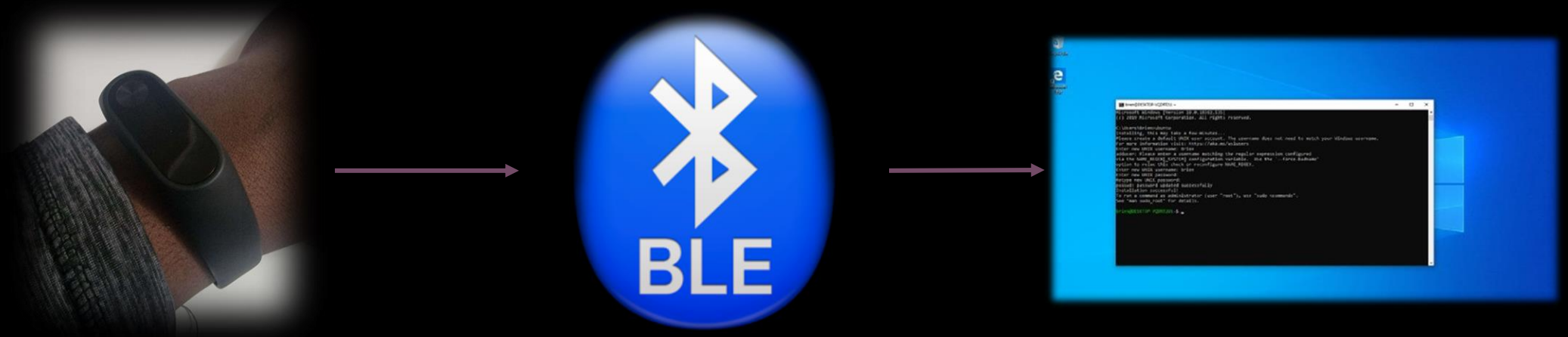
ETHICALLY HACKING A FITNESS TRACKER

BODRYE KAMDEM
RIFAT BIN ISLAM

PROJECT GOAL



Hack a Xiaomi Miband to intercept personal health data sent over bluetooth

WHAT IS BLE (BLUETOOTH LOW ENERGY)

- BLE is a wireless personal-area network technology standardized in Bluetooth 4.0 by the Bluetooth SIG.
- Designed specifically for intermittent data transfer with minimal power draw.

Common Use Cases

- Wearables (fitness trackers, smartwatches)
- IoT sensors (temperature, motion, environmental)
- Beacons for proximity/indoor positioning

WHAT IS BLE (BLUETOOTH LOW ENERGY)

