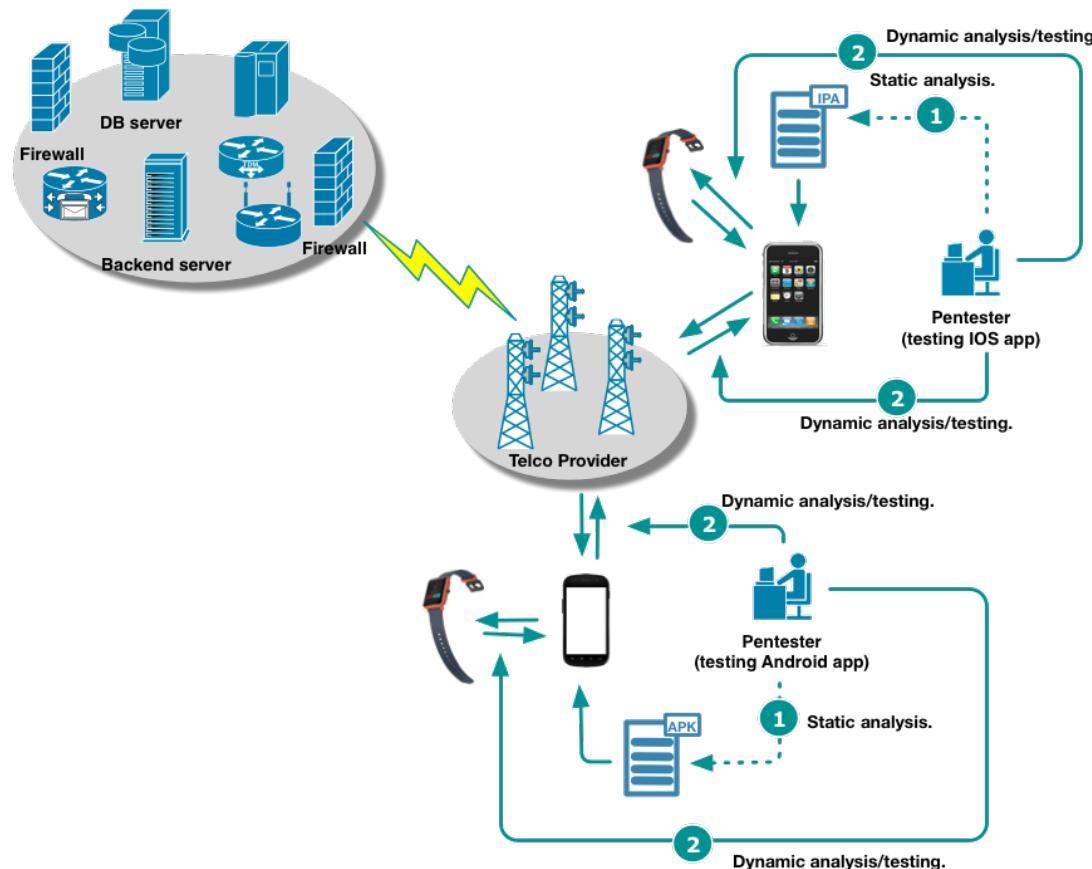


# #whoami

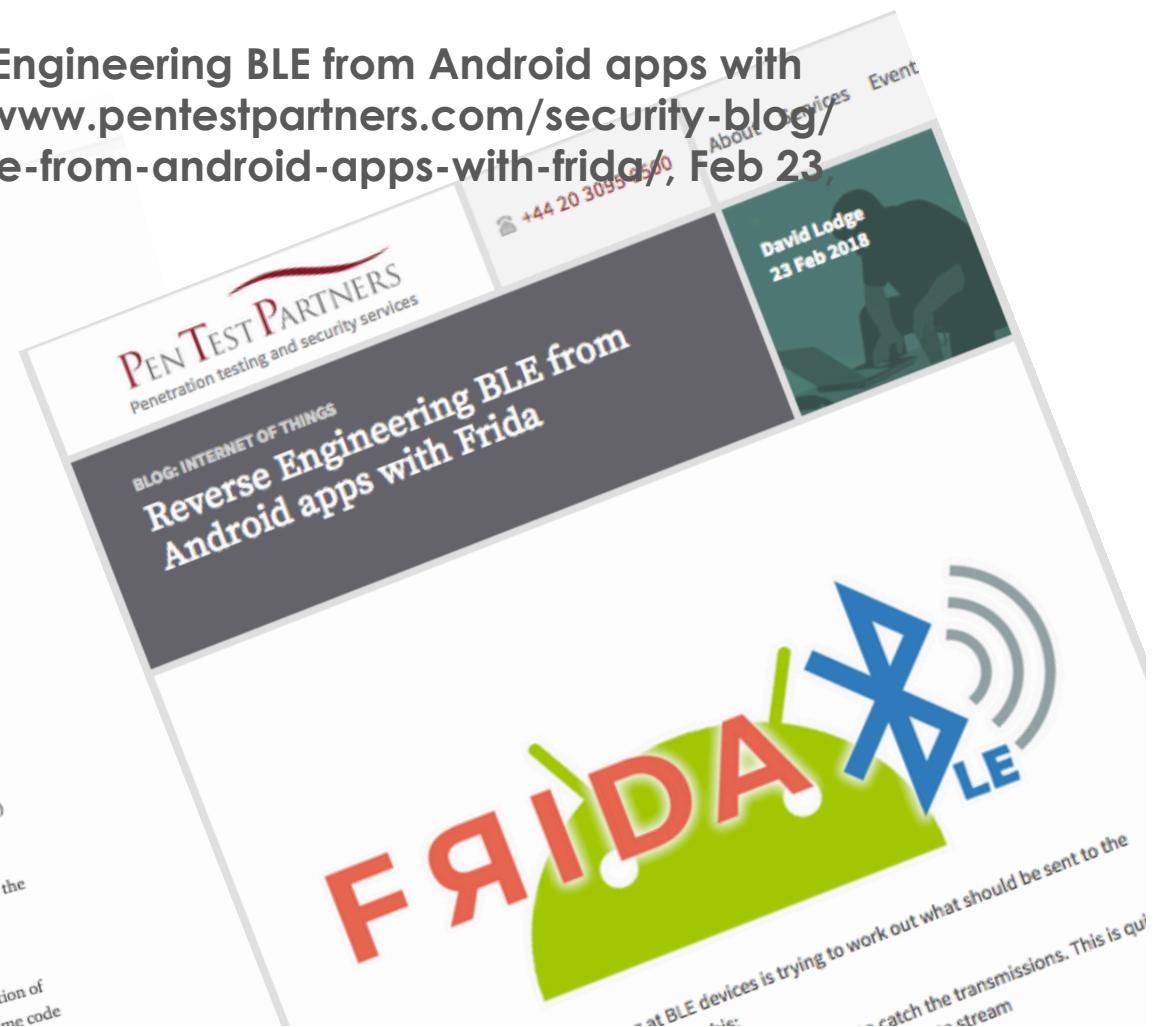
- ❑ Independent security researcher.
- ❑ My job is doing trick to impress client.
- ❑ Speaker Idsecconf 2013, 2014, 2015, 2019 etc.

