ESLab HW3

游祖鈞 B06209040

October 29, 2021

Reports with several issues and solutions presented. You may clone the project and configure per the instruction.
GitHub link: https://github.com/NOOMA-42/NTUEE-ESLab/tree/hw3
*Note: commit of different homework are in different branch.

1 general approach

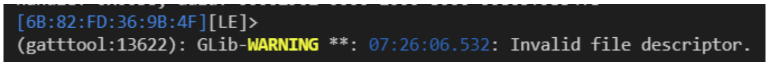
Rasberry Pi 3 serves as central and IPhone LightBlue as peripheral. Implement BLE CCCD notification.

1.1 hcconfig, hcitool, gatttool

Primary and char-desc command in gatttool are good to help me understand the structure of handle, UUID. [4]
Hcitool and gatttool have same issue over sensing Bluetooth data and the its ID is hidden and labled as unknown. I found out 2 ways to go about it. First is restart Lightblue and second is turn up and down the hcitool based on following code.

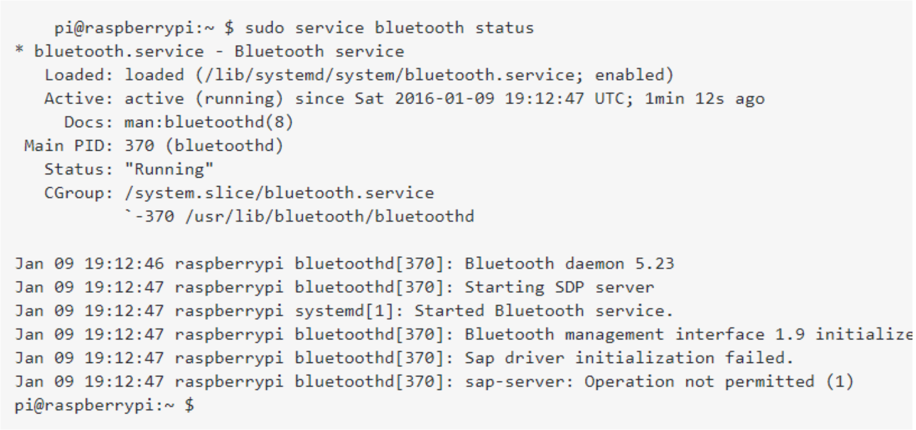
```
// Bluetooth dongle configuration
sudo hciconifg hci0 down
hcitool dev
>
Devices:
sudo hciconfig hci0 up
hcitool dev
>
Devices:
        hci0    00:1A:7D:DA:**:**
```

When I used gatttool with my Iphone as peripheral, even if I'm able to connect the peripheral, the connection will break up in 20 secs as shown below. With this in mind, I found out Bluetoothctl as a potential alternative and works just fine, although scan on and off in Bluetoothctl are extremely slow and sometimes might trigger crash. [9]
Another issue during interaction with peripheral with Bluetoothctl, Here's a command to see the bluetooth service status. I also learnt systemctl command in Linux [1]. This



```
[6B:82:FD:36:9B:4F][LE]>
(gatttool:13622): GLib-WARNING **: 07:26:06.532: Invalid file descriptor.
```

Figure 1: gatttool disconnect shortly after connection



```
    pi@raspberrypi:~ $ sudo service bluetooth status
* bluetooth.service - Bluetooth service
   Loaded: loaded (/lib/systemd/system/bluetooth.service; enabled)
   Active: active (running) since Sat 2016-01-09 19:12:47 UTC; 1min 12s ago
     Docs: man:bluetoothd(8)
 Main PID: 370 (bluetoothd)
   Status: "Running"
   CGroup: /system.slice/bluetooth.service
           `-370 /usr/lib/bluetooth/bluetoothd

Jan 09 19:12:46 raspberrypi bluetoothd[370]: Bluetooth daemon 5.23
Jan 09 19:12:47 raspberrypi bluetoothd[370]: Starting SDP server
Jan 09 19:12:47 raspberrypi systemd[1]: Started Bluetooth service.
Jan 09 19:12:47 raspberrypi bluetoothd[370]: Bluetooth management interface 1.9 initialize
Jan 09 19:12:47 raspberrypi bluetoothd[370]: Sap driver initialization failed.
Jan 09 19:12:47 raspberrypi bluetoothd[370]: sap-server: Operation not permitted (1)
pi@raspberrypi:~ $
```

