Crowdsourcing Bluetooth identity, to understand Bluetooth vulnerability

Blue2thprinting v2 & BTIDALPOOL

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

About Me

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

About Me

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

- 25% of my time doing consulting and research for **Dark Mentor LLC**

  - It's good to sip accomplishahol via *smaller* problems to solve

What I Want To Know:

What Bluetooth Chip Is Inside Any Device


DARK MENTOR


nest

Texas Instruments

Silicon Labs

Broadcom

?

Why I Want To Know It:

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

TEXAS INSTRUMENTS

SILICON LABS

BROADCOM®

ARMIS®

DST2.FYI

TEXAS INSTRUMENTS

SILICON LABS®

BROADCOM®

ARMIS®

DST2.FYI

TEXAS INSTRUMENTS

SEMC
SECURE MOBILE NETWORKING

SILICON LABS®

BROADCOM®

ARMIS®

DARK MENTOR

TEXAS INSTRUMENTS

SEEMO

SECURE MOBILE NETWORKING

SILICON LABS®

BROADCOM®

ARMIS®

DARK MENTOR

TEXAS INSTRUMENTS

SEEMO

SECURE MOBILE NETWORKING

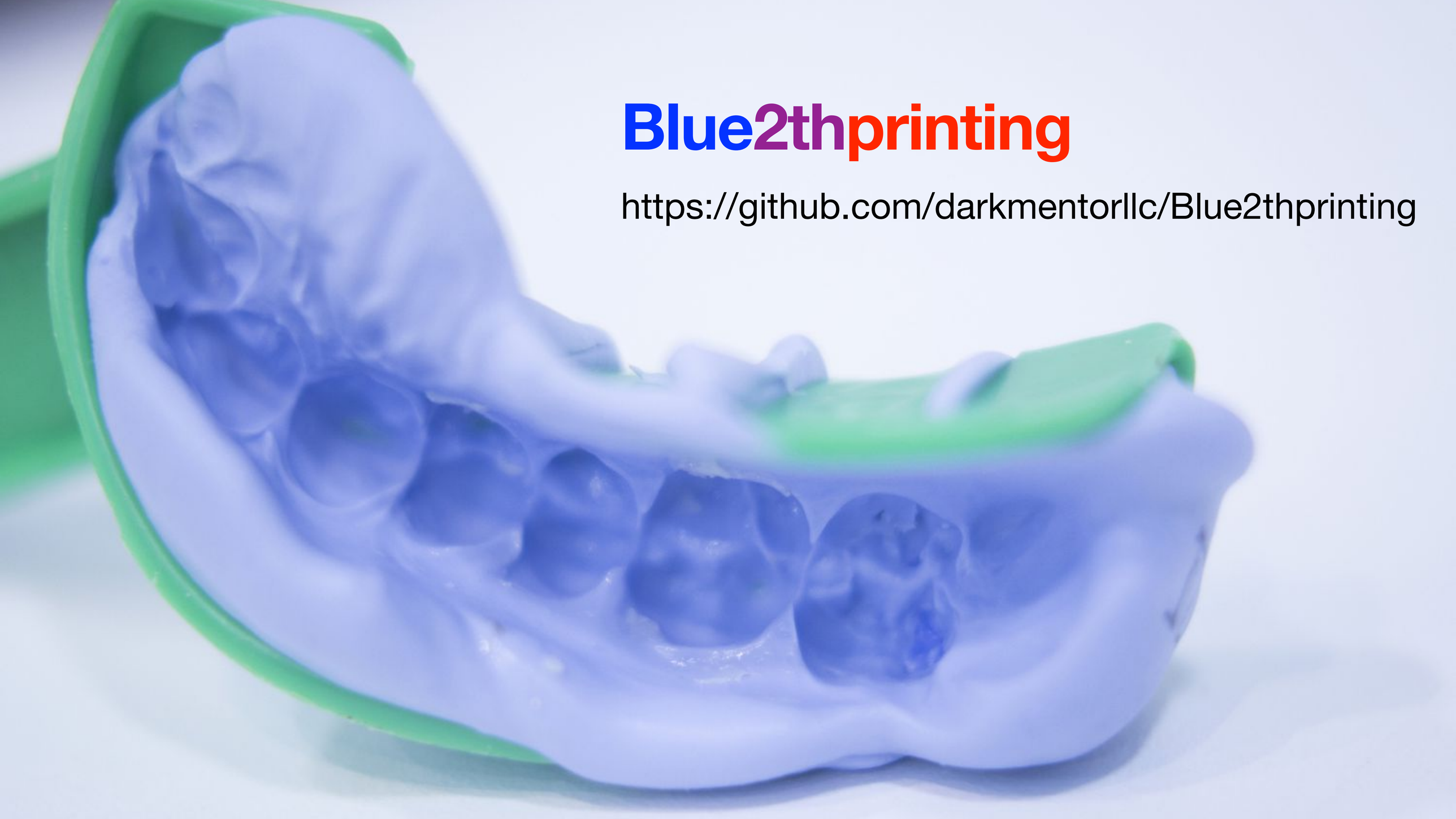
BROADCOM®

DARK MENTOR

SILICON LABS®

My Terminology

- BLE = Bluetooth Low Energy
- BC = Bluetooth Classic
  - i.e. the only "Bluetooth" protocols before BLE
- BDADDR = Bluetooth Device Address (looks like a MAC address, but doesn't always behave like one)

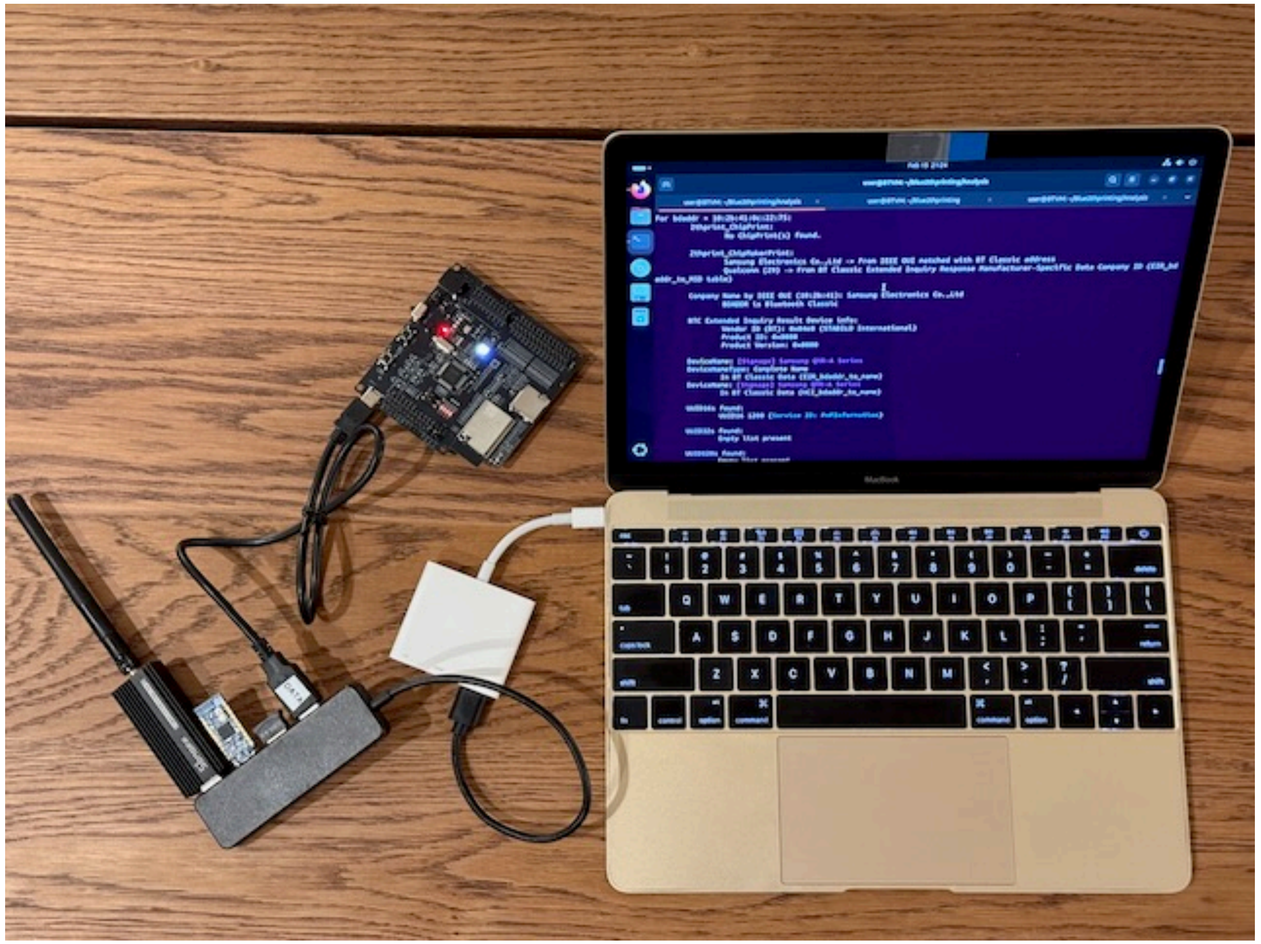


Blue2thprinting

https://github.com/darkmentorllc/Blue2thprinting

Data collection

Any random x86 laptop running an Ubuntu VM



Dongles/dev boards: $75 + USB hub: $10-$17

Data collection

tiny2th (still just linux)

Raspberry pi zero W = $15 + pick your preferred USB battery

Data collection

tiny2th (still just linux)

Showing that it's smaller than a Google Pixel 3 phone

Raspberry pi zero W = $15 + pick your preferred USB battery

Data collection

tiny2th (still just linux)

Showing that it's smaller than a Google Pixel 3 phone

Raspberry pi zero W = $15 + pick your preferred USB battery

Optionally: 2x$20 dongles + 1x$10 dongle + $10 USB hub

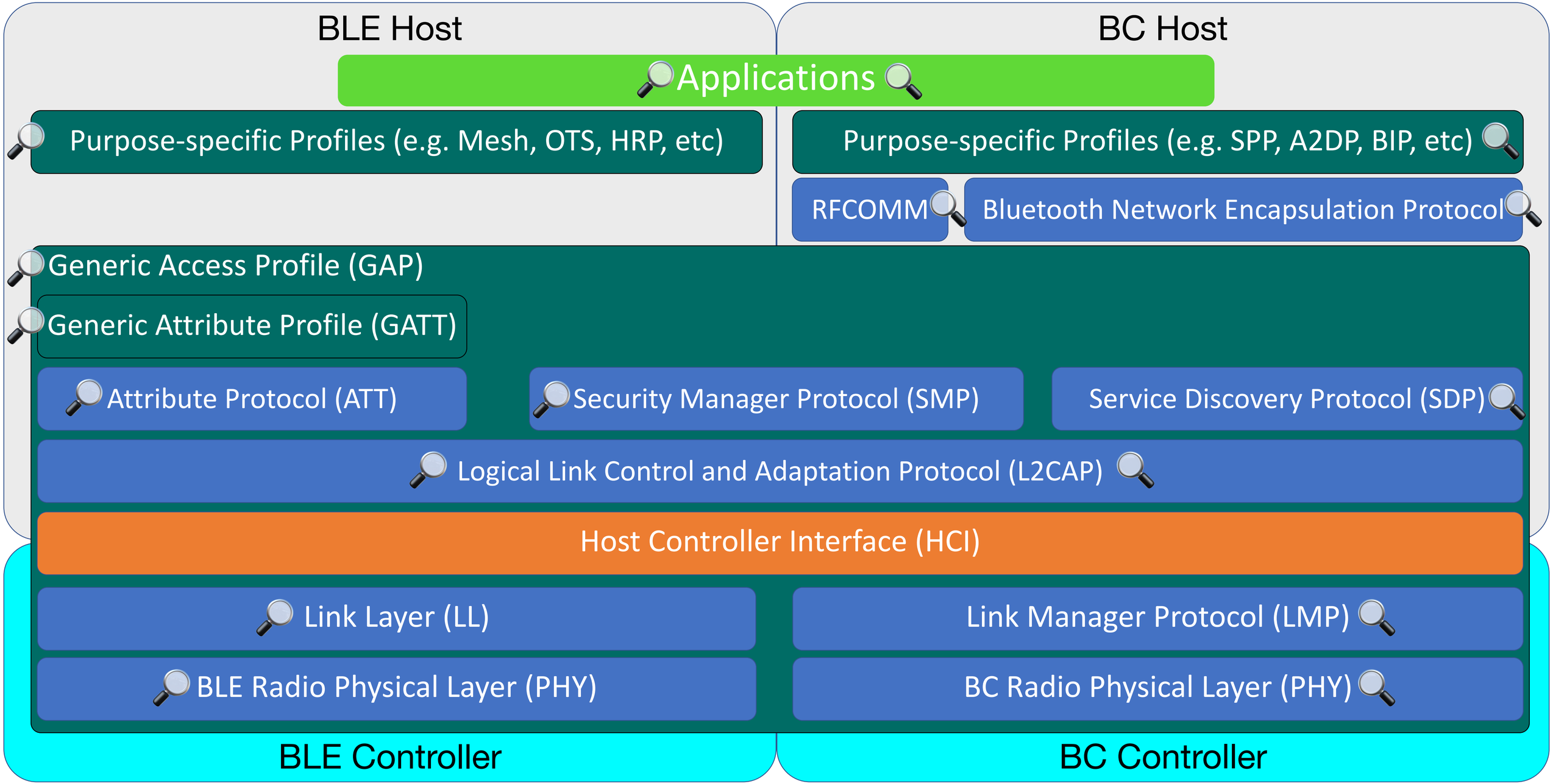
Data collection

Blue2thprinting Pro Max Extreme

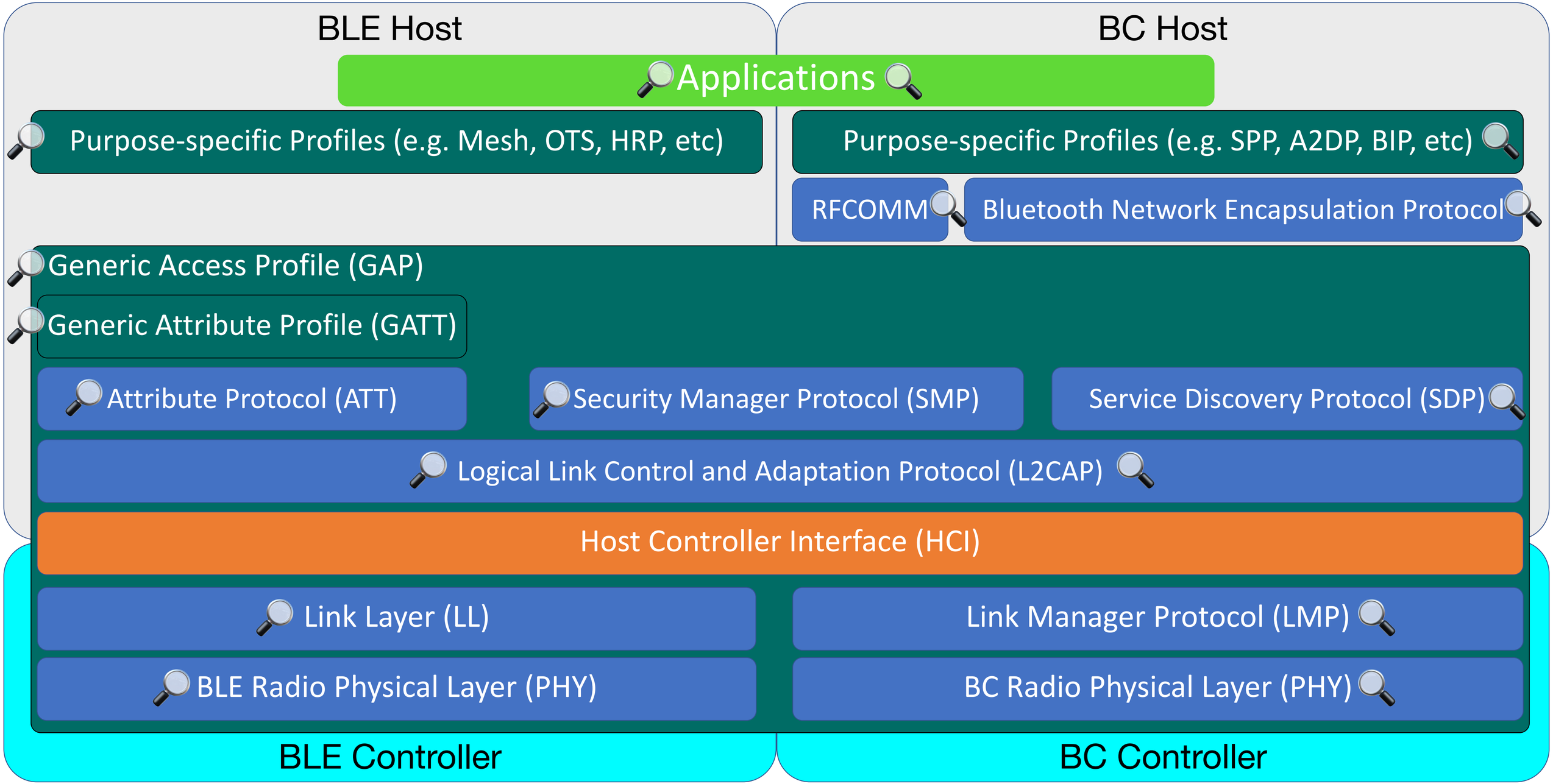
UP^2 x86 mini PC ~= $333, 2x$40 batteries, other stuff ~= $205

Total price ~= $620

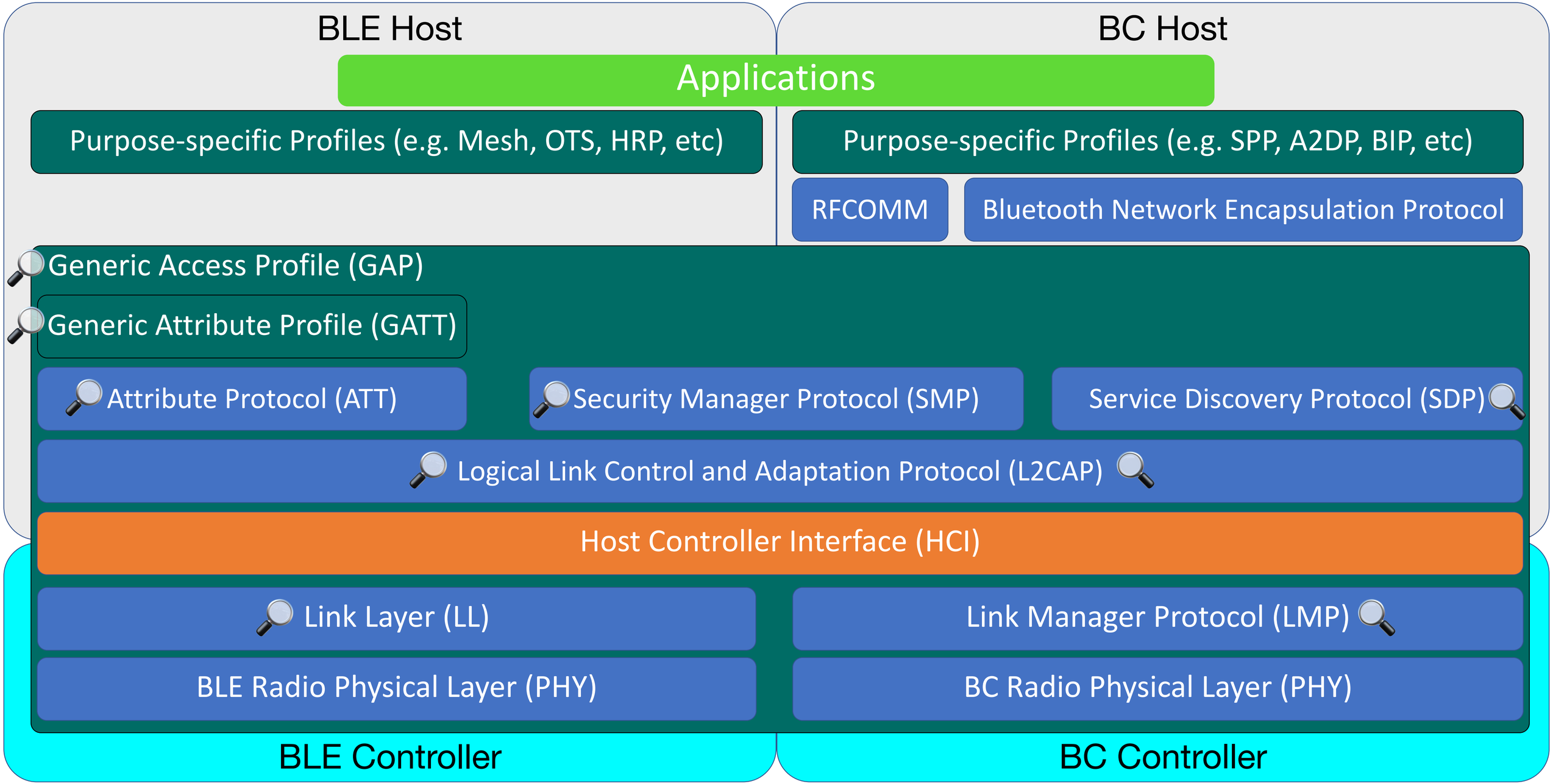
Where all ***should we*** inspect?



Where does Blue2thprinting ***currently*** inspect?



Where does Blue2thprinting ***currently*** inspect?



What's new in Blue2thprinting v2 (1)

- Massively simplified install scripts / preconfigured images
- Privacy/trackability report about individual devices
- Sniffle-based pcap capture that automatically scales to the number of Sonoff dongles you plug in
- *10x speedup on GATT enumeration* (and other improvements) by replacing Linux gatttool with custom Sniffle-based tool
- Adding BLEScope data about UUID-to-Android-app mappings
- Parsing more data types (from advertisements, and protocols like L2CAP and SDP)
  - Adding support to Scapy for missing data types
- New metadata format for capturing 2thprint info

What's new in Blue2thprinting v2 (2)

- **CLUES**
- **BTIDES** import/export
- **BTIDALPOOL** - Crowdsourced data sharing!

