# 材料说明

## 蓝牙的简介

### 1.1蓝牙的起源

公元940-985年，哈洛德.布美塔特(Harald Blatand)，后人称Harald Bluetooth，统一了整个丹麦。他的名字“Blatand”可能取自两个古老的丹麦词语。“bla”意思是黑皮肤的，而“tan”是伟人的含义。和许多君王一样 ，哈洛德四处扩张，为政治、经济和荣誉而征战。公元960年哈洛德到达了他权力的最高点，征服了整个丹麦和挪威。有人说是因为这个国王喜欢吃蓝莓，所以牙齿被染成了蓝色，这个绰号也由此得来。在蓝牙这项无线技术诞生后，蓝牙技术的创建者们借此含义，希望这项无线技术为允许不同工业领域之间的协调工作，例如计算机手机和汽车行业之间的工作，实现方便通用的数据传输过程。

蓝牙标志的由来：是围绕国王Harald名字第一个北欧字母符号的蓝色椭圆形，像个大写的B字母。

### 1.2蓝牙的发展历程

#### 1.2.1蓝牙在哪些方面有应用

近年来随着蓝牙技术的不断发展和深人，蓝牙已不再仅仅局限于初始的定义，开始将设备之间的无线连接融合起来，形成个人的无线网络，即个人区域网(PAN)，使得在其范围之内的各种信息化的移动设备都能实现无缝的资源共享。蓝牙的应用也随之不断的拓展，从手机、笔记本、耳机等这样的手持终端扩展到各行各业，如汽车、医疗、工业控制、办公应用、电子商务等等，所涉及的技术、功能、市场等要求越来越高，产业链也日益复杂，已成为人们所关注的重点。

#### 1.2.2蓝牙技术联盟（Bluetooth SIG）

说到蓝牙，就不得不提到蓝牙技术联盟。虽然对于我们这些终端消费者来说，这样一家组织说起来离自己实在有些遥远，但实际上却和我们息息相关。因为所有有关蓝牙技术的规范和发展方向都是由这家组织所制定的，我们每尝试的一项蓝牙新应用，每体验的一款蓝牙新产品都要由这家组织开发、授权。因此在蓝牙发展的这些年中，蓝牙技术联盟一直都在扮演着一个至关重要的角色。蓝牙技术联盟是在1998年创建的，由当时的爱立信、英特尔、IBM、诺基亚、东芝这5家公司组成，发展到今天，联盟的成员也在一天天增多，现在已经有1000多家。这个技术联盟的主要作用是通过与各成员的合作及创新，不断提升蓝牙品牌，使蓝牙技术成为了当今连接不同设备的首选短距离无线技术。

#### 1.2.3回顾历史

这些年，蓝牙从一个初出茅庐的新名词到被大家所广泛认知；从最初仅仅是在手机上的崭露头角而发展到目前包括笔记本电脑、打印机、音频产品、外设产品甚至汽车、医疗设备在内的多方位领域都加以采纳；从传统的语音通话、文件数据传输扩展为包括诸如打印、远程遥控、上网等多层面应用，无疑，蓝牙技术已经取得了长足的发展。总结了蓝牙发展的三个阶段如下：

第一阶段：由爱立信提出，其他四个成员一起组建了蓝牙技术联盟，由最初的5个成员发展到400多个；蓝牙1.0规范发布，同时蓝牙技术获得当年COMDEX“最佳

展示技术奖”。

第二阶段：诞生了第一部内置蓝牙技术的手机及PC卡，并在CeBIT2000上展示了蓝牙鼠标和蓝牙笔记本电脑样机。第一款基于蓝牙技术的打印机、笔记本电脑、免提车载套件等产品相继问世。蓝牙GPS接收设备以及蓝牙键盘和鼠标套件诞生，获得蓝牙无线认证的产品达到500种，同时IEEE批准了蓝牙技术标准802.15.1规范。

第三阶段：蓝牙MP3播放器诞生。蓝牙规范升级到V1.2，同时蓝牙技术进入医疗系统。蓝牙技术联盟推出V2.0规范和增强型数据速率（EDR）。随后诞生了第一款蓝牙立体声耳机。蓝牙芯片每周的出货量增长到500万，而蓝牙技术联盟的成员达到4000家。诞生了第一块蓝牙手表和蓝牙数码相框，蓝牙设备累计达10亿件。人们甚至可以买到蓝牙电视机产品了。而蓝牙技术联盟的成员更是达到了9000家。产品的日益丰富以及价格水平的不断降低使蓝牙这项技术变得越来越有人缘。根据研究机构Millward Brown的一份最新调查结果显示：在全球消费者对于主流传输技术的认知程度和整体印象中，蓝牙以85％高居榜首，排在第二位和第三位的分别是57％的ＵSB和53％的Wi-Fi。可见蓝牙已经完完全全融入我们的生活，并让我们的生活变得更加轻松。