# Methodology

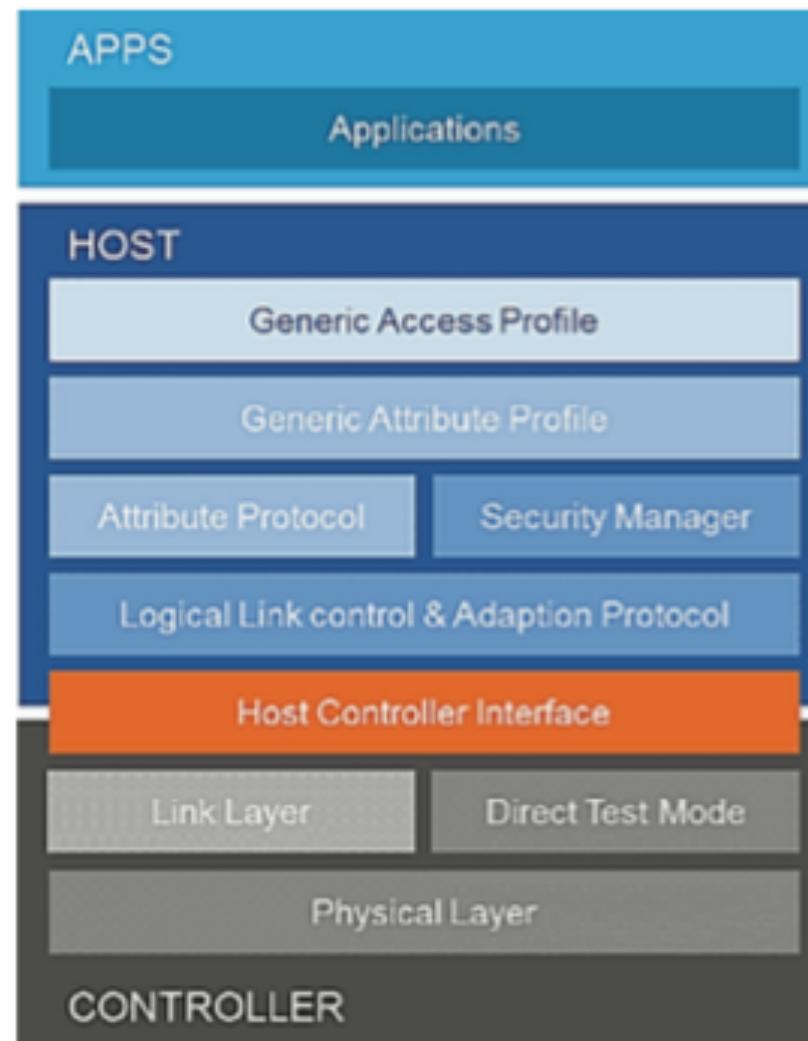


# Relevant Research

- Leo Soares. "Mi Band 2, Part 1: Authentication.", Internet: <https://leojrfs.github.io/writing/miband2-part1-auth/>, Nov. 25, 2017.
- David Lodge, "Reverse Engineering BLE from Android apps with Frida", Internet: <https://www.pentestpartners.com/security-blog/reverse-engineering-ble-from-android-apps-with-frida/>, Feb 23, 2018.



# BLE Communication Layer



# Characteristic & Handle

```
smrx86@smrx86:~$ sudo gatttool -I -b F0:F0:C4:48:B8:B5 -t random
[F0:F0:C4:48:B8:B5][LE]> connect
Attempting to connect to F0:F0:C4:48:B8:B5
Connection successful
[F0:F0:C4:48:B8:B5][LE]> primary
attr handle: 0x0001, end grp handle: 0x0009 uuid: 00001800-0000-1000-8000-00805f9b34fb
attr handle: 0x000c, end grp handle: 0x000f uuid: 00001801-0000-1000-8000-00805f9b34fb
attr handle: 0x0010, end grp handle: 0x001a uuid: 0000180a-0000-1000-8000-00805f9b34fb
attr handle: 0x001b, end grp handle: 0x0020 uuid: 00001530-0000-3512-2118-0009af100700
attr handle: 0x0021, end grp handle: 0x0048 uuid: 0000fee0-0000-1000-8000-00805f9b34fb
attr handle: 0x0049, end grp handle: 0x0061 uuid: 0000fee1-0000-1000-8000-00805f9b34fb
attr handle: 0x0062, end grp handle: 0x0067 uuid: 0000180d-0000-1000-8000-00805f9b34fb
attr handle: 0x0068, end grp handle: 0x006e uuid: 00001811-0000-1000-8000-00805f9b34fb
attr handle: 0x006f, end grp handle: 0x0071 uuid: 00001802-0000-1000-8000-00805f9b34fb
attr handle: 0x0072, end grp handle: 0x0075 uuid: 00003802-0000-1000-8000-00805f9b34fb
[F0:F0:C4:48:B8:B5][LE]> connect
Attempting to connect to F0:F0:C4:48:B8:B5
```

# Characteristic & Handle

```
[F0:F0:C4:48:B8:B5] [LE]> connect
Attempting to connect to F0:F0:C4:48:B8:B5
Connection successful
[F0:F0:C4:48:B8:B5] [LE]> char-read-hnd 0x03
Characteristic valuedescriptor: 41 6d 61 7a 66 69 74 20 42 69 70 20 57 61 74 63 68
[F0:F0:C4:48:B8:B5] [LE]>
```

# MAPPING the AUTH



# Android\_hcidump

(/data/misc/bluetooth/logs/btsnoop\_hci.log)

No.	Time	Source	Destination	Protocol	Length	Info
244	14.639182	controller	host	HCI_EVT	38	Rcvd LE Meta (LE Advertising Report)
245	16.598991	host	controller	HCI_CMD	7	Sent Vendor Command 0x0157 (opcode 0xFD57)
246	16.600223	controller	host	HCI_EVT	10	Rcvd Command Complete (Vendor Command 0x0157 [opcode 0xFD57...]
247	16.600560	host	controller	HCI_CMD	6	Sent LE Set Scan Enable
248	16.603122	controller	host	HCI_EVT	7	Rcvd Command Complete (LE Set Scan Enable)
249	16.603459	host	controller	HCI_CMD	11	Sent LE Set Scan Parameters
250	16.604377	controller	host	HCI_EVT	7	Rcvd Command Complete (LE Set Scan Parameters)
251	31.479223	host	controller	HCI_CMD	29	Sent LE Create Connection
252	31.483081	controller	host	HCI_EVT	7	Rcvd Command Status (LE Create Connection)
253	34.358857	controller	host	HCI_EVT	34	Rcvd LE Meta (LE Enhanced Connection Complete)
254	34.359411	host	controller	HCI_CMD	6	Sent LE Read Remote Used Features
255	34.360155	remote ()	04:92:26:22:6a:b8 (A...	L2CAP	207	Rcvd Connection oriented channel
256	34.363058	controller	host	HCI_EVT	7	Rcvd Command Status (LE Read Remote Used Features)

Event Type: Scan Response (0x04)  
Peer Address Type: Random Device Address (0x01)  
BD\_ADDR: f0:f0:c4:48:b8:b5 (f0:f0:c4:48:b8:b5)  
Data Length: 23

▼ Advertising Data

▼ Device Name: Amazfit Bip Watch  
Length: 18  
Type: Device Name (0x09)  
Device Name: Amazfit Bip Watch

▼ 16-bit Service Class UUIDs (incomplete)  
Length: 3  
Type: 16-bit Service Class UUIDs (incomplete) (0x02)  
UUID 16: Anhui Huami Information Technology Co. (0xfee0)

