pi-zero-w	CYW43438	https://www.cypress.com/file/298376/download https://infocenter.nordicsemi.com/pdf/nRF52832_PS_v1.4.pdf?cp=4_0_0_5_1#pdfjs.action=download	4.2 (Now they claim it's compat?)	BR TX: 8-12 dBm (depending on encoding) EDR EQ: -92 to -96 dBm (depending on encoding) BLE TX: 8.5 dBm BLE RX: -97 dBm		Yes	No mention
Carbon	yes	https://www.96boards.org/product/carbon/	Nordic nRF91622	https://www.nordicsemi.com/Products/Low-power-short-range-wireless/nRF9160 https://infocenter.nordicsemi.com/pdf/nRF9160_PS_v1.3.1.pdf	no # (BLE) Doesn't say explicitly	TX: +4dBm RX: -93dBm		Yes	No mention
Orange Pi 0S	yes	https://www.96boards.org/product/orangepi-0lts/	RDA RDA5991	https://www.aliexpress.com/item/4000482129782.html?spm=a2g0o.productlist.0.0.4ca6f2cbmeHqqb&algo_pvid=f6f9a7fa-f413-4e8c-92e0-1d6c7c1e6b7c&algo_exp_id=f6f9a7fa-f413-4e8c-92e0-1d6c7c1e6b7c-0&pdp_ext_f=%7B%22sku_id%22%3A%2212000034111855834%22%7D https://linkstechnology.com/wp-content/uploads/2019/12/RDA5991-Datasheet-V1.0.pdf	BT 2.1	TX: +20dBm RX: -90dBm "easy" it does +20dBm, but who cares if it's 2.1		No mention	No mention
Wireshare SDR+ Bluetooth 5 BLE Bluetooth HAT for Raspberry Pi	yes	https://www.crowdsupply.com/sdr-plus/sdr-compatible-bluetooth-hats	BlmCom B68	https://simcom.ae/module/sim68x-sim7x-series/B68	Doesn't say	Doesn't say anything about dBm for Bluetooth, only GPS.		no mention	no mention
Red Bear IoT RapidPi for Raspberry Pi	yes	https://redbear.cn/product/rapidpi/	Broadcom 43430	https://www.cypress.com/file/298376/download	4.2	8dBm	Table 24: Bluetooth Radiated RF Specifications*	no mention	no mention
hci0801	yes	https://www.speedyboy.co.za/shop/pi-zero-w-2-and-Bluetooth-v2/?gclid=EAIaIQobChMIsfqLuJ6R6wIVBrLrBR1HMwEAQYASABEgIJ-fD_BwE CPU: ARM Cortex-M0+ processor 200 MHz **Out of stock everywhere. Probably not likely to be web scraped.**	UniSoC UWP5661	https://github.com/yellows-github-io/yellows-github-io.github.io/raw/master/UWP5661/	5.0	10dBm bla, 20dBm classic		no mention	no mention
nRF52840 Micro Development Kit **V already has the full sized dev kit, but this one is also connected to NFC, not BT**	yes	https://www.speedyboy.co.za/shop/nRF52840-Micro-Development-Kit-p-3079.html	nRF52840	https://www.nordicsemi.com/Products/Low-power-short-range-wireless/nRF52840/Download#infotabs https://infocenter.nordicsemi.com/pdf/nRF52840_PS_v1.1.pdf	4.2	TX: +8dBm RX BLE sns: -95 dBm RX BLE long range: -100 dBm	3.2 supprot ? Bottom of the page: https://www.nordicsemi.com/Software-and-tools/Development-Kits/nRF52840-DK	no mention	yes!
CYW920719Q40EVB-01 **V already has this**	Yes, but must move a capacitor (same thing) up the board	https://www.cypress.com/documentation/development-kitsboards/cyw920719q40evb-01-evaluation-kit	CY4037/20581	https://www.cypress.com/file/298626/download	5.0 BR (only? not EDR?) + BLE	TX: +12 dBm RX BLE: -94.5 dBm		no mention	no mention
CYW920719Q40EVB-01 Evaluation Kit (purchased 1x)	Yes, but must move a capacitor https://community.cypress.com/message/36324#36324	https://www.cypress.com/documentation/development-kitsboards/cyw920719q40evb-01-evaluation-kit	CY4037-40939-00 CY4037-40939-02 CY4037-40940-02 CY920719	https://www.cypress.com/file/278311/download	5.0 SIG: EDR, BLE	TX BR: +20 dBm TX BLE: +20 dBm RX BLE: -95 dBm	OTA Update	no mention	no mention
Seeedstone Mesh Bluetooth Wireless	yes	https://www.seeedstudio.com/product/1653-Blue---BW-p-4134.html https://www.seeedstudio.com/Seeedstone-Mesh-Bluetooth-Wireless-Blue---BW-p-4135.html https://www.seeedstudio.com/Seeedstone-Mesh-Bluetooth-Wireless-Black---BW-p-4136.html https://www.seeedstudio.com/product/detail/1653.html	TI WL1835 (Combo)	https://github.com/SeeedDocument/Seeedstone-Mesh-Wireless/blob/master/Seeedstone_Mesh_Wireless_SCH.pdf https://www.ti.com/lit/ds/symlink/wl1835mod.pdf http://www.ti.com/lit/ds/symlink/wl1835mod.pdf	4.2	7 dBm BLE, 7.2dBm EDR, 11.7 BR			
Parallel Corporation EV nRF52832 Development board	yes	https://www.arrow.com/en/products/nrf52832-qiaa-r/parallel-corporation https://www.digikey.com/product-detail/en/parallel-corporation/nRF52832-QIAA-R/1965-1000-ND/9841356?utm_adgroup=Development%20Boards%2C%20Kits%2C%20Programmers&utm_source=google&utm_medium=cpc&utm_campaign=Shopping_Development%20Boards%2C%20Kits%2C%20Programmers_1_Manufacturer&utm_term=&utm_content=Development%20Boards%2C%20Kits%2C%20Programmers&gclid=EAIaIQobChMIsfqLuJ6R6wIVBrLrBR1HMwEAQYASABEgIJ-fD_BwE $46	nRF52832	https://static.squarespace.com/static/5b1c09a2e4966b540b425138/t/5d4f2c0c0e5e2a0001a0e1ac/1565964044970/nRF52832_Product_Brief_v1.0.pdf https://www.nordicsemi.com/eng/nordic/download_resource/58853/14/77772749/nRF52832_PS_v1.4.pdf	8.2 +PF = NB, but this module is claimed as 20dBm, and is apparently +-18.75dBm according to the FCC tests (https://fccid.io/2BBRBT832QB/) Is that a power amplifier under the shield? https://fccid.io/2BBRBT832QB/Block-Diagram Seems to be a SKY66112-11 based on the logo and guessing the writing: https://store.skyworksinc.com/products/sky66112-11-qfn-package-sip-dcdcmo-rev3-73668/ https://www.skyworksinc.com/-/media/SkyWorks/Documents/Products/3201-3300/SKY66112_11_20202044.pdf		https://www.arrow.com/en/products/nrf52832qiaar/parallel-corporation?gclid=EAIaIQobChMIsfqLuJ6R6wIVBrLrBR1HMwEAQYASABEgIJ-fD_BwE $46 before shipping	
Arduino BT	no	https://store.arduino.cc/usa/tiny-arduinobasebt	Bluetjpe WT11	https://www.sparkfun.com/datasheets/Sparkfun/data-sheets/BT/rn-41andother.pdf	BT 2.1 + EDR	13dBm / -86dBm			
nRF52TP Wireless Bluetooth Low Energy Radio Board (purchased 1x)	Yes, but must move a capacitor (same thing I didn't count/or until after I bought it)	https://www.seeedstudio.com/product/development-tools/development-tools.html?spm=a2g0o.detail.1116.1.3a1c1f4aBr-documentation-resources https://www.seeedstudio.com/wiki/index.php?title=Seeedstone_Mesh_Wireless_Module_SKU:_103030118_UserGuide_1–_18218.jpg_C1-Public.pdf	TLSR8410BA QFN32MQ1						
SVK-ANNA-B112 Evaluation kits for ANNA-B112 Bluetooth low energy module with Bluetooth 5 low energy and NFC	yes	https://www.u-blox.com/en/product/anna-b112#tab-documentation-resources https://www.u-blox.com/sites/default/files/SVK-ANNA-B112_UserGuide_UBX-18018358_C1-Public.pdf	u-Blox ANNA-B112	https://www.u-blox.com/sites/default/files/ANNA-B112_DataSheet_UBX-18011707_C1-Public.pdf	BT 5 BLE + Mesh (no classic?)	Typical +4 dBM, max w/ Antenna +5 dBm			

Board	Antenna connector?	link	BT chip	datasheet / description link(s)	Spec supported	TX power
Raspberry Pi 4B	no (PCB only), but you can hack one on using the guidance here: https://www.youtube.com/watch?v=MTwWnZG8wUY	https://www.raspberrypi.org/products/raspberry-pi-4-model-b/	Cypress 43455	https://www.cypress.com/file/358916/download	5.0	BR TX: +8-12 dBm BLE TX: +8.5 dBm **Table 30. Bluetooth Transmitter RF Specifications** **Note:** The specifications in this table are measured at the Bluetooth chip port output, unless otherwise defined. **General** Frequency range – 2402 – 2480 MHz Basic rate (GFSK) TX power at Bluetooth – – 12 – dBm QPSK TX Power at Bluetooth – – 8 – dBm 8PSK TX Power at Bluetooth – – 8 – dBm Power control step – 2 4 8 dB
Raspberry Pi Zero W	no (PCB only), but technically you could attach an external antenna if you can change a tiny-ass capacitor location: https://www.briandorey.com/post/raspberry-pi-zero-w-external-antenna-mod And FWIW here's an interesting default antenna analysis: https://www.embeddedcomputing.com/technology/analog-and-power/power-semiconductors-wireless-charging/a-lesson-in-wireless-engineering-from-the-raspberry-pi	https://www.raspberrypi.org/blog/raspberry-pi-zero-w-joins-family/	CYW43438	https://www.cypress.com/file/298076/download	4.2 (Now they claim 5.1 compat?)	BR TX: 8-12 dBm (depending on encoding) BR RX: -90 to -96 dBm (depending on encoding) BLE TX: 8.5 dBm BLE RX: -97 dBm

Board	Antenna connector?	link	BT chip	datasheet / description link(s)	Spec supported	TX power
Raspberry Pi 4B	no (PCB only), but you can hack one on using the guidance here: https://www.youtube.com/watch?v=MTwWnZG8wUY	https://www.raspberrypi.org/products/raspberry-pi-4-model-b/	Cypress 43455	https://www.cypress.com/file/358916/download	5.0	BR TX: +8-12 dBm BLE TX: +8.5 dBm **Table 30. Bluetooth Transmitter RF Specifications** **Parameter** / **Conditions** / **Minimum** / **Typical** / **Maximum** / **Unit** **Note:** The specifications in this table are measured at the Bluetooth chip port output, unless otherwise defined. **General** Frequency range – 2402 – 2480 MHz Basic rate (GFSK) TX power at Bluetooth – – 12 – dBm QPSK TX Power at Bluetooth – – 8 – dBm 8PSK TX Power at Bluetooth – – 8 – dBm Power control step – 2 4 8 dB
Raspberry Pi Zero W	no (PCB only), but technically you could attach an external antenna if you can change a tiny-ass capacitor location: https://www.briandorey.com/post/raspberry-pi-zero-w-external-antenna-mod And FWIW here's an interesting default antenna analysis: https://www.embeddedcomputing.com/technology/analog-and-power/power-semiconductors-wireless-charging/a-lesson-in-wireless-engineering-from-the-raspberry-pi	https://www.raspberrypi.org/blog/raspberry-pi-zero-w-joins-family/	CYW43438	https://www.cypress.com/file/298076/download	4.2 (Now they claim 5.1 compat?)	BR TX: 8-12 dBm (depending on encoding) BR RX: -90 to -96 dBm (depending on encoding) BLE TX: 8.5 dBm BLE RX: -97 dBm

A "Class 1" device has a maximum power of 20 dBm (decibel-milliwatts) (100 mW) ~= 100 Meters

A "Class 2" device has a maximum power of 4 dBm (2.5 mW) ~= 10 Meters

A "Class 3" device has a maximum power of 0 dBm (1 mW) ~= 1 Meter

Board	Antenna connector?	link	BT chip	datasheet / description link(s)	Spec supported	TX power
Raspberry Pi 4B	no (PCB only), but you can hack one on using the guidance here: https://www.youtube.com/watch?v=MTwWnZG8wUY	https://www.raspberrypi.org/products/raspberry-pi-4-model-b/	Cypress 43455	https://www.cypress.com/file/358916/download	5.0	BR TX: +8-12 dBm BLE TX: +8.5 dBm **Table 30. Bluetooth Transmitter RF Specifications** Parameter / Conditions / Minimum / Typica **Note:** The specifications in this table are measured at the Bluetooth chip port output, unless otherwise **General** Frequency range – 2402 – Basic rate (GFSK) TX power at Bluetooth – – 12 QPSK TX Power at Bluetooth – – 8 8PSK TX Power at Bluetooth – – 8 Power control step – 2 4
Raspberry Pi Zero W	no (PCB only), but technically you could attach an external antenna if you can change a tiny-ass capacitor location: https://www.briandorey.com/post/raspberry-pi-zero-w-external-antenna-mod And FWIW here's an interesting default antenna analysis: https://www.embeddedcomputing.com/technology/analog-and-power/power-semiconductors-wireless-charging/a-lesson-in-wireless-engineering-from-the-raspberry-pi	https://www.raspberrypi.org/blog/raspberry-pi-zero-w-joins-family/	CYW43438	https://www.cypress.com/file/298076/download	4.2 (Now they claim 5.1 compat?)	BR TX: 8-12 dBm (depending on encoding) BR RX: -90 to -96 dBm (depending on encoding) BLE TX: 8.5 dBm BLE RX: -97 dBm
BeagleBone black/blue Wireless	yes	https://www.sparkfun.com/products/14920 Blue - $95 https://www.arrow.com/en/products/bbblue/beagleboardorg Blue - $75 https://www.sparkfun.com/products/14162 black - $90 https://	TI WL1385 (Combo)	https://github.com/beagleboard/beaglebone-black-wireless/blob/master/BeagleBone_Black_Wireless_SCH.pdf http://www.ti.com/product/WL1835MOD http://www.ti.com/lit/ds/symlink/wl1835mod.pdf	4.2	7 dBm BLE, 7.2dBm EDR, 11.7 BR

Board	Antenna connector?	link	BT chip	datasheet / description link(s)	Spec supported	TX power
Raspberry Pi 4B	no (PCB only), but you can hack one on using the guidance here: https://www.youtube.com/watch?v=MTwWnZG8wUY	https://www.raspberrypi.org/products/raspberry-pi-4-model-b/	Cypress 43455	https://www.cypress.com/file/358916/download	5.0	BR TX: +8-12 dBm BLE TX: +8.5 dBm **Table 30. Bluetooth Transmitter RF Specifications** Parameter / Conditions / Minimum / Typica **Note:** The specifications in this table are measured at the Bluetooth chip port output, unless otherwise **General** Frequency range – 2402 – – Basic rate (GFSK) TX power at Bluetooth – – 12 QPSK TX Power at Bluetooth – – 8 8PSK TX Power at Bluetooth – – 8 Power control step – 2 4
Raspberry Pi Zero W	no (PCB only), but technically you could attach an external antenna if you can change a tiny-ass capacitor location: https://www.briandorey.com/post/raspberry-pi-zero-w-external-antenna-mod And FWIW here's an interesting default antenna analysis: https://www.embeddedcomputing.com/technology/analog-and-power/power-semiconductors-wireless-charging/a-lesson-in-wireless-engineering-from-the-raspberry-pi	https://www.raspberrypi.org/blog/raspberry-pi-zero-w-joins-family/	CYW43438	https://www.cypress.com/file/298076/download	4.2 (Now they claim 5.1 compat?)	BR TX: 8-12 dBm (depending on encoding) BR RX: -90 to -96 dBm (depending on encoding) BLE TX: 8.5 dBm BLE RX: -97 dBm
BeagleBone black/blue Wireless	yes	https://www.sparkfun.com/products/14920 Blue - $95 https://www.arrow.com/en/products/bbblue/beagleboardorg Blue - $75 https://www.sparkfun.com/products/14162 black - $90 https://	TI WL1385 (Combo)	https://github.com/beagleboard/beaglebone-black-wireless/blob/master/BeagleBone_Black_Wireless_SCH.pdf http://www.ti.com/product/WL1835MOD http://www.ti.com/lit/ds/symlink/wl1835mod.pdf	4.2	7 dBm BLE, 7.2dBm EDR, 11.7 BR

Board	Antenna connector?	link	BT chip	datasheet / description link(s)	Spec supported	TX power
Raspberry Pi 4B	no (PCB only), but you can hack one on using the guidance here: https://www.youtube.com/watch?v=MTwWnZG8wUY	https://www.raspberrypi.org/products/raspberry-pi-4-model-b/	Cypress 43455	https://www.cypress.com/file/358916/download	5.0	BR TX: +8-12 dBm BLE TX: +8.5 dBm **Table 30. Bluetooth Transmitter RF Specifications** **Parameter** / **Conditions** / **Minimum** / **Typica** **Note:** The specifications in this table are measured at the Bluetooth chip port output, unless otherwise **General** Frequency range – 2402 – Basic rate (GFSK) TX power at Bluetooth – – 12 QPSK TX Power at Bluetooth – – 8 8PSK TX Power at Bluetooth – – 8 Power control step – 2 4
Raspberry Pi Zero W	no (PCB only), but technically you could attach an external antenna if you can change a tiny-ass capacitor location: https://www.briandorey.com/post/raspberry-pi-zero-w-external-antenna-mod And FWIW here's an interesting default antenna analysis: https://www.embeddedcomputing.com/technology/analog-and-power/power-semiconductors-wireless-charging/a-lesson-in-wireless-engineering-from-the-raspberry-pi	https://www.raspberrypi.org/blog/raspberry-pi-zero-w-joins-family/	CYW43438	https://www.cypress.com/file/298076/download	4.2 (Now they claim 5.1 compat?)	BR TX: 8-12 dBm (depending on encoding) BR RX: -90 to -96 dBm (depending on encoding) BLE TX: 8.5 dBm BLE RX: -97 dBm
BeagleBone black/blue Wireless	yes	https://www.sparkfun.com/products/14920 Blue - $95 https://www.arrow.com/en/products/bbblue/beagleboardorg Blue - $75 https://www.sparkfun.com/products/14162 black - $90 https://	TI WL1385 (Combo)	https://github.com/beagleboard/beaglebone-black-wireless/blob/master/BeagleBone_Black_Wireless_SCH.pdf http://www.ti.com/product/WL1835MOD http://www.ti.com/lit/ds/symlink/wl1835mod.pdf	4.2	7 dBm BLE, 7.2dBm EDR, 11.7 BR

Hardware

By price & capability

Hardware

By price & capability

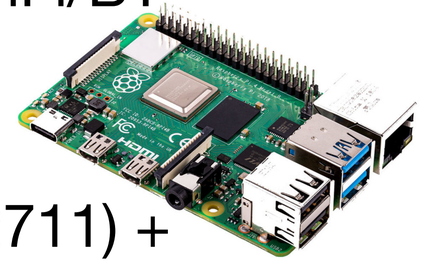
- Raspberry Pi Zero W (v1) - $15

  - .5GB RAM, 1GHz single-core ARMv6 CPU (BCM2835) + BCM43143 WiFi/BT

Hardware

By price & capability

- Raspberry Pi Zero W (v1) - $15
  - .5GB RAM, 1GHz single-core ARMv6 CPU (BCM2835) + BCM43143 WiFi/BT

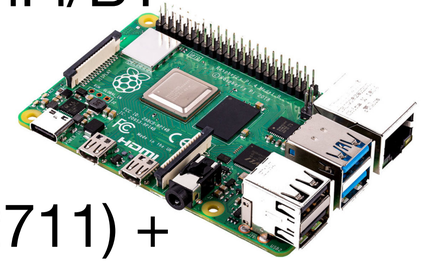


- Raspberry Pi 4 Model B - $35/$45/$55
  - 1/2/4GB RAM, 1.5GHz 64-bit quad-core ARM Cortex-A72 CPU (BCM2711) + CYW 43455 BT/WiFi

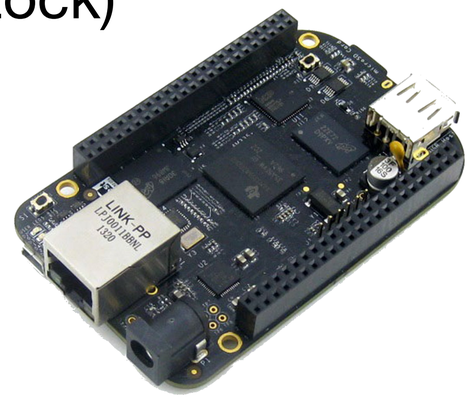
Hardware

By price & capability

- Raspberry Pi Zero W (v1) - $15
  - .5GB RAM, 1GHz single-core ARMv6 CPU (BCM2835) + BCM43143 WiFi/BT



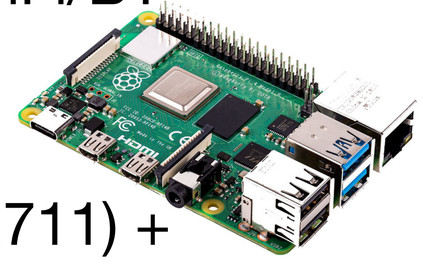
- Raspberry Pi 4 Model B - $35/$45/$55
  - 1/2/4GB RAM, 1.5GHz 64-bit quad-core ARM Cortex-A72 CPU (BCM2711) + CYW 43455 BT/WiFi
- BeagleBone Black Wireless - $72 (when I got it. Now $111 but out of stock)
  - .5GB RAM, 1GHz ARM Cortex-A8 + TI WL1385
  - **Antenna connector!**



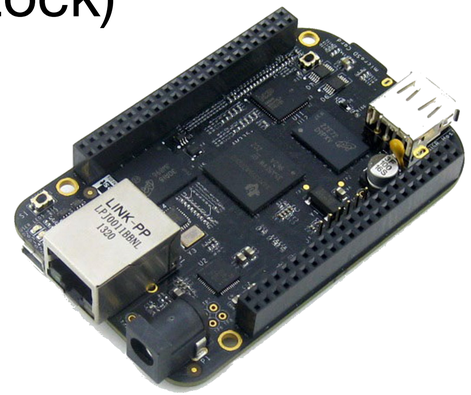
Hardware

By price & capability

- Raspberry Pi Zero W (v1) - $15
  - .5GB RAM, 1GHz single-core ARMv6 CPU (BCM2835) + BCM43143 WiFi/BT



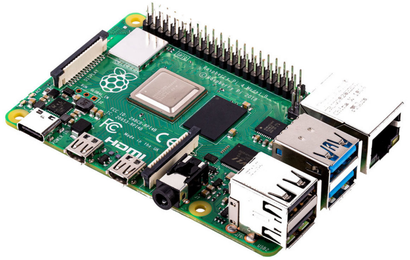
- Raspberry Pi 4 Model B - $35/$45/$55
  - 1/2/4GB RAM, 1.5GHz 64-bit quad-core ARM Cortex-A72 CPU (BCM2711) + CYW 43455 BT/WiFi
- BeagleBone Black Wireless - $72 (when I got it. Now $111 but out of stock)
  - .5GB RAM, 1GHz ARM Cortex-A8 + TI WL1385
  - **Antenna connector!**



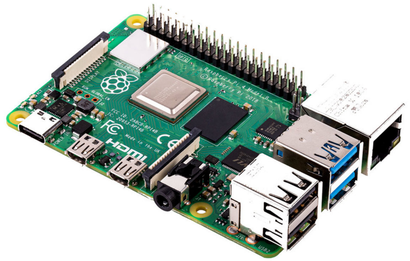
Hardware

What collects more?

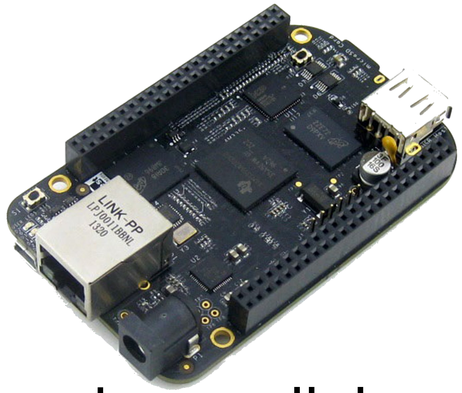
vs.



- Test 1: Pi Zero & Pi 4b in parallel
  - Pi0 = **113**, Pi4b = 65 *named devices*



vs.

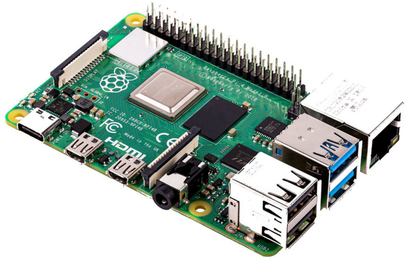


- Test 2: Pi 4b & Beagle Bone Black Wireless in parallel
  - Pi4b == BBBW == 422 *named devices*

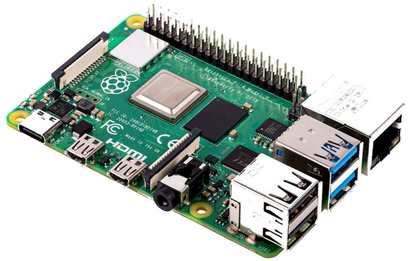
Hardware

What collects

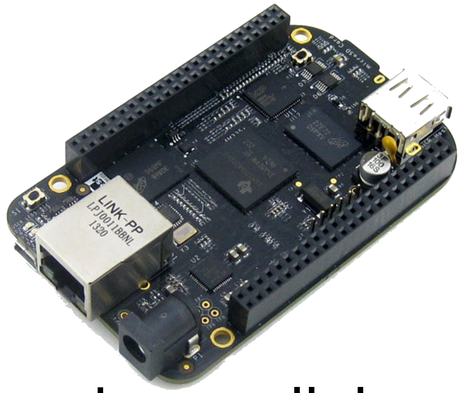
vs.



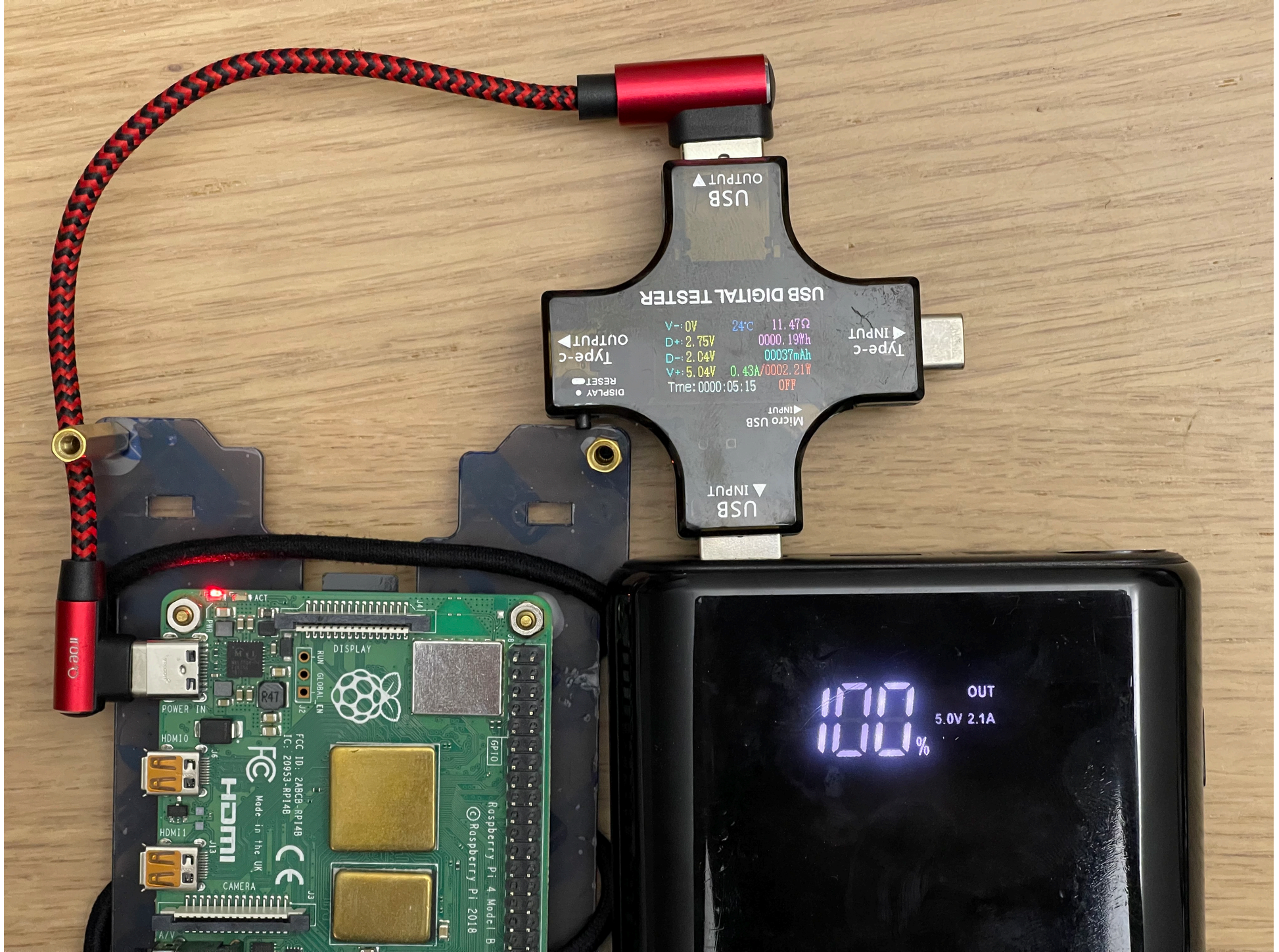
- Test 1: Pi Zero & Pi 4b in parallel
  - Pi0 = **113**, Pi4b = 65 *named devices*



vs.



- Test 2: Pi 4b & Beagle Bone Black Wireless in parallel
  - Pi4b == BBBW == 422 *named devices*


USB DIGITAL TESTER
V-:0V 24°C 11.47Ω
D+:2.75V 0000.19Wh
D-:2.04V 00037mAh
V+:5.04V 0.43A/0002.21W
Tme:0000:05:15 OFF
USB OUTPUT
USB INPUT
Type-c OUTPUT
Type-c INPUT
Micro USB INPUT
DISPLAY
RESET
100 %
OUT
5.0V 2.1A
POWER IN
HDMI0
HDMI1
CAMERA
DISPLAY
GPIO
Raspberry Pi 4 Model B
©Raspberry Pi 2018

USB DIGITAL TESTER

V-: 0V 24°C 12.00Ω
D+: 2.75V 0000.22Wh
D-: 2.04V 00045mAh
V+: 5.04V 0.42A 0002.11W
Time: 0000:06:16 OFF

Type-C OUTPUT

DISPLAY
RESET

Type-C INPUT

Micro USB INPUT

USB DIGITAL TESTER
V-:0V 20°C 07.63Ω
D+:2.71V 0047.69Wh
D-:2.01V 09445mAh
V+:4.91V 0.65A/0003.19W
Tme:0021:51:16 OFF
Type-c OUTPUT
Type-c INPUT
Micro USB INPUT
USB OUTPUT
USB INPUT
OUT
5.0V 2.1A

USB DIGITAL TESTER

V-: 0V
D+: 2.71V
D-: 2.01V
V+: 4.91V
Time: 0021:51:16

20°C
0.65A

07.63Ω
0047.69Wh
09445mAh
0003.19W
OFF

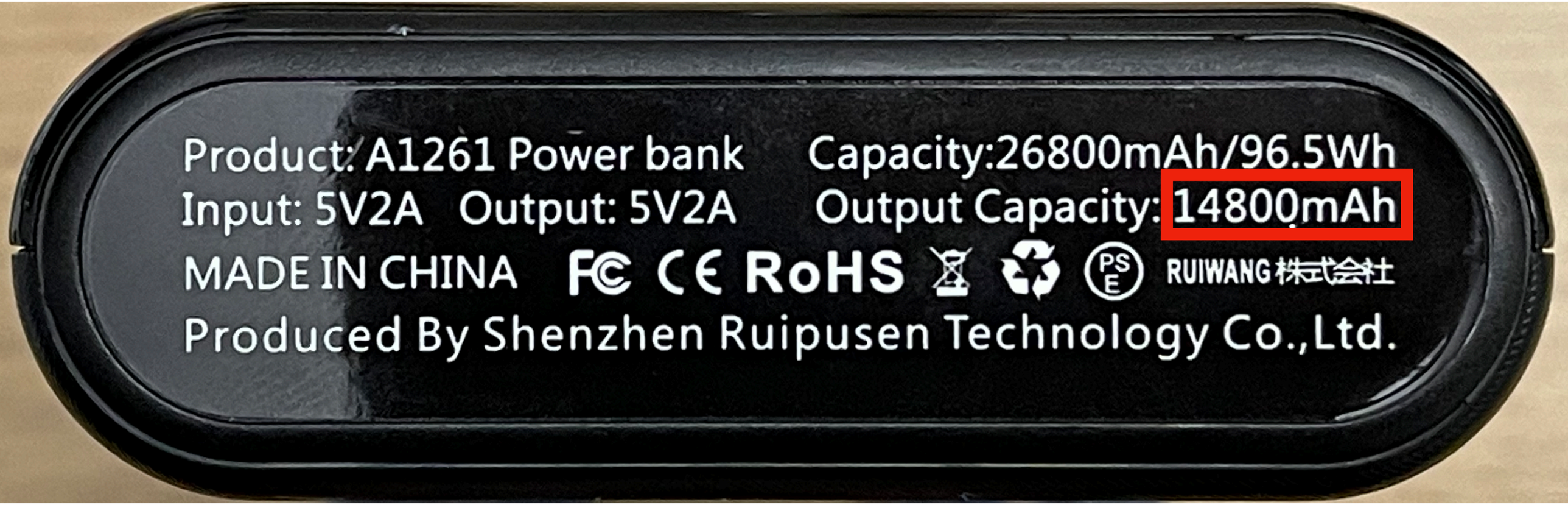
Type-c
OUTPUT

Type-c
INPUT

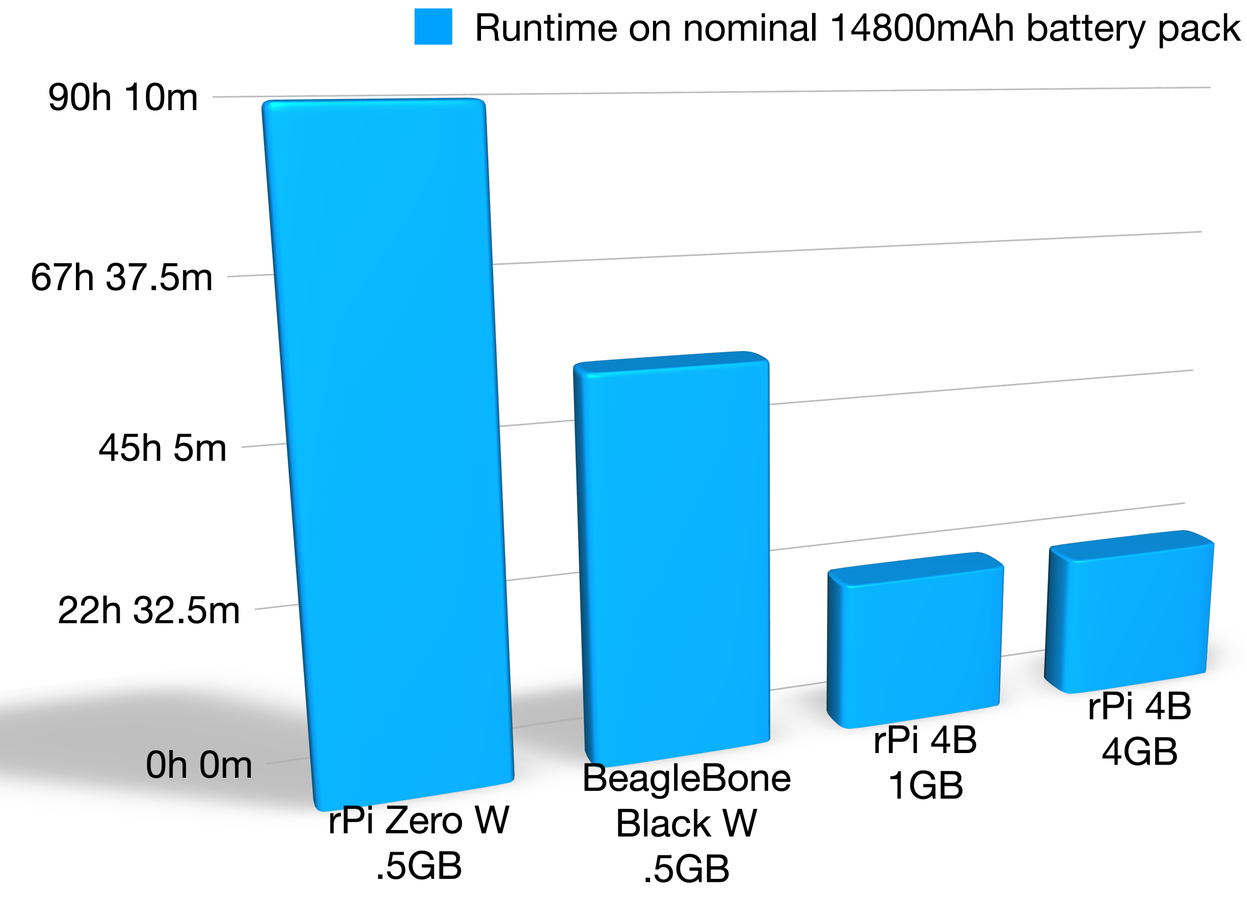
DISPLAY
RESET

Micro USB
INPUT

Battery currently down to
63.8% of rated capacity :-/

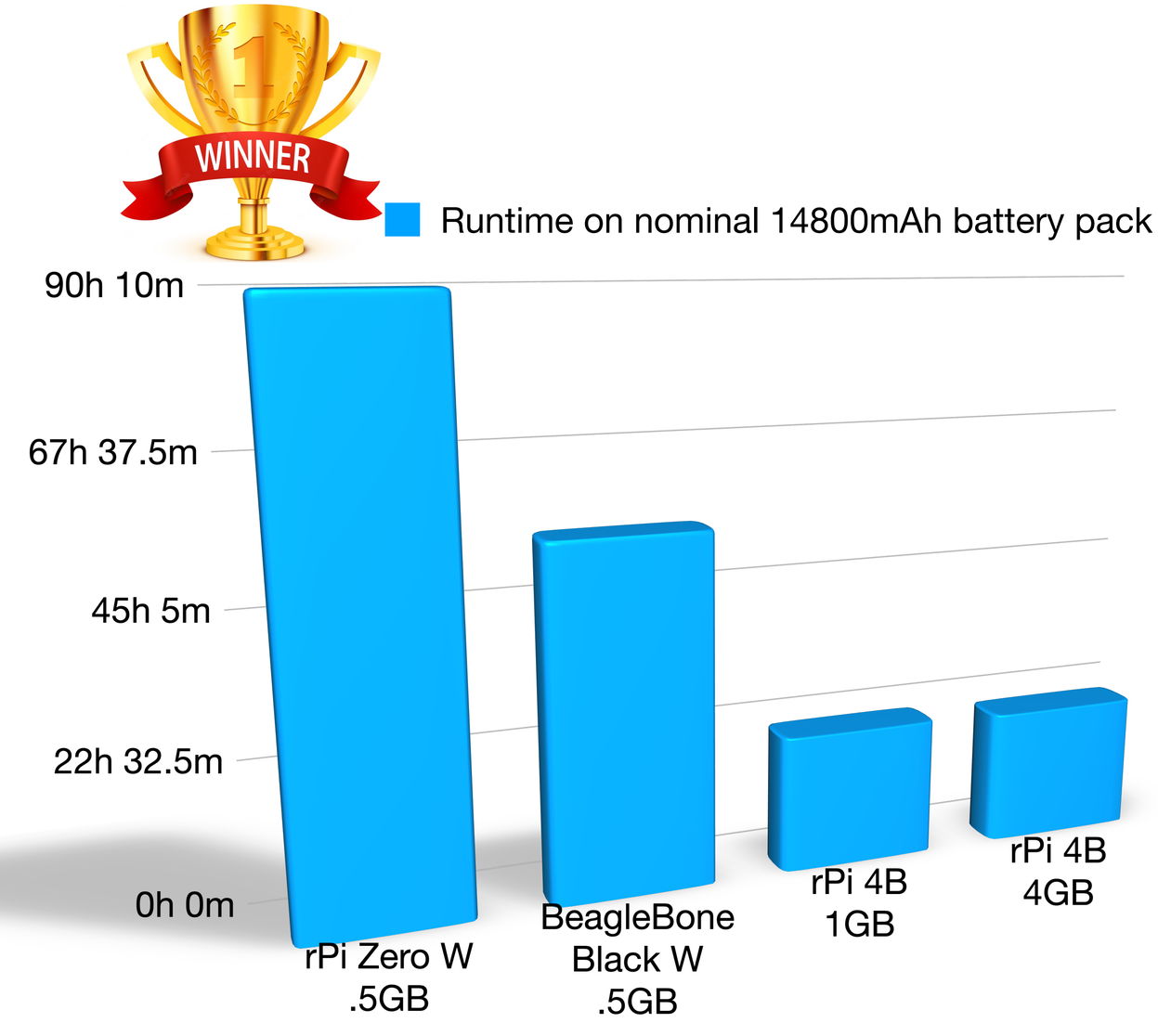


Run-time on Battery



Model	Runtime	RAM
rPi Zero W .5GB	90h 2m	.5 GB
BeagleBone Black W .5GB	55h 16m	.5GB
rPi 4B 1GB	21h 51m	1GB
rPi 4B 4GB	21h 21m	4GB

Run-time on Battery



Model	Runtime	RAM
rPi Zero W .5GB	90h 2m	.5 GB
BeagleBone Black W .5GB	55h 16m	.5GB
rPi 4B 1GB	21h 51m	1GB
rPi 4B 4GB	21h 21m	4GB

Software Setup

"Xeno be not proud" *OR* "Look on my works, ye Mighty, and despair!"
OR "Naïveté, thy name be Xeno" OR "I am dumb, and you can too!"

https://github.com/darkmentorllc/naiveBTsniffing

Software Setup

"Xeno be not proud" *OR* "Look on my works, ye Mighty, and despair!"
OR "Naïveté, thy name be Xeno" OR "I am dumb, and you can too!"

- v.0001 - Bash scripts around Linux CLI tools!

https://github.com/darkmentorllc/naiveBTsniffing

Software Setup

"Xeno be not proud" *OR* "Look on my works, ye Mighty, and despair!"
OR "Naïveté, thy name be Xeno" OR "I am dumb, and you can too!"

- v.0001 - Bash scripts around Linux CLI tools!
  - 99% of my data - Python scripts to analyze!

https://github.com/darkmentorllc/naiveBTsniffing

Software Setup

"Xeno be not proud" *OR* "Look on my works, ye Mighty, and despair!"
OR "Naïveté, thy name be Xeno" OR "I am dumb, and you can too!"

- v.0001 - Bash scripts around Linux CLI tools!
  - 99% of my data - Python scripts to analyze!
- v.001 - C-based BlueZ DBus-based API + MySQL DB
  - Only made this around Feb 2023, captures incomplete data compared to bash scripts! I basically don't even use this anymore, so I didn't release it.

https://github.com/darkmentorllc/naiveBTsniffing

Background - *BT Device Address (BDADDR)*

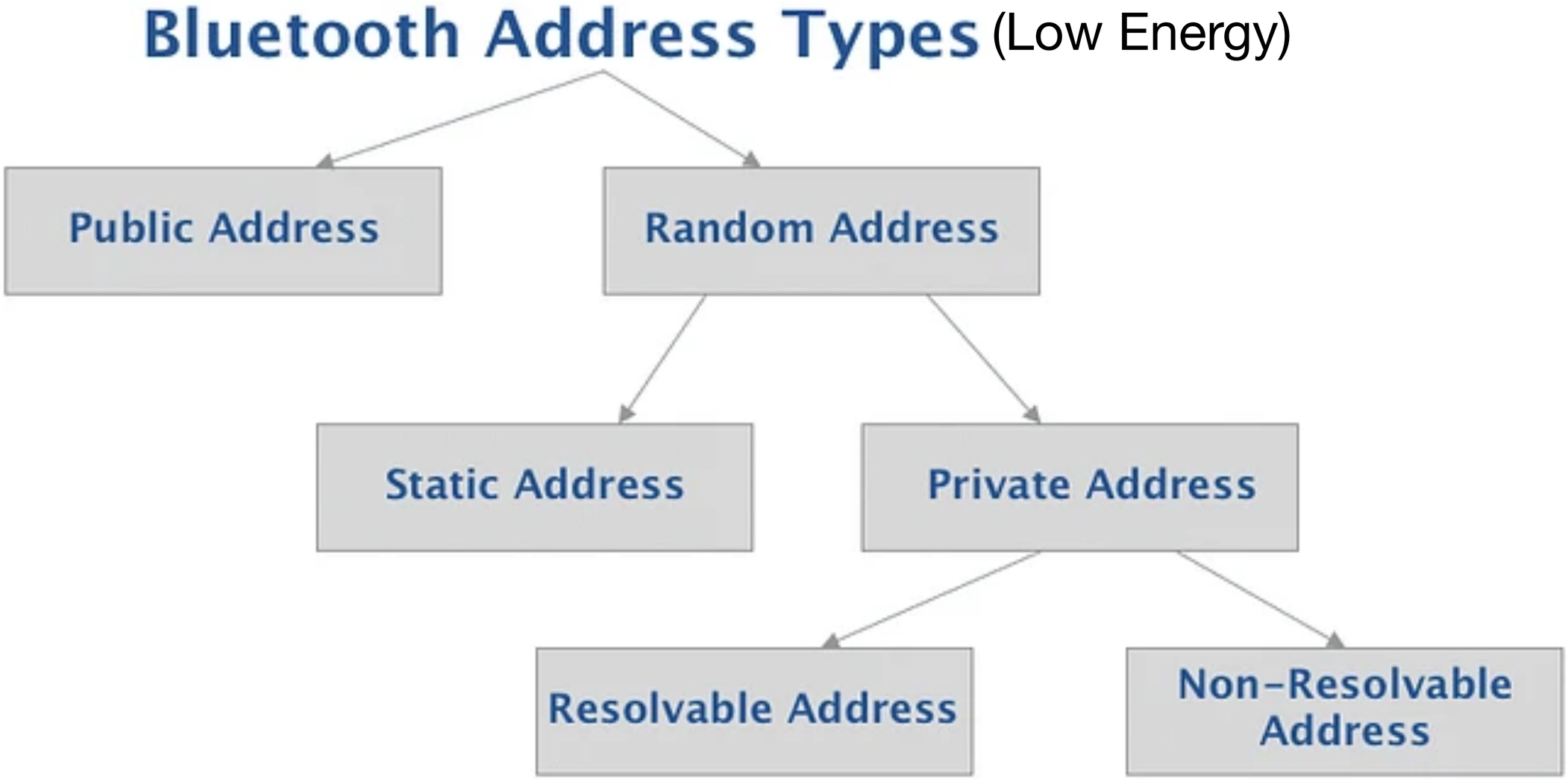


Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

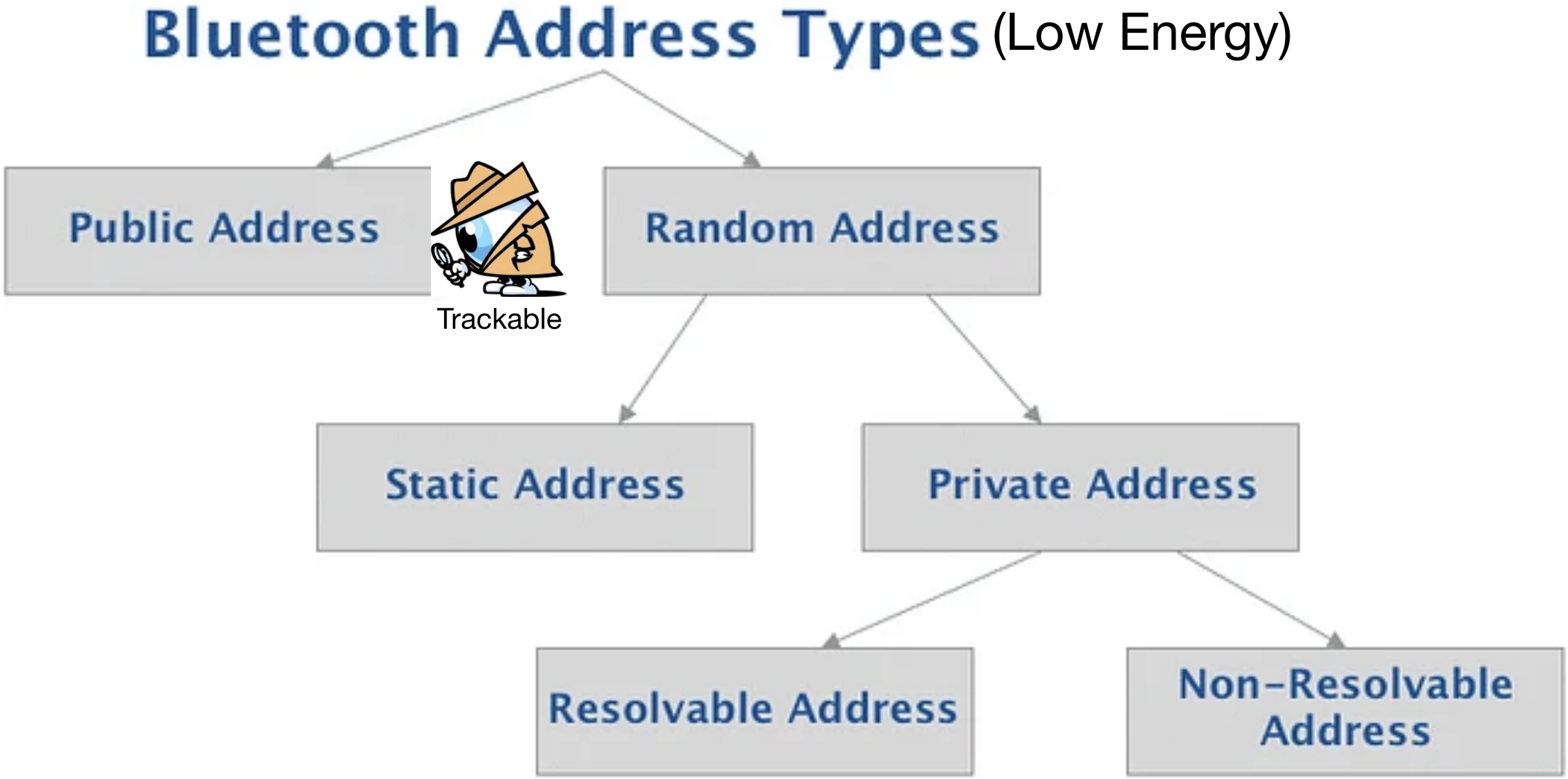


Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

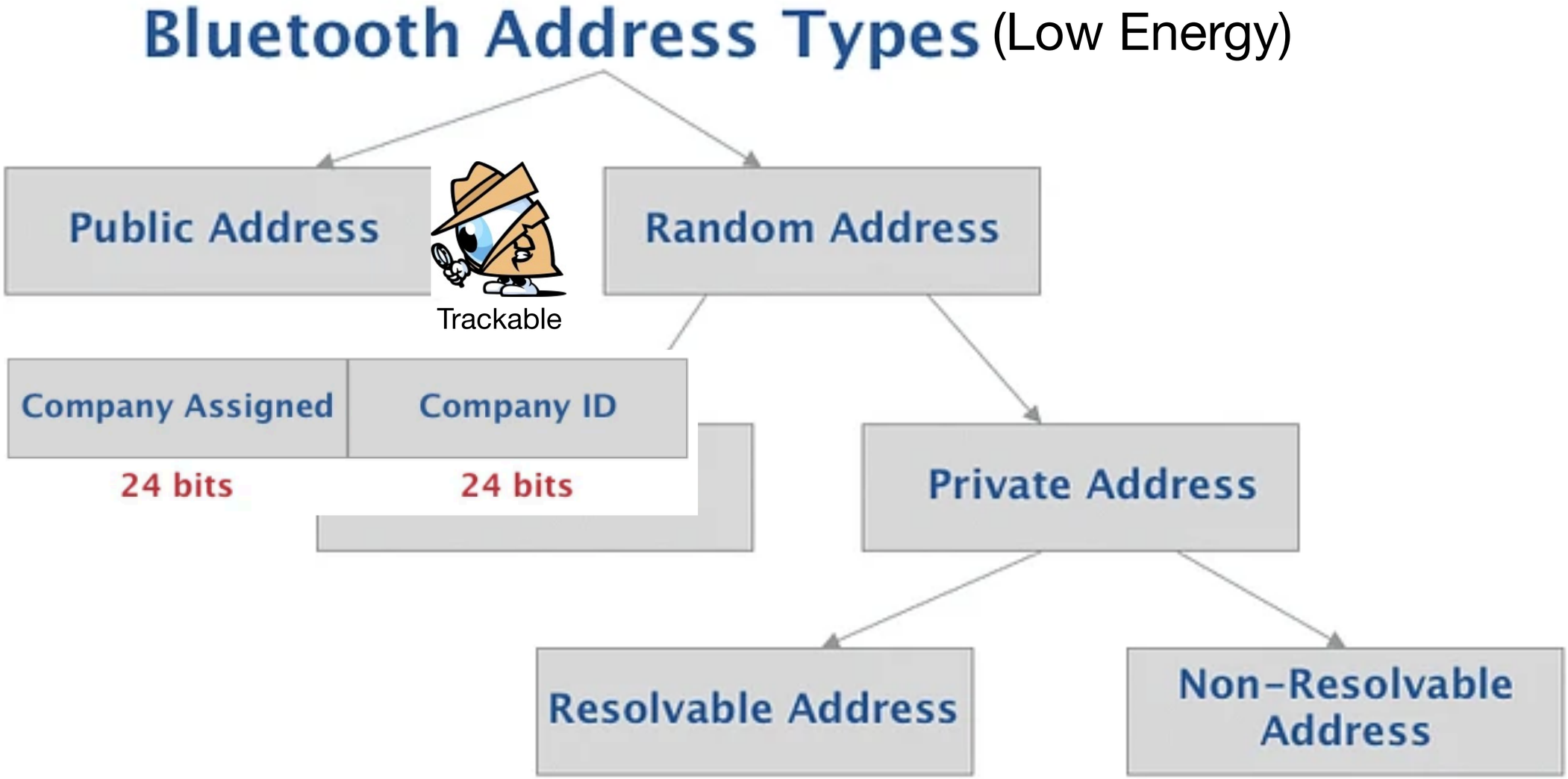


Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

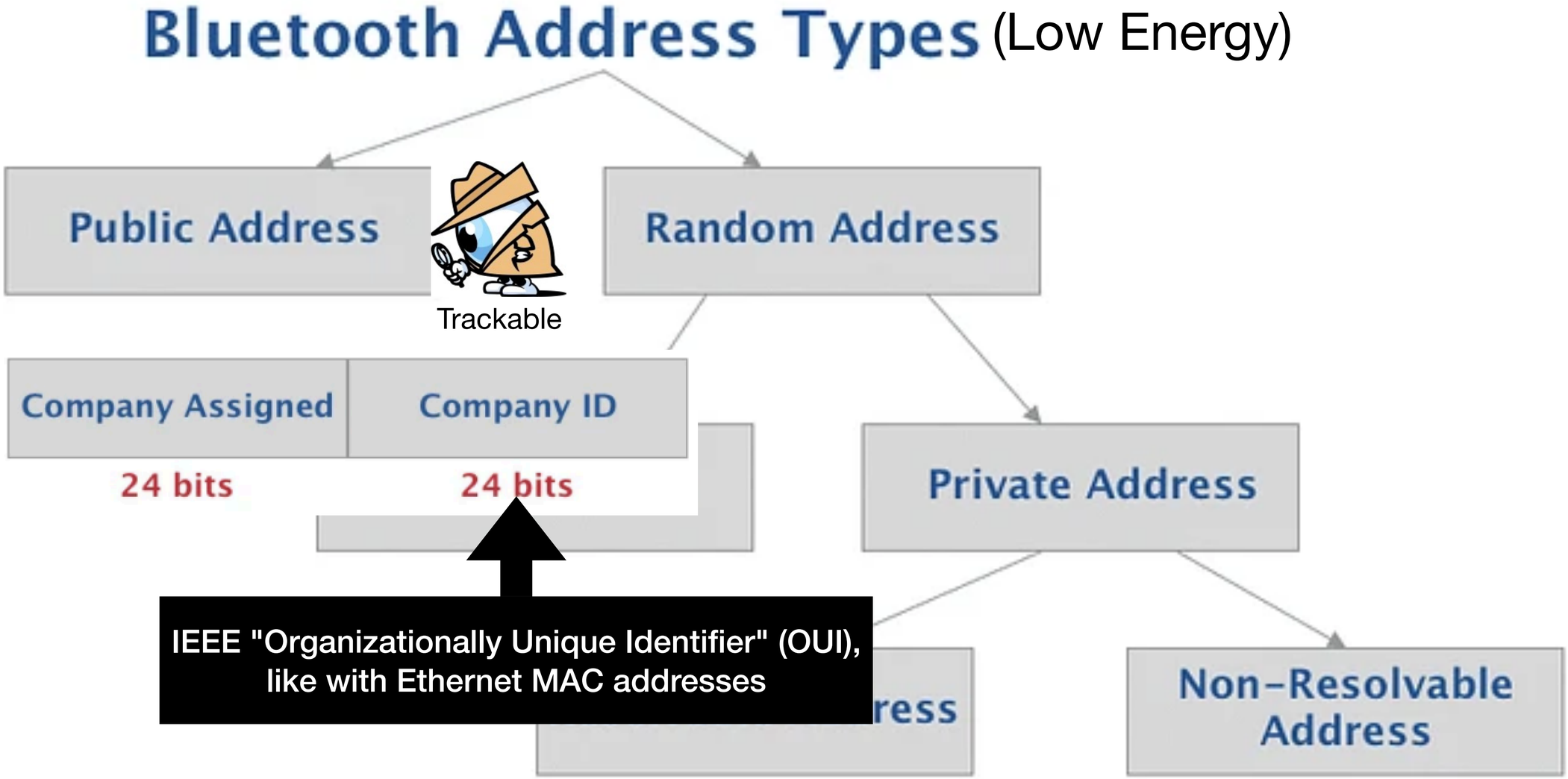


Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

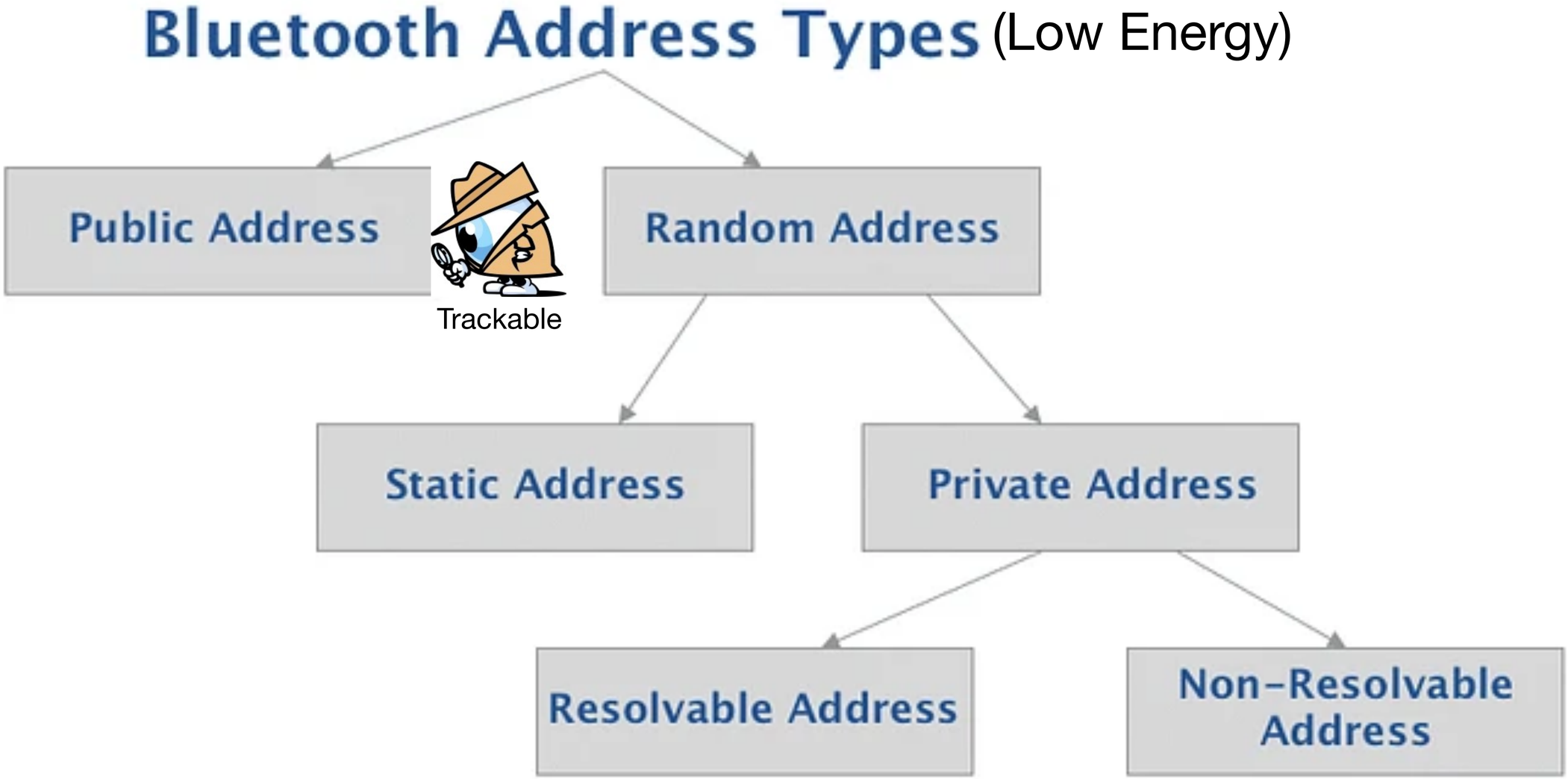


Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

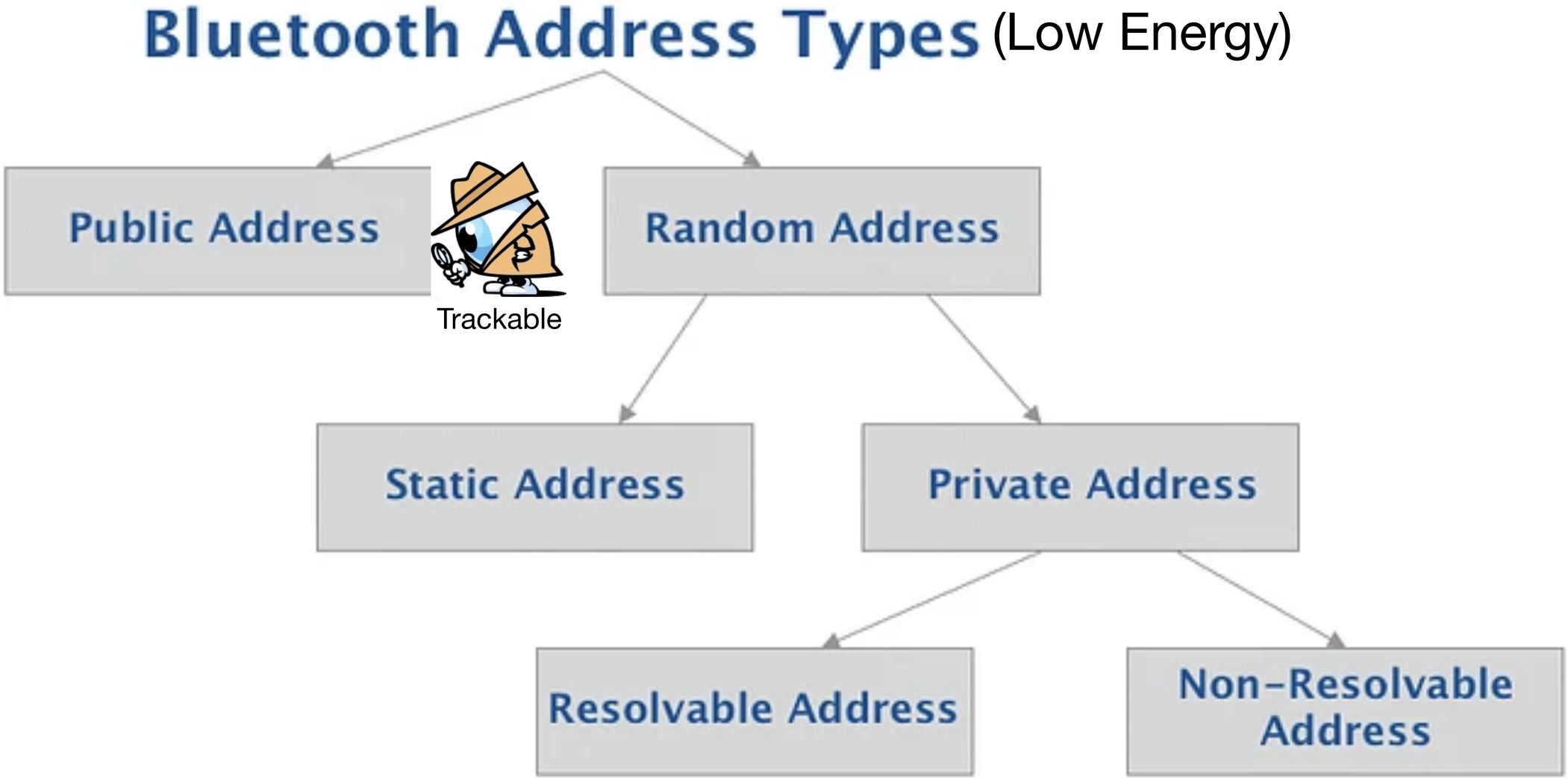


Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

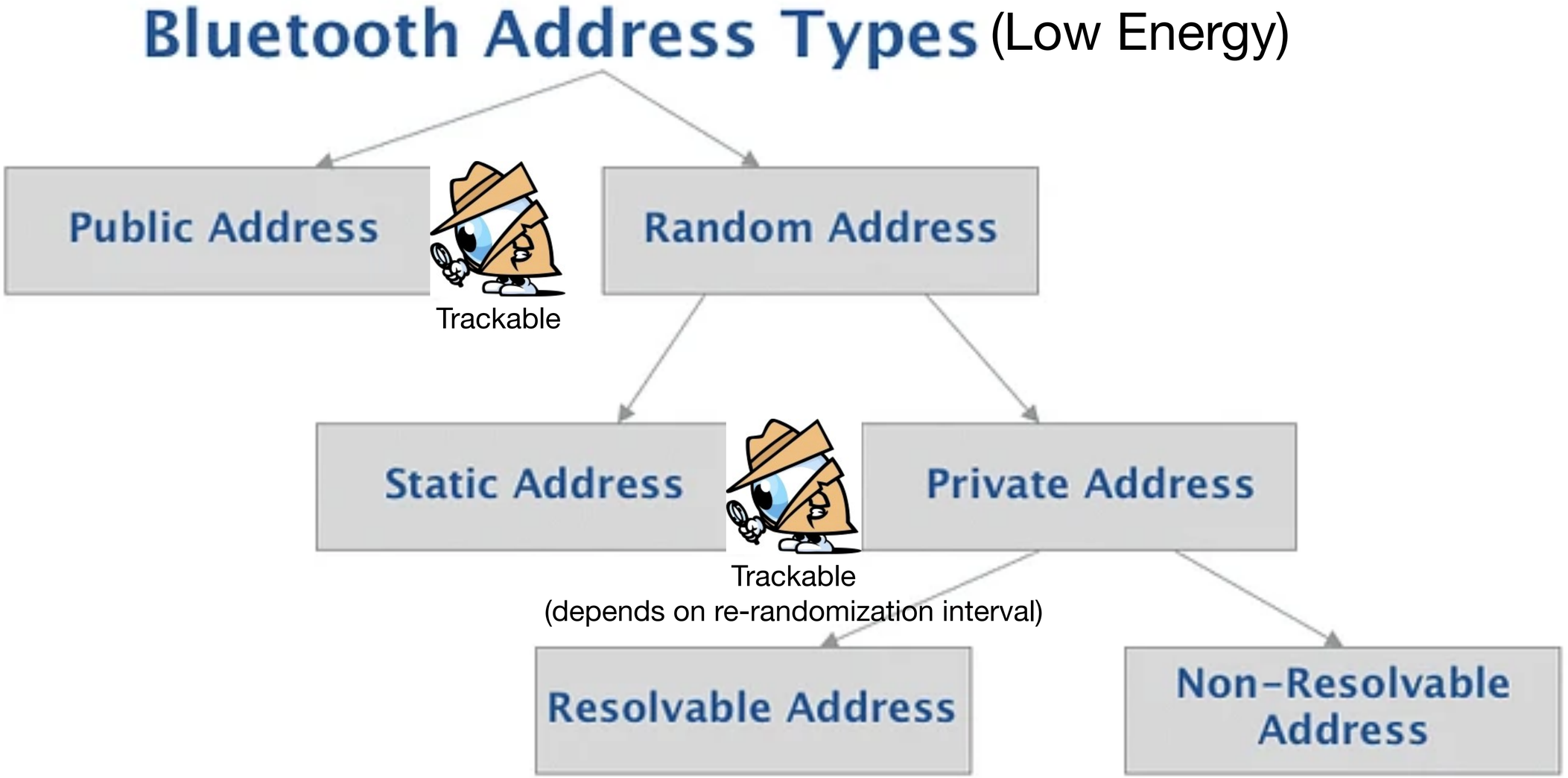


Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT De*

Random Static Addresses can be used in one of two ways:

- It can be assigned and fixed for the lifetime of the device
- It can be changed at bootup

However, it **cannot** be changed during runtime.

The format of Random Static Addresses looks like this:

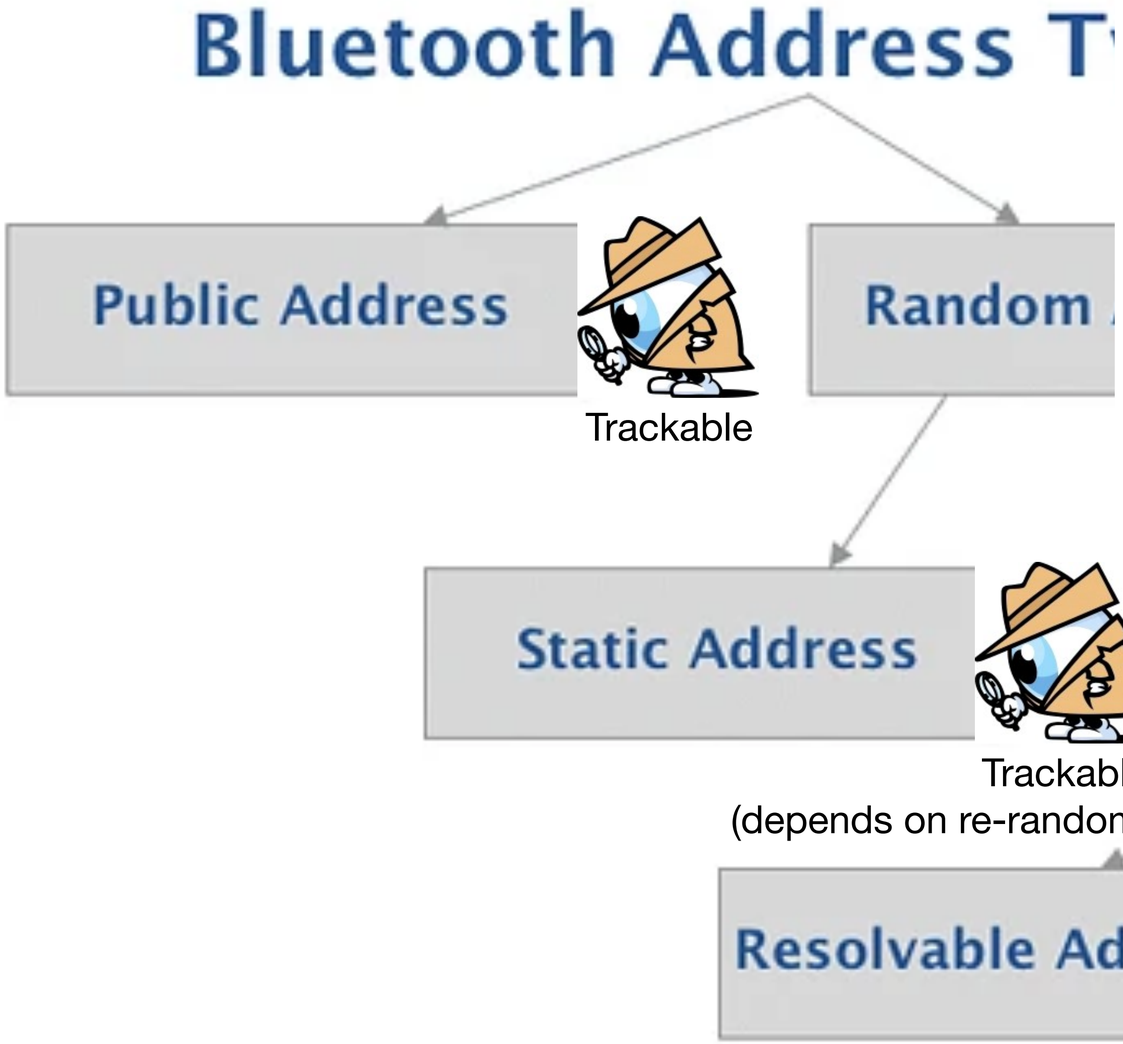


Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

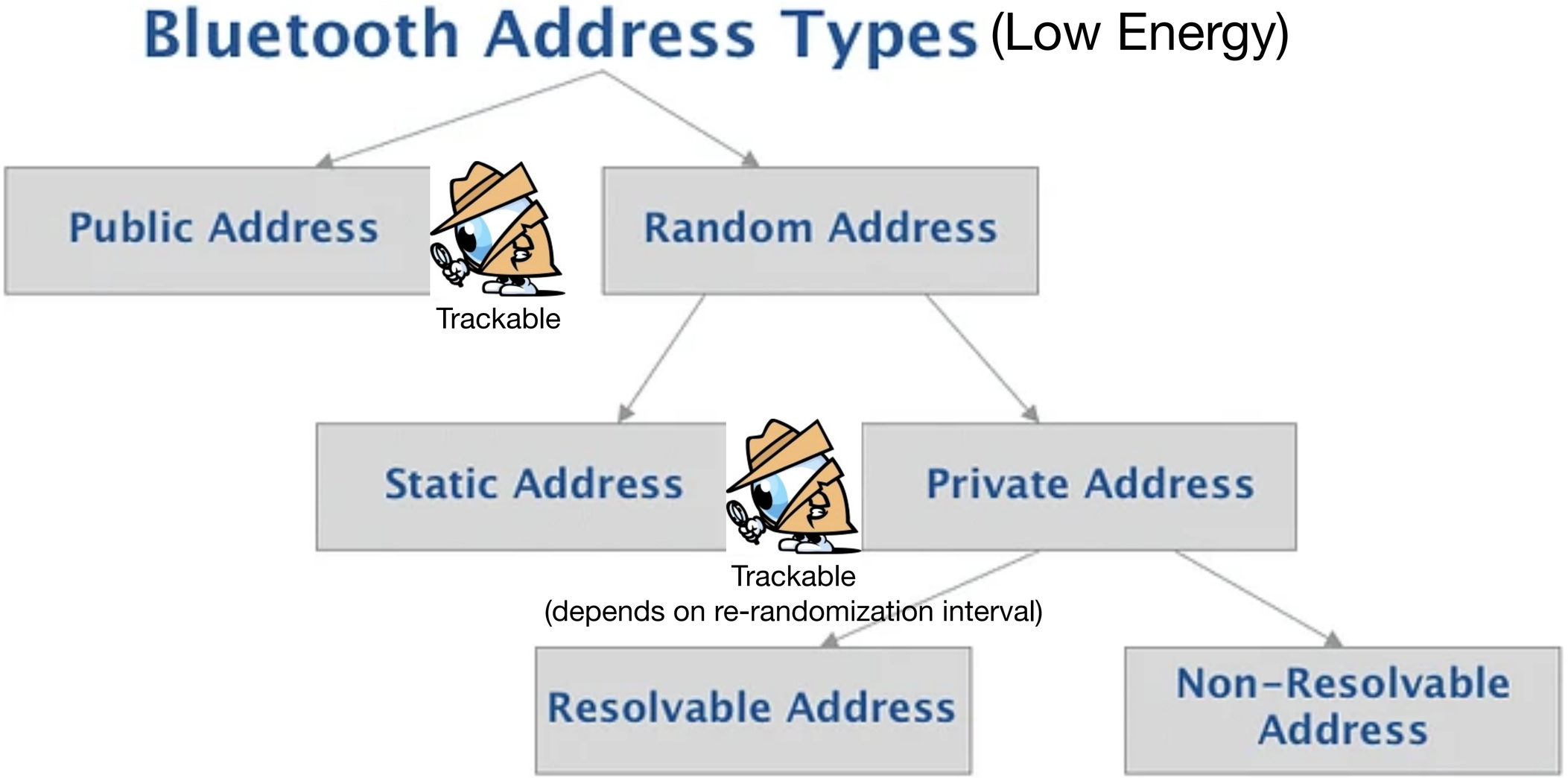


Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

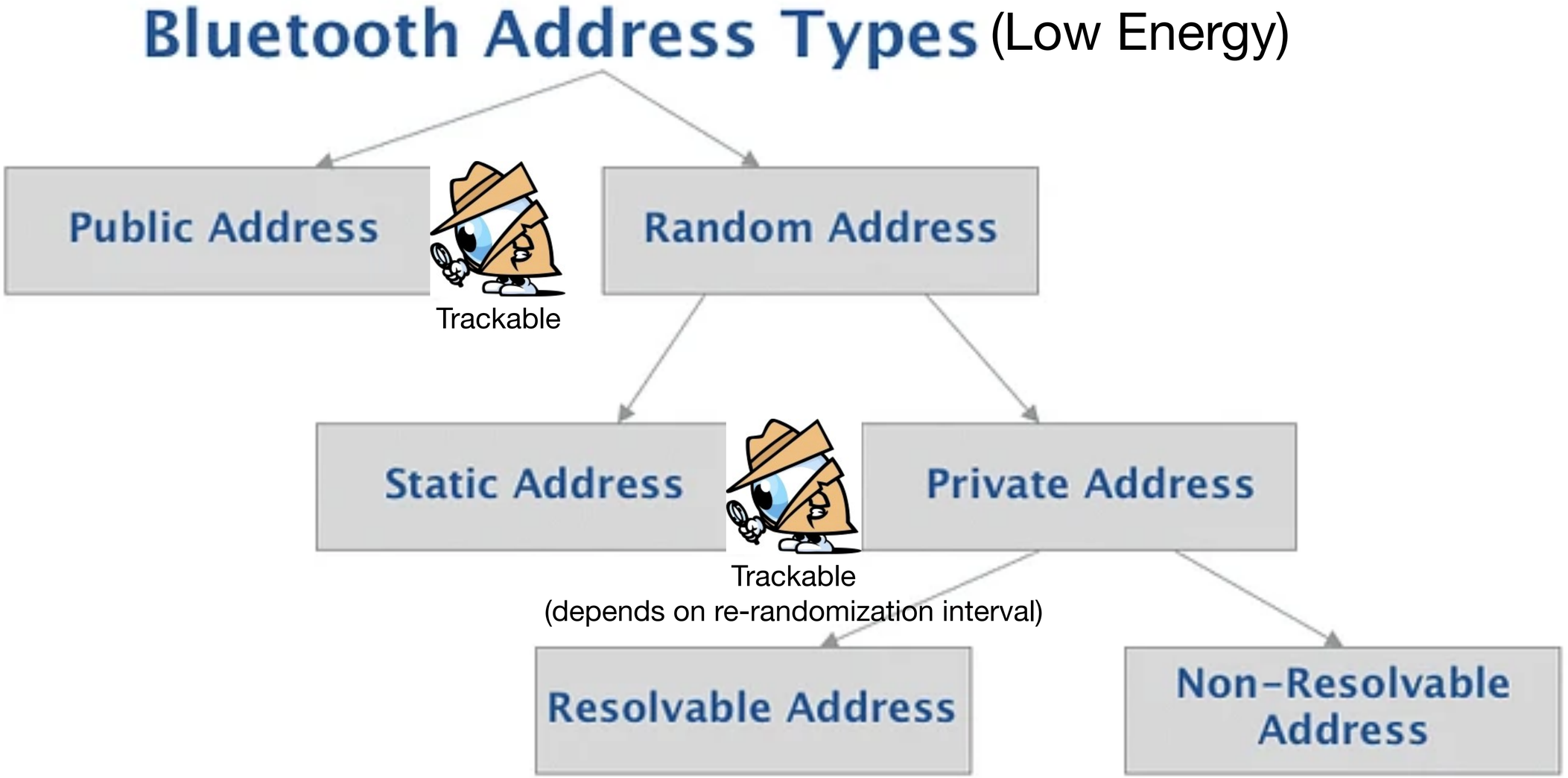


Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

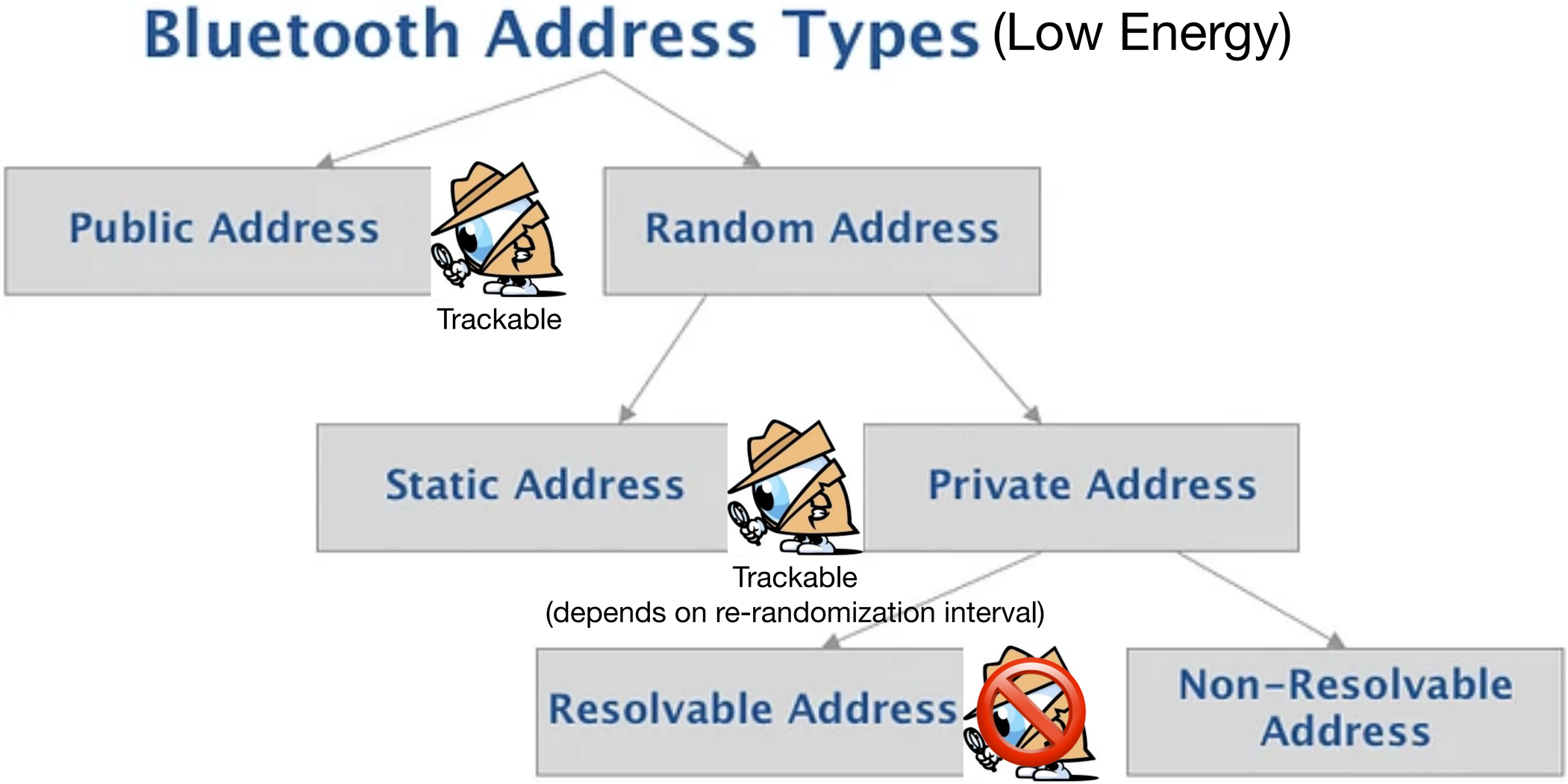
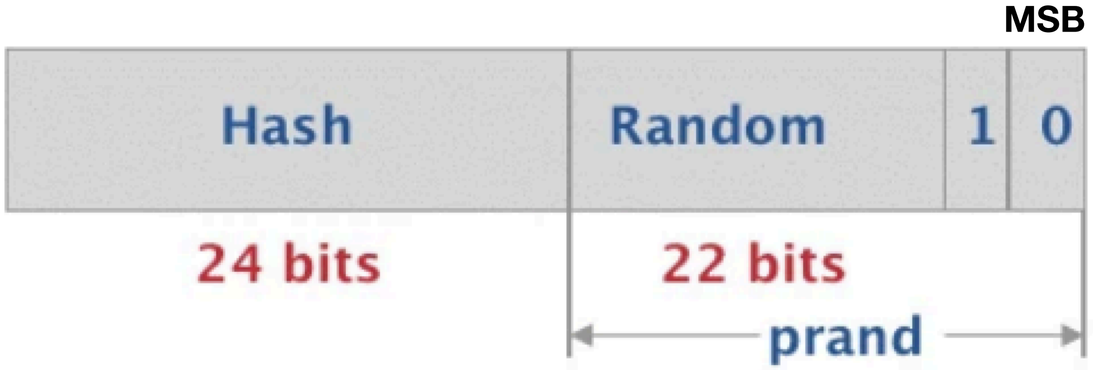


Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - E

Bluetooth Addr

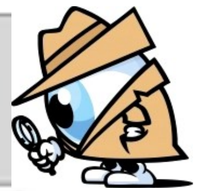
A Resolvable Random Private address is made up of the following fields:



Random Private Resolvable Address format (little-endian format)

- 0 and 1 are fixed in the most significant bits (MSB)
- The next 22 bits are randomly generated
- The **prand** constitutes of these most significant 24 bits
- The lower 24 bits represent a hash value which is generated using the **prand** and the **IRK**

Public Address



Trackable

Static Addre

Trackable
(depends on re-randomization interval)

Resolvable Address

Non-Resolvable Address

Minimally Trackable *(in principle)*
(Possibly trackable using device-specific data (e.g. names))

Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

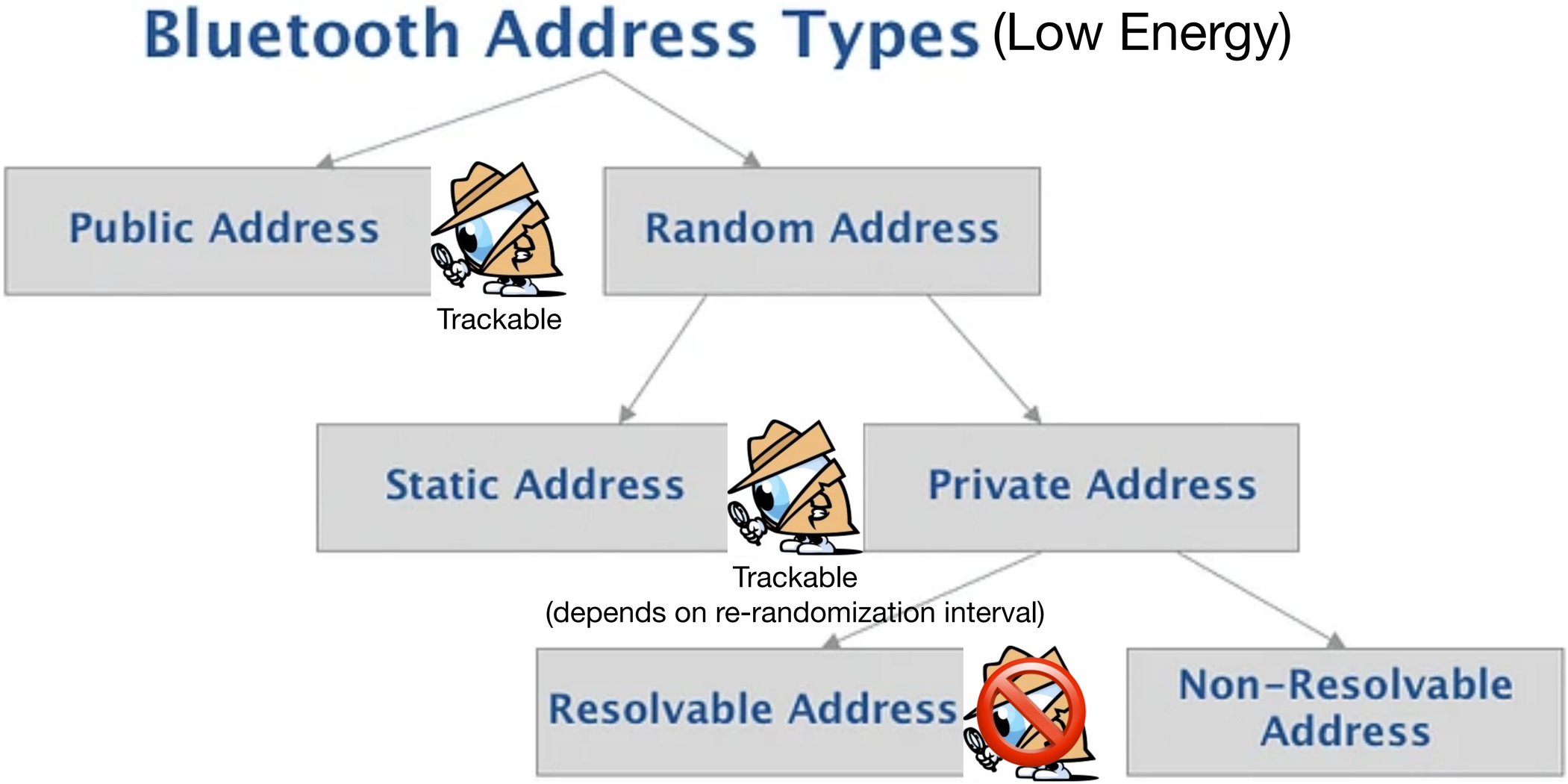


Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

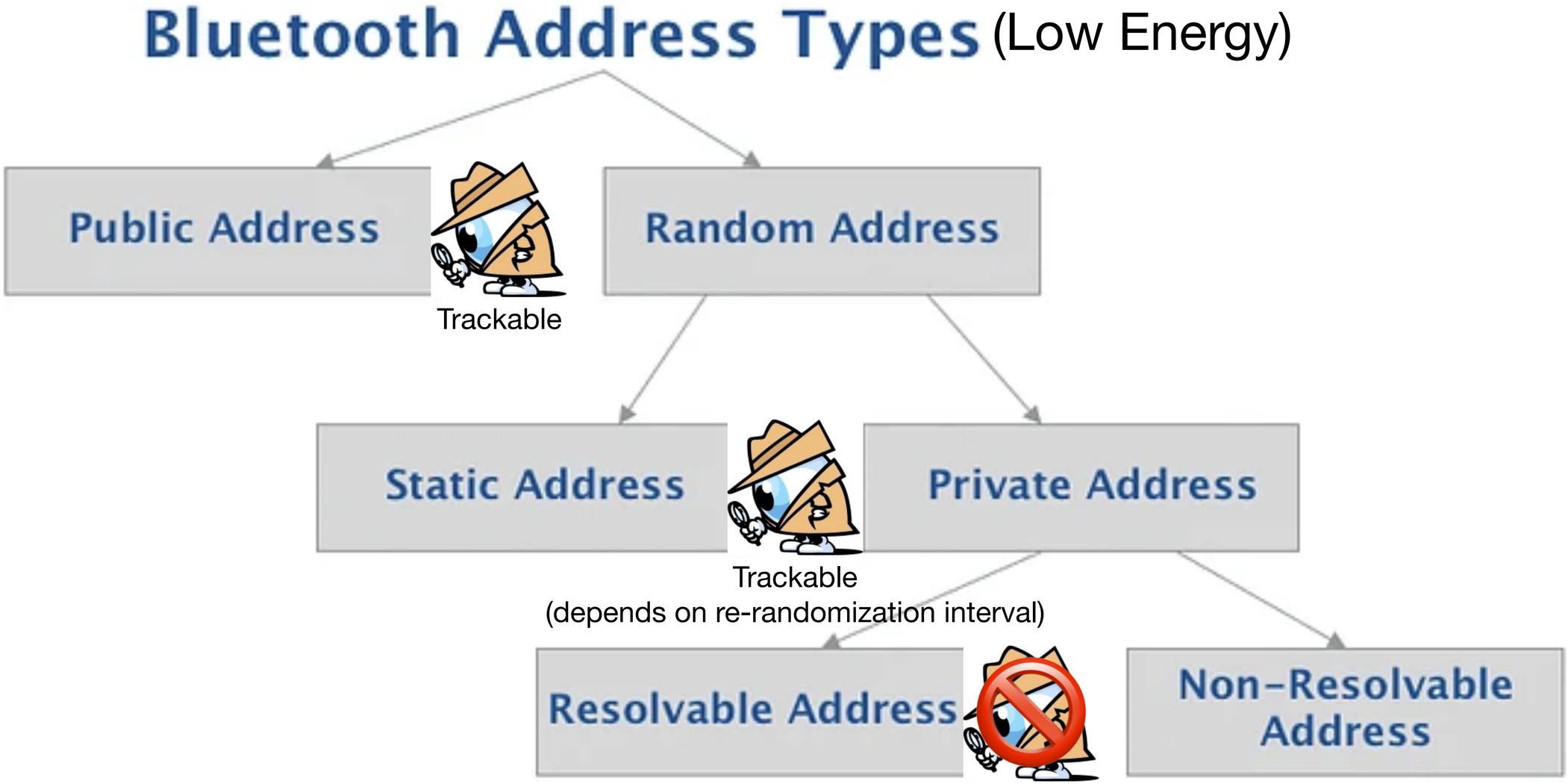


Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

Background - *BT Device Address (BDADDR)*

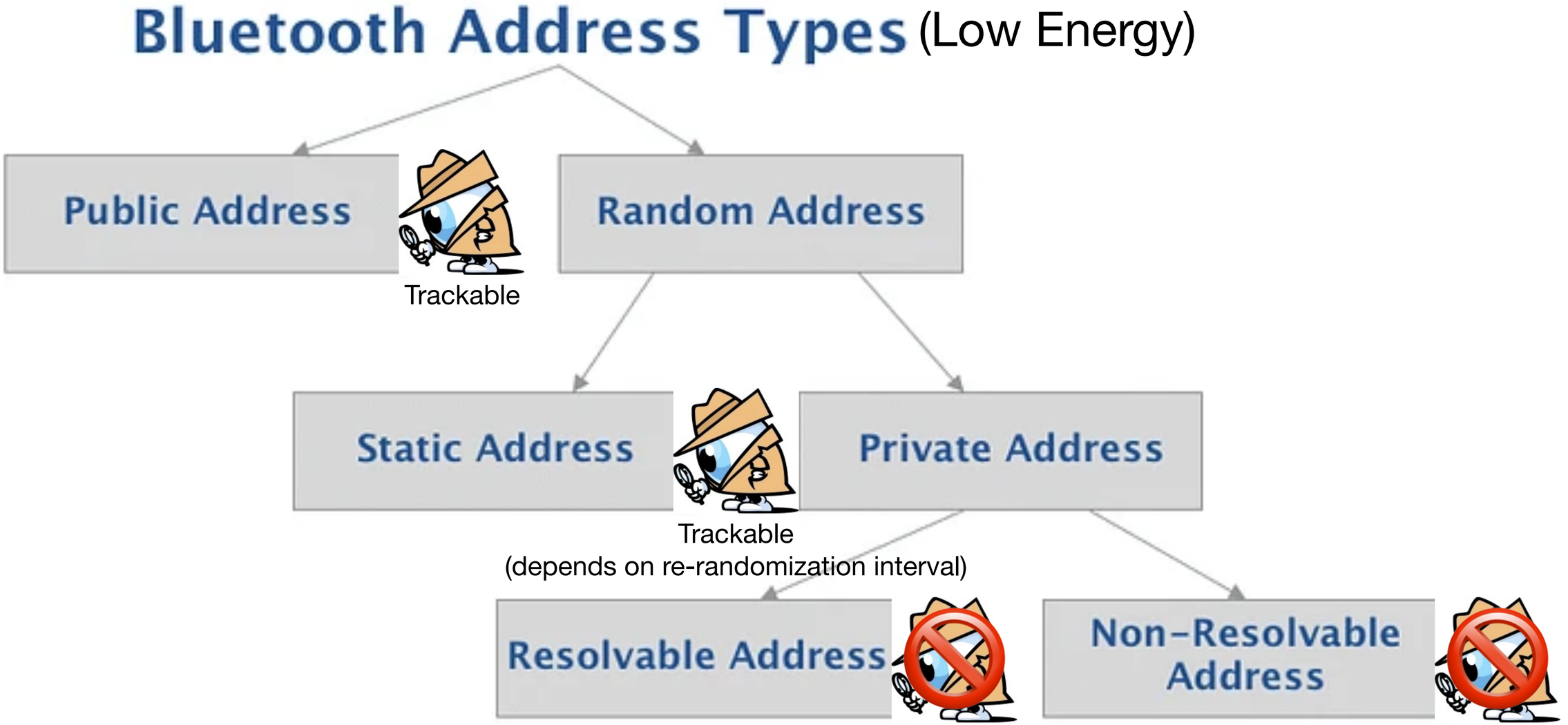
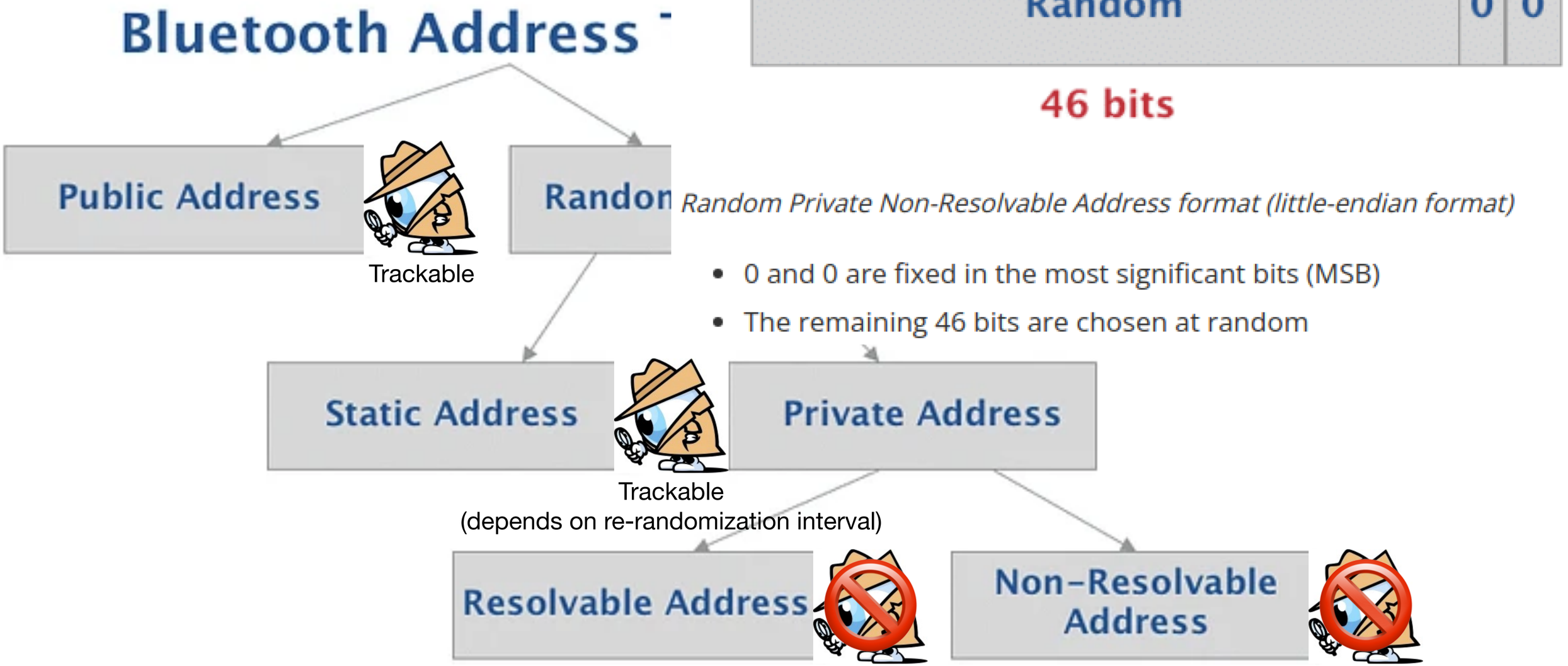
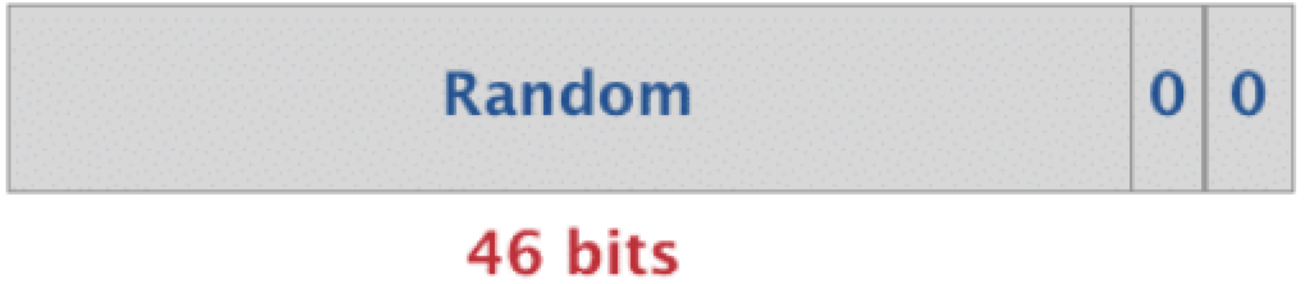


Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

The format of Non-Resolvable Random Private Addresses is as follows:

Background - *BT D*





Random Private Non-Resolvable Address format (little-endian format)

- 0 and 0 are fixed in the most significant bits (MSB)
- The remaining 46 bits are chosen at random

Image & slide-in text from
https://novelbits.io/bluetooth-address-privacy-ble/

btmon

- If you see output like the below in this presentation, it was captured by the *nix "btmon" tool, and/or output by it

```
> HCI Event: LE Meta Event (0x3e) plen 37
      LE Advertising Report (0x02)
        Num reports: 1
        Event type: Connectable undirected - ADV_IND (0x00)
        Address type: Public (0x00)
        Address: FF:FF:EA:00:34:84 (OUI FF-FF-EA)
        Data length: 25
        Flags: 0x06
          LE General Discoverable Mode
          BR/EDR Not Supported
        Name (complete): Triones-FFFFEA003484
        RSSI: -83 dBm (0xad)
```

btmon

- If you see output like the below in this presentation, it was captured by the *nix "btmon" tool, and/or output by it

```
> HCI Event: LE Meta Event (0x3e) plen 37
      LE Advertising Report (0x02)
        Num reports: 1
        Event type: Connecta                ected - ADV_IND (0x00)
        Address type: Public
        Address: FF:FF:EA:00:34:84 (OUI FF-FF-EA)
        Data length: 25
        Flags: 0x06
          LE General Discoverable Mode
          BR/EDR Not Supported
        Name (complete): Triones-FFFFEA003484
        RSSI: -83 dBm (0xad)
```

btmon

- If you see output like the below in this presentation, it was captured by the *nix "btmon" tool, and/or output by it

> HCI Event: LE Meta Event (0x3e) plen 37
  LE Advertising Report (0x02)
    Num reports: 1
    Event type: Connectable undirected - ADV_IND (0x00)
    Address type: **Public** (0x00)
    Address: **FF:FF:EA:00:34:84** (OUI FF-FF-EA)
    Data length: 25
    Flags: 0x06
      LE General Discoverable Mode
      BR/EDR Not Supported
    Name (complete): Triones-**FFFFEA003484**
    RSSI: -83 dBm (0xad)

btmon

- If you see output like the below in this presentation, it was captured by the *nix "btmon" tool, and/or output by it

> HCI Event: LE Meta Event (0x3e) plen 37
  LE Advertising Report (0x02)
    Num reports: 1
    Event type: Connectable undirected - ADV_IND (0x00)
    Address type: **Public** (0x00)
    Address: **FF:FF:EA:00:34:84** (OUI FF-FF-EA)
    Data length: 25
    Flags: 0x06
      LE General Discoverable Mode
      BR/EDR Not Supported
    Name (complete): Triones-**FFFFEA003484**
    RSSI: -83 dBm (0xad)

Congrats! Your car can now be tracked by its headlights!

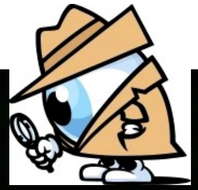
TellMeEverything.py

- If you see output like the below in this presentation, it's from my script I've released for analyzing log data

```
DeviceName: AP 000722ED 0E96AAC1000E09F2
        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)
```

TellMeEverything.py

- If you see output like the below in this presentation, it's from my script I've released for analyzing log data

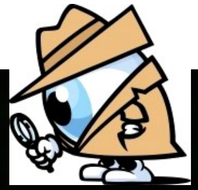


```
DeviceName: AP 000722ED 0E96AAC1000E09F2
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
        This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)
```

TellMeEverything.py

- If you see output like the below in this presentation, it's from my script I've released for analyzing log data

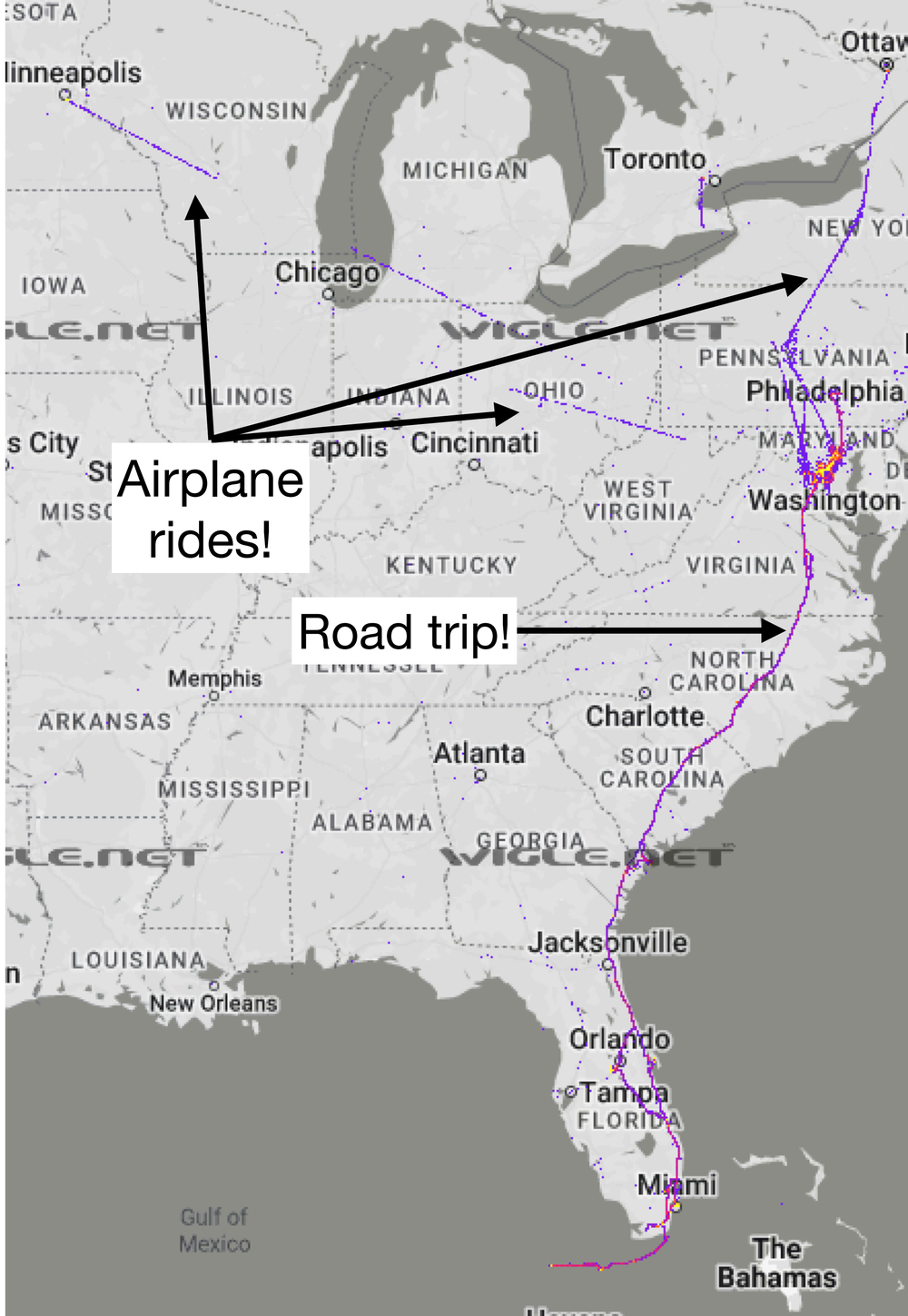
```
DeviceName: AP 000722ED 0E96AAC1000E09F2
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
        This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)
```



Congrats! You can now be tracked by your diabetes-management device

What About WiGLE?

- Good crowdsourcing infrastructure
- Originally for WiFi, Bluetooth support turned on by default in 2019
- I use the Android app on an old junk Pixel 3
- Missing most data we want for BT

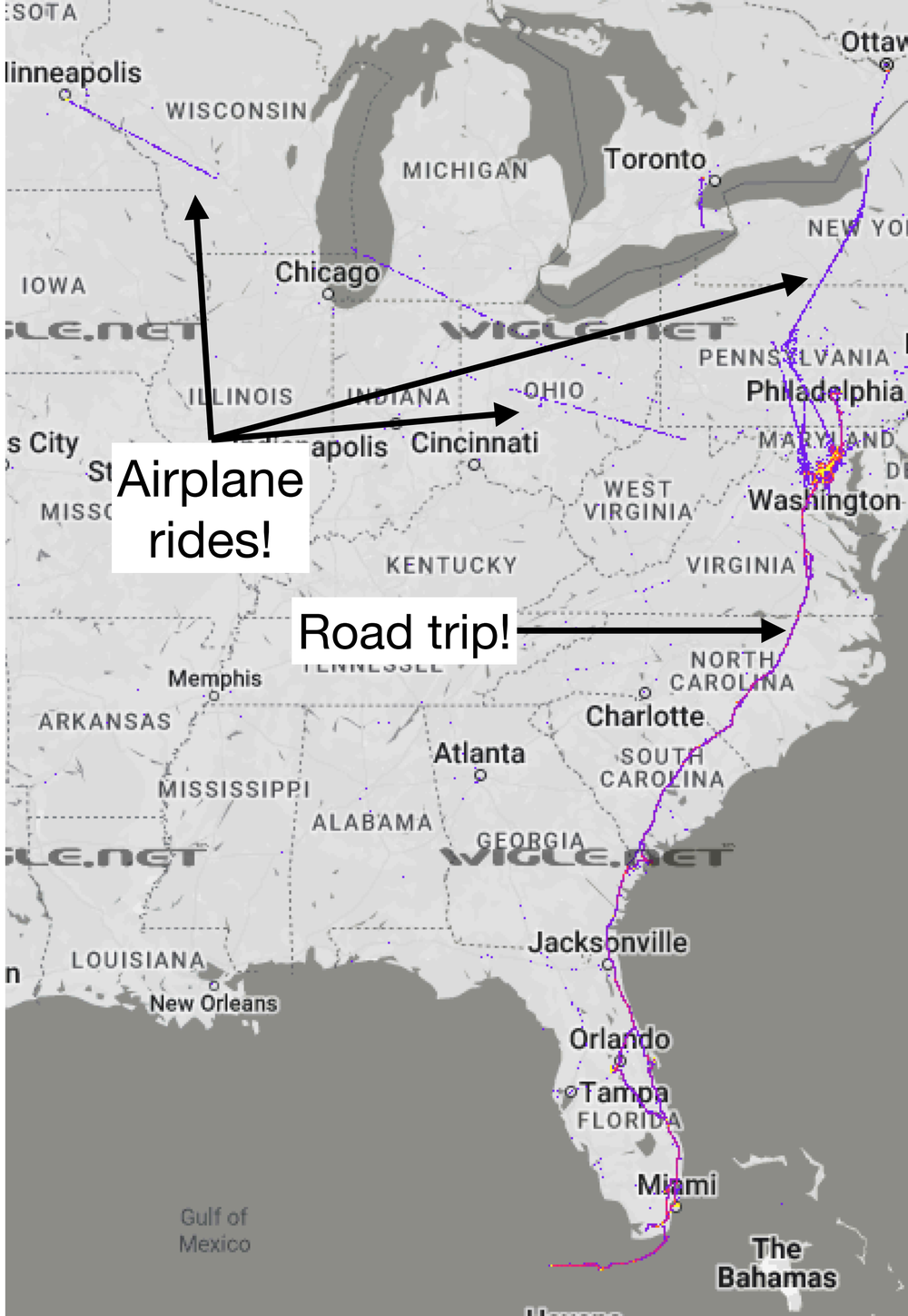


What About WiGLE?

- Good crowdsourcing infrastructure
- Originally for WiFi, Bluetooth support turned on by default in 2019
- I use the Android app on an old junk Pixel 3
- Missing most data we want for BT

Discovered + : 21,443
Seen Networks: 52,109
this month / last month with : 103 / 653

Discovered + : 380
Seen : 877
Discovered + : 706187
Seen : 764234



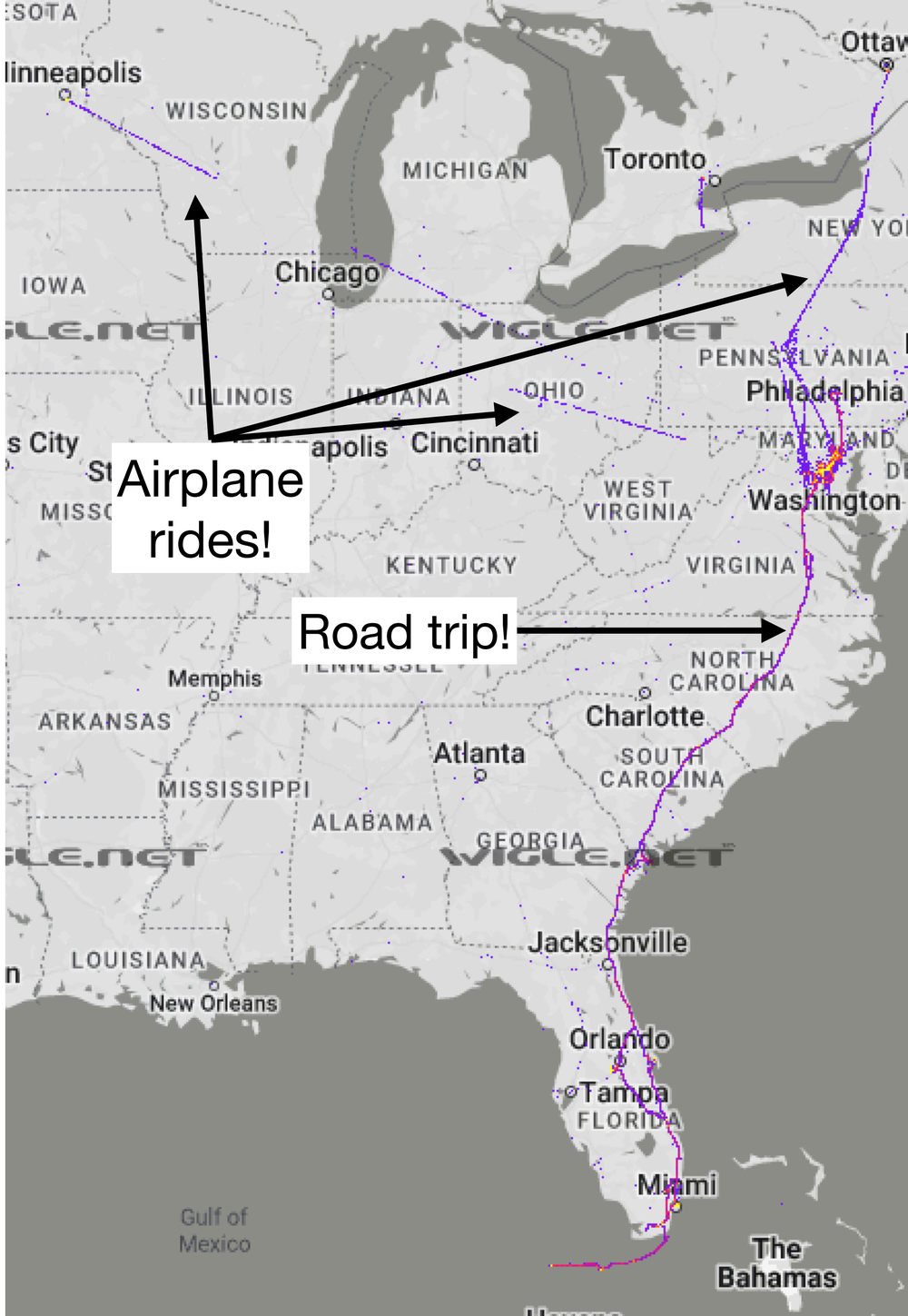
What About WiGLE?

- Good crowdsourcing infrastructure
- Originally for WiFi, Bluetooth support turned on by default in 2019
- I use the Android app on an old junk Pixel 3
- Missing most data we want for BT

Discovered + : 21,443
Seen **Networks:** 52,109
this month / last month with : 103 / 653

Order of magnitude more BT than WiFi!

Discovered + : 380
Seen : 877
Discovered + : 706187
Seen : 764234



What About WiGLE?

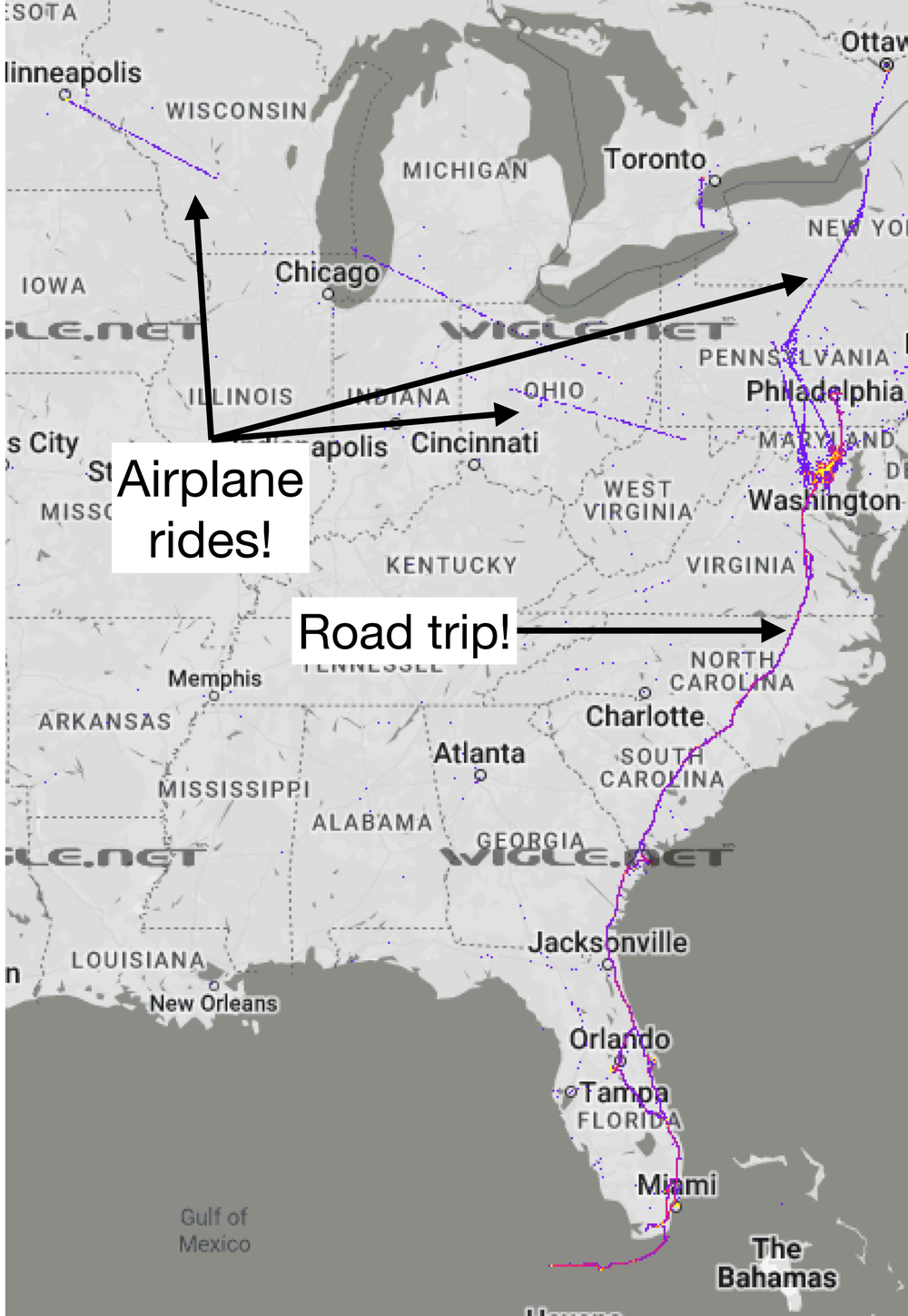
- Good crowdsourcing infrastructure
- Originally for WiFi, Bluetooth support turned on by default in 2019
- I use the Android app on an old junk Pixel 3
- Missing most data we want for BT

Discovered + : 21,443
Seen Networks: 52,109
this month / last month with : 103 / 653

Order of magnitude more BT than WiFi!

Discovered + : 380
Seen : 877
Discovered + : 706187
Seen : 764234

"Currently, the actual number of Bluetooth radios in use is four times higher than the number of Wi-Fi radios deployed." - Herfurt & Mulliner, "Blueprinting" 2004



Takeaways 1

- *Bluetooth sniffing goals are different from WiFi goals*, and consequently the sniffing tech is under-developed to help with those goals
- When there's a BT FW bug, **no one knows what all it affects**

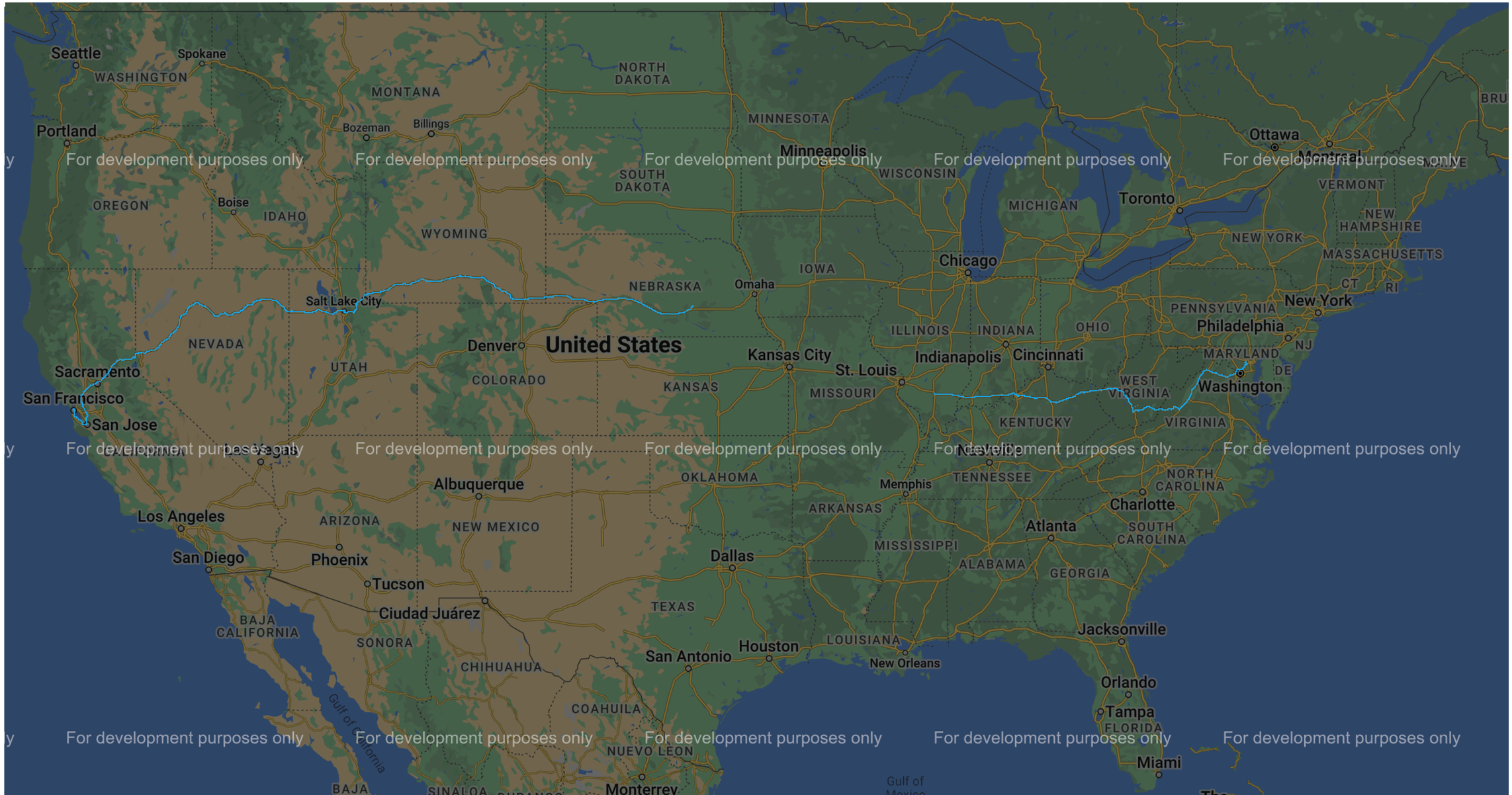
Takeaways 2

- There are lots of devices that do not have human-readable names, so it's not clear what they are
  - *Somebody (/me!)* ought to start learning to toothprint BT devices!
- There are lots of devices that are advertising names, but it's not clear what they are
  - I'm looking at you **"*B#a*"**
  - Somebody ought to start a database! Or at least a wiki?!

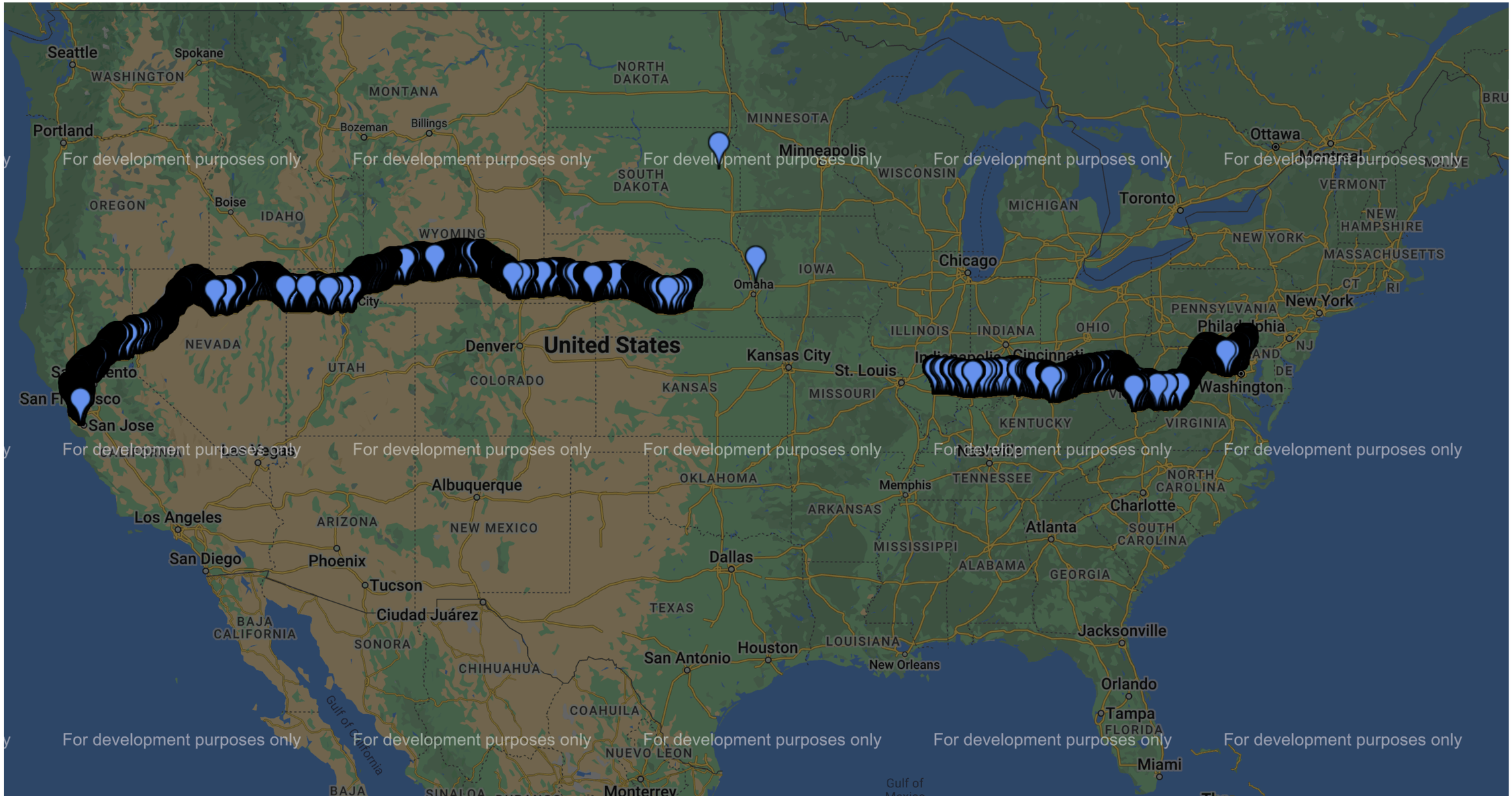
End - Prelude

Begin - Anecdotes - Locations

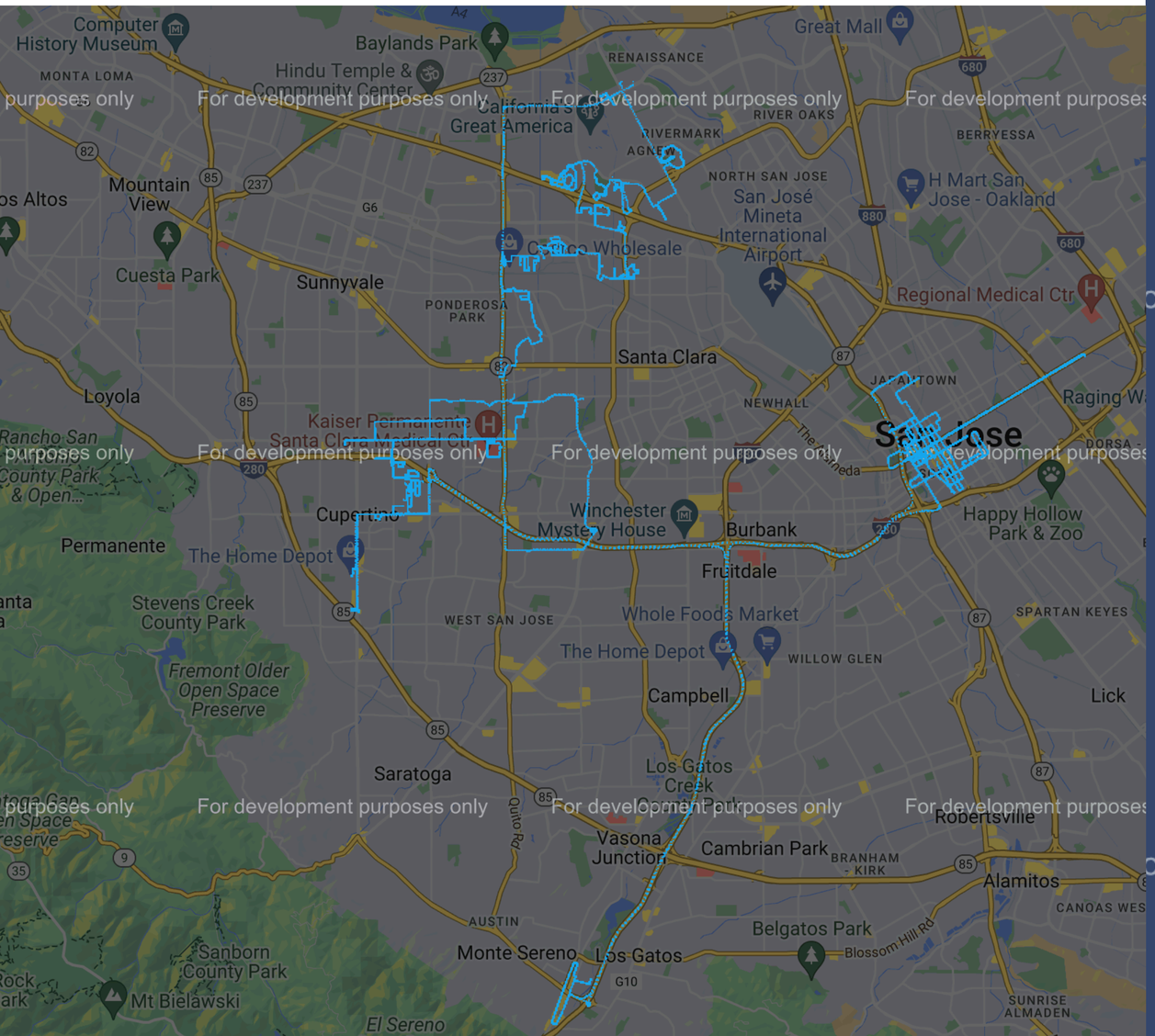
Across the USA - Pandemic Cannonball Run!

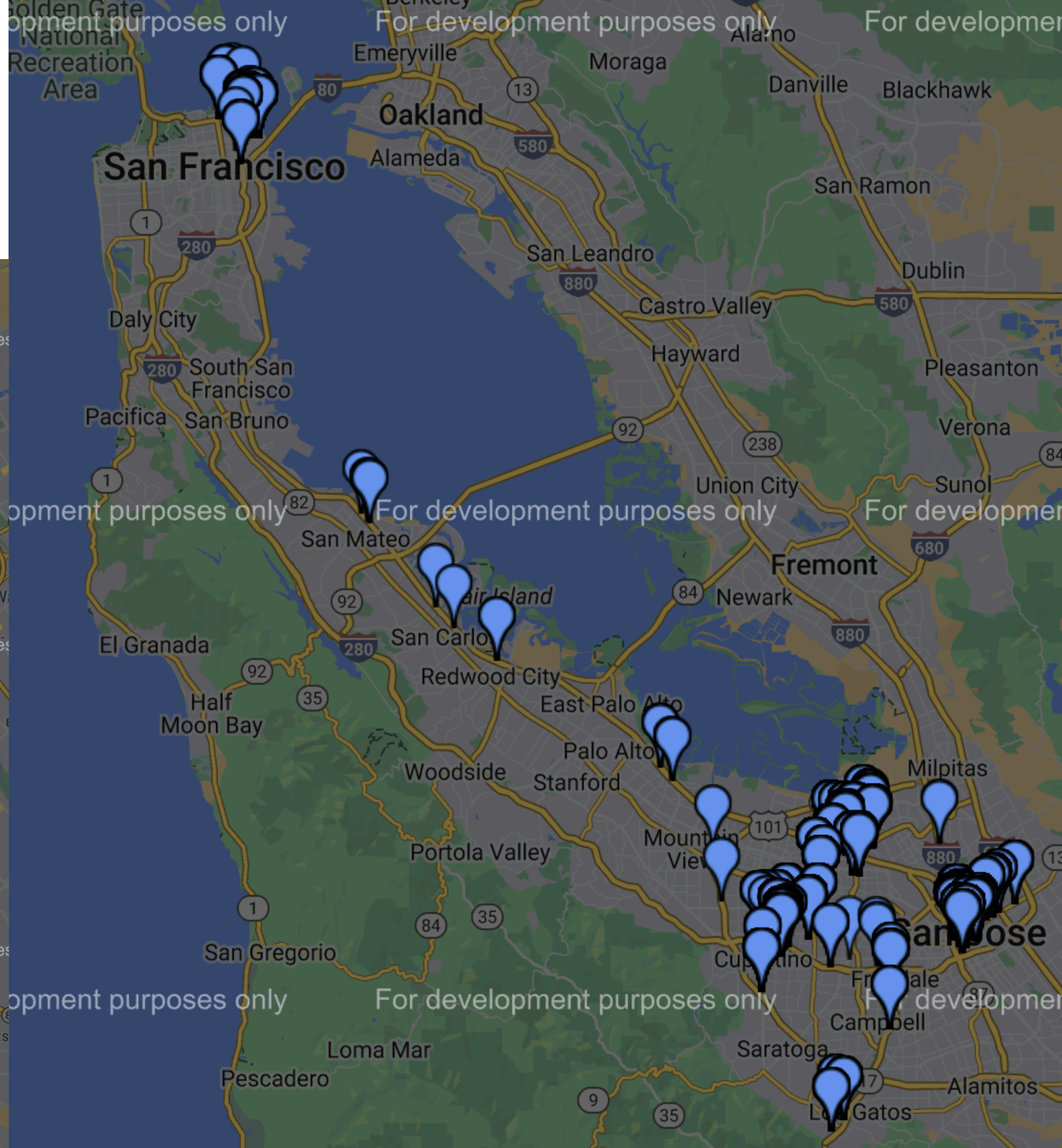


Across the USA - Pandemic Cannonball Run!



USA - SF Bay Area





USA - Maryland

- The curious case of "BLE003U"

Strangely US-specific?