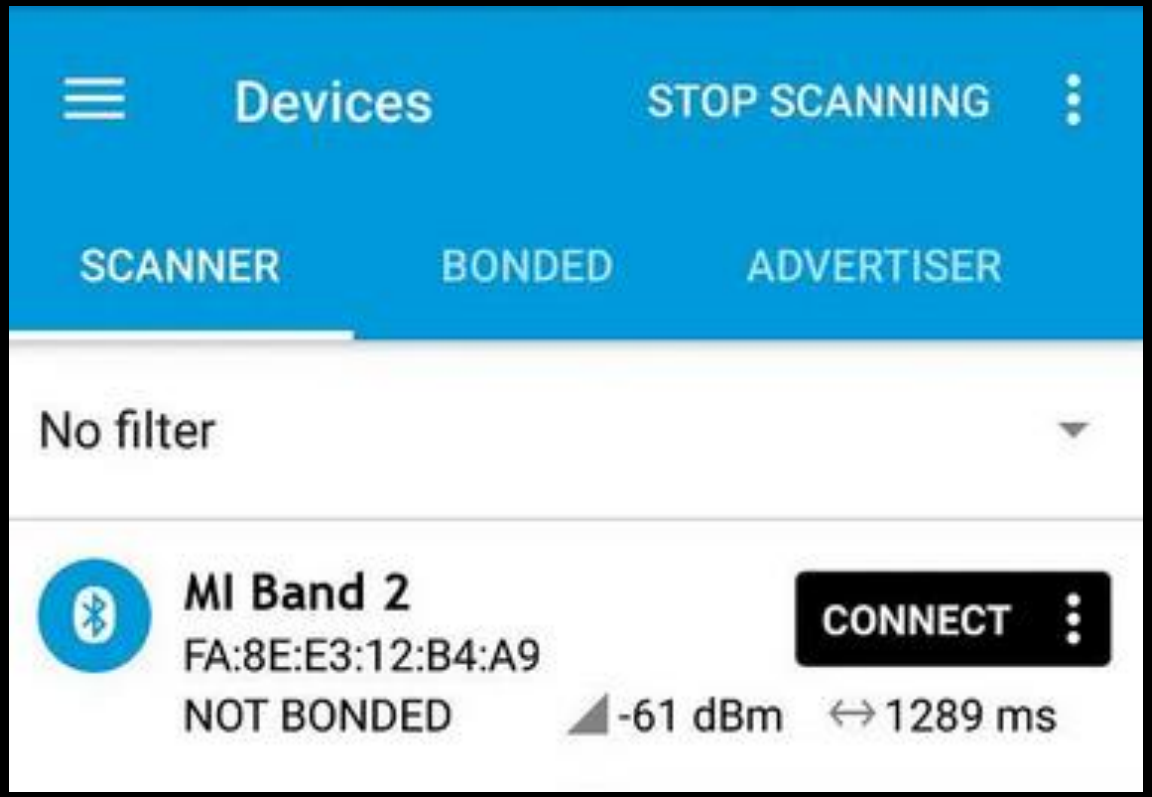
Protocol Stack Highlights

- Physical/RF layer: 2.4 GHz ISM band with 40 channels of 2 MHz each.
- Link layer & L2CAP: Manages connections, encryption, and packets.
- ATT/GATT profiles: Defines how data is structured and exchanged (services, characteristics).

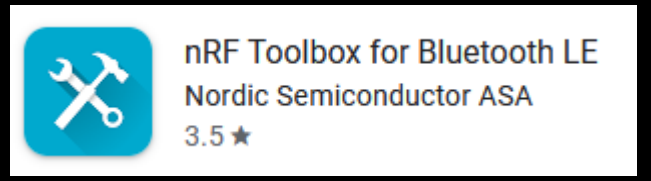
Key Features

- Ultra-low power: Can run on small coin-cell batteries for months or years.
- Fast connection times: Establishes links in just a few milliseconds.
- Flexible topology: Supports point-to-point, broadcast (beacons), and mesh networking.