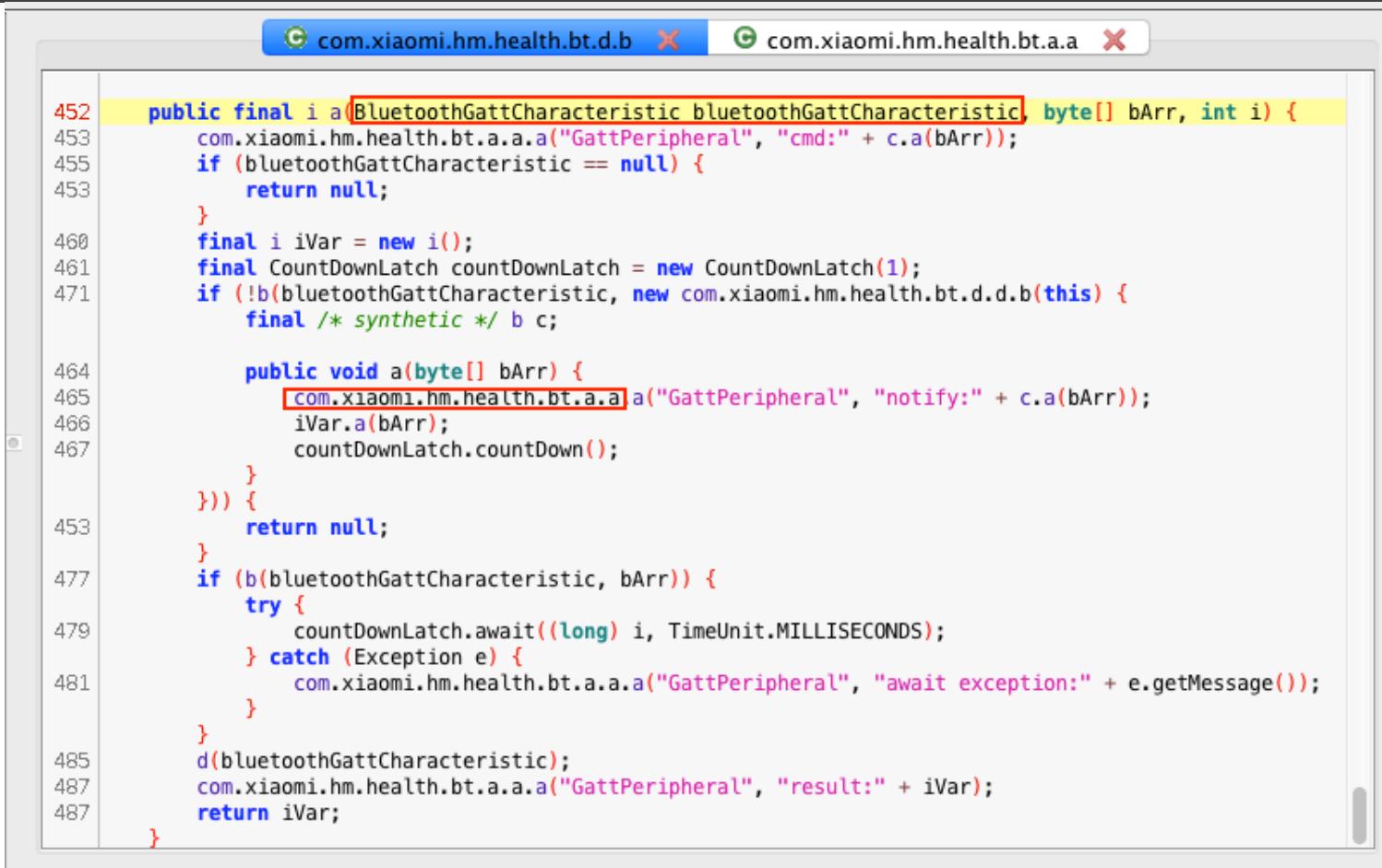
RSSI (dB): -38

0000	04	3e	23	02	01	04	01	b5	b8	48	c4	f0	f0	17	12	09	.>#..... .H.....
0010	41	6d	61	7a	66	69	74	20	42	69	70	20	57	61	74	63	Amazfit Bip Watc
0020	68	03	02	e0	fe	da											h.....

UUID 16 (btcommon.eir\_ad.entry.uuid\_16), 2 bytes

Packets: 1872 · Displayed: 1872 (100.0%) · Load time: 0:0.39 · Profile: Default

# (Active Sniffing) FRIDA



The screenshot shows the Frida debugger interface with two tabs: 'com.xiaomi.hm.health.bt.d.b' (selected) and 'com.xiaomi.hm.health.bt.a.a'. The code listed is from the 'com.xiaomi.hm.health.bt.d.b' tab.

```
452     public final i a(BluetoothGattCharacteristic bluetoothGattCharacteristic, byte[] bArr, int i) {
453         com.xiaomi.hm.health.bt.a.a.a("GattPeripheral", "cmd:" + c.a(bArr));
455         if (bluetoothGattCharacteristic == null) {
456             return null;
457         }
458         final i iVar = new i();
459         final CountDownLatch countDownLatch = new CountDownLatch(1);
460         if (!b(blueoothGattCharacteristic, new com.xiaomi.hm.health.bt.d.d.b(this)) {
461             final /* synthetic */ b c;
462
463             public void a(byte[] bArr) {
464                 com.xiaomi.hm.health.bt.a.a.a("GattPeripheral", "notify:" + c.a(bArr));
465                 iVar.a(bArr);
466                 countDownLatch.countDown();
467             }
468         })
469     }
470     return null;
471 }
472 if (b(blueoothGattCharacteristic, bArr)) {
473     try {
474         countDownLatch.await((long) i, TimeUnit.MILLISECONDS);
475     } catch (Exception e) {
476         com.xiaomi.hm.health.bt.a.a.a("GattPeripheral", "await exception:" + e.getMessage());
477     }
478 }
479 d(blueoothGattCharacteristic);
480 com.xiaomi.hm.health.bt.a.a.a("GattPeripheral", "result:" + iVar);
481
482 }
```

(mifit ver 3.3.2)

# (Active Sniffing) FRIDA



The screenshot shows a Frida debugger interface with two tabs at the top: "com.xiaomi.hm.health.bt.d.b" and "com.xiaomi.hm.health.bt.a.a". The "com.xiaomi.hm.health.bt.a.a" tab is active. Below the tabs, there is a code dump of Java code. The code is annotated with line numbers on the left and highlights in pink and blue on the right. The code is as follows:

```
291 private static String c() {
294     return new SimpleDateFormat("yyyy-MM-dd HH:mm:ss.SSS", Locale.getDefault()).format(new Date());
}
297
335 private static void a(String str, String str2, int i, char c) {
313     if (i) {
314         String str3 = "";
315         str3 = "";
316         switch (c) {
321             case 'd':
322                 Log.d(str, "" + str2 + "");
323                 return;
316             case 'e':
317                 Log.e(str, "" + str2 + "");
318                 return;
324             case 'i':
325                 Log.i(str, "" + str2 + "");
326                 return;
327             case 'v':
328                 Log.v(str, "" + str2 + "");
329                 return;
330             case 'w':
331                 Log.w(str, "" + str2 + "");
332                 return;
333             default:
334                 return;
335         }
336     }
337 }
```

(mifit ver 3.3.2)

