# Hardware Hacking:

## A Brief Primer on Reverse Engineering Bluetooth Transmissions

Edward Warren

# Overview

I. whoami
II. Getting Started
III. OSINT Resources for Bluetooth & IoT devices
IV. A Brief History of Bluetooth
V. Select Tools for Bluetooth IoT Analysis
VI. Select Tools for Bluetooth Sniffing
VII. Medical Information at Risk
VIII. Trial & Error
IX. Reverse Engineering BLE Transmissions
X. Android Application Secrets
XI. Conclusions

# #:whoami

- Jr. Security Analyst @ SEDARA™
- Former Managed Wi-Fi Technical Support Rep III at Spectrum Business
- A dude who likes more than *software* bugs
- From Buffalo, NY

(Actual footage of my Fence)

# Getting Started

- Recon the attack surface of the device or application

- Utilize Open Source Intelligence (OSINT)

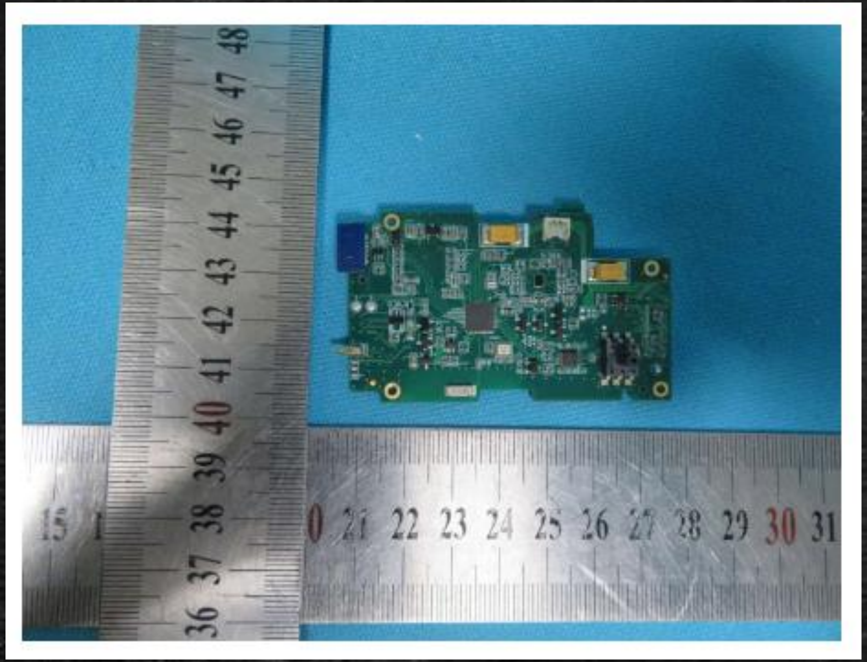
- Have a clear mission or objective

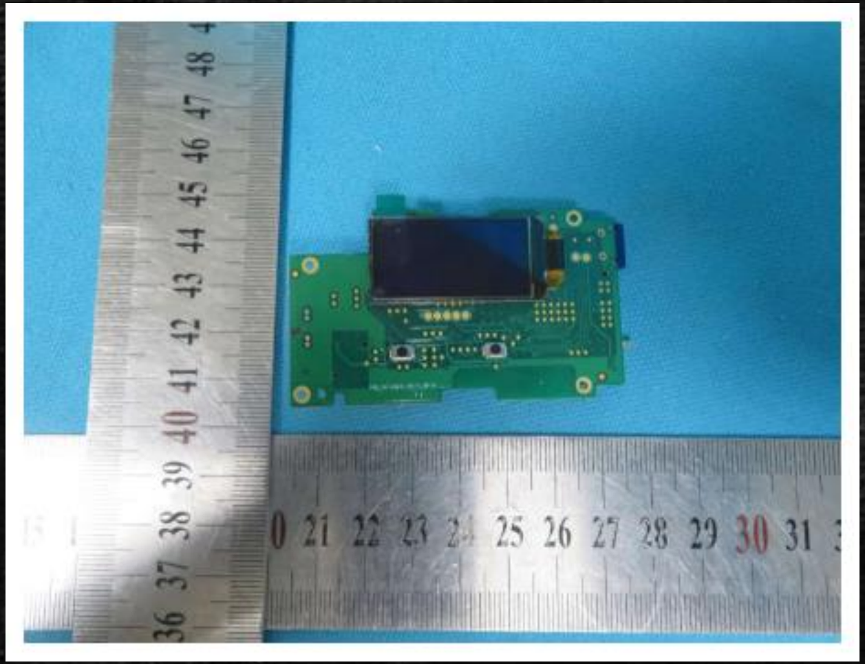
# OSINT Resources For Bluetooth & IoT Devices

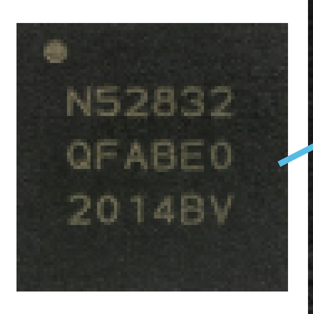
FCC IDs are required for all wireless emitting devices sold in the USA.

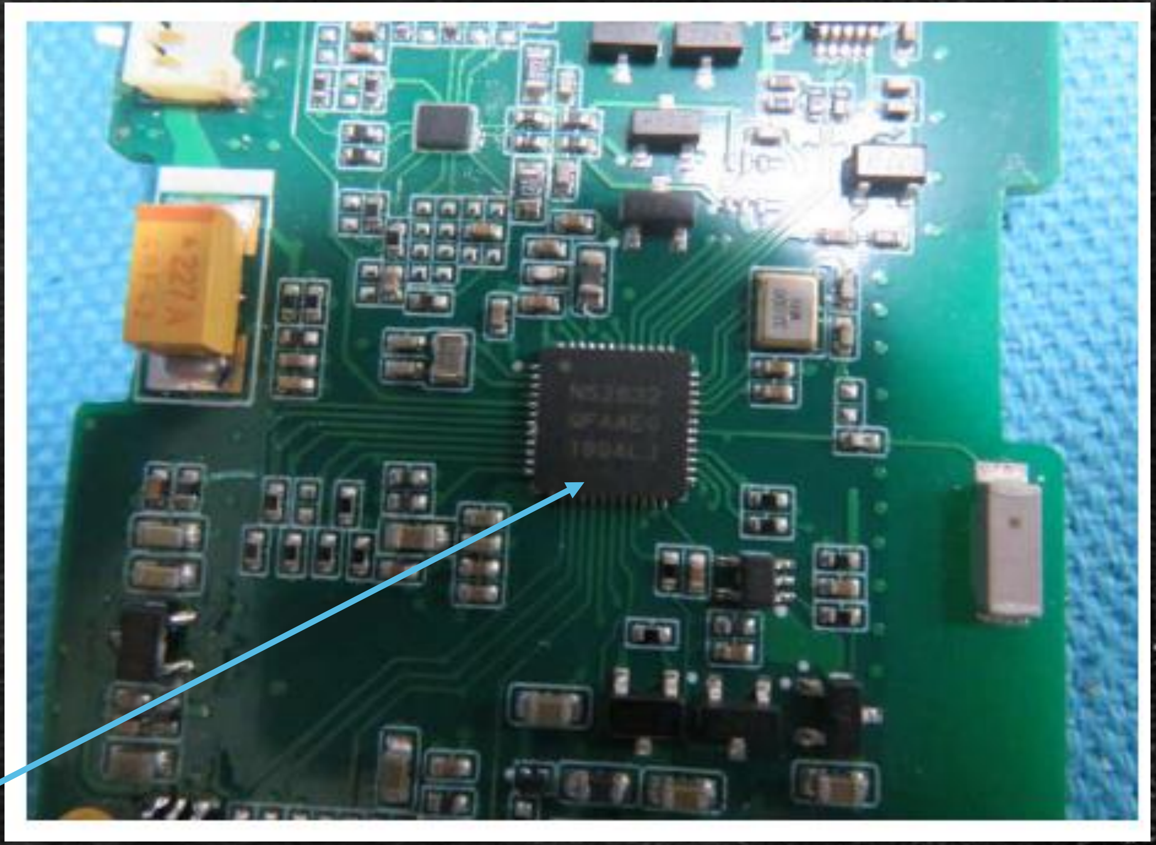
By searching an FCC ID, you can find details on the wireless operating frequency (including strength), photos of the device, user manuals for the device, and reports on the wireless emissions ect.

FCC Federal Communications Commission









fcc.io

**NRF52832**, Bluetooth SoC supporting Bluetooth Low Energy, Bluetooth mesh & NFC

(https://www.nordicsemi.com/-/media/Software-and-other-downloads/Product-Briefs/nRF52832-product-brief.pdf)

# A Brief history of Bluetooth

What is Bluetooth? It's not an acronym and doesn't stand for anything. So what does it mean?

The name dates back to the Viking era, specifically King Harald Gormsson, who earned the nickname Bluetooth due a dead tooth which had an apparently distinct blue color.

He is also known for unifying Denmark and Norway in 958 AD. The Bluetooth logo is a combination of two runes, Hagall (✱) and Bjarkan (ᛒ), which form the initials of Harald Bluetooth.

Bluetooth®

(https://www.bluetooth.com/about-us/bluetooth-origin)

# A Brief history of Bluetooth Continued…

Bluetooth Classic is better suited for applications that require high data transfer rates and longer range,

*whereas* BLE is better suited for applications that require low power consumption and intermittent communication.

Bluetooth®

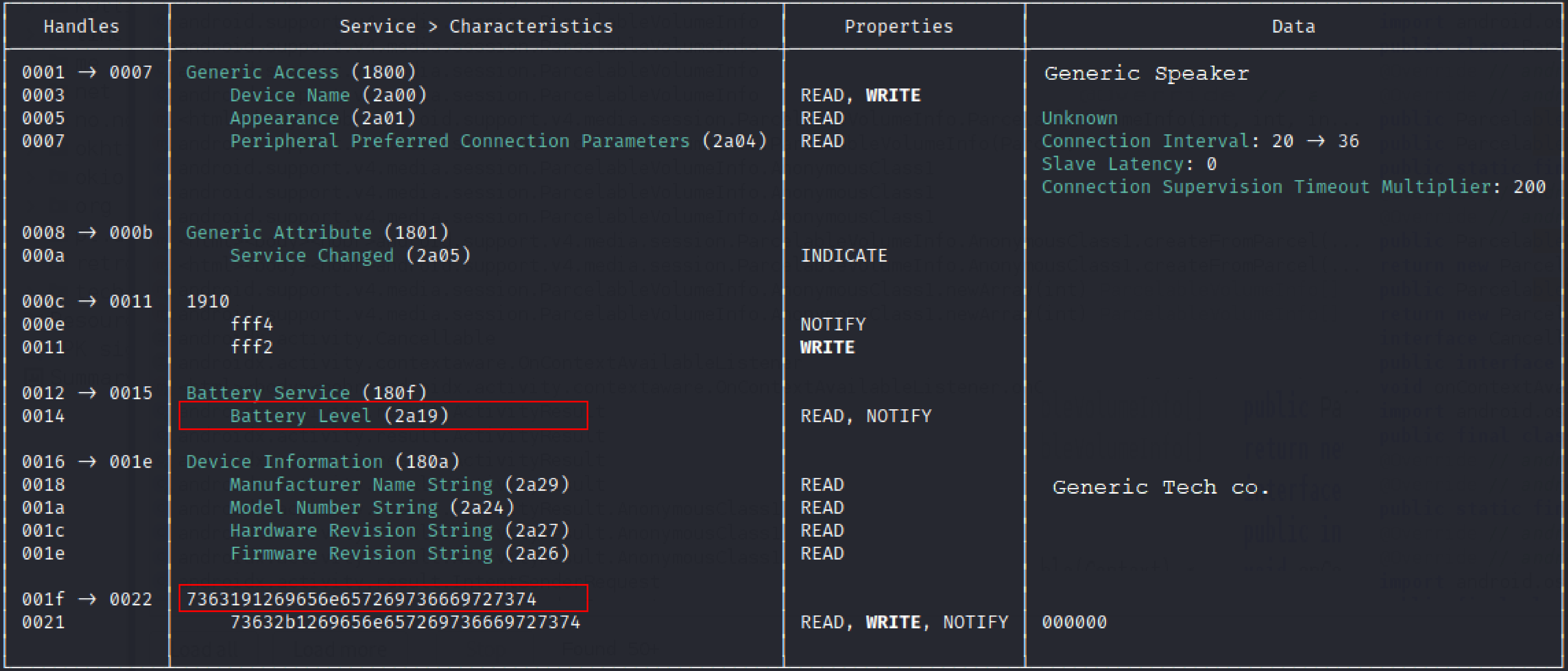
# Select Tools for Bluetooth IoT Analysis

github.com/skylot/jadx

www.bettercap.org

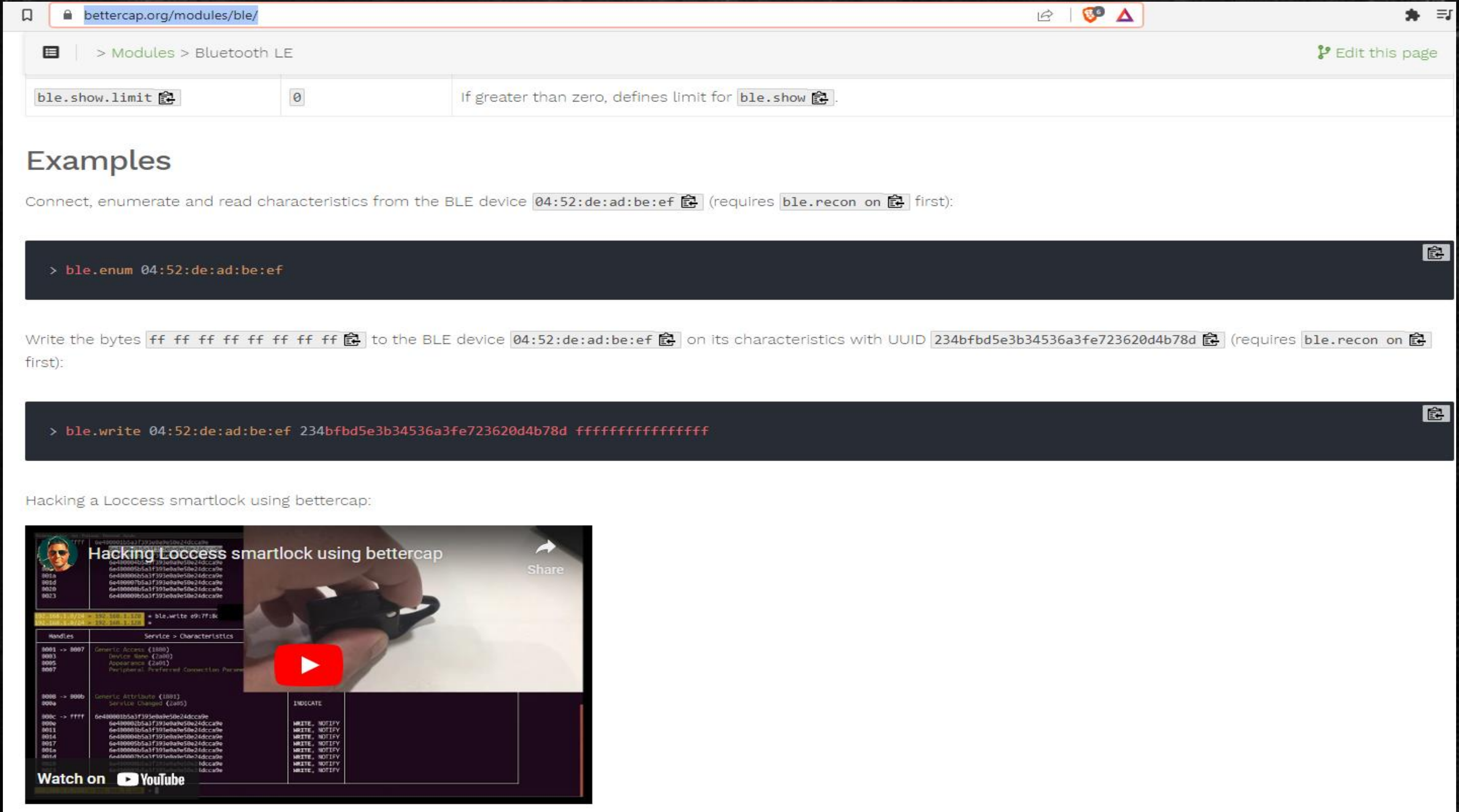
gitlab.com/AuroraOSS/AuroraStore

www.wireshark.org



```
Handles         Service > Characteristics                                        Properties              Data

0001 → 0007     Generic Access (1800)                                                                    Generic Speaker
0003                Device Name (2a00)                                           READ, WRITE
0005                Appearance (2a01)                                            READ                    Unknown
0007                Peripheral Preferred Connection Parameters (2a04)           READ                    Connection Interval: 20 → 36
                                                                                                         Slave Latency: 0
                                                                                                         Connection Supervision Timeout Multiplier: 200

0008 → 000b     Generic Attribute (1801)
000a                Service Changed (2a05)                                       INDICATE

000c → 0011     1910
000e                fff4                                                         NOTIFY
0011                fff2                                                         WRITE

0012 → 0015     Battery Service (180f)
0014                Battery Level (2a19)                                         READ, NOTIFY

0016 → 001e     Device Information (180a)
0018                Manufacturer Name String (2a29)                              READ                     Generic Tech co.
001a                Model Number String (2a24)                                   READ
001c                Hardware Revision String (2a27)                              READ
001e                Firmware Revision String (2a26)                              READ

001f → 0022     7363191269656e657269736669727374
0021                73632b1269656e657269736669727374                             READ, WRITE, NOTIFY     000000
```