### 1.3蓝牙的先进技术

1、 蓝牙传输有效范围

蓝牙设备的传输距离与功耗有着直接联系。最为常见的为 Class2模式，有效传输距离为10米，此外还有Class1模式和Class3模式，传输距离分别为100米和1米。

2、 蓝牙技术的工作频率

蓝牙无线技术是在无需政府牌照许可的2.4 GHz ISM波段上工作的。

3、 如何避免干扰

蓝牙是一种短距离的无线通信技术，无线通信最重要要克服多路径衰减及共频道干扰；它的传输范围还受功耗、抗干扰能力、地里环境、接收设备的灵敏度等的影响。蓝牙怎样克服这些不足的因素呢？蓝牙采用自适应跳频的方法，AFH是一种对蓝牙和无线局域网所使用频率进行分离的频率分离技术，在AFH方法中要求无线局域网所使用的频率信道带宽为26 MHz，而且必须要使用固定的信道。支持蓝牙功能的设备跳频一般是在带宽1 MHz的频率范围内设定79个信道，在is内对信道进行1 600次切换。AFH采用的方法是首先测定支持蓝牙设备在通信的第一阶段的数据包损失比例，从所有的79个信道中选择使用干扰较少的15个频率信道完成蓝牙数据的发送和接受，这样就能较大准确接收蓝牙数据。

4、 蓝牙技术的版本

先后有V1.0、V1.1、V1.2、V2.0和V2.1等版本。在V1.1版本中分清了主从角色；V1.2版本中加入适应性跳频技术；V2.0版本则在数据传输速度上大幅提升；V2.1进一步缩短配对时间（由配对的两个设备自动生成6位的PIN码自行配对），并且降低能耗。

5、 传输速率

EDR是enhanced data rate支持了这个,蓝牙的传输速率才能有比较大的改善。蓝牙 作为无线通讯的网络传输技术，对于构建一个良好的局域网络可能有着速度上的问题。在Bluetooth2.0的规范中，EDR作为补充出现的，它正确定义了调变技术的改变和额外的封包类型,这使它能够以3MBPS的速率传输.所以，我们通常看到的是"蓝牙核心规范2.0版本+ EDR"的说法。向下兼容蓝牙版本1.2. 蓝牙系统的主机最多可连接7台从属装置，最高传输速度为712 kb/s。

6、 安全性

蓝牙提供了服务级和连接级的安全保障。基于蓝牙的应用服务可以限定授权对象，而蓝牙设备间的连接则需要通过密码进行配对后方可建立连接。

7、 蓝牙技术的协议

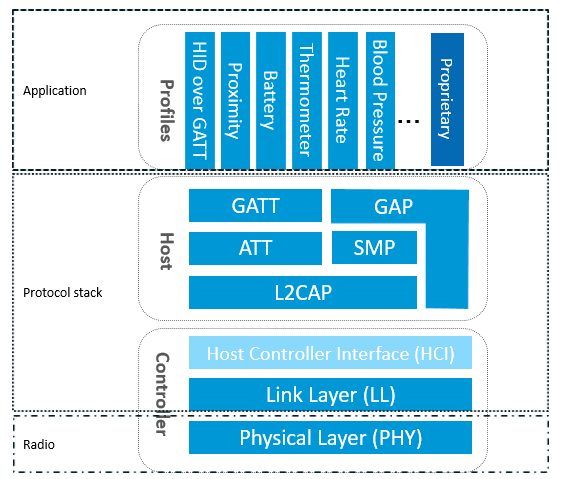
A2DP（高级音频发送，即立体声蓝牙），AVRCP（音、视频控制传输）、BIP（图像传送）、BPP（打印控制）、FAX（传真）、FTP（文件传输）、HID（人机输入）、DUN（网络拨号）等。

8、 应用在哪些方面

蓝牙技术的应用如今已经变得非常广泛。除了我们常见的手机、掌上电脑、GPS、笔记本电脑、打印机、游戏机等产品之外，还可以应用到耳机、音箱、键盘、鼠标等外设中。此外车载和医疗器械上也开始越来越多地应用蓝牙技术。

### 1.4蓝牙协议栈的分层结构

蓝牙技术规范的目的是使符合该规范的各种应用之间能够实现互操作。互操作的远端设备需要使用相同的协议栈，不同的应用需要不同的协议栈。但是，所有的应用都要使用蓝牙技术规范中的数据链路层和物理层。