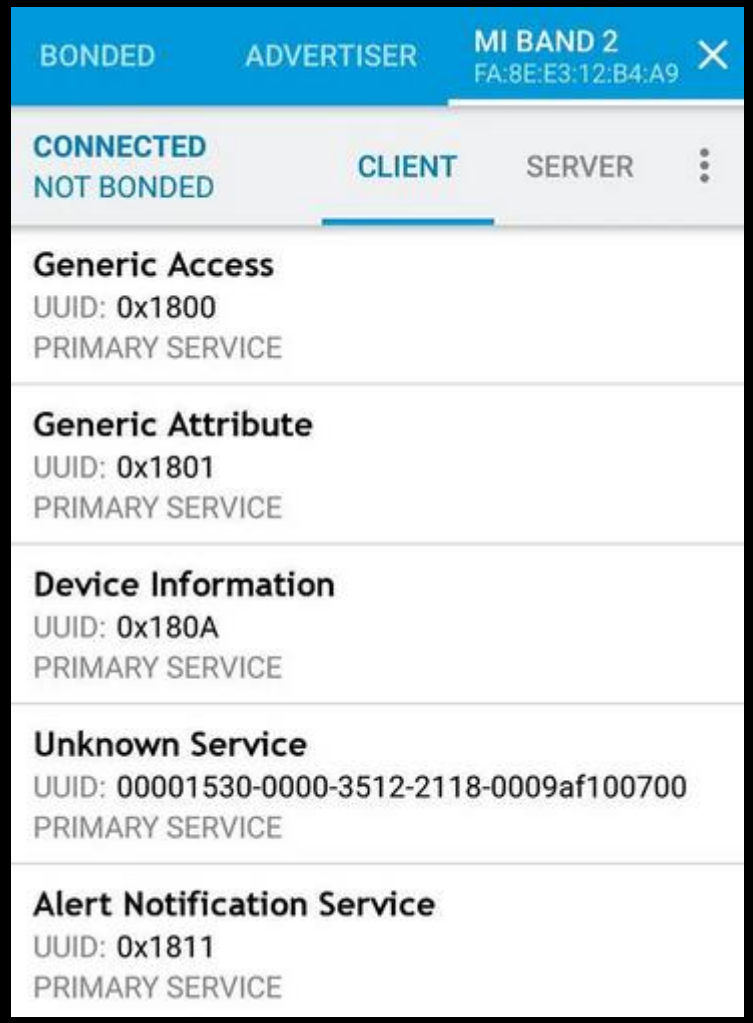
XIAOMI MIBAND – CHARACTERISTICS

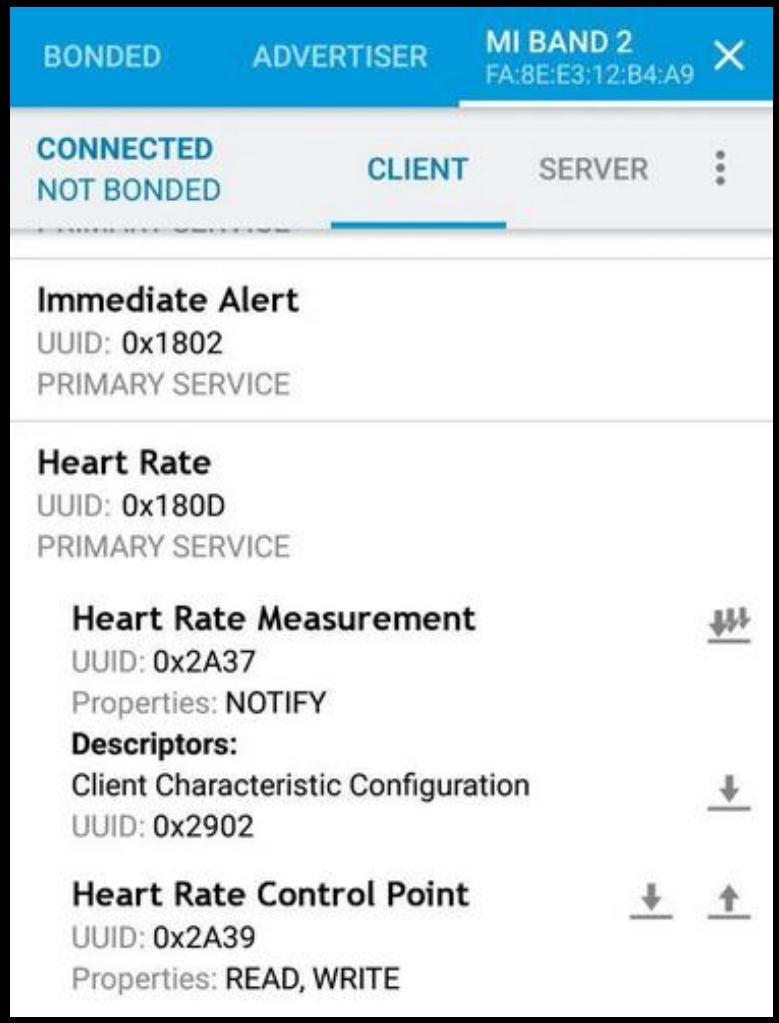


- Using a BLE debugger I can scan and explore my BLE devices and communicate with them



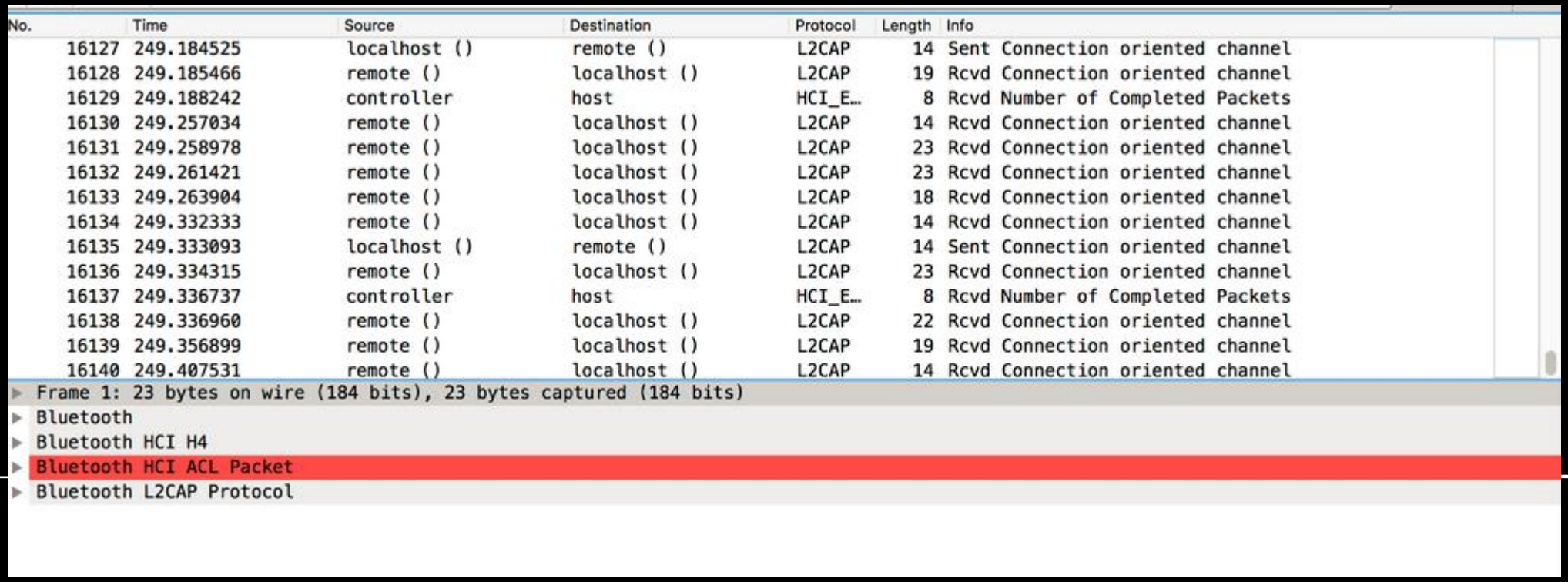
- Here I can see the intrinsic characteristics of the Xiomi Miband 2