In Bluetooth GATT or (Generic Attribute Profiles) is a protocol that defines how data is exchanged between Bluetooth devices. GATT is a client-server protocol, where a GATT server stores attribute data and provides access methods to a remote client.



| | | |
|---|---|---|
| `ble.show.limit` | `0` | If greater than zero, defines limit for `ble.show`. |

## Examples

Connect, enumerate and read characteristics from the BLE device `04:52:de:ad:be:ef` (requires `ble.recon on` first):

```
> ble.enum 04:52:de:ad:be:ef
```

Write the bytes `ff ff ff ff ff ff ff ff` to the BLE device `04:52:de:ad:be:ef` on its characteristics with UUID `234bfbd5e3b34536a3fe723620d4b78d` (requires `ble.recon on` first):

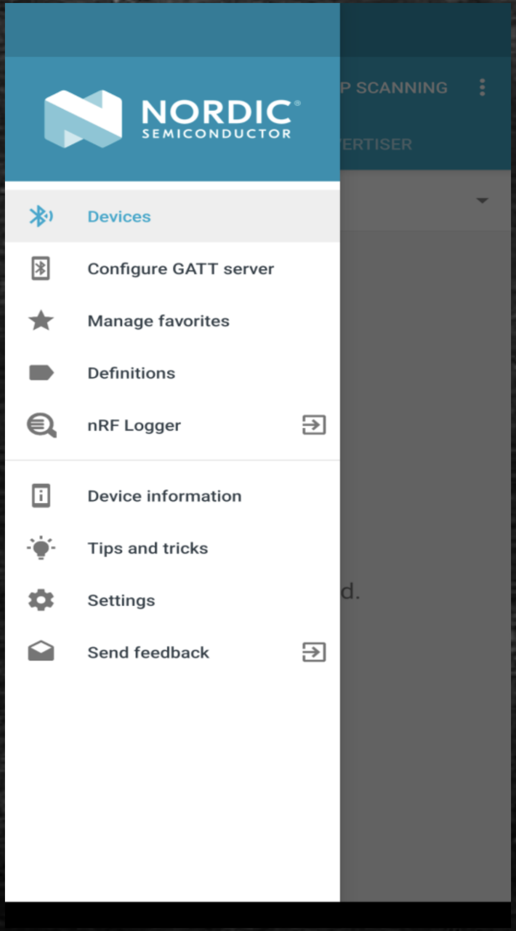
```
> ble.write 04:52:de:ad:be:ef 234bfbd5e3b34536a3fe723620d4b78d ffffffffffffffff
```

Hacking a Loccess smartlock using bettercap:

# Honorable Mention

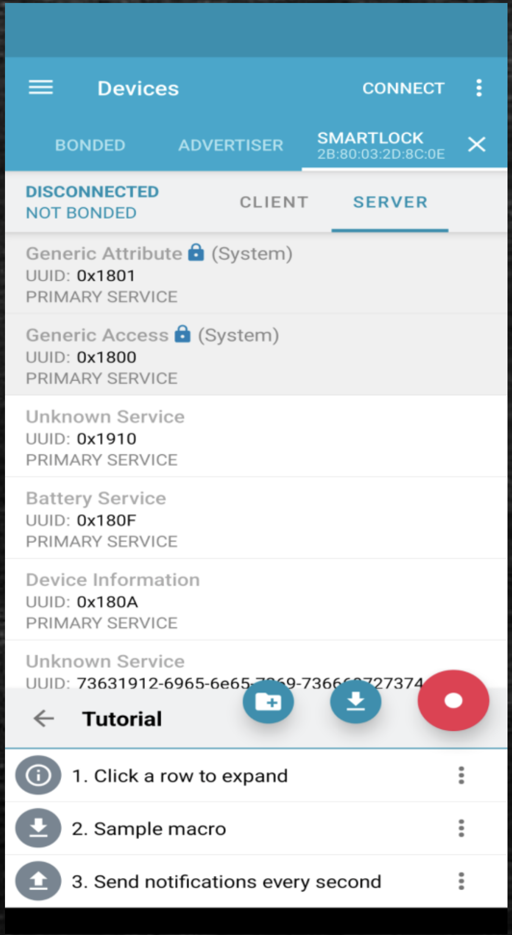
nRF Connect

A NORDIC SEMICONDUCTOR PRODUCT



NORDIC SEMICONDUCTOR

- Devices
- Configure GATT server
- Manage favorites
- Definitions
- nRF Logger
- Device information
- Tips and tricks
- Settings
- Send feedback



DISCONNECTED
NOT BONDED

Generic Attribute (System)
UUID: 0x1801
PRIMARY SERVICE

Generic Access (System)
UUID: 0x1800
PRIMARY SERVICE

Unknown Service
UUID: 0x1910
PRIMARY SERVICE

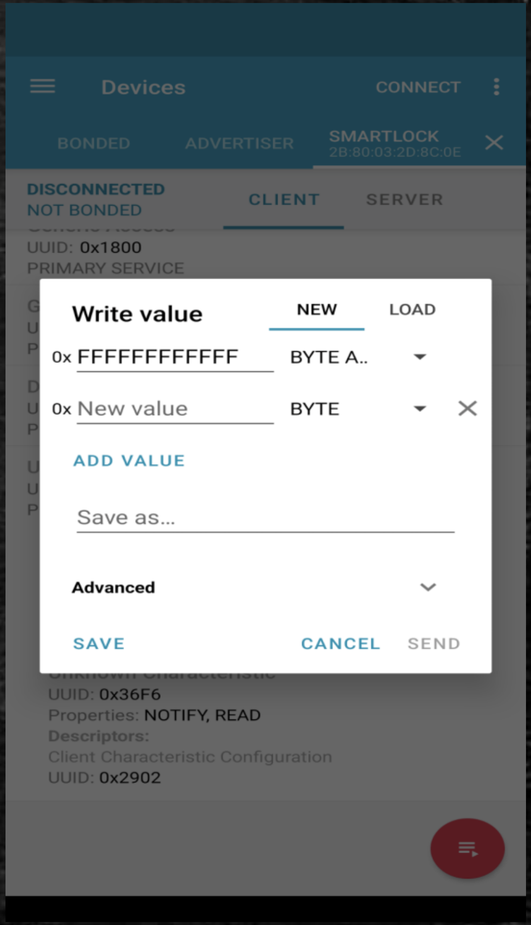
Battery Service
UUID: 0x180F
PRIMARY SERVICE

Device Information
UUID: 0x180A
PRIMARY SERVICE

Unknown Service
UUID: 73631912-6965-6e65-7269-736666727374

Tutorial

1. Click a row to expand
2. Sample macro
3. Send notifications every second



DISCONNECTED
NOT BONDED

UUID: 0x1800
PRIMARY SERVICE

Write value — NEW — LOAD

0x FFFFFFFFFFFF — BYTE A..

0x New value — BYTE

ADD VALUE

Save as...

Advanced

SAVE — CANCEL — SEND

UUID: 0x36F6
Properties: NOTIFY, READ
Descriptors:
Client Characteristic Configuration
UUID: 0x2902