BLE003U QoS: 0 type: BT
78:9c:e7:01:44:72? 2021-02-26 - 2021-02-26

BLE003U QoS: 0 type: BT
78:9c:e7:01:44:a0? 2020-09-14 - 2020-09-14

BLE003U QoS: 0 type: BLE
78:9c:e7:01:44:b0? 2020-12-20 - 2020-12-20

BLE003U QoS: 2 type: BLE
78:9c:e7:01:44:c0? 2021-12-17 - 2022-02-15

BLE003U QoS: 0 type: BLE
78:9c:e7:01:44:fb? 2019-01-02 - 2019-03-04

BLE003U QoS: 1 type: BLE
78:9c:e7:01:45:a3? 2022-09-18 - 2022-11-16

BLE003U QoS: 0 type: BLE
78:9c:e7:01:45:ca? 2023-01-03 - 2023-01-03

BLE003U QoS: 6 type: BLE
78:9c:e7:01:5c:1b? 2021-11-09 - 2023-04-08

BLE003U QoS: 6 type: BLE
78:9c:e7:01:5c:1d? 2020-07-25 - 2022-12-12

BLE003U QoS: 0 type: BLE
78:9c:e7:01:5c:1e? 2021-10-08 - 2022-08-05

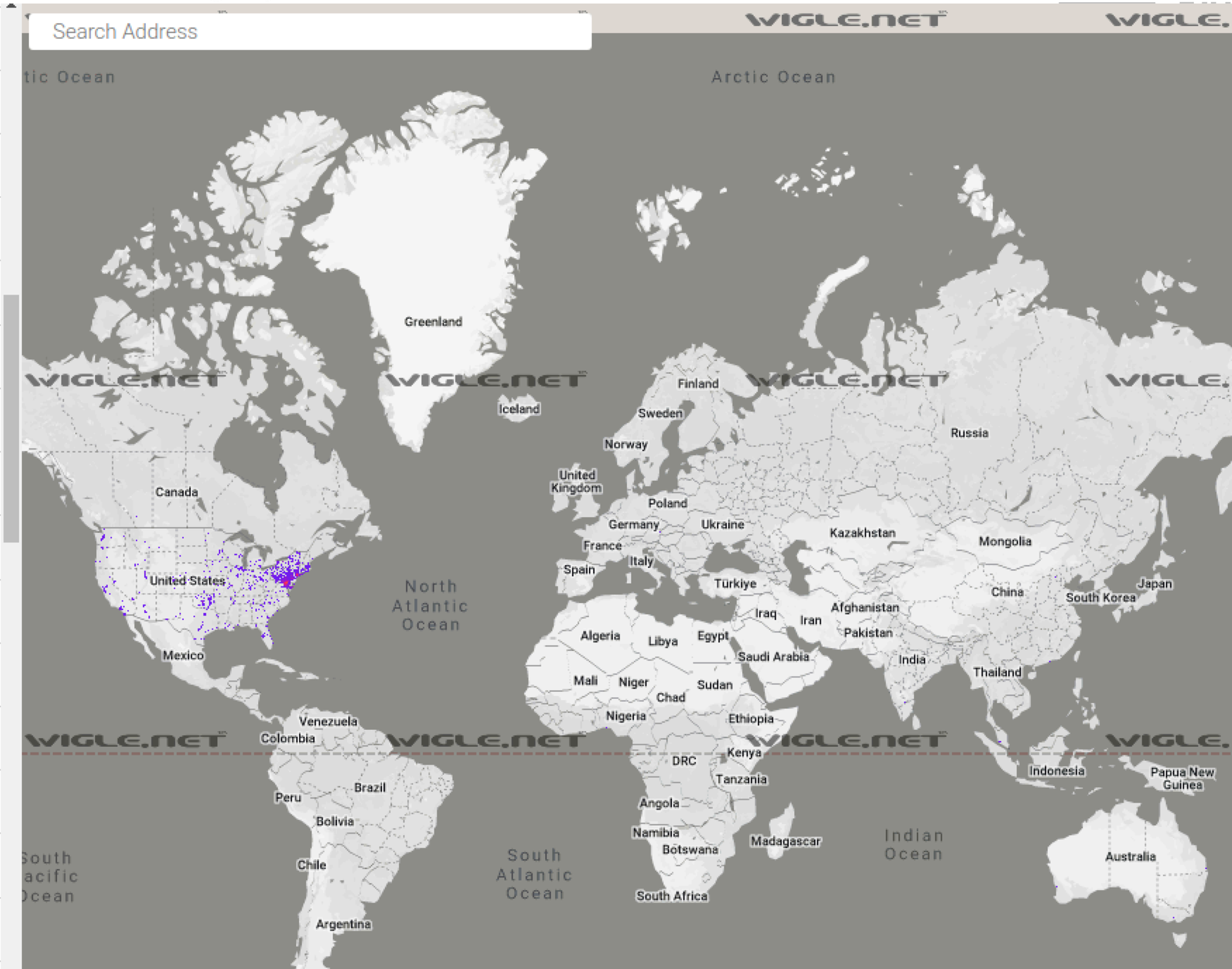
BLE003U QoS: 0 type: BLE
78:9c:e7:01:5c:1f? 2021-06-26 - 2021-06-26

BLE003U QoS: 7 type: BT
78:9c:e7:01:5c:20? 2019-03-14 - 2021-06-10

BLE003U QoS: 7 type: BLE
78:9c:e7:01:5c:25? 2019-11-08 - 2022-08-14

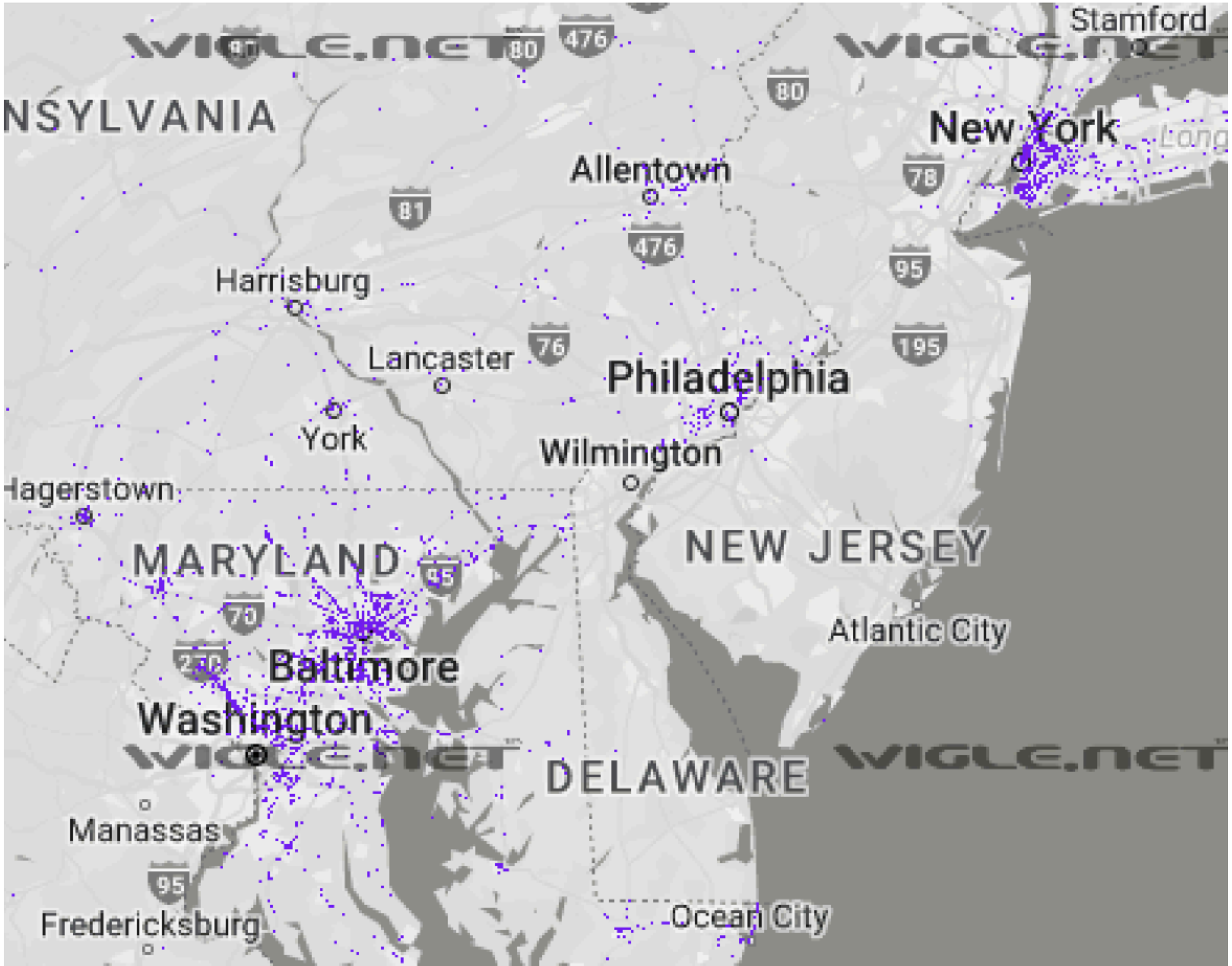
BLE003U QoS: 7 type: BT
78:9c:e7:01:5c:27? 2019-08-09 - 2023-03-09

BLE003U QoS: 7 type: BT
78:9c:e7:01:5c:2b? 2018-12-04 - 2023-03-21



Strangely DC/NY-concentrated?

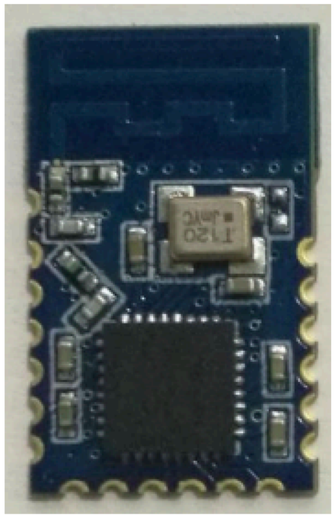
Strangely only in Maryland, *not DC or Virginia*? (There's like *2* in Virginia)

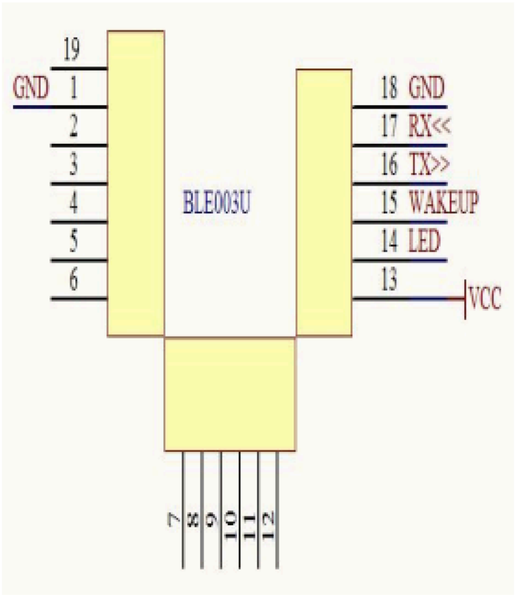


BLE003U FWIW

- A module that gets integrated into other stuff
- What stuff?
- IDK!
  - But probably cheap stuff where they don't care about changing the advertised ID?

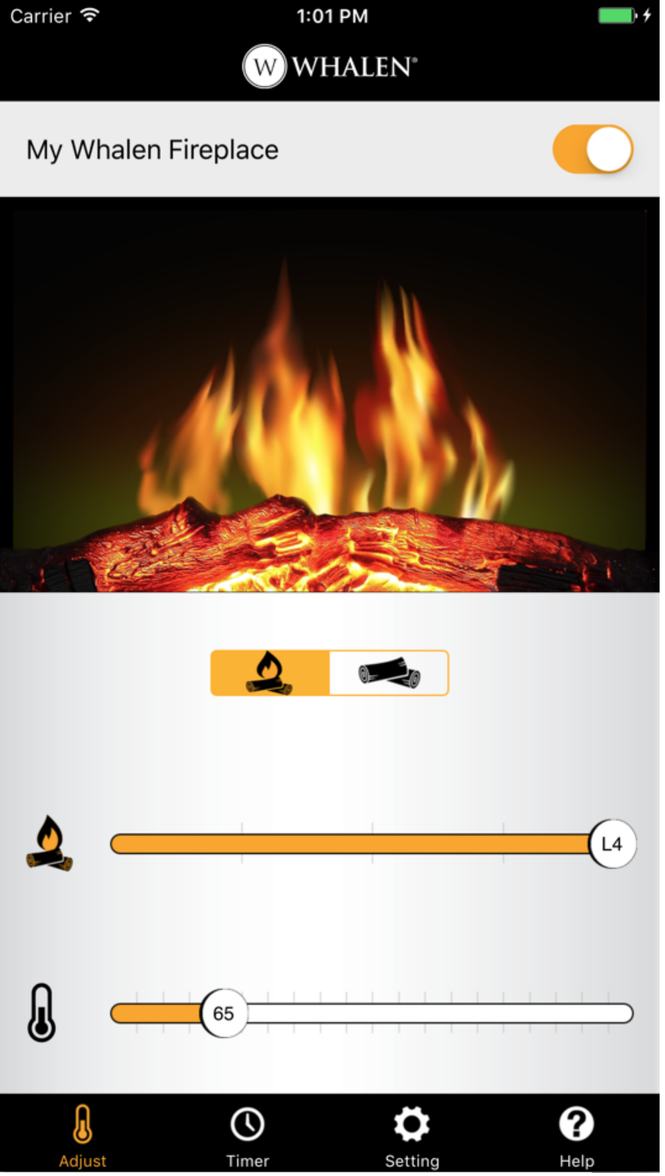
The **BLE003U** is a Bluetooth module which is lower energy consuming, compact designed size, stronger signal, quick start reading, higher reliability, higher cost-efficiency. This module highly integrates Bluetooth Low Energy radio, stack, profile and applications in a SoC. The BLE003U Bluetooth module is equipped with a variety of standard interfaces, UART, I2C, PWM, GPIO, etc. and also provides a Command Line Interface configuration, AT Instruction Set etc. User could easily integrate into their products , accelerate product development, shorten time to market. It provides users a low-cost & reliable wireless solutions. The module also offers flexible hardware interfaces for the different application.





BLE003U Module

https://fccid.io/2ATP5XLW-BLE003U/User-Manual/User-Manual-4353677



- ID: com.whalen.fireplace.ble003u
- Category: iOS Apps › Utilities
- OS: iOS 9.0 and up

https://appagg.com/ios/utilities/whalen-bluetooth-fireplace-27505128.html?hl=en

H6104 won't pair with phone (self.Govee)

submitted 2 years ago by UltraSalem

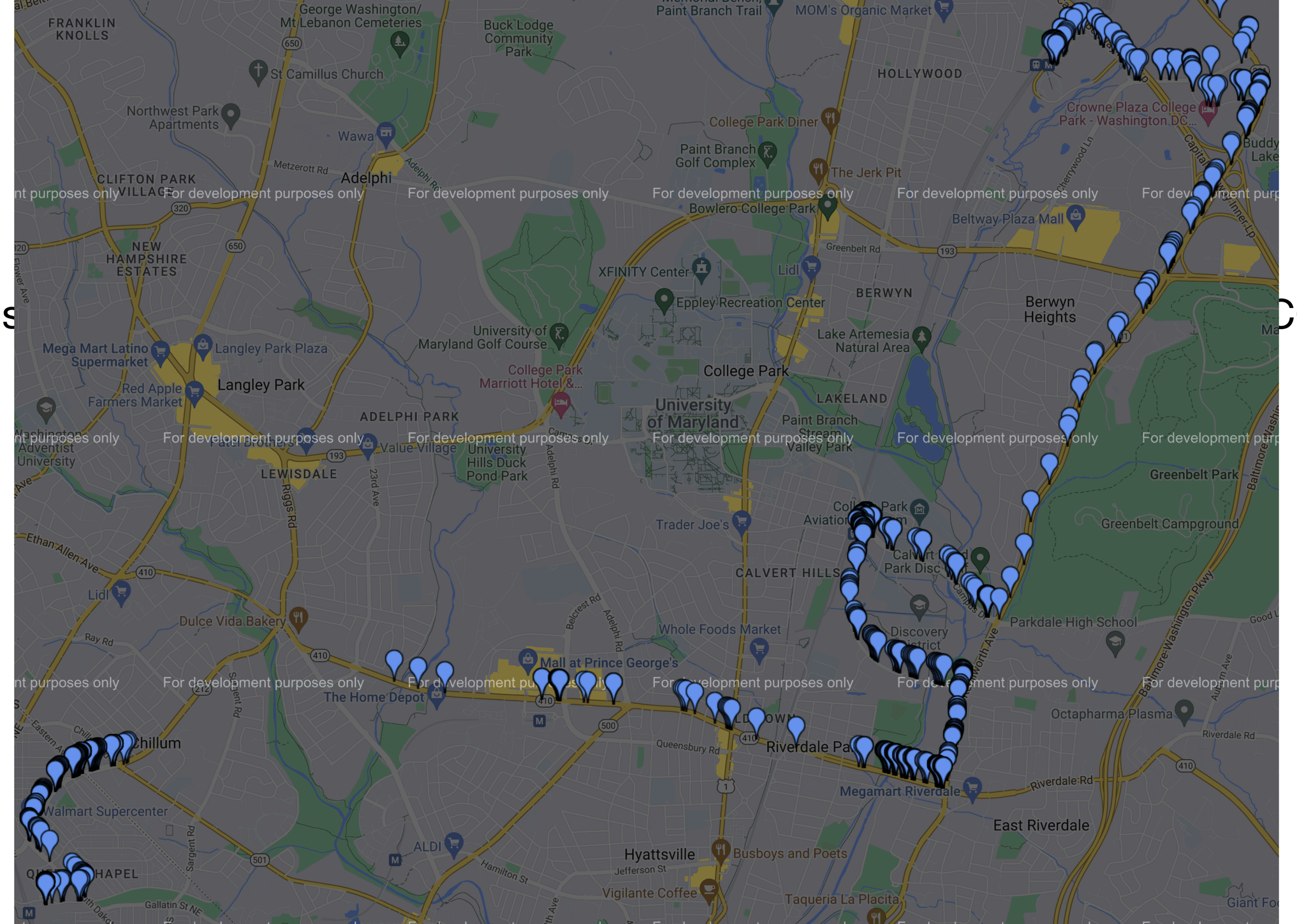
I'm having a weird issue with my brand new govee H6104 TV backlights. Everything powered up fine. App installed fine, created an account fine. But when I go to search for Bluetooth device, nothing comes up in the app. I then search "all Bluetooth devices" in the app, and nothing shows up. In my phone's Bluetooth settings (not the govee app) I can see BLE003u as a device, and when I turn off the power to the backlights that device disappears. So I am assuming it's them. But in the app, nothing is showing up. Are there any region locks or anything on it? My girlfriend bought the lights for me as a birthday present off Amazon AU, as we're in Australia. But it shipped from the US and the included plug was US. It supported Australian voltage so I just plugged it in with an adapter and it was happy to power up.

https://www.reddit.com/r/Govee/comments/l9ch0o/h6104_wont_pair_with_phone/

What other stuff?!?!
Inquiring minds want to know!

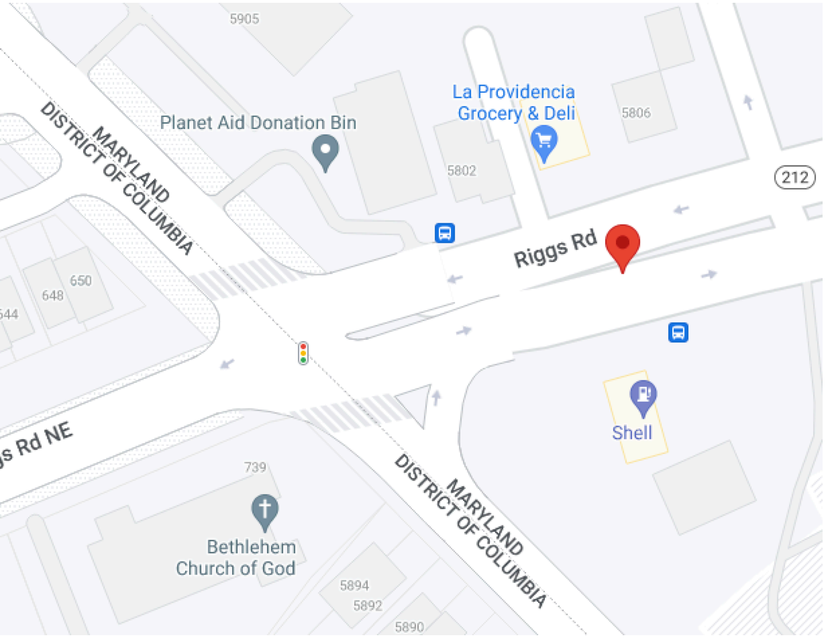
- Bus route due to disrupted metro on 8-14-2023 coming back from DEF CON

- Bus CON

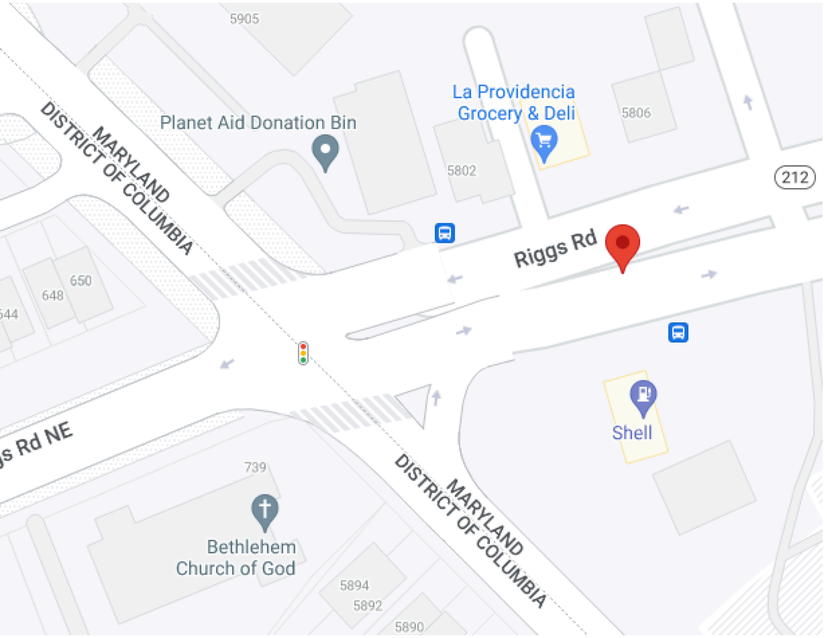


FRANKLIN KNOLLS
George Washington/ Mt Lebanon Cemeteries
Buck Lodge Community Park
Paint Branch Trail
MOM's Organic Market
HOLLYWOOD
St Camillus Church
Northwest Park Apartments
Wawa
College Park Diner
Crowne Plaza College Park - Washington DC...
Paint Branch Golf Complex
The Jerk Pit
CLIFTON PARK VILLAGE
Adelphi
Metzerott Rd
Bowlero College Park
Beltway Plaza Mall
NEW HAMPSHIRE ESTATES
Greenbelt Rd
XFINITY Center
Lidl
BERWYN
Eppley Recreation Center
Berwyn Heights
University of Maryland Golf Course
Lake Artemesia Natural Area
Mega Mart Latino Supermarket
Langley Park Plaza
College Park Marriott Hotel &...
College Park
Langley Park
Red Apple Farmers Market
LAKELAND
University of Maryland
ADELPHI PARK
Paint Branch Stream Valley Park
Value Village
University Hills Duck Pond Park
LEWISDALE
Greenbelt Park
Trader Joe's
Greenbelt Campground
Ethan Allen Ave
CALVERT HILLS
Lidl
Dulce Vida Bakery
Whole Foods Market
Parkdale High School
Discovery District
Mall at Prince George's
The Home Depot
Octapharma Plasma
Riverdale Rd
Queensbury Rd
Riverdale Pa
Megamart Riverdale
East Riverdale
Walmart Supercenter
ALDI
Hyattsville
Busboys and Poets
Jefferson St
Vigilante Coffee
Taqueria La Placita
Hamilton St
Gallatin St NE
Sargent Rd
Riggs Rd
Adelphi Rd
Belcrest Rd
Ray Rd
Baltimore-Washington Pkwy
Auburn Ave
Flower Ave
Sherrywood Ln
Capital Wy Inner Lp

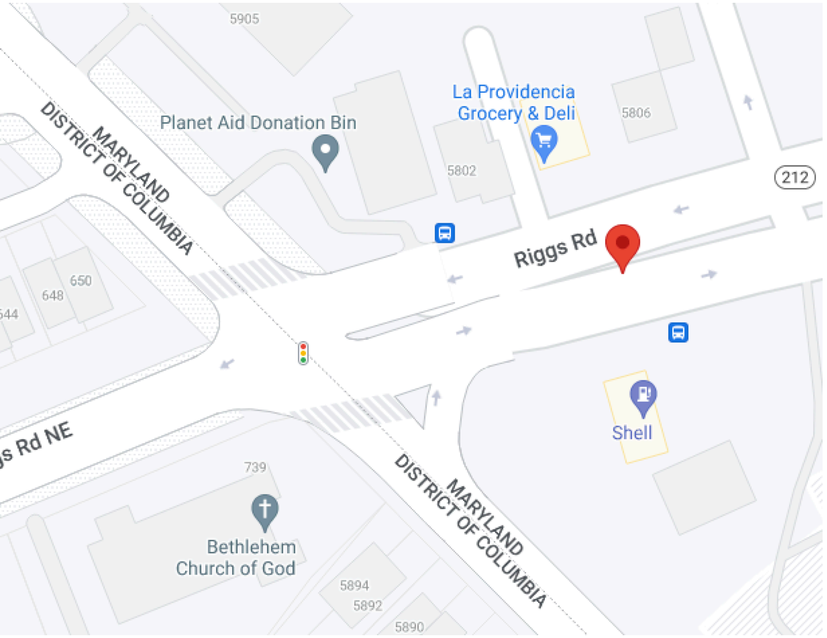
Frequently at Gas Stations & Liquor or Convenience Stores

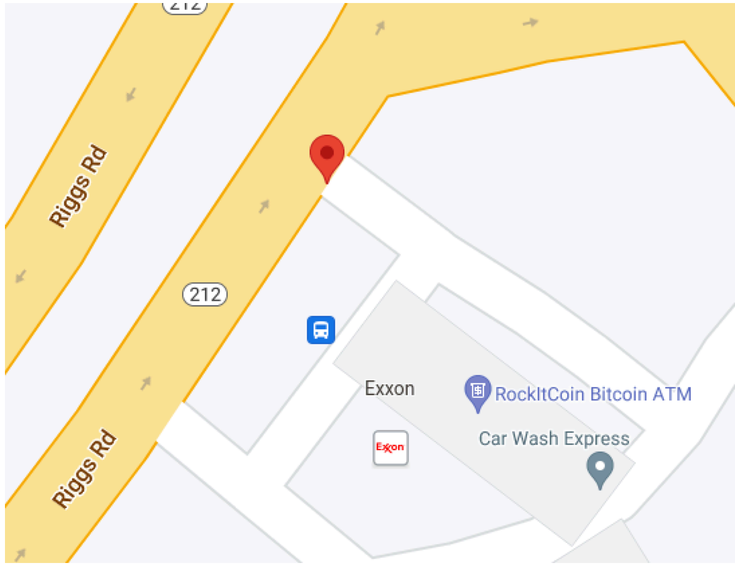


Frequently at Gas Stations & Liquor or Convenience Stores

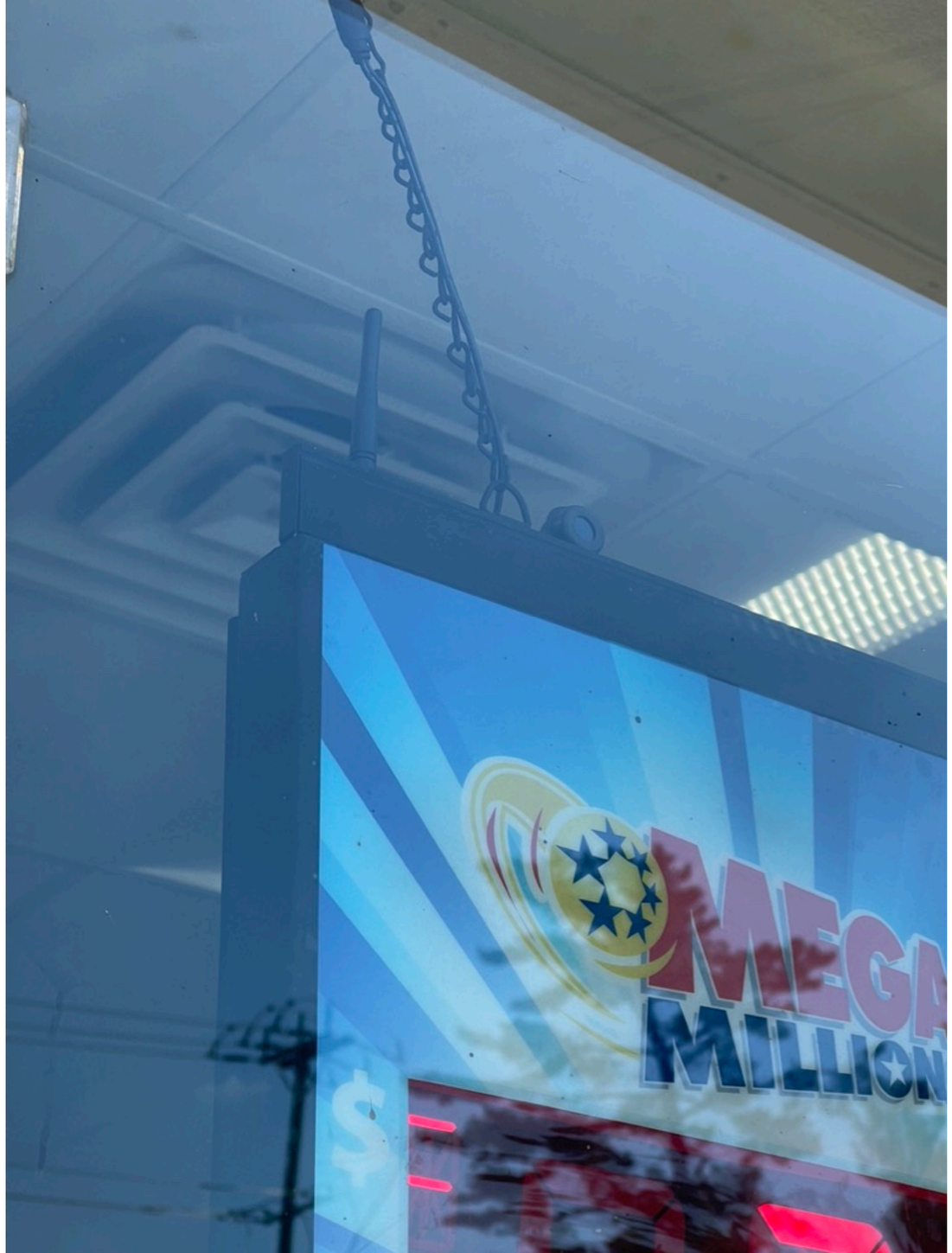


Frequently at Gas Stations & Liquor or Convenience Stores





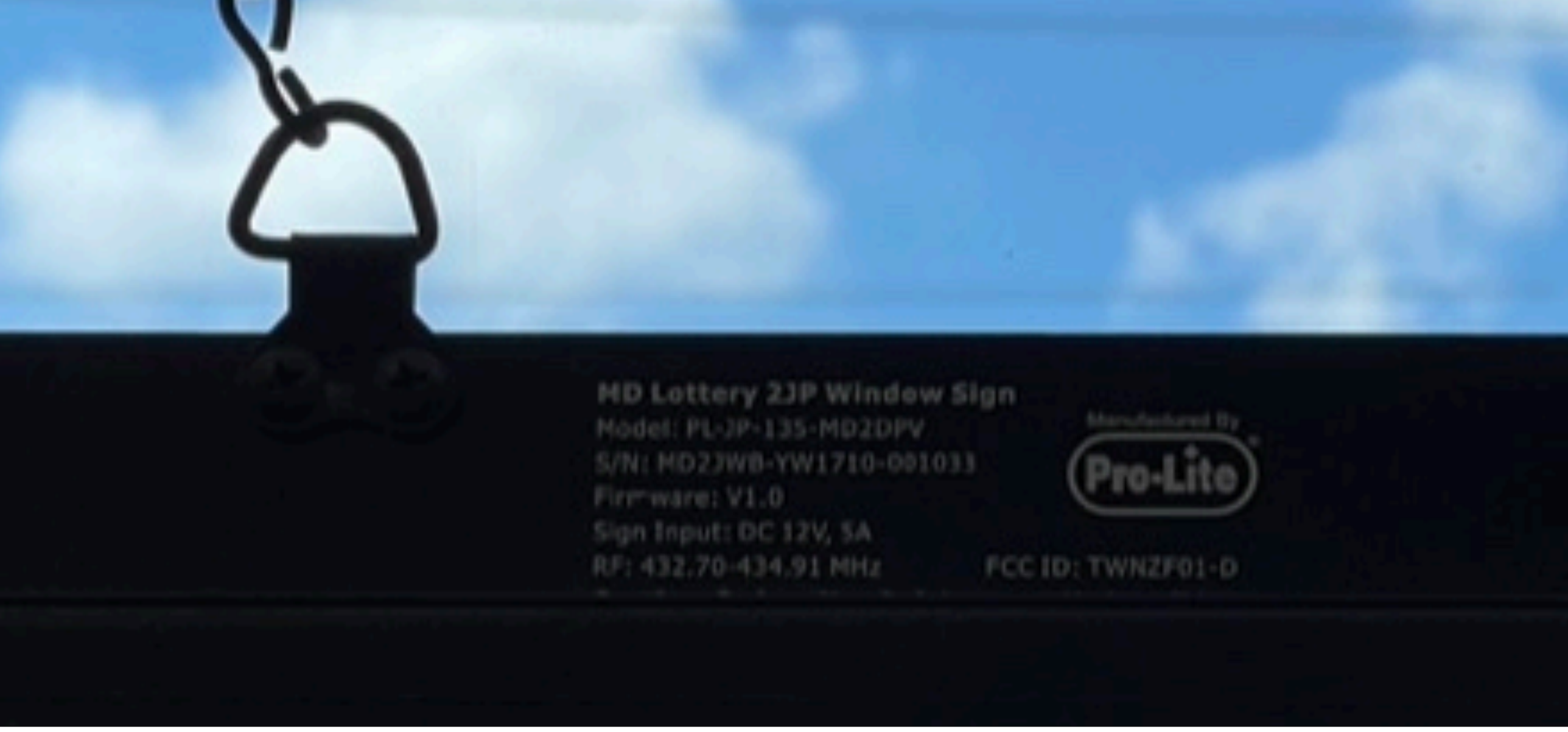
MEGA MILLIONS
$ FRI 20
MILLION
POWER BALL
$ SAT 264
MILLION
WARNING: Cigar smoking can cause lung cancer and heart disease.
BACKWOODS
ALWAYS TRUE
FREE RIDE GUARANTEED!
SIGN UP TODAY FOR FREE!
KINDA OUT HERE
Brisk
SAFEWAY

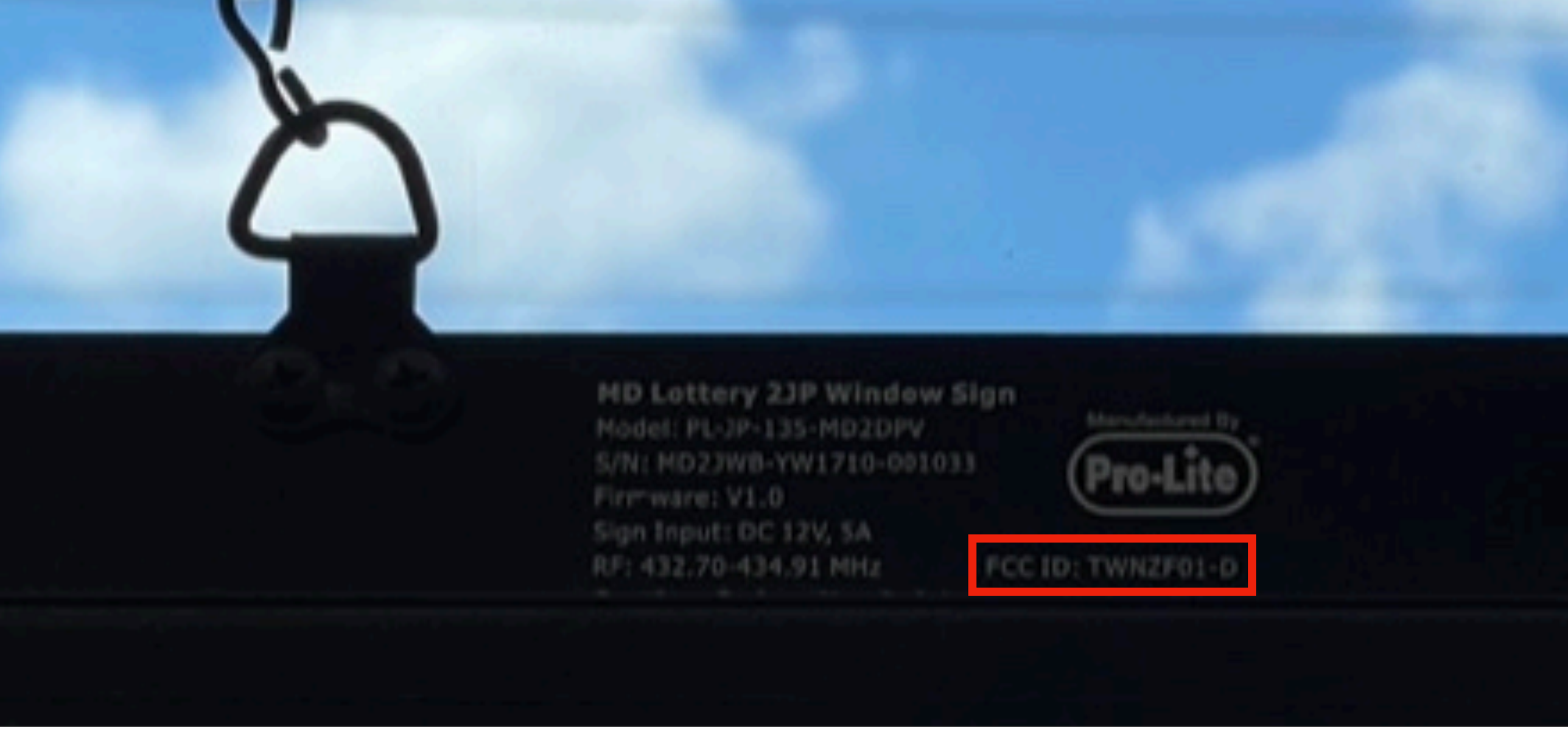

MEGA
MILLION

MEGA
MILLIONS
POWERBALL
Please play responsibly

Natural experiment!

Status: Elated!


MD Lottery 2JP Window Sign
Model: PL-JP-135-MD2DPV
S/N: MD2JW8-YW1710-001033
Firmware: V1.0
Sign Input: DC 12V, 5A
RF: 432.70-434.91 MHz
FCC ID: TWNZF01-D
Manufactured By
Pro-Lite


MD Lottery 2JP Window Sign
Model: PL-JP-135-MD2DPV
S/N: MD2JW8-YW1710-001033
Firmware: V1.0
Sign Input: DC 12V, 5A
RF: 432.70-434.91 MHz
Manufactured By
Pro-Lite
FCC ID: TWNZF01-D

Operating Frequencies

Device operates within approved CDMA 5,450 UP |

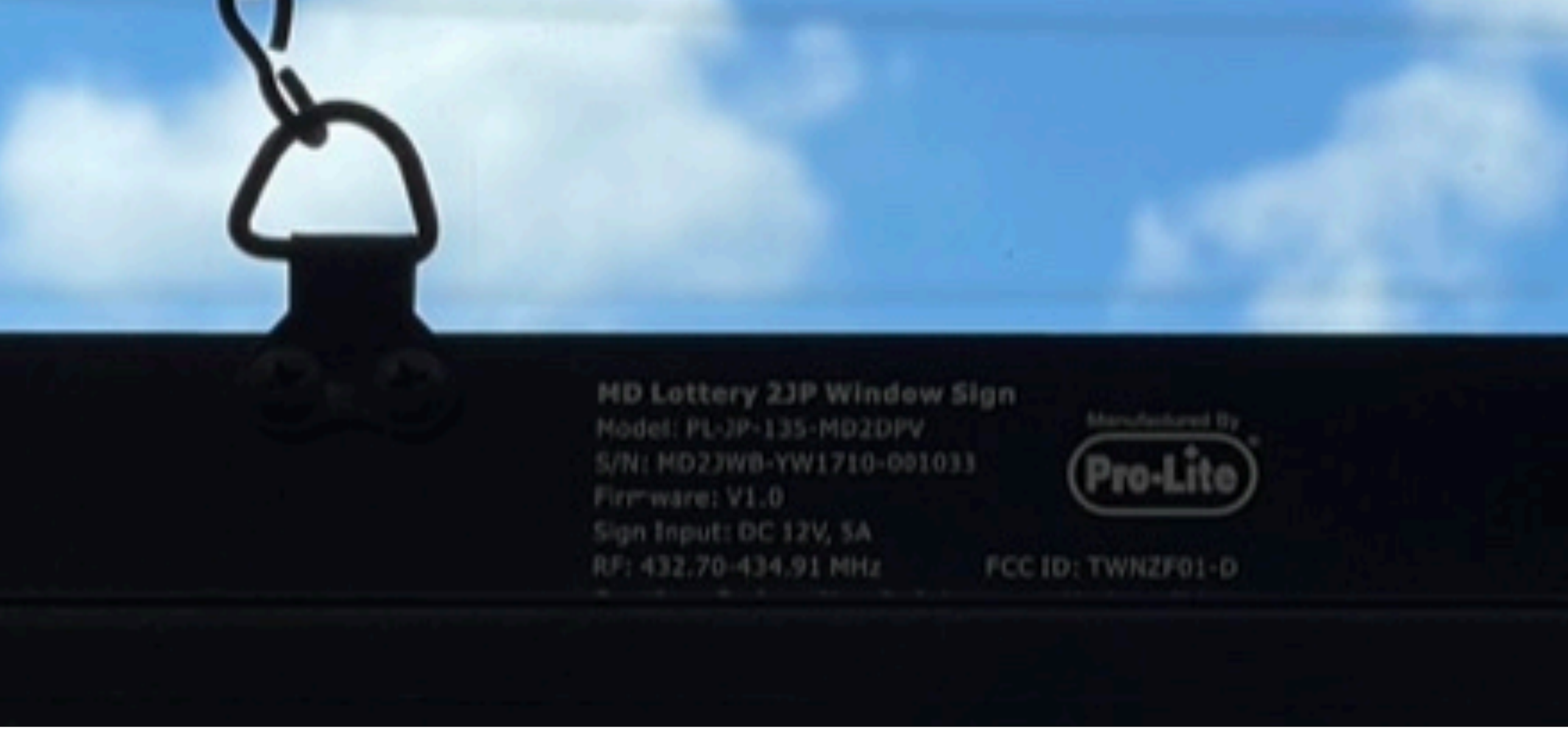
Frequency Range
432.7-434.91 MHz
432.7-434.91 MHz

Operating Frequencies

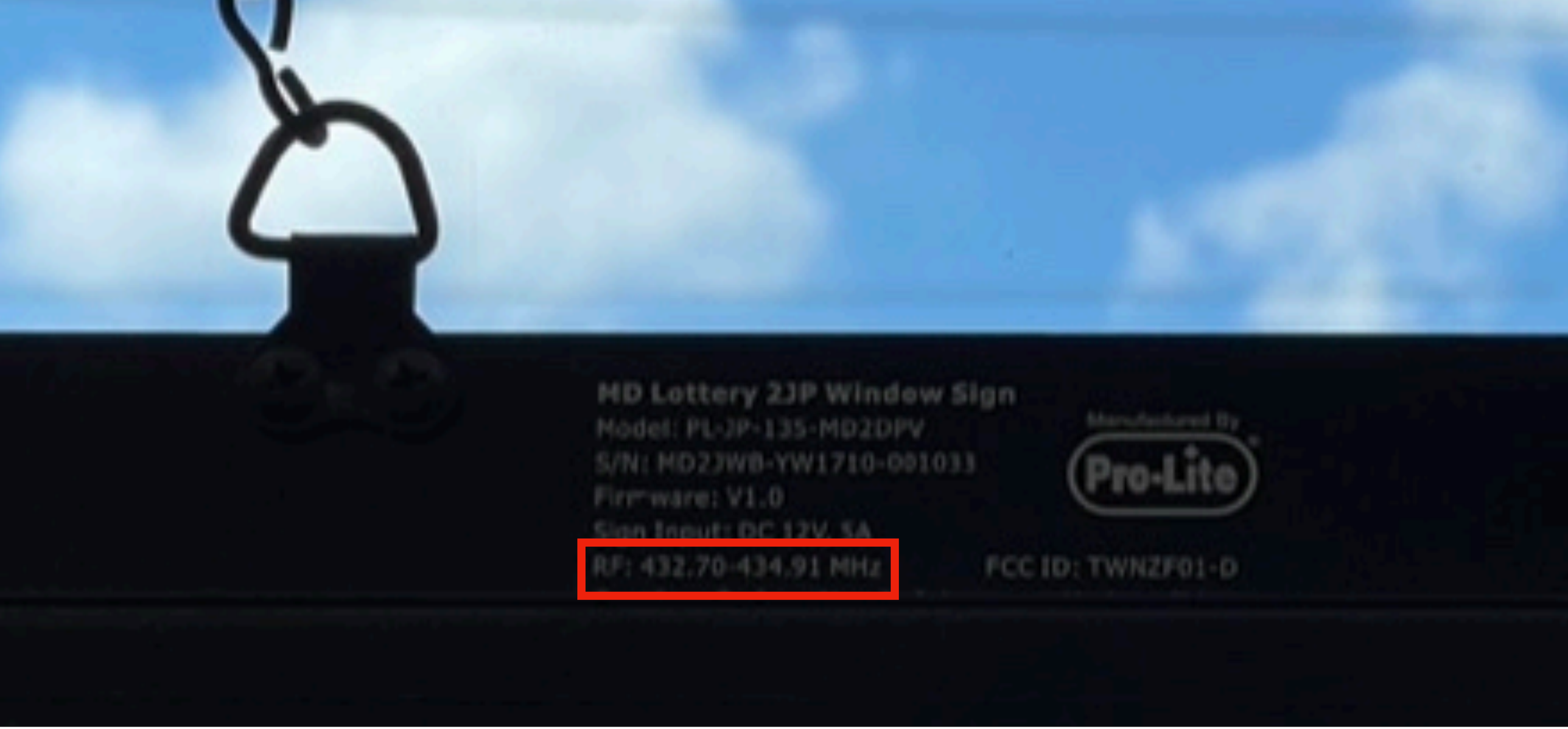
Device operates within approved CDMA 5,450 UP |

Frequency Range
432.7-434.91 MHz
432.7-434.91 MHz

OH NOES!😱

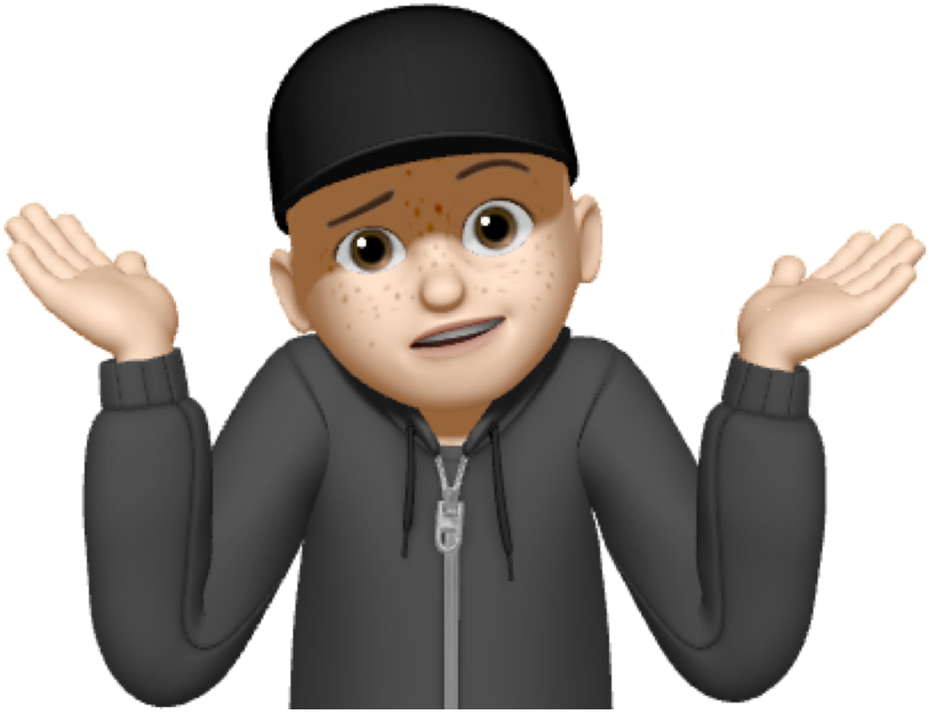

MD Lottery 2JP Window Sign
Model: PL-JP-135-MD2DPV
S/N: MD2JW8-YW1710-001033
Firmware: V1.0
Sign Input: DC 12V, 5A
RF: 432.70-434.91 MHz
FCC ID: TWNZF01-D
Manufactured By
Pro-Lite

OH NOES!😱


MD Lottery 2JP Window Sign
Model: PL-JP-135-MD2DPV
S/N: MD2JW8-YW1710-001033
Firmware: V1.0
Sign Input: DC 12V, 5A
RF: 432.70-434.91 MHz
Manufactured By
Pro-Lite
FCC ID: TWNZF01-D

OH NOES!😱

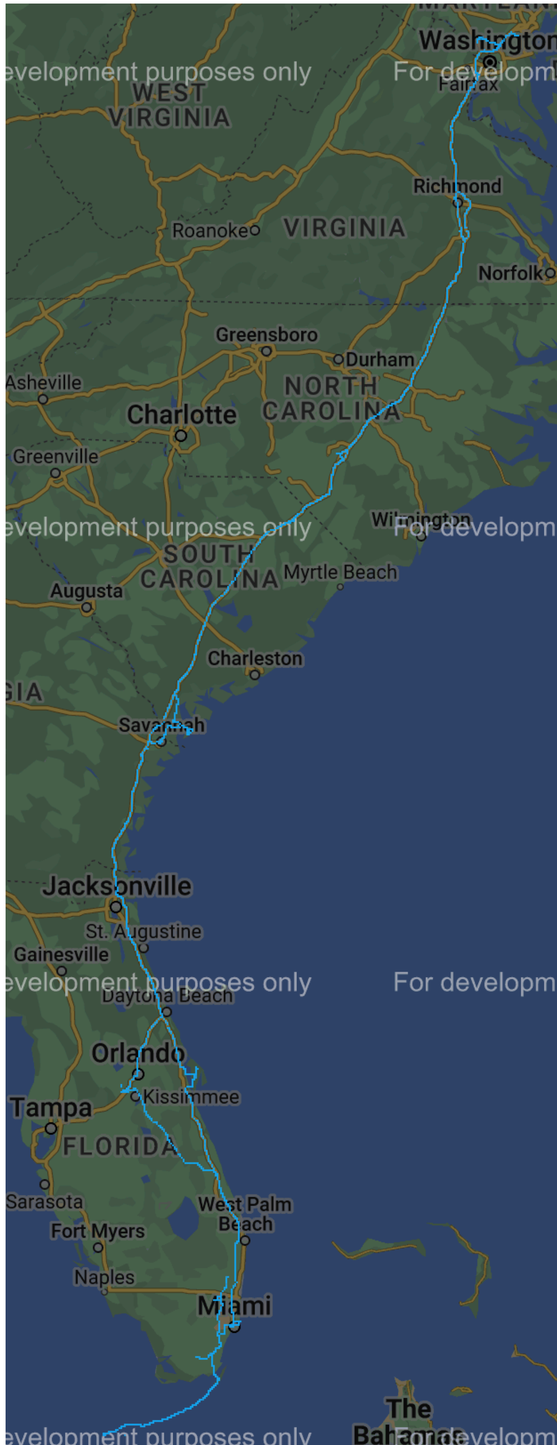
Status: VEXED!

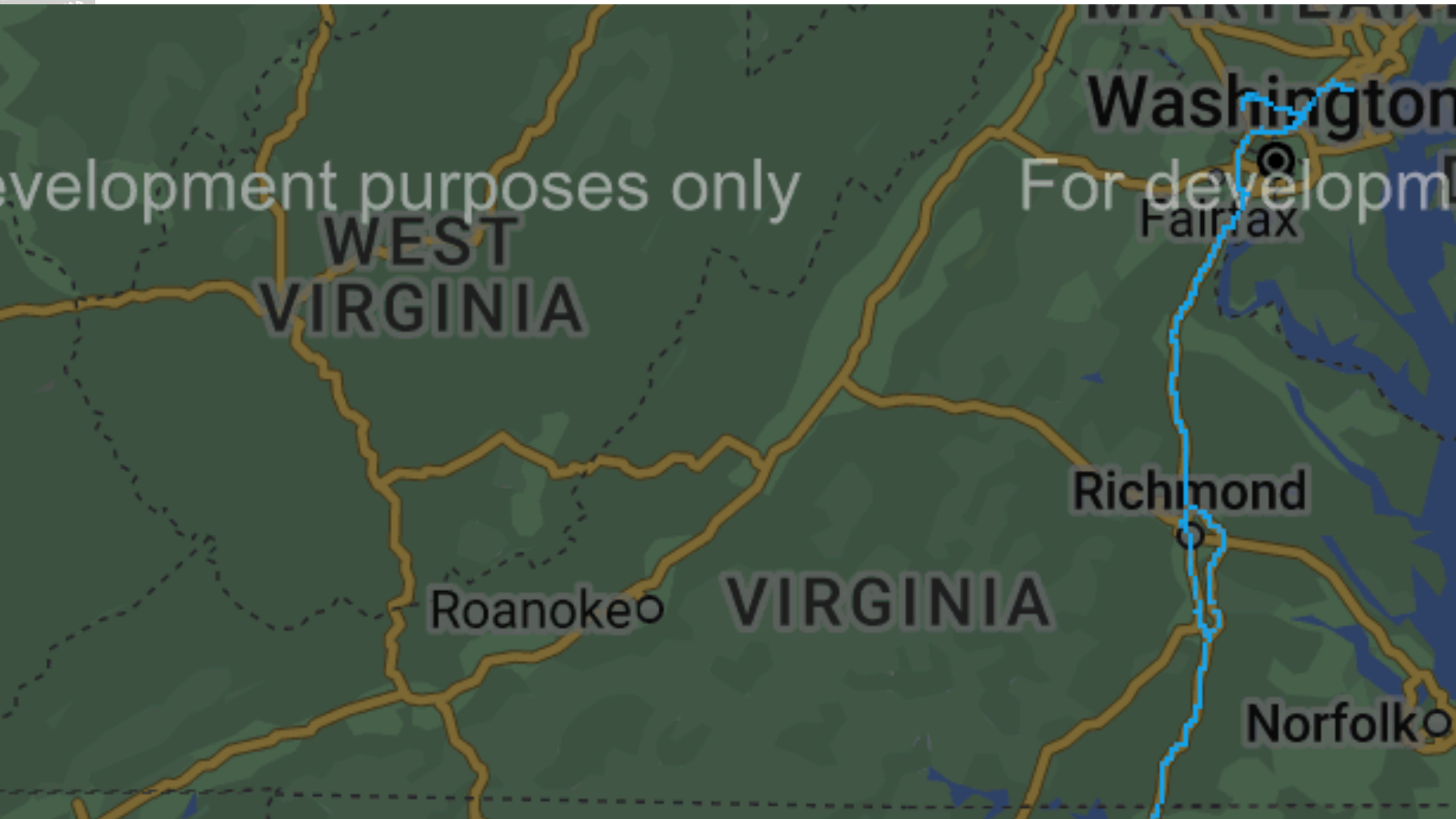


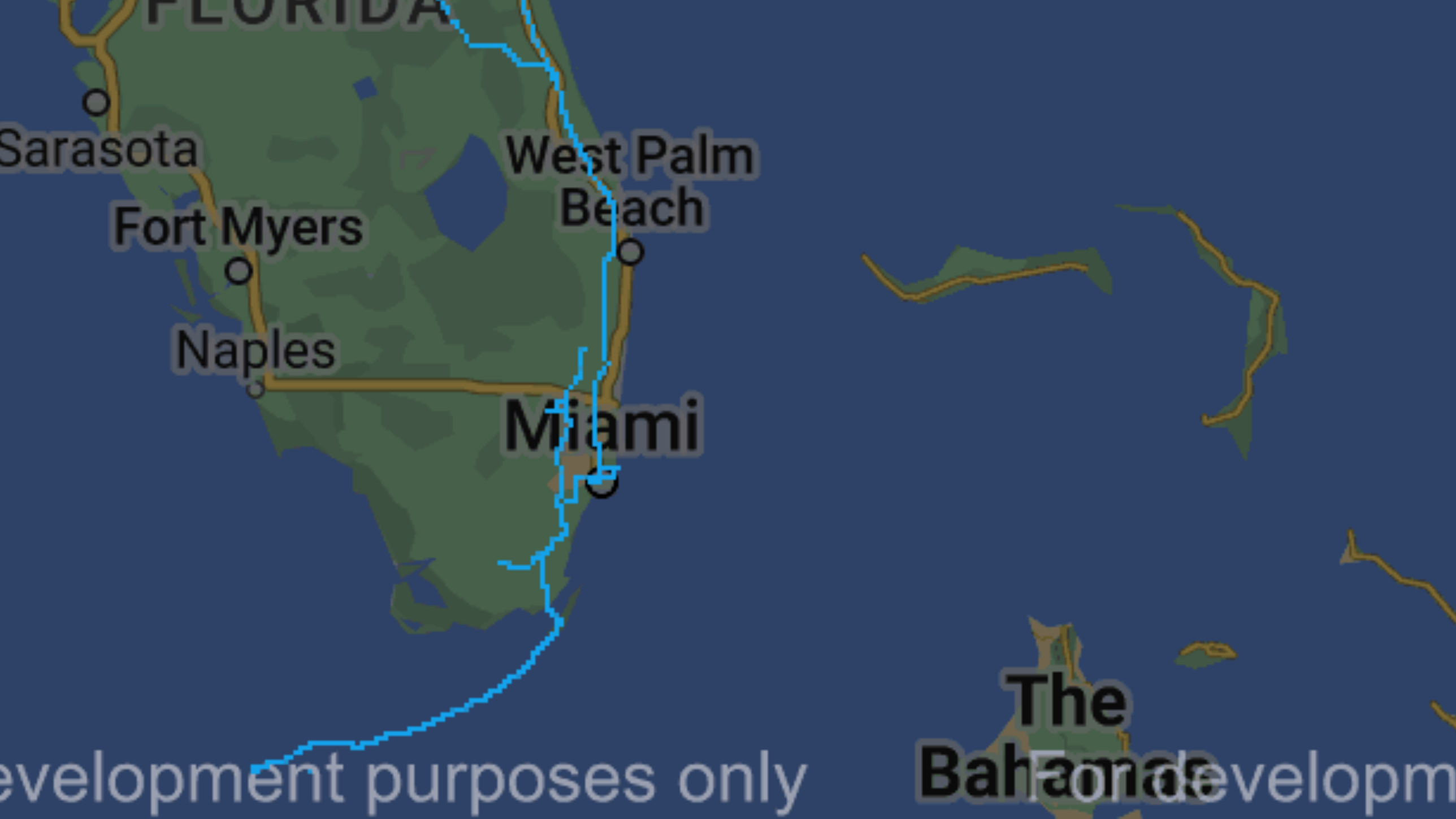
Status: VEXED!

Road Trip!

- Washington DC -> Savannah GA -> Orlando FL -> Key West FL -> Miami FL -> And Back to DC (by way of Cape Canaveral)

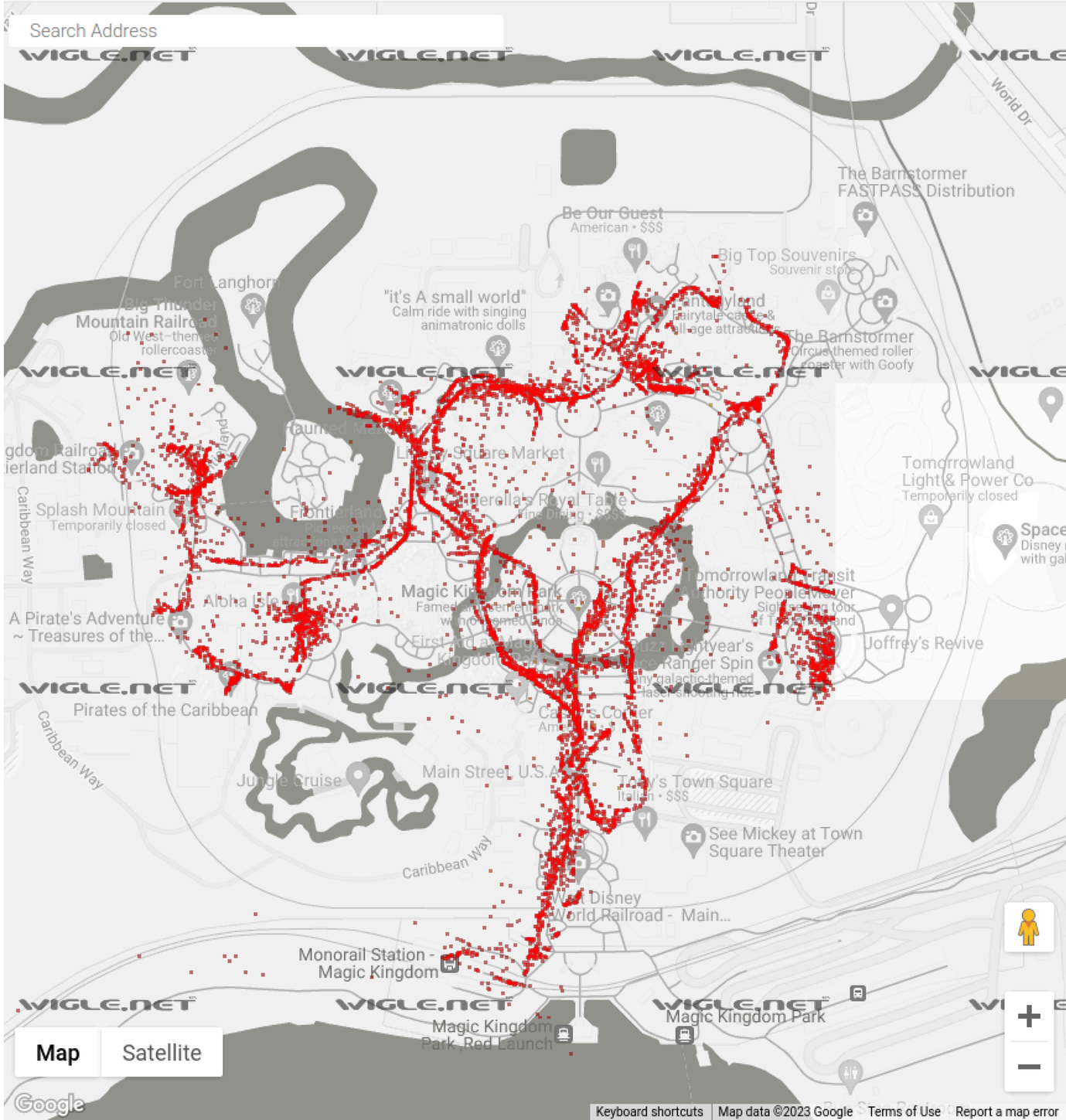



velopment purposes only
For developm
Washington
Fairfax
WEST
VIRGINIA
Richmond
Roanoke
VIRGINIA
Norfolk


FLORIDA
Sarasota
Fort Myers
Naples
West Palm Beach
Miami
The Bahamas
evelopment purposes only
evelopm

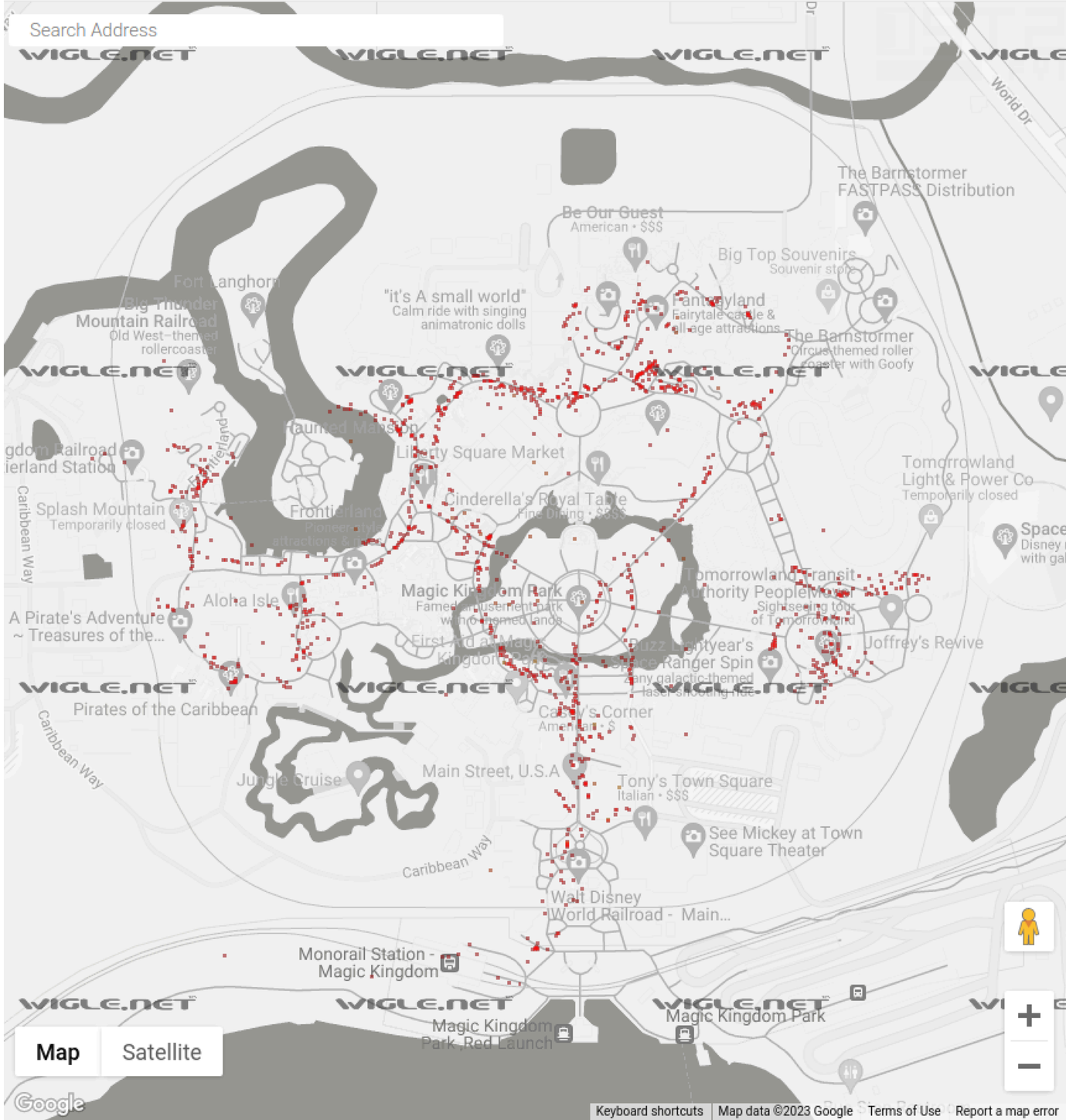
USA - Disney World

- My data only, all BT, including those without names



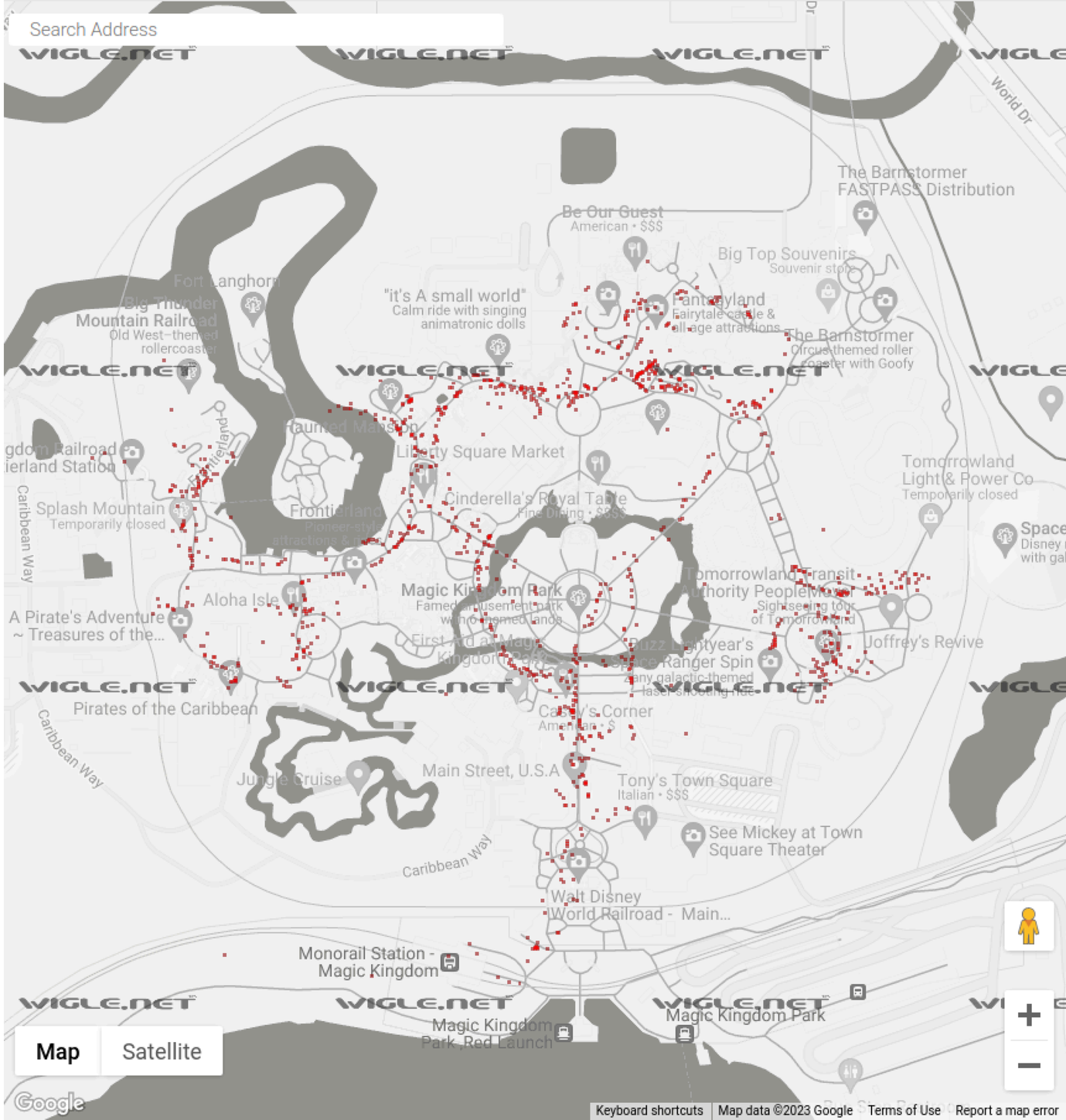
USA - Disney World

- My data only, only advertising a name
- One entry stands out as being very common: "DSNYMBLE"



USA - Disney World

- Only DSNYMBLE



https://disneyworld.disney.go.com/faq/star-wars-galaxys-edge/bluetooth-low-energy/
https://disneyworld.disney.go.com/faq/star-wars-galaxys-edge/bluetooth-privacy/

USA - Disney World

- Only DSNYMBLE

Star Wars: Galaxy's Edge – Frequently Asked Questions

Q: What is Bluetooth® Low Energy (BLE) and how is it used at the Walt Disney World Resort?

A: Bluetooth technology is a communication standard designed for short-range data exchange between devices. You may be familiar with it as it is commonly a feature in mobile phones, smart watches and even cars. BLE is a form of Bluetooth communication that requires only low power consumption, which is ideal for some kinds of device-to-device communication that only require small amounts of information to be sent or received.

Select locations throughout the Walt Disney World Resort (the "Resort") include BLE beacons, which are small radio transmitters. These BLE beacons may communicate with certain other Bluetooth-enabled devices, such as mobile phones or "smart" devices that have Bluetooth capability. The exchange of information is designed to allow you to enable certain interactive or personalized experiences and to improve the Guest experience.

Guests can visit the Resort without using BLE; however, certain features of the Resort experience are dependent upon BLE, including some personalized offerings. To participate using your Bluetooth-enabled mobile device, follow these 2 steps: (1) download the My Disney Experience app or the Play Disney Parks app (collectively the "Walt Disney World apps") to your mobile device, and (2) enable Bluetooth services using your device settings. Certain personalized experiences may also require that Guests be signed in to their Disney account on the app. For other BLE-enabled products, including, for example, Astromech Droid Units or Made with Magic Connected Ear Hats, the device will automatically enable the Bluetooth technology when the device is turned on.

https://disneyworld.disney.go.com/faq/star-wars-galaxys-edge/bluetooth-low-energy/
https://disneyworld.disney.go.com/faq/star-wars-galaxys-edge/bluetooth-privacy/

USA - Disney World

- Only DSNYMBLE

Star Wars: Galaxy's Edge – Frequently Asked Questions

Q: What information does the Walt Disney World Resort collect through Bluetooth® Low Energy (BLE) and how is this information used?

A: BLE beacons at locations within the Walt Disney World Resort (the "Resort") communicate with the My Disney Experience app or the Play Disney Parks app (collectively, "Walt Disney World apps") on your Bluetooth-enabled mobile device and certain other BLE-enabled devices or products, such as the Astromech Droid Units (collectively "your BLE-enabled devices") to trigger certain effects or experiences on your BLE-enabled devices.

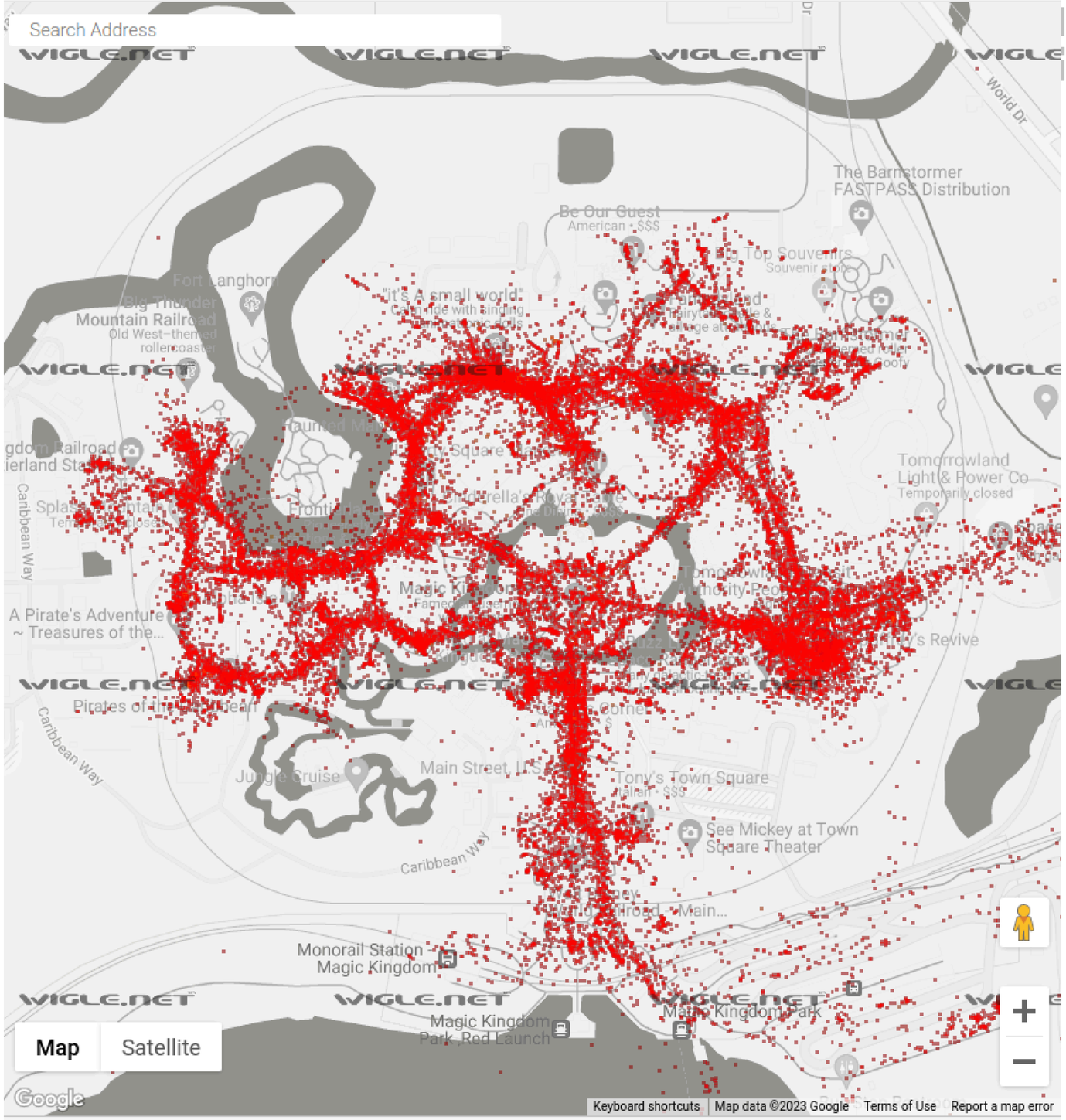
In addition, your BLE-enabled devices may also broadcast data that, when received by our BLE beacons, may allow us to provide other interactive or personalized experiences. For example, when you use the Play Disney Parks app at *Star Wars: Galaxy's Edge*, certain functions performed with the app may trigger physical effects in the land. Our BLE beacons may also receive data broadcast by your BLE-enabled devices to determine your relative position and enable certain personalized experiences.

The security, integrity and confidentiality of your information are extremely important to us. We have implemented technical, administrative and physical security measures that are designed to protect Guest information from unauthorized access, disclosure, use and modification. From time to time, we review our security procedures to consider appropriate new technology and methods. Please be aware that, despite our best efforts, no security measures are perfect or impenetrable.

https://disneyworld.disney.go.com/faq/star-wars-galaxys-edge/bluetooth-low-energy/
https://disneyworld.disney.go.com/faq/star-wars-galaxys-edge/bluetooth-privacy/

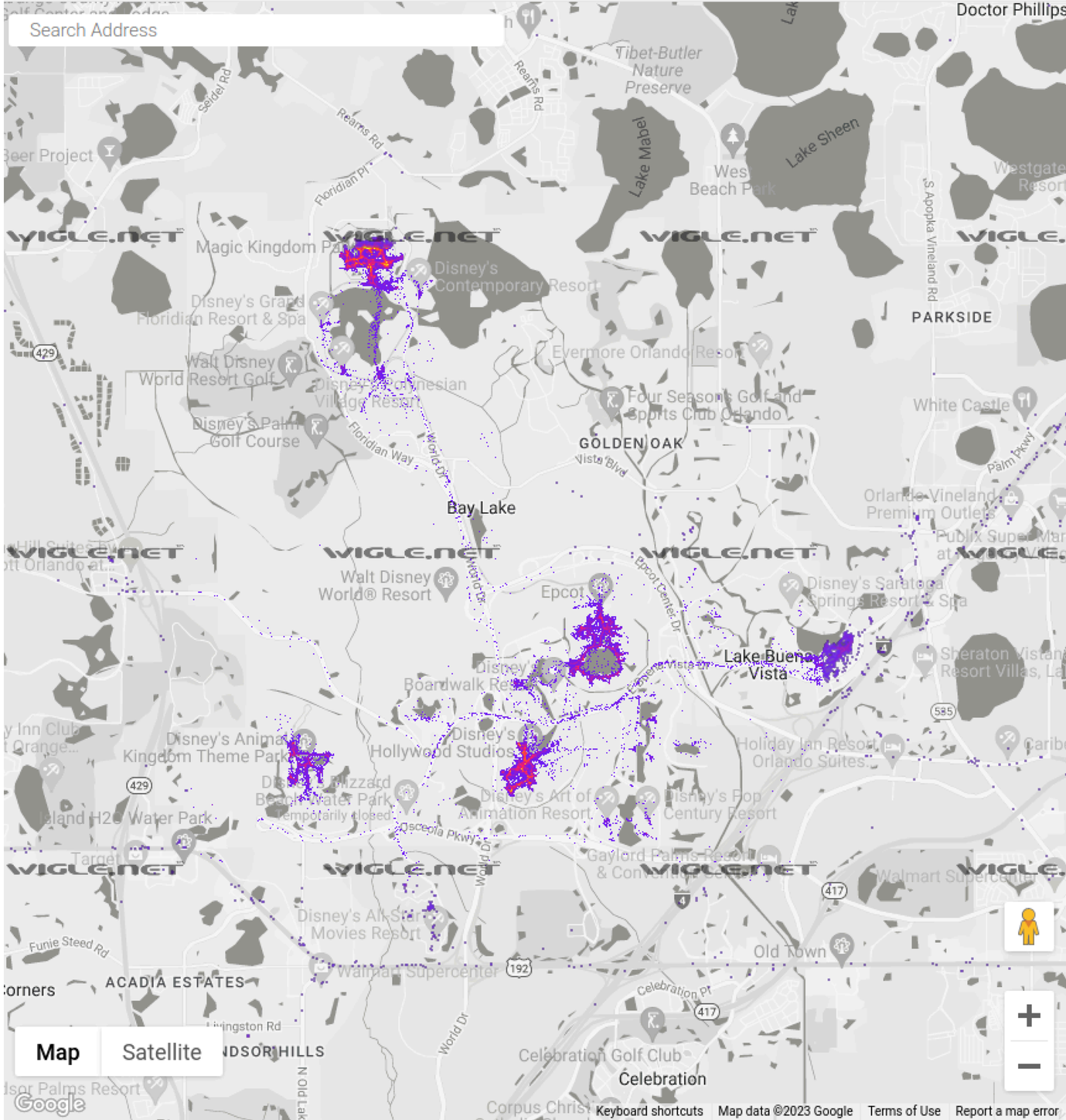
USA - Disney World

- Only DSNYMBLE
  - Everyone's WiGLE data, not just mine



USA - Disney World

- Only DSNYMBLE
  - Everyone, not just me
    - Other parks

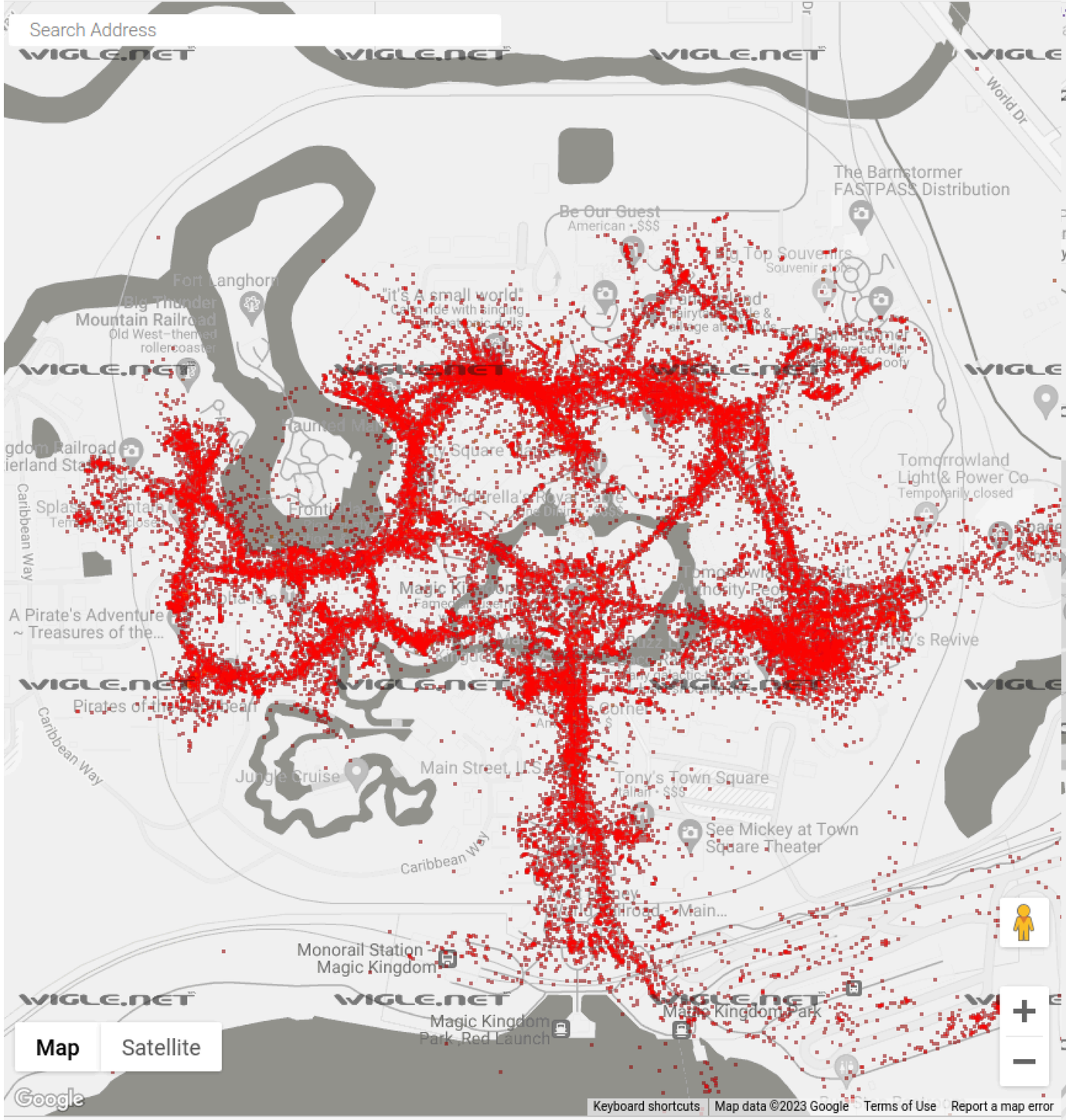


USA - Disney World

- Only DSNYMBLE
  - Everyone, not just me
    - Some use at resorts & buses?
    - Or do Magic Bands beacon?

USA - Disney World

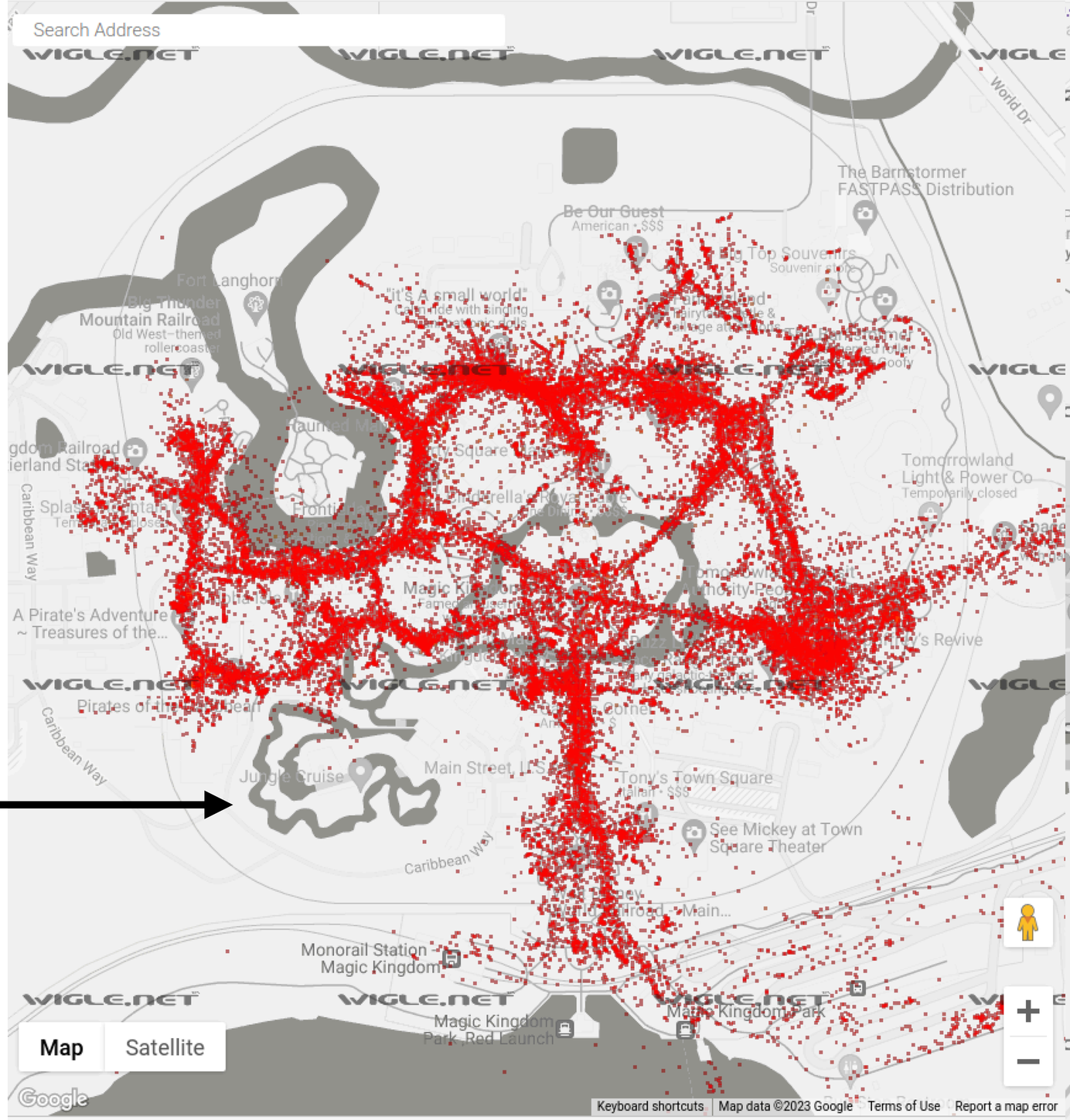
- Only DSNYMBLE
  - Everyone, not just me
    - Some use at resorts & buses?
    - Or do Magic Bands beacon?

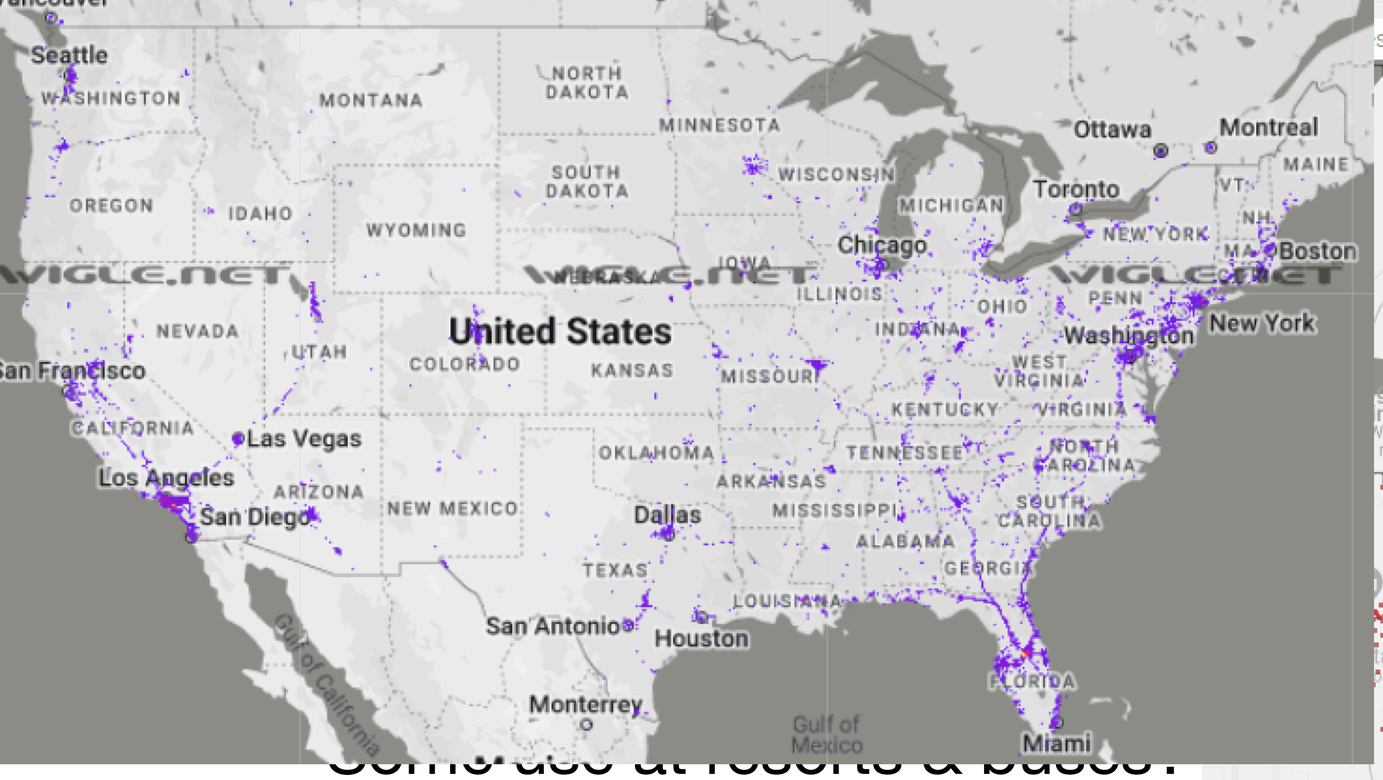


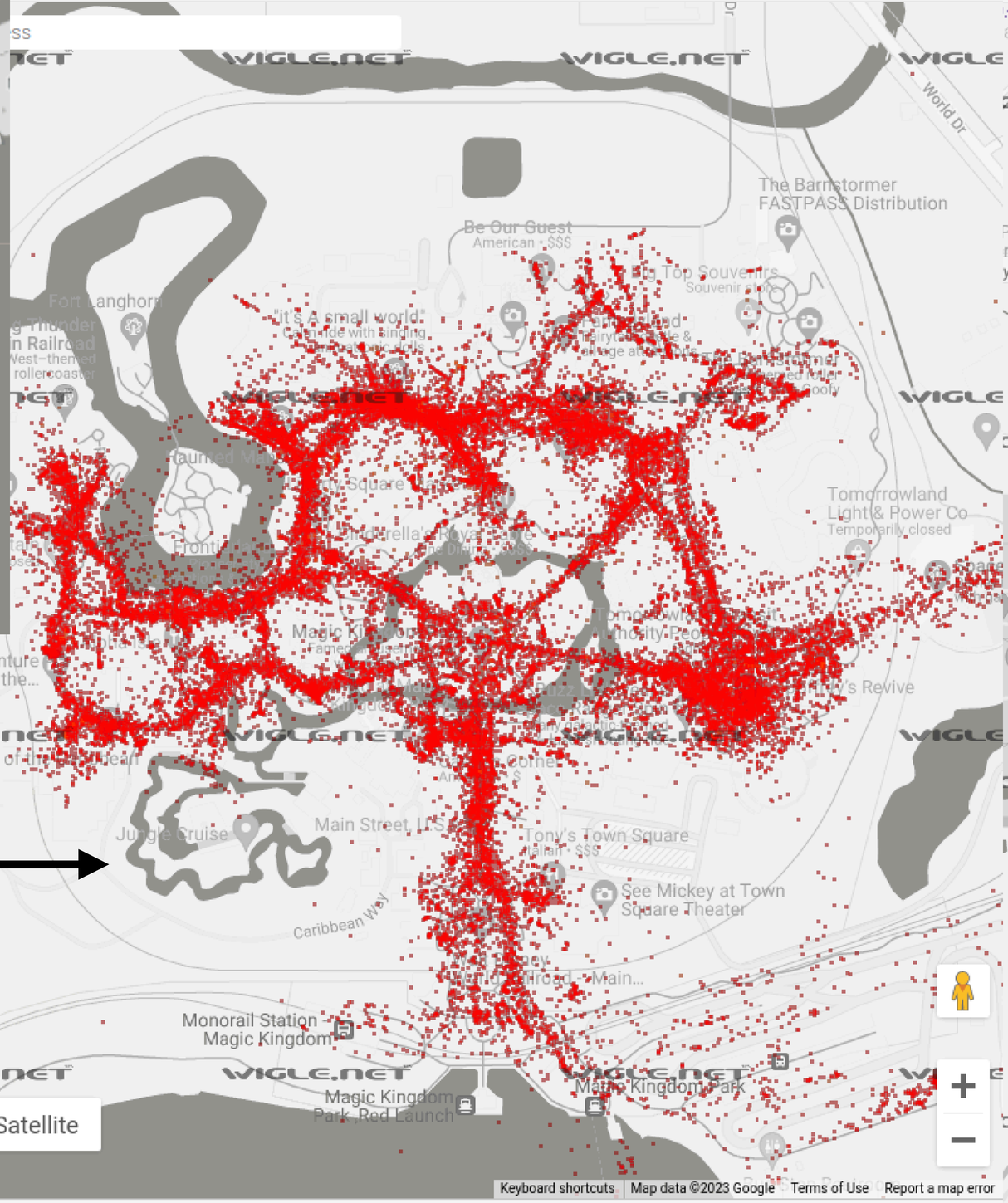
USA - Disney World

- Only DSNYMBLE
  - Everyone, not just me
    - Some use at resorts & buses?
    - Or do Magic Bands beacon?

At first I was inclined to think "no", because otherwise there should be evenly-distributed data in all areas of the park. But...



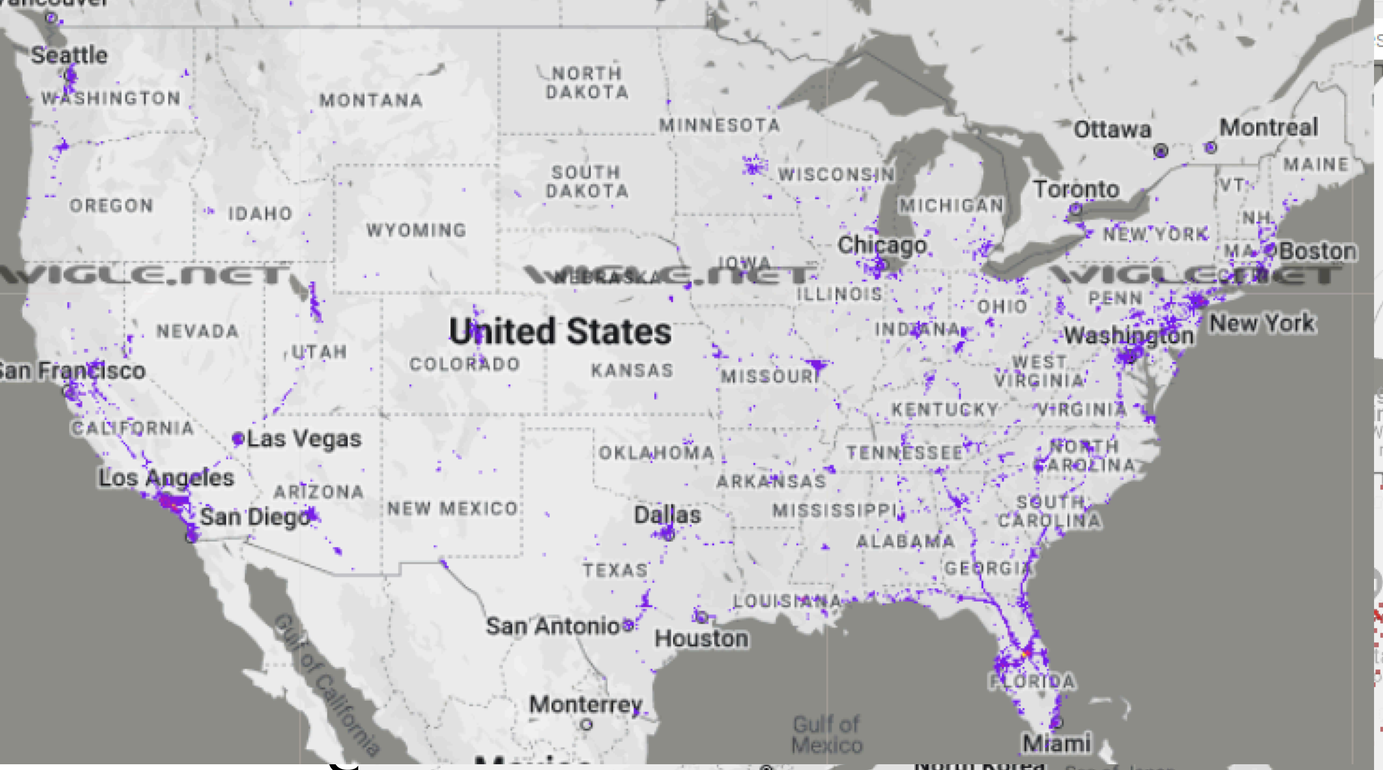




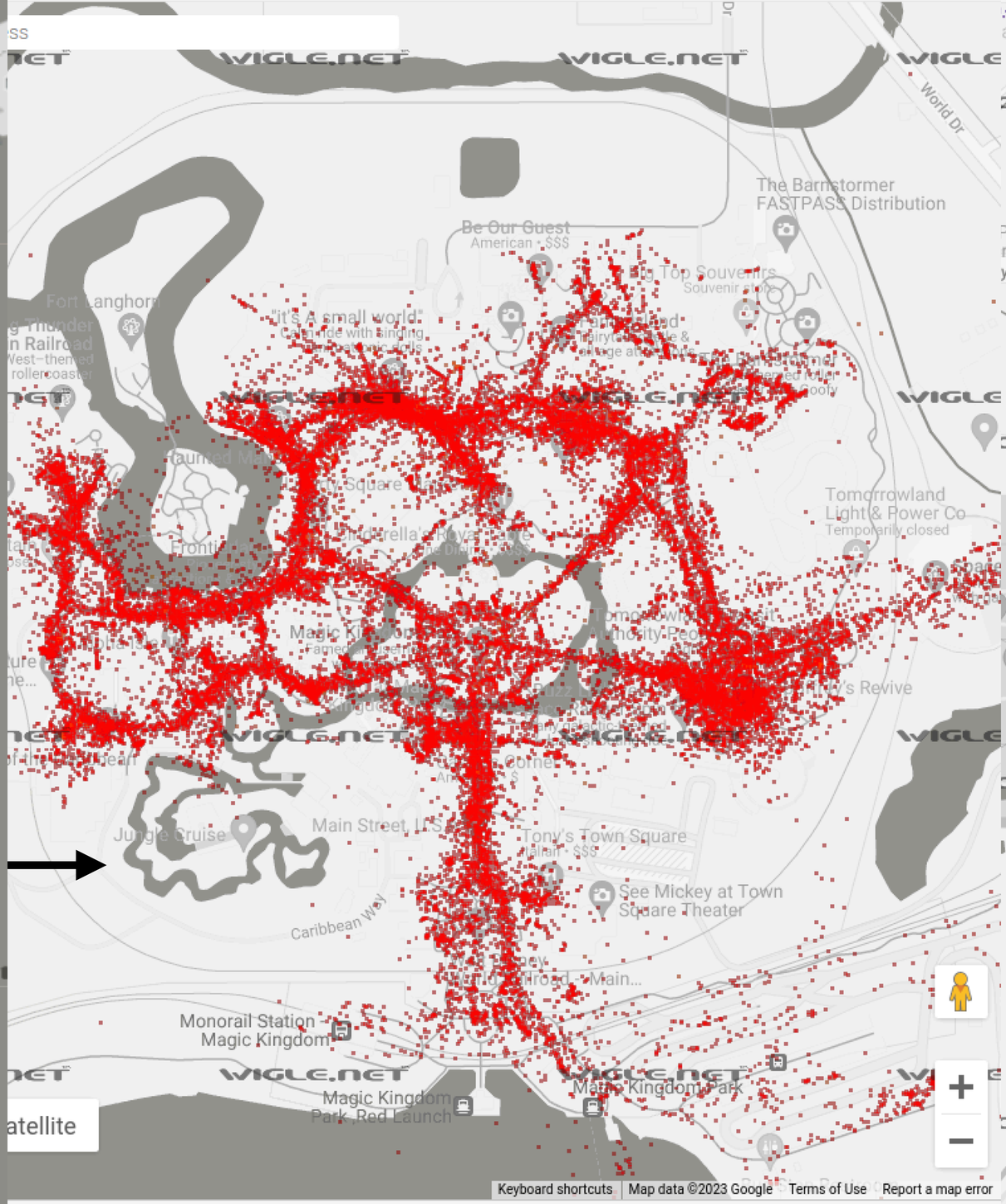
Some use at resorts & buses?

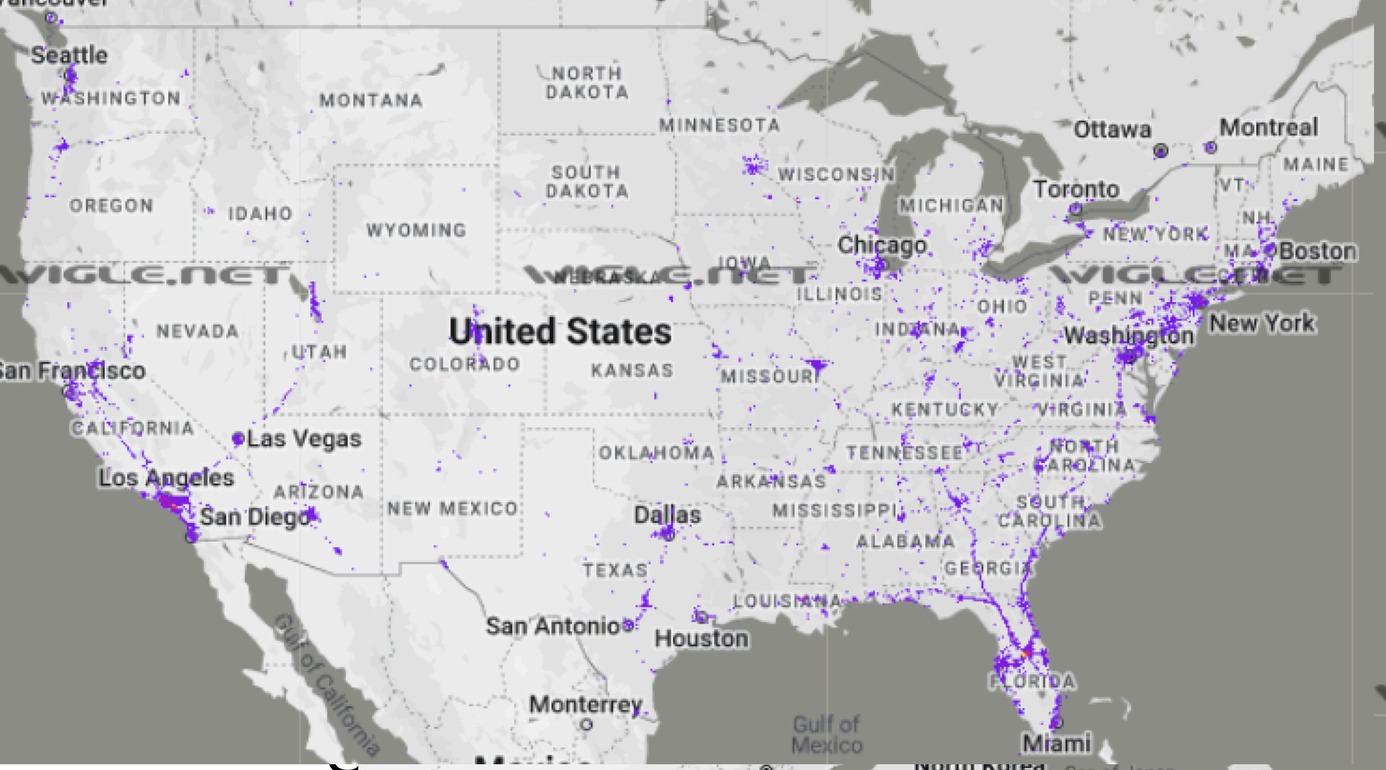
- Or do Magic Bands beacon?

At first I was inclined to think "no", because otherwise there should be evenly-distributed data in all areas of the park. But...

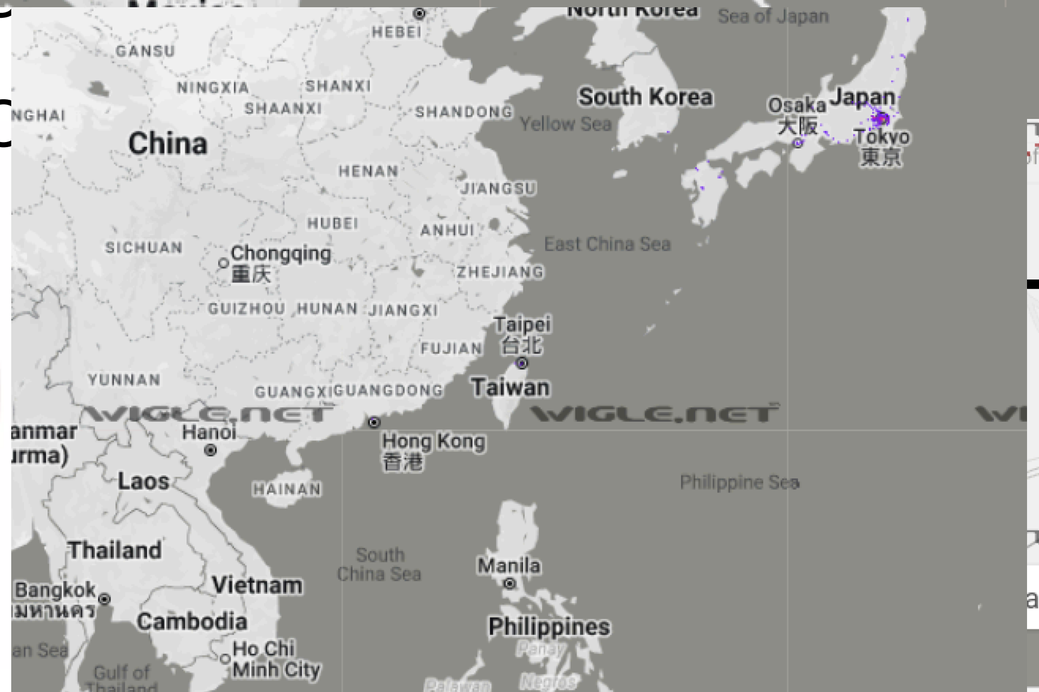

Seattle
WASHINGTON
MONTANA
NORTH DAKOTA
MINNESOTA
SOUTH DAKOTA
WISCONSIN
MICHIGAN
Ottawa
Montreal
Toronto
MAINE
VT.
NH.
MA
Boston
NEW YORK
OREGON
IDAHO
WYOMING
Chicago
IOWA
NEBRASKA
ILLINOIS
OHIO
PENN
Washington
New York
NEVADA
UTAH
COLORADO
KANSAS
MISSOURI
INDIANA
WEST VIRGINIA
KENTUCKY
VIRGINIA
San Francisco
CALIFORNIA
Las Vegas
OKLAHOMA
TENNESSEE
NORTH CAROLINA
Los Angeles
ARIZONA
NEW MEXICO
ARKANSAS
MISSISSIPPI
SOUTH CAROLINA
San Diego
Dallas
ALABAMA
GEORGIA
TEXAS
LOUISIANA
San Antonio
Houston
Gulf of California
FLORIDA
Monterrey
Gulf of Mexico
Miami
WIGLE.NET

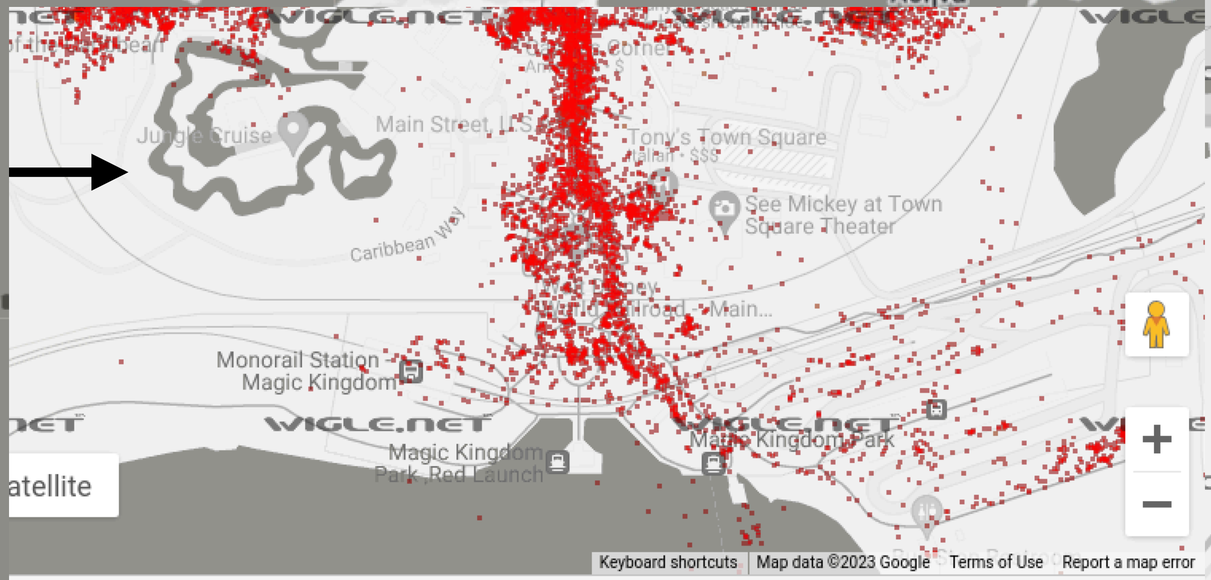
North Korea
Sea of Japan
HEBEI
GANSU
NINGXIA
SHANXI
SHAANXI
SHANDONG
South Korea
Osaka
Japan
大阪
Tokyo
東京
Yellow Sea
China
HENAN
JIANGSU
HUBEI
ANHUI
East China Sea
SICHUAN
Chongqing
重庆
ZHEJIANG
GUIZHOU
HUNAN
JIANGXI
Taipei
台北
FUJIAN
YUNNAN
GUANGXI
GUANGDONG
Taiwan
Hanoi
Hong Kong
香港
Laos
HAINAN
Philippine Sea
Thailand
South China Sea
Manila
Bangkok
Vietnam
Cambodia
Philippines
Ho Chi Minh City
Gulf of Thailand
WIGLE.NET


WIGLE.NET
The Barnstormer FASTPASS Distribution
Be Our Guest
American · $$$
Big Top Souvenirs
Souvenir shop
Fort Langhorn
it's A small world
Tomorrowland Light & Power Co
Temporarily closed
Tony's Revive
Jungle Cruise
Main Street, U.S.A.
Tony's Town Square
Italian · $$$
See Mickey at Town Square Theater
Caribbean Way
Monorail Station Magic Kingdom
Magic Kingdom Park Red Launch
Magic Kingdom Park
atellite
Keyboard shortcuts
Map data ©2023 Google
Terms of Use
Report a map error


Seattle
WASHINGTON
MONTANA
NORTH DAKOTA
MINNESOTA
SOUTH DAKOTA
WISCONSIN
MICHIGAN
OREGON
IDAHO
WYOMING
NEBRASKA
ILLINOIS
INDIANA
OHIO
PENN
NEW YORK
MAINE
VT.
NH.
MA
NEVADA
UTAH
COLORADO
KANSAS
MISSOURI
WEST VIRGINIA
KENTUCKY
VIRGINIA
CALIFORNIA
OKLAHOMA
TENNESSEE
NORTH CAROLINA
ARIZONA
NEW MEXICO
ARKANSAS
MISSISSIPPI
SOUTH CAROLINA
ALABAMA
GEORGIA
TEXAS
LOUISIANA
FLORIDA
United States
Ottawa
Montreal
Toronto
Chicago
Boston
New York
Washington
San Francisco
Las Vegas
Los Angeles
San Diego
Dallas
San Antonio
Houston
Monterrey
Miami
Gulf of California
Gulf of Mexico
WIGLE.NET

Baltic Sea
Estonia
Latvia
North Sea
United Kingdom
Denmark
Lithuania
Ireland
Netherlands
Berlin
Poland
Belarus
London
Warsaw
Germany
Kyiv
Київ
Belgium
Paris
Czechia
Slovakia
Ukraine
Austria
Moldova
Hungary
France
Romania
Croatia
Serbia
Marseille
Italy
Barcelona
Rome
Bulgaria
Portugal
Madrid
Spain
Lisbon
Tyrrhenian Sea
Istanbul
Ankara
Greece
Algiers
مدينة الجزائر
Tunis
تونس
Athens
Αθήνα
WIGLE.NET


North Korea
Sea of Japan
HEBEI
GANSU
NINGXIA
SHANXI
SHAANXI
SHANDONG
Yellow Sea
South Korea
Osaka
大阪
Japan
Tokyo
東京
China
HENAN
JIANGSU
HUBEI
ANHUI
East China Sea
SICHUAN
Chongqing
重庆
ZHEJIANG
GUIZHOU
HUNAN
JIANGXI
Taipei
台北
FUJIAN
YUNNAN
GUANGXI
GUANGDONG
Taiwan
Hanoi
Hong Kong
香港
Laos
HAINAN
Philippine Sea
Thailand
South China Sea
Manila
Bangkok
Vietnam
Cambodia
Philippines
Ho Chi Minh City
Gulf of Thailand
WIGLE.NET


Jungle Cruise
Main Street, U.S.A.
Tony's Town Square
See Mickey at Town Square Theater
Caribbean Way
Monorail Station
Magic Kingdom
Magic Kingdom Park
Magic Kingdom Park Red Launch
atellite
Keyboard shortcuts
Map data ©2023 Google
Terms of Use
Report a map error
WIGLE.NET

KSC

- Is Disney collecting data at **Kennedy Space Center** as well? Or do Magic Bands actually beacon?
- The conclusion has to be that they beacon

DSNYMBLE QoS: 0 type: BLE
40:d6:f3:bb:63:40? 2023-02-12 - 2023-02-12

DSNYMBLE QoS: 0 type: BT
42:df:ea:59:41:b3? 2022-04-01 - 2022-04-01

DSNYMBLE QoS: 0 type: BLE
49:2f:24:f6:90:e2? 2021-05-30 - 2021-05-31

DSNYMBLE QoS: 0 type: BLE
4a:b3:4b:c3:b3:7d? 2022-04-03 - 2022-04-03

DSNYMBLE QoS: 0 type: BLE
4c:9c:96:e4:bf:46? 2022-04-01 - 2022-04-01

DSNYMBLE QoS: 0 type: BT
54:c2:d5:30:1f:50? 2022-11-14 - 2022-12-01

DSNYMBLE QoS: 0 type: BT
5c:61:b7:e0:84:e3? 2022-09-18 - 2022-09-18

DSNYMBLE QoS: 0 type: BT
5d:f4:d9:24:fa:ba? 2023-02-12 - 2023-02-12

DSNYMBLE QoS: 0 type: BT
60:dc:49:74:01:ae? 2022-11-14 - 2022-12-01

DSNYMBLE QoS: 0 type: BT
61:16:af:cc:d3:d4? 2023-02-12 - 2023-02-12

DSNYMBLE QoS: 0 type: BLE
64:de:65:c9:44:d1? 2022-09-18 - 2022-09-18

DSNYMBLE QoS: 0 type: BLE
67:bf:c1:fb:a7:66? 2022-04-03 - 2022-04-03

DSNYMBLE QoS: 0 type: BT
69:7b:38:d5:c8:eb? 2022-11-14 - 2022-12-01

DSNYMBLE QoS: 0 type: BLE
69:d4:07:35:ef:5f? 2023-02-12 - 2023-02-12

DSNYMBLE QoS: 0 type: BLE
70:88:fc:18:99:b3? 2022-06-09 - 2022-06-09

DSNYMBLE QoS: 0 type: BT
73:26:ab:30:9a:ff? 2022-11-14 - 2022-12-01

DSNYMBLE QoS: 0 type: BLE
7b:7d:ab:56:c3:55? 2023-04-15 - 2023-04-15

DSNYMBLE QoS: 0 type: BT
7c:dd:60:e0:d4:64? 2022-11-14 - 2022-12-01

DSNYMBLE QoS: 0 type: BT
7f:29:52:07:0f:4e? 2022-04-01 - 2022-04-01

KSC

- Is Disney collecting data at **Kennedy Space Center** as well? Or do Magic Bands actually beacon?
- The conclusion has to be that they beacon

DSNYMBLE QoS: 0 type: BLE
40:d6:f3:bb:63:40? 2023-02-12 - 2023-02-12

DSNYMBLE QoS: 0 type: BT
42:df:ea:59:41:b3? 2022-04-01 - 2022-04-01

DSNYMBLE QoS: 0 type: BLE
49:2f:24:f6:90:e2? 2021-05-30 - 2021-05-31

DSNYMBLE QoS: 0 type: BLE
4a:b3:4b:c3:b3:7d? 2022-04-03 - 2022-04-03

DSNYMBLE QoS: 0 type: BLE
4c:9c:96:e4:bf:46? 2022-04-01 - 2022-04-01

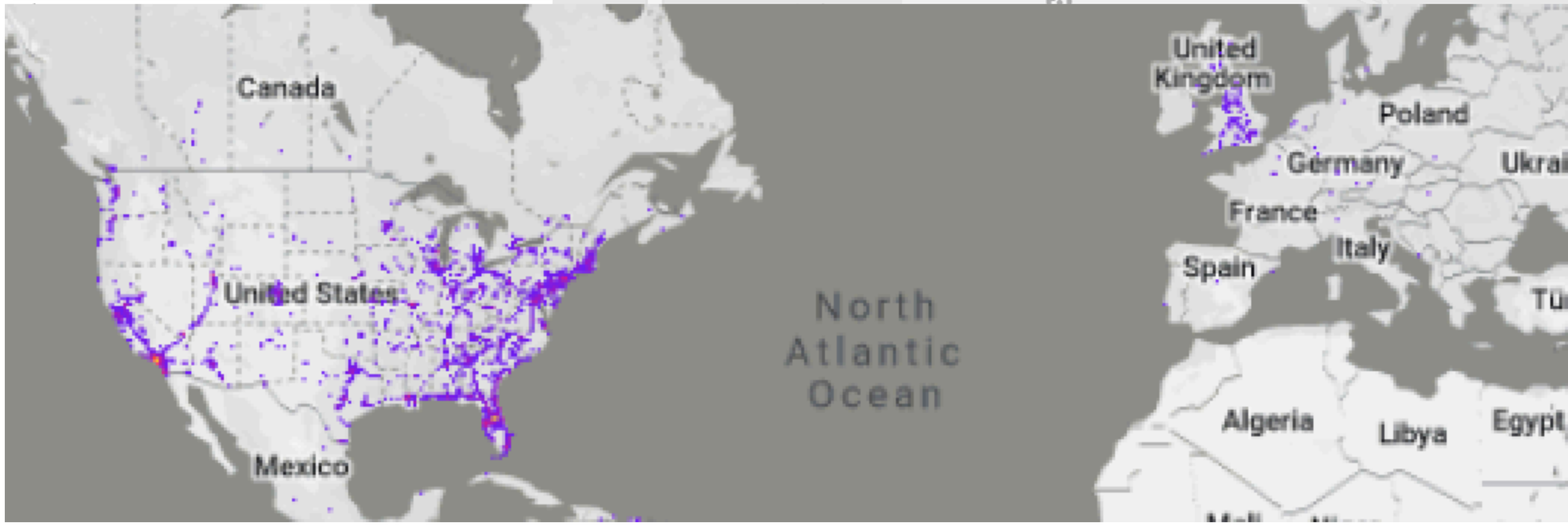
DSNYMBLE QoS: 0 type: BT
54:c2:d5:30:1f:50? 2022-11-14 - 2022-12-01

DSNYMBLE QoS: 0 type: BT
5c:61:b7:e0:84:e3? 2022-09-18 - 2022-09-18

DSNYMBLE QoS: 0 type: BT
5d:f4:d9:24:fa:ba? 2023-02-12 - 2023-02-12

DSNYMBLE QoS: 0 type: BT
60:dc:49:74:01:ae? 2022-11-14 - 2022-12-01

DSNYMBLE QoS: 0 type: BT
61:16:af:cc:d3:d4? 2023-02-12 - 2023-02-12



KSC 3

ABBOTT3MH00HPJ9C0 QoS: **0** type: **BT**
34:5b:98:f3:c9:5b ? 2023-02-12 - 2023-02-12

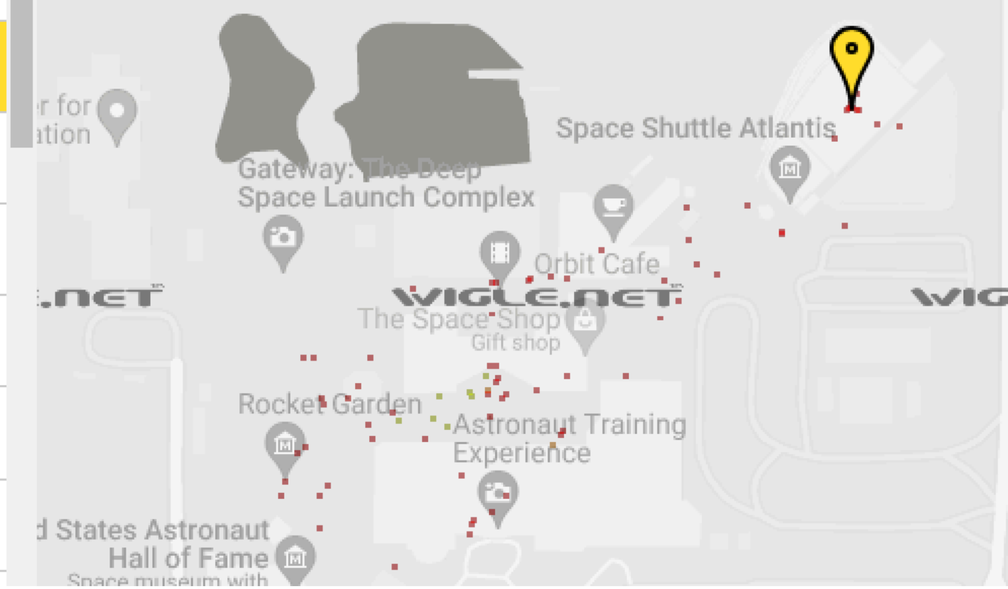
G7Xm3_F24FFC QoS: **0** type: **BT**
34:9f:7b:f5:95:f9 ? 2023-02-12 - 2023-02-12

DSNYMBLE QoS: **0** type: **BLE**
40:d6:f3:bb:63:40 ? 2023-02-12 - 2023-02-12

Galaxy Watch4 Classic (00NH) QoS: **0** type: **BLE**
43:96:92:01:d2:6a ? 2023-02-12 - 2023-02-12

NVIDIA SHIELD Remote QoS: **0** type: **BLE**
48:b0:2d:60:5a:73 ? 2023-02-12 - 2023-02-12

Galaxy Watch4 (A7CL) QoS: **0** type: **BLE**
4c:4d:76:75:76:cd ? 2023-02-12 - 2023-02-12



KSC 3

ABBOTT3MH00HPJ9C0 QoS: 0 type: BT
34:5b:98:f3:c9:5b ? 2023-02-12 - 2023-02-12

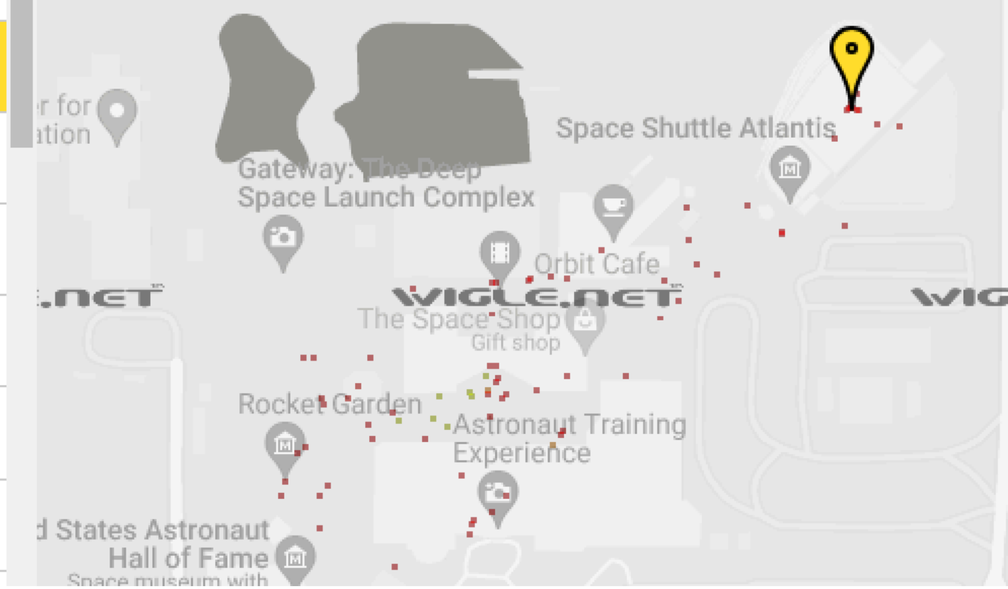
G7Xm3_F24FFC QoS: 0 type: BT
34:9f:7b:f5:95:f9 ? 2023-02-12 - 2023-02-12

DSNYMBLE QoS: 0 type: BLE
40:d6:f3:bb:63:40 ? 2023-02-12 - 2023-02-12

Galaxy Watch4 Classic (00NH) QoS: 0 type: BLE
43:96:92:01:d2:6a ? 2023-02-12 - 2023-02-12

NVIDIA SHIELD Remote QoS: 0 type: BLE
48:b0:2d:60:5a:73 ? 2023-02-12 - 2023-02-12

Galaxy Watch4 (A7CL) QoS: 0 type: BLE
4c:4d:76:75:76:cd ? 2023-02-12 - 2023-02-12



- But then while looking around I saw this "ABBOTT*" thing, and looked into it

KSC 3

ABBOTT3MH00HPJ9C0 QoS: 0 type: BT
34:5b:98:f3:c9:5b ? 2023-02-12 - 2023-02-12

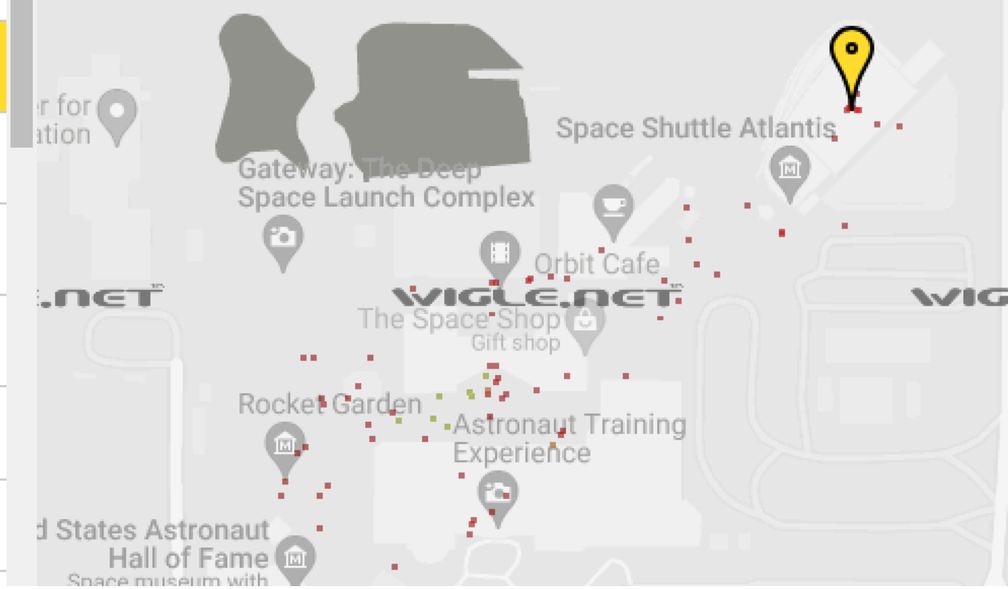
G7Xm3_F24FFC QoS: 0 type: BT
34:9f:7b:f5:95:f9 ? 2023-02-12 - 2023-02-12

DSNYMBLE QoS: 0 type: BLE
40:d6:f3:bb:63:40 ? 2023-02-12 - 2023-02-12

Galaxy Watch4 Classic (00NH) QoS: 0 type: BLE
43:96:92:01:d2:6a ? 2023-02-12 - 2023-02-12

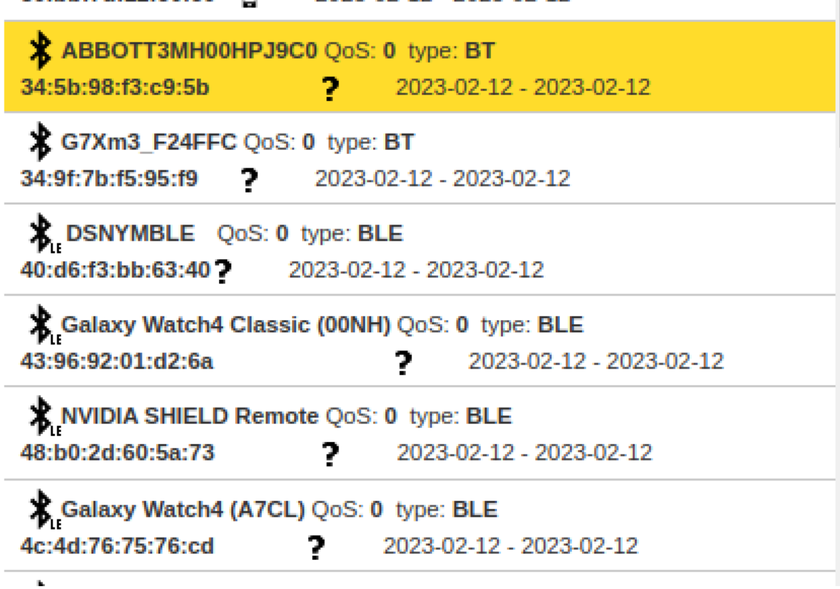
NVIDIA SHIELD Remote QoS: 0 type: BLE
48:b0:2d:60:5a:73 ? 2023-02-12 - 2023-02-12

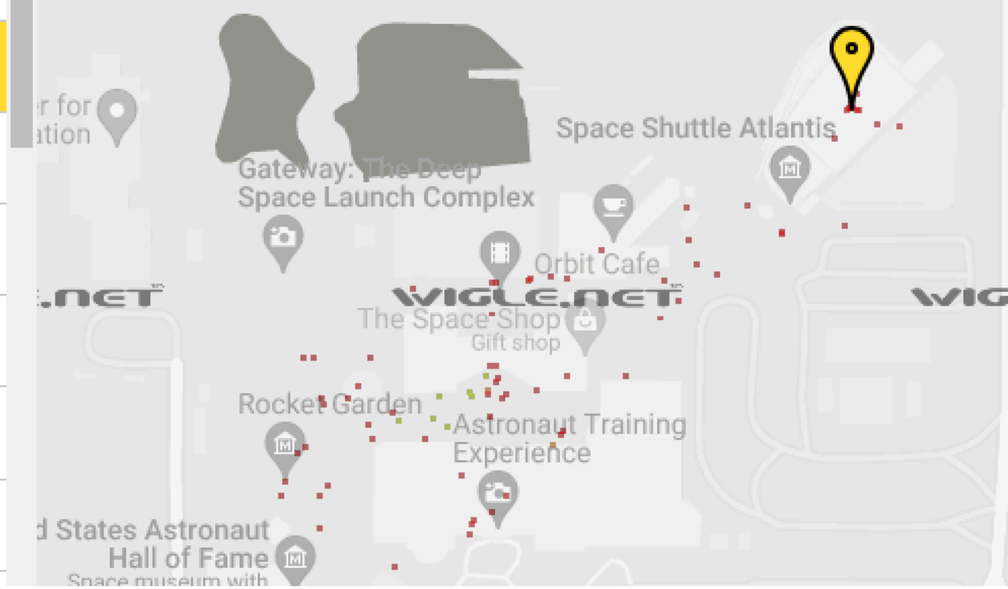
Galaxy Watch4 (A7CL) QoS: 0 type: BLE
4c:4d:76:75:76:cd ? 2023-02-12 - 2023-02-12



- But then while looking around I saw this "ABBOTT*" thing, and looked into it
- Turns out it is a glucose monitor!

KSC 3





- But then while looking around I saw this "ABBOTT*" thing, and looked into it
- Turns out it is a glucose monitor!
  - We'll come back to it later

USA - Miami

USA - Miami

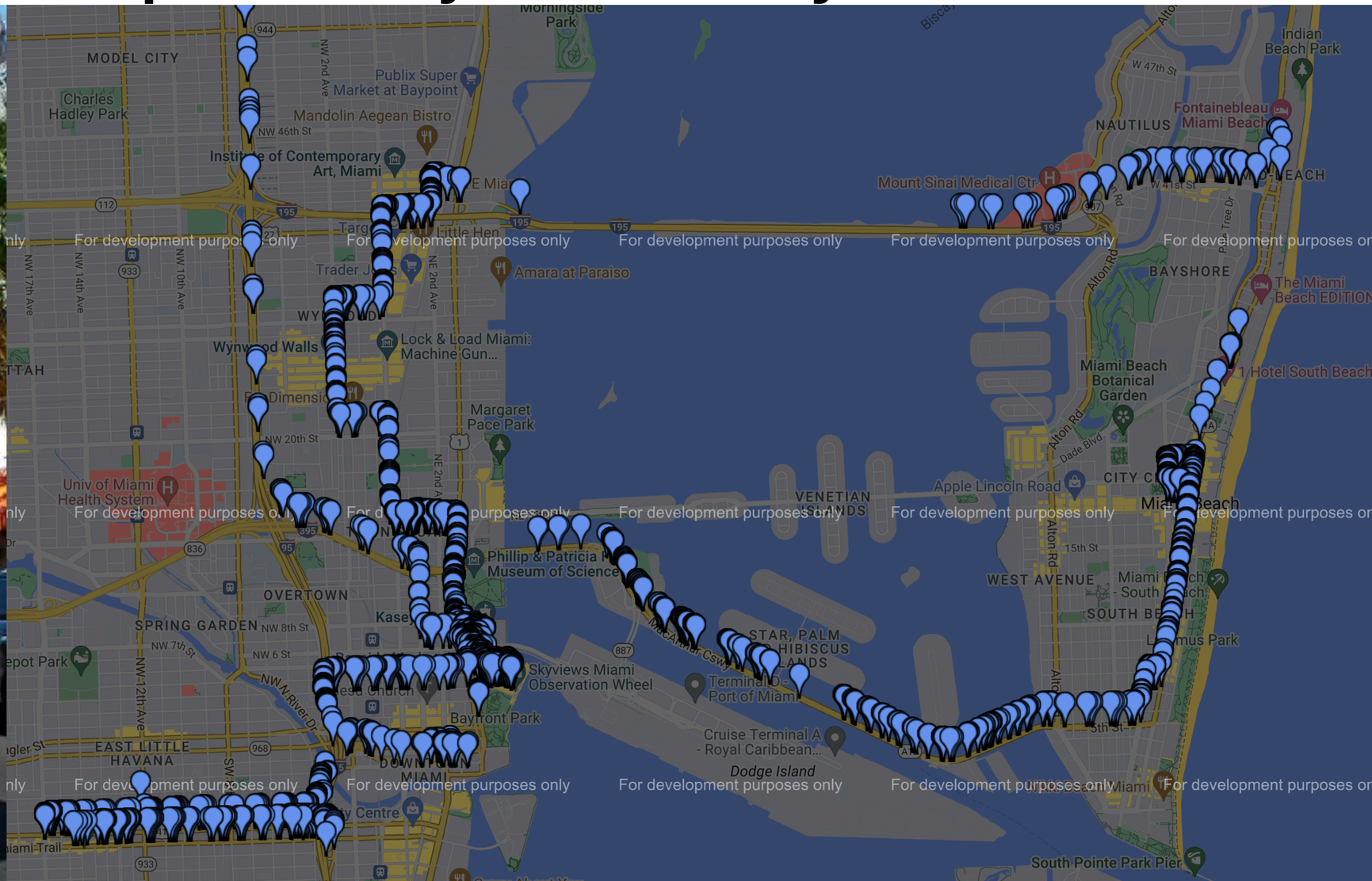
Hop-on-hop-off bus! The perfect way to sniff a city!

USA - Miami

Hop-on-hop-off bus! The perfect way to sniff a city!

USA - Miami

Hop-on-hop-off bus! The perfect way to sniff a city!