CLUES

Custom Lightweight UUID Exchange System

- JSON schema defining how to capture information about Universally Unique IDs (UUIDs) which are used extensively in Bluetooth
  - Standalone git repo can be incorporated as sub-module into projects and trivially reused across tools

CLUES

Custom Lightweight UUID Exchange System

- JSON schema defining how to capture information about Universally Unique IDs (UUIDs) which are used extensively in Bluetooth
    - Standalone git repo can be incorporated as sub-module into projects and trivially reused across tools
- Some UUIDs are reserved by the BT SIG, but everything else can be used by vendors to make up their own UUID for their own services
    - This means knowledge about a UUID can suggest a device's Model, Manufacturer, or even which vendor's BT silicon they use

CLUES

Custom Lightweight UUID Exchange System

- JSON schema defining how to capture information about Universally Unique IDs (UUIDs) which are used extensively in Bluetooth
    - Standalone git repo can be incorporated as sub-module into projects and trivially reused across tools
- Some UUIDs are reserved by the BT SIG, but everything else can be used by vendors to make up their own UUID for their own services
    - This means knowledge about a UUID can suggest a device's Model, Manufacturer, or even which vendor's BT silicon they use
- 382 High S/N UUIDs and counting (thousands to go tho ¯_(ツ)_/¯)

```
{
    "UUID": "00001530-1212-efde-1523-785feabcd123",
    "company": "Nordic",
    "UUID_purpose": "Device Firmware Update (DFU)",
    "UUID_name": "('Legacy'/insecure) Device Firmware Update (DFU)",
    "UUID_usage_array": [
        "GATT Service"
    ],
    "evidence_array": [
        {
            "URL": "https://web.archive.org/web/20250104224034/https://nordicsemiconductor.github.io/IOS-nRF-Connect/assets/files/UserManual.pdf",
            "submitter": "Xeno Kovah"
        }
    ]
},
{
    "UUID": "00001531-1212-efde-1523-785feabcd123",
    "company": "Nordic",
    "UUID_purpose": "Device Firmware Update (DFU) Control Point",
    "UUID_name": "DFU Control Point",
    "UUID_usage_array": [
        "GATT Characteristic"
    ],
    "evidence_array": [
        {
            "URL": "https://web.archive.org/web/20250105123559/https://github.com/adafruit/Bluefruit_LE_Connect_Android/blob/master/app/src/main/java/com/adafruit/bluefruit
            "submitter": "Xeno Kovah"
        }
    ],
    "parent_UUID": "00001530-1212-efde-1523-785feabcd123"
},
{
    "UUID": "00001532-1212-efde-1523-785feabcd123",
    "company": "Nordic",
    "UUID_purpose": "Device Firmware Update (DFU) input packets",
    "UUID_name": "DFU Packet",
    "UUID_usage_array": [
        "GATT Characteristic"
    ],
```

```
For bdaddr = d6:98:64:d4:a1:be:
  2thprint_ChipPrint:
     No ChipPrint(s) found.

  2thprint_ChipMakerPrint:
     Nordic Semiconductor -> From GATTprint match on 00001530-1212-efde-1523-785feabcd123 = "Service: Nordic: 'Legacy'(insecure) Device Firmware Update (DFU)"
(GATT_services table)

  Company Name by IEEE OUI: Not Applicable because this is a Random Static address

  DeviceName: SMART-U
  DeviceNameType: Shortened Name
     This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

  UUID128s found:
     UUID128 419c0001-1e89-11e6-b6ba-3e1d05defe78 (Unknown UUID128)
        Found in BT LE data (LE_bdaddr_to_UUID128s_list), bdaddr_random = 1 (Random Static)
        This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
     BLEScope Analysis: Vendor-specific UUIDs were found. Analyzing if there are any known associations with Android app packages based on BLEScope data.
        Service 419c00011e8911e6b6ba3e1d05defe78:
           This vendor-specific UUID128 is associated with the following Android packages in the BLEScope data:
           ch.details.laurastar


  Flags found:
  In BLE Data (LE_bdaddr_to_flags)
     BLE Limited Discoverable Mode: 0
     BLE General Discoverable Mode: 1
     BR/EDR Not Supported: 1
     Simultaneous BLE and BR/EDR Supported by Controller: 0
     Simultaneous BLE and BR/EDR Supported by Host: 0

  GATT Information:
     Service: GAP 1800:
     Begin Handle: 001, End Handle: 007
        2800 (Declaration: Primary Service), Attribute Handle: 001
        2803 (Declaration: Characteristic), Attribute Handle: 002
           2a00 (Characteristic Value: Device Name), Attribute Handle: 003
        2803 (Declaration: Characteristic), Attribute Handle: 004
           2a01 (Characteristic Value: Appearance), Attribute Handle: 005
        2803 (Declaration: Characteristic), Attribute Handle: 006
           2a04 (Characteristic Value: Peripheral Preferred Connection Parameters), Attribute Handle: 007
     Service: GATT 1801:
     Begin Handle: 008, End Handle: 011
        2800 (Declaration: Primary Service), Attribute Handle: 008
        2803 (Declaration: Characteristic), Attribute Handle: 009
           2a05 (Characteristic Value: Service Changed), Attribute Handle: 010
           2902 (Descriptor: Client Characteristic Configuration), Attribute Handle: 011
     Unknown UUID128 419c0001-1e89-11e6-b6ba-3e1d05defe78:
     Begin Handle: 012, End Handle: 023
        2800 (Declaration: Primary Service), Attribute Handle: 012
```

```
For bdaddr = d6:98:64:d4:a1:be:
  2thprint_ChipPrint:
    No ChipPrint(s) found.

  2thprint_ChipMakerPrint
    Nordic Semiconductor -> From GATTprint match on 00001530-1212-efde-1523-785feabcd123 = "Service: Nordic: 'Legacy'(insecure) Device Firmware Update (DFU)"
(GATT_services table)

  Company Name by IEEE OUI: Not Applicable because this is a Random Static address

  DeviceName: SMART-U
  DeviceNameType: Shortened Name
    This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

  UUID128s found:
    UUID128 419c0001-1e89-11e6-b6ba-3e1d05defe78 (Unknown UUID128)
      Found in BT LE data (LE_bdaddr_to_UUID128s_list), bdaddr_random = 1 (Random Static)
      This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
    BLEScope Analysis: Vendor-specific UUIDs were found. Analyzing if there are any known associations with Android app packages based on BLEScope data.
      Service 419c00011e8911e6b6ba3e1d05defe78:
        This vendor-specific UUID128 is associated with the following Android packages in the BLEScope data:
        ch.details.laurastar


  Flags found:
  In BLE Data (LE_bdaddr_to_flags)
    BLE Limited Discoverable Mode: 0
    BLE General Discoverable Mode: 1
    BR/EDR Not Supported: 1
    Simultaneous BLE and BR/EDR Supported by Controller: 0
    Simultaneous BLE and BR/EDR Supported by Host: 0

  GATT Information:
    Service: GAP 1800:
    Begin Handle: 001, End Handle: 007
      2800 (Declaration: Primary Service), Attribute Handle: 001
      2803 (Declaration: Characteristic), Attribute Handle: 002
        2a00 (Characteristic Value: Device Name), Attribute Handle: 003
      2803 (Declaration: Characteristic), Attribute Handle: 004
        2a01 (Characteristic Value: Appearance), Attribute Handle: 005
      2803 (Declaration: Characteristic), Attribute Handle: 006
        2a04 (Characteristic Value: Peripheral Preferred Connection Parameters), Attribute Handle: 007
    Service: GATT 1801:
    Begin Handle: 008, End Handle: 011
      2800 (Declaration: Primary Service), Attribute Handle: 008
      2803 (Declaration: Characteristic), Attribute Handle: 009
        2a05 (Characteristic Value: Service Changed), Attribute Handle: 010
        2902 (Descriptor: Client Characteristic Configuration), Attribute Handle: 011
    Unknown UUID128 419c0001-1e89-11e6-b6ba-3e1d05defe78:
    Begin Handle: 012, End Handle: 023
      2800 (Declaration: Primary Service), Attribute Handle: 012
```

```
For bdaddr = d6:98:64:d4:a1:be:
  2thprint_ChipPrint:
    No ChipPrint(s) found.

  2thprint_ChipMakerPrint
    Nordic Semiconductor -> From GATTprint match on 00001530-1212-efde-1523-785feabcd123 = "Service: Nordic: 'Legacy'(insecure) Device Firmware Update (DFU)"
(GATT_services table)

  Company Name by IEEE OUI: Not Applicable because this is a Random Static address

  DeviceName: SMART-U
  DeviceNameType: Shortened Name
    This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

  UUID128s found:
    UUID128 419c0001-1e89-11e6-b6ba-3e1d05defe78 (Unknown UUID128)
      Found in BT LE data (LE_bdaddr_to_UUID128s_list), bdaddr_random = 1 (Random Static)
      This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
    BLEScope Analysis: Vendor-specific UUIDs were found. Analyzing if there are any known associations with Android app packages based on BLEScope data.
      Service 419c00011e8911e6b6ba3e1d05defe78:
        This vendor-specific UUID128 is associated with the following Android packages in the BLEScope data:
        ch.details.laurastar


  Flags found:
  In BLE Data (LE_bdaddr_to_flags)
    BLE Limited Discoverable Mode: 0
    BLE General Discoverable Mode: 1
    BR/EDR Not Supported: 1
    Simultaneous BLE and BR/EDR Supported by Controller: 0
    Simultaneous BLE and BR/EDR Supported by Host: 0

  GATT Information:
    Service: GAP 1800:
    Begin Handle: 001, End Handle: 007
      2800 (Declaration: Primary Service), Attribute Handle: 001
      2803 (Declaration: Characteristic), Attribute Handle: 002
        2a00 (Characteristic Value: Device Name), Attribute Handle: 003
      2803 (Declaration: Characteristic), Attribute Handle: 004
        2a01 (Characteristic Value: Appearance), Attribute Handle: 005
      2803 (Declaration: Characteristic), Attribute Handle: 006
        2a04 (Characteristic Value: Peripheral Preferred Connection Parameters), Attribute Handle: 007
    Service: GATT 1801:
    Begin Handle: 008, End Handle: 011
      2800 (Declaration: Primary Service), Attribute Handle: 008
      2803 (Declaration: Characteristic), Attribute Handle: 009
        2a05 (Characteristic Value: Service Changed), Attribute Handle: 010
        2902 (Descriptor: Client Characteristic Configuration), Attribute Handle: 011
    Unknown UUID128 419c0001-1e89-11e6-b6ba-3e1d05defe78:
    Begin Handle: 012, End Handle: 023
      2800 (Declaration: Primary Service), Attribute Handle: 012
```

```
For bdaddr = d6:98:64:d4:a1:be:
  2thprint_ChipPrint:
    No ChipPrint(s) found.

  2thprint_ChipMakerPrint
    Nordic Semiconductor -> From GATTprint match on 00001530-1212-efde-1523-785feabcd123 = "Service: Nordic: 'Legacy'(insecure) Device Firmware Update (DFU)"
(GATT_services table)

  Company Name by IEEE OUI: Not Applicable because this is a Random Static address

  DeviceName: SMART-U
  DeviceNameType: Shortened Name
    This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

  UUID128s found:
    UUID128 419c0001-1e89-11e6-b6ba-3e1d05defe78 (Unknown UUID128)
      Found in BT LE data (LE_bdaddr_to_UUID128s_list), bdaddr_random = 1 (Random Static)
      This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
    BLEScope Analysis: Vendor-specific UUIDs were found. Analyzing if there are any known associations with Android app packages based on BLEScope data.
      Service 419c00011e8911e6b6ba3e1d05defe78:
        This vendor-specific UUID128 is associated with the following Android packages in the BLEScope data:
        ch.details.laurastar


  Flags found:
  In BLE Data (LE_bdaddr_to_flags)
    BLE Limited Discoverable Mode: 0
    BLE General Discoverable Mode: 1
    BR/EDR Not Supported: 1
    Simultaneous BLE and BR/EDR Supported by Controller: 0
    Simultaneous BLE and BR/EDR Supported by Host: 0

  GATT Information:
    Service: GAP 1800:
    Begin Handle: 001, End Handle: 007
      2800 (Declaration: Primary Service), Attribute Handle: 001
      2803 (Declaration: Characteristic), Attribute Handle: 002
        2a00 (Characteristic Value: Device Name), Attribute Handle: 003
      2803 (Declaration: Characteristic), Attribute Handle: 004
        2a01 (Characteristic Value: Appearance), Attribute Handle: 005
      2803 (Declaration: Characteristic), Attribute Handle: 006
        2a04 (Characteristic Value: Peripheral Preferred Connection Parameters), Attribute Handle: 007
    Service: GATT 1801:
    Begin Handle: 008, End Handle: 011
      2800 (Declaration: Primary Service), Attribute Handle: 008
      2803 (Declaration: Characteristic), Attribute Handle: 009
        2a05 (Characteristic Value: Service Changed), Attribute Handle: 010
        2902 (Descriptor: Client Characteristic Configuration), Attribute Handle: 011
    Unknown UUID128 419c0001-1e89-11e6-b6ba-3e1d05defe78:
    Begin Handle: 012, End Handle: 023
      2800 (Declaration: Primary Service), Attribute Handle: 012
```

```
For bdaddr = d6:98:64:d4:a1:be:
  2thprint_ChipPrint:
     No ChipPrint(s) found.

  2thprint_ChipMakerPrint:
     Nordic Semiconductor -> From GATTprint match on 00001530-1212-efde-1523-785feabcd123 = "Service: Nordic: 'Legacy'(insecure) Device Firmware Update (DFU)"
(GATT_services table)

  Company Name by IEEE OUI: Not Applicable because this is a Random Static address

  DeviceName: SMART-U
  DeviceNameType: Shortened Name
     This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

  UUID128s found:
     UUID128 419c0001-1e89-11e6-b6ba-3e1d05defe78 (Unknown UUID128)
        Found in BT LE data (LE_bdaddr_to_UUID128s_list), bdaddr_random = 1 (Random Static)
        This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)
     BLEScope Analysis: Vendor-specific UUIDs were found. Analyzing if there are any known associations with Android app packages based on BLEScope data.
        Service 419c00011e8911e6b6ba3e1d05defe78:
           This vendor-specific UUID128 is associated with the following Android packages in the BLEScope data:
           ch.details.laurastar


  Flags found:
  In BLE Data (LE_bdaddr_to_flags)
     BLE Limited Discoverable Mode: 0
     BLE General Discoverable Mode: 1
     BR/EDR Not Supported: 1
     Simultaneous BLE and BR/EDR Supported by Controller: 0
     Simultaneous BLE and BR/EDR Supported by Host: 0

  GATT Information:
     Service: GAP 1800:
     Begin Handle: 001, End Handle: 007
        2800 (Declaration: Primary Service), Attribute Handle: 001
        2803 (Declaration: Characteristic), Attribute Handle: 002
           2a00 (Characteristic Value: Device Name), Attribute Handle: 003
        2803 (Declaration: Characteristic), Attribute Handle: 004
           2a01 (Characteristic Value: Appearance), Attribute Handle: 005
        2803 (Declaration: Characteristic), Attribute Handle: 006
           2a04 (Characteristic Value: Peripheral Preferred Connection Parameters), Attribute Handle: 007
     Service: GATT 1801:
     Begin Handle: 008, End Handle: 011
        2800 (Declaration: Primary Service), Attribute Handle: 008
        2803 (Declaration: Characteristic), Attribute Handle: 009
           2a05 (Characteristic Value: Service Changed), Attribute Handle: 010
           2902 (Descriptor: Client Characteristic Configuration), Attribute Handle: 011
     Unknown UUID128 419c0001-1e89-11e6-b6ba-3e1d05defe78:
     Begin Handle: 012, End Handle: 023
        2800 (Declaration: Primary Service), Attribute Handle: 012
```

```
Service: GAP 1800:
Begin Handle: 001, End Handle: 007
  2800 (Declaration: Primary Service), Attribute Handle: 001
  2803 (Declaration: Characteristic), Attribute Handle: 002
    2a00 (Characteristic Value: Device Name), Attribute Handle: 003
  2803 (Declaration: Characteristic), Attribute Handle: 004
    2a01 (Characteristic Value: Appearance), Attribute Handle: 005
  2803 (Declaration: Characteristic), Attribute Handle: 006
    2a04 (Characteristic Value: Peripheral Preferred Connection Parameters), Attribute Handle: 007
Service: GATT 1801:
Begin Handle: 008, End Handle: 011
  2800 (Declaration: Primary Service), Attribute Handle: 008
  2803 (Declaration: Characteristic), Attribute Handle: 009
    2a05 (Characteristic Value: Service Changed), Attribute Handle: 010
    2902 (Descriptor: Client Characteristic Configuration), Attribute Handle: 011
Unknown UUID128 419c0001-1e89-11e6-b6ba-3e1d05defe78:
Begin Handle: 012, End Handle: 023
  2800 (Declaration: Primary Service), Attribute Handle: 012
  2803 (Declaration: Characteristic), Attribute Handle: 013
    419c0004-1e89-11e6-b6ba-3e1d05defe78 (Unknown UUID128), Attribute Handle: 014
    2902 (Descriptor: Client Characteristic Configuration), Attribute Handle: 015
  2803 (Declaration: Characteristic), Attribute Handle: 016
    419c0005-1e89-11e6-b6ba-3e1d05defe78 (Unknown UUID128), Attribute Handle: 017
  2803 (Declaration: Characteristic), Attribute Handle: 018
    419c0006-1e89-11e6-b6ba-3e1d05defe78 (Unknown UUID128), Attribute Handle: 019
  2803 (Declaration: Characteristic), Attribute Handle: 020
    419c0007-1e89-11e6-b6ba-3e1d05defe78 (Unknown UUID128), Attribute Handle: 021
  2803 (Declaration: Characteristic), Attribute Handle: 022
    419c0008-1e89-11e6-b6ba-3e1d05defe78 (Unknown UUID128), Attribute Handle: 023
Unknown UUID128 419c0002-1e89-11e6-b6ba-3e1d05defe78:
Begin Handle: 024, End Handle: 033
  2800 (Declaration: Primary Service), Attribute Handle: 024
  2803 (Declaration: Characteristic), Attribute Handle: 025
    419c0009-1e89-11e6-b6ba-3e1d05defe78 (Unknown UUID128), Attribute Handle: 026
    2902 (Descriptor: Client Characteristic Configuration), Attribute Handle: 027
  2803 (Declaration: Characteristic), Attribute Handle: 028
    419c000a-1e89-11e6-b6ba-3e1d05defe78 (Unknown UUID128), Attribute Handle: 029
  2803 (Declaration: Characteristic), Attribute Handle: 030
    419c000c-1e89-11e6-b6ba-3e1d05defe78 (Unknown UUID128), Attribute Handle: 031
  2803 (Declaration: Characteristic), Attribute Handle: 032
    419c000d-1e89-11e6-b6ba-3e1d05defe78 (Unknown UUID128), Attribute Handle: 033
Unknown UUID128 419c0003-1e89-11e6-b6ba-3e1d05defe78:
Begin Handle: 034, End Handle: 042
  2800 (Declaration: Primary Service), Attribute Handle: 034
  2803 (Declaration: Characteristic), Attribute Handle: 035
Service: Device Information 180a:
Begin Handle: 043, End Handle: 051
Custom UUID128: company: Nordic, name: ('Legacy'/insecure) Device Firmware Update (DFU) 00001530-1212-efde-1523-785feabcd123:
Begin Handle: 052, End Handle: 65535
GATT Service Unknown! Handle does not match any Service ranges that we received from the device!

Security Manager Protocol (SMP) data found:
```

```
      2803 (Declaration: Characteristic), Attribute Handle: 030
        419c000c-1e89-11e6-b6ba-3e1d05defe78 (Unknown UUID128), Attribute Handle: 031
      2803 (Declaration: Characteristic), Attribute Handle: 032
        419c000d-1e89-11e6-b6ba-3e1d05defe78 (Unknown UUID128), Attribute Handle: 033
    Unknown UUID128 419c0003-1e89-11e6-b6ba-3e1d05defe78:
    Begin Handle: 034, End Handle: 042
      2800 (Declaration: Primary Service), Attribute Handle: 034
      2803 (Declaration: Characteristic), Attribute Handle: 035
    Service: Device Information 180a:
    Begin Handle: 043, End Handle: 051
    Custom UUID128: company: Nordic, name: ('Legacy'/insecure) Device Firmware Update (DFU) 00001530-1212-efde-1523-785feabcd123:
    Begin Handle: 052, End Handle: 65535
    GATT Service Unknown! Handle does not match any Service ranges that we received from the device!

  Security Manager Protocol (SMP) data found:
    Pairing Response:
      Input/Output Capabilities: No Input, No Output
        WARNING: If accepted, this pairing will lead to "Just Works" pairing, which is guaranteed-insecure against MitM attacks!
      Authentication Requested Parameters:
        Bonding (Long Term Key storage): not requested
        Machine-in-the-Middle (MITM) protection: not requested!
          This will lead to pairing that is guaranteed-insecure against MitM attacks!
        Secure Connection pairing: not requested!
          If accepted, this will lead to Legacy Pairing which is guaranteed-insecure against eavesdropping & MITM attacks!
        Keypress notifications: not requested.
        CT2 (Cross-Transport key derivation support for the h7 function): not supported.
      Maxiumum encryption key size: 16
        16 is currently the maximum supported key size.
      Out-of-Band (OOB) authentication data: not present.
      Initiator Key Distribution:
        Initiator to send Long Term Key (LTK): not requested.
        Initiator to send Identity Resolving Key (IDK): not requested.
        Initiator to send Connection Signature Resolving Key (CSRK): not requested.
        Initiator request to derive BR/EDR Link Key from LE LTK (Cross-Transport Key Derivation): not requested.
      Responder Key Distribution:
        Responder to send Long Term Key (LTK): not requested.
        Responder to send Identity Resolving Key (IDK): not requested.
        Responder to send Connection Signature Resolving Key (CSRK): not requested.
        Responder request to derive BR/EDR Link Key from LE LTK (Cross-Transport Key Derivation): not requested.

  BLE 2thprint Info:
    BLE LL Ctrl Opcode: 9 (LL_FEATURE_RSP)
      BLE LL Features: 0x0000000000000001
        * LE Encryption

  Unique ID / Potential Trackability Report:
    Unique ID: BDADDR is of type *Random Static*, which is not randomized over time, and therefore can be used to track the device.
    *Possible* Unique ID: This device contains a name "SMART-U" found via Bluetooth Low Energy Advertisements. The name itself does not match a known-unique-ID
pattern, but that could just mean it has not been captured in our metadata yet.
          It is left to the user to investigate whether this name represents a unique ID or not. E.g. look for other instances of this name in your own data via the
--nameregex option, or search by name at wigle.net.
```

```
      2803 (Declaration: Characteristic), Attribute Handle: 030
        419c000c-1e89-11e6-b6ba-3e1d05defe78 (Unknown UUID128), Attribute Handle: 031
      2803 (Declaration: Characteristic), Attribute Handle: 032
        419c000d-1e89-11e6-b6ba-3e1d05defe78 (Unknown UUID128), Attribute Handle: 033
    Unknown UUID128 419c0003-1e89-11e6-b6ba-3e1d05defe78:
    Begin Handle: 034, End Handle: 042
      2800 (Declaration: Primary Service), Attribute Handle: 034
      2803 (Declaration: Characteristic), Attribute Handle: 035
    Service: Device Information 180a:
    Begin Handle: 043, End Handle: 051
    Custom UUID128: company: Nordic, name: ('Legacy'/insecure) Device Firmware Update (DFU) 00001530-1212-efde-1523-785feabcd123:
    Begin Handle: 052, End Handle: 65535
    GATT Service Unknown! Handle does not match any Service ranges that we received from the device!

  Security Manager Protocol (SMP) data found:
    Pairing Response:
      Input/Output Capabilities: No Input, No Output
        WARNING: If accepted, this pairing will lead to "Just Works" pairing, which is guaranteed-insecure against MitM attacks!
      Authentication Requested Parameters:
        Bonding (Long Term Key storage): not requested