# (Active Sniffing) FRIDA



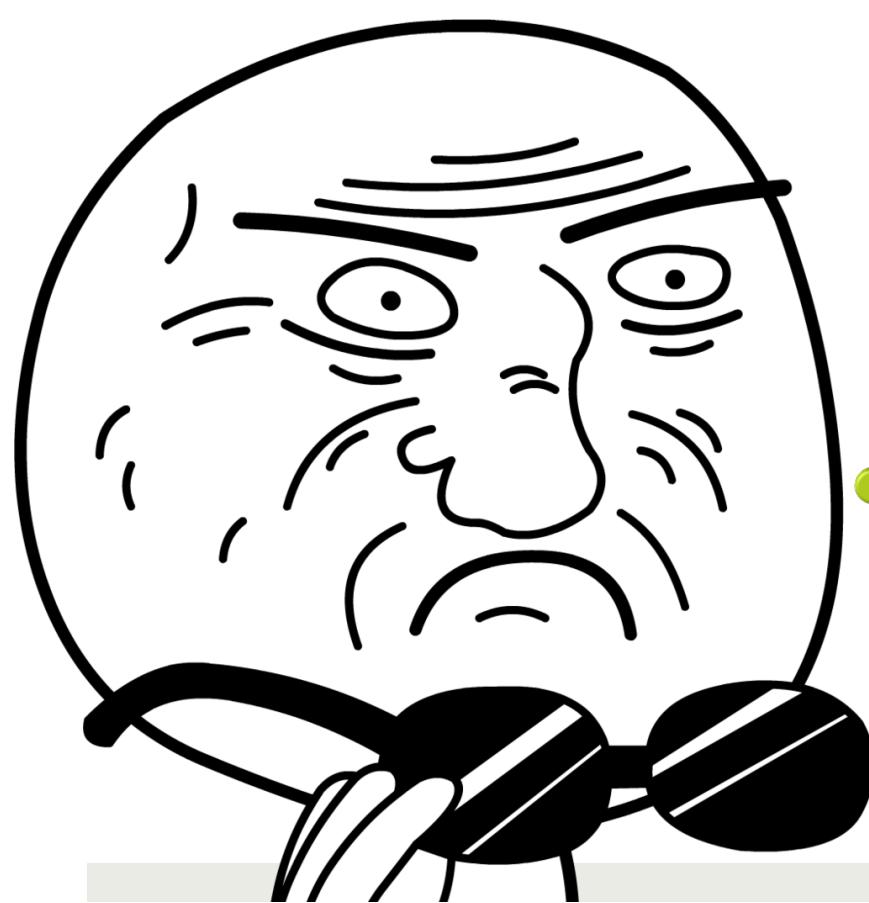
The screenshot shows a code editor window with a dark theme. The file is named 'sniff.js'. The code itself is a Frida script designed to intercept Java method calls. It uses the Java API to find a specific class ('com.xiaomi.hm.health.bt.a.a') and overrides its 'a' method to log incoming data to the console.

```
1 Java.perform(function() {
2
3     var ble = Java.use("com.xiaomi.hm.health.bt.a.a");
4     var sniff = ble.a.overload('java.lang.String');
5
6     sniff.implementation = function (data) {
7         console.log("(+) "+ data);
8     }
9 });
10
```

# (Active Sniffing) FRIDA

```
smrx86@Manilas-MacBook ~ $ frida -U -f com.xiaomi.hm.health -l ./sniff.js --no-pause
_____
| _ |   Frida 12.2.13 - A world-class dynamic instrumentation toolkit
|_||_| Commands:
|_||_|     help      -> Displays the help system
| . . . |     object?   -> Display information about 'object'
| . . . |     exit/quit -> Exit
| . . . |
| . . . |     More info at http://www.frida.re/docs/home/
Spawned `com.xiaomi.hm.health'. Resuming main thread!
[Asus ASUS_X00RD::com.xiaomi.hm.health]-> (+)           flag: 06
(+)   manufact: 57 01 00 a8 35 d7 40 a9 c4 83 d4 04 7a 65 a8 82 75 29 8f 02 f0 f0 c4 48 b8 b5
(+)     name: Amazfit Bip Watch
(+)   (*)serv16: e0 fe;
(+) device:
(+)     name: Amazfit Bip Watch
(+)     address: F0:F0:C4:48:B8:B5
(+)   bond state: BONDED
(+)     type: LE
(+) m_State: DISCONNECTED
(+) gatt=android.bluetooth.BluetoothGatt@b671d39, characteristic=android.bluetooth.BluetoothGattDescriptor@8e4ff7e
(+) Descriptor Write: 01 00
(+) gatt=android.bluetooth.BluetoothGatt@b671d39, characteristic=android.bluetooth.BluetoothGattCharacteristic@8cd5cdf
(+) Characteristic Write: 01 00 dd 3d ed 5b 44 e7 69 0f be 05 2d d8 14 5a 0f 16
(+) Characteristic Changed: 10 01 02
(+) gatt=android.bluetooth.BluetoothGatt@b671d39, characteristic=android.bluetooth.BluetoothGattDescriptor@8e4ff7e
(+) Descriptor Write: 00 00
(+) gatt=android.bluetooth.BluetoothGatt@b671d39, characteristic=android.bluetooth.BluetoothGattCharacteristic@65a7192
(+) Characteristic Read: e3 07 02 16 14 27 20 05 00 00 1c
(+) m_State: DISCONNECTED
```

# (Active Sniffing) FRIDA



WHERE IS  
CHAR UUID  
& HANDLE

# FRIDA + Android\_hcidump

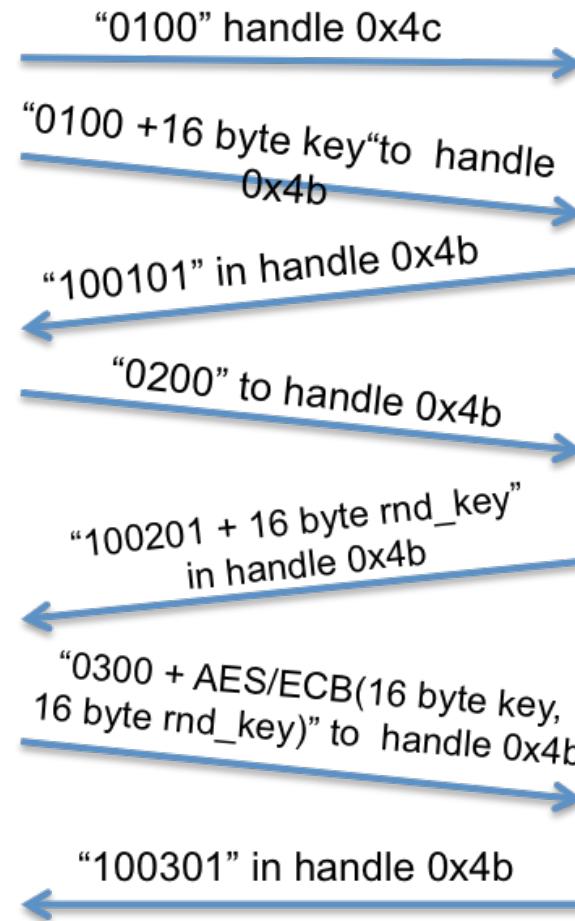
NetworkMiner Screenshot showing a Bluetooth HCI\_ACL\_Packet (Frame 223) with a handle of 0x004b.