Miami

"Coors Light Feature Clock" - lol

- Coors-branded LED sign. Uses BT to set the text

Coors Light Feature Clock QoS: **5** type: **BLE**
00:07:80:ad:9c:78 [BLE]2023-02-11 - 2023-07-29

ATOTO QoS: **0** type: **BT**
00:0e:11:a1:43:b3? 2023-02-11 - 2023-02-11

Shure AONIC TW2 QoS: **0** type: **BLE**
00:0e:dd:71:9b:65 ? 2023-02-11 - 2023-02-11

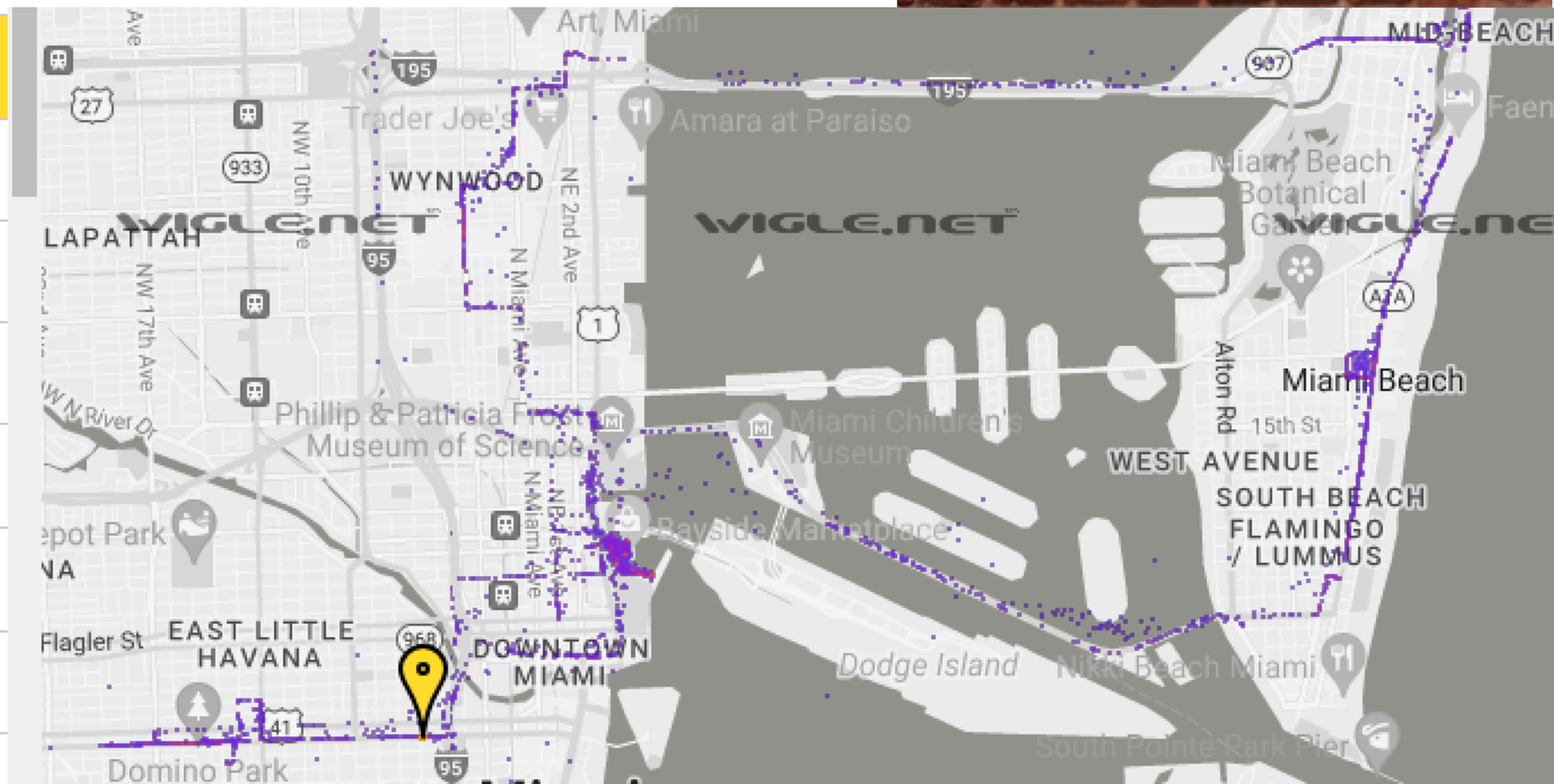
mC-Print3-G0328 QoS: **2** type: **BT**
00:11:62:22:51:0c ? 2023-02-12 - 2023-04-13

QoS: **0** type: **BLE**
00:15:57:0d:85:3c? 2023-02-11 - 2023-02-11

YamahaAV QoS: **2** type: **BLE**
00:19:01:c0:93:7b [BLE]2023-02-11 - 2023-04-09

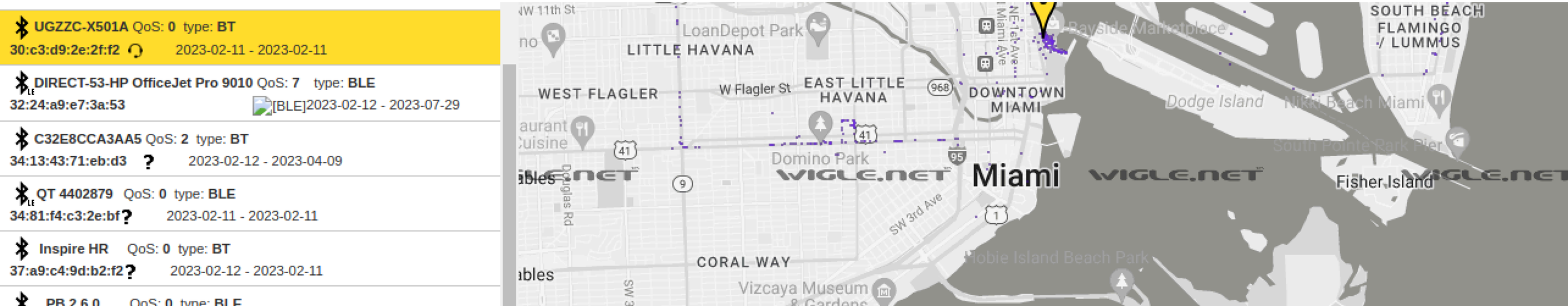
QoS: **0** type: **BLE**
00:1a:6d:3e:19:d1? 2023-02-11 - 2023-02-11

QoS: **0** type: **BLE**



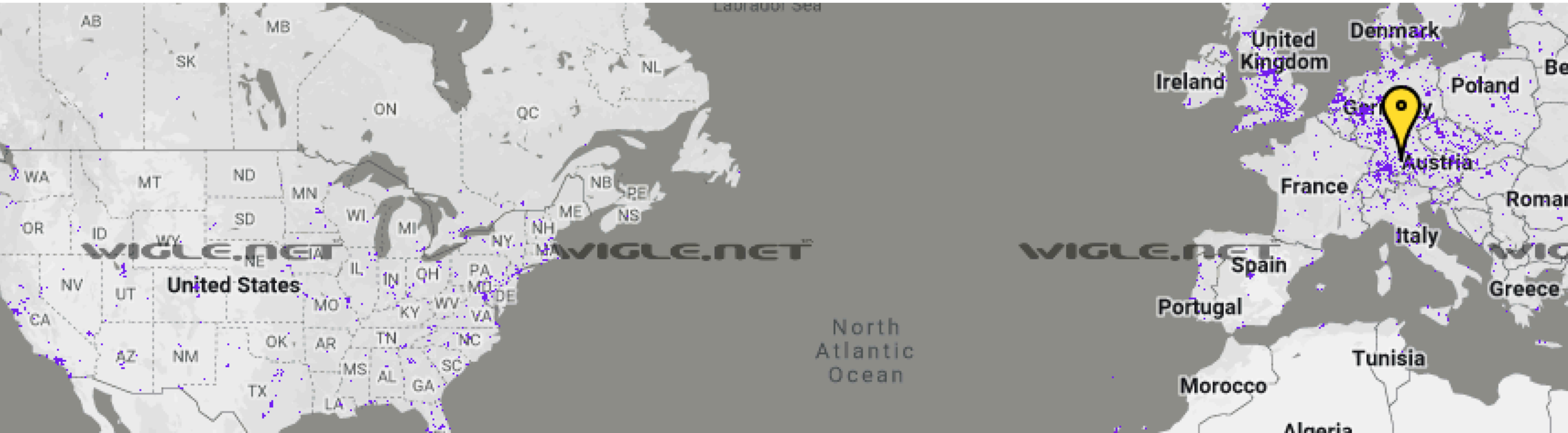
Miami
"UGZZ"

- Led me down a rabbit hole that UGZZC is the older BT 2.1 version of the UGZZF *module* from Alps, for use in cars
- Much more popular in EU than US. Probably used in German cars?



Miami
"UGZZ"

- Led me down a rabbit hole that UGZZC is the older BT 2.1 version of the UGZZF *module* from Alps, for use in cars
- Much more popular in EU than US. Probably used in German cars?



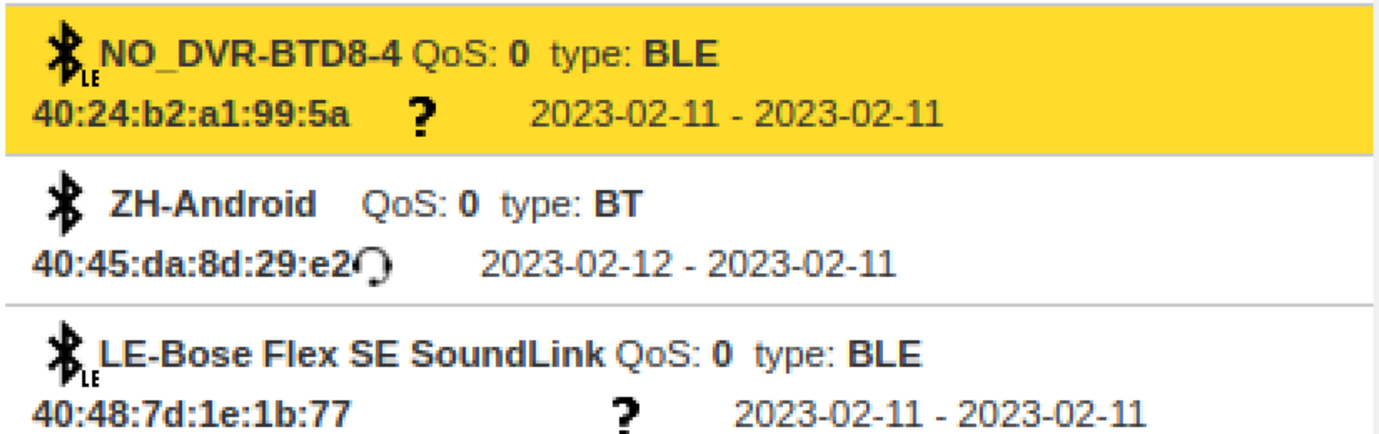
Miami

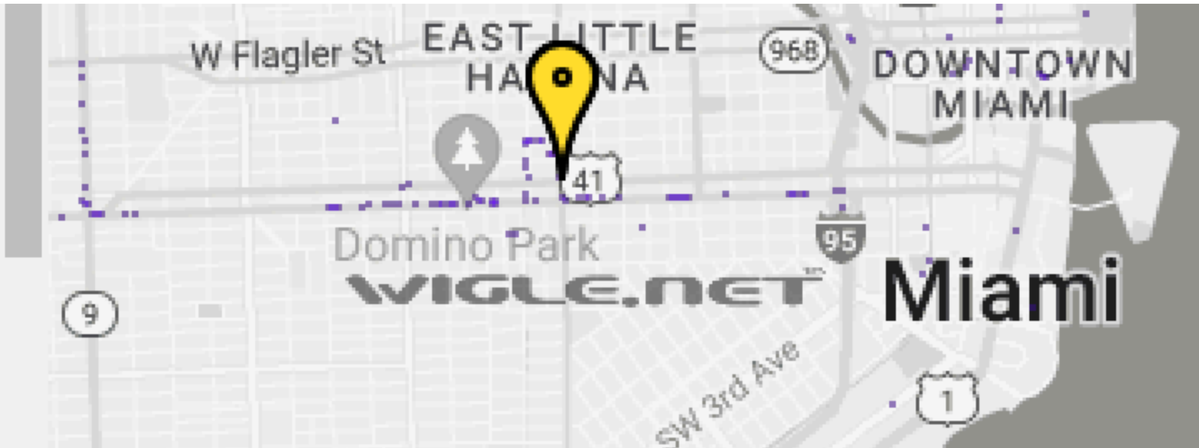
"NO_DVR"

Recorder Models

- DVR-BTD8-41/V2
- DVR-BTD8-81/V2
- DVR-BTD8-4POE-2/V2

- I was like "Why would it tell me there's no DVR???"
- It turns out it's a *Night Owl* DVR model BTD8-4* :D
  - You know, for security cameras!





Miami

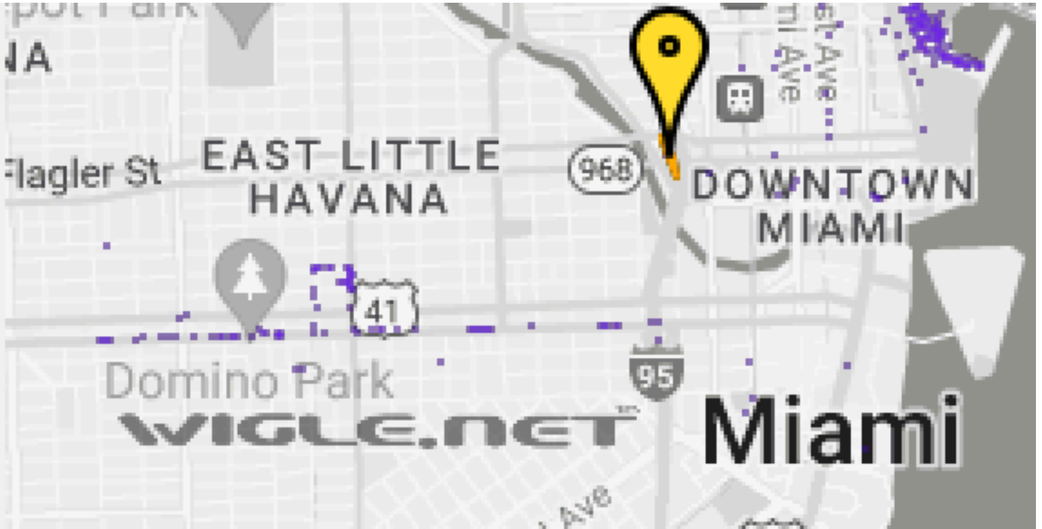
"Hello Fairy"

- Suspected this might just be a individual's named device. Checked WiGLE. Was wrong!
- Controllable LED lights

Hello Fairy-20B3 QoS: **5** type: **BLE**
48:53:54:01:20:b3 **?** 2023-02-12 - 2023-08-05

Nicaragua Libre QoS: **0** type: **BT**
48:74:12:58:a1:88 2023-02-12 - 2023-02-11

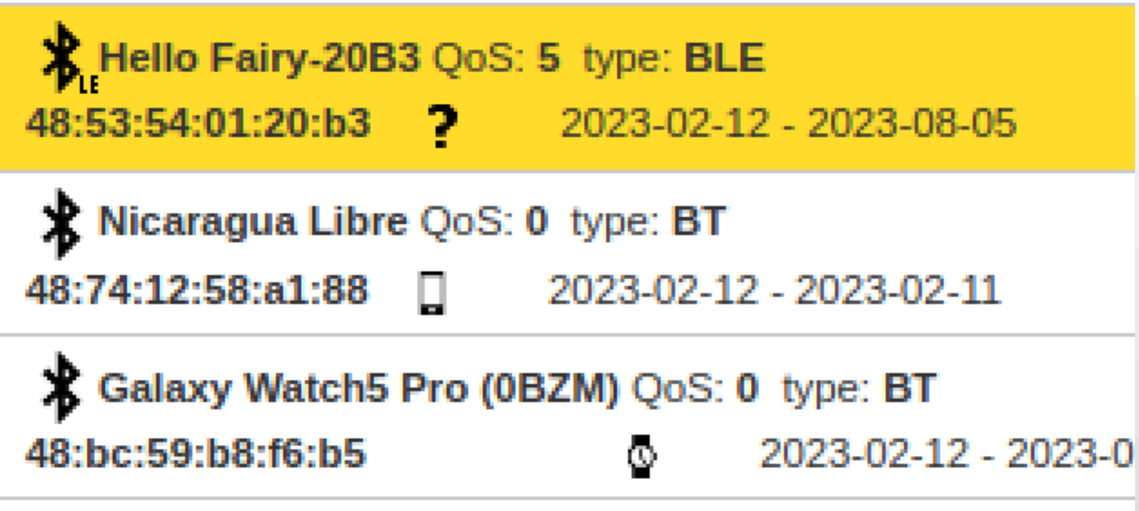
Galaxy Watch5 Pro (0BZM) QoS: **0** type: **BT**
48:bc:59:b8:f6:b5 2023-02-12 - 2023-02-11



Miami

"Hello Fairy"

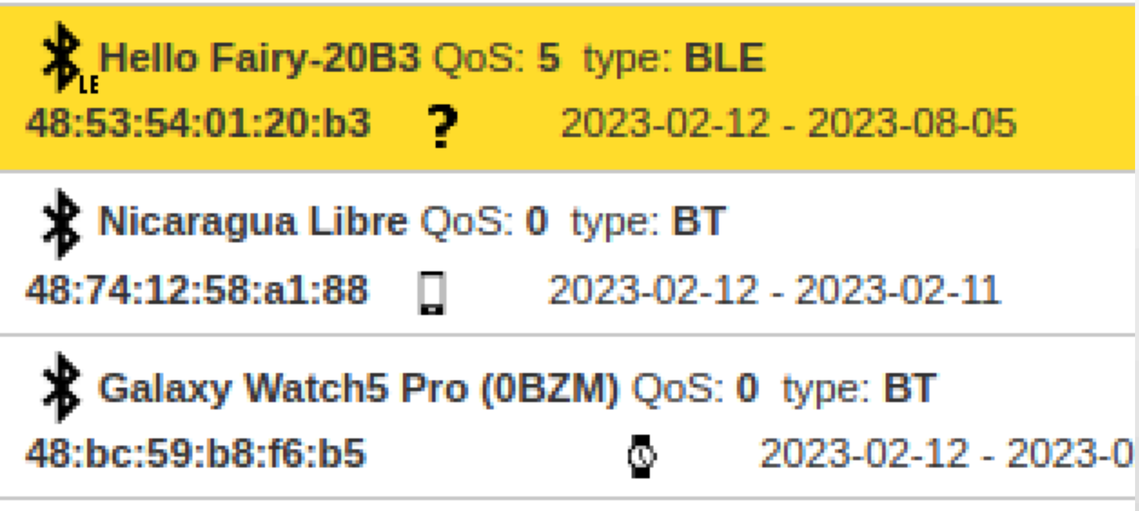
- Suspected this might just be a in
  Was wrong!
- Controllable LED lights



Miami

"Hello Fairy"

- Suspected this might just be a in
  Was wrong!
- Controllable LED lights



USA - Key West

USA - Key West

"I heard you like radio, so we put a BT radio in your radio..."

CTRL-RIDGID Jobsite Radio QoS: **0** type: **BLE**
00:75:58:df:b4:0a ? 2023-02-09 - 2023-02-09

watch QoS: **0** type: **BLE**
01:96:28:07:9a:ba ? 2023-02-09 - 2023-02-09

JBL Flip 4 QoS: **0** type: **BLE**
04:21:44:cb:7d:72 ? 2023-02-09 - 2023-02-09

LE-Bose QuietComfort 35 QoS: **0** type: **BLE**
04:52:c7:60:0d:71 ? 2023-02-09 - 2023-02-09

Bose Color II SoundLink QoS: **0** type: **BT**
04:52:c7:81:b9:0c ? 2023-02-09 - 2023-02-09

Bose Color II SoundLink QoS: **1** type: **BLE**
04:52:c7:b8:21:13 ? 2023-02-09 - 2023-02-09

21025699 ThermapenBlue QoS: **0** type: **BT**

USA - Key West

"I heard you like radio, so we put a BT radio in your radio..."

CTRL-RIDGID Jobsite Radio QoS: **0** type: **BLE**
00:75:58:df:b4:0a ? 2023-02-09 - 2023-02-09

watch QoS: **0** type: **BLE**
01:96:28:07:9a:ba ? 2023-02-09 - 2023-02-09

JBL Flip 4 QoS: **0** type: **BLE**
04:21:44:cb:7d:72 ? 2023-02-09 - 2023-02-09

LE-Bose QuietComfort 35 QoS: **0** type: **BLE**
04:52:c7:60:0d:71 ? 2023-02-09 - 2023-02-09

Bose Color II SoundLink QoS: **0** type: **BT**
04:52:c7:81:b9:0c ? 2023-02-09 - 2023-02-09

Bose Color II SoundLink QoS: **1** type: **BLE**
04:52:c7:b8:21:13 ? 2023-02-09 - 2023-02-09

21025699 ThermapenBlue QoS: **0** type: **BT**

USA - Key West

"I heard you like radio, so we put a BT radio in your radio..."

- I thought this was going to be walkie-talkies
- This is really just a Bluetooth speaker w/ "rugged" design to handle getting knocked around

CTRL-RIDGID Jobsite Radio QoS: **0** type: **BLE**
00:75:58:df:b4:0a ? 2023-02-09 - 2023-02-09

watch QoS: **0** type: **BLE**
01:96:28:07:9a:ba ? 2023-02-09 - 2023-02-09

JBL Flip 4 QoS: **0** type: **BLE**
04:21:44:cb:7d:72 ? 2023-02-09 - 2023-02-09

LE-Bose QuietComfort 35 QoS: **0** type: **BLE**
04:52:c7:60:0d:71 ? 2023-02-09 - 2023-02-09

Bose Color II SoundLink QoS: **0** type: **BT**
04:52:c7:81:b9:0c ? 2023-02-09 - 2023-02-09

Bose Color II SoundLink QoS: **1** type: **BLE**
04:52:c7:b8:21:13 ? 2023-02-09 - 2023-02-09

21025699 ThermapenBlue QoS: **0** type: **BT**

USA - Key West

"I heard you like radio, so we put a BT radio in your radio..."

- I thought this was going to be walkie-talkies
- This is really just a Bluetooth speaker w/ "rugged" design to handle getting knocked around

CTRL-RIDGID Jobsite Radio QoS: 0 type: BLE
00:75:58:df:b4:0a ? 2023-02-09 - 2023-02-09

watch QoS: 0 type: BLE
01:96:28:07:9a:ba ? 2023-02-09 - 2023-02-09

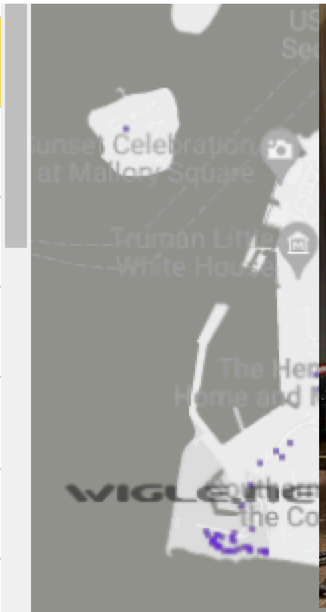
JBL Flip 4 QoS: 0 type: BLE
04:21:44:cb:7d:72 ? 2023-02-09 - 2023-02-09

LE-Bose QuietComfort 35 QoS: 0 type: BLE
04:52:c7:60:0d:71 ? 2023-02-09 - 2023-02-09

Bose Color II SoundLink QoS: 0 type: BT
04:52:c7:81:b9:0c ? 2023-02-09 - 2023-02-09

Bose Color II SoundLink QoS: 1 type: BLE
04:52:c7:b8:21:13 ? 2023-02-09 - 2023-02-09

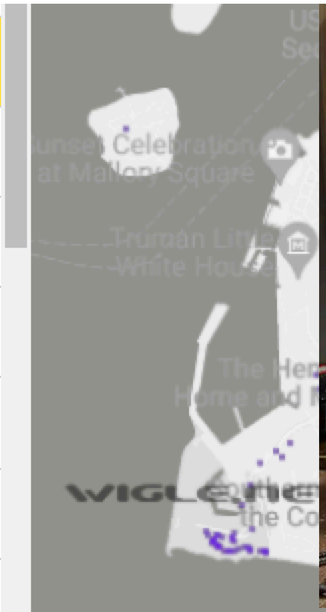
21025699 ThermapenBlue QoS: 0 type: BT



USA - Key West

"I heard you like radio, so we put a BT radio in your ra

- I thought this was going to be walkie-talkies
- This is really just a Bluetooth speaker w/ "rugged" design to handle getting knocked around



USA - Key West

"^[0-9]{8} ThermapenBlue$"

- A really-expensive thermometer!

21025699 ThermapenBlue QoS: **0** type: **BT**
04:91:62:ec:13:a4 **?** 2023-02-11 - 2023-02-11

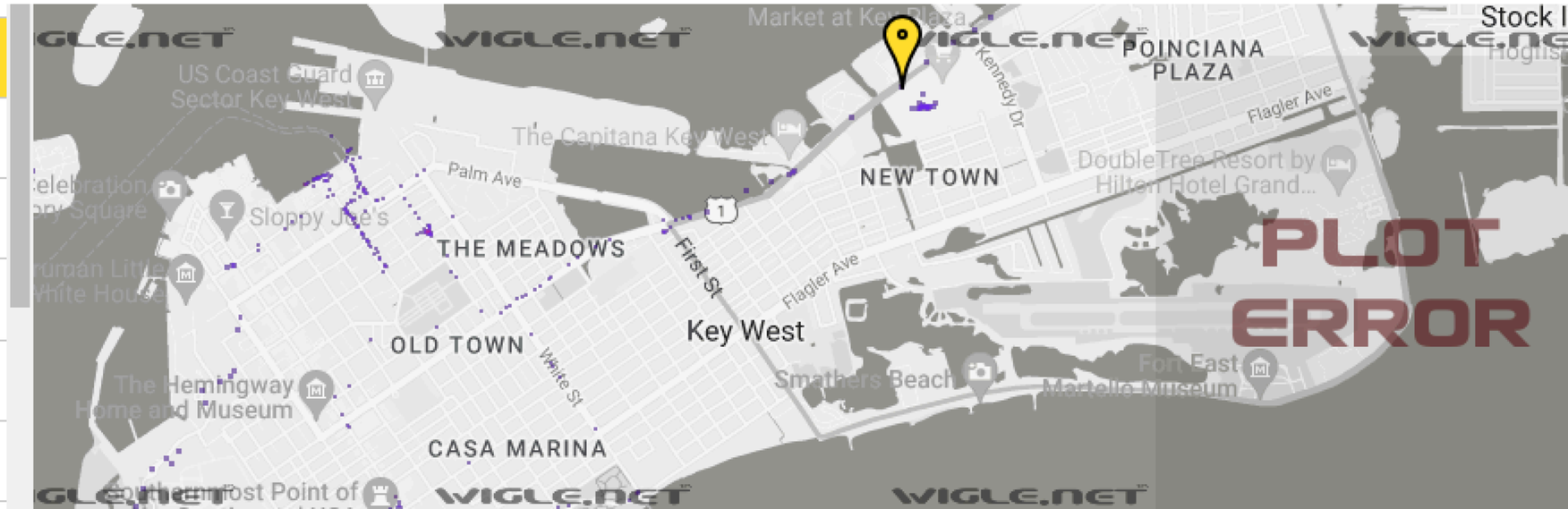
Square Reader 4409 QoS: **0** type: **BLE**
04:ee:03:08:94:97 **?** 2023-02-10 - 2023-02-11

ACVS QoS: **0** type: **BT**
08:6b:d7:20:91:72 **?** 2023-02-09 - 2023-02-09

Inspire QoS: **0** type: **BT**
0b:85:8a:69:85:da **?** 2023-02-11 - 2023-02-11

Square Reader 0123 QoS: **0** type: **BT**
0c:ec:80:08:08:86 **?** 2023-02-09 - 2023-02-09

[TV] Samsung 7 Series (43) QoS: **0** type: **BLE**
10:2b:41:1d:0f:d5 **?** 2023-02-10 - 2023-02-09



USA - Key West

"^[0-9]{8} ThermapenBlue$"

- A really-expensive thermometer!

21025699 ThermapenBlue QoS: **0** type: **BT**
04:91:62:ec:13:a4 ? 2023-02-11 - 2023-02-11

Square Reader 4409 QoS: **0** type: **BLE**
04:ee:03:08:94:97 ? 2023-02-10 - 2023-02-11

ACVS QoS: **0** type: **BT**
08:6b:d7:20:91:72 ? 2023-02-09 - 2023-02-09

Inspire QoS: **0** type: **BT**
0b:85:8a:69:85:da ? 2023-02-11 - 2023-02-11

Square Reader 0123 QoS: **0** type: **BT**
0c:ec:80:08:08:86 ? 2023-02-09 - 2023-02-09

[TV] Samsung 7 Series (43) QoS: **0** type: **BLE**
10:2b:41:1d:0f:d5 ? 2023-02-10 - 2023-02-09

Thermapen® Blue

★★★★★

Read 2 Reviews | 6 Questions, 140 Answers or Write a Review

SKU: THS-179-607

Bluetooth temperature probe, waterproof and built to last longer than all competitors in daily commercial kitchen use. NIST-traceable calibration certificate and best-in-class accuracy make Thermapen Blue the clear leader. Free mobile app.

$239.00

In Stock
Order now, ships today

5-up: $219.00 ea.
Call for larger volume pricing.
2 point calibration certificate included.

Quantity:

1 ADD TO CART

Pay in 4 interest-free payments of $59.75 with PayPal. Learn more

Add to Wish List

USA - Key West

"^[0-9]{8} ThermapenBlue$"

- A really-expensive thermometer!

21025699 ThermapenBlue QoS: 0 type: BT
04:91:62:ec:13:a4 ? 2023-02-11 - 2023-02-11

Square Reader 4409 QoS: 0 type: BLE
04:ee:03:08:94:97 ? 2023-02-10 - 2023-02-11

ACVS QoS: 0 type: BT
08:6b:d7:20:91:72 ? 2023-02-09 - 2023-02-09

Inspire QoS: 0 type: BT
0b:85:8a:69:85:da ? 2023-02-11 - 2023-02-11

Square Reader 0123 QoS: 0 type: BT
0c:ec:80:08:08:86 ? 2023-02-09 - 2023-02-09

[TV] Samsung 7 Series (43) QoS: 0 type: BLE
10:2b:41:1d:0f:d5 ? 2023-02-10 - 2023-02-09

Thermapen® Blue

★★★★★

Read 2 Reviews | 6 Questions, 140 Answers or Write a Review

SKU: THS-179-607

Bluetooth temperature probe, waterproof and built to last longer than all competitors in daily commercial kitchen use. NIST-traceable calibration certificate and best-in-class accuracy make Thermapen Blue the clear leader. Free mobile app.

$239.00

In Stock
Order now, ships today

5-up: $219.00 ea.
Call for larger volume pricing.
2 point calibration certificate included.

Quantity:

1 ADD TO CART

Pay in 4 interest-free payments of $59.75 with PayPal. Learn more

Add to Wish List

USA - Key West

"^Furbo3-S3$"

- Treat-tossing dog camera! THE FUTURE IS NOW!

PR BT 12ED QoS: **0** type: **BT**
00:1f:ff:b2:4b:c1? 2023-02-09 - 2023-02-09

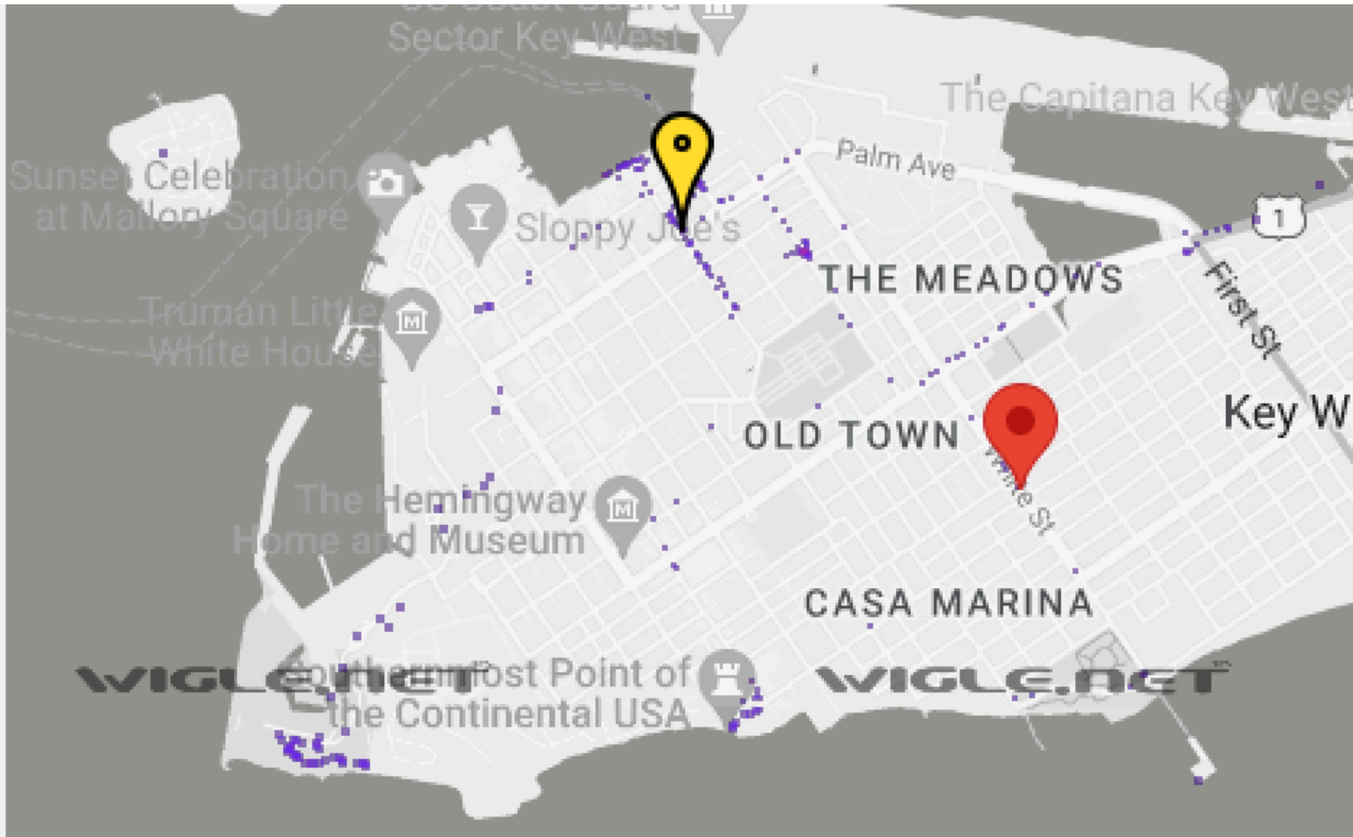
Furbo3-S3 QoS: **0** type: **BT**
00:2d:b3:00:78:fd? 2023-02-10 - 2023-02-11

Furbo3-S3 QoS: **0** type: **BT**
00:2d:b3:02:de:a7? 2023-02-09 - 2023-02-09

CTRL-RIDGID Jobsite Radio QoS: **0** type: **BLE**
00:75:58:df:b4:0a ? 2023-02-09 - 2023-02-09

watch QoS: **0** type: **BLE**
01:96:28:07:9a:ba? 2023-02-09 - 2023-02-09

JBL Flip 4 QoS: **0** type: **BLE**
04:21:44:cb:7d:72? 2023-02-09 - 2023-02-09



USA - Key West

"^Furbo3-S3$"

- Treat-tossing dog camera! THE F

PR BT 12ED QoS: 0 type: BT
00:1f:ff:b2:4b:c1? 2023-02-09 - 2023-02-09

Furbo3-S3 QoS: 0 type: BT
00:2d:b3:00:78:fd? 2023-02-10 - 2023-02-11

Furbo3-S3 QoS: 0 type: BT
00:2d:b3:02:de:a7? 2023-02-09 - 2023-02-09

CTRL-RIDGID Jobsite Radio QoS: 0 type: BLE
00:75:58:df:b4:0a ? 2023-02-09 - 2023-02-09

watch QoS: 0 type: BLE
01:96:28:07:9a:ba? 2023-02-09 - 2023-02-09

JBL Flip 4 QoS: 0 type: BLE
04:21:44:cb:7d:72? 2023-02-09 - 2023-02-09

LE Bose QuietComfort 35 QoS: 0 type: BLE

USA - Key West

"^Furbo3-S3$"

- Treat-tossing dog camera! THE F

PR BT 12ED QoS: 0 type: BT
00:1f:ff:b2:4b:c1? 2023-02-09 - 2023-02-09

Furbo3-S3 QoS: 0 type: BT
00:2d:b3:00:78:fd? 2023-02-10 - 2023-02-11

Furbo3-S3 QoS: 0 type: BT
00:2d:b3:02:de:a7? 2023-02-09 - 2023-02-09

CTRL-RIDGID Jobsite Radio QoS: 0 type: BLE
00:75:58:df:b4:0a ? 2023-02-09 - 2023-02-09

watch QoS: 0 type: BLE
01:96:28:07:9a:ba? 2023-02-09 - 2023-02-09

JBL Flip 4 QoS: 0 type: BLE
04:21:44:cb:7d:72? 2023-02-09 - 2023-02-09

LE Bose QuietComfort 35 QoS: 0 type: BLE

USA - Key West

"^Furbo3-S3$"

- Treat-tossing dog camera! THE F

PR BT 12ED QoS: 0 type: BT
00:1f:ff:b2:4b:c1 ? 2023-02-09 - 2023-02-09

Furbo3-S3 QoS: 0 type: BT
00:2d:b3:00:78:fd ? 2023-02-10 - 2023-02-11

Furbo3-S3 QoS: 0 type: BT
00:2d:b3:02:de:a7 ? 2023-02-09 - 2023-02-09

CTRL-RIDGID Jobsite Radio QoS: 0 type: BLE
00:75:58:df:b4:0a ? 2023-02-09 - 2023-02-09

watch QoS: 0 type: BLE
01:96:28:07:9a:ba ? 2023-02-09 - 2023-02-09

JBL Flip 4 QoS: 0 type: BLE
04:21:44:cb:7d:72 ? 2023-02-09 - 2023-02-09

USA - Key West

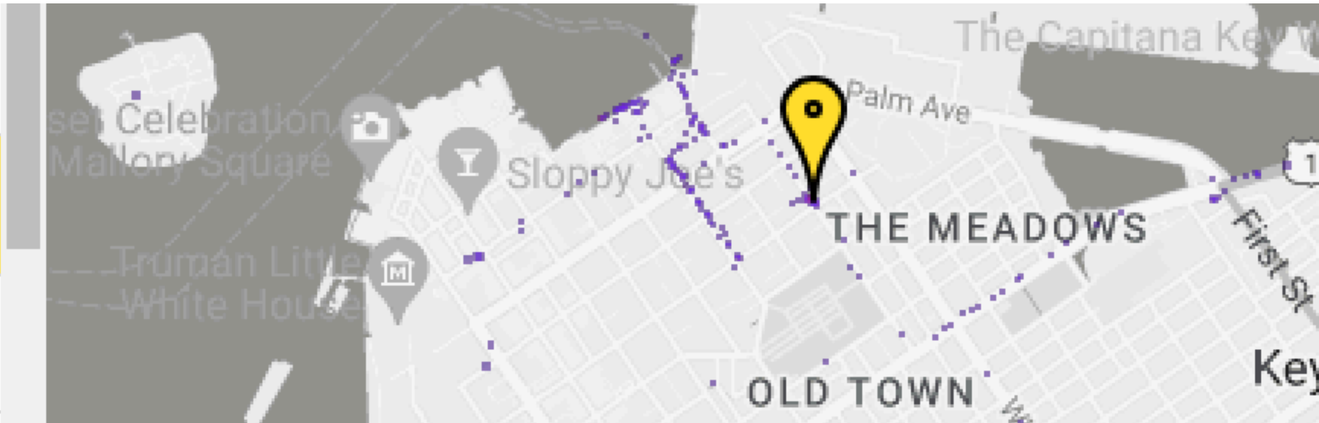
"^Philips Sonicare$"

- Tells you whether you're brushing correctly or not...

DN5BF4 QoS: 0 type: BLE
24:d7:eb:19:5b:f6 ? 2023-02-09 - 2023-02-09

Philips Sonicare QoS: 0 type: BT
24:e5:aa:2c:fe:55 ? 2023-02-10 - 2023-02-11

Chromebook QoS: 1 type: BLE
27:8e:41:dd:60:5c ? 2023-02-10 - 2023-02-11



USA - Key West

"^Philips Sonicare$"

- Tells you whether you're brushing correc

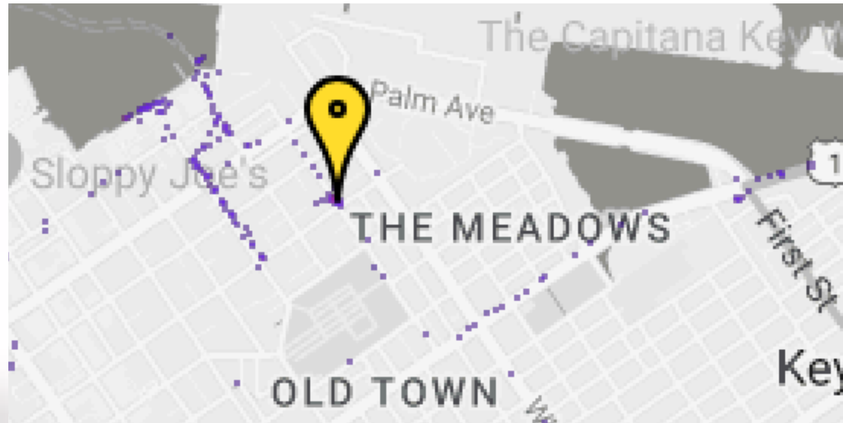
DN5BF4 QoS: 0 type: BLE
24:d7:eb:19:5b:f6 ? 2023-02-09 - 2023-02-09

Philips Sonicare QoS: 0 type: BT
24:e5:aa:2c:fe:55 ? 2023-02-10 - 2023-02-11

Chromebook QoS: 1 type: BLE
27:8e:41:dd:60:5c ? 2023-02-10 - 2023-02-11

PHILIPS
Sonicare
clean
white+
gum health
deep clean+
tongue care

PHILIPS
9:41 AM
100%
Last 7 days
Watch your pressure in these areas, Ken
1:38
Average session time
Coverage
Pressure
Scrubbing


The Capitana Key
Palm Ave
Sloppy Joe's
THE MEADOWS
First St
OLD TOWN

Netherlands

The Hague

Netherlands

The Hague

- Hardwear.io 2021: Sniffer wouldn't boot :'(

Netherlands

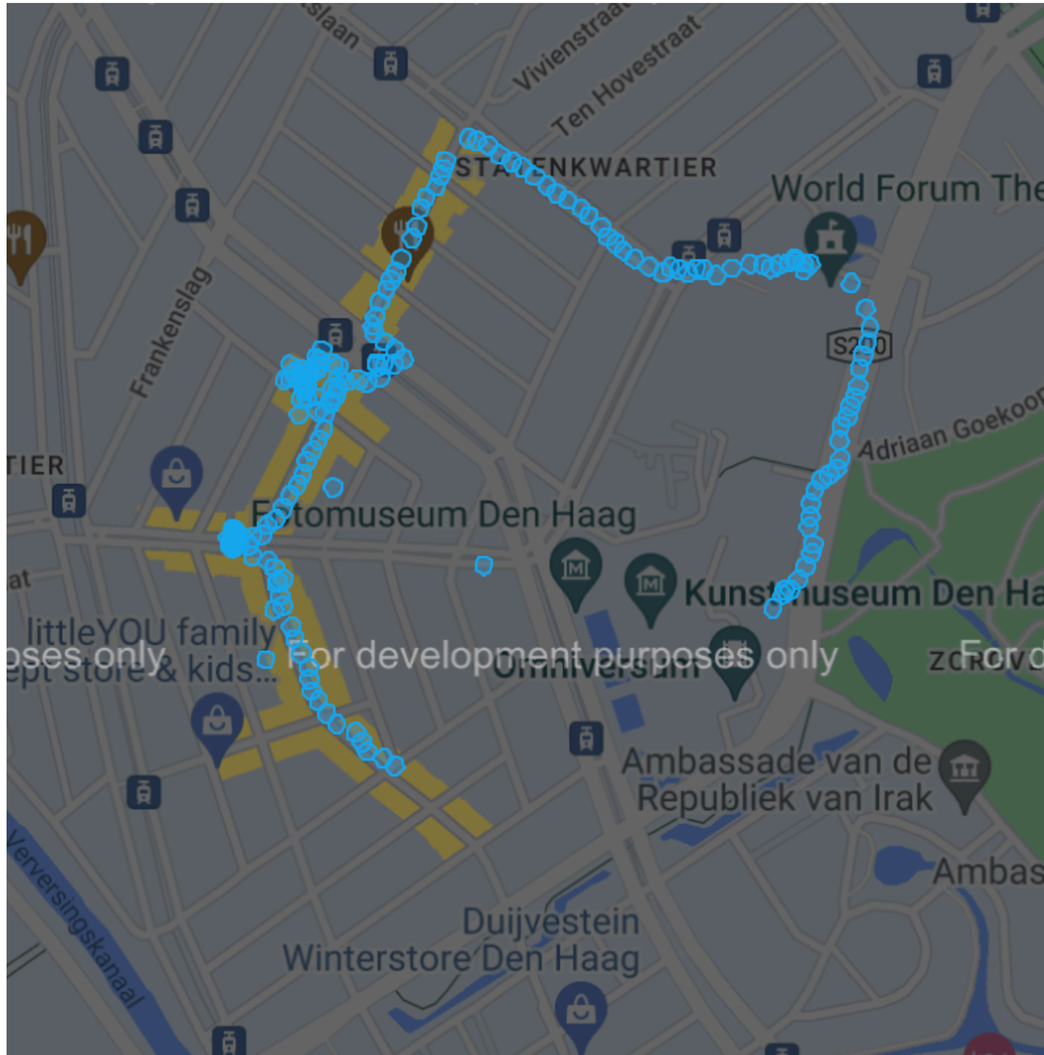
The Hague

- Hardwear.io 2021: Sniffer wouldn't boot :'(
- Hardwear.io 2022: Minimal GPS from when I wandered around outside the hotel

Netherlands

The Hague

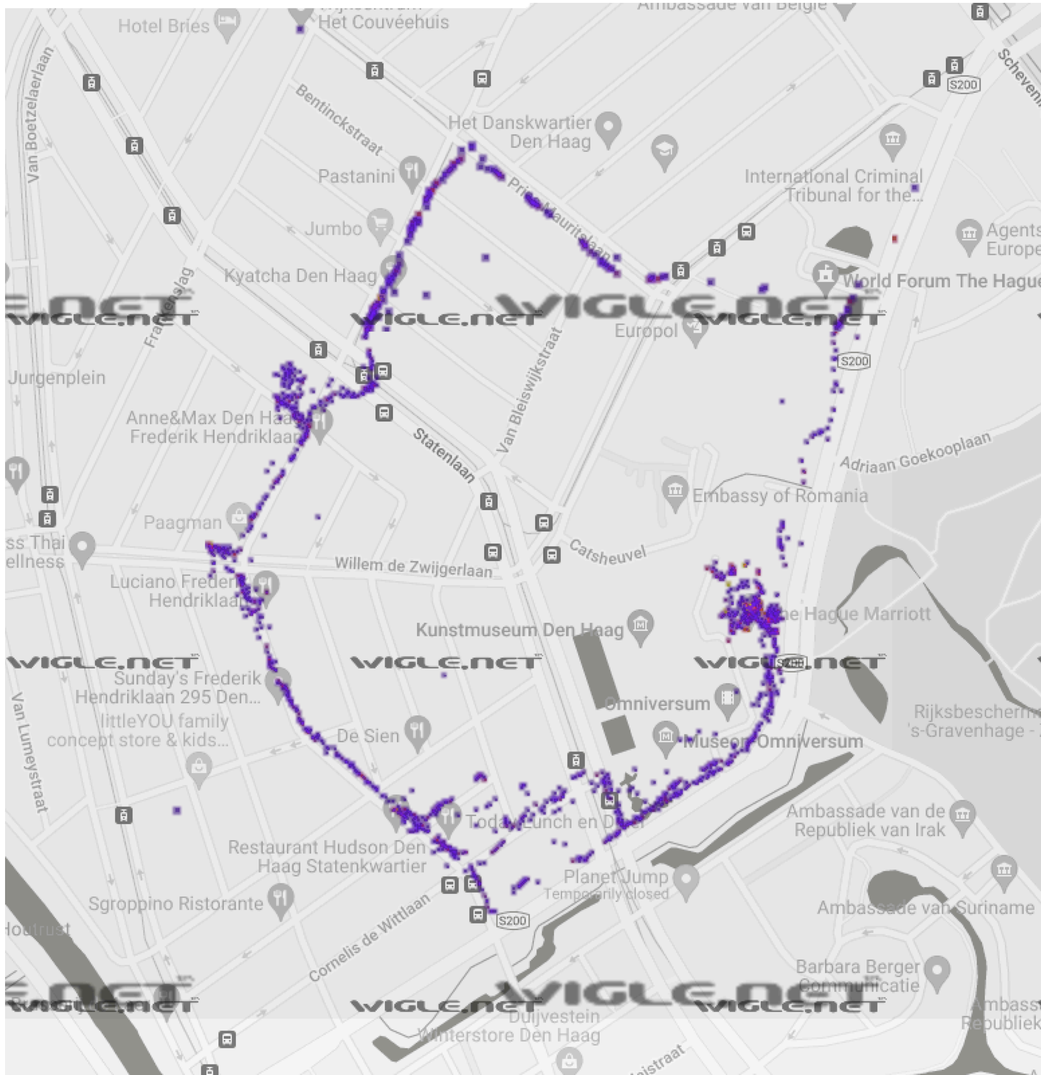
- Hardwear.io 2021: Sniffer wouldn't boot :'(
- Hardwear.io 2022: Minimal GPS from when I wandered around outside the hotel



Netherlands

The Hague

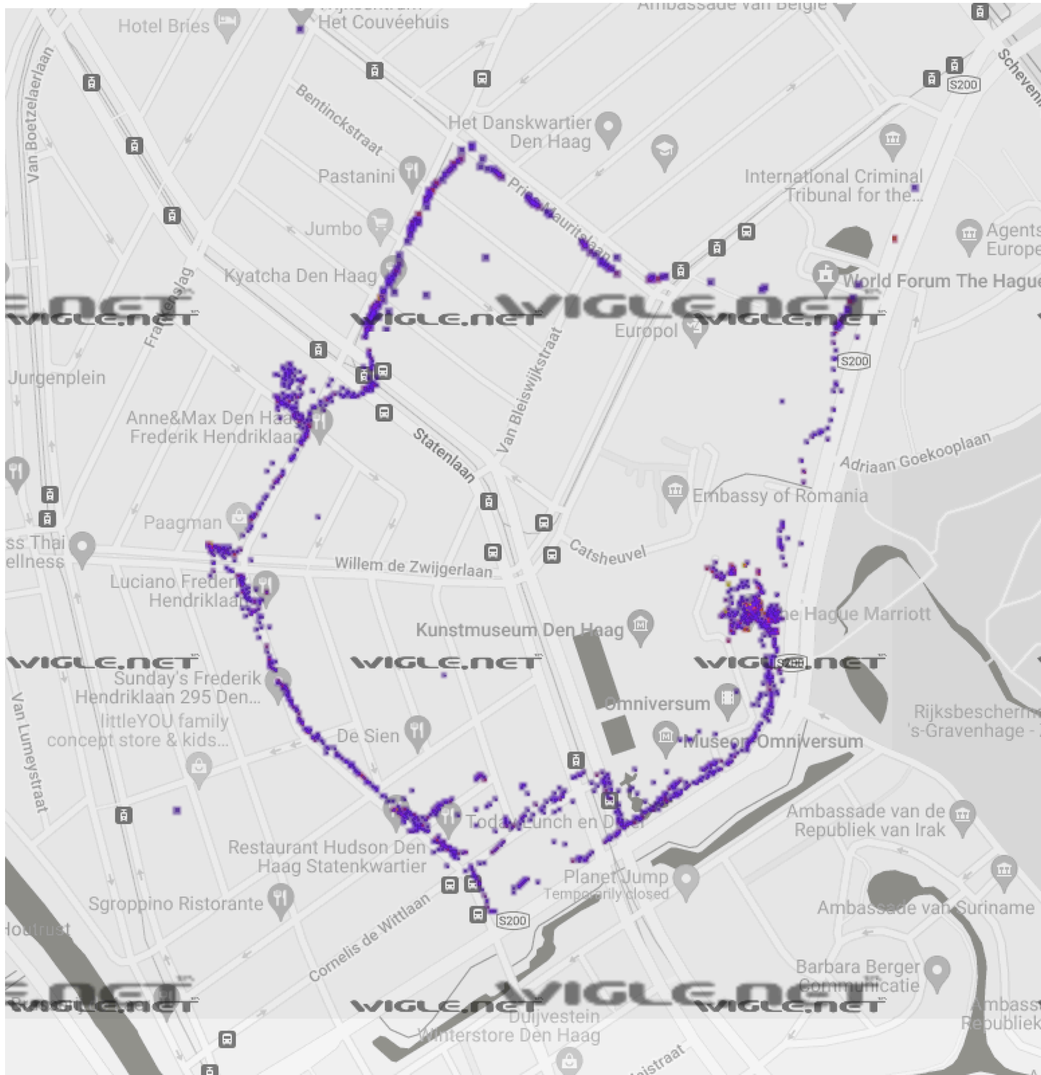
- Hardwear.io 2021: Sniffer wouldn't boot :'(
- Hardwear.io 2022: Minimal GPS from when I wandered around outside the hotel



Netherlands

The Hague

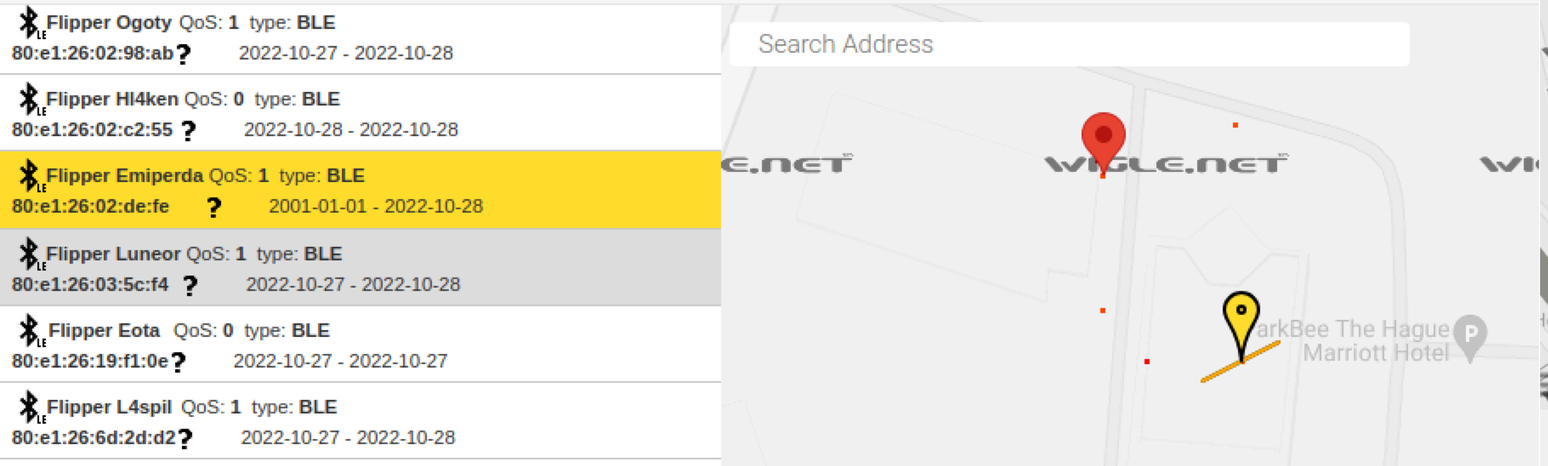
- Hardwear.io 2021: Sniffer wouldn't boot :'(
- Hardwear.io 2022: Minimal GPS from when I wandered around outside the hotel
- First time I noticed Flippers...

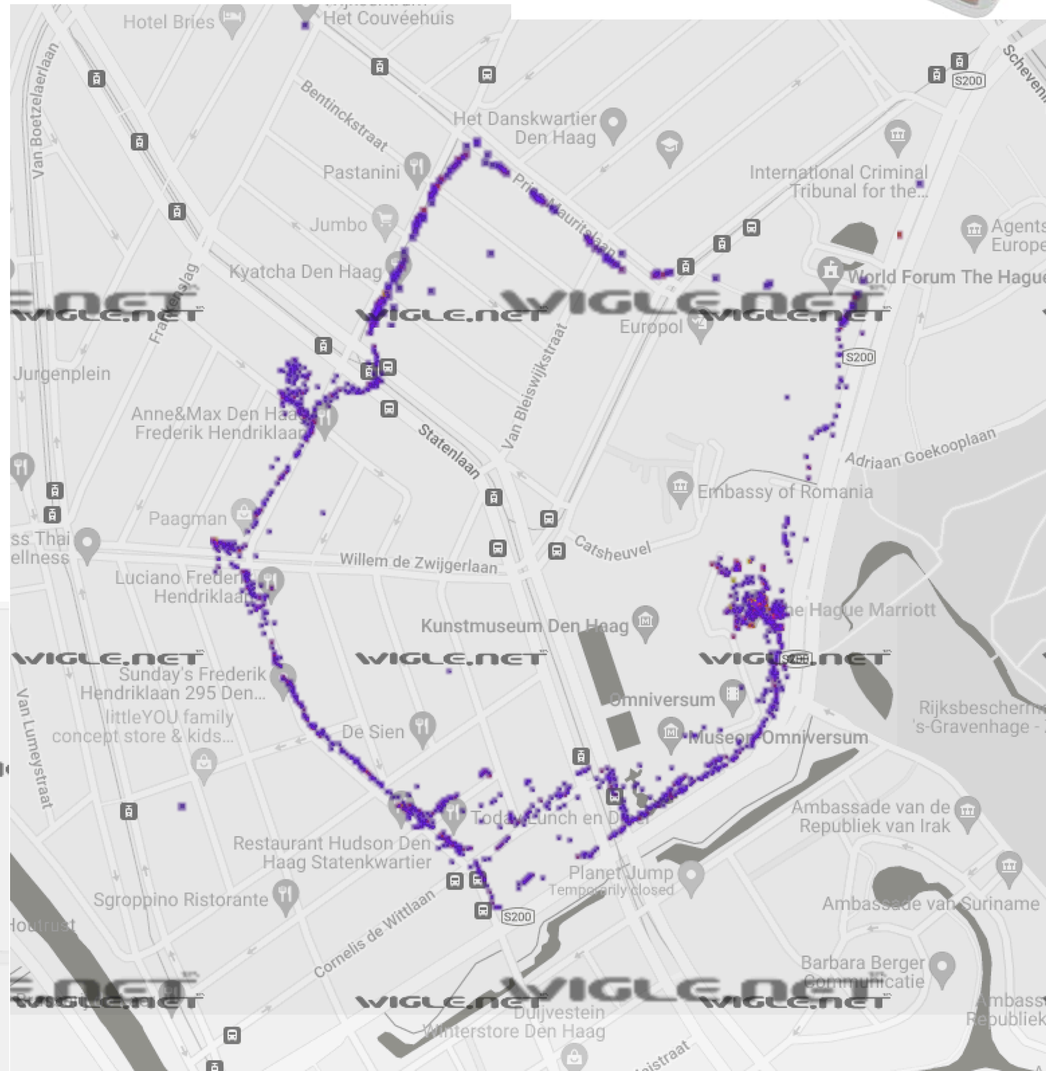


Netherlands

The Hague

- Hardwear.io 2021: Sniffer wouldn't boot :'(
- Hardwear.io 2022: Minimal GPS from when I wandered around outside the hotel
- First time I noticed Flippers...

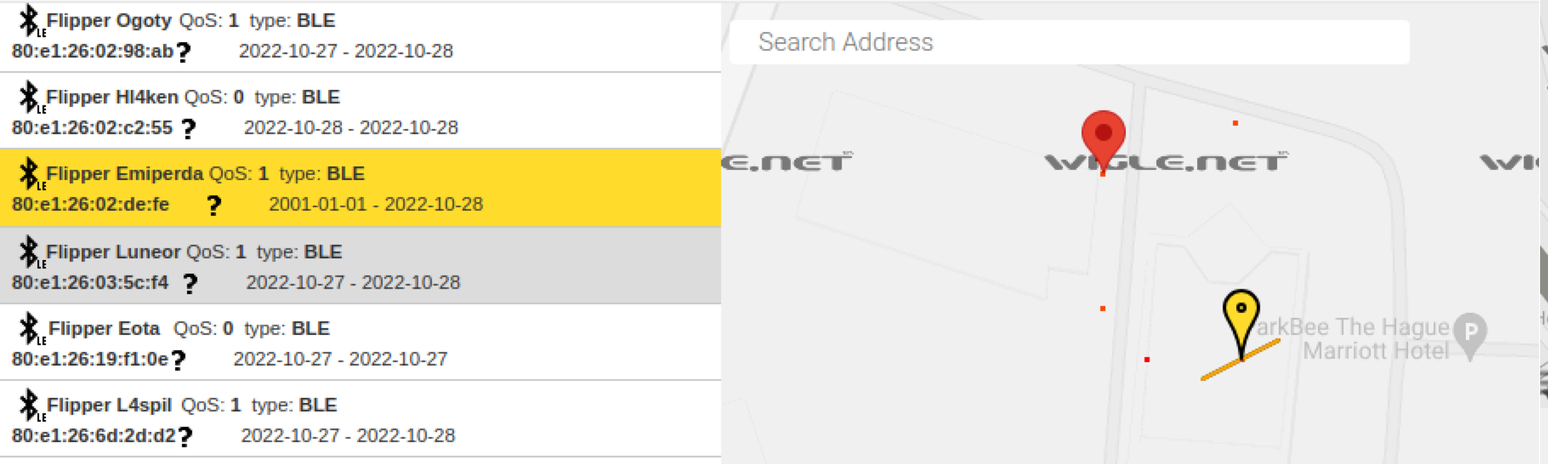


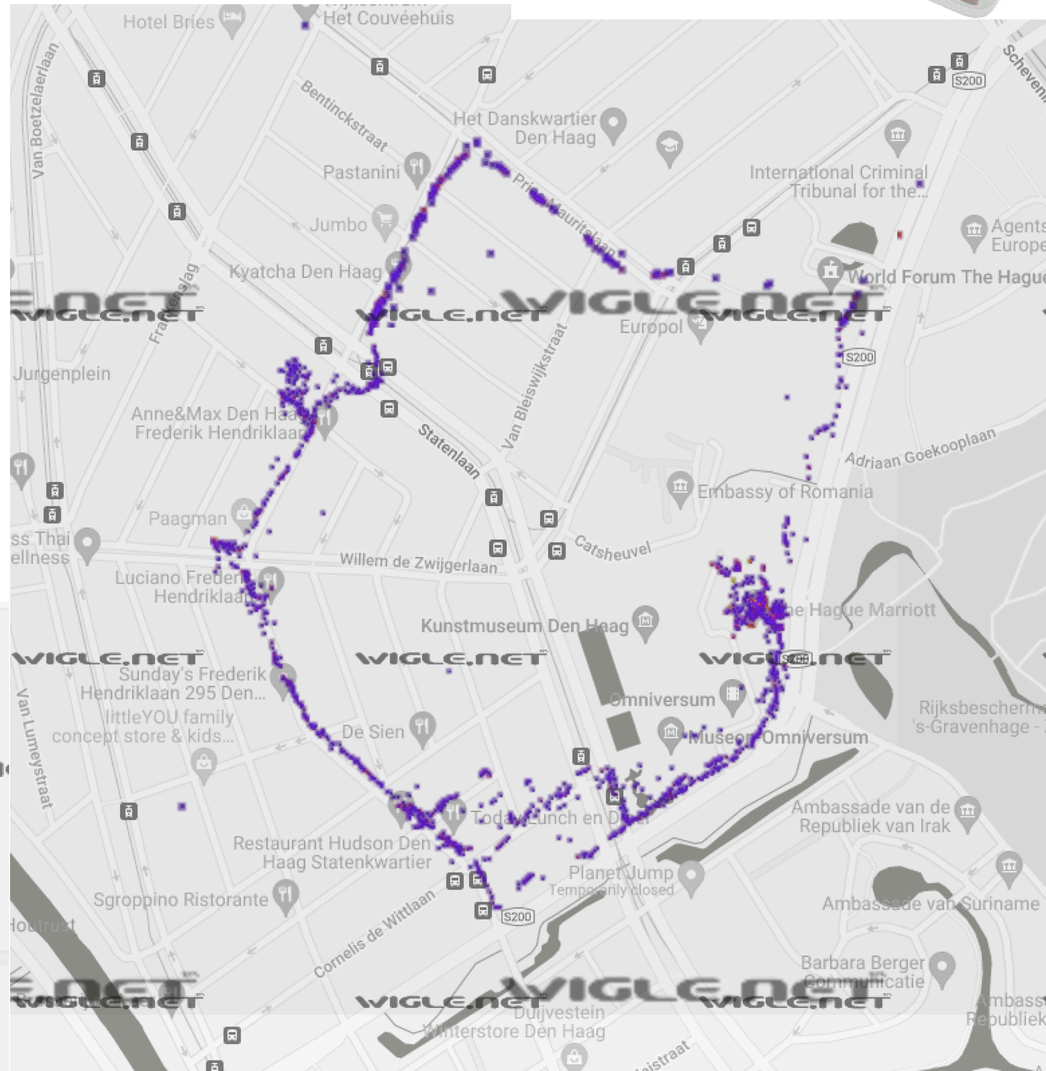


Netherlands

The Hague

- Hardwear.io 2021: Sniffer wouldn't boot :'(
- Hardwear.io 2022: Minimal GPS from when I wandered around outside the hotel
- First time I noticed Flippers...
  - We'll come back to those later



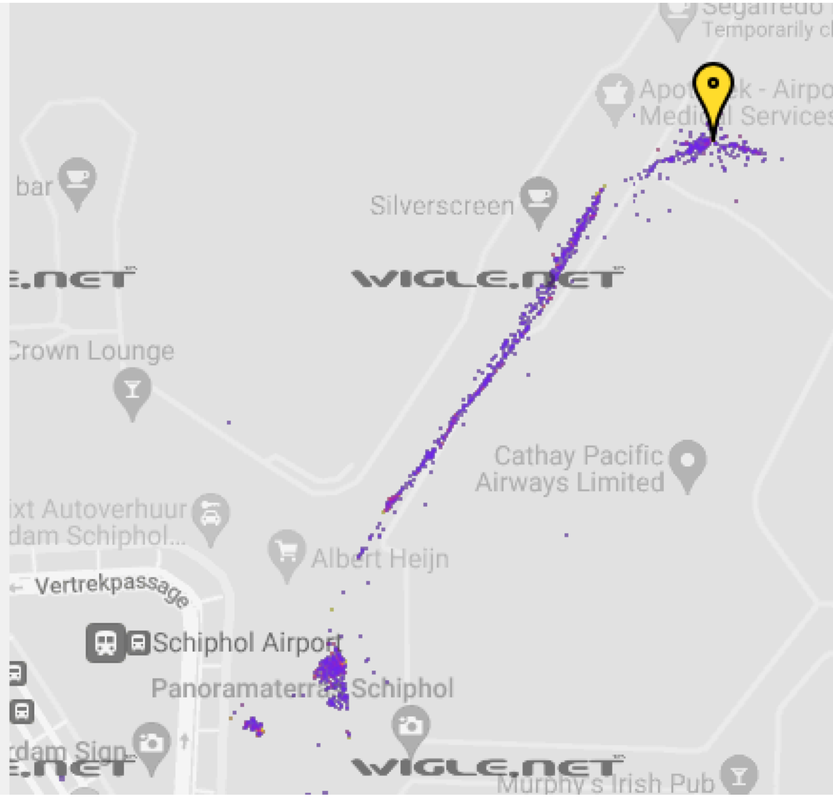


Netherlands

AMS Airport

- These "Melomandia 1+" earbuds apparently beacon separately for the left vs. right ear...which I hadn't seen before

QoS: **0** type: **BLE**	
00:1b:66:0f:43:f7 ?	2022-10-29 - 2022-10-29
PROCHBT001 QoS: **2** type: **BLE**	
00:1c:97:19:8f:f1 ?	2022-10-29 - 2023-02-02
QoS: **0** type: **BLE**	
00:1d:02:b3:0d:79 ?	2001-01-01 - 2022-10-29
Melomania 1+ R QoS: **0** type: **BT**	
00:1f:f0:13:44:c2 ?	2022-10-29 - 2022-10-29
Melomania 1+ L QoS: **0** type: **BT**	
00:1f:f0:13:7b:7f ?	2022-10-29 - 2022-10-29
QoS: **0** type: **BLE**	
00:21:2f:be:a6:af ?	2022-10-29 - 2022-10-29
QoS: **0** type: **BLE**	
00:2d:81:fd:32:89 ?	2022-10-29 - 2022-10-29
QoS: **0** type: **BLE**	
00:37:f6:6a:0a:5d ?	2022-10-29 - 2022-10-29
QoS: **0** type: **BLE**	
00:39:d7:8f:da:a5 ?	2022-10-29 - 2022-10-29



https://www.cambridgeaudio.com/usa/en/products/headphones/melomania-1-plus

Netherlands

AMS Airport

- These "Melomandia 1+" earbuds apparently beacon separately for the left vs. right ear...which I hadn't seen before

QoS: **0** type: **BLE**
00:1b:66:0f:43:f7 ? 2022-10-29 - 2022-10-29

PROCHBT001 QoS: **2** type: **BLE**
00:1c:97:19:8f:f1 ? 2022-10-29 - 2023-02-02

QoS: **0** type: **BLE**
00:1d:02:b3:0d:79 ? 2001-01-01 - 2022-10-29

Melomania 1+ R QoS: **0** type: **BT**
00:1f:f0:13:44:c2 ? 2022-10-29 - 2022-10-29

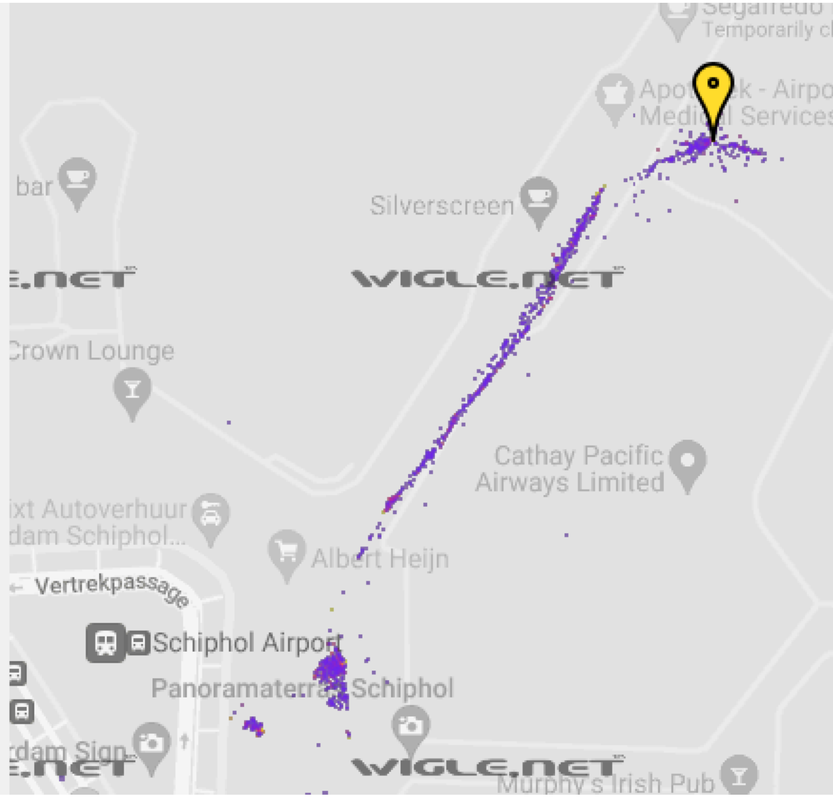
Melomania 1+ L QoS: **0** type: **BT**
00:1f:f0:13:7b:7f ? 2022-10-29 - 2022-10-29

QoS: **0** type: **BLE**
00:21:2f:be:a6:af ? 2022-10-29 - 2022-10-29

QoS: **0** type: **BLE**
00:2d:81:fd:32:89 ? 2022-10-29 - 2022-10-29

QoS: **0** type: **BLE**
00:37:f6:6a:0a:5d ? 2022-10-29 - 2022-10-29

QoS: **0** type: **BLE**
00:39:d7:8f:da:a5 ? 2022-10-29 - 2022-10-29



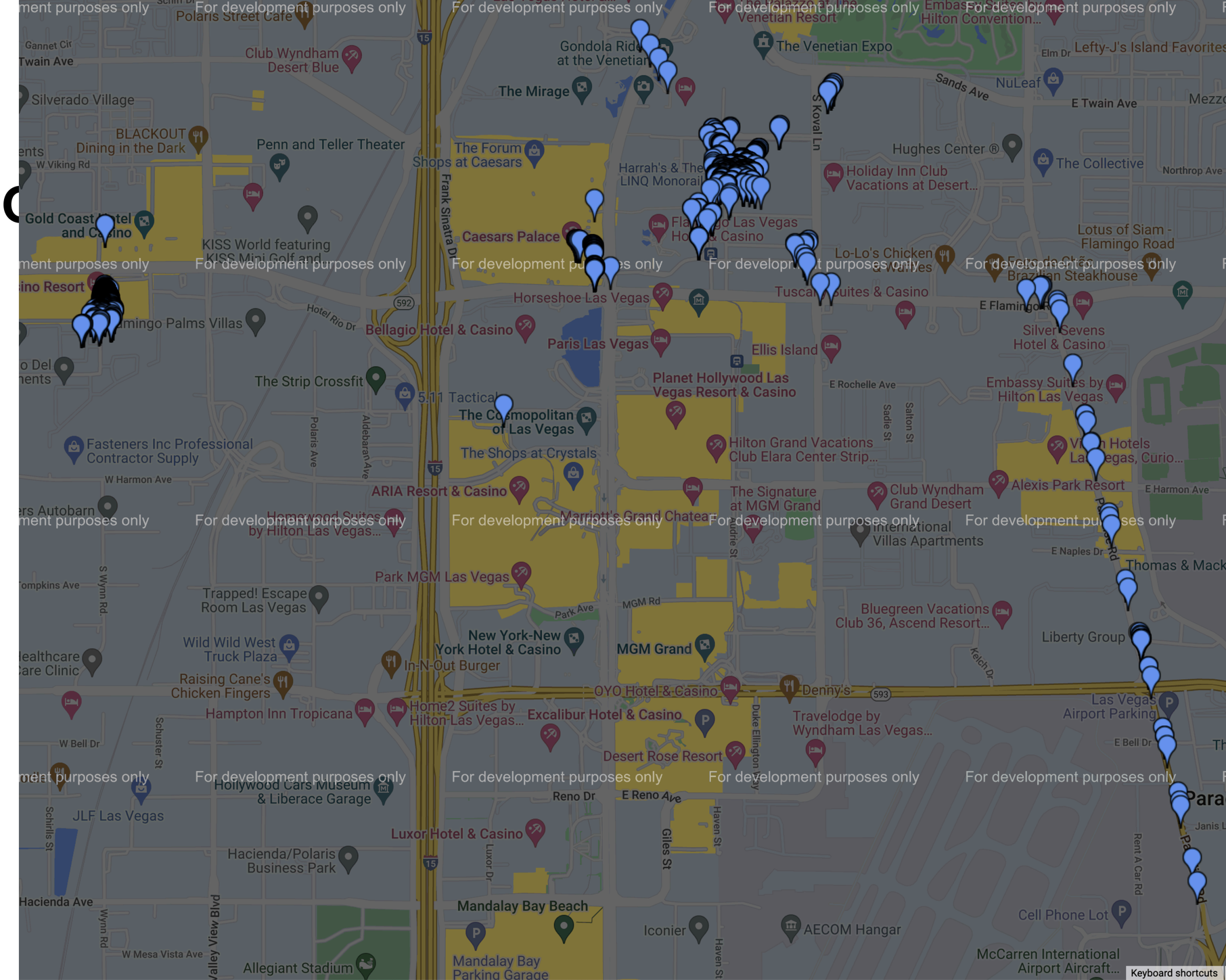
https://www.cambridgeaudio.com/usa/en/products/headphones/melomania-1-plus

Las Vegas

RingZer0 & DEF CON 2023

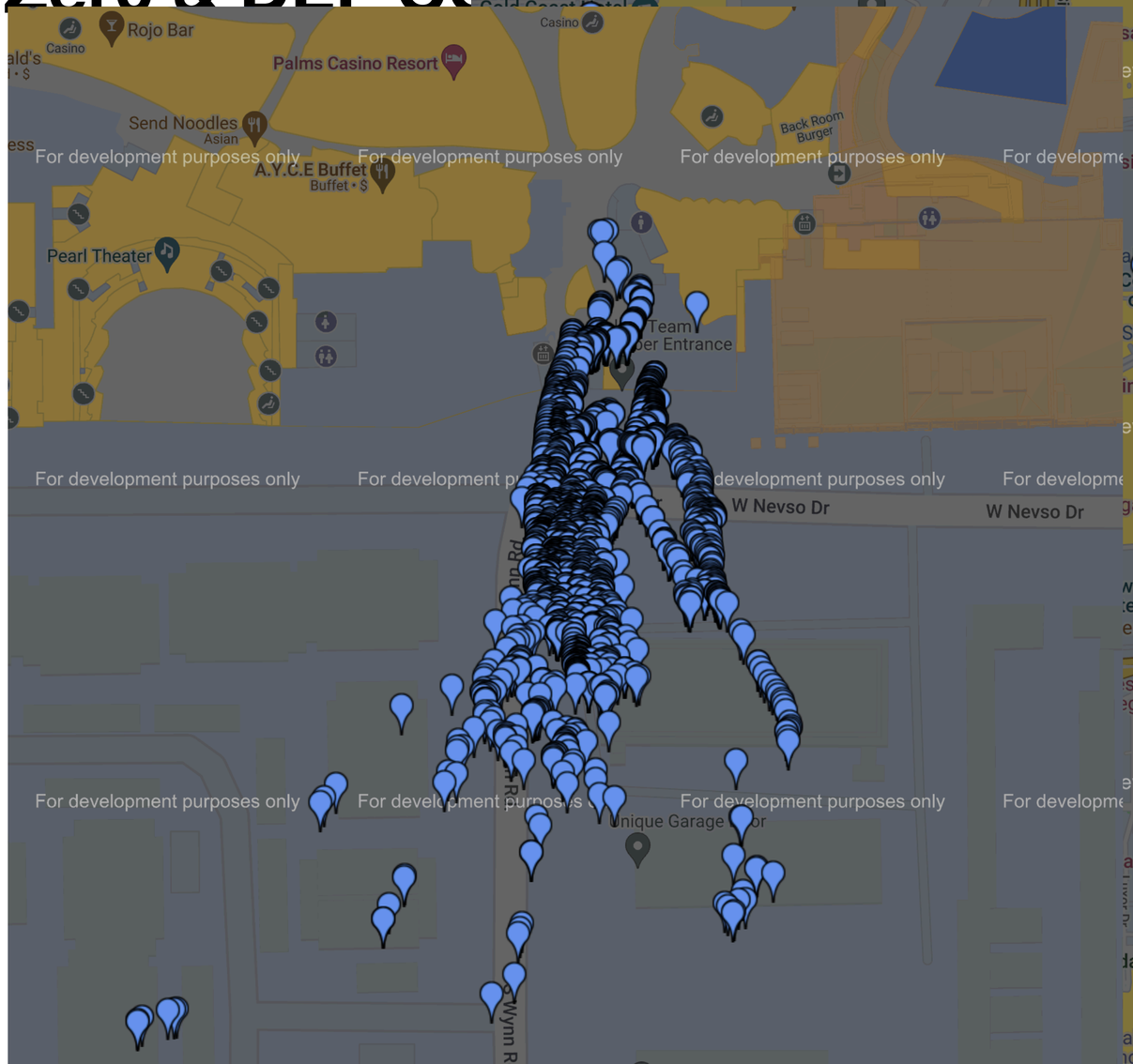
Las Vegas

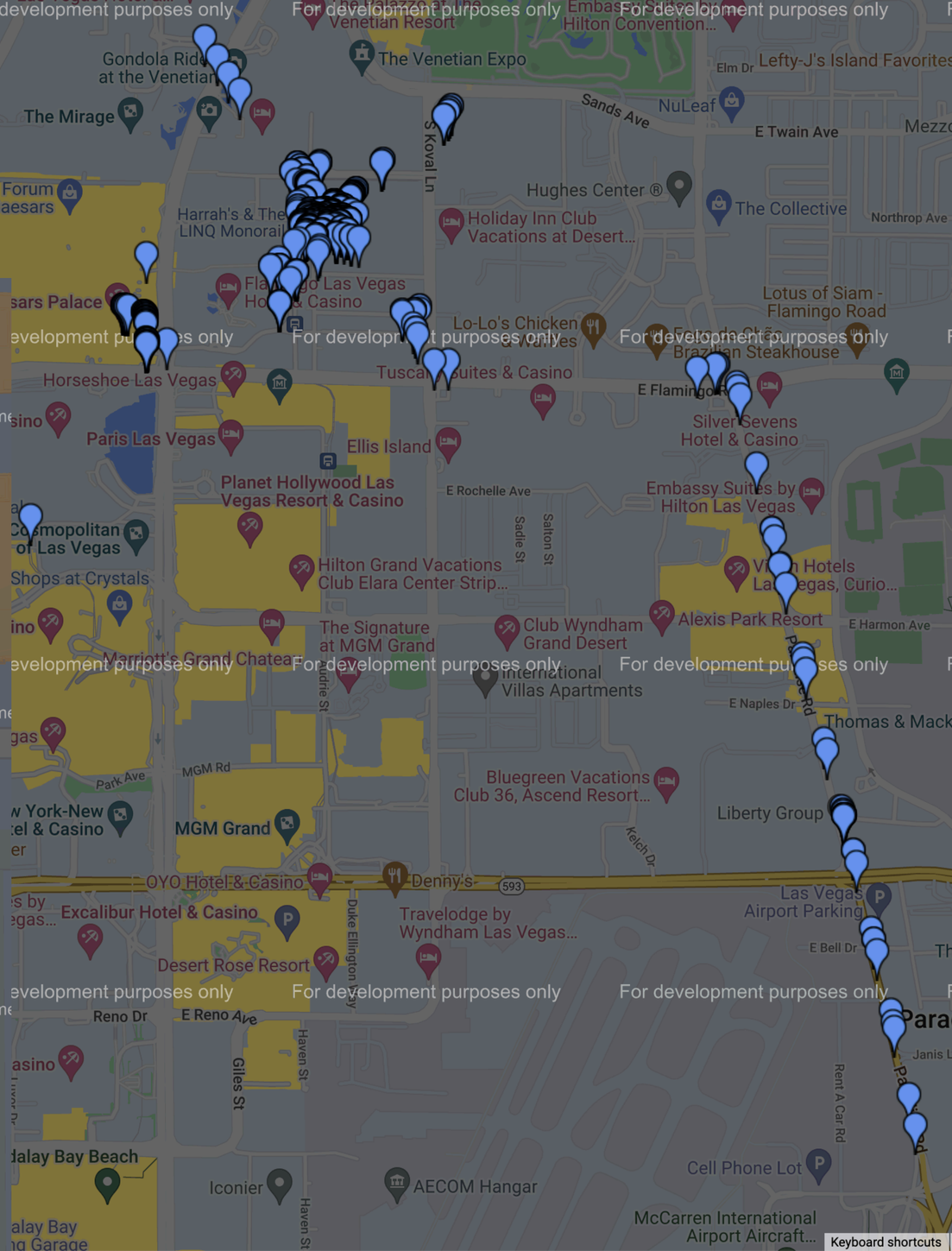
RingZer0 & DEF CO



Las Vegas

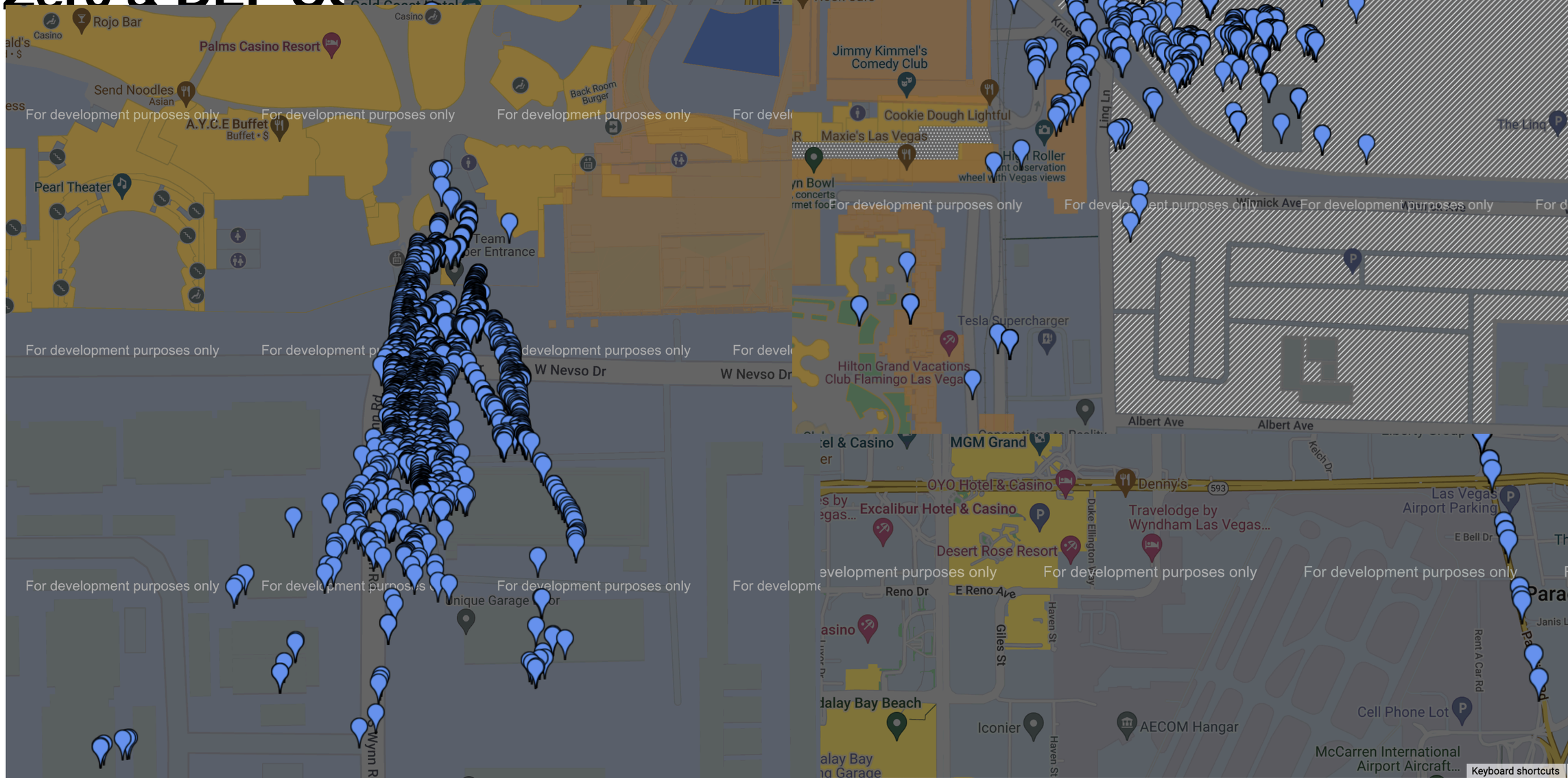
RingZer0 & DEF CO





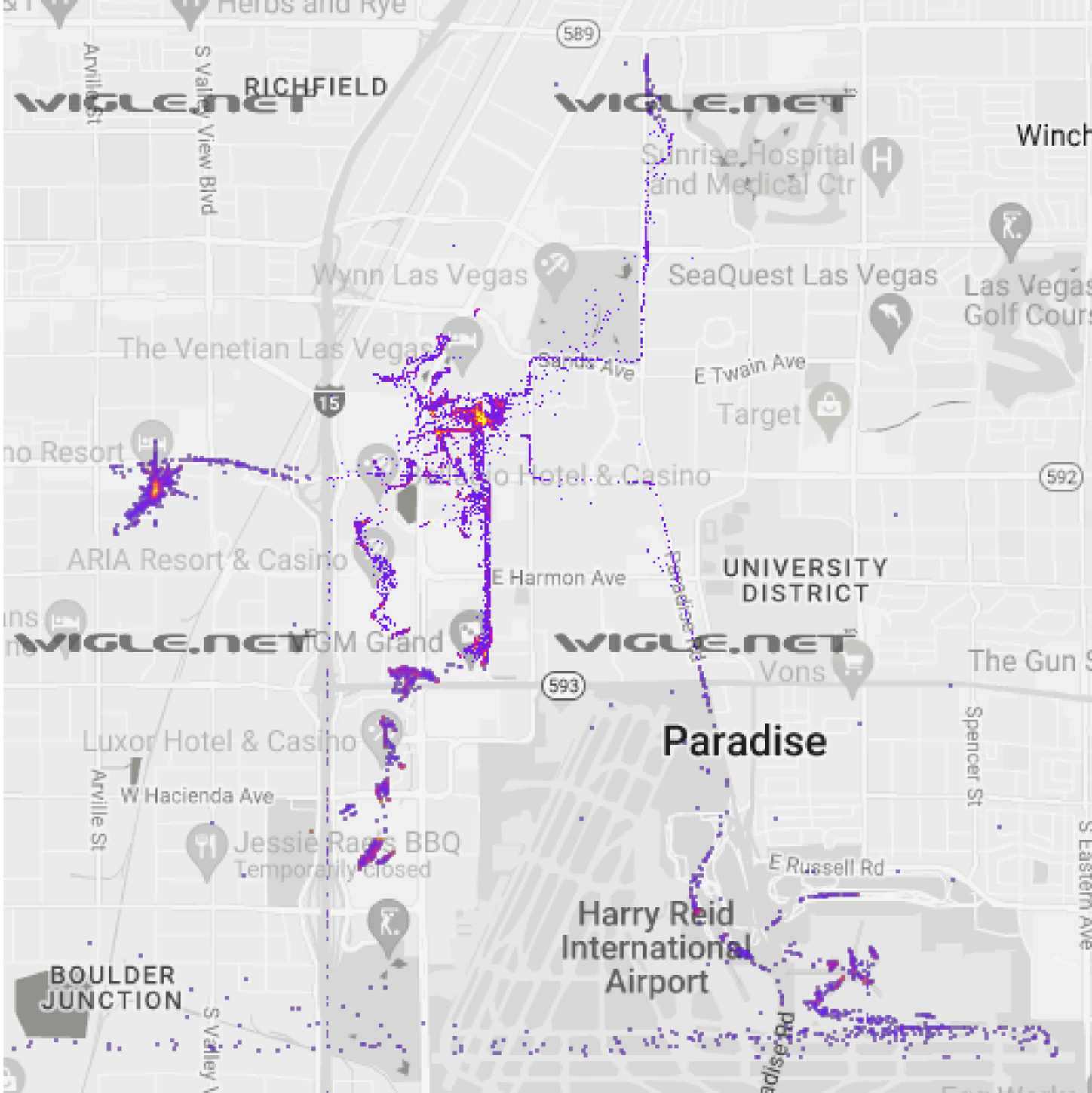
Las Vegas

RingZer0 & DEF CO



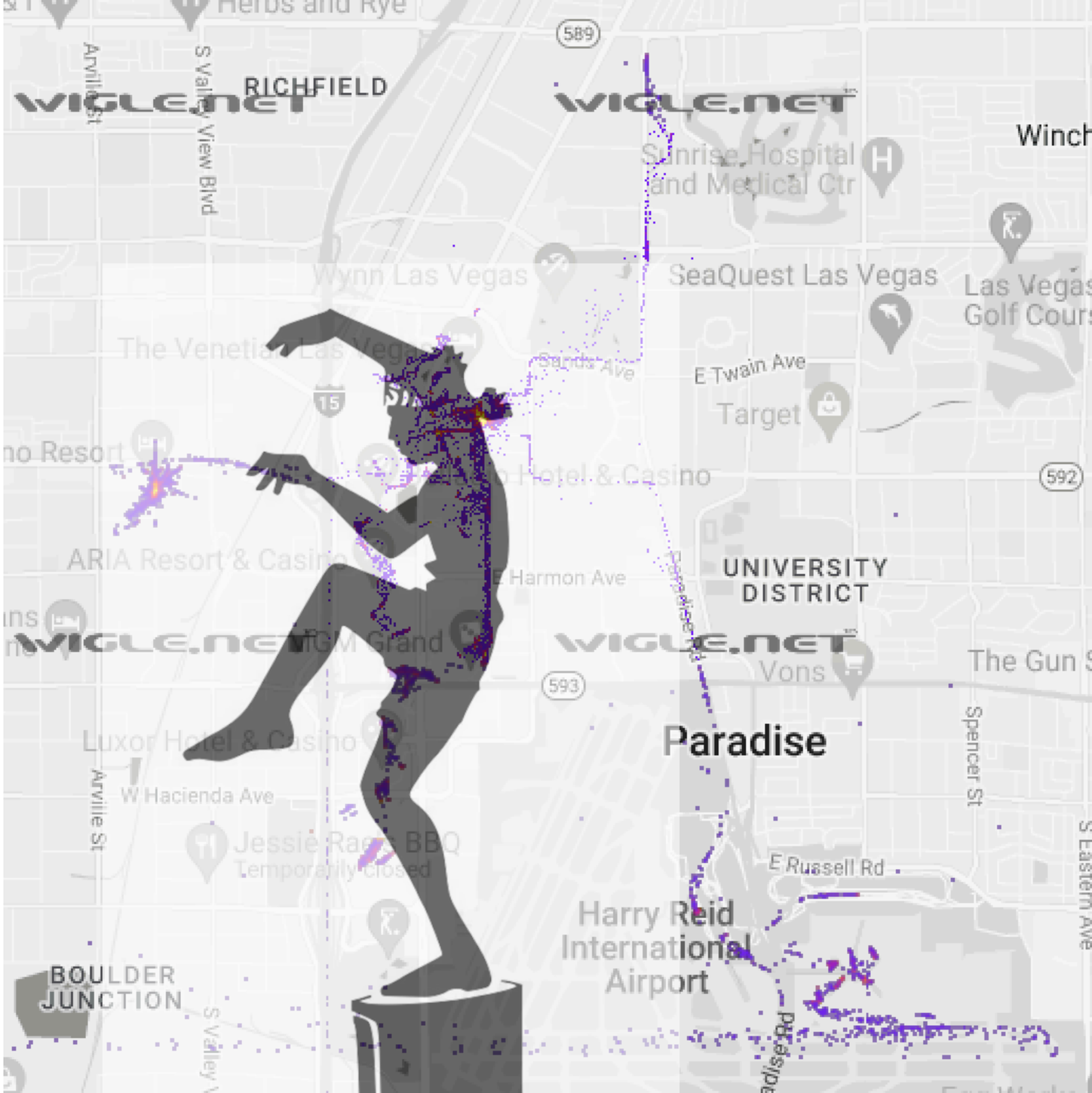
Las Vegas

RingZer0 & DEF CON 2023



Las Vegas

RingZer0 & DEF CON 2023



Las Vegas

RingZer0.Training 2023 @ Palms

- Saw 1347 unique *named* devices from Aug 5-8 at Palms casino
- Misc I noticed:
  - 7 Flippers
    - It's almost as if they're a secret signal that hackers are around ;)
      - How many do you think I'll find at RSA? ;)
  - 3 Glucose monitors (2 Dexcom, 1 Abbot)
  - One BT-enabled LG webOS TV *per room* in the *good* tower (not the tower I was staying in ;))

Las Vegas

RingZer0.Training 2023 @ Palms

- Regex: ^PayRange$ but also ^BlueRadios[A-F0-9]{6}$
  - Semantically: the [A-F0-9]{6} are the last 6 digits of the BDADDR
- Device would advertise as PayRange but send back e.g. BlueRadios169B67 when asked what its name is. Some would also reply "BluKeyPayRange"

https://shop.payrange.com/industries/vending/

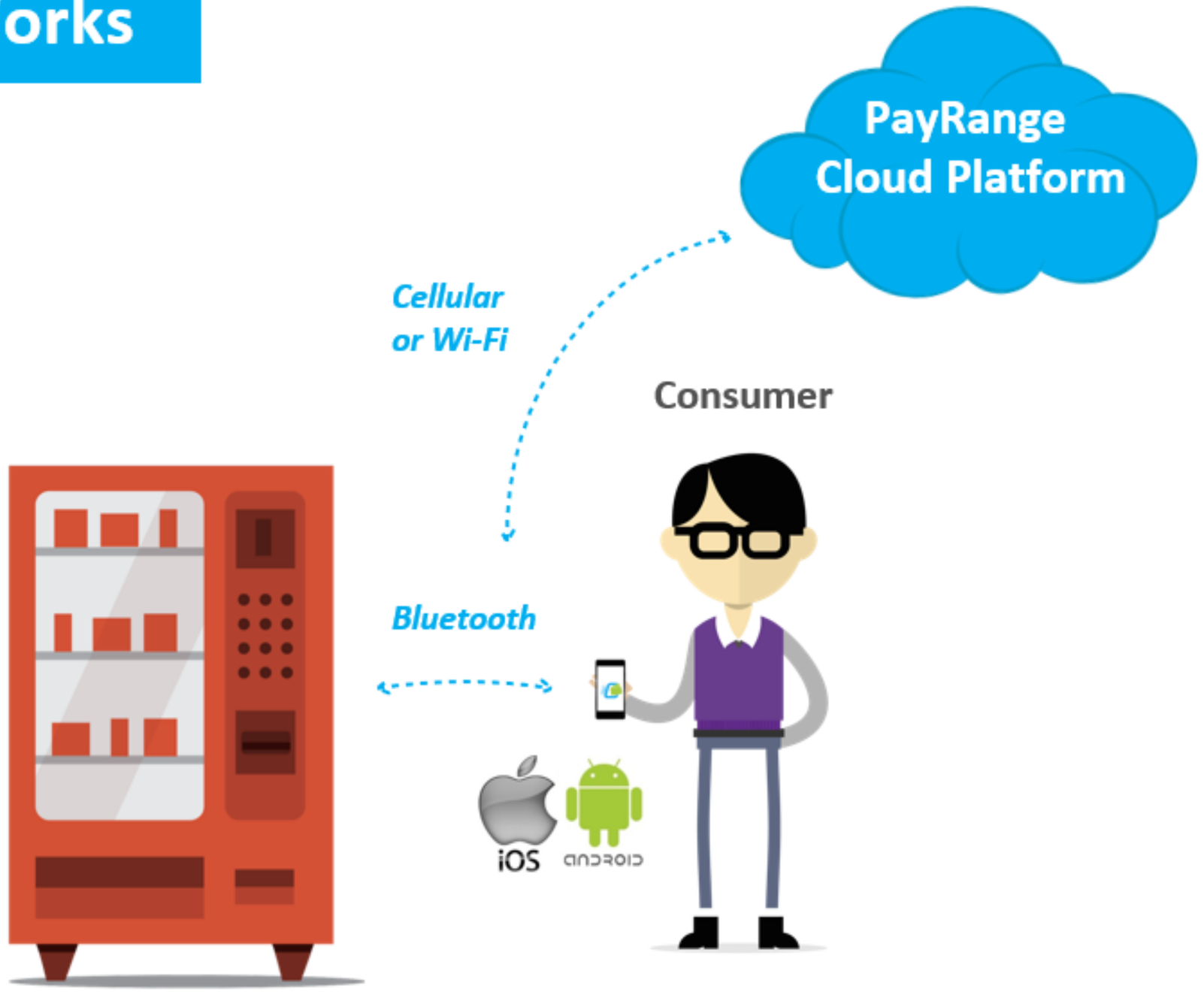
Las Vegas

RingZer0.Training 2023 @ Palms

- Regex: ^PayRange$ but also ^BlueRadios[A-F0-9]{6}$
  - Semantically: the [A-F0-9]{6} are the last 6 digits of the BDADDR
- Device would advertise as PayRange but send back e.g. BlueRadios169B67 when asked what its name is. Some would also reply "BluKeyPayRange"

https://shop.payrange.com/industries/vending/

How It Works



67 when asked what

uKey for
ending

LIMITED TIME OFFER!
OFFER ENDS AUGUST 31

~~.00~~ $49.95

ble options:

ct Assurance Plan – $4.99

selection

$54.94

Las Vegas

RingZer0.Training 2023 @ Palms

- Uses "BlueRadios, Inc." *bluetooth module* based on its (public) BDADDR and manufacturer-specific data
  - Which is actually just a Nordic NRF52840 chip

```
For bdaddr = ec:fe:7e:16:5d:f1:
        Company Name by IEEE OUI (ec:fe:7e): BlueRadios, Inc

        No BTC Extended Inquiry Result Device info.

        DeviceName: PayRange
                In BT LE Data (LE_bdaddr_to_name), bdaddr_ranc
                        NamePrint: match found for ^PayRange$:
                This was found in an event of type 19 which cc

        No UUID16s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x0085 (BlueRadios, Inc) -
```

https://www.blueradios.com/nBlue%20BR-LE5.0-S1A%20Summary%20Datasheet.pdf

Las

RingZ

- Uses
  manu
  - Wh

```
For bdaddr = ec:fe
        Company Na

        No BTC Ext

        DeviceName
                In

                Th

        No UUID16s

        No transmi

        No Appeara

        Manufactur
                De
```

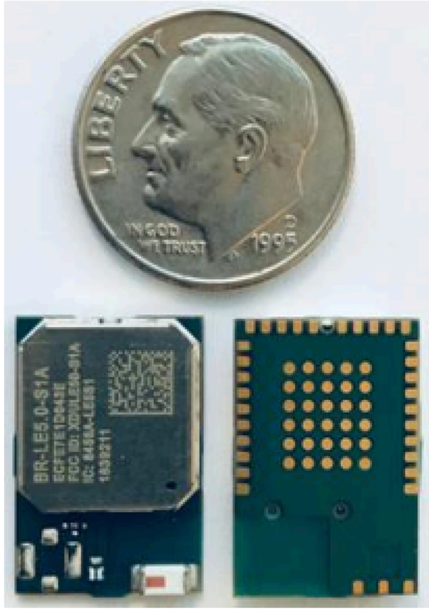
https://www.blueradios.

*n*Blue BR-LE5.0-S1A Module Summary Datasheet
Copyright © 2002-2021 BlueRadios, Inc.
v1.3

BT5.0 Low Energy Single Mode Class 1 SoC Module

*n*Blue™ BR-LE5.0-S1A (nRF52840)

- ***AT HOME. AT WORK. ON THE ROAD.*** ***USING BT5.0 LOW ENERGY WIRELESS TECHNOLOGY MEANS TOTAL FREEDOM FROM THE CONSTRAINTS AND CLUTTER OF WIRES IN YOUR LIFE.***
- **FCC, IC, CE, RoHS, and BT5.0 Certified ISM 2.4GHz module supporting BT5.0 high speed mode, long range mode and advertising extensions. Can also support BT5.0 Mesh, 802.15.4 for Thread and Zigbee, ANT or proprietary 2.4Ghz.**
- **Utilizes the Nordic nRF52840 SoC. 64Mhz ARM® Cortex™ M4F 32-bit processor with FPU, 1MB Flash, 256K RAM, built in DC-DC converter and ARM CryptoCell cryptographic accelerator.**
- **Programmable output power from -40dBm to +8dBm for short to long range applications.**
- **Over 1000 meter line of site distance with integrated antenna. External antenna can be connected to RF_OUT pad or through optional u.FL connector (requires moving RF path resistor).**
- **Can be externally controlled via simple ASCII AT commands over UART, USB and BT5.0, or programmed with custom applications embedded in the module.**



FCC CE RoHS -Certified-

Las

RingZ

- Uses
  manu
  - Wh

```
For bdaddr = ec:fe
        Company Na

        No BTC Ext

        DeviceName
                In

                Th

        No UUID16s

        No transmi

        No Appeara

        Manufactur
                De
```

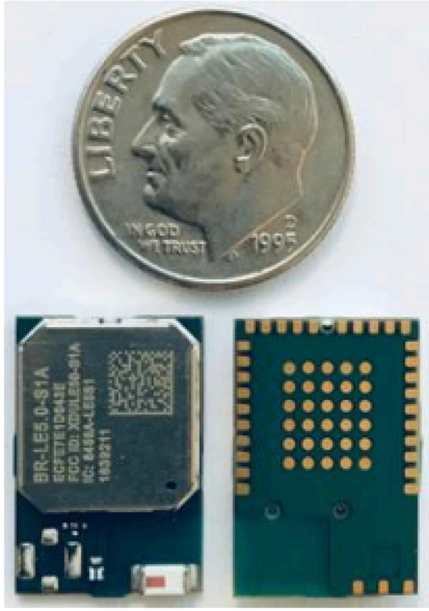
https://www.blueradios.

*n*Blue BR-LE5.0-S1A Module Summary Datasheet
Copyright © 2002-2021 BlueRadios, Inc.
v1.3

BT5.0 Low Energy Single Mode Class 1 SoC Module

*n*Blue™ BR-LE5.0-S1A (nRF52840)

- *AT HOME. AT WORK. ON THE ROAD. USING BT5.0 LOW ENERGY WIRELESS TECHNOLOGY MEANS TOTAL FREEDOM FROM THE CONSTRAINTS AND CLUTTER OF WIRES IN YOUR LIFE.*
- FCC, IC, CE, RoHS, and BT5.0 Certified ISM 2.4GHz module supporting BT5.0 high speed mode, long range mode and advertising extensions. Can also support BT5.0 Mesh, 802.15.4 for Thread and Zigbee, ANT or proprietary 2.4Ghz.
- Utilizes the Nordic nRF52840 SoC 64Mhz ARM® Cortex™ M4F 32-bit processor with FPU, 1MB Flash, 256K RAM, built in DC-DC converter and ARM CryptoCell cryptographic accelerator.
- Programmable output power from -40dBm to +8dBm for short to long range applications.
- Over 1000 meter line of site distance with integrated antenna. External antenna can be connected to RF_OUT pad or through optional u.FL connector (requires moving RF path resistor).
- Can be externally controlled via simple ASCII AT commands over UART, USB and BT5.0, or programmed with custom applications embedded in the module.



FCC CE RoHS -Certified-

Mini-Takeaway

Chip identification

- Identification of a BT module-maker can give you a *set* of possible chips that they use in their modules
  - And which chip a device is using, is one of the things I want to know!

Las Vegas
DEF CON 2023

- I can't tell you how many unique named devices I saw, because I was also explicitly walking all around nearby casinos every morning to collect more data

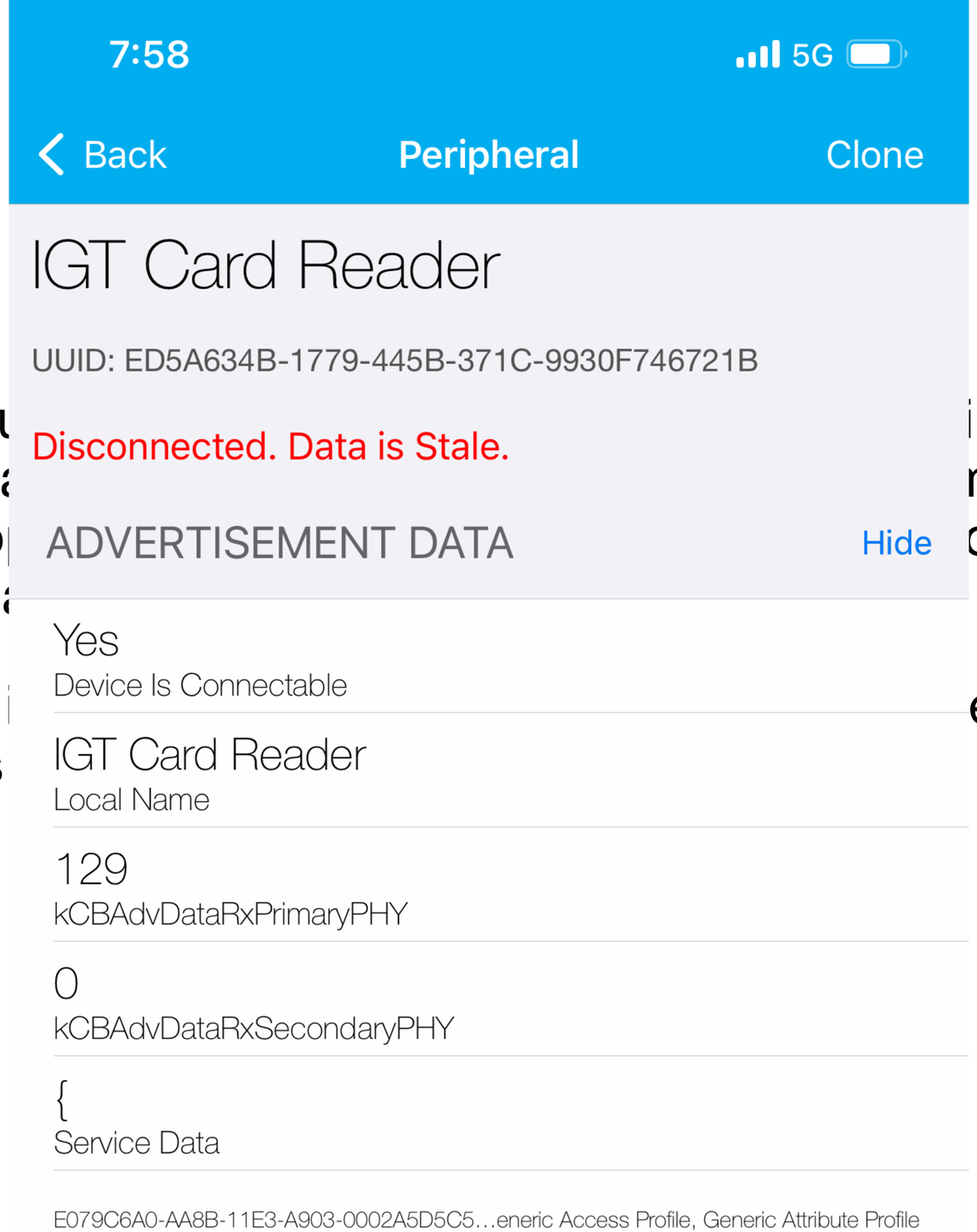
Las Vegas
DEF CON 2023

- When walking around, I would often have basic BT scanning phone apps open, so that if I saw anything with an interesting new name I hadn't seen before, I could stop and give my scanner an opportunity to potentially collect more data about it

- When I wandered into the Wynn casino area, all of a sudden my phone app lit up with all sorts of ^IGT Card Reader$ entries!

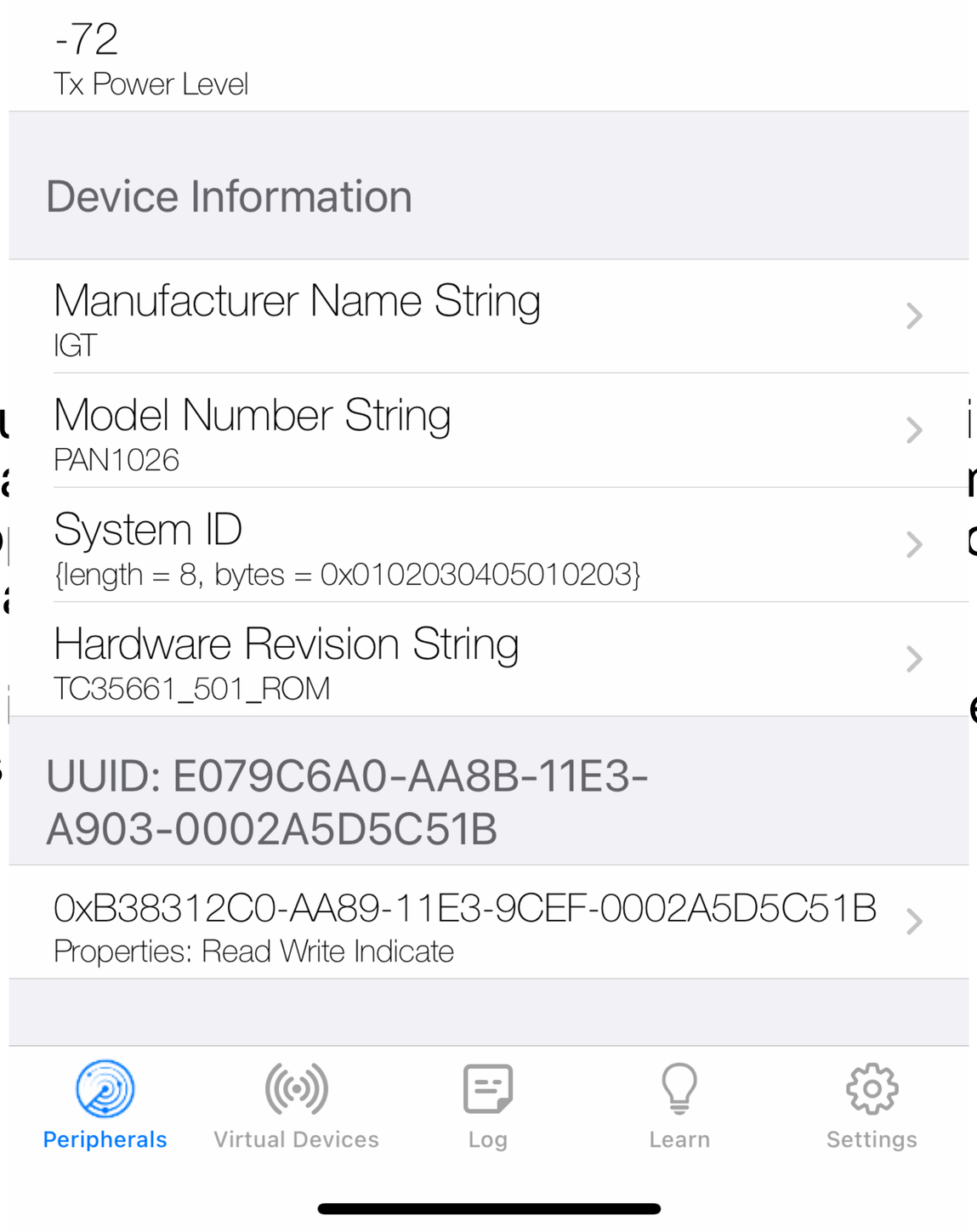
Las Vegas
DEF CON 2023

- When walking arou ing phone apps open, so that if I sa ne I hadn't seen before, I could sto o potentially collect more data a
- When I wandered i en my phone app lit up with all sorts



Las Vegas
DEF CON 2023

- When walking arou ing phone apps open, so that if I sa ne I hadn't seen before, I could sto o potentially collect more data a
- When I wandered en my phone app lit up with all sorts



Las Vegas
DEF CON 2023

- So what's IGT?
- ~~Gambling~~ Gaming machine hardware maker!

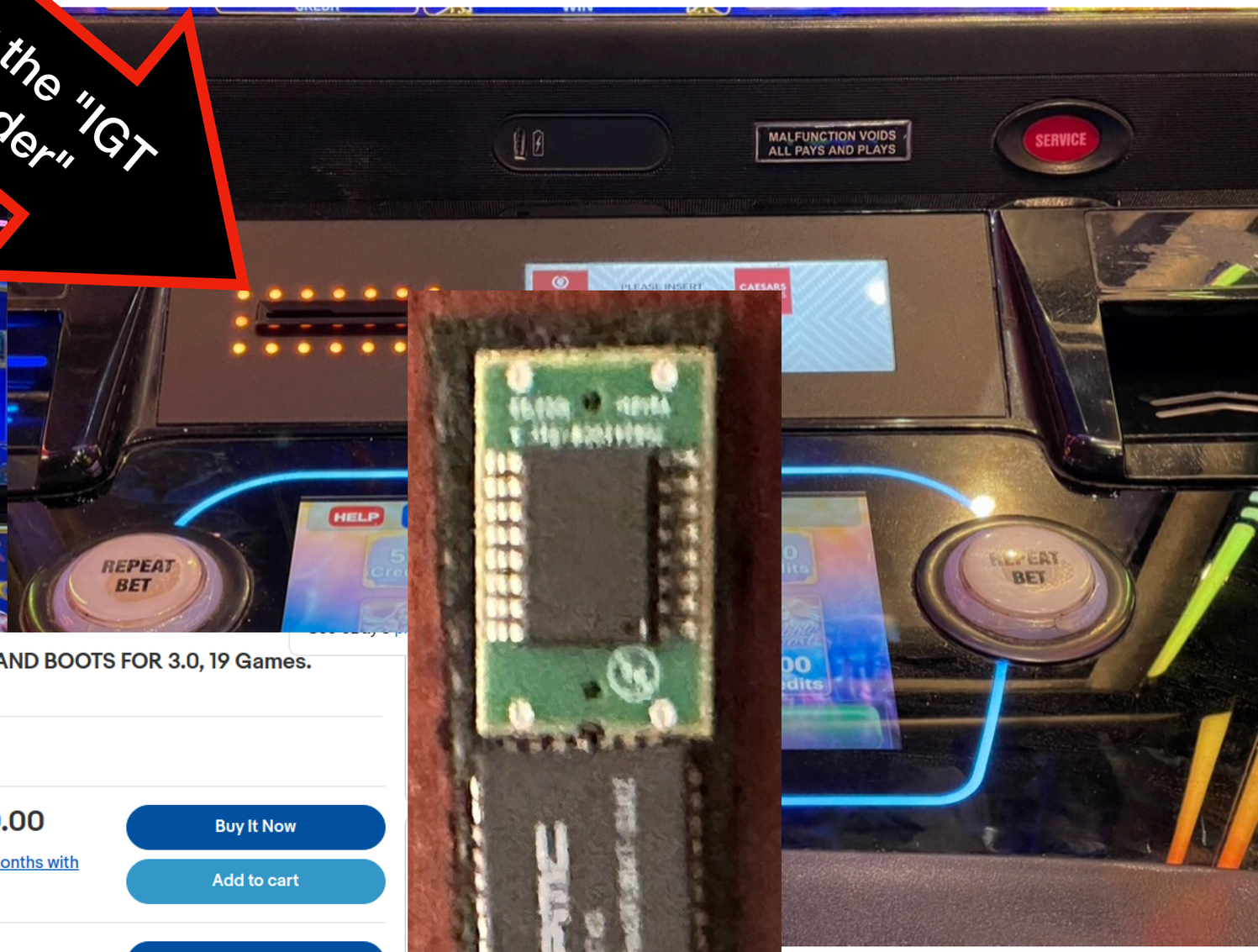
https://store.igt.com/32916691

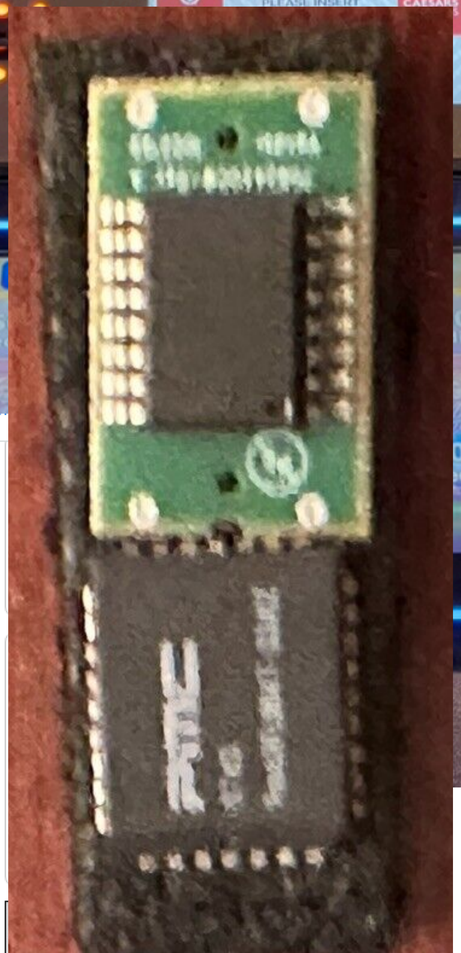
IGT
OCEAN Magic
WILD

CASH OUT
MALFUNCTION VOIDS ALL PAYS AND PLAYS
SERVICE
CAESARS PALACE LAS VEGAS
PLEASE INSERT PLAYER CARD
CAESARS REWARDS
IGT
HELP
LOCK BUTTON PANEL
REPEAT BET
50 Credits
100 Credits
150 Credits
200 Credits
250 Credits
100 Credits
200 Credits
300 Credits
400 Credits
500 Credits
REPEAT BET

Nominally the "IGT Card Reader"
IGT
OCEAN Magic
WILD
MALFUNCTION VOIDS ALL PAYS AND PLAYS
SERVICE
CAESARS PALACE
PLEASE INSERT PLAYER CARD
CAESARS REWARDS
IGT
HELP
LOCK BUTTON PANEL
50 Credits
100 Credits
150 Credits
200 Credits
250 Credits
100 Credits
200 Credits
300 Credits
400 Credits
500 Credits
REPEAT BET
REPEAT BET
REPEAT BET

Nominally the "IGT Card Reader"





IGT AVP FAMILY 20 SSD AND BOOTS FOR 3.0, 19 Games.

3 watched in the last 24 hours

Condition: Used

Price: US $600.00

$28.81 for 24 months with PayPal Credit*

Buy It Now

Add to cart

Best Offer:

Make offer

♡ Add to watchlist

Las Vegas
DEF CON 2023

- So what's IGT?
- ~~Gambling~~ Gaming machine hardware maker!

https://www.igt.com/products-and-services/gaming/systems/-/media/248ae3be76cc4cd8a60cd213357e9e0e.ashx

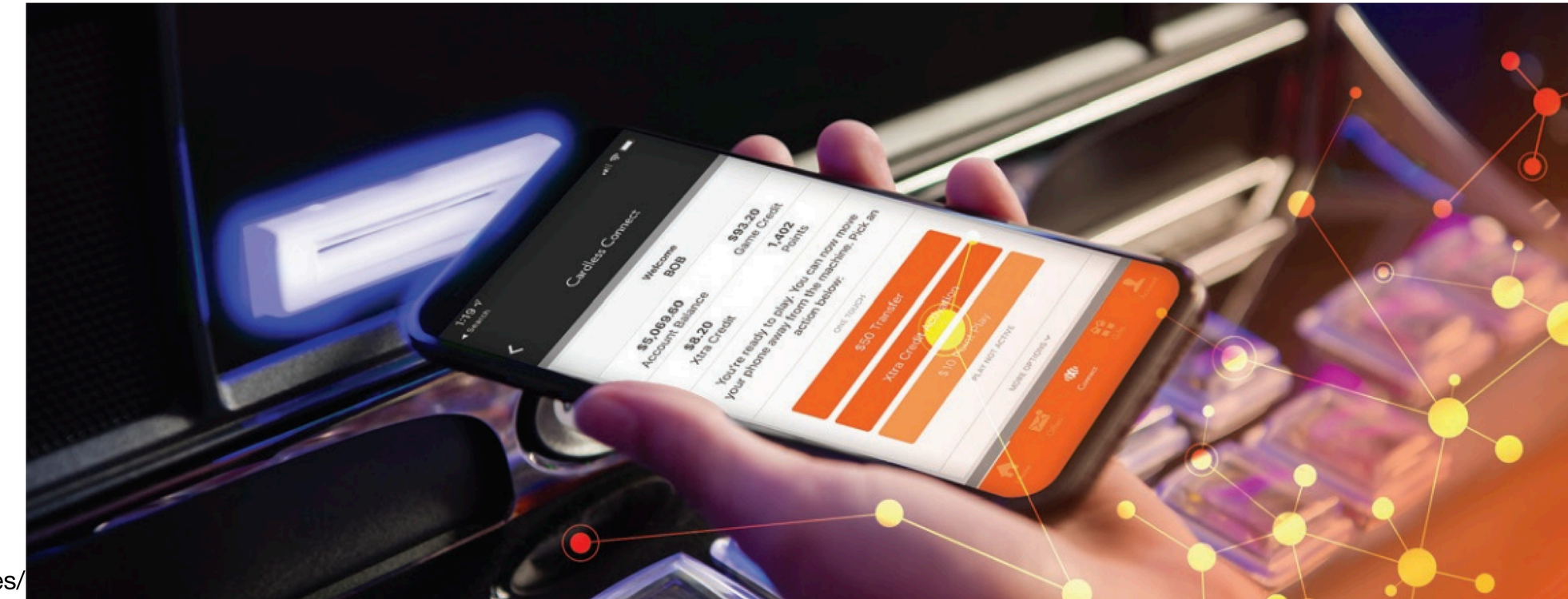
Las Vegas
DEF CON 2023

- So what's IGT?
- ~~Gambling~~ Gami

Resort Wallet works by:

- Leveraging branding (player downloads property branded casino app)
- Leveraging phone biometrics through app sign in authentication (face ID, pin, fingerprint ID)
- Multiple methods (player funds wallet)
- Ubiquitous (player taps bluetooth sensor)
- Icons, symbols, text (players presses transfer)
- Funds are transferred

Players add funds to an EGM by tapping a button on their mobile phone enabling funds to be deposited directly to the EGM, reducing or eliminating the need to carry cash or wait in line at an ATM. Operators experience reduced overhead due to ticket or cash related issues, such as a ticket printer jam or lack of ticket stock. In addition, operators have less overhead related to cash and ticket handling.



https://www.igt.com/products-and-services/

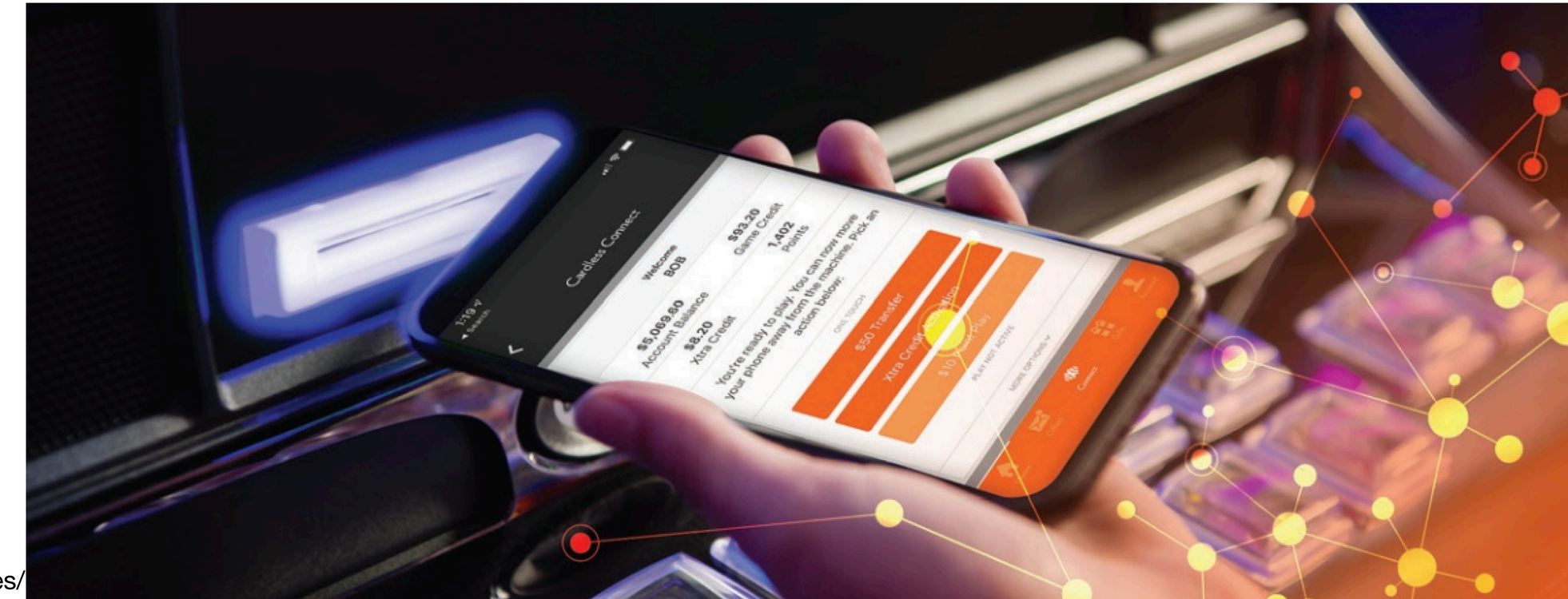
Las Vegas
DEF CON 2023

- So what's IGT?
- ~~Gambling~~ Gami

Resort Wallet works by:

- Leveraging branding (player downloads property branded casino app)
- Leveraging phone biometrics through app sign in authentication (face ID, pin, fingerprint ID)
- Multiple methods (player funds wallet)
- Ubiquitous (player taps bluetooth sensor)
- Icons, symbols, text (players presses transfer)
- Funds are transferred

Players add funds to an EGM by tapping a button on their mobile phone enabling funds to be deposited directly to the EGM, reducing or eliminating the need to carry cash or wait in line at an ATM. Operators experience reduced overhead due to ticket or cash related issues, such as a ticket printer jam or lack of ticket stock. In addition, operators have less overhead related to cash and ticket handling.



https://www.igt.com/products-and-services/

IGT Card Reader

UUID: ED5A634B-1779-445B-371(

Disconnected. Data is Stale.

ADVERTISEMENT DATA

Yes
Device Is Connectable

IGT Card Reader
Local Name

129
kCBAdvDataRxPrimaryPHY

0
kCBAdvDataRxSecondaryPHY

{
Service Data

E079C6A0-AA8B-11E3-A903-0002A5D5C5…en
Service UUIDs

713458723.6085089
kCBAdvDataTimestamp

-72
Tx Power Level

Resort Wallet works by:

- Leveraging branding (player downloads property branded casino app)
- Leveraging phone biometrics through app sign in authentication (face ID, pin, fingerprint ID)
- Multiple methods (player funds wallet)
- Ubiquitous (player taps bluetooth sensor)
- Icons, symbols, text (players presses transfer)
- Funds are transferred

Players add funds to an EGM by tapping a button on their mobile phone enabling funds to be deposited directly to the EGM, reducing or eliminating the need to carry cash or wait in line at an ATM. Operators experience reduced overhead due to ticket or cash related issues, such as a ticket printer jam or lack of ticket stock. In addition, operators have less overhead related to cash and ticket handling.

https

IGT Card Reader

UUID: ED5A634B-1779-445B-371(

Disconnected. Data is Stale.

ADVERTISEMENT DATA

Yes
Device Is Connectable

IGT Card Reader
Local Name

129
kCBAdvDataRxPrimaryPHY

0
kCBAdvDataRxSecondaryPHY

{
Service Data

E079C6A0-AA8B-11E3-A903-0002A5D5C5…er
Service UUIDs

713458723.6085089
kCBAdvDataTimestamp

-72
Tx Power Level

Resort Wallet works by:

- Leveraging branding (player downloads property branded casino app)
- Leveraging phone biometrics through app sign in authentication (face ID, pin, fingerprint ID)
- Multiple methods (player funds wallet)
- Ubiquitous (player taps bluetooth sensor)
- Icons, symbols, text (players presses transfer)
- Funds are transferred

Players add funds to an EGM by tapping a button on their mobile phone enabling funds to be deposited directly to the EGM, reducing or eliminating the need to carry cash or wait in line at an ATM. Operators experience reduced overhead due to ticket or cash related issues, such as a ticket printer jam or lack of ticket stock. In addition, operators have less overhead related to cash and ticket handling.

https

IGT Card Reader

UUID: ED5A634B-1779-445B-371(

Disconnected. Data is Stale.

ADVERTISEMENT DATA

Yes
Device Is Connectable

IGT Card Reader
Local Name

129
kCBAdvDataRxPrimaryPHY

0
kCBAdvDataRxSecondaryPHY

{
Service Data

E079C6A0-AA8B-11E3-A903-0002A5D5C5…er
Service UUIDs

713458723.6085089
kCBAdvDataTimestamp

-72
Tx Power Level

Resort Wallet works by:

- Leveraging branding (player downloads property branded casino app)
- Leveraging phone biometrics through app sign in authentication (face ID, pin, fingerprint ID)
- Multiple methods (player funds wallet)
- Ubiquitous (player taps bluetooth sensor)
- Icons, symbols, text (players presses transfer)
- Funds are transferred

Players add funds to an EGM by tapping a button on their mobile phone enabling funds to be deposited directly to the EGM, reducing or eliminating the need to carry cash or wait in line at an ATM. Operators experience reduced overhead due to ticket or cash related issues, such as a ticket printer jam or lack of ticket stock. In addition, operators have less overhead related to cash and ticket handling.

https

Las Vegas
DEF CON 2023

- Where else besides Wynn are there "IGT Card Reader" devices advertising?

IGT Card Reader QoS: 0 type: BLE
00:13:43:42:f5:ca ? 2001-12-31 - 2001-01-01

IGT Card Reader QoS: 0 type: BLE
00:13:43:42:f5:df ? 2001-12-31 - 2001-01-01

IGT Card Reader QoS: 0 type: BLE
00:13:43:42:f5:e0 ? 2001-12-31 - 2001-01-01

IGT Card Reader QoS: 0 type: BLE
00:13:43:42:f5:fd ? 2001-12-31 - 2001-01-01

IGT Card Reader QoS: 0 type: BLE
00:13:43:42:f6:42 ? 2001-12-31 - 2001-01-01

IGT Card Reader QoS: 0 type: BLE
00:13:43:42:f6:4c ? 2001-12-31 - 2001-01-01

IGT Card Reader QoS: 0 type: BLE
00:13:43:42:f6:5f ? 2001-12-31 - 2001-01-01

IGT Card Reader QoS: 0 type: BLE
00:13:43:42:f6:6d ? 2001-12-31 - 2001-01-01

IGT Card Reader QoS: 0 type: BLE
00:13:43:42:f6:70 ? 2001-12-31 - 2001-01-01

IGT Card Reader QoS: 0 type: BT
00:13:43:42:f6:bd ? 2001-12-31 - 2001-01-01

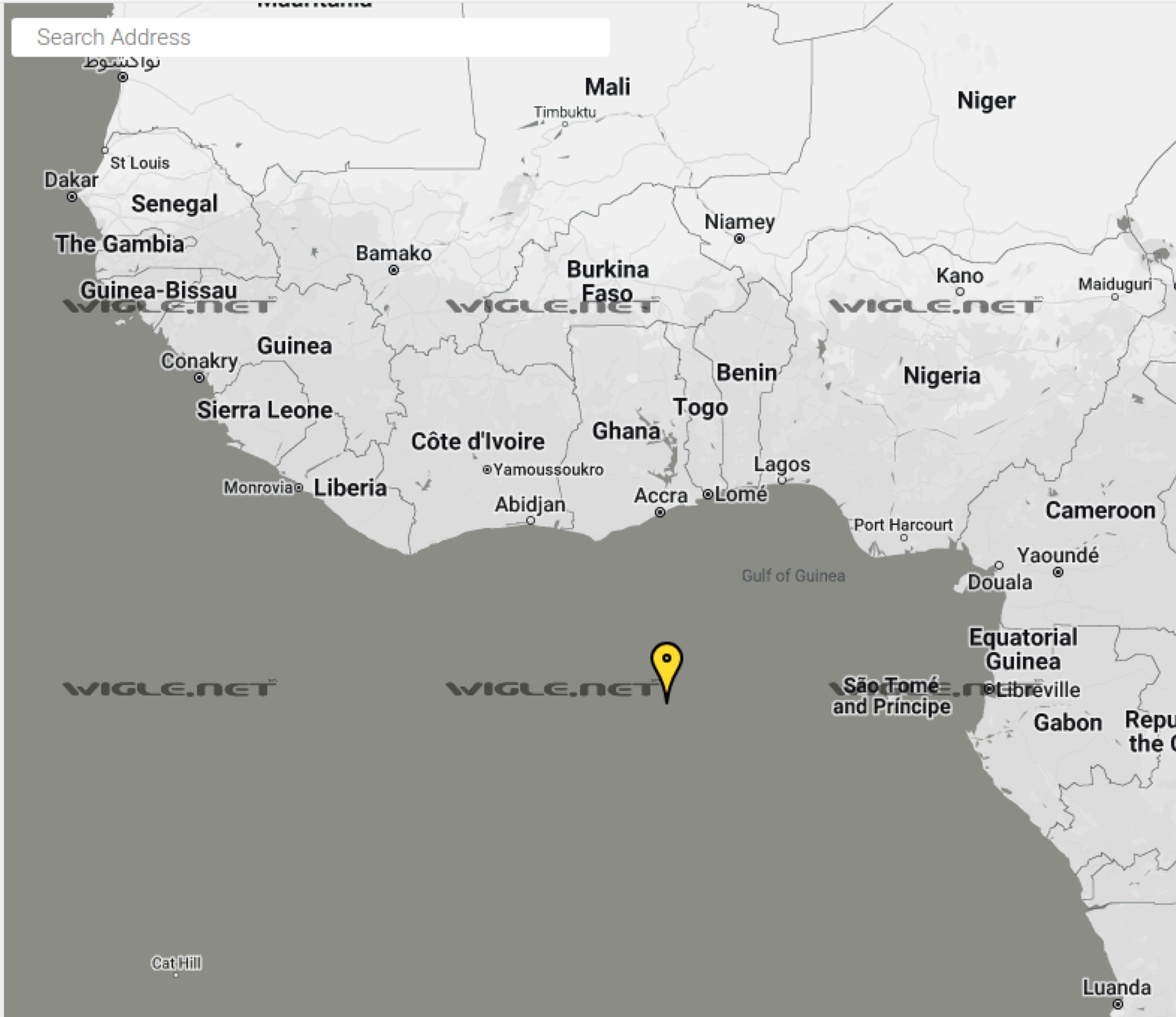
IGT Card Reader QoS: 0 type: BLE
00:13:43:42:f6:d4 ? 2001-12-31 - 2001-01-01

IGT Card Reader QoS: 0 type: BLE
00:13:43:42:f6:f3 ? 2001-12-31 - 2001-01-01

IGT Card Reader QoS: 0 type: BLE
00:13:43:42:f7:9b ? 2001-12-31 - 2001-01-01

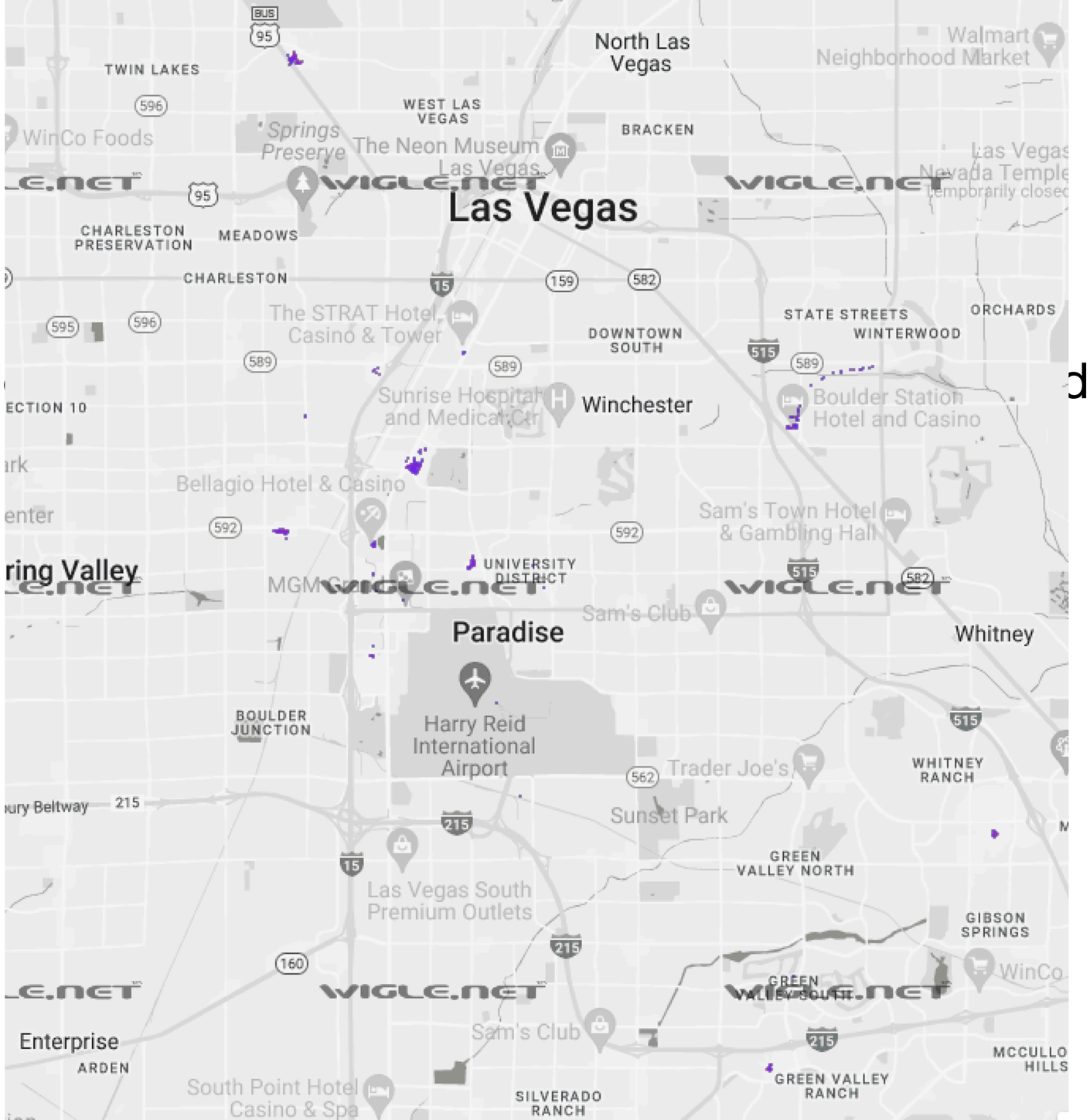
IGT Card Reader QoS: 0 type: BLE
00:13:43:42:f7:b3 ? 2001-12-31 - 2001-01-01

IGT Card Reader QoS: 0 type: BLE
00:13:43:42:f7:fa ? 2001-12-31 - 2001-01-01



Las Vegas
DEF CON 2023

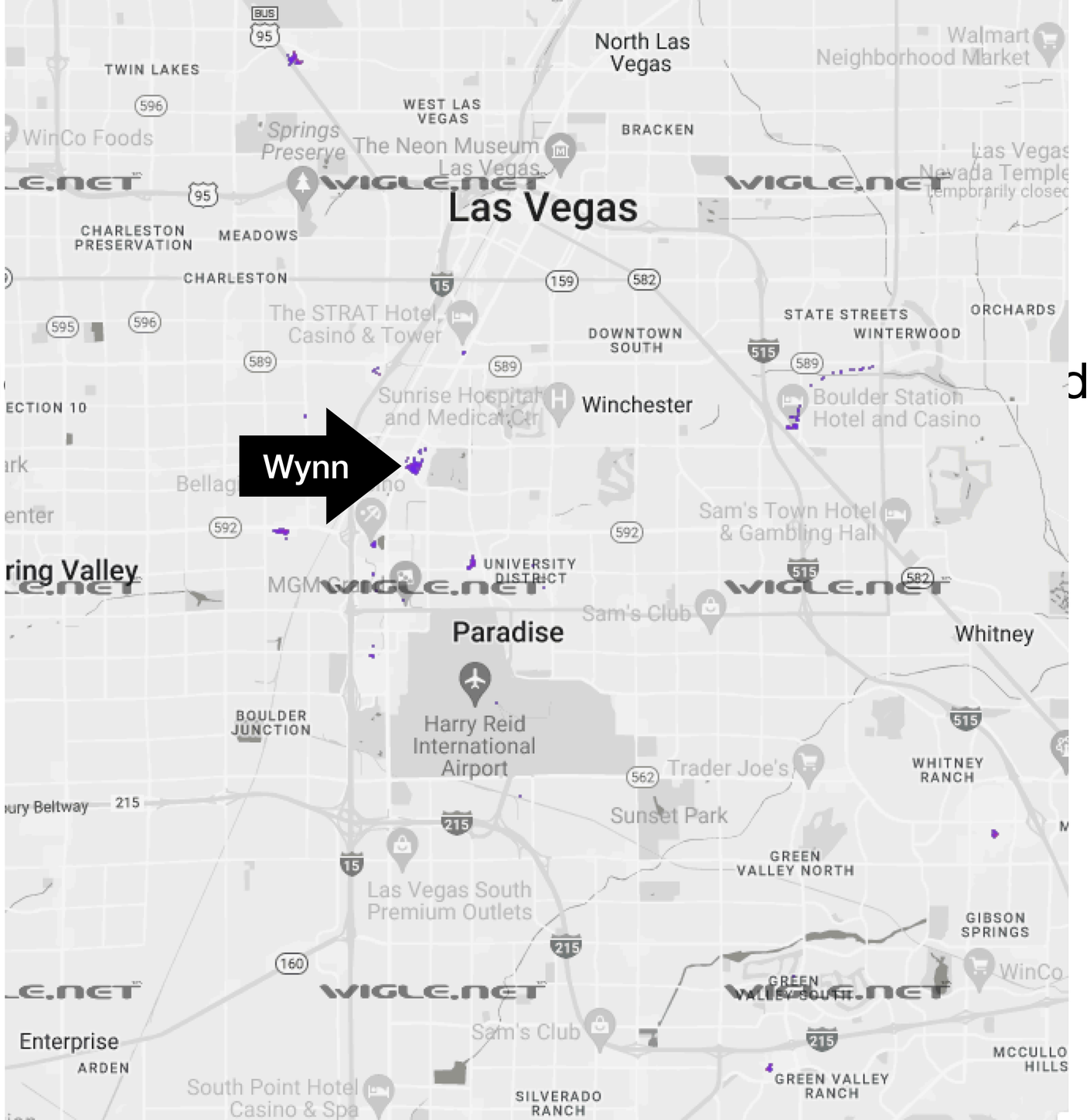
- Where else besid dvertising?