# Select Tools for Bluetooth Sniffing

nrf52840 sniffer

~25$

Ubertooth One

~125$

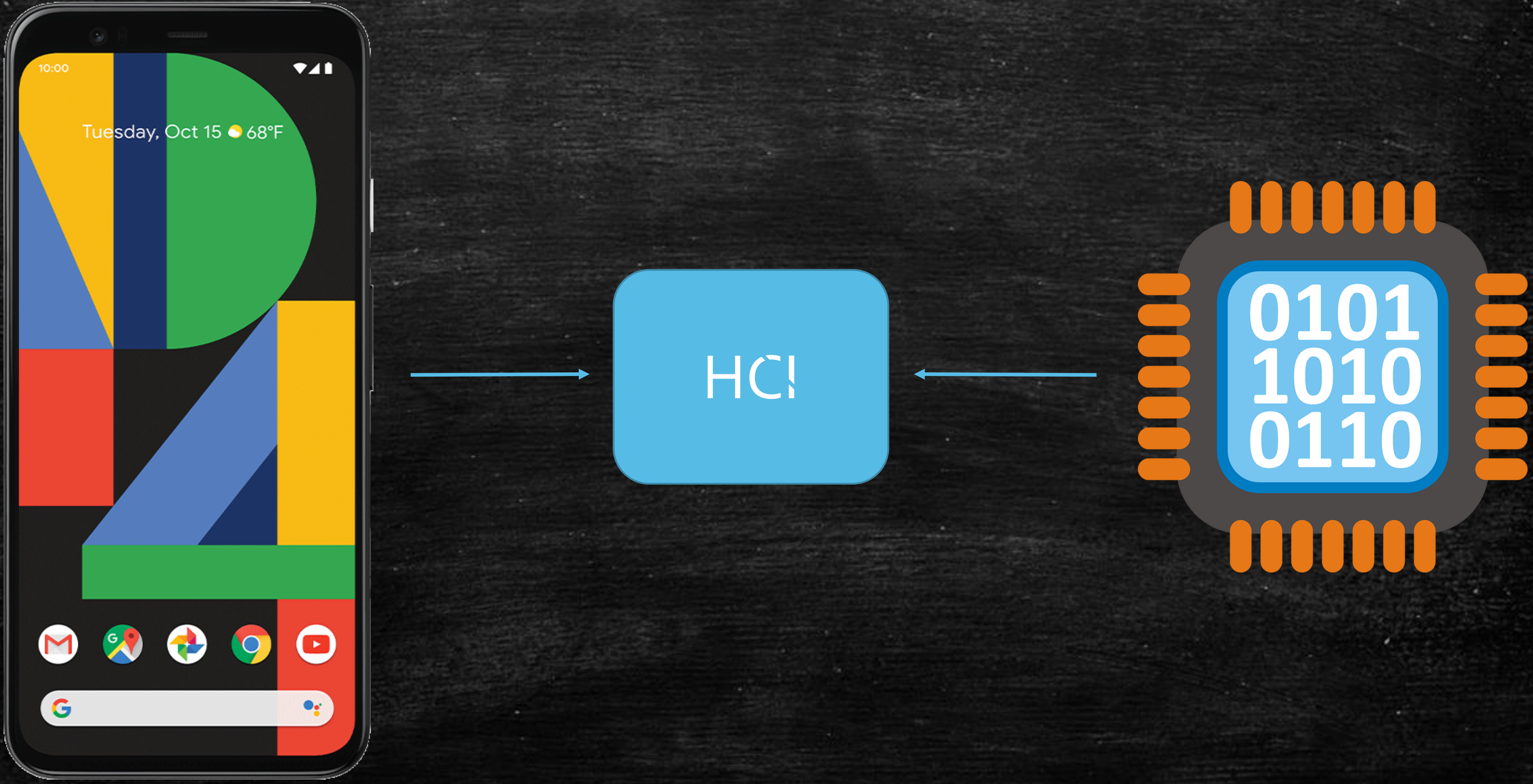
Ellisys Bluetooth Explorer

~25,000$

HOST

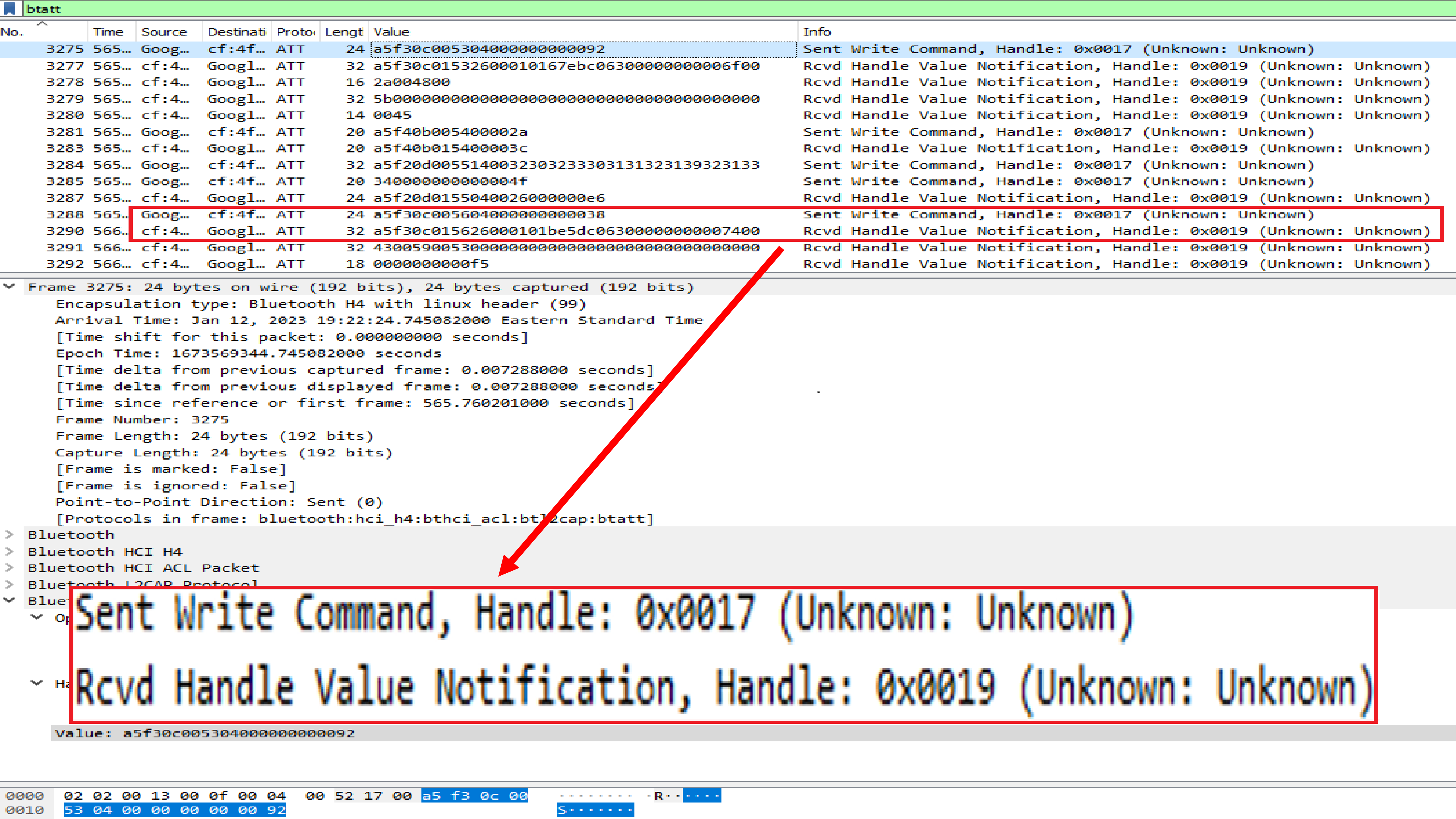
INTERFACE

CONTROLLER



HCI

# Find . -name "Random Bluetooth Blood Pressure Monitor"



btatt

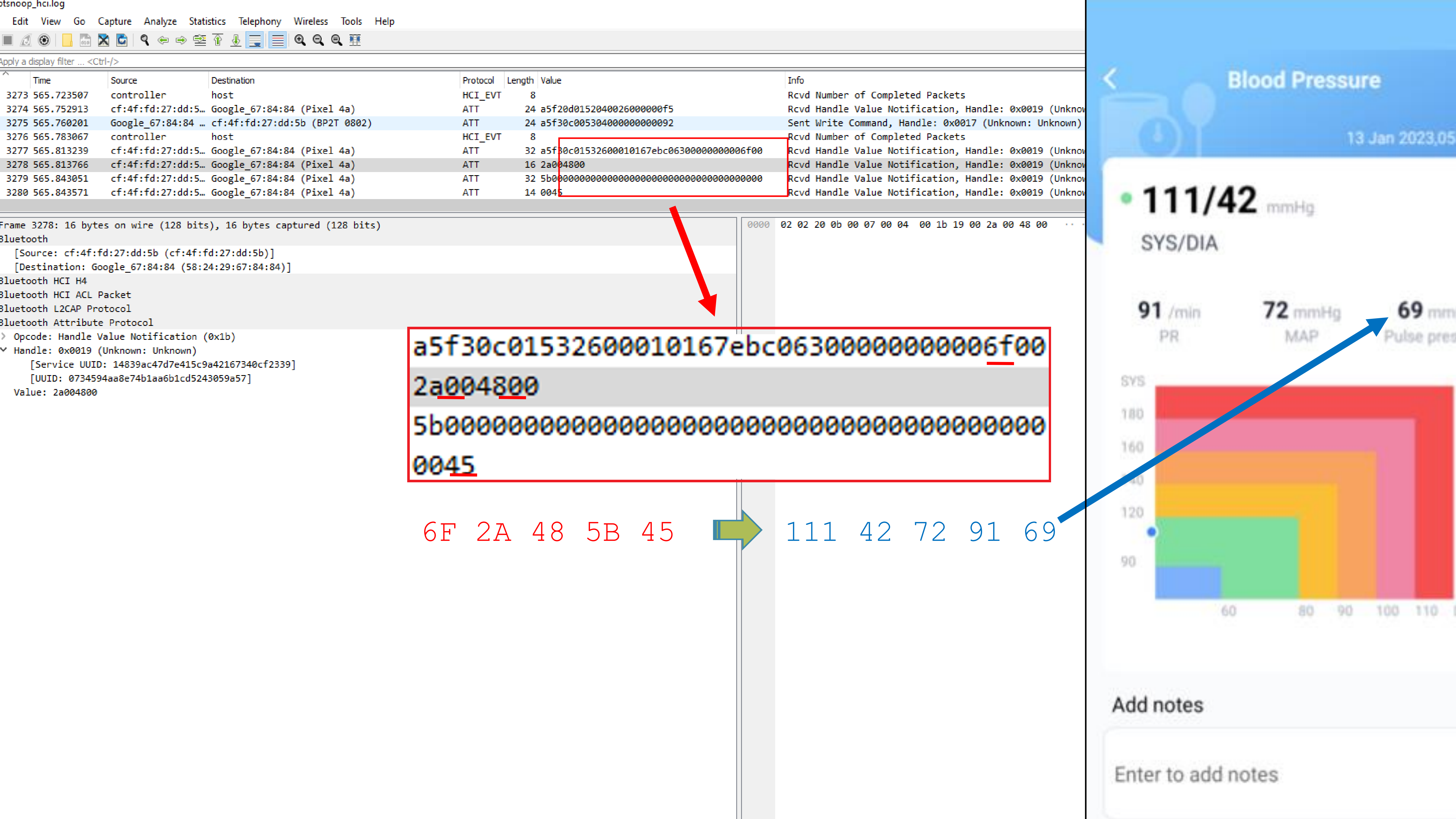
| No. | Time | Source | Destinati | Proto | Lengt | Value | Info |
|---|---|---|---|---|---|---|---|
| 3275 | 565… | Goog… | cf:4f… | ATT | 24 | a5f30c0053040000000000092 | Sent Write Command, Handle: 0x0017 (Unknown: Unknown) |
| 3277 | 565… | cf:4… | Googl… | ATT | 32 | a5f30c01532600010167ebc06300000000006f00 | Rcvd Handle Value Notification, Handle: 0x0019 (Unknown: Unknown) |
| 3278 | 565… | cf:4… | Googl… | ATT | 16 | 2a004800 | Rcvd Handle Value Notification, Handle: 0x0019 (Unknown: Unknown) |
| 3279 | 565… | cf:4… | Googl… | ATT | 32 | 5b000000000000000000000000000000000000000 | Rcvd Handle Value Notification, Handle: 0x0019 (Unknown: Unknown) |
| 3280 | 565… | cf:4… | Googl… | ATT | 14 | 0045 | Rcvd Handle Value Notification, Handle: 0x0019 (Unknown: Unknown) |
| 3281 | 565… | Goog… | cf:4f… | ATT | 20 | a5f40b005400002a | Sent Write Command, Handle: 0x0017 (Unknown: Unknown) |
| 3283 | 565… | cf:4… | Googl… | ATT | 20 | a5f40b015400003c | Rcvd Handle Value Notification, Handle: 0x0019 (Unknown: Unknown) |
| 3284 | 565… | Goog… | cf:4f… | ATT | 32 | a5f20d0055140032303233303131323139323133 | Sent Write Command, Handle: 0x0017 (Unknown: Unknown) |
| 3285 | 565… | Goog… | cf:4f… | ATT | 20 | 340000000000004f | Sent Write Command, Handle: 0x0017 (Unknown: Unknown) |
| 3287 | 565… | cf:4… | Googl… | ATT | 24 | a5f20d01550400260000000e6 | Rcvd Handle Value Notification, Handle: 0x0019 (Unknown: Unknown) |
| 3288 | 565… | Goog… | cf:4f… | ATT | 24 | a5f30c0056040000000000038 | Sent Write Command, Handle: 0x0017 (Unknown: Unknown) |
| 3290 | 566… | cf:4… | Googl… | ATT | 32 | a5f30c01562600010 1be5dc06300000000007400 | Rcvd Handle Value Notification, Handle: 0x0019 (Unknown: Unknown) |
| 3291 | 566… | cf:4… | Googl… | ATT | 32 | 43005900530000000000000000000000000000000 | Rcvd Handle Value Notification, Handle: 0x0019 (Unknown: Unknown) |
| 3292 | 566… | cf:4… | Googl… | ATT | 18 | 00000000000f5 | Rcvd Handle Value Notification, Handle: 0x0019 (Unknown: Unknown) |

```
Frame 3275: 24 bytes on wire (192 bits), 24 bytes captured (192 bits)
    Encapsulation type: Bluetooth H4 with linux header (99)
    Arrival Time: Jan 12, 2023 19:22:24.745082000 Eastern Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1673569344.745082000 seconds
    [Time delta from previous captured frame: 0.007288000 seconds]
    [Time delta from previous displayed frame: 0.007288000 seconds]
    [Time since reference or first frame: 565.760201000 seconds]
    Frame Number: 3275
    Frame Length: 24 bytes (192 bits)
    Capture Length: 24 bytes (192 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    Point-to-Point Direction: Sent (0)
    [Protocols in frame: bluetooth:hci_h4:bthci_acl:btl2cap:btatt]
Bluetooth
Bluetooth HCI H4
Bluetooth HCI ACL Packet
Bluetooth L2CAP Protocol
Blue
  Op

  Ha

    Value: a5f30c0053040000000000092
```

Sent Write Command, Handle: 0x0017 (Unknown: Unknown)

Rcvd Handle Value Notification, Handle: 0x0019 (Unknown: Unknown)

```
0000  02 02 00 13 00 0f 00 04  00 52 17 00 a5 f3 0c 00   ········ ·R······
0010  53 04 00 00 00 00 00 92                             S·······
```


tsnoop_hci.log
Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
     Time       Source              Destination                    Protocol  Length Value                                        Info
3273 565.723507 controller          host                           HCI_EVT      8                                                Rcvd Number of Completed Packets
3274 565.752913 cf:4f:fd:27:dd:5…   Google_67:84:84 (Pixel 4a)     ATT         24 a5f20d0152040026000000f5                  Rcvd Handle Value Notification, Handle: 0x0019 (Unknow
3275 565.760201 Google_67:84:84 …   cf:4f:fd:27:dd:5b (BP2T 0802)  ATT         24 a5f30c005304000000000092                  Sent Write Command, Handle: 0x0017 (Unknown: Unknown)
3276 565.783067 controller          host                           HCI_EVT      8                                                Rcvd Number of Completed Packets
3277 565.813239 cf:4f:fd:27:dd:5…   Google_67:84:84 (Pixel 4a)     ATT         32 a5f30c01532600010167ebc06300000000006f00  Rcvd Handle Value Notification, Handle: 0x0019 (Unknow
3278 565.813766 cf:4f:fd:27:dd:5…   Google_67:84:84 (Pixel 4a)     ATT         16 2a004800                                  Rcvd Handle Value Notification, Handle: 0x0019 (Unknow
3279 565.843051 cf:4f:fd:27:dd:5…   Google_67:84:84 (Pixel 4a)     ATT         32 5b000000000000000000000000000000000000  Rcvd Handle Value Notification, Handle: 0x0019 (Unknow
3280 565.843571 cf:4f:fd:27:dd:5…   Google_67:84:84 (Pixel 4a)     ATT         14 0045                                      Rcvd Handle Value Notification, Handle: 0x0019 (Unknow
```

```
Frame 3278: 16 bytes on wire (128 bits), 16 bytes captured (128 bits)
Bluetooth
    [Source: cf:4f:fd:27:dd:5b (cf:4f:fd:27:dd:5b)]
    [Destination: Google_67:84:84 (58:24:29:67:84:84)]
Bluetooth HCI H4
Bluetooth HCI ACL Packet
Bluetooth L2CAP Protocol
Bluetooth Attribute Protocol
  > Opcode: Handle Value Notification (0x1b)
  v Handle: 0x0019 (Unknown: Unknown)
        [Service UUID: 14839ac47d7e415c9a42167340cf2339]
        [UUID: 0734594aa8e74b1aa6b1cd5243059a57]
    Value: 2a004800
```

```
0000  02 02 20 0b 00 07 00 04  00 1b 19 00 2a 00 48 00   ··
```

```
a5f30c01532600010167ebc06300000000006f00
2a004800
5b00000000000000000000000000000000000000
0045
```

6F 2A 48 5B 45 ➡ 111 42 72 91 69

Blood Pressure

13 Jan 2023,05

111/42 mmHg

SYS/DIA

91 /min PR

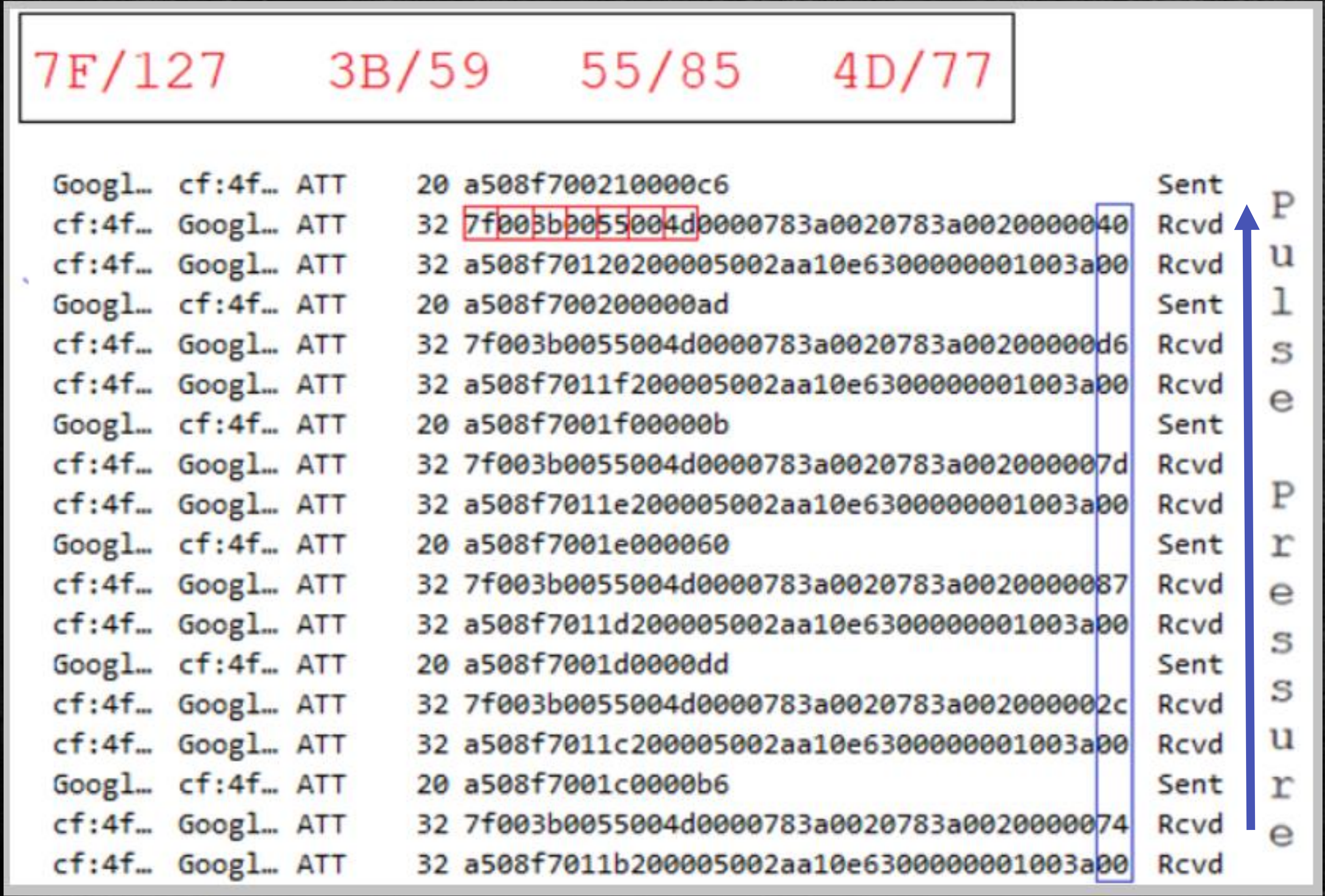
72 mmHg MAP

69 mm Pulse pres

Add notes

Enter to add notes

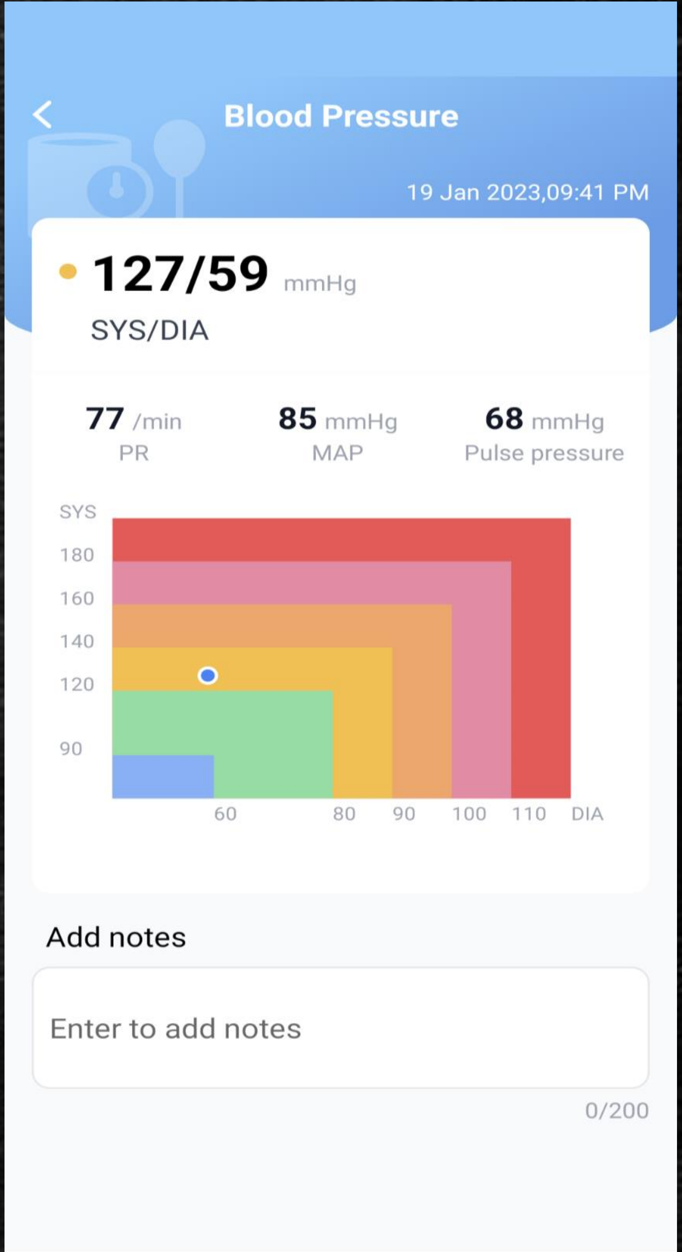
# Trial && ERROR



7F/127    3B/59    55/85    4D/77

