Taking D-Bus to Explore the Bluetooth Landscape

Paul A. Wortman, PhD
Mauddib28

August 7, 2024

Table of contents

Whoami

- PhD
- Bluetooth Security Researcher
- Research Scientist

Whatisthis?

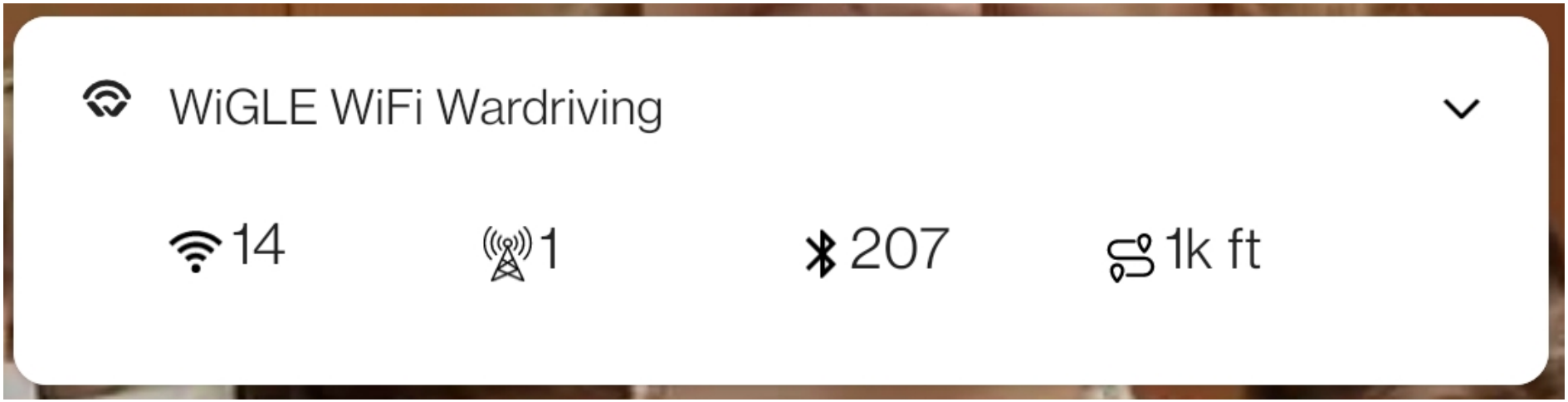


Figure 1: Wiggle War Drive - Landing Strip

“Lightning” Headphones That Require Bluetooth

Josh Whiton:

> A crazy experience — I lost my earbuds in a remote town in Chile, so tried buying a new pair at the airport before flying out. But the new wired, iPhone, lightning-cable headphones didn’t work. Strange.

But... Why?

- Surveying the Bluetooth Landscape
- Improve Bluetooth Wildlife Observation
- Augment Research Community Access to Bluetooth

BLE - Host Controller Interface

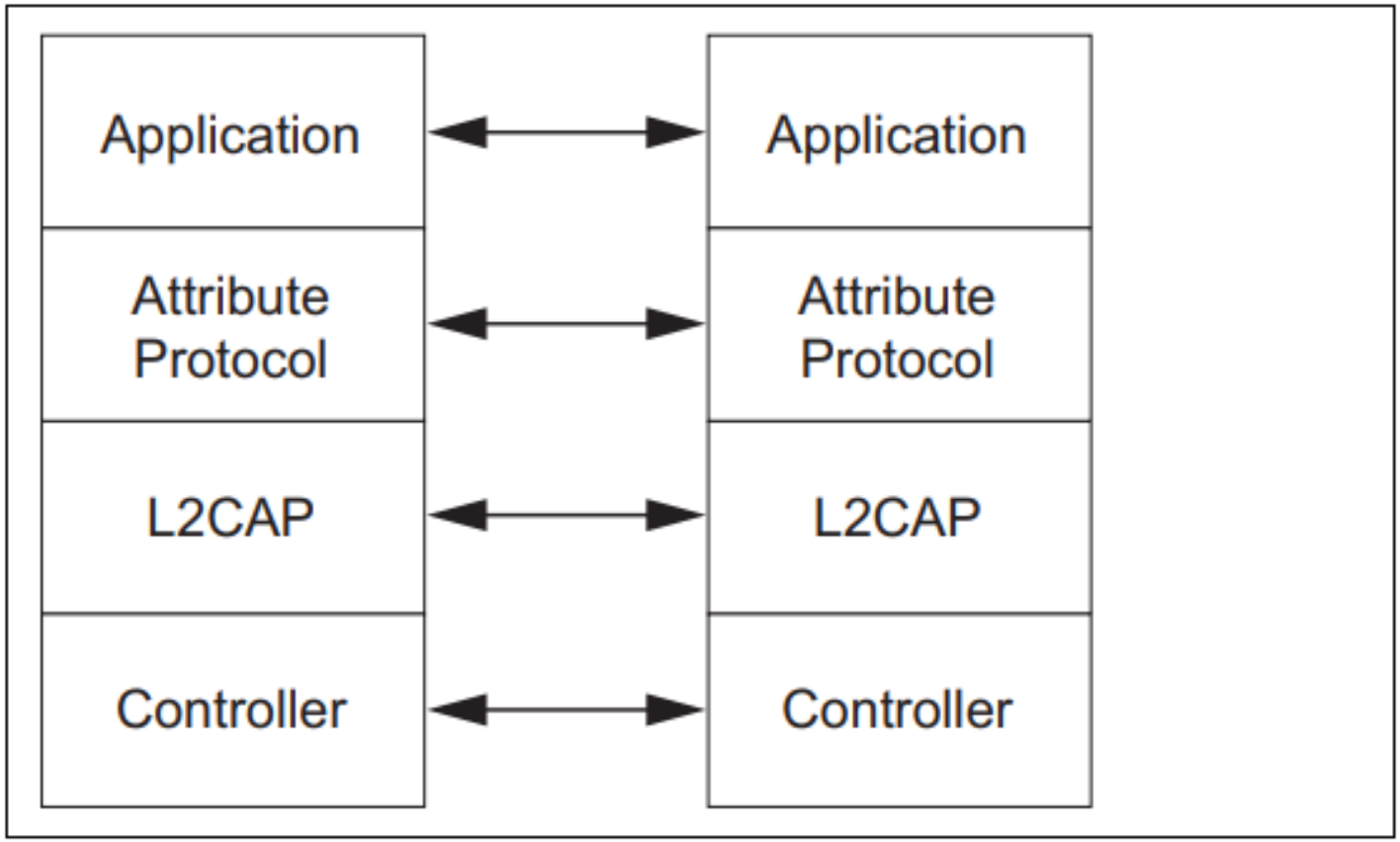


Figure 3: Protocol model [14]

- Everything goes through the HCI Layer; bottom most layer
  - HW-2-SW translation

BLE - Must Know Basics - High-level BLE Structure

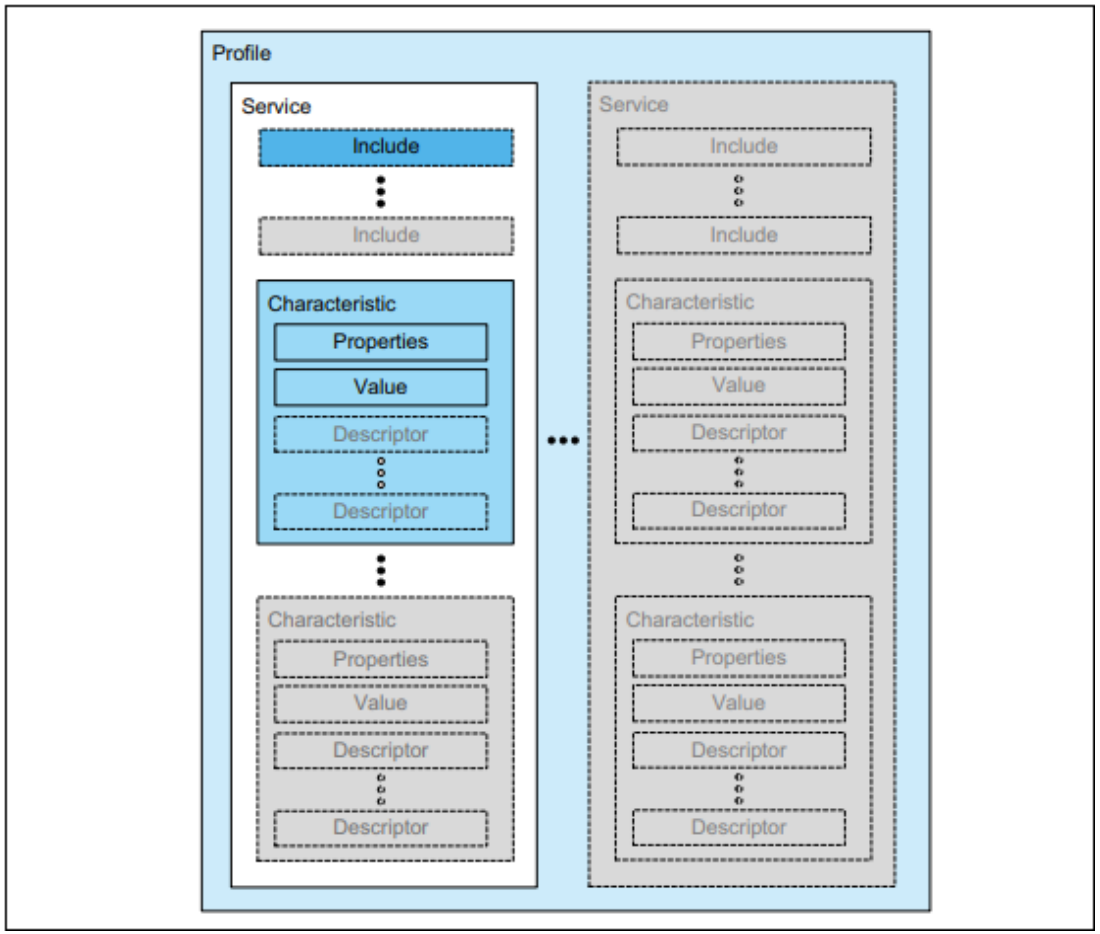


Figure 4: GATT-Based Profile hierarchy [14]

- Device, Services, Characteristics, Descriptors
- Characteristics have to be read once to populate data
  - Second read allows determining the data

What the BLEEP is this?