BONDED
ADVERTISER
MI BAND 2
FA:8E:E3:12:B4:A9
CONNECTED
NOT BONDED
CLIENT
SERVER
Generic Access
UUID: 0x1800
PRIMARY SERVICE
Generic Attribute
UUID: 0x1801
PRIMARY SERVICE
Device Information
UUID: 0x180A
PRIMARY SERVICE
Unknown Service
UUID: 00001530-0000-3512-2118-0009af100700
PRIMARY SERVICE
Alert Notification Service
UUID: 0x1811
PRIMARY SERVICE


BONDED
ADVERTISER
MI BAND 2
FA:8E:E3:12:B4:A9
CONNECTED
NOT BONDED
CLIENT
SERVER
Immediate Alert
UUID: 0x1802
PRIMARY SERVICE
Heart Rate
UUID: 0x180D
PRIMARY SERVICE
Heart Rate Measurement
UUID: 0x2A37
Properties: NOTIFY
Descriptors:
Client Characteristic Configuration
UUID: 0x2902
Heart Rate Control Point
UUID: 0x2A39
Properties: READ, WRITE

SNIFFING DATA

- To sniff data, a Bluetooth HCI (Host Controller Interface) is used
- On android, a Bluetooth HCI (Host Controller Interface) snoop log provides a detailed record of communication between the Bluetooth host and the Bluetooth controller.
- It captures low-level Bluetooth activity, including commands, events, and data exchanged.