DST2.FYI

Las Vegas
DEF CON 2023

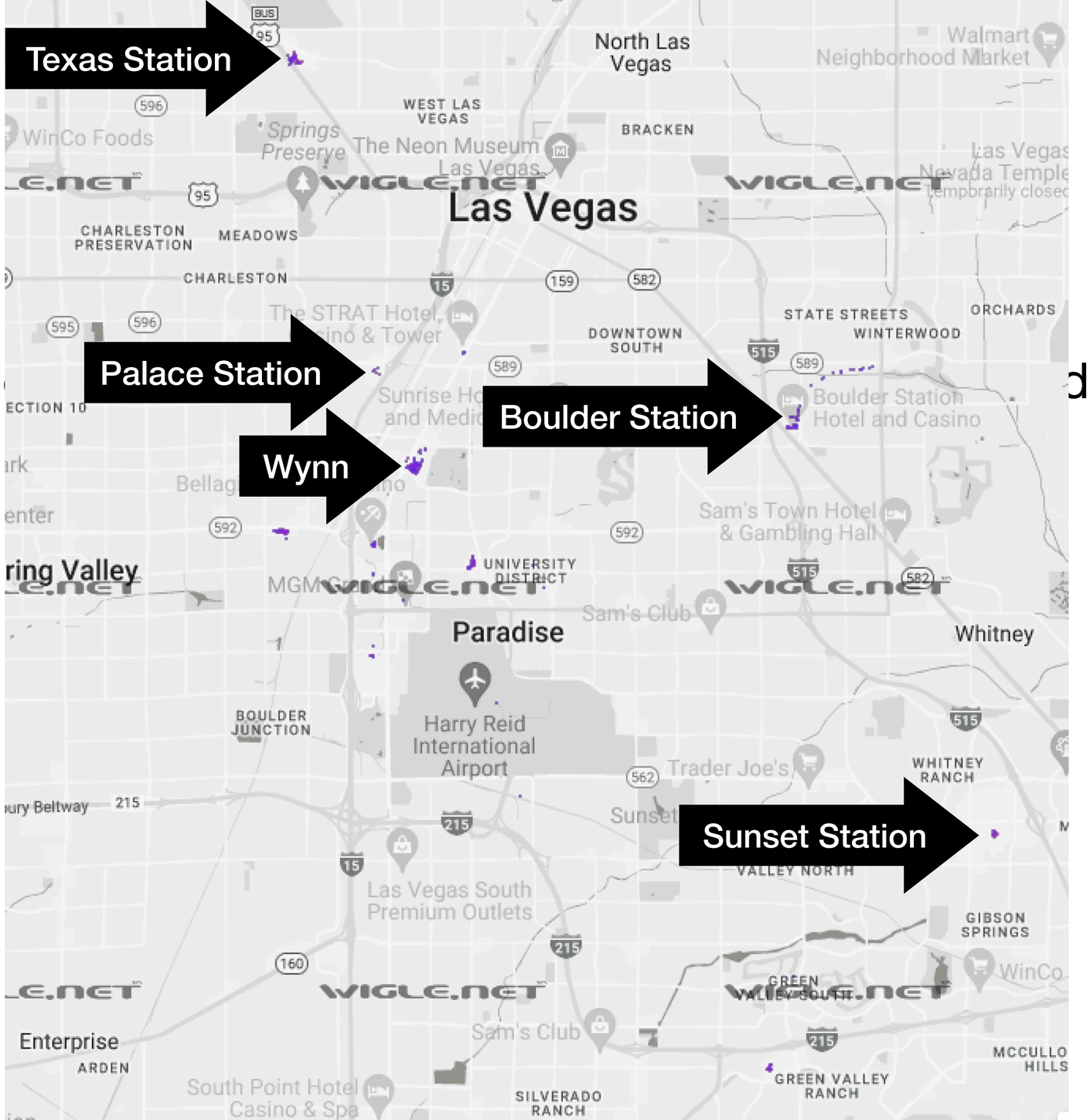
- Where else besid dvertising?



Las Vegas

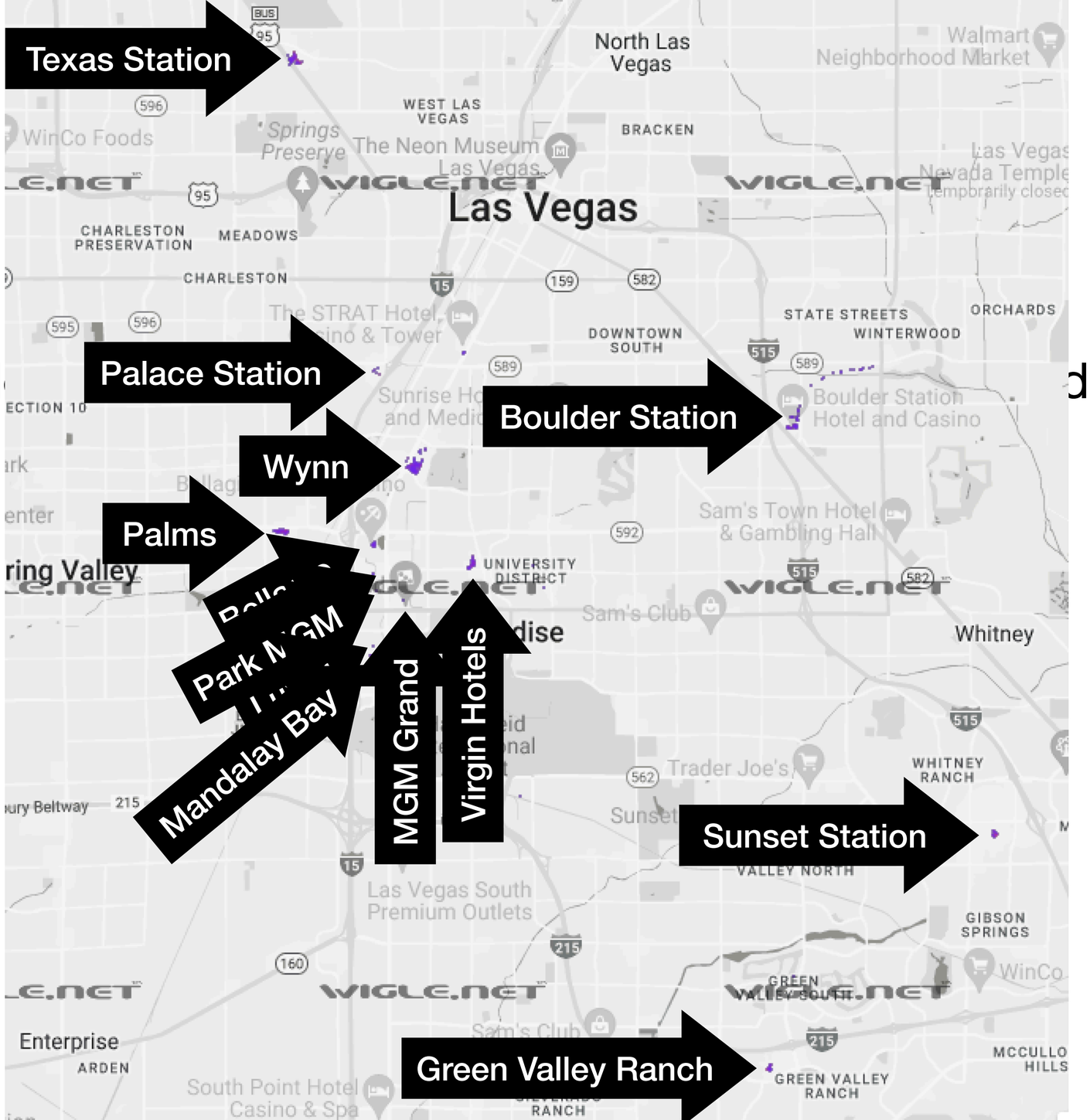
DEF CON 2023

- Where else besid dvertising?



Las Vegas
DEF CON 2023

- Where else besid dvertising?



Las Vegas
DEF CON 2023

- Where else besid dvertising?

Texas Station

Palace Station

Boulder Station

Wynn

Palms

Park MGM

Mandalay Bay

MGM Grand

Virgin Hotels

Sunset Station

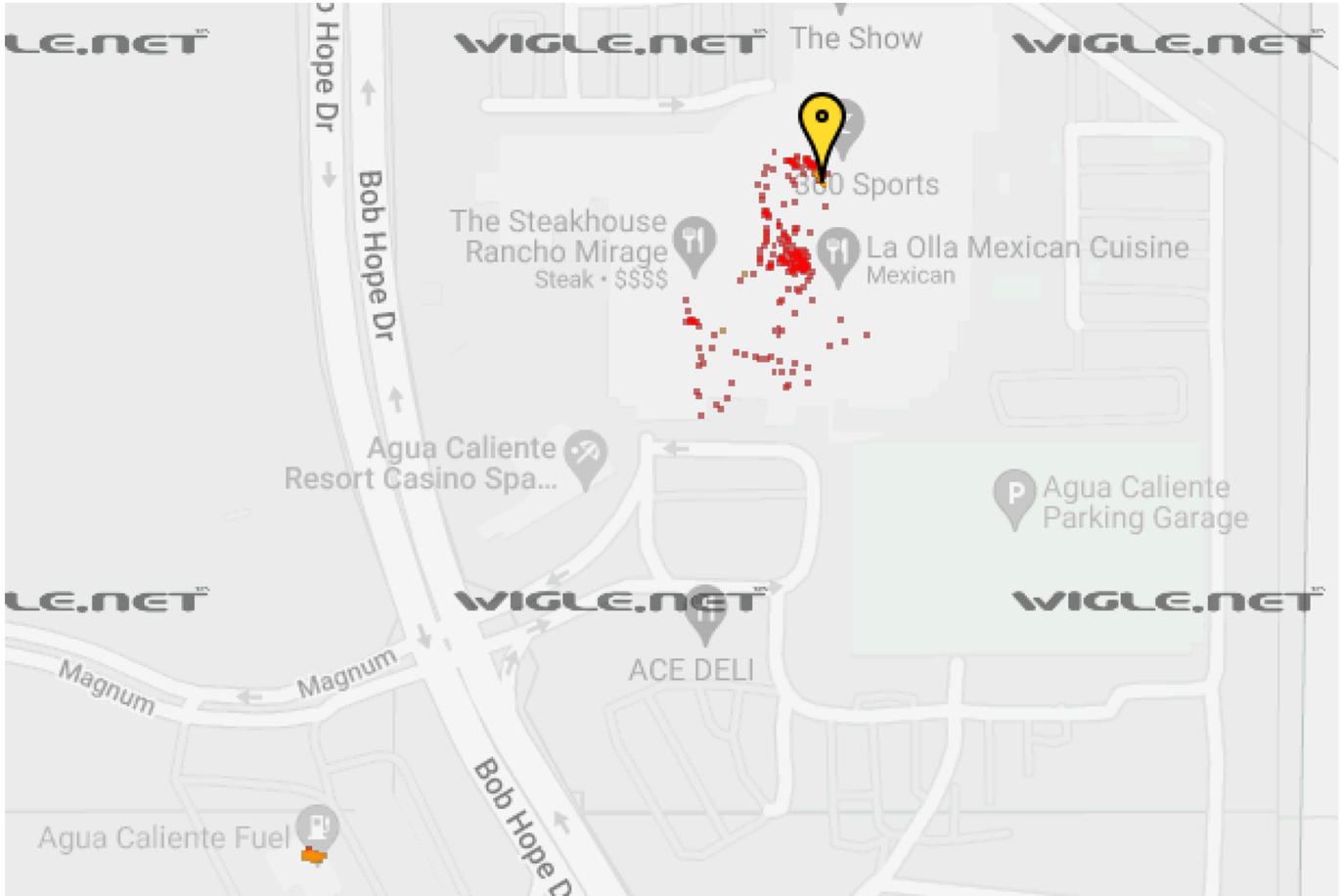
Green Valley Ranch

Remember, that's just where WiGLE users had a GPS signal! Which is uncommon in the middle of mega-casinos!

Las Vegas
DEF CON 2023

- Where else besides Wynn are there "IGT Card Reader" devices advertising?

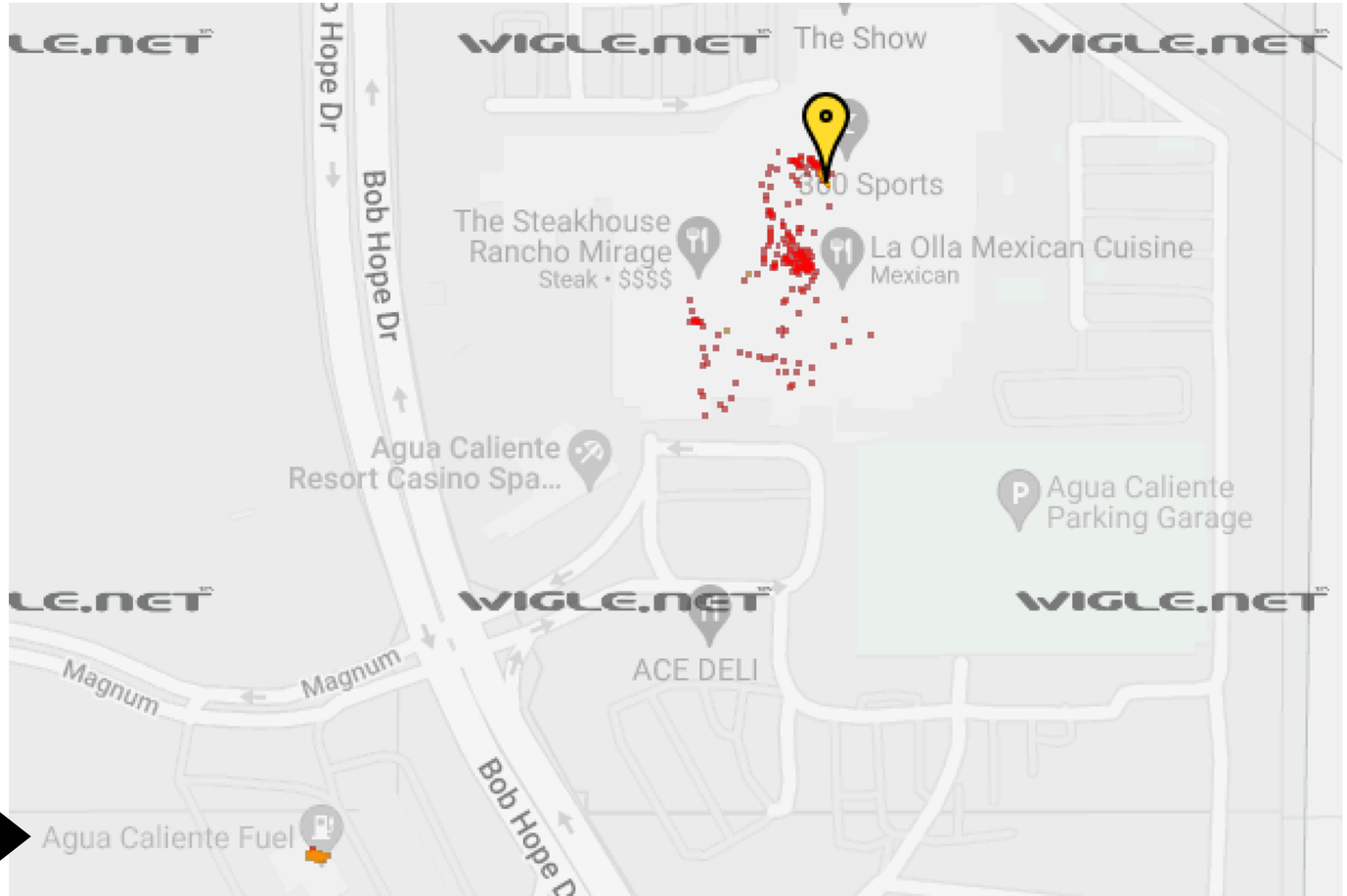
Aqua Caliente Resort Casino,
Palm Springs, CA



Las Vegas
DEF CON 2023

- Where else besides Wynn are there "IGT Card Reader" devices advertising?

Aqua Caliente Resort Casino,
Palm Springs, CA

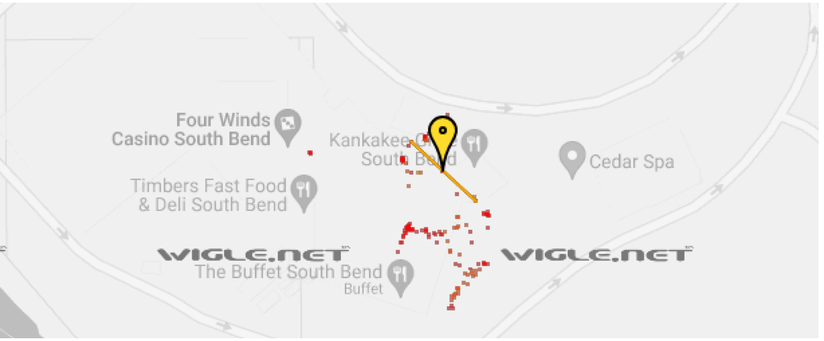


And also their gas station! :D

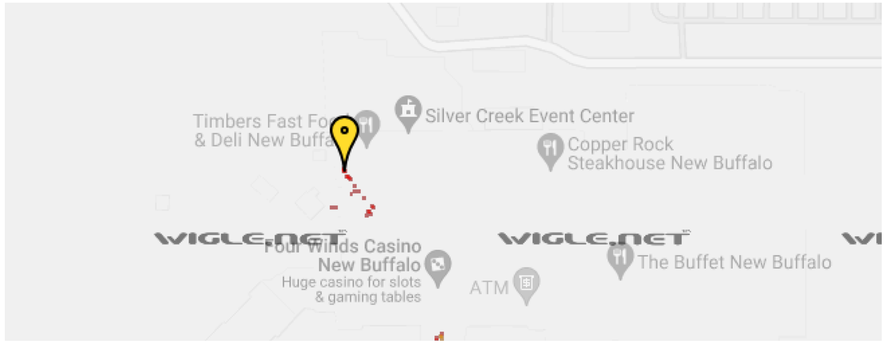
Las Vegas
DEF CON 2023

- Where else besides Wynn are there "IGT Card Reader" devices advertising?

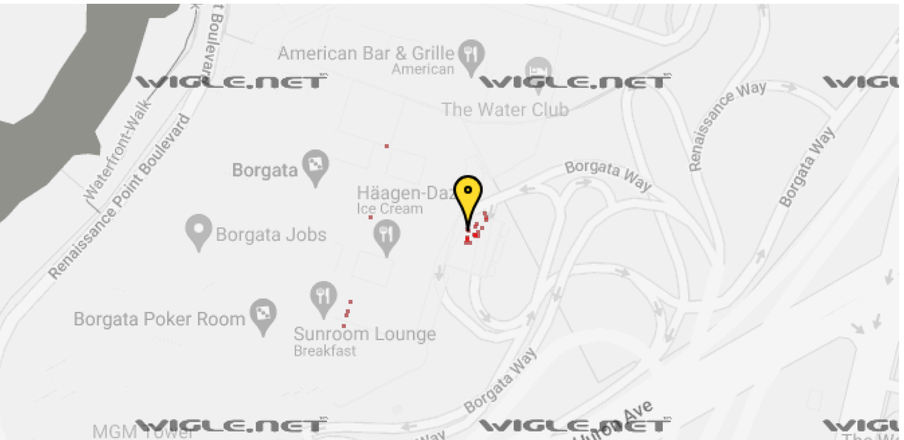
Four Winds Casino, South Bend, IN



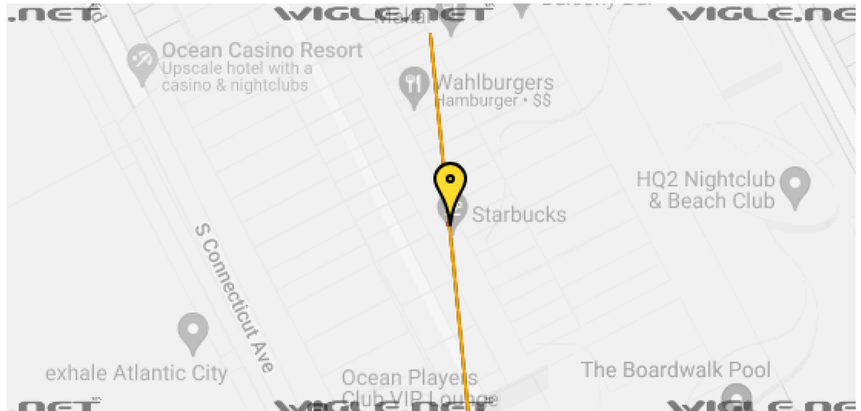
Four Winds Casino, New Buffalo, MI



Borgata, Atlantic City, NJ



Ocean Casino, Atlantic City, NJ
(Exactly 1? Or just GPS worked exactly once while indoors?)



Las Vegas
DEF CON 2023

- Are they supposed to be advertising or are they misconfigured?
- ¯_(ツ)_/¯

Las Vegas

Low ROI Places to Sniff!

- Where do they NOT have many BT devices worth sniffing in the wee hours of the morning?
- The fancy-pants shops!

DIOR
Alexander McQUEEN

TIFFANY & Co.

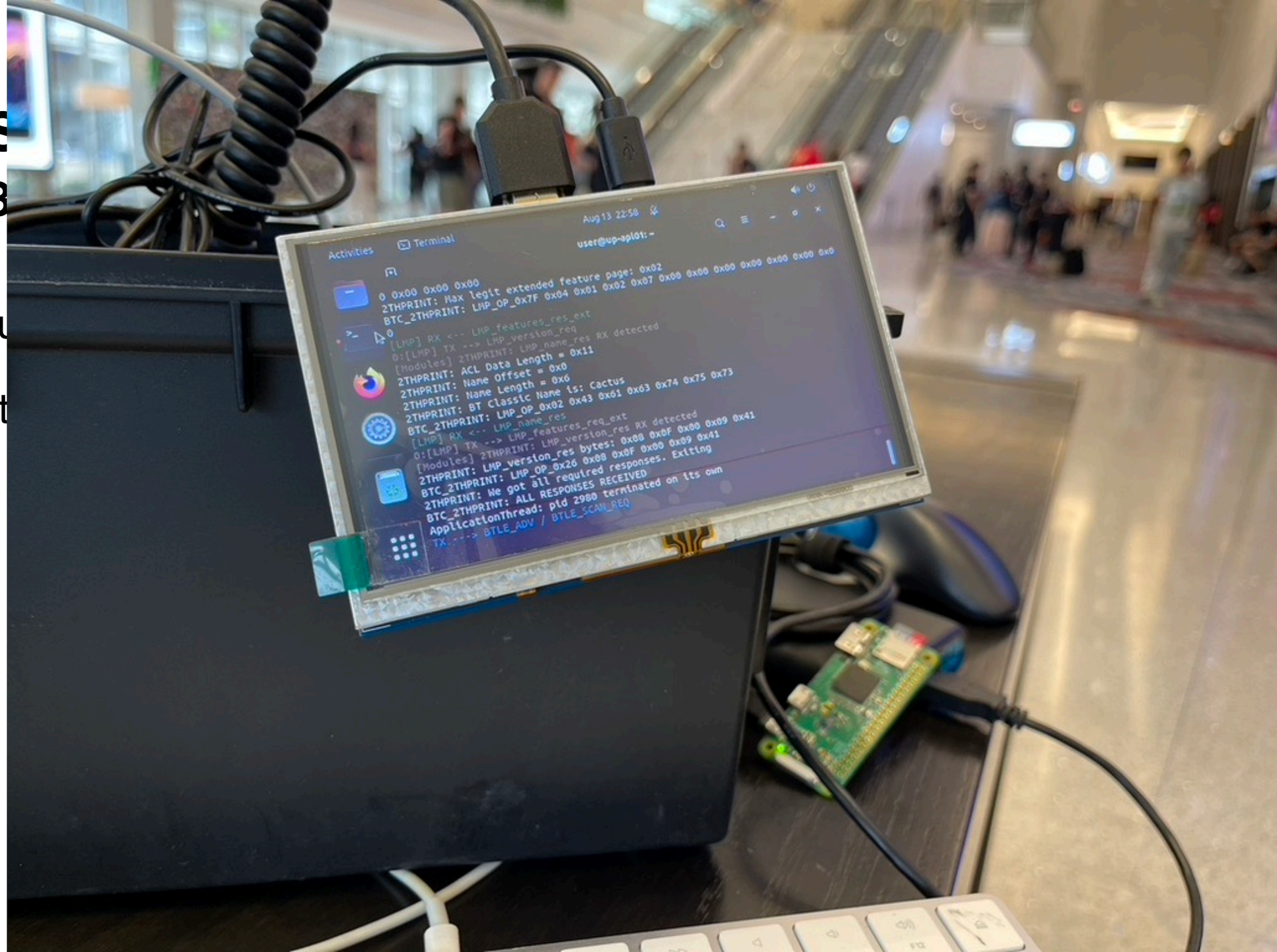
Las Vegas
DEF CON 2023

- Sneak peek of upcoming work!
- Always sniff at the chokepoints of human traffic flow!

Las Vegas

DEF CON 2023

- Sneak peek of u
- Always sniff at t



Hungary - Budapest

- Hacktivity 2023

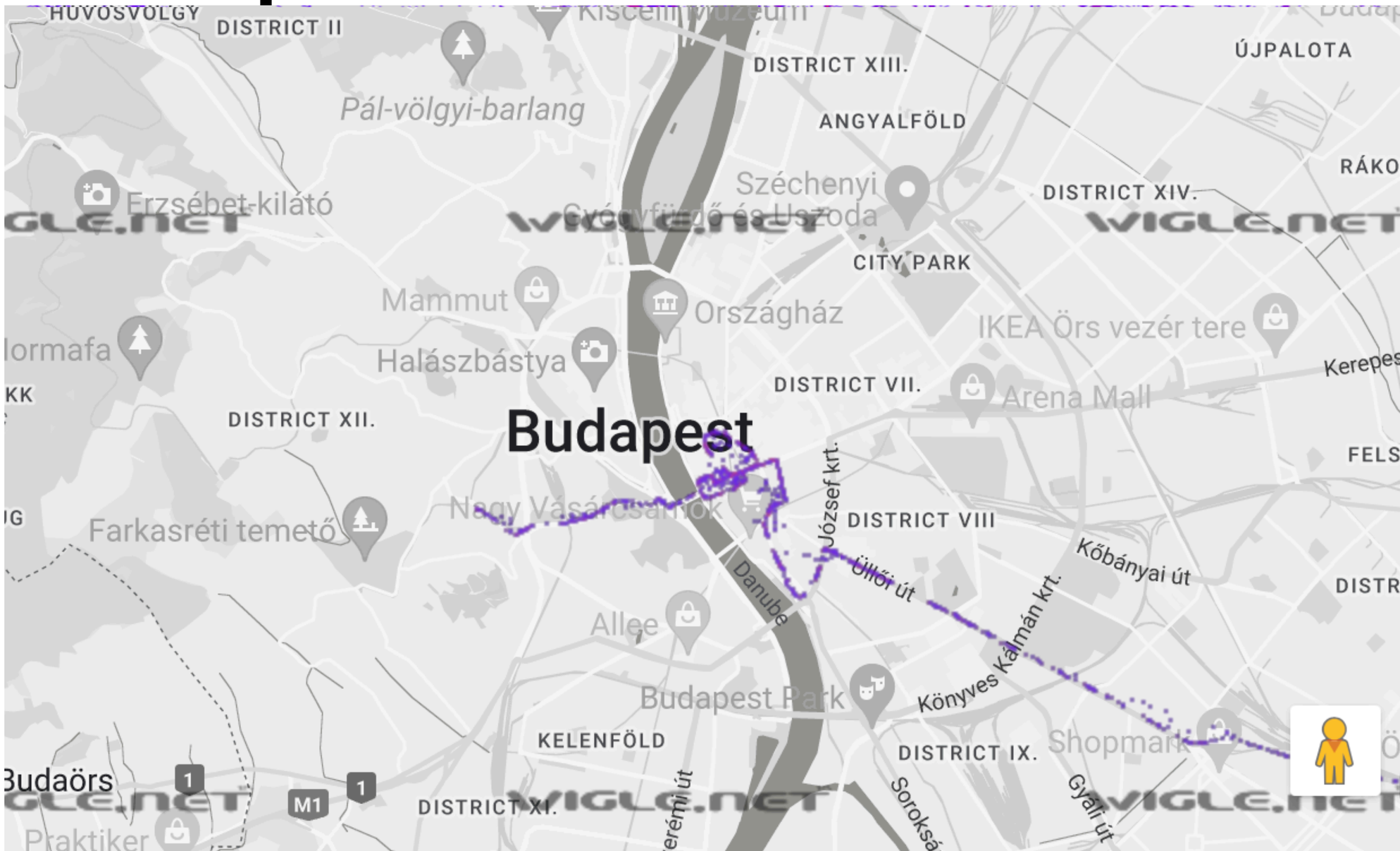
Hungary - Budapest

- All WiGLE data

Hungary - Budapest

- My data from airport to Hacktivity
- Took the miniBUD shuttle, got dropped off last, and was happy about it!

AIRPORT SHUTTLE



Hungary - Budapest

- Regex: ^Hipernet TV Box$ or ^HIPERNET TV BOX$

Hungary - Budapest

- Regex: ^Hipernet TV Box$ or ^HIPERNET TV BOX$

Hipernet TV Box QoS: **0** type: **BT**
68:b9:c2:6e:a4:e1 2023-09-18 - 2023-09-18

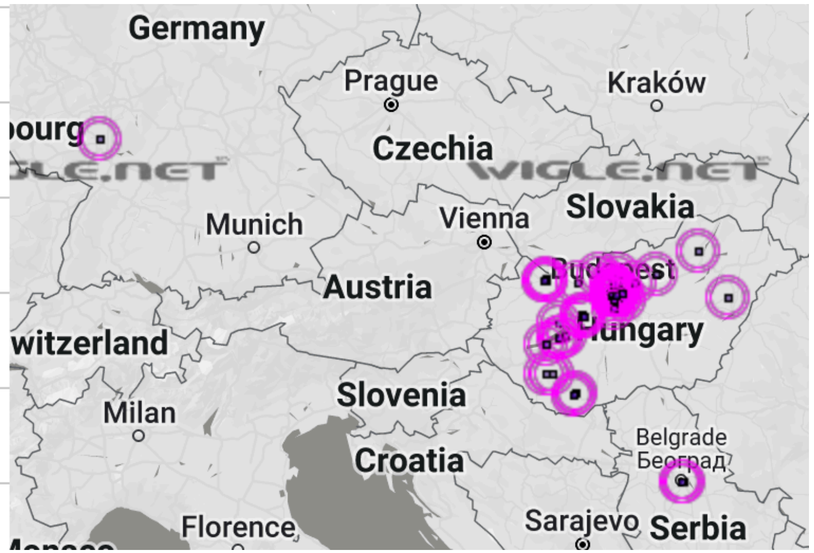
Hipernet TV Box QoS: **3** type: **BT**
68:b9:c2:6e:a5:19 2023-05-07 - 2023-05-13

Hipernet TV Box QoS: **0** type: **BT**
68:b9:c2:6e:db:f1 2023-06-10 - 2023-06-27

Hipernet TV Box QoS: **0** type: **BT**
68:b9:c2:6e:db:f9 2023-04-05 - 2023-04-05

Hipernet TV Box QoS: **0** type: **BT**
68:b9:c2:8a:d4:38 2023-07-26 - 2023-07-26

Hipernet TV Box QoS: **0** type: **BT**



Hungary - Budapest

- Regex: ^Hipernet TV Box$ or ^HIPERNET TV BOX$

Hipernet TV Box QoS: **0** type: **BT**
68:b9:c2:6e:a4:e1 2023-09-18 - 2023-09-18

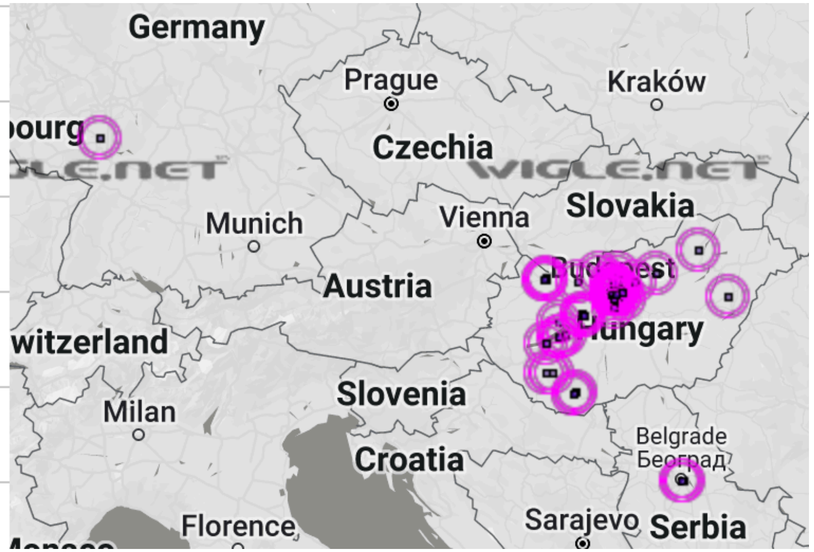
Hipernet TV Box QoS: **3** type: **BT**
68:b9:c2:6e:a5:19 2023-05-07 - 2023-05-13

Hipernet TV Box QoS: **0** type: **BT**
68:b9:c2:6e:db:f1 2023-06-10 - 2023-06-27

Hipernet TV Box QoS: **0** type: **BT**
68:b9:c2:6e:db:f9 2023-04-05 - 2023-04-05

Hipernet TV Box QoS: **0** type: **BT**
68:b9:c2:8a:d4:38 2023-07-26 - 2023-07-26

Hipernet TV Box QoS: **0** type: **BT**



HIPERNET TV BOX QoS: **7** type: **BLE**
24:18:c6:aa:3b:c7 2022-09-09 - 2023-09-27

HIPERNET TV BOX QoS: **0** type: **BT**
24:18:c6:aa:3c:54 2023-07-24 - 2023-07-24

HIPERNET TV BOX QoS: **2** type: **BT**
24:18:c6:aa:3e:8f 2022-08-16 - 2023-01-02

HIPERNET TV BOX QoS: **0** type: **BT**
24:18:c6:aa:3f:bb 2022-12-19 - 2023-02-16

HIPERNET TV BOX QoS: **0** type: **BT**
24:18:c6:aa:3f:c3 2022-12-19 - 2023-02-16

Hungary - Budapest

- Regex: ^Hipernet TV Box$ or ^HIPERNET TV BOX$

Hipernet TV Box QoS: 0 type: BT
68:b9:c2:[redacted]e:a4:e1 2023-09-18 - 2023-09-18

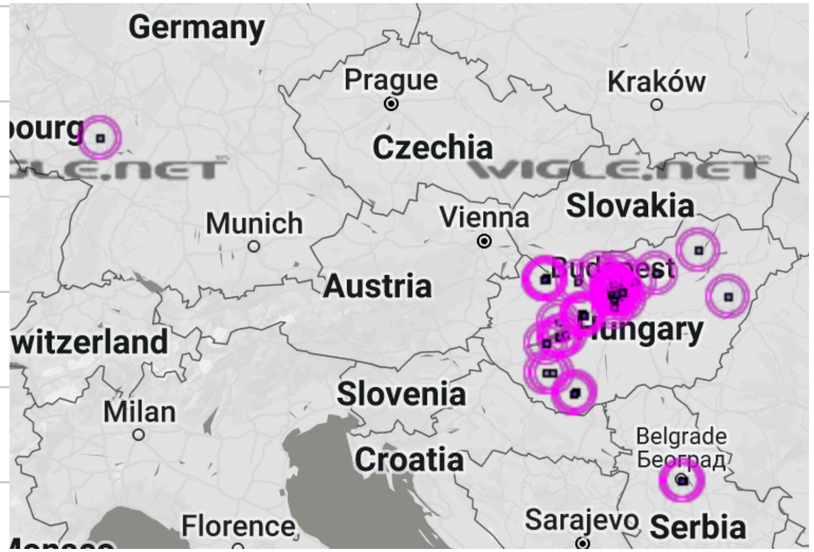
Hipernet TV Box QoS: 3 type: BT
68:b9:c2:[redacted]e:a5:19 2023-05-07 - 2023-05-13

Hipernet TV Box QoS: 0 type: BT
68:b9:c2:[redacted]e:db:f1 2023-06-10 - 2023-06-27

Hipernet TV Box QoS: 0 type: BT
68:b9:c2:[redacted]e:db:f9 2023-04-05 - 2023-04-05

Hipernet TV Box QoS: 0 type: BT
68:b9:c2:[redacted]a:d4:38 2023-07-26 - 2023-07-26

Hipernet TV Box QoS: 0 type: BT



HIPERNET TV BOX QoS: 7 type: BLE
24:18:c6:[redacted]a:3b:c7 2022-09-09 - 2023-09-27

HIPERNET TV BOX QoS: 0 type: BT
24:18:c6:[redacted]a:3c:54 2023-07-24 - 2023-07-24

HIPERNET TV BOX QoS: 2 type: BT
24:18:c6:[redacted]a:3e:8f 2022-08-16 - 2023-01-02

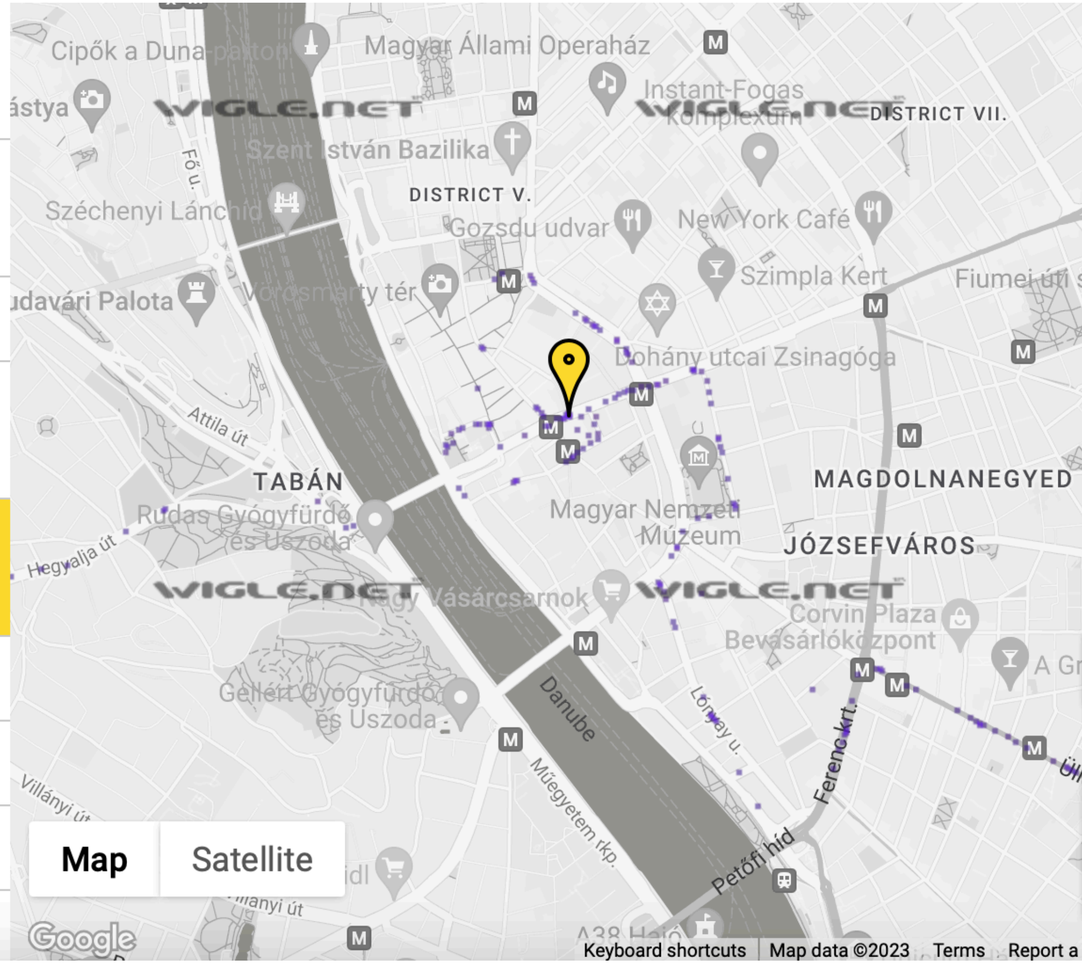
HIPERNET TV BOX QoS: 0 type: BT
24:18:c6:[redacted]a:3f:bb 2022-12-19 - 2023-02-16

HIPERNET TV BOX QoS: 0 type: BT
24:18:c6:[redacted]a:3f:c3 2022-12-19 - 2023-02-16

Bonus: *Primarily* Eastern Europe?

- Regex: ^iHunt Watch.* e.g. “iHunt Watch6T-C0F6”, “iHunt Watch 3T”, “iHunt Watch 11 PRO”

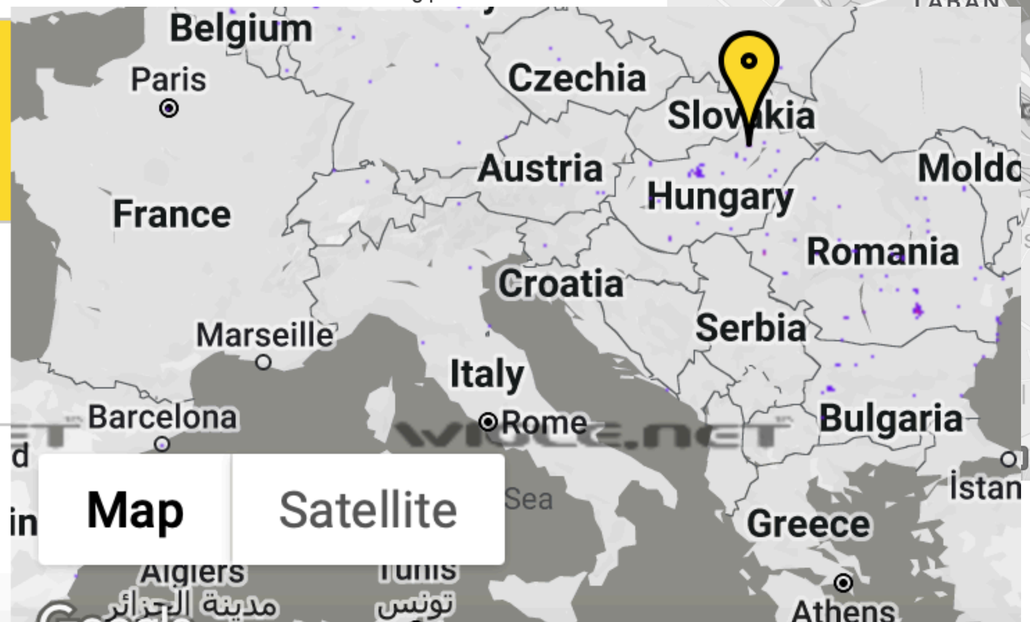
Galaxy Watch4 Classic (HSWF)	QoS: **0**	type: **BLE**	
74:9d:7e:04:2e:58	**?**	2023-10-04 - 2023-10-04	
JBL TUNE125TWS-LE	QoS: **0**	type: **BT**	
74:aa:74:ed:e8:2c	**?**	2023-10-04 - 2023-10-04	
29610DER	QoS: **0**	type: **BT**	
76:2f:a4:ae:a2:79	**?**	2023-10-04 - 2023-10-04	
LAPTOP-46AF717R	QoS: **0**	type: **BT**	
77:f0:7e:75:11:e9	**?**	2023-10-04 - 2023-10-04	
iHunt Watch6T-C0F6	QoS: **0**	type: **BLE**	
78:02:b7:97:c0:f6	**?**	2023-10-04 - 2023-10-04	
Jabra Evolve2 65	QoS: **0**	type: **BLE**	
78:04:3a:05:1c:7d	**?**	2023-10-04 - 2023-10-04	
Hertz	QoS: **0**	type: **BT**	
79:7a:ac:fc:a6:1c	**?**	2023-10-04 - 2023-10-04	
Voyager-BT	QoS: **0**	type: **BT**	
7b:ce:52:e0:41:81	**?**	2023-10-04 - 2023-10-04	
WH-CH720N	QoS: **0**	type: **BLE**	
84:d3:52:54:a2:4a	**?**	2023-10-04 - 2023-10-04	

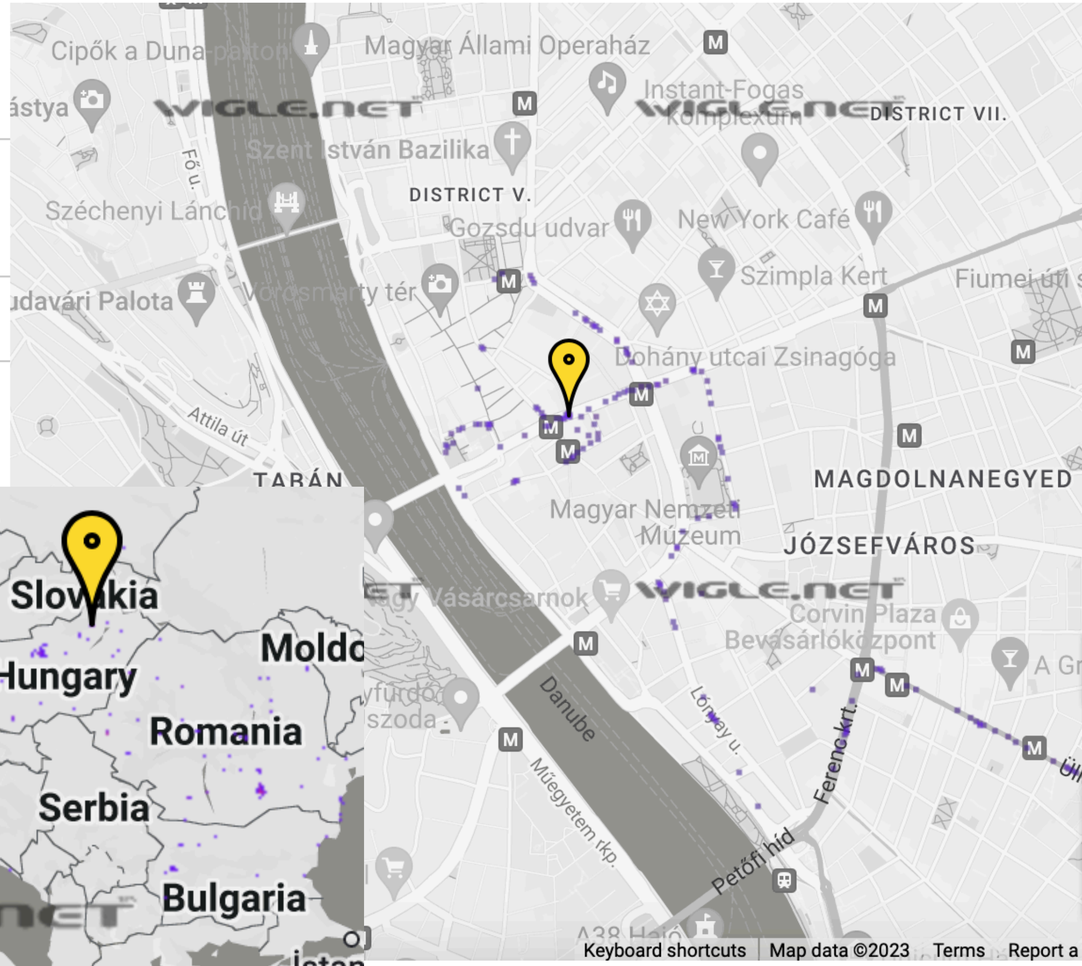


Bonus: *Primarily* Eastern Europe?

- Regex: ^iHunt Watch.* e.g. “iHunt Watch6T-C0F6”, “iHunt Watch 3T”, “iHunt Watch 11 PRO”

iHunt Watch6T-FED3	QoS: **0**	type: **BT**	
5d:67:09:c4:89:72	**?**	2023-05-30 - 2023-06-06	
iHunt Watch6T-3468	QoS: **0**	type: **BLE**	
78:02:b7:0f:34:68	**?**	2001-01-01 - 2001-01-01	
iHunt Watch6T-3492	QoS: **0**	type: **BLE**	
78:02:b7:0f:34:92	**?**	2022-09-10 - 2022-09-10	
Galaxy Watch4 Classic (HSWF)	QoS: **0**	type: **BLE**	
74:9d:7e:04:2e:58	**?**	2023-10-04 - 2023-10-04	
JBL TUNE125TWS-LE	QoS: **0**	type: **BT**	
74:aa:74:ed:e8:2c	**?**	2023-10-04 - 2023-10-04	
29610DER	QoS: **0**	type: **BT**	
76:2f:a4:ae:a2:79	**?**	2023-10-04 - 2023-10-04	
LAPTOP-46AF717R	QoS: **0**	type: **BT**	
77:f0:7e:75:11:e9	**?**	2023-10-04 - 2023-10-04	



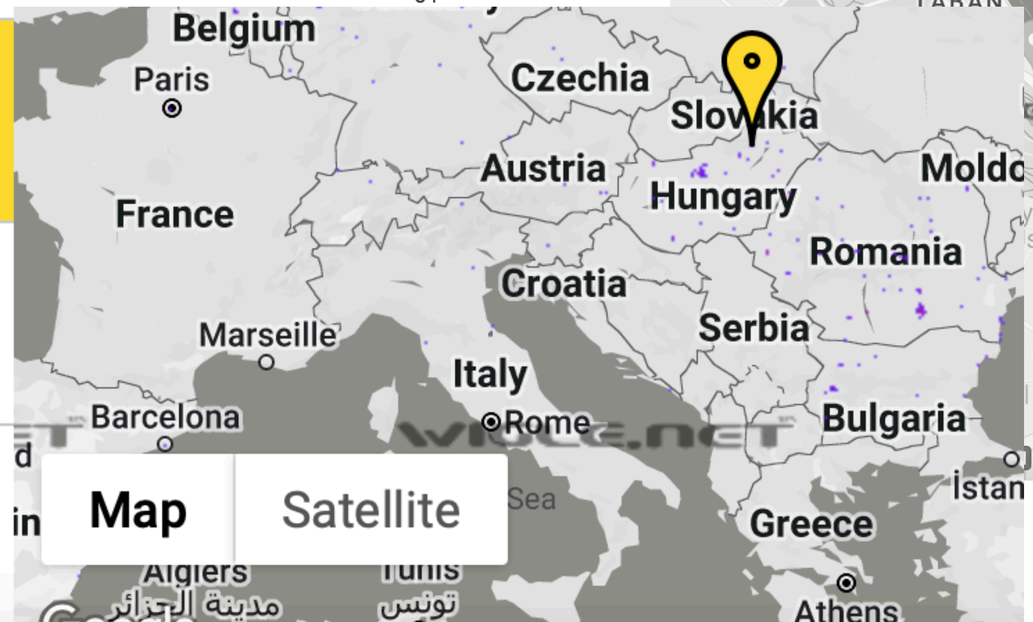


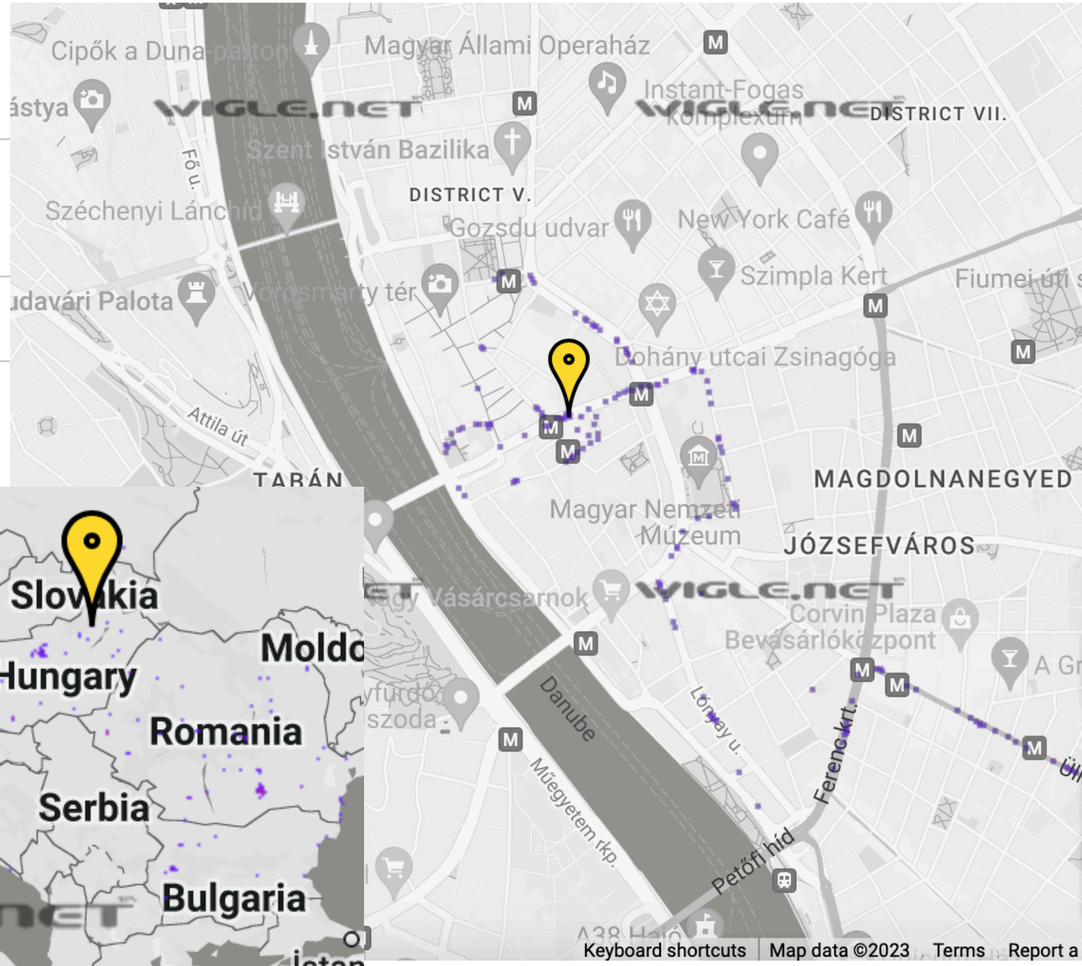
Bonus: *Primarily* Eastern Europe?

- Regex: ^iHunt Watch.* e.g. “iHunt Watch6T-C0F6”, “iHunt Watch 3T”, “iHunt Watch 11 PRO”

iHunt Watch6T-FED3	QoS: **0**	type: **BT**	
5d:67:09:c4:89:72	**?**	2023-05-30 - 2023-06-06	
iHunt Watch6T-3468	QoS: **0**	type: **BLE**	
78:02:b7:0:34:68	**?**	2001-01-01 - 2001-01-01	
iHunt Watch6T-3492	QoS: **0**	type: **BLE**	
78:02:b7:0f:34:92	**?**	2022-09-10 - 2022-09-10	

Galaxy Watch4 Classic (HSWF)	QoS: **0**	type: **BLE**	
74:9d:7e:04:2e:58	**?**	2023-10-04 - 2023-10-04	
JBL TUNE125TWS-LE	QoS: **0**	type: **BT**	
74:aa:74:ed:e8:2c	**?**	2023-10-04 - 2023-10-04	
29610DER	QoS: **0**	type: **BT**	
76:2f:a4:ae:a2:79	**?**	2023-10-04 - 2023-10-04	
LAPTOP-46AF717R	QoS: **0**	type: **BT**	
77:f0:7e:75:11:e9	**?**	2023-10-04 - 2023-10-04	



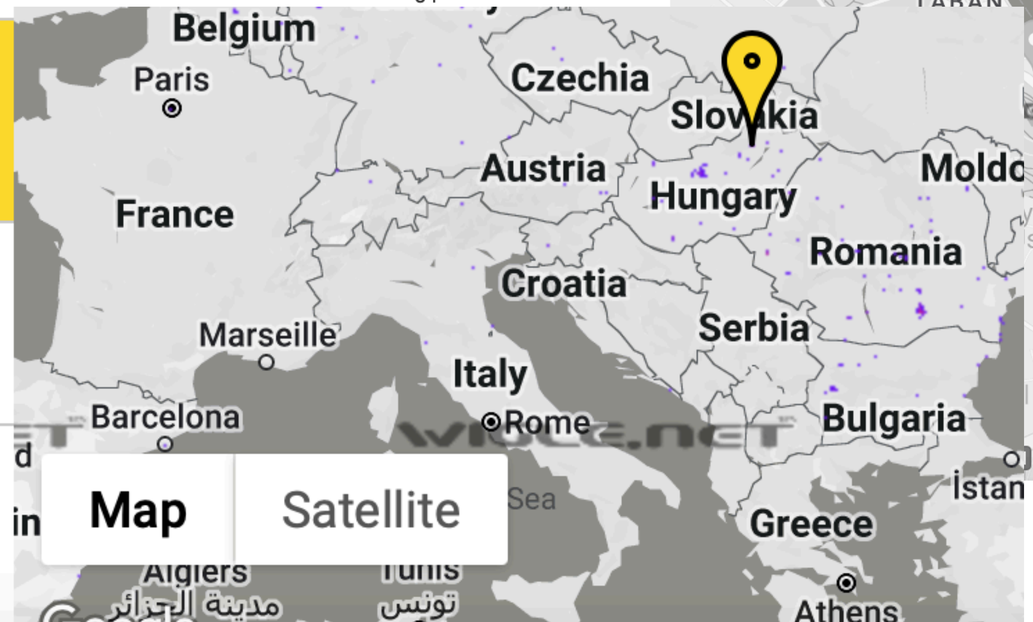


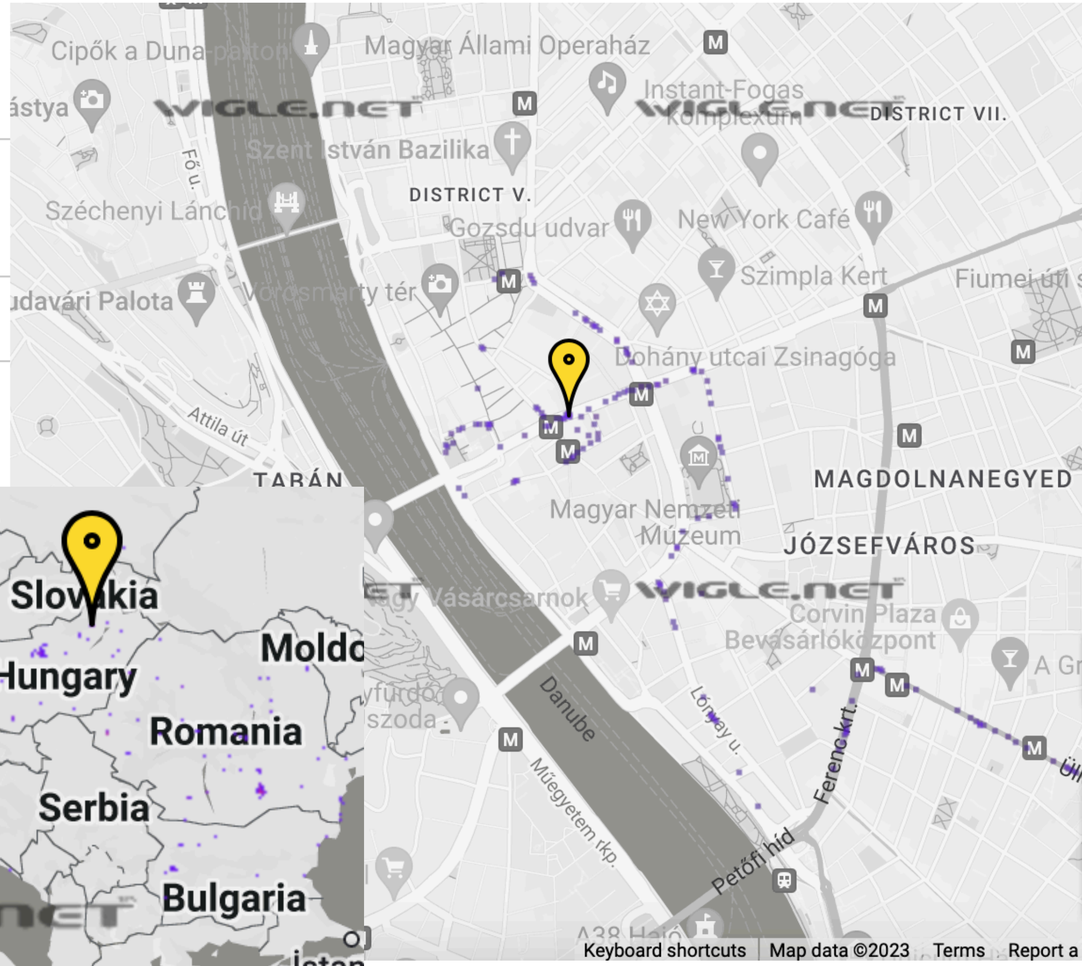
Bonus: *Primarily* Eastern Europe?

- Regex: ^iHunt Watch.* e.g. “iHunt Watch6T-C0F6”, “iHunt Watch 3T”, “iHunt Watch 11 PRO”

iHunt Watch6T-FED3	QoS: **0**	type: **BT**	
5d:67:09:c4:89:72	**?**	2023-05-30 - 2023-06-06	
iHunt Watch6T-3468	QoS: **0**	type: **BLE**	
78:02:b7:0:34:68	**?**	2001-01-01 - 2001-01-01	
iHunt Watch6T-3492	QoS: **0**	type: **BLE**	
78:02:b7:0f:34:92	**?**	2022-09-10 - 2022-09-10	

Galaxy Watch4 Classic (HSWF)	QoS: **0**	type: **BLE**	
74:9d:7e:04:2e:58	**?**	2023-10-04 - 2023-10-04	
JBL TUNE125TWS-LE	QoS: **0**	type: **BT**	
74:aa:74:ed:e8:2c	**?**	2023-10-04 - 2023-10-04	
29610DER	QoS: **0**	type: **BT**	
76:2f:a4:ae:a2:79	**?**	2023-10-04 - 2023-10-04	
LAPTOP-46AF717R	QoS: **0**	type: **BT**	
77:f0:7e:75:11:e9	**?**	2023-10-04 - 2023-10-04	



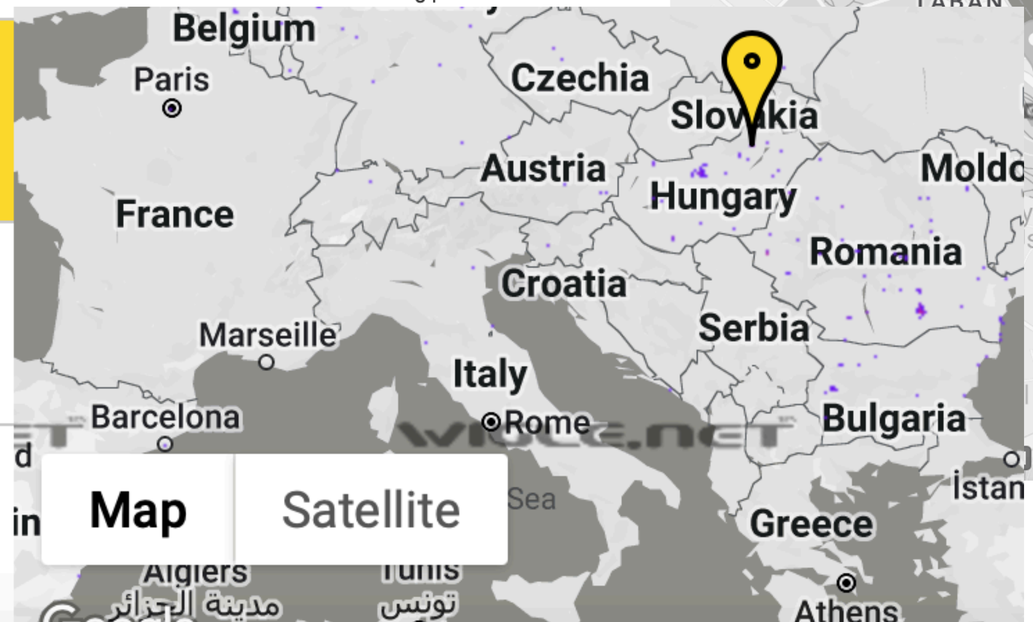


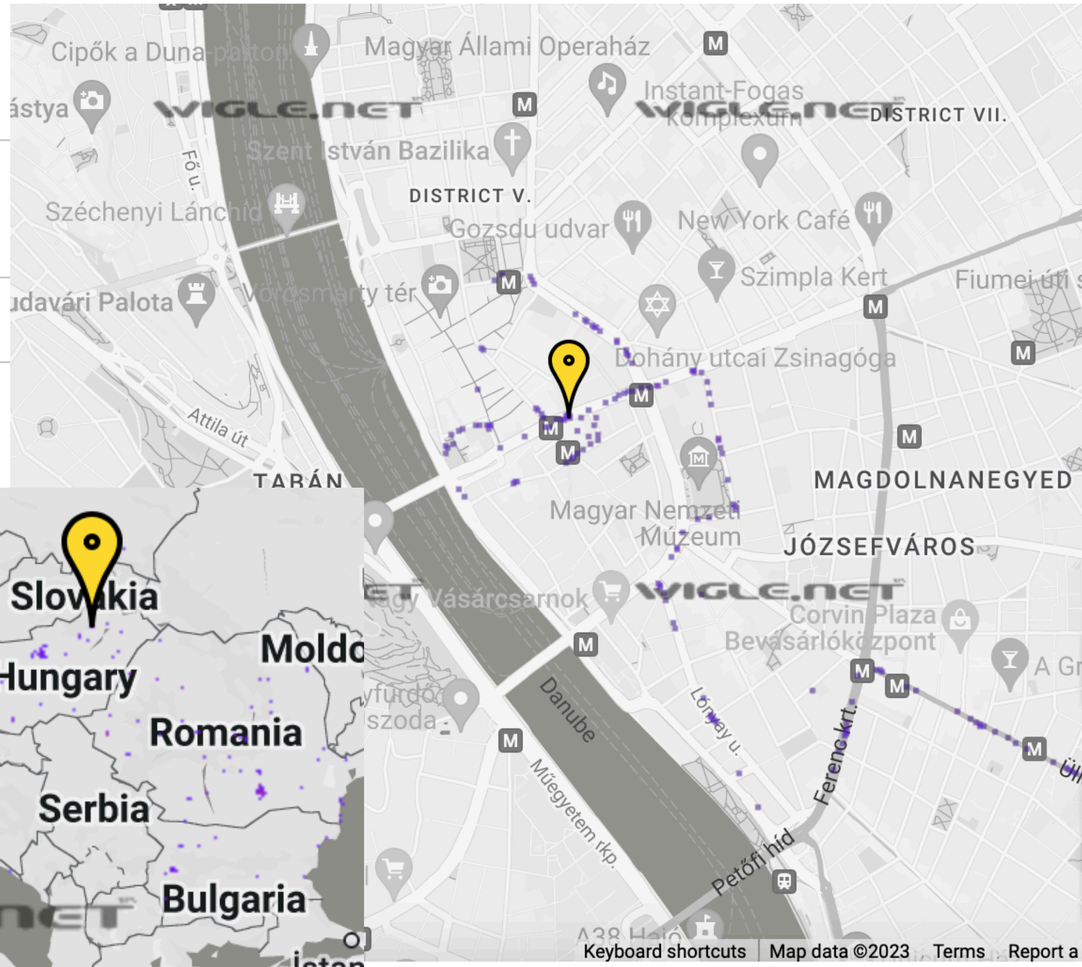
Bonus: *Primarily* Eastern Europe?

- Regex: ^iHunt Watch.* e.g. “iHunt Watch6T-C0F6”, “iHunt Watch 3T”, “iHunt Watch 11 PRO”

iHunt Watch6T-FED3	QoS: **0**	type: **BT**	
5d:67:09:c4:89:72	**?**	2023-05-30 - 2023-06-06	
iHunt Watch6T-3468	QoS: **0**	type: **BLE**	
78:02:b7:0:34:68	**?**	2001-01-01 - 2001-01-01	
iHunt Watch6T-3492	QoS: **0**	type: **BLE**	
78:02:b7:0f:34:92	**?**	2022-09-10 - 2022-09-10	

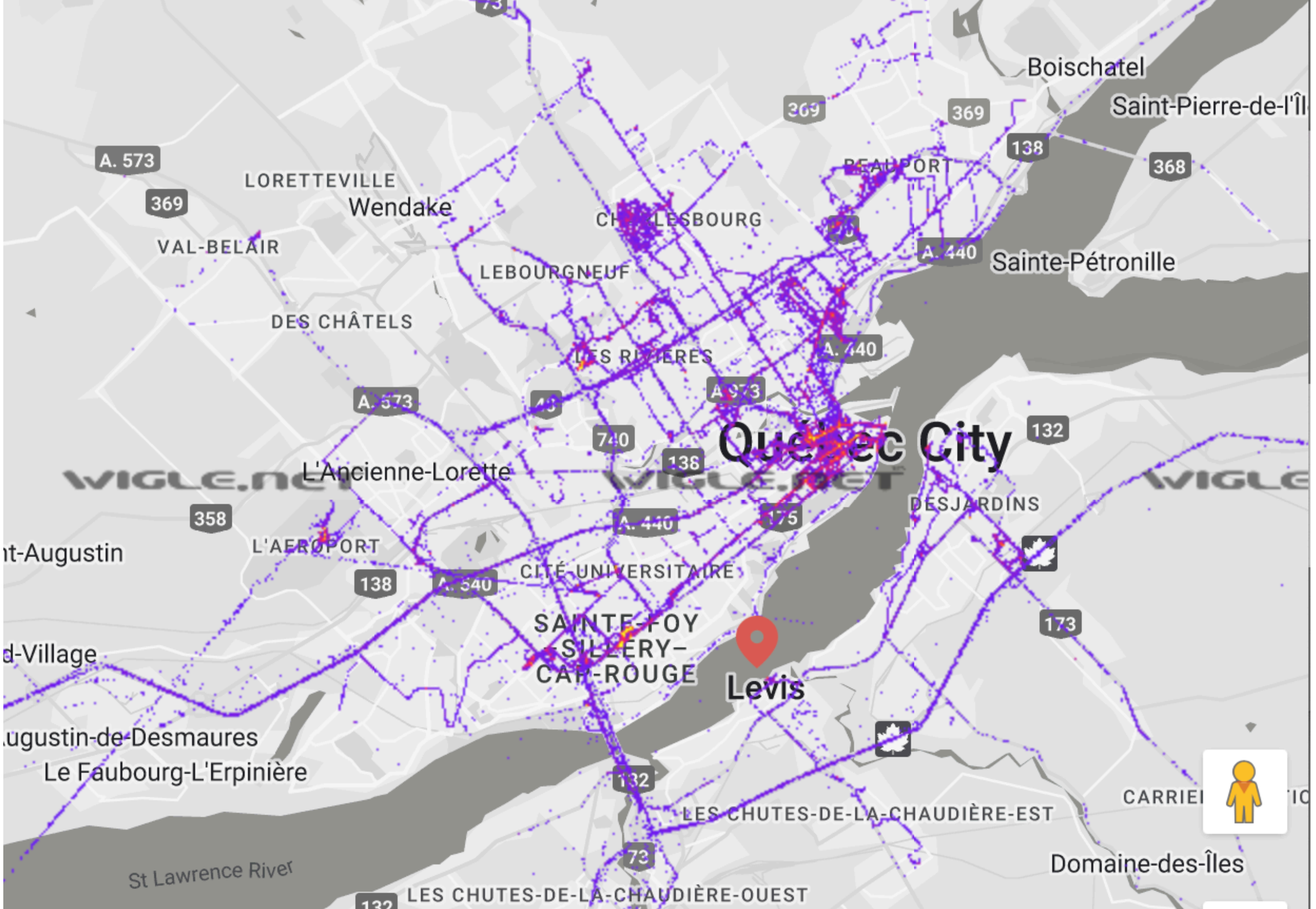
Galaxy Watch4 Classic (HSWF)	QoS: **0**	type: **BLE**	
74:9d:7e:04:2e:58	**?**	2023-10-04 - 2023-10-04	
JBL TUNE125TWS-LE	QoS: **0**	type: **BT**	
74:aa:74:ed:e8:2c	**?**	2023-10-04 - 2023-10-04	
29610DER	QoS: **0**	type: **BT**	
76:2f:a4:ae:a2:79	**?**	2023-10-04 - 2023-10-04	
LAPTOP-46AF717R	QoS: **0**	type: **BT**	
77:f0:7e:75:11:e9	**?**	2023-10-04 - 2023-10-04	



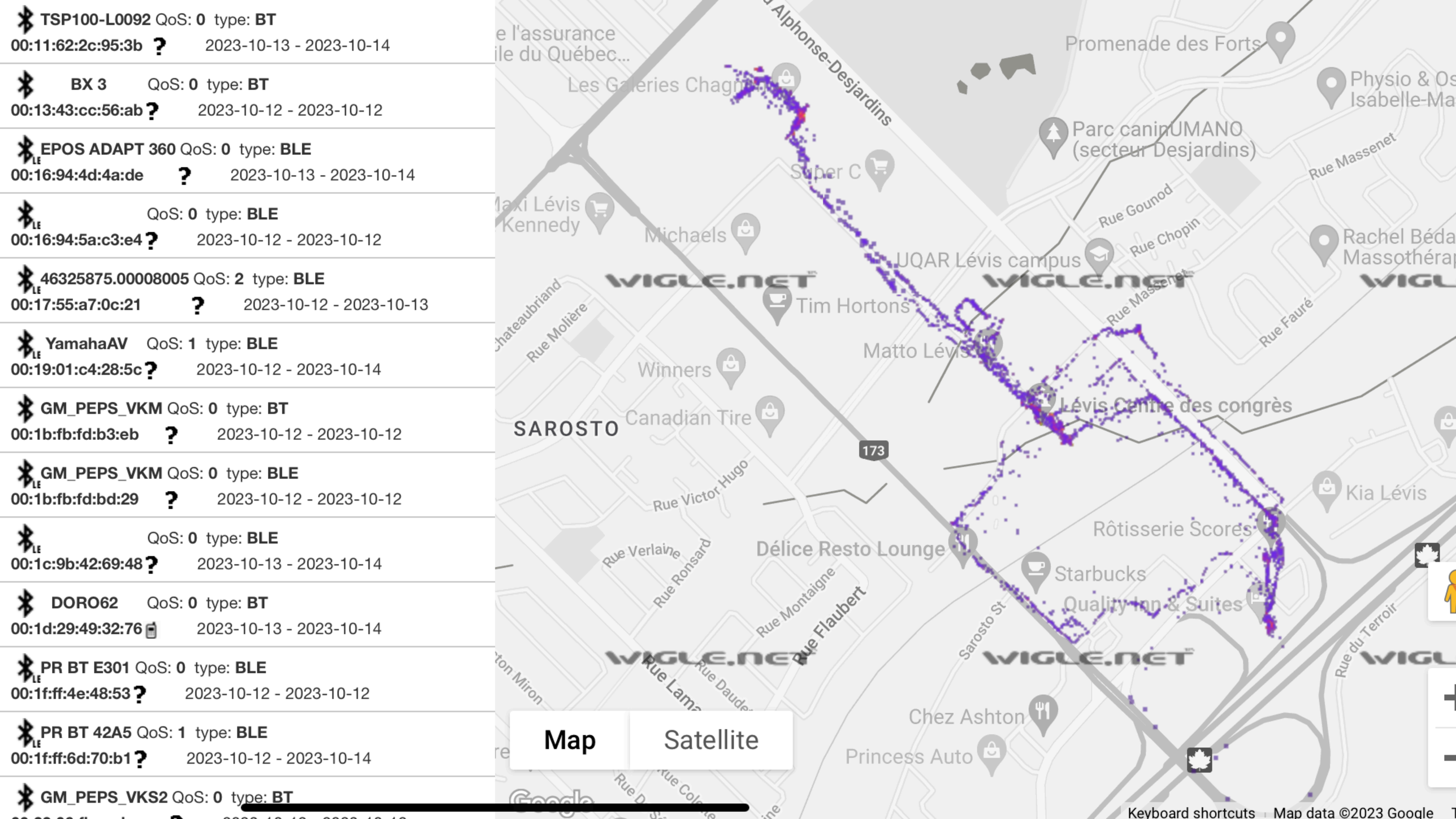


Canada - Lévis

- Hackfest.ca 2023


Boischatel
Saint-Pierre-de-l'Île
LORETTEVILLE
Wendake
VAL-BELAIR
LEBOURGNEUF
DES CHÂTELS
Sainte-Pétronille
L'Ancienne-Lorette
Quebec City
DESJARDINS
L'AEROPORT
CITÉ-UNIVERSITAIRE
SAINTE-FOY
SILLERY–
CAP-ROUGE
Levis
Le Faubourg-L'Erpinière
LES CHUTES-DE-LA-CHAUDIÈRE-EST
Domaine-des-Îles
St Lawrence River
LES CHUTES-DE-LA-CHAUDIÈRE-OUEST
A. 573
A. 440
369
138
368
740
132
358
175
173
73

Boischatel
Saint-Pierre-de-l'Îl
369
369
138
368
A. 573
LORETTEVILLE
Wendake
BEAUPORT
369
CHARLESBOURG
40
VAL-BELAIR
A. 440
Sainte-Pétronille
LEBOURGNEUF
DES CHÂTELS
LES RIVIÈRES
A. 440
A 973
A. 573
40
740
Québec City
132
138
L'Ancienne-Lorette
WIGLE.net
WIGLE.net
WIGLE
DESJARDINS
358
A. 440
175
nt-Augustin
L'AEROPORT
CITÉ-UNIVERSITAIRE
138
A. 540
SAINTE-FOY
–SILLERY–
CAP-ROUGE
173
d-Village
Levis
ugustin-de-Desmaures
Le Faubourg-L'Erpinière
132
LES CHUTES-DE-LA-CHAUDIÈRE-EST
CARRIE
73
Domaine-des-Îles
St Lawrence River
LES CHUTES-DE-LA-CHAUDIÈRE-OUEST


TSP100-L0092 QoS: 0 type: BT
00:11:62:2c:95:3b ? 2023-10-13 - 2023-10-14
BX 3 QoS: 0 type: BT
00:13:43:cc:56:ab ? 2023-10-12 - 2023-10-12
EPOS ADAPT 360 QoS: 0 type: BLE
00:16:94:4d:4a:de ? 2023-10-13 - 2023-10-14
QoS: 0 type: BLE
00:16:94:5a:c3:e4 ? 2023-10-12 - 2023-10-12
46325875.00008005 QoS: 2 type: BLE
00:17:55:a7:0c:21 ? 2023-10-12 - 2023-10-13
YamahaAV QoS: 1 type: BLE
00:19:01:c4:28:5c ? 2023-10-12 - 2023-10-14
GM_PEPS_VKM QoS: 0 type: BT
00:1b:fb:fd:b3:eb ? 2023-10-12 - 2023-10-12
GM_PEPS_VKM QoS: 0 type: BLE
00:1b:fb:fd:bd:29 ? 2023-10-12 - 2023-10-12
QoS: 0 type: BLE
00:1c:9b:42:69:48 ? 2023-10-13 - 2023-10-14
DORO62 QoS: 0 type: BT
00:1d:29:49:32:76 2023-10-13 - 2023-10-14
PR BT E301 QoS: 0 type: BLE
00:1f:ff:4e:48:53 ? 2023-10-12 - 2023-10-12
PR BT 42A5 QoS: 1 type: BLE
00:1f:ff:6d:70:b1 ? 2023-10-12 - 2023-10-14
GM_PEPS_VKS2 QoS: 0 type: BT
Promenade des Forts
Parc canin UMANO (secteur Desjardins)
Super C
Michaels
UQAR Lévis campus
Tim Hortons
Matto Lévis
Winners
Canadian Tire
SAROSTO
Lévis Centre des congrès
Kia Lévis
Rôtisserie Scores
Délice Resto Lounge
Starbucks
Quality Inn & Suites
Chez Ashton
Princess Auto
Rue Alphonse-Desjardins
Rue Massenet
Rue Gounod
Rue Chopin
Rue Fauré
Rue Molière
Rue Victor Hugo
Rue Verlaine
Rue Ronsard
Rue Montaigne
Rue Flaubert
Sarosto St
Rue du Terroir
173
WIGLE.NET
Map
Satellite
Keyboard shortcuts
Map data ©2023 Google

Canada - Lévis

Sounds Good Ultimate V6 earbuds

- Regex: “^Ultimate V6$”

Wireless headphones

ULTIMATE V6

★★★★½ (284)

99.99$ CAD

Quantity

1

Add

Canada - Lévis

Sounds Good Ultimate V6 earbuds

Wireless headphones

ULTIMATE V6

★★★★½ (284)

99.99$ CAD

Quantity

1

Add

- Regex: “^Ultimate V6$”

The Sounds Good adventure began in 2019, at a local flea market in Quebec City. From the very beginning, we aimed to offer quality audio products at affordable prices that you would feel confident recommending to your friends, and whose customer service would blow away even the most renowned companies.

Canada - Lévis

Sounds Good Ultimate V6 earbuds

Wireless headphones

ULTIMATE V6

★★★★½ (284)

99.99$ CAD

Quantity

1

Add

- Regex: “^Ultimate V6$”

The Sounds Good adventure began in 2019, at a local flea market in Quebec City. From the very beginning, we aimed to offer quality audio products at affordable prices that you would feel confident recommending to your friends, and whose customer service would blow away even the most renowned companies.

```
For bdaddr = 98:d3:31:50:0d:d2:
        Company Name by IEEE OUI (98:d3:31): Shenzhen Bolutek Technology Co.,Ltd.
                BDADDR is Bluetooth Low Energy Public

        No BTC Extended Inquiry Result Device info.

        DeviceName: Ultimate V6
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 19 which corresponds to (New wireshark) Connectable, Scannable

        UUID16s found:
                UUID16 0x180f (GATT Service ID: Battery)
                UUID16 0xfd92 (Company ID: Qualcomm Technologies International, Ltd. (QTIL))
                        Found in BT LE data (LE_bdaddr_to_UUID16s), bdaddr_random = 0 (Public)
                This was found in an event of type 19 which corresponds to (New wireshark) Connectable, Scannable
```

Canada - Lévis

Sounds Good Ultimate V6 earbuds

Wireless headphones

ULTIMATE V6

★★★★½ (284)

99.99$ CAD

Quantity

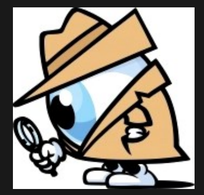
1

Add

- Regex: “^Ultimate V6$”

The Sounds Good adventure began in 2019, at a local flea market in Quebec City. From the very beginning, we aimed to offer quality audio products at affordable prices that you would feel confident recommending to your friends, and whose customer service would blow away even the most renowned companies.

```
For bdaddr = 98:d3:31:50:0d:d2:
        Company Name by IEEE OUI (98:d3:31): Shenzhen Bolutek Technology Co.,Ltd.
                BDADDR is Bluetooth Low Energy Public

        No BTC Extended Inquiry Result Device info.

        DeviceName: Ultimate V6
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 19 which corresponds to (New wireshark) Connectable, Scannable

        UUID16s found:
                UUID16 0x180f (GATT Service ID: Battery)
                UUID16 0xfd92 (Company ID: Qualcomm Technologies International, Ltd. (QTIL))
                        Found in BT LE data (LE_bdaddr_to_UUID16s), bdaddr_random = 0 (Public)
                This was found in an event of type 19 which corresponds to (New wireshark) Connectable, Scannable
```



Canada - Lévis

Sounds Good Ultimate V6 earbuds

Wireless headphones

ULTIMATE V6

★★★★½ (284)

99.99$ CAD

Quantity

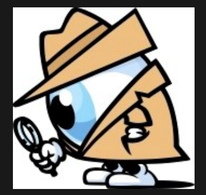
1

Add

- Regex: “^Ultimate V6$”

The Sounds Good adventure began in 2019, at a local flea market in Quebec City. From the very beginning, we aimed to offer quality audio products at affordable prices that you would feel confident recommending to your friends, and whose customer service would blow away even the most renowned companies.

```
For bdaddr = 98:d3:31:50:0d:d2:
        Company Name by IEEE OUI (98:d3:31): Shenzhen Bolutek Technology Co.,Ltd.
                BDADDR is Bluetooth Low Energy Public

        No BTC Extended Inquiry Result Device info.

        DeviceName: Ultimate V6
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 19 which corresponds to (New wireshark) Connectable, Scannable

        UUID16s found:
                UUID16 0x180f (GATT Service ID: Battery)
                UUID16 0xfd92 (Company ID: Qualcomm Technologies International, Ltd. (QTIL))
                        Found in BT LE data (LE_bdaddr_to_UUID16s), bdaddr_random = 0 (Public)
                This was found in an event of type 19 which corresponds to (New wireshark) Connectable, Scannable
```



Canada - Lévis

Sounds Good Ultimate V6 earbuds

Wireless headphones

ULTIMATE V6

★★★★½ (284)

99.99$ CAD

Quantity

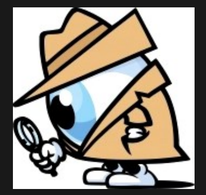
1

Add

- Regex: “^Ultimate V6$”

The Sounds Good adventure began in 2019, at a local flea market in Quebec City. From the very beginning, we aimed to offer quality audio products at affordable prices that you would feel confident recommending to your friends, and whose customer service would blow away even the most renowned companies.

```
For bdaddr = 98:d3:31:50:0d:d2:
        Company Name by IEEE OUI (98:d3:31): Shenzhen Bolutek Technology Co.,Ltd.
                BDADDR is Bluetooth Low Energy Public

        No BTC Extended Inquiry Result Device info.

        DeviceName: Ultimate V6
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 19 which corresponds to (New wireshark) Connectable, Scannable

        UUID16s found:
                UUID16 0x180f (GATT Service ID: Battery)
                UUID16 0xfd92 (Company ID: Qualcomm Technologies International, Ltd. (QTIL))
                        Found in BT LE data (LE_bdaddr_to_UUID16s), bdaddr_random = 0 (Public)
                This was found in an event of type 19 which corresponds to (New wireshark) Connectable, Scannable
```



Canada - Lévis

Sounds Good Ultimate V6 earbuds

Wireless headphones

ULTIMATE V6

★★★★½ (284)

99.99$ CAD

Quantity

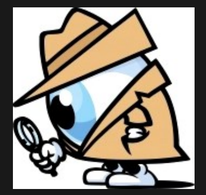
1

Add

- Regex: “^Ultimate V6$”

The Sounds Good adventure began in 2019, at a local flea market in Quebec City. From the very beginning, we aimed to offer quality audio products at affordable prices that you would feel confident recommending to your friends, and whose customer service would blow away even the most renowned companies.

```
For bdaddr = 98:d3:31:50:0d:d2:
        Company Name by IEEE OUI (98:d3:31): Shenzhen Bolutek Technology Co.,Ltd.
                BDADDR is Bluetooth Low Energy Public

        No BTC Extended Inquiry Result Device info.

        DeviceName: Ultimate V6
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 19 which corresponds to (New wireshark) Connectable, Scannable

        UUID16s found:
                UUID16 0x180f (GATT Service ID: Battery)
                UUID16 0xfd92 (Company ID: Qualcomm Technologies International, Ltd. (QTIL))
                        Found in BT LE data (LE_bdaddr_to_UUID16s), bdaddr_random = 0 (Public)
                This was found in an event of type 19 which corresponds to (New wireshark) Connectable, Scannable
```



Ca

Sou

- Re

The Sounds G
audio produc
blow away eve

```
For bdaddr =
        Comp

        No B

        Devi


        UUID
```

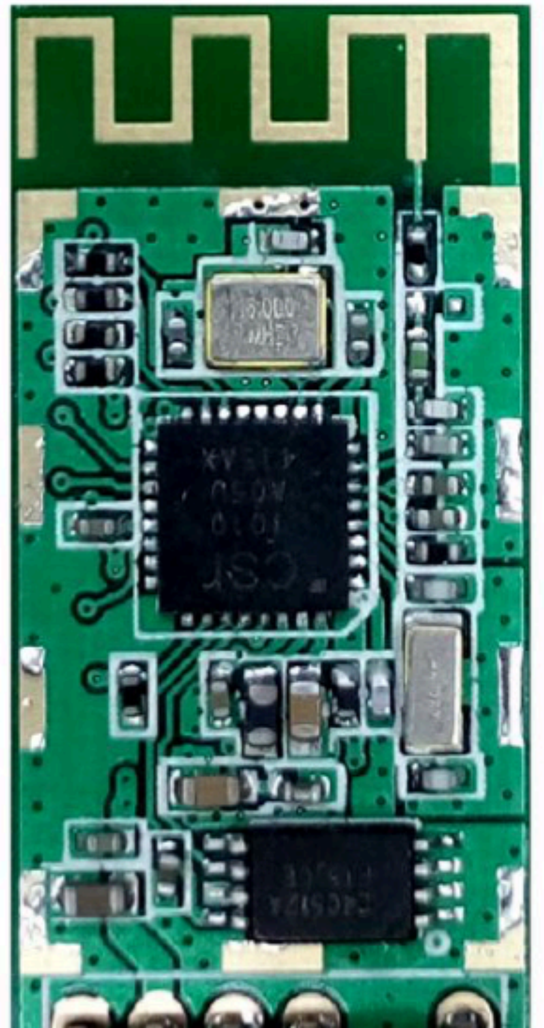
BOLUTEK

BOLUTEK MESH-1010-D MESH MODULE

1. Overview

MESH-1010-D MESH module Shenzhen BOLUTEK Electronics Technology Co., Ltd. is designed for data transmission and intelligent MESH build, using Qualcomm chip solution, compliant with the Bluetooth V4.0 specification.

This module uses 2.0mm pitch pin connections, low cost, small size, low power consumption, high receive sensitivity, easy to use and flexible, etc., can be composed of Mesh networks, network between each module.



ireless headphones

LTIMATE V6

★★★★⯪ (284)

9.99$ CAD

uantity

Add

offer quality
vice would

Scannable

Scannable

. Overview

MESH-1010-D MESH module Shenzhen BOLUTEK lectronics Technology Co., Ltd. is designed for data ansmission and intelligent MESH build, using ualcomm chip solution, compliant with the Bluetooth 4.0 specification.

This module uses 2.0mm pitch pin connections, low ost, small size, low power consumption, high receive

Canad

Sounds

- Regex:

The Sounds Good ad
audio products at affo
blow away even the m

```
For bdaddr = 98:d3
        Company Na
                BD

        No BTC Ext

        DeviceName
                In
                Th

        UUID16s fo
                UU
                UU

                Th
```

low

th

Canad

Sounds

- Regex:

The Sounds Good ad
audio products at affo
blow away even the m

```
For bdaddr = 98:d3
        Company Na
                BD

        No BTC Ext

        DeviceName
                In
                Th

        UUID16s fo
                UU
                UU

                Th
```

Québec City
Trois-Rivières
Algonquin
Provincial
Park
Ottawa
Montreal
Sherbrooke
VERMONT
Kingston
Toronto
NEW

Canada - Toronto

SecTor 2023

QoS: **0** type: **BLE**
00:02:3c:7f:d8:c1 ? 2023-10-24 - 2023-10-24

QoS: **0** type: **BLE**
00:07:80:a6:3a:6a ? 2023-10-24 - 2023-10-24

PIX0lnl QoS: **0** type: **BLE**
00:07:ce:d0:89:c8 ? 2023-10-24 - 2023-10-24

PIX5iyE QoS: **0** type: **BLE**
00:07:ce:e6:2c:84 ? 2023-10-24 - 2023-10-24

LE_ATH-M50xBT2 QoS: **0** type: **BLE**
00:0a:45:23:b5:89 ? 2023-10-24 - 2023-10-24

QoS: **0** type: **BLE**
00:0c:8a:63:ec:9f ? 2023-10-24 - 2023-10-24

QoS: **0** type: **BLE**
00:0d:e2:2d:6e:55 ? 2023-10-24 - 2023-10-24

QoS: **0** type: **BLE**
00:0e:db:97:48:b6 ? 2023-10-24 - 2023-10-24

QoS: **0** type: **BLE**
00:10:68:9c:88:fc ? 2023-10-24 - 2023-10-24

QoS: **0** type: **BLE**
00:10:7f:9a:10:e1 ? 2023-10-24 - 2023-10-24

QoS: **0** type: **BLE**
00:10:7f:9a:15:d7 ? 2023-10-24 - 2023-10-24

QoS: **0** type: **BLE**
00:12:14:bf:81:89 ? 2023-10-24 - 2023-10-24

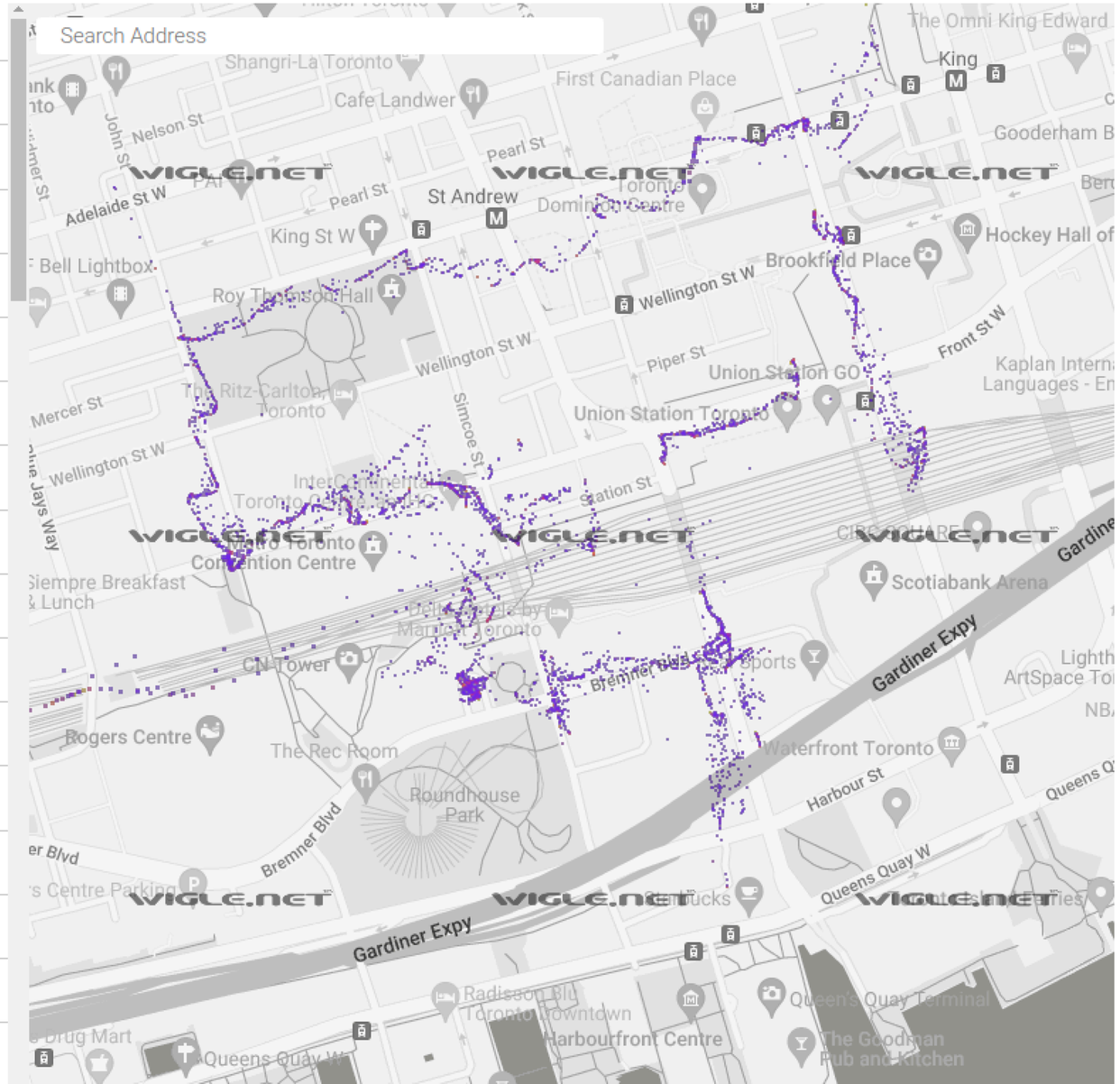
QoS: **0** type: **BLE**
00:14:fa:1b:59:61 ? 2023-10-24 - 2023-10-24

Cubinote-BFF2 QoS: **0** type: **BT**
00:15:83:0d:bf:f2 ? 2023-10-24 - 2023-10-24

QoS: **0** type: **BLE**
00:1b:66:0d:79:33 ? 2023-10-24 - 2023-10-24

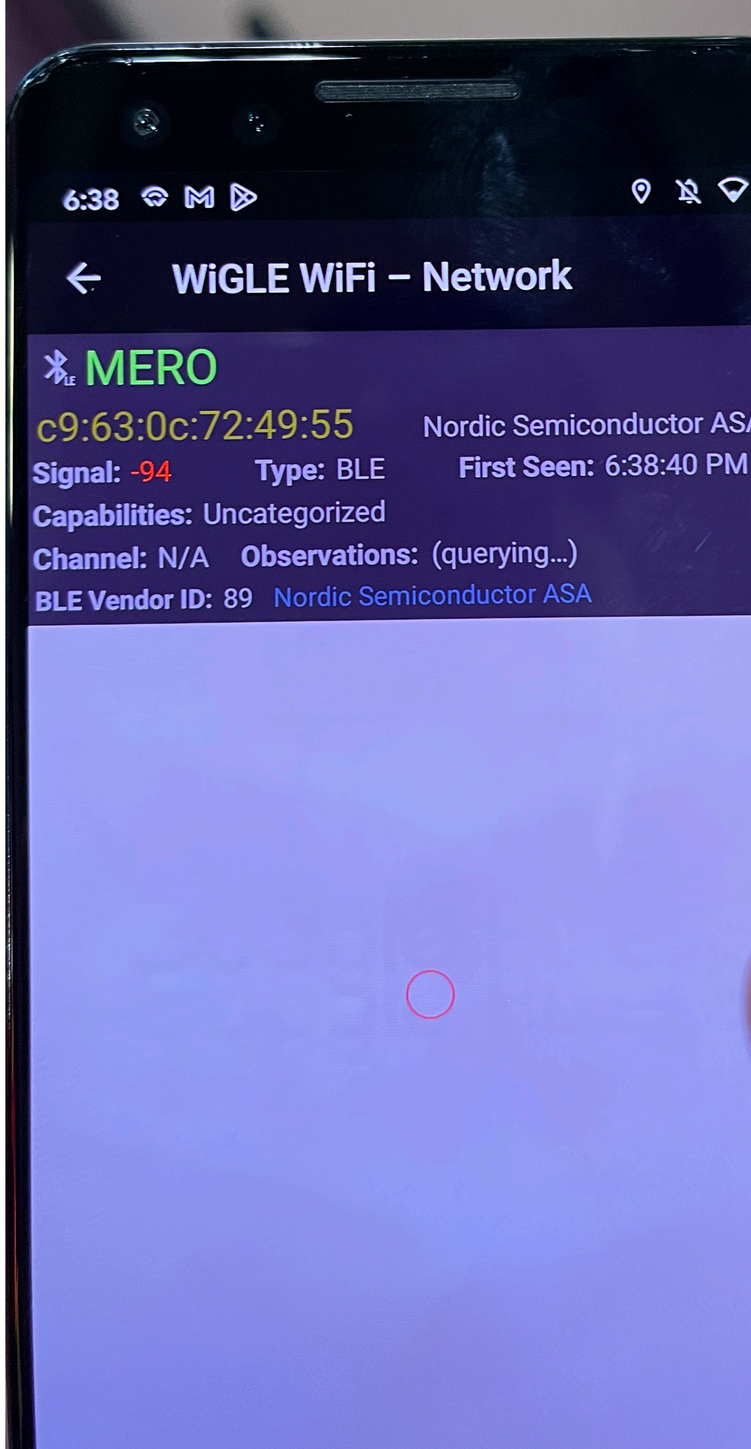
QoS: **0** type: **BLE**
00:1b:66:0f:38:ee ? 2023-10-24 - 2023-10-24

CX Plus True Wireless QoS: **0** type: **BLE**
00:1b:66:13:f8:a5 ? 2023-10-24 - 2023-10-24



Canada - Toronto

- Regex: ^MERO$



Canada - Toronto

- Regex: ^MERO$

MERO QoS: 0 type: BLE
ef:90:d6:fe:30:34? 2022-12-29 - 2022-12-31

MERO QoS: 0 type: BLE
f0:3e:26:ae:52:93? 2023-03-01 - 2023-03-01

MERO QoS: 0 type: BLE
f0:98:8f:3f:3a:32? 2022-12-29 - 2022-12-31

MERO QoS: 0 type: BLE
f2:9a:04:48:25:a5? 2023-02-20 - 2023-02-21

MERO QoS: 0 type: BLE
f2:a1:31:fe:8e:d5? 2023-10-24 - 2023-10-24

MERO QoS: 0 type: BLE
f3:bb:9b:33:b4:4b? 2022-08-14 - 2022-08-14

MERO QoS: 0 type: BLE
f4:a3:7b:6e:49:28? 2022-09-12 - 2022-09-12

MERO QoS: 0 type: BLE
f4:f1:8f:c3:af:e7? 2023-10-24 - 2023-10-24

MERO QoS: 0 type: BLE
f5:0a:5d:25:1c:f8? 2023-03-01 - 2023-03-01

MERO QoS: 0 type: BLE
f5:18:fc:44:46:97? 2022-12-29 - 2022-12-31

The visibility and insights you need deliver stellar cleaning results

Understand what's happening across your sites, pinpoint problem areas, get recommendations on how to maximize productivity, and put them into action - all from one platform.

SEE IT IN ACTION

From https://mero.co

276 Queen St W Unit 200
Toronto, ON
M5V 2A1

The visibility and insights you need deliver stellar cleaning results

Understand what's happening across your sites, pinpoint problem areas, get recommendations on how to maximize productivity, and put them into action - all from one platform.

SEE IT IN ACTION

From https://mero.co

Canada - Toronto

```
For bdaddr = cb:9c:77:d7:9b:7c:
        Company Name by IEEE OUI: Not Applicable because this is a Random Static address

        No BTC Extended Inquiry Result Device info.

        DeviceName: MERO
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 16 which corresponds to (New wireshark) (none of scannable, connectable, etc listed)

        No UUID16s found.

        No Service Solicit UUID16s found.

        No UUID128s found.

        No Service Solicit UUID128s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x0059 (Nordic Semiconductor ASA) - 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): 0x5900 (No Match)
                Raw Data: 0502be77723d0000000000000005
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 1 (Random Static)
                        This was found in an event of type 16 which corresponds to (New wireshark) (none of scannable, connectable, etc listed)
```

Canada - Toronto

```
For bdaddr = cb:9c:77:d7:9b:7c:
        Company Name by IEEE OUI: Not Applicable because this is a Random Static address

        No BTC Extended Inquiry Result Device info.

        DeviceName: MERO
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 16 which corresponds to (New wireshark) (none of scannable, connectable, etc listed)

        No UUID16s found.

        No Service Solicit UUID16s found.

        No UUID128s found.

        No Service Solicit UUID128s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x0059 (Nordic Semiconductor ASA) - 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): 0x5900 (No Match)
                Raw Data: 0502be77723d0000000000000005
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 1 (Random Static)
                        This was found in an event of type 16 which corresponds to (New wireshark) (none of scannable, connectable, etc listed)
```

Canada - Toronto

```
For bdaddr = cb:9c:77:d7:9b:7c:
        Company Name by IEEE OUI: Not Applicable because this is a Random Static address

        No BTC Extended Inquiry Result Device info.

        DeviceName: MERO
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 16 which corresponds to (New wireshark) (none of scannable, connectable, etc listed)

        No UUID16s found.

        No Service Solicit UUID16s found.

        No UUID128s found.

        No Service Solicit UUID128s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x0059 (Nordic Semiconductor ASA) - 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): 0x5900 (No Match)
                Raw Data: 0502be77723d0000000000000005
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 1 (Random Static)
                        This was found in an event of type 16 which corresponds to (New wireshark) (none of scannable, connectable, etc listed)
```

```
                Raw Data: 0502028bad820000000000000005

                Raw Data: 010210ee146b011f000000000005
```

Different devices broadcast different data

Italy - Milan / Bergamo - NoHat 2023

GR-AC_10001_10_6804_SC QoS: **0** type: **BT**
00:00:00:03:3c:01 ? 2023-10-20 - 2023-10-20

DST+0048 QoS: **0** type: **BT**
00:07:80:49:5f:1d ? 2023-10-20 - 2023-10-20

QoS: **0** type: **BT**
00:08:e0:1b:bd:ca ? 2023-10-20 - 2023-10-20

QoS: **0** type: **BT**
00:0a:9b:2d:e6:ed ? 2023-10-20 - 2023-10-20

STANMORE II QoS: **0** type: **BLE**
00:12:6f:56:64:31 ? 2023-10-20 - 2023-10-20

HD 450SE QoS: **0** type: **BLE**
00:1b:66:05:65:f5 ? 2023-10-20 - 2023-10-20

HD 250BT QoS: **0** type: **BLE**
00:1b:66:0c:ea:52 ? 2023-10-20 - 2023-10-20

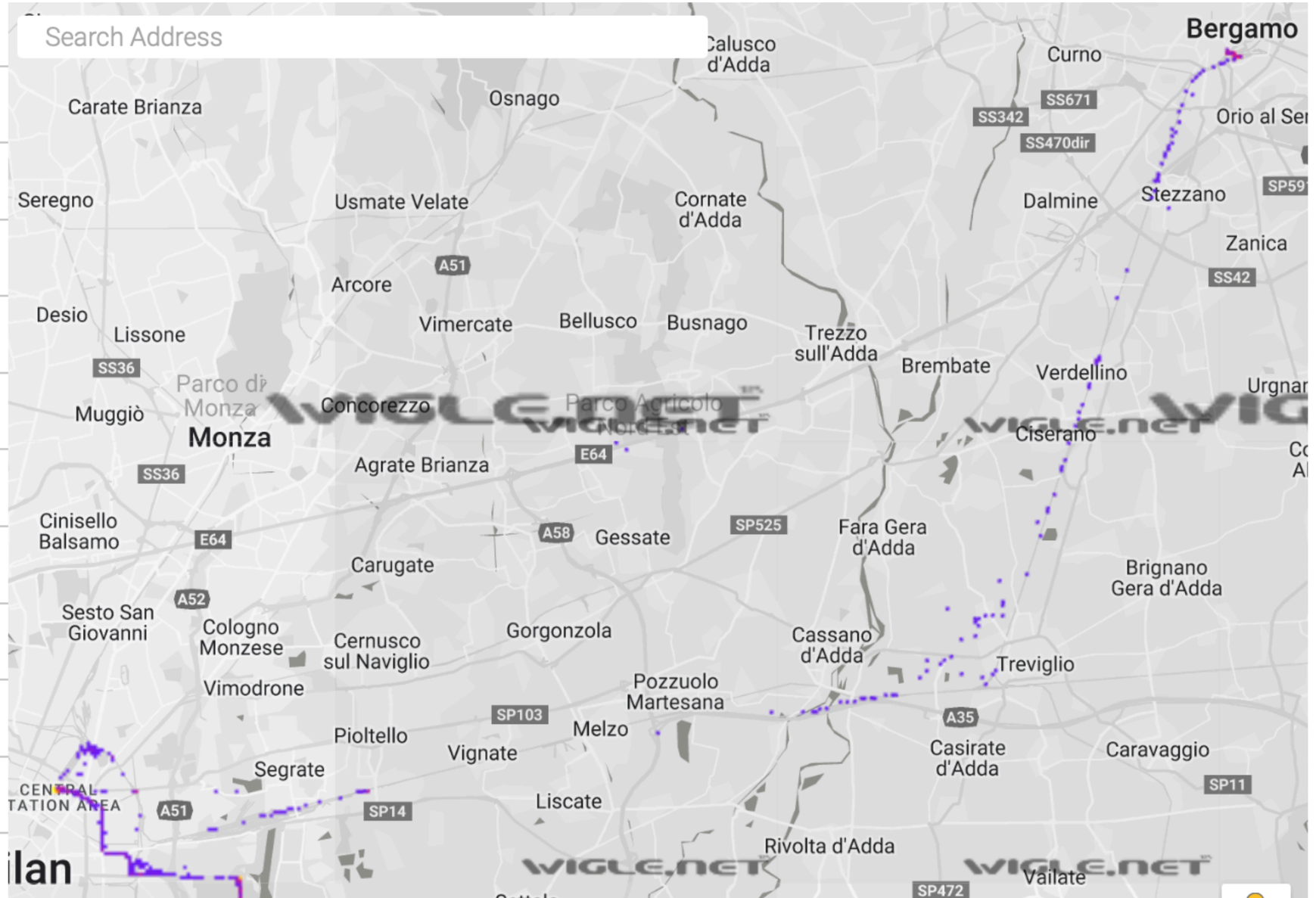
QoS: **0** type: **BT**
00:23:3d:13:d0:79 ? 2023-10-20 - 2023-10-20

QoS: **0** type: **BLE**
00:3c:84:97:73:fb ? 2023-10-20 - 2023-10-20

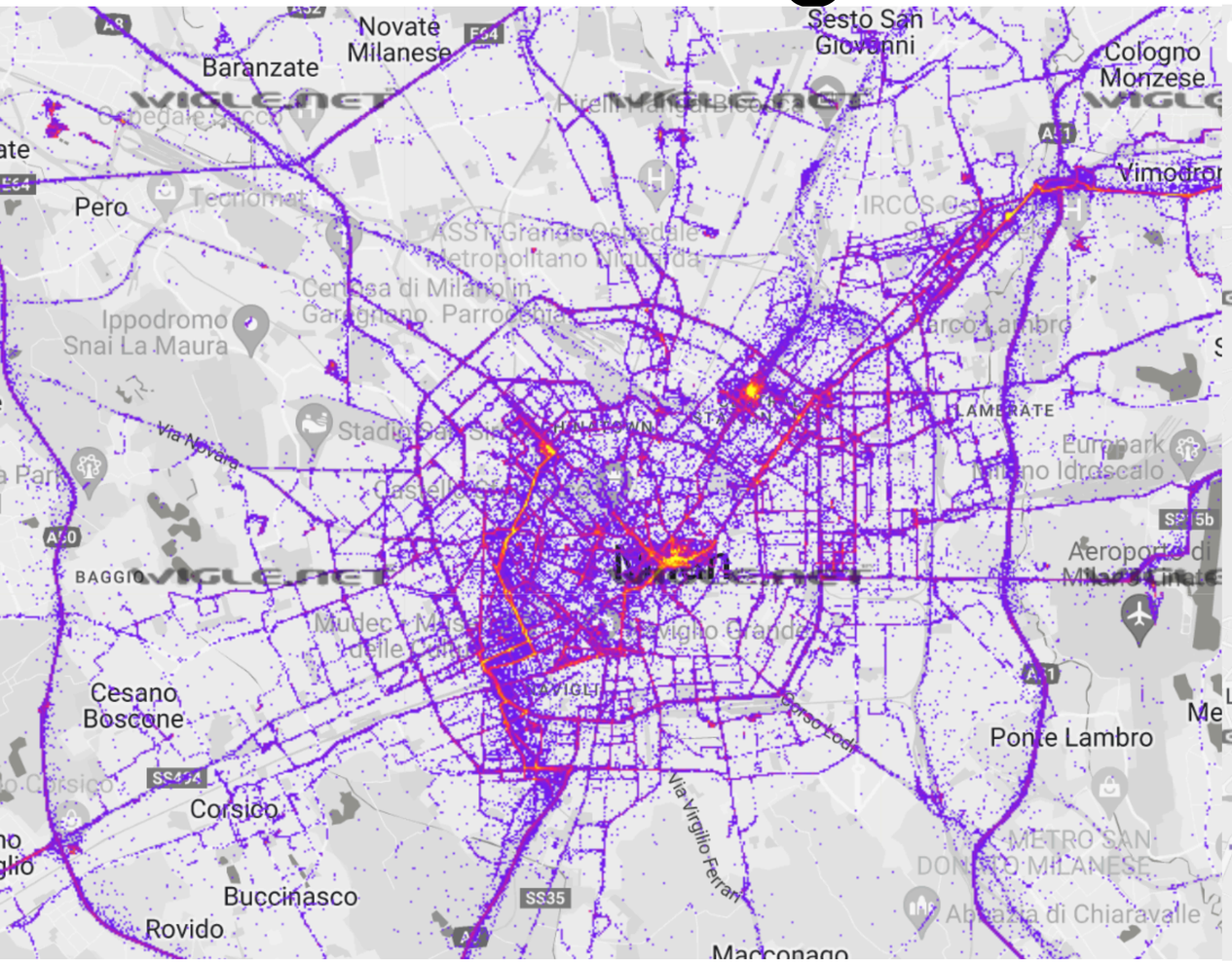
QoS: **0** type: **BLE**
00:42:56:5b:49:d3 ? 2023-10-20 - 2023-10-20

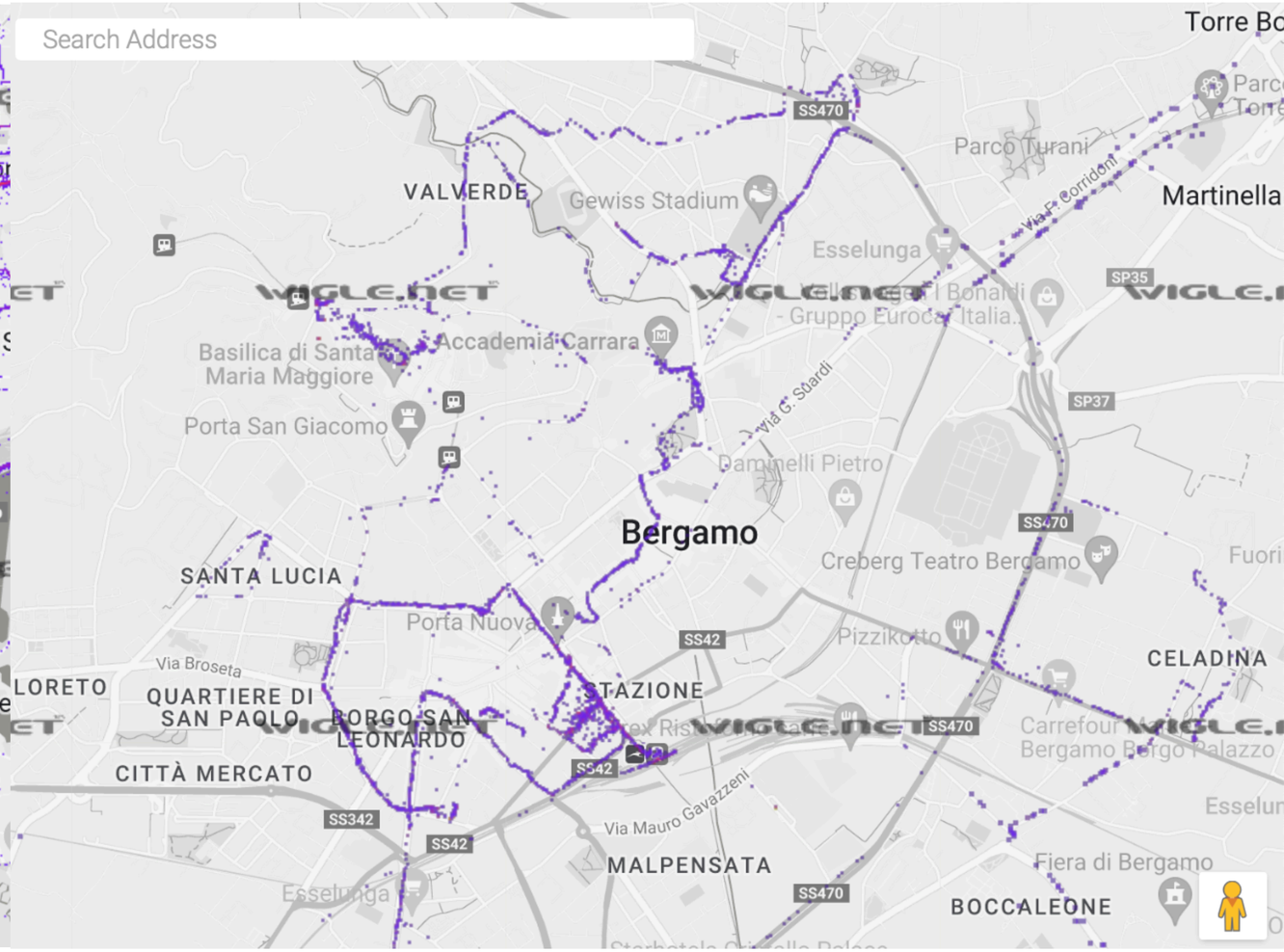
QoS: **0** type: **BLE**
00:53:00:cd:93:cb ? 2023-10-20 - 2023-10-20

C03 QoS: **0** type: **BLE**
00:62:16:2f:25:0f ? 2023-10-20 - 2023-10-20

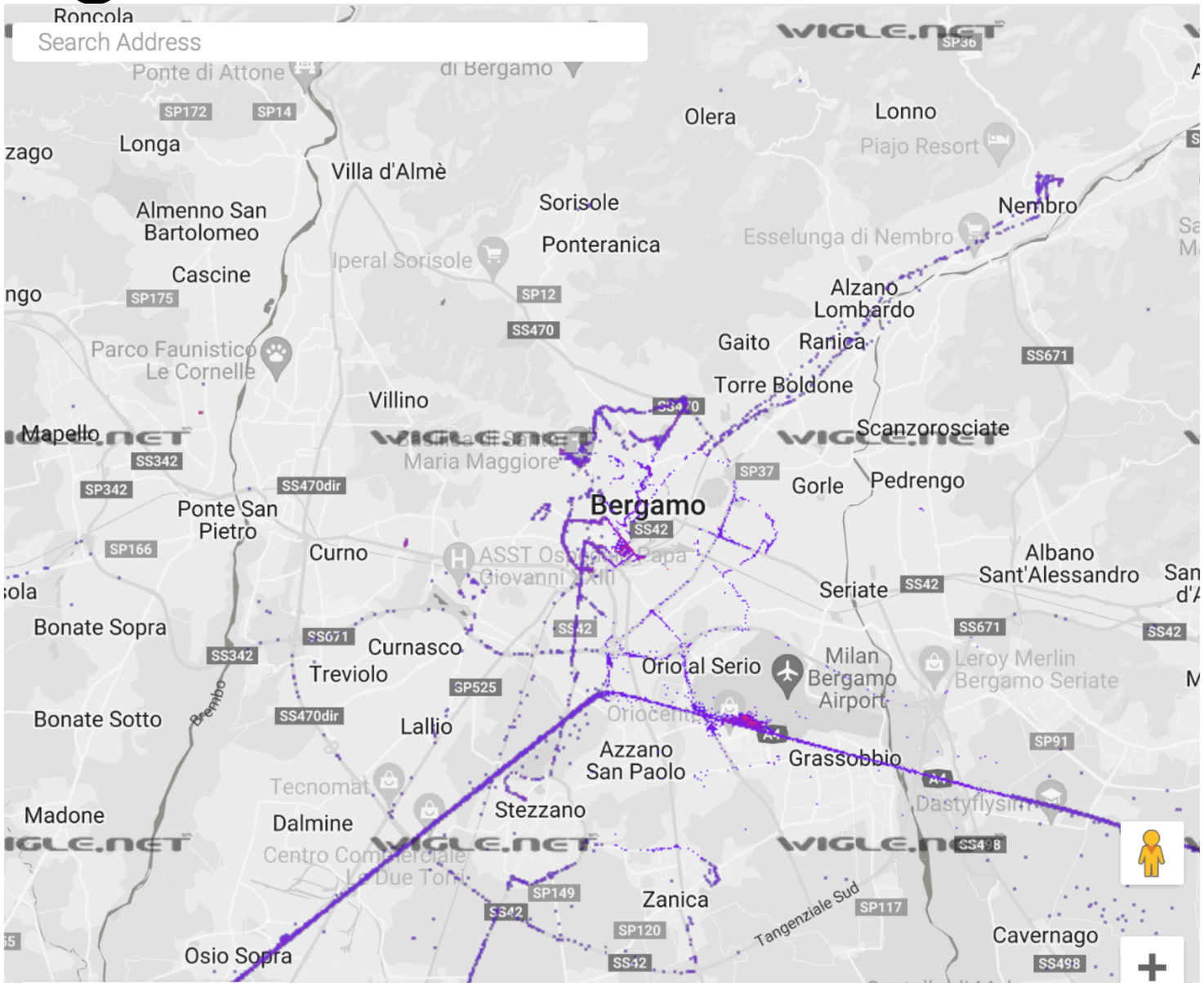


Milan vs. Bergamo

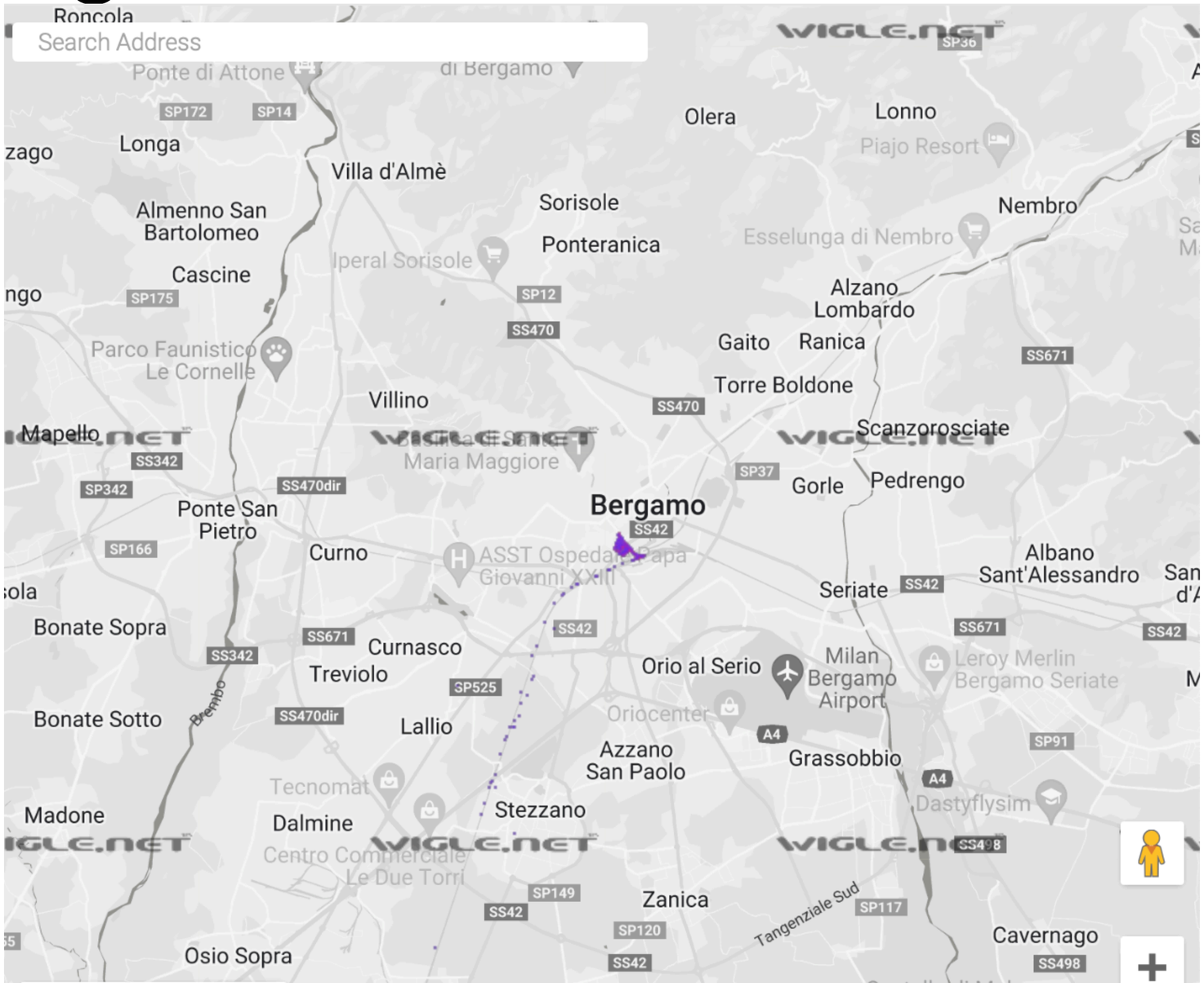




Italy - Bergamo

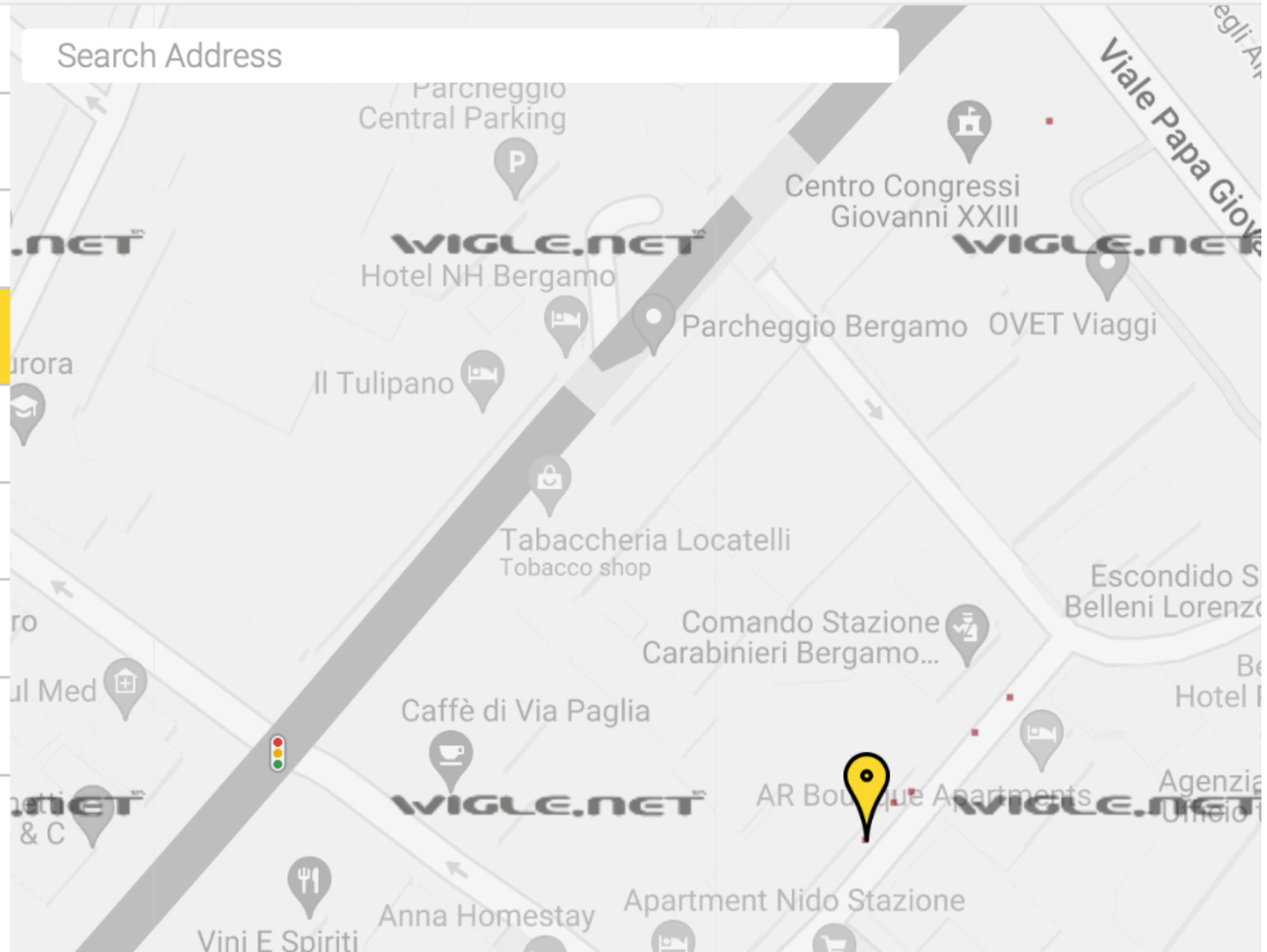


Italy - Bergamo



Italy - Daikin

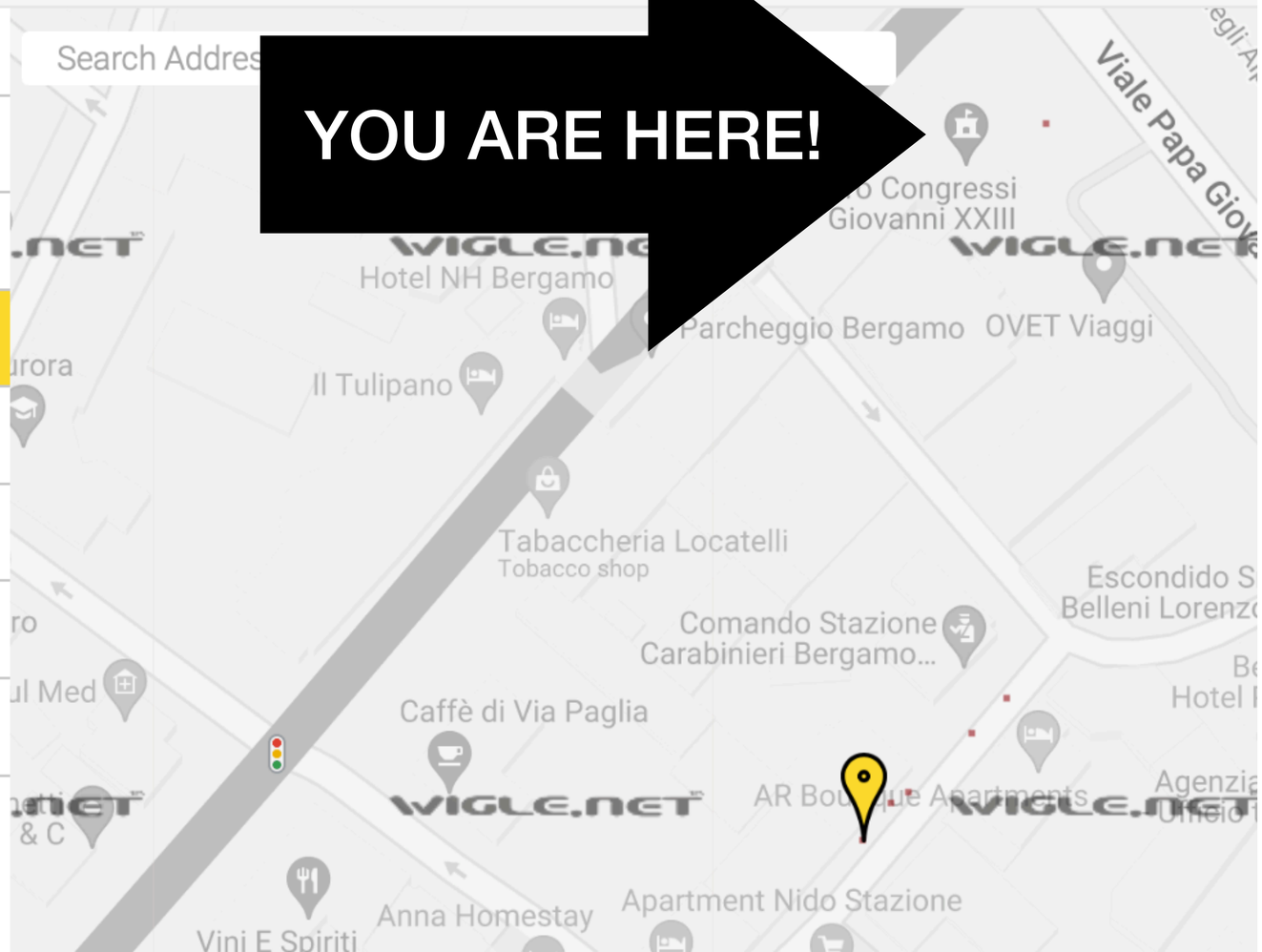
Daikin	QoS: 0 type: BLE	
50:61:f6:67:73:ca ?	2023-10-20 - 2023-10-20	
Daikin	QoS: 0 type: BLE	
50:61:f6:67:8b:01 ?	2023-10-20 - 2023-10-20	
Daikin	QoS: 0 type: BLE	
50:61:f6:67:93:46 ?	2023-10-20 - 2023-10-20	
Daikin	QoS: 0 type: BLE	
50:61:f6:67:c2:92 ?	2023-10-20 - 2023-10-20	
Daikin	QoS: 0 type: BLE	
50:61:f6:6e:4e:fd ?	2023-10-20 - 2023-10-20	
Daikin	QoS: 0 type: BLE	
50:61:f6:6e:aa:fa ?	2023-10-20 - 2023-10-20	
Daikin	QoS: 0 type: BLE	
50:61:f6:6e:c9:75 ?	2023-10-20 - 2023-10-20	
Daikin	QoS: 0 type: BLE	
f4:93:1c:88:a0:82 ?	2023-10-20 - 2023-10-20	



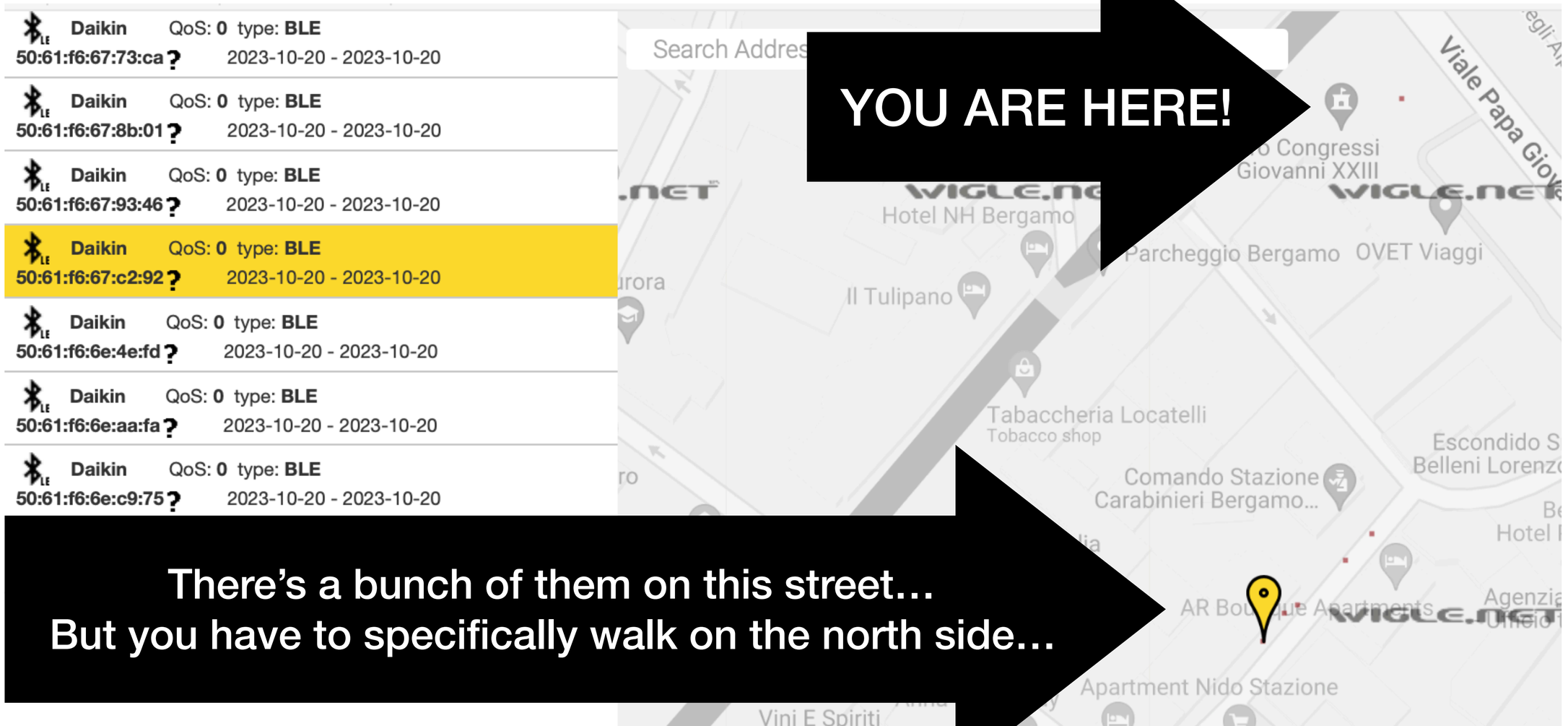
Italy - Daikin

Daikin	QoS: 0 type: BLE	
50:61:f6:67:73:ca ?	2023-10-20 - 2023-10-20	
Daikin	QoS: 0 type: BLE	
50:61:f6:67:8b:01 ?	2023-10-20 - 2023-10-20	
Daikin	QoS: 0 type: BLE	
50:61:f6:67:93:46 ?	2023-10-20 - 2023-10-20	
Daikin	QoS: 0 type: BLE	
50:61:f6:67:c2:92 ?	2023-10-20 - 2023-10-20	
Daikin	QoS: 0 type: BLE	
50:61:f6:6e:4e:fd ?	2023-10-20 - 2023-10-20	
Daikin	QoS: 0 type: BLE	
50:61:f6:6e:aa:fa ?	2023-10-20 - 2023-10-20	
Daikin	QoS: 0 type: BLE	
50:61:f6:6e:c9:75 ?	2023-10-20 - 2023-10-20	
Daikin	QoS: 0 type: BLE	
f4:93:1c:88:a0:82 ?	2023-10-20 - 2023-10-20	

YOU ARE HERE!