Bluetooth Landscape Exploration & Enumeration Platform
(B.L.E.E.P.)

Figure 5: The BLEEP-ing Logo

BLEEP Capabilities - Specifics

- Basics:
  - Discover and connect to Bluetooth (BLE) devices
  - Identify properties and services accurately
  - Read + Write I/O
    - Arbitrary and directed
  - Wrapped under User Interface
- Advanced:
  - Automation + Logging
  - Capturing Signals
  - Cartography of Landscape Features

State of the Code - Binoculars for Wildlife

Time for a BLEEP-ing Safari

Safari Goals:

- Learn what wildlife is out there
- Start documenting their aspects (e.g. shape, behavior)
- Locate the “weird ones”

Safari Time - Google Pixel - GAP

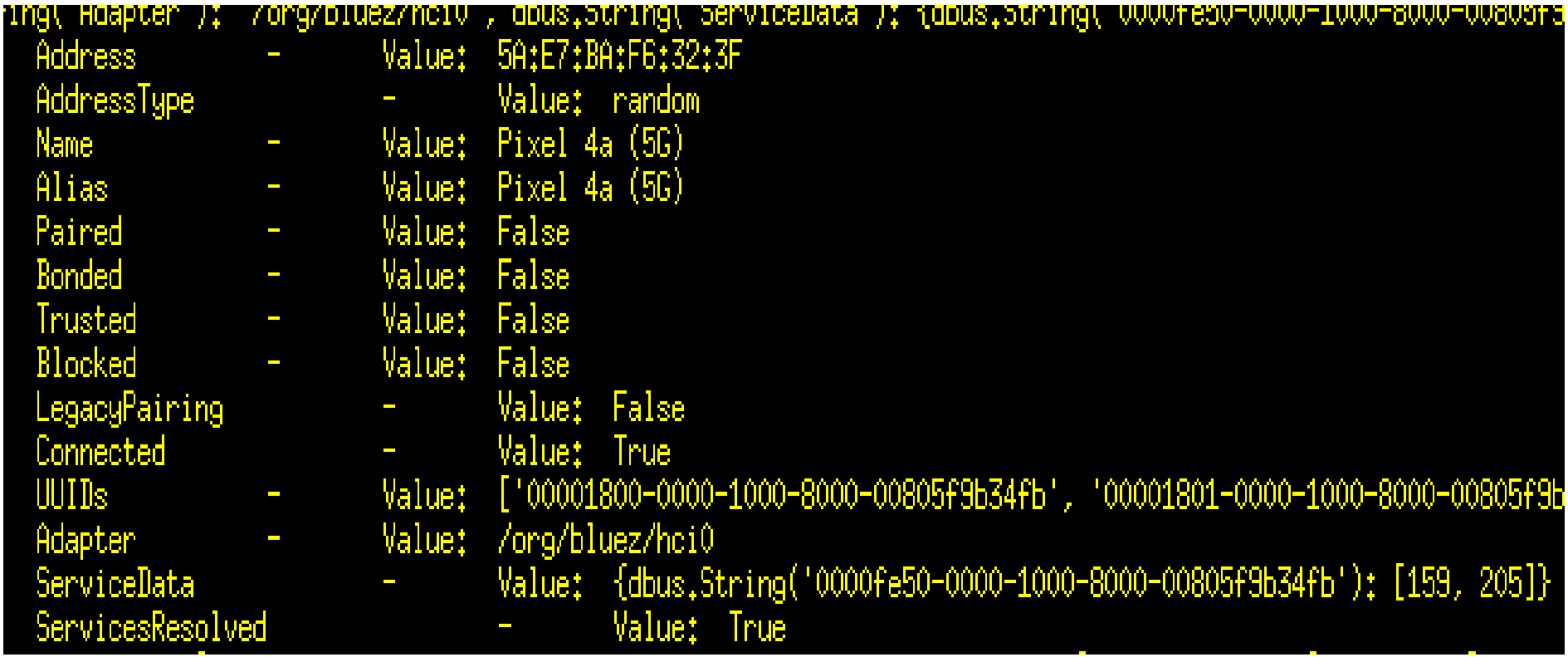


Figure 6: Safari Time - Pixel 4a

Safari Time - Google Pixel - Print Out

```
[+] BLE Class::Reconnect_check  -       Device [3A:E7:BA:F6:32:3F] is already connected
Service UUID:   00001801-0000-1000-8000-00805f9b34fb          -             Generic Attribute Service
       Characteristic UUID:    00002a05-0000-1000-8000-00805f9b34fb          -             Service Changed
       Characteristic Flags:   ['indicate']
       Characteristic UUID:    00002b3a-0000-1000-8000-00805f9b34fb          -             Unknown
       Characteristic Flags:   ['read']
       Characteristic Value (ASCii):
       Characteristic UUID:    00002b29-0000-1000-8000-00805f9b34fb          -             Unknown
       Characteristic Flags:   ['read', 'write']
       Characteristic Value (ASCii):
              [-] Writes not being attempted  -      Passive Scan
       Characteristic UUID:    00002b2a-0000-1000-8000-00805f9b34fb          -             Unknown
       Characteristic Flags:   ['read']
       Characteristic Value (ASCii):   b'\x89\x91\xc4b\xeb\xe9\xd9\x0b\x9e\xa0\xda>\x16\xd0\xf5\x13'
[*] User Interactive Exploration Tool - Select Action
```

Figure 7: Safari Time - Pixel 4a

Safari Time - Unknown Device with Manufacturer ID

```
Device  78:75:0E:7B:D0:99
        Properties:             {dbus.String('Address'): '78:75:0E:7B:D0:99', dbus.String('AddressType'): '
ocked'): False, dbus.String('LegacyPairing'): False, dbus.String('Connected'): True, dbus.String('UUIDs'):
', 'd0611e78-bbb4-4591-a5f8-487910ae4366'], dbus.String('Adapter'): '/org/bluez/hci0', dbus.String('Manufac
        Address         -       Value:  78:75:0E:7B:D0:99
        AddressType             -       Value:  random
        Alias           -       Value:  78-75-0E-7B-D0-99
        Paired          -       Value:  False
        Bonded          -       Value:  False
        Trusted         -       Value:  False
        Blocked         -       Value:  False
        LegacyPairing           -       Value:  False
        Connected               -       Value:  True
        UUIDs           -       Value:  ['00001800-0000-1000-8000-00805f9b34fb', '00001801-0000-1000-8000-0
        Adapter         -       Value:  /org/bluez/hci0
        ManufacturerData                -       Value:  {dbus.UInt16(76): [16, 5, 39, 152, 240, 110, 85]}
        ServicesResolved                -       Value:  True
```

Safari Time - Unknown Device - Print Out

```
[=] Warning! The generated Device Map will only be a skeleton of the target device. Reads have NOT been performed against the device yet...
Service UUID:   00001801-0000-1000-8000-00805f9b34fb          -          Generic Attribute Service          -          [service0006]
       Characteristic UUID:    00002a05-0000-1000-8000-00805f9b34fb          -          Service Changed          -          [char0007]
       Characteristic Flags:   ['indicate']
              Descriptor UUID:       00002902-0000-1000-8000-00805f9b34fb          -          Client Characteristic Configuration
              Descriptor Value:      []
Service UUID:   0000180a-0000-1000-8000-00805f9b34fb          -          Device Information Service          -          [service000a]
       Characteristic UUID:    00002a29-0000-1000-8000-00805f9b34fb          -          Unknown          -          [char000b]
       Characteristic Flags:   ['read']
       Characteristic Value (ASCii):   Apple Inc.
       Characteristic UUID:    00002a24-0000-1000-8000-00805f9b34fb          -          Model Number String          -          [char000d]
       Characteristic Flags:   ['read']
       Characteristic Value (ASCii):   Watch6,6
Service UUID:   d0611e78-bbb4-4591-a5f8-487910ae4366          -          Unknown          -          [service000f]
       Characteristic UUID:    8667556c-9a37-4c91-84ed-54ee27d90049          -          Unknown          -          [char0010]
       Characteristic Flags:   ['write', 'notify', 'extended-properties', 'reliable-write']
              [-] Writes not being attempted  -       Passive Scan
              Descriptor UUID:       00002900-0000-1000-8000-00805f9b34fb          -          Unknown          -          [desc0012]
              Descriptor Value:      [1, 0]
              Descriptor UUID:       00002902-0000-1000-8000-00805f9b34fb          -          Client Characteristic Configuration
              Descriptor Value:      []
Service UUID:   9fa480e0-4967-4542-9390-d343dc5d04ae          -          Unknown          -          [service0014]
       Characteristic UUID:    af0badb1-5b99-43cd-917a-a77bc549e3cc          -          Unknown          -          [char0015]
       Characteristic Flags:   ['write', 'notify', 'extended-properties', 'reliable-write']
              [-] Writes not being attempted  -       Passive Scan
              Descriptor UUID:       00002900-0000-1000-8000-00805f9b34fb          -          Unknown          -          [desc0017]
              Descriptor Value:      [1, 0]
              Descriptor UUID:       00002902-0000-1000-8000-00805f9b34fb          -          Client Characteristic Configuration
              Descriptor Value:      []
[*] User Interactive Exploration Tool - Select Option
```