        Machine-in-the-Middle (MITM) protection: not requested!
          This will lead to pairing that is guaranteed-insecure against MitM attacks!
        Secure Connection pairing: not requested!
          If accepted, this will lead to Legacy Pairing which is guaranteed-insecure against eavesdropping & MITM attacks!
        Keypress notifications: not requested.
        CT2 (Cross-Transport key derivation support for the h7 function): not supported.
      Maxiumum encryption key size: 16
        16 is currently the maximum supported key size.
      Out-of-Band (OOB) authentication data: not present.
      Initiator Key Distribution:
        Initiator to send Long Term Key (LTK): not requested.
        Initiator to send Identity Resolving Key (IDK): not requested.
        Initiator to send Connection Signature Resolving Key (CSRK): not requested.
        Initiator request to derive BR/EDR Link Key from LE LTK (Cross-Transport Key Derivation): not requested.
      Responder Key Distribution:
        Responder to send Long Term Key (LTK): not requested.
        Responder to send Identity Resolving Key (IDK): not requested.
        Responder to send Connection Signature Resolving Key (CSRK): not requested.
        Responder request to derive BR/EDR Link Key from LE LTK (Cross-Transport Key Derivation): not requested.

  BLE 2thprint Info:
    BLE LL Ctrl Opcode: 9 (LL_FEATURE_RSP)
      BLE LL Features: 0x0000000000000001
        * LE Encryption

  Unique ID / Potential Trackability Report:
    Unique ID: BDADDR is of type *Random Static*, which is not randomized over time, and therefore can be used to track the device.
    *Possible* Unique ID: This device contains a name "SMART-U" found via Bluetooth Low Energy Advertisements. The name itself does not match a known-unique-ID
pattern, but that could just mean it has not been captured in our metadata yet.
          It is left to the user to investigate whether this name represents a unique ID or not. E.g. look for other instances of this name in your own data via the
--nameregex option, or search by name at wigle.net.
```

```
      2803 (Declaration: Characteristic), Attribute Handle: 030
        419c000c-1e89-11e6-b6ba-3e1d05defe78 (Unknown UUID128), Attribute Handle: 031
      2803 (Declaration: Characteristic), Attribute Handle: 032
        419c000d-1e89-11e6-b6ba-3e1d05defe78 (Unknown UUID128), Attribute Handle: 033
    Unknown UUID128 419c0003-1e89-11e6-b6ba-3e1d05defe78:
    Begin Handle: 034, End Handle: 042
      2800 (Declaration: Primary Service), Attribute Handle: 034
      2803 (Declaration: Characteristic), Attribute Handle: 035
    Service: Device Information 180a:
    Begin Handle: 043, End Handle: 051
    Custom UUID128: company: Nordic, name: ('Legacy'/insecure) Device Firmware Update (DFU) 00001530-1212-efde-1523-785feabcd123:
    Begin Handle: 052, End Handle: 65535
    GATT Service Unknown! Handle does not match any Service ranges that we received from the device!

  Security Manager Protocol (SMP) data found:
    Pairing Response:
      Input/Output Capabilities: No Input, No Output
        WARNING: If accepted, this pairing will lead to "Just Works" pairing, which is guaranteed-insecure against MitM attacks!
      Authentication Requested Parameters:
        Bonding (Long Term Key storage): not requested
        Machine-in-the-Middle (MITM) protection: not requested!
          This will lead to pairing that is guaranteed-insecure against MitM attacks!
        Secure Connection pairing: not requested!
          If accepted, this will lead to Legacy Pairing which is guaranteed-insecure against eavesdropping & MITM attacks!
        Keypress notifications: not requested.
        CT2 (Cross-Transport key derivation support for the h7 function): not supported.
      Maxiumum encryption key size: 16
        16 is currently the maximum supported key size.
      Out-of-Band (OOB) authentication data: not present.
      Initiator Key Distribution:
        Initiator to send Long Term Key (LTK): not requested.
        Initiator to send Identity Resolving Key (IDK): not requested.
        Initiator to send Connection Signature Resolving Key (CSRK): not requested.
        Initiator request to derive BR/EDR Link Key from LE LTK (Cross-Transport Key Derivation): not requested.
      Responder Key Distribution:
        Responder to send Long Term Key (LTK): not requested.
        Responder to send Identity Resolving Key (IDK): not requested.
        Responder to send Connection Signature Resolving Key (CSRK): not requested.
        Responder request to derive BR/EDR Link Key from LE LTK (Cross-Transport Key Derivation): not requested.

  BLE 2thprint Info:
    BLE LL Ctrl Opcode: 9 (LL_FEATURE_RSP)
      BLE LL Features: 0x0000000000000001
        * LE Encryption

  Unique ID / Potential Trackability Report:
    Unique ID: BDADDR is of type *Random Static*, which is not randomized over time, and therefore can be used to track the device.
    *Possible* Unique ID: This device contains a name "SMART-U" found via Bluetooth Low Energy Advertisements. The name itself does not match a known-unique-ID
pattern, but that could just mean it has not been captured in our metadata yet.
          It is left to the user to investigate whether this name represents a unique ID or not. E.g. look for other instances of this name in your own data via the
--nameregex option, or search by name at wigle.net.
```

```
For bdaddr = 78:b8:99:2d:1e:f4:
  2thprint_ChipPrint:
    No ChipPrint(s) found.

  2thprint_ChipMakerPrint:
    Silicon Laboratories -> From GATTprint match on 1D14D6EE-FD63-4FA1-BFA4-8F47B42119F0 = "Service: Silicon Labs: Over The Air firmware update protocol"
(GATT_services table)

  Company Name by IEEE OUI: Not Applicable because this is a Random Resolvable address

  UUID16s found:
    UUID16 fe03 (Company-specific Service UUID: Amazon:Alexa Mobile Accessories (AMA))
    This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

  Transmit Power: 4dB
    This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

  Flags found:
  In BLE Data (LE_bdaddr_to_flags)
    BLE Limited Discoverable Mode: 0
    BLE General Discoverable Mode: 1
    BR/EDR Not Supported: 1
    Simultaneous BLE and BR/EDR Supported by Controller: 0
    Simultaneous BLE and BR/EDR Supported by Host: 0

  Manufacturer-specific Data:
    Device Company ID: 0x0171 (Amazon.com Services LLC) - 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): 0x7101 (No Match)
    Raw Data: 041380b601f918e0
      In BT LE Data (LE_bdaddr_to_MSD), bdaddr_random = 1 (Random Resolvable)
      This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

  GATT Information:
    Service: GATT 1801:
    Begin Handle: 001, End Handle: 008
      2800 (Declaration: Primary Service), Attribute Handle: 001
      2803 (Declaration: Characteristic), Attribute Handle: 002
        2a05 (Characteristic Value: Service Changed), Attribute Handle: 003
        2902 (Descriptor: Client Characteristic Configuration), Attribute Handle: 004
      2803 (Declaration: Characteristic), Attribute Handle: 005
        2b2a (Characteristic Value: Database Hash), Attribute Handle: 006
        GATT Characteristic Value read as b'\xd4\xd6\xfe\xc4T\x11l?Q\xef\xd1;\xce\xde\xf0\xb2'
      2803 (Declaration: Characteristic), Attribute Handle: 007
        2b29 (Characteristic Value: Client Supported Features), Attribute Handle: 008
        GATT Characteristic Value read as b'\x00'
    Service: GAP 1800:
    Begin Handle: 009, End Handle: 013
      2800 (Declaration: Primary Service), Attribute Handle: 009
      2803 (Declaration: Characteristic), Attribute Handle: 010
        2a00 (Characteristic Value: Device Name), Attribute Handle: 011
        GATT Characteristic Value read as b'MagicBand+ A139'
```

```
For bdaddr = 78:b8:99:2d:1e:f4:
  2thprint_ChipPrint:
    No ChipPrint(s) found.

  2thprint_ChipMakerPrint
    Silicon Laboratories -> From GATTprint match on 1D14D6EE-FD63-4FA1-BFA4-8F47B42119F0 = "Service: Silicon Labs: Over The Air firmware update protocol"
(GATT_services table)

  Company Name by IEEE OUI: Not Applicable because this is a Random Resolvable address

  UUID16s found:
    UUID16 fe03 (Company-specific Service UUID: Amazon:Alexa Mobile Accessories (AMA))
    This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

  Transmit Power: 4dB
    This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

  Flags found:
  In BLE Data (LE_bdaddr_to_flags)
    BLE Limited Discoverable Mode: 0
    BLE General Discoverable Mode: 1
    BR/EDR Not Supported: 1
    Simultaneous BLE and BR/EDR Supported by Controller: 0
    Simultaneous BLE and BR/EDR Supported by Host: 0

  Manufacturer-specific Data:
    Device Company ID: 0x0171 (Amazon.com Services LLC) - 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): 0x7101 (No Match)
    Raw Data: 041380b601f918e0
      In BT LE Data (LE_bdaddr_to_MSD), bdaddr_random = 1 (Random Resolvable)
      This was found in an event of type 0 which corresponds to Connectable Undirected Advertising (ADV_IND)

  GATT Information:
    Service: GATT 1801:
    Begin Handle: 001, End Handle: 008
      2800 (Declaration: Primary Service), Attribute Handle: 001
      2803 (Declaration: Characteristic), Attribute Handle: 002
        2a05 (Characteristic Value: Service Changed), Attribute Handle: 003
        2902 (Descriptor: Client Characteristic Configuration), Attribute Handle: 004
      2803 (Declaration: Characteristic), Attribute Handle: 005
        2b2a (Characteristic Value: Database Hash), Attribute Handle: 006
        GATT Characteristic Value read as b'\xd4\xd6\xfe\xc4T\x11l?Q\xef\xd1;\xce\xde\xf0\xb2'
      2803 (Declaration: Characteristic), Attribute Handle: 007
        2b29 (Characteristic Value: Client Supported Features), Attribute Handle: 008
        GATT Characteristic Value read as b'\x00'
    Service: GAP 1800:
    Begin Handle: 009, End Handle: 013
      2800 (Declaration: Primary Service), Attribute Handle: 009
      2803 (Declaration: Characteristic), Attribute Handle: 010
        2a00 (Characteristic Value: Device Name), Attribute Handle: 011
        GATT Characteristic Value read as b'MagicBand+ A139'
```

```
  Service: GATT 1801:
  Begin Handle: 001, End Handle: 008
    2800 (Declaration: Primary Service), Attribute Handle: 001
    2803 (Declaration: Characteristic), Attribute Handle: 002
      2a05 (Characteristic Value: Service Changed), Attribute Handle: 003
      2902 (Descriptor: Client Characteristic Configuration), Attribute Handle: 004
    2803 (Declaration: Characteristic), Attribute Handle: 005
      2b2a (Characteristic Value: Database Hash), Attribute Handle: 006
      GATT Characteristic Value read as b'\xd4\xd6\xfe\xc4T\x11l?Q\xef\xd1;\xce\xde\xf0\xb2'
    2803 (Declaration: Characteristic), Attribute Handle: 007
      2b29 (Characteristic Value: Client Supported Features), Attribute Handle: 008
      GATT Characteristic Value read as b'\x00'
  Service: GAP 1800:
  Begin Handle: 009, End Handle: 013
    2800 (Declaration: Primary Service), Attribute Handle: 009
    2803 (Declaration: Characteristic), Attribute Handle: 010
      2a00 (Characteristic Value: Device Name), Attribute Handle: 011
      GATT Characteristic Value read as b'MagicBand+ A139'
    2803 (Declaration: Characteristic), Attribute Handle: 012
      2a01 (Characteristic Value: Appearance), Attribute Handle: 013
      GATT Characteristic Value read as b'\x00\x00'
  Custom UUID128: company: Silicon Labs, name: OTA Firmware Update 1d14d6ee-fd63-4fa1-bfa4-8f47b42119f0:
  Begin Handle: 014, End Handle: 018
    2800 (Declaration: Primary Service), Attribute Handle: 014
    2803 (Declaration: Characteristic), Attribute Handle: 015
      f7bf3564-fb6d-4e53-88a4-5e37e0326063 (Custom UUID128: company: Silicon Labs, name: Control Attribute), Attribute Handle: 016
    2803 (Declaration: Characteristic), Attribute Handle: 017
      984227f3-34fc-4045-a5d0-2c581f81a153 (Custom UUID128: company: Silicon Labs, name: Data Attribute), Attribute Handle: 018
  Company-specific Service UUID: Amazon:Alexa Mobile Accessories (AMA) fe03:
  Begin Handle: 019, End Handle: 029
    2800 (Declaration: Primary Service), Attribute Handle: 019
    2803 (Declaration: Characteristic), Attribute Handle: 020
      f04eb177-3005-43a7-ac61-a390ddf83076 (Custom UUID128: company: Amazon, name: Transmit (TX)), Attribute Handle: 021
    2803 (Declaration: Characteristic), Attribute Handle: 022
      2beea05b-1879-4bb4-8a2f-72641f82420b (Custom UUID128: company: Amazon, name: Receive (RX)), Attribute Handle: 023
      2902 (Descriptor: Client Characteristic Configuration), Attribute Handle: 024
    2803 (Declaration: Characteristic), Attribute Handle: 025
  Company ID: Disney Worldwide Services, Inc. fd98:
  Begin Handle: 030, End Handle: 65535
  GATT Service Unknown! Handle does not match any Service ranges that we received from the device!


BLE 2thprint Info:
  BLE LL Ctrl Opcode: 9 (LL_FEATURE_RSP)
    BLE LL Features: 0x000000000000000d
      * LE Encryption
      * Extended Reject Indication
      * Peripheral-initiated Features Exchange

Unique ID / Potential Trackability Report:
  No privacy report results found. (But current checks are far from exhaustive.)
```

```
  Service: GATT 1801:
  Begin Handle: 001, End Handle: 008
    2800 (Declaration: Primary Service), Attribute Handle: 001
    2803 (Declaration: Characteristic), Attribute Handle: 002
      2a05 (Characteristic Value: Service Changed), Attribute Handle: 003
      2902 (Descriptor: Client Characteristic Configuration), Attribute Handle: 004
    2803 (Declaration: Characteristic), Attribute Handle: 005
      2b2a (Characteristic Value: Database Hash), Attribute Handle: 006
      GATT Characteristic Value read as b'\xd4\xd6\xfe\xc4T\x11l?Q\xef\xd1;\xce\xde\xf0\xb2'
    2803 (Declaration: Characteristic), Attribute Handle: 007
      2b29 (Characteristic Value: Client Supported Features), Attribute Handle: 008
      GATT Characteristic Value read as b'\x00'
  Service: GAP 1800:
  Begin Handle: 009, End Handle: 013
    2800 (Declaration: Primary Service), Attribute Handle: 009
    2803 (Declaration: Characteristic), Attribute Handle: 010
      2a00 (Characteristic Value: Device Name), Attribute Handle: 011
      GATT Characteristic Value read as b'MagicBand+ A139'
    2803 (Declaration: Characteristic), Attribute Handle: 012
      2a01 (Characteristic Value: Appearance), Attribute Handle: 013
      GATT Characteristic Value read as b'\x00\x00'
  Custom UUID128: company: Silicon Labs, name: OTA Firmware Update 1d14d6ee-fd63-4fa1-bfa4-8f47b42119f0:
  Begin Handle: 014, End Handle: 018
    2800 (Declaration: Primary Service), Attribute Handle: 014
    2803 (Declaration: Characteristic), Attribute Handle: 015
      f7bf3564-fb6d-4e53-88a4-5e37e0326063 (Custom UUID128: company: Silicon Labs, name: Control Attribute), Attribute Handle: 016
    2803 (Declaration: Characteristic), Attribute Handle: 017
      984227f3-34fc-4045-a5d0-2c581f81a153 (Custom UUID128: company: Silicon Labs, name: Data Attribute), Attribute Handle: 018
  Company-specific Service UUID: Amazon:Alexa Mobile Accessories (AMA) fe03:
  Begin Handle: 019, End Handle: 029
    2800 (Declaration: Primary Service), Attribute Handle: 019
    2803 (Declaration: Characteristic), Attribute Handle: 020
      f04eb177-3005-43a7-ac61-a390ddf83076 (Custom UUID128: company: Amazon, name: Transmit (TX)), Attribute Handle: 021
    2803 (Declaration: Characteristic), Attribute Handle: 022
      2beea05b-1879-4bb4-8a2f-72641f82420b (Custom UUID128: company: Amazon, name: Receive (RX)), Attribute Handle: 023
      2902 (Descriptor: Client Characteristic Configuration), Attribute Handle: 024
    2803 (Declaration: Characteristic), Attribute Handle: 025
  Company ID: Disney Worldwide Services, Inc. fd98
  Begin Handle: 030, End Handle: 65535
  GATT Service Unknown! Handle does not match any Service ranges that we received from the device!


BLE 2thprint Info:
  BLE LL Ctrl Opcode: 9 (LL_FEATURE_RSP)
    BLE LL Features: 0x000000000000000d
      * LE Encryption
      * Extended Reject Indication
      * Peripheral-initiated Features Exchange

Unique ID / Potential Trackability Report:
  No privacy report results found. (But current checks are far from exhaustive.)
```

```
  Service: GATT 1801:
  Begin Handle: 001, End Handle: 008
    2800 (Declaration: Primary Service), Attribute Handle: 001
    2803 (Declaration: Characteristic), Attribute Handle: 002
      2a05 (Characteristic Value: Service Changed), Attribute Handle: 003
      2902 (Descriptor: Client Characteristic Configuration), Attribute Handle: 004
    2803 (Declaration: Characteristic), Attribute Handle: 005
      2b2a (Characteristic Value: Database Hash), Attribute Handle: 006
      GATT Characteristic Value read as b'\xd4\xd6\xfe\xc4T\x11l?Q\xef\xd1;\xce\xde\xf0\xb2'
    2803 (Declaration: Characteristic), Attribute Handle: 007
      2b29 (Characteristic Value: Client Supported Features), Attribute Handle: 008
      GATT Characteristic Value read as b'\x00'
  Service: GAP 1800:
  Begin Handle: 009, End Handle: 013
    2800 (Declaration: Primary Service), Attribute Handle: 009
    2803 (Declaration: Characteristic), Attribute Handle: 010
      2a00 (Characteristic Value: Device Name), Attribute Handle: 011
      GATT Characteristic Value read as b'MagicBand+ A139'
    2803 (Declaration: Characteristic), Attribute Handle: 012
      2a01 (Characteristic Value: Appearance), Attribute Handle: 013
      GATT Characteristic Value read as b'\x00\x00'
  Custom UUID128: company: Silicon Labs, name: OTA Firmware Update 1d14d6ee-fd63-4fa1-bfa4-8f47b42119f0:
  Begin Handle: 014, End Handle: 018
    2800 (Declaration: Primary Service), Attribute Handle: 014
    2803 (Declaration: Characteristic), Attribute Handle: 015
      f7bf3564-fb6d-4e53-88a4-5e37e0326063 (Custom UUID128: company: Silicon Labs, name: Control Attribute), Attribute Handle: 016
    2803 (Declaration: Characteristic), Attribute Handle: 017
      984227f3-34fc-4045-a5d0-2c581f81a153 (Custom UUID128: company: Silicon Labs, name: Data Attribute), Attribute Handle: 018
  Company-specific Service UUID: Amazon:Alexa Mobile Accessories (AMA) fe03:
  Begin Handle: 019, End Handle: 029
    2800 (Declaration: Primary Service), Attribute Handle: 019
    2803 (Declaration: Characteristic), Attribute Handle: 020
      f04eb177-3005-43a7-ac61-a390ddf83076 (Custom UUID128: company: Amazon, name: Transmit (TX)), Attribute Handle: 021
    2803 (Declaration: Characteristic), Attribute Handle: 022
      2beea05b-1879-4bb4-8a2f-72641f82420b (Custom UUID128: company: Amazon, name: Receive (RX)), Attribute Handle: 023
      2902 (Descriptor: Client Characteristic Configuration), Attribute Handle: 024
    2803 (Declaration: Characteristic), Attribute Handle: 025
  Company ID: Disney Worldwide Services, Inc. fd98
  Begin Handle: 030, End Handle: 65535
  GATT Service Unknown! Handle does not match any Service ranges that we received from the device!


BLE 2thprint Info:
  BLE LL Ctrl Opcode: 9 (LL_FEATURE_RSP)
    BLE LL Features: 0x000000000000000d
      * LE Encryption
      * Extended Reject Indication
      * Peripheral-initiated Features Exchange

Unique ID / Potential Trackability Report:
  No privacy report results found. (But current checks are far from exhaustive.)
```

```
  Service: GATT 1801:
  Begin Handle: 001, End Handle: 008
    2800 (Declaration: Primary Service), Attribute Handle: 001
    2803 (Declaration: Characteristic), Attribute Handle: 002
      2a05 (Characteristic Value: Service Changed), Attribute Handle: 003
      2902 (Descriptor: Client Characteristic Configuration), Attribute Handle: 004
    2803 (Declaration: Characteristic), Attribute Handle: 005
      2b2a (Characteristic Value: Database Hash), Attribute Handle: 006
      GATT Characteristic Value read as b'\xd4\xd6\xfe\xc4T\x11l?Q\xef\xd1;\xce\xde\xf0\xb2'
    2803 (Declaration: Characteristic), Attribute Handle: 007
      2b29 (Characteristic Value: Client Supported Features), Attribute Handle: 008
      GATT Characteristic Value read as b'\x00'
  Service: GAP 1800:
  Begin Handle: 009, End Handle: 013
    2800 (Declaration: Primary Service), Attribute Handle: 009
    2803 (Declaration: Characteristic), Attribute Handle: 010
      2a00 (Characteristic Value: Device Name), Attribute Handle: 011
      GATT Characteristic Value read as b'MagicBand+ A139'
    2803 (Declaration: Characteristic), Attribute Handle: 012
      2a01 (Characteristic Value: Appearance), Attribute Handle: 013
      GATT Characteristic Value read as b'\x00\x00'
  Custom UUID128: company: Silicon Labs, name: OTA Firmware Update 1d14d6ee-fd63-4fa1-bfa4-8f47b42119f0:
  Begin Handle: 014, End Handle: 018
    2800 (Declaration: Primary Service), Attribute Handle: 014
    2803 (Declaration: Characteristic), Attribute Handle: 015
      f7bf3564-fb6d-4e53-88a4-5e37e0326063 (Custom UUID128: company: Silicon Labs, name: Control Attribute)  Attribute Handle: 016
    2803 (Declaration: Characteristic), Attribute Handle: 017
      984227f3-34fc-4045-a5d0-2c581f81a153 (Custom UUID128: company: Silicon Labs, name: Data Attribute), Attribute Handle: 018
  Company-specific Service UUID: Amazon:Alexa Mobile Accessories (AMA) fe03:
  Begin Handle: 019, End Handle: 029
    2800 (Declaration: Primary Service), Attribute Handle: 019
    2803 (Declaration: Characteristic), Attribute Handle: 020
      f04eb177-3005-43a7-ac61-a390ddf83076 (Custom UUID128: company: Amazon, name: Transmit (TX)), Attribute Handle: 021
    2803 (Declaration: Characteristic), Attribute Handle: 022
      2beea05b-1879-4bb4-8a2f-72641f82420b (Custom UUID128: company: Amazon, name: Receive (RX)), Attribute Handle: 023
      2902 (Descriptor: Client Characteristic Configuration), Attribute Handle: 024
    2803 (Declaration: Characteristic), Attribute Handle: 025
  Company ID: Disney Worldwide Services, Inc. fd98
  Begin Handle: 030, End Handle: 65535
  GATT Service Unknown! Handle does not match any Service ranges that we received from the device!


BLE 2thprint Info:
  BLE LL Ctrl Opcode: 9 (LL_FEATURE_RSP)
    BLE LL Features: 0x000000000000000d
      * LE Encryption
      * Extended Reject Indication
      * Peripheral-initiated Features Exchange

Unique ID / Potential Trackability Report:
  No privacy report results found. (But current checks are far from exhaustive.)
```

https://blog.quarkslab.com/breaking-secure-boot-on-the-silicon-labs-gecko-platform.html

Breaking Secure Boot on the Silicon Labs Gecko platform

Date Mon 21 August 2023 By Sami Babigeon Benoît Forgette Category Vulnerability Tags reverse-engineering exploitation vulnerability 2023

In this blog post, we present a new vulnerability on the Gecko Bootloader from Silicon Labs more precisely inside the OTA parser.