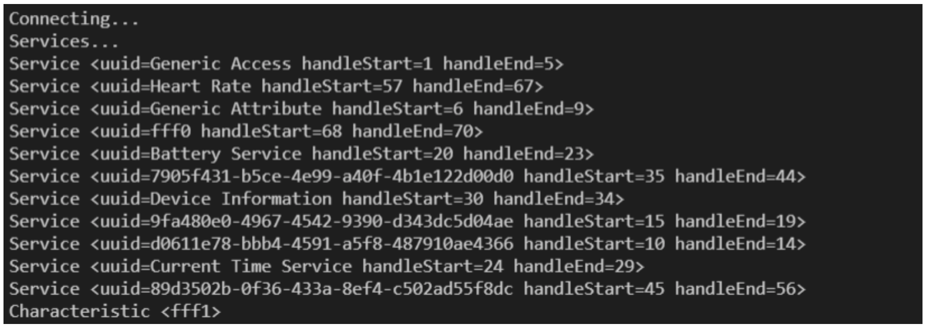
Figure 2: Bluetoothctl

allows us to check the system service and proceed with proper modification with these services.

1.2 LightBlue

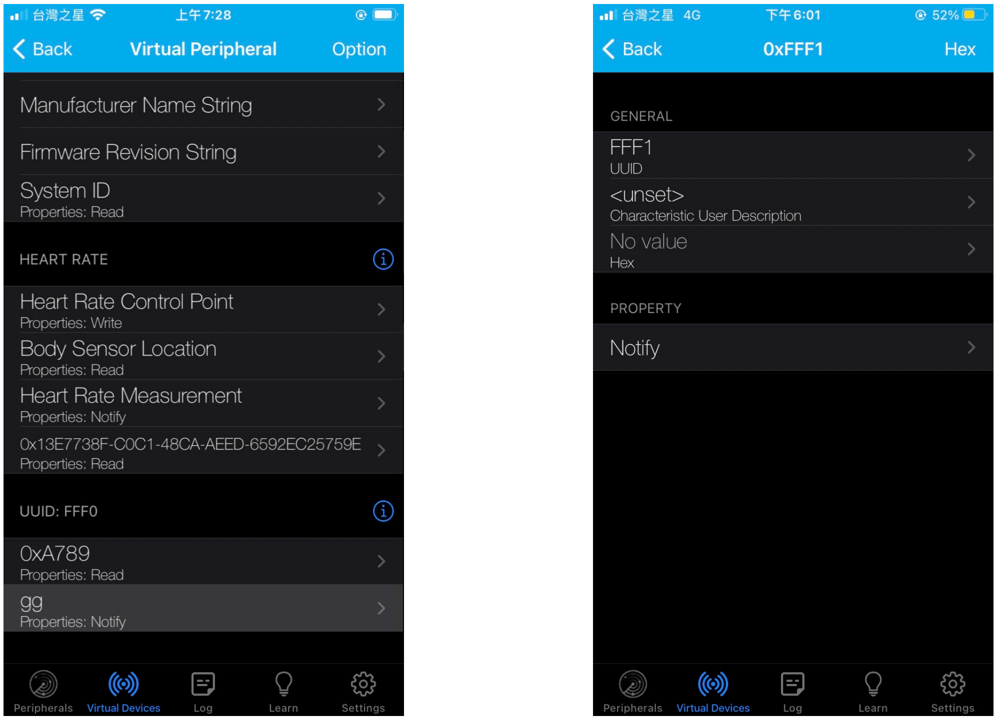
LightBlue is an IOS app for BLE scan. As 4 shows, I created a custom service and set up the character UUID and service UUID. Here's a few important findouts: First, Several services not specified by me jump out. In the post [7], we see LightBlue's Time profile can get us Current Time characteristic notifications. From this and screenshot 3, I knew these service belong to LightBlue and it its functionality.