Safari Time - Apple Watch - Characteristics

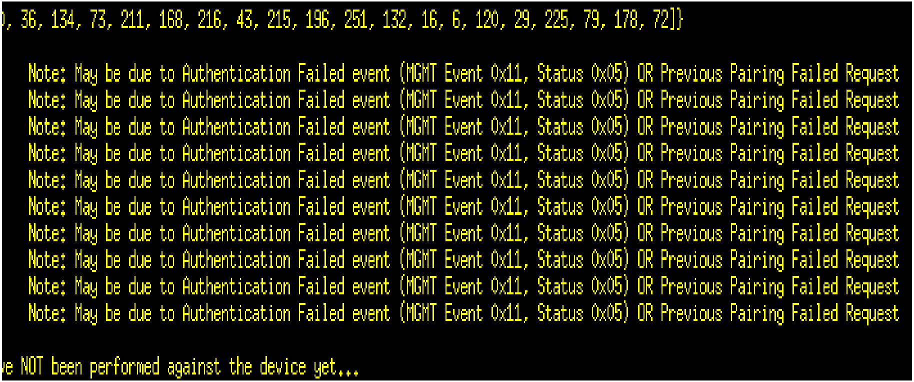
```
[*] Providing List of All Read Values Associated to known Characteristics
        [ Char Handle ] -       [ Value (ASCii) ]
[!] Error: May not have permission for R/W; perhaps need more than just con
        org.bluez.Error.NotPermitted: Read not permitted
        char0007        -       None
        char000b        -       Apple Inc.
        char000d        -       Watch6,6
[!] Error: May not have permission for R/W; perhaps need more than just con
        org.bluez.Error.NotPermitted: Read not permitted
        char0010        -       None
[!] Error: May not have permission for R/W; perhaps need more than just con
        org.bluez.Error.NotPermitted: Read not permitted
        char0015        -       None
[+] Completed print of all characteristics and values
Select an Action to Take:
```

Figure 8: Safari Time - Apple Watch - No Obvious Marking - Characteristics

Safari Time - Apple iPhone - GAP

```
Device  5B:41:5B:44:B8:DC
        Properties:             {dbus.String('Address'): '5B:41:5B:44:B8:DC', dbus.String('AddressType'):
lse, dbus.String('Blocked'): False, dbus.String('LegacyPairing'): False, dbus.String('Connected'): True, d
00-8000-00805f9b34fb', '0000180f-0000-1000-8000-00805f9b34fb', '7905f431-b5ce-4e99-a40f-4b1e122d00d0', '89
, dbus.String('ManufacturerData'): {dbus.UInt16(76): [12, 14, 0, 255, 10, 36, 134, 73, 211, 168, 216, 43,
        Address         -       Value:  5B:41:5B:44:B8:DC
        AddressType             -       Value:  random
        Name            -       Value:  iPhone
        Alias           -       Value:  iPhone
        Paired          -       Value:  False
        Bonded          -       Value:  False
        Trusted         -       Value:  False
        Blocked         -       Value:  False
        LegacyPairing           -       Value:  False
        Connected               -       Value:  True
        UUIDs           -       Value:  ['00001800-0000-1000-8000-00805f9b34fb', '00001801-0000-1000-8000-
-4b1e122d00d0', '89d3502b-0f36-433a-8ef4-c502ad55f8dc', '9fa480e0-4967-4542-9390-d343dc5d04ae', 'd0611e78-
        Adapter         -       Value:  /org/bluez/hci0
        ManufacturerData                -       Value:  {dbus.UInt16(76): [12, 14, 0, 255, 10, 36, 134, 73
        ServicesResolved                -       Value:  True
[-] connect_and_enumerate__bluetooth__low_energy::Error target device is not connected  -       Note:  May
```

Safari Time - Apple iPhone - Auth Error



```
, 36, 134, 73, 211, 168, 216, 43, 215, 196, 251, 132, 16, 6, 120, 29, 225, 79, 178, 72]}

   Note: May be due to Authentication Failed event (MGMT Event 0x11, Status 0x05) OR Previous Pairing Failed Request
   Note: May be due to Authentication Failed event (MGMT Event 0x11, Status 0x05) OR Previous Pairing Failed Request
   Note: May be due to Authentication Failed event (MGMT Event 0x11, Status 0x05) OR Previous Pairing Failed Request
   Note: May be due to Authentication Failed event (MGMT Event 0x11, Status 0x05) OR Previous Pairing Failed Request
   Note: May be due to Authentication Failed event (MGMT Event 0x11, Status 0x05) OR Previous Pairing Failed Request
   Note: May be due to Authentication Failed event (MGMT Event 0x11, Status 0x05) OR Previous Pairing Failed Request
   Note: May be due to Authentication Failed event (MGMT Event 0x11, Status 0x05) OR Previous Pairing Failed Request
   Note: May be due to Authentication Failed event (MGMT Event 0x11, Status 0x05) OR Previous Pairing Failed Request
   Note: May be due to Authentication Failed event (MGMT Event 0x11, Status 0x05) OR Previous Pairing Failed Request
   Note: May be due to Authentication Failed event (MGMT Event 0x11, Status 0x05) OR Previous Pairing Failed Request

ve NOT been performed against the device yet...
```

Figure 9: Safari Time - Apple iPhone - Authentication Failed - Error

Safari Time - Unknown Device - First Half

```
[ DEVICE        -       4C:24:98:15:36:68 ]
Service -       service000c
-       Handle:                 None
-       UUID:                   00001801-0000-1000-8000-00805f9b34fb
        Characteristic  -       char000d
        -       UUID:                   00002a05-0000-1000-8000-00805f9b34fb
        -       Handle:                 None
        -       Flags:                  ['indicate']
        -       Value:                  []
        -       ASCii:                  -=!=- UNKNOWN -=!=-
                Descriptor      -                       desc000f
                -       UUID:                   00002902-0000-1000-8000-00805f9b34fb
                -       Flags:                  None
                -       Value:                  []
Service -       service0010
-       Handle:                 None
-       UUID:                   0000180a-0000-1000-8000-00805f9b34fb
        Characteristic  -       char0011
        -       UUID:                   00002a24-0000-1000-8000-00805f9b34fb
        -       Handle:                 None
        -       Flags:                  ['read']
        -       Value:                  [90, 68, 52, 49, 48]
        -       ASCii:                  ZD410
        Characteristic  -       char0013
        -       UUID:                   00002a25-0000-1000-8000-00805f9b34fb
        -       Handle:                 None
        -       Flags:                  ['read']
        -       Value:                  [53, 48, 74, 49, 57, 51, 49, 48, 54, 49, 48, 56]
        -       ASCii:                  50J193106108
        Characteristic  -       char0015
        -       UUID:                   00002a26-0000-1000-8000-00805f9b34fb
        -       Handle:                 None
        -       Flags:                  ['read']
        -       Value:                  [86, 56, 52, 46, 50, 48, 46, 49, 53, 90]
        -       ASCii:                  V84.20.15Z
        Characteristic  -       char0017
        -       UUID:                   00002a27-0000-1000-8000-00805f9b34fb
        -       Handle:                 None
        -       Flags:                  ['read']
        -       Value:                  [90, 68, 52, 49, 72, 50, 50, 45, 68, 48, 49, 69, 48, 48, 69, 90]
        -       ASCii:                  ZD41H22-D01E00EZ
```

Safari Time - Unknown Device - Second Half

```
        -       Flags:                  ['read']
        -       Value:                  [90, 68, 52, 49, 72, 50, 50, 45, 68, 48, 49, 69, 48, 48, 69, 90]
        -       ASCii:                  ZD41H22-D01E00EZ
        Characteristic  -       char0019
        -       UUID:                   00002a28-0000-1000-8000-00805f9b34fb
        -       Handle:                 None
        -       Flags:                  ['read']
        -       Value:                  [53, 46, 50]
        -       ASCii:                  5.2
        Characteristic  -       char001b
        -       UUID:                   00002a29-0000-1000-8000-00805f9b34fb
        -       Handle:                 None
        -       Flags:                  ['read']
        -       Value:                  [90, 101, 98, 114, 97, 32, 84, 101, 99, 104, 110, 111, 108, 111, 103, 105, 101, 115]
        -       ASCii:                  Zebra Technologies
        Characteristic  -       char001d
        -       UUID:                   00002a50-0000-1000-8000-00805f9b34fb
        -       Handle:                 None
        -       Flags:                  ['read']
        -       Value:                  [1, 241, 1, 28, 1, 17, 1]
        -       ASCii:                  b'\x01\xf1\x01\x1c\x01\x11\x01'
Service -       service001f
-       Handle:                 None
-       UUID:                   38eb4a80-c570-11e3-9507-0002a5d5c51b
        Characteristic  -       char0020
        -       UUID:                   38eb4a81-c570-11e3-9507-0002a5d5c51b
        -       Handle:                 None
```

Safari Time - Zebra Details - Zoom

```
[*] Characteristc to be Explored [ char0011 ]
----------      Start of Detailed Pretty Print of Characteristic Information Provided
        UUID:                   00002a24-0000-1000-8000-00805f9b34fb
        Service:                /org/bluez/hci0/dev_4C_24_98_15_36_68/service0010
        Value:                  ZD410
        WriteAcquired:          None
        NotifyAcquired:         None
        Notify:                 None
        Flags:                  ['read']
        Handle:                 None
        MTU:                    23
        Descriptors:            {}
        Notifying:              None
---     End of Characteristic Detailed Infomration
[*] Characteristc to be Explored [ char0013 ]
----------      Start of Detailed Pretty Print of Characteristic Information Provided
        UUID:                   00002a25-0000-1000-8000-00805f9b34fb
        Service:                /org/bluez/hci0/dev_4C_24_98_15_36_68/service0010
        Value:                  50J193106108
        WriteAcquired:          None
        NotifyAcquired:         None
        Notify:                 None
        Flags:                  ['read']
        Handle:                 None
        MTU:                    23
        Descriptors:            {}
        Notifying:              None
---     End of Characteristic Detailed Infomration
```

Safari Time - Zebra Details - Zoom Two

```
[*] Characteristc to be Explored [ char0015 ]
----------       Start of Detailed Pretty Print of Characteristic Information Provided
        UUID:                   00002a26-0000-1000-8000-00805f9b34fb
        Service:                /org/bluez/hci0/dev_4C_24_98_15_36_68/service0010
        Value:                  V84.20.15Z
        WriteAcquired:          None
        NotifyAcquired:         None
        Notify:                 None
        Flags:                  ['read']
        Handle:                 None
        MTU:                    23
        Descriptors:            {}
        Notifying:              None
---     End of Characteristic Detailed Infomration
[*] Characteristc to be Explored [ char0017 ]
----------       Start of Detailed Pretty Print of Characteristic Information Provided
        UUID:                   00002a27-0000-1000-8000-00805f9b34fb
        Service:                /org/bluez/hci0/dev_4C_24_98_15_36_68/service0010
        Value:                  ZD41H22-D01E00EZ
        WriteAcquired:          None
        NotifyAcquired:         None
        Notify:                 None
        Flags:                  ['read']
        Handle:                 None
        MTU:                    23
        Descriptors:            {}
        Notifying:              None
---     End of Characteristic Detailed Infomration
```

Safari Time - Behind the Curtain

Dive! Dive! Dive!