Introduction

Silicon Labs is a chip manufacturer with several network-targeted features like Bluetooth and Zigbee. These chips are the base of a large number of connected objects, and compromising them means compromising all of these connected objects insofar as they use the vulnerable functionality.

We decided to look into the open source SDK offered by Silicon Labs: the Gecko SDK (GSDK), in particular it's OTA functionality which seems to be state of the art of secure over-the-air updates.

This R&D work was carried out during Sami Babigeon's internship at Quarkslab, as part of his Master's degree program at the University of Rouen Normandie.

```
      2a01 (Characteristic Value: Appearance), Attribute Handle: 013
      GATT Characteristic Value read as b'\x00\x00'
  Custom UUID128: company: Silicon Labs, name: OTA Firmware Update 1d14d6ee-fd63-4fa1-bfa4-8f47b42119f0:
  Begin Handle: 014, End Handle: 018
    2800 (Declaration: Primary Service), Attribute Handle: 014
    2803 (Declaration: Characteristic), Attribute Handle: 015
      f7bf3564-fb6d-4e53-88a4-5e37e0326063 (Custom UUID128: company: Silicon Labs, name: Control Attribute)  Attribute Handle: 016
    2803 (Declaration: Characteristic), Attribute Handle: 017
      984227f3-34fc-4045-a5d0-2c581f81a153 (Custom UUID128: company: Silicon Labs, name: Data Attribute), Attribute Handle: 018
  Company-specific Service UUID: Amazon:Alexa Mobile Accessories (AMA) fe03:
  Begin Handle: 019, End Handle: 029
    2800 (Declaration: Primary Service), Attribute Handle: 019
    2803 (Declaration: Characteristic), Attribute Handle: 020
      f04eb177-3005-43a7-ac61-a390ddf83076 (Custom UUID128: company: Amazon, name: Transmit (TX)), Attribute Handle: 021
    2803 (Declaration: Characteristic), Attribute Handle: 022
      2beea05b-1879-4bb4-8a2f-72641f82420b (Custom UUID128: company: Amazon, name: Receive (RX)), Attribute Handle: 023
      2902 (Descriptor: Client Characteristic Configuration), Attribute Handle: 024
    2803 (Declaration: Characteristic), Attribute Handle: 025
  Company ID: Disney Worldwide Services, Inc. fd98
  Begin Handle: 030, End Handle: 65535
  GATT Service Unknown! Handle does not match any Service ranges that we received from the device!


BLE 2thprint Info:
  BLE LL Ctrl Opcode: 9 (LL_FEATURE_RSP)
    BLE LL Features: 0x000000000000000d
      * LE Encryption
      * Extended Reject Indication
      * Peripheral-initiated Features Exchange

Unique ID / Potential Trackability Report:
  No privacy report results found. (But current checks are far from exhaustive.)
```

https://blog.quarkslab.com/breaking-secure-boot-on-the-silicon-labs-gecko-platform.html

Breaking Secure Boot on the Silicon Labs Gecko platform

Date Mon 21 August 2023 By Sami Babigeon Benoît Forgette Category Vulnerability Tags reverse-engineering exploitation vulnerability 2023

In this blog post, we present a new vulnerability on the Gecko Bootloader from Silicon Labs more precisely inside the OTA parser.

Introduction

Silicon Labs is a chip manufacturer with several network-targeted features like Bluetooth and Zigbee. These chips are the base of a large number of connected objects, and compromising them means compromising all of these connected objects insofar as they use the vulnerable functionality.

We decided to look into the open source SDK offered by Silicon Labs: the Gecko SDK (GSDK), in particular it's OTA functionality which seems to be state of the art of secure over-the-air updates.

This R&D work was carried out during Sami Babigeon's internship at Quarkslab, as part of his Master's degree program at the University of Rouen Normandie.

```
      2a01 (Characteristic Value: Appearance), Attribute Handle: 013
      GATT Characteristic Value read as b'\x00\x00'
  Custom UUID128: company: Silicon Labs, name: OTA Firmware Update 1d14d6ee-fd63-4fa1-bfa4-8f47b42119f0:
  Begin Handle: 014, End Handle: 018
    2800 (Declaration: Primary Service), Attribute Handle: 014
    2803 (Declaration: Characteristic), Attribute Handle: 015
      f7bf3564-fb6d-4e53-88a4-5e37e0326063 (Custom UUID128: company: Silicon Labs, name: Control Attribute)  Attribute Handle: 016
    2803 (Declaration: Characteristic), Attribute Handle: 017
      984227f3-34fc-4045-a5d0-2c581f81a153 (Custom UUID128: company: Silicon Labs, name: Data Attribute), Attribute Handle: 018
  Company-specific Service UUID: Amazon:Alexa Mobile Accessories (AMA) fe03:
  Begin Handle: 019, End Handle: 029
    2800 (Declaration: Primary Service), Attribute Handle: 019
    2803 (Declaration: Characteristic), Attribute Handle: 020
      f04eb177-3005-43a7-ac61-a390ddf83076 (Custom UUID128: company: Amazon, name: Transmit (TX)), Attribute Handle: 021
    2803 (Declaration: Characteristic), Attribute Handle: 022
      2beea05b-1879-4bb4-8a2f-72641f82420b (Custom UUID128: company: Amazon, name: Receive (RX)), Attribute Handle: 023
      2902 (Descriptor: Client Characteristic Configuration), Attribute Handle: 024
    2803 (Declaration: Characteristic), Attribute Handle: 025
  Company ID: Disney Worldwide Services, Inc. fd98
  Begin Handle: 030, End Handle: 65535
  GATT Service Unknown! Handle does not match any Service ranges that we received from the device!


BLE 2thprint Info:
  BLE LL Ctrl Opcode: 9 (LL_FEATURE_RSP)
    BLE LL Features: 0x000000000000000d
      * LE Encryption
      * Extended Reject Indication
      * Peripheral-initiated Features Exchange

Unique ID / Potential Trackability Report:
  No privacy report results found. (But current checks are far from exhaustive.)
```

https://blog.quarkslab.com/breaking-secure-boot-on-the-silicon-labs-gecko-platform.html

Breaking Secure Boot on the Silicon Labs Gecko platform

Date Mon 21 August 2023 By Sami Babigeon Benoît Forgette Category Vulnerability Tags reverse-engineering exploitation vulnerability 2023

In this blog post, we present a new vulnerability on the Gecko Bootloader from Silicon Labs more precisely inside the OTA parser.

Introduction

Silicon Labs is a chip manufacturer with several network-targeted features like Bluetooth and Zigbee. These chips are the base of a large number of connected objects, and compromising them means compromising all of these connected objects insofar as they use the vulnerable functionality.

We decided to look into the open source SDK offered by Silicon Labs: the Gecko SDK (GSDK), in particular it's OTA functionality which seems to be state of the art of secure over-the-air updates.

This R&D work was carried out during Sami Babigeon's internship at Quarkslab, as part of his Master's degree program at the University of Rouen Normandie.

```
      2a01 (Characteristic Value: Appearance), Attribute Handle: 013
      GATT Characteristic Value read as b'\x00\x00'
  Custom UUID128: company: Silicon Labs, name: OTA Firmware Update 1d14d6ee-fd63-4fa1-bfa4-8f47b42119f0:
  Begin Handle: 014, End Handle: 018
    2800 (Declaration: Primary Service), Attribute Handle: 014
    2803 (Declaration: Characteristic), Attribute Handle: 015
      f7bf3564-fb6d-4e53-88a4-5e37e0326063 (Custom UUID128: company: Silicon Labs, name: Cont
    2803 (Declaration: Characteristic), Attribute Handle: 017
      984227f3-34fc-4045-a5d0-2c581f81a153 (Custom UUID128: company: Silicon Labs, name: Data
  Company-specific Service UUID: Amazon:Alexa Mobile Accessories (AMA) fe03:
  Begin Handle: 019, End Handle: 029
    2800 (Declaration: Primary Service), Attribute Handle: 019
    2803 (Declaration: Characteristic), Attribute Handle: 020
      f04eb177-3005-43a7-ac61-a390ddf83076 (Custom UUID128: company: Amazon, name: Transmit (
    2803 (Declaration: Characteristic), Attribute Handle: 022
      2beea05b-1879-4bb4-8a2f-72641f82420b (Custom UUID128: company: Amazon, name: Receive (R
      2902 (Descriptor: Client Characteristic Configuration), Attribute Handle: 024
    2803 (Declaration: Characteristic), Attribute Handle: 025
  Company ID: Disney Worldwide Services, Inc. fd98
  Begin Handle: 030, End Handle: 65535
  GATT Service Unknown! Handle does not match any Service ranges that we received from the dev


BLE 2thprint Info:
  BLE LL Ctrl Opcode: 9 (LL_FEATURE_RSP)
    BLE LL Features: 0x000000000000000d
      * LE Encryption
      * Extended Reject Indication
      * Peripheral-initiated Features Exchange

Unique ID / Potential Trackability Report:
  No privacy report results found. (But current checks are far from exhaustive.)
```

The Disney version of Alexa will be available on any Echo device, but a special version will be embedded in Echo smart displays and speakers at Disney resort hotels. MagicBand+ will also be compatible with “Hey, Disney!” Guests at home or in Disney resorts can play games with their Echo and MagicBand+, which will act as a game show-style buzzer reacting with lights and haptics.

```
For bdaddr = 98:07:2d:f3:5b:f4:
  2thprint_ChipPrint:
    No ChipPrint(s) found.

  2thprint_ChipMakerPrint:
    Texas Instruments -> From IEEE OUI matched with BT Classic address
    Texas Instruments -> From GATTprint match on f000ffc0-0451-4000-b000-000000000000 = "Service: Texas Instruments: Over the Air Download (OAD) firmware update"
(GATT_services table)

  Company Name by IEEE OUI (98:07:2d): Texas Instruments
    BDADDR is Bluetooth Low Energy Public

  DeviceName: 5AAA=mS*+5cFH~EeDtyd;kDTAqfE;
  DeviceNameType: Complete Name
    This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)
  DeviceName: 5AAA=mS*+5cFH~EeDwVdjJ4SAqfF3
  DeviceNameType: Complete Name
    This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)
  DeviceName: 5AAA=mS*+6!cs3EeDt^@c;lzAqfF9
  DeviceNameType: Complete Name
    This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)
  DeviceName: 5AAA=mS*+6!cs3EeDtm@c;lzAqfF9
  DeviceNameType: Complete Name
    This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)
  DeviceName: 5AAA=mS*+6!cs3EeDuN@c;lzAqfF9
  DeviceNameType: Complete Name
    This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)
  DeviceName: 5AAA=mS*+6!cs3EeDur@c;lzAqfF9
  DeviceNameType: Complete Name
    This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)
  DeviceName: 5AAA=mS*+6!cs3EeDvi@BjcyAqfFP
  DeviceNameType: Complete Name
    This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

  Flags found:
  In BLE Data (LE_bdaddr_to_flags)
    BLE Limited Discoverable Mode: 0
    BLE General Discoverable Mode: 1
    BR/EDR Not Supported: 1
    Simultaneous BLE and BR/EDR Supported by Controller: 0
    Simultaneous BLE and BR/EDR Supported by Host: 0

  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 (Apple, Inc. (wrong-endian))
    Raw Data: 0215a49e2f4853964586803fe6c9140980f703e80555c4
    Apple iBeacon:
      UUID128: a49e2f48-5396-4586-803f-e6c9140980f7
      Major ID: 03e8
      Minor ID: 0555
      RSSI at 1 meter: -60dBm
```

```
For bdaddr = 98:07:2d:f3:5b:f4:
  2thprint_ChipPrint:
    No ChipPrint(s) found.

  2thprint_ChipMakerPrint:
    Texas Instruments -> From IEEE OUI matched with BT Classic address
    Texas Instruments -> From GATTprint match on f000ffc0-0451-4000-b000-000000000000 = "Service: Texas Instruments: Over the Air Download (OAD) firmware update"
(GATT_services table)

  Company Name by IEEE OUI (98:07:2d): Texas Instruments
    BDADDR is Bluetooth Low Energy Public

  DeviceName: 5AAA=mS*+5cFH~EeDtyd;kDTAqfE;
  DeviceNameType: Complete Name
    This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)
  DeviceName: 5AAA=mS*+5cFH~EeDwVdjJ4SAqfF3
  DeviceNameType: Complete Name
    This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)
  DeviceName: 5AAA=mS*+6!cs3EeDt^@c;lzAqfF9
  DeviceNameType: Complete Name
    This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)
  DeviceName: 5AAA=mS*+6!cs3EeDtm@c;lzAqfF9
  DeviceNameType: Complete Name
    This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)
  DeviceName: 5AAA=mS*+6!cs3EeDuN@c;lzAqfF9
  DeviceNameType: Complete Name
    This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)
  DeviceName: 5AAA=mS*+6!cs3EeDur@c;lzAqfF9
  DeviceNameType: Complete Name
    This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)
  DeviceName: 5AAA=mS*+6!cs3EeDvi@BjcyAqfFP
  DeviceNameType: Complete Name
    This was found in an event of type 4 which corresponds to Scan Response (SCAN_RSP)

  Flags found:
  In BLE Data (LE_bdaddr_to_flags)
    BLE Limited Discoverable Mode: 0
    BLE General Discoverable Mode: 1
    BR/EDR Not Supported: 1
    Simultaneous BLE and BR/EDR Supported by Controller: 0
    Simultaneous BLE and BR/EDR Supported by Host: 0

  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 (Apple, Inc. (wrong-endian))
    Raw Data: 0215a49e2f4853964586803fe6c9140980f703e80555c4
    Apple iBeacon:
      UUID128: a49e2f48-5396-4586-803f-e6c9140980f7
      Major ID: 03e8
      Minor ID: 0555
      RSSI at 1 meter: -60dBm
```

```
  2803 (Declaration: Characteristic), Attribute Handle: 002
    2a00 (Characteristic Value: Device Name), Attribute Handle: 003
    GATT Characteristic Value read as b'Beacon'
  2803 (Declaration: Characteristic), Attribute Handle: 004
    2a01 (Characteristic Value: Appearance), Attribute Handle: 005
    GATT Characteristic Value read as b'\x00\x00'
  2803 (Declaration: Characteristic), Attribute Handle: 006
    2a04 (Characteristic Value: Peripheral Preferred Connection Parameters), Attribute Handle: 007
    GATT Characteristic Value read as b'P\x00\xa0\x00\x00\x00\xe8\x03'
Service: GATT 1801:
Begin Handle: 008, End Handle: 008
  2800 (Declaration: Primary Service), Attribute Handle: 008
Service: Device Information 180a:
Begin Handle: 009, End Handle: 021
  2800 (Declaration: Primary Service), Attribute Handle: 009
  2803 (Declaration: Characteristic), Attribute Handle: 010
    2a23 (Characteristic Value: System ID), Attribute Handle: 011
    GATT Characteristic Value read as b'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'
  2803 (Declaration: Characteristic), Attribute Handle: 012
    2a24 (Characteristic Value: Model Number String), Attribute Handle: 013
    GATT Characteristic Value read as b'LS-BT20'
  2803 (Declaration: Characteristic), Attribute Handle: 014
    2a25 (Characteristic Value: Serial Number String), Attribute Handle: 015
    GATT Characteristic Value read as b'aruba-98072df35bf4'
  2803 (Declaration: Characteristic), Attribute Handle: 016
    2a27 (Characteristic Value: Hardware Revision String), Attribute Handle: 017
    GATT Characteristic Value read as b'1 050617'
  2803 (Declaration: Characteristic), Attribute Handle: 018
    2a28 (Characteristic Value: Software Revision String), Attribute Handle: 019
    GATT Characteristic Value read as b'OAD-E 1.2-9'
  2803 (Declaration: Characteristic), Attribute Handle: 020
    2a29 (Characteristic Value: Manufacturer Name String), Attribute Handle: 021
    GATT Characteristic Value read as b'HPE Aruba'
Service: Battery 180f:
Begin Handle: 022, End Handle: 027
  2800 (Declaration: Primary Service), Attribute Handle: 022
  2803 (Declaration: Characteristic), Attribute Handle: 023
    2a19 (Characteristic Value: Battery Level), Attribute Handle: 024
    GATT Characteristic Value read as b'd'
    2902 (Descriptor: Client Characteristic Configuration), Attribute Handle: 025
    2908 (Descriptor: Report Reference), Attribute Handle: 026
    2904 (Descriptor: Characteristic Presentation Format), Attribute Handle: 027
Unknown UUID128 272fe150-6c6c-4718-a3d4-6de8a3735cff:
Begin Handle: 028, End Handle: 074
  2800 (Declaration: Primary Service), Attribute Handle: 028
  2803 (Declaration: Characteristic), Attribute Handle: 029
    272fe151-6c6c-4718-a3d4-6de8a3735cff (Unknown UUID128), Attribute Handle: 030
    GATT Characteristic Value read as b'\xa4\x9e/HS\x96E\x86\x80?\xe6\xc9\x14\t\x80\xf7'
  2803 (Declaration: Characteristic), Attribute Handle: 031
    272fe152-6c6c-4718-a3d4-6de8a3735cff (Unknown UUID128), Attribute Handle: 032
    GATT Characteristic Value read as b'\xe8\x03'
```

```
  2803 (Declaration: Characteristic), Attribute Handle: 002
    2a00 (Characteristic Value: Device Name), Attribute Handle: 003
    GATT Characteristic Value read as b'Beacon'
  2803 (Declaration: Characteristic), Attribute Handle: 004
    2a01 (Characteristic Value: Appearance), Attribute Handle: 005
    GATT Characteristic Value read as b'\x00\x00'
  2803 (Declaration: Characteristic), Attribute Handle: 006
    2a04 (Characteristic Value: Peripheral Preferred Connection Parameters), Attribute Handle: 007
    GATT Characteristic Value read as b'P\x00\xa0\x00\x00\x00\xe8\x03'
Service: GATT 1801:
Begin Handle: 008, End Handle: 008
  2800 (Declaration: Primary Service), Attribute Handle: 008
Service: Device Information 180a:
Begin Handle: 009, End Handle: 021
  2800 (Declaration: Primary Service), Attribute Handle: 009
  2803 (Declaration: Characteristic), Attribute Handle: 010
    2a23 (Characteristic Value: System ID), Attribute Handle: 011
    GATT Characteristic Value read as b'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'
  2803 (Declaration: Characteristic), Attribute Handle: 012
    2a24 (Characteristic Value: Model Number String), Attribute Handle: 013
    GATT Characteristic Value read as b'LS-BT20'
  2803 (Declaration: Characteristic), Attribute Handle: 014
    2a25 (Characteristic Value: Serial Number String), Attribute Handle: 015
    GATT Characteristic Value read as b'aruba-98072df35bf4'
  2803 (Declaration: Characteristic), Attribute Handle: 016
    2a27 (Characteristic Value: Hardware Revision String), Attribute Handle: 017
    GATT Characteristic Value read as b'1 050617'
  2803 (Declaration: Characteristic), Attribute Handle: 018
    2a28 (Characteristic Value: Software Revision String), Attribute Handle: 019
    GATT Characteristic Value read as b'OAD-E 1.2-9'
  2803 (Declaration: Characteristic), Attribute Handle: 020
    2a29 (Characteristic Value: Manufacturer Name String), Attribute Handle: 021
    GATT Characteristic Value read as b'HPE Aruba'
Service: Battery 180f:
Begin Handle: 022, End Handle: 027
  2800 (Declaration: Primary Service), Attribute Handle: 022
  2803 (Declaration: Characteristic), Attribute Handle: 023
    2a19 (Characteristic Value: Battery Level), Attribute Handle: 024
    GATT Characteristic Value read as b'd'
    2902 (Descriptor: Client Characteristic Configuration), Attribute Handle: 025
    2908 (Descriptor: Report Reference), Attribute Handle: 026
    2904 (Descriptor: Characteristic Presentation Format), Attribute Handle: 027
Unknown UUID128 272fe150-6c6c-4718-a3d4-6de8a3735cff:
Begin Handle: 028, End Handle: 074
  2800 (Declaration: Primary Service), Attribute Handle: 028
  2803 (Declaration: Characteristic), Attribute Handle: 029
    272fe151-6c6c-4718-a3d4-6de8a3735cff (Unknown UUID128), Attribute Handle: 030
    GATT Characteristic Value read as b'\xa4\x9e/HS\x96E\x86\x80?\xe6\xc9\x14\t\x80\xf7'
  2803 (Declaration: Characteristic), Attribute Handle: 031
    272fe152-6c6c-4718-a3d4-6de8a3735cff (Unknown UUID128), Attribute Handle: 032
    GATT Characteristic Value read as b'\xe8\x03'
```

```
      272fe162-6c6c-4718-a3d4-6de8a3735cff (Unknown UUID128), Attribute Handle: 054
  Custom UUID128: company: Texas Instruments, name: Over-the-Air Download (OAD) f000ffc0-0451-4000-b000-000000000000:
  Begin Handle: 075, End Handle: 65535
  GATT Service Unknown! Handle does not match any Service ranges that we received from the device!


BLE 2thprint Info:
  BLE LL Ctrl Opcode: 9 (LL_FEATURE_RSP)
    BLE LL Features: 0x0000000000000001
      * LE Encryption

L2CAP data found:
  L2CAP_CONNECTION_PARAMETER_UPDATE_REQ:
    Direction: Peripheral to Central
    Packet command/response association ID: 1
    Data Length: 8
    Requested minimum connection interval (in units of 1.25ms): 16
    Requested maximum connection interval (in units of 1.25ms): 32
    Requested Peripheral Latency (number of connection events Peripheral can skip responding): 0
    Requested timeout (in units of 10ms): 600

Unique ID / Potential Trackability Report:
  Unique ID: BDADDR is of type *Public*, which is not randomized over time, and therefore can be used to track the device.
  *Possible* Unique ID: This device contains a name "5AAA=mS*+5cFH~EeDtyd;kDTAqfE;" found via Bluetooth Low Energy Advertisements. The name itself does not match a known-unique-ID pattern, but that could just mean it has not been captured in our metadata yet.
        It is left to the user to investigate whether this name represents a unique ID or not. E.g. look for other instances of this name in your own data via the --nameregex option, or search by name at wigle.net.
  *Possible* Unique ID: This device contains a name "5AAA=mS*+5cFH~EeDwVdjJ4SAqfF3" found via Bluetooth Low Energy Advertisements. The name itself does not match a known-unique-ID pattern, but that could just mean it has not been captured in our metadata yet.
        It is left to the user to investigate whether this name represents a unique ID or not. E.g. look for other instances of this name in your own data via the --nameregex option, or search by name at wigle.net.
  *Possible* Unique ID: This device contains a name "5AAA=mS*+6!cs3EeDt^@c;lzAqfF9" found via Bluetooth Low Energy Advertisements. The name itself does not match a known-unique-ID pattern, but that could just mean it has not been captured in our metadata yet.
        It is left to the user to investigate whether this name represents a unique ID or not. E.g. look for other instances of this name in your own data via the --nameregex option, or search by name at wigle.net.
  *Possible* Unique ID: This device contains a name "5AAA=mS*+6!cs3EeDtm@c;lzAqfF9" found via Bluetooth Low Energy Advertisements. The name itself does not match a known-unique-ID pattern, but that could just mean it has not been captured in our metadata yet.
        It is left to the user to investigate whether this name represents a unique ID or not. E.g. look for other instances of this name in your own data via the --nameregex option, or search by name at wigle.net.
  *Possible* Unique ID: This device contains a name "5AAA=mS*+6!cs3EeDuN@c;lzAqfF9" found via Bluetooth Low Energy Advertisements. The name itself does not match a known-unique-ID pattern, but that could just mean it has not been captured in our metadata yet.
        It is left to the user to investigate whether this name represents a unique ID or not. E.g. look for other instances of this name in your own data via the --nameregex option, or search by name at wigle.net.
  *Possible* Unique ID: This device contains a name "5AAA=mS*+6!cs3EeDur@c;lzAqfF9" found via Bluetooth Low Energy Advertisements. The name itself does not match a known-unique-ID pattern, but that could just mean it has not been captured in our metadata yet.
        It is left to the user to investigate whether this name represents a unique ID or not. E.g. look for other instances of this name in your own data via the --nameregex option, or search by name at wigle.net.
  *Possible* Unique ID: This device contains a name "5AAA=mS*+6!cs3EeDvi@BjcyAqfFP" found via Bluetooth Low Energy Advertisements. The name itself does not match a known-unique-ID pattern, but that could just mean it has not been captured in our metadata yet.
        It is left to the user to investigate whether this name represents a unique ID or not. E.g. look for other instances of this name in your own data via the --nameregex option, or search by name at wigle.net.
```