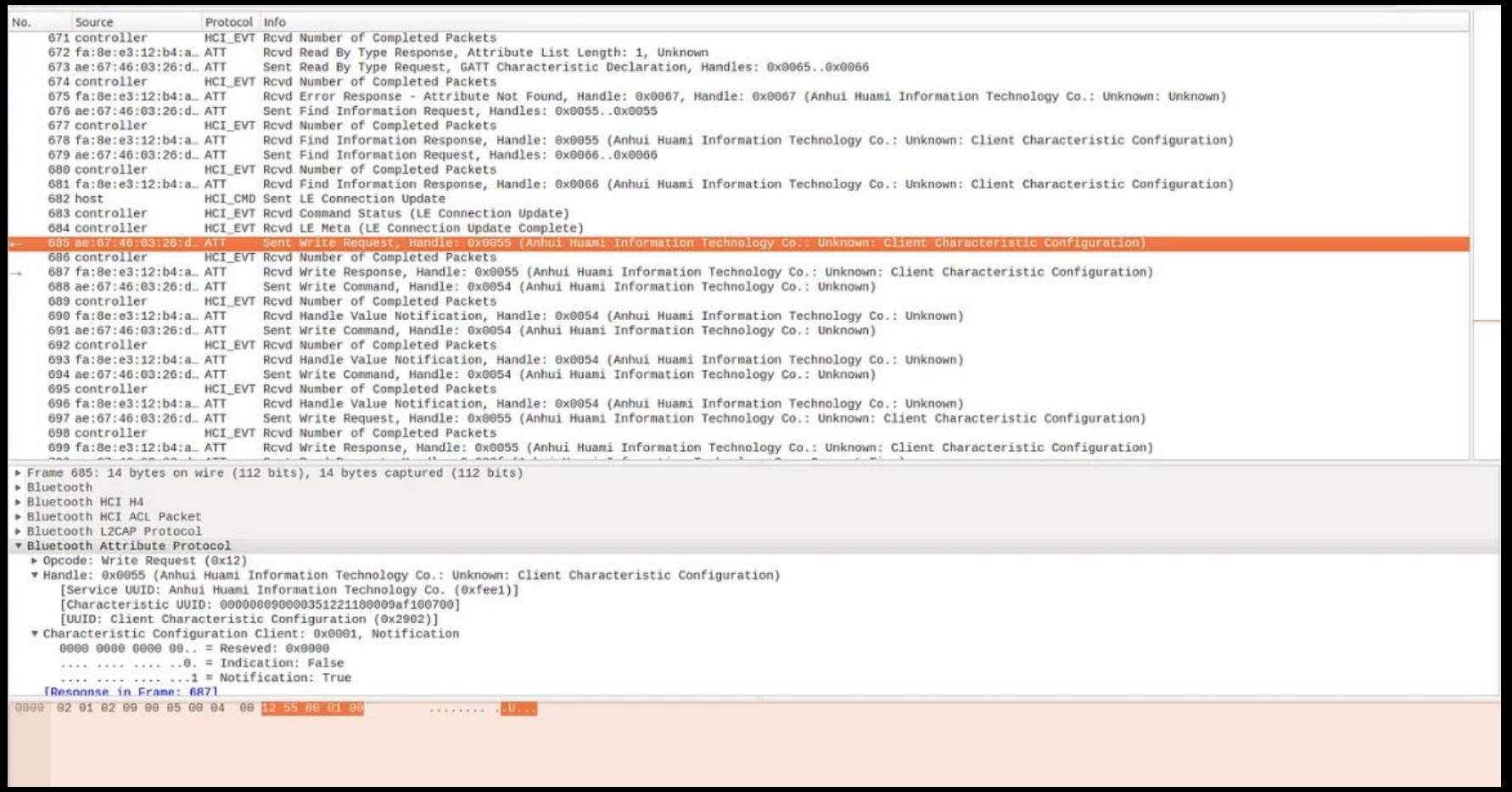


No.	Time	Source	Destination	Protocol	Length	Info
16127	249.184525	localhost ()	remote ()	L2CAP	14	Sent Connection oriented channel
16128	249.185466	remote ()	localhost ()	L2CAP	19	Rcvd Connection oriented channel
16129	249.188242	controller	host	HCI_E…	8	Rcvd Number of Completed Packets
16130	249.257034	remote ()	localhost ()	L2CAP	14	Rcvd Connection oriented channel
16131	249.258978	remote ()	localhost ()	L2CAP	23	Rcvd Connection oriented channel
16132	249.261421	remote ()	localhost ()	L2CAP	23	Rcvd Connection oriented channel
16133	249.263904	remote ()	localhost ()	L2CAP	18	Rcvd Connection oriented channel
16134	249.332333	remote ()	localhost ()	L2CAP	14	Rcvd Connection oriented channel
16135	249.333093	localhost ()	remote ()	L2CAP	14	Sent Connection oriented channel
16136	249.334315	remote ()	localhost ()	L2CAP	23	Rcvd Connection oriented channel
16137	249.336737	controller	host	HCI_E…	8	Rcvd Number of Completed Packets
16138	249.336960	remote ()	localhost ()	L2CAP	22	Rcvd Connection oriented channel
16139	249.356899	remote ()	localhost ()	L2CAP	19	Rcvd Connection oriented channel
16140	249.407531	remote ()	localhost ()	L2CAP	14	Rcvd Connection oriented channel

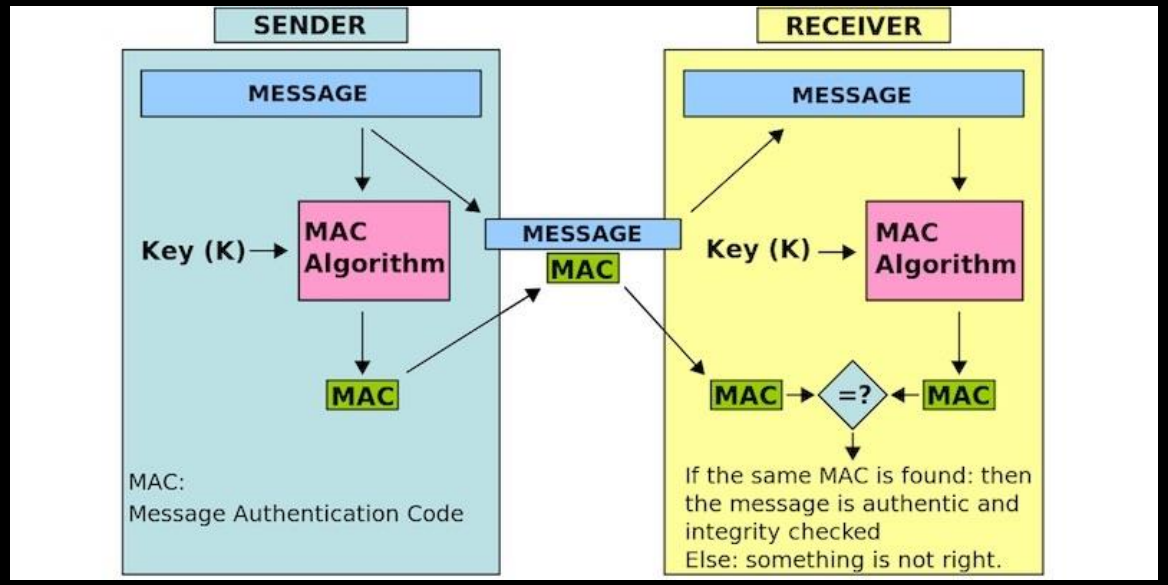
WIRESHARK

- This bluetooth log information '**btsnoop_hci.log**' is used to detect information sent between the watch and the phone

- The first ATT protocol request '**0x0055**' is marked on the log as information sent to Anhui, the company responsible for the device



WIRESHARK - AUTHENTICATION



1. Authentication occurs by enabling auth notifications: write the two-byte request 0x01 0x00 to the authentication characteristic.