Safari Time - Behind the Curtain

- What is happening on the HCI Layer?
- What commands are being communicated?
  - Is there a pattern to behavior?
- Corroborate the tools' guesses?

Safari Time - Attempt to Pair

```
> ACL Data RX: Handle 76 flags 0x02 dlen 9
      ATT: Error Response (0x01) len 4
        Read Request (0x0a)
        Handle: 0x002a
        Error: Insufficient Authentication (0x05)
< ACL Data TX: Handle 76 flags 0x00 dlen 11
      SMP: Pairing Request (0x01) len 6
        IO capability: NoInputNoOutput (0x03)
        OOB data: Authentication data not present (0x00)
        Authentication requirement: No bonding, No MITM, SC, No Keypresses, CT2 (0x28)
        Max encryption key size: 16
        Initiator key distribution: <none> (0x08)
        Responder key distribution: IdKey LinkKey (0x0a)
> HCI Event: Number of Completed Packets (0x13) plen 5
        Num handles: 1
        Handle: 76
        Count: 1
> ACL Data RX: Handle 76 flags 0x02 dlen 11
      SMP: Pairing Response (0x02) len 6
        IO capability: KeyboardDisplay (0x04)
        OOB data: Authentication data not present (0x00)
        Authentication requirement: Bonding, MITM, Legacy, No Keypresses (0x05)
        Max encryption key size: 16
        Initiator key distribution: <none> (0x00)
        Responder key distribution: IdKey (0x02)
@ MGMT Event: User Confirmation Request (0x000f) plen 12
        LE Address: 47:F1:A9:A9:AC:19 (Resolvable)
        Confirm hint: 0x01
        Value: 0x00000000
```

Safari Time - Attempt to Pair - Agent Problem

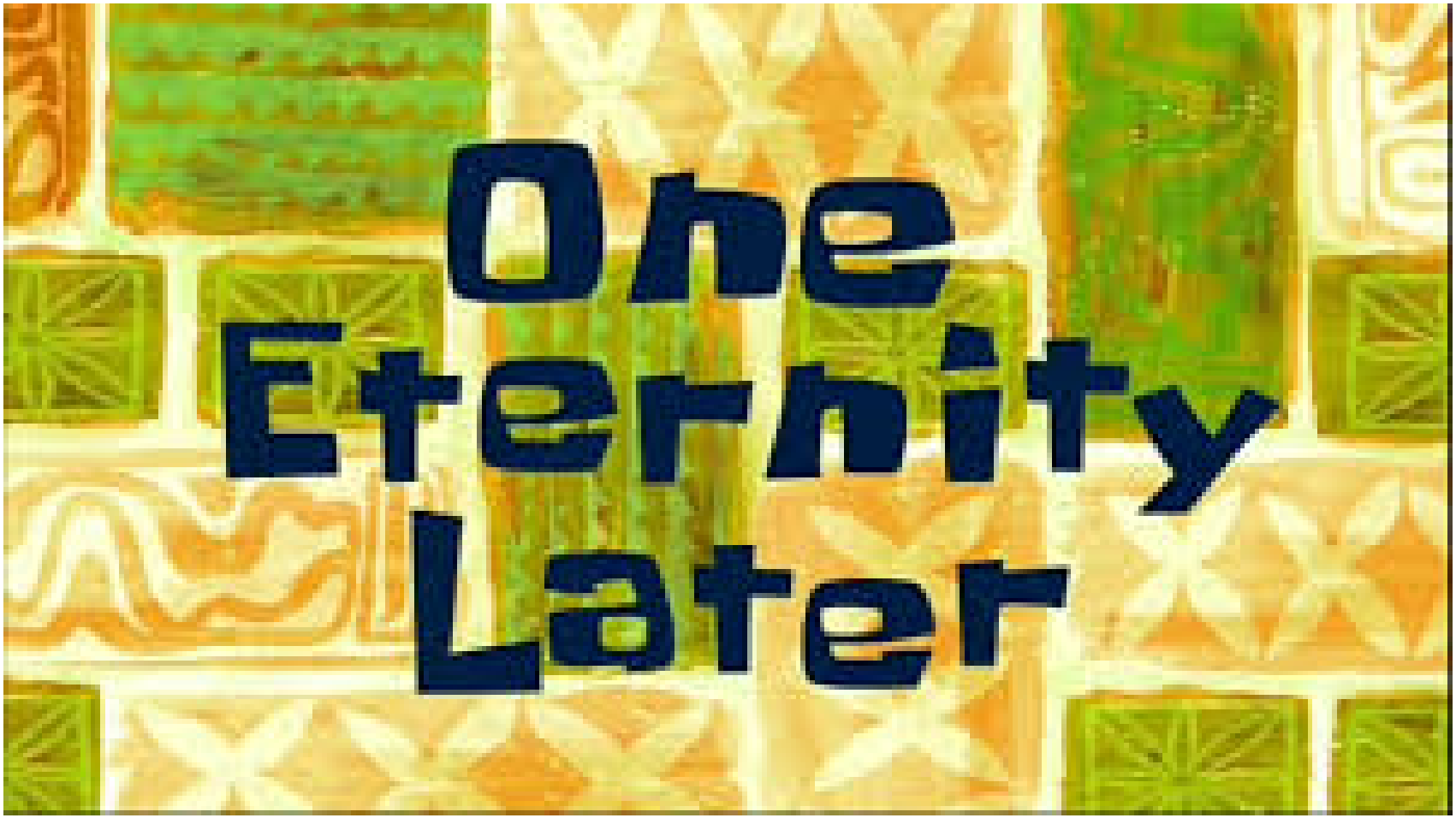
```
@ MGMT Event: User Confirmation Request (0x000f) plen 12
        LE Address: 47:F1:A9:A9:AC:19 (Resolvable)
        Confirm hint: 0x01
        Value: 0x00000000
@ MGMT Event: User Confirmation Request (0x000f) plen 12
        LE Address: 47:F1:A9:A9:AC:19 (Resolvable)
        Confirm hint: 0x01
        Value: 0x00000000
= bluetoothd[485]: src/device.c:new_auth() No agent available for request type 2
= bluetoothd[485]: device_confirm_passkey: Operation not permitted
@ MGMT Command: User Confirmation Negative Reply (0x001d) plen 7
        LE Address: 47:F1:A9:A9:AC:19 (Resolvable)
@ MGMT Event: Authentication Failed (0x0011) plen 8
        LE Address: 47:F1:A9:A9:AC:19 (Resolvable)
        Status: Authentication Failed (0x05)
@ MGMT Event: Authentication Failed (0x0011) plen 8
        LE Address: 47:F1:A9:A9:AC:19 (Resolvable)
        Status: Authentication Failed (0x05)
@ MGMT Event: Command Complete (0x0001) plen 10
      User Confirmation Negative Reply (0x001d) plen 7
        Status: Success (0x00)
        LE Address: 47:F1:A9:A9:AC:19 (Resolvable)
< ACL Data TX: Handle 76 flags 0x00 dlen 6
      SMP: Pairing Failed (0x05) len 1
        Reason: Passkey entry failed (0x01)
> HCI Event: Number of Completed Packets (0x13) plen 5
        Num handles: 1
        Handle: 76
        Count: 1
> HCI Event: Disconnect Complete (0x05) plen 4
        Status: Success (0x00)
        Handle: 76
```

Safari Time - Intel Computer Book

```
< ACL Data TX: Handle 76 flags 0x00 dlen 12
      L2CAP: Connection Request (0x02) ident 3 len 4
        PSM: 1 (0x0001)
        Source CID: 64
> HCI Event: Remote Name Req Complete (0x07) plen 255
        Status: Success (0x00)
        Address: 30:89:4A:3E:A3:40 (Intel Corporate)
        Name: BOOK-J7RI58FLT9
@ MGMT Event: Device Connected (0x000b) plen 35
        BR/EDR Address: 30:89:4A:3E:A3:40 (Intel Corporate)
        Flags: 0x00000008
          Unknown device flag (0x00000008)
        Data length: 22
        Name (complete): BOOK-J7RI58FLT9
        Class: 0x2a410c
          Major class: Computer (desktop, notebook, PDA, organizers)
          Minor class: Laptop
          invalid service class
@ MGMT Event: Device Connected (0x000b) plen 35
        BR/EDR Address: 30:89:4A:3E:A3:40 (Intel Corporate)
        Flags: 0x00000008
          Unknown device flag (0x00000008)
        Data length: 22
        Name (complete): BOOK-J7RI58FLT9
        Class: 0x2a410c
          Major class: Computer (desktop, notebook, PDA, organizers)
          Minor class: Laptop
          invalid service class
```

Safari Time - Intel Computer Book

```
> ACL Data RX: Handle 76 flags 0x02 dlen 16
      L2CAP: Connection Response (0x03) ident 3 len 8
        Destination CID: 64
        Source CID: 64
        Result: Connection pending (0x0001)
        Status: No further information available (0x0000)
> ACL Data RX: Handle 76 flags 0x02 dlen 16
      L2CAP: Connection Response (0x03) ident 3 len 8
        Destination CID: 64
        Source CID: 64
        Result: Connection successful (0x0000)
        Status: No further information available (0x0000)
> ACL Data RX: Handle 76 flags 0x02 dlen 16
      L2CAP: Configure Request (0x04) ident 24 len 8
        Destination CID: 64
        Flags: 0x0000
        Option: Maximum Transmission Unit (0x01) [mandatory]
          MTU: 1024
< ACL Data TX: Handle 76 flags 0x00 dlen 23
      L2CAP: Configure Request (0x04) ident 4 len 15
        Destination CID: 64
        Flags: 0x0000
        Option: Retransmission and Flow Control (0x04) [mandatory]
          Mode: Basic (0x00)
          TX window size: 0
          Max transmit: 0
          Retransmission timeout: 0
          Monitor timeout: 0
          Maximum PDU size: 0
< ACL Data TX: Handle 76 flags 0x00 dlen 18
      L2CAP: Configure Response (0x05) ident 24 len 10
```