272fe162-6c6c-4718-a3d4-6de8a3735cff (Unknown UUID128) Attribute Handle: 054
Custom UUID128: company: Texas Instruments, name: Over-the-Air Download (OAD) f000ffc0-0451-4000-b000-000000000000
Begin Handle: 075, End Handle: 65535
GATT Service Unknown! Handle does not match any Service ranges that we received from the device!

BLE 2thprint Info:
BLE LL Ctrl Opcode: 9 (LL_FEATURE_RSP)
BLE LL Features: 0x0000000000000001
* LE Encryption

L2CAP data found:
L2CAP_CONNECTION_PARAMETER_UPDATE_REQ:
Direction: Peripheral to Central
Packet command/response association ID: 1
Data Length: 8
Requested minimum connection interval (in units of 1.25ms): 16
Requested maximum connection interval (in units of 1.25ms): 32
Requested Peripheral Latency (number of connection events Peripheral can skip responding): 0
Requested timeout (in units of 10ms): 600

Unique ID / Potential Trackability Report:
Unique ID: BDADDR is of type *Public*, which is not randomized over time, and therefore can be used to track the device.
Possible Unique ID: This device contains a name "5AAA=mS*+5cFH~EeDtyd;kDTAqfE;" found via Bluetooth Low Energy Advertisements. The name itself does not match a known-unique-ID pattern, but that could just mean it has not been captured in our metadata yet.
It is left to the user to investigate whether this name represents a unique ID or not. E.g. look for other instances of this name in your own data via the --nameregex option, or search by name at wigle.net.
Possible Unique ID: This device contains a name "5AAA=mS*+5cFH~EeDwVdjJ4SAqfF3" found via Bluetooth Low Energy Advertisements. The name itself does not match a known-unique-ID pattern, but that could just mean it has not been captured in our metadata yet.
It is left to the user to investigate whether this name represents a unique ID or not. E.g. look for other instances of this name in your own data via the --nameregex option, or search by name at wigle.net.
Possible Unique ID: This device contains a name "5AAA=mS*+6!cs3EeDt^@c;lzAqfF9" found via Bluetooth Low Energy Advertisements. The name itself does not match a known-unique-ID pattern, but that could just mean it has not been captured in our metadata yet.
It is left to the user to investigate whether this name represents a unique ID or not. E.g. look for other instances of this name in your own data via the --nameregex option, or search by name at wigle.net.
Possible Unique ID: This device contains a name "5AAA=mS*+6!cs3EeDtm@c;lzAqfF9" found via Bluetooth Low Energy Advertisements. The name itself does not match a known-unique-ID pattern, but that could just mean it has not been captured in our metadata yet.
It is left to the user to investigate whether this name represents a unique ID or not. E.g. look for other instances of this name in your own data via the --nameregex option, or search by name at wigle.net.
Possible Unique ID: This device contains a name "5AAA=mS*+6!cs3EeDuN@c;lzAqfF9" found via Bluetooth Low Energy Advertisements. The name itself does not match a known-unique-ID pattern, but that could just mean it has not been captured in our metadata yet.
It is left to the user to investigate whether this name represents a unique ID or not. E.g. look for other instances of this name in your own data via the --nameregex option, or search by name at wigle.net.
Possible Unique ID: This device contains a name "5AAA=mS*+6!cs3EeDur@c;lzAqfF9" found via Bluetooth Low Energy Advertisements. The name itself does not match a known-unique-ID pattern, but that could just mean it has not been captured in our metadata yet.
It is left to the user to investigate whether this name represents a unique ID or not. E.g. look for other instances of this name in your own data via the --nameregex option, or search by name at wigle.net.
Possible Unique ID: This device contains a name "5AAA=mS*+6!cs3EeDvi@BjcyAqfFP" found via Bluetooth Low Energy Advertisements. The name itself does not match a known-unique-ID pattern, but that could just mean it has not been captured in our metadata yet.
It is left to the user to investigate whether this name represents a unique ID or not. E.g. look for other instances of this name in your own data via the --nameregex option, or search by name at wigle.net.

```
    272fe162-6c6c-4718-a3d4-6de8a3735cff (Unknown
  Custom UUID128: company: Texas Instruments, name: (
  Begin Handle: 075, End Handle: 65535
  GATT Service Unknown! Handle does not match any Ser


BLE 2thprint Info:
  BLE LL Ctrl Opcode: 9 (LL_FEATURE_RSP)
    BLE LL Features: 0x0000000000000001
      * LE Encryption

L2CAP data found:
  L2CAP_CONNECTION_PARAMETER_UPDATE_REQ:
    Direction: Peripheral to Central
    Packet command/response association ID: 1
    Data Length: 8
    Requested minimum connection interval (in units
    Requested maximum connection interval (in units
    Requested Peripheral Latency (number of connecti
    Requested timeout (in units of 10ms): 600

  Unique ID / Potential Trackability Report:
    Unique ID: BDADDR is of type *Public*, which is not
    *Possible* Unique ID: This device contains a name
known-unique-ID pattern, but that could just mean it has
          It is left to the user to investigate wheth
--nameregex option, or search by name at wigle.net.
    *Possible* Unique ID: This device contains a name "5AAA=mS*+5cFH~EeDwVdjJ4SAqfF3" found via Bluetooth Low Energy Advertisements. The name itself does not match a
known-unique-ID pattern, but that could just mean it has not been captured in our metadata yet.
          It is left to the user to investigate whether this name represents a unique ID or not. E.g. look for other instances of this name in your own data via the
--nameregex option, or search by name at wigle.net.
    *Possible* Unique ID: This device contains a name "5AAA=mS*+6!cs3EeDt^@c;lzAqfF9" found via Bluetooth Low Energy Advertisements. The name itself does not match a
known-unique-ID pattern, but that could just mean it has not been captured in our metadata yet.
          It is left to the user to investigate whether this name represents a unique ID or not. E.g. look for other instances of this name in your own data via the
--nameregex option, or search by name at wigle.net.
    *Possible* Unique ID: This device contains a name "5AAA=mS*+6!cs3EeDtm@c;lzAqfF9" found via Bluetooth Low Energy Advertisements. The name itself does not match a
known-unique-ID pattern, but that could just mean it has not been captured in our metadata yet.
          It is left to the user to investigate whether this name represents a unique ID or not. E.g. look for other instances of this name in your own data via the
--nameregex option, or search by name at wigle.net.
    *Possible* Unique ID: This device contains a name "5AAA=mS*+6!cs3EeDuN@c;lzAqfF9" found via Bluetooth Low Energy Advertisements. The name itself does not match a
known-unique-ID pattern, but that could just mean it has not been captured in our metadata yet.
          It is left to the user to investigate whether this name represents a unique ID or not. E.g. look for other instances of this name in your own data via the
--nameregex option, or search by name at wigle.net.
    *Possible* Unique ID: This device contains a name "5AAA=mS*+6!cs3EeDur@c;lzAqfF9" found via Bluetooth Low Energy Advertisements. The name itself does not match a
known-unique-ID pattern, but that could just mean it has not been captured in our metadata yet.
          It is left to the user to investigate whether this name represents a unique ID or not. E.g. look for other instances of this name in your own data via the
--nameregex option, or search by name at wigle.net.
    *Possible* Unique ID: This device contains a name "5AAA=mS*+6!cs3EeDvi@BjcyAqfFP" found via Bluetooth Low Energy Advertisements. The name itself does not match a
known-unique-ID pattern, but that could just mean it has not been captured in our metadata yet.
          It is left to the user to investigate whether this name represents a unique ID or not. E.g. look for other instances of this name in your own data via the
--nameregex option, or search by name at wigle.net.
```

Case Study: OAD feature used by BLE chip embedded in Aruba Access Points - CVE-2018-7080

Aruba Networks (today part of HP Enterprise) is one of the first vendors to add built-in BLE features to their enterprise wireless solution. Initially, Aruba manufactured two types of BLE beacon devices: a stand-alone beacon and a BLE USB dongle that can be added to existing Aruba access points (mainly from series 2xx). These devices were used to enable BLE based location-services. A couple of years later, Aruba integrated the BLE beacons directly into their access points. All access points from series 3xx have a built in BLE chip - TI's CC2540.

https://media.armis.com/PDFs/wp-bleedingbit-ble-chips-en.pdf

```
  2803 (Declaration: Characteristic), Attribute Handle: 012
    2a24 (Characteristic Value: Model Number String), Attribute Handle: 013
    GATT Characteristic Value read as b'LS-BT20'
  2803 (Declaration: Characteristic), Attribute Handle: 014
    2a25 (Characteristic Value: Serial Number String), Attribute Handle: 015
    GATT Characteristic Value read as b'aruba-98072df35bf4'
  2803 (Declaration: Characteristic), Attribute Handle: 016
    2a27 (Characteristic Value: Hardware Revision String), Attribute Handle: 017
    GATT Characteristic Value read as b'1 050617'
  2803 (Declaration: Characteristic), Attribute Handle: 018
    2a28 (Characteristic Value: Software Revision String), Attribute Handle: 019
    GATT Characteristic Value read as b'OAD-E 1.2-9'
  2803 (Declaration: Characteristic), Attribute Handle: 020
    2a29 (Characteristic Value: Manufacturer Name String), Attribute Handle: 021
    GATT Characteristic Value read as b'HPE Aruba'
Service: Battery 180f:
Begin Handle: 022, End Handle: 027
  2800 (Declaration: Primary Service), Attribute Handle: 022
  2803 (Declaration: Characteristic), Attribute Handle: 023
    2a19 (Characteristic Value: Battery Level), Attribute Handle: 024
    GATT Characteristic Value read as b'd'
    2902 (Descriptor: Client Characteristic Configuration), Attribute Handle: 025
    2908 (Descriptor: Report Reference), Attribute Handle: 026
    2904 (Descriptor: Characteristic Presentation Format), Attribute Handle: 027
Unknown UUID128 272fe150-6c6c-4718-a3d4-6de8a3735cff:
Begin Handle: 028, End Handle: 074
  2800 (Declaration: Primary Service), Attribute Handle: 028
  2803 (Declaration: Characteristic), Attribute Handle: 029
    272fe151-6c6c-4718-a3d4-6de8a3735cff (Unknown UUID128), Attribute Handle: 030
    GATT Characteristic Value read as b'\xa4\x9e/HS\x96E\x86\x80?\xe6\xc9\x14\t\x80\xf7'
  2803 (Declaration: Characteristic), Attribute Handle: 031
    272fe152-6c6c-4718-a3d4-6de8a3735cff (Unknown UUID128), Attribute Handle: 032
    GATT Characteristic Value read as b'\xe8\x03'
  2803 (Declaration: Characteristic), Attribute Handle: 033
    272fe153-6c6c-4718-a3d4-6de8a3735cff (Unknown UUID128), Attribute Handle: 034
    GATT Characteristic Value read as b'U\x05'
  2803 (Declaration: Characteristic), Attribute Handle: 035
    272fe154-6c6c-4718-a3d4-6de8a3735cff (Unknown UUID128), Attribute Handle: 036
    GATT Characteristic Value read as b'\xc4'
  2803 (Declaration: Characteristic), Attribute Handle: 037
    272fe155-6c6c-4718-a3d4-6de8a3735cff (Unknown UUID128), Attribute Handle: 038
    GATT Characteristic Value read as b'\x0e'
  2803 (Declaration: Characteristic), Attribute Handle: 039
    272fe157-6c6c-4718-a3d4-6de8a3735cff (Unknown UUID128), Attribute Handle: 040
  2803 (Declaration: Characteristic), Attribute Handle: 041
    272fe158-6c6c-4718-a3d4-6de8a3735cff (Unknown UUID128), Attribute Handle: 042
  2803 (Declaration: Characteristic), Attribute Handle: 043
    272fe159-6c6c-4718-a3d4-6de8a3735cff (Unknown UUID128), Attribute Handle: 044
    GATT Characteristic Value read as b'\xf4\x01'
  2803 (Declaration: Characteristic), Attribute Handle: 045
    272fe15e-6c6c-4718-a3d4-6de8a3735cff (Unknown UUID128), Attribute Handle: 046
    GATT Characteristic Value read as b'\x07'
```

https://cert.europa.eu/publications/security-advisories/2018-028/pdf

Affected Access Points

- AP-3xx and IAP-3xx series access points
- AP-203R
- AP-203RP
- ArubaOS 6.4.4.x prior to 6.4.4.20
- ArubaOS 6.5.3.x prior to 6.5.3.9

- ArubaOS 6.5.4.x prior to 6.5.4.9
- ArubaOS 8.x prior to 8.2.2.2
- ArubaOS 8.3.x prior to 8.3.0.4

```
  2803 (Declaration: Characteristic), Attribute Handle: 012
    2a24 (Characteristic Value: Model Number String), Attribute Handle: 013
    GATT Characteristic Value read as b'LS-BT20'
  2803 (Declaration: Characteristic), Attribute Handle: 014
    2a25 (Characteristic Value: Serial Number String), Attribute Handle: 015
    GATT Characteristic Value read as b'aruba-98072df35bf4'
  2803 (Declaration: Characteristic), Attribute Handle: 016
    2a27 (Characteristic Value: Hardware Revision String), Attribute Handle: 017
    GATT Characteristic Value read as b'1 050617'
  2803 (Declaration: Characteristic), Attribute Handle: 018
    2a28 (Characteristic Value: Software Revision String), Attribute Handle: 019
    GATT Characteristic Value read as b'OAD-E 1.2-9'
  2803 (Declaration: Characteristic), Attribute Handle: 020
    2a29 (Characteristic Value: Manufacturer Name String), Attribute Handle: 021
    GATT Characteristic Value read as b'HPE Aruba'
Service: Battery 180f:
Begin Handle: 022, End Handle: 027
  2800 (Declaration: Primary Service), Attribute Handle: 022
  2803 (Declaration: Characteristic), Attribute Handle: 023
    2a19 (Characteristic Value: Battery Level), Attribute Handle: 024
    GATT Characteristic Value read as b'd'
    2902 (Descriptor: Client Characteristic Configuration), Attribute Handle: 025
    2908 (Descriptor: Report Reference), Attribute Handle: 026
    2904 (Descriptor: Characteristic Presentation Format), Attribute Handle: 027
Unknown UUID128 272fe150-6c6c-4718-a3d4-6de8a3735cff:
Begin Handle: 028, End Handle: 074
  2800 (Declaration: Primary Service), Attribute Handle: 028
  2803 (Declaration: Characteristic), Attribute Handle: 029
    272fe151-6c6c-4718-a3d4-6de8a3735cff (Unknown UUID128), Attribute Handle: 030
    GATT Characteristic Value read as b'\xa4\x9e/HS\x96E\x86\x80?\xe6\xc9\x14\t\x80\xf7'
  2803 (Declaration: Characteristic), Attribute Handle: 031
    272fe152-6c6c-4718-a3d4-6de8a3735cff (Unknown UUID128), Attribute Handle: 032
    GATT Characteristic Value read as b'\xe8\x03'
  2803 (Declaration: Characteristic), Attribute Handle: 033
    272fe153-6c6c-4718-a3d4-6de8a3735cff (Unknown UUID128), Attribute Handle: 034
    GATT Characteristic Value read as b'U\x05'
  2803 (Declaration: Characteristic), Attribute Handle: 035
    272fe154-6c6c-4718-a3d4-6de8a3735cff (Unknown UUID128), Attribute Handle: 036
    GATT Characteristic Value read as b'\xc4'
  2803 (Declaration: Characteristic), Attribute Handle: 037
    272fe155-6c6c-4718-a3d4-6de8a3735cff (Unknown UUID128), Attribute Handle: 038
    GATT Characteristic Value read as b'\x0e'
  2803 (Declaration: Characteristic), Attribute Handle: 039
    272fe157-6c6c-4718-a3d4-6de8a3735cff (Unknown UUID128), Attribute Handle: 040
  2803 (Declaration: Characteristic), Attribute Handle: 041
    272fe158-6c6c-4718-a3d4-6de8a3735cff (Unknown UUID128), Attribute Handle: 042
  2803 (Declaration: Characteristic), Attribute Handle: 043
    272fe159-6c6c-4718-a3d4-6de8a3735cff (Unknown UUID128), Attribute Handle: 044
    GATT Characteristic Value read as b'\xf4\x01'
  2803 (Declaration: Characteristic), Attribute Handle: 045
    272fe15e-6c6c-4718-a3d4-6de8a3735cff (Unknown UUID128), Attribute Handle: 046
    GATT Characteristic Value read as b'\x07'
```

https://cert.europa.eu/publications/security-advisories/2018-028/pdf

Affected Access Points

- AP-3xx and IAP-3xx series access points
- AP-203R
- AP-203RP
- ArubaOS 6.4.4.x prior to 6.4.4.20
- ArubaOS 6.5.3.x prior to 6.5.3.9

- ArubaOS 6.5.4.x prior to 6.5.4.9
- ArubaOS 8.x prior to 8.2.2.2
- ArubaOS 8.3.x prior to 8.3.0.4

CLUES

Custom Lightweight UUID Exchange System

```
# From assigned_numbers/uuids/member_uuids.yaml
uuids:
 - uuid: 0xFEFF
   name: GN Netcom
 - uuid: 0xFEFE
   name: GN Hearing A/S
 - uuid: 0xFEFD
   name: "Gimbal, Inc."
 - uuid: 0xFEFC
   name: "Gimbal, Inc."
 - uuid: 0xFEFB
   name: Telit Wireless Solutions (Formerly Stollmann E+V GmbH)
 - uuid: 0xFEFA
   name: "PayPal, Inc."
 - uuid: 0xFEF9
   name: "PayPal, Inc."
 - uuid: 0xFEF8
...
   name: Tencent Holdings Limited.
 - uuid: 0xFEE6
   name: "Silvair, Inc."
 - uuid: 0xFEE5
   name: Nordic Semiconductor ASA
 - uuid: 0xFEE4
   name: Nordic Semiconductor ASA
 - uuid: 0xFEE3
...
```