Selected Hex value: 01 00 26 08 1f ad 92 a3 09 07 4b e4 1f 5a 88 9e 4d 93

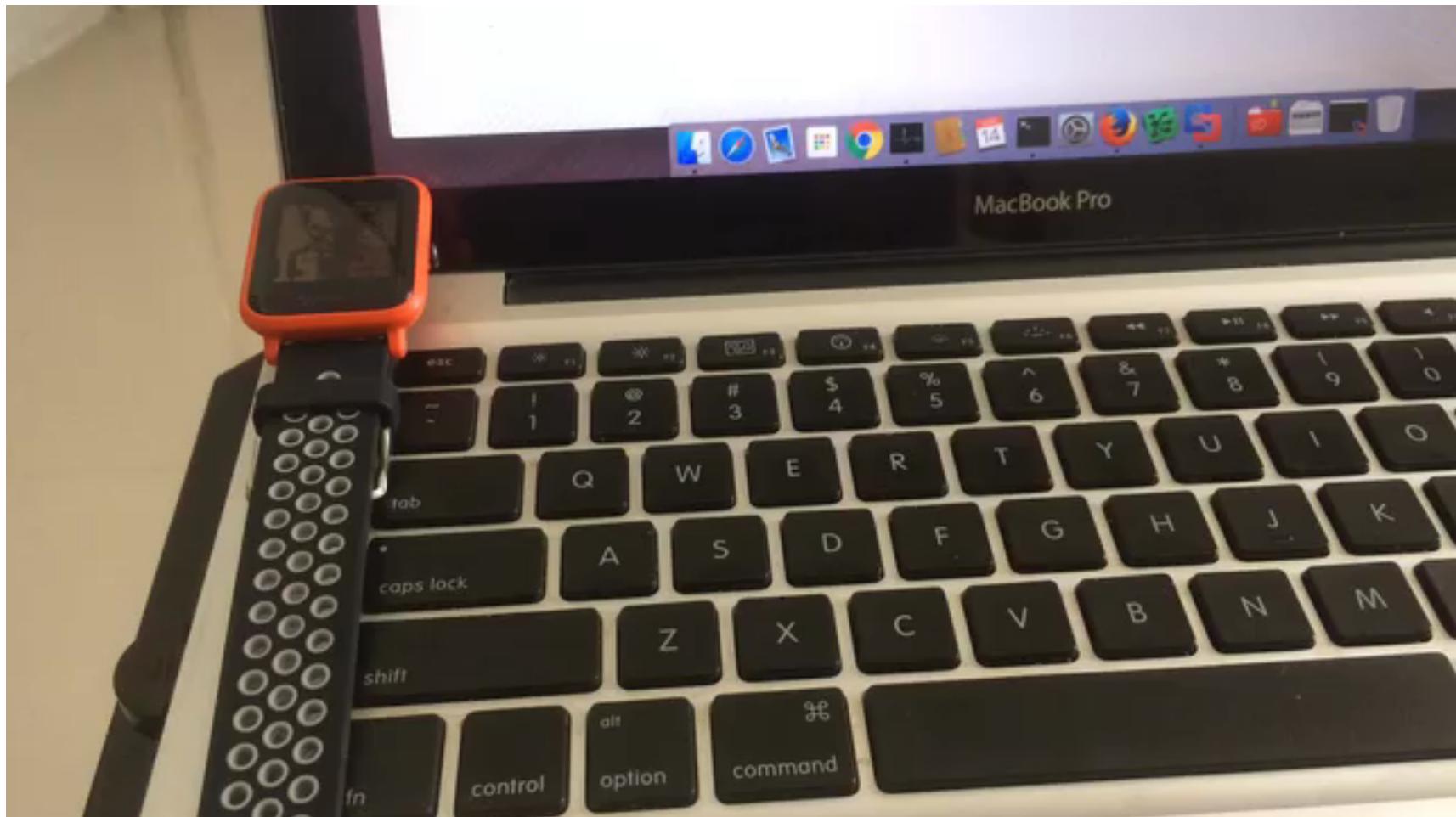
No.	Tim	Source	Destination	Protocol	Length	Info
212	4..	controller	host	HCI_EVT	7	Rcvd Command Status (LE Read Remote Used Features)
213	4..	controller	host	HCI_EVT	15	Rcvd LE Meta (LE Read Remote Used Features Complete)
214	4..	host	controller	HCI_CMD	6	Sent Read Remote Version Information
215	4..	controller	host	HCI_EVT	7	Rcvd Command Status (Read Remote Version Information)
216	4..	controller	host	HCI_EVT	11	Rcvd Read Remote Version Information Complete
217	4..	host	controller	HCI_CMD	32	Sent LE Start Encryption
218	4..	controller	host	HCI_EVT	7	Rcvd Command Status (LE Start Encryption)
219	4..	04:92:26:22:6a:b8 (A..	remote ()	ATT	14	Sent Write Request, Handle: 0x004c
220	4..	controller	host	HCI_EVT	7	Rcvd Encryption Change
221	4..	controller	host	HCI_EVT	8	Rcvd Number of Completed Packets
222	4..	remote ()	04:92:26:22:6...	ATT	10	Rcvd Write Response
223	4..	04:92:26:22:6a:b8 (A..	remote ()	ATT	30	Sent Write Command, Handle: 0x004b

Frame details:

- Frame 223: 30 bytes on wire (240 bits), 30 bytes captured (240 bits)
- Bluetooth
- Bluetooth HCI H4
- Bluetooth HCI ACL Packet
- Bluetooth L2CAP Protocol
- Bluetooth Attribute Protocol
  - Opcode: Write Command (0x52)
  - Handle: 0x004b
  - Value: 010026081fad92a309074be41f5a889e4d93



## Authentification Procedure



# POC script is adjustment of recent @leojrs (0x08 > 0x00)

leojrfs / miband2

Watch 4 Star 29 Fork 17

Code Issues 0 Pull requests 0 Insights

Branch: master miband2 / miband2\_auth.py Find file Copy path

Fetching contributors...

Cannot retrieve contributors at this time.

Executable File | 137 lines (117 sloc) 5.01 KB

Raw Blame History

```
1 #!/usr/bin/env python2
2 import struct
3 import time
4 import sys
5 import argparse
6 from Crypto.Cipher import AES
7 from bluepy.btle import Peripheral, DefaultDelegate, ADDR_TYPE_RANDOM
8
9
10 class MiBand2(Peripheral):
11     _KEY = b'\x30\x31\x32\x33\x34\x35\x36\x37\x38\x39\x30\x41\x42\x43\x44\x45'
12     _send_key_cmd = struct.pack('<18s', b'\x01\x08' + _KEY)
13     _send_rnd_cmd = struct.pack('<2s', b'\x02\x08')
14     _send_enc_key = struct.pack('<2s', b'\x03\x08')
15
16     def __init__(self, addr):
17         Peripheral.__init__(self, addr, addrType=ADDR_TYPE_RANDOM)
18         print("Connected")
19         self.handle = 0
```

# DATA and PRIVACY



- Send data to backend constantly

POST request to https://api-mifit.huami.com/v1/data/band\_data.json?r=A4BB6DFC-8BB1-4BBE-A008-1BD7D60E5599&t=1540623996843