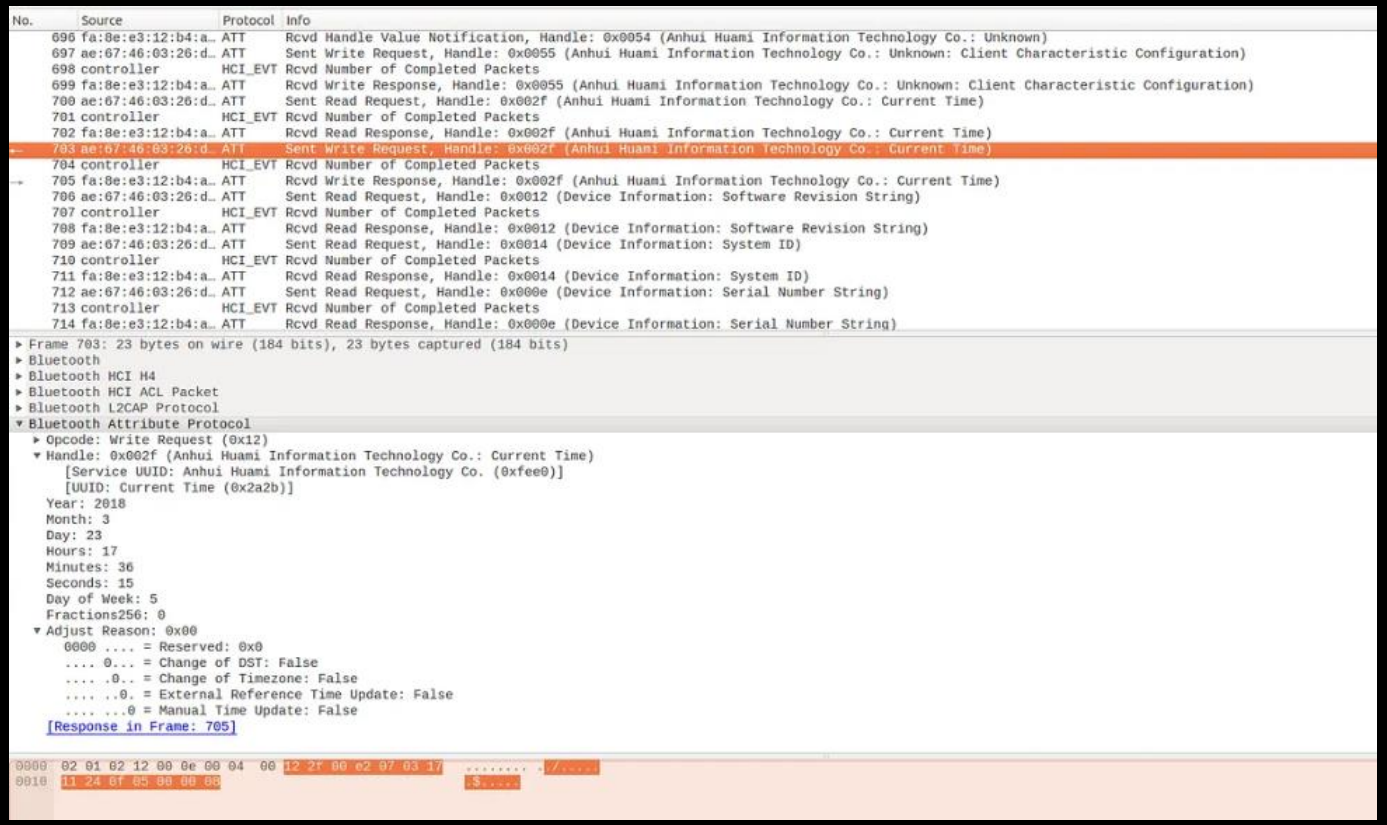
2. Sending a 16-byte encryption key, preceded by 0x01 0x00, to the same characteristic.

3. Writing the two-byte request 0x02 0x00 to the characteristic to prompt the device for a random value.

4. Extracting the last 16 bytes as the random number when the device replies

5. Encryting the16-byte random number with a key using AES-ECB then writing 0x03 0x00 plus the encrypted block back to the characteristic.