5 and 6 shows handle-UUID-Value table with gatttool, we can see the table with char description is 1 row more than the one with char desc unset. Both of them end with UUID 2902 (in the middle) which represent CCCD and start with 2803 for service starting UUID. Right below the 2803 we see the fff1, a value set by me.
However, to enable notification in LightBlue on IOS, it seems that we're not allowd to set the characteristic descriptor (chardesciption unset) and change the character type to multi mode (only notify works). I'm unable to eliminate this issue even I make sure



```
Connecting...
Services...
Service <uuid=Generic Access handleStart=1 handleEnd=5>
Service <uuid=Heart Rate handleStart=57 handleEnd=67>
Service <uuid=Generic Attribute handleStart=6 handleEnd=9>
Service <uuid=fff0 handleStart=68 handleEnd=70>
Service <uuid=Battery Service handleStart=20 handleEnd=23>
Service <uuid=7905f431-b5ce-4e99-a40f-4b1e122d00d0 handleStart=35 handleEnd=44>
Service <uuid=Device Information handleStart=30 handleEnd=34>
Service <uuid=9fa480e0-4967-4542-9390-d343dc5d04ae handleStart=15 handleEnd=19>
Service <uuid=d0611e78-bbb4-4591-a5f8-487910ae4366 handleStart=10 handleEnd=14>
Service <uuid=Current Time Service handleStart=24 handleEnd=29>
Service <uuid=89d3502b-0f36-433a-8ef4-c502ad55f8dc handleStart=45 handleEnd=56>
Characteristic <fff1>
```

Figure 3: unspecified service jump out



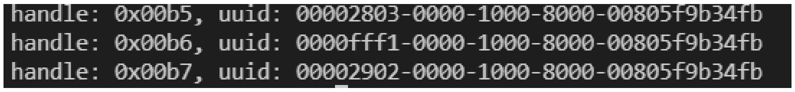
Manufacturer Name String
Firmware Revision String
System ID
Properties: Read
HEART RATE
Heart Rate Control Point
Properties: Write
Body Sensor Location
Properties: Read
Heart Rate Measurement
Properties: Notify
0x13E7738F-C0C1-48CA-AEED-6592EC25759E
Properties: Read
UUID: FFF0
0xA789
Properties: Read
gg
Properties: Notify

GENERAL
FFF1
UUID
<unset>
Characteristic User Description
No value
Hex
PROPERTY
Notify

(a) Heart Rate Service

(b)

Figure 4: LightBlue



```
handle: 0x00b5, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x00b6, uuid: 0000fff1-0000-1000-8000-00805f9b34fb
handle: 0x00b7, uuid: 00002902-0000-1000-8000-00805f9b34fb
```

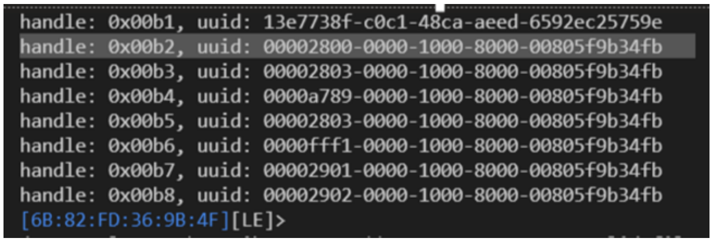
Figure 5: With char description unset, notify type

the handle of CCCD in the second case is 1 row more. Therefore, it remain unsolved for now.

1.3 ble_scan_connect

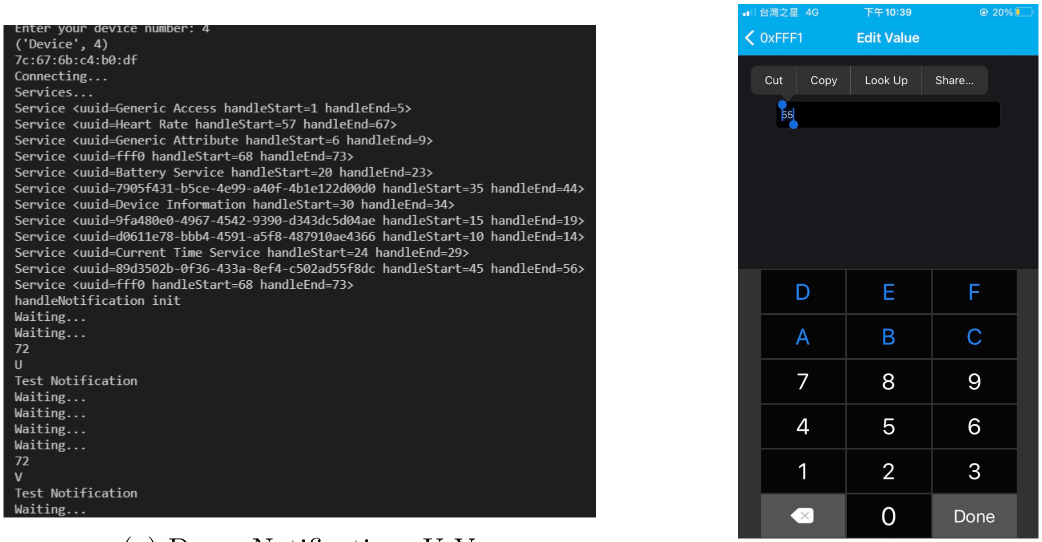
I referenced the bluepy API doc and added Peripheral class encapsulating delegate object and waitNotification loop. In order to receive the notification, I have to turn on notification functionality by writing 0100 into CCCD (UUID) [2]