CLUES

Custom Lightweight UUID Exchange System

- A word about company-reserved UUIDs (in the range 0xFEFF-0xFC60 at the date of writing, but continuously being added at lower values)

```
# From assigned_numbers/uuids/member_uuids.yaml
uuids:
 - uuid: 0xFEFF
   name: GN Netcom
 - uuid: 0xFEFE
   name: GN Hearing A/S
 - uuid: 0xFEFD
   name: "Gimbal, Inc."
 - uuid: 0xFEFC
   name: "Gimbal, Inc."
 - uuid: 0xFEFB
   name: Telit Wireless Solutions (Formerly Stollmann E+V GmbH)
 - uuid: 0xFEFA
   name: "PayPal, Inc."
 - uuid: 0xFEF9
   name: "PayPal, Inc."
 - uuid: 0xFEF8
...
   name: Tencent Holdings Limited.
 - uuid: 0xFEE6
   name: "Silvair, Inc."
 - uuid: 0xFEE5
   name: Nordic Semiconductor ASA
 - uuid: 0xFEE4
   name: Nordic Semiconductor ASA
 - uuid: 0xFEE3
...
```

CLUES

Custom Lightweight UUID Exchange System

- A word about company-reserved UUIDs (in the range 0xFEFF-0xFC60 at the date of writing, but continuously being added at lower values)

- For these UUIDs we know which company they're associated with (so I can cross-correlate with my silicon vendor list), but we don't know what they're used for!

```
# From assigned_numbers/uuids/member_uuids.yaml
uuids:
 - uuid: 0xFEFF
   name: GN Netcom
 - uuid: 0xFEFE
   name: GN Hearing A/S
 - uuid: 0xFEFD
   name: "Gimbal, Inc."
 - uuid: 0xFEFC
   name: "Gimbal, Inc."
 - uuid: 0xFEFB
   name: Telit Wireless Solutions (Formerly Stollmann E+V GmbH)
 - uuid: 0xFEFA
   name: "PayPal, Inc."
 - uuid: 0xFEF9
   name: "PayPal, Inc."
 - uuid: 0xFEF8
...
   name: Tencent Holdings Limited.
 - uuid: 0xFEE6
   name: "Silvair, Inc."
 - uuid: 0xFEE5
   name: Nordic Semiconductor ASA
 - uuid: 0xFEE4
   name: Nordic Semiconductor ASA
 - uuid: 0xFEE3
...
```

CLUES

Custom Lightweight UUID Exchange System


```
        "UUID": "fe03",
        "company": "Amazon",
        "UUID_purpose": "Alexa Gadgets (older) or Amazon Sidewalk (newer) allows devices to connect to Amazon Echo devices. 'The BLE GATT Alexa Gadgets Service is a custom service that manages Alexa Gadgets stream transactions.'",
        "UUID_name": "Alexa Mobile Accessories (AMA)",
...
        "UUID": "fe2c",
        "company": "Google",
        "UUID_purpose": "Fast Pair",
        "UUID_name": "Fast Pair",
...
        "UUID": "fe8d",
        "company": "Interaxon Inc.",
        "UUID_purpose": "Muse EEG Headset",
...
```

CLUES

Custom Lightweight UUID Exchange System

- CLUES helps us capture what's know about them.


```
        "UUID": "fe03",
        "company": "Amazon",
        "UUID_purpose": "Alexa Gadgets (older) or Amazon Sidewalk (newer) allows devices to connect to Amazon Echo devices. 'The BLE GATT Alexa Gadgets Service is a custom service that manages Alexa Gadgets stream transactions.'",
        "UUID_name": "Alexa Mobile Accessories (AMA)",
...
        "UUID": "fe2c",
        "company": "Google",
        "UUID_purpose": "Fast Pair",
        "UUID_name": "Fast Pair",
...
        "UUID": "fe8d",
        "company": "Interaxon Inc.",
        "UUID_purpose": "Muse EEG Headset",
...
```

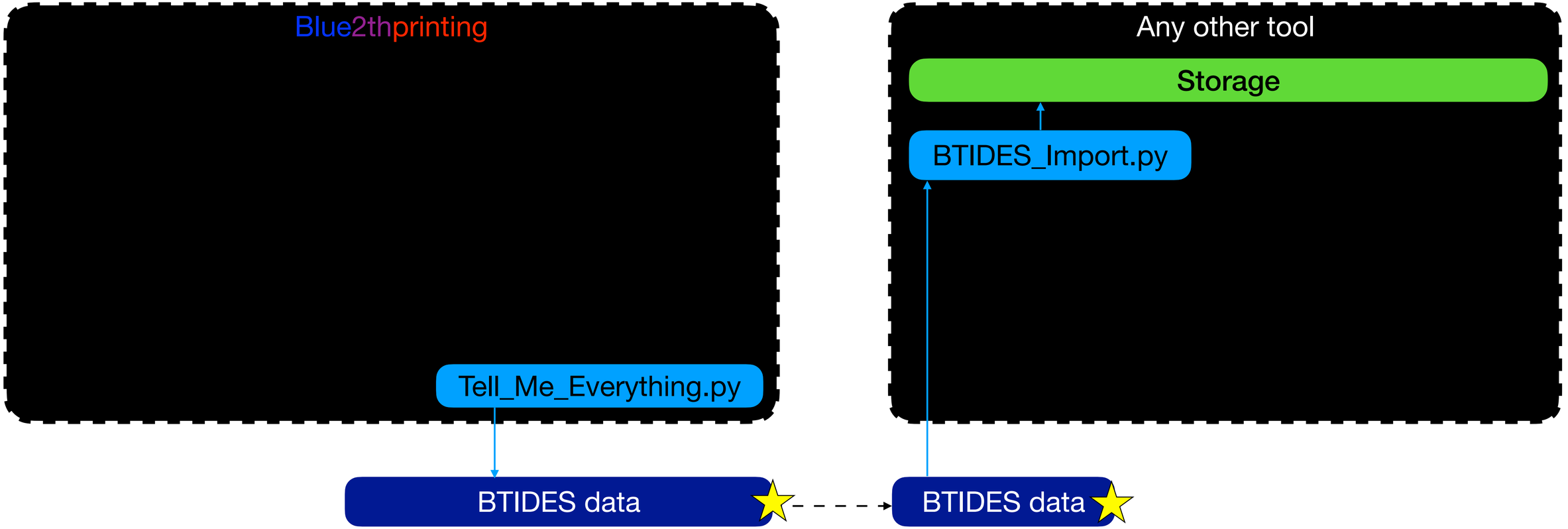
BTIDES

BlueTooth Information Data Exchange Schema

- JSON schema defining how to capture information about Bluetooth traffic and other metadata such as GATT Service/Characteristic hierarchy
  - Can collect a ***semantic superset*** of what's available in either over-the-air pcaps, or on-host HCI logs
  - Moves us from dangerous binary format parsing to JSON data that can be easily sanity checked against the BTIDES schema before processing

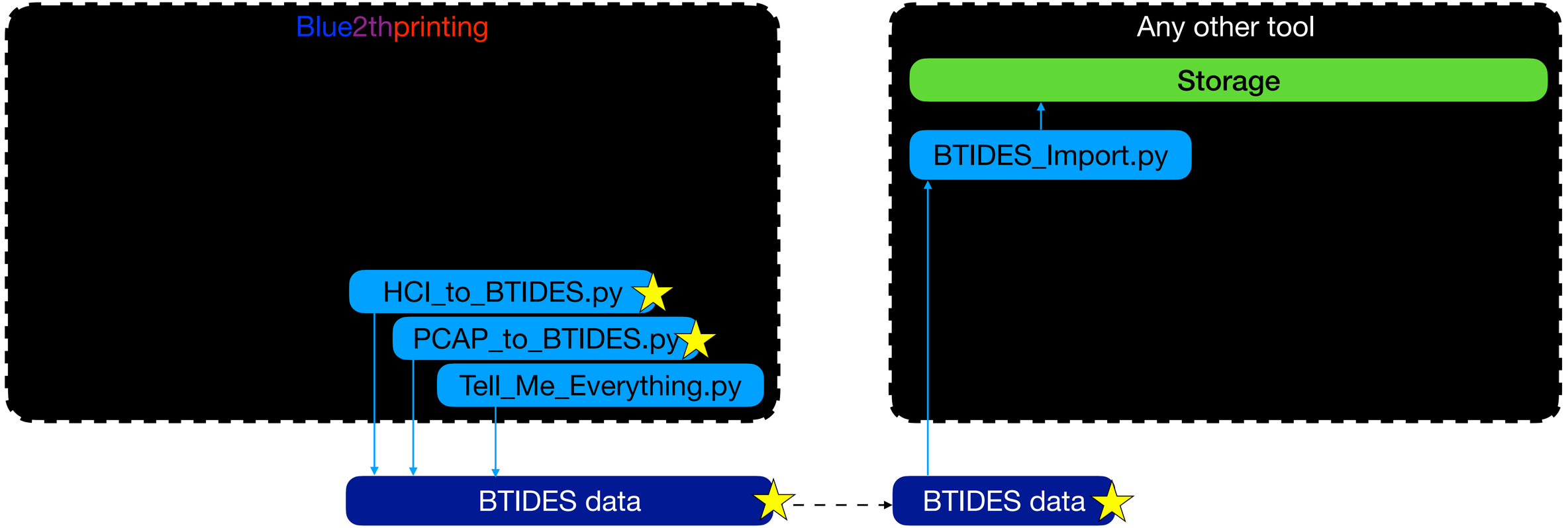
GOTO web schema viewer

P2P data sharing



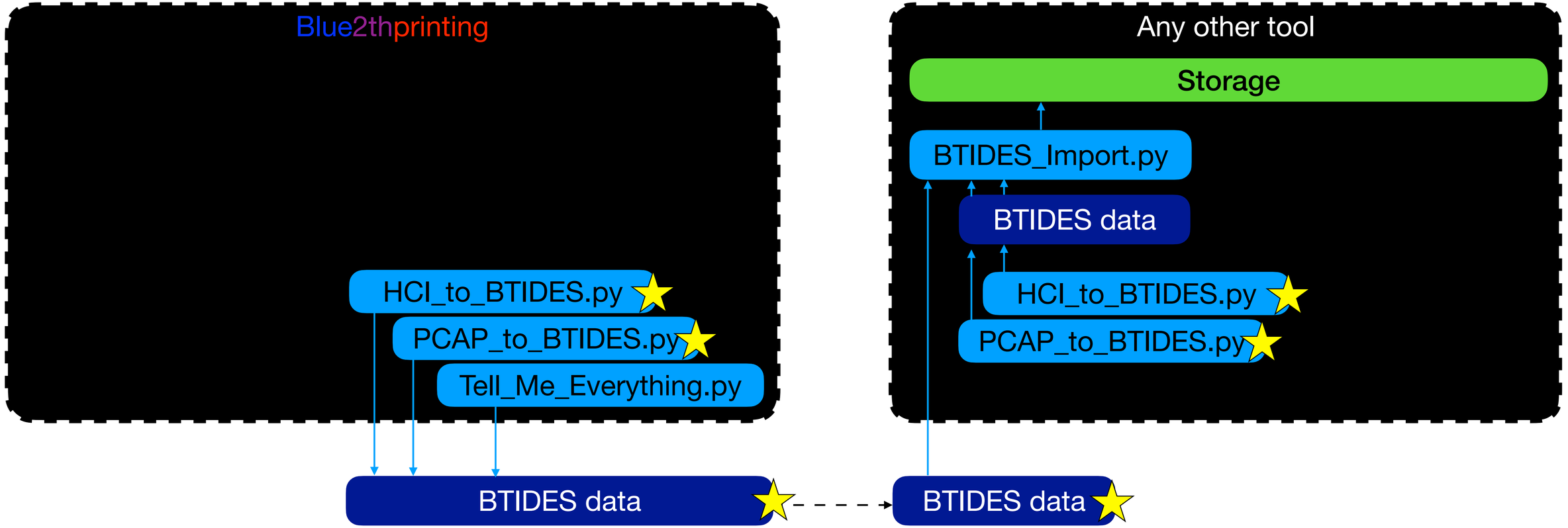
★ Reusable by others

P2P data sharing



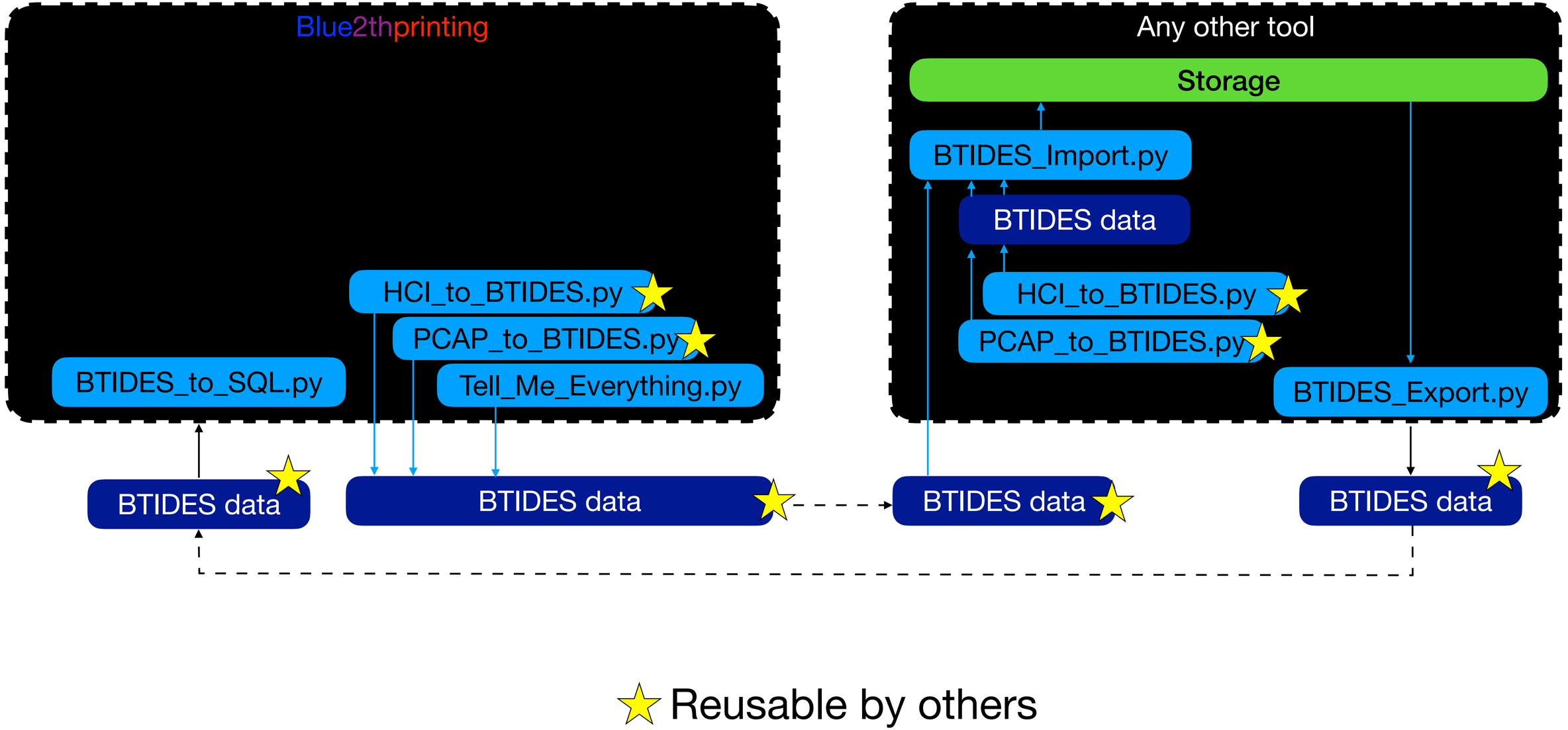
★ Reusable by others

P2P data sharing



★ Reusable by others

P2P data sharing



★ Reusable by others

BTIDALPOOL

Images from
https://en.wikipedia.org/wiki/Tide_pool
https://en.wikipedia.org/wiki/Moon

BTIDALPOOL

BTIDES-based server for crowdsourced data sharing

- Remote MySQL server for sending or retrieving data

BTIDALPOOL

BTIDES-based server for crowdsourced data sharing

- Remote MySQL server for sending or retrieving data
- Access-controlled via Google SSO (so I don't need to maintain any authentication database)
  - Create a throwaway gmail account and you're good to go

BTIDALPOOL

BTIDES-based server for crowdsourced data sharing

- Remote MySQL server for sending or retrieving data
- Access-controlled via Google SSO (so I don't need to maintain any authentication database)
  - Create a throwaway gmail account and you're good to go
- ***I've uploaded a bunch of data to let people explore even if they've never captured any data themselves!***
  - E.g. traffic from **DEF CON, Hardwear.io USA/NL, RingZer0, H2HC, Hack.lu, NoHat, SecTor, CanSecWest**, etc.
    - *And soon, DistrictCon ;)*

BTIDALPOOL quick start

Ubuntu 24.04 instructions

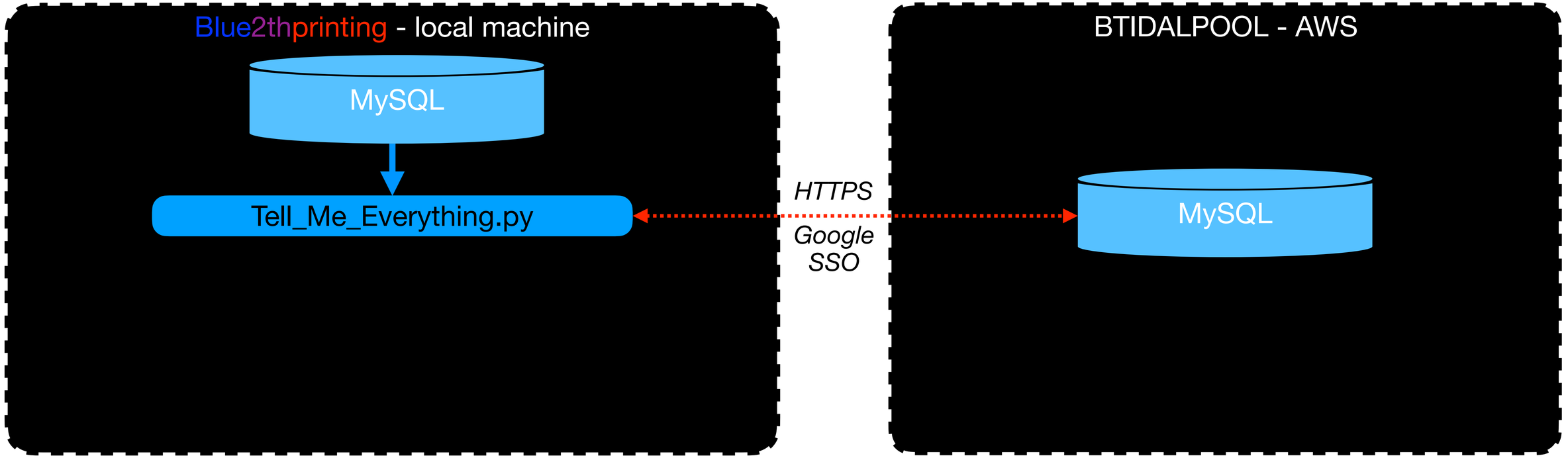
- git clone https://github.com/darkmentorllc/Blue2thprinting
- cd Blue2thprinting
- sudo ./setup_analysis_helper_debian-based.sh
- cd Analysis
- python3 ./Tell_Me_Everything.py **--query-BTIDALPOOL** --name-regex "Samsung"

GOTO live demo

- SHOW EXAMPLES

BTIDALPOOL - Blue2thprinting receive

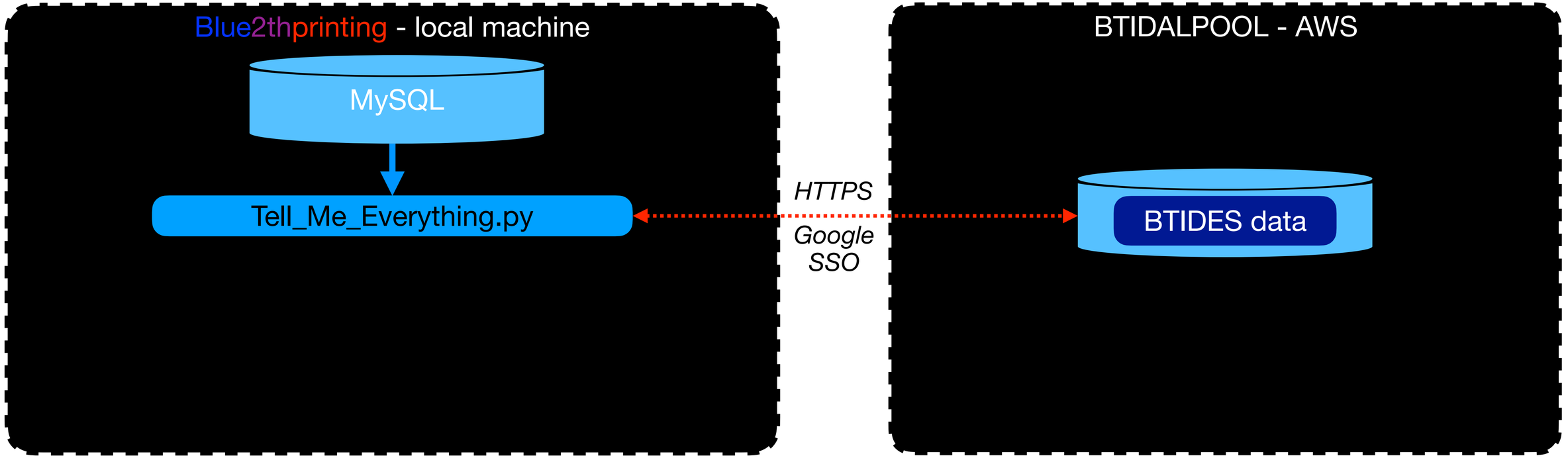
👋handwavy-don't-have-time-for-the-real-view version!👋



Just pass "--query-BTIDALPOOL"!