HOW THIS WAS USED



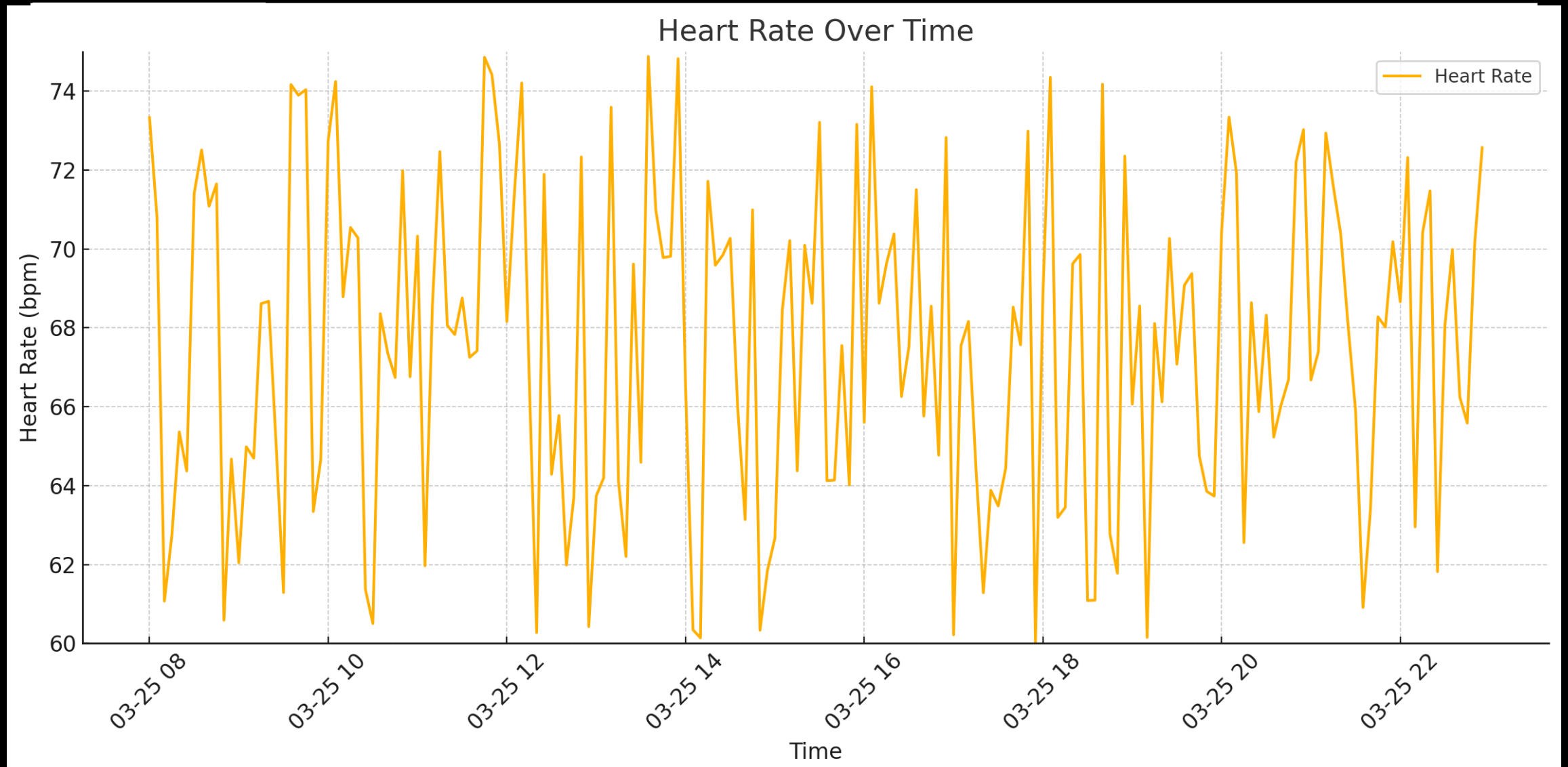
By using this information we could turn on Gyroscope and Heart raw data by sending a command to SENS ***\x01\x03\x19***

We could start continuous heart measurements by sending a request to HMC ***\x15\x01\x01***