Body encoding: JSON

Request Response

Raw Headers Hex JSON Beautifier

```
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Content-Type: application/json; charset=utf-8
Date: Sat, 27 Oct 2018 07:06:47 GMT
Date: Sat, 27 Oct 2018 07:06:48 GMT
Expires: 0
Pragma: no-cache
Server: Jetty(9.4.7.v20170914)
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Application-Context: zuul-service:production,SG,production_SG,cloud:10
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Request-Id: F9CBC4FB-0021-43A4-95EF-874CF7358F80
X-Vcap-Request-Id: 45dbb101-8a42-4064-5558-cfa5c2b5ef84
X-Vcap-Request-Id: b7aeacbb1-eb76-4086-78fb-01c262c17275
X-Xss-Protection: 1; mode=block
Content-Length: 30
Connection: Close

{"code":1,"message":"success"}
```

? < + > [ ] 0 matches

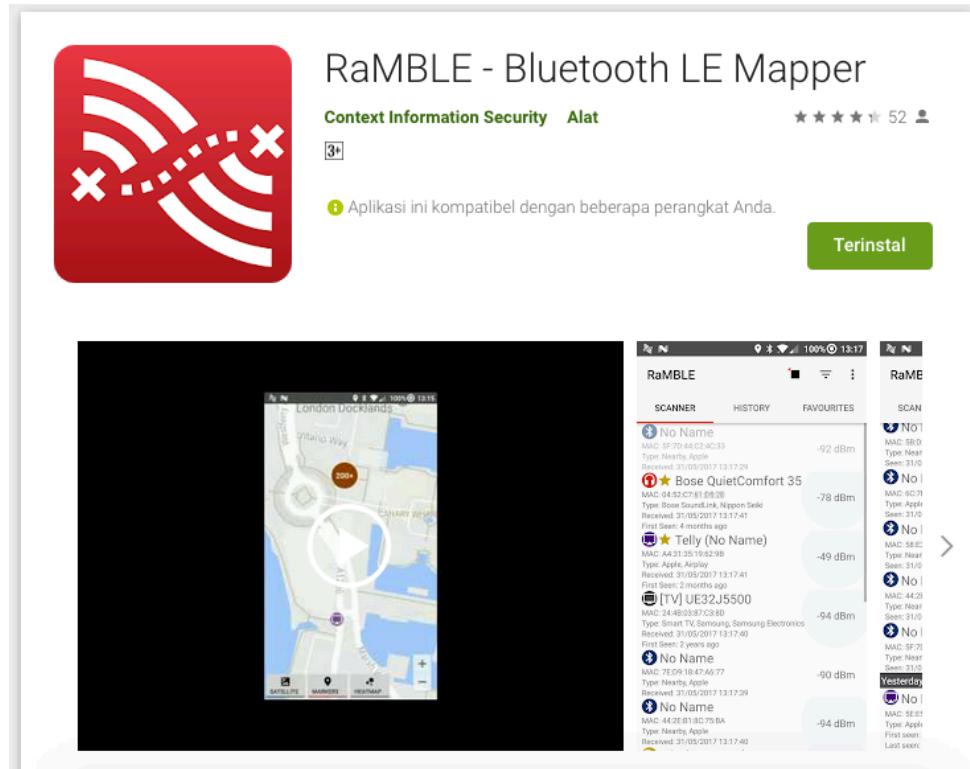
- Log & stored everything /data/user/0/com.xiaomi.hm.health/files/log

```
[ASUS_X00R_2:/data/user/0/com.xiaomi.hm.health/files/log # ls -al
total 732
drwx----- 3 u0_a162 u0_a162 4096 2019-02-21 23:59 .
drwxrwx--x 5 u0_a162 u0_a162 4096 2019-02-22 16:35 ..
drwx----- 2 u0_a162 u0_a162 4096 2019-02-21 23:59 gpx
-rw----- 1 u0_a162 u0_a162 732845 2019-02-22 16:35 mili_log.txt
ASUS_X00R_2:/data/user/0/com.xiaomi.hm.health/files/log # ]
```

```
mililog21022019.txt *
```

34248 >>> Call <<<  
34249 https://api-mifit-us.huami.com/v1/data/band\_data.json?r=03b11a84-c7f7-448c-a727-65b089c377e7&t=1550639386816  
34250 2019-02-20 12:09:46.823 HTTP\_Response NetType:4g  
34251 2019-02-20 12:09:46.856 AbsGattCallback registerNotification:00000005-0000-3512-2118-0009af100700,ret:true  
34252 2019-02-20 12:09:46.856 AbsGattCallback registerNotification:00000004-0000-3512-2118-0009af100700  
34253 2019-02-20 12:09:46.860 GattPeripheral result:true  
34254 2019-02-20 12:09:46.988 ProfileUtils getTimezoneOffset key:28  
34255 2019-02-20 12:09:46.988 ProfileUtils getTimezoneOffset rawOffset:25200000  
34256 2019-02-20 12:09:46.991 ProfileUtils getTimezoneOffset key:28  
34257 2019-02-20 12:09:46.991 ProfileUtils getTimezoneOffset rawOffset:25200000  
34258 2019-02-20 12:09:46.992 HMDeviceManager Bound device MILI sync time is : Wed Feb 20 12:09:00 GMT+07:00 2019  
34259 2019-02-20 12:09:46.994 HMDeviceManager Bound device MILI sync time is : Wed Feb 20 12:09:00 GMT+07:00 2019  
34260 2019-02-20 12:09:47.052 HMPieceProfile patchWrite notify:10 00 c1 01 01  
34261 2019-02-20 12:09:47.059 GattPeripheral cmd:00 01 00 01 f4 dd 6c 5c 1c 05 04 04 04 1f 18 54 68 75 6e 64 65  
34262 2019-02-20 12:09:47.052 AbsGattCallback registerNotification:00000004-0000-3512-2118-0009af100700,ret:true  
34263 2019-02-20 12:09:47.060 HMBaseProfile type:2,year:2019,month:2,day:17,hours:23,minutes:49,seconds:27,tz:28  
34264 2019-02-20 12:09:47.062 GattPeripheral cmd:01 02 e3 07 02 11 17 31 1b 1c  
34265 2019-02-20 12:09:47.066 GattPeripheral result:true  
34266 2019-02-20 12:09:47.067 GattPeripheral cmd:00 41 01 72 73 74 6f 72 6d 00 04 04 04 1f 17 54 68 75 6e 64 65  
34267 2019-02-20 12:09:47.070 GattPeripheral result:true  
34268 2019-02-20 12:09:47.074 GattPeripheral result:true  
34269 2019-02-20 12:09:47.076 GattPeripheral cmd:00 41 02 72 73 74 6f 72 6d 00 04 22 1f 17 54 68 75 6e 64 65  
34270 2019-02-20 12:09:47.080 GattPeripheral result:true  
34271 2019-02-20 12:09:47.083 GattPeripheral cmd:00 41 03 72 73 74 6f 72 6d 20 74 6f 20 52 61 69 6e 00 01 01  
34272 2019-02-20 12:09:47.087 GattPeripheral result:true  
34273 2019-02-20 12:09:47.088 GattPeripheral cmd:00 41 04 20 17 43 6c 6f 75 64 79 00 01 04 1f 18 43 6c 6f 75  
34274 2019-02-20 12:09:47.092 GattPeripheral result:true  
34275 2019-02-20 12:09:47.094 GattPeripheral cmd:00 41 05 64 79 20 74 6f 20 54 68 75 6e 64 65 72 73 74 6f 72  
34276 2019-02-20 12:09:47.098 GattPeripheral result:true  
34277 2019-02-20 12:09:47.099 GattPeripheral cmd:00 81 06 6d 00  
34278 2019-02-20 12:09:47.104 GattPeripheral result:true  
34279 2019-02-20 12:09:47.149 HMDeviceManager getDeviceInternal:MILI,isCreate:false  
34280 2019-02-20 12:09:47.153 HMDeviceManager Bound device MILI gps sync time is : Sun Feb 17 23:49:27 GMT+07:00 2019  
34281 2019-02-20 12:09:47.197 HMBaseProfile notify:10 01 01 00 00 00 e3 07 02 11 10 31 1b 00  
34282 2019-02-20 12:09:47.199 ProfileUtils getTimezoneOffset key:0  
34283 2019-02-20 12:09:47.200 ProfileUtils getTimezoneOffset rawOffset:0  
34284 2019-02-20 12:09:47.201 HMBaseProfile type:2 data header:DataHeader{calendar=Sun Feb 17 23:49:27 GMT+07:00 2019,  
size=0, error=1}  
34285 2019-02-20 12:09:47.202 GattPeripheral cmd:03  
34286 2019-02-20 12:09:47.205 GattPeripheral result:true  
34287 2019-02-20 12:09:47.295 HMPieceProfile patchWrite notify:10 00 81 01 01