```
Googl… cf:4f… ATT    20 a508f700210000c6                            Sent
cf:4f… Googl… ATT    32 7f003b0055004d0000783a0020783a0020000040    Rcvd
cf:4f… Googl… ATT    32 a508f70120200005002aa10e6300000001003a00    Rcvd
Googl… cf:4f… ATT    20 a508f700200000ad                            Sent
cf:4f… Googl… ATT    32 7f003b0055004d0000783a0020783a00200000d6    Rcvd
cf:4f… Googl… ATT    32 a508f7011f200005002aa10e6300000001003a00    Rcvd
Googl… cf:4f… ATT    20 a508f7001f00000b                            Sent
cf:4f… Googl… ATT    32 7f003b0055004d0000783a0020783a002000007d    Rcvd
cf:4f… Googl… ATT    32 a508f7011e200005002aa10e6300000001003a00    Rcvd
Googl… cf:4f… ATT    20 a508f7001e000060                            Sent
cf:4f… Googl… ATT    32 7f003b0055004d0000783a0020783a0020000087    Rcvd
cf:4f… Googl… ATT    32 a508f7011d200005002aa10e6300000001003a00    Rcvd
Googl… cf:4f… ATT    20 a508f7001d0000dd                            Sent
cf:4f… Googl… ATT    32 7f003b0055004d0000783a0020783a002000002c    Rcvd
cf:4f… Googl… ATT    32 a508f7011c200005002aa10e6300000001003a00    Rcvd
Googl… cf:4f… ATT    20 a508f7001c0000b6                            Sent
cf:4f… Googl… ATT    32 7f003b0055004d0000783a0020783a0020000074    Rcvd
cf:4f… Googl… ATT    32 a508f7011b200005002aa10e6300000001003a00    Rcvd
```

Pulse Pressure



19 Jan 2023,09:41 PM

127/59 mmHg

SYS/DIA

77 /min PR

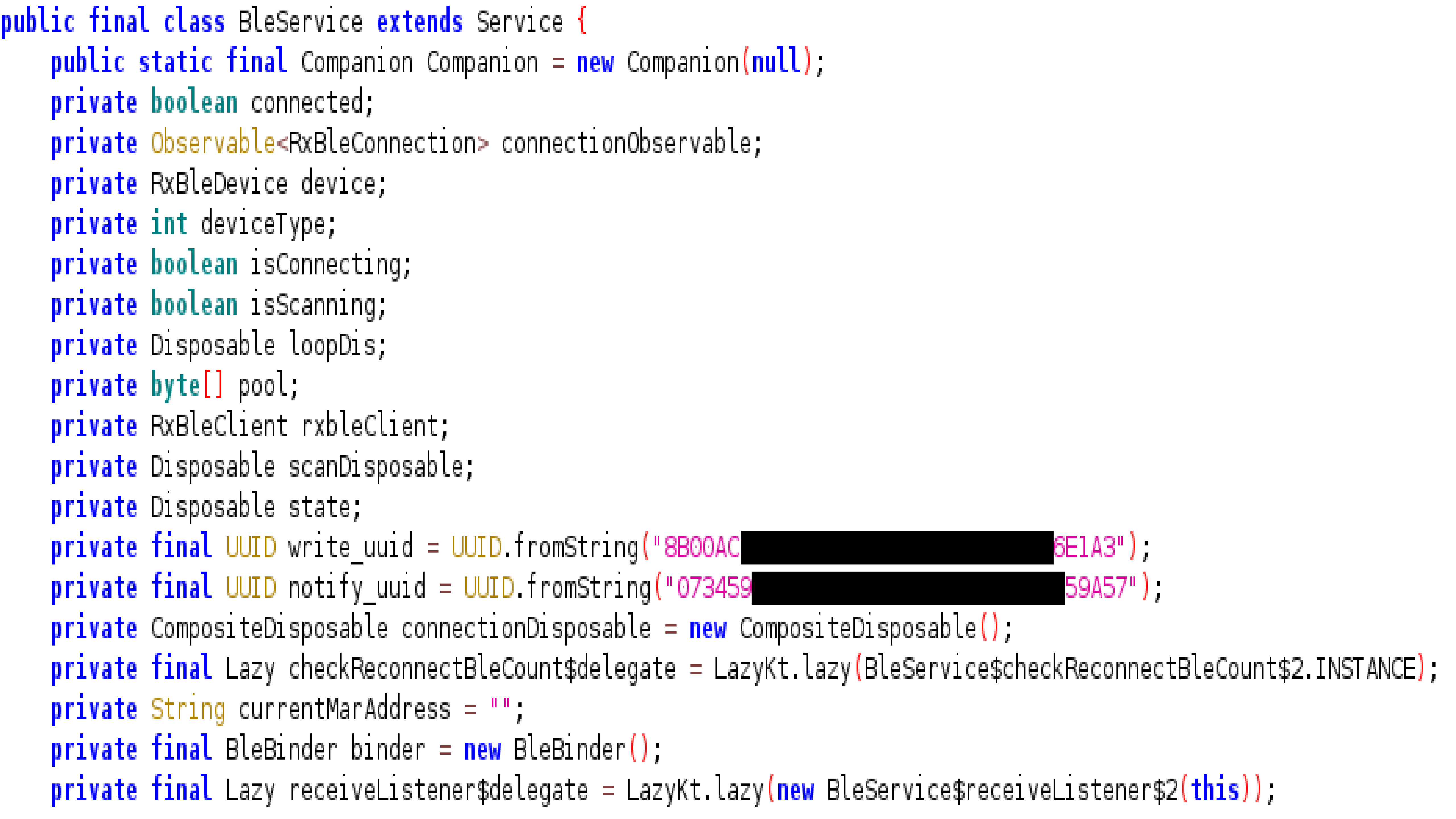
85 mmHg MAP

68 mmHg Pulse pressure

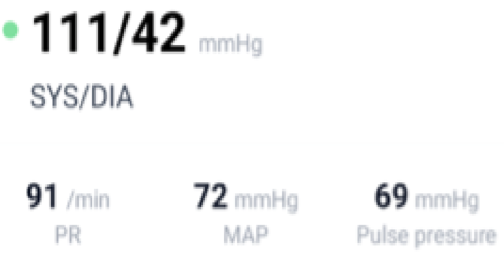
Add notes

Enter to add notes

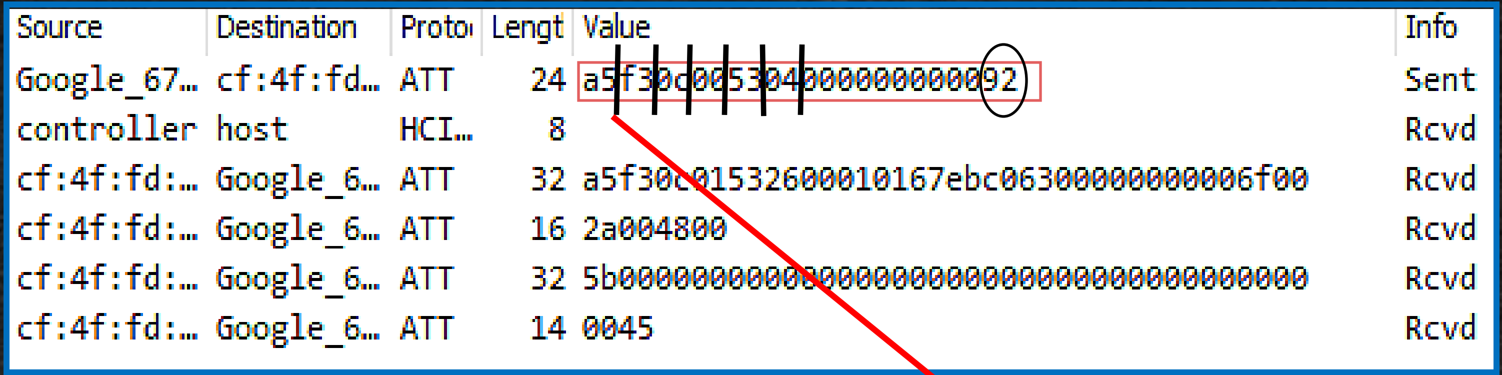
0/200



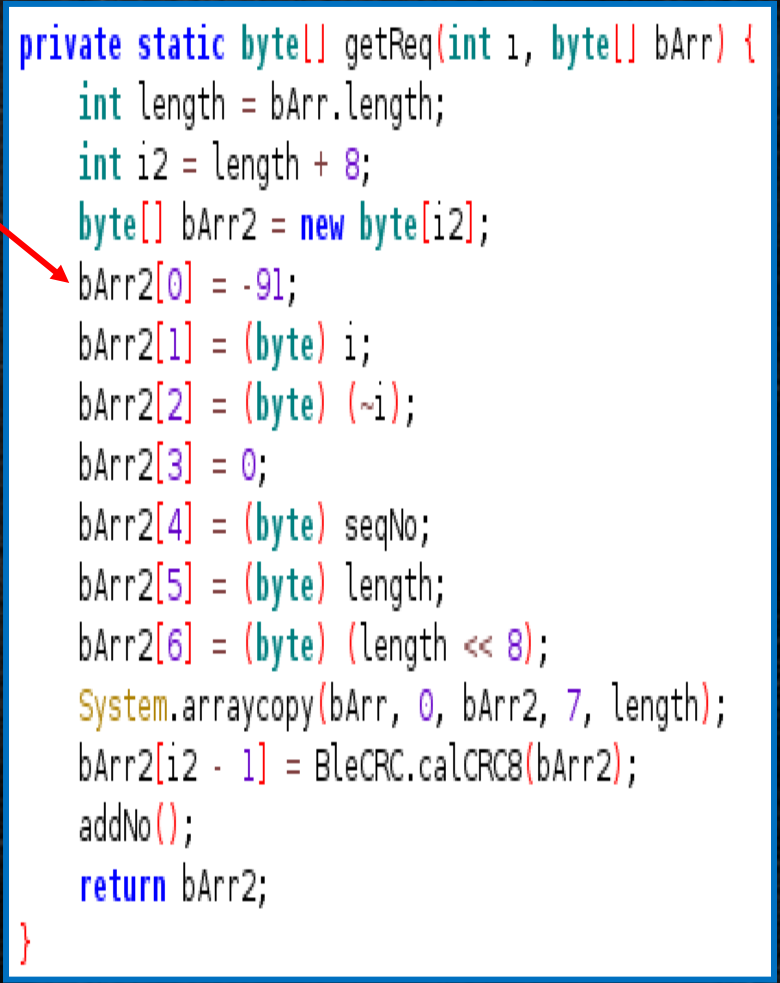
```java
public final class BleService extends Service {
    public static final Companion Companion = new Companion(null);
    private boolean connected;
    private Observable<RxBleConnection> connectionObservable;
    private RxBleDevice device;
    private int deviceType;
    private boolean isConnecting;
    private boolean isScanning;
    private Disposable loopDis;
    private byte[] pool;
    private RxBleClient rxbleClient;
    private Disposable scanDisposable;
    private Disposable state;
    private final UUID write_uuid = UUID.fromString("8B00AC[redacted]6E1A3");
    private final UUID notify_uuid = UUID.fromString("073459[redacted]59A57");
    private CompositeDisposable connectionDisposable = new CompositeDisposable();
    private final Lazy checkReconnectBleCount$delegate = LazyKt.lazy(BleService$checkReconnectBleCount$2.INSTANCE);
    private String currentMarAddress = "";
    private final BleBinder binder = new BleBinder();
    private final Lazy receiveListener$delegate = LazyKt.lazy(new BleService$receiveListener$2(this));
```



| 6F | 2A | 48 | 5B | 45 |
|---|---|---|---|---|
| 111 | 42 | 72 | 91 | 69 |



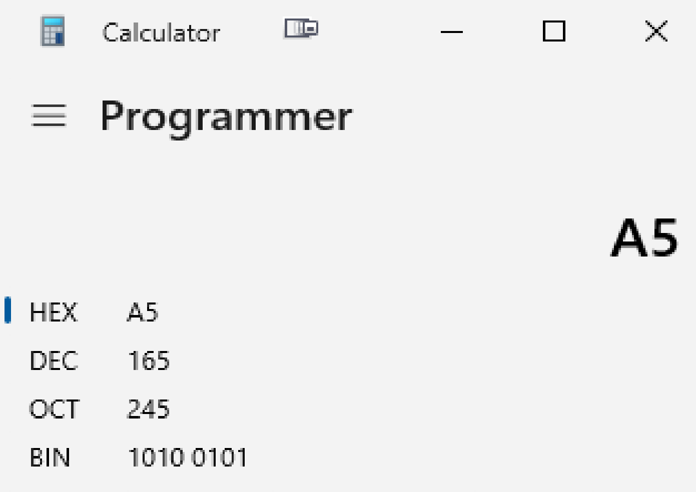
| Source | Destination | Proto | Lengt | Value | Info |
|---|---|---|---|---|---|
| Google_67… | cf:4f:fd… | ATT | 24 | a5f30c005304000000000092 | Sent |
| controller | host | HCI… | 8 | | Rcvd |
| cf:4f:fd:… | Google_6… | ATT | 32 | a5f30c01532600010167ebc06300000000006f00 | Rcvd |
| cf:4f:fd:… | Google_6… | ATT | 16 | 2a004800 | Rcvd |
| cf:4f:fd:… | Google_6… | ATT | 32 | 5b00000000000000000000000000000000000000 | Rcvd |
| cf:4f:fd:… | Google_6… | ATT | 14 | 0045 | Rcvd |