Italy - Daikin



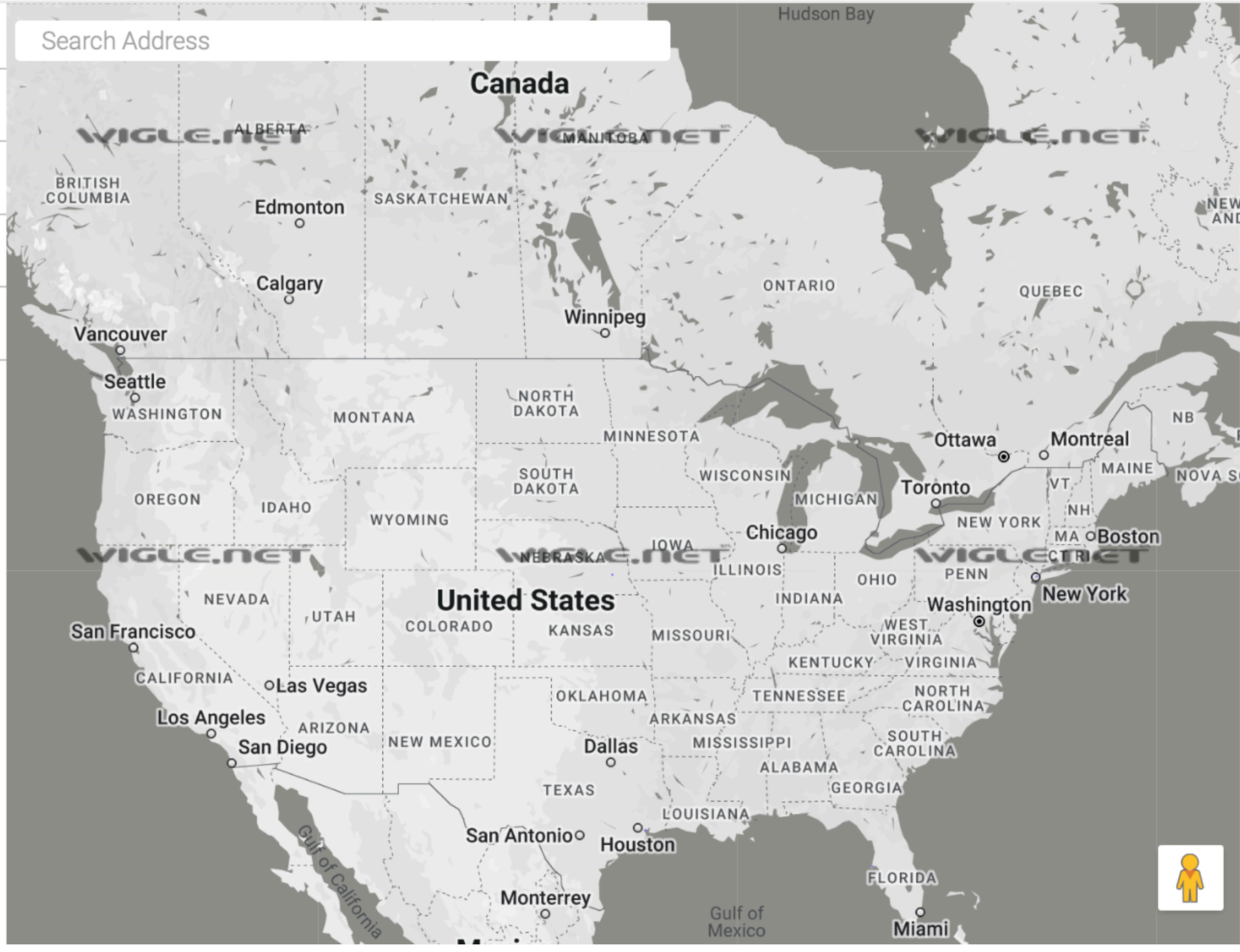
Daikin QoS: **0** type: **BLE**
8c:3a:7e:f3:bc:15 ? 2023-07-04 - 2023-07-04

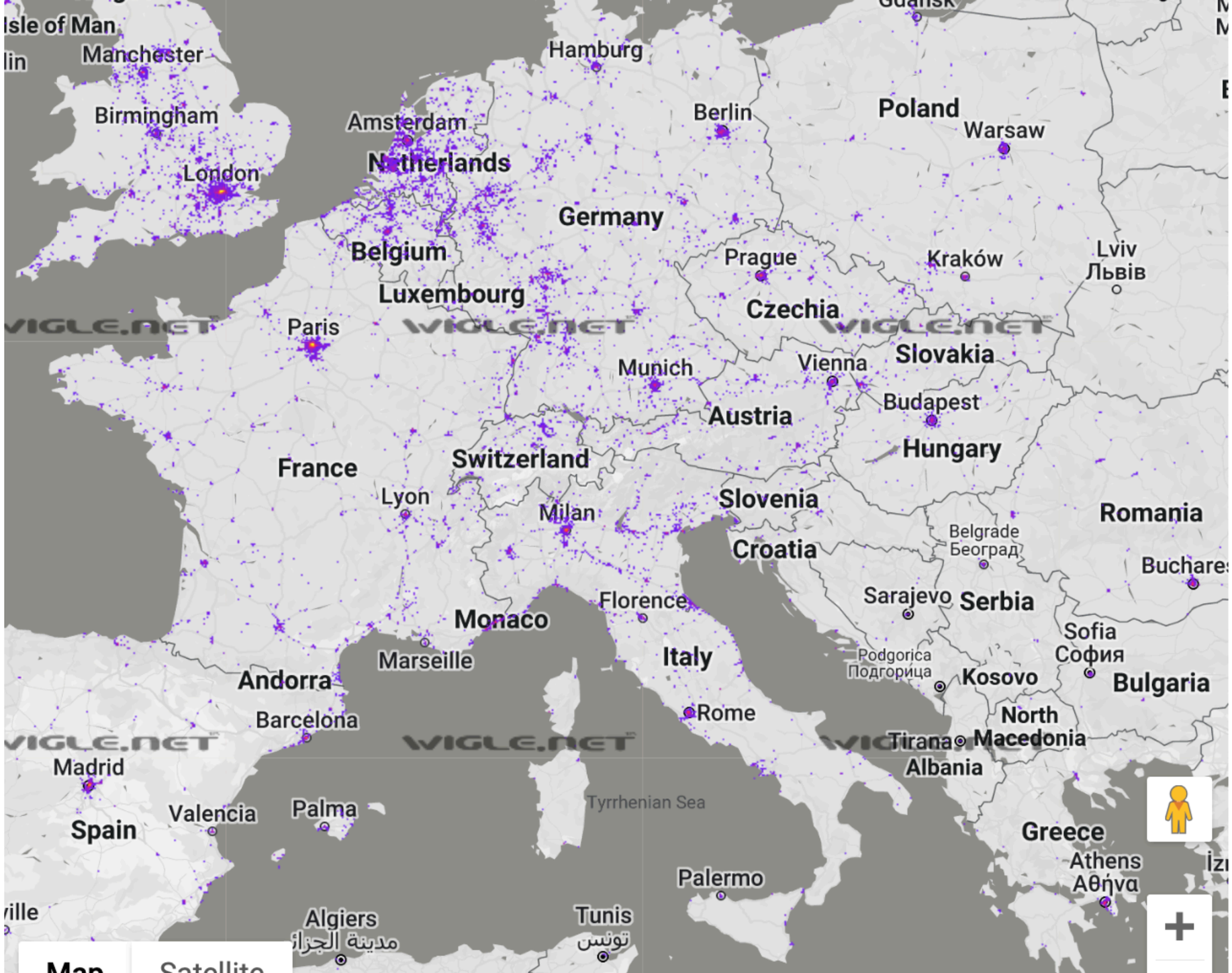
Daikin QoS: **0** type: **BLE**
8c:3a:7e:f3:cc:3c ? 2023-07-04 - 2023-07-04

Daikin QoS: **4** type: **BLE**
94:0d:2d:47:0e:26 ? 2023-08-20 - 2023-10-09

Daikin QoS: **5** type: **BLE**
b8:e3:ee:4e:82:90 ? 2021-11-04 - 2022-05-24

Daikin QoS: **6** type: **BLE**
ef:bb:b3:31:2c:79 ? 2021-06-02 - 2022-09-20




Isle of Man
Manchester
Hamburg
Birmingham
Amsterdam
Berlin
Poland
Warsaw
Netherlands
London
Germany
Belgium
Prague
Kraków
Lviv
Львів
Luxembourg
Czechia
Paris
Slovakia
Munich
Vienna
Budapest
Austria
Hungary
France
Switzerland
Lyon
Slovenia
Milan
Romania
Belgrade
Београд
Croatia
Florence
Sarajevo
Serbia
Monaco
Sofia
София
Marseille
Italy
Podgorica
Подгорица
Kosovo
Andorra
Bulgaria
Barcelona
Rome
North
Macedonia
Tirana
Albania
Madrid
Tyrrhenian Sea
Valencia
Palma
Spain
Greece
Athens
Αθήνα
Palermo
Algiers
مدينة الجزائر
Tunis
تونس
Map
Satellite

~~Italy~~ Europe - Daikin

daikin bluetooth

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

About 5,740,000 results (0.28 seconds)

Tip: Limit this search to **English** language results. Learn more about filtering by language

DENV | Daikin
https://www.daikin.eu › ... › Control systems

Madoka wired remote control

Connect with your smartphone via **Bluetooth** Low Energy communication; Visual interface helps you schedule, set point restriction and offers other settings for ...

~~Italy~~ Europe - Daikin

daikin bluetooth

Shopping | Images | Videos | News | Maps | Books

About 5,740,000 results (0.28 seconds)

Tip: Limit this search to **English** language results. Learn more ab

DENV | Daikin
https://www.daikin.eu › ... › Control systems

Madoka wired remote control

Connect with your smartphone via **Bluetooth** Low Energy communication; interface helps you schedule, set point restriction and offers other settings

~~Italy~~ Europe - Daikin

```
For bdaddr = 00:cc:3f:93:8f:ce:
        Company Name by IEEE OUI (00:cc:3f): Universal Electronics, Inc.
                BDADDR is Bluetooth Low Energy Public

        No BTC Extended Inquiry Result Device info.

        DeviceName: Daikin
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 19 which corresponds to (New wireshark) Connectable, Scannable
        DeviceName: Sala
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response

        No UUID16s found.

        No Service Solicit UUID16s found.

        No UUID128s found.

        No Service Solicit UUID128s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x0093 (Universal Electronics, 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): 0x9300 (No Match)
                Raw Data: e000
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
                        This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response
```

~~Italy~~ Europe - Daikin

```
For bdaddr = 00:cc:3f:93:8f:ce:
        Company Name by IEEE OUI (00:cc:3f): Universal Electronics, Inc.
                BDADDR is Bluetooth Low Energy Public

        No BTC Extended Inquiry Result Device info.

        DeviceName: Daikin
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 19 which corresponds to (New wireshark) Connectable, Scannable
        DeviceName: Sala
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response

        No UUID16s found.

        No Service Solicit UUID16s found.

        No UUID128s found.

        No Service Solicit UUID128s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x0093 (Universal Electronics, 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): 0x9300 (No Match)
                Raw Data: e000
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
                        This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response
```

~~Italy~~ Europe - Daikin

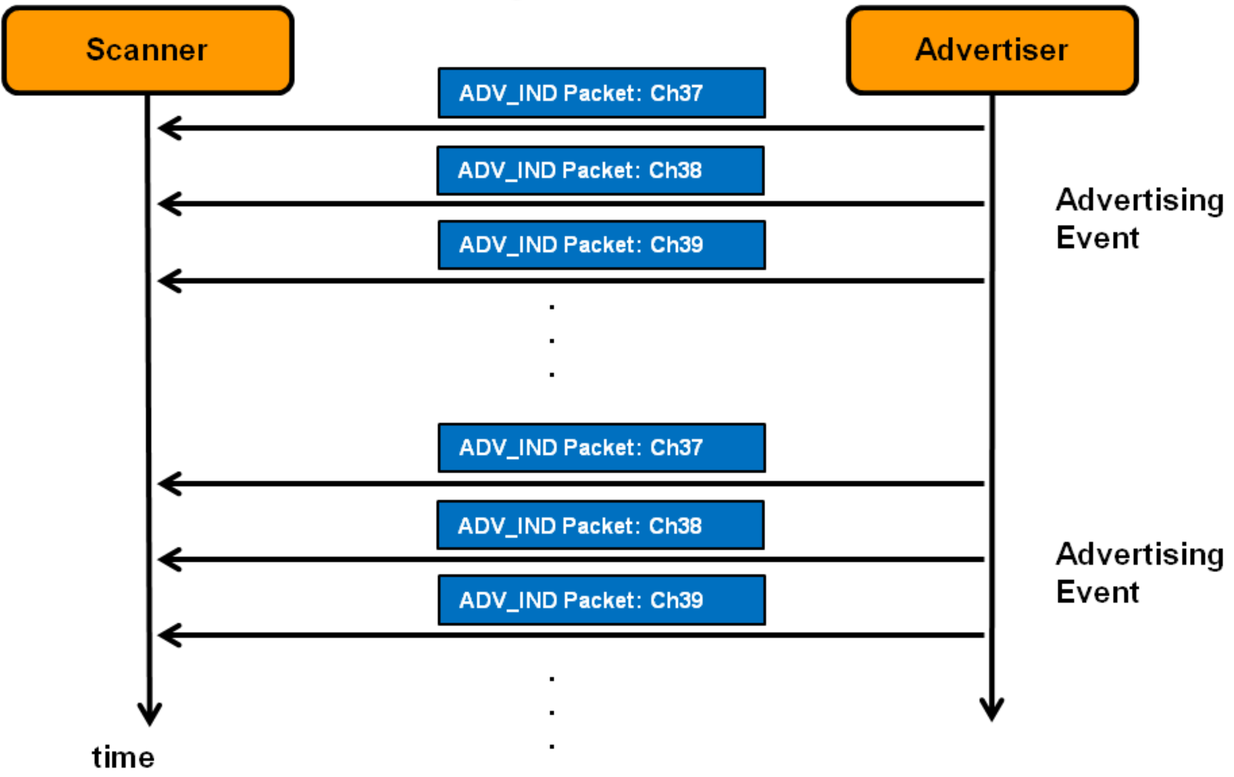
```
For bdaddr = 00:cc:3f:93:8f:ce:
        Company Name by IEEE OUI (00:cc:3f): Universal Electronics, Inc.
                BDADDR is Bluetooth Low Energy Public

        No BTC Extended Inquiry Result Device info.

        DeviceName: Daikin
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 19 which corresponds to (New wireshark) Connectable, Scannable
        DeviceName: Sala
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response

        No UUID16s found.

        No Service Solicit UUID16s found.

        No UUID128s found.

        No Service Solicit UUID128s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x0093 (Universal Electronics, 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): 0x9300 (No Match)
                Raw Data: e000
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
                        This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response
```

~~Italy~~ Europe - Daikin

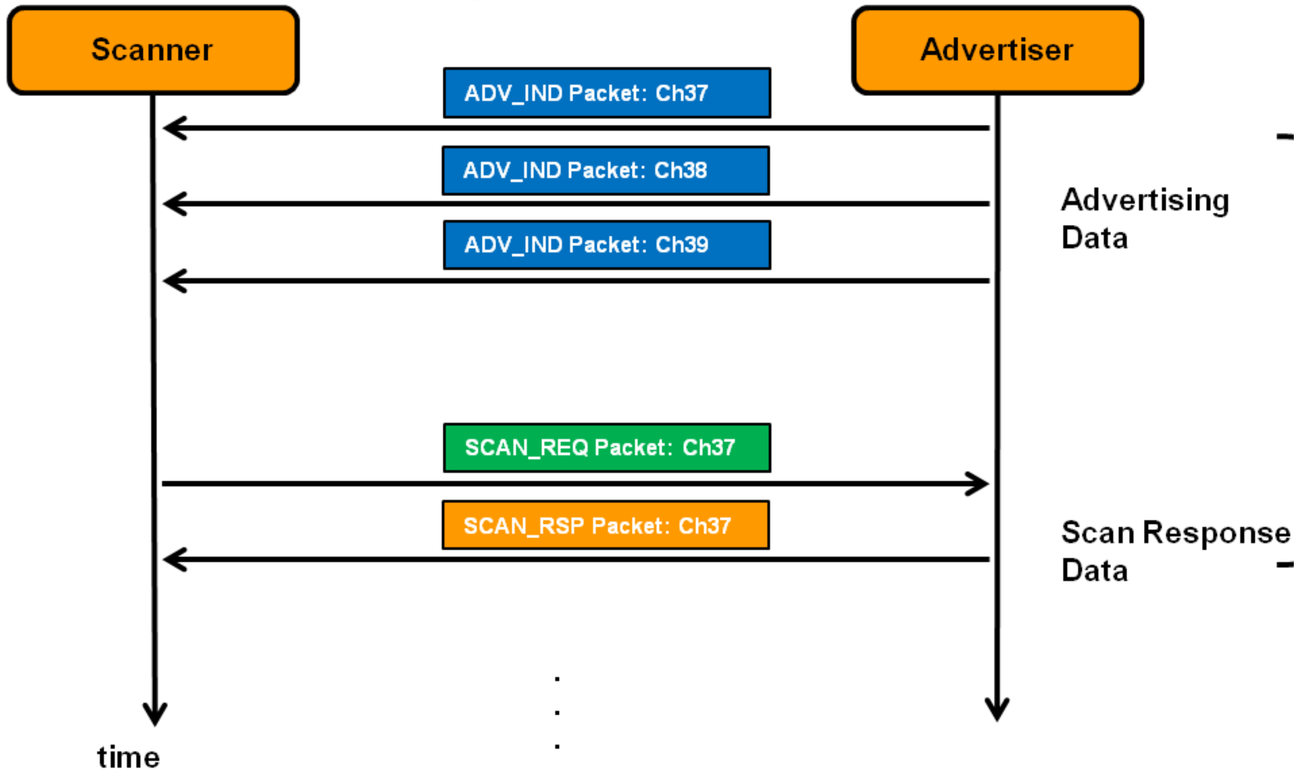
```
For bdaddr = 00:cc:3f:93:8f:ce:
        Company Name by IEEE OUI (00:cc:3f): Universal Electronics, Inc.
                BDADDR is Bluetooth Low Energy Public

        No BTC Extended Inquiry Result Device info.

        DeviceName: Daikin
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 19 which corresponds to (New wireshark) Connectable, Scannable
        DeviceName: Sala
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response

        No UUID16s found.

        No Service Solicit UUID16s found.

        No UUID128s found.

        No Service Solicit UUID128s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x0093 (Universal Electronics, 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): 0x9300 (No Match)
                Raw Data: e000
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
                        This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response
```

Background

Passive Scanning



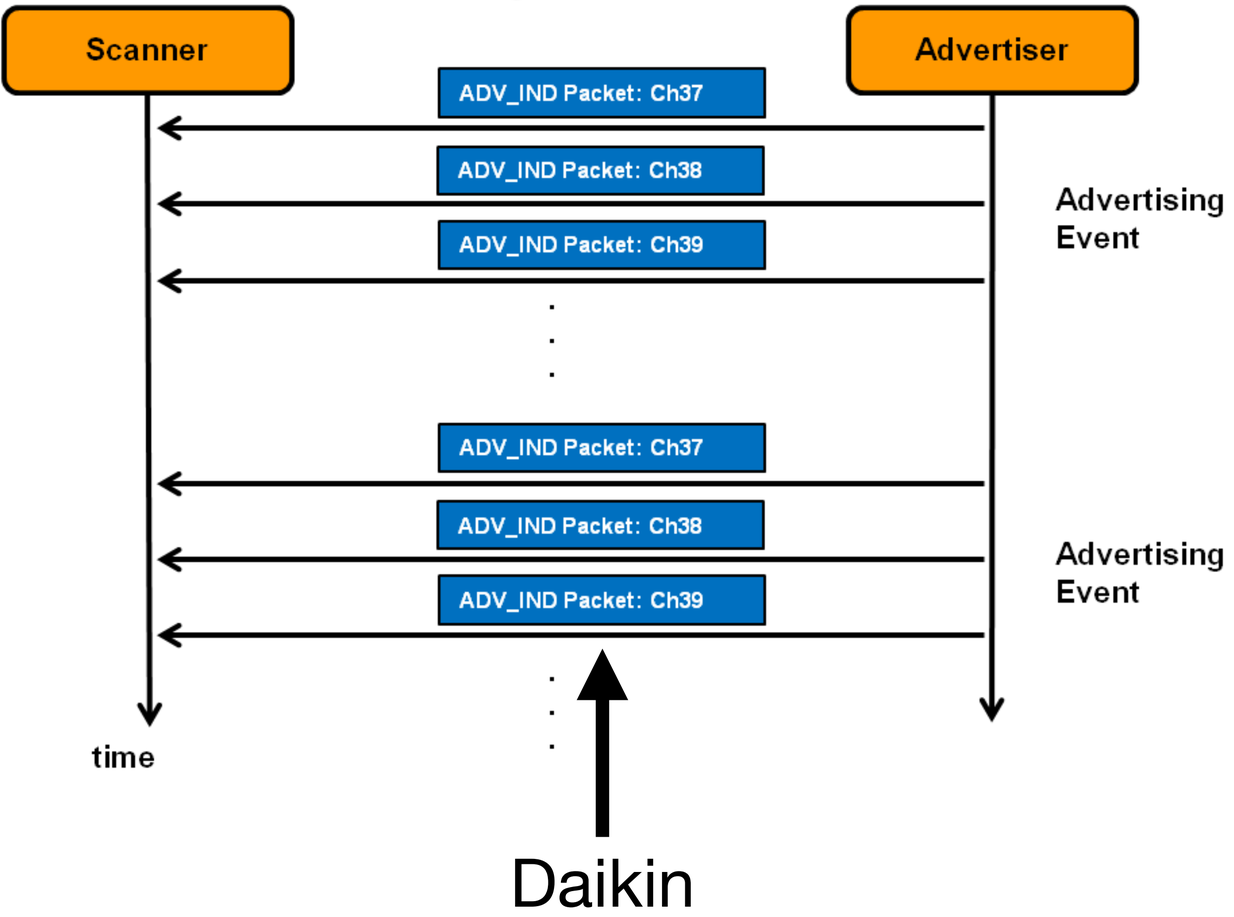
Active Scanning



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

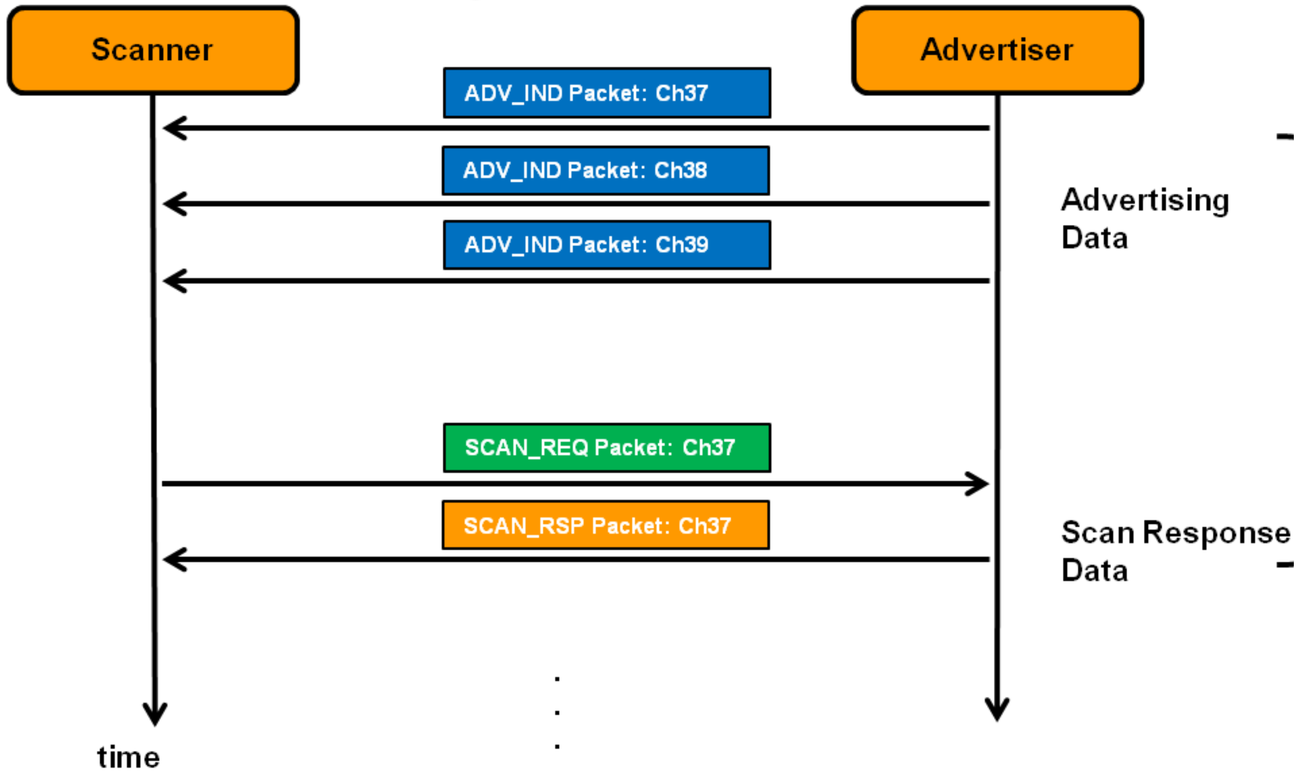
Background

Passive Scanning



Daikin

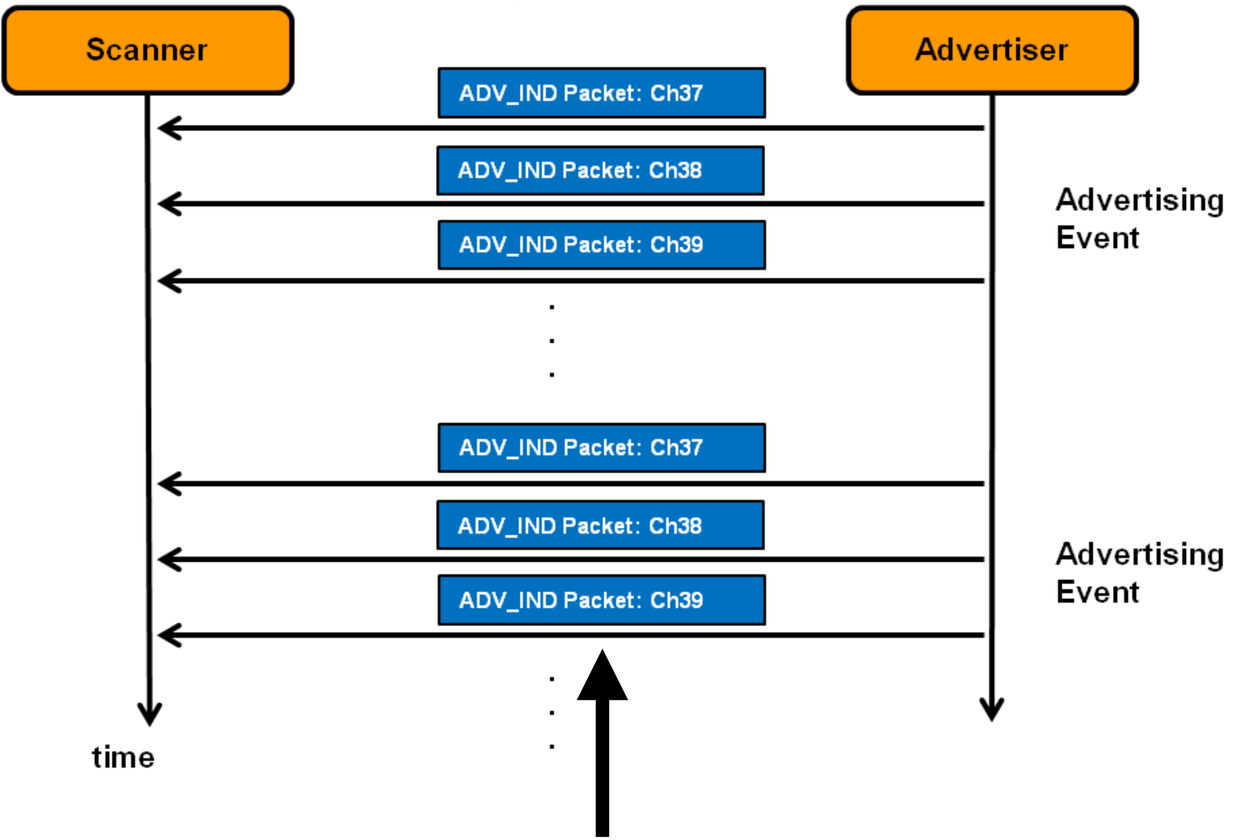
Active Scanning



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

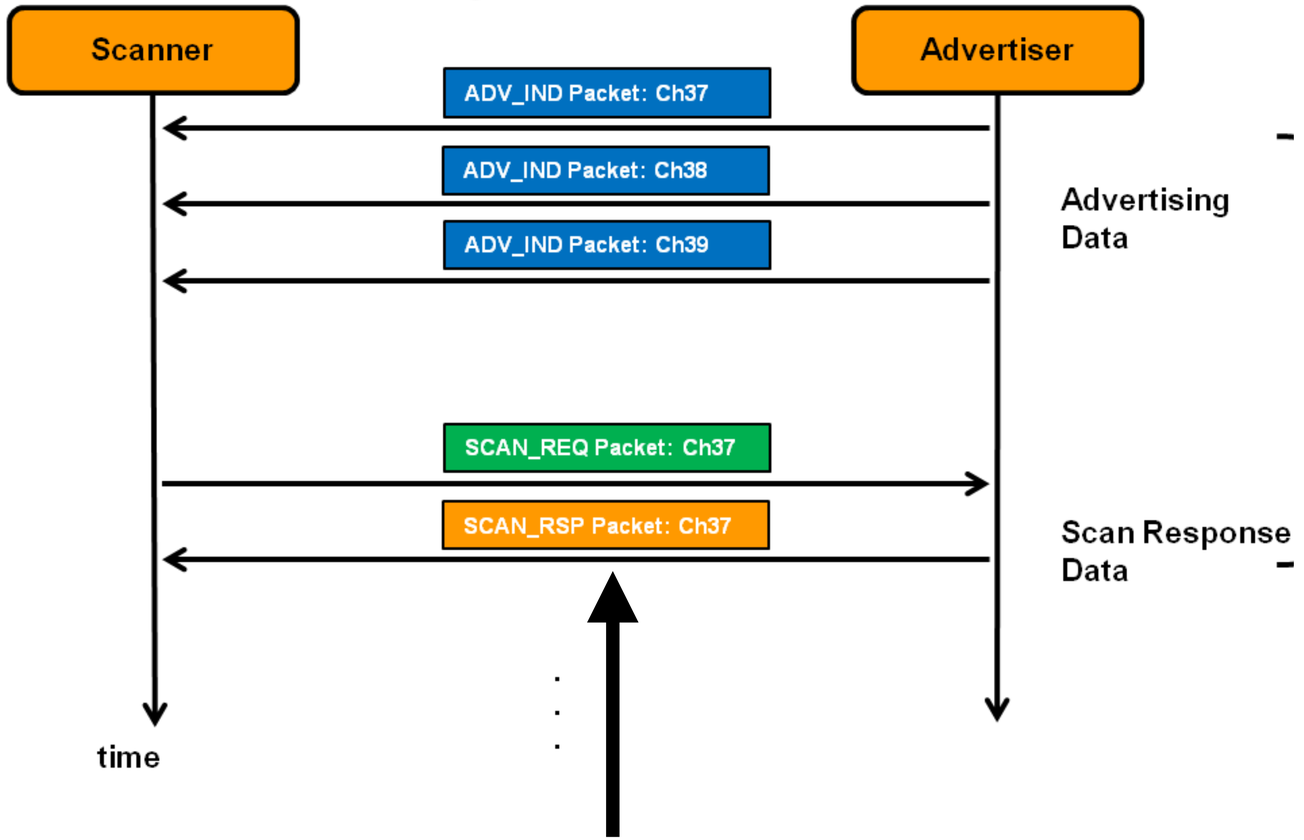
Background

Passive Scanning



Daikin

Active Scanning



Customer-customized name (?)

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

~~Italy~~ Europe - Daikin

```
For bdaddr = 00:cc:3f:93:8f:ce:
        Company Name by IEEE OUI (00:cc:3f): Universal Electronics, Inc.
                BDADDR is Bluetooth Low Energy Public

        No BTC Extended Inquiry Result Device info.

        DeviceName: Daikin
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 19 which corresponds to (New wireshark) Connectable, Scannable
        DeviceName: Sala
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response

        No UUID16s found.

        No Service Solicit UUID16s found.

        No UUID128s found.

        No Service Solicit UUID128s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x0093 (Universal Electronics, 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): 0x9300 (No Match)
                Raw Data: e000
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
                        This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response
```

~~Italy~~ Europe - Daikin

```
For bdaddr = 00:cc:3f:93:8f:ce:
        Company Name by IEEE OUI (00:cc:3f): Universal Electronics, Inc.
                BDADDR is Bluetooth Low Energy Public

        No BTC Extended Inquiry Result Device info.

        DeviceName: Daikin
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable

        DeviceName: Sala
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response

        No UUID16s found.

        No Service Solicit UUID16s found.

        No UUID128s found.

        No Service Solicit UUID128s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x0093 (Universal Electronics, 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): 0x9300 (No Match)
                Raw Data: e000
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
                        This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response
```

DeviceName: Daikin
In BT LE Da bdaddr_random = 0 (Public)
This was fo 19 which corresponds to (New wireshark) Connectable, Scannable
DeviceName: Cucina

~~Italy~~ Europe - Daikin

```
For bdaddr = 00:cc:3f:93:8f:ce:
        Company Name by IEEE OUI (00:cc:3f): Universal Electronics, Inc.
                BDADDR is Bluetooth Low Energy Public

        No BTC Extended Inquiry Result Device info.

        DeviceName: Daikin
                In BT LE Data
                This was found                                  wireshark) Connectable, Scannable
        DeviceName: Sala
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response

        No UUID16s found.

        No Service Solicit UUID16s found.

        No UUID128s found.

        No Service Solicit UUID128s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x0093 (Universal Electronics, 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): 0x9300 (No Match)
                Raw Data: e000
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
                        This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response
```

```
DeviceName: Daikin
        In BT LE Da
        This was fo
DeviceName: Cucina
```

```
DeviceName: Daikin
        In BT LE Data
        This was found
DeviceName: Ricircolo
```

~~Italy~~ Europe - Daikin

```
For bdaddr = 00:cc:3f:93:8f:ce:
        Company Name by IEEE OUI (00:cc:3f): Universal Electronics, Inc.
                BDADDR is Bluetooth Low Energy Public

        No BTC Extended Inquiry Result Device info.

        DeviceName: Daikin
                In BT LE Data
                This was found
        DeviceName: Sala
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response

        For bdaddr = 1c:41:90:50:31:18:
                Company Name by IEEE OUI (1
                        BDADDR is Bluetooth

                No BTC Extended Inquiry Res

                DeviceName: Daikin
                        In BT LE Data (LE_b
                        This was found in a
                DeviceName: BRC1H 50:31:18

        Manufacturer-specific Data:
                Device Company ID: 0x0093 (Universal Electronics, 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): 0x9300 (No Match)
                Raw Data: e000
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
                        This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response
```

```
DeviceName: Daikin
        In BT LE Data
        This was found
DeviceName: Cucina
```

```
DeviceName: Daikin
        In BT LE Data
        This was found
DeviceName: Ricircolo
```

~~Italy~~ Europe - Daikin

```
For bdaddr = 00:cc:3f:93:8f:ce:
        Company Name by IEEE OUI (00:cc:3f): Universal Electronics, Inc.
                BDADDR is Bluetooth Low Energy Public

        No BTC Extended Inquiry Result Device info.

        DeviceName: Daikin
                In BT LE Data
                This was found
        DeviceName: Sala
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response

        For bdaddr = 1c:41:90:50:31:18:
                Company Name by IEEE OUI (1
                        BDADDR is Bluetooth

                No BTC Extended Inquiry Res

                DeviceName: Daikin
                        In BT LE Data (LE_b
                        This was found in a
                DeviceName: BRC1H 50:31:18

        DeviceName: Daikin
                In BT LE Data
                This was found
        DeviceName: Cucina

        DeviceName: Daikin
                In BT LE Data
                This was found
        DeviceName: Ricircolo

        For bdaddr = 00:cc:3f:a5:e4:91:
                Company Name by IEEE OUI (0
                        BDADDR is Bluetooth

                No BTC Extended Inquiry Res

                DeviceName: Daikin
                        In BT LE Data (LE_b
                        This was found in a
                DeviceName: BRC1H A5:E4:91

        Manufacturer-specific Data:
                Device Company ID: 0x0093 (Universal Electronics, 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): 0x9300 (No Match)
                Raw Data: e000
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
                        This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response
```

~~Italy~~ Europe - Daikin

```
For bdaddr = 00:cc:3f:93:8f:ce:
        Company Name by IEEE OUI (00:cc:3f): Universal Electronics, Inc.
                BDADDR is Bluetooth Low Energy Public

        No BTC Extended Inquiry Result Device info.

        DeviceName: Daikin
                In BT LE Data
                This was found
        DeviceName: Sala
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response
```

```
DeviceName: Daikin
        In BT LE Da
        This was fo
DeviceName: Cucina
```

```
DeviceName: Daikin
        In BT LE Data
        This was found
DeviceName: Ricircolo
```

```
For bdaddr = 1c:41:90:50:31:18:
        Company Name by IEEE OUI (1
                BDADDR is Bluetooth

        No BTC Extended Inquiry Res

        DeviceName: Daikin
                In BT LE Data (LE_b
                This was found in a
        DeviceName: BRC1H 50:31:18
```

Telecomando a filo Madoka.

Madoka - BRC1H519W

> Un regolatore completamente riprogettato pensato per ottimizzare l'esperienza dell'utente

CERCA PUNTO VENDITA

```
        Manufacturer-specific Data:
                Device Company ID: 0x0093 (Universal Electronics, 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): 0x9300 (No Match)
                Raw Data: e000
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
                        This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response
```

~~Italy~~ Europe - Daikin

```
For bdaddr = 00:cc:3f:93:8f:ce:
        Company Name by IEEE OUI (00:cc:3f): Universal Electronics, Inc.
                BDADDR is Bluetooth Low Energy Public

        No BTC Extended Inquiry Result Device info.

        DeviceName: Daikin
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 19 which corresponds to (New wireshark) Connectable, Scannable
        DeviceName: Sala
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response

        No UUID16s found.

        No Service Solicit UUID16s found.

        No UUID128s found.

        No Service Solicit UUID128s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x0093 (Universal Electronics, 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): 0x9300 (No Match)
                Raw Data: e000
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
                        This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response
```

~~Italy~~ Europe - Daikin

```
For bdaddr = 00:cc:3f:93:8f:ce:
        Company Name by IEEE OUI (00:cc:3f): Universal Electronics, Inc.
                BDADDR is Bluetooth Low Energy Public

        No BTC Extended Inquiry Result Device info.

        DeviceName: Daikin
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 19 which corresponds to (New wireshark) Connectable, Scannable
        DeviceName: Sala
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response

        No UUID16s found.

        No Service Solicit UUID16s found.

        No UUID128s found.

        No Service Solicit UUID128s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x0093 (Universal Electronics, 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): 0x9300 (No Match)
                Raw Data: e000
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
                        This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response
```

~~Italy~~ Europe - Daikin

```
For bdaddr = 00:cc:3f:93:8f:ce:
        Company Name by IEEE OUI (00:cc:3f): Universal Electronics, Inc.
                BDADDR is Bluetooth Low Energy Public

        No BTC Extended Inquiry Result Device info.

        DeviceName: Daikin
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 19 which corresponds to (New wireshark) Connectable, Scannable
        DeviceName: Sala
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response

        No UUID16s found.

        No Service Solicit UUID16s found.

        No UUID128s found.

        No Service Solicit UUID128s found.

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x0093 (Universal Electronics, 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): 0x9300 (No Match)
                Raw Data: e000
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
                        This was found in an event of type 27 which corresponds to (New wireshark) Connectable, Scannable, Scan Response
```

About Universal Electronics

Universal Electronics Inc. (NASDAQ:UEIC),, the global leader in wireless universal control solutions for home entertainment and smart home devices; designs, develops, manufactures, ships and supports hardware and software control and sensor technology solutions. UEI partners with many Fortune 500 customers, including Comcast, Vivint Smart Home, Samsung, LG, Sony, and Daikin to serve video, telecommunications, security service providers, television, smart home, and HVAC system manufacturers. For over 35 years, UEI has been pioneering breakthrough innovations such as voice control and QuickSet cloud, the world's leading platform for automated set-up and control of devices in the home. For more information visit www.uei.com

About Universal Electronics

Universal Electronics Inc. (NASDAQ:UEIC),, the global leader in wireless universal control solutions for home entertainment and smart home devices; designs, develops, manufactures, ships and supports hardware and software control and sensor technology solutions. UEI partners with many Fortune 500 customers, including Comcast, Vivint Smart Home, Samsung, LG, Sony, and Daikin to serve video, telecommunications, security service providers, television, smart home, and HVAC system manufacturers. For over 35 years, UEI has been pioneering breakthrough innovations such as voice control and QuickSet cloud, the world's leading platform for automated set-up and control of devices in the home. For more information visit www.uei.com

https://www.uei.com/news/universal-electronics-announces-four-new-matter-enhanced-solutions-at-ces-2023

Home automation and security thermostats

Our range of thermostat platforms are compatible with different protocols, including Zigbee 3.0, Z-Wave and BLE 4.2, and can be integrated with existing security system panels or hubs. Used with our low-power silicon module designed for HVAC control, we can lower costs while offering the best product for your customers.

existing ecosystems. In addition to its UE61 module, UEI will introduce an extension of its line-up, with UE51, a bare metal Wi-Fi and Bluetooth LE connectivity module. With secure and scalable QuickSet® Cloud support, they can be easily integrated into standard home appliances to make them smart-enabled, connected devices.

https://www.uei.com/news/universal-electronics-announces-four-new-matter-enhanced-solutions-at-ces-2023

GATT Info

```
GATT Information:
        GATT Service: Begin Handle: 1   End Handle: 7          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 Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 4
                GATT Descriptor: 00002a01-0000-1000-8000-00805f9b34fb, Descriptor Handle: 5
                GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 6
                GATT Descriptor: 00002aa6-0000-1000-8000-00805f9b34fb, Descriptor Handle: 7
        GATT Service: Begin Handle: 16  End Handle: 19          UUID128: 00001801-0000-1000-8000-00805f9b34fb (Generic Attribute)
                GATT Descriptor: 00002800-0000-1000-8000-00805f9b34fb, Descriptor Handle: 16
                GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 17
                GATT Descriptor: 00002a05-0000-1000-8000-00805f9b34fb, Descriptor Handle: 18
                GATT Descriptor: 00002902-0000-1000-8000-00805f9b34fb, Descriptor Handle: 19
        GATT Service: Begin Handle: 48  End Handle: 66          UUID128: 0000180a-0000-1000-8000-00805f9b34fb (Device Information
                GATT Descriptor: 00002800-0000-1000-8000-00805f9b34fb, Descriptor Handle: 48
                GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 49
                GATT Descriptor: 00002a29-0000-1000-8000-00805f9b34fb, Descriptor Handle: 50
                GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 51
                GATT Descriptor: 00002a23-0000-1000-8000-00805f9b34fb, Descriptor Handle: 52
                GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 53
                GATT Descriptor: 00002a24-0000-1000-8000-00805f9b34fb, Descriptor Handle: 54
                GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 55
                GATT Descriptor: 00002a25-0000-1000-8000-00805f9b34fb, Descriptor Handle: 56
                GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 57
                GATT Descriptor: 00002a26-0000-1000-8000-00805f9b34fb, Descriptor Handle: 58
                GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 59
                GATT Descriptor: 00002a27-0000-1000-8000-00805f9b34fb, Descriptor Handle: 60
                GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 61
        GATT Service: Begin Handle: 256 End Handle: 264         UUID128: 2141e100-213a-11e6-b67b-9e71128cae77 (Unknown UUID128)
        GATT Service: Begin Handle: 512 End Handle: 65535       UUID128: 2141e110-213a-11e6-b67b-9e71128cae77 (Unknown UUID128)
```

GATT Info

```
GATT Information:
        GATT Service: Begin Handl                28: 00001800-0000-1000-8000-00805f9b34fb (Generic Access)
                GATT Descriptor:                 , Descriptor Handle: 1
                GATT Descriptor:                 , Descriptor Handle: 2
                GATT Descriptor:                 , Descriptor Handle: 3
                GATT Descriptor:                 , Descriptor Handle: 4
                GATT Descriptor:                 , Descriptor Handle: 5
                GATT Descriptor:                 , Descriptor Handle: 6
                GATT Descriptor:                 , Descriptor Handle: 7
        GATT Service: Begin Handl                28: 00001801-0000-1000-8000-00805f9b34fb (Generic Attribute)
                GATT Descriptor:                 , Descriptor Handle: 16
                GATT Descriptor:                 , Descriptor Handle: 17
                GATT Descriptor:                 , Descriptor Handle: 18
                GATT Descriptor:                 , Descriptor Handle: 19
        GATT Service: Begin Handl                28: 0000180a-0000-1000-8000-00805f9b34fb (Device Information
                GATT Descriptor:                 , Descriptor Handle: 48
                GATT Descriptor:                 , Descriptor Handle: 49
                GATT Descriptor:                 , Descriptor Handle: 50
                GATT Descriptor:                 , Descriptor Handle: 51
                GATT Descriptor:                 , Descriptor Handle: 52
                GATT Descriptor:                 , Descriptor Handle: 53
                GATT Descriptor:                 , Descriptor Handle: 54
                GATT Descriptor:                 , Descriptor Handle: 55
                GATT Descriptor:                 , Descriptor Handle: 56
                GATT Descriptor:                 , Descriptor Handle: 57
                GATT Descriptor:                 , Descriptor Handle: 58
                GATT Descriptor:                 , Descriptor Handle: 59
                GATT Descriptor:                 , Descriptor Handle: 60
                GATT Descriptor:                 , Descriptor Handle: 61
        GATT Service: Begin Handl                28: 2141e100-213a-11e6-b67b-9e71128cae77 (Unknown UUID128)
        GATT Service: Begin Handl                28: 2141e110-213a-11e6-b67b-9e71128cae77 (Unknown UUID128)
```

5:05 4G

74 of 182

Daikin

Ericsson Technology Licensing

E3E61245-477C-CB4B-E2AC-F7EE48A784B8

SIGNAL	CONNECTION
16%	Interrogating

SERVICES

3

ADVERTISEMENT DATA

17:05:36 Timestamp

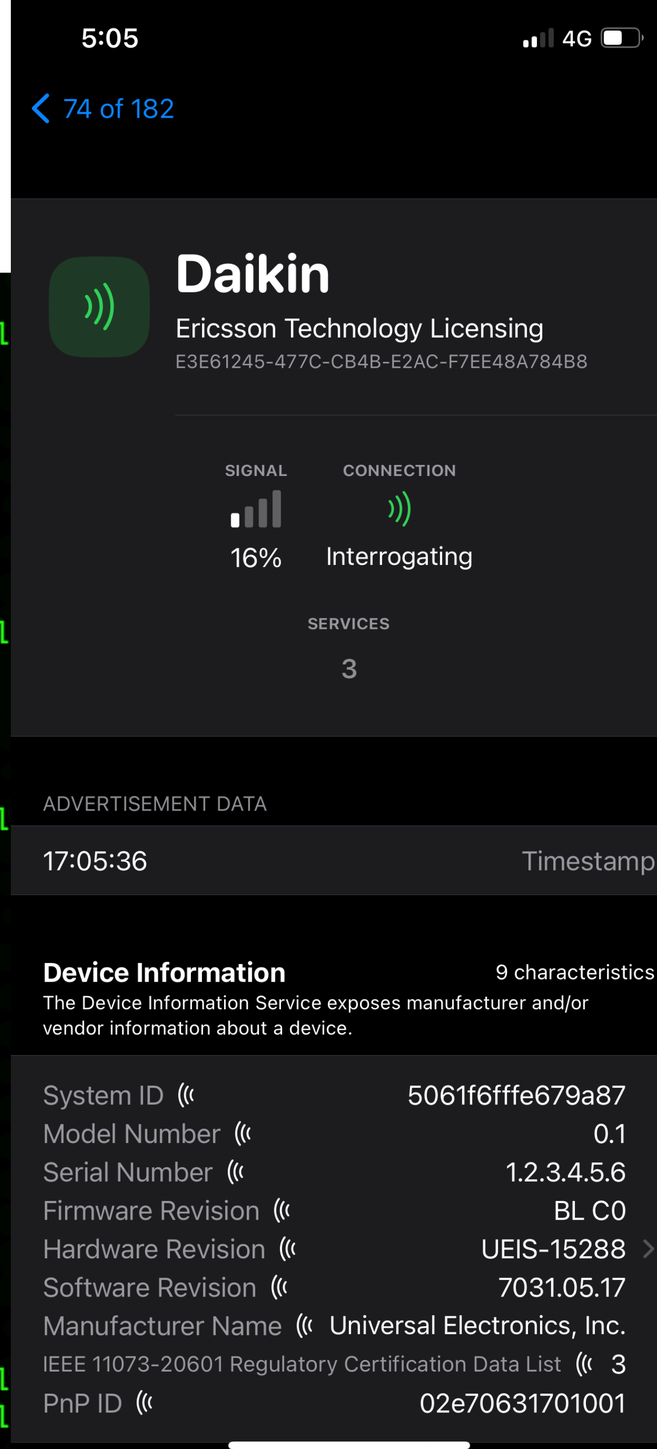
Device Information 9 characteristics

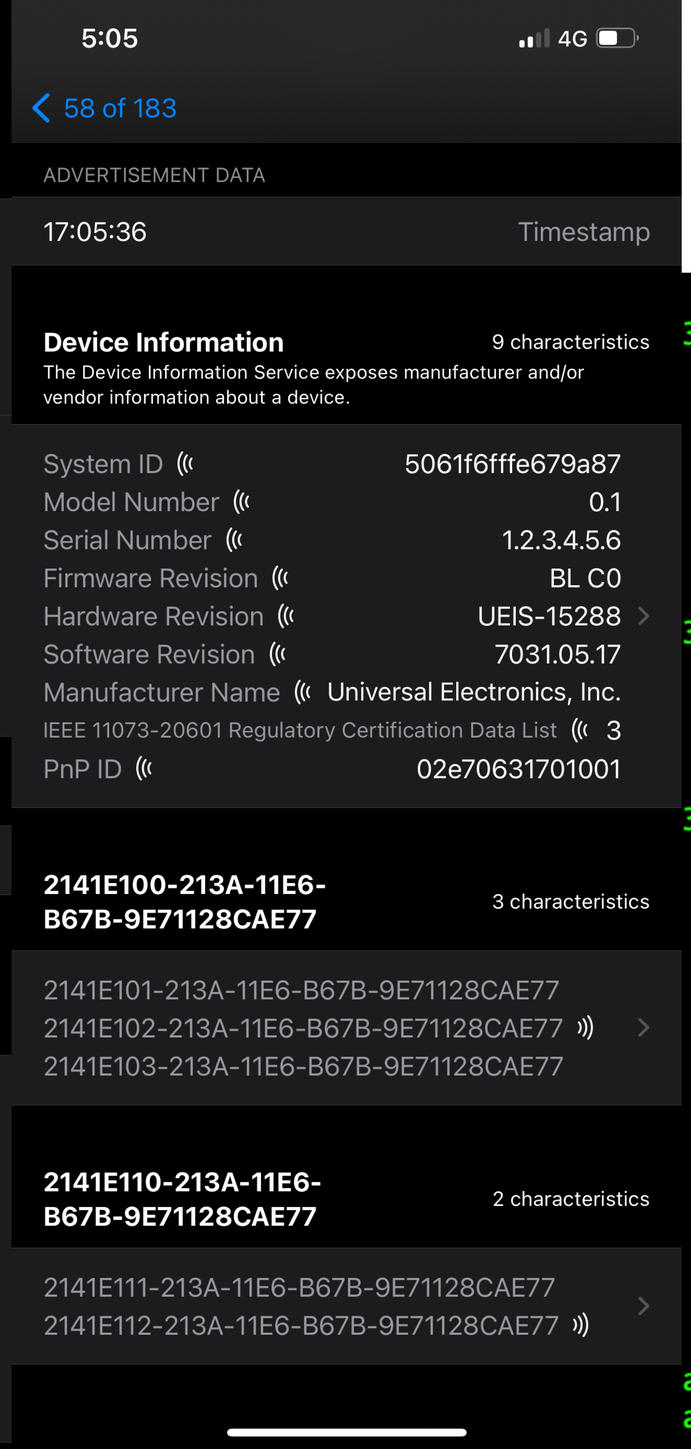
The Device Information Service exposes manufacturer and/or vendor information about a device.

System ID	5061f6fffe679a87
Model Number	0.1
Serial Number	1.2.3.4.5.6
Firmware Revision	BL C0
Hardware Revision	UEIS-15288
Software Revision	7031.05.17
Manufacturer Name	Universal Electronics, Inc.
IEEE 11073-20601 Regulatory Certification Data List	3
PnP ID	02e70631701001

GATT Info

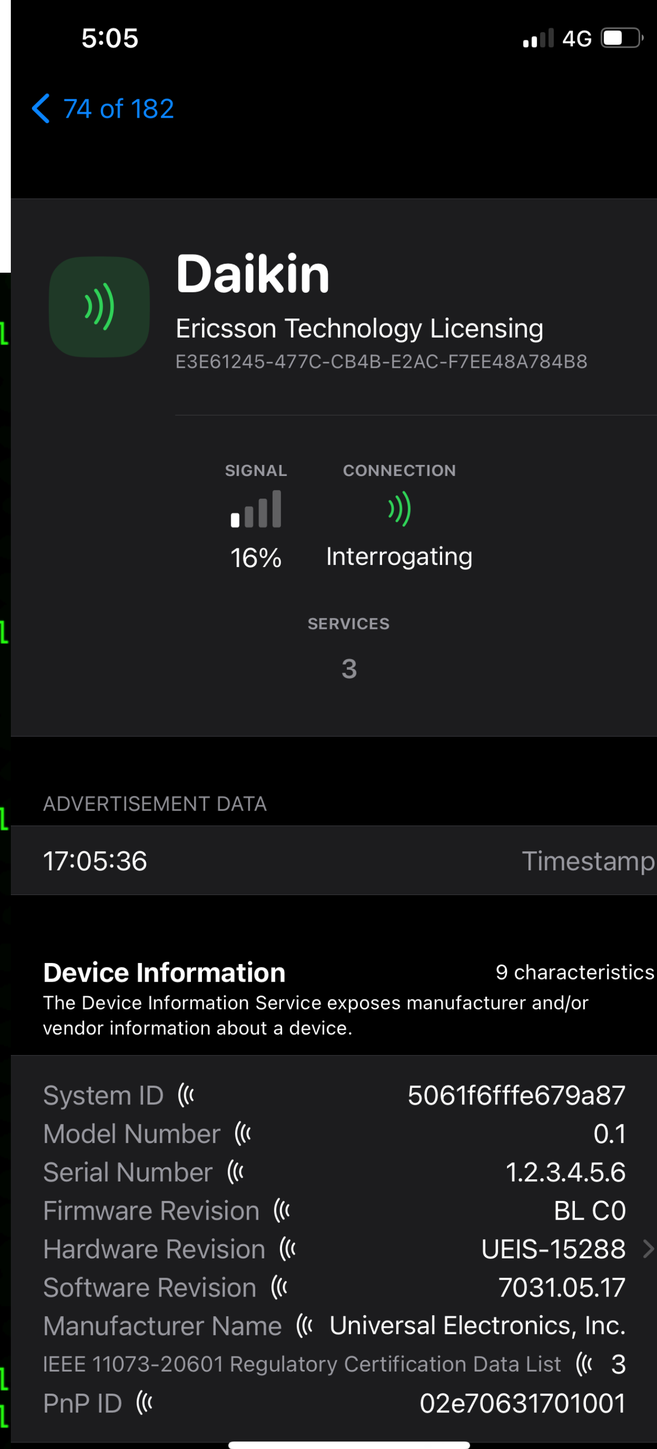
```
GATT Information:
        GATT Service: Begin Handl                                    34fb (Generic Access)
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
        GATT Service: Begin Handl                                    34fb (Generic Attribute)
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
        GATT Service: Begin Handl                                    34fb (Device Information
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
        GATT Service: Begin Handl                                    ae77 (Unknown UUID128)
        GATT Service: Begin Handl                                    ae77 (Unknown UUID128)
```

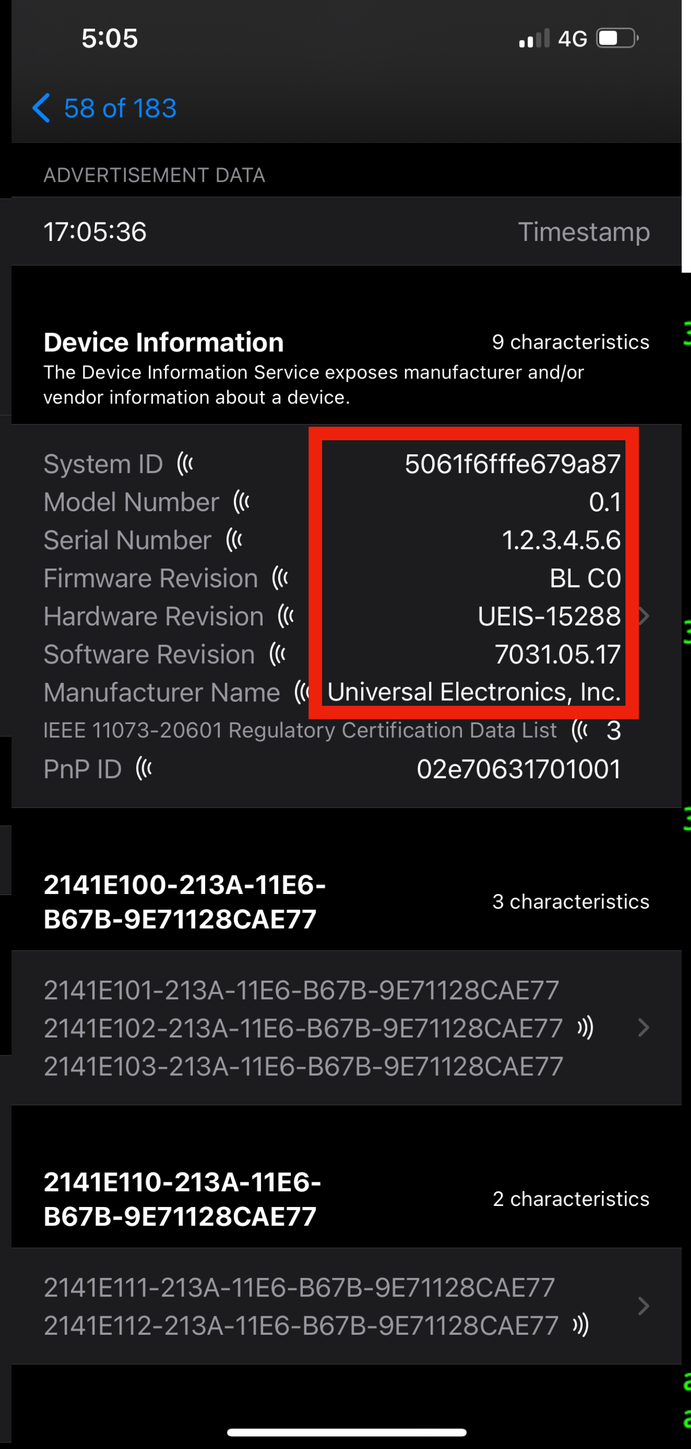




GATT Info

```
GATT Information:
        GATT Service: Begin Handl                                    34fb (Generic Access)
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
        GATT Service: Begin Handl                                    34fb (Generic Attribute)
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
        GATT Service: Begin Handl                                    34fb (Device Information)
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
                GATT Descriptor:
        GATT Service: Begin Handl                                    ae77 (Unknown UUID128)
        GATT Service: Begin Handl                                    ae77 (Unknown UUID128)
```

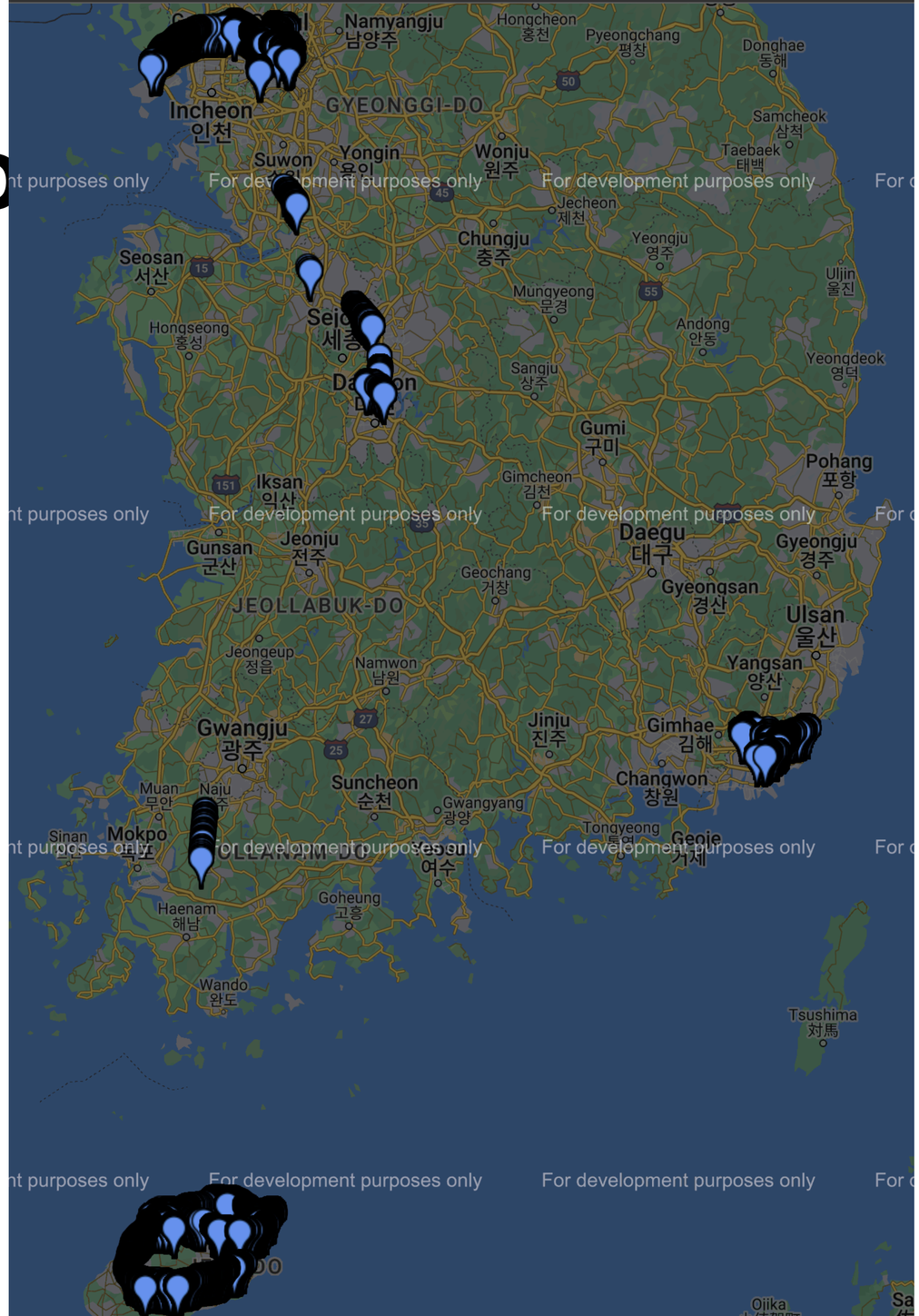




South Korea - All

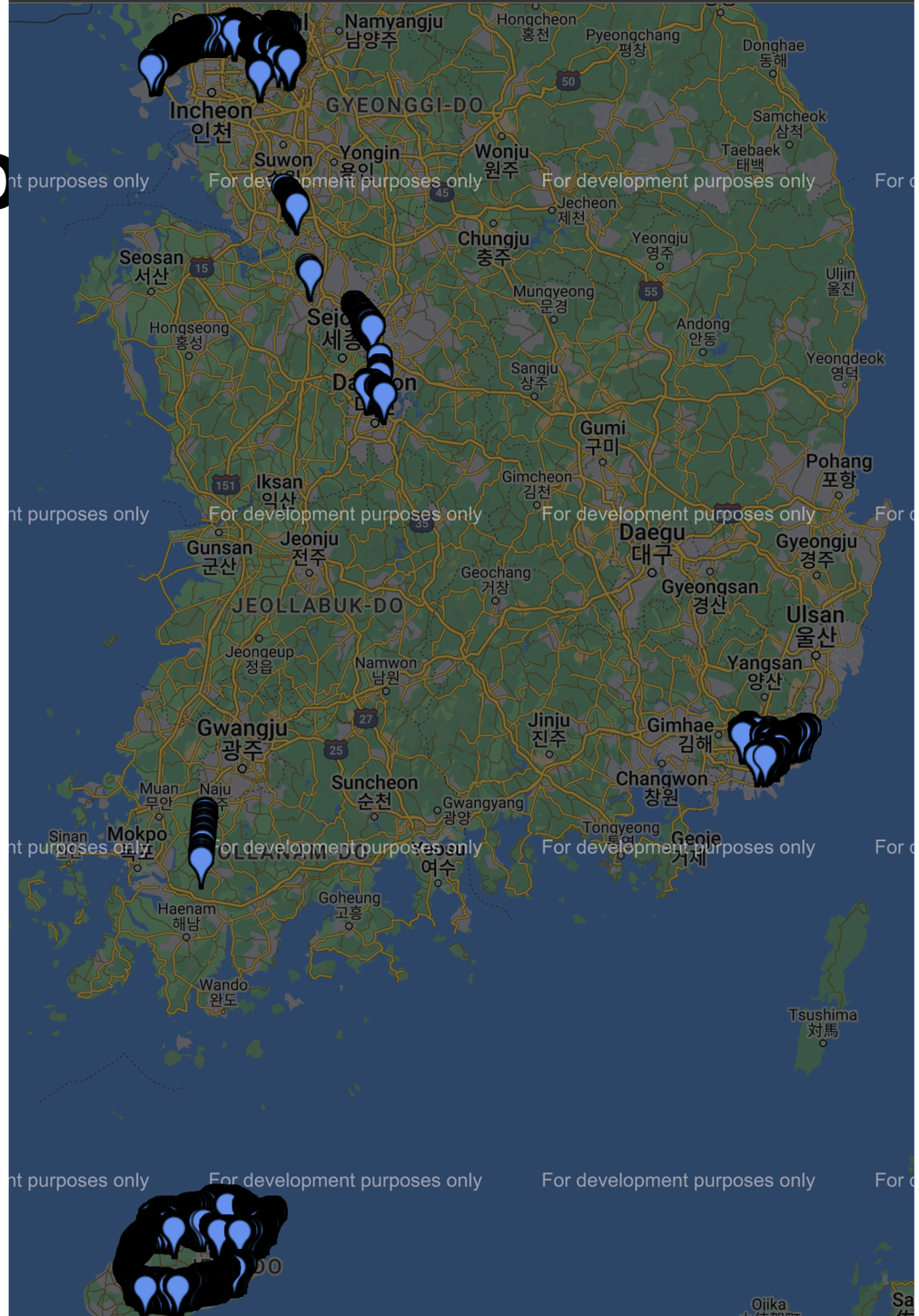
DARK MENTOR

So


Namyangju
남양주
Hongcheon
홍천
Pyeongchang
평창
Donghae
동해
Incheon
인천
GYEONGGI-DO
Samcheok
삼척
Taebaek
태백
Suwon
Yongin
용인
Wonju
원주
Jecheon
제천
Chungju
충주
Yeongju
영주
Seosan
서산
Uljin
울진
Mungyeong
문경
Hongseong
홍성
Andong
안동
Yeongdeok
영덕
Sangju
상주
Gumi
구미
Pohang
포항
Iksan
익산
Gimcheon
김천
Gunsan
군산
Jeonju
전주
Daegu
대구
Gyeongju
경주
Geochang
거창
Gyeongsan
경산
JEOLLABUK-DO
Ulsan
울산
Jeongeup
정읍
Namwon
남원
Yangsan
양산
Gwangju
광주
Jinju
진주
Gimhae
김해
Changwon
창원
Muan
무안
Naju
Suncheon
순천
Gwangyang
광양
Sinan
Mokpo
목포
Tongyeong
Geoje
거제
Yeosu
여수
Goheung
고흥
Haenam
해남
Wando
완도
Tsushima
対馬
Ojika

DARK MENTOR

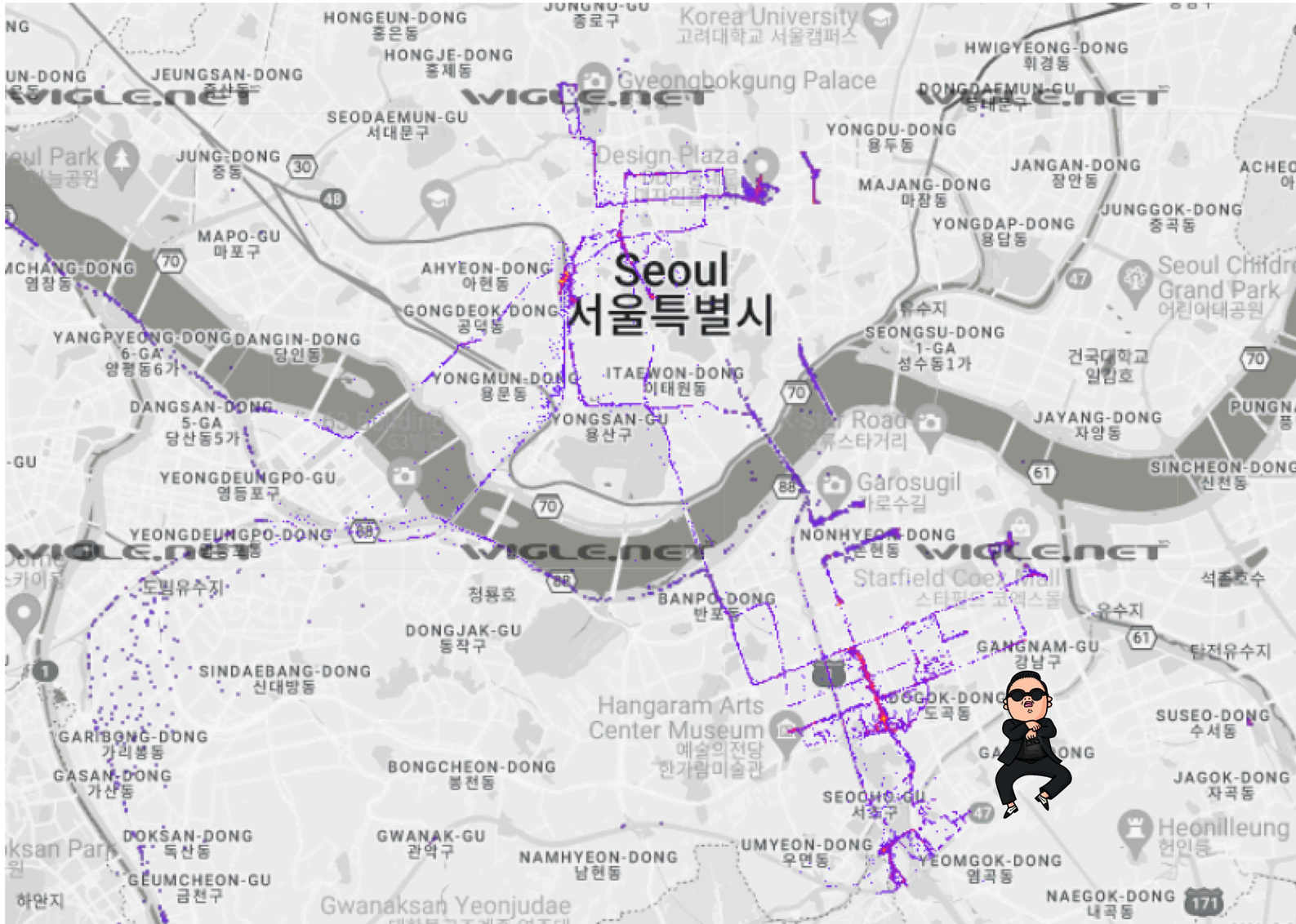
So


Namyangju
남양주
Hongcheon
홍천
Pyeongchang
평창
Donghae
동해
Incheon
인천
GYEONGGI-DO
Samcheok
삼척
Taebaek
태백
Suwon
Yongin
용인
Wonju
원주
Jecheon
제천
Chungju
충주
Yeongju
영주
Seosan
서산
Uljin
울진
Mungyeong
문경
Hongseong
홍성
Andong
안동
Yeongdeok
영덕
Sangju
상주
Gumi
구미
Pohang
포항
Iksan
익산
Gimcheon
김천
Gunsan
군산
Jeonju
전주
Daegu
대구
Gyeongju
경주
Geochang
거창
Gyeongsan
경산
JEOLLABUK-DO
Ulsan
울산
Jeongeup
정읍
Namwon
남원
Yangsan
양산
Gwangju
광주
Jinju
진주
Gimhae
김해
Changwon
창원
Muan
무안
Naju
Suncheon
순천
Gwangyang
광양
Sinan
Mokpo
목포
Tongyeong
통영
Geoje
거제
Yeosu
여수
Goheung
고흥
Haenam
해남
Wando
완도
Tsushima
対馬
Ojika
For development purposes only

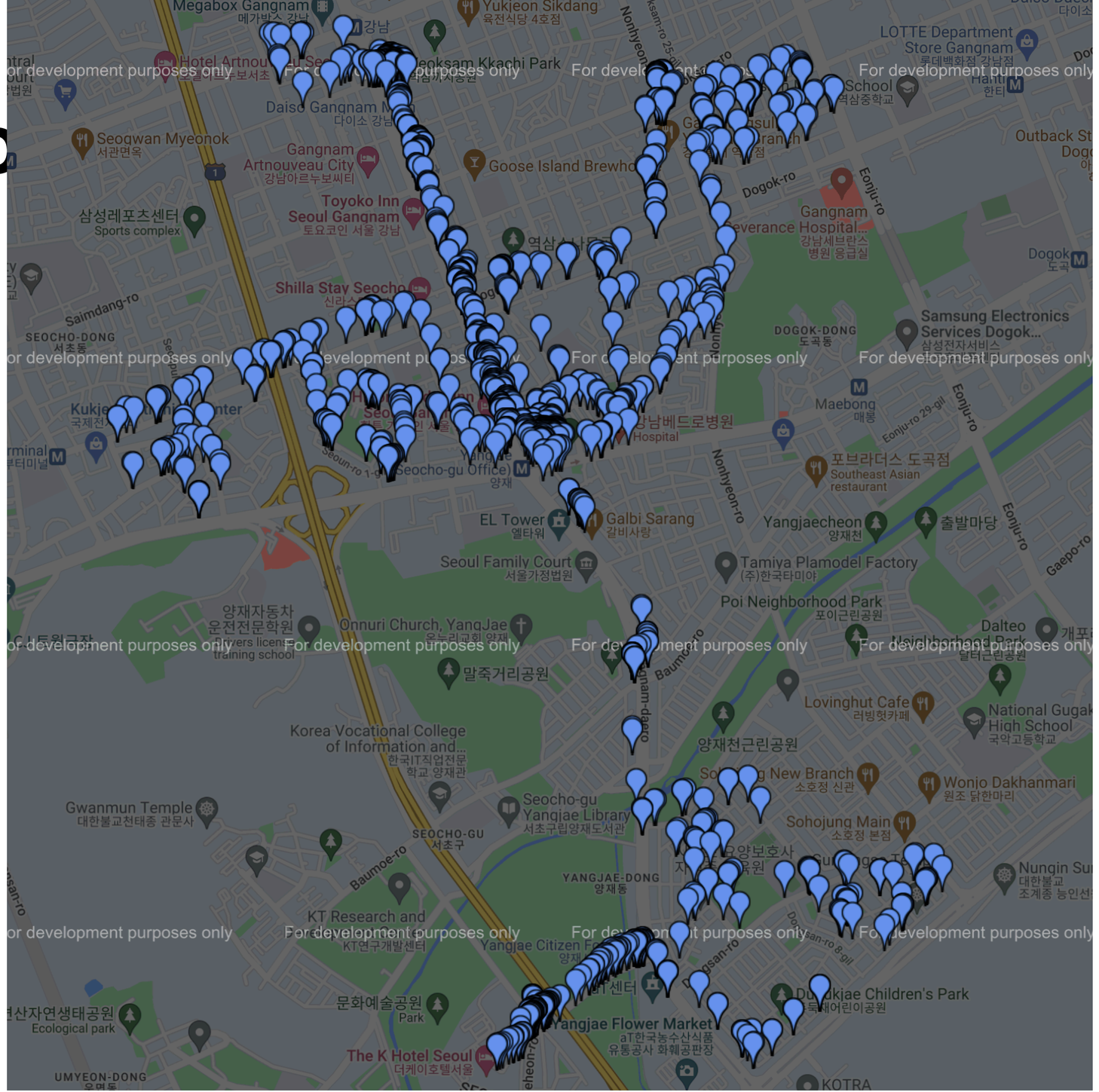
Seoul
서울
GANGWON-DO
Incheon
인천
GYEONGGI-DO
Donghae
동해
CHUNGCHEONGBUK-DO
CHUNGCHEONGNAM-DO
Daejeon
대전
Pohang
포항
Daegu
대구
Jeonju
전주
JEOLLABUK-DO
GYEONGSANGNAM-DO
Gwangju
광주
Changwon
창원
Busan
부산
JEOLLANAM-DO
JEJU-DO
Seogwipo
WIGLE.NET

South Korea - Seoul

- Yes, I ran around Gangnam with the sniffer...



South Ko

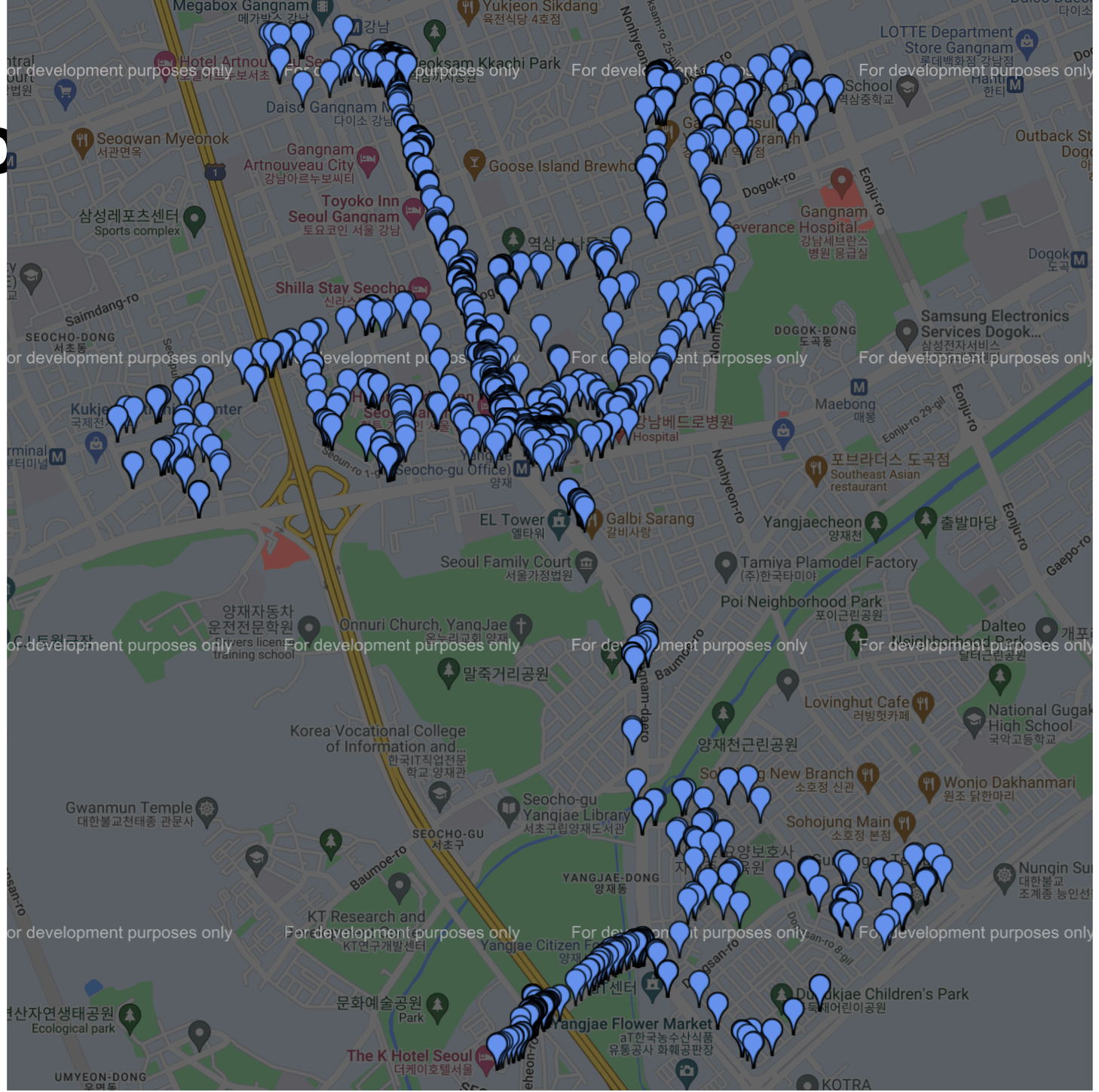


Megabox Gangnam
Yukjeon Sikdang
LOTTE Department Store Gangnam
Seogwan Myeonok
Gangnam Artnouveau City
Goose Island Brewho
Toyoko Inn Seoul Gangnam
삼성레포츠센터
Sports complex
Shilla Stay Seocho
Gangnam Severance Hospital
Samsung Electronics Services Dogok...
Maebong
포브라더스 도곡점
Southeast Asian restaurant
EL Tower
Galbi Sarang
Yangjaecheon
Seoul Family Court
Tamiya Plamodel Factory
Poi Neighborhood Park
Onnuri Church, YangJae
Dalteo
Lovinghut Cafe
National Gugak High School
Korea Vocational College of Information and...
Wonjo Dakhanmari
Gwanmun Temple
Seocho-gu Yangjae Library
Sohojung Main
KT Research and
Yangjae Citizen Fo
Yangjae Flower Market
The K Hotel Seoul
KOTRA
Saimdang-ro
SEOCHO-DONG
DOGOK-DONG
Dogok-ro
Eonju-ro
Nonhyeon-ro
Baumoe-ro
SEOCHO-GU
YANGJAE-DONG
UMYEON-DONG
For development purposes only

South Ko

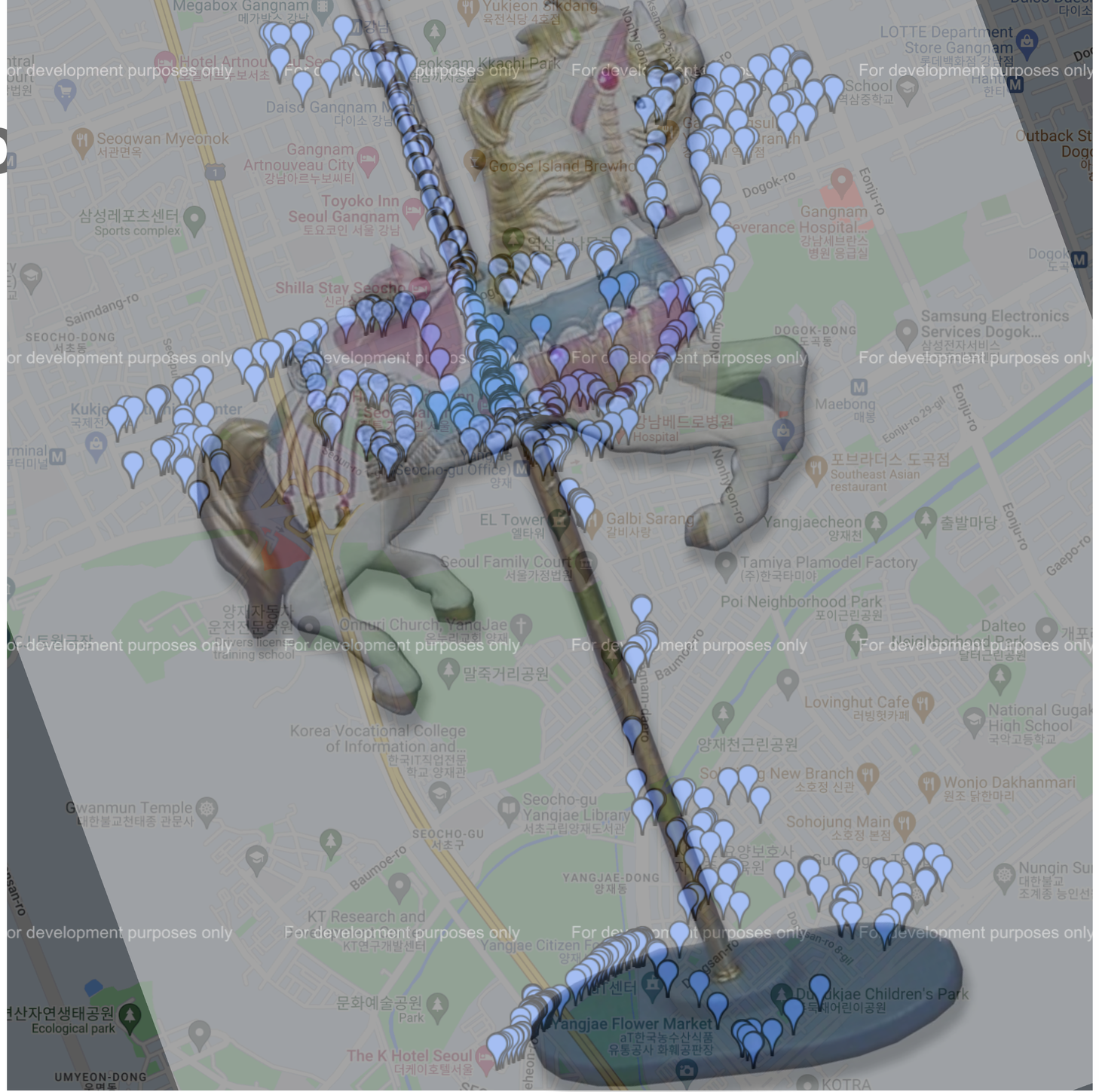
Megabox Gangnam
Yukjeon Sikdang
LOTTE Department Store Gangnam
Seogwan Myeonok
Gangnam Artnouveau City
Goose Island Brewho
Toyoko Inn Seoul Gangnam
Gangnam Severance Hospital
Shilla Stay Seocho
Samsung Electronics Services Dogok...
Maebong
Southeast Asian restaurant
EL Tower
Galbi Sarang
Yangjaecheon
Seoul Family Court
Tamiya Plamodel Factory
Poi Neighborhood Park
Onnuri Church, YangJae
Korea Vocational College of Information and...
Lovinghut Cafe
National Gugak High School
Wonjo Dakhanmari
Gwanmun Temple
Seocho-gu Yangjae Library
Sohojung Main
KT Research and
Yangjae Flower Market
The K Hotel Seoul
Ecological park
KOTRA
Dogok-ro
Eonju-ro
Nonhyeon-ro
Baumoe-ro
Gaepo-ro
Saimdang-ro
SEOCHO-DONG
DOGOK-DONG
SEOCHO-GU
YANGJAE-DONG
UMYEON-DONG

South Ko



Megabox Gangnam
Yukjeon Sikdang
LOTTE Department Store Gangnam
Seogwan Myeonok
Gangnam Artnouveau City
Goose Island Brewho
Toyoko Inn Seoul Gangnam
삼성레포츠센터
Sports complex
Shilla Stay Seocho
Gangnam Severance Hospital
Samsung Electronics Services Dogok...
Maebong
포브라더스 도곡점
Southeast Asian restaurant
EL Tower
Galbi Sarang
Yangjaecheon
Seoul Family Court
Tamiya Plamodel Factory
Poi Neighborhood Park
Onnuri Church, YangJae
Dalteo
Lovinghut Cafe
National Gugak High School
Korea Vocational College of Information and...
Wonjo Dakhanmari
Gwanmun Temple
Seocho-gu Yangjae Library
Sohojung Main
KT Research and
Yangjae Citizen Fo
Yangjae Flower Market
The K Hotel Seoul
KOTRA
Saimdang-ro
SEOCHO-DONG
DOGOK-DONG
Dogok-ro
Eonju-ro
Nonhyeon-ro
Baumoe-ro
SEOCHO-GU
YANGJAE-DONG
UMYEON-DONG
For development purposes only

South Ko



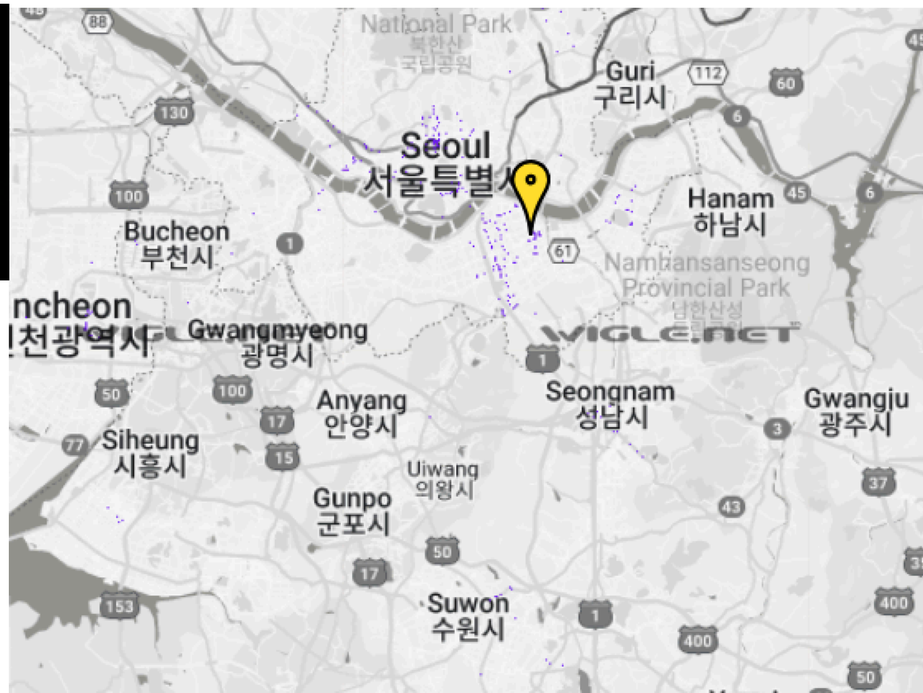
Megabox Gangnam
Yukjeon Sikdang
LOTTE Department Store Gangnam
Hotel Artnouveau
Seoksam Kkachi Park
Daiso Gangnam
Seogwan Myeonok
Gangnam Artnouveau City
Goose Island Brewhouse
Toyoko Inn Seoul Gangnam
삼성레포츠센터
Sports complex
Gangnam Severance Hospital
Shilla Stay Seocho
Saimdang-ro
SEOCHO-DONG
DOGOK-DONG
Samsung Electronics Services Dogok...
Maebong
Hospital
포브라더스 도곡점
Southeast Asian restaurant
EL Tower
Galbi Sarang
Yangjaecheon
출발마당
Seoul Family Court
Tamiya Plamodel Factory
Poi Neighborhood Park
Onnuri Church, YangJae
Dalteo
Lovinghut Cafe
National Gugak High School
Korea Vocational College of Information and...
양재천근린공원
Wonjo Dakhanmari
Gwanmun Temple
Seocho-gu Yangjae Library
Sohojung Main
SEOCHO-GU
YANGJAE-DONG
KT Research and
Yangjae Citizen Fo
Yangjae Flower Market
The K Hotel Seoul
Ecological park
UMYEON-DONG
KOTRA
For development purposes only

South Korea - Seoul

Scooters

- Regex: ^KICKGOING$
- Not just a country-specific, but city-specific devices!

```
Company Name by IEEE OUI (10:52:1c): Espressif Inc.

No BTC Extended Inquiry Result Device info.

DeviceName: KICKGOING
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
```

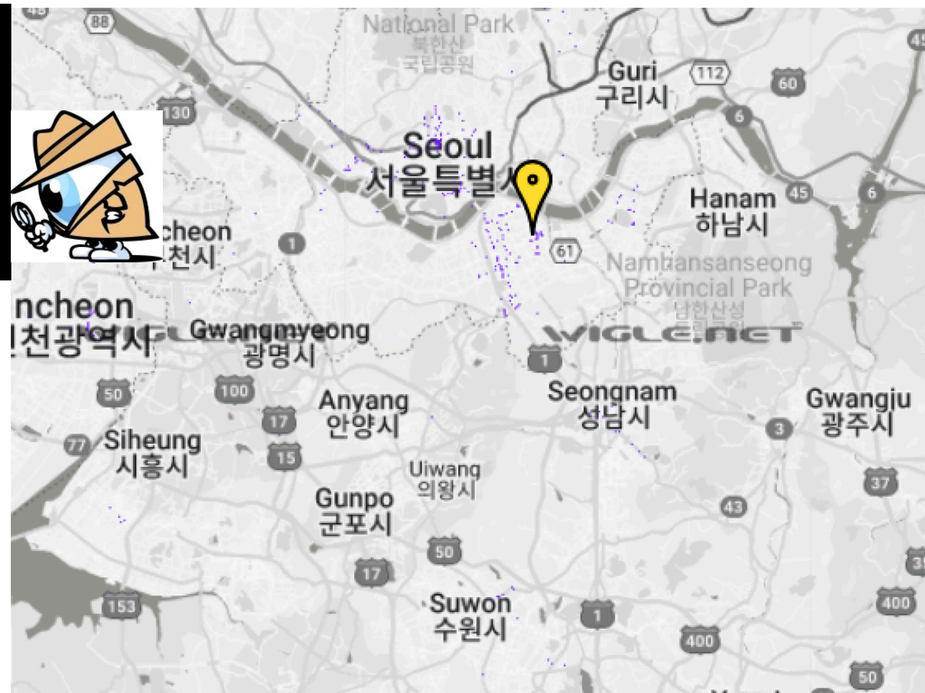


South Korea - Seoul

Scooters

- Regex: ^KICKGOING$
- Not just a country-specific, but city-specific devices!

```
Company Name by IEEE OUI (10:52:1c): Espressif Inc.

No BTC Extended Inquiry Result Device info.

DeviceName: KICKGOING
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
```

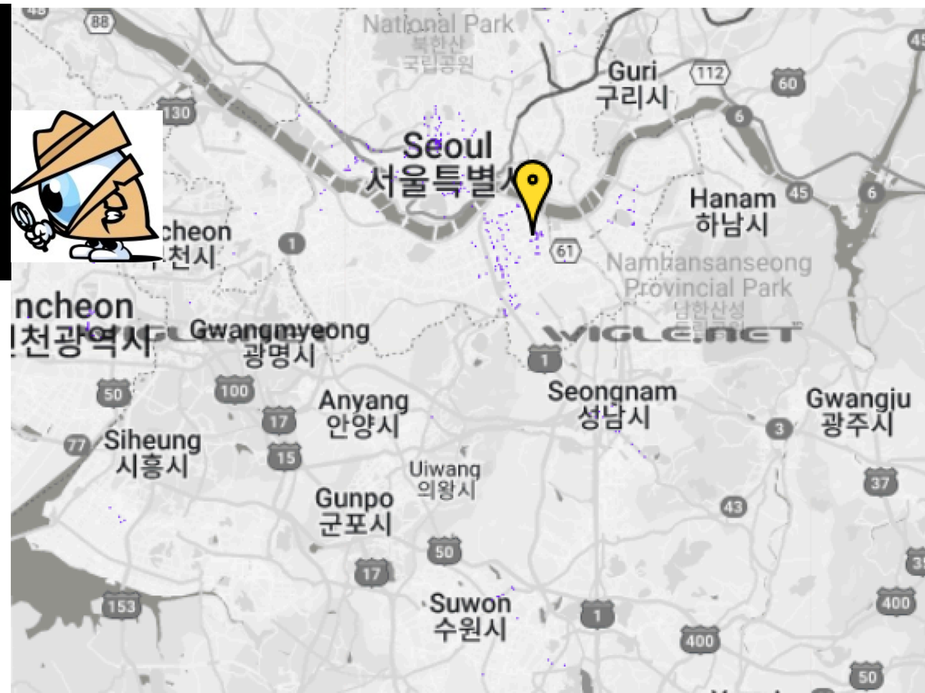


South Korea - Seoul

Scooters

- Regex: ^KICKGOING$
- Not just a country-specific, but city-specific devices!

```
Company Name by IEEE OUI (10:52:1c): Espressif Inc.

No BTC Extended Inquiry Result Device info.

DeviceName: KICKGOING
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
```



Mini-Takeaway

Chip identification

- *Sometimes* devices which are using BT Classic, or BLE *Public* BDADDRs have an OUI which is from a *chip-maker*
- This can give a pretty strong signal of which chip a device is using
  - And which chip a device is using, is one of the things I want to know!

MPEON

Toll-road payment system

- Regex: ^MPEON(| SMART LE)\\\([A-F0-9]{6}\\\)$
  - Semantically: Last 6 are from BDADDR
- Advertises a different name for BT Classic vs. BLE

```
For bdaddr = 00:19:01:71:ab:30:
        Company Name by IEEE OUI (00:19:01): F1MEDIA

        No BTC Extended Inquiry Result Device info.

        DeviceName: MPEON SMART BT(71AB30)
                In BT Classic Data (EIR_bdaddr_to_name)
        DeviceName: MPEON SMART LE(71AB30)
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 0 which corresponds to Con

        UUID16s found:
                UUID16 0x110a (Service ID: AudioSource)
```

https://mpeon.com/hipass

MPEON

Toll-road payment system

- Regex: ^MPEON(| SMART LE)\\\([A-F0-9]{6}\\\)$
  - Semantically: Last 6 are from BDADDR
- Advertises a different name for BT Classic vs. BLE

```
For bdaddr = 00:19:01:71:ab:30:
        Company Name by IEEE OUI (00:19:01): F1MEDIA

        No BTC Extended Inquiry Result Device info.

        DeviceName: MPEON SMART BT(71AB30)
                In BT Classic Data (EIR_bdaddr_to_name)
        DeviceName: MPEON SMART LE(71AB30)
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 0 which corresponds to Con

        UUID16s found:
                UUID16 0x110a (Service ID: AudioSource)
```

https://mpeon.com/hipass

MPEON

Toll-road payment system

- Regex: ^MPEON(| SMART LE)\\\([A-F0-9]{6}\\\)$
  - Semantically: Last 6 are from BDADDR
- Advertises a different name for BT Classic vs. BLE

```
For bdaddr = 00:19:01:71:ab:30:
        Company Name by IEEE OUI (00:19:01): F1MEDIA

        No BTC Extended Inquiry Result Device info.

        DeviceName: MPEON SMART BT(71AB30)
                In [illegible]addr_to_name)
        DeviceName: MPEON SMART LE(71AB30)
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 0 which corresponds to Con

        UUID16s found:
                UUID16 0x110a (Service ID: AudioSource)
```

https://mpeon.com/hipass

MPEON

Toll-road paym

- Regex: ^MPEOI
  - Semantically:
- Advertises a diff

```
For bdaddr = 00:19:01:71:ab:3
        Company Name by IEEE

        No BTC Extended Inqui

        DeviceName: MPEON SMA
                In BT Classic
        DeviceName: MPEON SMA
                In BT LE Data
                This was foun

        UUID16s found:
                UUID16 0x110a
```

SET-560

Rechargeable, horizontal design, premium

SET-550

Rechargeable, horizontal design

SET-S40

SET-550, SET-560 Solar Cradle

SET-535

rechargeable, circular design, premium

SET-525

Rechargeable, circular design

SET-S30

SET-525, SET-535 Solar Cradle

https://mpeon.com/hipass

MPEON

Toll-road paym

- Regex: ^MPEOI
  - Semantically:
- Advertises a diff

```
For bdaddr = 00:19:01:71:ab:3
        Company Name by IEEE

        No BTC Extended Inqui

        DeviceName: MPEON SMA
                In BT Classic
        DeviceName: MPEON SMA
                In BT LE Data
                This was foun

        UUID16s found:
                UUID16 0x110a
```

SET-560

Rechargeable, horizontal design, premium

SET-S40

SET-550, SET-560 Solar Cradle

SET-535

rechargeable, circular design, premium

SET-525

Rechargeable, circular design

SET-S30

SET-525, SET-535 Solar Cradle

https://mpeon.com/hipass

MPEON

Toll-road payment system

- Regex: ^MPEON(| SMART LE)\\\([A-F0-9]{6}\\\)$
  - Semantically: Last 6 are from BDADDR
- Advertises a different name for BT Classic vs. BLE

```
For bdaddr = 00:19:01:71:ab:30:
        Company Name by IEEE OUI (00:19:01): F1MEDIA

        No BTC Extended Inquiry Result Device info.

        DeviceName: MPEON SMART BT(71AB30)
                In BT Classic Data (EIR_bdaddr_to_name)
        DeviceName: MPEON SMART LE(71AB30)
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 0 which corresponds to Con

        UUID16s found:
                UUID16 0x110a (Service ID: AudioSource)
```

https://mpeon.com/hipass

MPEON

Toll-road payment system

- Regex: ^MPEON(| SMART LE)\\\([A-F0-9]{6}\\\)$
  - Semantically: Last 6 are from BDADDR
- Advertises a different name for BT Classic vs. BLE

```
For bdaddr = 00:19:01:71:ab:30:
        Company Name by IEEE OUI (00:19:01): F1MEDIA

        No BTC Extended Inquiry Result Device info.

        DeviceName: MPEON SMART BT(71AB30)
                In BT Classic Data (EIR_bdaddr_to_name)
        DeviceName: MPEON SMART LE(71AB30)
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 0 which corresponds to Con

        UUID16s found:
                UUID16 0x110a (Service ID: AudioSource)
```

https://mpeon.com/hipass

MPEON

Toll-road payment system

- Regex: ^MPEON(| SMART LE)\\\([A-F0-9]{6}\\\)$
  - Semantically: Last 6 are from BDADDR
- Advertises a different name for BT Classic vs. BLE

```
For bdaddr = 00:19:01:71:ab:30:
        Company Name by IEEE OUI (00:19:01): F1MEDIA

        No BTC Exte

        DeviceName:
                In
        DeviceName:
                In
                Thi

        UUID16s fou
                UUID16 0x110a (Service ID: AudioSource
```

Smart Alarm

Voice support service that informs by sound

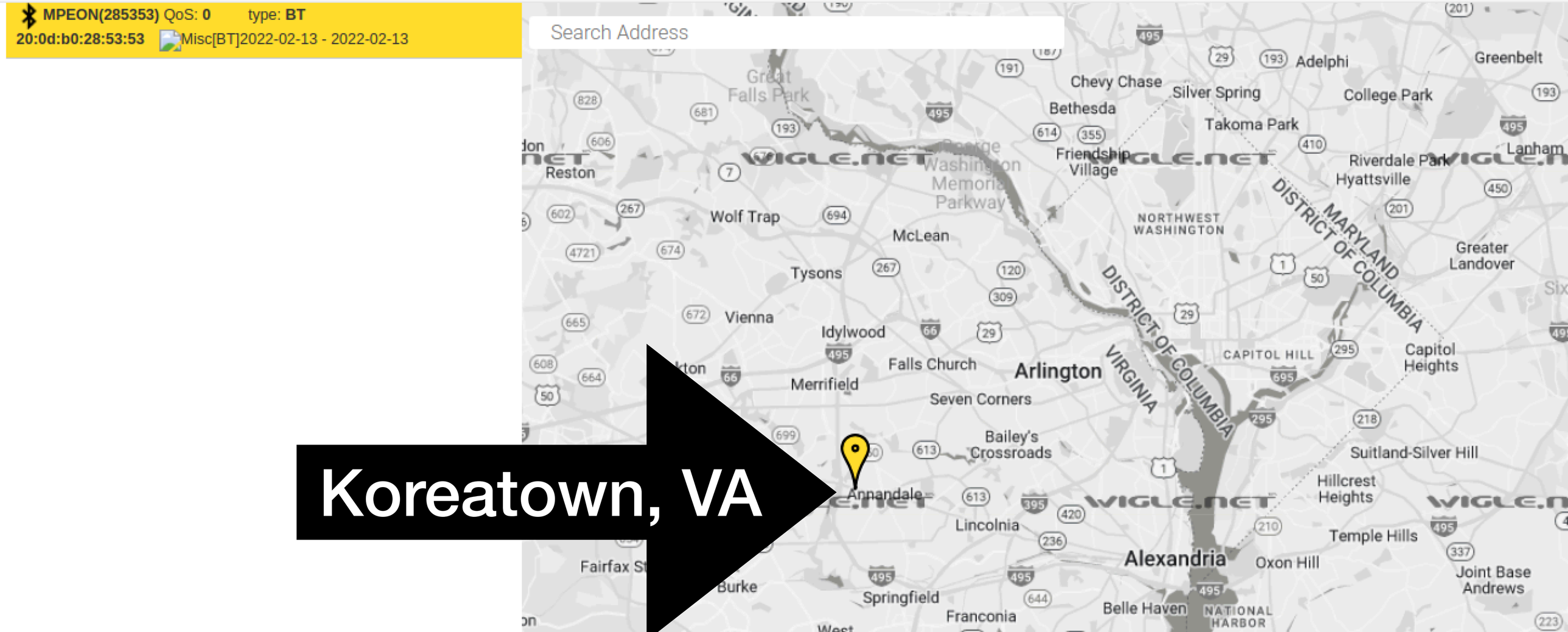
It supports clear and clear voice so that you can concentrate on driving.

Provides all information using Hi-Pass with a clear voice. Voice support with adjustable volume from 0 to 8 helps the driver to focus more on driving.

https://mpeon.com/hipass

MPEON Goes to America!

Exactly one seen in Koreatown (Annandale) in VA outside DC



Can this be used to identify high Korean populations

Across North America?

MPEON SMART LE(4F2D89) QoS: **0** type: **BLE**
00:19:01:4f:2d:89 ? 2022-07-31 - 2022-07-31

MPEON SMART LE(4F2DF0) QoS: **0** type: **BT**
00:19:01:4f:2d:f0 ? 2021-08-06 - 2021-08-06

MPEON SMART LE(4F2E14) QoS: **2** type: **BT**
00:19:01:4f:2e:14 ? 2020-03-25 - 2020-05-24

MPEON SMART LE(4F2EFB) QoS: **0** type: **BLE**
00:19:01:4f:2e:fb ? 2020-05-23 - 2020-06-05

MPEON SMART LE(4F2F00) QoS: **0** type: **BT**
00:19:01:4f:2f:00 ? 2020-12-24 - 2021-01-03

MPEON SMART LE(4F2F40) QoS: **2** type: **BLE**
00:19:01:4f:2f:40 ? 2022-02-26 - 2023-06-14

MPEON SMART LE(4F2F63) QoS: **7** type: **BT**
00:19:01:4f:2f:63 ? 2019-11-11 - 2021-09-01

MPEON SMART LE(71AD1E) QoS: **0** type: **BT**
00:19:01:71:ad:1e ? 2021-12-09 - 2021-12-09

MPEON SMART LE(71AF3F) QoS: **4** type: **BLE**
00:19:01:71:af:3f ? 2020-01-31 - 2022-05-06

MPEON SMART LE(71AF40) QoS: **1** type: **BLE**
00:19:01:71:af:40 ? 2020-02-22 - 2021-10-28

Can this be used to identify high Korean populations

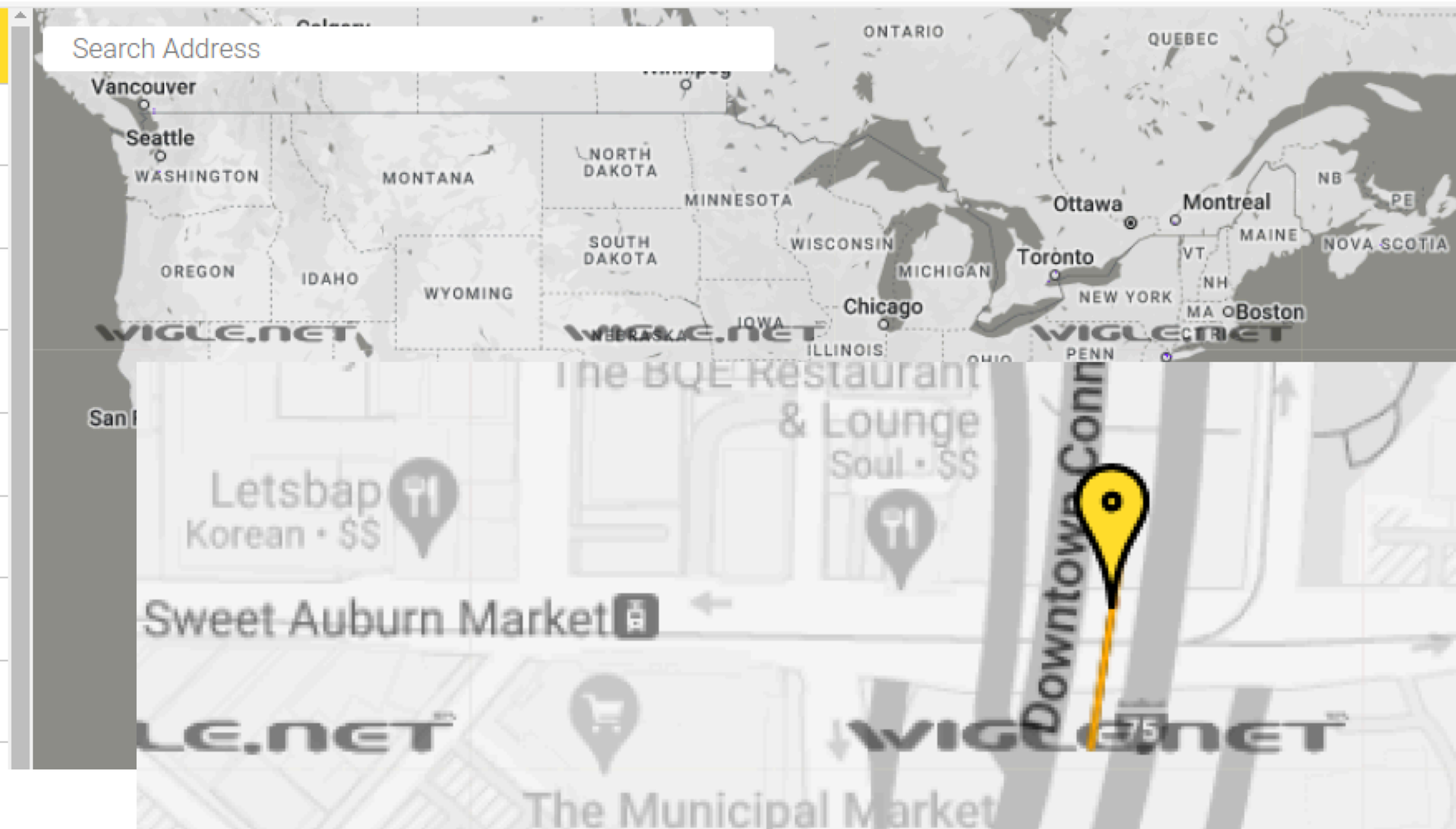
Across North America?

MPEON SMART LE(4F26B5) QoS: 0 type: BLE 00:19:01:4f:26:b5	?	2021-05-04 - 2021-06-15
MPEON SMART LE(4F26EB) QoS: 0 type: BT 00:19:01:4f:26:eb	?	2019-09-08 - 2021-03-31
MPEON SMART LE(4F2959) QoS: 0 type: BT 00:19:01:4f:29:59	?	2021-10-13 - 2021-10-14
MPEON SMART BT(4F2BFF) QoS: 0 type: BT 00:19:01:4f:2b:ff	?	2020-07-27 - 2020-07-27
MPEON SMART LE(4F2D89) QoS: 0 type: BLE 00:19:01:4f:2d:89	?	2022-07-31 - 2022-07-31
MPEON SMART LE(4F2DF0) QoS: 0 type: BT 00:19:01:4f:2d:f0	?	2021-08-06 - 2021-08-06
MPEON SMART LE(4F2E14) QoS: 2 type: BT 00:19:01:4f:2e:14	?	2020-03-25 - 2020-05-24
MPEON SMART LE(4F2EFB) QoS: 0 type: BLE 00:19:01:4f:2e:fb	?	2020-05-23 - 2020-06-05
MPEON SMART LE(4F2F00) QoS: 0 type: BT 00:19:01:4f:2f:00	?	2020-12-24 - 2021-01-03
MPEON SMART LE(4F2F40) QoS: 2 type: BLE		

Can this be used to identify high Korean populations

Across North America?

MPEON SMART LE(4F26B5) QoS: 0 type: BLE 00:19:01:4f:26:b5	?	2021-05-04 - 2021-06-15
MPEON SMART LE(4F26EB) QoS: 0 type: BT 00:19:01:4f:26:eb	?	2019-09-08 - 2021-03-31
MPEON SMART LE(4F2959) QoS: 0 type: BT 00:19:01:4f:29:59	?	2021-10-13 - 2021-10-14
MPEON SMART BT(4F2BFF) QoS: 0 type: BT 00:19:01:4f:2b:ff	?	2020-07-27 - 2020-07-27
MPEON SMART LE(4F2D89) QoS: 0 type: BLE 00:19:01:4f:2d:89	?	2022-07-31 - 2022-07-31
MPEON SMART LE(4F2DF0) QoS: 0 type: BT 00:19:01:4f:2d:f0	?	2021-08-06 - 2021-08-06
MPEON SMART LE(4F2E14) QoS: 2 type: BT 00:19:01:4f:2e:14	?	2020-03-25 - 2020-05-24
MPEON SMART LE(4F2EFB) QoS: 0 type: BLE 00:19:01:4f:2e:fb	?	2020-05-23 - 2020-06-05
MPEON SMART LE(4F2F00) QoS: 0 type: BT 00:19:01:4f:2f:00	?	2020-12-24 - 2021-01-03
MPEON SMART LE(4F2F40) QoS: 2 type: BLE		



Can this be used to identify high Korean populations

Across North America?

MPEON SMART LE(4F26B5) QoS: 0 type: BLE
00:19:01:4f:26:b5 ? 2021-05-04 - 2021-06-15

MPEON SMART LE(4F26EB) QoS: 0 type: BT
00:19:01:4f:26:eb ? 2019-09-08 - 2021-03-31

MPEON SMART LE(4F2959) QoS: 0 type: BT
00:19:01:4f:29:59 ? 2021-10-13 - 2021-10-14

MPEON SMART BT(4F2BFF) QoS: 0 type: BT
00:19:01:4f:2b:ff ? 2020-07-27 - 2020-07-27

MPEON SMART LE(4F2D89) QoS: 0 type: BLE
00:19:01:4f:2d:89 ? 2022-07-31 - 2022-07-31

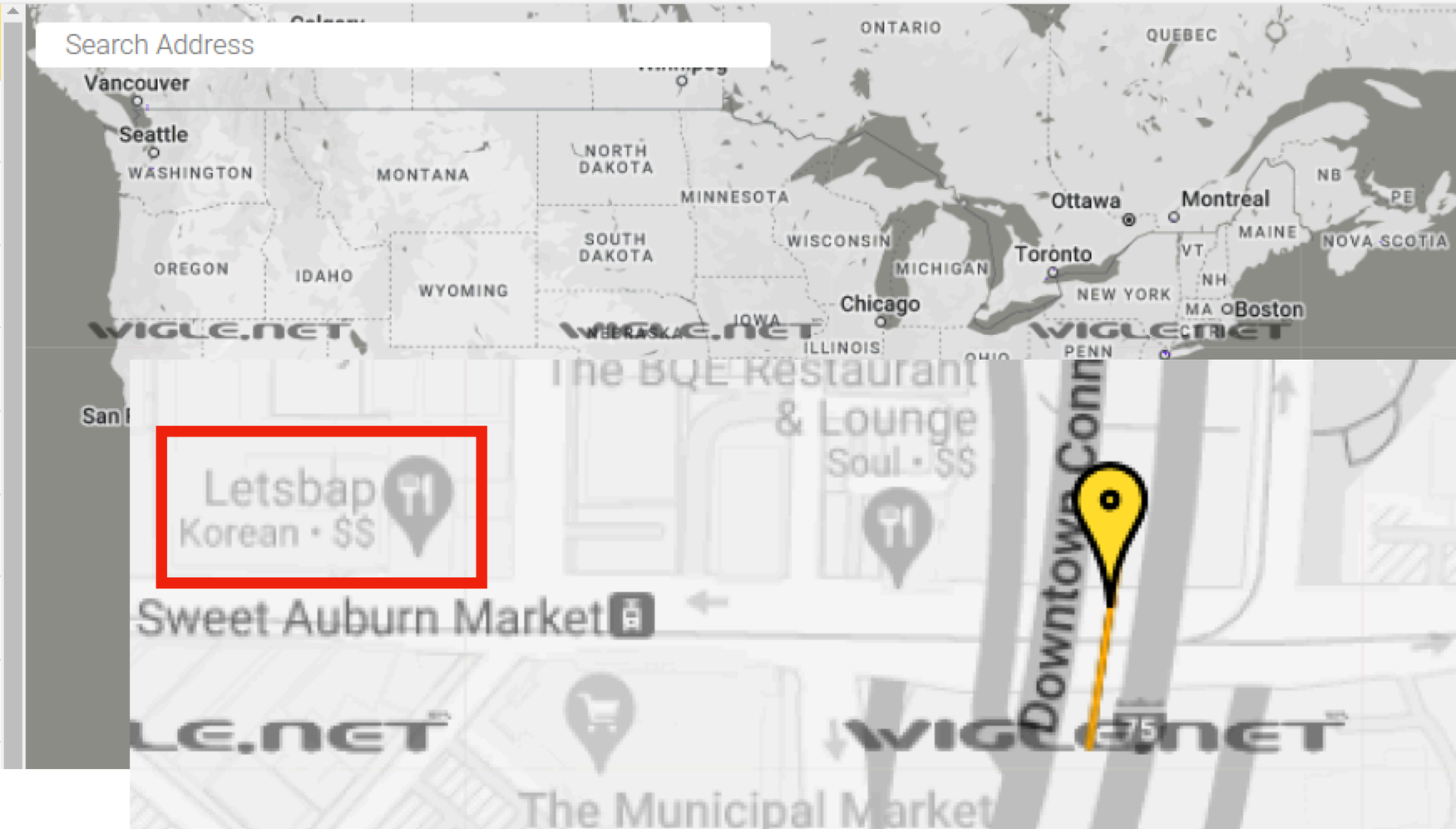
MPEON SMART LE(4F2DF0) QoS: 0 type: BT
00:19:01:4f:2d:f0 ? 2021-08-06 - 2021-08-06

MPEON SMART LE(4F2E14) QoS: 2 type: BT
00:19:01:4f:2e:14 ? 2020-03-25 - 2020-05-24

MPEON SMART LE(4F2EFB) QoS: 0 type: BLE
00:19:01:4f:2e:fb ? 2020-05-23 - 2020-06-05

MPEON SMART LE(4F2F00) QoS: 0 type: BT
00:19:01:4f:2f:00 ? 2020-12-24 - 2021-01-03

MPEON SMART LE(4F2F40) QoS: 2 type: BLE



Can this be used to identify high Korean populations

Across North America?