# BLE WARDRIVING



DB Browser for SQLite - /RambleProj/RaMBLE\_playstore\_v35.14\_20190808\_2034.sqlite

New Database Open Database Write Changes Revert Changes

Database Structure Browse Data Edit Pragmas Execute SQL

Table: devices

New Record Delete Record

	<a href="#">id</a>	<a href="#">address</a>	<a href="#">adv_flags</a>	<a href="#">device_name</a>	<a href="#">device_type</a>	<a href="#">first_seen</a>	<a href="#">last_seen</a>	<a href="#">msd_key</a>	<a href="#">msd_field</a>	<a href="#">sel</a>
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	62:00:D6:D8:B4:37	26	NULL	Apple, Nearby	155376...	1553763961	76	10050318007a9b	NULL
2	2	F0:F0:C4:48:B8:B5	6	Amazfit Bip Watch	Anhui Huami Information Tech...	155376...	1565236581	343	00fd7c257a6f8963cf778f0333af5da0210f0c448b8b5	fee0
3	3	50:56:3D:2E:92:E7	26	NULL	Apple, Nearby	155376...	1553763959	76	100503180eb969	NULL
4	4	60:9A:0D:E2:FE:DE	26	NULL	Apple, Nearby	155376...	1553763961	76	10050b1c1e52e	NULL

< < 1 - 4 of 532 > >

Go to: 2

UTF-8

```

XXXXXXXX( )XXXXXXP
XXXX X.'v'.X XXXX
XP^X`'b d'X^XX
X. 9 ` ' P )X
`b ` ' d'
` `

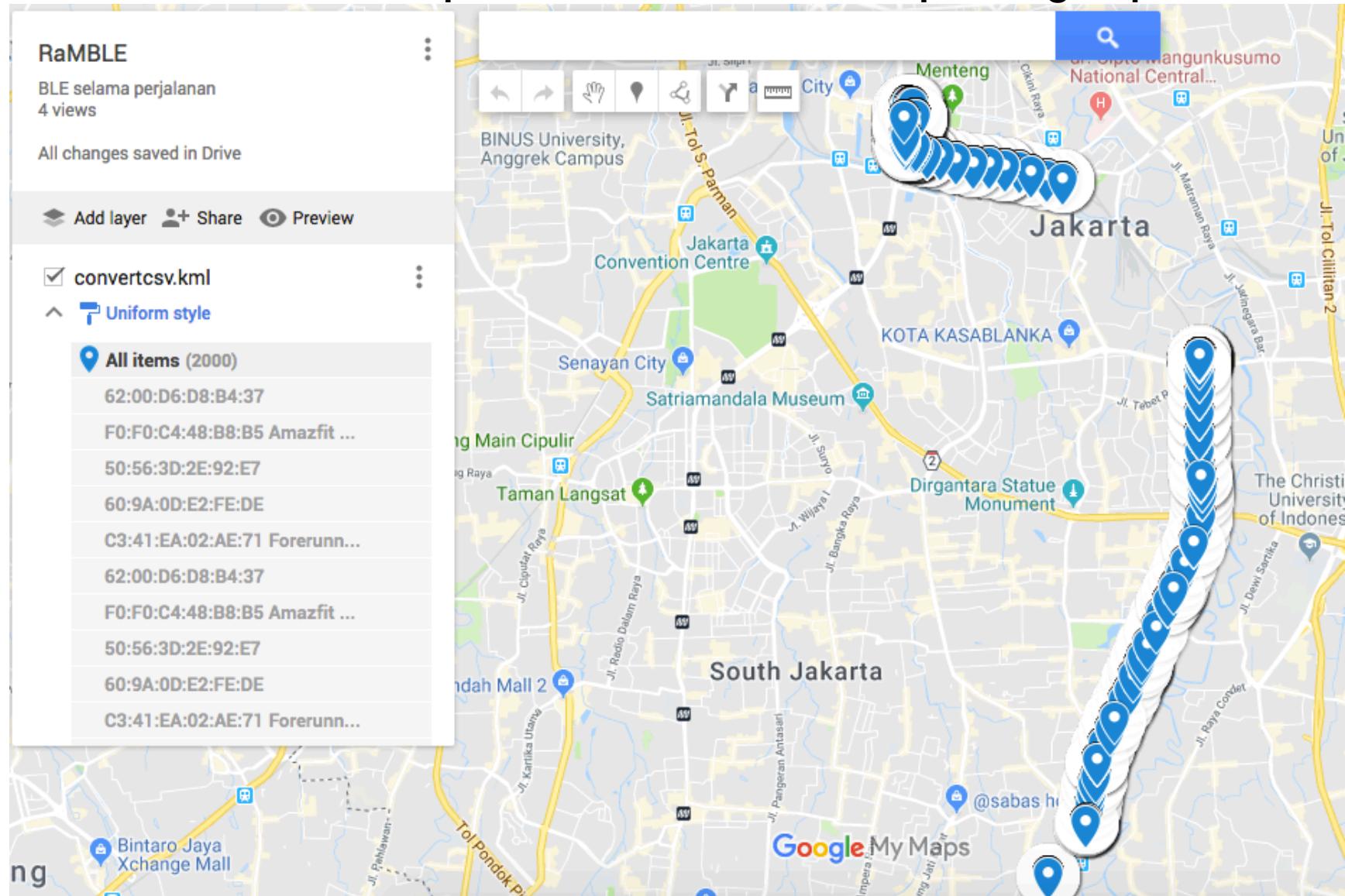
Made with by Simone 'evilsocket' Margaritelli