```java
private static byte[] getReq(int i, byte[] bArr) {
    int length = bArr.length;
    int i2 = length + 8;
    byte[] bArr2 = new byte[i2];
    bArr2[0] = -91;
    bArr2[1] = (byte) i;
    bArr2[2] = (byte) (~i);
    bArr2[3] = 0;
    bArr2[4] = (byte) seqNo;
    bArr2[5] = (byte) length;
    bArr2[6] = (byte) (length << 8);
    System.arraycopy(bArr, 0, bArr2, 7, length);
    bArr2[i2 - 1] = BleCRC.calCRC8(bArr2);
    addNo();
    return bArr2;
}
```

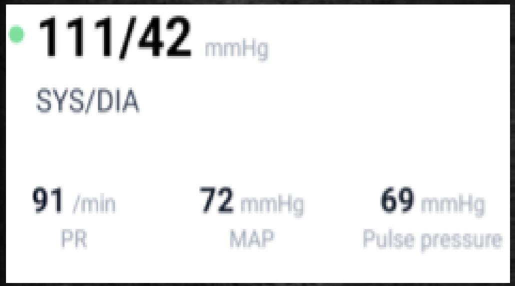
```
01011011  = 91
10100101  =-91
```

| Hex | A5 | F3 | 0C | 00 | 53 | 04 |
|---|---|---|---|---|---|---|
| Dec | 165 | 243 | 12 | 0 | 83 | 4 |
| Byte Array Position | 0 | 1 | 2 | 3 | 4 | 5 |

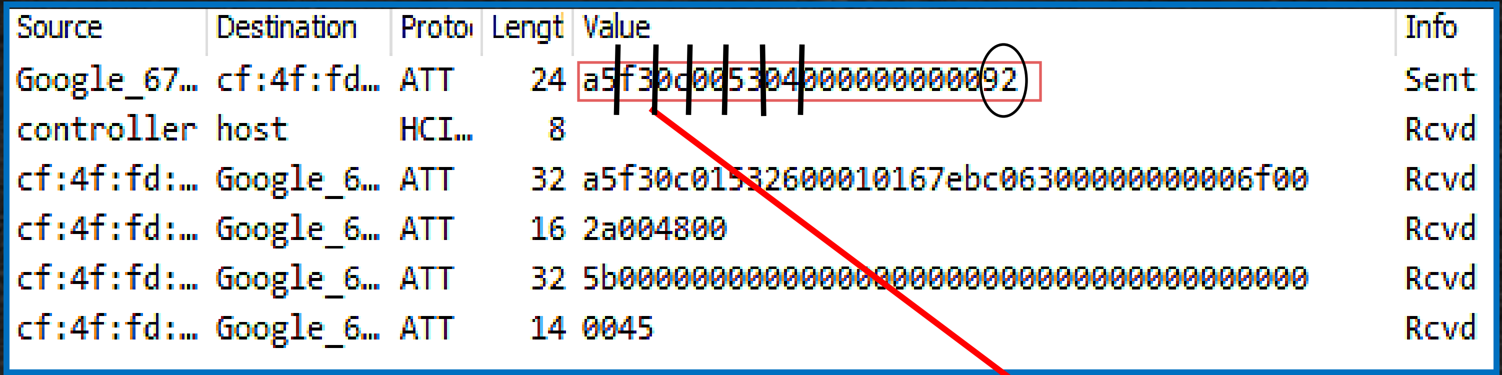


A5

HEX A5
DEC 165
OCT 245
BIN 1010 0101

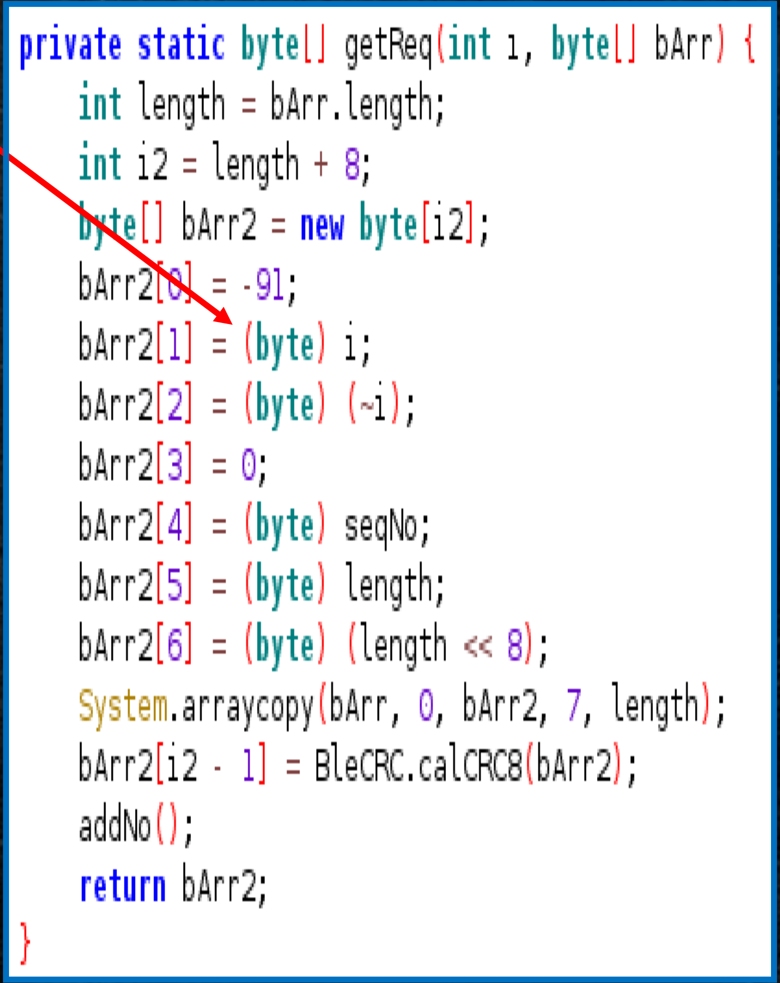


| 6F | 2A | 48 | 5B | 45 |
|---|---|---|---|---|
| 111 | 42 | 72 | 91 | 69 |

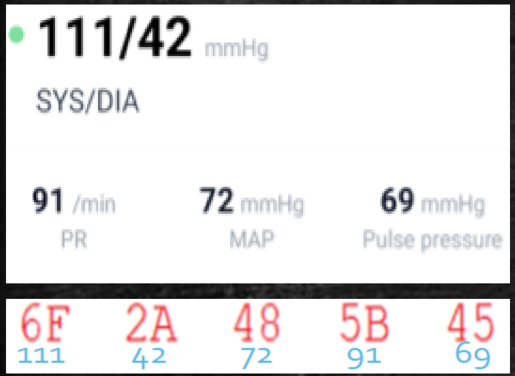


| Source | Destination | Proto | Lengt | Value | Info |
|---|---|---|---|---|---|
| Google_67… | cf:4f:fd… | ATT | 24 | a5f30c0053040000000000092 | Sent |
| controller | host | HCI… | 8 | | Rcvd |
| cf:4f:fd:… | Google_6… | ATT | 32 | a5f30c01532600010167ebc06300000000006f00 | Rcvd |
| cf:4f:fd:… | Google_6… | ATT | 16 | 2a004800 | Rcvd |
| cf:4f:fd:… | Google_6… | ATT | 32 | 5b00000000000000000000000000000000000000 | Rcvd |
| cf:4f:fd:… | Google_6… | ATT | 14 | 0045 | Rcvd |

| Hex | A5 | F3 | 0C | 00 | 53 | 04 |
|---|---|---|---|---|---|---|
| Dec | 165 | 243 | 12 | 0 | 83 | 4 |
| Byte Array Position | 0 | 1 | 2 | 3 | 4 | 5 |



```java
private static byte[] getReq(int i, byte[] bArr) {
    int length = bArr.length;
    int i2 = length + 8;
    byte[] bArr2 = new byte[i2];
    bArr2[0] = -91;
    bArr2[1] = (byte) i;
    bArr2[2] = (byte) (~i);
    bArr2[3] = 0;
    bArr2[4] = (byte) seqNo;
    bArr2[5] = (byte) length;
    bArr2[6] = (byte) (length << 8);
    System.arraycopy(bArr, 0, bArr2, 7, length);
    bArr2[i2 - 1] = BleCRC.calCRC8(bArr2);
    addNo();
    return bArr2;
}
```



111/42 mmHg

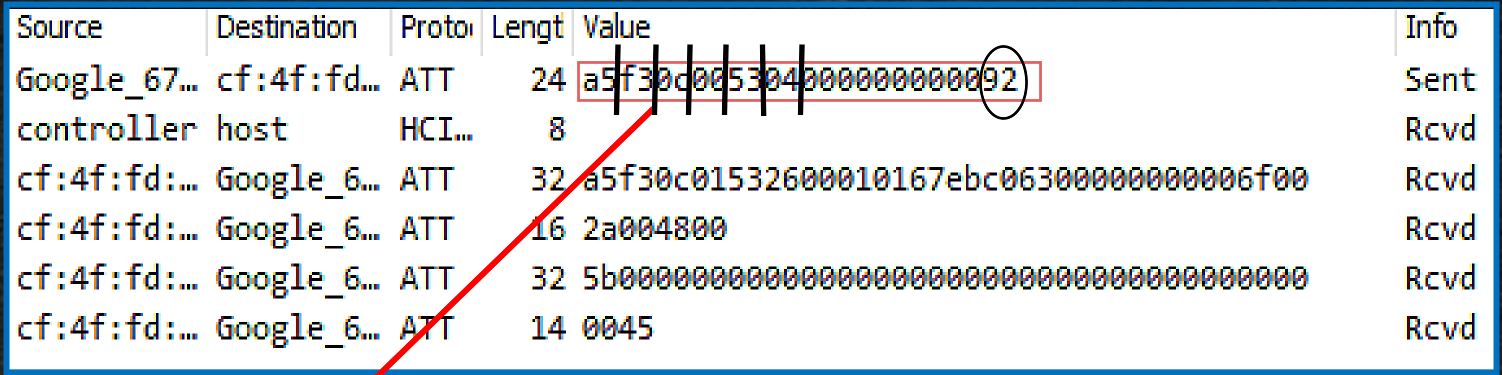
SYS/DIA

91 /min PR

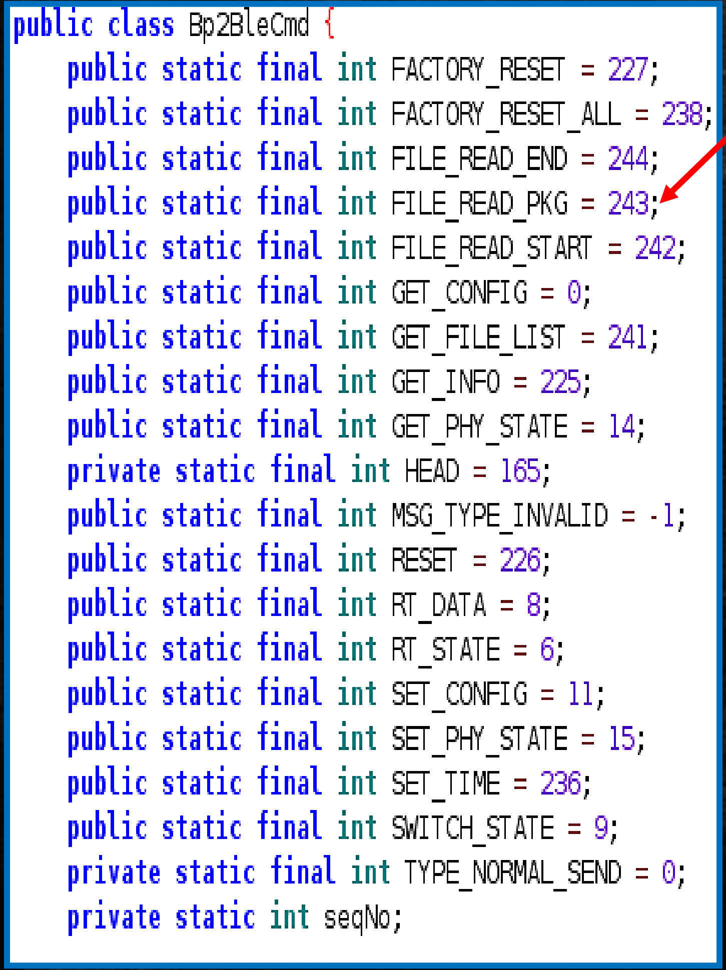
72 mmHg MAP

69 mmHg Pulse pressure

| 6F | 2A | 48 | 5B | 45 |
|---|---|---|---|---|
| 111 | 42 | 72 | 91 | 69 |

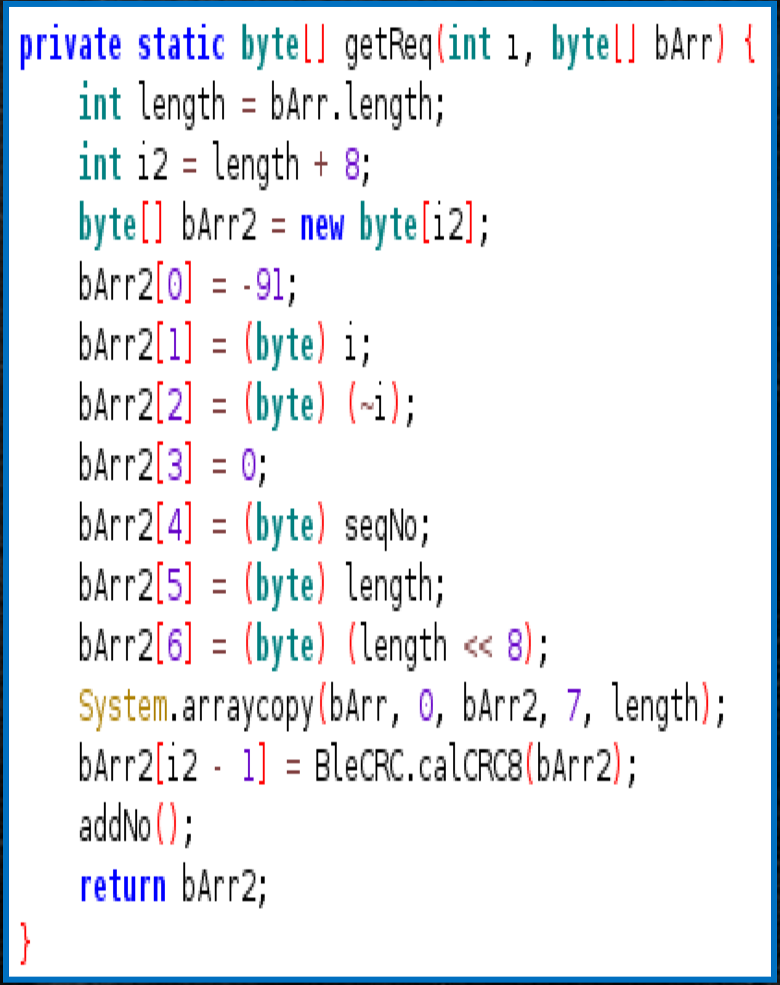


```
Source          Destination   Proto  Lengt  Value                                      Info
Google_67…      cf:4f:fd…     ATT      24   a5f30c005304000000000092                   Sent
controller      host          HCI…      8                                              Rcvd
cf:4f:fd:…      Google_6…     ATT      32   a5f30c01532600010167ebc06300000000006f00   Rcvd
cf:4f:fd:…      Google_6…     ATT      16   2a004800                                   Rcvd
cf:4f:fd:…      Google_6…     ATT      32   5b00000000000000000000000000000000000000   Rcvd
cf:4f:fd:…      Google_6…     ATT      14   0045                                       Rcvd
```

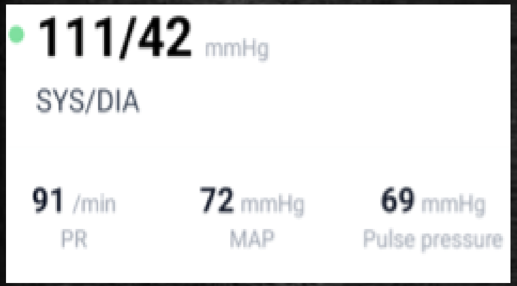