The waitNotification instance method enables asynchronous data hearing. Once the peripheral notify the central. This method returns true and handleNotification in pe-



```
handle: 0x00b1, uuid: 13e7738f-c0c1-48ca-aeed-6592ec25759e
handle: 0x00b2, uuid: 00002800-0000-1000-8000-00805f9b34fb
handle: 0x00b3, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x00b4, uuid: 0000a789-0000-1000-8000-00805f9b34fb
handle: 0x00b5, uuid: 00002803-0000-1000-8000-00805f9b34fb
handle: 0x00b6, uuid: 0000fff1-0000-1000-8000-00805f9b34fb
handle: 0x00b7, uuid: 00002901-0000-1000-8000-00805f9b34fb
handle: 0x00b8, uuid: 00002902-0000-1000-8000-00805f9b34fb
[6B:82:FD:36:9B:4F][LE]>
```

Figure 6: With char description set, notify type



```
Enter your device number: 4
('Device', 4)
7c:67:6b:c4:b0:df
Connecting...
Services...
Service <uuid=Generic Access handleStart=1 handleEnd=5>
Service <uuid=Heart Rate handleStart=57 handleEnd=67>
Service <uuid=Generic Attribute handleStart=6 handleEnd=9>
Service <uuid=fff0 handleStart=68 handleEnd=73>
Service <uuid=Battery Service handleStart=20 handleEnd=23>
Service <uuid=7905f431-b5ce-4e99-a40f-4b1e122d00d0 handleStart=35 handleEnd=44>
Service <uuid=Device Information handleStart=30 handleEnd=34>
Service <uuid=9fa480e0-4967-4542-9390-d343dc5d04ae handleStart=15 handleEnd=19>
Service <uuid=d0611e78-bbb4-4591-a5f8-487910ae4366 handleStart=10 handleEnd=14>
Service <uuid=Current Time Service handleStart=24 handleEnd=29>
Service <uuid=89d3502b-0f36-433a-8ef4-c502ad55f8dc handleStart=45 handleEnd=56>
Service <uuid=fff0 handleStart=68 handleEnd=73>
handleNotification init
Waiting...
Waiting...
72
U
Test Notification
Waiting...
Waiting...
Waiting...
Waiting...
72
V
Test Notification
Waiting...
```

(a) Demo Notification: U V

(b) U V in hex on LightBlue

Figure 7: Demo

ripheral instance triggers.

1.4 Project Demo

The project demo screenshot is . I input 55 and 56 in hexadecimal. They are translated into U and V in the console.