BTIDALPOOL - Blue2thprinting receive

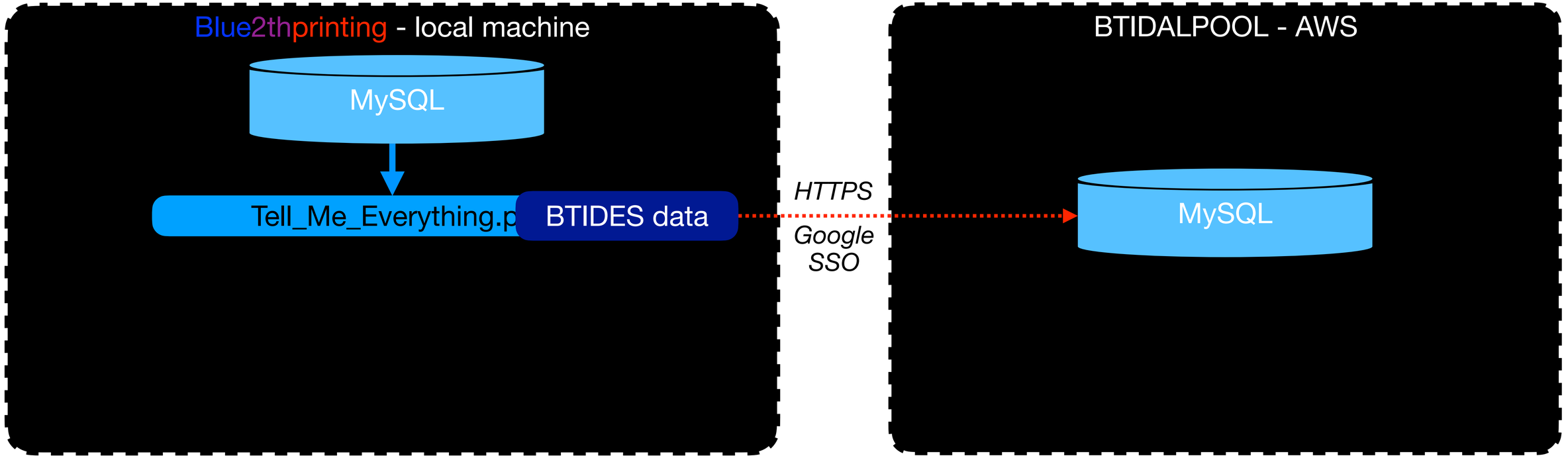
👋handwavy-don't-have-time-for-the-real-view version!👋



Just pass "--query-BTIDALPOOL"!

BTIDALPOOL - Blue2thprinting receive

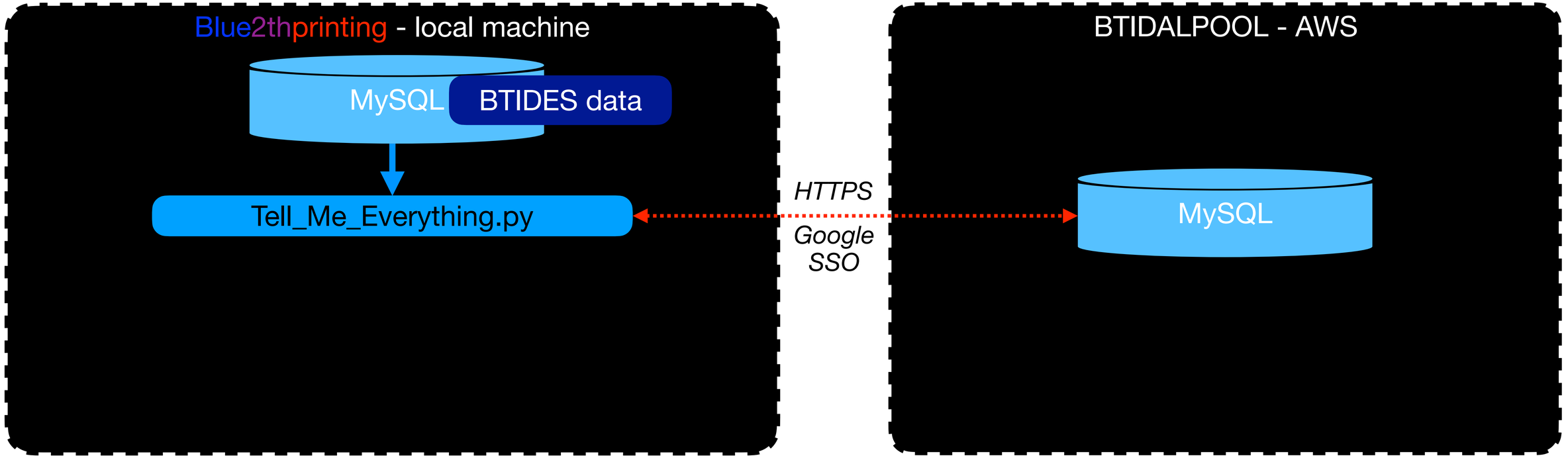
👋handwavy-don't-have-time-for-the-real-view version!👋



Just pass "--query-BTIDALPOOL"!

BTIDALPOOL - Blue2thprinting receive

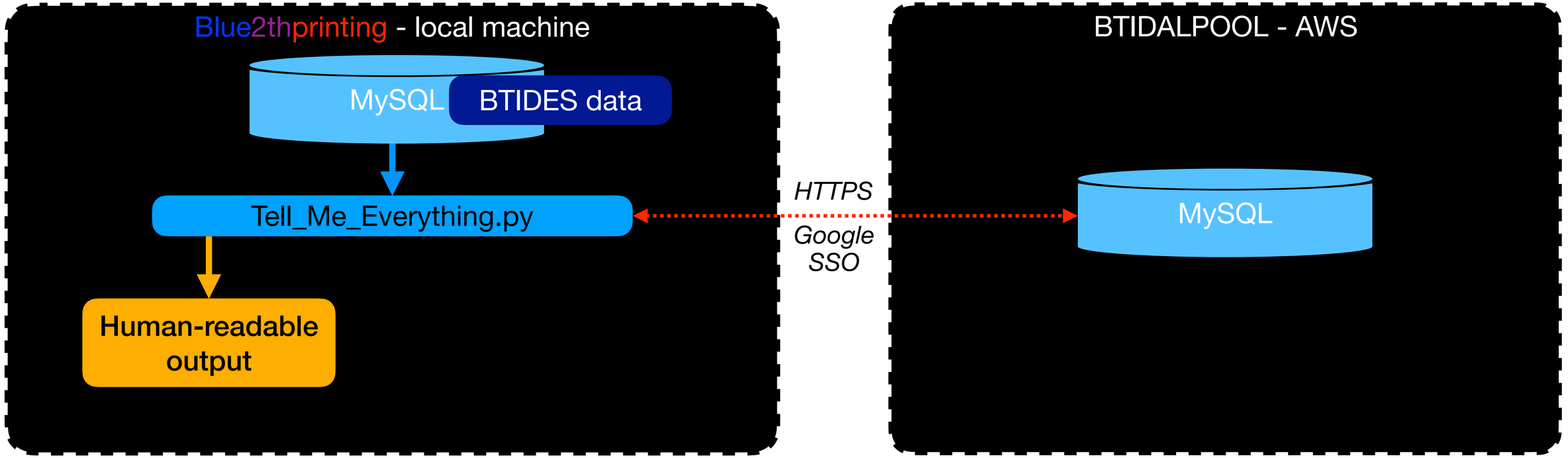
👋handwavy-don't-have-time-for-the-real-view version!👋



Just pass "--query-BTIDALPOOL"!

BTIDALPOOL - Blue2thprinting receive

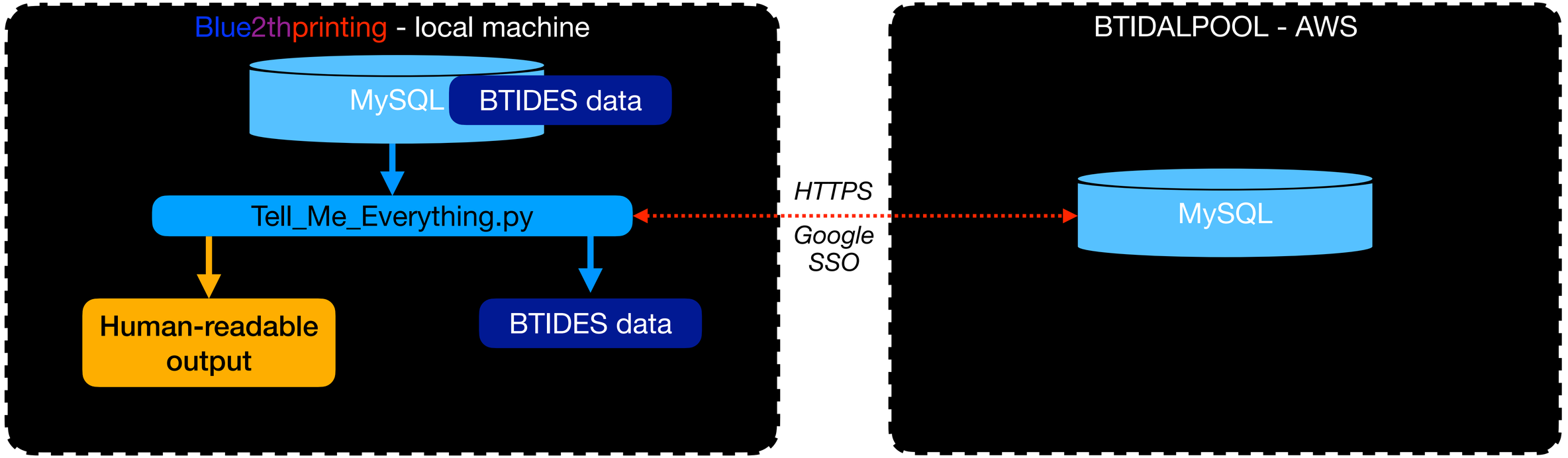
👋handwavy-don't-have-time-for-the-real-view version!👋



Just pass "--query-BTIDALPOOL"!

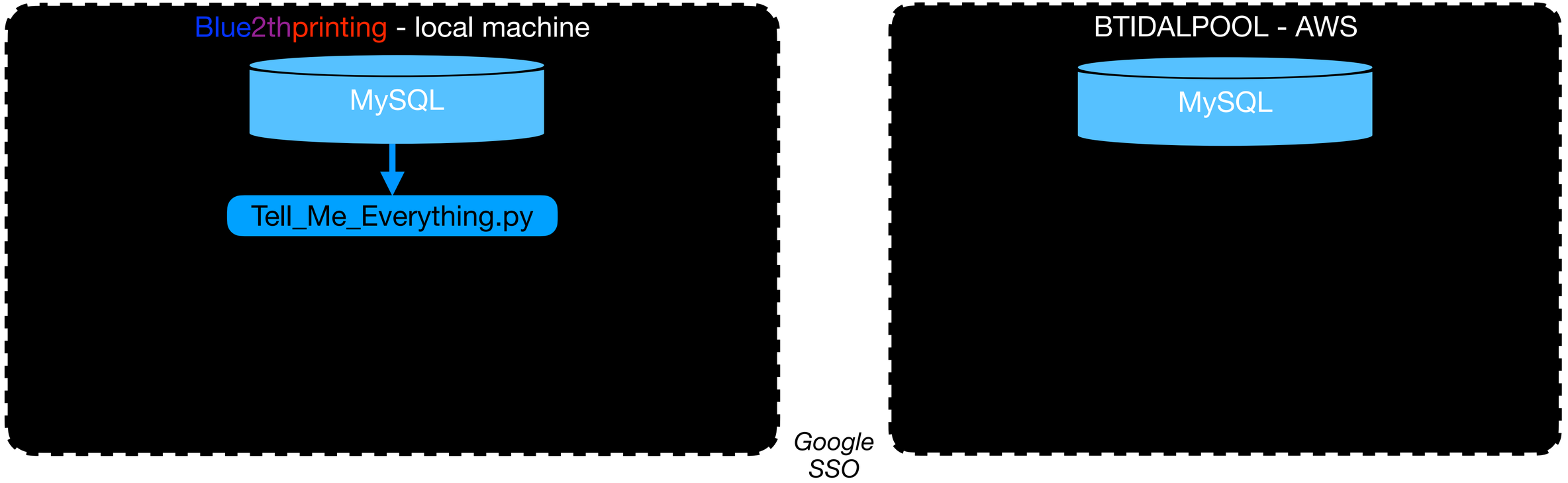
BTIDALPOOL - Blue2thprinting receive

👋handwavy-don't-have-time-for-the-real-view version!👋



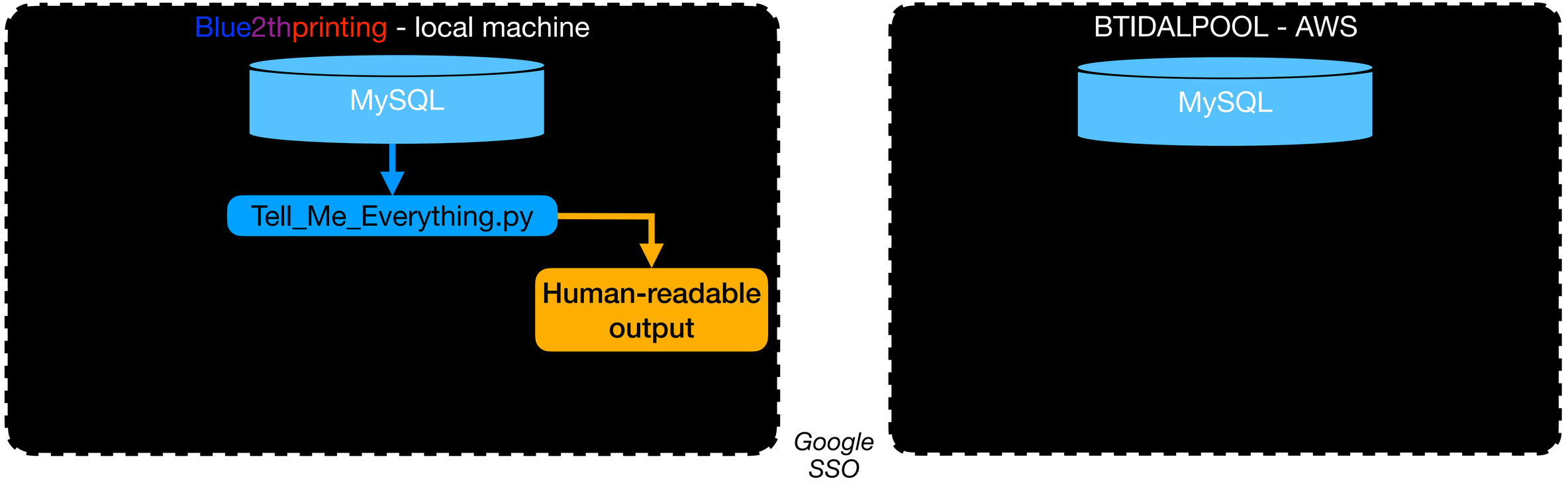
Just pass "--query-BTIDALPOOL"!

BTIDALPOOL - Blue2thprinting send



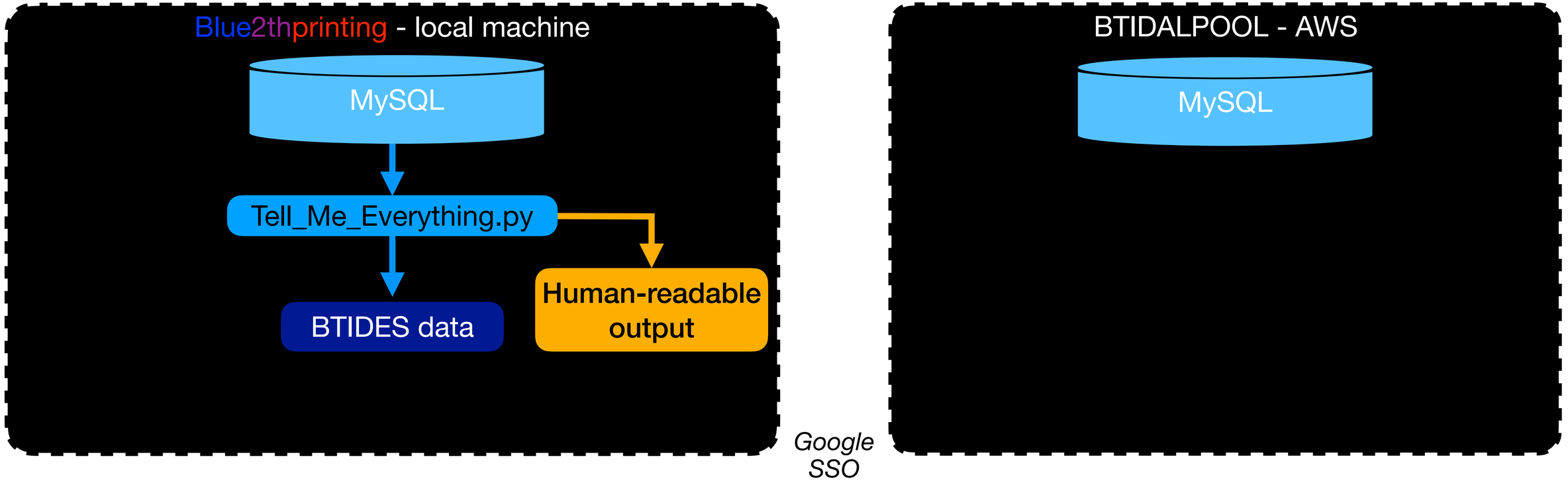
Just pass "--to-BTIDALPOOL"!

BTIDALPOOL - Blue2thprinting send



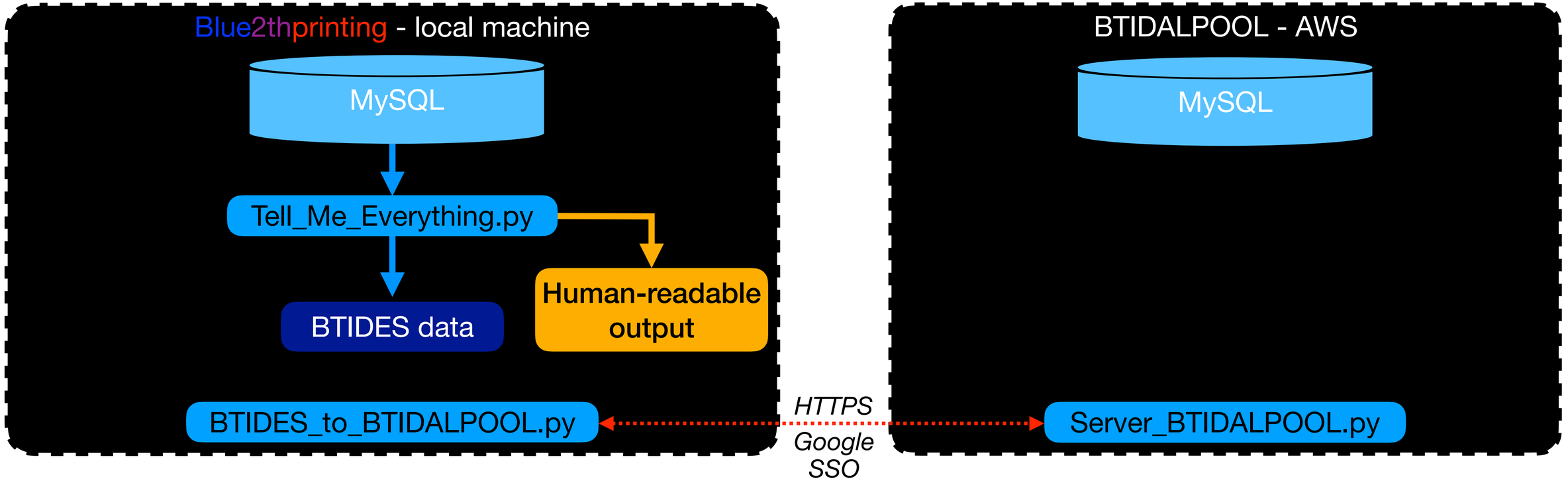
Just pass "--to-BTIDALPOOL"!

BTIDALPOOL - Blue2thprinting send



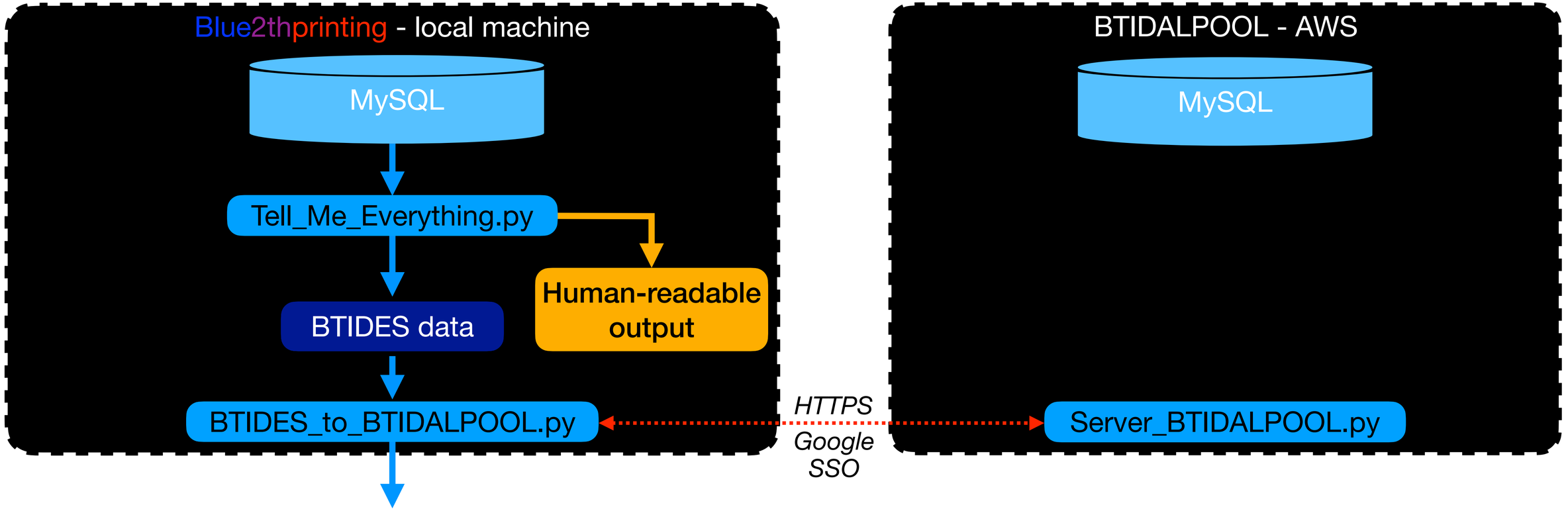
Just pass "--to-BTIDALPOOL"!