```java
public class Bp2BleCmd {
    public static final int FACTORY_RESET = 227;
    public static final int FACTORY_RESET_ALL = 238;
    public static final int FILE_READ_END = 244;
    public static final int FILE_READ_PKG = 243;
    public static final int FILE_READ_START = 242;
    public static final int GET_CONFIG = 0;
    public static final int GET_FILE_LIST = 241;
    public static final int GET_INFO = 225;
    public static final int GET_PHY_STATE = 14;
    private static final int HEAD = 165;
    public static final int MSG_TYPE_INVALID = -1;
    public static final int RESET = 226;
    public static final int RT_DATA = 8;
    public static final int RT_STATE = 6;
    public static final int SET_CONFIG = 11;
    public static final int SET_PHY_STATE = 15;
    public static final int SET_TIME = 236;
    public static final int SWITCH_STATE = 9;
    private static final int TYPE_NORMAL_SEND = 0;
    private static int seqNo;
```

| Hex | A5 | F3 | 0C | 00 | 53 | 04 |
|---|---|---|---|---|---|---|
| Dec | 165 | 243 | 12 | 0 | 83 | 4 |
| Byte Array Position | 0 | 1 | 2 | 3 | 4 | 5 |



```java
private static byte[] getReq(int i, byte[] bArr) {
    int length = bArr.length;
    int i2 = length + 8;
    byte[] bArr2 = new byte[i2];
    bArr2[0] = -91;
    bArr2[1] = (byte) i;
    bArr2[2] = (byte) (~i);
    bArr2[3] = 0;
    bArr2[4] = (byte) seqNo;
    bArr2[5] = (byte) length;
    bArr2[6] = (byte) (length << 8);
    System.arraycopy(bArr, 0, bArr2, 7, length);
    bArr2[i2 - 1] = BleCRC.calCRC8(bArr2);
    addNo();
    return bArr2;
}
```



111/42 mmHg

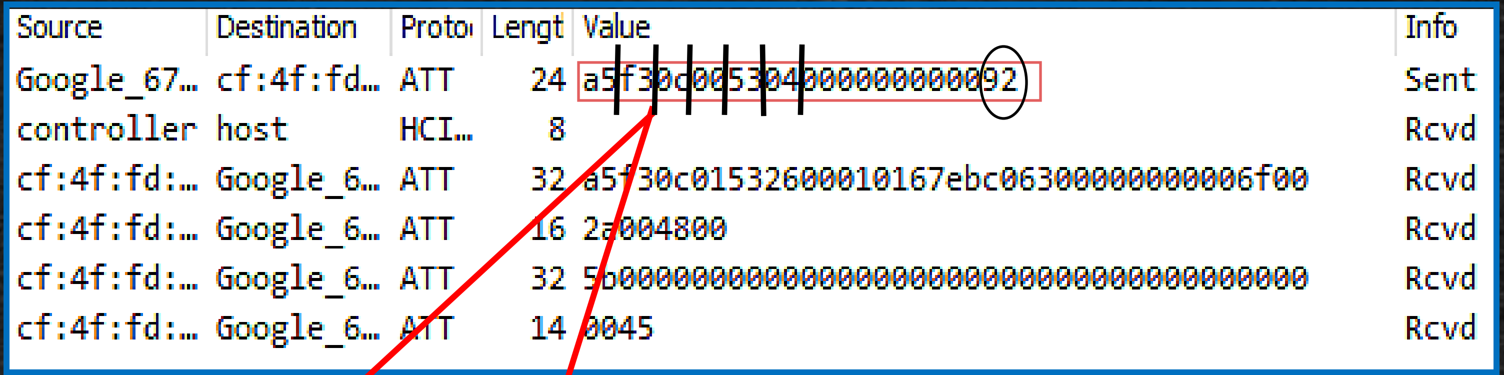
SYS/DIA

91 /min
PR

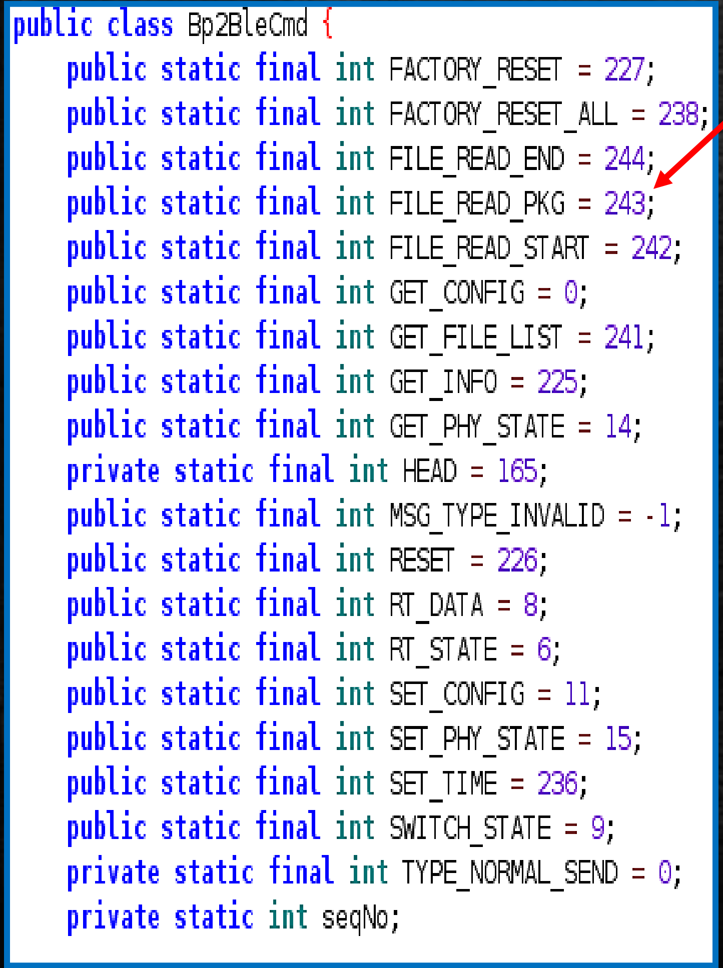
72 mmHg
MAP

69 mmHg
Pulse pressure

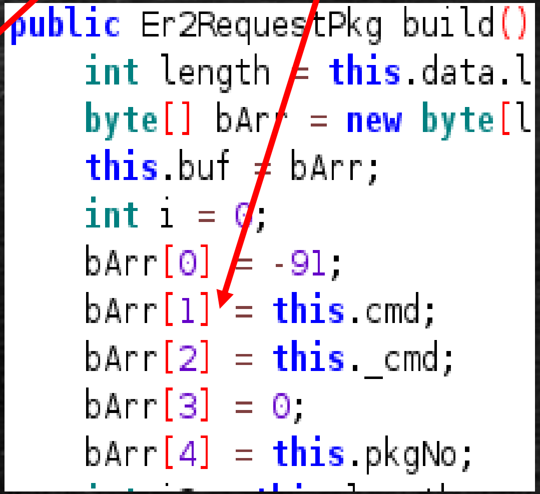
| 6F | 2A | 48 | 5B | 45 |
|---|---|---|---|---|
| 111 | 42 | 72 | 91 | 69 |



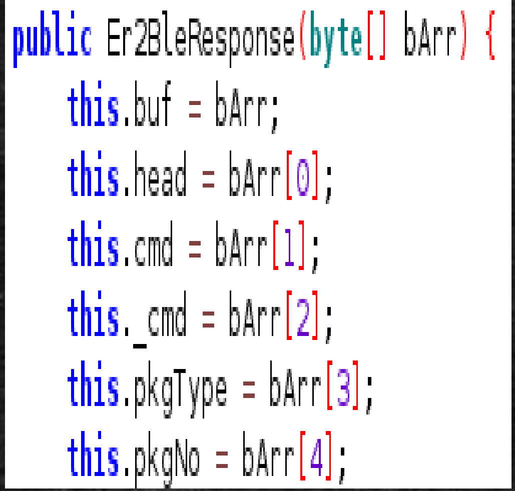
```
Source          Destination     Proto   Lengt  Value                                          Info
Google_67…      cf:4f:fd…       ATT        24  a5f30c005304000000000092                       Sent
controller      host            HCI…        8                                                 Rcvd
cf:4f:fd:…      Google_6…       ATT        32  a5f30c01532600010167ebc06300000000006f00       Rcvd
cf:4f:fd:…      Google_6…       ATT        16  2a004800                                       Rcvd
cf:4f:fd:…      Google_6…       ATT        32  5b0000000000000000000000000000000000000        Rcvd
cf:4f:fd:…      Google_6…       ATT        14  0045                                           Rcvd
```



```java
public class Bp2BleCmd {
    public static final int FACTORY_RESET = 227;
    public static final int FACTORY_RESET_ALL = 238;
    public static final int FILE_READ_END = 244;
    public static final int FILE_READ_PKG = 243;
    public static final int FILE_READ_START = 242;
    public static final int GET_CONFIG = 0;
    public static final int GET_FILE_LIST = 241;
    public static final int GET_INFO = 225;
    public static final int GET_PHY_STATE = 14;
    private static final int HEAD = 165;
    public static final int MSG_TYPE_INVALID = -1;
    public static final int RESET = 226;
    public static final int RT_DATA = 8;
    public static final int RT_STATE = 6;
    public static final int SET_CONFIG = 11;
    public static final int SET_PHY_STATE = 15;
    public static final int SET_TIME = 236;
    public static final int SWITCH_STATE = 9;
    private static final int TYPE_NORMAL_SEND = 0;
    private static int seqNo;
```

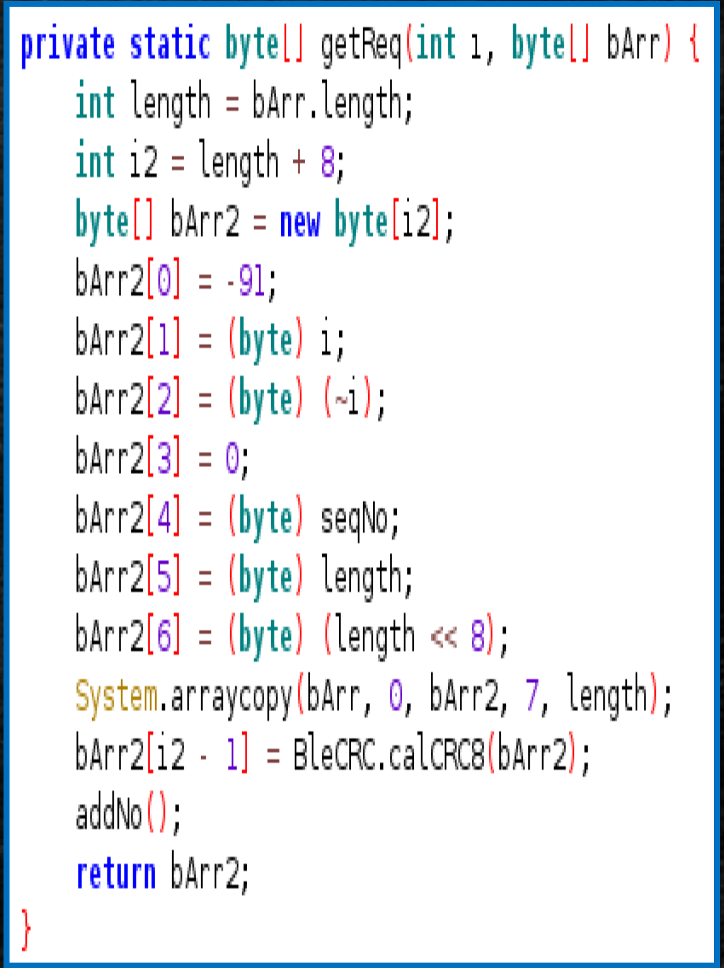


```java
public Er2RequestPkg build()
    int length = this.data.l
    byte[] bArr = new byte[l
    this.buf = bArr;
    int i = 0;
    bArr[0] = -91;
    bArr[1] = this.cmd;
    bArr[2] = this._cmd;
    bArr[3] = 0;
    bArr[4] = this.pkgNo;
```

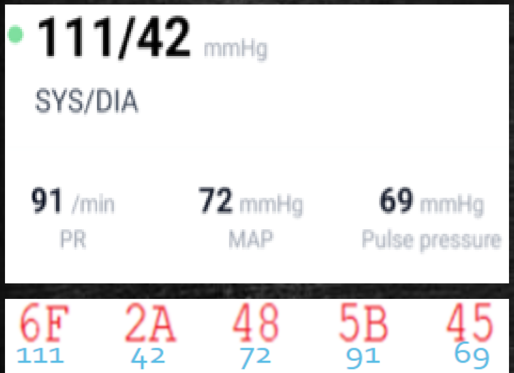