```

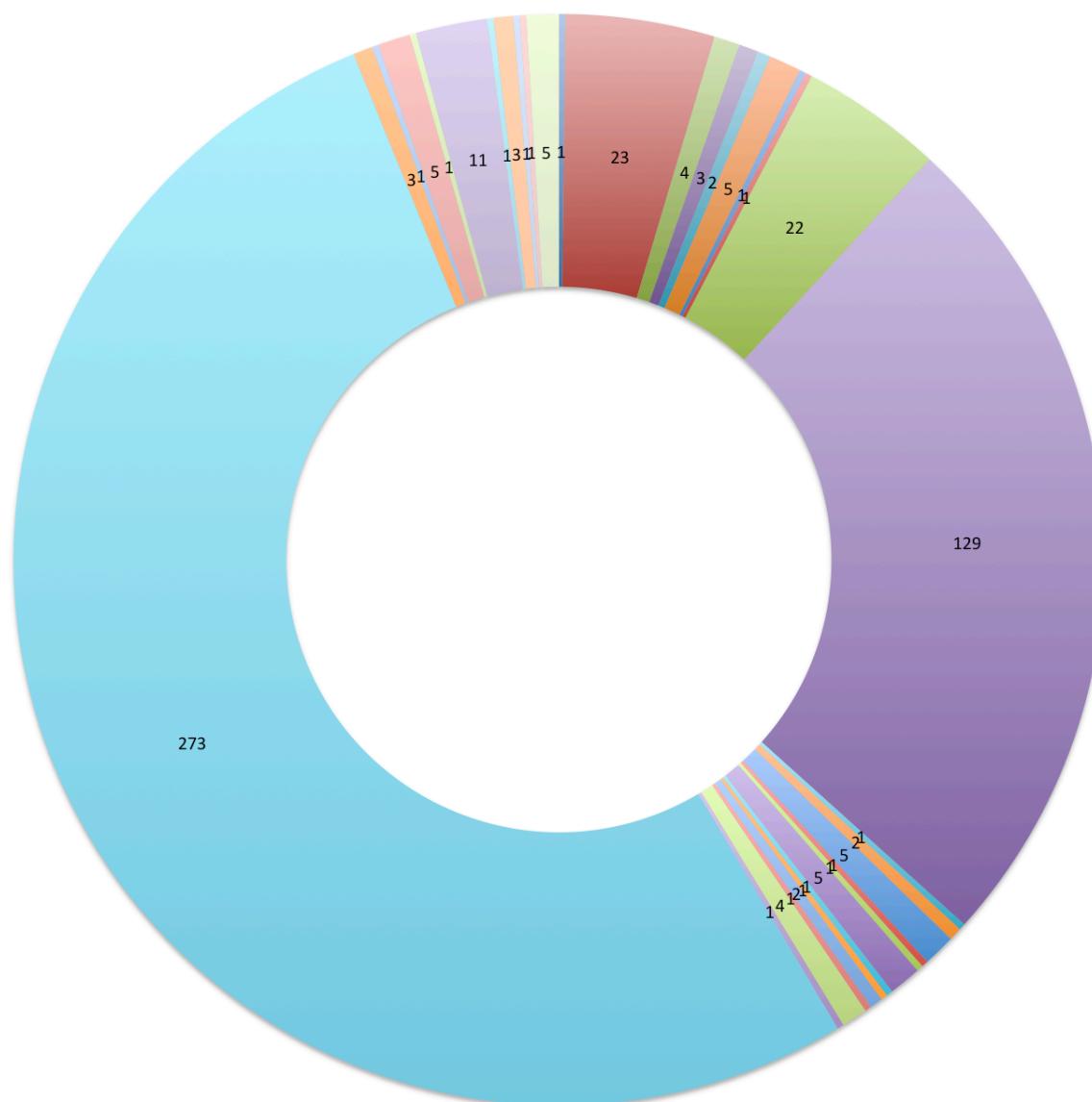
@ Scanning for 5s [-128 dBm of sensitivity] ...

f0:f0:c4:48:b8:b5 (-45 dBm)	?
Vendor	?
Allows Connections	random
Address Type	'0000fee0-0000-1000-8000-00805f9b34fb'
Incomplete 16b Services	u'570100deb7d8700815142b5b622903178da8bd01f0f0c448b8b5'
Manufacturer	Amazfit Bip Watch
Complete Local Name	LE General Discoverable, BR/EDR Not Supported
Flags	

## Convert sqlite >> csv >> kml, then export to gmaps



BLE devices found during wardriving 08/08/2019



no	Device type	qty
1	Airplay, Apple	1
2	Anhui Huami Information Technology	23
3	Anhui Huami Information Technology, MI	4
4	Apple, Airdrop	3
5	Apple, Airplay source	2
6	Apple, Airpods	5
7	Apple, Apple Watch	1
8	Apple, Beats®	1
9	Apple, Handoff	22
10	Apple, Nearby	129
11	Apple, Powerbeats³	1
12	Apple, iOS Wifi Search	2
13	Bose SoundLink	5
14	Current Time Service, Heart Rate, Swirl Networks, Tencent	1
15	Cycling Power, Anhui Huami Information Technology	1
16	Eddystone beacon	5
17	Garmin International	1
18	Garmin International, Garmin	1
19	HUAWEI Technologies, Human Interface Device	2
20	Harman International Industries	1
21	LG Electronics, LG Phone	4
22	Link Loss	1
23	Microsoft	273
24	Quuppa Oy.	3
25	Salt	1
26	Samsung Electronics	5
27	Sensoro beacon, iBeacon	1
28	Smart TV, Samsung Electronics	11
29	Smart TV, Samsung, Samsung Electronics	1
30	Tencent, Apple Notification Center Service	3
31	Tencent, Ericsson Technology Licensing	1
32	iBeacon	5

# Solution: Free ur watch from being watched

The screenshot shows a web browser window displaying the F-Droid app store. The URL in the address bar is <https://f-droid.org/en/packages/nodomain.freeyourgadget.gadgetbridge/>. The page is titled "Gadgetbridge" and features a blue circular icon with a white hand holding a device. Below the title, it says "Communicate with Pebble/Mi Band/Amazfit Bip/Hplus devices and more". A section titled "New in version 0.36.0" lists several updates, including support for Mijia LYWSD02, Mi Band 3/4 NFC menu, Amazfit Cor/Bip language setting, and Mi Band 4 V2 font support. Below this, a note states: "Use your Pebble/Mi Band/Amazfit Bip/Hplus device without the vendor's closed source application and without the need to create an account and transmit any of your data to the vendor's servers." Another note says: "You can get notifications on your wrist and (depending on the device):" followed by a bullet point: "• collect data from the device sensors". To the right of the main content, there is a sidebar with a "Find Apps" search bar and a "Last Updated" section listing three apps: Zoisii, openHAB Beta, and Hauk.

Gadgetbridge

Communicate with Pebble/Mi Band/Amazfit Bip/Hplus devices and more

New in version 0.36.0

- \* Initial Mijia LYWSD02 support (Smart Clock with Humidity and Temperature Sensor), just for setting the time
- \* Mi Band 3/4: Allow enabling the NFC menu where supported (useless for now)
- \* Mi Band 3/4, Amazfit Cor/Bip: Set language immediately when changing it (not only on connect)
- \* Mi Band 3/4, Amazfit Cor/Bip: Add icons for "swimming" and "exercise"
- \* Mi Band 4: Support flashing the V2 font
- \* Mi Band 4: Fix weather location not being updated on the Band
- \* Mi Band 4: remove unsupported DND set

Use your Pebble/Mi Band/Amazfit Bip/Hplus device without the vendor's closed source application and without the need to create an account and transmit any of your data to the vendor's servers.

You can get notifications on your wrist and (depending on the device):

- collect data from the device sensors

Find Apps

SEARCH

Last Updated

Zoisii

A simple game: swipe to delete numbers on a square space.

openHAB Beta

Vendor and technology agnostic open source home automation

Hauk

Self-hosted real-time location sharing