One
Eternity
Later

Safari Time - Intel Computer Book - A2DP Error

```
              SDP (0x0001)
          Attribute: Browse Group List (0x0005) [len 2]
            UUID (3) with 2 bytes [0 extra bits] len 3
              Public Browse Root (0x1002)
          Attribute: Language Base Attribute ID List (0x0006) [len 2]
            Unsigned Integer (1) with 2 bytes [0 extra bits] len 3
              0x656e
            Unsigned Integer (1) with 2 bytes [0 extra bits] len 3
              0x006a
            Unsigned Integer (1) with 2 bytes [0 extra bits] len 3
              0x0100
          Attribute: Unknown (0x0100) [len 2]
            Device ID Service Record [len 24]
          Attribute: Unknown (0x0101) [len 2]
            Device ID Service Record [len 24]
          Attribute: Unknown (0x0200) [len 2]
            0x0103
          Attribute: Unknown (0x0201) [len 2]
            0x0006
          Attribute: Unknown (0x0202) [len 2]
            0x0001
          Attribute: Unknown (0x0203) [len 2]
            0x0a00
          Attribute: Unknown (0x0204) [len 2]
            true
          Attribute: Unknown (0x0205) [len 2]
            0x0001
        Continuation state: 0
= bluetoothd[485]: src/service.c:btd_service_connect() a2dp-sink profile connect failed for 30:89:4A:3E:A3:40: Protocol not available
= bluetoothd[485]: src/service.c:btd_service_connect() a2dp-source profile connect failed for 30:89:4A:3E:A3:40: Protocol not available
< ACL Data TX: Handle 76 flags 0x00 dlen 12
```

Safari Time - Intel Computer Book - Disconnect

```
< ACL Data TX: Handle 76 flags 0x00 dlen 12
      L2CAP: Disconnection Request (0x06) ident 5 len 4
        Destination CID: 64
        Source CID: 64
> HCI Event: Number of Completed Packets (0x13) plen 5
        Num handles: 1
        Handle: 76
        Count: 1
> ACL Data RX: Handle 76 flags 0x02 dlen 12
      L2CAP: Disconnection Response (0x07) ident 5 len 4
        Destination CID: 64
        Source CID: 64
< HCI Command: Disconnect (0x01|0x0006) plen 3
        Handle: 76
        Reason: Remote User Terminated Connection (0x13)
> HCI Event: Command Status (0x0f) plen 4
      Disconnect (0x01|0x0006) ncmd 1
        Status: Success (0x00)
> HCI Event: Disconnect Complete (0x05) plen 4
        Status: Success (0x00)
        Handle: 76
        Reason: Connection Terminated By Local Host (0x16)
@ MGMT Event: Device Disconnected (0x000c) plen 8
        BR/EDR Address: 30:89:4A:3E:A3:40 (Intel Corporate)
        Reason: Connection terminated by local host (0x02)
@ MGMT Event: Device Disconnected (0x000c) plen 8
        BR/EDR Address: 30:89:4A:3E:A3:40 (Intel Corporate)
        Reason: Connection terminated by local host (0x02)
@ MGMT Command: Remove Device (0x0034) plen 7
```

Safari Time - Bobbing Time!

Safari Time - Apple iPhone Dive - Auth Error

```
< ACL Data TX: Handle 75 flags 0x00 dlen 7
      ATT: Read Request (0x0a) len 2
        Handle: 0x001b
> HCI Event: Number of Completed Packets (0x13) plen 5
        Num handles: 1
        Handle: 75
        Count: 1
> ACL Data RX: Handle 75 flags 0x02 dlen 9
      ATT: Error Response (0x01) len 4
        Read Request (0x0a)
        Handle: 0x001b
        Error: Insufficient Authentication (0x05)
< ACL Data TX: Handle 75 flags 0x00 dlen 11
      SMP: Pairing Request (0x01) len 6
        IO capability: NoInputNoOutput (0x03)
        OOB data: Authentication data not present (0x00)
        Authentication requirement: No bonding, No MITM, SC, No Keypresses, CT2 (0x28)
        Max encryption key size: 16
        Initiator key distribution: <none> (0x08)
        Responder key distribution: IdKey LinkKey (0x0a)
> HCI Event: Number of Completed Packets (0x13) plen 5
        Num handles: 1
        Handle: 75
        Count: 1
> ACL Data RX: Handle 75 flags 0x02 dlen 6
      SMP: Pairing Failed (0x05) len 1
        Reason: Unspecified reason (0x08)
@ MGMT Event: Authentication Failed (0x0011) plen 8
        LE Address: 7D:DC:43:0C:E9:C0 (Resolvable)
        Status: Authentication Failed (0x05)
```

Safari Time - Apple iPhone Dive - Remote Disconnect

```
> ACL Data RX: Handle 75 flags 0x02 dlen 6
      SMP: Pairing Failed (0x05) len 1
        Reason: Unspecified reason (0x08)
@ MGMT Event: Authentication Failed (0x0011) plen 8
        LE Address: 7D:DC:43:0C:E9:C0 (Resolvable)
        Status: Authentication Failed (0x05)
@ MGMT Event: Authentication Failed (0x0011) plen 8
        LE Address: 7D:DC:43:0C:E9:C0 (Resolvable)
        Status: Authentication Failed (0x05)
< HCI Command: Disconnect (0x01|0x0006) plen 3
        Handle: 75
        Reason: Authentication Failure (0x05)
> HCI Event: Command Status (0x0f) plen 4
      Disconnect (0x01|0x0006) ncmd 1
        Status: Success (0x00)
> HCI Event: Disconnect Complete (0x05) plen 4
        Status: Success (0x00)
        Handle: 75
        Reason: Connection Terminated By Local Host (0x16)
@ MGMT Event: Device Disconnected (0x000c) plen 8
        LE Address: 7D:DC:43:0C:E9:C0 (Resolvable)
        Reason: Connection terminated by local host (0x02)
@ MGMT Event: Device Disconnected (0x000c) plen 8
        LE Address: 7D:DC:43:0C:E9:C0 (Resolvable)
        Reason: Connection terminated by local host (0x02)
```

Safari Time - Apple iPhone Dive - Err Resp II

```
< ACL Data TX: Handle 75 flags 0x00 dlen 7
      ATT: Read Request (0x0a) len 2
        Handle: 0x0011
> HCI Event: Number of Completed Packets (0x13) plen 5
        Num handles: 1
        Handle: 75
        Count: 1
> ACL Data RX: Handle 75 flags 0x02 dlen 9
      ATT: Error Response (0x01) len 4
        Read Request (0x0a)
        Handle: 0x0011
        Error: Insufficient Authentication (0x05)
< ACL Data TX: Handle 75 flags 0x00 dlen 11
      SMP: Pairing Request (0x01) len 6
        IO capability: NoInputNoOutput (0x03)
        OOB data: Authentication data not present (0x00)
        Authentication requirement: No bonding, No MITM, SC, No Keypresses, CT2 (0x28)
        Max encryption key size: 16
        Initiator key distribution: <none> (0x08)
        Responder key distribution: IdKey LinkKey (0x0a)
> HCI Event: Number of Completed Packets (0x13) plen 5
        Num handles: 1
        Handle: 75
        Count: 1
> ACL Data RX: Handle 75 flags 0x02 dlen 6
      SMP: Pairing Failed (0x05) len 1
        Reason: Unspecified reason (0x08)
@ MGMT Event: Authentication Failed (0x0011) plen 8
        LE Address: 7F:25:A6:ED:7F:16 (Resolvable)
        Status: Authentication Failed (0x05)
```

Safari Time - Decoding Scatt(ered data)

- Notice pattern of `Error Resp` to `Pairing Failure`
  - Enumeration of devices leads to disconnection occurring
  - Not initiated by **BLEEP** tool
- List of Observed Handles
  - `0x001b` - Laptop, Apple (iPhones, Watches, iPad), Unknowns
  - `0x0019` - Light Orb
  - `0x003b` - Unknowns
  - `0x002a` - Unknowns

Safari Time - Decoding Scatt(ered data)

- What do we notice about this data?
  - Attempt to read Characteristic data
  - Notice “tripping” of “panic reaction” for device disconnect
- What does **BLEEP** show?