MPEON SMART BT(4F2BFF) QoS: **0** type: **BT**
00:19:01:4f:2b:ff ? 2020-07-27 - 2020-07-27

MPEON SMART LE(4F2D89) QoS: **0** type: **BLE**
00:19:01:4f:2d:89 ? 2022-07-31 - 2022-07-31

MPEON SMART LE(4F2DF0) QoS: **0** type: **BT**
00:19:01:4f:2d:f0 ? 2021-08-06 - 2021-08-06

MPEON SMART LE(4F2E14) QoS: **2** type: **BT**
00:19:01:4f:2e:14 ? 2020-03-25 - 2020-05-24

MPEON SMART LE(4F2EFB) QoS: **0** type: **BLE**
00:19:01:4f:2e:fb ? 2020-05-23 - 2020-06-05

MPEON SMART LE(4F2F00) QoS: **0** type: **BT**
00:19:01:4f:2f:00 ? 2020-12-24 - 2021-01-03

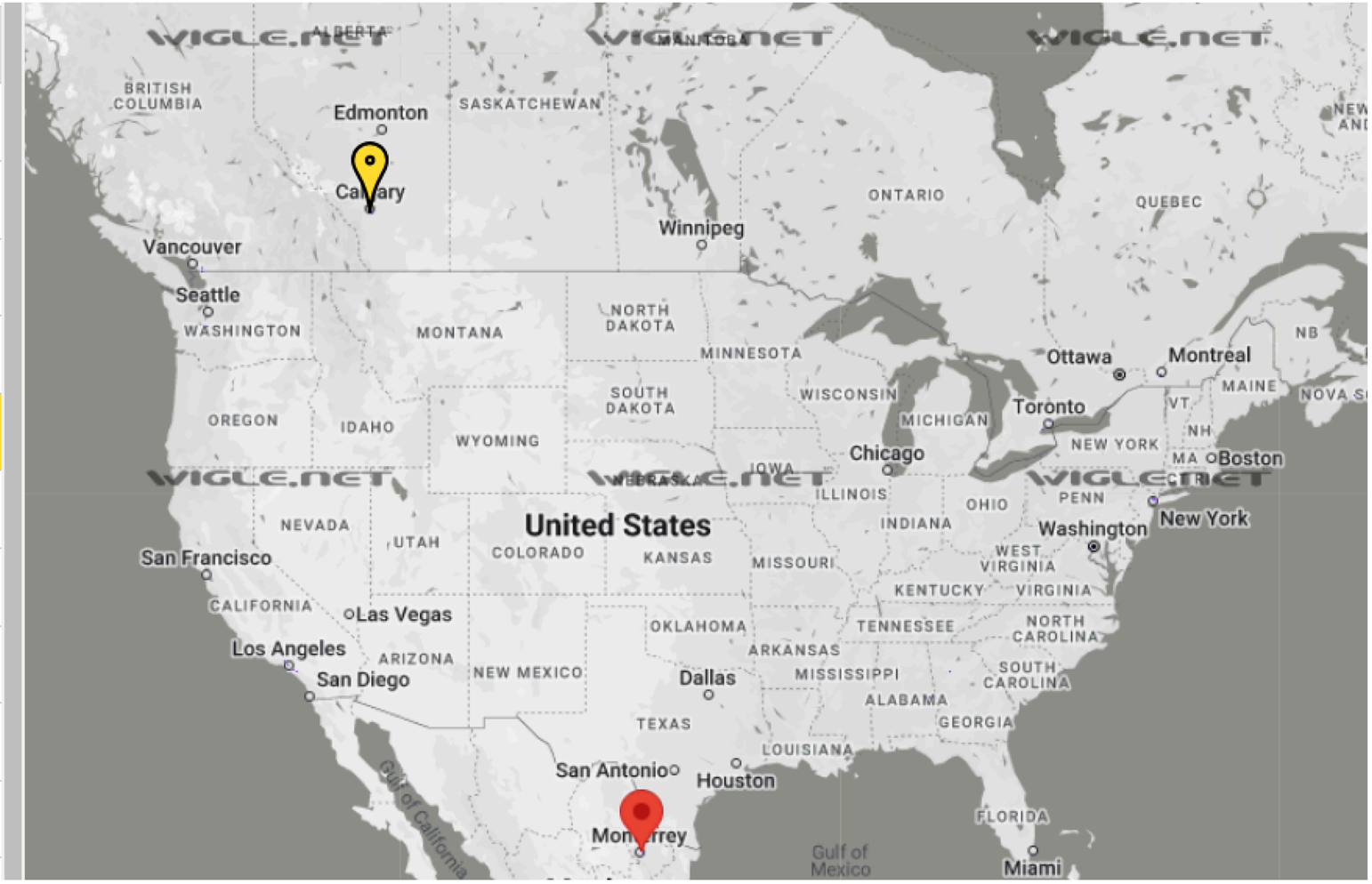
MPEON SMART LE(4F2F40) QoS: **2** type: **BLE**
00:19:01:4f:2f:40 ? 2022-02-26 - 2023-06-14

MPEON SMART LE(4F2F63) QoS: **7** type: **BT**
00:19:01:4f:2f:63 ? 2019-11-11 - 2021-09-01

MPEON SMART LE(71AD1E) QoS: **0** type: **BT**
00:19:01:71:ad:1e ? 2021-12-09 - 2021-12-09

MPEON SMART LE(71AF3F) QoS: **4** type: **BLE**
00:19:01:71:af:3f ? 2020-01-31 - 2022-05-06

MPEON SMART LE(71AF40) QoS: **1** type: **BLE**
00:19:01:71:af:40 ? 2020-02-22 - 2021-10-28



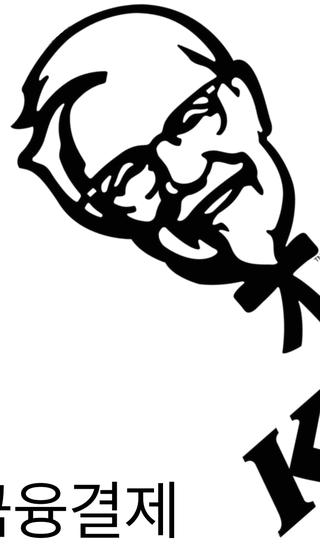
KFTC BANKPOS

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)
```

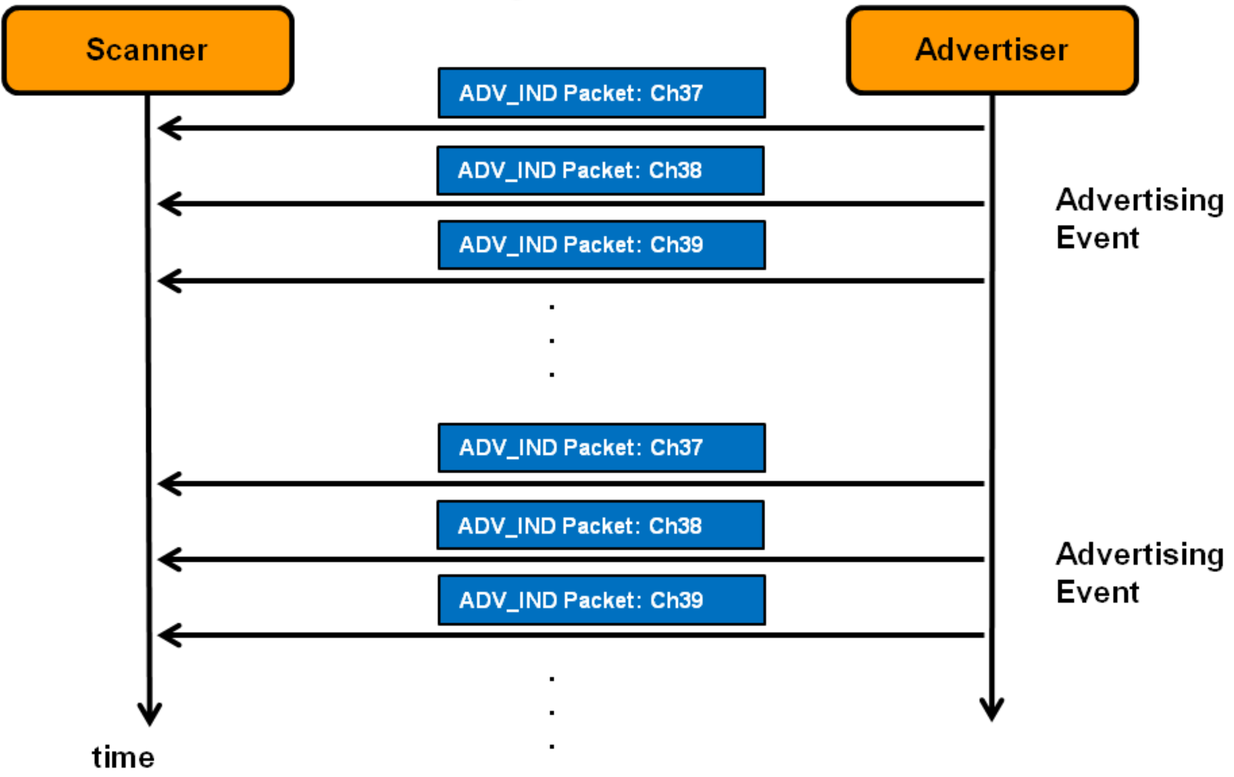
KFTC BANKPOS

Point of Sale terminal

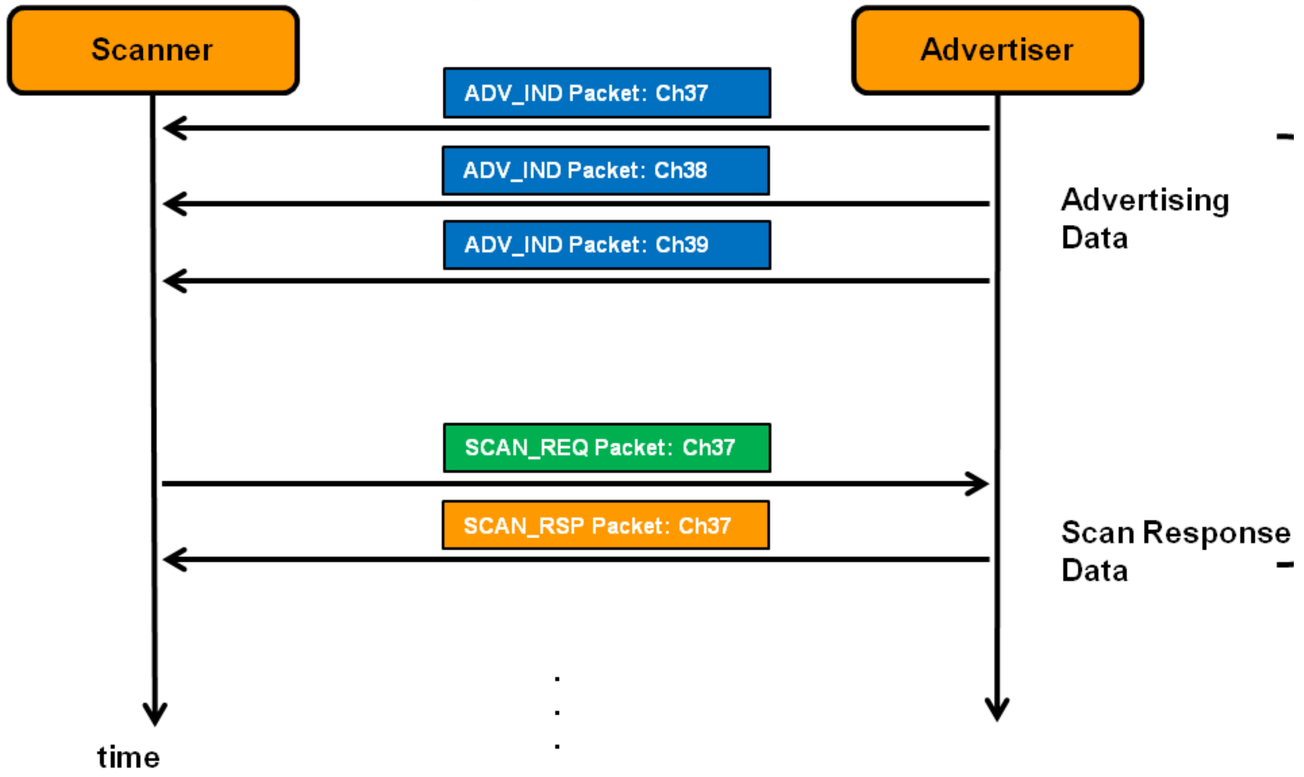
```
For bdaddr = 04:32:f4:18:48:d7:
        Company Name by IEEE OUI (04:32:f4): Partron

        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)
```

Background

Passive Scanning



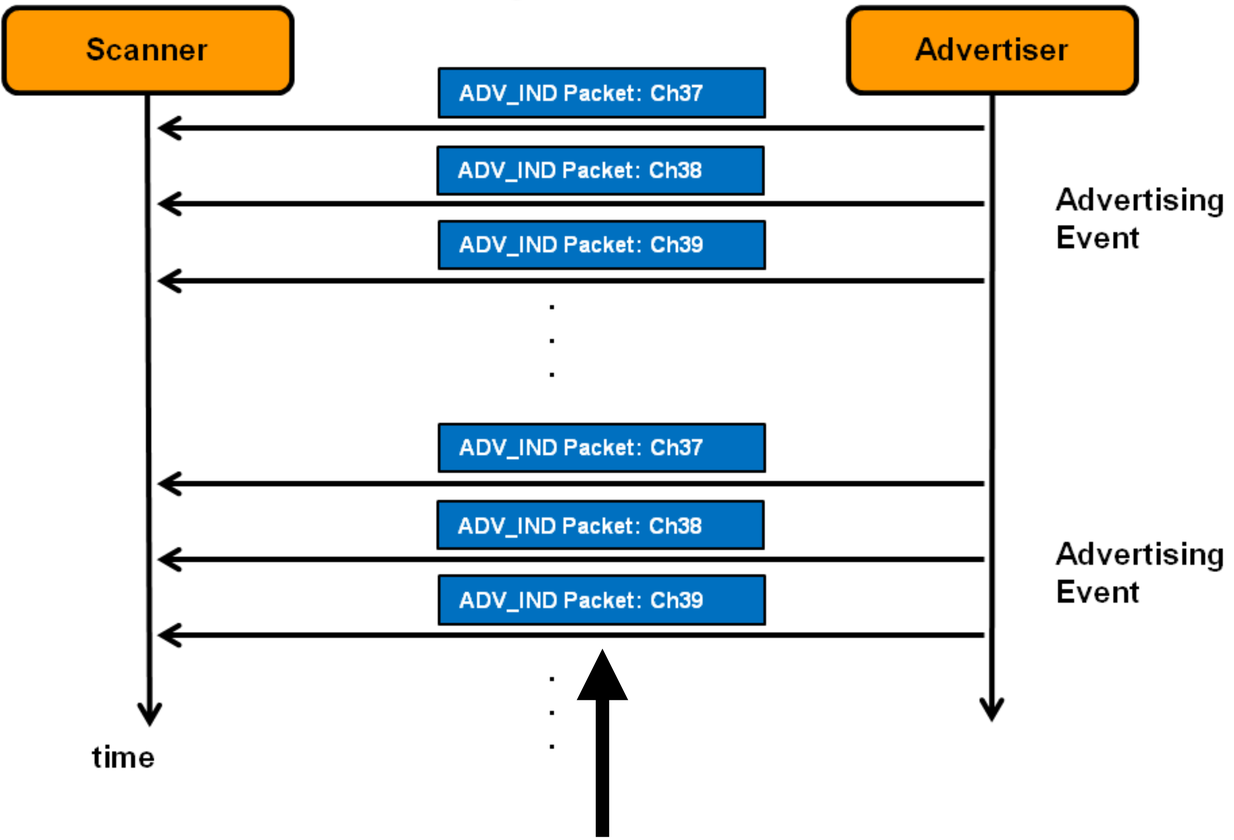
Active Scanning



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

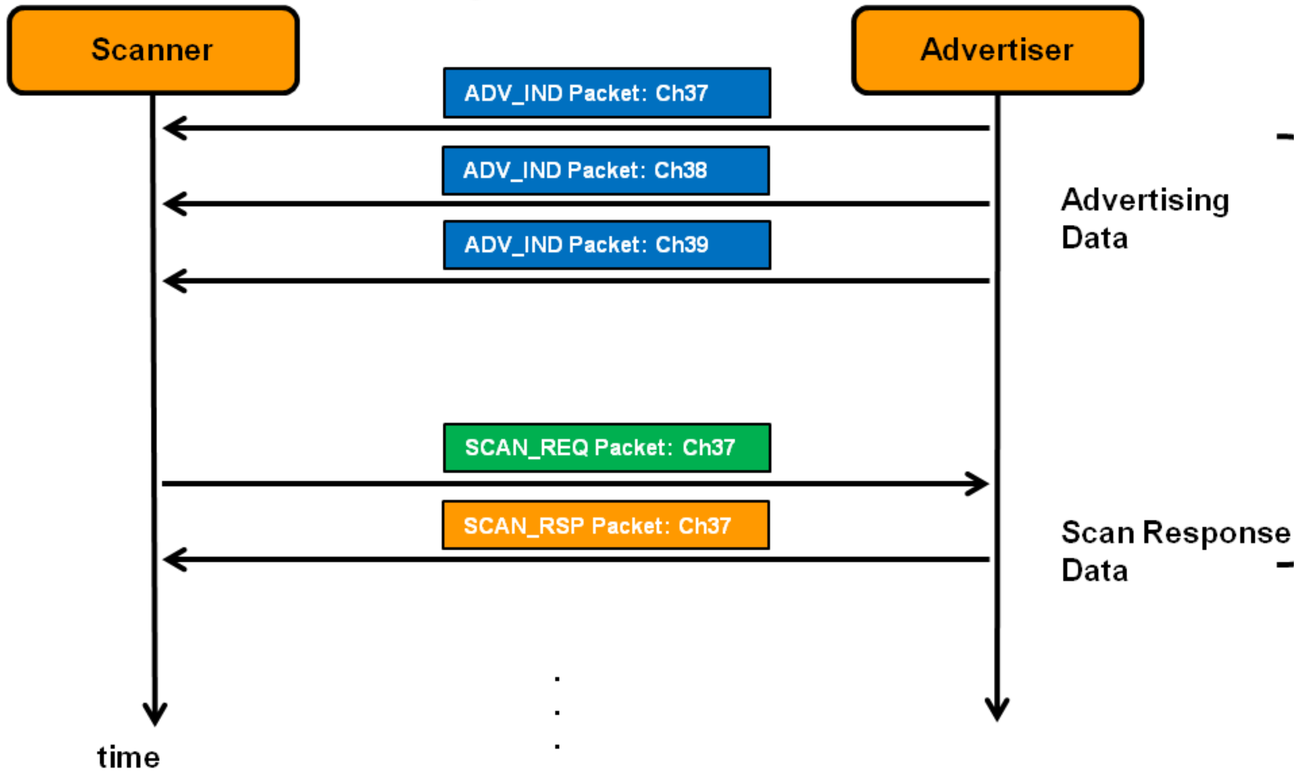
Background

Passive Scanning



Sometimes the name will be here

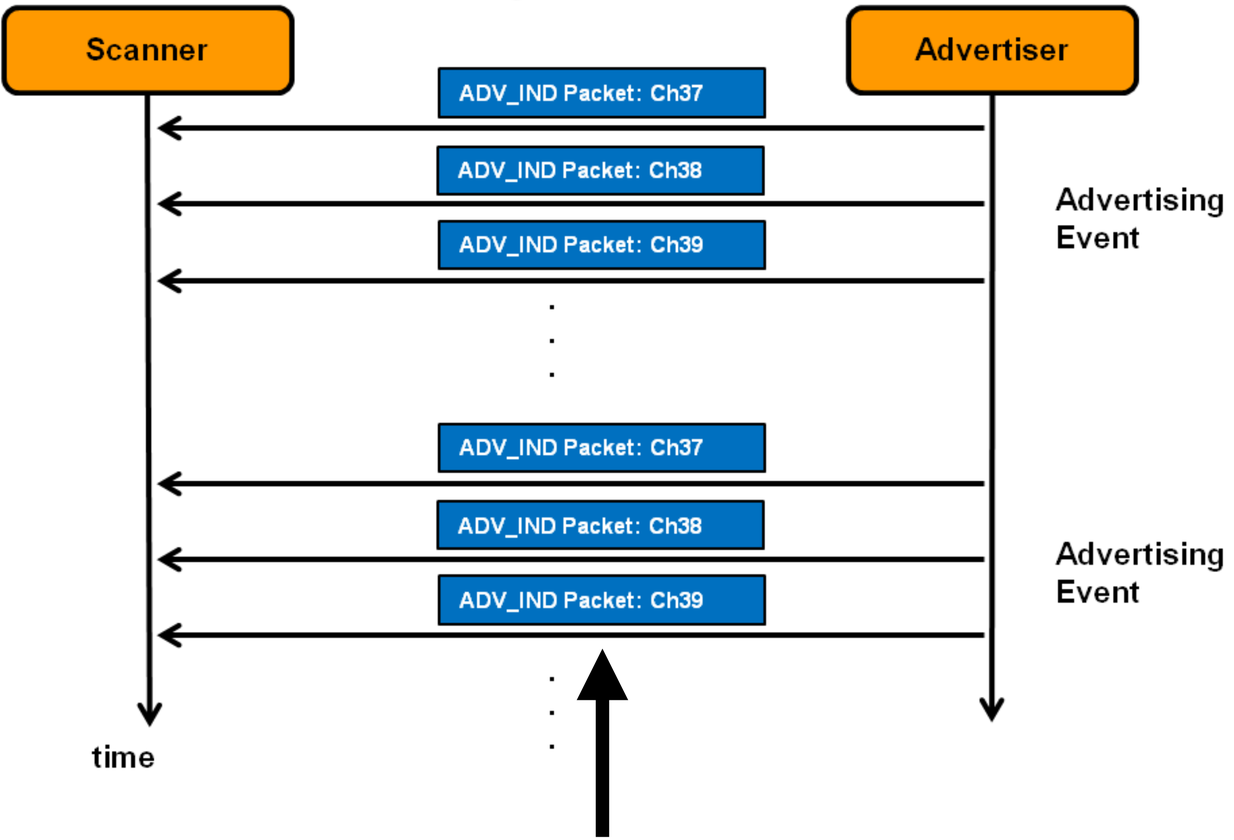
Active Scanning



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

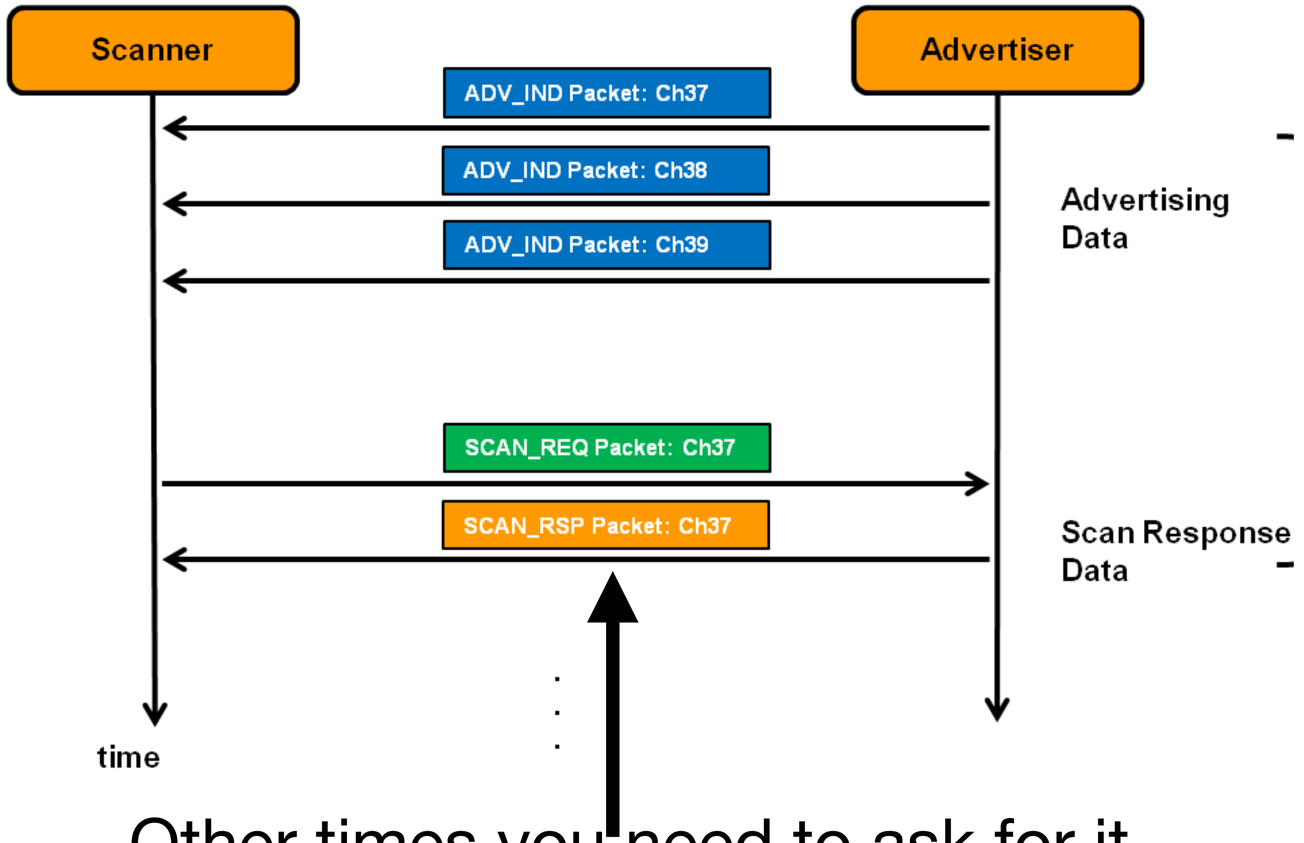
Background

Passive Scanning



Sometimes the name will be here

Active Scanning



Other times you need to ask for it, and it comes back in the SCAN_RSP

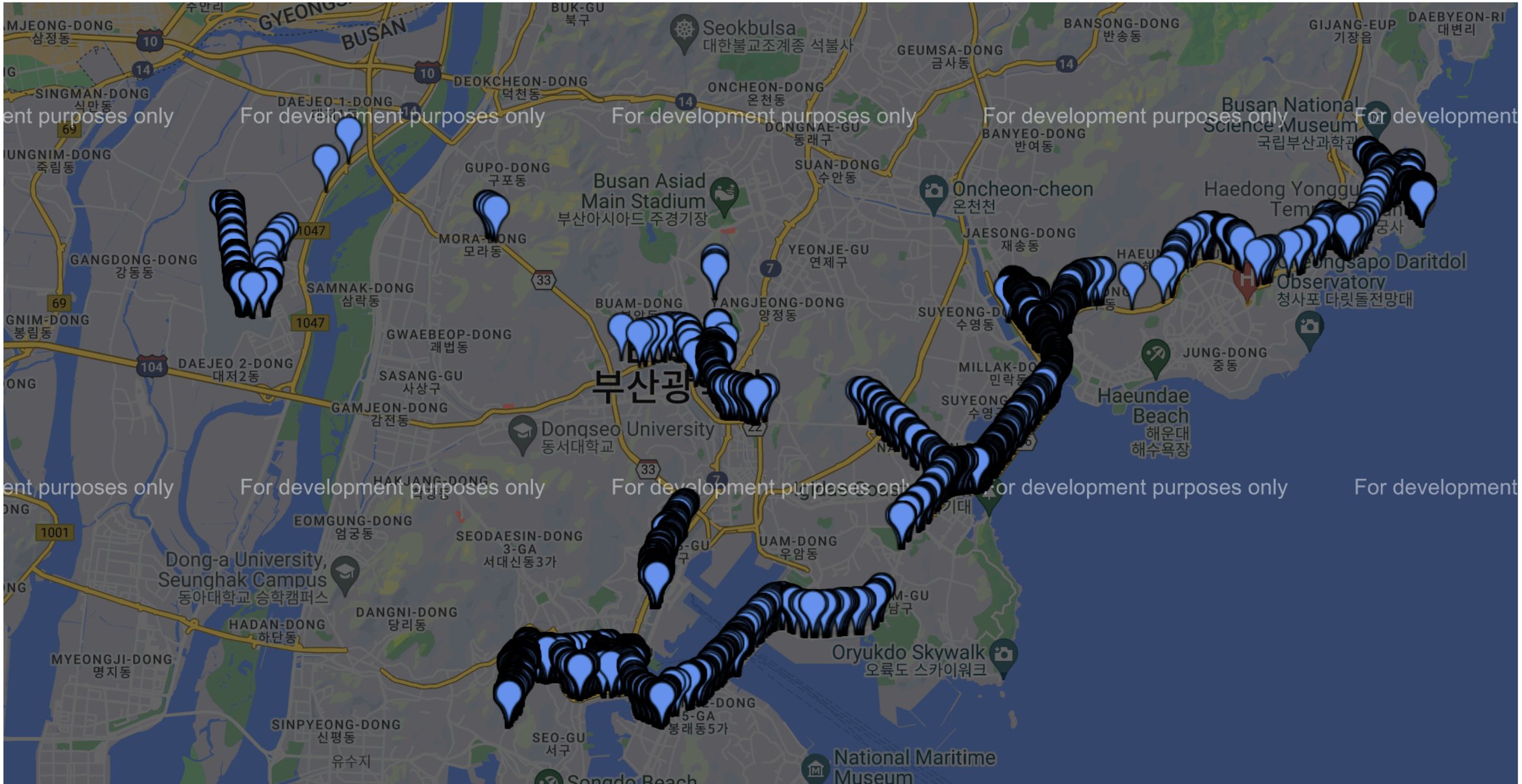
Images from https://microchipdeveloper.com/wireless:ble-link-layer-discovery

Mini-Takeaway

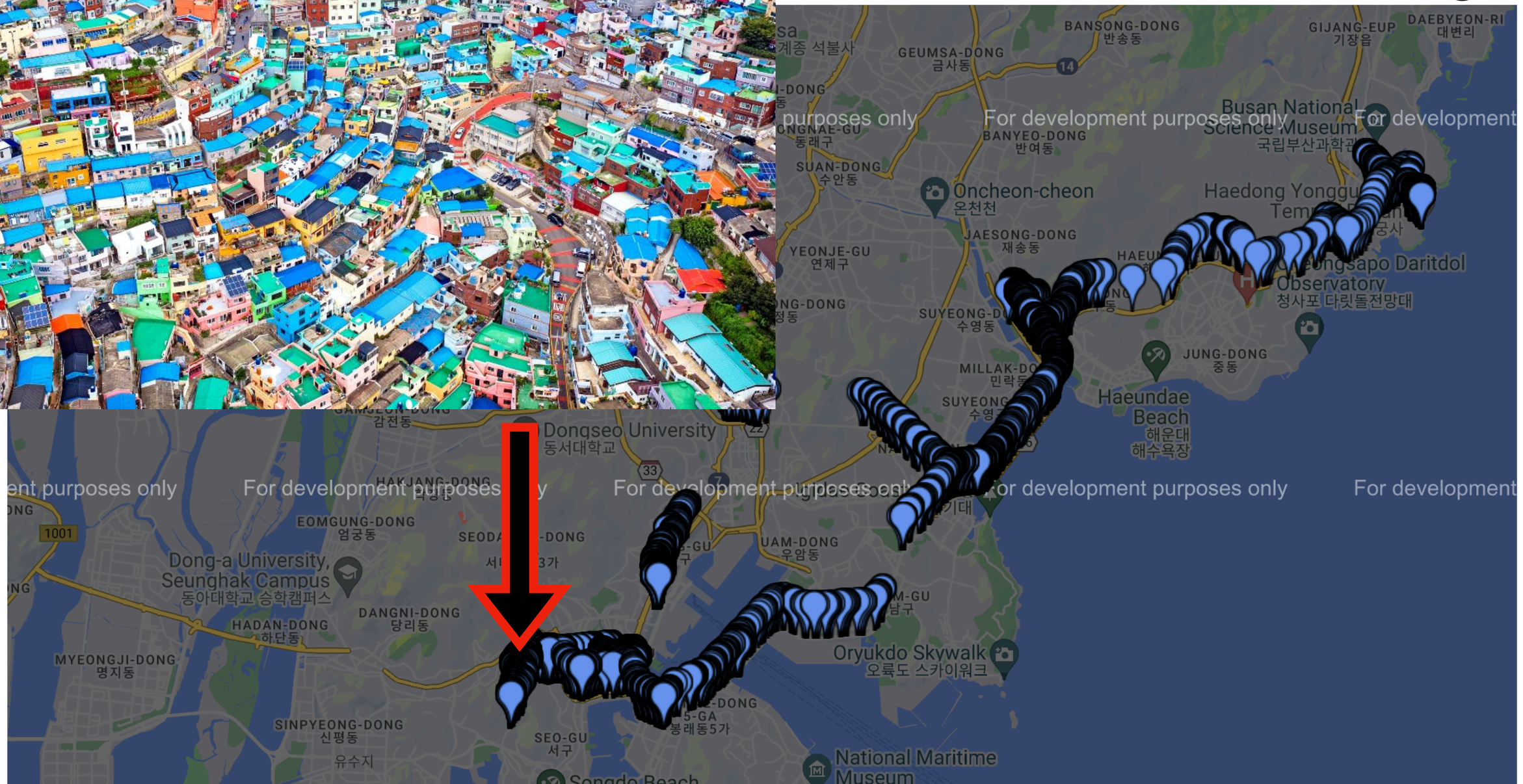
Model identification

- Parsing iBeacons to extract the UUID128 within can be useful for identifying *unnamed devices* that are with high probability the same model as other devices where the name has been found

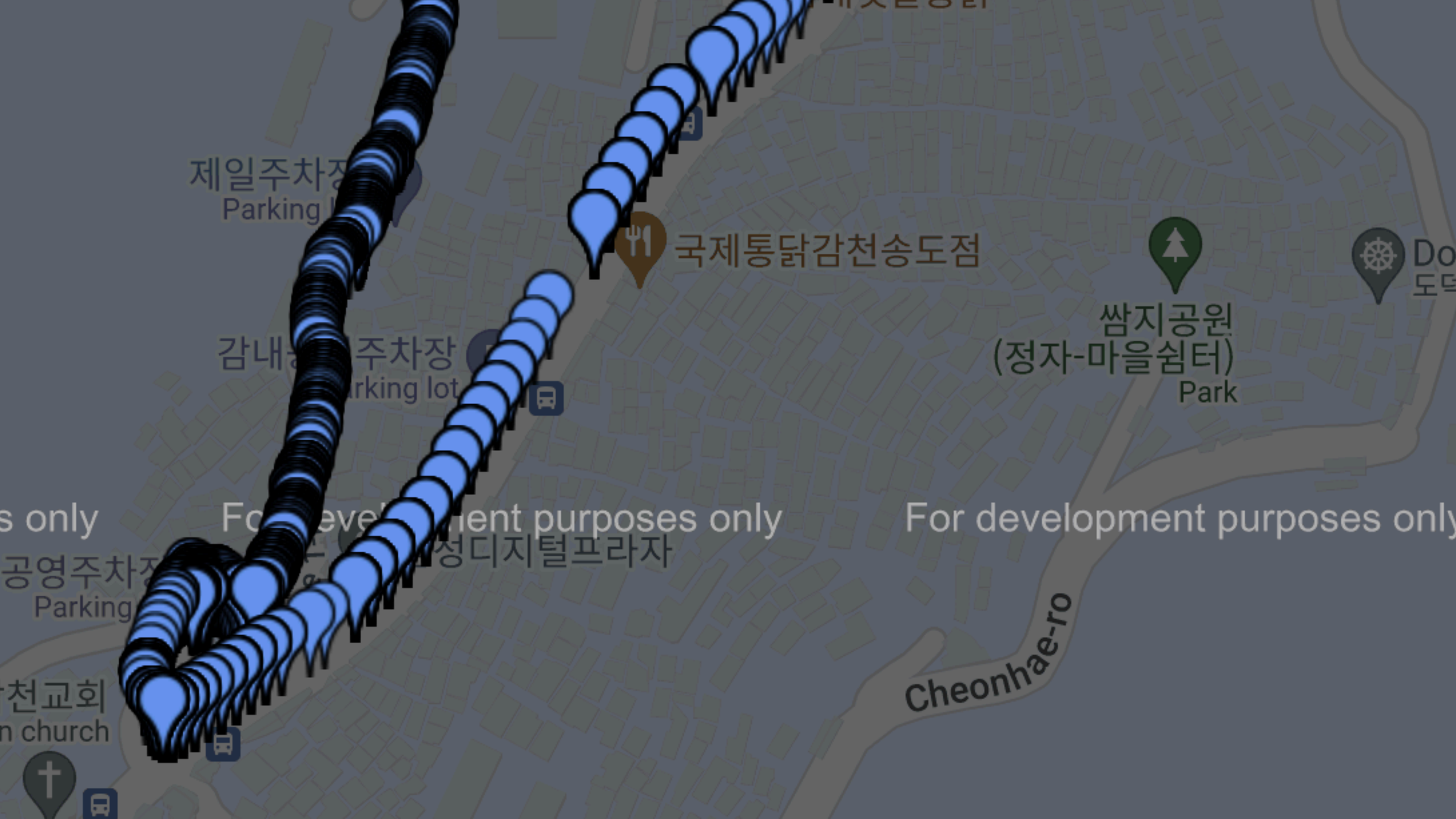
South Korea - Busan

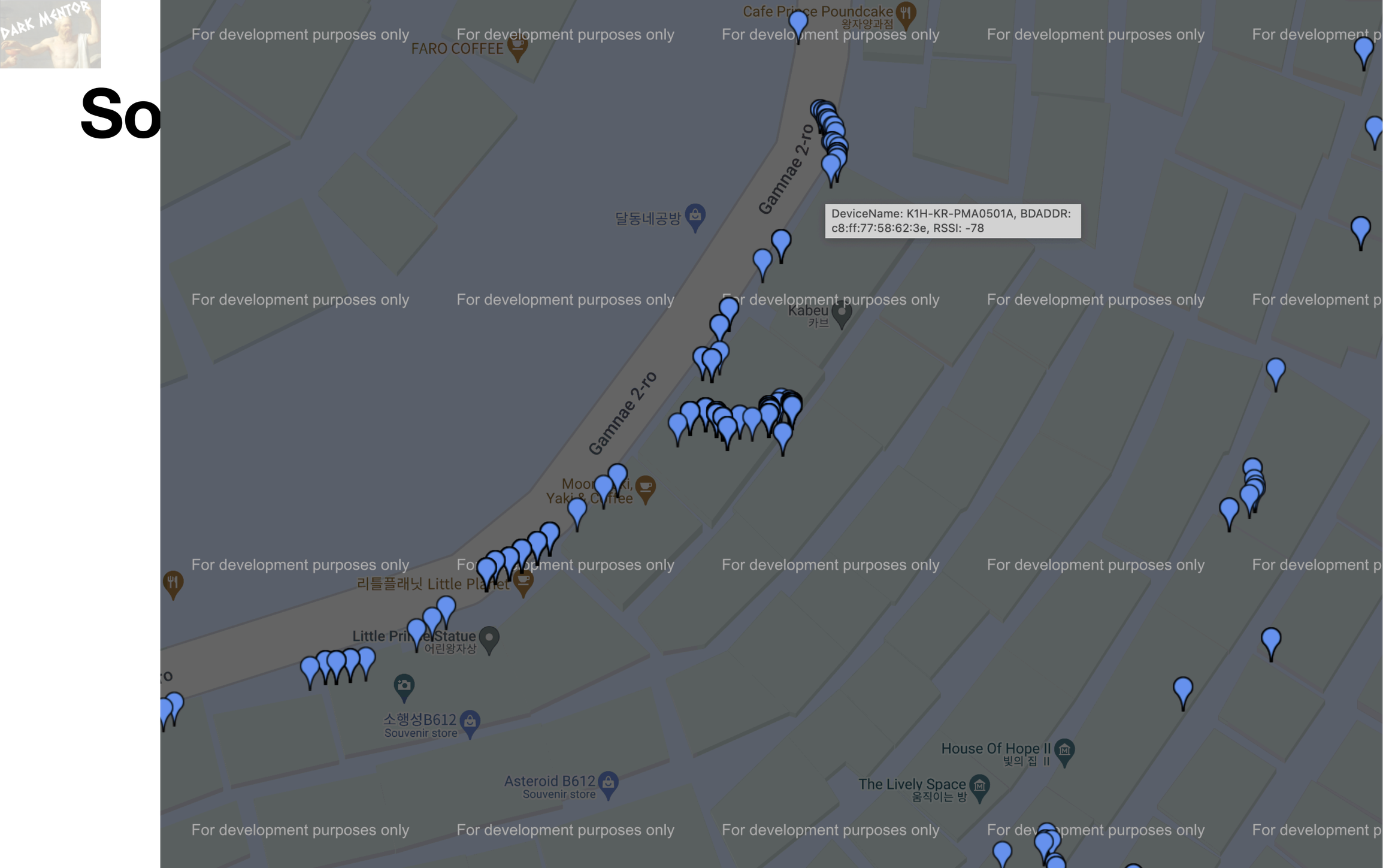


"Gamcheon Culture Village"

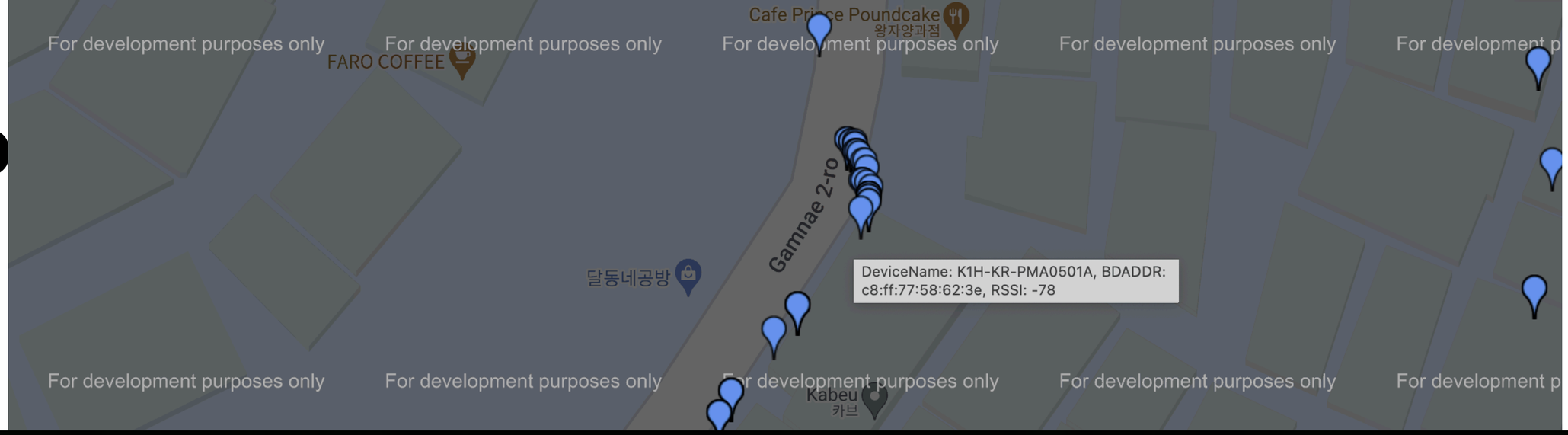


Jungkook & Jimin Mura
정국&지민
Haneul Ma
감천문화마을
하늘마루전망대
구름이쉬어가
For development pur
development pu
FARO COFFEE
Little Prince Sta
아미
복지예사랑병
Hosp
더플레이트 The Plat
Brunch
부건어패럴

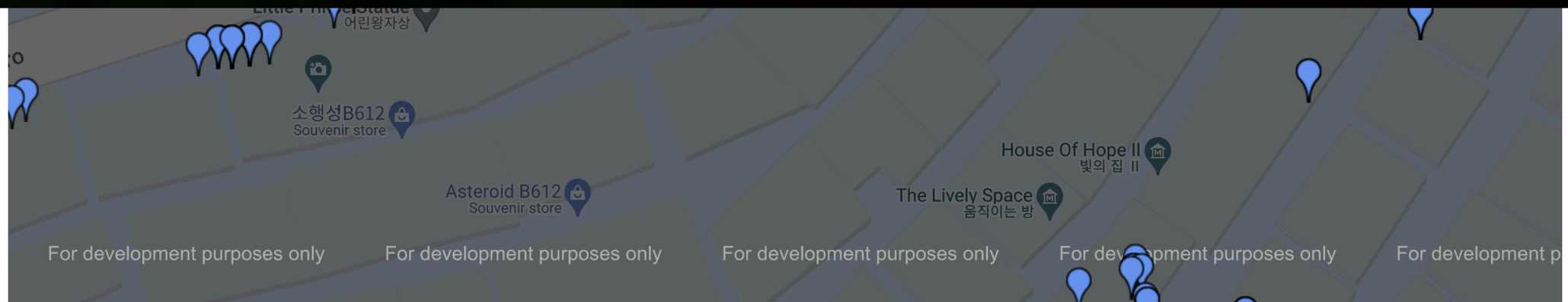

제일주차장
Parking
국제통닭감천송도점
쌈지공원
(정자-마을쉼터)
Park
주차장
rking lot
s only
For development purposes only
For development purposes only
공영주차장
Parking
성디지털프라자
천교회
n church
Cheonhae-ro


Cafe Prince Poundcake
왕자양과점
FARO COFFEE
Gamnae 2-ro
DeviceName: K1H-KR-PMA0501A, BDADDR: c8:ff:77:58:62:3e, RSSI: -78
달동네공방
Kabeu
카브
Gamnae 2-ro
Moon Yaki, Yaki & Coffee
리틀플래닛 Little Planet
Little Prince Statue
어린왕자상
소행성B612
Souvenir store
Asteroid B612
Souvenir store
House Of Hope II
빛의 집 II
The Lively Space
움직이는 방
For development purposes only

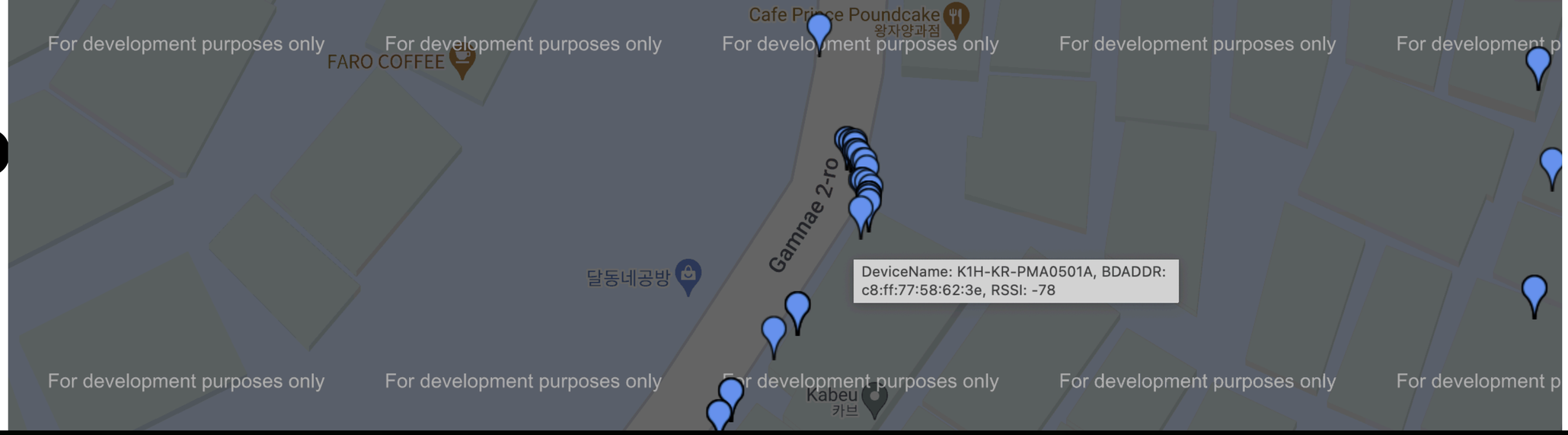
So



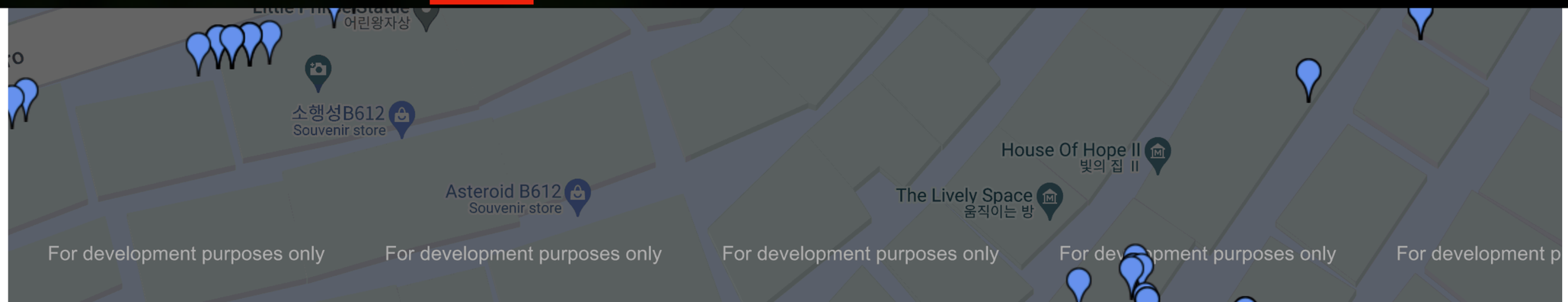

```
Company Name by IEEE OUI (c8:ff:77): Dyson Limited

No BTC Extended Inquiry Result Device info.

DeviceName: K1H-KR-PMA0501A
```



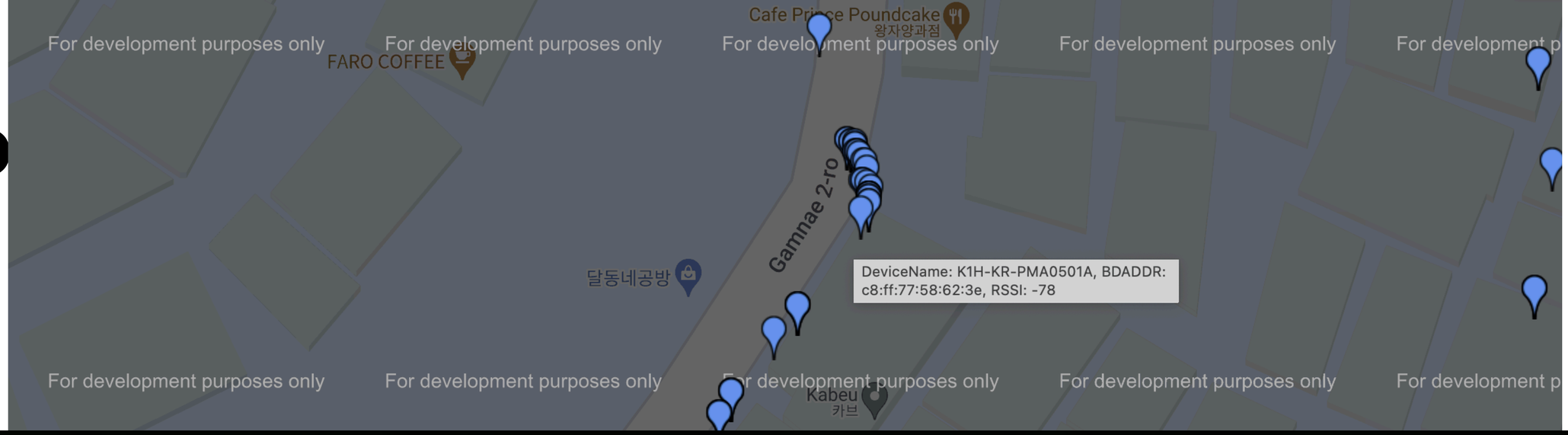
So




```
Company Name by IEEE OUI (c8:ff:77): Dyson Limited

No BTC Extended Inquiry Result Device info.

DeviceName: K1H-KR-PMA0501A
```



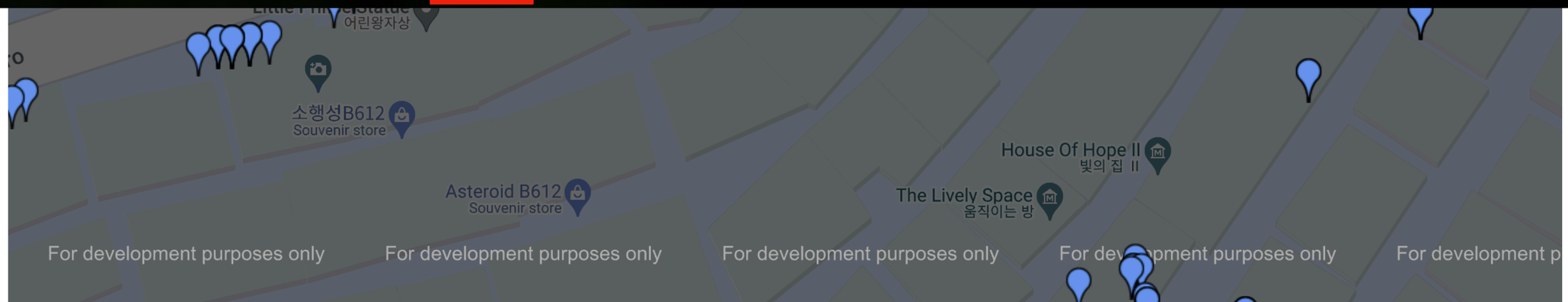
So



Company Name by IEEE OUI (c8:ff:77): Dyson Limited

No BTC Extended Inquiry Result Device info.

DeviceName: K1H-KR-PMA0501A



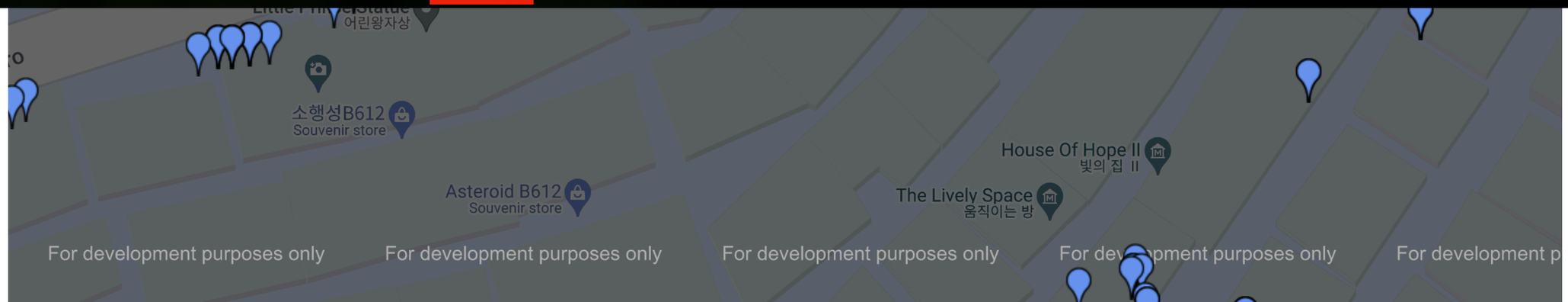
So

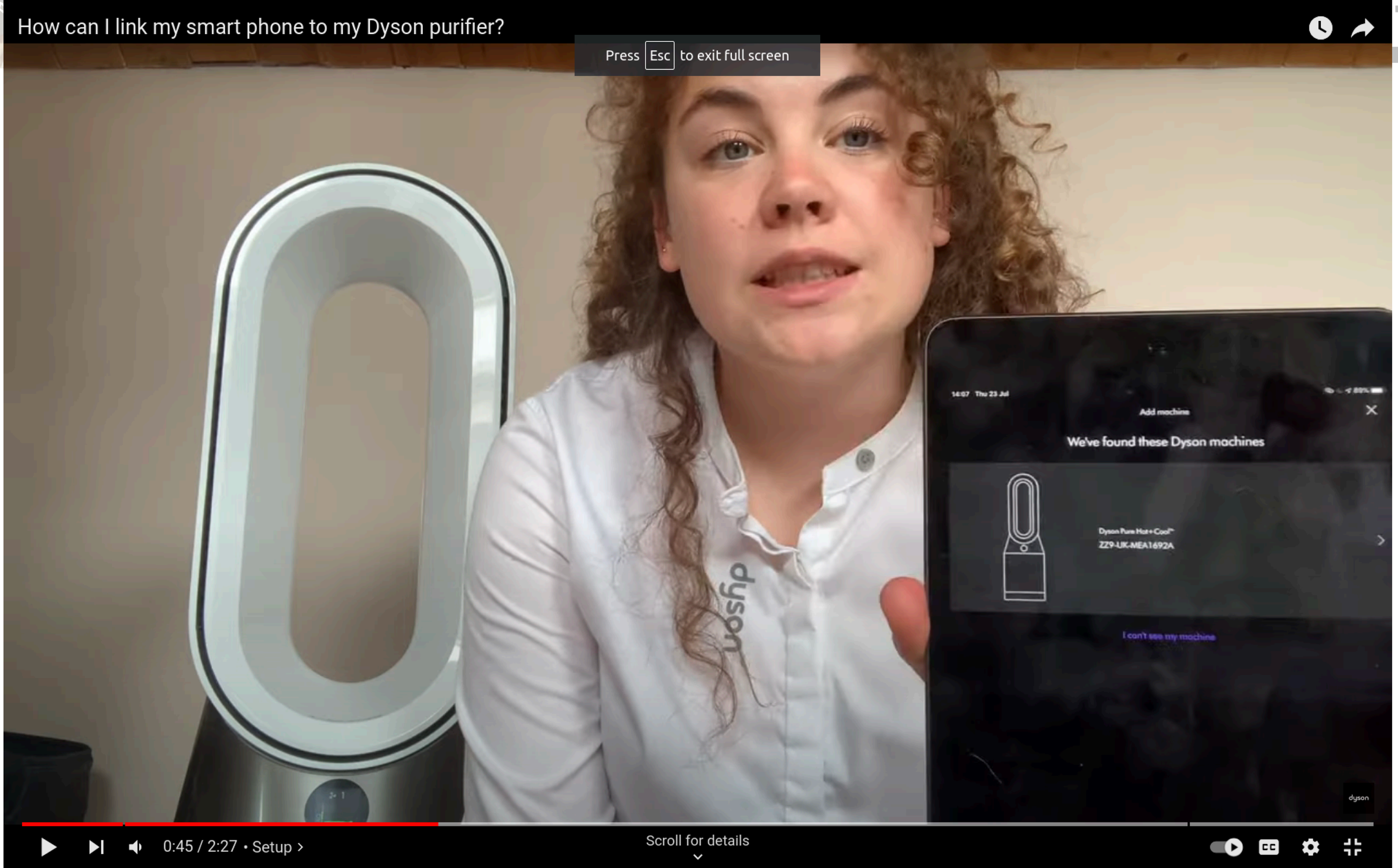
???

Company Name by IEEE OUI (c8:ff:77): Dyson Limited

No BTC Extended Inquiry Result Device info.

DeviceName: K1H-KR-PMA0501A





https://youtu.be/Z65QgA_BKgc?t=45

Add machine

We've found these Dyson machines

Dyson Pure Hot+Cool™

ZZ9-UK-MEA1692A

I can't see my machine

https://youtu.be/Z65QgA_BKgc?t=45

Dyson Devices

Hot/Cold Air Fans

- Per-country/region naming scheme

```
mysql> select * from LE_bdaddr_to_name where device_name regexp "^[A-Z0-9]{3}-[A-Z]{2}-[A-Z]{3}[0-9]{4}A$";
+--------+------------------+--------------+-------------+-----------------+
| id     | device_bdaddr    | bdaddr_random | le_evt_type | device_name     |
+--------+------------------+--------------+-------------+-----------------+
|  33559 | 44:6f:f8:01:0f:b4 |             0 |           4 | X1S-KR-RGA0042A |
|  79630 | 44:6f:f8:07:94:a2 |             0 |          27 | X2Z-US-RNA0094A |
|  79392 | 44:6f:f8:0a:3e:3e |             0 |          27 | X4U-US-RJA5283A |
|  78183 | 44:6f:f8:0e:92:a0 |             0 |           4 | X4E-US-RKA1519A |
|  94608 | 44:6f:f8:0e:92:a0 |             0 |          27 | X4E-US-RKA1519A |
|  79393 | 44:6f:f8:0f:af:90 |             0 |          27 | X4U-US-RKA3032A |
|  11188 | c8:ff:77:14:1f:0c |             0 |           4 | G1B-US-NMA0199A |
|  78433 | c8:ff:77:16:76:4a |             0 |           4 | K3W-US-NNA0223A |
|  94662 | c8:ff:77:16:76:4a |             0 |          27 | K3W-US-NNA0223A |
|  72489 | c8:ff:77:16:dc:ac |             0 |          27 | J8W-US-PAA2151A |
|  78434 | c8:ff:77:17:21:1e |             0 |           4 | J8W-US-NNA0621A |
|  79041 | c8:ff:77:17:21:1e |             0 |          27 | J8W-US-NNA0621A |
|  11189 | c8:ff:77:18:48:e0 |             0 |           4 | C4B-US-NNA2741A |
|  72271 | c8:ff:77:19:4f:2a |             0 |          27 | J8W-US-PAA1105A |
|  78435 | c8:ff:77:19:58:4e |             0 |           4 | J9N-US-PAA0790A |
|  94663 | c8:ff:77:19:58:4e |             0 |          27 | J9N-US-PAA0790A |
|   6735 | c8:ff:77:21:e3:41 |             0 |           4 | ZZ4-US-NKA4061A |
|  93844 | c8:ff:77:2b:61:76 |             0 |           4 | K3B-US-RFA0488A |
|  94664 | c8:ff:77:2b:61:76 |             0 |          27 | K3B-US-RFA0488A |
|  78436 | c8:ff:77:2d:b5:fe |             0 |           4 | K1N-US-REA0223A |
|  79135 | c8:ff:77:2d:b5:fe |             0 |          27 | K1N-US-REA0223A |
|  78437 | c8:ff:77:2d:db:a0 |             0 |           4 | K1M-US-RGA1542A |
|  78968 | c8:ff:77:2d:db:a0 |             0 |          27 | K1M-US-RGA1542A |
|  79640 | c8:ff:77:44:27:1d |             0 |          27 | ZZ4-US-PAA2610A |
|  19785 | c8:ff:77:55:e3:fe |             0 |           4 | K3X-US-PHA0445A |
|  33635 | c8:ff:77:58:5f:4e |             0 |           4 | K1H-KR-PMA0645A |
|  20373 | c8:ff:77:58:62:3e |             0 |           4 | K1H-KR-PMA0501A |
|  20374 | c8:ff:77:5a:98:08 |             0 |           4 | K3M-KR-PJA0452A |
|  33636 | c8:ff:77:67:6a:6a |             0 |           4 | K2K-KR-PMA0980A |
| 137883 | c8:ff:77:69:9e:44 |             0 |           4 | K1M-US-REA0055A |
|  71842 | c8:ff:77:6c:51:0a |             0 |          27 | X6K-US-RHA0425A |
|   4217 | c8:ff:77:88:76:66 |             0 |           4 | YN1-US-MHA0492A |
|  29220 | c8:ff:77:8d:78:cf |             0 |           4 | E1J-KR-MKA0180A |
|   6926 | c8:ff:77:90:f1:ee |             0 |           4 | ZZ4-US-MNA3159A |
|  24294 | c8:ff:77:96:96:48 |             0 |           4 | VS9-EU-NFA8472A |
|  13541 | c8:ff:77:99:c0:da |             0 |           4 | F5N-US-NHA2866A |
|  44528 | c8:ff:77:99:c0:da |             0 |          27 | F5N-US-NHA2866A |
|  14433 | c8:ff:77:9a:0d:a0 |             0 |           4 | ZZ4-US-NHA0899A |
|  29221 | c8:ff:77:be:03:6c |             0 |           4 | VX2-KR-KFA7189A |
|  22618 | c8:ff:77:c0:ae:dc |             0 |           4 | A2N-KR-KGA0329A |
|   4071 | c8:ff:77:c2:3b:85 |             0 |           4 | VS3-US-KHB1290A |
|  33357 | c8:ff:77:c5:3b:57 |             0 |           4 | VT8-KR-MBA1557A |
|  37243 | c8:ff:77:c5:b0:87 |             0 |           4 | VT8-KR-KNA5358A |
|  18118 | c8:ff:77:c8:d6:87 |             0 |           4 | ZZ4-US-KMB1319A |
|  78438 | c9:a2:50:65:85:0d |             1 |           4 | F6V-US-NKA0114A |
|  79042 | c9:a2:50:65:85:0d |             1 |          27 | F6V-US-NKA0114A |
|  78440 | ca:89:d1:32:6d:f1 |             1 |           4 | E5R-US-RMA0290A |
|  94665 | ca:89:d1:32:6d:f1 |             1 |          27 | E5R-US-RMA0290A |
|  20477 | f5:03:67:6e:cc:03 |             1 |           4 | E5H-KR-NBA0032A |
|  33665 | f6:e8:32:82:e1:9a |             1 |           4 | E5H-KR-NBA0017A |
+--------+------------------+--------------+-------------+-----------------+
```

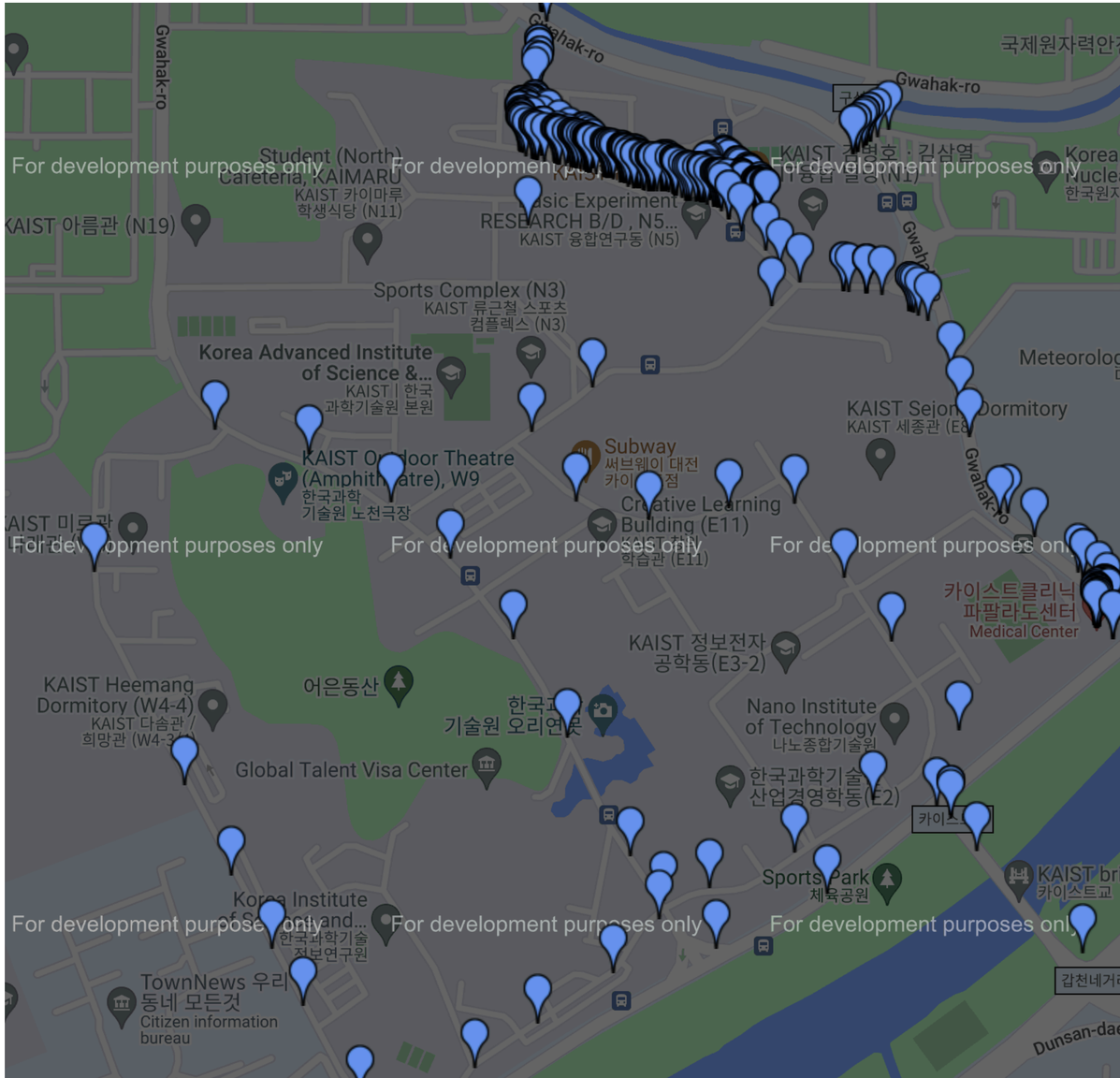
:2d:db:a0	0	27	K1M-US-RGA1542A
:44:27:1d	0	27	ZZ4-US-PAA2610A
:55:e3:fe	0	4	K3X-US-PHA0445A
:58:5f:4e	0	4	K1H-KR-PMA0645A
:58:62:3e	0	4	K1H-KR-PMA0501A
:5a:98:08	0	4	K3M-KR-PJA0452A
:67:6a:6a	0	4	K2K-KR-PMA0980A
:69:9e:44	0	4	K1M-US-REA0055A
:6c:51:0a	0	27	X6K-US-RHA0425A
:88:76:66	0	4	YN1-US-MHA0492A
:8d:78:cf	0	4	E1J-KR-MKA0180A
:90:f1:ee	0	4	ZZ4-US-MNA3159A
:96:96:48	0	4	VS9-EU-NFA8472A
:99:c0:da	0	4	F5N-US-NHA2866A
:99:c0:da	0	27	F5N-US-NHA2866A
:9a:0d:a0	0	4	ZZ4-US-NHA0899A
:be:03:6c	0	4	VX2-KR-KFA7189A
:c0:ae:dc	0	4	A2N-KR-KGA0329A
:c2:3b:85	0	4	VS3-US-KHB1290A
:c5:3b:57	0	4	VT8-KR-MBA1557A

:2d:db:a0	0	27	K1M-US-RGA1542A
:44:27:1d	0	27	ZZ4-US-PAA2610A
:55:e3:fe	0	4	K3X-US-PHA0445A
:58:5f:4e	0	4	K1H-KR-PMA0645A
:58:62:3e	0	4	K1H-KR-PMA0501A
:5a:98:08	0	4	K3M-KR-PJA0452A
:67:6a:6a	0	4	K2K-KR-PMA0980A
:69:9e:44	0	4	K1M-US-REA0055A
:6c:51:0a	0	27	X6K-US-RHA0425A
:88:76:66	0	4	YN1-US-MHA0492A
:8d:78:cf	0	4	E1J-KR-MKA0180A
:90:f1:ee	0	4	ZZ4-US-MNA3159A
:96:96:48	0	4	VS9-EU-NFA8472A
:99:c0:da	0	4	F5N-US-NHA2866A
:99:c0:da	0	27	F5N-US-NHA2866A
:9a:0d:a0	0	4	ZZ4-US-NHA0899A
:be:03:6c	0	4	VX2-KR-KFA7189A
:c0:ae:dc	0	4	A2N-KR-KGA0329A
:c2:3b:85	0	4	VS3-US-KHB1290A
:c5:3b:57	0	4	VT8-KR-MBA1557A

South Korea - Daejeon

KAIST

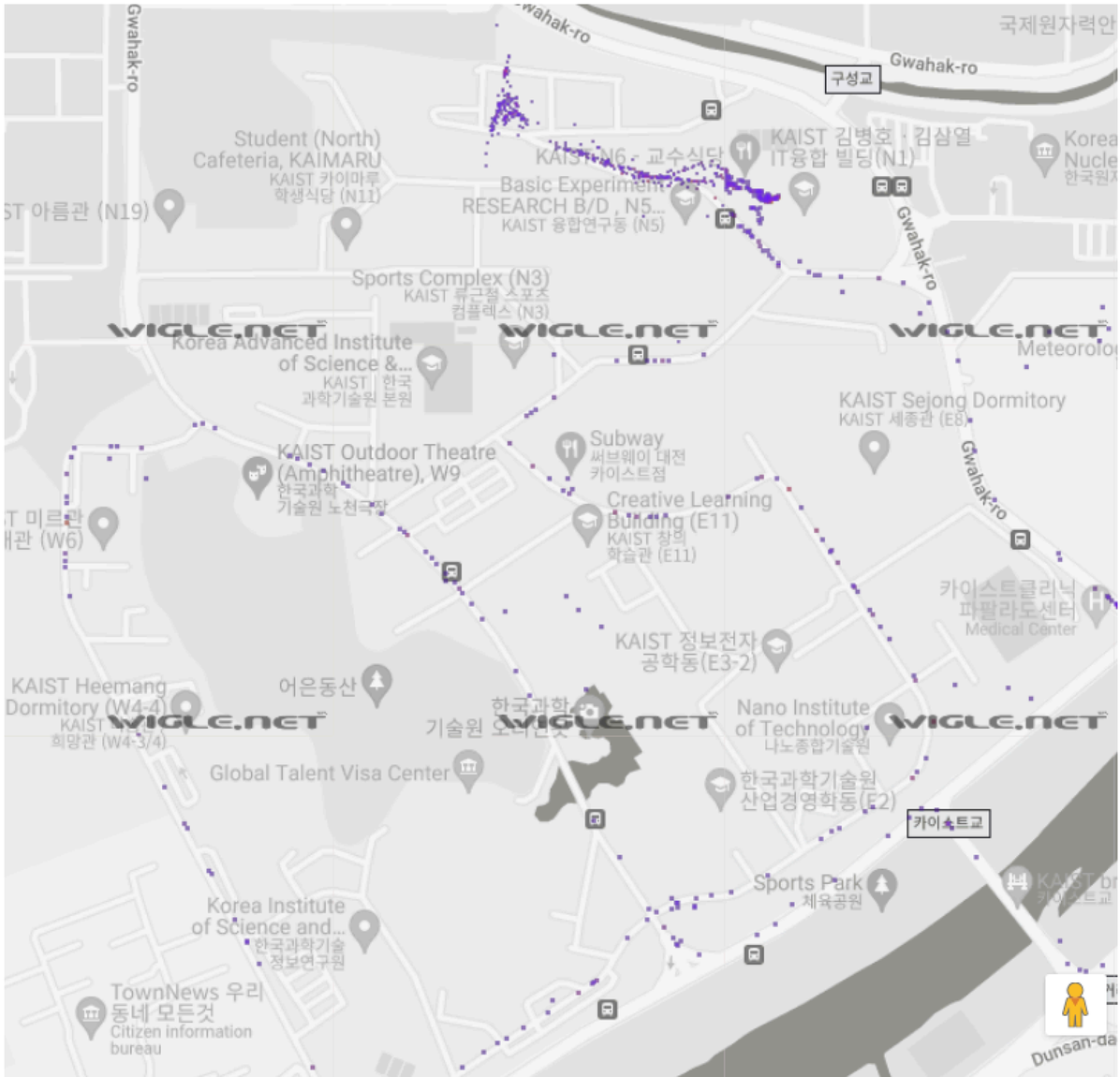
- Regex: ^IVT-[A-F0-9]{4}$



South Korea - Daejeon

KAIST

- Regex: ^IVT-[A-F0-9]{4}$

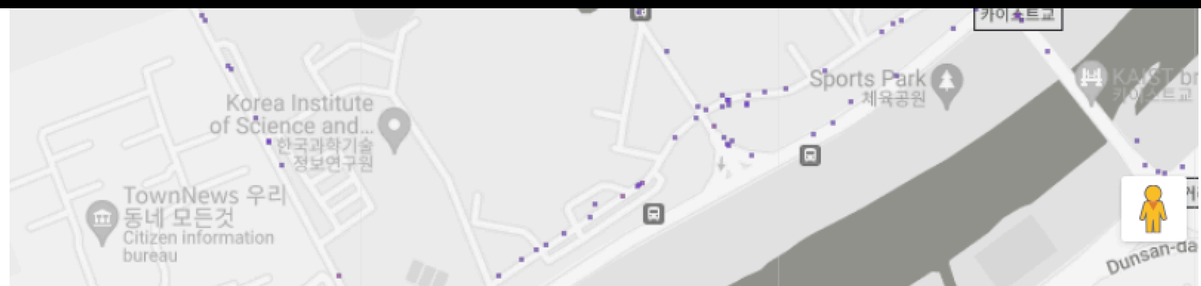


South Korea - Daejeon

KAIST

- Regex: ^IVT-[A-F0-9]{4}$

```
Company Name by IEEE OUI (74:f0:7d): BnCOM Co.,Ltd

No BTC Extended Inquiry Result Device info.

DeviceName: IVT-125F
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
        This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

No UUID16s found.

Transmit Power: 8dB
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
        This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
```

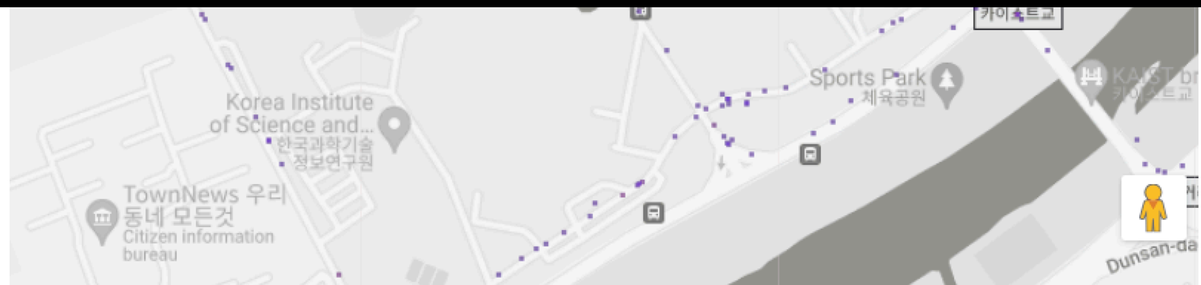


South Korea - Daejeon

KAIST

- Regex: ^IVT-[A-F0-9]{4}$

```
Company Name by IEEE OUI (74:f0:7d): BnCOM Co.,Ltd

No BTC Extended Inquiry Result Device info.

DeviceName: IVT-125F
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
        This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

No UUID16s found.

Transmit Power: 8dB
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
        This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
```

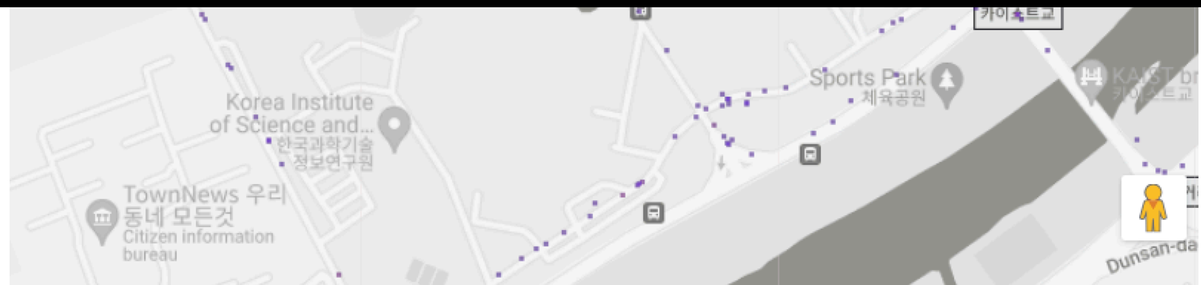


South Korea - Daejeon

KAIST

- Regex: ^IVT-[A-F0-9]{4}$

```
Company Name by IEEE OUI (74:f0:7d): BnCOM Co.,Ltd

No BTC Extended Inquiry Result Device info.

DeviceName: IVT-125F
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
        This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

No UUID16s found.

Transmit Power: 8dB 👀
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
        This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
```

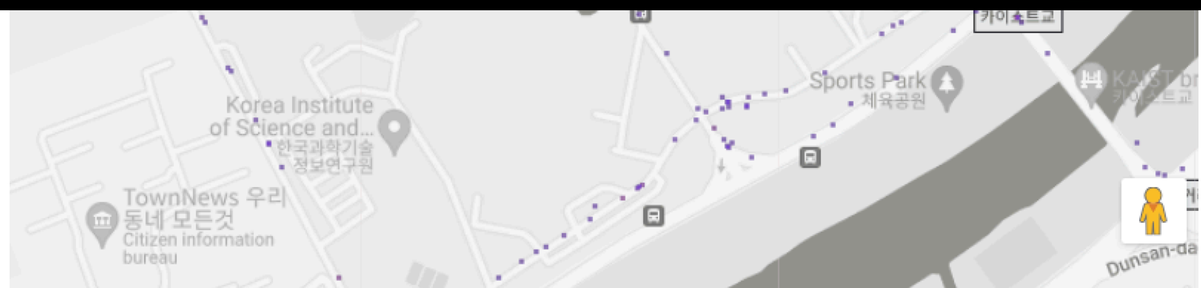


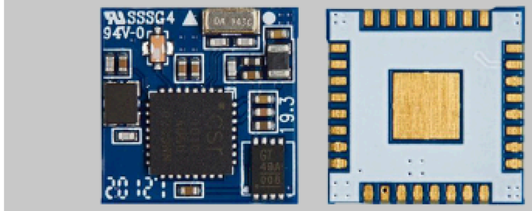
South Korea - Daejeon

KAIST

- Regex: ^IVT-[A-F0-9]{4}$

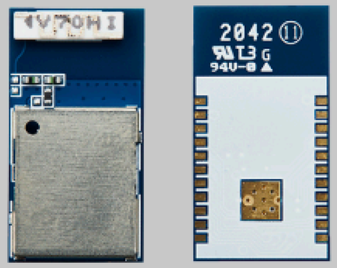
```
Company Name by IEEE OUI (74:f0:7d): BnCOM Co.,Ltd

No BTC Extended Inquiry Result Device info.

DeviceName: IVT-125F
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
        This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

No UUID16s found.

Transmit Power: 8dB
        In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
        This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
```





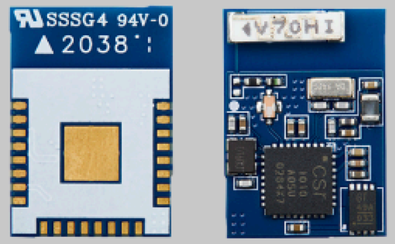
BCM-L101-A

v4.1/CSR1010
17 X 12 X 2



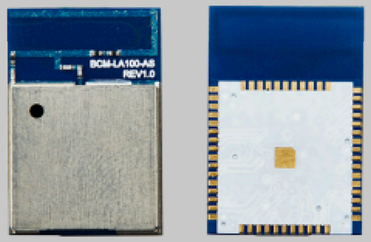
BCM-L102-A

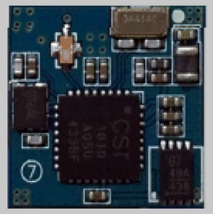
v4.1 / CSR1012
18.7 X 10 X 2.3

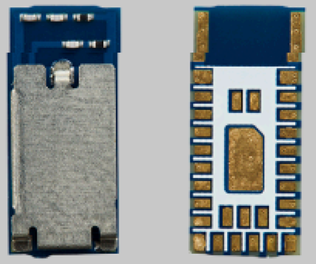


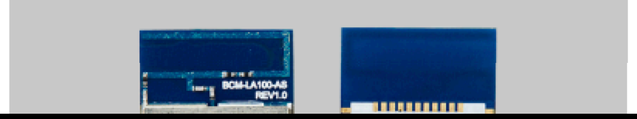
BCM-L101-A

v4.1 / CSR1010
17 X 12 X 2









```
For bdaddr = 74:f0:7d:12:74:a9:
        Company Name by IEEE OUI (74:f0:7d): BnCOM Co.,Ltd

        No BTC Extended Inquiry Result Device info.

        DeviceName: BCM-LN300-AS
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
```

BCM-LA100-AS

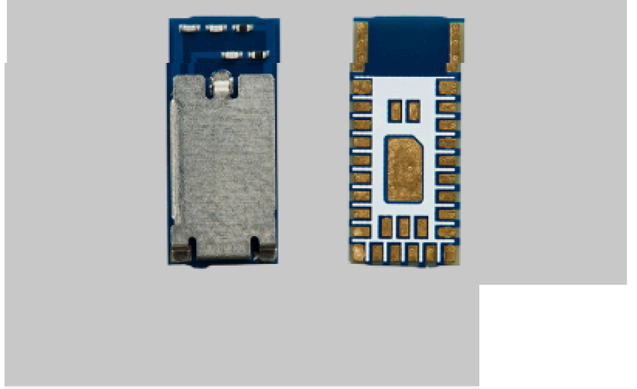
Ver5.0 / Airoha AB1611

11 X 16 X 2.5

BCM-L101

v4.1 / CSR1010

12 X 12 X 2



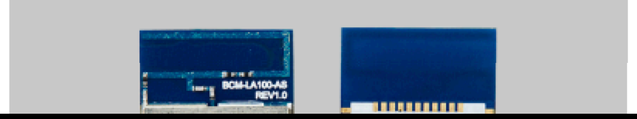
BCM-LN100-AS

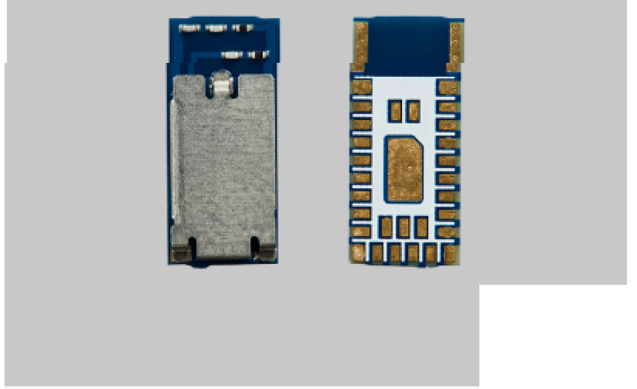
v5.2 / nRF52832

5 x 11 x 1.63

BCM-LN200-AS

v5.2 / nRF52810





```
For bdaddr = 74:f0:7d:12:74:a9:
        Company Name by IEEE OUI (74:f0:7d): BnCOM Co.,Ltd

        No BTC Extended Inquiry Result Device info.

        DeviceName: BCM-LN300-AS
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
```

BCM-LA100-AS

Ver5.0 / Airoha AB1611

11 X 16 X 2.5

BCM-L101

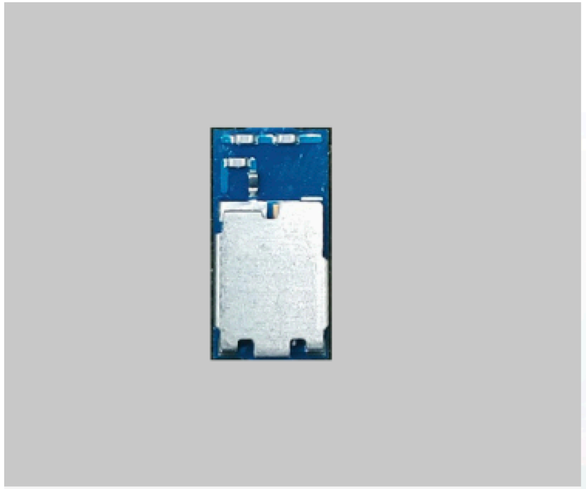
v4.1 / CSR1010

12 X 12 X 2

BCM-LN100-AS

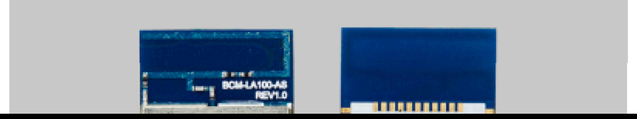
v5.2 / nRF52832

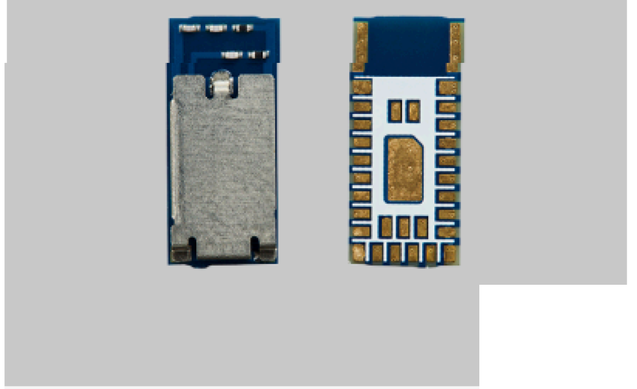
5 x 11 x 1.63



BCM-LN200-AS

v5.2 / nRF52810





```
For bdaddr = 74:f0:7d:12:74:a9:
        Company Name by IEEE OUI (74:f0:7d): BnCOM Co.,Ltd

        No BTC Extended Inquiry Result Device info.

        DeviceName: BCM-LN300-AS
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
```

BCM-LA100-AS

Ver5.0 / Airoha AB1611

11 X 16 X 2.5

BCM-L101

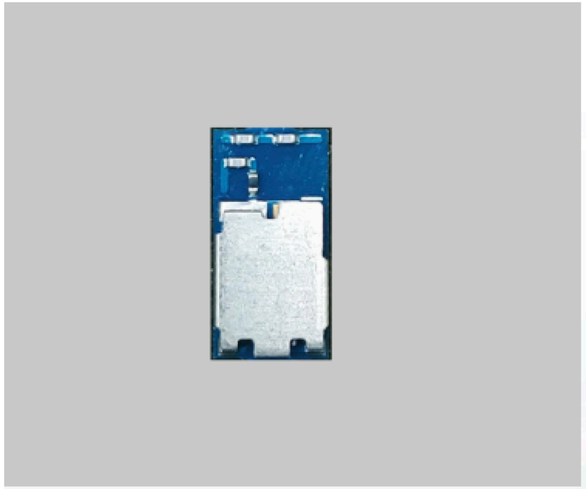
v4.1 / CSR1010

12 X 12 X 2

BCM-LN100-AS

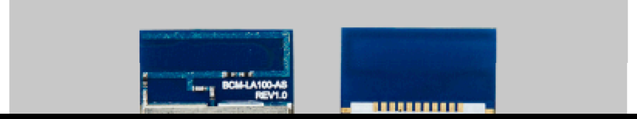
v5.2 / nRF52832

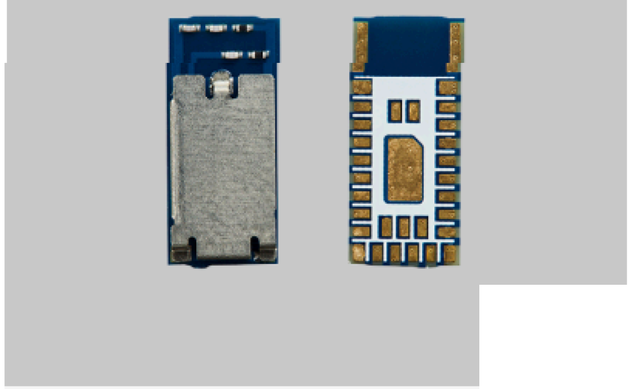
5 x 11 x 1.63



BCM-LN200-AS

v5.2 / nRF52810





```
For bdaddr = 74:f0:7d:12:74:a9:
        Company Name by IEEE OUI (74:f0:7d): BnCOM Co.,Ltd

        No BTC Extended Inquiry Result Device info.

        DeviceName: BCM-LN300-AS
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
```

BCM-LA100-AS

Ver5.0 / Airoha AB1611

11 X 16 X 2.5

BCM-L101

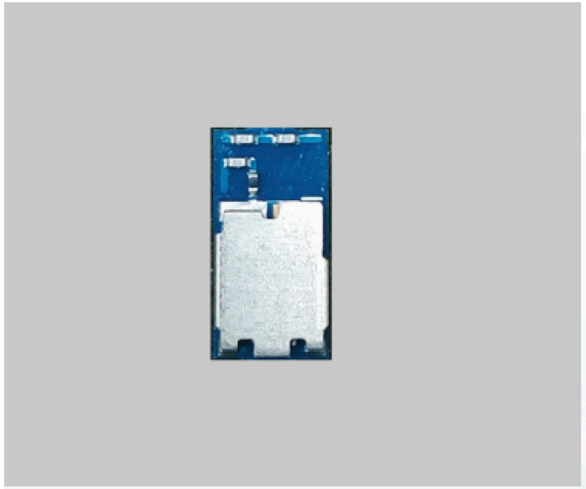
v4.1 / CSR1010

12 X 12 X 2

BCM-LN100-AS

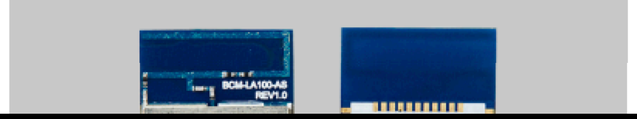
v5.2 / nRF52832

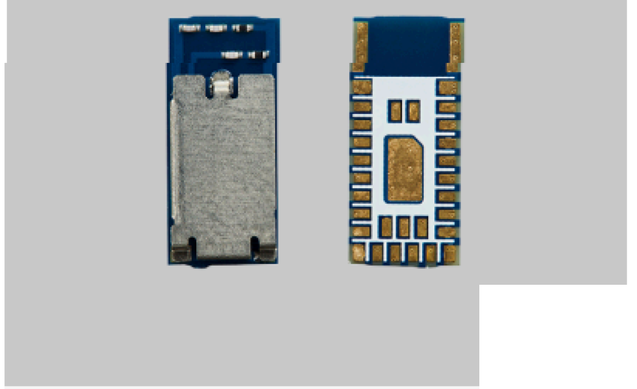
5 x 11 x 1.63



BCM-LN200-AS

v5.2 / nRF52810





```
For bdaddr = 74:f0:7d:12:74:a9:
        Company Name by IEEE OUI (74:f0:7d): BnCOM Co.,Ltd

        No BTC Extended Inquiry Result Device info.

        DeviceName: BCM-LN300-AS
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
```

BCM-LA100-AS

Ver5.0 / Airoha AB1611

11 X 16 X 2.5

BCM-L101

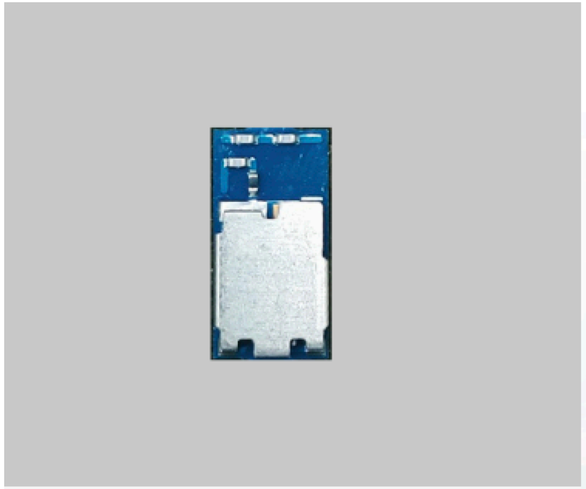
v4.1 / CSR1010

12 X 12 X 2

BCM-LN100-AS

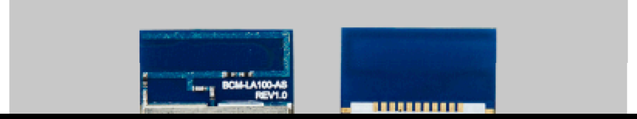
v5.2 / nRF52832

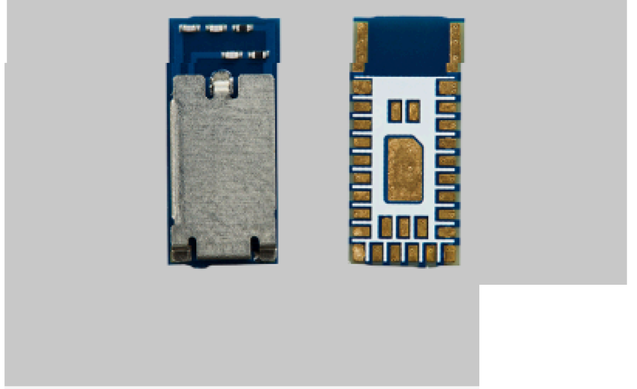
5 x 11 x 1.63



BCM-LN200-AS

v5.2 / nRF52810





```
For bdaddr = 74:f0:7d:12:74:a9:
        Company Name by IEEE OUI (74:f0:7d): BnCOM Co.,Ltd

        No BTC Extended Inquiry Result Device info.

        DeviceName: BCM-LN300-AS
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
```

BCM-LA100-AS

Ver5.0 / Airoha AB1611

11 X 16 X 2.5

BCM-L101

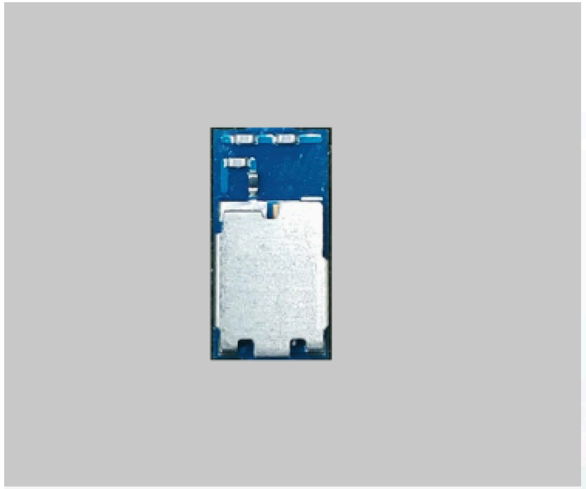
v4.1 / CSR1010

12 X 12 X 2

BCM-LN100-AS

v5.2 / nRF52832

5 x 11 x 1.63

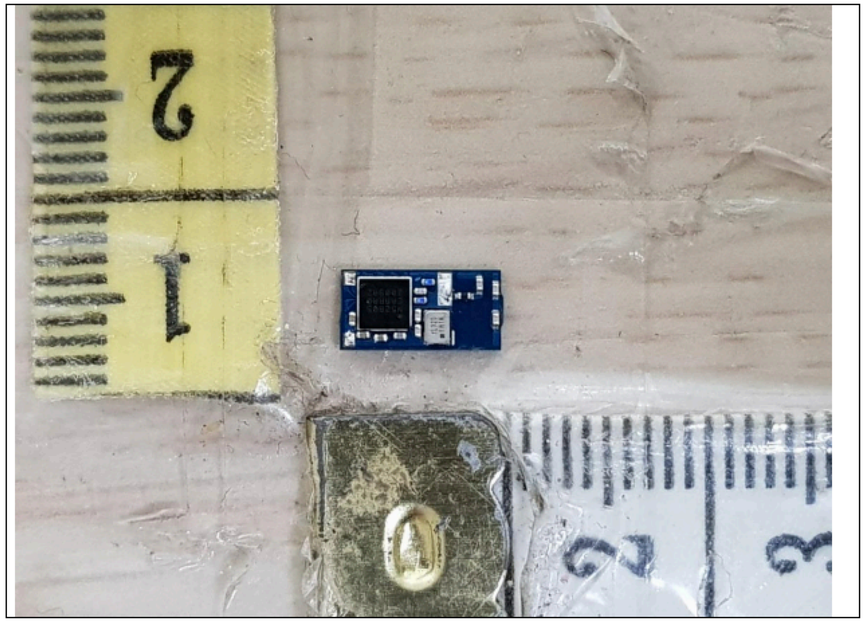


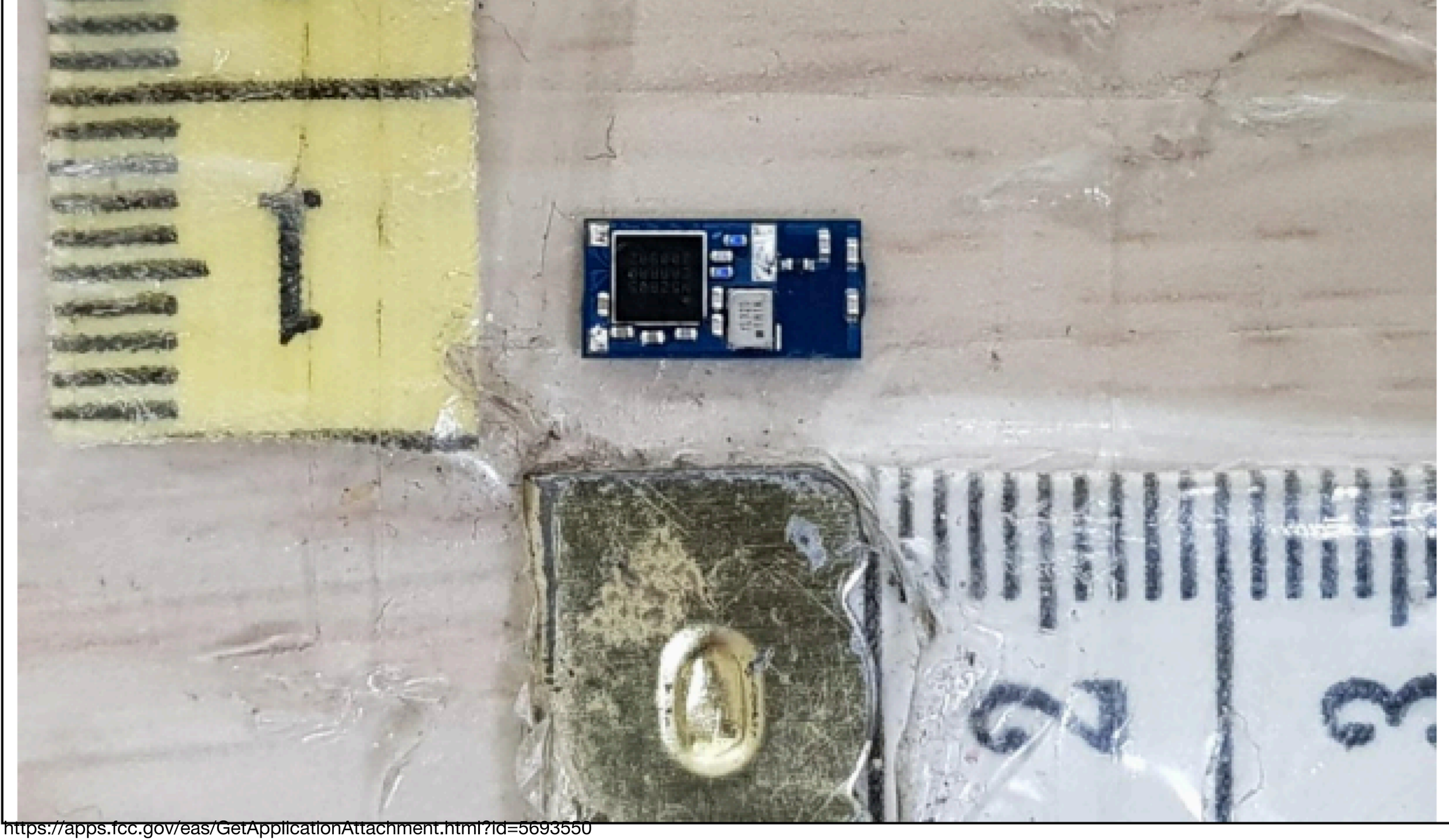
BCM-LN200-AS

v5.2 / nRF52810

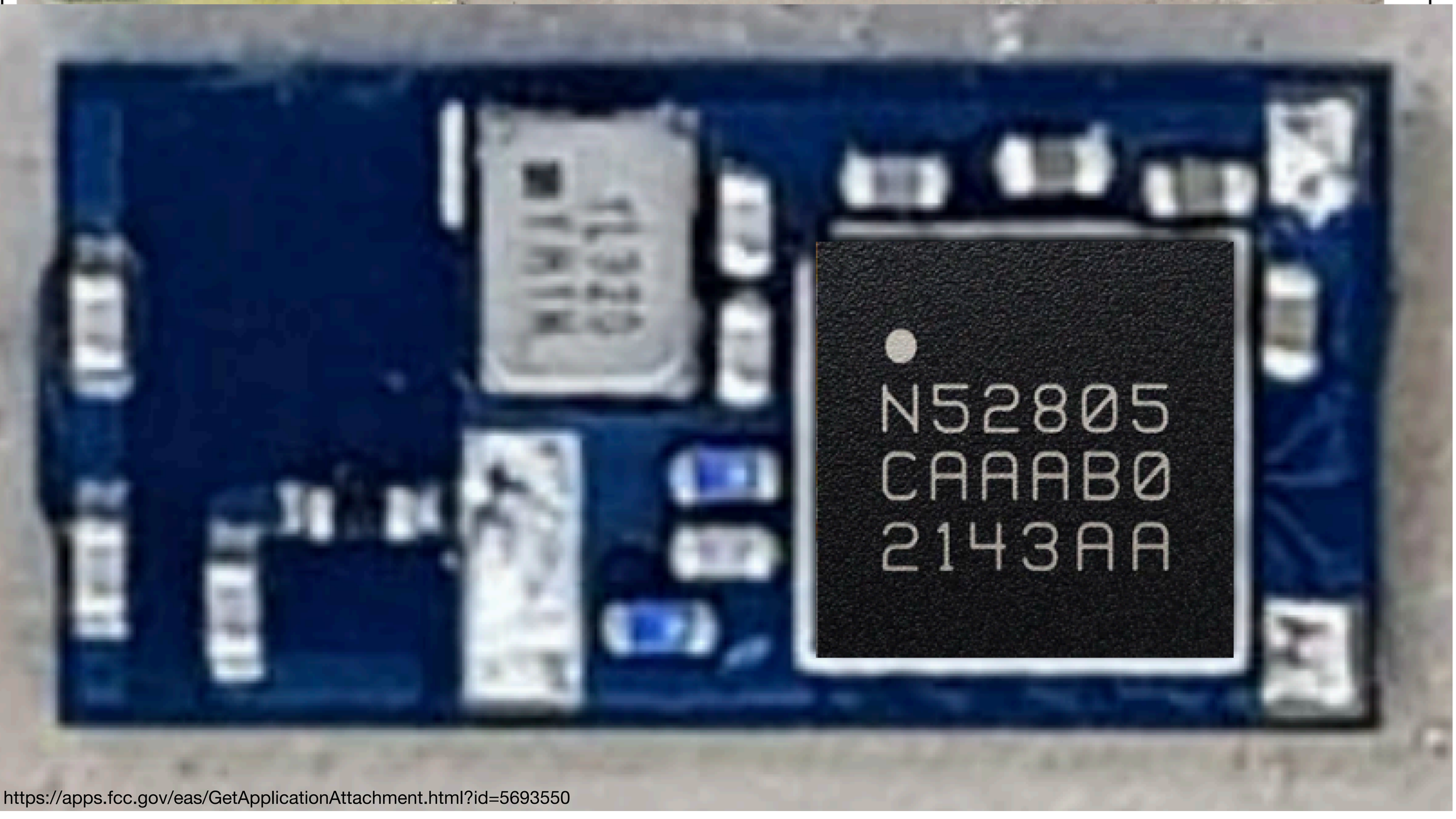
FCC ID: 2APDI-BCM-LN300-AS

Main Board Front





https://apps.fcc.gov/eas/GetApplicationAttachment.html?id=5693550



https://apps.fcc.gov/eas/GetApplicationAttachment.html?id=5693550

Mini-Takeaway

Chip identification

- FCC "Internal Photos" pictures can be used to identify chips for devices *in some cases*
  - And which chip a device is using, is one of the things I want to know!

End - Anecdotes - Locations

Takeaways 1

- *Bluetooth sniffing goals are different from WiFi goals*, and consequently the sniffing tech is under-developed to help with those goals
- When there's a BT FW bug, **no one knows what all it affects**

Takeaways 2

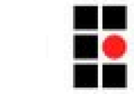
- There are lots of devices that are advertising names, but it's not clear what they are
  - I'm looking at you **"*SVE5CLAG[0-9]{9}*"**
  - Somebody ought to start a database! Or at least a wiki?!

Begin - Anecdotes - Devices

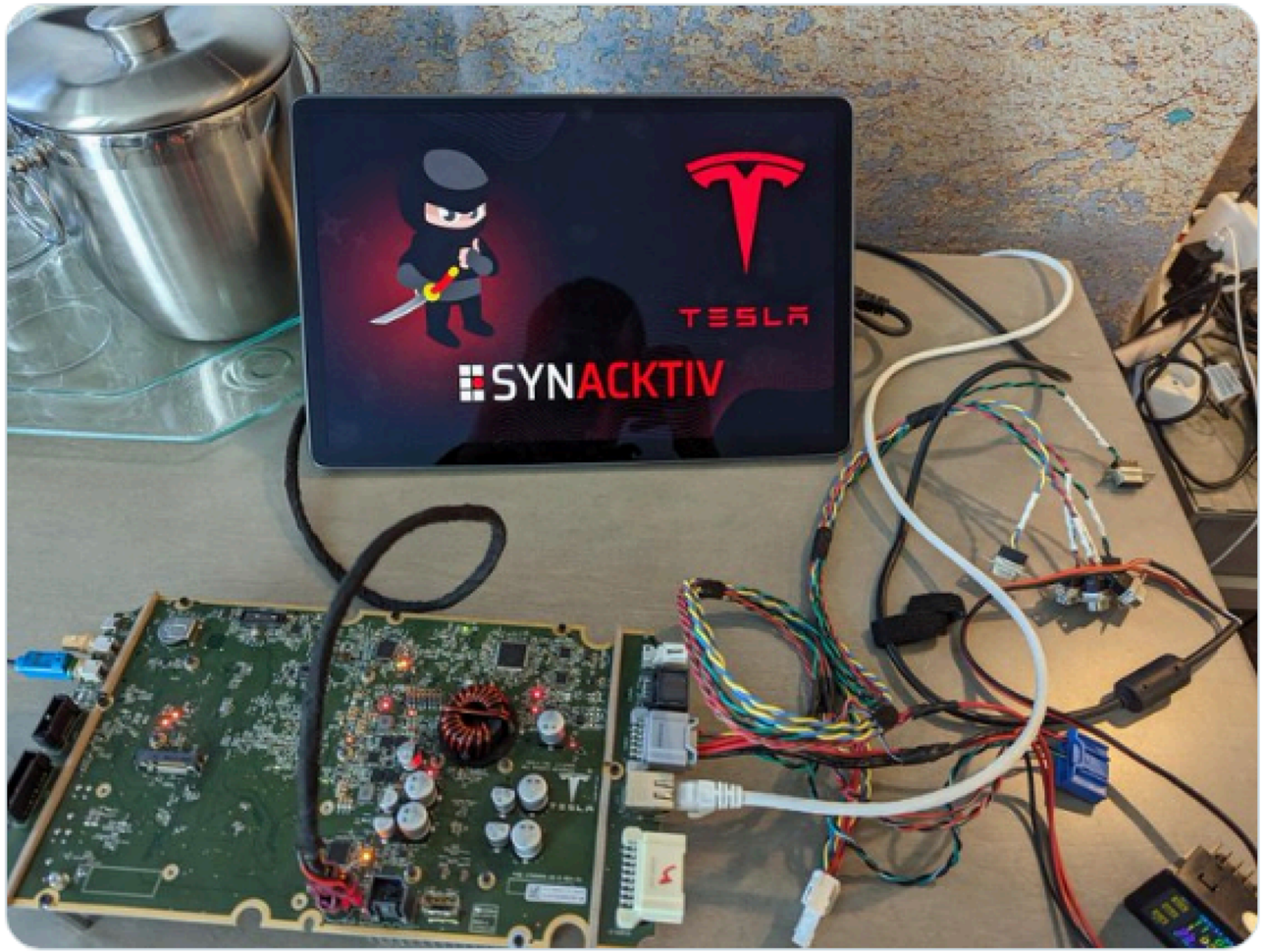
Teslas

- "Random static" BDADDR (that has never changed on my Model 3)
- Non-randomized advertised name
  - Regex: ^S[0-9a-f]{16}C$ e.g. S83952932d49bc8aeC
  - Semantically: the [0-9a-f]{16} is *part of the SHA hash of the VIN*
    - https://trifinite.org/Downloads/20220916_tempa_presentation_sec-t_public.pdf
- https://teslaradar.com/ to crowdsource Tesla tracking
  - But don't use that, use WiGLE instead!

Teslas

Synacktiv 
@Synacktiv

After having finished their exploit in an hotel room, @_p0ly_ and @vdehors successfully compromised the Tesla Model 3 infotainment through bluetooth and elevated their privileges to root!
Combined with the previous entry, this could have been a full chain to take over the car!

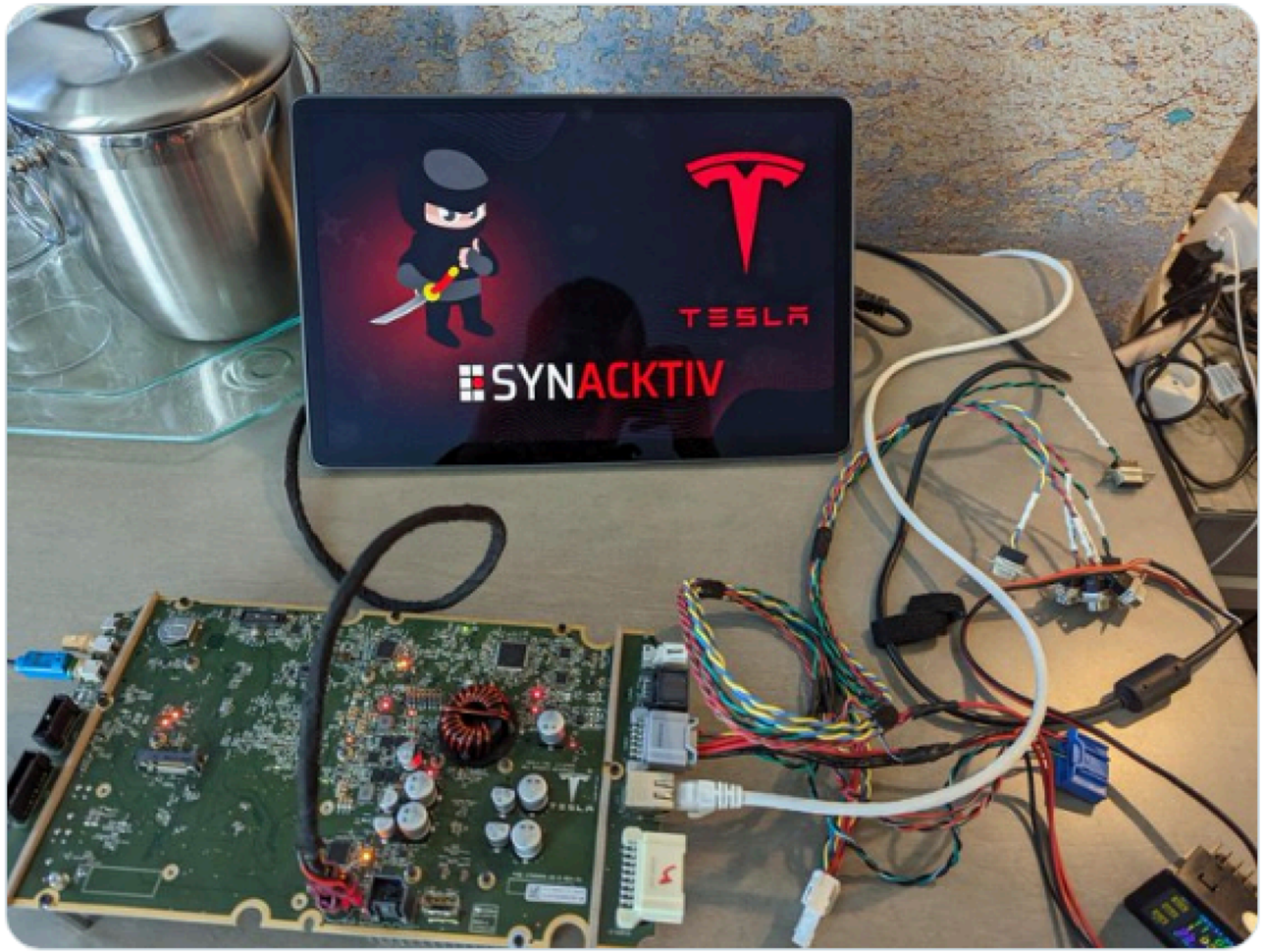


https://twitter.com/Synacktiv/status/1638996681260781574

Teslas

Synacktiv
@Synacktiv

After having finished their exploit in an hotel room, @_p0ly_ and @vdehors successfully compromised the Tesla Model 3 infotainment through bluetooth and elevated their privileges to root!
Combined with the previous entry, this could have been a full chain to take over the car!



https://twitter.com/Synacktiv/status/1638996681260781574

Lexus

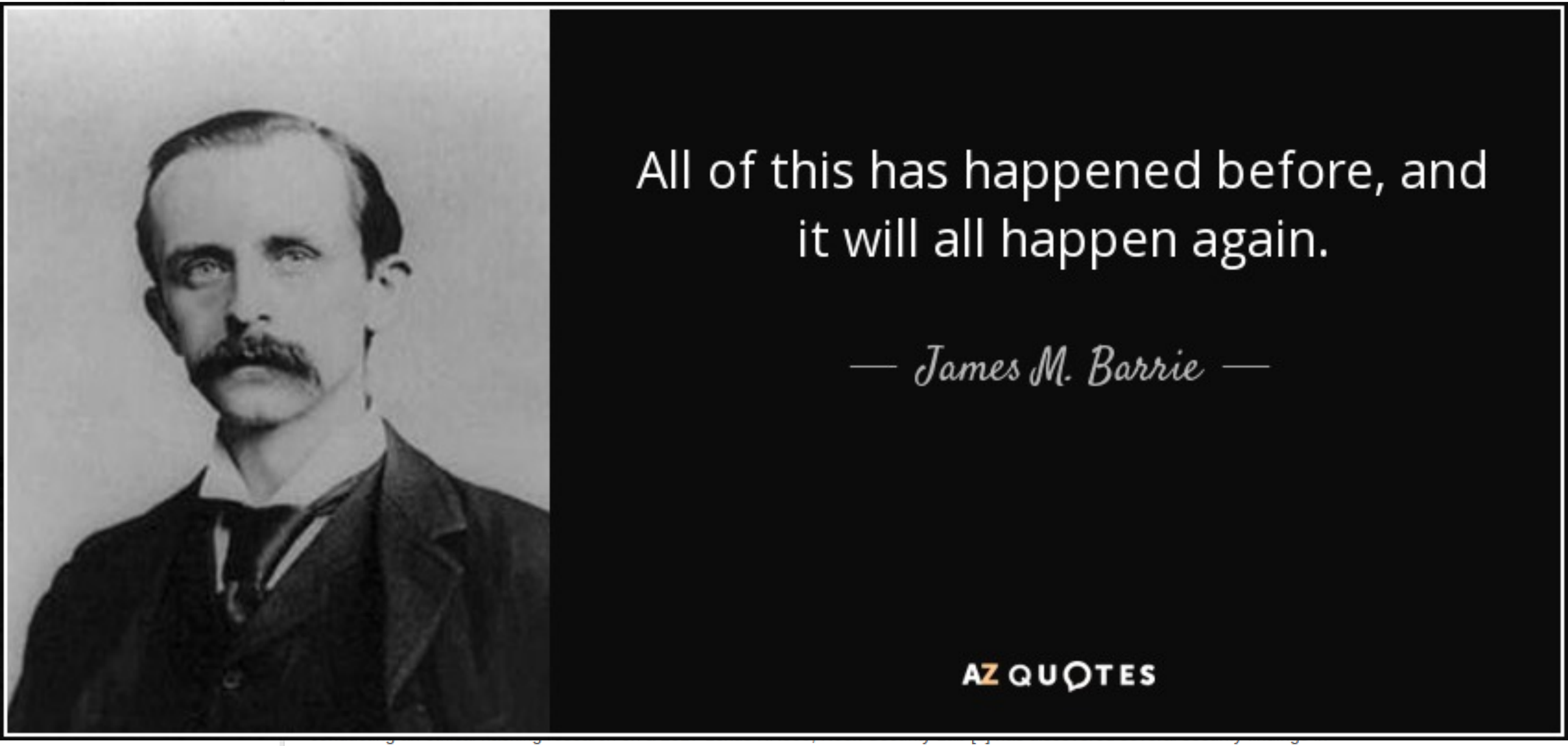
2020-03-30

Tencent Keen Security Lab: Experimental Security Assessment on Lexus Cars

by Tencent Keen Security Lab

Since 2017, Lexus has equipped several models (including Lexus NX, LS and ES series) with a new generation infotainment, which is also known as AVN (Audio, Visual and Navigation) unit. Compared to some Intelligent connected infotainment units, like Tesla IVI and BMW ConnectedDrive system, the new Lexus AVN unit seems to be a bit more traditional. From a security perspective, it may highly reduce the possibility of being attacked by potential cybersecurity issues. But a new system is always introducing new security risks. After conducting an ethical hacking research on a 2017 Lexus NX300, Keen Security Lab [1] has discovered several security findings in Bluetooth and vehicular diagnosis functions on the car, which would compromise AVN unit, internal CAN network and related ECUs. By

https://keenlab.tencent.com/en/2020/03/30/Tencent-Keen-Security-Lab-Experimental-Security-Assessment-on-Lexus-Cars/



Bluetooth and vehicular diagnosis functions on the car, which would compromise AVN unit, internal CAN network and related ECUs. By

https://keenlab.tencent.com/en/2020/03/30/Tencent-Keen-Security-Lab-Experimental-Security-Assessment-on-Lexus-Cars/

All of this has happened before, and it will all happen again.

— James M. Barrie —

AZ QUOTES

Bluetooth and vehicular diagnosis functions on the car, which would compromise AVN unit, internal CAN network and related ECUs. By

https://keenlab.tencent.com/en/2020/03/30/Tencent-Keen-Security-Lab-Experimental-Security-Assessment-on-Lexus-Cars/

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

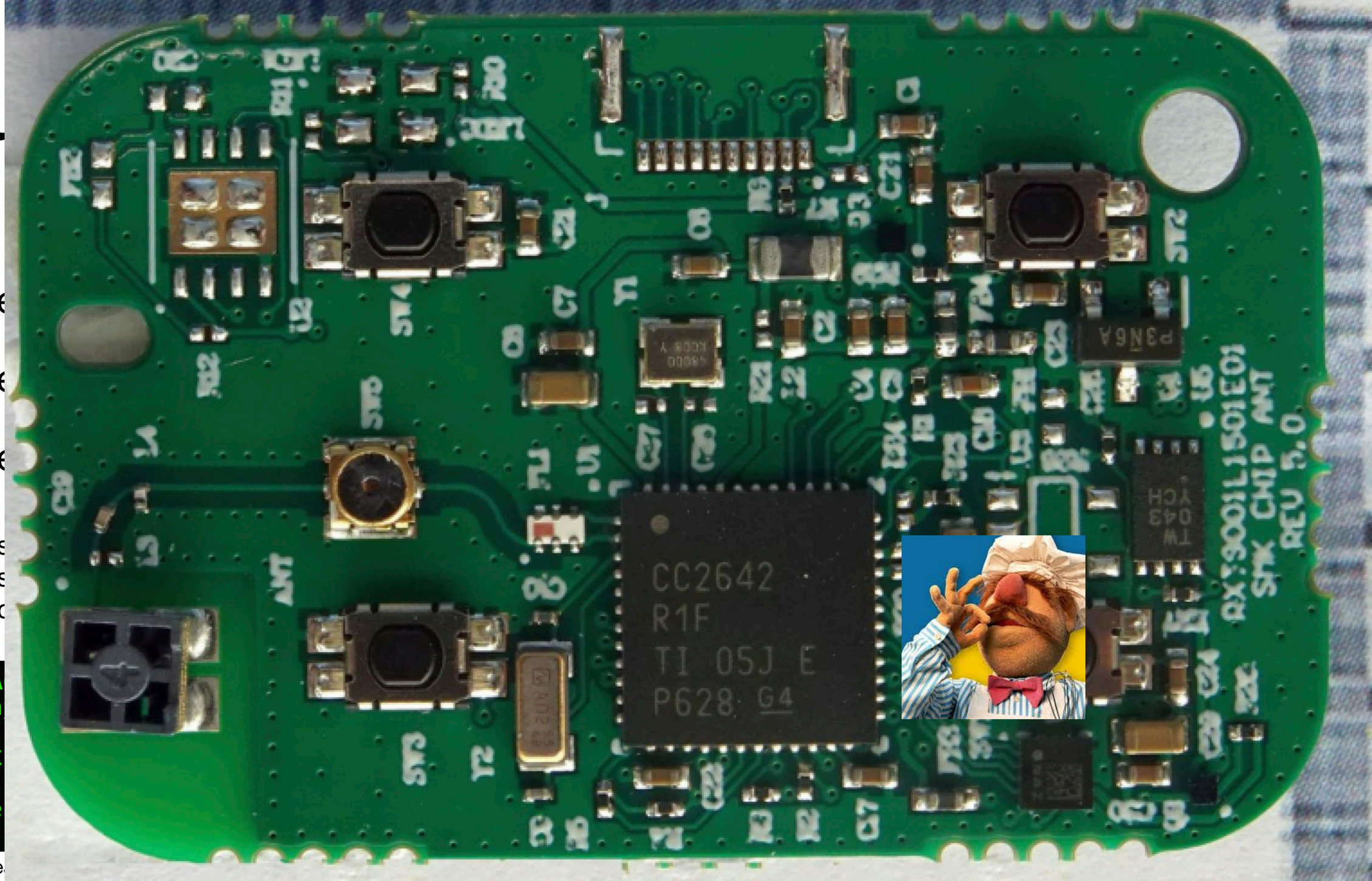
E Tu

- Rege
- Rege
- Rege

Address
Address
Name (c

```
For bdaddr = A
        Compan

        No BTC

        Device
```

https://apps.fcc.gov/e



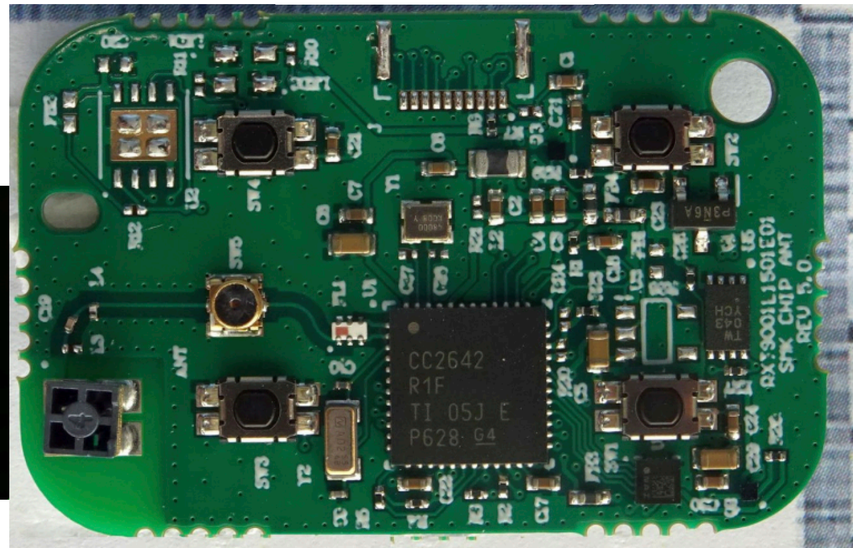
E Tu Rivian?

- 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)
```

Rivian Key Fob



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

Other Car Things

- Regex: "^Tesla Model S.*", "^Tesla Model X.*" e.g. "Tesla Model S IDRISS"
- Regex: "^TOYOTA 4Runner$", "^TOYOTA Camry$", "^TOYOTA Corolla$", "^TOYOTA Highlander$", "^TOYOTA Rav 4$", "^TOYOTA RAV4$", "^TOYOTA SIENNA$"
- Regex: "^GM_PEPS_VKM$", "^GM_PEPS_VKM[1234]$"
- Regex: "^Audi_MMI_[0-9]{4}$", "^Audi MMI [0-9]{4}$"
- Regex: "^VW BT [0-9]{4}$"
- Regex: "^Porsche BT [0-9]{4}$"
- Regex: "^Polestar2$"

Other Car Things

- Regex: "^Tesla Model S.*", "^Tesla Model X.*" e.g. "Tesla Model S IDRISS"

- Regex: "^TOYOTA 4Runner$", "^TOYOTA Camry$", "^TOYOTA Corolla$", "^TOYOTA Highlander$", "^TOYOTA Rav 4$", "^TOYOTA RAV4$", "^TOYOTA SIENNA$"

- Regex: "^GM_PEPS_VKM$", "^GM_PEPS_VKM[1234]$"

- Regex: "^Audi_MMI_[0-9]{4}$", "^Audi MMI [0-9]{4}$"

- Regex: "^VW BT [0-9]{4}$"

- Regex: "^Porsche BT [0-9]{4}$"

- Regex: "^Polestar2$"

Surveillance Cameras

Google Nest

- Regex: ^Nest Cam$
- Regex: ^N[A-Z0-9]{4}$ e.g. N0037

Surveillance Cameras

Google Nest

- Regex: ^Nest Cam$
- Regex: ^N[A-Z0-9]{4}$ e.g. N0037

> HCI Event: LE Meta Event (0x3e) plen 26
LE Advertising Report (0x02)
Num reports: 1
Event type: Connectable undirected - ADV_IND (0x00)
Address type: *Random* (0x01)
Address: 42:39:35:69:EC:22 (*Resolvable*)
Data length: 14
Flags: 0x02
LE General Discoverable Mode
16-bit Service UUIDs (partial): 1 entry
Nest Labs Inc. (0xfeaf)
Name (complete): **N0037**
RSSI: -90 dBm (0xa6)

> HCI Event: LE Meta Event (0x3e) plen 26
LE Advertising Report (0x02)
Num reports: 1
Event type: Connectable undirected - ADV_IND (0x00)
Address type: *Random* (0x01)
Address: 78:4E:57:0D:C4:22 (*Resolvable*)
Data length: 14
Flags: 0x02
LE General Discoverable Mode
16-bit Service UUIDs (partial): 1 entry
Nest Labs Inc. (0xfeaf)
Name (complete): **N6ANS**
RSSI: -93 dBm (0xa3)

Surveillance Cameras

Google Nest

- Regex: ^Nest Cam$
- Regex: ^N[A-Z0-9]{4}$ e.g. N0037

> HCI Event: LE Meta Event (0x3e) plen 26
LE Advertising Report (0x02)
Num reports: 1
Event type: Connectable undirected - ADV_IND (0x00)
Address type: *Random* (0x01)
Address: 42:39:35:69:EC:22 (*Resolvable*)
Data length: 14
Flags: 0x02
LE General Discoverable Mode
16-bit Service UUIDs (partial): 1 entry
Nest Labs Inc. (0xfeaf)
Name (complete): **N0037**
RSSI: -90 dBm (0xa6)

> HCI Event: LE Meta Event (0x3e) plen 26
LE Advertising Report (0x02)
Num reports: 1
Event type: Connectable undirected - ADV_IND (0x00)
Address type: *Random* (0x01)
Address: 78:4E:57:0D:C4:22 (*Resolvable*)
Data length: 14
Flags: 0x02
LE General Discoverable Mode
16-bit Service UUIDs (partial): 1 entry
Nest Labs Inc. (0xfeaf)
Name (complete): **N6ANS**
RSSI: -93 dBm (0xa3)

Surveillance Cameras

Google Nest

- Regex: ^Nest Cam$
- Regex: ^N[A-Z0-9]{4}$ e.g. N0037

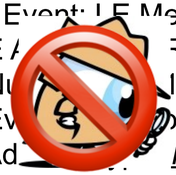
```
> HCI Event: LE Meta Event (0x3e) plen 26
      LE Advertising Report (0x02)
        Num reports: 1
        Event type: Connectable undirected - ADV_IND (0x00)
        Address type: Random (0x01)
        Address: 42:39:35:69:EC:22 (Resolvable)
        Data length: 14
        Flags: 0x02
          LE General Discoverable Mode
        16-bit Service UUIDs (partial): 1 entry
          Nest Labs Inc. (0xfeaf)
        Name (complete): N0037
        RSSI: -90 dBm (0xa6)
```

```
> HCI Event: LE Meta Event (0x3e) plen 26
      LE Advertising Report (0x02)
        Num reports: 1
        Event type: Connectable undirected - ADV_IND (0x00)
        Address type: Random (0x01)
        Address: 78:4E:57:0D:C4:22 (Resolvable)
        Data length: 14
        Flags: 0x02
          LE General Discoverable Mode
        16-bit Service UUIDs (partial): 1 entry
          Nest Labs Inc. (0xfeaf)
        Name (complete): N6ANS
        RSSI: -93 dBm (0xa3)
```

Surveillance Cameras

Google Nest

- Regex: ^Nest Cam$
- Regex: ^N[A-Z0-9]{4}$ e.g. N0037



```
> HCI Event: LE Meta Event (0x3e) plen 26
    LE Advertising Report (0x02)
      Num reports: 1
      Event type: Connectable undirected - ADV_IND (0x00)
      Address type: Random (0x01)
      Address: 42:39:35:69:EC:22 (Resolvable)
      Data length: 14
      Flags: 0x02
        LE General Discoverable Mode
      16-bit Service UUIDs (partial): 1 entry
        Nest Labs Inc. (0xfeaf)
      Name (complete): N0037
      RSSI: -90 dBm (0xa6)
```

```
> HCI Event: LE Meta Event (0x3e) plen 26
    LE Advertising Report (0x02)
      Num reports: 1
      Event type: Connectable undirected - ADV_IND (0x00)
      Address type: Random (0x01)
      Address: 78:4E:57:0D:C4:22 (Resolvable)
      Data length: 14
      Flags: 0x02
        LE General Discoverable Mode
      16-bit Service UUIDs (partial): 1 entry
        Nest Labs Inc. (0xfeaf)
      Name (complete): N6ANS
      RSSI: -93 dBm (0xa3)
```

Where in the world is Nest 0001?

Surveillance Cameras

Google Nest

- Regex: ^Nest Cam$
- Regex: ^N[A-Z0-9]{4}$ e.g. N0037

```
> HCI Event: LE Meta Event (0x3e) plen 26
    LE Advertising Report (0x02)
      Num reports: 1
      Event type: Connectable undirected - ADV_IND (0x00)
      Address type: Random (0x01)
      Address: 42:39:35:69:EC:22 (Resolvable)
      Data length: 14
      Flags: 0x02
        LE General Discoverable Mode
      16-bit Service UUIDs (partial): 1 entry
        Nest Labs Inc. (0xfeaf)
      Name (complete): N0037
      RSSI: -90 dBm (0xa6)
```

```
> HCI Event: LE Meta Event (0x3e) plen 26
    LE Advertising Report (0x02)
      Num reports: 1
      Event type: Connectable undirected - ADV_IND (0x00)
      Address type: Random (0x01)
      Address: 78:4E:57:0D:C4:22 (Resolvable)
      Data length: 14
      Flags: 0x02
        LE General Discoverable Mode
      16-bit Service UUIDs (partial): 1 entry
        Nest Labs Inc. (0xfeaf)
      Name (complete): N6ANS
      RSSI: -93 dBm (0xa3)
```

Where in the world is Nest 0001?

WiGLE data ->


```
"trilat": 44.85729218,
"trilong": -93.43252563,
"ssid": "N0001",
"qos": 0,
"transid": "20190615-00000",
"firsttime": "2019-06-15T17:00:00.000Z",
"lasttime": "2019-06-15T16:00:00.000Z",
"lastupdt": "2019-06-15T16:00:00.000Z",
"netid": "6c:06:d0:eb:7d:4d",
"type": "BLE",
"capabilities": [
  "Uncategorized"
],
"userfound": false,
"device": 7936,
"name": "N0001",
"country": "US",
"region": "MN",
"road": "Singletree Lane",
"city": "Eden Prairie",
"housenumber": "12300",
"postalcode": "55344"
```

Surveillance Cameras

Google Nest

- Regex: ^Nest Cam$
- Regex: ^N[A-Z0-9]{4}$ e.g. N0037

```
> HCI Event: LE Meta Event (0x3e) plen 26
    LE Advertising Report (0x02)
      Num reports: 1
      Event type: Connectable undirected - ADV_IND (0x00)
      Address type: Random (0x01)
      Address: 42:39:35:69:EC:22 (Resolvable)
      Data length: 14
      Flags: 0x02
        LE General Discoverable Mode
      16-bit Service UUIDs (partial): 1 entry
        Nest Labs Inc. (0xfeaf)
      Name (complete): N0037
      RSSI: -90 dBm (0xa6)
```

```
> HCI Event: LE Meta Event (0x3e) plen 26
    LE Advertising Report (0x02)
      Num reports: 1
      Event type: Connectable undirected - ADV_IND (0x00)
      Address type: Random (0x01)
      Address: 78:4E:57:0D:C4:22 (Resolvable)
      Data length: 14
      Flags: 0x02
        LE General Discoverable Mode
      16-bit Service UUIDs (partial): 1 entry
        Nest Labs Inc. (0xfeaf)
      Name (complete): N6ANS
      RSSI: -93 dBm (0xa3)
```

Where in the world is Nest 0001?

WiGLE data ->


```
"trilat": 35.68451691,
"trilong": 139.74157715,
"ssid": "N0001",
"qos": 0,
"transid": "20230223-00000",
"firsttime": "2023-02-23T16:00:00.000Z",
"lasttime": "2023-02-23T06:00:00.000Z",
"lastupdt": "2023-02-23T06:00:00.000Z",
"netid": "69:e3:a2:9a:1e:81",
"type": "BLE",
"capabilities": [
  "Misc"
],
"userfound": false,
"device": 0,
"name": "N0001",
"country": "JP",
"region": "麹町一丁目",
"road": "麹町学園通り",
"city": "千代田区",
"housenumber": null,
"postalcode": "102-0083"
```

Surveillance Cameras

Google Nest

- Regex: ^Nest Cam$
- Regex: ^N[A-Z0-9]{4}$ e.g. N0037

```
> HCI Event: LE Meta Event (0x3e) plen 26
    LE Advertising Report (0x02)
      Num reports: 1
      Event type: Connectable undirected - ADV_IND (0x00)
      Address type: Random (0x01)
      Address: 42:39:35:69:EC:22 (Resolvable)
      Data length: 14
      Flags: 0x02
        LE General Discoverable Mode
      16-bit Service UUIDs (partial): 1 entry
        Nest Labs Inc. (0xfeaf)
      Name (complete): N0037
      RSSI: -90 dBm (0xa6)
```

```
> HCI Event: LE Meta Event (0x3e) plen 26
    LE Advertising Report (0x02)
      Num reports: 1
      Event type: Connectable undirected - ADV_IND (0x00)
      Address type: Random (0x01)
      Address: 78:4E:57:0D:C4:22 (Resolvable)
      Data length: 14
      Flags: 0x02
        LE General Discoverable Mode
      16-bit Service UUIDs (partial): 1 entry
        Nest Labs Inc. (0xfeaf)
      Name (complete): N6ANS
      RSSI: -93 dBm (0xa3)
```

Where in the world is Nest 0001?

WiGLE data ->


```
"trilat": 52.28806686,
"trilong": -1.58548605,
"ssid": "N0001",
"qos": 0,
"transid": "20190505-00000",
"firsttime": "2019-05-05T15:00:00.000Z",,
"lasttime": "2019-05-05T07:00:00.000Z",
"lastupdt": "2023-03-08T14:00:00.000Z",
"netid": "68:ad:8f:18:f0:d3",
"type": "BLE",
"capabilities": [
  "Misc"
],
"userfound": false,
"device": 0,
"name": "N0001",
"country": "GB",
"region": "England",
"road": "Wathen Road",
"city": "Warwick",
"housenumber": null,
"postalcode": "CV34 5BG"
```

Mini-Takeaway

Vendor identification

- 16 bit service UUIDs are useful
  - *to associate products with vendors*
  - to differentiate between different products with similar names
- Filed tickets with WiGLE to request they be added

https://github.com/wiglenet/wigle-wifi-wardriving/issues/614
https://github.com/wiglenet/wigle-wifi-wardriving/issues/615
https://github.com/wiglenet/wigle-wifi-wardriving/issues/616

Flippers

- Regex: ^Flipper [A-Za-z0-9]{8}$ e.g. "Flipper Eironeoo"
- Flippers beaconing to find other Flippers? Or just because?
Bluetooth LE 5.0	TX Power: 0 dBm max
	RX Sensitivity: -96 dBm
	Data rate: 2 Mbps

https://flipperzero.one/

Flippers

- Regex: ^Flipper [A-Za-z0-9]{8}$ e.g. "Flipper Eironeoo"
- Flippers beaconing to find other Flippers? Or just because?
- **Bluetooth LE 5.0**

  TX Power: 0 dBm max

  RX Sensitivity: -96 dBm

  Data rate: 2 Mbps

https://flipperzero.one/

Flippers

- Regex: ^Flipper [A-Za-z0-
- Flippers beaconing to finc
- **Bluetooth LE 5.0**

Data rate: 2 Mbps

The Bluetooth Range Estimator

Calculate the expected range between two Bluetooth devices

Receiver Sensitivity (dBm)

select a Bluetooth PHY to see how it influences typical receiver sensitivity

EDR 3M | EDR 2M | BR 1M | LE 2M | **LE 1M** | LE 500K (CODED) | LE 125K (CODED)

-70 … -96 … -110

TYPICAL LE 1M

Path Loss

select a representative environment

Outdoor | Industrial | Office | Home

Transmit Power (dBm): -20 … 0 … 20

Transmitter Antenna Gain (dBi): -10 … 0 … 10

Receiver Antenna Gain (dBi): -10 … 0 … 10

Estimated Range

15 to 21 meters

https://www.bluetooth.com/learn-about-bluetooth/key-attributes/range/#estimator

https://flipperzero.one/

Flippers

- Regex: ^Flipper [A-Za-z0-9]{8}$ e.g. "Flipper Eironeoo"
- Flippers beaconing to find other Flippers? Or just because?
- **Bluetooth LE 5.0**

  TX Power: 0 dBm max

  RX Sensitivity: -96 dBm

  Data rate: 2 Mbps

https://flipperzero.one/

Flippers

- Regex: ^Flipper [A-Za-z0-9]{8}$ e.g. "Flipper Eironeoo"
- Flippers beaconing to find other Flippers? Or just because?
- **Bluetooth LE 5.0**

TX Power: 0 dBm max

RX Sensitivity: -96 dBm

Data rate: 2 Mbps

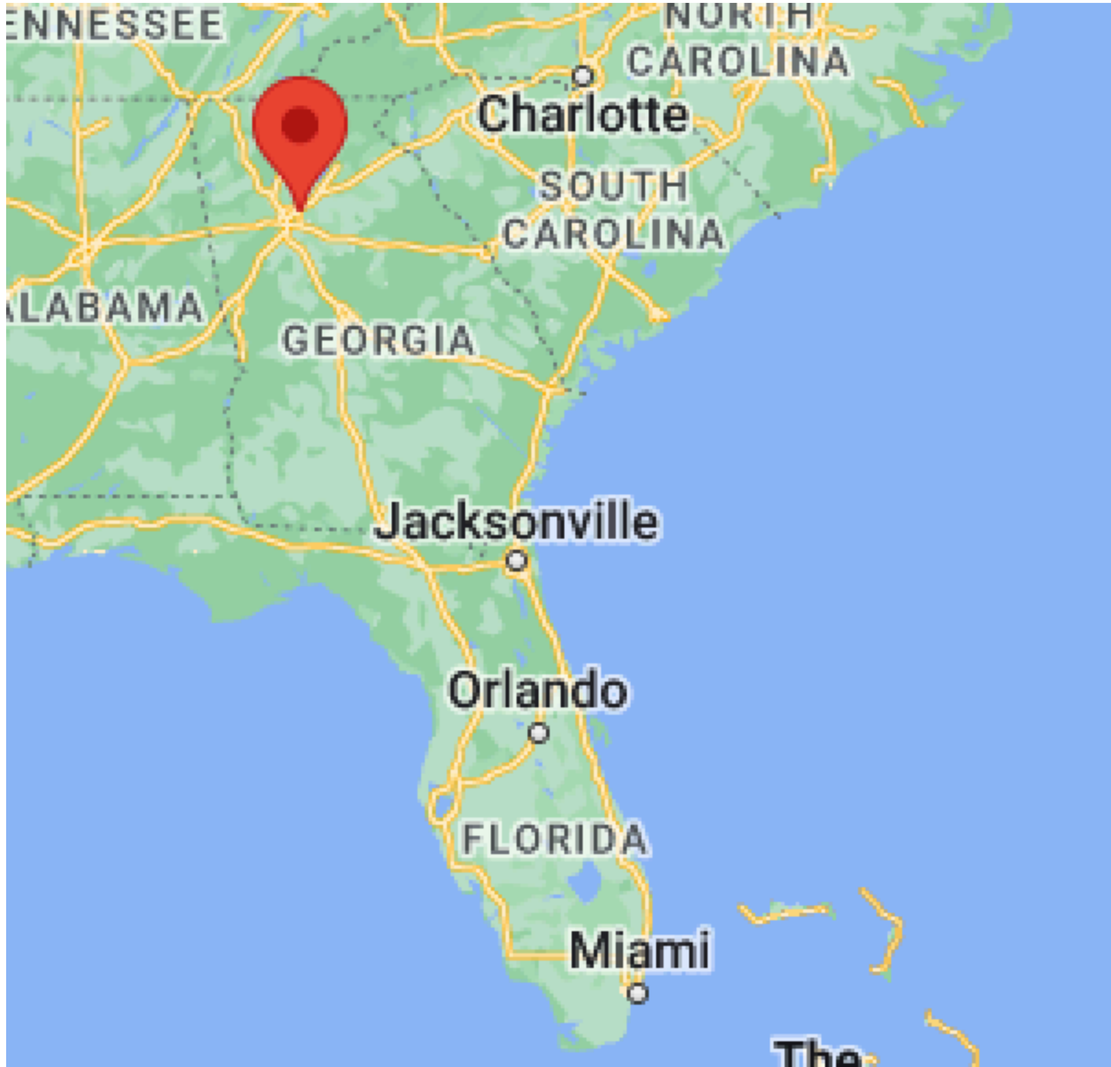
← This low transmit power diminishes the long-term utility as a BT active-scanning/ attack tool

https://flipperzero.one/

- Flipper Ectruv
- **Flipper Eironeoo**
- Flipper Emiperda
- Flipper Eota
- Flipper Ew1csed4
- Flipper Himuti
- Flipper Hl4ken
- Flipper Iludaow
- Flipper Inudy
- Flipper Itey
- Flipper Jaalmo
- Flipper Kiteko
- Flipper L4spil
- Flipper Leotar
- Flipper Luneor
- Flipper Noda
- Flipper Nyn4k4
- Flipper Ogoty
- Flipper Opot
- Flipper Orable
- Flipper Ost4rder
- Flipper Otaro
- Flipper R4g0
- Flipper R4u0
- Flipper Roswigd
- Flipper Tuna
- Flipper Un1l0
- Flipper Ylepjl0d

Flipper Eironeoo

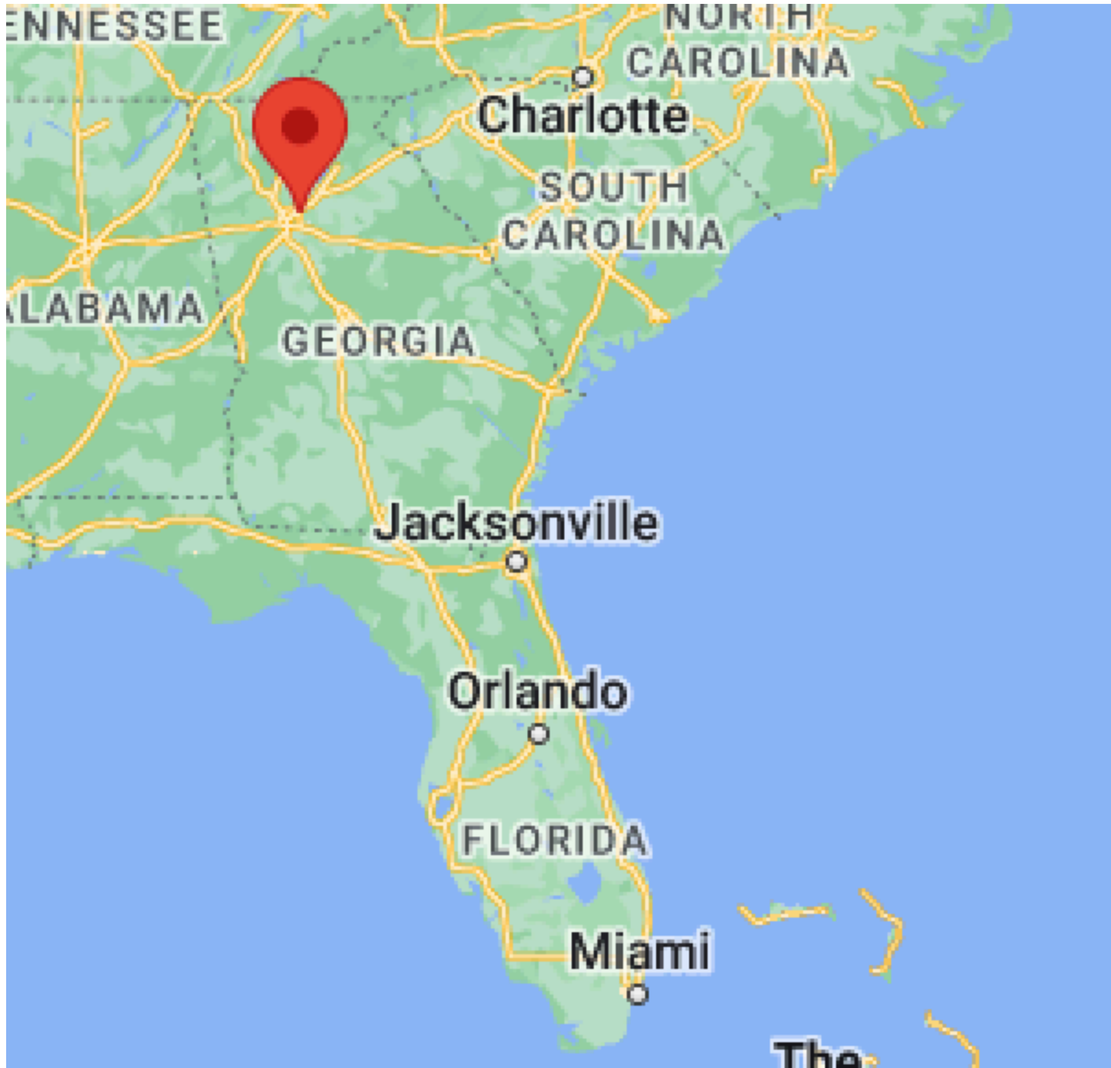
- WiGLE data saw it near a *Panera Bread* in Peachtree Corners, GA (outside Atlanta GA)
- I saw at Hardwear.io 2022 in The Hague
  - WiGLE doesn't have that data, probably because I didn't have GPS lock in the hotel



Flipper Eironeoo

- WiGLE data saw it near a *Panera Bread* in Peachtree Corners, GA (outside Atlanta GA)
- I saw at Hardwear.io 2022 in The Hague
  - WiGLE doesn't have that data, probably because I didn't have GPS lock in the hotel

Address type: **Public** (0x00)
Address: **80:E1:26**:6A:4A:E6 (OUI 80-E1-26)
Data length: 28
Flags: 0x06
  LE General Discoverable Mode
  BR/EDR Not Supported
Name (complete): **Flipper Eironeoo**

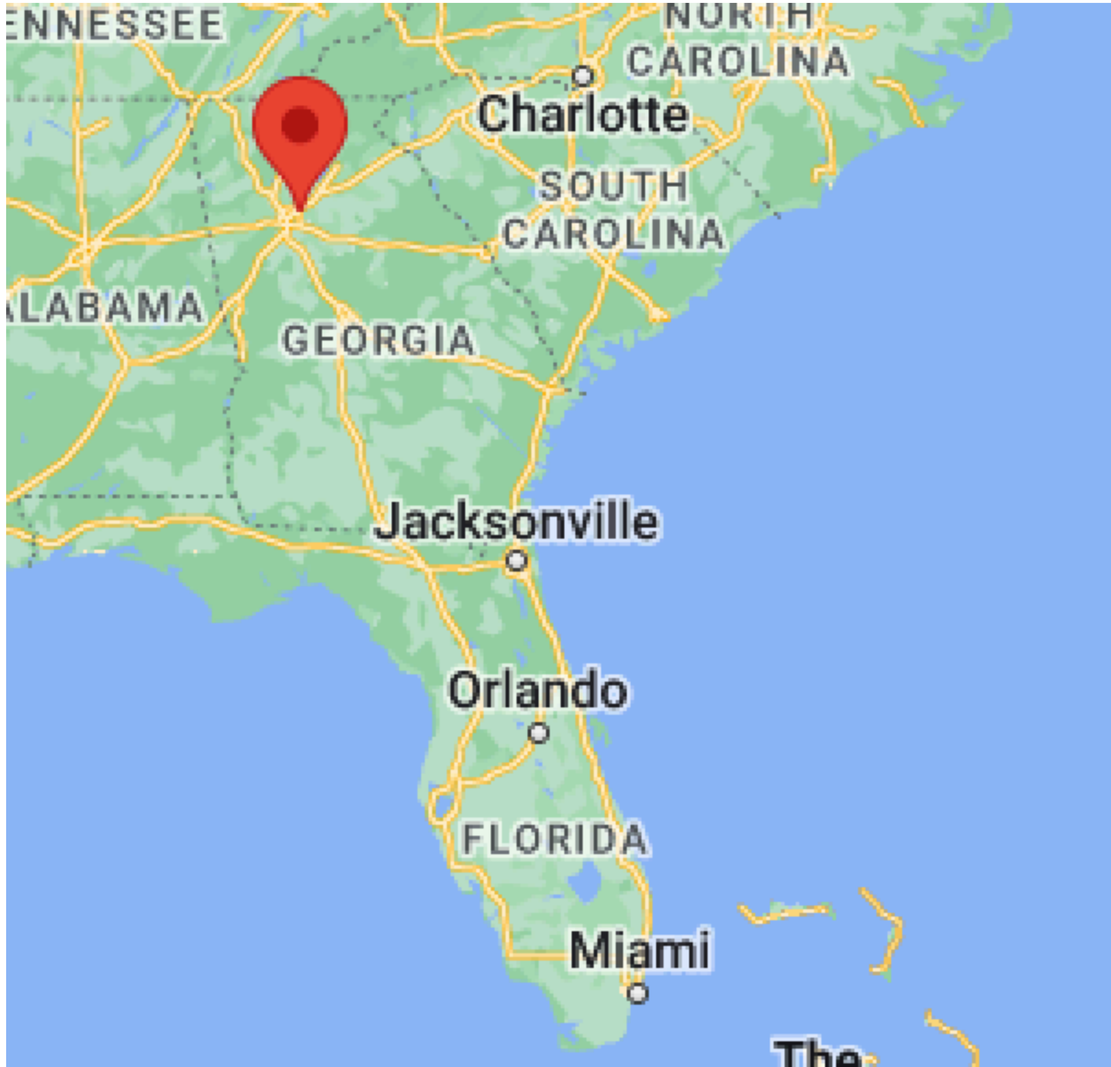


Flipper Eironeoo

- WiGLE data saw it near a *Panera Bread* in Peachtree Corners, GA (outside Atlanta GA)
- I saw at Hardwear.io 2022 in The Hague
  - WiGLE doesn't have that data, probably because I didn't have GPS lock in the hotel

Even if the name is changed, the BDADDR is not randomized...

Address type: **Public** (0x00)
Address: **80:E1:26**:6A:4A:E6 (OUI 80-E1-26)
Data length: 28
Flags: 0x06
  LE General Discoverable Mode
  BR/EDR Not Supported
Name (complete): **Flipper Eironeoo**



Change Dolphin Name?

Cwruidth Jun '22

This is almost certainly answered somewhere, but i've been searching around and couldn't find a topic for it:
Is it possible to change the unique dolphin name, or should i just reserve my effort for learning to love the goofy name mine was supplied by the factory?

created	last reply	12	8.5k	10	6	1
Jun '22	16d	replies	views	users	likes	link

Astra Support Jun '22

The Dolphin name is written into the OTP (one-time programmable) memory, so changing it is not possible.
However, you can edit the firmware to read the name from a string instead.

HRadt.1 (Customer) asked a question.
November 26, 2020 at 5:50 PM

Example Projects/Generated Code - Bluetooth Mac Address OUI validity

All Examples for the STM32WB have the following code in their app_ble.c:

```
1  const uint8_t* BleGetBdAddress( void ) {
2      ...
3      udn = LL_FLASH_GetUDN();
4      if(udn != 0xFFFFFFFF) {
5          company_id = LL_FLASH_GetSTCompanyID();
6          device_id = LL_FLASH_GetDeviceID();
7
8          bd_addr_udn[0] = (uint8_t)(udn & 0x000000FF);
9          bd_addr_udn[1] = (uint8_t)( (udn & 0x0000FF00) >> 8 );
10         bd_addr_udn[2] = (uint8_t)( (udn & 0x00FF0000) >> 16 );
11         bd_addr_udn[3] = (uint8_t)device_id;
12         bd_addr_udn[4] = (uint8_t)(company_id & 0x000000FF);;
13         bd_addr_udn[5] = (uint8_t)( (company_id & 0x0000FF00) >> 8 );
14
15     ...
16 }
```

Also Application Note AN5289 has the same listing.
Comments and descriptions lets me believe this yields a valid public bluetooth address.

The address created is "80:E1:26:XX:XX:XX". The first part is the OUI which should belong to ST Microelectronics. But in fact 80:E1:26 is not assigned. STMs OUI is 00:80:E1.

So I have to assume that ST does not supply a valid MAC address for the STM32WB devices? In that case this should be mentioned somewhere clearly!

https://community.st.com/s/question/0D53W00000PSj69SAD/example-projectsgenerated-code-bluetooth-mac-address-oui-validity

Flipper Zero: Changing Bluetooth MAC Address

Date: **February 3, 2023**

Author: **Salvador Mendoza**

0 Comments

Intro

Flipper Zero is a flexible, portable and popular tool that implements different technologies:

- NFC
- Bluetooth
- Transceiver
- RFID
- ...

Focusing on Bluetooth, the device utilize the dual-core and multi-protocol STM32WB55RG. As researcher or pentester, sometimes, we need

Inside of this function, the *aci_gap_set_discoverable* is set; with this our Flipper is discoverable. If we wish, we can add the advertising packet with *aci_gap_update_adv_data(size,data)*. After this, now we can modify our Bluetooth MAC Address. For this purpose, we call the ***aci_hal_write_config_data*** function, it will write a specific configuration to the Bluetooth, in this case, the change of the Bluetooth MAC Address. This function is useful to set up directly some low level parameters for the system in the runtime.

```
1 uint8_t bdaddnew[] = {0xFF, 0xEE, 0xDD, 0xCC, 0xBB, 0xA
2 aci_hal_write_config_data(CONFIG_DATA_PUBADDR_OFFSET, C
```

Flipper Zero: Changing Bluetooth MAC Address

Date: **February 3, 2023**

Author: **Salvador Mendoza**

0 Comments

Intro

Flipper Zero is a flexible, portable and popular tool that implements different technologies:

- NFC
- Bluetooth
- Transceiver
- RFID
- ...

Focusing on Bluetooth, the device utilize the dual-core and multi-protocol STM32WB55RG. As researcher or pentester, sometimes, we need

Inside of this function, the *aci_gap_set_discoverable* is set; with this our Flipper is discoverable. If we wish, we can add the advertising packet with *aci_gap_update_adv_data(size,data)*. After this, now we can modify our Bluetooth MAC Address. For this purpose, we call the ***aci_hal_write_config_data*** function, it will write a specific configuration to the Bluetooth, in this case, the change of the Bluetooth MAC Address. This function is useful to set up directly some low level parameters for the system in the runtime.

```
1 uint8_t bdaddnew[] = {0xFF, 0xEE, 0xDD, 0xCC, 0xBB, 0xA
2 aci_hal_write_config_data(CONFIG_DATA_PUBADDR_OFFSET, C
```

😬

Setting different hardcoded/static BDADDR

¯_(ツ)_/¯

Maybe they will change it

Someday

- https://github.com/flipperdevices/flipperzero-firmware/issues/2031
  - Filed November 2022, last post April 2023
  - Still open as of today
- Until then, if you've got a Flipper 👁️🌊👊

Around the home

Misc

- Regex: ^\\\[Refrigerator\\\] Samsung$"

Around the home

Misc

- Regex: ^\\\[Refrigerator\\\] Samsung$"
- Regex: ^Oral-B Toothbrush$

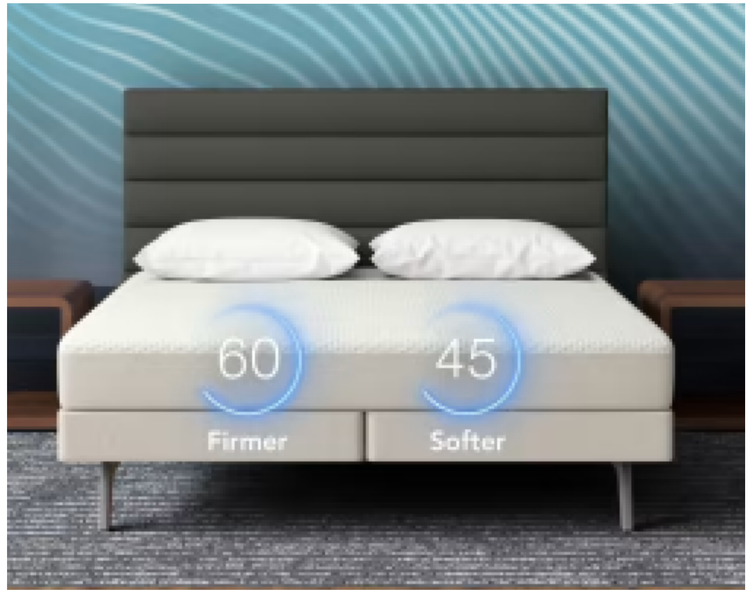
Around the home

Misc

- Regex: ^\\\[Refrigerator\\\] Samsung$"
- Regex: ^Oral-B Toothbrush$

Around the home

Misc



- Regex: ^\\\[Refrigerator\\\] Samsung$"
- Regex: ^Oral-B Toothbrush$
- "Sleep Number" beds advertise as their BDADDR
  - So regex: ^([0-9A-Fa-f]{2}[:]){5}[0-9A-Fa-f]{2}$ (and BDADDR OUI of "Select Comfort", because some Huawei devices also are just named after the BDADDR)

Around the home

Misc

- Regex: ^\\\[Refrigerator\\\] Samsung$"
- Regex: ^Oral-B Toothbrush$
- "Sleep Number" beds advertise as their BDADDF
  - So regex: ^([0-9A-Fa-f]{2}[:]){5}[0-9A-Fa-f]{2}$ (and BDADDR OUI of "Select Comfort", because some Huawei devices also are just named after the BDADDR)
- "Ooler" cooling bed pad regex: ^OOLER-[0-9]{10,11}$

OOLER Control Unit Only

This unit powers the OOLER sleep system and comes with a power cord. A Cool Mesh pad isn't included.Note: Co...