BTIDALPOOL - Blue2thprinting send



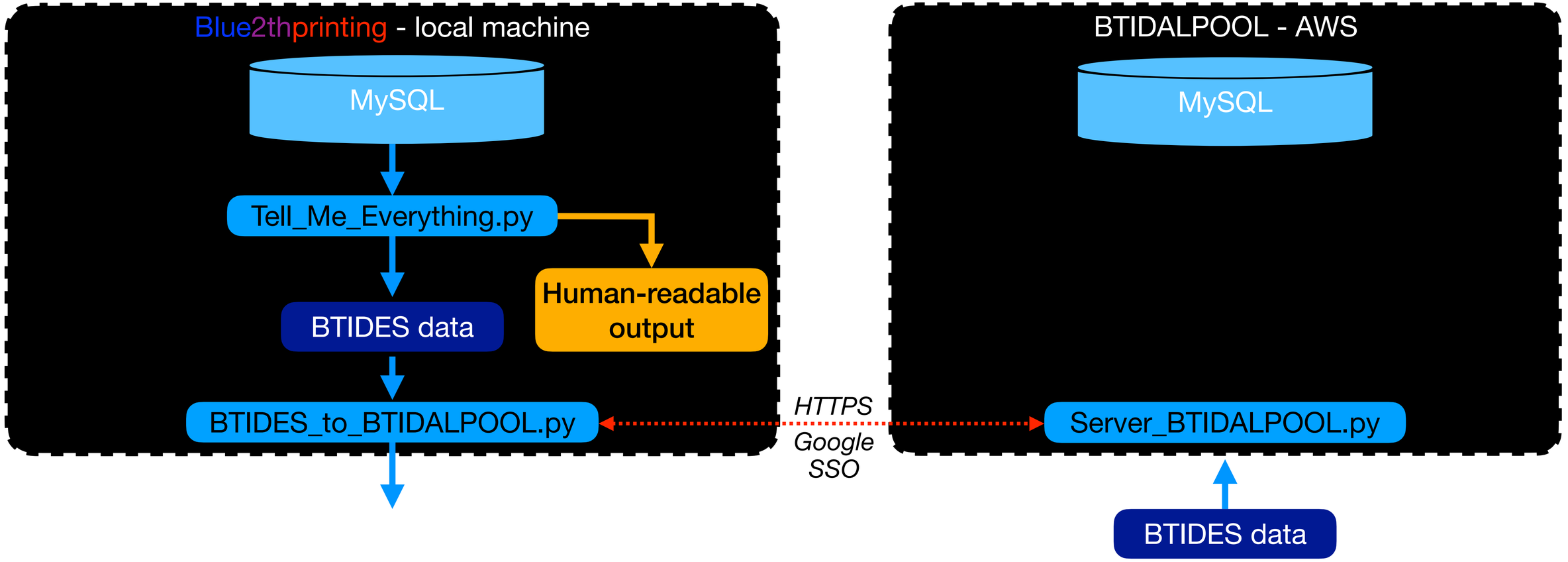
Just pass "--to-BTIDALPOOL"!

BTIDALPOOL - Blue2thprinting send



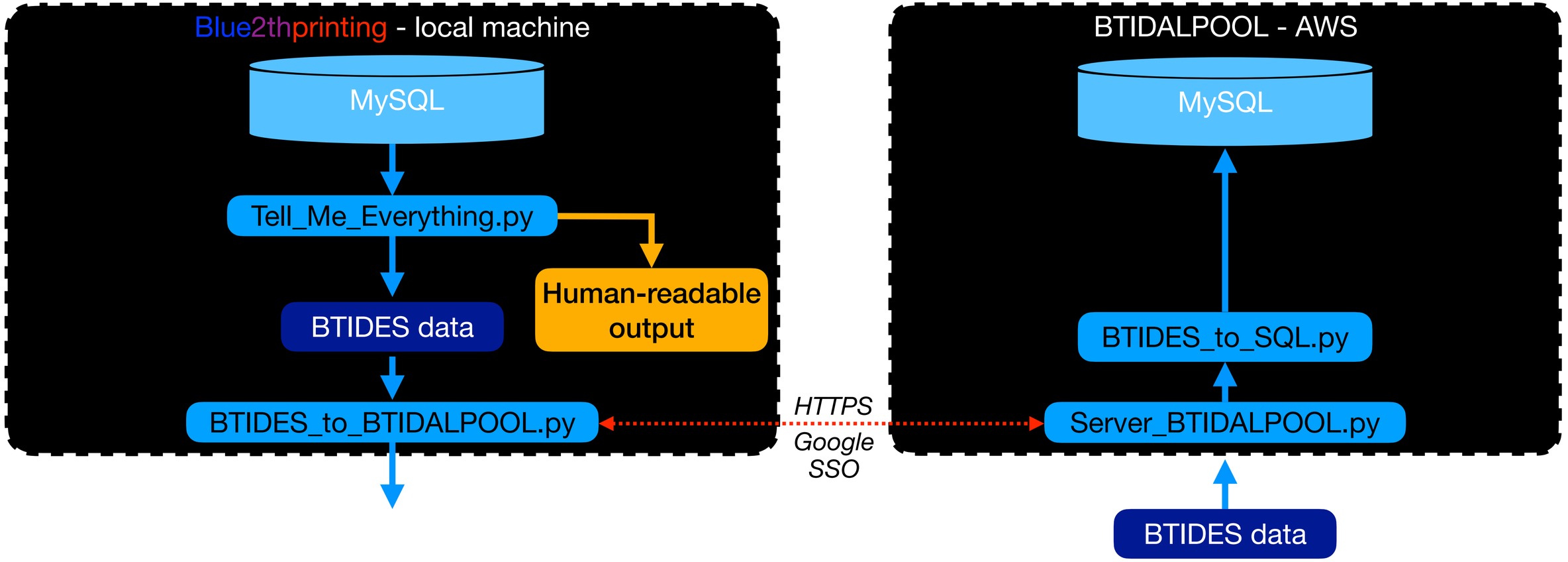
Just pass "--to-BTIDALPOOL"!

BTIDALPOOL - Blue2thprinting send



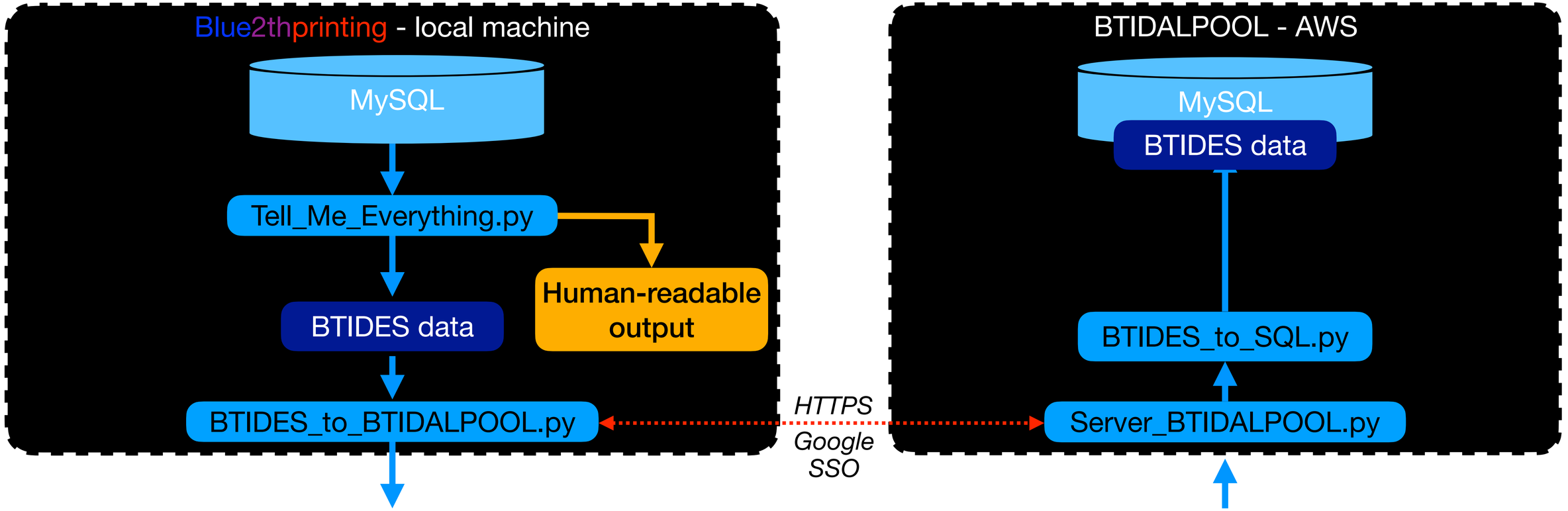
Just pass "--to-BTIDALPOOL"!

BTIDALPOOL - Blue2thprinting send



Just pass "--to-BTIDALPOOL"!

BTIDALPOOL - Blue2thprinting send



Just pass "--to-BTIDALPOOL"!

Why not just use WiGLE?

- The data necessary to capture BT data (BTIDES) is far more complex than the WiGLE db schema currently can accommodate
  - From sqlite export:

```
PRAGMA table_info(network);
0|bssid|TEXT|1||1
1|ssid|TEXT|1||0
2|frequency|INT|1||0
3|capabilities|TEXT|1||0
4|lasttime|long|1||0
5|lastlat|double|1||0
6|lastlon|double|1||0
7|type|TEXT|1|'W'|0
8|bestlevel|INTEGER|1|0|0
9|bestlat|double|1|0|0
10|bestlon|double|1|0|0
11|rcois|TEXT|1|''|0
12|mfgrid|INTEGER|1|0|0
13|service|TEXT|1|''|0
```

```
PRAGMA table_info(location);
0|_id|INTEGER|0||1
1|bssid|TEXT|1||0
2|level|INTEGER|1||0
3|lat|double|1||0
4|lon|double|1||0
5|altitude|double|1||0
6|accuracy|float|1||0
7|time|long|1||0
8|external|INTEGER|1|0|0
9|mfgrid|INTEGER|1|0|0
```

But we can at least *WIGLE_to_BTIDES.py*!

- I often use a phone running WiGLE to capture GPS data, because I find it gets a GPS lock faster than a Linux-compatible USB dongle
- BTIDES is good for converting subsets of the overall available data from tools into a standardized format (and making it clear what the subset is)

```
00:1d:a5:00:f9:57|Micro Mechanic|7936|
Uncategorized;10|1718377789000|
39.0943573639532|-77.1535686182564|B|-86|
25.7790127142375|-80.18755428307l1|0|
```


```
[
    {
        "bdaddr": "00:1d:a5:00:f9:57",
        "bdaddr_rand": 0,
        "HCIArray": [
            {
                "event_code": 7,
                "status": 0,
                "remote_name_hex_str": "4d6963726f204d656368616e6963",
                "event_code_str": "HCI_Remote_Name_Request_Complete",
                "utf8_name": "Micro Mechanic"
            }
        ],
        "GPSArray": [
            {
                "time": {
                    "unix_time_milli": 1718377789000
                },
                "lat": 25.779012714237457,
                "lon": -80.18755428307105
            }
        ]
    },
    {
        "bdaddr": "6c:17:f8:0e:45:46",
        "bdaddr_rand": 1,
        "GPSArray": [
            {
```


```
6c:17:f8:0e:45:46||7936|Misc|1716197115000|
25.0334084400852|121.563349744686|E|-86|
25.0334084400852|121.563349744686||0|
```

Conclusion:

All we know about Bluetooth is that we know nothing!

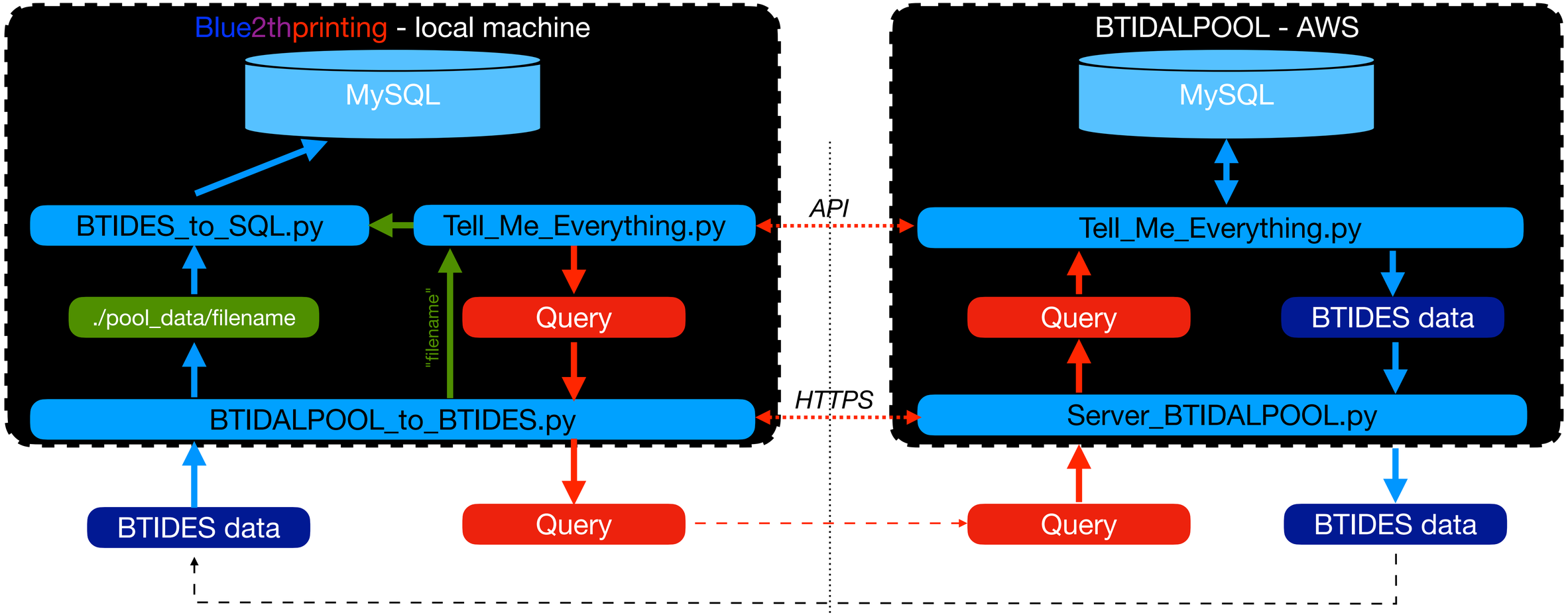
- We need to share more visibility from more devices around the world to bring us out of the dark ages
- You can play with Blue2thprinting & BTIDALPOOL today!
- Dark Mentor will be releasing 5 days of free trainings on BLE to OST2 later this year so more folks can become experts in this space
  - 1 day Blue2thprinting, 3 days BLE deep dive, 1 day BLE vuln hunting
  - Follow one of the below to know when the beta classes open up

https://www.linkedin.com/company/dark-mentor/
https://bsky.app/profile/darkmentor.com
https://infosec.exchange/@DarkMentor
https://twitter.com/DarkMentorLLC

https://www.linkedin.com/company/OST2
https://bsky.app/profile/OpenSecTraining
https://infosec.exchange/@OpenSecurityTraining2
https://twitter.com/OpenSecTraining

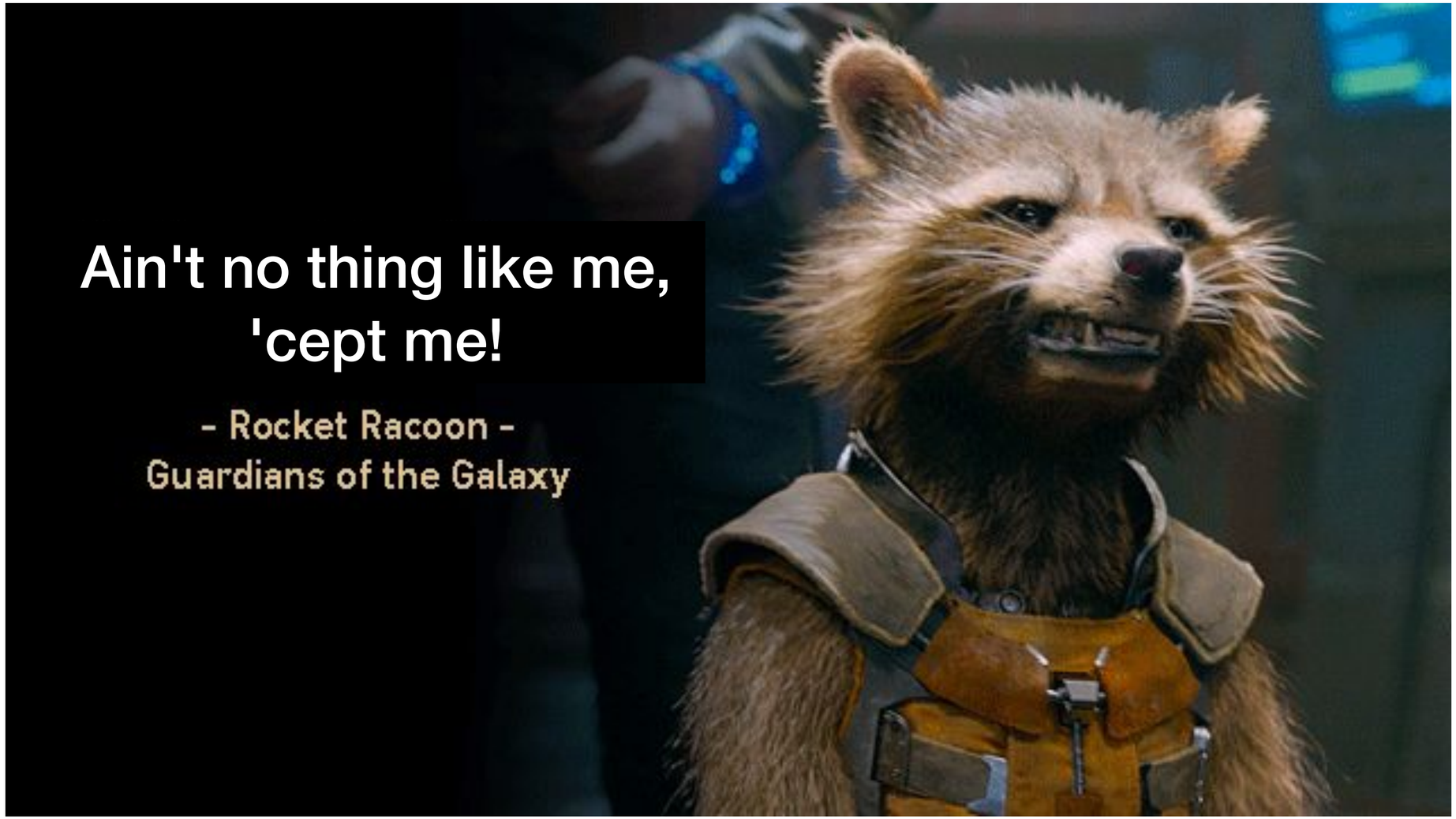
Backup

BTIDALPOOL - Blue2thprinting receive



Just pass "--query-BTIDALPOOL"!

Blue2thprinting vs. other tools?



Blue2thprinting vs. other tools?

Comparison to other tools

	BLE (spec version supported)	BC	Last update / Public release
Blue2thprinting https://github.com/darkmentorllc/Blue2thprinting	**5.2** (TI CC2652P)	✅	Jan 2025 / Nov 2023
Bluing https://github.com/fO-000/bluing	**4.2 + misc** (Linux BlueZ)	✅	Apr 2023 / Sept 2019
whad-client https://github.com/whad-team/whad-client/	**4.0** (custom stack)	❌	Jan 2025 / Aug 2024
RattaGATTa https://github.com/xen0bit/rattagatta	**5.0** (ESP32-S3)	❌	Sept 2024 / Jan 2024

Comparison - BC-specific

	Blue2thprinting (Multiple tools)	Bluing (BlueZ)
Device discovery (inquiry/extended inquiry)	✅	✅
Service Discovery Protocol (SDP)	✅	✅
Link Manager Protocol (LMP) active querying	✅	❌

Comparison - BC-specific

	Blue2thprinting (Multiple tools)	Bluing (BlueZ)
Device discovery (inquiry/extended inquiry)	✅	✅
Service Discovery Protocol (SDP)	✅	✅
Link Manager Protocol (LMP) active querying	✅	❌

Comparison - BC-specific

	Blue2thprinting (Multiple tools)	Bluing (BlueZ)
Device discovery (inquiry/extended inquiry)	✅	✅
Service Discovery Protocol (SDP)	✅	✅
Link Manager Protocol (LMP) active querying	✅	❌

https://asset-group.github.io/disclosures/braktooth/

Comparison - BLE-specific

	Blue2thprinting (Multiple tools)	Bluing (BlueZ)	WHAD (Custom)	RattaGATTa (NimBLE)
Machine-parsable output and/or database storage	✅	❌	✅	✅
Device discovery - legacy advertisement	✅	✅	✅	✅
Device discovery - extended advertisement	✅	✅	❌	❌
"Manufacturer-specific data" parsing	✅	❌	❌	❌
All-protocol pcap passive collection (with connection following)	✅	❌	✅	❌
Link Layer (LL) Protocol active collection	✅	❌	❌	❌
Security Manager Protocol (SMP) active collection	✅	❌	✅	❌
GATT Primary Services & Characteristics	✅	✅	✅	✅
GATT Secondary Services enumeration	✅	❌	✅	❌
"Characteristic User Description" descriptor reading	✅	❌	❌	✅
UUID lookup by CLUES	✅	❌	Planned	Planned

Comparison - BLE-specific

	Blue2thprinting (Multiple tools)	Bluing (BlueZ)	WHAD (Custom)	RattaGATTa (NimBLE)
Machine-parsable output and/or database storage	Custom ✅	❌	✅	✅
Device discovery - legacy advertisement	✅	 ✅	✅	✅
Device discovery - extended advertisement	✅	 ✅	❌	❌
"Manufacturer-specific data" parsing	Custom ✅	❌	❌	❌
All-protocol pcap passive collection (with connection following)	Sniffle ✅	❌	✅	❌
Link Layer (LL) Protocol active collection	Custom ✅	❌	❌	❌
Security Manager Protocol (SMP) active collection	Custom ✅	❌	✅	❌
GATT Primary Services & Characteristics	Custom ✅	 ✅	✅	✅
GATT Secondary Services enumeration	Custom ✅	❌	✅	❌
"Characteristic User Description" descriptor reading	Custom ✅	❌	❌	✅
UUID lookup by CLUES	CLUES ✅	❌	Planned	Planned