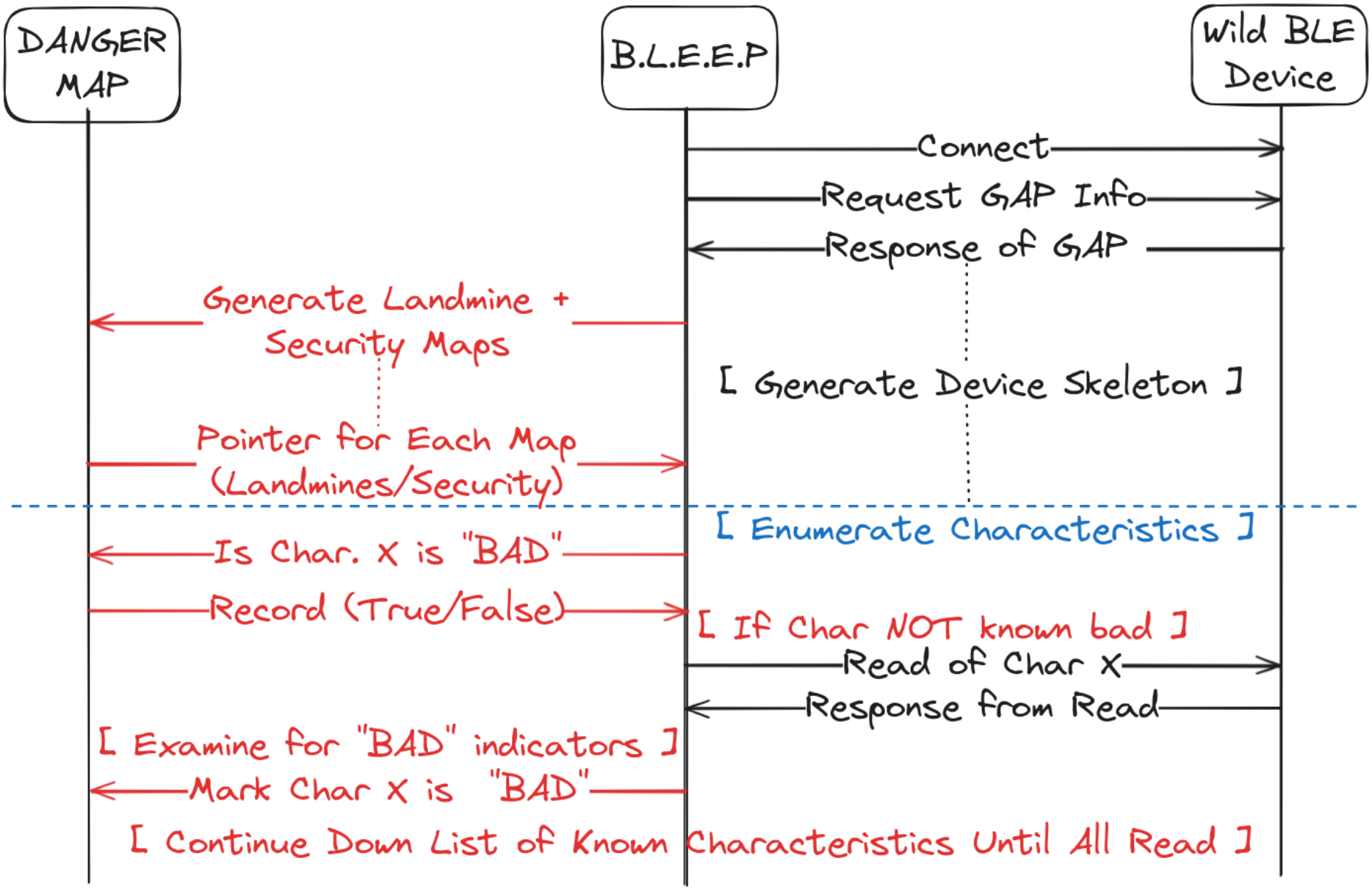
Safari Time - Apple iPhone - Panic / Protection

```
        ManufacturerData                     -       Value:  {dbus.UInt16(76): [16, 7, 51, 31, 169, 2
        ServicesResolved                     -       Value:  True
[!] Error: D-Bus error  -       org.bluez.Error.Failed: Operation failed with ATT error: 0x0e
        Type:   org.bluez.Error.Failed: Operation failed with ATT error: 0x0e
        Args:   ('Operation failed with ATT error: 0x0e',)
        D-Bus Message:  Operation failed with ATT error: 0x0e
[-] connect_and_enumerate__bluetooth__low_energy::Error target device is not connected
[-] connect_and_enumerate__bluetooth__low_energy::Error target device is not connected
[-] connect_and_enumerate__bluetooth__low_energy::Error target device is not connected
[-] connect_and_enumerate__bluetooth__low_energy::Error target device is not connected
[-] connect_and_enumerate__bluetooth__low_energy::Error target device is not connected
[-] connect_and_enumerate__bluetooth__low_energy::Error target device is not connected
[-] connect_and_enumerate__bluetooth__low_energy::Error target device is not connected
[-] connect_and_enumerate__bluetooth__low_energy::Error target device is not connected
[-] connect_and_enumerate__bluetooth__low_energy::Error target device is not connected
[-] connect_and_enumerate__bluetooth__low_energy::Error target device is not connected
[+] Exploration Basics Successfully Created
[=] Warning! The generated Device Map will only be a skeleton of the target device. Reads have N
Service UUID:   00001801-0000-1000-8000-00805f9b34fb            -               Generic Attribut
        Characteristic UUID:    00002a05-0000-1000-8000-00805f9b34fb            -
```

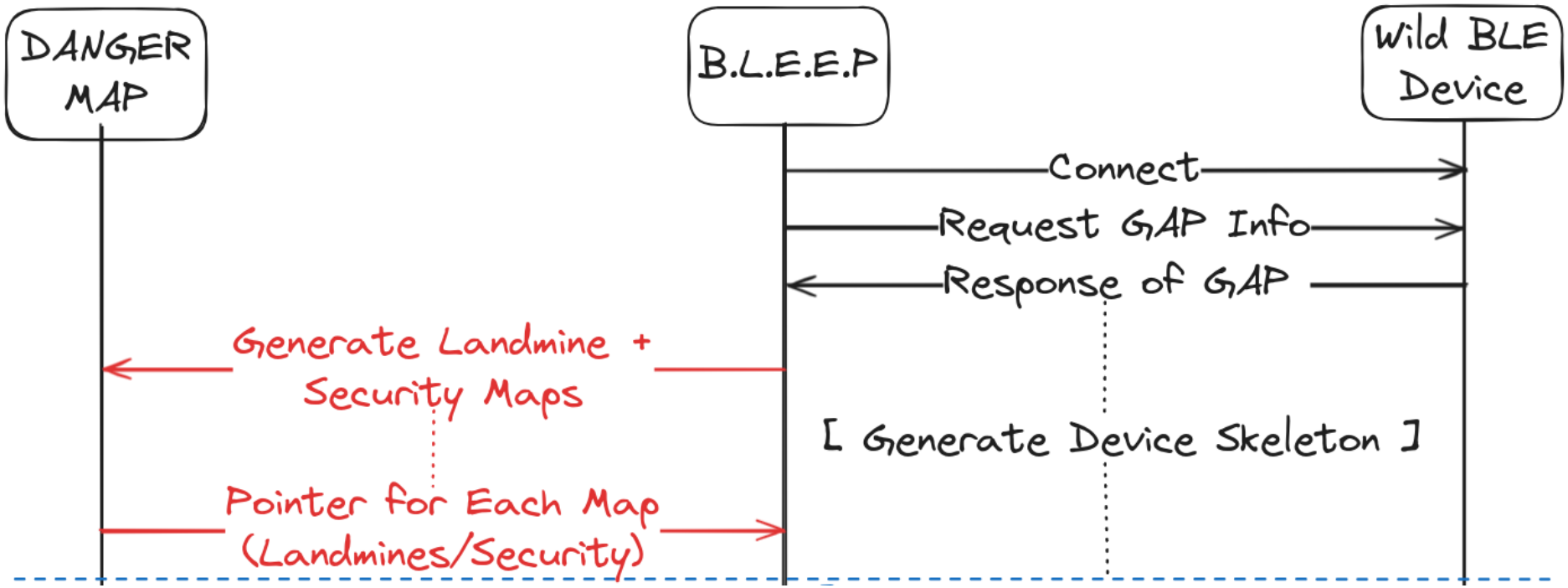
Safari Augmentation - Mapping Landmines

- What do we want to map?
  - Landmines
  - Security-related
- Can we prevent the disconnection?
- What do we notice about this data?