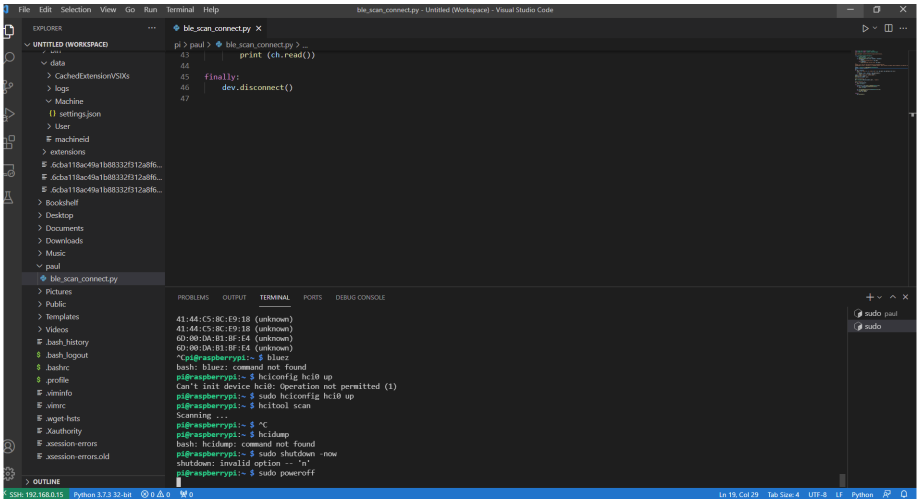
2 Miscellaneous Learning

2.1 helpful tool

WSL (Windows Subsystem for Linux) do not support hardware and I don't know what's the alternative for hcitool and gattool on windows so I can't test the pi3 as peripheral. VScode enable remote editing through SSH. [5] Therefore, I used SSH to remotely code the Raspberry Pi 3, which help me get rid of environment setup. [6]

3 Potential Improvement

First, Everytime I log in SSH remote I have to type the password. An dev environment without password will be awesome, Second, I'm unable to edit file in VSCode which requires sudo, there seems to be a config could be set in the setting.json. Third, Bluepy seems deprecated, and here exist other library like pybluez, gattpy. I might be trying other library. [3] and [8] someday. Fourthly, LightBlue issue still remain unsolved and worthy of investigated further.



```
        print (ch.read())

finally:
    dev.disconnect()

```

```
41:44:C5:8C:E9:18 (unknown)
41:44:C5:8C:E9:18 (unknown)
6D:00:DA:B1:BF:E4 (unknown)
6D:00:DA:B1:BF:E4 (unknown)
^Cpi@raspberrypi:~ $ bluez
bash: bluez: command not found
pi@raspberrypi:~ $ hciconfig hci0 up
Can't init device hci0: Operation not permitted (1)
pi@raspberrypi:~ $ sudo hciconfig hci0 up
pi@raspberrypi:~ $ hcitool scan
Scanning ...
pi@raspberrypi:~ $ ^C
pi@raspberrypi:~ $ hcidump
bash: hcidump: command not found
pi@raspberrypi:~ $ sudo shutdown -now
shutdown: invalid option -- 'n'
pi@raspberrypi:~ $ sudo poweroff
```

File Edit Selection View Go Run Terminal Help
ble_scan_connect.py - Untitled (Workspace) - Visual Studio Code
EXPLORER
UNTITLED (WORKSPACE)
ble_scan_connect.py
pi > paul > ble_scan_connect.py > ...
PROBLEMS OUTPUT TERMINAL PORTS DEBUG CONSOLE
SSH: 192.168.0.15
Python 3.7.3 32-bit

Figure 8: SSH through VScode

References

[1] GTW. linux-basic-systemctl-systemd-service-unit-tutorial-examples. https://blog.gtwang.org/linux/linux-basic-systemctl-systemd-service-unit-tutorial-examples/.

[2] Bluepy Github Issue. Code for notification? https://github.com/IanHarvey/bluepy/issues/124.

[3] PunchThrough. bluetooth-low-energy-peripheral-testing. https://punchthrough.com/bluetooth-low-energy-peripheral-testing/.

[4] qingfeng. 树莓派上使用低功耗蓝牙 ble 功能. https://blog.csdn.net/qingfengxd1/article/details/105142193.

[5] Raspberry. coding-on-raspberry-pi-remotely-with-visual-studio-code. https://www.raspberrypi.com/news/coding-on-raspberry-pi-remotely-with-visual-studio-code/.

[6] Raspberry. remote access. https://www.raspberrypi.com/documentation/computers/remote-access.html.

[7] StackOverflow. ios - punchthrough lightblue how do you make a virtual device send a notification? - stack overflow. https://stackoverflow.com/questions/63513988/punchthrough-lightblue-how-do-you-make-a-virtual-device-send-a-notification.

[8] zhuo lee new. Bluez, gattpy. https://blog.csdn.net/zhuo_lee_new/article/details/108649169.

[9] zjutlitao. 使用 bluetoothctl 搜索、连接、配对、读写、使能 notify 蓝牙低功耗设备. https://www.cnblogs.com/zjutlitao/p/9589661.html.