```java
public Er2BleResponse(byte[] bArr) {
    this.buf = bArr;
    this.head = bArr[0];
    this.cmd = bArr[1];
    this._cmd = bArr[2];
    this.pkgType = bArr[3];
    this.pkgNo = bArr[4];
```

| Hex | A5 | F3 | 0C | 00 | 53 | 04 |
|---|---|---|---|---|---|---|
| Dec | 165 | 243 | 12 | 0 | 83 | 4 |
| Byte Array Position | 0 | 1 | 2 | 3 | 4 | 5 |



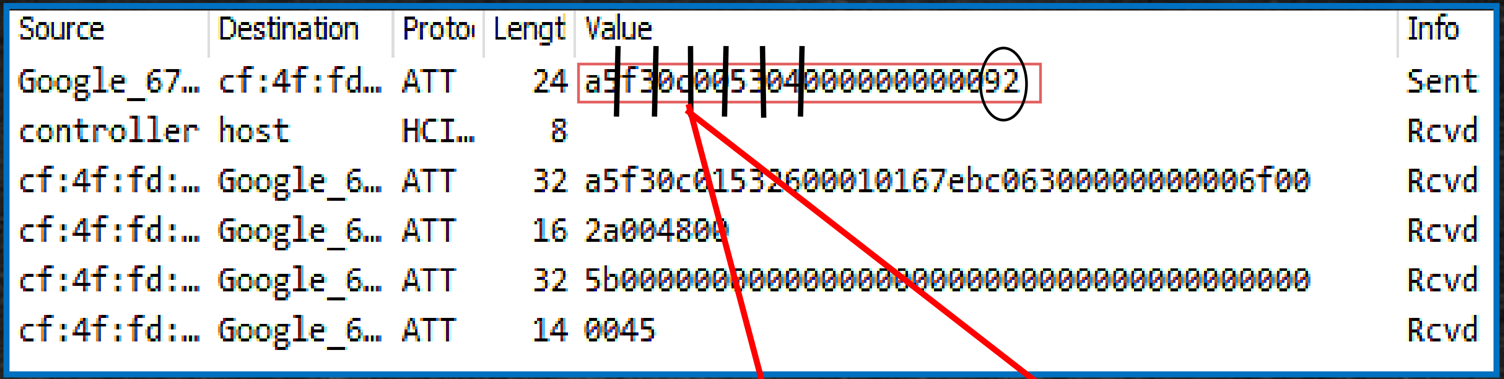
```java
private static byte[] getReq(int i, byte[] bArr) {
    int length = bArr.length;
    int i2 = length + 8;
    byte[] bArr2 = new byte[i2];
    bArr2[0] = -91;
    bArr2[1] = (byte) i;
    bArr2[2] = (byte) (~i);
    bArr2[3] = 0;
    bArr2[4] = (byte) seqNo;
    bArr2[5] = (byte) length;
    bArr2[6] = (byte) (length << 8);
    System.arraycopy(bArr, 0, bArr2, 7, length);
    bArr2[i2 - 1] = BleCRC.calCRC8(bArr2);
    addNo();
    return bArr2;
}
```



111/42 mmHg
SYS/DIA

| 91 /min | 72 mmHg | 69 mmHg |
|---|---|---|
| PR | MAP | Pulse pressure |

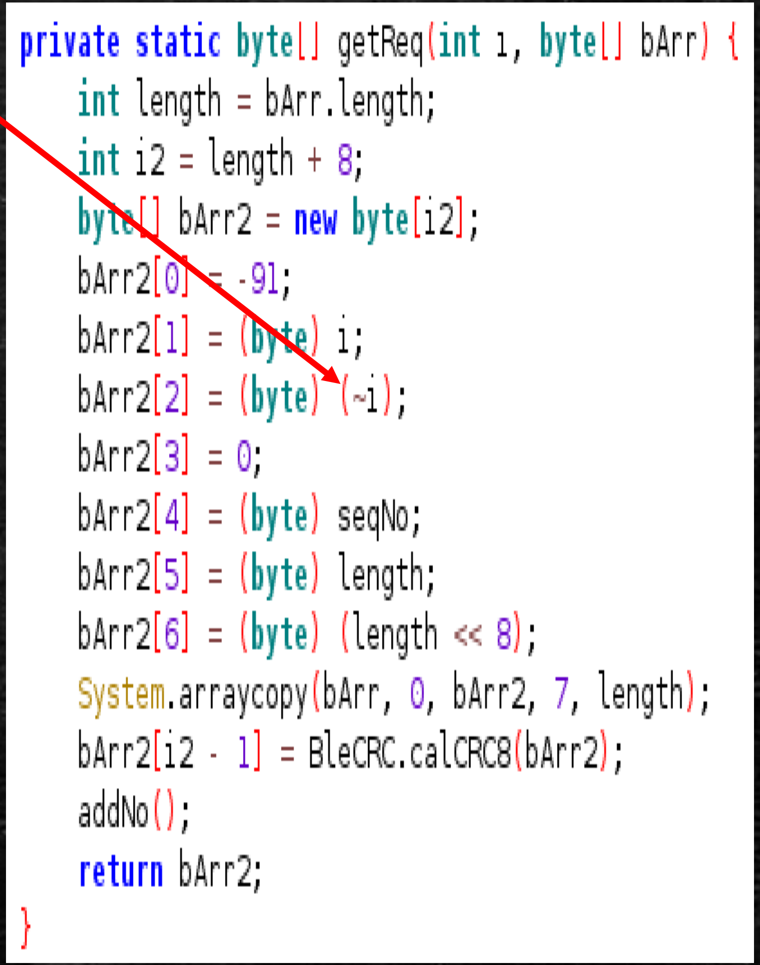
| 6F | 2A | 48 | 5B | 45 |
|---|---|---|---|---|
| 111 | 42 | 72 | 91 | 69 |



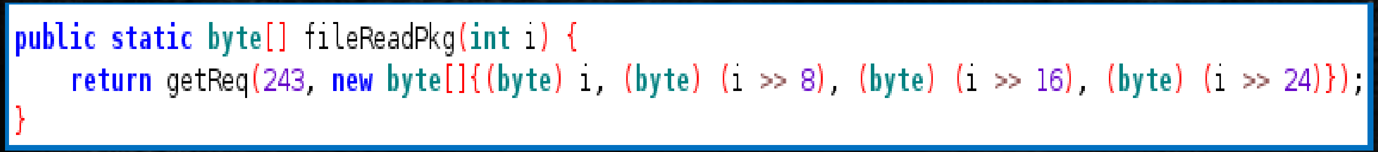
| Source | Destination | Proto | Lengt | Value | Info |
|---|---|---|---|---|---|
| Google_67… | cf:4f:fd… | ATT | 24 | a5f30c005304000000000092 | Sent |
| controller | host | HCI… | 8 |  | Rcvd |
| cf:4f:fd:… | Google_6… | ATT | 32 | a5f30c01532600010167ebc06300000000006f00 | Rcvd |
| cf:4f:fd:… | Google_6… | ATT | 16 | 2a004800 | Rcvd |
| cf:4f:fd:… | Google_6… | ATT | 32 | 5b000000000000000000000000000000000000000 | Rcvd |
| cf:4f:fd:… | Google_6… | ATT | 14 | 0045 | Rcvd |

11110011 = 243
00001100 = 12

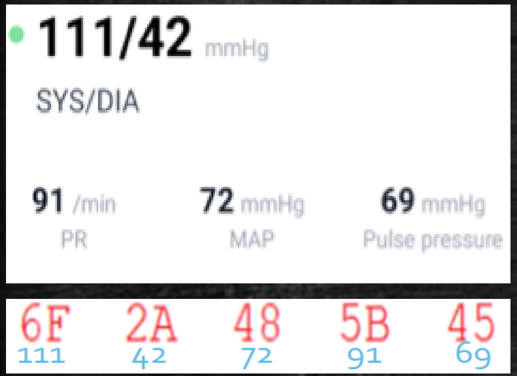
| Hex | A5 | F3 | 0C | 00 | 53 | 04 |
|---|---|---|---|---|---|---|
| Dec | 165 | 243 | 12 | 0 | 83 | 4 |
| Byte Array Position | 0 | 1 | 2 | 3 | 4 | 5 |



```java
private static byte[] getReq(int i, byte[] bArr) {
    int length = bArr.length;
    int i2 = length + 8;
    byte[] bArr2 = new byte[i2];
    bArr2[0] = -91;
    bArr2[1] = (byte) i;
    bArr2[2] = (byte) (~i);
    bArr2[3] = 0;
    bArr2[4] = (byte) seqNo;
    bArr2[5] = (byte) length;
    bArr2[6] = (byte) (length << 8);
    System.arraycopy(bArr, 0, bArr2, 7, length);
    bArr2[i2 - 1] = BleCRC.calCRC8(bArr2);
    addNo();
    return bArr2;
}
```



```java
public static byte[] fileReadPkg(int i) {
    return getReq(243, new byte[]{(byte) i, (byte) (i >> 8), (byte) (i >> 16), (byte) (i >> 24)});
}
```

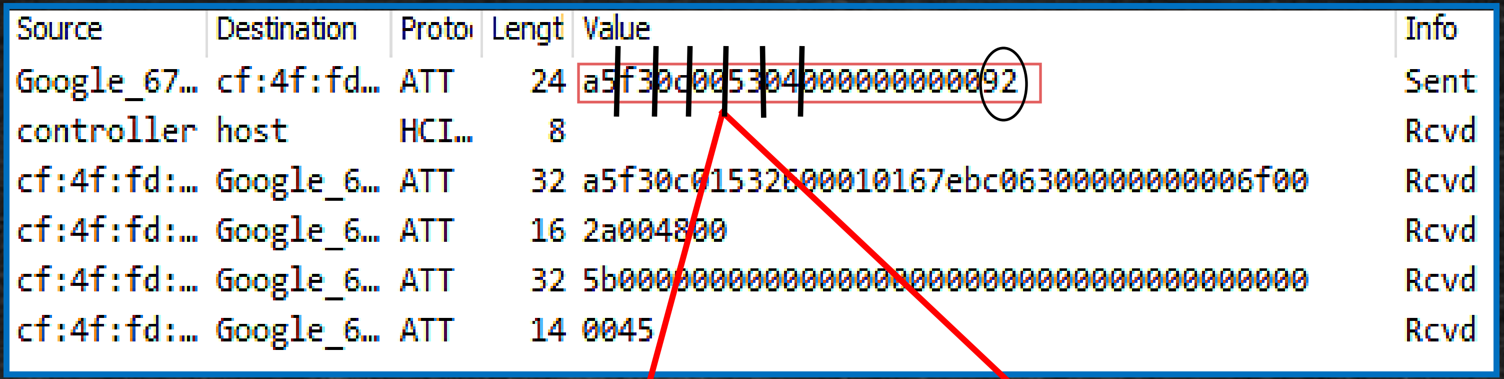


111/42 mmHg

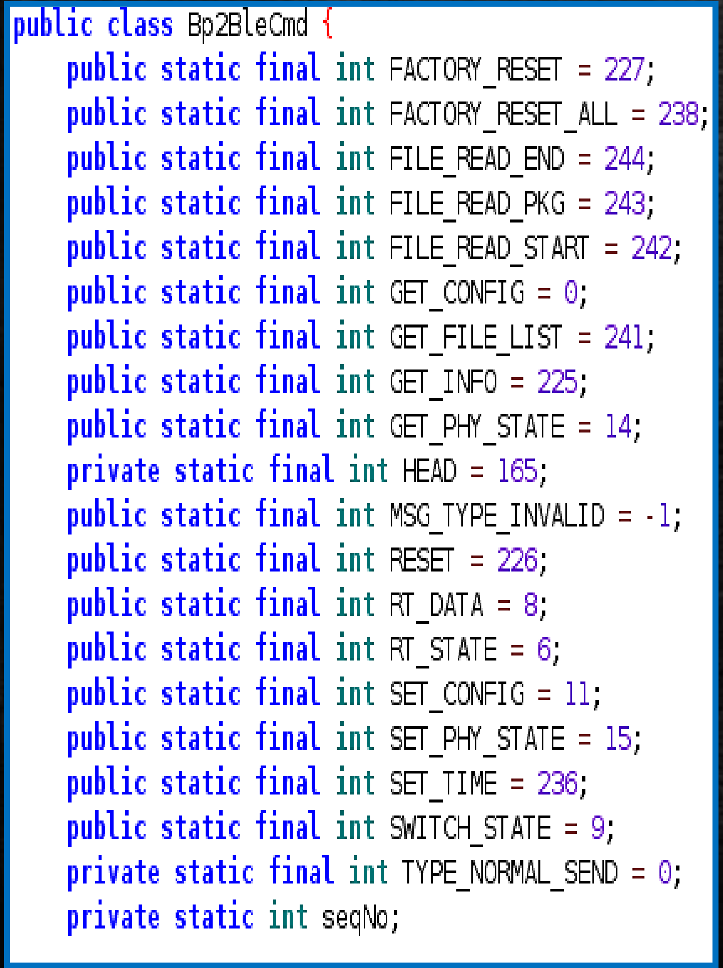
SYS/DIA

| 91 /min | 72 mmHg | 69 mmHg |
|---|---|---|
| PR | MAP | Pulse pressure |

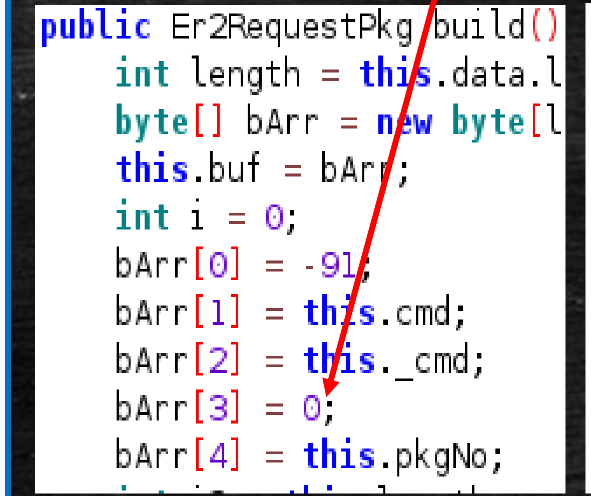
| 6F | 2A | 48 | 5B | 45 |
|---|---|---|---|---|
| 111 | 42 | 72 | 91 | 69 |



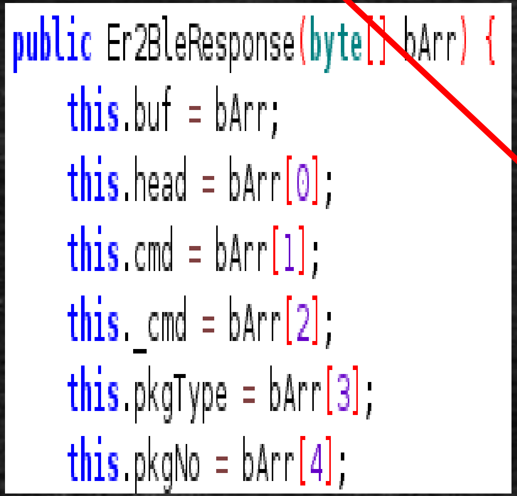
| Source | Destination | Proto | Lengt | Value | Info |
|---|---|---|---|---|---|
| Google_67… | cf:4f:fd… | ATT | 24 | a5f30c005304000000000092 | Sent |
| controller | host | HCI… | 8 | | Rcvd |
| cf:4f:fd:… | Google_6… | ATT | 32 | a5f30c01532600010167ebc0630000000000006f00 | Rcvd |
| cf:4f:fd:… | Google_6… | ATT | 16 | 2a004800 | Rcvd |
| cf:4f:fd:… | Google_6… | ATT | 32 | 5b000000000000000000000000000000000000000 | Rcvd |
| cf:4f:fd:… | Google_6… | ATT | 14 | 0045 | Rcvd |



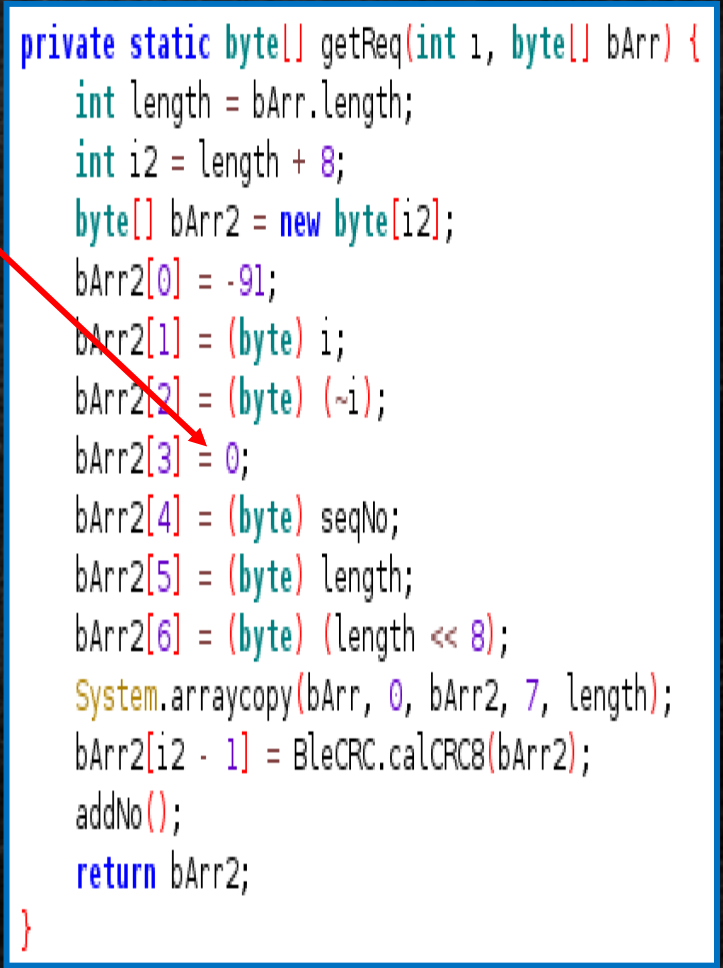
```java
public class Bp2BleCmd {
    public static final int FACTORY_RESET = 227;
    public static final int FACTORY_RESET_ALL = 238;
    public static final int FILE_READ_END = 244;
    public static final int FILE_READ_PKG = 243;
    public static final int FILE_READ_START = 242;
    public static final int GET_CONFIG = 0;
    public static final int GET_FILE_LIST = 241;
    public static final int GET_INFO = 225;
    public static final int GET_PHY_STATE = 14;
    private static final int HEAD = 165;
    public static final int MSG_TYPE_INVALID = -1;
    public static final int RESET = 226;
    public static final int RT_DATA = 8;
    public static final int RT_STATE = 6;
    public static final int SET_CONFIG = 11;
    public static final int SET_PHY_STATE = 15;
    public static final int SET_TIME = 236;
    public static final int SWITCH_STATE = 9;
    private static final int TYPE_NORMAL_SEND = 0;
    private static int seqNo;
```



```java
public Er2RequestPkg build()
    int length = this.data.l
    byte[] bArr = new byte[l
    this.buf = bArr;
    int i = 0;
    bArr[0] = -91;
    bArr[1] = this.cmd;
    bArr[2] = this._cmd;
    bArr[3] = 0;
    bArr[4] = this.pkgNo;
```

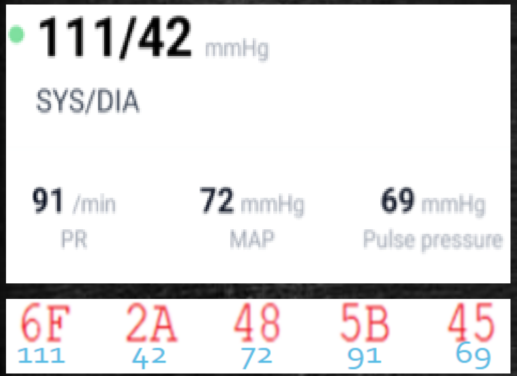