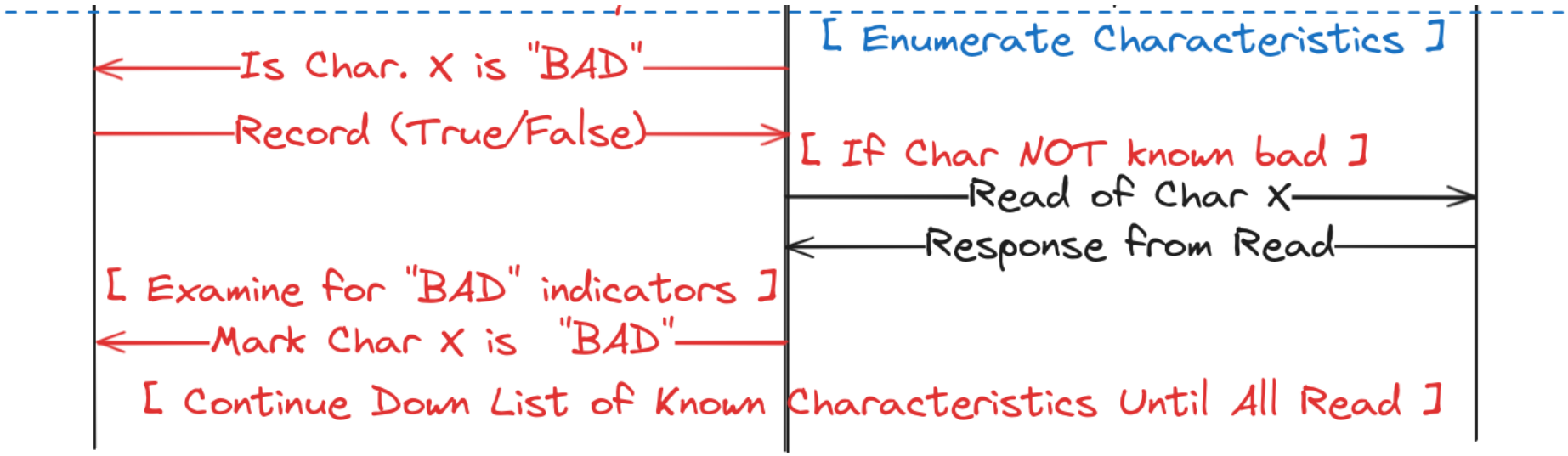
Safari Augmentation - New Enumeration



Safari Augmentation - New Enumeration



Safari Augmentation - New Enumeration



Safari Time - Apple iPhone - Bird Camo

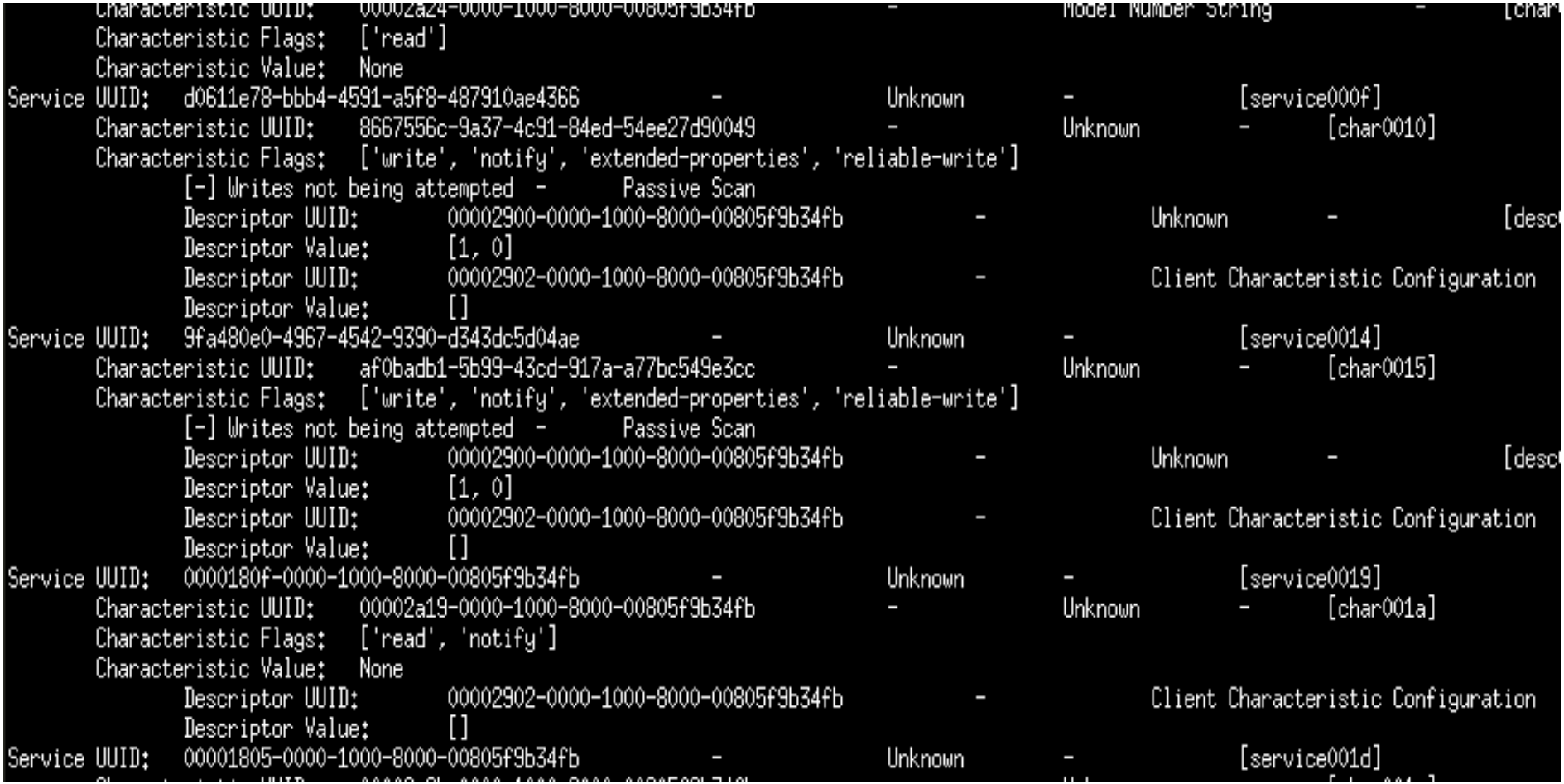


Figure 17: Safari Time - iPhone - Mapping - Example 001

Safari Time - Apple iPhone - Bird Camo

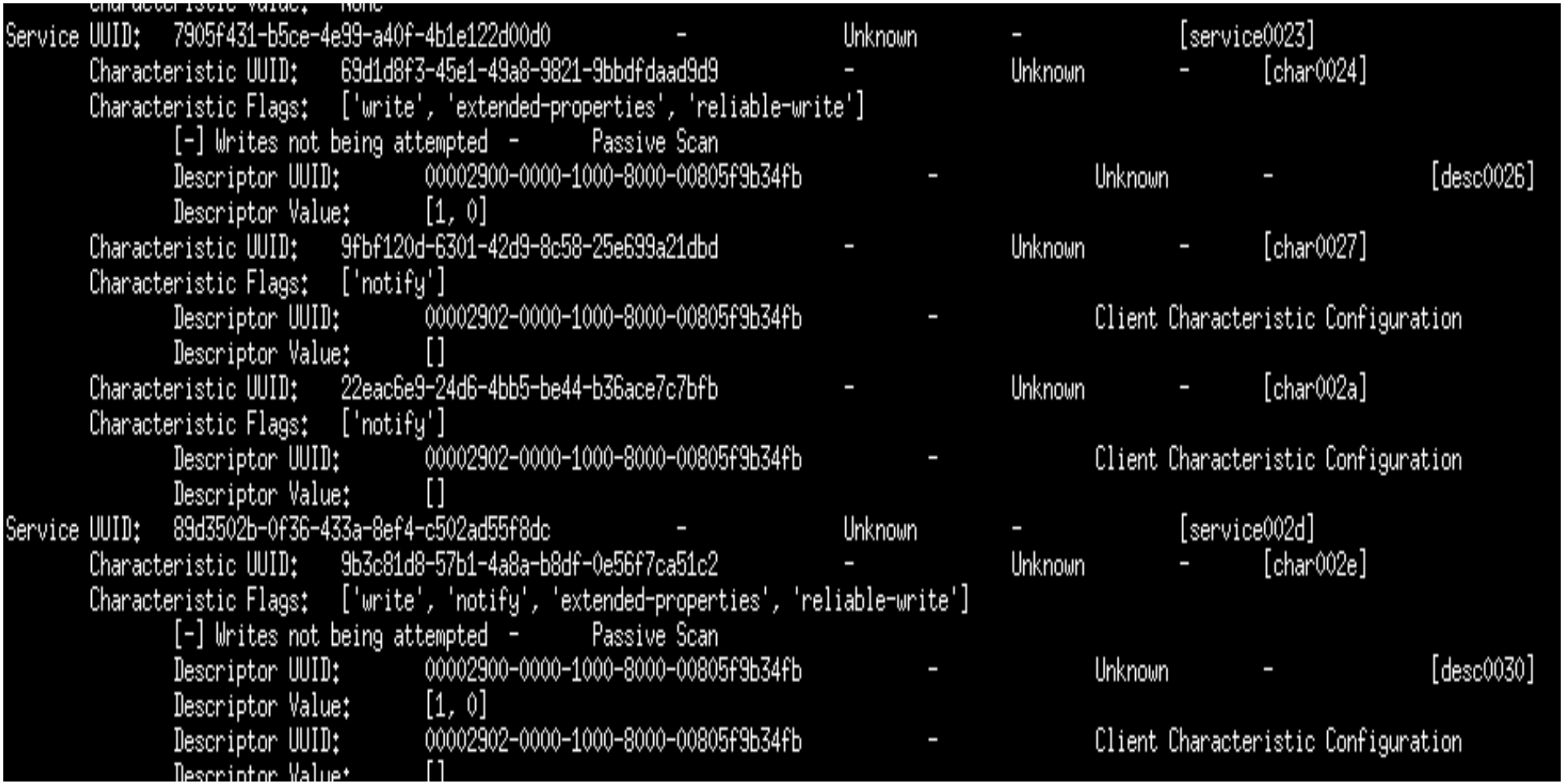


Figure 18: Safari Time - iPhone - Mapping - Example 002

Safari Time - Apple iPhone - Bird Camo

```
        Characteristic UUID:    9b3c81d8-57b1-4a8a-b8df-0e56f7ca51c2          -               Unknown         -       [char002e]
        Characteristic Flags:   ['write', 'notify', 'extended-properties', 'reliable-write']
                [-] Writes not being attempted  -       Passive Scan
                Descriptor UUID:        00002900-0000-1000-8000-00805f9b34fb          -               Unknown         -               [desc0030]
                Descriptor Value:       [1, 0]
                Descriptor UUID:        00002902-0000-1000-8000-00805f9b34fb          -               Client Characteristic Configuration
                Descriptor Value:       []
        Characteristic UUID:    2f7cabce-808d-411f-9a0c-bb92ba96c102          -               Unknown         -       [char0032]
        Characteristic Flags:   ['write', 'notify', 'extended-properties', 'reliable-write']
                [-] Writes not being attempted  -       Passive Scan
                Descriptor UUID:        00002900-0000-1000-8000-00805f9b34fb          -               Unknown         -               [desc0034]
                Descriptor Value:       [1, 0]
                Descriptor UUID:        00002902-0000-1000-8000-00805f9b34fb          -               Client Characteristic Configuration
                Descriptor Value:       []
        Characteristic UUID:    c6b2f38c-23ab-46d8-a6ab-a3a870bbd5d7          -               Unknown         -       [char0036]
        Characteristic Flags:   ['read', 'write', 'extended-properties', 'reliable-write']
        Characteristic Value:   None
                [-] Writes not being attempted  -       Passive Scan
                Descriptor UUID:        00002900-0000-1000-8000-00805f9b34fb          -               Unknown         -               [desc0038]
                Descriptor Value:       [1, 0]
[*] User Interactive Exploration Tool - Select Action
        - 'print' to Pretty Print the known user device internals map
        - 'info' to print device information
        - 'generate' to Access the Generation Sub-Menu
        - 'explore' to Access the Exploration Sub-Menu
        - 'read' to Access the Reading Sub-Menu
        - 'write' to Access the Writing Sub-Menu
        - 'help' to print this information
        - 'quit' to exit user exploration
        Nota Bene:      Complete Re-Read of the Device may be required to update the Device Internals Map
        Ssh.....
```