Around the home

Amazon Echo

- Regex: ^Echo-[A-Z0-9]{3}$ e.g. Echo-M3G
- Regex: ^Echo Dot-[A-Z0-9]{3}$ e.g. Echo Dot-7RT
- Regex: ^Echo Show-[0-9]{1}-[A-Z0-9]{3}$ e.g. Echo Show 5-48D or Echo Show 8-K0U
- Regex: ^Echo Spot-[A-Z0-9]{3}$ e.g. Echo Spot-1SD

Around the home

Amazon Echo

- Regex: ^Echo-[A-Z0-9]{3}$ e.g. Echo-M3G
- Regex: ^Echo Dot-[A-Z0-9]{3}$ e.g. Echo Dot-7RT
- Regex: ^Echo Show-[0-9]{1}-[A-Z0-9]{3}$ e.g. Echo Show 5-48D or Echo Show 8-K0U
- Regex: ^Echo Spot-[A-Z0-9]{3}$ e.g. Echo Spot-1SD

Echo & Echo Dot are BLE:
Address type: *Random* (0x01)
Address: 78:55:90:D6:DA:A4 (*Resolvable*)

Around the home

Amazon Echo

- Regex: ^Echo-[A-Z0-9]{3}$ e.g. Echo-M3G
- Regex: ^Echo Dot-[A-Z0-9]{3}$ e.g. Echo Dot-7RT
- Regex: ^Echo Show-[0-9]{1}-[A-Z0-9]{3}$ e.g. Echo Show 5-48D or Echo Show 8-K0U
- Regex: ^Echo Spot-[A-Z0-9]{3}$ e.g. Echo Spot-1SD

Echo & Echo Dot are BLE:
Address type: *Random* (0x01)
Address: 78:55:90:D6:DA:A4 (*Resolvable*)

Except of course that they have unique names!

Around the home

Amazon Echo

- Regex: ^Echo-[A-Z0-9]{3}$ e.g. Echo-M3G
- Regex: ^Echo Dot-[A-Z0-9]{3}$ e.g. Echo Dot-7RT
- Regex: ^Echo Show-[0-9]{1}-[A-Z0-9]{3}$ e.g. Echo Show 5-48D or Echo Show 8-K0U
- Regex: ^Echo Spot-[A-Z0-9]{3}$ e.g. Echo Spot-1SD

Echo & Echo Dot are BLE:
Address type: *Random* (0x01)
Address: 78:55:90:D6:DA:A4 (*Resolvable*)

Except of course that they have unique names!

Around the home

Amazon Echo

- Regex: ^Echo-[A-Z0-9]{3}$ e.g. Echo-M3G
- Regex: ^Echo Dot-[A-Z0-9]{3}$ e.g. Echo Dot-7RT
- Regex: ^Echo Show-[0-9]{1}-[A-Z0-9]{3}$ e.g. Echo Show 5-48D or Echo Show 8-K0U
- Regex: ^Echo Spot-[A-Z0-9]{3}$ e.g. Echo Spot-1SD

Echo & Echo Dot are BLE:
Address type: *Random* (0x01)
Address: 78:55:90:D6:DA:A4 (*Resolvable*)

Except of course that they have unique names!

Echo Show & Echo Spot are BT **Classic**:
Address: 40:A2:DB:9F:D3:9E (Amazon Technologies Inc.)
Name: Echo Show 5-48D

Mobile Point of Sale (MPOS)

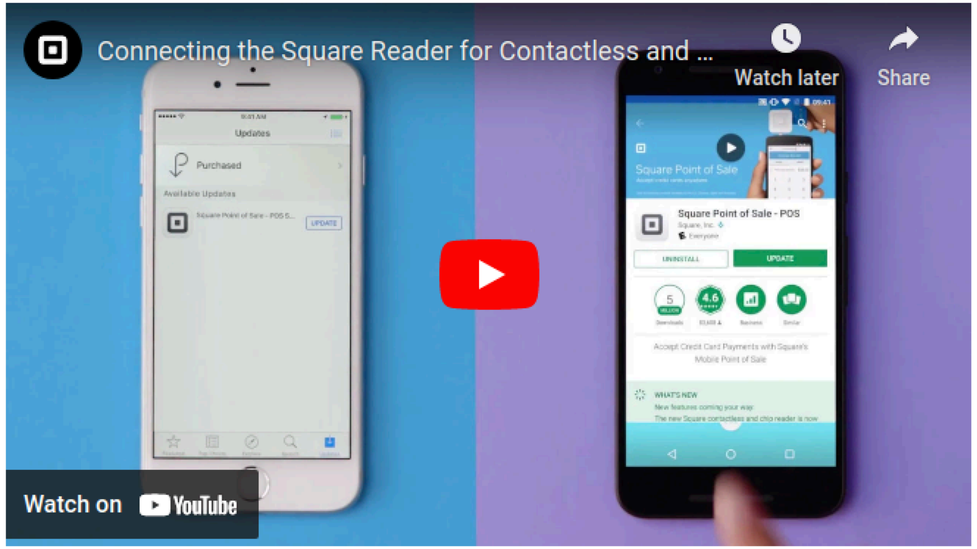
Square

- Regex: ^Square Reader [0-9]{4}$ e.g. "Square Reader 7249"

3. Wirelessly Connect Your Square Reader

The new reader connects wirelessly with Bluetooth Low Energy (Bluetooth LE). Be sure you have the latest version of the Square app for your device. **Note**: For optimal performance, please ensure your device is running the latest version of its operating system and the Square app.

Watch this video to learn how to wirelessly connect your reader:



https://squareup.com/help/us/en/article/5639-set-up-the-square-reader-for-contactless-and-chip

Mobile Point of Sale (MPOS)

Square

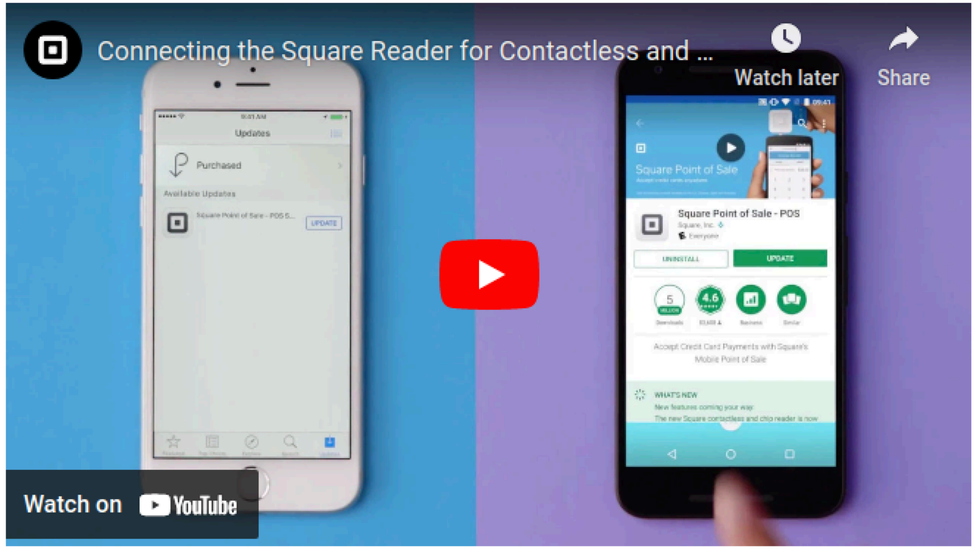
- Regex: ^Square Reader [0-9]{4}$ e.g. "Square Reader 7249"

Address type: **Public** (0x00)
Address: 04:EE:03:03:2A:FF (OUI 04-EE-03) <- Texas Instruments

3. Wirelessly Connect Your Square Reader

The new reader connects wirelessly with Bluetooth Low Energy (Bluetooth LE). Be sure you have the latest version of the Square app for your device. **Note**: For optimal performance, please ensure your device is running the latest version of its operating system and the Square app.

Watch this video to learn how to wirelessly connect your reader:



https://squareup.com/help/us/en/article/5639-set-up-the-square-reader-for-contactless-and-chip

Mobile Point of Sale (MPOS)

Square

- Regex: ^Square Reader [0-9]{4}$ e.g. "Square Reader 7249"

Mobile Point of Sale (MPOS)

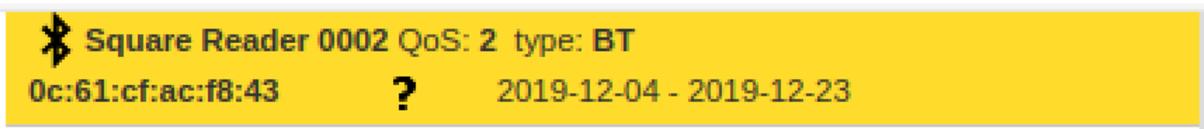
Square

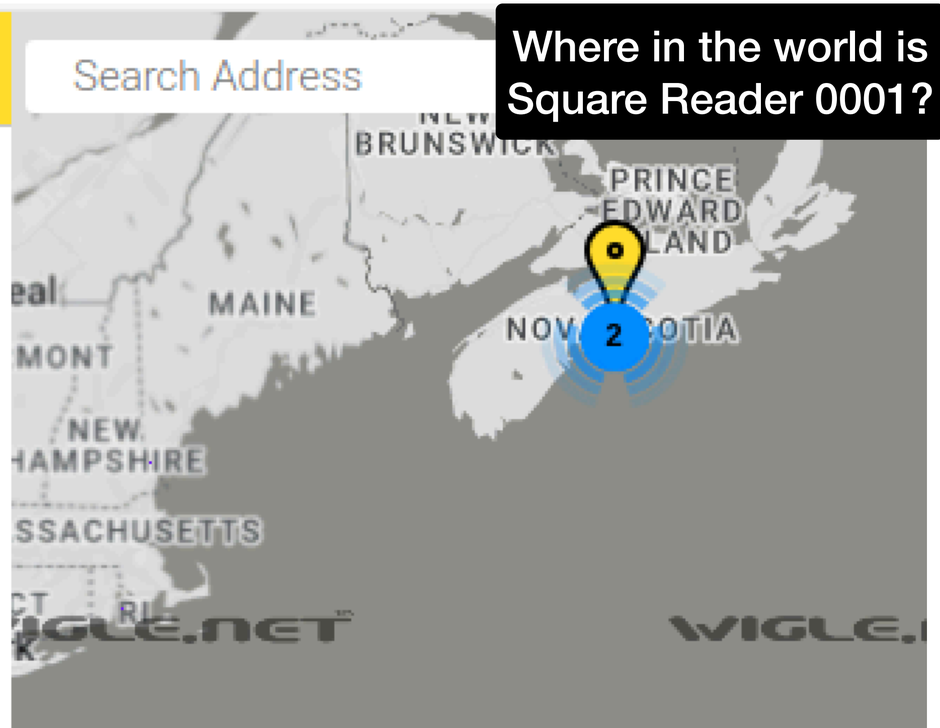
- Regex: ^Square Reader [0-9]{4}$ e.g. "Square Reader 7249"

Mobile Point of Sale (MPOS)

Square

- Regex: ^Square Reader [0-9]{4}$ e.g. "Square Reader 7249"





Mobile Point of Sale (MPOS)

eDynamo

- Regex: ^eDynamo-B[A-F0-9]{6}$ e.g. "eDynamo-B4A4AAB"

Mobile Card Reader with Bluetooth LE or USB Connection

Bluetooth LE gives you the freedom you need for mobile card reader payments. The low energy power consumption extends the life of the rechargeable batteries. If wireless is not preferred, then use the micro-USB cable and connect to a PC or mobile device with a USB host.

https://www.magtek.com/product/edynamo

Mobile Point of Sale (MPOS)

eDynamo

- Regex: ^eDynamo-B[A-F0-9]{6}$ e.g. "eDynamo-B4A4AAB"

Address type: **Public** (0x00)
Address: 90:E2:02:2E:89:BE (Texas Instruments)

Mobile Card Reader with Bluetooth LE or USB Connection

Bluetooth LE gives you the freedom you need for mobile card reader payments. The low energy power consumption extends the life of the rechargeable batteries. If wireless is not preferred, then use the micro-USB cable and connect to a PC or mobile device with a USB host.

https://www.magtek.com/product/edynamo

Turning my phone into a skimming device: MPos Solutions

Dan Borgogno & Ileana Barrionuevo

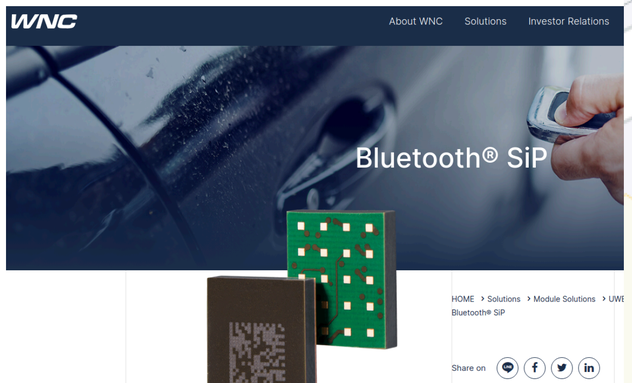
https://media.defcon.org/DEF%20CON%2031/DEF%20CON%2031%20presentations/Dan%20Borgogno%20Ileana%20Barrionuevo%20-%20Turning%20my%20virtual%20wallet%20into%20a%20skimming%20device%20mPOS%20solutions.pdf

Hotels

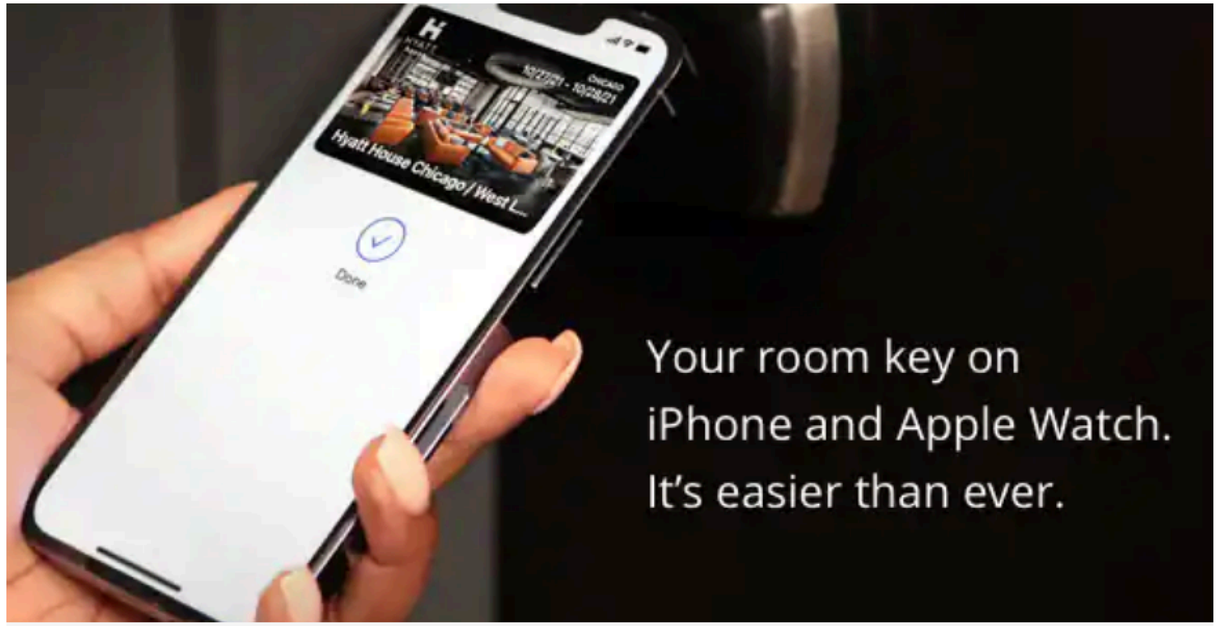
- Regex: ^TGNODE-([0-9A-F]{2}[:]){5}[0-9A-F]{2}$
  - e.g. TGNODE-2C:DC:AD:19:C4:FE
  - Semantically: The BDADDR-looking thing is != the static random BDADDR (*so maybe it's the original non-randomized BDADDR?*)
    - 2C:DC:AD && 74:6F:F7 == Wistron
  - Saw 149 instances
- Hyatt or Hilton?

Hotels

- Regex: ^TGNODE-([0-9A-F]{2}[:]){5}[0-9A-F]{2}$
  - e.g. TGNODE-2C:DC:AD:19:C4:FE
  - Semantically: The BDADDR-looking thing is != the static random BDADDR (*so maybe it's the original non-randomized BDADDR?*)
    - 2C:DC:AD && 74:6F:F7 == Wistron
  - Saw 149 instances
- Hyatt or Hilton?



Hyatt Digital Keys



Unlock your stay more quickly at select Hyatt hotels with Apple Wallet.

How is a room key in Apple Wallet different from other digital keys?

Hyatt's standard digital key utilizes Bluetooth technology that allows guests to use the World of Hyatt app on their iPhone or Android phone as a digital key.

Your room key in Apple Wallet can be securely used without opening an app or even unlocking your device. If you change rooms or add a few extra nights to your stay, your room key automatically updates in the background — so there's no extra work for you, and no extra trips to the front desk. And if you're out late to dinner, your room key in Apple Wallet may work for up to five hours after your device needs a charge.

https://world.hyatt.com/content/gp/en/landing/digital-key.html

Hilton Digital Keys

How does Digital Key work?

Unlock your door with Digital Key

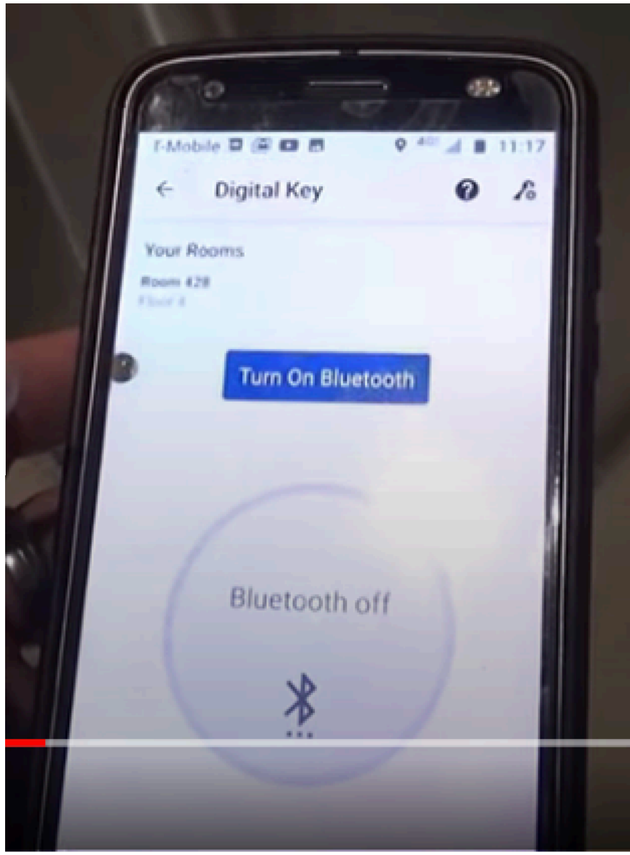
Go straight to your room, tap the Hilton Honors app, and unlock your room door with your phone using Digital Key.

Digital Key opens any door you'd normally access with a key card, including:

- Rooms
- Elevators
- Side doors
- Fitness center
- Parking garage

After you check in digitally, you can choose to use a Digital Key during your stay. Once your room is ready on the day of your arrival, we'll send a push notification to your smartphone that the key has been delivered. You can then use it via your Hilton Honors app until you check out.

To use on property, open the Hilton Honors app, and when you're within range of an equipped lock, simply push the button to unlock.

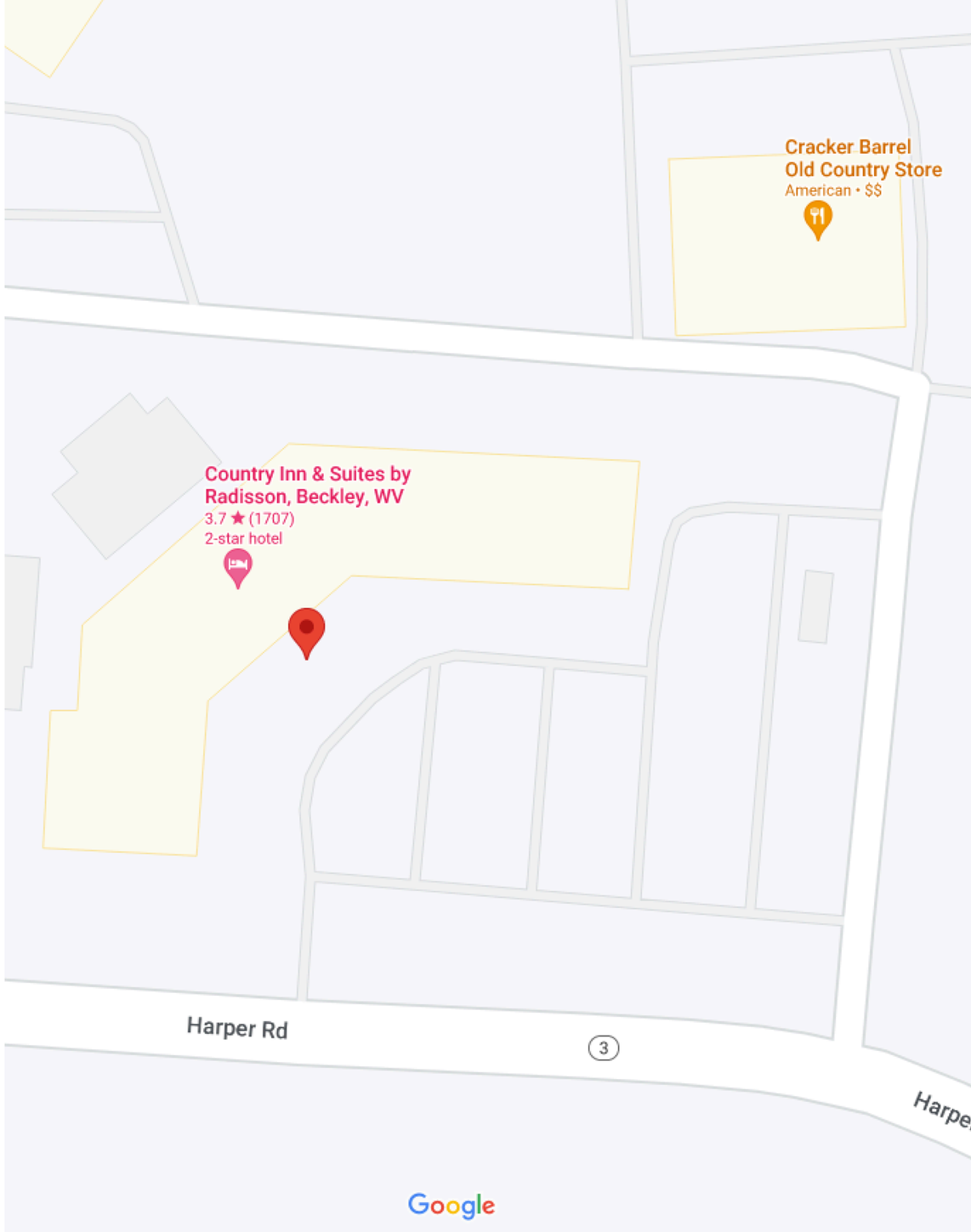


https://help.hilton.com/s/article/How-does-Digital-Key-work

https://www.youtube.com/watch?v=y8QiqAdSmSA

Hotels

- Regex: ^[0-9]{8}\.[0-9]{8}$
  - E.g. 46351777.00007702
- At the time I saw no obvious semantic association between the first portion of the name and either the BDADDR or room number
- Saw 17 instances from my room

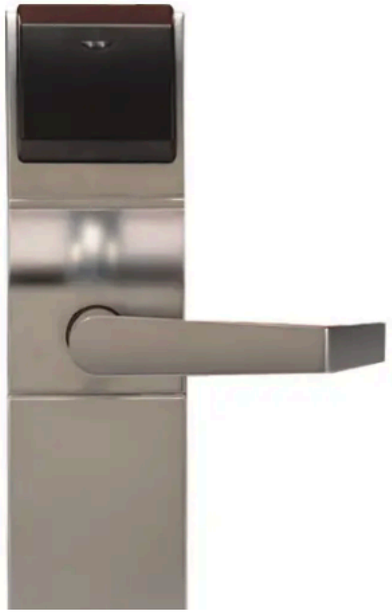


Hotels

- Door physically looked like this:

Onity
United Technologies

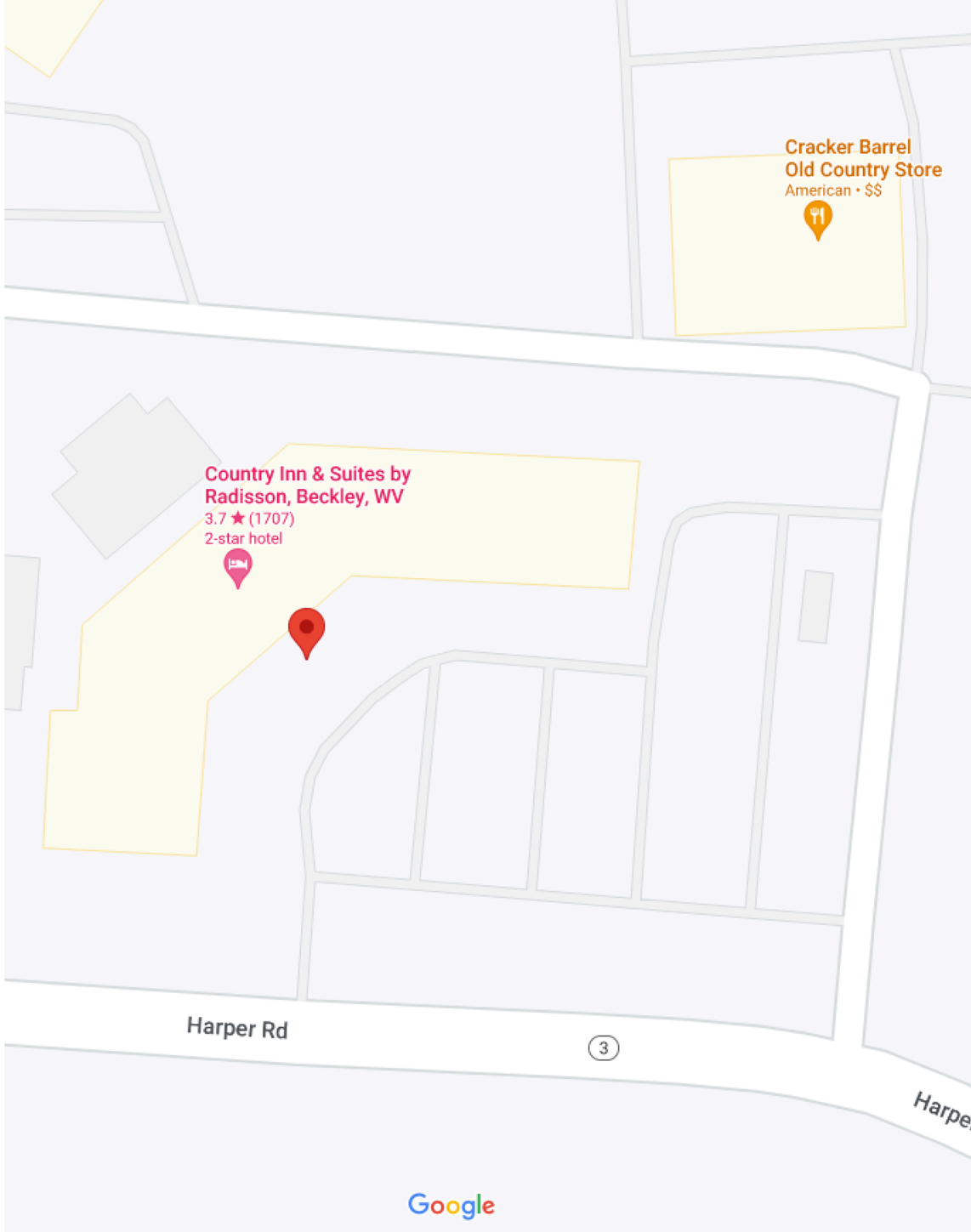
HT RFID Lock with DirectKey™ Module



Features

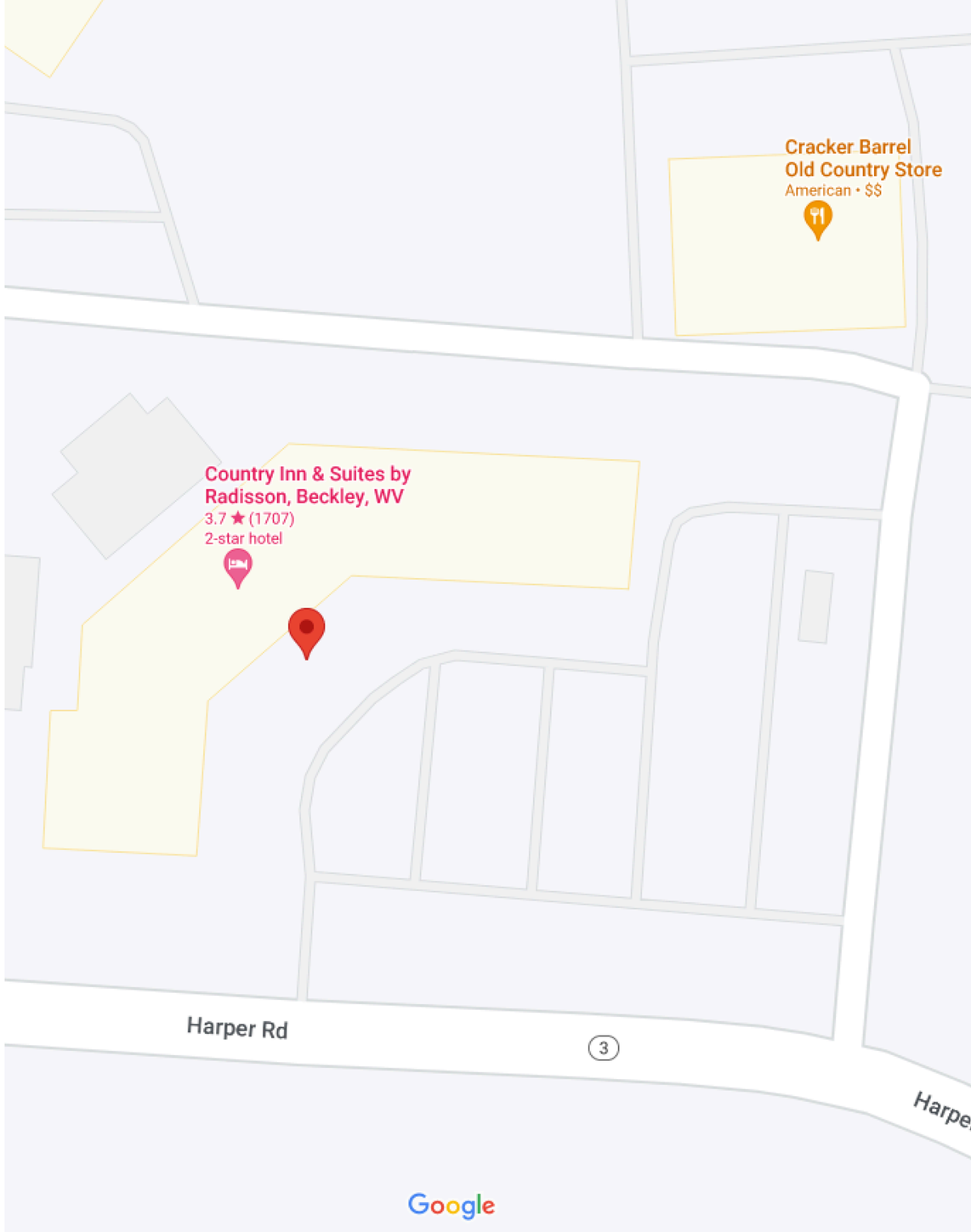
- On-board DirectKey module provides secure wireless communication of credentials from a user's smartphone to a locking device via Bluetooth® Smart communications
- Reading technology: contactless RFID (ISO14443A, 14443B part 4, NFC)
- Multiple opening devices available: keycards, wristbands, keychains, etc.
- Average battery life: approximately 2 years
- Non-volatile memory records the last 500 lock openings – including date, time and card used
- Programmable to customer needs (meeting rooms, offices, housekeeping, etc.)
- LEDs to indicate lock status including a low battery warning
- MIFARE® compatibility - no need for proprietary keycards
- Corrosion-treated for normal atmospheric conditions

https://fccid.io/R32-HT34RFIDBT/User-Manual/user-manual-3020324

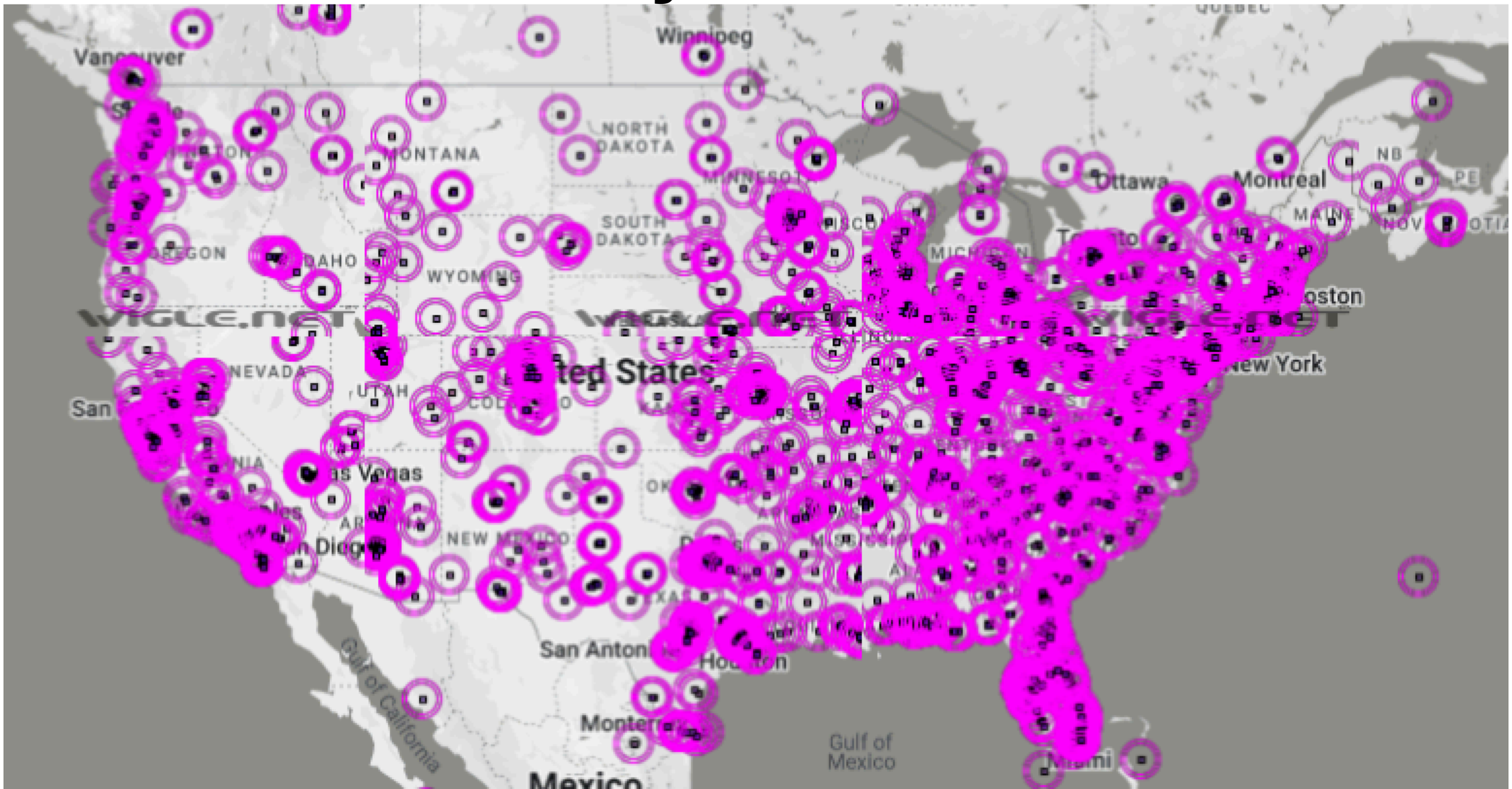


Hotels

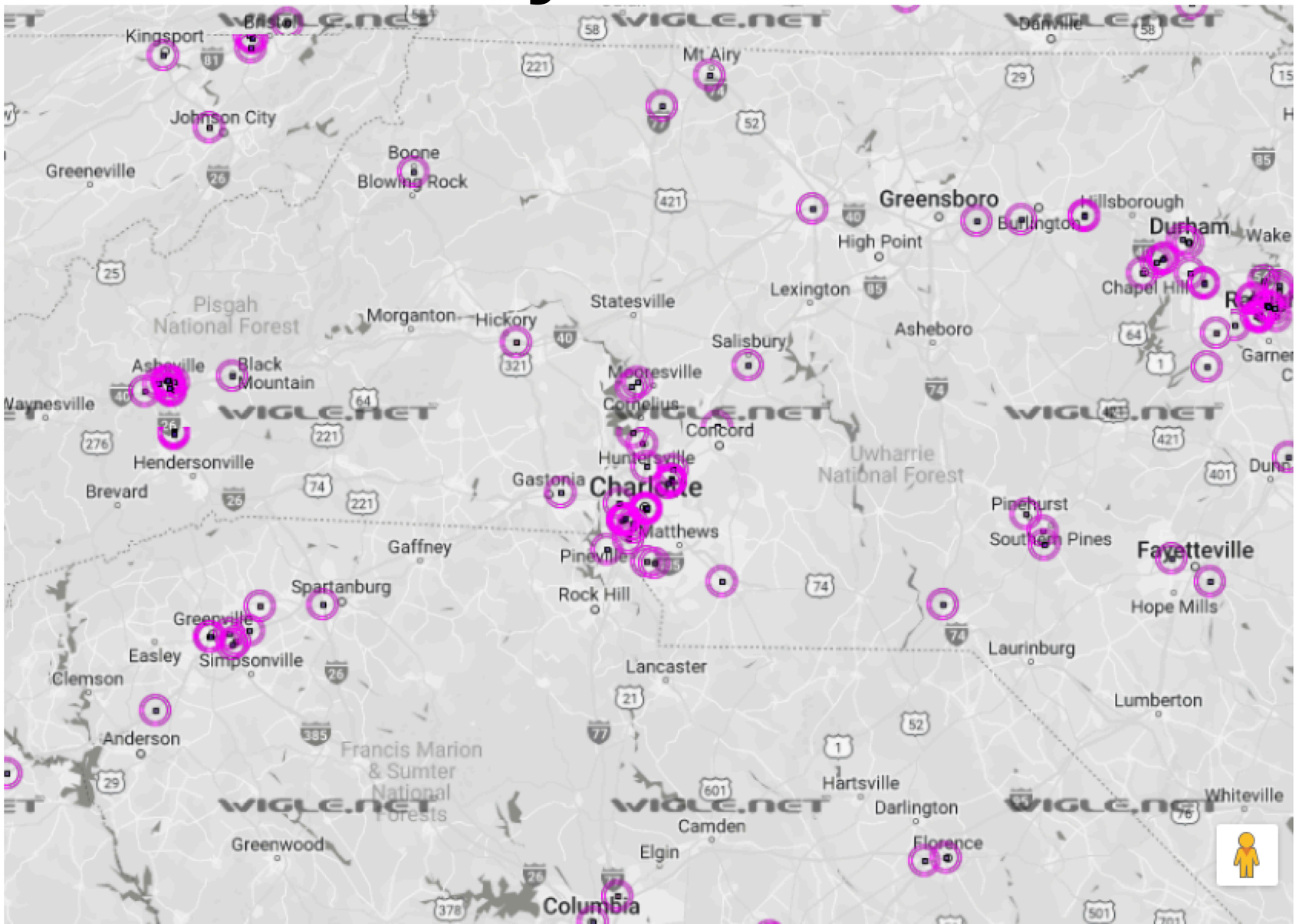
- Company Name by IEEE OUI (00:17:55): *GE Security*
- UUID16 0xfea7 (Company ID: *UTC Fire and Security*)
- What's WiGLE say if we search for that OUI?



Hotels - GE Security OUI 00:17:55



Hotels - GE Security OUI 00:17:55



Hotels - GE Security OUI 00:17:55

WiFi | Cell | BT

Lat: 35.1879 **to:** 35.1889

Lon: -80.9156 **to:** -80.9145

Last Updated: 20010925174546

BSSID/MAC: 00:17:55

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

foorbar or foobar%

Only Nets I Was the First to See

Query

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

44039037.00008208 QoS: **1** type: **BLE**
00:17:55:a3:f2:61 ? 2022-02-08 - 2022-02-11

44084700.00008208 QoS: **1** type: **BLE**
00:17:55:a4:a4:c0 ? 2022-02-08 - 2022-02-11

44084714.00008208 QoS: **1** type: **BLE**
00:17:55:a4:a4:ce ? 2022-02-08 - 2022-02-11

44084738.00008208 QoS: **1** type: **BLE**
00:17:55:a4:a4:e6 ? 2021-11-15 - 2022-02-11

44084798.00008208 QoS: **1** type: **BLE**
00:17:55:a4:a5:22 ? 2022-02-08 - 2022-02-11

44084906.00008208 QoS: **1** type: **BLE**
00:17:55:a4:a5:8e ? 2022-02-08 - 2022-02-11

44084915.00008208 QoS: **1** type: **BLE**
00:17:55:a4:a5:97 ? 2022-02-08 - 2022-02-11

44085226.00008208 QoS: **1** type: **BLE**
00:17:55:a4:a6:ce ? 2022-02-08 - 2022-02-11

44085241.00008208 QoS: **1** type: **BLE**
00:17:55:a4:a6:dd ? 2022-02-08 - 2022-02-11

44085256.00008208 QoS: **1** type: **BLE**

Hotels - GE Security OUI 00:17:55 @ Hilton

search for networks

WiFi | Cell | BT

Lat: 35.1909 **to:** 35.192

Lon: -80.9245 **to:** -80.9233

Last Updated: 20010925174546

BSSID/MAC: 00:17:55

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

foobar or foobar%

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

Query

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

00:17:55:14:aa:a0	?	2023-06-27 - 2023-06-29
44039037.00008208 QoS: 1 type: BLE		
00:17:55:a3:f2:61	?	2022-02-08 - 2022-02-11
44084700.00008208 QoS: 1 type: BLE		
00:17:55:a4:a4:c0	?	2022-02-08 - 2022-02-11
44084714.00008208 QoS: 1 type: BLE		
00:17:55:a4:a4:ce	?	2022-02-08 - 2022-02-11
44084738.00008208 QoS: 1 type: BLE		
00:17:55:a4:a4:e6	?	2021-11-15 - 2022-02-11
44084798.00008208 QoS: 1 type: BLE		
00:17:55:a4:a5:22	?	2022-02-08 - 2022-02-11
44084906.00008208 QoS: 1 type: BLE		
00:17:55:a4:a5:8e	?	2022-02-08 - 2022-02-11
44084915.00008208 QoS: 1 type: BLE		
00:17:55:a4:a5:97	?	2022-02-08 - 2022-02-11
44085226.00008208 QoS: 1 type: BLE		
00:17:55:a4:a6:ce	?	2022-02-08 - 2022-02-11
44085241.00008208 QoS: 1 type: BLE		
00:17:55:a4:a6:dd	?	2022-02-08 - 2022-02-11
44085256.00008208 QoS: 1 type: BLE		
00:17:55:a4:a6:ec	?	2022-02-08 - 2022-02-11
44085259.00008208 QoS: 1 type: BLE		
00:17:55:a4:a6:ef	?	2022-02-08 - 2022-02-11
44085260.00008208 QoS: 1 type: BLE		
00:17:55:a4:a6:f0	?	2022-02-08 - 2022-02-11

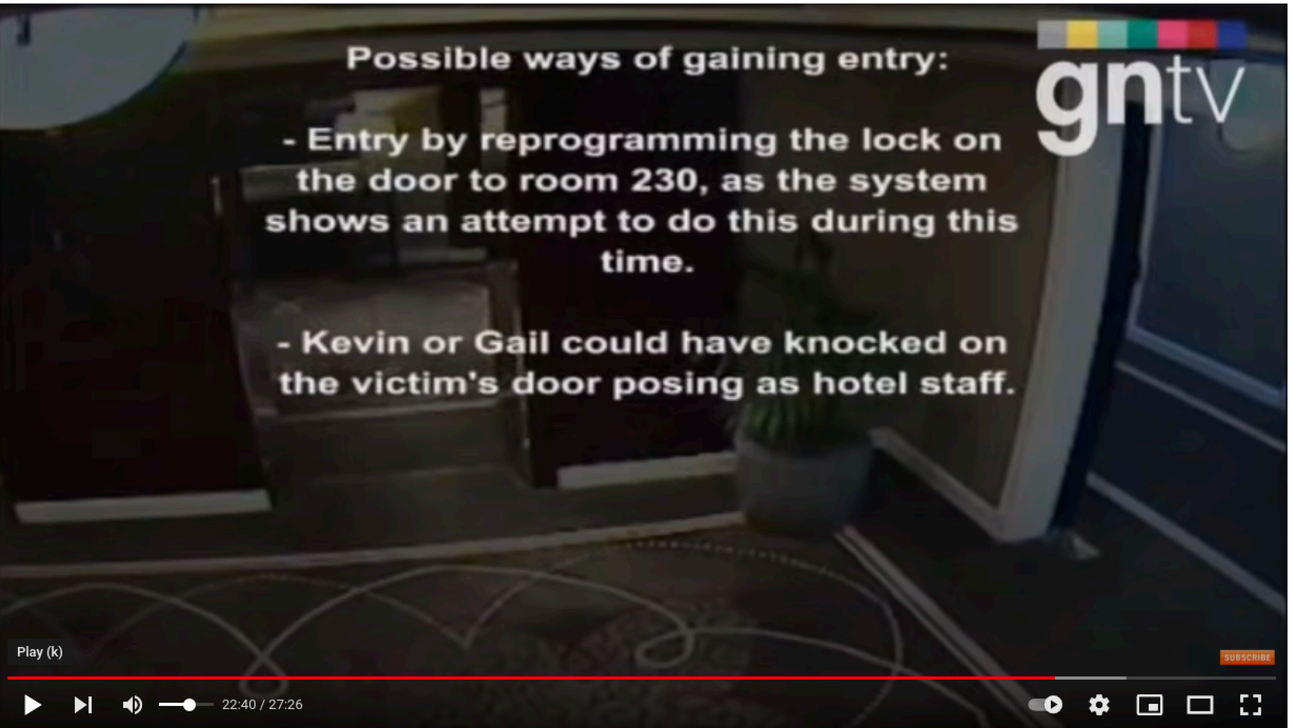
Hotels - GE Security OUI 00:17:55 @ Hilton

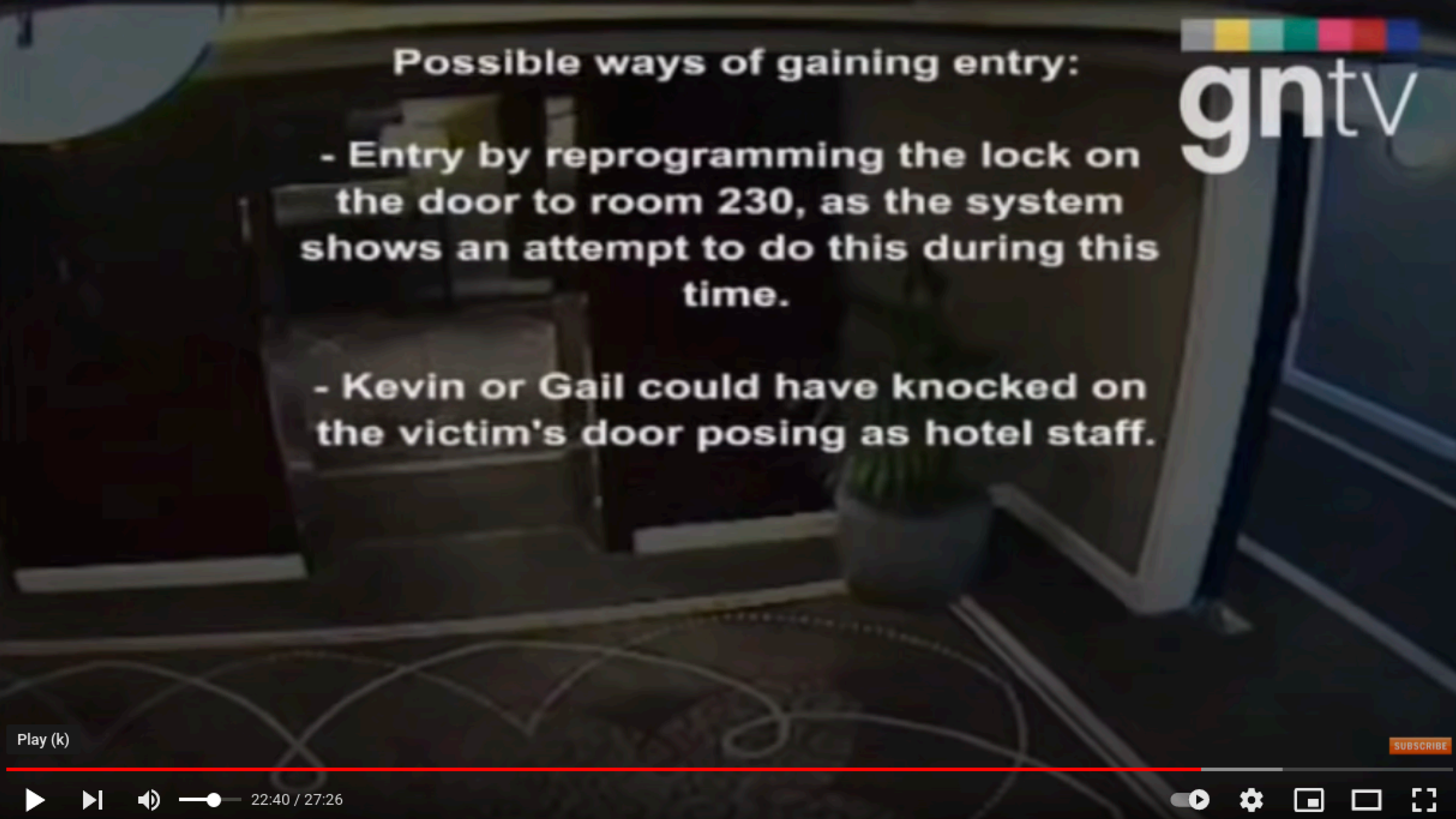
https://i.blackhat.com/USA-19/Thursday/us-19-Ray-Moving-From-Hacking-IoT-Gadgets-To-Breaking-Into-One-Of-Europes-Highest-Hotel-Suites.pdf

Reminder Why Hotel Room Security Matters...

2010 Hotel Assassination of Hamas leader by Mossad

- https://www.wired.com/2010/02/alleged-assassins-caught-on-tape/
- https://www.youtube.com/watch?v=bJujlwtdk8w



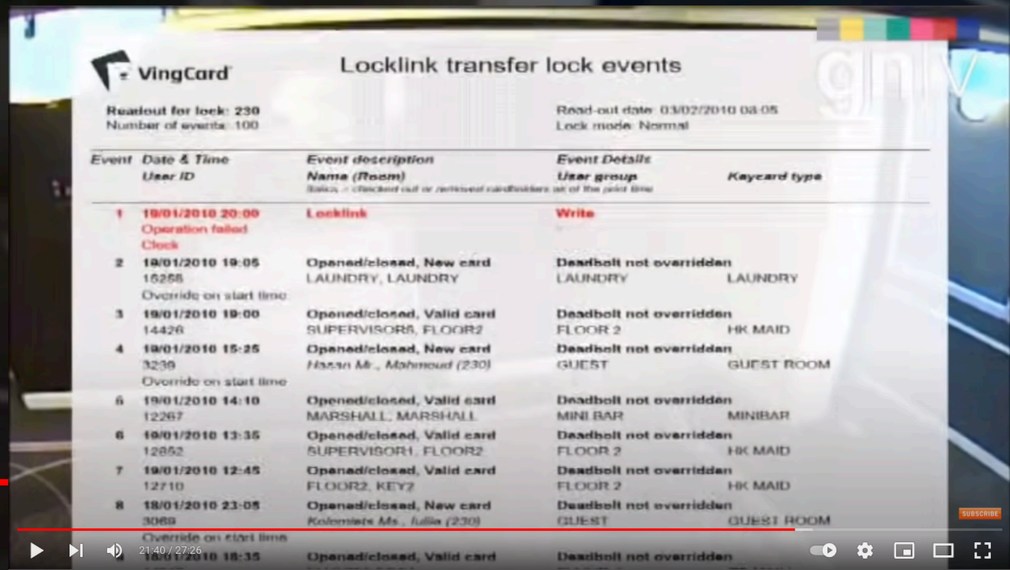

Possible ways of gaining entry:
- Entry by reprogramming the lock on the door to room 230, as the system shows an attempt to do this during this time.
- Kevin or Gail could have knocked on the victim's door posing as hotel staff.
gntv
Play (k)
SUBSCRIBE
22:40 / 27:26

Possible ways of gaining entry:

- Entry by reprogramming the lock on the door to room 230, as the system shows an attempt to do this during this time.

- Kevin or Gail could have knocked on the victim's door posing as hotel staff.

gntv



Play (k)

22:40 / 27:26

VingCard

Locklink transfer lock events

Readout for lock: 230
Number of events: 100

Read-out date: 03/02/2010 03:05
Lock mode: Normal

Event	Date & Time / User ID	Event description / Name (Room)	Event Details / User group	Keycard type
		Status = checked out or retrieved cardholders as of the point time		
1	**19/01/2010 20:00** Operation failed Clock	**Locklink**	**Write**	
2	**19/01/2010 19:05** 15258 Override on start time	**Opened/closed, New card** LAUNDRY, LAUNDRY	**Deadbolt not overridden** LAUNDRY	LAUNDRY
3	**19/01/2010 19:00** 14426	**Opened/closed, Valid card** SUPERVISOR5, FLOOR2	**Deadbolt not overridden** FLOOR 2	HK MAID
4	**19/01/2010 15:25** 3239 Override on start time	**Opened/closed, New card** *Hassan Mr., Mahmoud (230)*	**Deadbolt not overridden** GUEST	GUEST ROOM
5	**19/01/2010 14:10** 12267	**Opened/closed, Valid card** MARSHALL, MARSHALL	**Deadbolt not overridden** MINI BAR	MINIBAR
6	**19/01/2010 13:35** 12852	**Opened/closed, Valid card** SUPERVISOR1, FLOOR2	**Deadbolt not overridden** FLOOR 2	HK MAID
7	**19/01/2010 12:45** 12710	**Opened/closed, Valid card** FLOOR2, KEY2	**Deadbolt not overridden** FLOOR 2	HK MAID
8	**18/01/2010 23:05** 3069 Override on start time	**Opened/closed, New card** *Kolemiate Ms., Iuliia (230)*	**Deadbolt not overridden** GUEST	GUEST ROOM

Random - "^Pokemon GO Plus$"

- Regex: ^Pokemon GO Plus$
- "The Pokémon GO Plus is a small device that lets you enjoy Pokémon GO while you're on the move and not looking at your smartphone
- The device connects to a smartphone via Bluetooth low energy and notifies you about events in the game, such as the appearance of a Pokémon nearby using an LED and vibration
- The Pokémon GO Plus will begin to blink and vibrate whenever you're within range of a PokéStop; Press the Pokémon GO Plus button to search the PokéStop for items; If you find any items, they'll immediately be added to your inventory"

Canada
United States
Mexico
North Atlantic Ocean
Kingdom
Poland
Germany
France
Spain
Italy
Ukraine
Türkiye
Kazakhstan
Mongolia
China
Japan
South Korea
Afghanistan
Iraq
Iran
Pakistan
India
Thailand
Algeria
Libya
Egypt
Saudi Arabia
Mali
Niger
Chad
Sudan
Nigeria
Ethiopia
Kenya
DRC
Tanzania
Angola
Namibia
Botswana
South Africa
Madagascar
Indonesia
Papua New Guinea
Australia
Indian Ocean
Venezuela
Colombia
Peru
Brazil
Bolivia
Chile
Argentina
South Atlantic Ocean
WIGLE.NET
WIGLE.NET
WIGLE.NET

Transportation - Scooters

- Regex: ^Segway IoT$

Segway Ninebot ZK601LE

battery bluetooth ip67 lte micromobility scooter

Segway Ninebot ZK601LE is an IoT device for shared scooter management. The device allows to lock/unlock, power on /off, turn on/off the throttle, and switch between different riding modes, etc. You can also monitor the state of the scooter through its communications with the server, such as sending alarms, firmware version information, battery temperatures, etc. It also has auxiliary features like prompt voice, superior waterproof design (IP67), and a built-in 1000 mAh battery.

Make your Segway Ninebot ZK601LE devices a part of any infrastructure by connecting them via flespi telematics hub. Manage the device settings using flespi device management platform. Learn how to configure Segway Ninebot ZK601LE with flespi.

- ^NBScooter[0-9]{4}$ e.g. "NBScooter1173" - "NineBot Scooter"? (Chinese company "Ninebot" acquired Segway in 2015)

Address type: **Random** (0x01)
Address: F9:32:A8:F8:9E:F6 (**Static**)

Bose

The world is awash in headphones & speakers. Only one example due to lack of time

- Regex: ^LE-.*$
- Semantically: LE-<custom name set by owner>
  - "LE-rock lobstah"
  - "LE-The Chairman"
  - "LE-KC Butterball"
  - "LE-Hans K<censored>"

Bose

The world is awash in headphones & spea

due to lack of time

- Regex: ^LE-.*$
- Semantically: LE-<custom name set by owner>
  - "LE-rock lobstah"
  - "LE-The Chairman"
  - "LE-KC Butterball"
  - "LE-Hans K<censored>"

Bose

The world is awash in headphones & spea

due to lack of time

- Regex: ^LE-.*$
- Semantically: LE-<custom name set by owner>
  - "LE-rock lobstah"
  - "LE-The Chairman"
  - "LE-KC Butterball"
  - "LE-Hans K<censored>"

Bose

The world is awash in headphones & spea

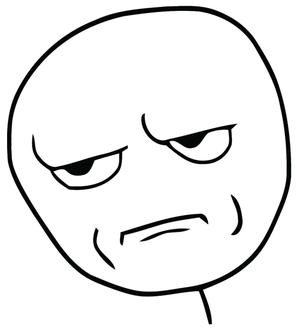
due to lack of time

- Regex: ^LE-.*$
- Semantically: LE-<custom name set by owner>
  - "LE-rock lobstah"
  - "LE-The Chairman"
  - "LE-KC Butterball"
  - "LE-Hans K<censored>"

Bose

The world is awash in headphones & spea

due to lack of time

- Regex: ^LE-.*$
- Semantically: LE-<custom name set by owner>
  - "LE-rock lobstah"
  - "LE-The Chairman"
  - "LE-KC Butterball"
  - "LE-Hans K<censored>" 

^LE-.*$ Seems like a bit too generic a pattern...

- You're in luck!
- A ton of devices seems to use a public address with the Bose OUI, in case it's ambiguous...

^LE-.*$ Seems like a bit too generic a pattern...

- You're in luck!
- A ton of devices seems to use a public address with the Bose OUI, in case it's ambiguous...

Address type: **Public** (0x00) Address: 2C:41:A1:95:FE:B6 (**Bose Corporation**) TX power: 10 dBm Name (complete): LE-Bose Revolve+ SoundLink	Address type: **Public** (0x00) Address: 2C:41:A1:E7:C5:F5 (**Bose Corporation**) TX power: 8 dBm Name (complete): LE-Bose SoundSport	Address type: **Public** (0x00) Address: 28:11:A5:1C:7E:E0 (**Bose Corporation**) TX power: 8 dBm Name (complete): LE-reserved_Y
Address type: **Public** (0x00) Address: 28:11:A5:B0:74:1A (**Bose Corporation**) TX power: 10 dBm Name (complete): LE-Bose Micro SoundLink	Address type: **Public** (0x00) Address: 4C:87:5D:66:A8:5D (**Bose Corporation**) TX power: 8 dBm Name (complete): LE-Bose Free SoundSport	Address type: **Public** (0x00) Address: 4C:87:5D:66:B4:99 (**Bose Corporation**) TX power: 8 dBm Name (complete): LE-reserved_C
Address type: **Public** (0x00) Address: 60:AB:D2:0B:0B:B8 (**Bose Corporation**) TX power: 10 dBm Name (complete): LE-Night	Address type: **Public** (0x00) Address: 2C:41:A1:5F:A8:63 (**Bose Corporation**) TX power: 8 dBm Name (complete): LE-**olix**	Address type: **Public** (0x00) Address: 2C:41:A1:5F:CC:09 (**Bose Corporation**) TX power: 8 dBm Name (complete): LE-reserved_p

^LE-.*$ Seems like a bit too generic a pattern...

- You're in luck!
- A ton of devices seems to use a public address with the Bose OUI, in case it's ambiguous...

Address type: **Public** (0x00) Address: 2C:41:A1:95:FE:B6 (**Bose Corporation**) TX power: 10 dBm Name (complete): LE-Bose Revolve+ SoundLink	Address type: **Public** (0x00) Address: 2C:41:A1:E7:C5:F5 (**Bose Corporation**) TX power: 8 dBm Name (complete): LE-Bose SoundSport	Address type: **Public** (0x00) Address: 28:11:A5:1C:7E:E0 (**Bose Corporation**) TX power: 8 dBm Name (complete): LE-reserved_Y
Address type: **Public** (0x00) Address: 28:11:A5:B0:74:1A (**Bose Corporation**) TX power: 10 dBm Name (complete): LE-Bose Micro SoundLink	Address type: **Public** (0x00) Address: 4C:87:5D:66:A8:5D (**Bose Corporation**) TX power: 8 dBm Name (complete): LE-Bose Free SoundSport	Address type: **Public** (0x00) Address: 4C:87:5D:66:B4:99 (**Bose Corporation**) TX power: 8 dBm Name (complete): LE-reserved_C
Address type: **Public** (0x00) Address: 60:AB:D2:0B:0B:B8 (**Bose Corporation**) TX power: 10 dBm Name (complete): LE-Night	Address type: **Public** (0x00) Address: 2C:41:A1:5F:A8:63 (**Bose Corporation**) TX power: 8 dBm Name (complete): LE-**olix**	Address type: **Public** (0x00) Address: 2C:41:A1:5F:CC:09 (**Bose Corporation**) TX power: 8 dBm Name (complete): LE-reserved_p

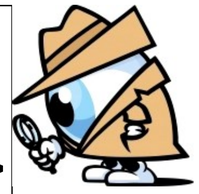
Address type: *Random* (0x01)
Address: 60:E1:4F:72:7E:22 (*Resolvable*)
Name (complete): **LE-Hans K<censored>**

^LE-.*$ Seems like a bit too generic a pattern...

- You're in luck!
- A ton of devices seems to use a public address with the Bose OUI, in case it's ambiguous...

Address type: **Public** (0x00) Address: 2C:41:A1:95:FE:B6 (**Bose Corporation**) TX power: 10 dBm Name (complete): LE-Bose Revolve+ SoundLink	Address type: **Public** (0x00) Address: 2C:41:A1:E7:C5:F5 (**Bose Corporation**) TX power: 8 dBm Name (complete): LE-Bose SoundSport	Address type: **Public** (0x00) Address: 28:11:A5:1C:7E:E0 (**Bose Corporation**) TX power: 8 dBm Name (complete): LE-reserved_Y
Address type: **Public** (0x00) Address: 28:11:A5:B0:74:1A (**Bose Corporation**) TX power: 10 dBm Name (complete): LE-Bose Micro SoundLink	Address type: **Public** (0x00) Address: 4C:87:5D:66:A8:5D (**Bose Corporation**) TX power: 8 dBm Name (complete): LE-Bose Free SoundSport	Address type: **Public** (0x00) Address: 4C:87:5D:66:B4:99 (**Bose Corporation**) TX power: 8 dBm Name (complete): LE-reserved_C
Address type: **Public** (0x00) Address: 60:AB:D2:0B:0B:B8 (**Bose Corporation**) TX power: 10 dBm Name (complete): LE-Night	Address type: **Public** (0x00) Address: 2C:41:A1:5F:A8:63 (**Bose Corporation**) TX power: 8 dBm Name (complete): LE-**olix**	Address type: **Public** (0x00) Address: 2C:41:A1:5F:CC:09 (**Bose Corporation**) TX power: 8 dBm Name (complete): LE-reserved_p

Address type: *Random* (0x01)
Address: 60:E1:4F:72:7E:22 (*Resolvable*)
Name (complete): **LE-Hans K<censored>**



This is what I meant by "Minimally Trackable *(in principle)*"
(*Possibly trackable using device-specific data*)

Mini-Takeaway

Tracking

- Even if a company does "the right thing" to prevent tracking, by making the BDADDR random and non-static, other information such as unique names can still make a device trackable

Fitness (*People?*) Trackers / Watches

Huawei

- Regex: ^HUAWEI Band(| 2| 3e)-[A-F0-9]{3}$ e.g. HUAWEI Band 3e-***4D8***
  - Semantically: [A-F0-9]{3} are last 3 digits of BDADDR
- Regex: ^HUAWEI WATCH (3|3 Pro|GT|GT-2e)-[A-F0-9]{3}$ e.g. HUAWEI WATCH GT-***98E***
  - Semantically: [A-F0-9]{3} are last 3 digits of BDADDR
- I have yet to see a Huawei watch/fitness tracker that isn't uniquely identifiable and therefore trackable either by its BDADDR or name

Fitness (*People?*) Trackers / Watches

Huawei

- Regex: ^HUAWEI Band(| 2| 3e)-[A-F0-9]{3}$ e.g. HUAWEI Band 3e-***4D8***
  - Semantically: [A-F0-9]{3} are last 3 digits of BDADDR

Address type: **Public** (0x00)
Address: **D0:D7:83**:F1:C***4:D8*** (HUAWEI)

- Regex: ^HUAWEI WATCH (3|3 Pro|GT|GT-2e)-[A-F0-9]{3}$ e.g. HUAWEI WATCH GT-***98E***
  - Semantically: [A-F0-9]{3} are last 3 digits of BDADDR
- I have yet to see a Huawei watch/fitness tracker that isn't uniquely identifiable and therefore trackable either by its BDADDR or name

Fitness (*People?*) Trackers / Watches

Huawei

- Regex: ^HUAWEI Band(| 2| 3e)-[A-F0-9]{3}$ e.g. HUAWEI Band 3e-***4D8***
  - Semantically: [A-F0-9]{3} are last 3 digits of BDADDR

Address type: **Public** (0x00)
Address: **D0:D7:83**:F1:C***4:D8*** (HUAWEI)

- Regex: ^HUAWEI WATCH (3|3 Pro|GT|GT-2e)-[A-F0-9]{3}$ e.g. HUAWEI WATCH GT-***98E***
  - Semantically: [A-F0-9]{3} are last 3 digits of BDADDR

Address type: **Public** (0x00)
Address: **88:11:96**:52:6***9:8E*** (HUAWEI)

- I have yet to see a Huawei watch/fitness tracker that isn't uniquely identifiable and therefore trackable either by its BDADDR or name

Fitness (*People?*) Trackers / Watches

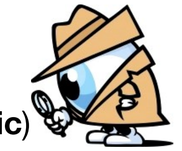
Samsung

- Regex: ^Gear S(2|3) \\\([A-F0-9]{4}\\\) LE$ e.g. Gear S3 (DB10) LE
- Regex: ^Gear Sport \\\([A-F0-9]{4}\\\) LE$ e.g. Gear Sport (DD36) LE
- Regex: ^Gear Fit(|2)(Pro) \\\([A-F0-9]{4}\\\)$ e.g. Gear Fit2 (***9BFB***)
- Regex: ^Galaxy Watch(|2|3|4|5) \\\([A-F0-9]{4}\\\) LE$ e.g. Galaxy Watch3 (68FB) LE
- Regex: ^Galaxy Watch Active(|2|3) \\\([A-F0-9]{4}\\\) LE$ e.g. Galaxy Watch Active2(21FE) LE

- I have yet to see a Samsung watch/fitness tracker that isn't uniquely identifiable and therefore trackable either by its BDADDR or name

Fitness (*People?*) Trackers / Watches

Samsung



Address type: Random (0x01)
Address: D0:63:50:30:F6:20 (**Static**)

- Regex: ^Gear S(2|3) \\\([A-F0-9]{4}\\\) LE$ e.g. Gear S3 (DB10) LE
- Regex: ^Gear Sport \\\([A-F0-9]{4}\\\) LE$ e.g. Gear Sport (DD36) LE
- Regex: ^Gear Fit(|2)(Pro) \\\([A-F0-9]{4}\\\)$ e.g. Gear Fit2 (***9BFB***)
- Regex: ^Galaxy Watch(|2|3|4|5) \\\([A-F0-9]{4}\\\) LE$ e.g. Galaxy Watch3 (68FB) LE
- Regex: ^Galaxy Watch Active(|2|3) \\\([A-F0-9]{4}\\\) LE$ e.g. Galaxy Watch Active2(21FE) LE

- I have yet to see a Samsung watch/fitness tracker that isn't uniquely identifiable and therefore trackable either by its BDADDR or name

Fitness (*People?*) Trackers / Watches

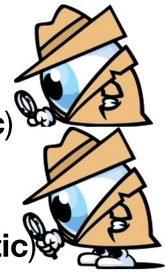
Samsung

- Regex: ^Gear S(2|3) \\\([A-F0-9]{4}\\\) LE$ e.g. Gear S3 (DB10) LE

Address type: Random (0x01)
Address: D0:63:50:30:F6:20 (**Static**)

- Regex: ^Gear Sport \\\([A-F0-9]{4}\\\) LE$ e.g. Gear Sport (DD36) LE

Address type: Random (0x01)
Address: D8:D0:87:BB:3A:6C (**Static**)



- Regex: ^Gear Fit(|2)(Pro) \\\([A-F0-9]{4}\\\)$ e.g. Gear Fit2 (***9BFB***)
- Regex: ^Galaxy Watch(|2|3|4|5) \\\([A-F0-9]{4}\\\) LE$ e.g. Galaxy Watch3 (68FB) LE
- Regex: ^Galaxy Watch Active(|2|3) \\\([A-F0-9]{4}\\\) LE$ e.g. Galaxy Watch Active2(21FE) LE

- I have yet to see a Samsung watch/fitness tracker that isn't uniquely identifiable and therefore trackable either by its BDADDR or name

Fitness (*People?*) Trackers / Watches

Samsung

- Regex: ^Gear S(2|3) \\\([A-F0-9]{4}\\\) LE$ e.g. Gear S3 (DB10) LE

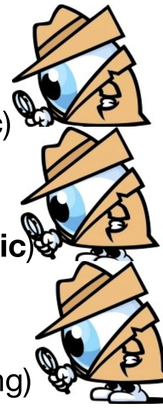
Address type: Random (0x01)
Address: D0:63:50:30:F6:20 (**Static**)

- Regex: ^Gear Sport \\\([A-F0-9]{4}\\\) LE$ e.g. Gear Sport (DD36) LE

Address type: Random (0x01)
Address: D8:D0:87:BB:3A:6C (**Static**)

- Regex: ^Gear Fit(|2)(Pro) \\\([A-F0-9]{4}\\\)$ e.g. Gear Fit2 (***9BFB***)

Address type: **Public** (0x00)
Address: **78:00:9E**:A9:***9B:FB*** (Samsung)



- Regex: ^Galaxy Watch(|2|3|4|5) \\\([A-F0-9]{4}\\\) LE$ e.g. Galaxy Watch3 (68FB) LE
- Regex: ^Galaxy Watch Active(|2|3) \\\([A-F0-9]{4}\\\) LE$ e.g. Galaxy Watch Active2(21FE) LE

- I have yet to see a Samsung watch/fitness tracker that isn't uniquely identifiable and therefore trackable either by its BDADDR or name

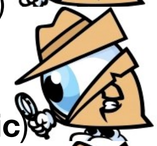
Fitness (*People?*) Trackers / Watches

Samsung

- Regex: ^Gear S(2|3) \\\([A-F0-9]{4}\\\) LE$ e.g. Gear S3 (DB10) LE

Address type: Random (0x01)
Address: D0:63:50:30:F6:20 (**Static**)

- Regex: ^Gear Sport \\\([A-F0-9]{4}\\\) LE$ e.g. Gear Sport (DD36) LE

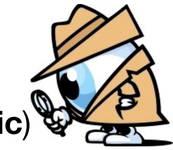


Address type: Random (0x01)
Address: D8:D0:87:BB:3A:6C (**Static**)

- Regex: ^Gear Fit(|2)(Pro) \\\([A-F0-9]{4}\\\)$ e.g. Gear Fit2 (***9BFB***)

Address type: **Public** (0x00)
Address: **78:00:9E**:A9:***9B:FB*** (Samsung)

- Regex: ^Galaxy Watch(|2|3|4|5) \\\([A-F0-9]{4}\\\) LE$ e.g. Galaxy Watch3 (68FB) LE



Address type: Random (0x01)
Address: E4:06:FE:C2:D0:F7 (**Static**)

- Regex: ^Galaxy Watch Active(|2|3) \\\([A-F0-9]{4}\\\) LE$ e.g. Galaxy Watch Active2(21FE) LE

- I have yet to see a Samsung watch/fitness tracker that isn't uniquely identifiable and therefore trackable either by its BDADDR or name

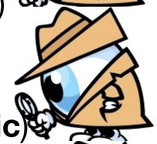
Fitness (*People?*) Trackers / Watches

Samsung

- Regex: ^Gear S(2|3) \\\([A-F0-9]{4}\\\) LE$ e.g. Gear S3 (DB10) LE

Address type: Random (0x01)
Address: D0:63:50:30:F6:20 (**Static**)

- Regex: ^Gear Sport \\\([A-F0-9]{4}\\\) LE$ e.g. Gear Sport (DD36) LE



Address type: Random (0x01)
Address: D8:D0:87:BB:3A:6C (**Static**)

- Regex: ^Gear Fit(|2)(Pro) \\\([A-F0-9]{4}\\\)$ e.g. Gear Fit2 (***9BFB***)

Address type: **Public** (0x00)
Address: **78:00:9E**:A9:***9B:FB*** (Samsung)

- Regex: ^Galaxy Watch(|2|3|4|5) \\\([A-F0-9]{4}\\\) LE$ e.g. Galaxy Watch3 (68FB) LE

Address type: Random (0x01)
Address: E4:06:FE:C2:D0:F7 (**Static**)

- Regex: ^Galaxy Watch Active(|2|3) \\\([A-F0-9]{4}\\\) LE$ e.g. Galaxy Watch Active2(21FE) LE

Address type: Random (0x01)
Address: C0:B9:B5:F8:E3:B2 (**Static**)

- I have yet to see a Samsung watch/fitness tracker that isn't uniquely identifiable and therefore trackable either by its BDADDR or name

Galaxy Watch Active2(21FE) LE On Vacation?

(Ocean City is a Maryland vacation / beach town)

Galaxy Watch Active2(21FE) LE On Vacation?

(Ocean City is a Maryland vacation / beach town)

Mini-Takeaway

Tracking

- If there were some other service than WiGLE, keeping *all* data points, then crowdsourced collection would show increasingly-detailed information about the movements of non-randomized devices (and thus people)

Fitness (*People?*) Trackers / Watches

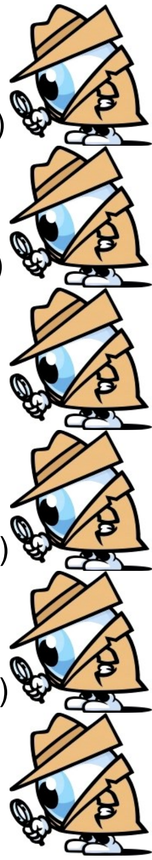
Fitbit

- Regex: ^Versa(| 2| 3| 4| Lite)$ e.g. Versa 2
- Regex: ^Inspire(| HR| 2| 3)$ e.g. Inspire HR
- Regex: ^Alta(| HR)$ e.g. Alta HR
- Regex: ^Ionic$
- Regex: ^Flex(| 2)$ e.g. Flex 2
- Regex: ^One$ e.g. One

Fitness (*People?*) Trackers / Watches

Fitbit

- Regex: ^Versa(| 2| 3| 4| Lite)$ e.g. Versa 2
- Regex: ^Inspire(| HR| 2| 3)$ e.g. Inspire HR
- Regex: ^Alta(| HR)$ e.g. Alta HR
- Regex: ^Ionic$
- Regex: ^Flex(| 2)$ e.g. Flex 2
- Regex: ^One$ e.g. One



Address type: Random (0x01)
Address: ED:BD:7C:77:18:EC (**Static**)

Address type: Random (0x01)
Address: D8:D0:87:BB:3A:6C (**Static**)

Address type: Random (0x01)
Address: DF:22:47:91:6D:B7 (**Static**)

Address type: Random (0x01)
Address: CA:C3:40:DB:BC:64 (**Static**)

Address type: Random (0x01)
Address: CA:C3:40:DB:BC:64 (**Static**)

Address type: Random (0x01)
Address: F2:0A:E8:4C:4D:4B (**Static**)

Vendor-specific 128-bit UUIDs

- *abba*ff00-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

- *abba*ff00-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)
```

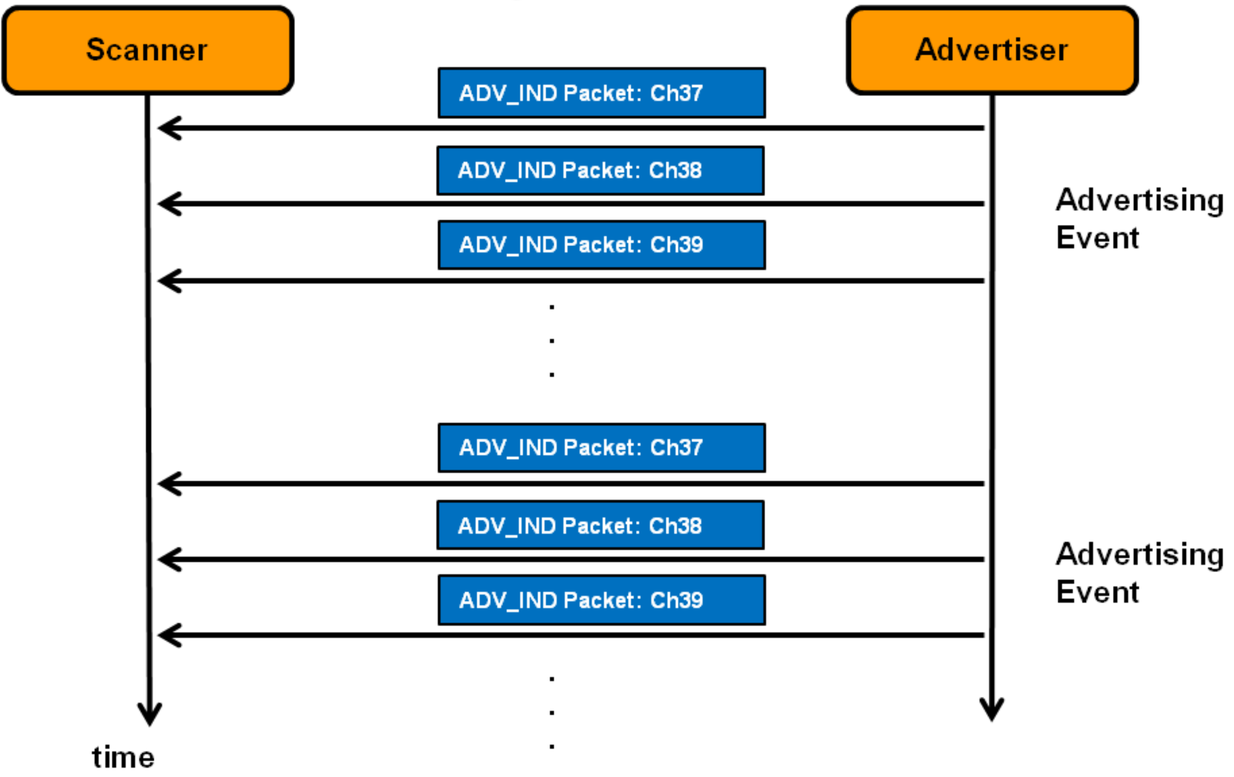
Vendor-specific 128-bit UUIDs

- *abba*ff00-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

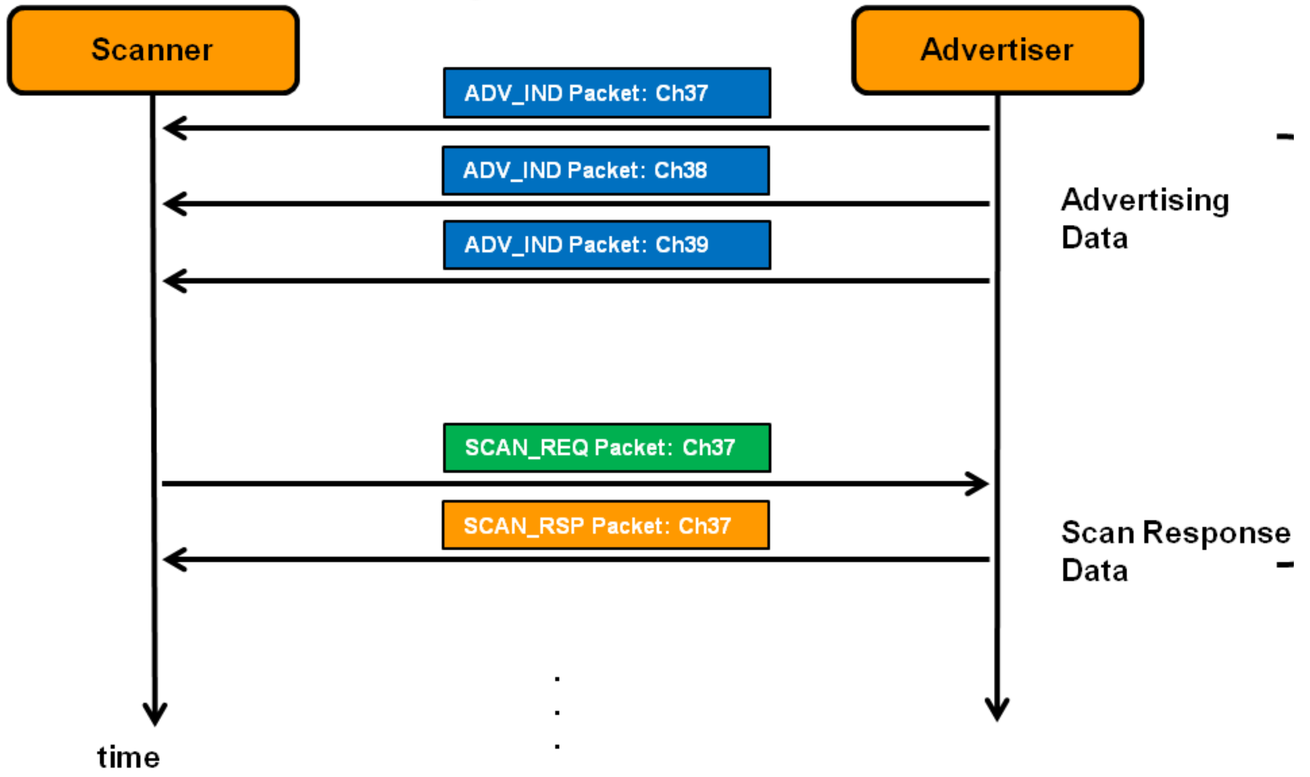
> HCI Event: LE Meta Event (0x3e) plen 42
  LE Advertising Report (0x02)
    Num reports: 1
    Event type: Connectable undirected - **ADV_IND** (0x00)
    Address type: Random (0x01)
    Address: F5:6E:B2:C3:73:D2 (Static)
    Data length: 30
    Flags: 0x06
      LE General Discoverable Mode
      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)

Background

Passive Scanning



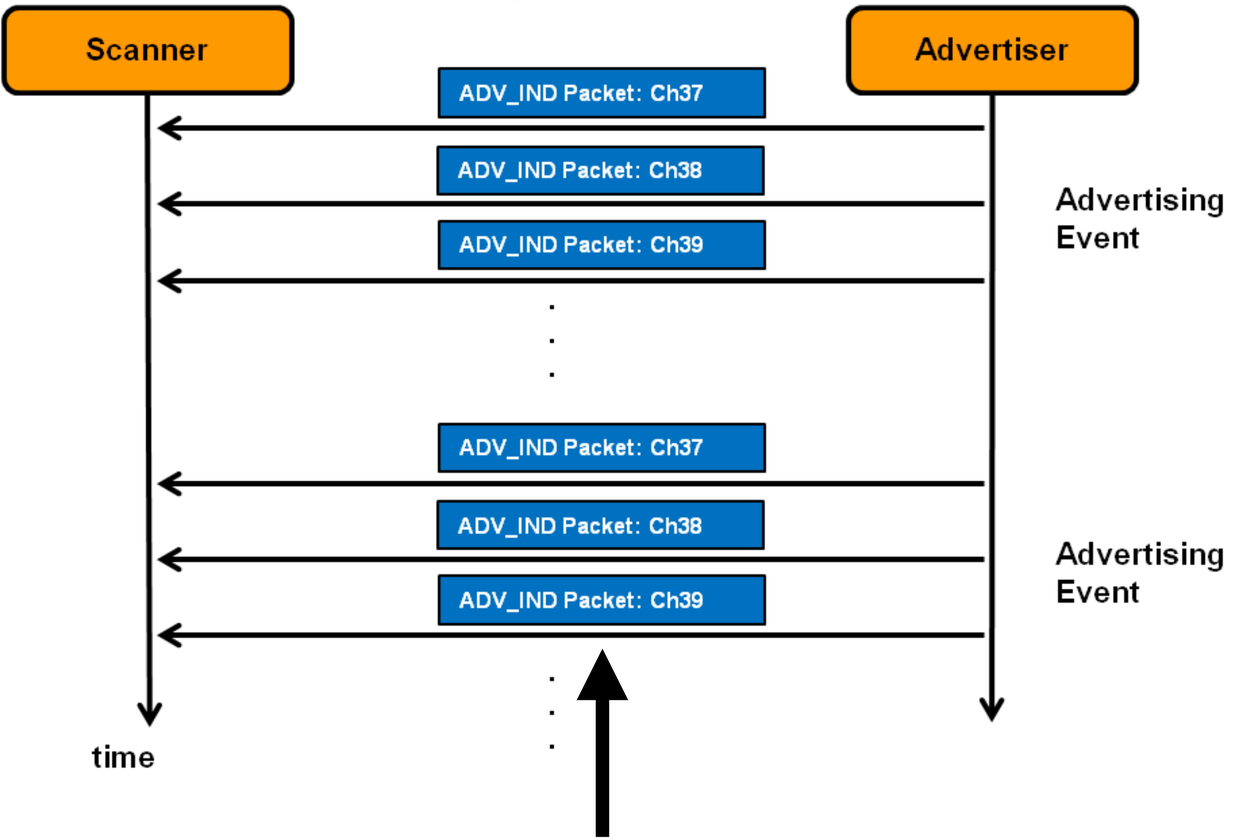
Active Scanning



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

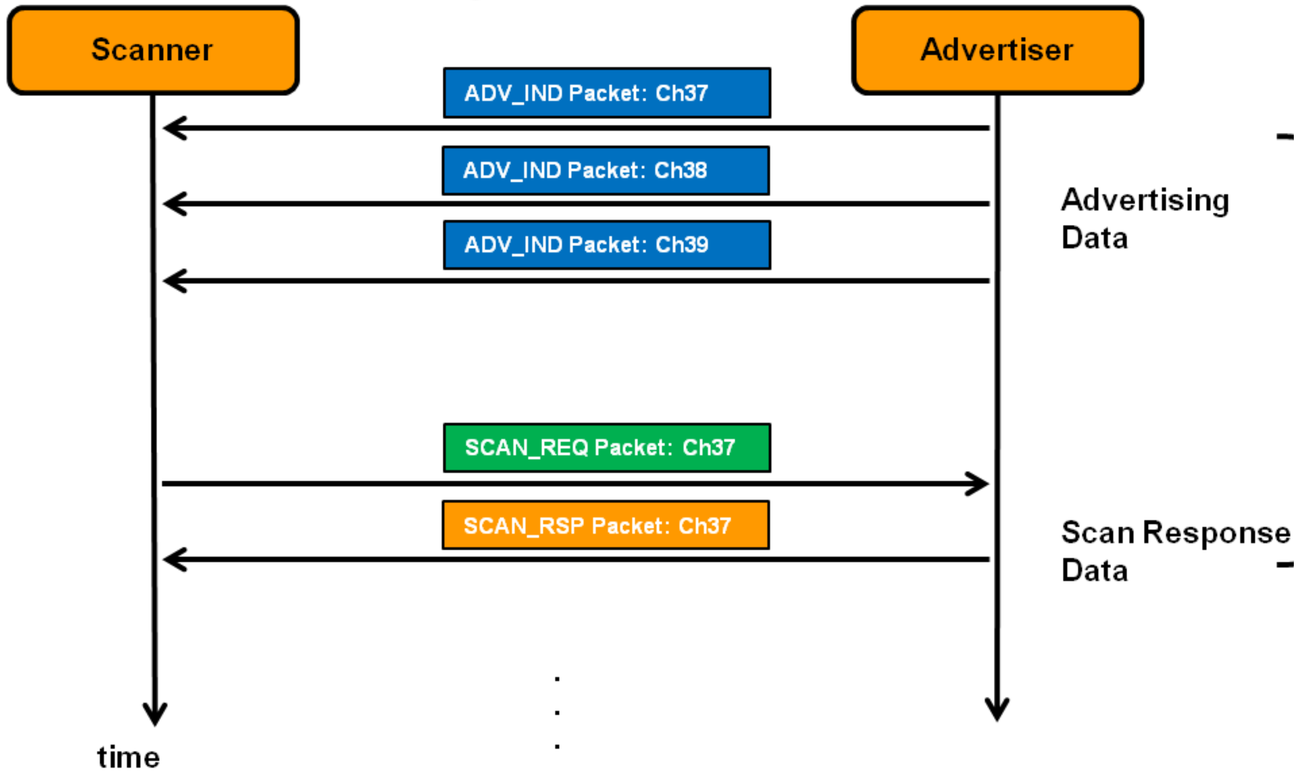
Background

Passive Scanning



Sometimes the name will be here

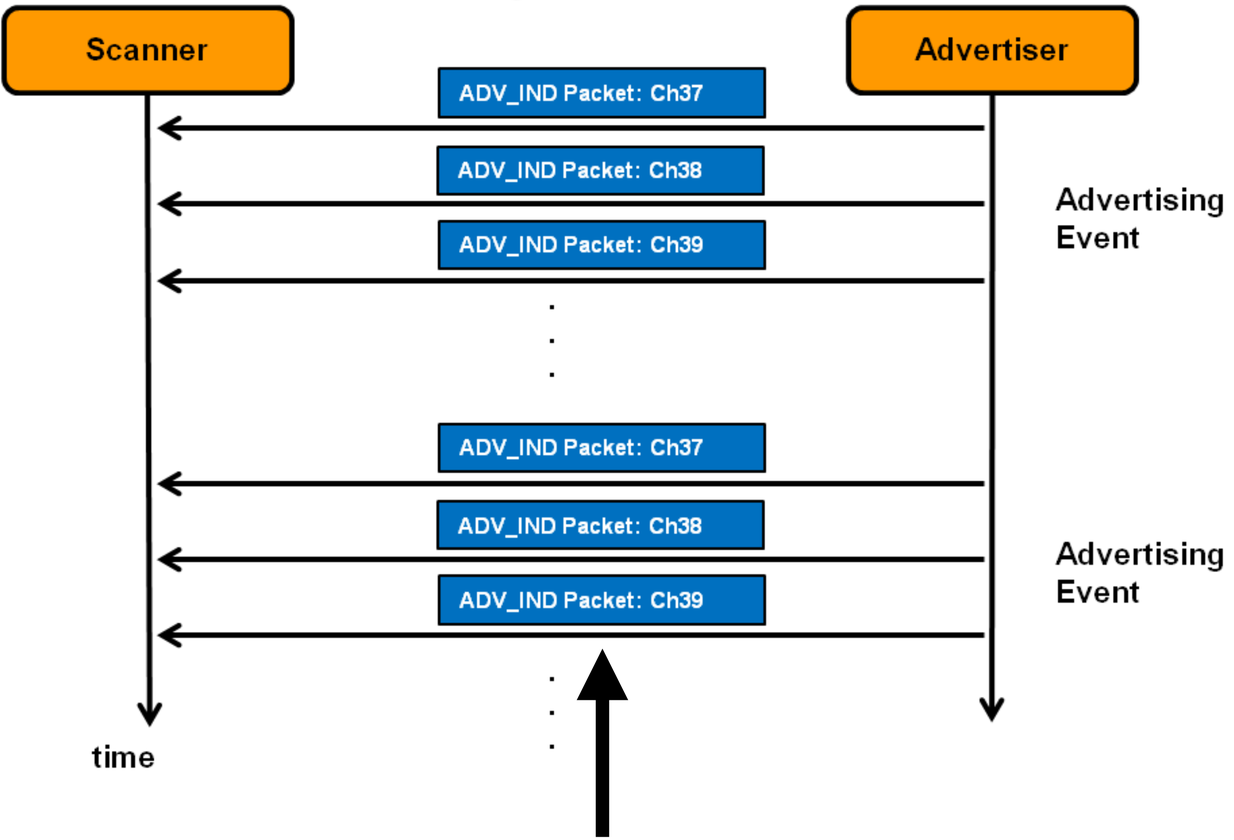
Active Scanning



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

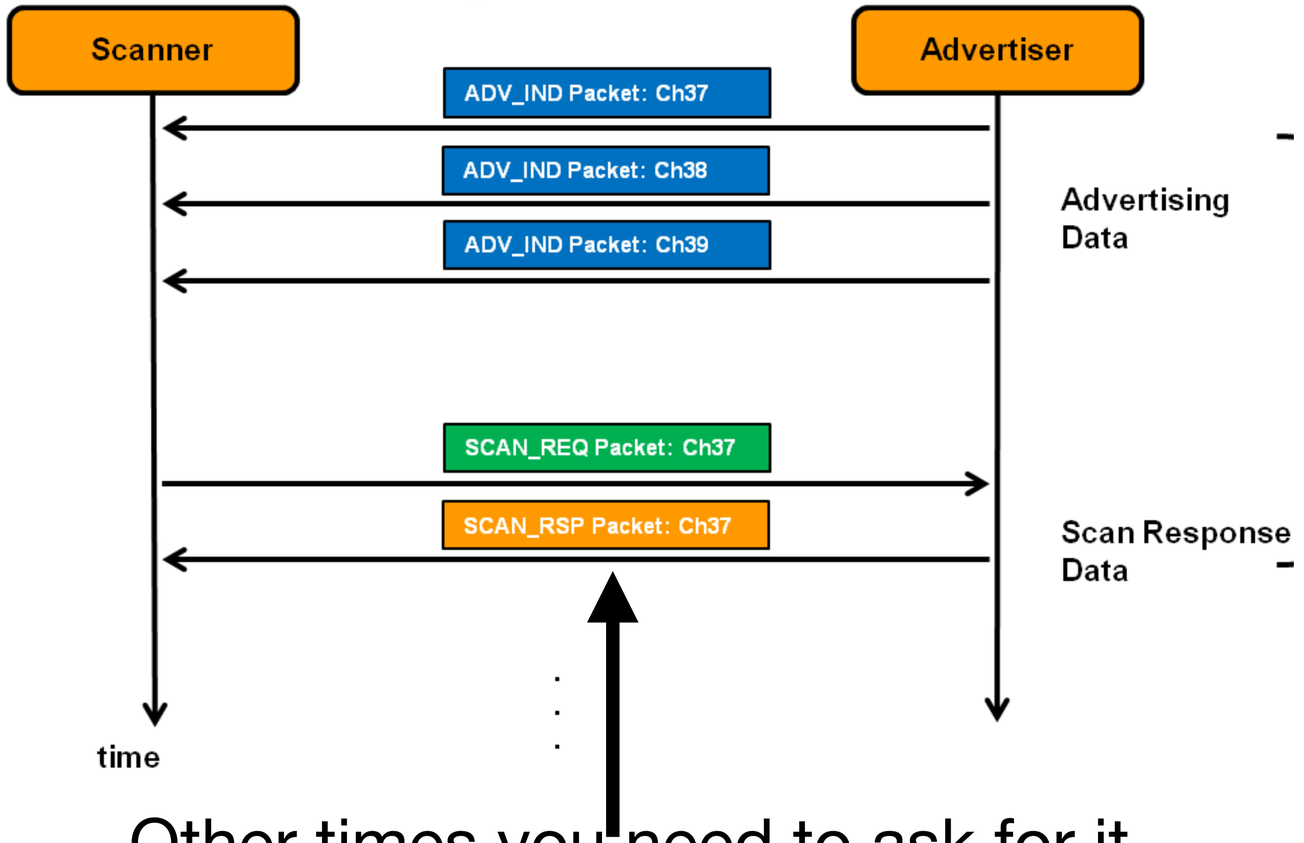
Background

Passive Scanning



Sometimes the name will be here

Active Scanning



Other times you need to ask for it, and it comes back in the SCAN_RSP

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

Find New Devices

I hadn't previously sorted any of the devices in bold as being fitbits

I suppose I should have looked at https://en.wikipedia.org/wiki/List_of_Fitbit_products, but I didn't care that much

btmon -T -r logs/btmon/2023-02-07-05-51-24_pi1.bin | grep -A 3 **bffaa68956ba** | grep Name | sort | uniq

Name (complete): **Ace 2**

Name (complete): **Ace 3**

Name (complete): Alta HR

Name (complete): **Blaze**

Name (complete): **Charge 2**

Name (complete): **Charge 3**

Name (complete): Flex 2

Name (complete): Inspire 2

Name (complete): Inspire HR

Name (complete): Versa Lite

Name (complete): **Zip**

btmon -T -r logs/btmon/2023-02-07-05-51-24_pi1.bin | grep -A 3 **8b17cf6cbfe8** | grep Name | sort | uniq

Name (complete): **Charge 4**

Name (complete): **Charge 5**

Name (complete): Inspire 3

Name (complete): **Luxe**

Name (complete): **Sense**

Name (complete): Versa

Name (complete): Versa 2

Name (complete): Versa 3

Mini-Takeaway

Vendor & model identification

- 128 bit service UUIDs are useful
  - *to associate products with vendors*, even without human-readable names
    - and even within a *completely passive* scanner
  - to determine how similar one generation of product is to the next
  - to find similarities across product lines

Fitness (*People?*) Trackers / Watches

Apple

Fitness (*People?*) Trackers / Watches

Apple

- Apple *does the right thing* (from a spec perspective) and sets the BDADDR as a "random private resolvable address" that changes every ~15 minutes

Fitness (*People?*) Trackers / Watches

Apple

- Apple *does the right thing* (from a spec perspective) and sets the BDADDR as a "random private resolvable address" that changes every ~15 minutes

Fitness (*People?*) Trackers / Watches

Apple

- Apple *does the right thing* (from a spec perspective) and sets the BDADDR as a "random private resolvable address" that changes every ~15 minutes
- However☝🤓... privacy researchers have found that messages shared over Bluetooth to support the "Continuity/Hand-Off" features (seamless hand-off / data transfer between devices) can still be used to enable tracking on Apple devices

Fitness (*People?*) Trackers / Watches

Apple

- Apple *does the right thing* (from a spec perspective) and sets the BDADDR as a "random private resolvable address" that changes every ~15 minutes
- However☝🤓... privacy researchers have found that messages shared over Bluetooth to support the "Continuity/Hand-Off" features (seamless hand-off / data transfer between devices) can still be used to enable tracking on Apple devices

DE GRUYTER OPEN Proceedings on Privacy Enhancing Technologies ..; .. (..):1–20

Jeremy Martin*, Douglas Alpuche, Kristina Bodeman, Lamont Brown, Ellis Fenske*, Lucas Foppe, Travis Mayberry*, Erik Rye*, Brandon Sipes, and Sam Teplov

Handoff All Your Privacy – A Review of Apple's Bluetooth Low Energy Continuity Protocol

https://arxiv.org/pdf/1904.10600.pdf

sciendo Proceedings on Privacy Enhancing Technologies ; 2020 (1):26–46

Guillaume Celosia* and Mathieu Cunche

Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols

https://petsymposium.org/popets/2020/popets-2020-0003.pdf

In the Car

ODBII-to-BT

- ^FIXD$: ("ISSC Technologies Corp." or "SHENZHEN XIN FEI JIA ELECTRONIC CO. LTD." or "SST Taiwan Ltd." or no match OUI)
  - I connected to one of these with their app, and it didn't seem to have auth? (But couldn't get meaningful data since car was turned off)
- ^OBDBLE$ and ^Zus$: ("NO NDA Inc" OUI)
- ^OBDeleven 2$: Voltas IT https://obdeleven.com/ ("Teltonika" OUI)
- ^OBDLink CX$: OBD Solutions, LLC. ("Dialog Semiconductor Hellas SA" OUI)
- ^OBDII$: Unknown brand (could be white-label), but highly likely ODBII-to-BT car monitor

Plug-N-Pwned: Comprehensive Vulnerability Analysis of OBD-II Dongles as A New Over-the-Air Attack Surface in Automotive IoT

Haohuang Wen[1], Qi Alfred Chen[2], Zhiqiang Lin[1]

[1]Ohio State University
[2]University of California, Irvine

USENIX Security 2020

From https://www.usenix.org/system/files/sec20_slides_wen.pdf

In the Car

Misc

In the Car

Misc

- ^ESCORT REDLINE 360c$: Radar Detector (illegal in many countries & 2 US states)

In the Car

Misc

- ^ESCORT REDLINE 360c$: Radar Detector (illegal in many countries & 2 US states)
- ^RAD 480i$: Radar Detector

In the Car

Misc

- ^ESCORT REDLINE 360c$: Radar Detector (illegal in man states)
- ^RAD 480i$: Radar Detector
- Custom LED headlights
  - ^Triones[-#:^][0-9A-F]{8,12}$ e.g. "Triones#FFFF700F4871" or "Triones-B7FED4EA"
  - Semantically: Triones#{non-deliminated BDADDR}

In the Car

Misc

- ^ESCORT REDLINE 360c$: Radar Detector (illegal in man states)
- ^RAD 480i$: Radar Detector
- Custom LED headlights
  - ^Triones[-#:^][0-9A-F]{8,12}$ e.g. "Triones#FFFF700F4871" or "Triones-B7FED4EA"
  - Semantically: Triones#{non-deliminated BDADDR}

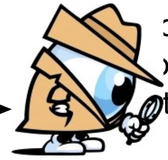
```
> HCI Event: LE Meta Event (0x3e) plen 37
    LE Advertising Report (0x02)
      Num reports: 1
      Event type: Connectable undirected - ADV_IND (0x00)
      Address type: Public (0x00)
      Address: FF:FF:EA:00:34:84 (OUI FF-FF-EA)
      Data length: 25
      Flags: 0x06
        LE General Discoverable Mode
        BR/EDR Not Supported
      Name (complete): Triones-FFFFEA003484
      RSSI: -83 dBm (0xad)
```

In the Car

Misc

- ^ESCORT REDLINE 360c$: Radar Detector (illegal in man states)
- ^RAD 480i$: Radar Detector
- Custom LED headlights
  - ^Triones[-#:^][0-9A-F]{8,12}$ e.g. "Triones#FFFF700F4871" or "Triones-B7FED4EA"
  - Semantically: Triones#{non-

Congrats! Your car can now be tracked by its headlights!



> HCI Event: LE Meta Event (0x3e) plen 37
LE Advertising Report (0x02)
orts: 1
e: Connectable undirected - ADV_IND (0x00)
type: **Public** (0x00)
FF:FF:EA:00:34:84 (OUI FF-FF-EA)
Data length: 25
Flags: 0x06
LE General Discoverable Mode
BR/EDR Not Supported
Name (complete): Triones-**FFFFEA003484**
RSSI: -83 dBm (0xad)

A Quick Word About Threat Models

BT sniffers vs. automated license plate readers (ALPRs)

- It is starting to become common to surreptitiously install automated license plate scanners in public places [1][2]
- For any device that is *not* adequately randomizing its identity, bluetooth scanners can serve as much the same function
  - I once spoke with a local county police officer who had brought this up without prompting
- Thus far I've only seen BT tracking discussed in the context of advertisement [3], not forensically placing criminals at a given location based on BT data

[1] https://www.eff.org/pages/automated-license-plate-readers-alpr
[2] https://theintercept.com/2023/03/22/hoa-surveillance-license-plate-police-flock/
[3] https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html

A Quick Word About Threat Models

Surveillance vs. Sousveillance

- The sword cuts both ways ⚔️: surveillance or sousveillance
  - "Sousveillance (/suːˈveɪləns/ soo-VAY-lənss) is the recording of an activity by a member of the public, rather than a person or organisation in authority, typically by way of small wearable or portable personal technologies."
    - https://en.wikipedia.org/wiki/Sousveillance
  - WiGLE is an example of sousveilance

Body Worn Cameras

- Regex: ^TW370_[A-Z]{3}[0-9]{5}$ e.g. TW370_QDA00224
  - Semantically: TW370_{serial}
- I knew based on the GPS location, that I had driven past an officer who had stopped a motorist in an uncommon location

Body Worn Cameras

- Regex: ^TW370_[A-Z]{3}[0-9]{5}$ e.g. TW370_QDA00224
  - Semantically: TW370_{serial}

From eBay

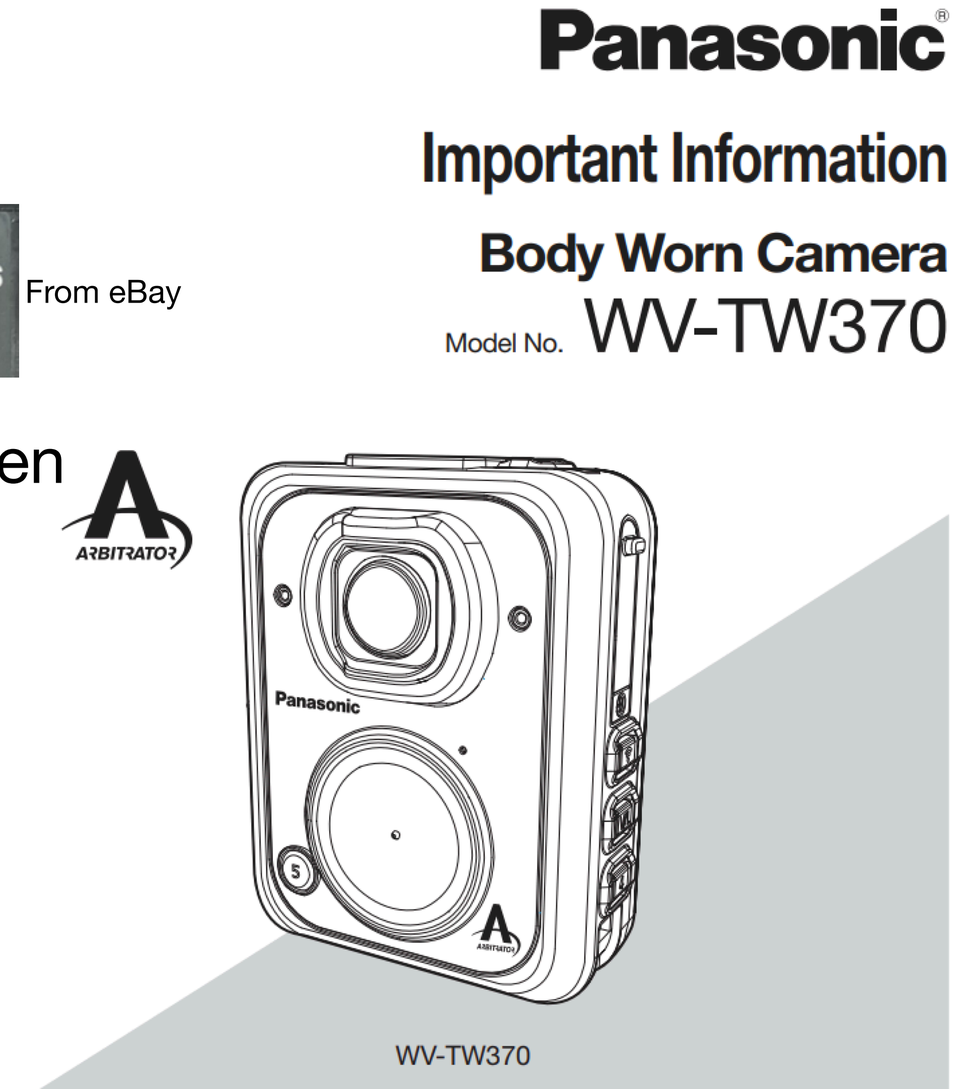
- I knew based on the GPS location, that I had driven past an officer who had stopped a motorist in an uncommon location

Body Worn Cameras

- Regex: ^TW370_[A-Z]{3}[0-9]{5}$ e.g. TW370_QDA00224
  - Semantically: TW370_{serial}

From eBay

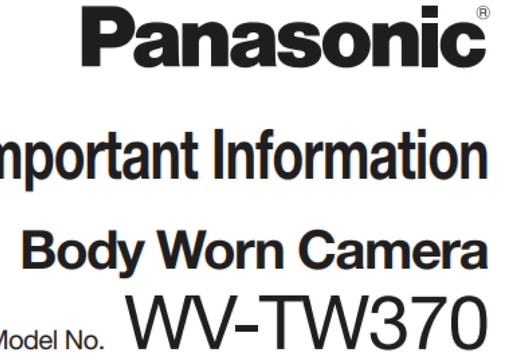
- I knew based on the GPS location, that I had driven past an officer who had stopped a motorist in an uncommon location



Body Worn Cameras

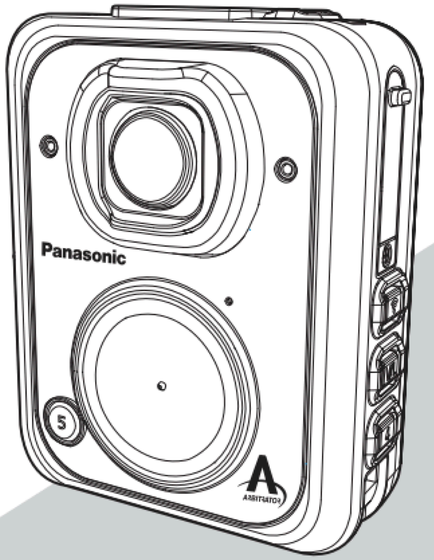
- Regex: ^TW370_[A-Z]{3}[0-9]{5}$ e.g. TW370_QDA00224
  - Semantically: TW370_{serial}

From eBay



- I knew based on the GPS location, that I had driven past an officer who had stopped a motorist in an uncommon location

> HCI Event: LE Meta Event (0x3
  LE Advertising Report (0x02)
    Num reports: 1
    Event type: Connectable und_IND (0x00)
    Address type: **Public** (0x00)
    Address: BC:C3:42:54:63:AD (**Panasonic Communications Co., Ltd.**)
    Data length: 21
    Flags: 0x06
      LE General Discoverable Mode
      BR/EDR Not Supported
    128-bit Service UUIDs (complete): 1 entry

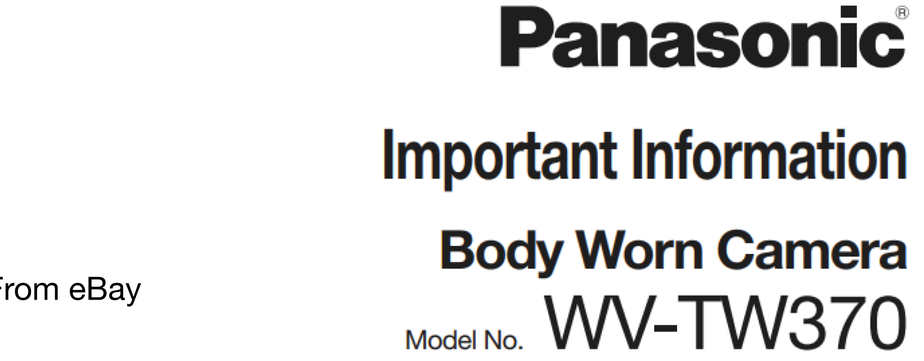


WV-TW370

Body Worn Cameras

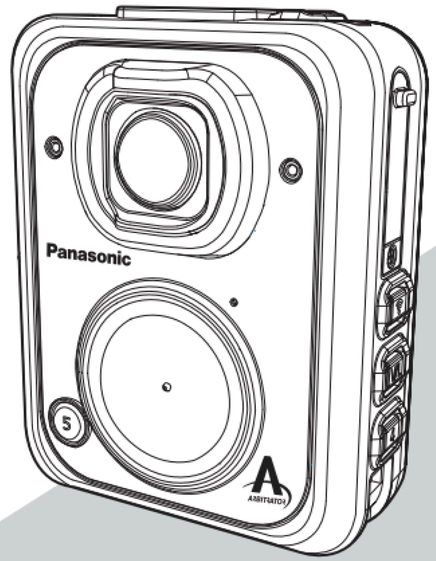
- Regex: ^TW370_[A-Z]{3}[0-9]{5}$ e.g. TW370_QDA00224
  - Semantically: TW370_{serial}

From eBay

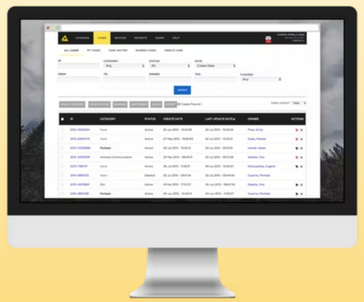


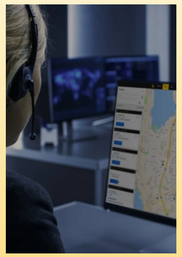
- I knew based on the GPS location, that I had driven past an officer who had stopped a motorist in an uncommon location

> HCI Event: LE Meta Event (0x3
  LE Advertising Report (0x02)
    Num reports: 1
    Event type: Connectable und _IND (0x00)
    Address type: **Public** (0x00)
    Address: BC:C3:42:54:63:AD (**Panasonic Communications Co., Ltd.**)
    Data length: 21
    Flags: 0x06
      LE General Discoverable Mode
      BR/EDR Not Supported
    128-bit Service UUIDs (complete): 1 entry

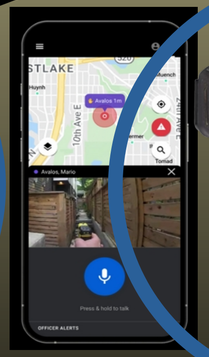


WV-TW370

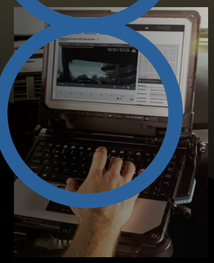


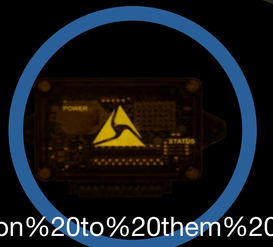


Evidence.com



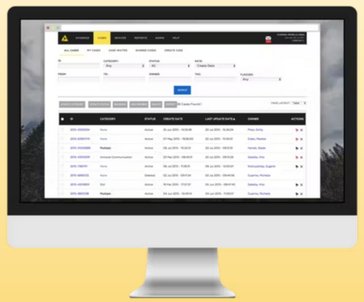
“Drone as first responder”

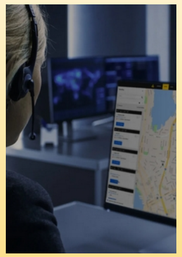




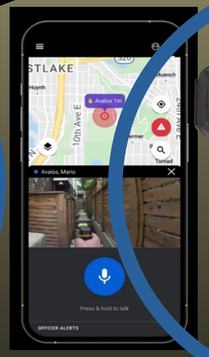
“[Bi-directional communications] is a lot faster than to have to stop what I am doing, to key up on my radio.”

https://media.defcon.org/DEF%20CON%2031/DEF%20CON%2031%20presentations/nullagent%20rekcahdam%20-%20Snoop%20on%20to%20them%20as%20they%20snoop%20on%20to%20us.pdf

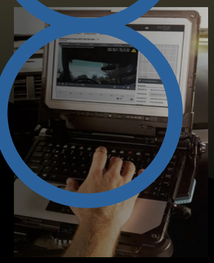


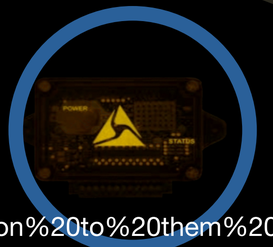


Evidence.com



“Drone as first responder”



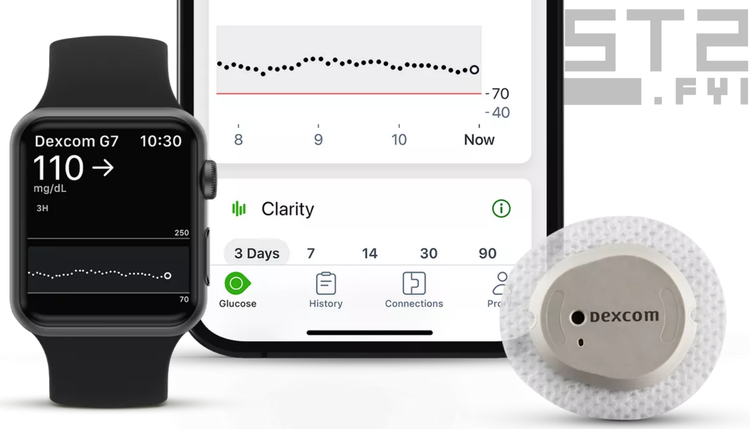


“[Bi-directional communications] is a lot faster than to have to stop what I am doing, to key up on my radio.”

https://media.defcon.org/DEF%20CON%2031/DEF%20CON%2031%20presentations/nullagent%20rekcahdam%20-%20Snoop%20on%20to%20them%20as%20they%20snoop%20on%20to%20us.pdf

Medical 😬

Continuous Glucose Monitoring System



- Regex: ^Dexcom[A-Z0-9]{2}$ e.g. "DexcomBR" or "Dexcom36"

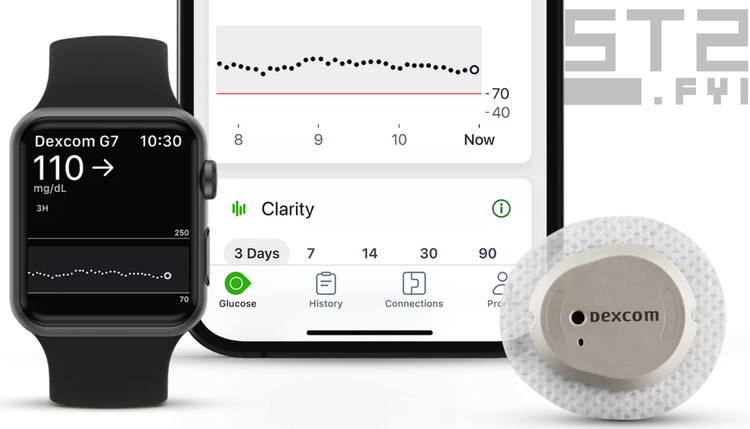
```
For bdaddr = c2:33:98:f6:fd:4f:
        Company Name by IEEE OUI (c2:33:98): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: Dexcom9Q
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^Dexcom[A-Z0-9]{2}$: Dexcom Continuous Glucose Monitoring System (https://www.d
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
        DeviceName: Dexcom9Q
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^Dexcom[A-Z0-9]{2}$: Dexcom Continuous Glucose Monitoring System (https://www.d
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        UUID16s found:
                UUID16 0xfebc (Company ID: Dexcom Inc)
                         Found in BT LE data (LE_bdaddr_to_UUID16s)
                UUID16 0xfebc (Company ID: Dexcom Inc)
                         Found in BT LE data (LE_bdaddr_to_UUID16s)

        No transmit power found.

        No Appearance data found.
```

Dexcom
Pairing
Please wait, transmitter and receiver pairing...
May take 30 minutes.
Keep receiver within 6 meters of transmitter.
DexcomG6
70
40
8
9
10
Now
Clarity
3 Days
7
14
30
90
Glucose
History
Connections
dexcom
toring System (https://www.d
tising (ADV_IND)
toring System (https://www.d

Dexcom
Pairing
Please wait, transmitter and receiver pairing...
May take 30 minutes. Keep receiver within 6 meters of transmitter.

Medical 😬

Continuous Glucose Monitoring System

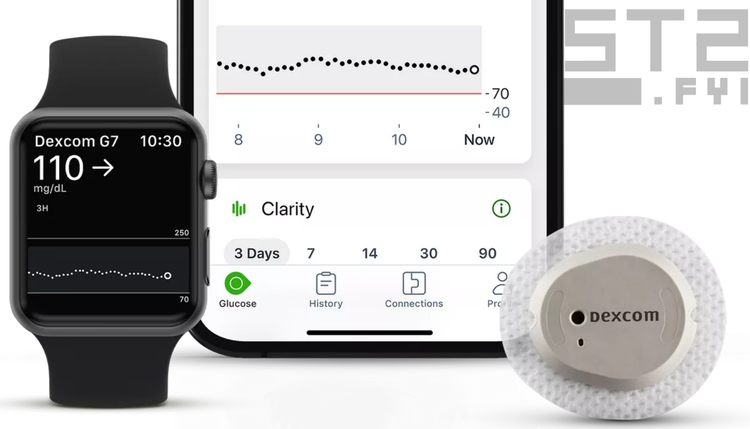


- Regex: ^Dexcom[A-Z0-9]{2}$ e.g. "DexcomBR" or "Dexcom36"

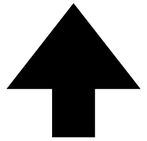
```
For bdaddr = c2:33:98:f6:fd:4f:
        Company Name by IEEE OUI (c2:33:98): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: Dexcom9Q
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^Dexcom[A-Z0-9]{2}$: Dexcom Continuous Glucose Monitoring System (https://www.d
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
        DeviceName: Dexcom9Q
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^Dexcom[A-Z0-9]{2}$: Dexcom Continuous Glucose Monitoring System (https://www.d
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        UUID16s found:
                UUID16 0xfebc (Company ID: Dexcom Inc)
                         Found in BT LE data (LE_bdaddr_to_UUID16s)
                UUID16 0xfebc (Company ID: Dexcom Inc)
                         Found in BT LE data (LE_bdaddr_to_UUID16s)

        No transmit power found.

        No Appearance data found.
```

Medical 😬

Continuous Glucose Monitoring System



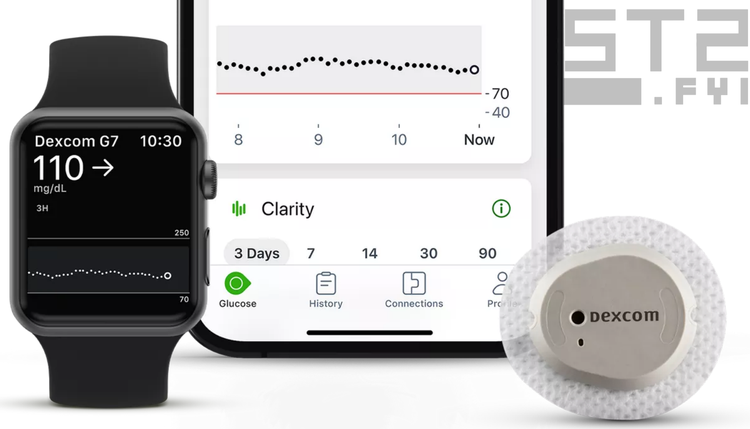
- Regex: ^Dexcom[A-Z0-9]{2}$ e.g. "DexcomBR" or "Dexcom36"



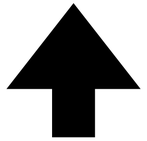
```
For bdaddr = c2:33:98:f6:fd:4f:
        Company Name by IEEE OUI (c2:33:98): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: Dexcom9Q
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^Dexcom[A-Z0-9]{2}$: Dexcom Continuous Glucose Monitoring System (https://www.d
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
        DeviceName: Dexcom9Q
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^Dexcom[A-Z0-9]{2}$: Dexcom Continuous Glucose Monitoring System (https://www.d
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        UUID16s found:
                UUID16 0xfebc (Company ID: Dexcom Inc)
                        Found in BT LE data (LE_bdaddr_to_UUID16s)
                UUID16 0xfebc (Company ID: Dexcom Inc)
                        Found in BT LE data (LE_bdaddr_to_UUID16s)

        No transmit power found.

        No Appearance data found.
```

Medical 😬

Continuous Glucose Monitoring System



- Regex: ^Dexcom[A-Z0-9]{2}$ e.g. "DexcomBR" or "Dexcom36"



```
For bdaddr = c2:33:98:f6:fd:4f:
        Company Name by IEEE OUI (c2:33:98): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: Dexcom9Q
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^Dexcom[A-Z0-9]{2}$: Dexcom Continuous Glucose Monitoring System (https://www.d
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
        DeviceName: Dexcom9Q
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^Dexcom[A-Z0-9]{2}$: Dexcom Continuous Glucose Monitoring System (https://www.d
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        UUID16s found:
                UUID16 0xfebc (Company ID: Dexcom Inc)
                        Found in BT LE data (LE_bdaddr_to_UUID16s)
                UUID16 0xfebc (Company ID: Dexcom Inc)
                        Found in BT LE data (LE_bdaddr_to_UUID16s)

        No transmit power found.

        No Appearance data found.
```

👀

Medical 😬

```
For bdaddr = c2:33:98:t6:fd:4f:
        Company Name by IEEE OUI (c2:33:98): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: Dexcom9Q
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^Dexcom[A-Z0-9]{2}$: Dexcom Continuous Glucose Monitoring System (http   www.d
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
        DeviceName: Dexcom9Q
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^Dexcom[A-Z0-9]{2}$: Dexcom Continuous Glucose Monitoring System (https://www.d
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        UUID16s found:
                UUID16 0xfebc (Company ID: Dexcom Inc)
                        Found in BT LE data (LE_bdaddr_to_UUID16s)
                UUID16 0xfebc (Company ID: Dexcom Inc)
                        Found in BT LE data (LE_bdaddr_to_UUID16s)

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x00d0 (Dexcom, Inc  ke with a grain of salt, not all companies populate this accurately!
                        Endianness-flipped device comp    (in case the vendor used the wrong endianness): 0xd000 (No Match)
                Raw Data: 3703
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 1 (Random Static)
                        This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
                Device Company ID: 0x00d0 (Dexcom, 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): 0xd000 (No Match)
                Raw Data: 3703
```

👀

Medical 😬

```
For bdaddr = c2:33:98:t6:fd:4f:
        Company Name by IEEE OUI (c2:33:98): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: Dexcom9Q
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^Dexcom[A-Z0-9]{2}$: Dexcom Continuous Glucose Monitoring System (http   www.d
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
        DeviceName: Dexcom9Q
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^Dexcom[A-Z0-9]{2}$: Dexcom Continuous Glucose Monitoring System (https://www.d
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        UUID16s found:
                UUID16 0xfebc (Company ID: Dexcom Inc)
                        Found in BT LE data (LE_bdaddr_to_UUID16s)
                UUID16 0xfebc (Company ID: Dexcom Inc)
                        Found in BT LE data (LE_bdaddr_to_UUID16s)

        No transmit power found.

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x00d0 (Dexcom, Inc.) - take with a grain of salt, not all companies populate this accurately!
                        Endian   flipped device company ID (in case the vendor used the wrong endianness): 0xd000 (No Match)
                Raw Data: 3703
                        In BT L  Da a (LE_bdaddr_to_mf_specific), bdaddr_random = 1 (Random Static)
                        This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
                Device Company ID: 0x00d0 (Dexcom, 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): 0xd000 (No Match)
                Raw Data: 3703
```

👀

Medical 😬

Insulin Pump

- Regex: ^tslim X2 ***[0-9]{3}$ e.g. "tslim X2 ***611"
    - Semantically: I'm *guessing* the ***[0-9]{3} is a masked form of the serial number, for people to more easily identify their device

Medical 😬

Insulin Pump

- Regex: ^tslim X2 ***[0-9]{3}$ e.g. "tslim X2 ***611"
  - Semantically: I'm *guessing* the ***[0-9]{3} is a masked form of the serial number, for people to more easily identify their device

https://fccid.io/CWO-TWM001/Internal-Photos/internal-photos-1721032

Medical 😬

Insulin Pump

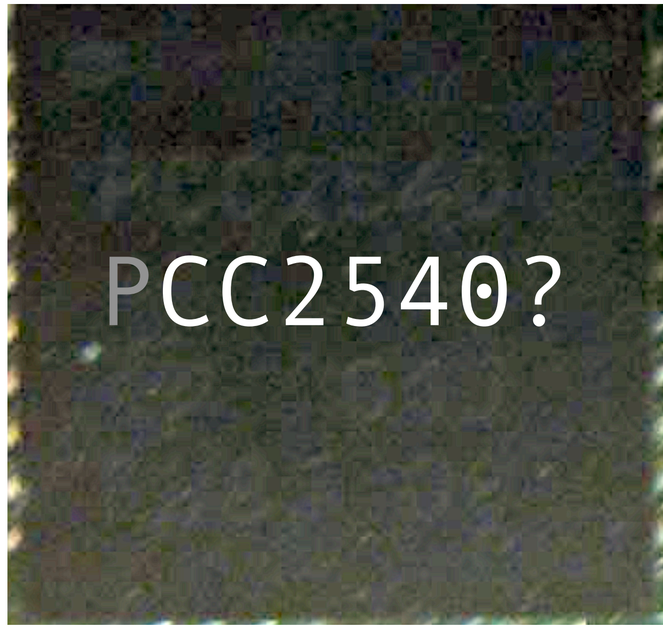
- Regex: ^tslim X2 ***[0-9]{3}$ e.g. "tslim X2 ***611"
  - Semantically: I'm *guessing* the ***[0-9]{3} is a masked form of the serial number, for people to more easily identify their device

https://fccid.io/CWO-TWM001/Internal-Photos/internal-photos-1721032

Medical 😬

Insulin Pump

- Regex: ^tslim X2 ***[0-9]{3}$ e.g. "tslim X2 ***611"
  - Semantically: I'm *guessing* the ***[0-9]{3} is a masked form of the serial number, for people to more easily identify their device



https://fccid.io/CWO-TWM001/Internal-Photos/internal-photos-1721032

Medical 😬

Insulin Pump

- Regex: ^tslim X2 ***[0-9]{3}$ e.g. "tslim X2 ***611"
  - Semantically: I'm *guessing* the ***[0-9]{3} is a masked form of the serial number, for people to more easily identify their device

```
For bdaddr = cd:a5:53:4d:49:5d:
        Company Name by IEEE OUI (cd:a5:53): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: tslim X2 ***611
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        UUID16s found:
                UUID16 0xfdfb (Company ID: Tandem Diabetes Care)
                        Found in BT LE data (LE_bdaddr_to_UUID16s)

        Transmit Power: 4dB
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
```

Medical 😬

Insulin Pump

- Regex: ^tslim X2 ***[0-9]{3}$ e.g. "tslim X2 ***611"
  - Semantically: I'm *guessing* the ***[0-9]{3} is a masked form of the serial number, for people to more easily identify their device

```
For bdaddr = cd:a5:53:4d:49:5d:
        Company Name by IEEE OUI (cd:a5:53): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: tslim X2 ***611
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        UUID16s found:
                UUID16 0xfdfb (Company ID: Tandem Diabetes Care)
                        Found in BT LE data (LE_bdaddr_to_UUID16s)

        Transmit Power: 4dB
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
```

Medical 😬

Insulin Pump

- Regex: ^tslim X2 ***[0-9]{3}$ e.g. "tslim X2 ***611"
  - Semantically: I'm *guessing* the ***[0-9]{3} is a masked form of the serial number, for people to more easily identify their device

```
For bdaddr = cd:a5:53:4d:49:5d:
        Company Name by IEEE OUI (cd:a5:53): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: tslim X2 ***611
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        UUID16s found:
                UUID16 0xfdfb (Company ID: Tandem Diabetes Care)
                        Found in BT LE data (LE_bdaddr_to_UUID16s)

        Transmit Power: 4dB
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
```

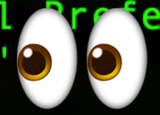
👀

```
For bdaddr = cd:a5:53:4d:49:5d:
        Company Name by IEEE OUI (cd:a5:53): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: tslim X2 ***611
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        UUID16s found:
                UUID16 0xfdfb (Company ID: Tandem Diabetes Care)
                        Found in BT LE data (LE_bdaddr_to_UUID16s)

        Transmit Power: 4dB
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        No Appearance data found.

        No Manufacturer-specific Data found.

        No Class of Device Data found.

        GATT Information:
                GATT Service: Begin Handle: 1   End Handle: 9           UUID128: 00001800-0000-1000-8000
                        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),
                                GATT Characteristic value read as b'tslim X2 ***611'
                        GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 4
```

```
For bdaddr = cd:a5:53:4d:49:5d:
        Company Name by IEEE OUI (cd:a5:53): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: tslim X2 ***611
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        UUID16s found:
                UUID16 0xfdfb (Company ID: Tandem Diabetes Care)
                        Found in BT LE data (LE_bdaddr_to_UUID16s)

        Transmit Power: 4dB
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        No Appearance data found.

        No Manufacturer-specific Data found.

        No Class of Device Data found.