```java
public Er2BleResponse(byte[] bArr) {
    this.buf = bArr;
    this.head = bArr[0];
    this.cmd = bArr[1];
    this._cmd = bArr[2];
    this.pkgType = bArr[3];
    this.pkgNo = bArr[4];
```



```java
private static byte[] getReq(int i, byte[] bArr) {
    int length = bArr.length;
    int i2 = length + 8;
    byte[] bArr2 = new byte[i2];
    bArr2[0] = -91;
    bArr2[1] = (byte) i;
    bArr2[2] = (byte) (~i);
    bArr2[3] = 0;
    bArr2[4] = (byte) seqNo;
    bArr2[5] = (byte) length;
    bArr2[6] = (byte) (length << 8);
    System.arraycopy(bArr, 0, bArr2, 7, length);
    bArr2[i2 - 1] = BleCRC.calCRC8(bArr2);
    addNo();
    return bArr2;
}
```

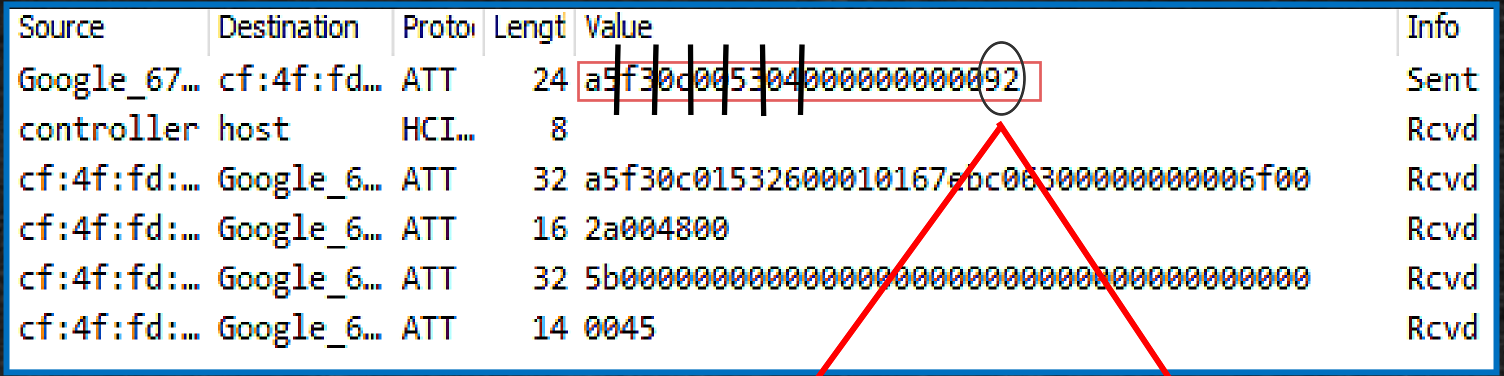
| Hex | A5 | F3 | 0C | 00 | 53 | 04 |
|---|---|---|---|---|---|---|
| Dec | 165 | 243 | 12 | 0 | 83 | 4 |
| Byte Array Position | 0 | 1 | 2 | 3 | 4 | 5 |



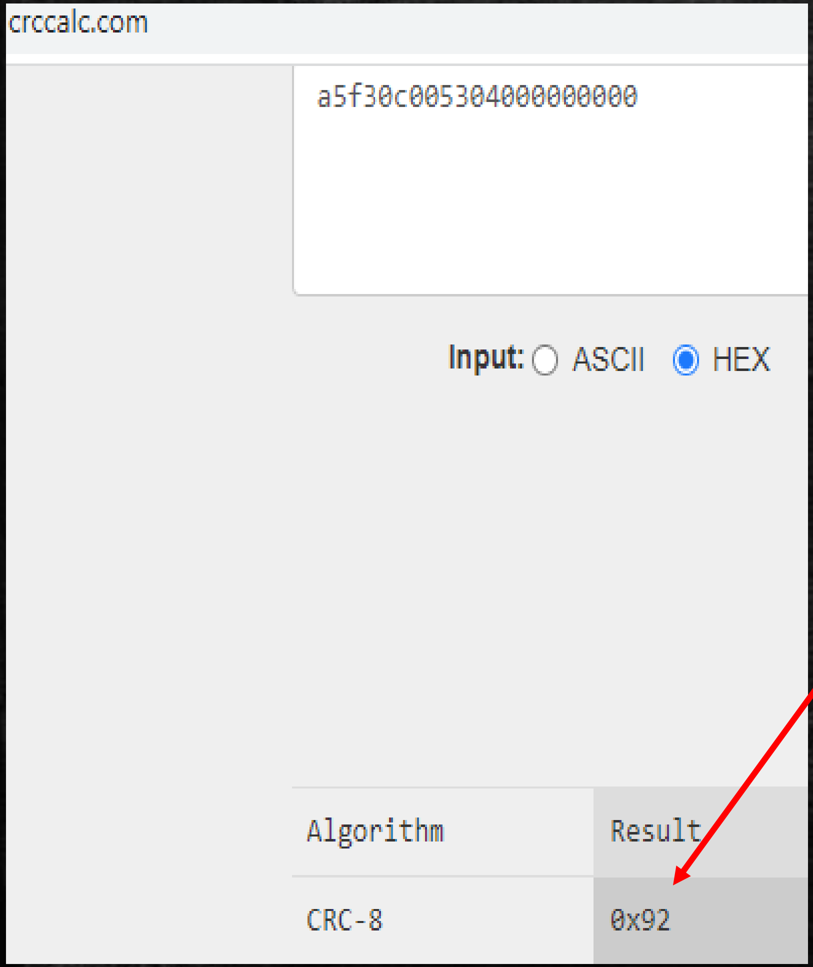
111/42 mmHg
SYS/DIA

| 91 /min | 72 mmHg | 69 mmHg |
|---|---|---|
| PR | MAP | Pulse pressure |

| 6F | 2A | 48 | 5B | 45 |
|---|---|---|---|---|
| 111 | 42 | 72 | 91 | 69 |



```
Source        Destination   Proto  Lengt  Value                                     Info
Google_67…    cf:4f:fd…     ATT       24  a5f30c005304000000000092                  Sent
controller    host          HCI…       8                                            Rcvd
cf:4f:fd:…    Google_6…     ATT       32  a5f30c01532600010167ebc06300000000006f00  Rcvd
cf:4f:fd:…    Google_6…     ATT       16  2a004800                                  Rcvd
cf:4f:fd:…    Google_6…     ATT       32  5b00000000000000000000000000000000000000  Rcvd
cf:4f:fd:…    Google_6…     ATT       14  0045                                      Rcvd
```



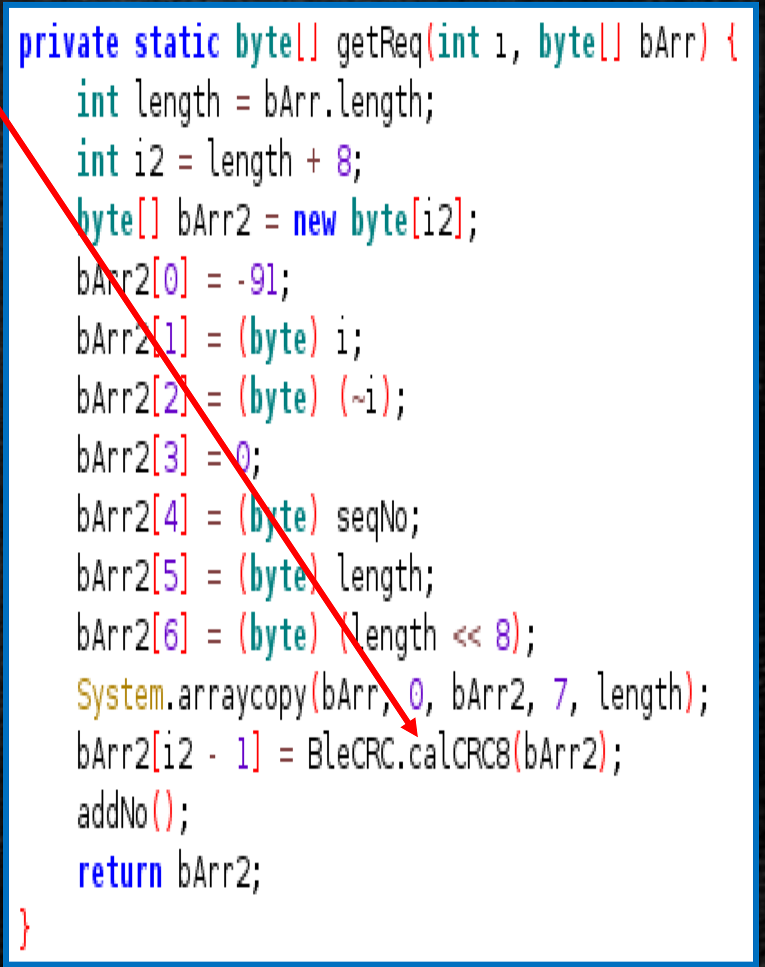
crccalc.com

a5f30c005304000000000000

Input: ○ ASCII ● HEX

| Algorithm | Result |
|---|---|
| CRC-8 | 0x92 |

| Hex | A5 | F3 | 0C | 00 | 53 | 04 |
|---|---|---|---|---|---|---|
| Dec | 165 | 243 | 12 | 0 | 83 | 4 |
| Byte Array Position | 0 | 1 | 2 | 3 | 4 | 5 |

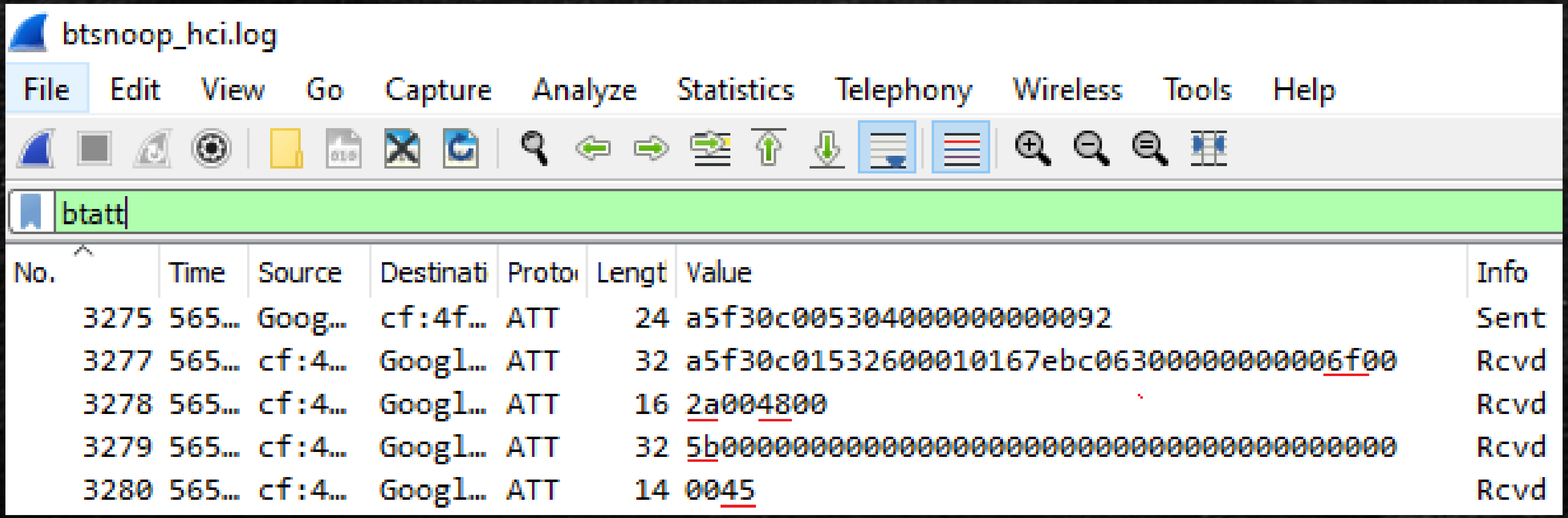


```java
private static byte[] getReq(int i, byte[] bArr) {
    int length = bArr.length;
    int i2 = length + 8;
    byte[] bArr2 = new byte[i2];
    bArr2[0] = -91;
    bArr2[1] = (byte) i;
    bArr2[2] = (byte) (~i);
    bArr2[3] = 0;
    bArr2[4] = (byte) seqNo;
    bArr2[5] = (byte) length;
    bArr2[6] = (byte) (length << 8);
    System.arraycopy(bArr, 0, bArr2, 7, length);
    bArr2[i2 - 1] = BleCRC.calCRC8(bArr2);
    addNo();
    return bArr2;
}
```

# Wireshark Search Filter Basic Cheat sheet

btatt
bthci_cmd.le_long_term_key [BLE]
bthci_cmd.link_key Bluetooth Classic

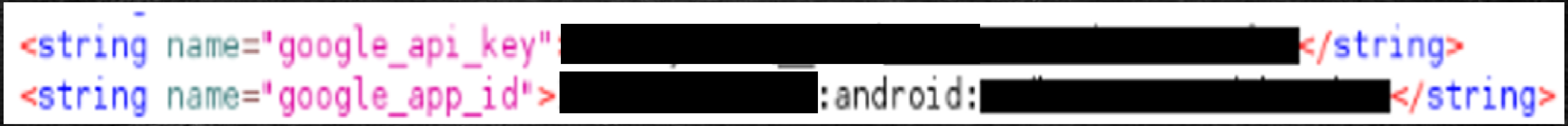
If neither of these strings are present then the devices aren't using Bluetooth Encryption.



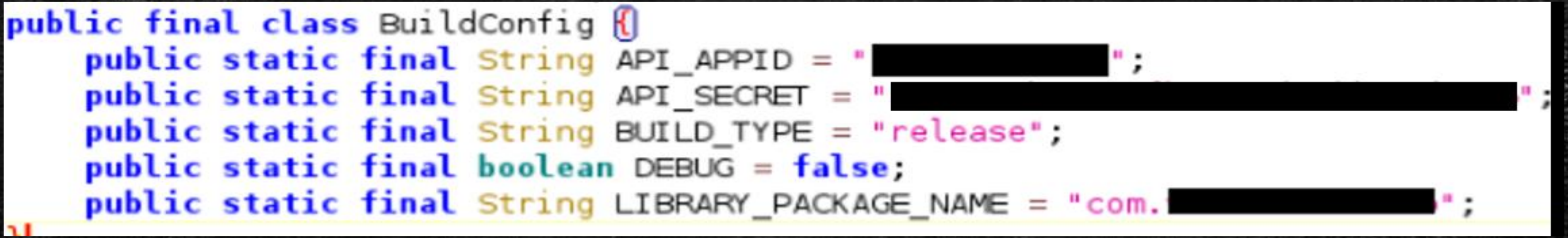
btatt

```
No.   Time Source Destinati Proto Lengt Value                                    Info
3275 565… Goog… cf:4f… ATT    24 a5f30c005304000000000092                 Sent
3277 565… cf:4… Googl… ATT    32 a5f30c01532600010167ebc06300000000006f00 Rcvd
3278 565… cf:4… Googl… ATT    16 2a004800                                 Rcvd
3279 565… cf:4… Googl… ATT    32 5b00000000000000000000000000000000000000 Rcvd
3280 565… cf:4… Googl… ATT    14 0045                                     Rcvd
```

# Android App Secrets



```
<string name="google_api_key"[redacted]</string>
<string name="google_app_id">[redacted]:android:[redacted]</string>
```



```
public final class BuildConfig {
    public static final String API_APPID = "[redacted]";
    public static final String API_SECRET = "[redacted]";
    public static final String BUILD_TYPE = "release";
    public static final boolean DEBUG = false;
    public static final String LIBRARY_PACKAGE_NAME = "com.[redacted]";
}
```

# Conclusions

- ➢ **CWE-311: Missing Encryption of Sensitive Data**

- ➢ **CWE-798: Use of Hard-coded Credentials**

- ➢ https://cwe.mitre.org/data/definitions/311.html
- ❑

- ❑ /in/edwardwar/

- ❑ github.com/actuator/bsides
- ➢