Figure 19: Safari Time - iPhone - Mapping - Example 003

Safari Time - Bird Camo - HCI Layer

```
> ACL Data RX: Handle 75 flags 0x02 dlen 14
      ATT: Read Response (0x0b) len 9
        Value: 5761746368352c3131
< ACL Data TX: Handle 75 flags 0x00 dlen 7
      ATT: Read Request (0x0a) len 2
        Handle: 0x000e
> HCI Event: Number of Completed Packets (0x13) plen 5
        Num handles: 1
        Handle: 75
        Count: 1
> ACL Data RX: Handle 75 flags 0x02 dlen 14
      ATT: Read Response (0x0b) len 9
        Value: 5761746368352c3131
> HCI Event: Disconnect Complete (0x05) plen 4
        Status: Success (0x00)
        Handle: 75
        Reason: Connection Timeout (0x08)
@ MGMT Event: Device Disconnected (0x000c) plen 8
        LE Address: 6D:B7:6A:FB:02:8A (Resolvable)
        Reason: Connection timeout (0x01)
```

Figure 20: Safari Time - iPhone - Mapping - HCI Layer

Safari Time - Bird Camo - HCI Layer

```
> ACL Data RX: Handle 75 flags 0x02 dlen 14
      ATT: Read Response (0x0b) len 9
        Value: 5761746368352c3131
< ACL Data TX: Handle 75 flags 0x00 dlen 7
      ATT: Read Request (0x0a) len 2
        Handle: 0x000e
> HCI Event: Number of Completed Packets (0x13) plen 5
        Num handles: 1
        Handle: 75
        Count: 1
> ACL Data RX: Handle 75 flags 0x02 dlen 14
      ATT: Read Response (0x0b) len 9
        Value: 5761746368352c3131
> HCI Event: Disconnect Complete (0x05) plen 4
        Status: Success (0x00)
        Handle: 75
        Reason: Connection Timeout (0x08)
@ MGMT Event: Device Disconnected (0x000c) plen 8
        LE Address: 6D:B7:6A:FB:02:8A (Resolvable)
        Reason: Connection timeout (0x01)
```

Safari Time - Lessons I

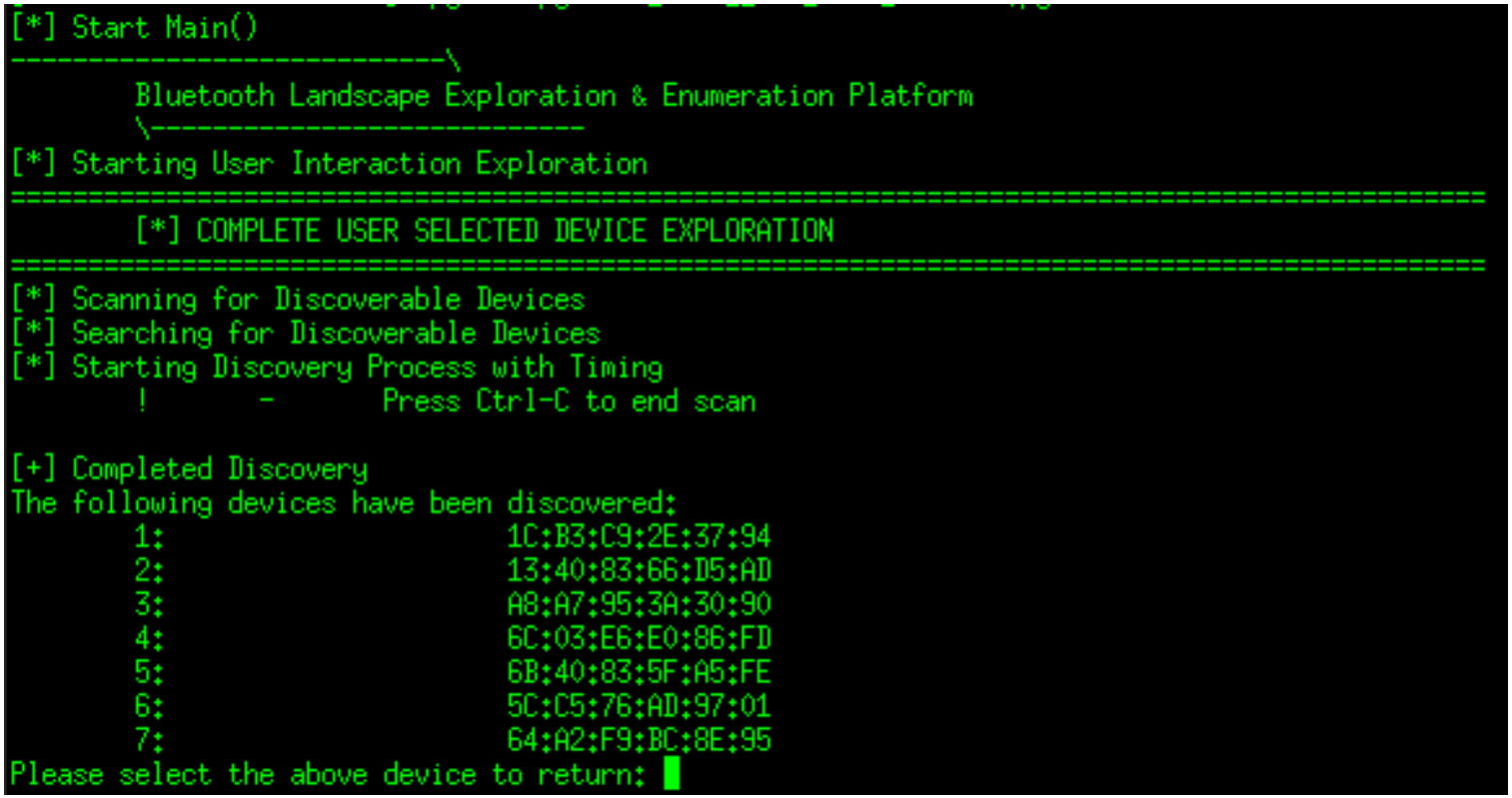
- Platform continues to reveal the implementation-specific landscape of the Bluetooth wildlife
  - Majority is manufacturer dependent
  - Variety within each manufacturer
- Found a literal Zebra device
  - Assumed a barcode scanner; encountered in real-life

Safari Time - Lessons II

- Connection canaries
  - Noticed more after Flipper-fix patch
- Audio vs No Audio
  - Packages/Functionality of client dictates compatibility with GATT server
  - Installing pulse-audio package opens up connect-ability

Research Details

- Git Repo: https://github.com/Mauddib28/bleep-tool



Questions

Questions?
(While Demo Happens)

Bibliography References I

Freedesktop

What is D-Bus, Published 2022

https://www.freedesktop.org/wiki/Software/dbus/

Last Accessed: 2024-03-28 22:43:19 EST

GNU

Knowing the Details of D-Bus Services

https://www.gnu.org/software/emacs/manual/html_node/dbus/Introspection.html

Last Accessed: 2024-04-01 19:48:34 EST

Programiz

Python Decorators

https://www.programiz.com/python-programming/decorator

Last Accessed: 2024-04-01 19:52:34 EST

Bibliography References II

hbldh

characteristic.py

https://github.com/hbldh/bleak/blob/63adefa24cb6ed11c8cf154fa41f51ecff1df98c/bleak/backends/characteristic.py

Last Accessed: 2024-04-01 19:56:34 EST

elsampsa

Bluetooth + DBus + gobject demo

https://github.com/elsampsa/btdemo

Last Accessed: 2024-04-01 19:54:52 EST

Freedesktop

DbusTools, Published May 07 2021

https://www.freedesktop.org/wiki/Software/DbusTools/

Last Accessed: 2024-03-28 22:57:29 EST

Bibliography References III


Bluetooth SIG
assigned_numbers
https://bitbucket.org/bluetooth-SIG/public/src/main/assigned_numbers/
Last Accessed: 2024-04-01 21:00:29 EST


Bluetooth SIG
public bitbucket
https://bitbucket.org/bluetooth-SIG/public/src/main/
Last Accessed: 2024-04-02 15:13:33 EST


Archlinux Forum
Activation via systemd failed for unit dbus-org.bluez.service
https://bbs.archlinux.org/viewtopic.php?id=155714
Last Accessed: 2024-04-02 15:09:42 EST

Bibliography References IV

oscaracena

gattlib.h

https://github.com/oscaracena/pygattlib/blob/7d08c0805313201b2ab12628e19544bb180218a8/src/gattlib.h

Last Accessed: 2024-04-02 15:09:42 EST

Bluetooth SIG

Bluetooth for Linux Developers Study Guide - Versions 1.0, 1.0.1

https://www.bluetooth.com/bluetooth-resources/bluetooth-for-linux/

Last Accessed: 2021-12-29 10:26:27 EST, 2022-10-18 18:54:02 EST

Bibliography References V

Bluetooth SIG

Developer Study Guide Bluetooth Internet Gateways - Version 2.0.0

https://www.bluetooth.com/blog/the-bluetooth-internet-gateway-study-guide/

Last Accessed: 2021-07-21 14:46:56 EST

Bluetooth SIG

Bluetooth LE Developer Study Guide - Version 5.2.0

https://www.bluetooth.com/bluetooth-resources/bluetooth-le-developer-starter-kit/

Last Accessed: 2023-02-16 11:36:57 EST

Bibliography References VI

Bluetooth SIG

Bluetooth Core Specification - Versions 5.3, 5.4

https://www.bluetooth.com/specifications/specs/core-specification-5-[3—4]/

Last Accessed: 2023-12-19 13:24:22 EST, 2023-12-16 11:33:37 EST

Bluetooth SIG

Generic Attribute Profile (GATT)

https://www.bluetooth.com/wp-content/uploads/Files/Specification/HTML/Core-54/out/en/host/generic-attribute-profile–gatt-.html

Last Accessed: 2023-12-16 11:22:03 EST

Marcel Holtmann, Maxim Krasnyansky, Qualcomm

BlueZ - Bluetooth protocol stack for Linux

https://git.kernel.org/pub/scm/bluetooth/bluez.git/tree/doc

Last Accessed: 2024-04-11 10:39:23 EST

Bibliography References VII


Josh Whiton
"Lightning" Headphones That Require Bluetooth
https://mjtsai.com/blog/2024/06/03/lightning-headphones-that-require-bluetooth/
Last Accessed: 2024-07-08 10:16:42 EST