        GATT Information:
                GATT Service: Begin Handle: 1   End Handle: 9           UUID128: 00001800-0000-1000-8000
                        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),
                                GATT Characteristic value read as b'tslim X2 ***611'
                        GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 4
```

```
ice Data found.

n:
rvice: Begin Handle: 1   End Handle: 9          UUID128: 00001800-0000-1000-8000-00805f9b34fb (Generic A
 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 ('Readab
        GATT Characteristic value read as b'tslim X2 ***611'
 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\x00'
                Appearance decodes as: Category (0): Unknown, Sub-Category (0): Generic
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 6
 GATT Descriptor: 00002a04-0000-1000-8000-00805f9b34fb, Descriptor Handle: 7
        GATT Characteristic: 00002a04-0000-1000-8000-00805f9b34fb (Peripheral Preferred Connection Param
        GATT Characteristic value read as b'\x0c\x00\x18\x00\x1d\x00\x0f\x01'
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 8
 GATT Descriptor: 00002aa6-0000-1000-8000-00805f9b34fb, Descriptor Handle: 9
        GATT Characteristic: 00002aa6-0000-1000-8000-00805f9b34fb (Central Address Resolution), Properti
        GATT Characteristic value read as b'\x01'
rvice: Begin Handle: 10  End Handle: 13         UUID128: 00001801-0000-1000-8000-00805f9b34fb (Generic A
 GATT Descriptor: 00002800-0000-1000-8000-00805f9b34fb, Descriptor Handle: 10
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 11
 GATT Descriptor: 00002a05-0000-1000-8000-00805f9b34fb, Descriptor Handle: 12
        GATT Characteristic: 00002a05-0000-1000-8000-00805f9b34fb (Service Changed), Properties: 32 ('In
 GATT Descriptor: 00002902-0000-1000-8000-00805f9b34fb, Descriptor Handle: 13
rvice: Begin Handle: 14  End Handle: 22         UUID128: 0000180a-0000-1000-8000-00805f9b34fb (Device In
 GATT Descriptor: 00002800-0000-1000-8000-00805f9b34fb, Descriptor Handle: 14
rvice: Begin Handle: 23  End Handle: 65535      UUID128: 0000fdfb-0000-1000-8000-00805f9b34fb (This is a
```

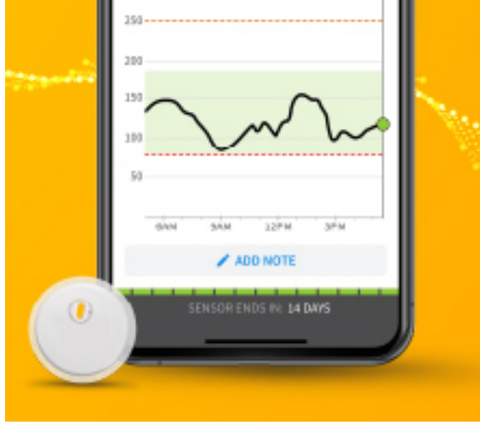
```
ice Data found.

n:
rvice: Begin Handle: 1   End Handle: 9          UUID128: 00001800-0000-1000-8000-00805f9b34fb (Generic A
 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 ('Readab
        GATT Characteristic value read as b'tslim X2 ***611'
 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\x00'
                Appearance decodes as: Category (0): Unknown, Sub-Category (0): Generic
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 6
 GATT Descriptor: 00002a04-0000-1000-8000-00805f9b34fb, Descriptor Handle: 7
        GATT Characteristic: 00002a04-0000-1000-8000-00805f9b34fb (Peripheral Preferred Connection Param
        GATT Characteristic value read as b'\x0c\x00\x18\x00\x1d\x00\x0f\x01'
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 8
 GATT Descriptor: 00002aa6-0000-1000-8000-00805f9b34fb, Descriptor Handle: 9
        GATT Characteristic: 00002aa6-0000-1000-8000-00805f9b34fb (Central Address Resolution), Properti
        GATT Characteristic value read as b'\x01'
rvice: Begin Handle: 10  End Handle: 13         UUID128: 00001801-0000-1000-8000-00805f9b34fb (Generic A
 GATT Descriptor: 00002800-0000-1000-8000-00805f9b34fb, Descriptor Handle: 10
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 11
 GATT Descriptor: 00002a05-0000-1000-8000-00805f9b34fb, Descriptor Handle: 12
        GATT Characteristic: 00002a05-0000-1000-8000-00805f9b34fb (Service Changed), Properties: 32 ('In
 GATT Descriptor: 00002902-0000-1000-8000-00805f9b34fb, Descriptor Handle: 13
rvice: Begin Handle: 14  End Handle: 22         UUID128: 0000180a-0000-1000-8000-00805f9b34fb (Device In
 GATT Descriptor: 00002800-0000-1000-8000-00805f9b34fb, Descriptor Handle: 14
rvice: Begin Handle: 23  End Handle: 65535      UUID128: 0000fdfb-0000-1000-8000-00805f9b34fb (This is a
```



```
ice Data found.

n:
rvice: Begin Handle: 1   End Handle: 9          UUID128: 00001800-0000-1000-8000-00805f9b34fb (Generic A
 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 ('Readab
         GATT Characteristic value read as b'tslim X2 ***611'
 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\x00'
                 Appearance decodes as: Category (0): Unknown, Sub-Category (0): Generic
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 6
 GATT Descriptor: 00002a04-0000-1000-8000-00805f9b34fb, Descriptor Handle: 7
         GATT Characteristic: 00002a04-0000-1000-8000-00805f9b34fb (Peripheral Preferred Connection Param
         GATT Characteristic value read as b'\x0c\x00\x18\x00\x1d\x00\x0f\x01'
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 8
 GATT Descriptor: 00002aa6-0000-1000-8000-00805f9b34fb, Descriptor Handle: 9
         GATT Characteristic: 00002aa6-0000-1000-8000-00805f9b34fb (Central Address Resolution), Properti
         GATT Characteristic value read as b'\x01'
rvice: Begin Handle: 10  End Handle: 13         UUID128: 00001801-0000-1000-8000-00805f9b34fb (Generic A
 GATT Descriptor: 00002800-0000-1000-8000-00805f9b34fb, Descriptor Handle: 10
 GATT Descriptor: 00002803-0000-1000-8000-00805f9b34fb, Descriptor Handle: 11
 GATT Descriptor: 00002a05-0000-1000-8000-00805f9b34fb, Descriptor Handle: 12
         GATT Characteristic: 00002a05-0000-1000-8000-00805f9b34fb (Service Changed), Properties: 32 ('In
 GATT Descriptor: 00002902-0000-1000-8000-00805f9b34fb, Descriptor Handle: 13
rvice: Begin Handle: 14  End Handle: 22         UUID128: 0000180a-0000-1000-8000-00805f9b34fb (Device In
 GATT Descriptor: 00002800-0000-1000-8000-00805f9b34fb, Descriptor Handle: 14
rvice: Begin Handle: 23  End Handle: 65535      UUID128: 0000fdfb-0000-1000-8000-00805f9b34fb (This is a
```

Medical 😬

Continuous Glucose Monitoring System



- Regex: ^ABBOTT3MH[A-Z0-9]{8}$ e.g. "ABBOTT3MH00N3A09D"

Sensor Pack
Used with the Sensor Applicator to prepare the Sensor for use.

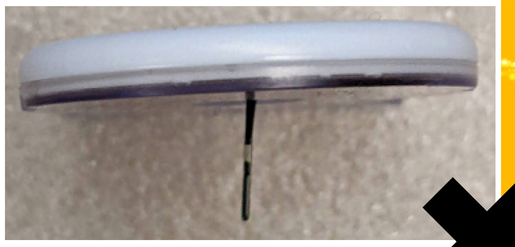
Sensor Applicator
Applies the Sensor to your body.

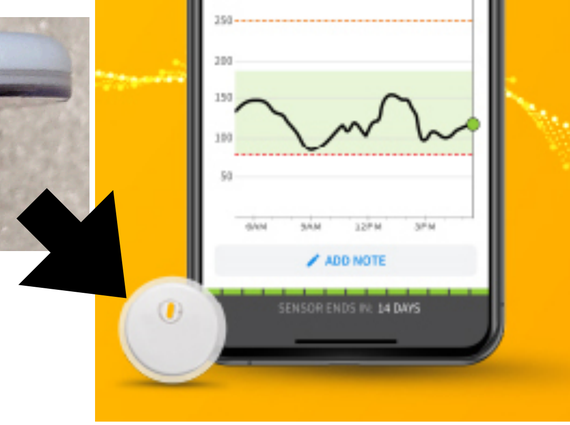
The Sensor measures and stores glucose readings when worn on your body. It initially comes in two parts: one part is in the Sensor Pack and the other part is in the Sensor Applicator. By following the instructions, you prepare and apply the Sensor on the back of your upper arm. The Sensor has a small, flexible tip that is inserted just under the skin. The Sensor can be worn for up to 14 days.

Sensor
Measures your glucose while on your body (only visible after applied).

https://www.binsons.com/uploads/userfiles/files/documents/products/Libre%202%20User%20Manual.pdf

https://fccid.io/QXS-LIB03S/External-Photos/External-Photos-5926517.pdf
https://fccid.io/QXS-LIB03S/Internal-Photos/Internal-Photos-5926526.pdf





Medical 😬

Continuous Glucose Monitoring System

- Regex: ^ABBOTT3MH[A-Z0-9]{8}$ e.g. "ABBOTT3MH00N3A09D"

Sensor Pack
Used with the Sensor Applicator to prepare the Sensor for use.

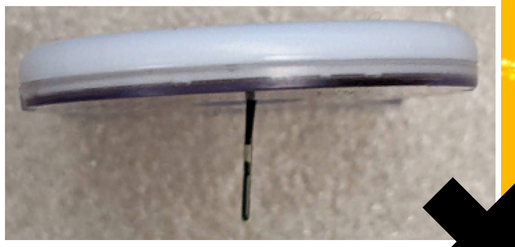
Sensor Applicator
Applies the Sensor to your body.

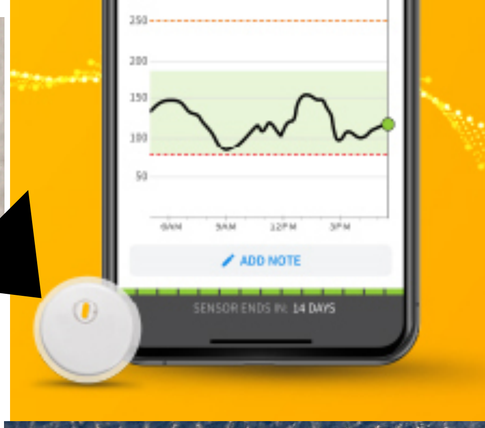
The Sensor measures and stores glucose readings when worn on your body. It initially comes in two parts: one part is in the Sensor Pack and the other part is in the Sensor Applicator. By following the instructions, you prepare and apply the Sensor on the back of your upper arm. The Sensor has a small, flexible tip that is inserted just under the skin. The Sensor can be worn for up to 14 days.

Sensor
Measures your glucose while on your body (only visible after applied).

https://www.binsons.com/uploads/userfiles/files/documents/products/Libre%202%20User%20Manual.pdf

https://fccid.io/QXS-LIB03S/External-Photos/External-Photos-5926517.pdf
https://fccid.io/QXS-LIB03S/Internal-Photos/Internal-Photos-5926526.pdf





Medical 😬

Continuous Glucose Monitoring System

- Regex: ^ABBOTT3MH[A-Z0-9]{8}$ e.g. "ABBOTT3MH00N3A09D"

Sensor Pack
Used with the Sensor Applicator to prepare the Sensor for use.

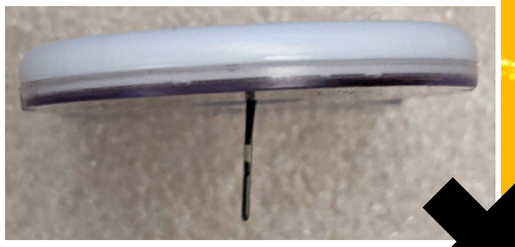
Sensor Appli
Applies the Se

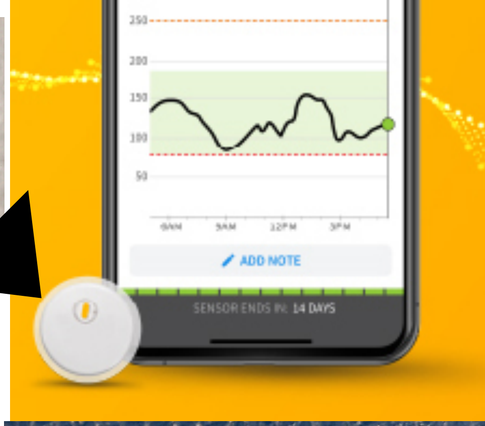
The Sensor measures and stores glucose readings when worn on your body. It initially comes in two parts: one part is in the Sensor Pack and the other part is in the Sensor Applicator. By following the instructions, you prepare and apply the Sensor on the back of your upper arm. The Sensor has a small, flexible tip that is inserted just under the skin. The Sensor can be worn for up to 14 days.

Sensor
Measures your glucose while on your body (only visible after applied).

https://www.binsons.com/uploads/userfiles/files/documents/products/Libre%202%20User%20Manual.pdf

https://fccid.io/QXS-LIB03S/External-Photos/External-Photos-5926517.pdf
https://fccid.io/QXS-LIB03S/Internal-Photos/Internal-Photos-5926526.pdf





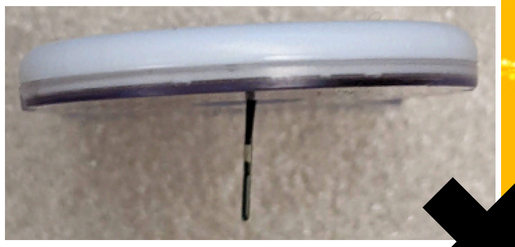
Medical 😬

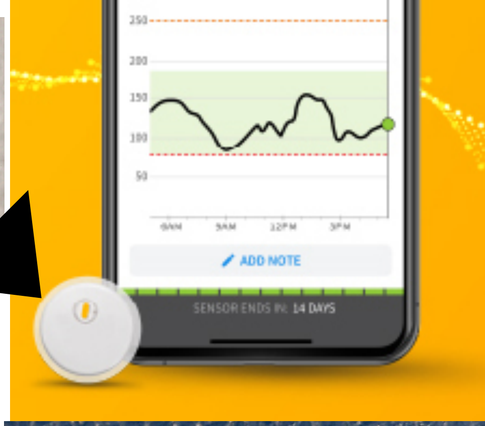
Continuous Glucose Monitoring System

- Regex: ^ABBOTT3MH[A-Z0-9]{8}$ e.g. "ABBOTT3MH00N3A09D"

```
For bdaddr = 34:5b:98:fc:7a:5d:
        Company Name by IEEE OUI (34:5b:98): EM Microelectronic

        No BTC Extended Inquiry Result Device info.

        DeviceName: ABBOTT3MH00HW4V04
                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)

        UUID16s found:
                UUID16 0xfde3 (Company ID: Abbott Diabetes Care)
                        Found in BT LE data (LE_bdaddr_to_UUID16s)

        Transmit Power: 0dB
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x03bb (Abbott) - 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): 0xbb03 (No Mat
                Raw Data: 5d7afc985b34
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
```

https://fccid.io/QXS-LIB03S/External-Photos/External-Photos-5926517.pdf
https://fccid.io/QXS-LIB03S/Internal-Photos/Internal-Photos-5926526.pdf





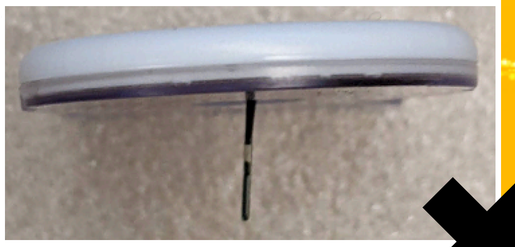
Medical 😬

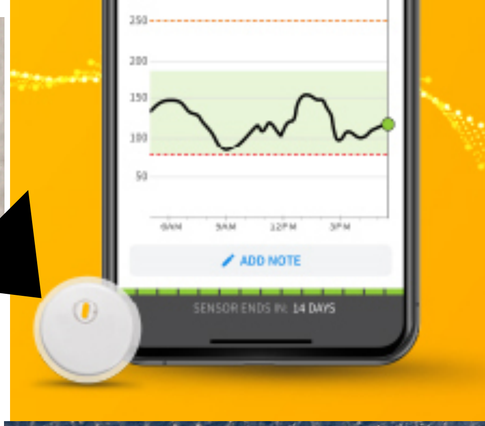
Continuous Glucose Monitoring System

- Regex: ^ABBOTT3MH[A-Z0-9]{8}$ e.g. "ABBOTT3MH00N3A09D"

```
For bdaddr = 34:5b:98:fc:7a:5d:
        Company Name by IEEE OUI (34:5b:98): EM Microelectronic

        No BTC Extended Inquiry Result Device info.

        DeviceName: ABBOTT3MH00HW4V04
                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)

        UUID16s found:
                UUID16 0xfde3 (Company ID: Abbott Diabetes Care)
                        Found in BT LE data (LE_bdaddr_to_UUID16s)

        Transmit Power: 0dB
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x03bb (Abbott) - 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): 0xbb03 (No Mat
                Raw Data: 5d7afc985b34
```

https://fccid.io/QXS-LIB03S/External-Photos/External-Photos-5926517.pdf
https://fccid.io/QXS-LIB03S/Internal-Photos/Internal-Photos-5926526.pdf





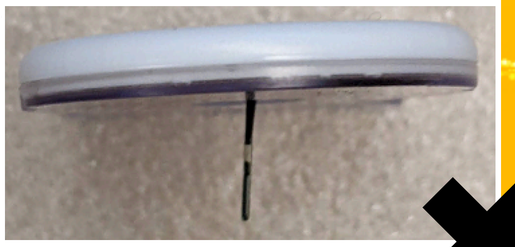
Medical 😬

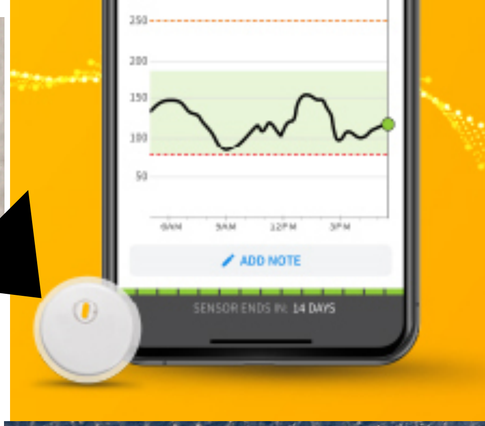
Continuous Glucose Monitoring System

- Regex: ^ABBOTT3MH[A-Z0-9]{8}$ e.g. "ABBOTT3MH00N3A09D"

```
For bdaddr = 34:5b:98:fc:7a:5d:
        Company Name by IEEE OUI (34:5b:98): EM Microelectronic 👀

        No BTC Extended Inquiry Result Device info.

        DeviceName: ABBOTT3MH00HW4V04
                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)

        UUID16s found:
                UUID16 0xfde3 (Company ID: Abbott Diabetes Care)
                        Found in BT LE data (LE_bdaddr_to_UUID16s)

        Transmit Power: 0dB
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x03bb (Abbott) - 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): 0xbb03 (No Mat
                Raw Data: 5d7afc985b34
```

https://fccid.io/QXS-LIB03S/External-Photos/External-Photos-5926517.pdf
https://fccid.io/QXS-LIB03S/Internal-Photos/Internal-Photos-5926526.pdf





Medical 😬

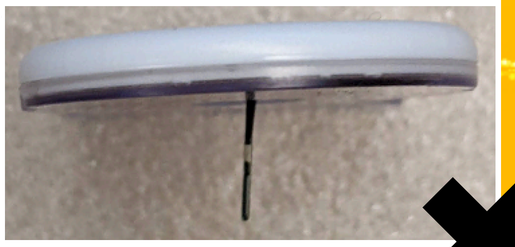
Continuous Glucose Monitoring System

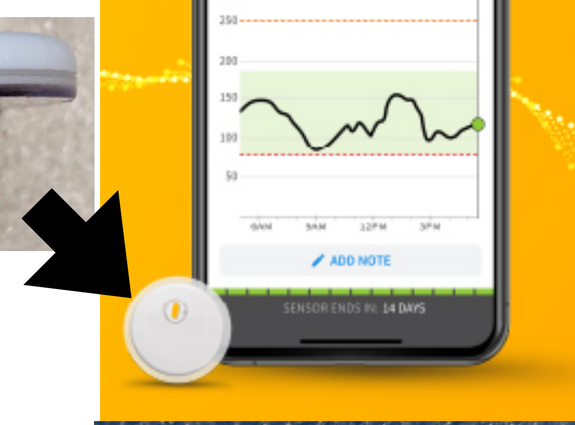
- Regex: ^ABBOTT3MH[A-Z0-9]{8}$ e.g. "ABBOTT3MH00N3A09D"

```
For bdaddr = 34:5b:98:fc:7a:5d:
        Company Name by IEEE OUI (34:5b:98): EM Microelectronic

        No BTC Extended Inquiry Result Device info.

        DeviceName: ABBOTT3MH00HW4V04
                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)

        UUID16s found:
                UUID16 0xfde3 (Company ID: Abbott Diabetes Care)
                        Found in BT LE data (LE_bdaddr_to_UUID16)

        Transmit Power: 0dB
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x03bb (Abbott) - 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): 0xbb03 (No Mat
                Raw Data: 5d7afc985b34
```

👀

https://fccid.io/QXS-LIB03S/External-Photos/External-Photos-5926517.pdf
https://fccid.io/QXS-LIB03S/Internal-Photos/Internal-Photos-5926526.pdf





Medical 😬

Continuous Glucose Monitoring System

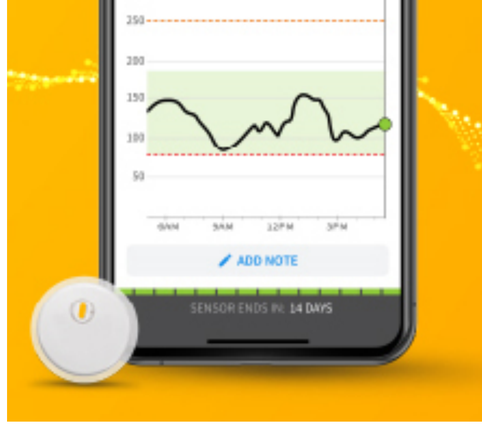
- Regex: ^ABBOTT3MH[A-Z0-9]{8}$ e.g. "ABBOTT3MH00N3A09D"

```
For bdaddr = 34:5b:98:fc:7a:5d:
        Company Name by IEEE OUI (34:5b:98): EM Microelectronic

        No BTC Extended Inquiry Result Device info.

        DeviceName: ABBOTT3MH00HW4V04
                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)

        UUID16s found:
                UUID16 0xfde3 (Company ID: Abbott Diabetes Care)
                        Found in BT LE data (LE_bdaddr_to_UUID16s)

        Transmit Power: 0dB
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

        No Appearance data found.

        Manufacturer-specific Data:
                Device Company ID: 0x03bb (Abbott)  e with a grain of salt, not all companies populate this accurately!
                        Endianness-flipped device  ompany ID (in case the vendor used the wrong endianness): 0xbb03 (No Mat
                Raw Data: 5d7afc985b34
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
```

👀

Medical 😬

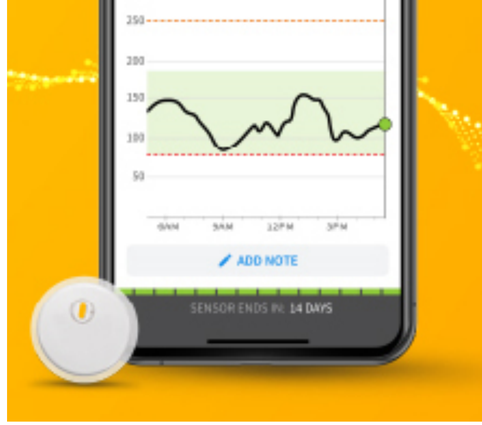
Continuous Glucose Monitoring System



- Regex: ^ABBOTT3MH[A-Z0-9]{8}$ e.g. "ABBOTT3MH00N3A09D"

Medical 😬

Continuous Glucose Monitoring System



- Regex: ^ABBOTT3MH[A-Z0-9]{8}$ e.g. "ABBOTT3MH00N3A09D"

MikeMM

on 02/20/2020 21:28:47 | IP (hash): 1428929226

to create an answer | Quote

Rank: Beginner

points: 0

Posts: 2

Member since: 02/20/2020

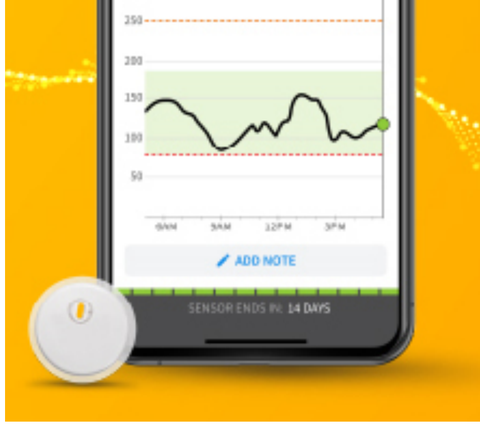
Hello everyone,

today my work colleagues asked me if I was diabetic, I asked how did you get on the train?
You said, whenever I'm around, an ABBOTT....serial number appears in your Bluetooth scanner,

well, thank you ABBOTT for this outing, many colleagues and employers still associate this disease with a lot of negative things, often sick, not resilient, an accident can happen at any time.....

Medical 😬

Continuous Glucose Monitoring System



- Regex: ^ABBOTT3MH[A-Z0-9]{8}$ e.g. "ABBOTT3MH00N3A09D"

MikeMM

on 02/20/2020 21:28:47 | IP (hash): 1428929226

to create an answer | Quote

Rank: Beginner

points: 0

Posts: 2

Member since: 02/20/2020

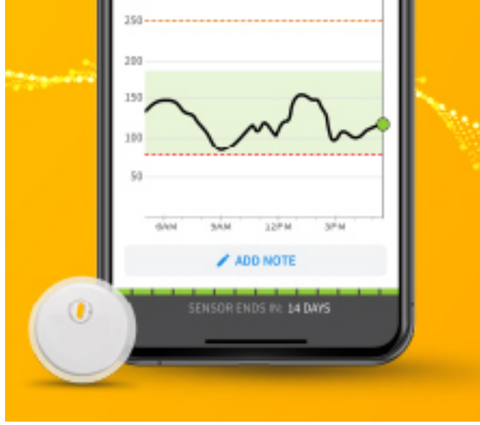
Hello everyone,

today my work colleagues asked me if I was diabetic, I asked how did you get on the train?
You said, whenever I'm around, an ABBOTT....serial number appears in your Bluetooth scanner,

well, thank you ABBOTT for this outing, many colleagues and employers still associate this disease with a lot of negative things, often sick, not resilient, an accident can happen at any time.....

Medical 😬

Continuous Glucose Monitoring System



- Regex: ^ABBOTT3MH[A-Z0-9]{8}$ e.g. "ABBOTT3MH00N3A09D"

MikeMM

on 02/20/2020 21:28:47 | IP (hash): 1428929226

to create an answer | Quote

Rank: Beginner
points: 0
Posts: 2
Member since: 02/20/2020

Hello everyone,

today my work colleagues asked me if I was diabetic, I asked how did you get on the train?
You said, whenever I'm around, an ABBOTT....serial number appears in your Bluetooth scanner,

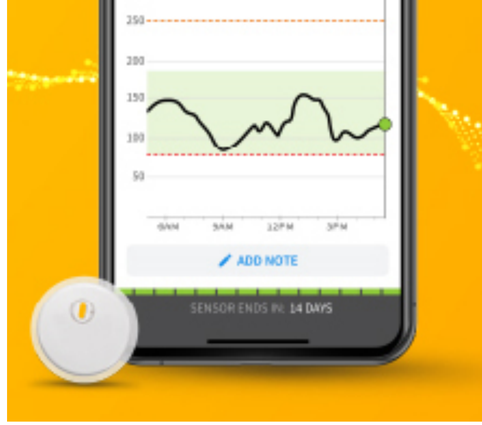
well, thank you ABBOTT for this outing, many colleagues and employers still associate this disease with a lot of negative things, often sick, not resilient, an accident can happen at any time.....

Rank: Beginner
points: 0
Posts: 2
Member since: 02/20/2020

nowadays everyone has Bluetooth active on their smartphones and notebooks. I heard that Bluetooth cannot be deactivated on the new Apple devices. That means the smartphone and notebook scans its surroundings at certain intervals and notifies you of what is nearby, or someone is actively looking for HIS new device (headphones, smart TV, notebook, speakers, ceiling light, smart home devices, car radio, etc. and with this search all participants in the area are displayed) I'm sitting at the PC and the Bletooth scanner reports ABBOTT3MH every 30 seconds.....

Medical 😬

Continuous Glucose Monitoring System



- Regex: ^ABBOTT3MH[A-Z0-9]{8}$ e.g. "ABBOTT3MH00N3A09D"

MikeMM

on 02/20/2020 21:28:47 | IP (hash): 1428929226

to create an answer | Quote

Rank: Beginner
points: 0
Posts: 2
Member since: 02/20/2020

Hello everyone,

today my work colleagues asked me if I was diabetic, I asked how did you get on the train?
You said, whenever I'm around, an ABBOTT....serial number appears in your Bluetooth scanner,

well, thank you ABBOTT for this outing, many colleagues and employers still associate this disease with a lot of negative things, often sick, not resilient, an accident can happen at any time.....

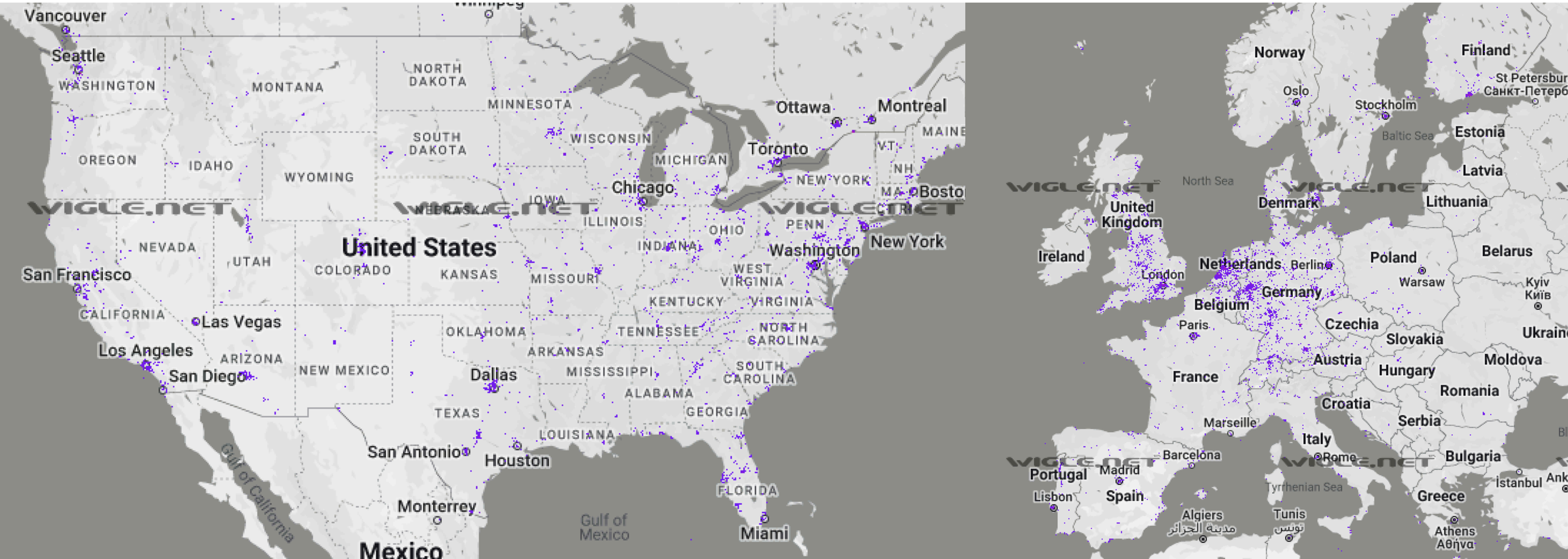
Rank: Beginner
points: 0
Posts: 2
Member since: 02/20/2020

nowadays everyone has Bluetooth active on their smartphones and notebooks. I heard that Bluetooth cannot be deactivated on the new Apple devices. That means the smartphone and notebook scans its surroundings at certain intervals and notifies you of what is nearby, or someone is actively looking for HIS new device (headphones, smart TV, notebook, speakers, ceiling light, smart home devices, car radio, etc. and with this search all participants in the area are displayed) I'm sitting at the PC and the Bletooth scanner reports ABBOTT3MH every 30 seconds.....

Medical 😬

Continuous Glucose Monitoring System

- "Where my diabetics at?!"



Aside: "insertable cardiac monitor (ICM)"

(Haven't seen one of these yet (AFAIK)...but...)

An insertable cardiac monitor (ICM), which is placed just under the skin during a minimally invasive procedure to continuously monitor your heart's rhythm for signs of atrial fibrillation.

https://www.abbott.com/corpnewsroom/products-and-innovation/heart-monitoring-everywhere-you-go.html

Aside: "insertable cardiac monitor (ICM)"

(Haven't seen one of these yet (AFAIK)...but...)

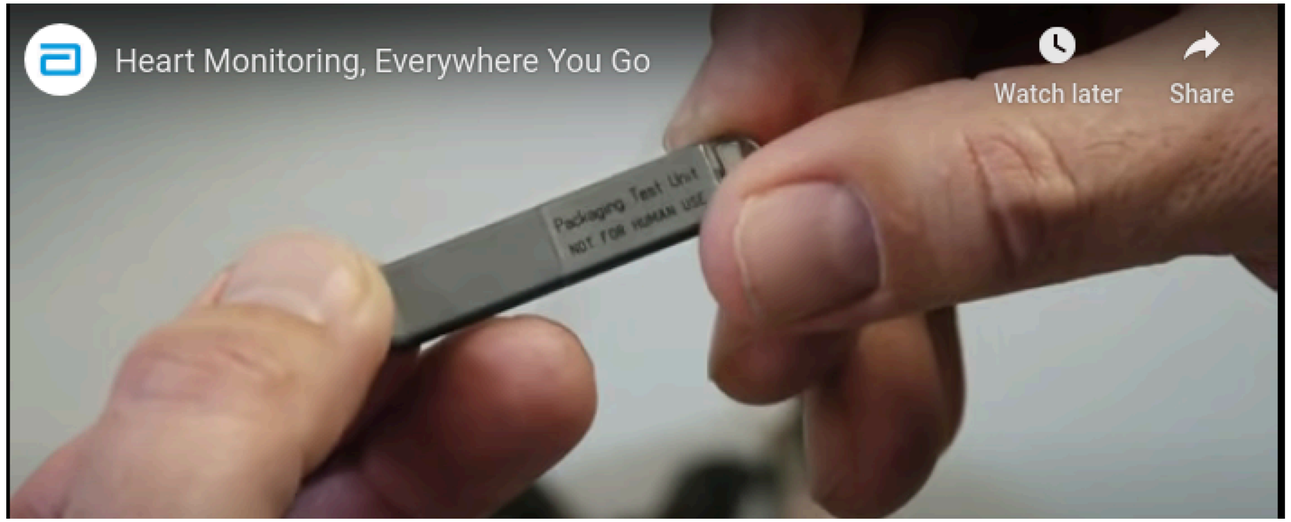
An insertable cardiac monitor (ICM), which is placed just under the skin during a minimally invasive procedure to continuously monitor your heart's rhythm for signs of atrial fibrillation.

https://www.abbott.com/corpnewsroom/products-and-innovation/heart-monitoring-everywhere-you-go.html

Aside: "insertable cardiac monitor (ICM)"

(Haven't seen one of these yet (AFAIK)...but...)

An insertable cardiac monitor (ICM), which is placed just under the skin during a minimally invasive procedure to continuously monitor your heart's rhythm for signs of atrial fibrillation.



https://www.abbott.com/corpnewsroom/products-and-innovation/heart-monitoring-everywhere-you-go.html

Aside: "insertable cardiac monitor (ICM)"

(Haven't seen one of these yet (AFAIK)...but...)

An insertable cardiac monitor (ICM), which is placed just under the skin during a minimally invasive procedure to continuously monitor your heart's rhythm for signs of atrial fibrillation.

Even better: Abbotts Confirm RxTM ICM, which is designed not only to detect arrhythmias but also to wirelessly transmit data via Bluetooth to your smart phone for data transmission to the Merlin.netTM Patient Care Network so your doctor has real-time access anywhere in the world to how your heart is performing.

https://www.abbott.com/corpnewsroom/products-and-innovation/heart-monitoring-everywhere-you-go.html

Aside: "insertable cardiac monitor (ICM)"

(Haven't seen one of these yet (AFAIK)...but...)

An insertable cardiac monitor (ICM), which is placed just under the skin during a minimally invasive procedure to continuously monitor your heart's rhythm for signs of atrial fibrillation.

Even better: Abbotts Confirm RxTM ICM, which is designed not only to detect arrhythmias but also to wirelessly transmit data via Bluetooth to your smart phone for data transmission to the Merlin.netTM Patient Care Network so your doctor has real-time access anywhere in the world to how your heart is performing.

https://www.abbott.com/corpnewsroom/products-and-innovation/heart-monitoring-everywhere-you-go.html

Aside: "insertable cardiac monitor (ICM)"

(Haven't seen one of these yet (AFAIK)...but...)

An insertable cardiac monitor (ICM), which is placed just under the skin during a minimally invasive procedure to continuously monitor your heart's rhythm for signs of atrial fibrillation.

Even better: Abbotts Confirm RxTM ICM, which is designed not only to detect arrhythmias but also to wirelessly transmit data via Bluetooth to your smart phone for data transmission to the Merlin.netTM Patient Care Network so your doctor has real-time access anywhere in the world to how your heart is performing.

https://www.abbott.com/corpnewsroom/products-and-innovation/heart-monitoring-everywhere-you-go.html

Aside: "insertable cardiac monitor (ICM)"

(Haven't seen one of these yet (AFAIK)...but...)

An insertable cardiac monitor (ICM), which is placed just under the skin during a minimally invasive procedure to continuously monitor your heart's rhythm for signs of atrial fibrillation.

Even better: Abbotts Confirm RxTM ICM, which is designe
arrhythmias but also to wirelessly transmit data via Bluetoot
data transmission to the Merlin.netTM Patient Care Network
time access anywhere in the world to how your heart is perfo

https://www.abbott.com/corpnewsroom/products-and-innovation/heart-monitoring-everywhere-you-go.html

Medical 😬

CGM + Insulin Pump (or its helper display?)

- Regex: ^AP [A-F0-9]{8} [A-F0-9]{16}$$ e.g. "AP 000722ED 0E96AAC1000E09F2"
- "Omnipod" by Insulet Corporation

```
For bdaddr = 50:c1:f0:e9:5e:cc:
        Company Name by IEEE OUI (50:c1:f0): NXP Semiconductor (Tianjin) LTD.

        No BTC Extended Inquiry Result Device info.

        DeviceName: AP 000722ED 0E96AAC1000E09F2
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                        NamePrint: match found for ^AP [A-F0-9]{8} [A-F0-9]{16}$: Insulet Corporation unknown model of device (possibly
ay (Personal Diabetes Manager))
                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: 0x0360 (Insulet Corporation) - 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): 0x6003 (No Match)
                Raw Data: 0002100000
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
```

Medical 😬

CGM + Insulin Pump (or its helper display?)

- Regex: ^AP [A-F0-9]{8} [A-F0-9]{16}$$ e.g. "AP 000722ED 0E96AAC1000E09F2"
- "Omnipod" by Insulet Corporation

```
For bdaddr = 50:c1:f0:e9:5e:cc:
        Company Name by IEEE OUI (50:c1:f0): NXP Semiconductor (Tianjin) LTD.

        No BTC Extended Inquiry Result Device info.

        DeviceName: AP 000722ED 0E96AAC1000E09F2
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                        NamePrint: match found for ^AP [A-F0-9]{8} [A-F0-9]{16}$: Insulet Corporation unknown model of device (possibly
ay (Personal Diabetes Manager))
                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: 0x0360 (Insulet Corporation) - 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): 0x6003 (No Match)
                Raw Data: 0002100000
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
```

Medical 😬

CGM + Insulin Pump (or its helper display?)

- Regex: ^AP [A-F0-9]{8} [A-F0-9]{16}$$ e.g. "AP 000722ED 0E96AAC1000E09F2"
- "Omnipod" by Insulet Corporation

```
For bdaddr = 50:c1:f0:e9:5e:cc:
        Company Name by IEEE OUI (50:c1:f0): NXP Semiconductor (Tianjin) LTD.

        No BTC Extended Inquiry Result Device info.

        DeviceName: AP 000722ED 0E96AAC1000E09F2
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                        NamePrint: match found for ^AP [A-F0-9]{8} [A-F0-9]{16}$: Insulet Corporation unknown model of device (possibly
ay (Personal Diabetes Manager))
                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: 0x0360 (Insulet Corporation) - 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): 0x6003 (No Match)
                Raw Data: 0002100000
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
```

Medical 😬

CGM + Insulin Pump (or its helper display?)

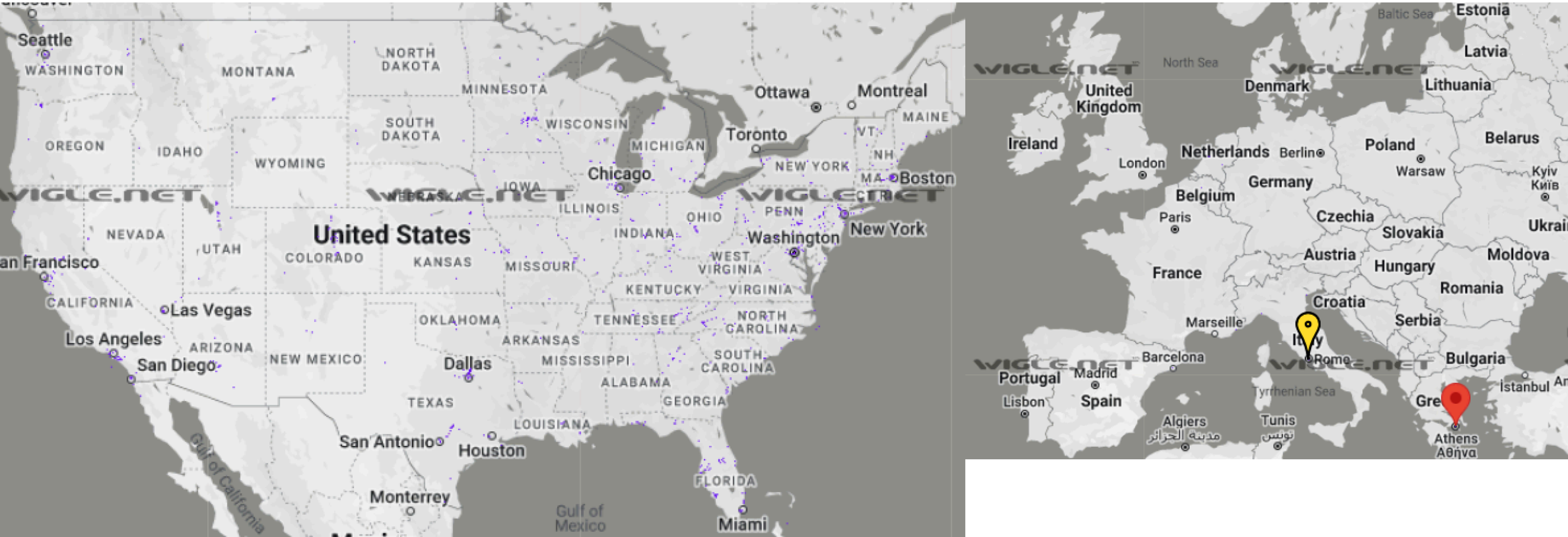
- Regex: ^AP [A-F0-9]{8} [A-F0-9]{16}$$ e.g. "AP 000722ED 0E96AAC1000E09F2"
- "Omnipod" by Insulet Corporation

```
For bdaddr = 50:c1:f0:e9:5e:cc:
        Company Name by IEEE OUI (50:c1:f0): NXP Semiconductor (Tianjin) LTD.

        No BTC Extended Inquiry Result Device info.

        DeviceName: AP 000722ED 0E96AAC1000E09F2
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                        NamePrint: match found for ^AP [A-F0-9]{8} [A-F0-9]{16}$: Insulet Corporation unknown model of device (possibly
ay (Personal Diabetes Manager))
                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: 0x0360 (Insulet Corporation) 👀 with a grain of salt, not all companies populate this accurately!
                        Endianness-flipped device company ID (i  ca  the vendor used the wrong endianness): 0x6003 (No Match)
                Raw Data: 0002100000
                        In BT LE Data (LE_bdaddr_to_mf_specific), bdaddr_random = 0 (Public)
```

Medical 😬

Continuous Glucose Monitoring System

- "Where my diabetics at?!" (My theory for Europe? Americans on vacation)



Medical 😬

Blood Glucose Meter

- Regex: ^OneTouch [A-Z0-9]{4}$ e.g. "OneTouch C8SW"

https://www.onetouch.com/products/glucose-meters/onetouch-verio-sync

Medical 😬

Blood Glucose Meter

- Regex: ^OneTouch [A-Z0-9]{4}$ e.g. "OneTouch C8SW"

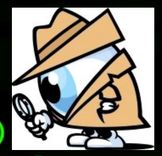
```
For bdaddr = d8:eb:92:07:c8:c8:
        Company Name by IEEE OUI (d8:eb:92): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: OneTouch G6MX
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^OneTouch [A-Z0-9]{4}$: OneTouch glucose test meter (https://www.onetouch.com/p
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

        UUID16s found:
                UUID16 0x180a (GATT Service ID: Device Information)
                         Found in BT LE data (LE_bdaddr_to_UUID16s)

        Transmit Power: -4dB
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        Appearance: Category (32): Window Covering, Sub-Category (0): Generic
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

        Manufacturer-specific Data:
                Device Company ID: 0x016d (LifeScan Inc) - take with a grain of salt, not all companies populate this accurately!
```

Medical 😬

Blood Glucose Meter

- Regex: ^OneTouch [A-Z0-9]{4}$ e.g. "OneTouch C8SW"

```
For bdaddr = d8:eb:92:07:c8:c8:
        Company Name by IEEE OUI (d8:eb:92): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: OneTouch G6MX
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^OneTouch [A-Z0-9]{4}$: OneTouch glucose test meter (https://www.onetouch.com/p
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

        UUID16s found:
                UUID16 0x180a (GATT Service ID: Device Information)
                         Found in BT LE data (LE_bdaddr_to_UUID16s)

        Transmit Power: -4dB
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        Appearance: Category (32): Window Covering, Sub-Category (0): Generic
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

        Manufacturer-specific Data:
                Device Company ID: 0x016d (LifeScan Inc) - take with a grain of salt, not all companies populate this accurately!
```

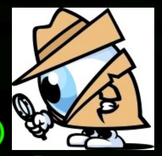


Medical 😬

Blood Glucose Meter

- Regex: ^OneTouch [A-Z0-9]{4}$ e.g. "OneTouch C8SW"

```
For bdaddr = d8:eb:92:07:c8:c8:
        Company Name by IEEE OUI (d8:eb:92): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: OneTouch G6MX
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^OneTouch [A-Z0-9]{4}$: OneTouch glucose test meter (https://www.onetouch.com/p
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

        UUID16s found:
                UUID16 0x180a (GATT Service ID: Device Information)
                        Found in BT LE data (LE_bdaddr_to_UUID16s)

        Transmit Power: -4dB
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        Appearance: Category (32): Window Covering, Sub-Category (0): Generic
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

        Manufacturer-specific Data:
                Device Company ID: 0x016d (LifeScan Inc) - take with a grain of salt, not all companies populate this accurately!
```



👀

Medical 😬

Blood Glucose Meter

- Regex: ^OneTouch [A-Z0-9]{4}$ e.g. "OneTouch C8SW"

```
For bdaddr = d8:eb:92:07:c8:c8:
        Company Name by IEEE OUI (d8:eb:92): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: OneTouch G6MX
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^OneTouch [A-Z0-9]{4}$: OneTouch glucose test meter (https://www.onetouch.com/p
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

        UUID16s found:
                UUID16 0x180a (GATT Service ID: Device Information)
                         Found in BT LE data (LE_bdaddr_to_UUID16s)

        Transmit Power: -4dB
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        Appearance: Category (32): Window Covering, b  tegory (0): Generic
                In BT LE Data (LE_bdaddr_to_name), b    _random = 1 (Random Static)
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

        Manufacturer-specific Data:
                Device Company ID: 0x016d (LifeScan Inc) - take with a grain of salt, not all companies populate this accurately!
```

👀

Medical 😬

Blood Glucose Meter

- Regex: ^OneTouch [A-Z0-9]{4}$ e.g. "OneTouch C8SW"

```
For bdaddr = d8:eb:92:07:c8:c8:
        Company Name by IEEE OUI (d8:eb:92): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: OneTouch G6MX
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^OneTouch [A-Z0-9]{4}$: OneTouch glucose test meter (https://www.onetouch.com/p
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

        UUID16s found:
                UUID16 0x180a (GATT Service ID: Device Information)
                         Found in BT LE data (LE_bdaddr_to_UUID16s)

        Transmit Power: -4dB
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        Appearance: Category (32): Window Covering, b      tegory (0): Generic
                In BT LE Data (LE_bdaddr_to_name), b      _random = 1 (Random Static)
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

        Manufacturer-specific Data:
                Device Company ID: 0x016d (LifeScan Inc) - take with a grain of salt, not all companies populate this accurately!
```

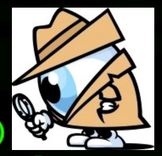
👀 ???

Medical 😬

Blood Glucose Meter

- Regex: ^OneTouch [A-Z0-9]{4}$ e.g. "OneTouch C8SW"

```
For bdaddr = d8:eb:92:07:c8:c8:
        Company Name by IEEE OUI (d8:eb:92): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: OneTouch G6MX
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                        NamePrint: match found for ^OneTouch [A-Z0-9]{4}$: OneTouch glucose test meter (https://www.onetouch.com/p
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

        UUID16s found:
                UUID16 0x180a (GATT Service ID: Device Information)
                        Found in BT LE data (LE_bdaddr_to_UUID16s)

        Transmit Power: -4dB
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        Appearance: Category (32): Window Covering, Sub-Category (0): Generic
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

        Manufacturer-specific Data:
                Device Company ID: 0x016d (LifeScan Inc)  with a grain of salt, not all companies populate this accurately!
```



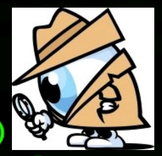
???

Medical 😬

Blood Glucose Meter

- Regex: ^OneTouch [A-Z0-9]{4}$ e.g. "OneTouch C8SW"

```
For bdaddr = d8:eb:92:07:c8:c8:
        Company Name by IEEE OUI (d8:eb:92): No Match

        No BTC Extended Inquiry Result Device info.

        DeviceName: OneTouch G6MX
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
```



```
ch glucose test meter (https://www.onetouch.com/p
able Undirected Advertising (ADV_IND)
```

February 15, 2012

Insulet Announces Global Agreement With LifeScan, Inc to Integrate Their OneTouch Blood Glucose Monitoring Technologies Into the OmniPod(R) Insulin Pump

https://investors.insulet.com/news/news-details/2012/Insulet-Announces-Global-Agreement-With-LifeScan-Inc-to-Integrate-Their-OneTouch-Blood-Glucose-Monitoring-Technologies-Into-the-OmniPodR-Insulin-Pump/default.aspx

```
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

        Appearance: Category (32): Window Covering, Sub-Category (0): Generic
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 1 (Random Static)
                This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

        Manufacturer-specific Data:
                Device Company ID: 0x016d (LifeScan Inc)
```

???

```
with a grain of salt, not all companies populate this accurately!
```

Medical 😬

- Regex: ^PR BT [A-F0-9]{4}$ e.g. "PR BT BE14"
- Phillips Respironics System One CPAP
  - CPAP = "continuous positive airway pressure"
  - Treats *sleep apnea*

Medical 😬

- Regex: ^PR BT [A-F0-9]{4}$ e.g. "PR BT BE14"
- Phillips Respironics System One CPAP
  - CPAP = "continuous positive airway pressure"
  - Treats *sleep apnea*

```
For bdaddr = 00:1f:ff:5f:0d:5a:
        Company Name by IEEE OUI (00:1f:ff): Respironics, Inc.

        No BTC Extended Inquiry Result Device info.

        DeviceName: PR BT 5C0A
                In BT Classic Data (EIR_bdaddr_to_name)
                        NamePrint: match found for ^PR BT [A-F0-9]{4}$: Philli
        DeviceName: PR BT 5C0A
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                        NamePrint: match found for ^PR BT [A-F0-9]{4}$: Philli
                This was found in an event of type 0 which corresponds to Conn

        UUID16s found:
                UUID16 0x1101 (Service ID: SerialPort)
                        Found in BT Classic data (EIR_bdaddr_to_UUID16s)
```

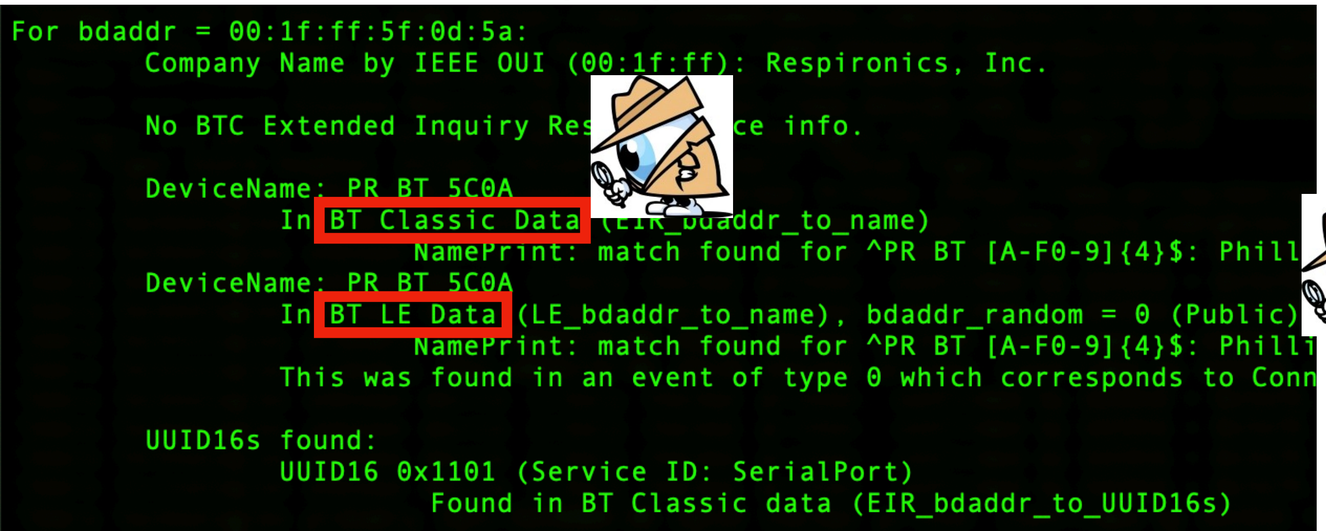
Medical 😬

- Regex: ^PR BT [A-F0-9]{4}$ e.g. "PR BT BE14"
- Phillips Respironics System One CPAP
  - CPAP = "continuous positive airway pressure"
  - Treats *sleep apnea*

```
For bdaddr = 00:1f:ff:5f:0d:5a:
        Company Name by IEEE OUI (00:1f:ff): Respironics, Inc.

        No BTC Extended Inquiry Result Device info.

        DeviceName: PR BT 5C0A
                In BT Classic Data (EIR_bdaddr_to_name)
                        NamePrint: match found for ^PR BT [A-F0-9]{4}$: Philli
        DeviceName: PR BT 5C0A
                In BT LE Data (LE_bdaddr_to_name), bdaddr_random = 0 (Public)
                        NamePrint: match found for ^PR BT [A-F0-9]{4}$: Philli
                This was found in an event of type 0 which corresponds to Conn

        UUID16s found:
                UUID16 0x1101 (Service ID: SerialPort)
                        Found in BT Classic data (EIR_bdaddr_to_UUID16s)
```

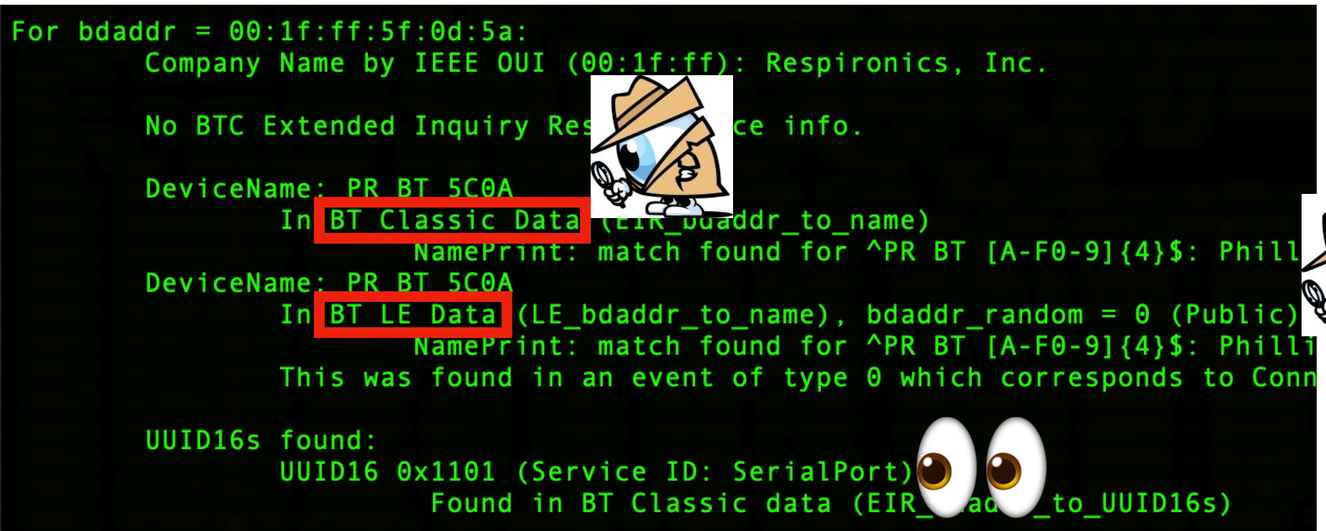
Medical 😬

- Regex: ^PR BT [A-F0-9]{4}$ e.g. "PR BT BE14"
- Phillips Respironics System One CPAP
  - CPAP = "continuous positive airway pressure"
  - Treats *sleep apnea*



Medical 😬

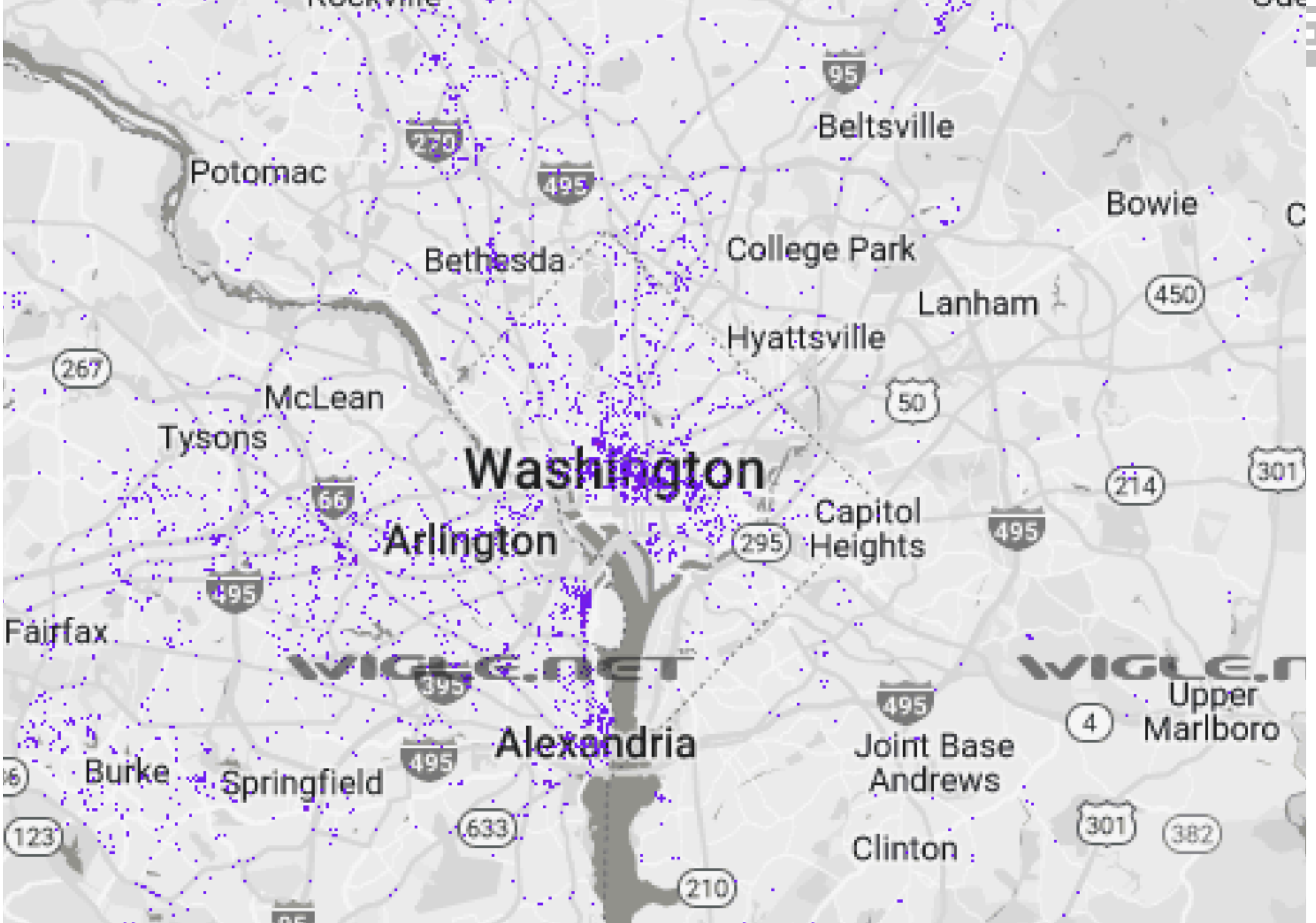
- Regex: ^PR BT [A-F0-9]{4}$ e.g. "PR BT BE14"
- Phillips Respironics System One CPAP
  - CPAP = "continuous positive airway pressure"
  - Treats *sleep apnea*

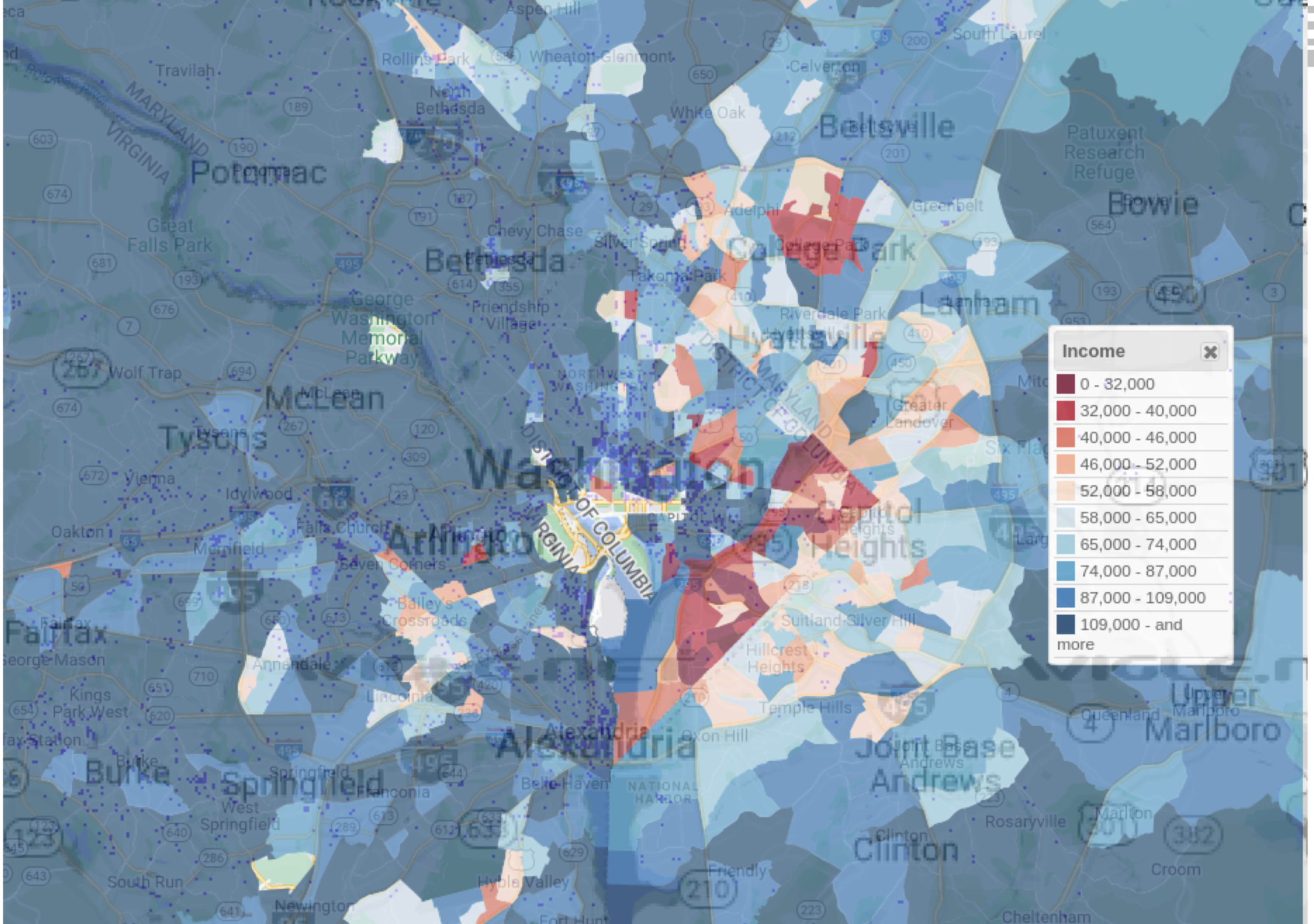


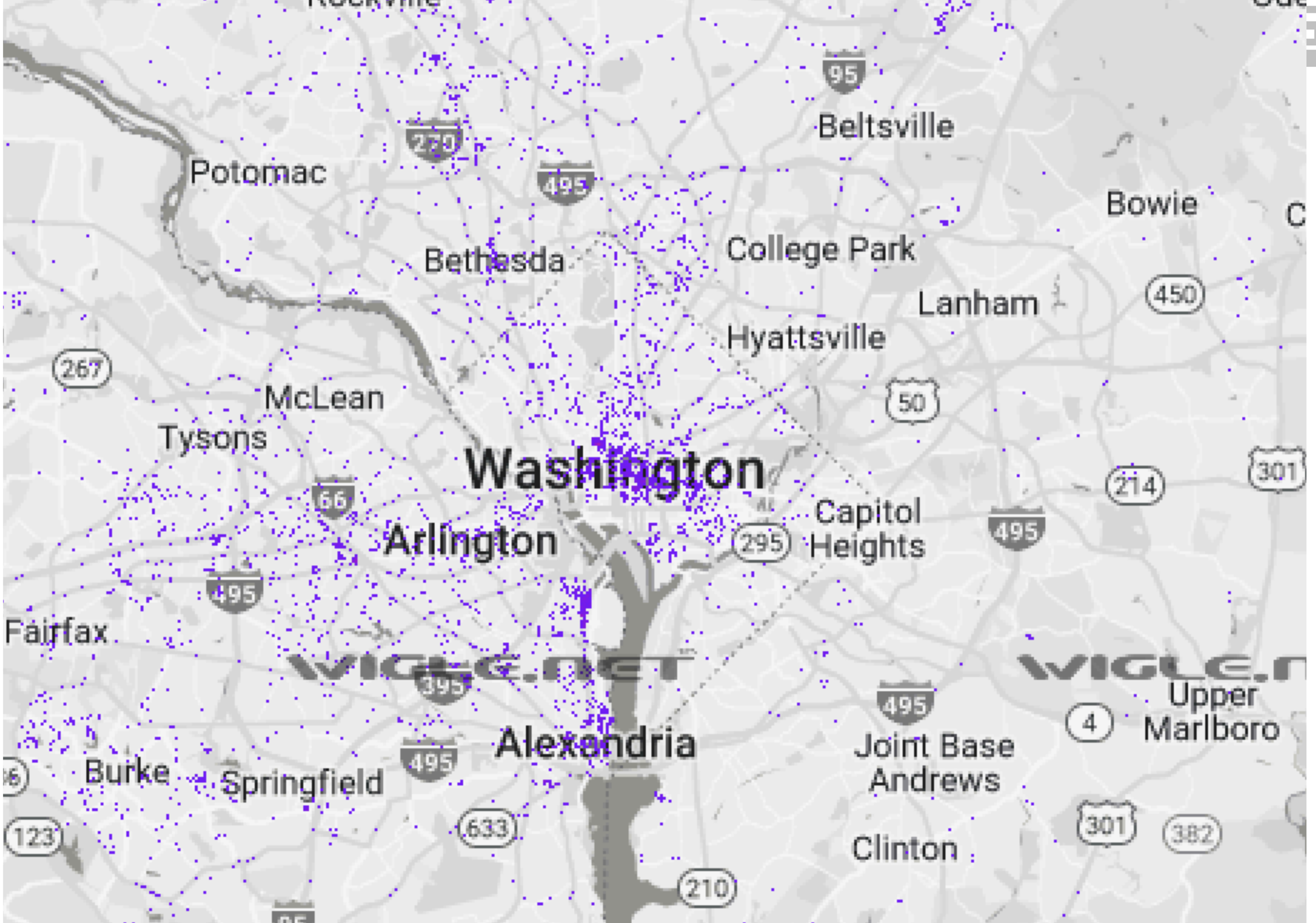
Sleep Apnea <- Obesity <- Poverty

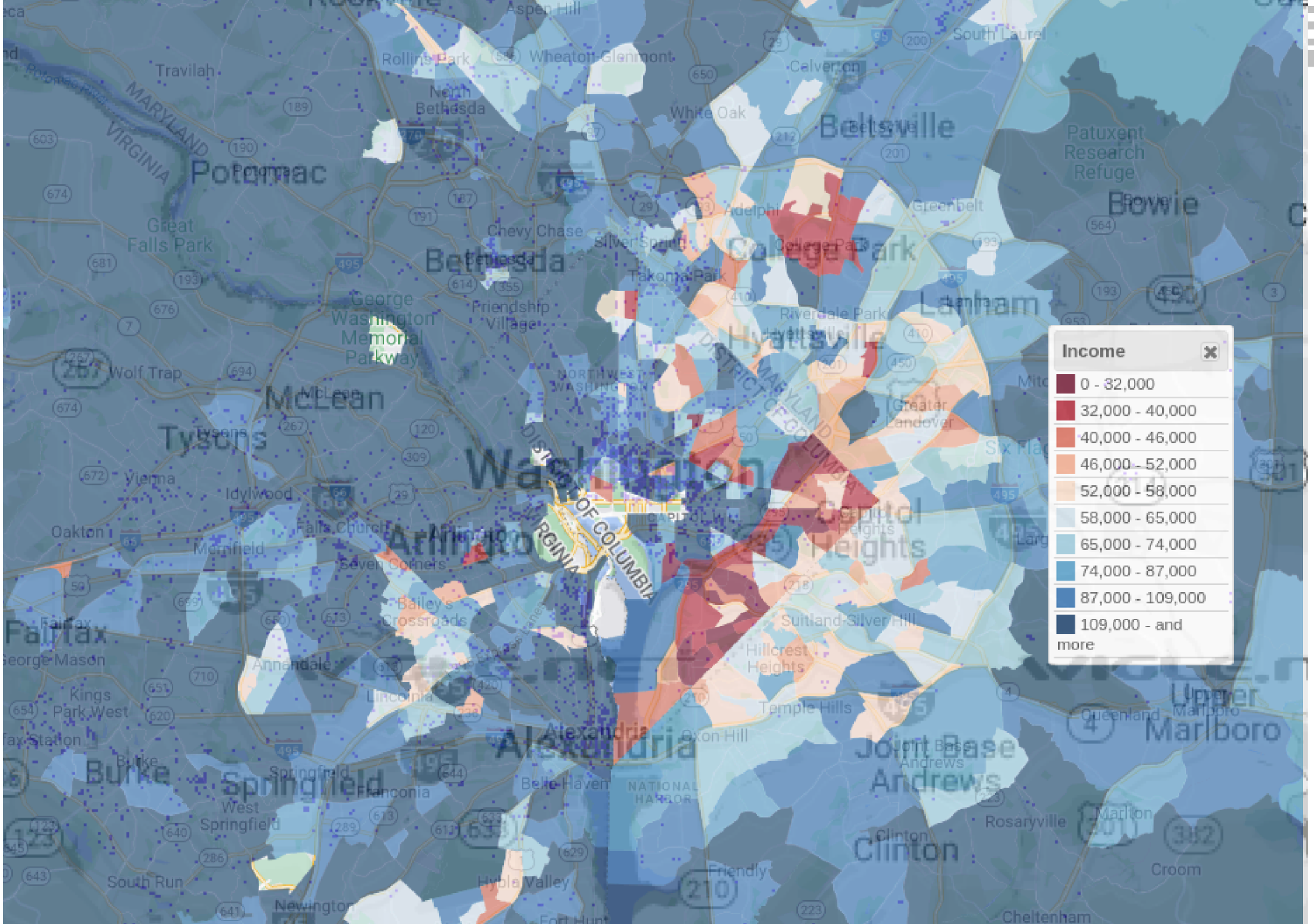
- "There is a linear correlation between obesity and OSA [sleep apnea]"[1]
- There is a link between poverty and obesity[2][3]
- Is a neighborhood with lots of sleep apnea machines likely to be a poorer neighborhood?
- *Or* can the people in poorer neighborhoods not afford bluetooth sleep apnea machines?

[1] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5836788/#:~:text=There%20is%20a%20linear%20correlation,ultimately%20resulting%20in%20sleep%20apnea.
[2] https://www.seacaa.org/post/the-link-between-poverty-and-obesity#:~:text=There%20tends%20to%20be%20fewer,major%20contributing%20factor%20to%20obesity.
[3] https://scholars.org/contribution/why-poverty-leads-obesity-and-life-long-problems


Potomac
Beltsville
Bethesda
College Park
Bowie
Lanham
Hyattsville
McLean
Tyson's
Washington
Arlington
Capitol Heights
Fairfax
Alexandria
Joint Base Andrews
Upper Marlboro
Burke
Springfield
Clinton
95
270
495
450
267
50
66
295
214
301
395
4
123
633
210
382


Income
0 - 32,000
32,000 - 40,000
40,000 - 46,000
46,000 - 52,000
52,000 - 58,000
58,000 - 65,000
65,000 - 74,000
74,000 - 87,000
87,000 - 109,000
109,000 - and more
Potomac
Bethesda
Washington
Arlington
Alexandria
Springfield
Fairfax
Tysons
McLean
Beltsville
College Park
Hyattsville
Capitol Heights
Joint Base Andrews
Clinton
Bowie
Upper Marlboro
Patuxent Research Refuge
Great Falls Park
Wolf Trap
Oakton
Vienna
Idylwood
Falls Church
Seven Corners
Bailey's Crossroads
Annandale
Lincolnia
Kings Park West
Burke
West Springfield
Franconia
South Run
Newington
Hybla Valley
Belle Haven
Oxon Hill
Temple Hills
Hillcrest Heights
Suitland-Silver Hill
Greater Landover
Riverdale Park
Lanham
Greenbelt
Adelphi
Takoma Park
Silver Spring
Chevy Chase
Friendship Village
George Washington Memorial Parkway
Travilah
Rollins Park
North Bethesda
Wheaton-Glenmont
Aspen Hill
White Oak
Calverton
South Laurel
Friendly
Clinton
Rosaryville
Marlton
Croom
Cheltenham
Queenland
Upper Marlboro
MARYLAND
VIRGINIA
DISTRICT OF COLUMBIA
NATIONAL HARBOR


Potomac
Beltsville
Bethesda
College Park
Bowie
Lanham
Hyattsville
McLean
Tyson's
Washington
Arlington
Capitol Heights
Fairfax
Alexandria
Joint Base Andrews
Upper Marlboro
Burke
Springfield
Clinton
95
270
495
450
267
50
66
295
214
301
395
4
123
633
210
382


Income
0 - 32,000
32,000 - 40,000
40,000 - 46,000
46,000 - 52,000
52,000 - 58,000
58,000 - 65,000
65,000 - 74,000
74,000 - 87,000
87,000 - 109,000
109,000 - and more
Potomac
Bethesda
Washington
Arlington
Alexandria
Springfield
Fairfax
Tysons
McLean
Beltsville
College Park
Hyattsville
Capitol Heights
Joint Base Andrews
Clinton
Bowie
Upper Marlboro
Patuxent Research Refuge
Great Falls Park
Wolf Trap
Oakton
Vienna
Idylwood
Falls Church
Seven Corners
Bailey's Crossroads
Annandale
Lincolnia
Kings Park West
Burke
West Springfield
Franconia
South Run
Newington
Hybla Valley
Belle Haven
Oxon Hill
Temple Hills
Hillcrest Heights
Suitland-Silver Hill
Greater Landover
Riverdale Park
Lanham
Greenbelt
Adelphi
Takoma Park
Silver Spring
Chevy Chase
Friendship Village
George Washington Memorial Parkway
Travilah
Rollins Park
North Bethesda
Wheaton-Glenmont
Aspen Hill
White Oak
Calverton
South Laurel
Friendly
Clinton
Rosaryville
Marlton
Croom
Cheltenham
Queenland
Upper Marlboro
MARYLAND
VIRGINIA
DISTRICT OF COLUMBIA
NATIONAL HARBOR

Heavy Machinery

- Regex: ^CATBTNT-0(4|7) [A-Z]{3}[0-9]{5}$ (3 char model, 5 serial?)
  - "CATBTNT-04 DKS02123"
  - "CATBTNT-04 LHW00220"
  - "CATBTNT-07 WCH10725"

https://fccid.io/PQMA5S4/User-Manual/Exhibit-D-Users-Manual-per-2-1033-b3-3137980.pdf

Heavy Machinery

- Regex: ^CATBTNT-0(4|7) [A-Z]{3}[0-9]{5}$ (3 char model,
  - "CATBTNT-04 DKS02123"
  - "CATBTNT-04 LHW00220"
  - "CATBTNT-07 WCH10725"

Cat Bluetooth Network Transceiver Overview

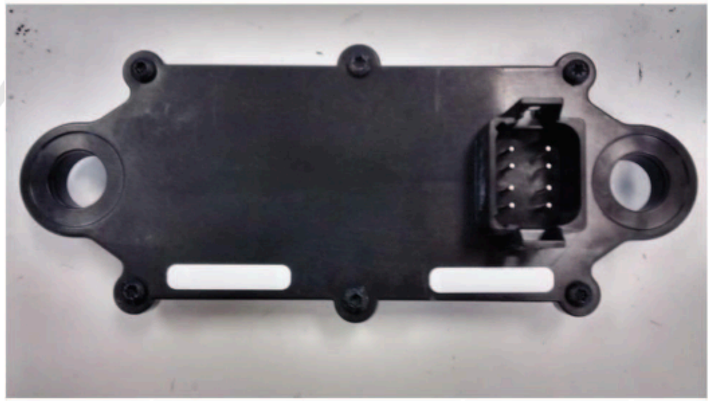
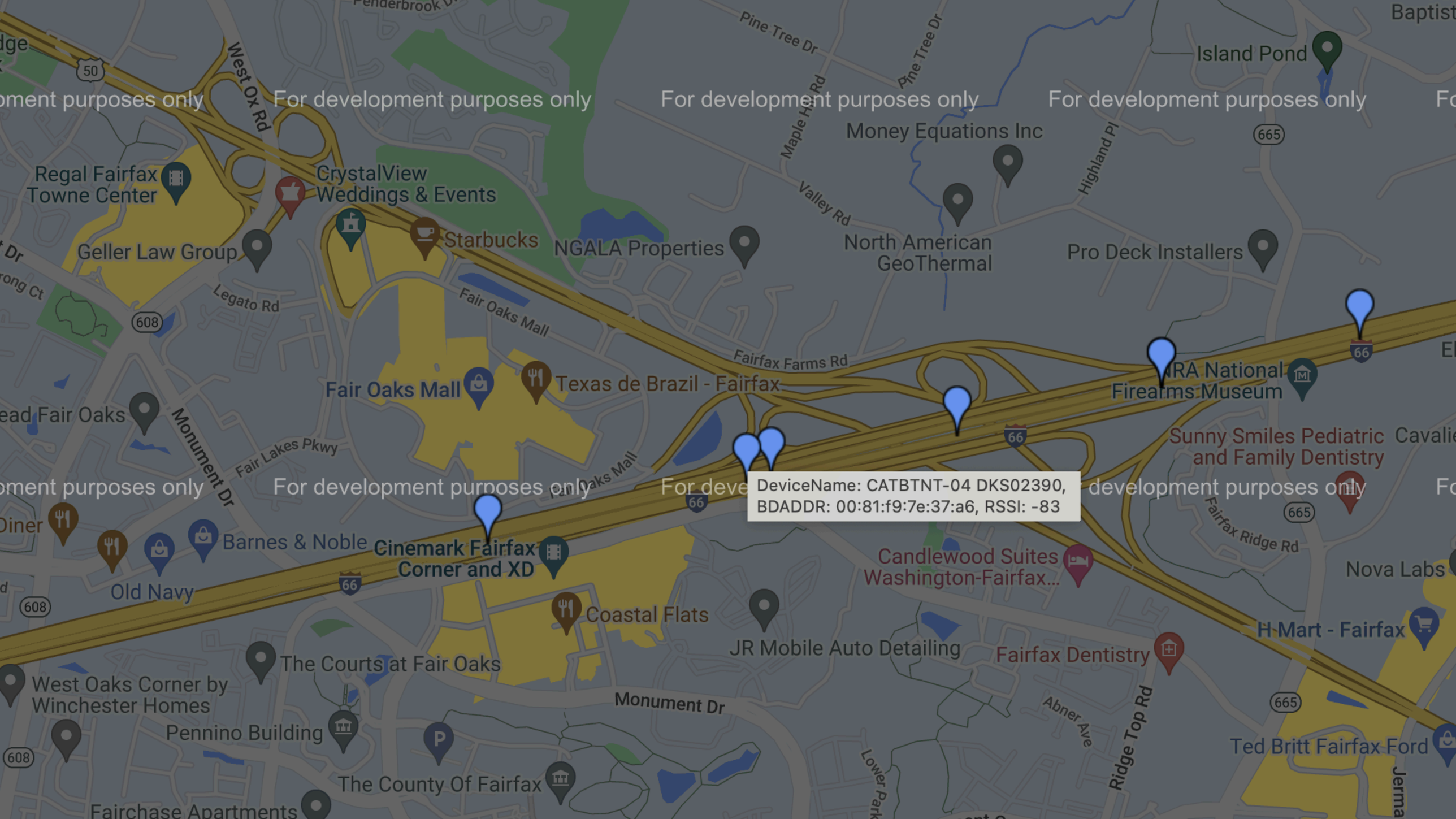


Illustration 1 g06087602

The Cat BTNT acts as a central hub for wireless Bluetooth devices on Cat machines. The Bluetooth network uses Bluetooth Low Energy technology. This technology enables the machine to read Cat key fobs and sensors wirelessly and convert the data to standard and proprietary J1939 messages. These messages are sent over the CAN datalink to a machine control ECM to enable operator identification or machine system security.

https://fccid.io/PQMA5S4/User-Manual/Exhibit-D-Users-Manual-per-2-1033-b3-3137980.pdf


DeviceName: CATBTNT-04 DKS02390,
BDADDR: 00:81:f9:7e:37:a6, RSSI: -83
For development purposes only
Regal Fairfax Towne Center
CrystalView Weddings & Events
Starbucks
Geller Law Group
NGALA Properties
Money Equations Inc
North American GeoThermal
Pro Deck Installers
Island Pond
Fair Oaks Mall
Texas de Brazil - Fairfax
NRA National Firearms Museum
Sunny Smiles Pediatric and Family Dentistry
Barnes & Noble
Cinemark Fairfax Corner and XD
Old Navy
Coastal Flats
Candlewood Suites Washington-Fairfax...
Nova Labs
H Mart - Fairfax
JR Mobile Auto Detailing
Fairfax Dentistry
The Courts at Fair Oaks
West Oaks Corner by Winchester Homes
Pennino Building
The County Of Fairfax
Ted Britt Fairfax Ford
Fairchase Apartments
Monument Dr
Fairfax Farms Rd
Fair Oaks Mall
Fair Lakes Pkwy
Legato Rd
Valley Rd
Pine Tree Dr
West Ox Rd
Highland Pl
Abner Ave
Ridge Top Rd
Fairfax Ridge Rd
Lower Park
50
608
66
665

Name of product: Cat® Bluetooth® Network
Make: Cat® Brand
Model: CATBTNT
(A5:S4)
Type: Wireless Device (Module for the reception-transmission of data from Bluetooth® Key Fob and sensors)
SMCS Code: 7008; 7600-ZM

The CATBTNT part number 504-4980 is the buy-level part that includes a radio equipment and a software tied to the machine integration. The radio equipment contained in the CATBTNT is 462-0441. Such radio equipment complies with the applicable regional product compliance requirements as demonstrated with the attached DoC. The software included in the buy-level part does not impact regulatory performance parameters.

Name of product: Cat® Bluetooth® FOB
Make: Cat® Brand
Model: CATBTFOB
(A1:S1)
Type: Wireless Device (Chip-key for operator identification with Bluetooth®)
SMCS Code: 7008; 7600-ZM

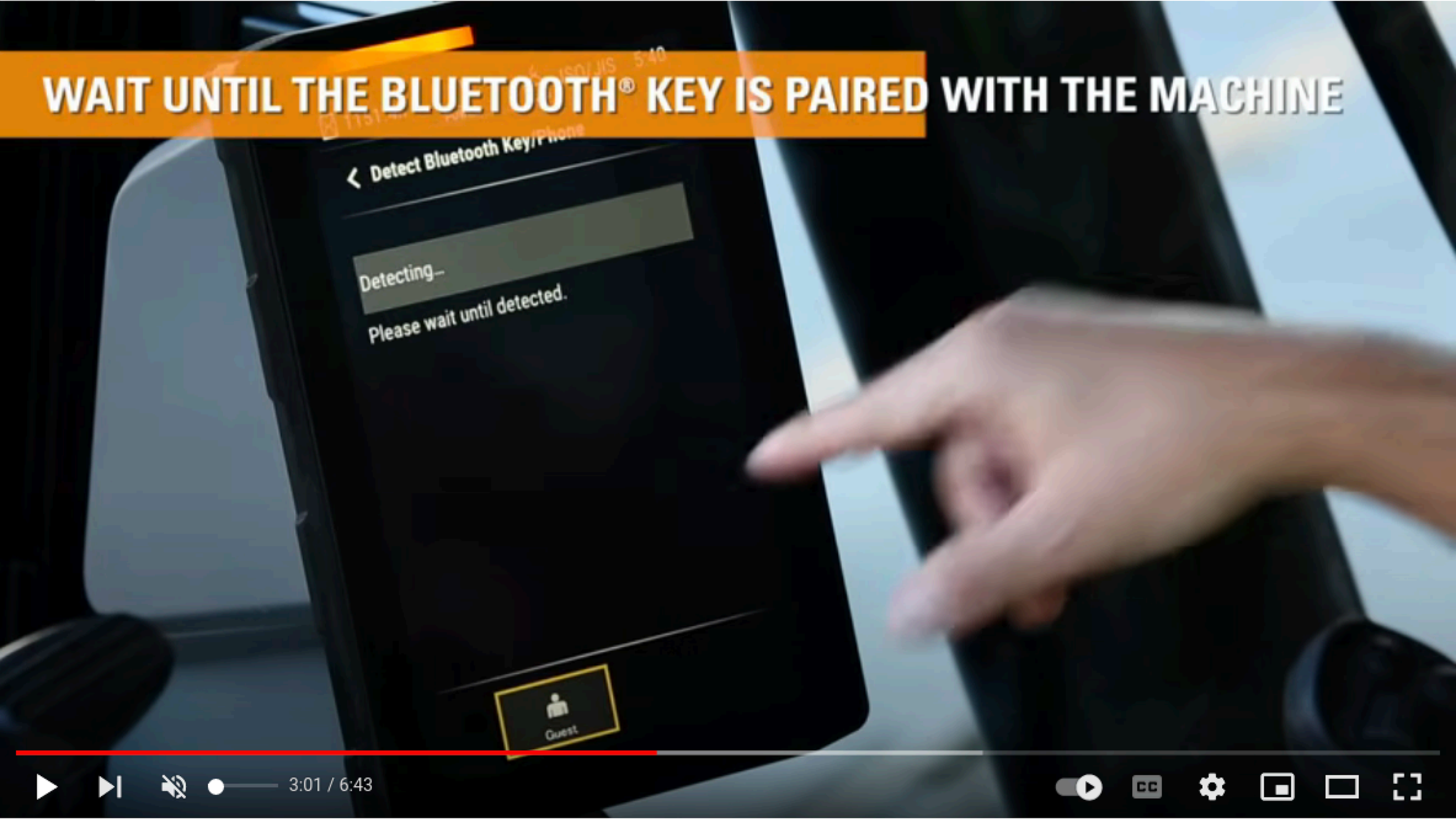
https://s7d2.scene7.com/is/content/Caterpillar/CM20201217-d18d8-0b502

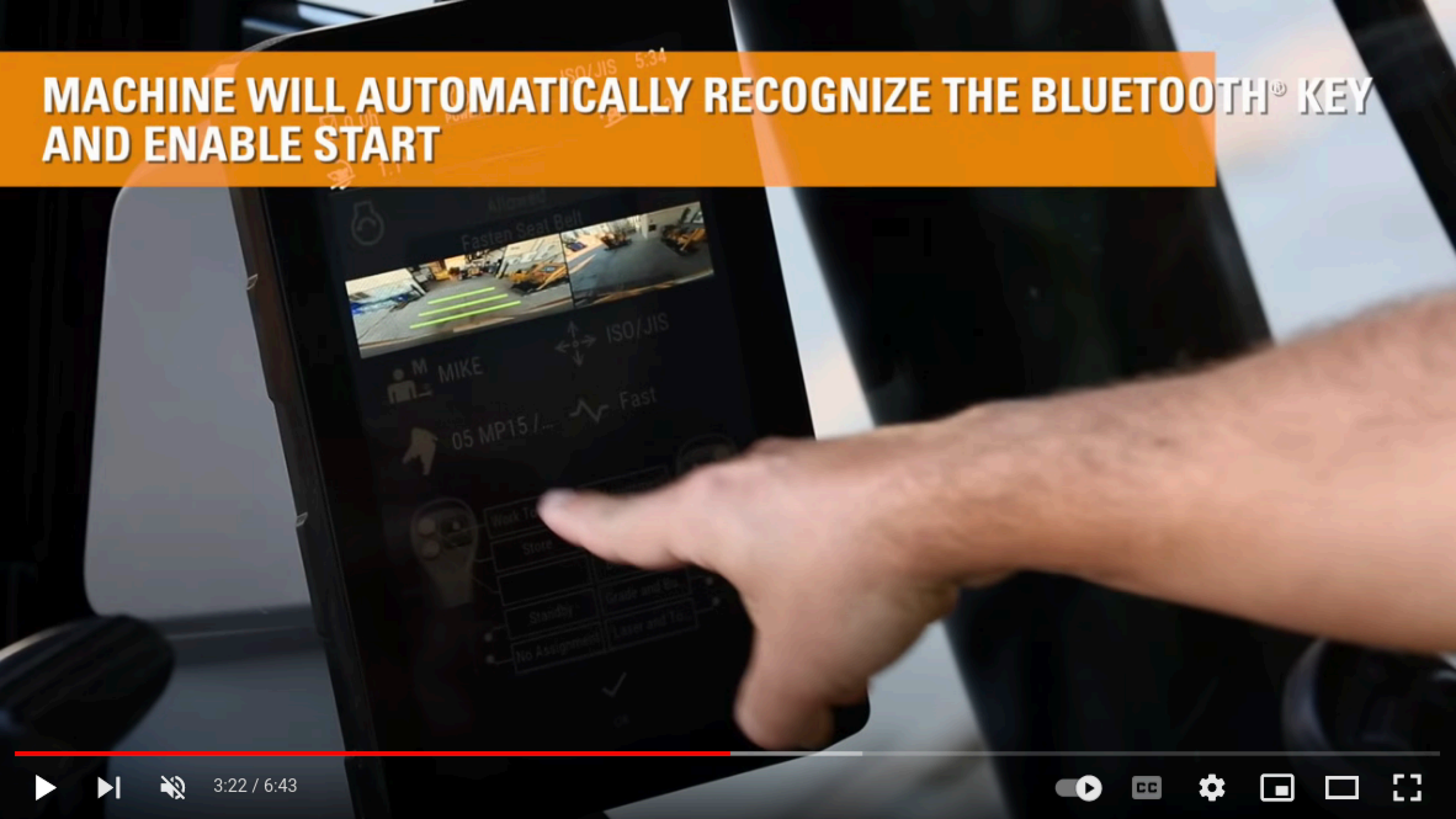
INTRODUCE THE MAC ID KEY CODE
Key Code
5065
1 2 3 4 5
6 7 8 9 0
A B C
D E F
Close
OK
P/N: 487-3004-03
S/N: AK0W00DVA1
MAC ID: 5065837D1887
MODEL: CATBTFOB
CMIIT ID: 2016DJ9153
TA= 2016 2631
ASSEMBLED IN USA
TRA
REGISTERED No:
ER49295/16
DEALER No:
DA0130583/14
ictQATAR
Type Approval reg. No:
CRA/SA/2016/R-5775
This Telecommunications equipment conforms to NTC technical requirements
2:44 / 6:43

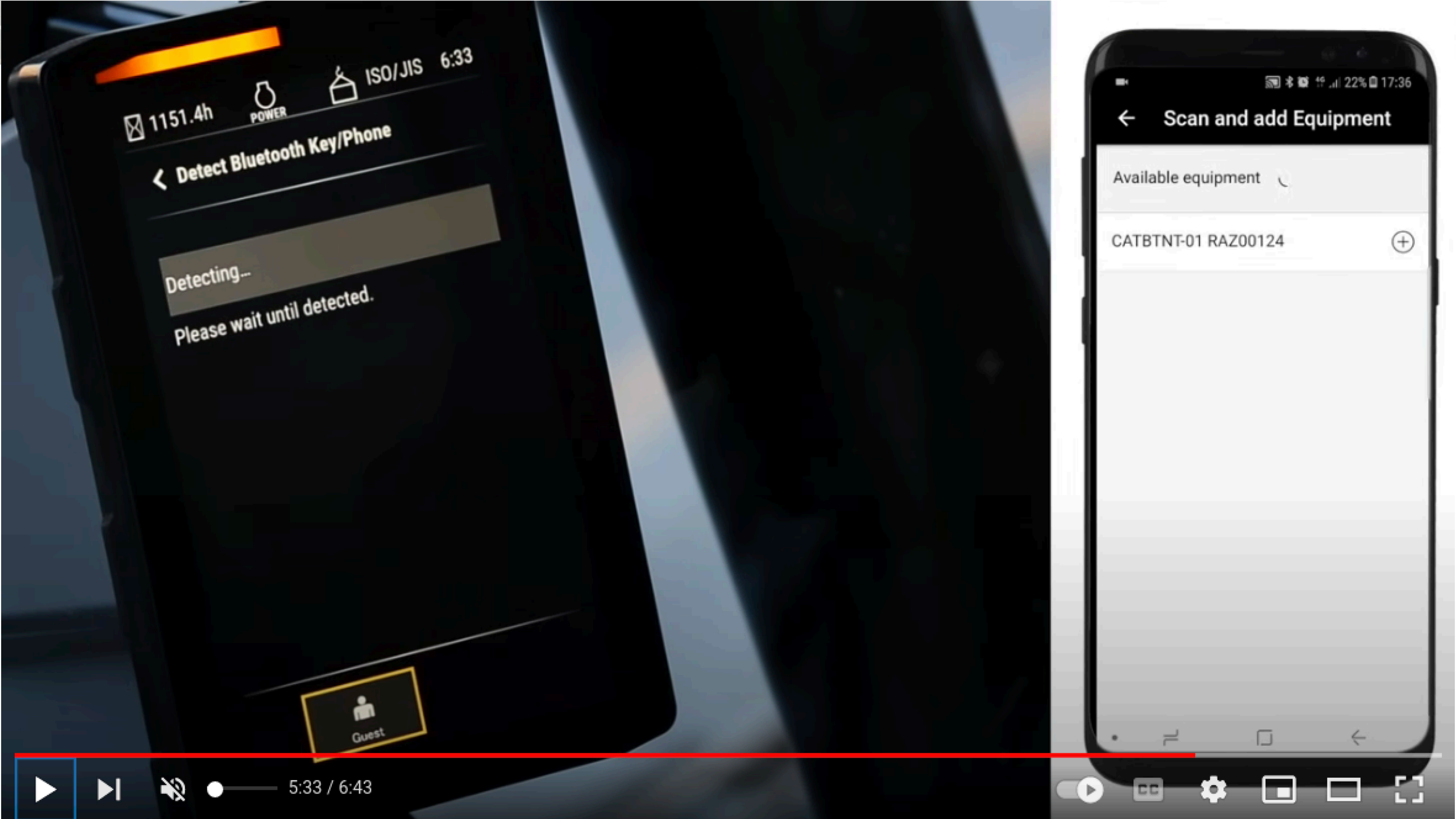
INTRODUCE THE MAC ID KEY CODE
Key Code
5065
1 2 3 4 5
6 7 8 9 0
A B C
D E F
Close
OK
Note: "50:65:83" is a Texas Instruments OUI (and all devices in my data use public TI BDADDRS)
P/N: 487-3004-03
S/N: AK0W00DVA1
MAC ID: 5065837D1887
MODEL: CATBTFOB
CMIIT ID: 2016DJ9153
TA= 2016:2631
ASSEMBLED IN USA
TRA REGISTERED No: ER49295/16
DEALER No: DA0130583/14
ictQATAR
Type Approval reg. No: CRA/SA/2016/R-5775
This Telecommunications equipment conforms to NTC technical requirements
2:44 / 6:43

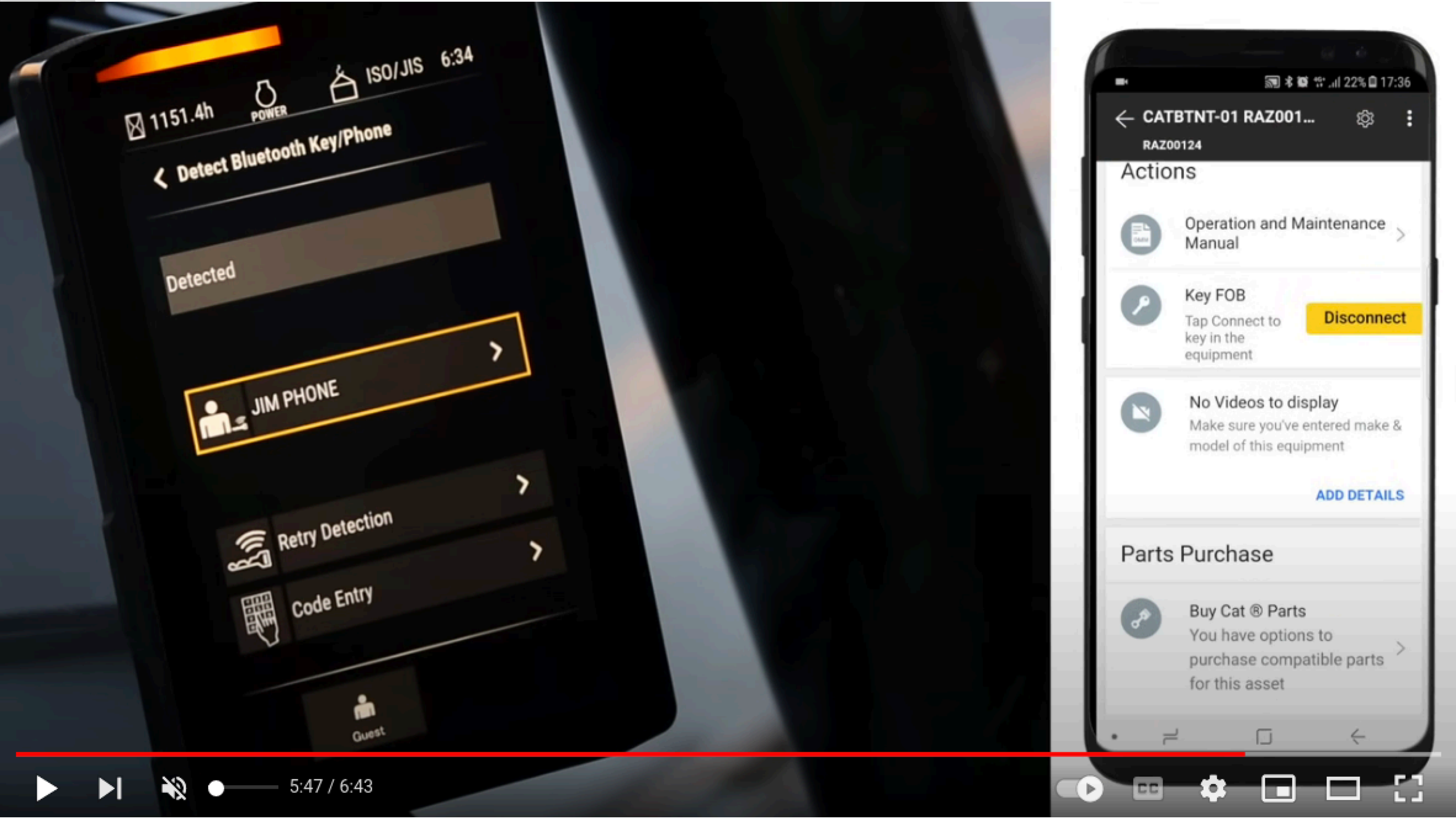
INTRODUCE THE MAC ID KEY CODE
Key Code
5065
1 2 3 4 5
6 7 8 9 0
A B C
D E F
Close
OK
Note: "50:65:83" is a Texas Instruments OUI (and all devices in my data use public TI BDADDRS)
P/N: 487-3004-03
S/N: AK0W00DVA1
MAC ID: 5065837D1887
MODEL: CATBTFOB
CMIIT ID: 2016DJ9153
TA= 2016:2631
ASSEMBLED IN USA
TRA REGISTERED No: ER49295/16 DEALER No: DA0130583/14
ictQATAR Type Approval reg. No: CRA/SA/2016/R-5775
This Telecommunications equipment conforms to NTC technical requirements
2:44 / 6:43

INTRODUCE THE MAC ID KEY CODE
Key Code
5065837D1
1 2 3 4 5
6 7 8 0
A B C
D E F
Close
OK
CMIIT ID: 2016DJ9153
MAC ID:
5065837D1887
2:49 / 6:43

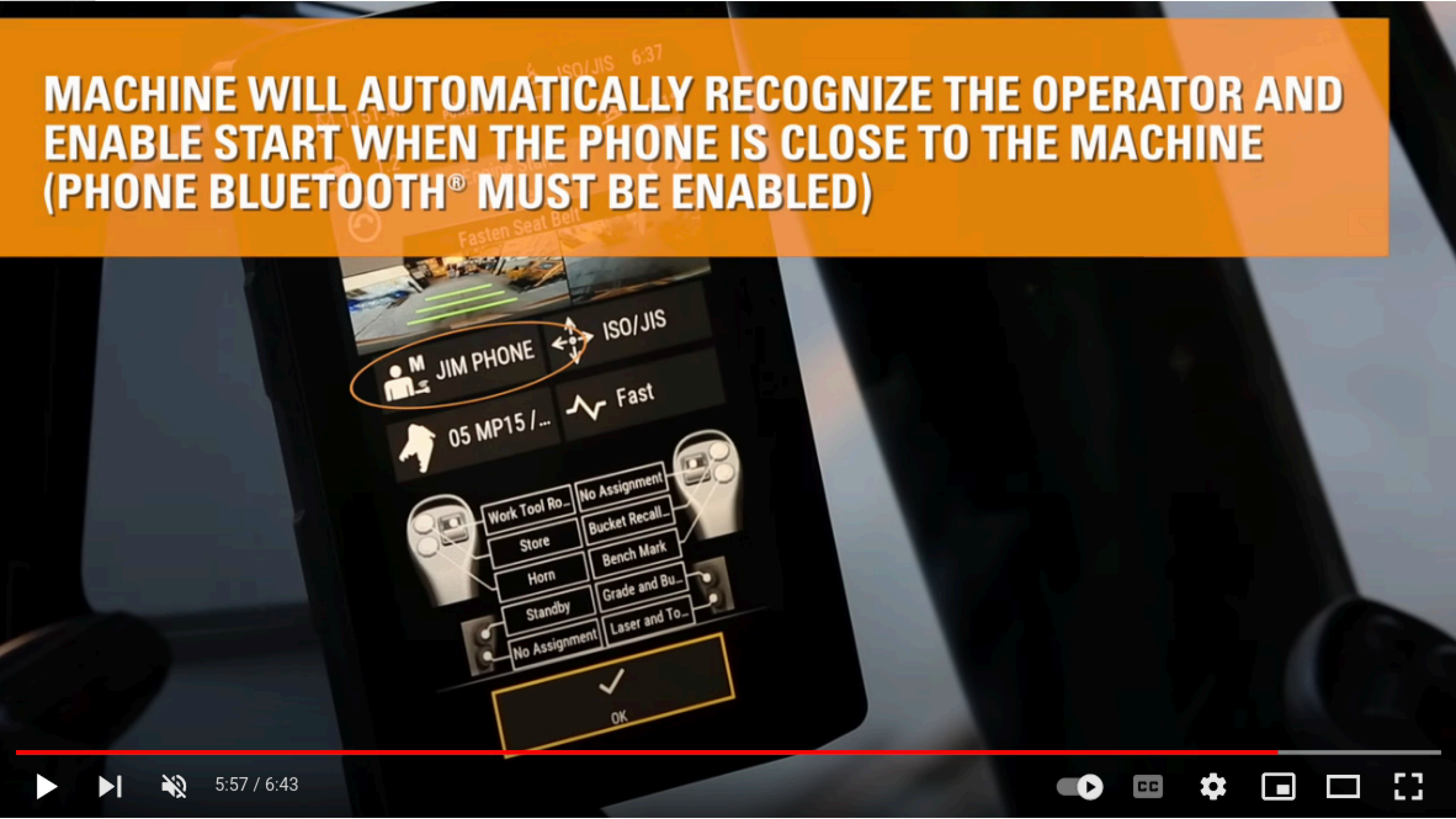

WAIT UNTIL THE BLUETOOTH® KEY IS PAIRED WITH THE MACHINE
Detect Bluetooth Key/Phone
Detecting...
Please wait until detected.
Guest
3:01 / 6:43


MACHINE WILL AUTOMATICALLY RECOGNIZE THE BLUETOOTH® KEY AND ENABLE START
Fasten Seat Belt
ISO/JIS
MIKE
Fast
05 MP15 /...
3:22 / 6:43


1151.4h
POWER
ISO/JIS
6:33
Detect Bluetooth Key/Phone
Detecting...
Please wait until detected.
Guest
22% 17:36
Scan and add Equipment
Available equipment
CATBTNT-01 RAZ00124
5:33 / 6:43

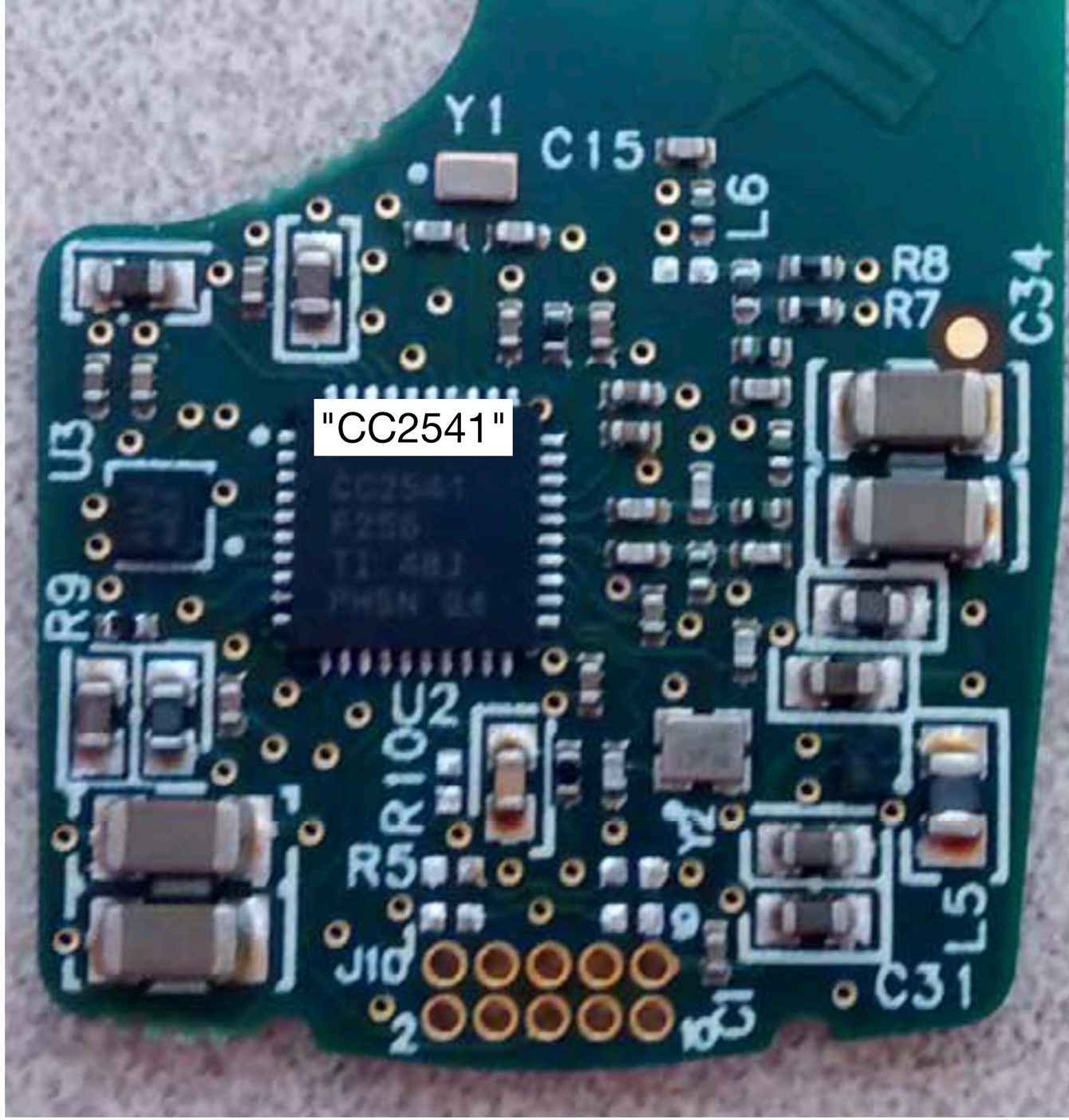

1151.4h
POWER
ISO/JIS
6:34
Detect Bluetooth Key/Phone
Detected
JIM PHONE
Retry Detection
Code Entry
Guest
22% 17:36
CATBTNT-01 RAZ001...
RAZ00124
Actions
Operation and Maintenance Manual
Key FOB
Tap Connect to key in the equipment
Disconnect
No Videos to display
Make sure you've entered make & model of this equipment
ADD DETAILS
Parts Purchase
Buy Cat ® Parts
You have options to purchase compatible parts for this asset
5:47 / 6:43

MACHINE WILL AUTOMATICALLY RECOGNIZE THE OPERATOR AND ENABLE START WHEN THE PHONE IS CLOSE TO THE MACHINE (PHONE BLUETOOTH® MUST BE ENABLED)



https://www.youtube.com/watch?v=caJT5qqj_cI

https://www.youtube.com/watch?v=caJT5qqj_cI



https://fccid.io/PQMA1S1/Internal-Photos/Exhibit-C-Internal-Photographs-per-2-1033-b7-3154594.pdf

DARK MENTOR

2.4-GHz *Bluetooth*™ low energy and Proprietary System-on-Chip

Check for Samples: CC2541

FEATURES

- RF
  - 2.4-GHz *Bluetooth* low energy Compliant and Proprietary RF System-on-Chip
  - Supports 250-kbps, 500-kbps, 1-Mbps, 2-Mbps Data Rates
  - Excellent Link Budget, Enabling Long-Range Applications Without External Front End
  - Programmable Output Power up to 0 dBm
  - Excellent Receiver Sensitivity (–94 dBm at 1 Mbps), Selectivity, and Blocking Performance
  - Suitable for Systems Targeting Compliance With Worldwide Radio Frequency Regulations: ETSI EN 300 328 and EN 300 440 Class 2 (Europe), FCC CFR47 Part 15 (US), and ARIB STD-T66 (Japan)
- Layout
  - Few External Components
  - Reference Design Provided
  - 6-mm × 6-mm QFN-40 Package
  - Pin-Compatible With CC2540 (When Not Using USB or I^2C)
- Low Power
  - Active-Mode RX Down to: 17.9 mA
  - Active-Mode TX (0 dBm): 18.2 mA
  - Power Mode 1 (4-μs Wake-Up): 270 μA
  - Power Mode 2 (Sleep Timer On): 1 μA
  - Power Mode 3 (External Interrupts): 0.5 μA
  - Wide Supply-Voltage Range (2 V–3.6 V)
- TPS62730 Compatible Low Power in Active Mode
  - RX Down to: 14.7 mA (3-V supply)
  - TX (0 dBm): 14.3 mA (3-V supply)
- Microcontroller
  - High-Performance and Low-Power 8051 Microcontroller Core With Code Prefetch
  - In-System-Programmable Flash, 128- or 256-KB
  - 8-KB RAM With Retention in All Power Modes
  - Hardware Debug Support
  - Extensive Baseband Automation, Including Auto-Acknowledgment and Address Decoding
  - Retention of All Relevant Registers in All Power Modes
- Peripherals
  - Powerful Five-Channel DMA
  - General-Purpose Timers (One 16-Bit, Two 8-Bit)
  - IR Generation Circuitry
  - 32-kHz Sleep Timer With Capture
  - Accurate Digital RSSI Support
  - Battery Monitor and Temperature Sensor
  - 12-Bit ADC With Eight Channels and Configurable Resolution
  - AES Security Coprocessor
  - Two Powerful USARTs With Support for Several Serial Protocols
  - 23 General-Purpose I/O Pins (21 × 4 mA, 2 × 20 mA)
  - I^2C interface
  - 2 I/O Pins Have LED Driving Capabilities
  - Watchdog Timer
  - Integrated High-Performance Comparator
- Development Tools
  - CC2541 Evaluation Module Kit (CC2541EMK)
  - CC2541 Mini Development Kit (CC2541DK-MINI)
  - SmartRF™ Software
  - IAR Embedded Workbench™ Available

Please be aware that an important notice concerning availability, standard warranty, and use in critical applications of Texas Instruments semiconductor products and disclaimers thereto appears at the end of this data sheet.

Bluetooth is a trademark of Bluetooth SIG, Inc..
ZigBee is a registered trademark of ZigBee Alliance.

PRODUCTION DATA information is current as of publication date. Products conform to specifications per the terms of the Texas Instruments standard warranty. Production processing does not necessarily include testing of all parameters.

Copyright © 2012–2013, Texas Instruments Incorporated

https://www.ti.com/lit/ds/symlink/cc2541.pdf?ts=1680851781995&ref_url=http%253A%252F%252Fwww.google.com

CC2541DK-MINI

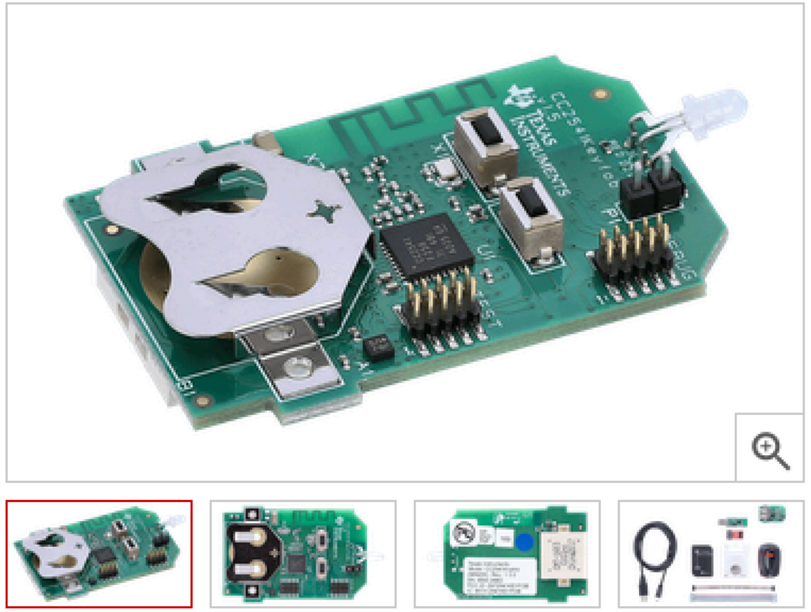
CC2541 Mini Development Kit

Order now

Overview

Description & features | Supported products

The CC2541DK-MINI development kit provides a working reference design for software development of single-mode *Bluetooth* low energy (BLE) applications based on the Texas Instruments CC2541. The included "keyfob" board operates as a BLE peripheral device, and contains modifiable software that can be tailored towards different applications. Using BTool (Windows PC application) along with the included CC2540 USB Dongle, the Texas Instruments BLE stack can be tested and verified while developing custom applications.



Features

The kit contains the following hardware components:

Price

$ Min to $ Max

See all

Buying Format

- All Listings
- Accepts Offers
- Auction
- Buy It Now

All Listings | Accepts Offers | Auction | Buy It Now | Condition | Shipping | Local

0 results for **CATBTNT** Save this search

Shipping to: 20705

No exact matches found

Save this search to receive email alerts and notifications when new items are available.

Save this search

Tell us what you think

CAT 5 Caterpillar Keys Loader Skidder Paver Tractor Excavator Compactor Dozer

Condition: **New**

Bulk savings:

Buy 1	Buy 2	Buy 3
$8.95/ea	**$8.06/ea**	**$7.61/ea**

4 or more for $7.16/ea

Quantity: 1 More than 10 available / **84 sold**

Price: **US $8.95/ea**

Buy It Now

Add to cart

♡ Add to Watchlist

Fast and reliable. Ships from United States.

This one's trending. 84 have already sold.

Caterpillar (CAT) Equipment Igniton / Door / Hood Key

Golden Color

Parts No: 5P8500 , 5P-8500

A package contains 5 keys

If you are fed up with heavy and thick keys, It will be your best choice

Compatible models

Wheel-Type Loader

901C 901C2 902 902C 902C2 903C 903C2 903D 904B 904H 906 906H 906H2 906K 906M 907H 907H2 907K 907M 908 908H 908H2 908K 908M 910 910E 910F 910K 910M 914G 914G2 914K 914M 916 918F 918M 920 920K 924F 924G 924GZ 924H 924HZ 924K 926 926E 926M 928F 928G 928H 928HZ 930 930G 930H 930K 930M 930R 930T 936 936E 936F 938F 938G 938G II 938H 938K 938M 950 950 GC 950B 950B/950E 950E 950F 950F II 950G 950G II 950H 950K 950L 950M 950M Z 960F 962 962G 962G II 962H 962K 962L 962M 962M Z 966 GC 966C 966D 966E 966F 966F II 966G 966G II 966H 966K 966K XE 966L 966M 966M XE 970F 972G 972G II 972H 972K 972L 972M 972M XE 980 980B 980C 980F 980F II 980G 980G II 980H 980K 980K HLG 980L 980M 980XE 982 982M 982XE 986H 986K 988 988B 988F 988F II 988G 988H 988K 988K XE 990 990 II 990H 990K 992C 992D 992G 992K 993K 994 994D 994F 994H 994K G910 G916 G926 G936

Challenger

35 45 55 65 65B 75

Engine - Generator Set

3406C 3512 3512B 3516 3516B 3516B GEN 3516C 3516E C13 C13GENSET C15 C175-16 C2.2 C32 C4.4 C6.6 C7.1 DG150 DG60 G3412C G3516H PM3412 PM3456 PM3508 PM3512 PM3516 PMG3516 XQC1200 XQC1600 XQG400

Wheel-Type Skidder

120C 508 515 518 518C 525 525B 525C 525D 528 528B 530B 535B 535C 535D 545 545C 545D 555D

Off-Highway Truck

69D 768C 769 769B 769C 769D 770 770G 770G OEM 771C 771D 772 772B 772G 772G OEM 773B 773D 773E 773F 773G 773G LRC 773G OEM 773GC 775B 775D 775E 775F 775G 775G LRC 775G OEM 776 776B 776C 776D 777 777B 777C 777D 777E 777F 777G 784B 784C 785 785B 785C 785D 785G 789 789B 789C 789D 789G 793 793B 793C 793D 793F 793F AC 793F CMD 793F OEM 793F XQ 794 AC 795F AC 795F XQ 796 AC 797 797B 797F 798 798 AC

Track-Type Loader

931 931B 931C 931C II 933 933C 935B 935C 935C II 939 939C 941 943 951 951B 951C 953 953B 953C 953D 953K 955 955L 963 963B 963C 963D 963K 973 973C 973D 973K 977 977L 983 983B

Engine - Industrial

3126B 3176C 3196 3306B 3406C 3406E 3408E 3412 3412C 3412E 3456 3508 3508B 3512 3512B 3512C 3516 3516B 3516C 3516E C-10 C-12 C-15 C-16 C-9 C11 C13 C13B C15 C15 I6 C175-16 C18 C18 I6 C27 C32 C4.4 C7 C9 C9 GEN SET C9.3 C9.3B DG100 DG125 DG60 DG80 G3508 G3512 G3512E G3512H G3516 G3516B G3516C G3516E G3516H G3520 G3520C G3520E G3520H PM3412

Articulated Dump Truck

725 725C 725C2 730 730C 730C2 730C2 EJ 735 735 OEM 735B 735C 740 740 GC 740B 740C 745 745C D20D D250B D250D D250E D250E II D25C D25D D300B D300D D300E D300E II D30C D30D D350C D350D D350E D350E II D35C D35HP D400 D400D D400E D400E II D40D

Mini Hydraulic Excavator

300.9D 301.4C 301.5 301.6 301.6C 301.7D 301.7D CR 301.8 301.8C 302.2D 302.4D 302.5 302.5C 302.7D 303 303.5 303.5C 303.5D 303.5E 303.5E2 303.5E2 CR 303E CR 304 304.5 304.5E2 304E 304E2 304E2 CR 305 305.5 305.5D 305.5E 305.5E2 305.5E2 CR 305C CR 305D CR 305E 305E2 305E2 CR 306 306.5 306E 306E2 307 307-A 307.5 307B 307D 307E 307E2 308 308.5 308D 308E 308E2 308E2 CR 309 310

Road Reclaimer

RM-250C RM-300 RM-350 RM-350B RM-500 RM400 RM500B RR-250 RR-250B SM-350 SS-250 SS-250B

Motor Grader

120 120G 120H 120H ES 120H NA 120K 120K 2 120M 120M 2 12F 12G 12H 12H ES 12H NA 12K 12M 12M 2 12M 3 12M 3 AWD 130G 135H 135H NA 14 140 140 GC 140G 140H 140H ES 140H NA 140K 140K 2 140M 140M 2 140M 3 140M 3 AWD 143H 14G 14H 14H NA 14L 14M 14M-3 14M3 150 16 160 160G 160H 160H ES 160H NA 160K 160M 160M 2 160M 3 160M 3 AWD 163H 163H NA 16G 16H 16H NA 16M 16M3 18 18M3 24 24H 24M 404F-22

Track-Type Skidder

120C 125C 4P 517 527 54H D4HTSK II D4HTSK III D5HTSK II

TELEHANDLER

RT100 RT50 RT50SA RT60 RT80 RTC60 TH103 TH210 TH215 TH220B TH255C TH306D TH314D TH330B TH336C TH337C TH340B TH350B TH3510D TH355B TH357D TH360B TH406C TH407C TH408D TH414C TH417C TH417D TH460B TH514C TH514D TH560B TH580B TH62 TH63 TH82 TH83 TL1055C TL1055D TL1255C TL1255D TL642C TL642D TL943C TL943D

Wheel Dozer

814 814B 814F 814F II 814K 824B 824C 824G 824G II 824H 824K 824S 834 834B 834G 834H 834K 834S 834U 844 844H 844K 854G 854K

Backhoe Loader

414E 415 415F2 415F2 IL 416 416B 416C 416D 416E 416F 416F2 420 420D 420E 420F 420F2 420XE 422E 422F 422F2 424B 424B HD 424B2 424D 426 F2 426B 426C 427F2 428 428B 428C 428D 428E 428F 428F2 430 430D 430E 430F 430F2 432 432D 432E 432F 432F2 434 434E 434F 434F2 436B 436C 438B 438C 438D 440 442D 442E 444 444E 444F 444F2 446B 446D 450 450E 450F

Skid Steer Loader

216 216B 216B3 226 226B 226B3 226D 226D3 232B 232D3 236 236B 236B3 236D 236D3 239D3 242B 242B3 242D 242D3 246 246B 246C 246D 246D3 247B 247B3 248B 249D 249D3 252 252B 252B3 256C 257B 257B3 257D 257D3 259B3 259D 259D3 262 262B 262C 262C2 262D 262D3 267 267B 268B 272C 272D 272D XHP 272D2 272D2 XHP 272D3 272D3 XE 277 277B 277C 277C2 277D 279C 279C2 279D 279D3 287 287B 287C 287C2 287D 289C 289C2 289D 289D3 297C 297D 297D XHP 297D2 297D2 XHP 299C 299D 299D XHP 299D2 299D2 XHP 299D3 299D3 XE

Asphalt Paver

10 FT 10-20B 10-20WB 10B 8 FT 8-16B AP-1000 AP-1000B AP-1000D AP-1000E AP-1000F AP-1050 AP-1050B AP-1055B AP-1055D AP-1055E AP-1055F AP-200 AP-200B AP-255E AP-300D AP-500E AP-555E AP-600D AP-650B AP-655C AP-655D AP-800 AP-800B AP-800C AP-800D AP-900B AP300F AP355F AP500F AP555F AP600F AP655F AP655F L AS2251 AS2252C AS2301 AS2302 AS2302C AS3251C AS3301C AS4252C BG-2255C BG-225C BG-230 BG-230D BG-240C BG-2455C BG-2455D BG-245C BG-260C BG-260D BG1000E BG1055E BG500E BG555E BG600D BG655D SE50 V SE50 VT SE60 V SE60 V XW SE60 VT XW SE60VT XW

Pipelayer

561D 561M 561N 571G 572G 572R 572R II 578 583K 583R 583T 587R 587T 589 594H PL61 PL72 PL83 PL87

Integrated Toolcarrier

IT12 IT12B IT14B IT14F IT14G IT14G2 IT18 IT18B IT18F IT24F IT28 IT28B IT28F IT28G IT38F IT38G IT38G II IT38H IT62G IT62G II IT62H

Marine Products

3126B 3412E 3508B 3512B 3516B C12 C30 C32 C7 C9

Expanded Mining Products

6015B 6020B MD5150C MD6200 MD6250 MD6310 MD6640

Track-Type Tractor

10 10C 10S 10SU 10U 11 11SU 11U 140 141 143 153 163 183B 3 3P 3S 4 4A 4P 4S 5 53 54 55 56 56H 57 57H 58 58L 59 59L 59N 5A 5A PAT 5P 5S 6 6A 6S 6SU 7 7A 7S 7S LGP 7SU 7U 8 8A 8D 8S 8SU 8U 9 9C 9S 9SU 9U D1 D10 D10N D10R D10T D10T2 D11 D11N D11R D11T D2 D3 D3B D3C D3C II D3C III D3G D3K LGP D3K XL D3K2 LGP D3K2 XL D4 D4B D4C D4C II D4C III D4D D4E D4E SR D4G D4H D4H III D4H XL D4K LGP D4K XL D4K2 LGP D4K2 XL D5 D5B D5C D5C III D5C PAT D5C PATLGP D5E D5G D5H D5H XL D5K LGP D5K XL D5K2 LGP D5K2 XL D5M D5N D5R2 D6 D6 XE D6C D6D D6D SR D6E D6E SR D6F SR D6G D6G SR D6G2 LGP D6G2 XL D6GC D6H D6H II D6H XL D6H XR D6K D6K LGP D6K XL D6K2 D6K2 LGP D6K2 XL D6M D6N D6N LGP D6N OEM D6N XL D6R D6R II D6R III D6R LGP D6R STD D6R XL D6T D6T LGP D6T LGPPAT D6T XL D6T XL PAT D6T XW D6T XW PAT D6XE D7E D7E LGP D7F D7G D7G2 D7H D7R D7R II D7R LGP D7R SERIES D7R XR D8H D8K D8L D8N D8R D8R II D8T D9G D9H D9L D9N D9R D9T

Load, Haul, Dump

R1300 R1300G R1300G II R1600 R1600G R1600H R1700 II R1700G R1700K R2900 R2900G R3000H

Utility Vehicle

CUV102D CUV105D CUV82 CUV85

Oem Solutions

CAT WDS

eBay

FCC

User Manual

Buy TI development board
eBay used parts to hack
Find keys that can steal most CAT devices
Find keys that can steal most CAT devices

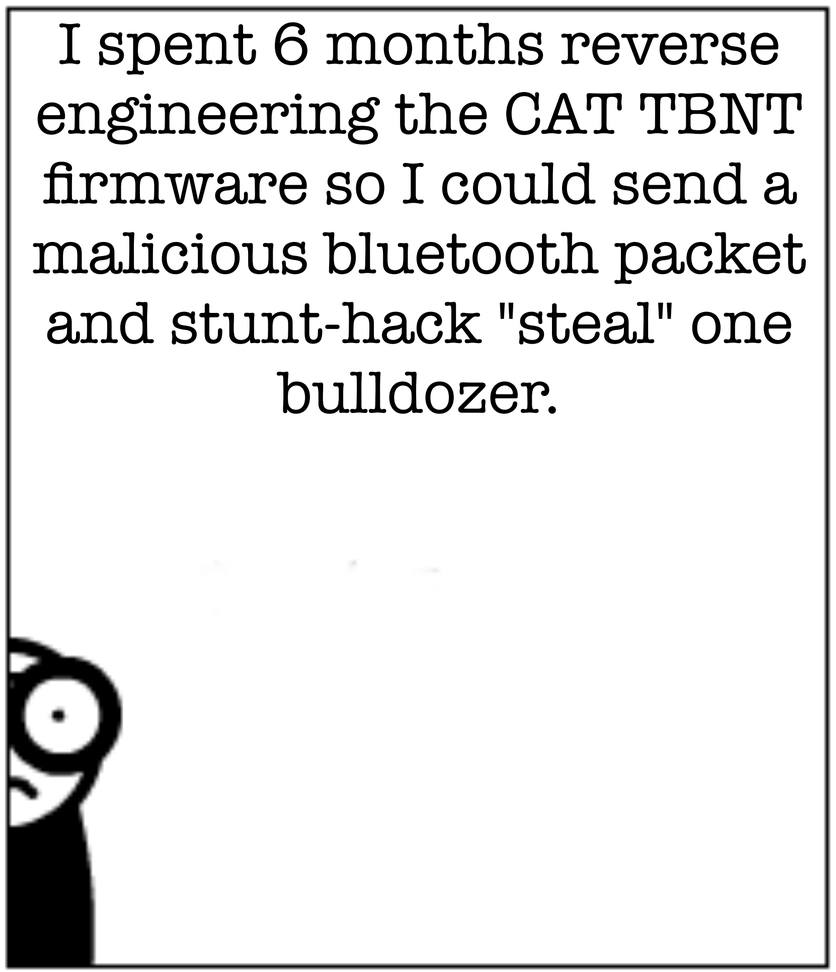
DST2
.FYI

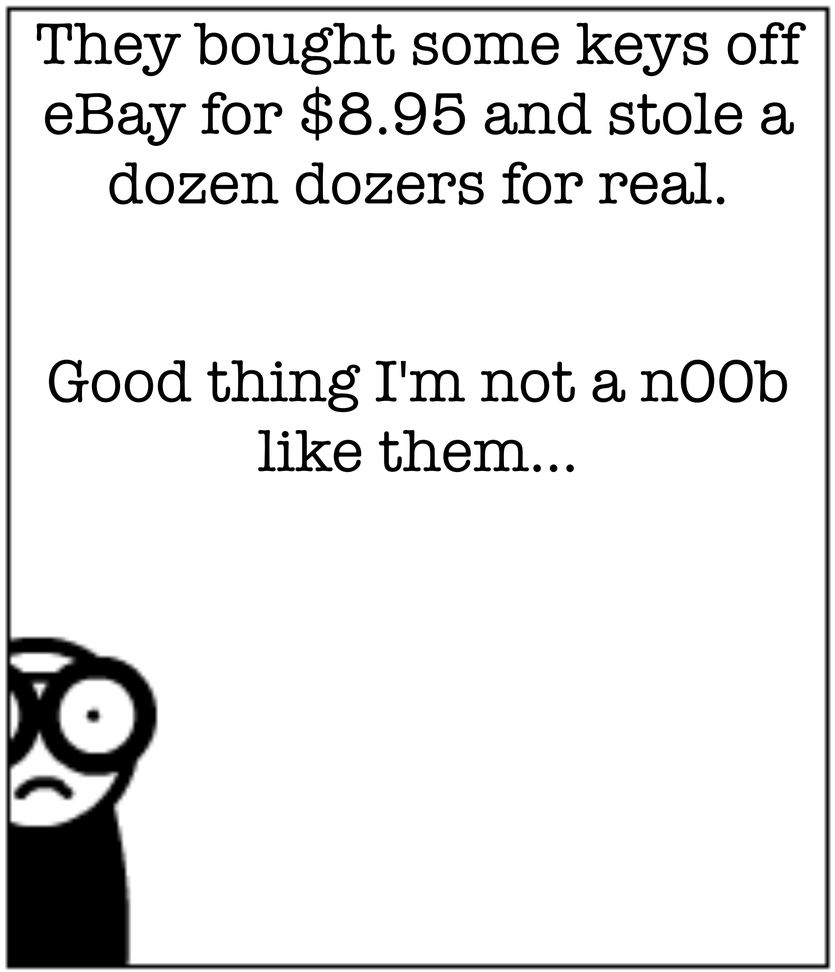
I spent 6 months reverse engineering the CAT TBNT firmware so I could send a malicious bluetooth packet and stunt-hack "steal" one bulldozer.

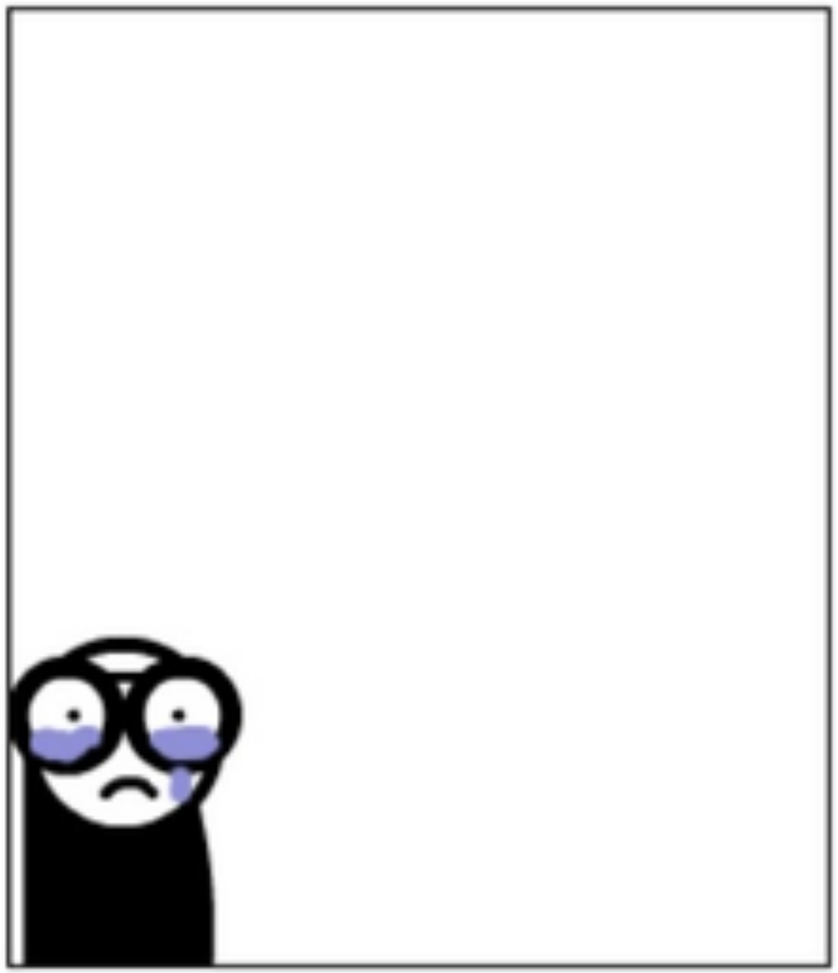
They bought some keys off eBay for $8.95 and stole a dozen dozers for real.

Good thing I'm not a n00b like them...

Template from http://infosuck.org/







Template from http://infosuck.org/

Me: It's probably possible to steal expensive construction equipment with a Bluetooth exploit!
Them: The security baseline for construction equipment is very low, and it's actually super easy to steal them with cheap universal physical keys...
Me:

So...This is Actually A Security Win?!

- If my understanding is correct, and the prior state of physical security for these devices was that it only required a universal physical key to steal one of them[1]...
- Then clearly adding a BT proximity requirement is a ***net security improvement!***
- An important reminder to consider the *total threat model*

[1]https://www.quora.com/Is-it-true-that-you-can-operate-all-Caterpillar-machinery-with-one-key

End - Anecdotes - Devices

Final Takeaways 1

- *Bluetooth sniffing goals are different from WiFi goals*, and consequently the sniffing tech is under-developed to help with those goals
- When there's a BT FW bug, **no one knows what all it affects**

Final Takeaways 2

- There are lots of devices that do not have human-readable names, so it's not clear what they are
  - *Somebody (/me!)* ought to start learning to *toothprint* BT devices!
- There are lots of devices that are advertising names, but it's not clear what they are
  - I'm looking at you "***UGZZF_X[AB10]{4}***"
  - Somebody ought to start a database! Or at least a wiki?!

Call To Action!

Call To Action!

- WiGLE's Android app is open source! If you know Android dev, it'd be great if you could help get more Bluetooth info collected within WiGLE
- I'd like to crowdsource more information, but my web-fu is weak
  - I could use help creating a website that allows people to contribute as well as query this kind of information
- Go collect some information and then share what you find out
  - My data will be available to other researchers on a "share and share alike" basis - you need to collect some useful information that you share with me, and then I'll share my data back

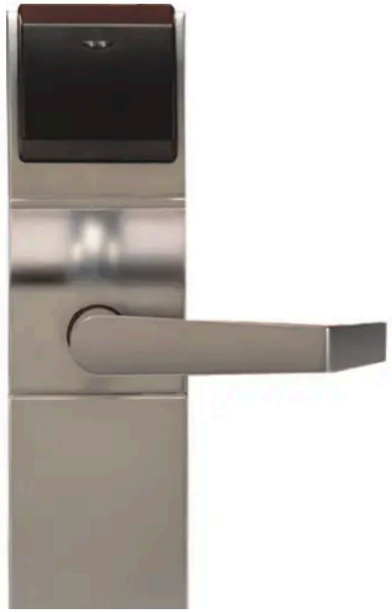
What I Want To Know:

What Bluetooth Chip Is Inside Any Device

DARK MENTOR

DARK MENTOR

nest

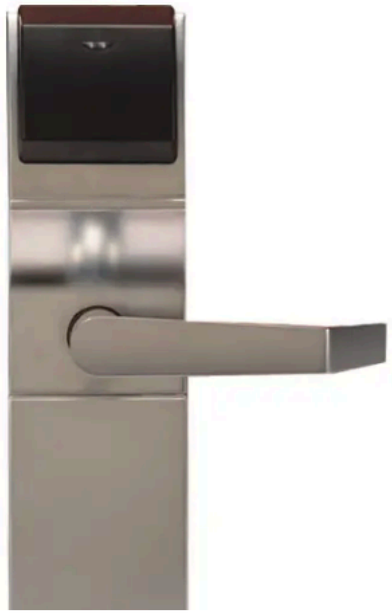


DST2
.FYI

TEXAS INSTRUMENTS

BROADCOM®

SILICON LABS



?

Why I Want To Know It:

So I Know If It's Vulnerable To A Firmware-Level Exploit

DST2.FYI

TEXAS INSTRUMENTS

SILICON LABS

BROADCOM®

ARMIS®

DST2.FYI

Texas Instruments

SILICON LABS®

BROADCOM®

ARMIS®

DARK MENTOR

TEXAS INSTRUMENTS

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

Silicon Vendors (>20)

BROADCOM · Qualcomm · Texas Instruments · bluegiga Silicon Labs · Realtek

Nordic Semiconductor · Apple · Samsung Semiconductors · intel · CSR · ESPRESSIF · ST

Cypress Semiconductor · Infineon · NXP · Telink · Renesas · Microchip

em microelectronic (A company of the Swatch Group) · YiChip · oppo · MediaTek · BES Technic · Marvell

Module-Makers (IDEK how many)

LG Innotek · JingXun · ACKme Networks · BlueRadios (A Wireless World) · Rayson · Laird · muRata (Innovator in Electronics)

BCOM · partron · WNC

Product-Makers

3289 *registered* with Bluetooth SIG as of the time of writing!

Conclusion

What I now know I didn't know

- Basic Bluetooth sniffing can *sometimes* give me some of the information I'm looking for, in a roundabout way:
  - If the BDADDR is for a BT Classic device or BLE Public device, if OUI is a silicon vendor (like Texas Instruments), this provides a good indication of which chip they're likely using
    - The same holds true for two other 16-bit IDs that have assigned companies according to the BT assigned numbers document (Member UUID16 and BT Member Company ID)

Conclusion

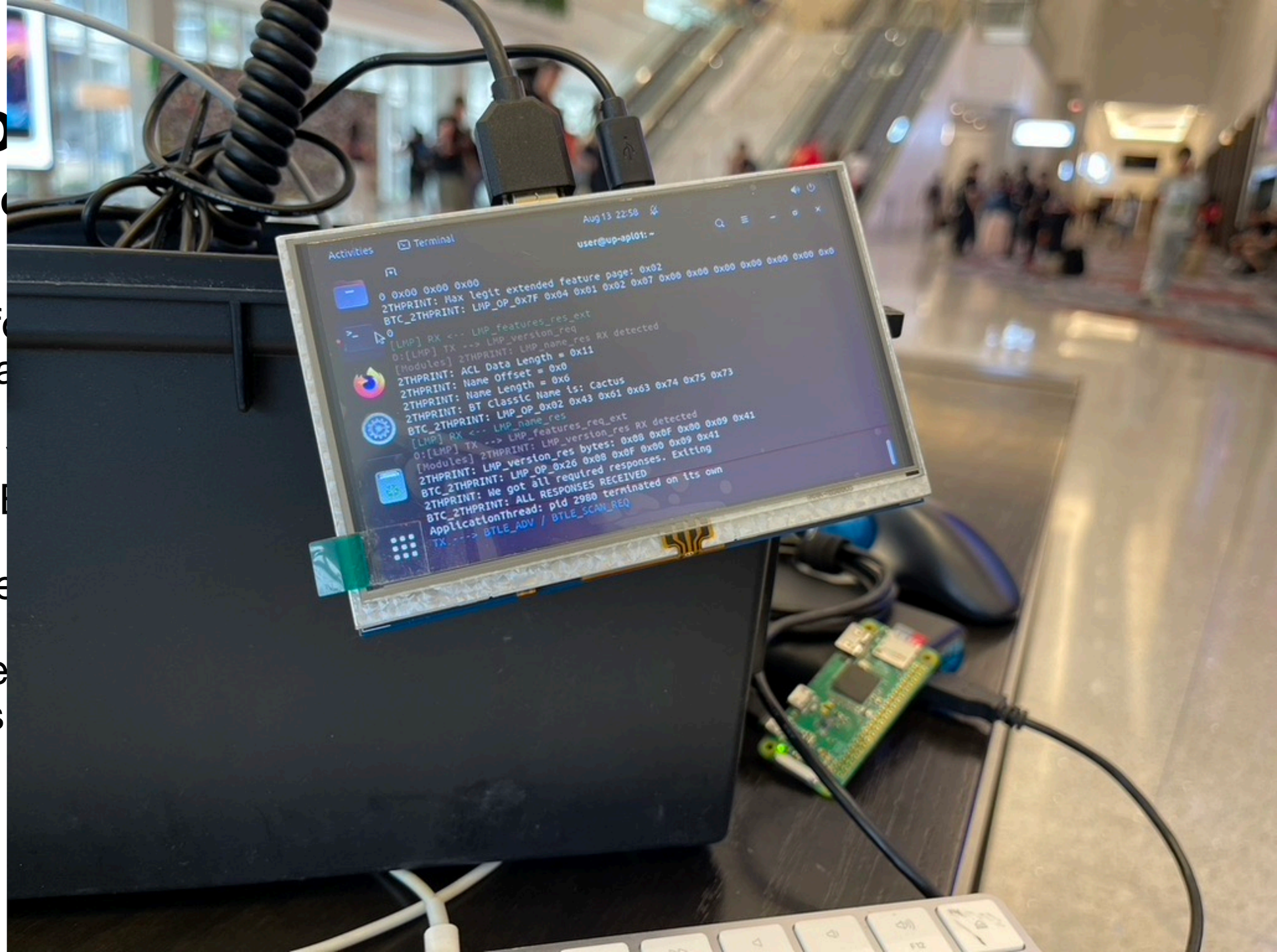
What I now know I didn't know

- Some of the information mentioned in the BT spec that would help point at which BT chip a device uses, is not exposed
  - Even though when I did raw BT sniffing, I could see that it's actually queried by the Linux BlueZ stack in some cases!
  - Therefore I need to collect it myself...
    - One problem is that this will not be collectable via phone apps, and thus will be less scalable

Conclusio

What I now kn

- Some of the inf
  which BT chip a
  - Even though
    by the Linux
  - Therefore I ne
    - One proble
      will be less



Conclusion

What I now know

Stay tuned (@XenoKovah) for the next research!

Conclusion

What I now know

Stay tuned (@XenoKovah) for the next research!

Fin

- BT research is pretty cool IMHO
- 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!