EXTRACTED DATA

```
Raw heart: 02102d8c348c448c458c3d8c428c488c 16
Raw heart: 0218468c418c3d8c468c3f8c398c418c 16
Realtime heart: 93
Raw heart: 0220408c448c3f8c428c498c3c8c3d8c 16
Raw heart: 02283d8c398c488c3e8c468c488c328c 16
Realtime heart: 99
Raw heart: 0230438c408c378c3a8c318c458c388c 16
Realtime heart: 102
Raw heart: 02404f8c408c458c428c4d8c558c4d8c 16
Raw heart: 02483e8c3b8c3f8c348c398c318c428c 16
Realtime heart: 98
Raw heart: 02504c8c428c5e8c4f8c588c498c558c 16
Raw heart: 0258478c458c3c8c4e8c3f8c468c4d8c 16
Realtime heart: 100
Raw heart: 0260518c4d8c4f8c4b8c4f8c528c458c 16
Raw heart: 0268408c3f8c538c4d8c408c548c598c 16
Realtime heart: 102
Raw heart: 0278418c508c4e8c548c588c468c498c 16
Raw heart: 0280368c328c2e8c3c8c338c308c3f8c 16
Realtime heart: 101
```

```
Raw gyro: 01de49ffd9ff3c004cffd8ff3b004dffdcff4400
Raw gyro: 01df4cffd6ff44004dffd8ff40004cffd1ff4700
Raw gyro: 02e1103231323d3274328e329632af32c732cf32
Raw gyro: 01e34fffd7ff56004bffc7ff590049ffccff4c00
Raw gyro: 01e443ffccff43004effcdff40005bffd4ff4c00
Raw gyro: 01e558ffc9ff5f005effbfff66005fffb0ff5900
Raw gyro: 01e64cffacff60005cffa7ff410066ffc9ff4600
Raw gyro: 01e760ffdcff4b0051ffe4ff4f0034ffdeff5300
Raw gyro: 02e903365c3681366336103654368837 4139fe3a
Raw gyro: 01eb4bffc3ff50004fffc1ff430047ffbbff4100
Raw gyro: 01ec3effb2ff3c0050ffbfff560047ffccff7300
Raw gyro: 01ed4fffe0ff78005cffebff8e0056fff6ff8300
Raw gyro: 01ee7efffbffa1008bff0f00bc00b1ff1900b800
Raw gyro: 01ef9bff0c00d10095fff3ffd600b7ff0800df00
Raw gyro: 02f12445314600479e473348aa481c499749244a
Raw gyro: 01f3c3ff1600fe00beff1800f200a6ff0800e700
Raw gyro: 01f4a9fff8ffd300a7fff3ffd700a9fff1ffdf00
Raw gyro: 01f5b1fff8ffe800b4fff1fff700acfffcffef00
Raw gyro: 01f67ffff7ffc0006bfff4ffb00078ffe9ffb600
Raw gyro: 01f786ffecffc0006ffff0ffbc0060fff1ffc000
Raw gyro: 02f9ca4cbb4c784c964ca84c784c854c444c1b4c
Raw gyro: 01fb7cff0f00bb007eff2700ae0083ff30009800
Raw gyro: 01fc79ff1800b00076ff0f00bc0068ff0900d900
Raw gyro: 01fd78ff07000c01f6fffbff19011c000b00f600
Raw gyro: 01fe4b001100d30054000700c3004300efffeb00
Raw gyro: 01ff1f00d0ff1701fbffe8ff1b01e3ffffff1101
Raw gyro: 0201214b014bec4ad04aba4acb4abe4aba4abd4a
Raw gyro: 0103efffecfffc00e3fff3fff300defff3fffc00
Raw gyro: 0104e3fff0fff400e6ffefff0301dbffe9ff0c01
Raw gyro: 0105e3fff0ff0301e6ffe6fffc00dcffecfffc00
Raw gyro: 0106dffff0fff700dbffeefff600d6fff0fff400
Raw gyro: 0107dfffecffff00e1fff0ff0301defff3fffc00
```


Heart Rate Over Time
Heart Rate
Heart Rate (bpm)
74
72
70
68
66
64
62
60
03-25 08
03-25 10
03-25 12
03-25 14
03-25 16
03-25 18
03-25 20
03-25 22
Time

IMPLICATIONS

- Any gadget with an equally simplistic GATT-level auth routine can be compromised with comparable effort—no proprietary hardware required.
- BLE operates within a range of 10m so with the right equipment you can tap into sensitive physical and personal information
- Necessity of Robust BLE Pairing: Only wearables using LE Secure Connections (ECDH-based pairing) or equivalent hardened schemes resist such passive snooping and replay attacks.

REFERENCES

- Bluetooth, S. I. G. "Bluetooth low energy." *Dosegljivo: https://www. bluetooth. com/what-is-bluetooth-technology/bluetooth-technologybasics/low-energy.[Dostopano: februar 2016]* (2015).

- Levi, Albert, et al. "Relay attacks on bluetooth authentication and solutions." *Computer and Information Sciences-ISCIS 2004: 19th International Symposium, Kemer-Antalya, Turkey, October 27-29, 2004. Proceedings 19*. Springer Berlin Heidelberg, 2004.

- https://github.com/dotintent/awesome-ble

- https://github.com/wireshark/wireshark

THANK YOU

Bodrye Kamdem
Rifat Bin Islam