如上图所述，要实现一个BLE应用，首先需要一个支持BLE射频的芯片，然后还需要提供一个与此芯片配套的BLE协议栈，最后在协议栈上开发自己的应用。可以看出BLE协议栈是连接芯片和应用的桥梁，是实现整个BLE应用的关键。那BLE协议栈具体包含哪些功能呢？简单来说，BLE协议栈主要用来对你的应用数据进行层层封包，以生成一个满足BLE协议的空中数据包，也就是说，把应用数据包裹在一系列的帧头（header）和帧尾（tail）中。具体来说，BLE协议栈主要由如下几部分组成：

* PHY层（Physical layer物理层）。PHY层用来指定BLE所用的无线频段，调制解调方式和方法等。PHY层做得好不好，直接决定整个BLE芯片的功耗，灵敏度以及selectivity等射频指标。
* LL层（Link Layer链路层）。LL层是整个BLE协议栈的核心，也是BLE协议栈的难点和重点。像Nordic的BLE协议栈能同时支持20个link（连接），就是LL层的功劳。LL层要做的事情非常多，比如具体选择哪个射频通道进行通信，怎么识别空中数据包，具体在哪个时间点把数据包发送出去，怎么保证数据的完整性，ACK如何接收，如何进行重传，以及如何对链路进行管理和控制等等。LL层只负责把数据发出去或者收回来，对数据进行怎样的解析则交给上面的GAP或者GATT。
* HCI（Host controller interface）。HCI是可选的（具体请参考文章： 三种蓝牙架构实现方案（蓝牙协议栈方案）），HCI主要用于2颗芯片实现BLE协议栈的场合，用来规范两者之间的通信协议和通信命令等。
* GAP层（Generic access profile）。GAP是对LL层payload（有效数据包）如何进行解析的两种方式中的一种，而且是最简单的那一种。GAP简单的对LL payload进行一些规范和定义，因此GAP能实现的功能极其有限。GAP目前主要用来进行广播，扫描和发起连接等。
* L2CAP层（Logic link control and adaptation protocol）。L2CAP对LL进行了一次简单封装，LL只关心传输的数据本身，L2CAP就要区分是加密通道还是普通通道，同时还要对连接间隔进行管理。
* SMP（Secure manager protocol）。SMP用来管理BLE连接的加密和安全的，如何保证连接的安全性，同时不影响用户的体验，这些都是SMP要考虑的工作。
* ATT（Attribute protocol）。简单来说，ATT层用来定义用户命令及命令操作的数据，比如读取某个数据或者写某个数据。BLE协议栈中，开发者接触最多的就是ATT。BLE引入了attribute概念，用来描述一条一条的数据。Attribute除了定义数据，同时定义该数据可以使用的ATT命令，因此这一层被称为ATT层。
* GATT（Generic attribute profile ）。GATT用来规范attribute中的数据内容，并运用group（分组）的概念对attribute进行分类管理。没有GATT，BLE协议栈也能跑，但互联互通就会出问题，也正是因为有了GATT和各种各样的应用profile，BLE摆脱了ZigBee等无线协议的兼容性困境，成了出货量最大的2.4G无线通信产品。

### 1.5 蓝牙的应用

1、 在办公室（In Your Office）

蓝牙是办公室里不可或缺的一份子。首先蓝牙适配器的诞生让更多设备生长出蓝牙的翅膀，尤其对于办公室里那些老旧的台式机，大大提升了其活力。在办公室里，你也看到越来越多的桌面开始变得整洁，原本繁杂的鼠标、键盘连接线被看不见的蓝牙所代替，同时可以实现长达10米的连接距离。利用蓝牙来进行文件传输也成为办公室里更高效的选择，无论是文件共享还是打印都易如反掌。此外，诸如视频会议设备、手写板以及麦克风也开始将蓝牙技术融入其中。

2、 在汽车里（In Your Car）

对于车载产品来讲，蓝牙技术并不陌生。蓝牙耳机或者蓝牙免提装置是最常见的，它能保障司机在开车过程中解放双手，进行更安全的通话。你甚至还可以通过车中的导航显示屏来浏览自己手机中的电话簿。想在车中进行GPS地图或兴趣点的升级和更新吗？如果你的GPS设备有蓝牙功能一切就会变得简单。你可以通过蓝牙将GPS连接至手机，然后上网进行更新。而通过A2DP，在车里面欣赏无线立体声音乐也变为了现实，任何一部蓝牙音频播放设备都可以与车中的蓝牙音响来连接。当然如果播放器不支持蓝牙，也可以通过外接蓝牙适配器来解决这一问题。

3、 在手机上（On Your Phone）

手机一直都是蓝牙设备的理想应用平台，因为手机体积小巧，携带方便，同时蓝牙的低功耗特点也不会为手机带来更多的能耗负担。蓝牙在手机上最初的应用无疑是音频通话，而这也是到目前为止人们最普及的应用之一。 当然除此之外，蓝牙在手机上还能干更多事情。例如它可以帮助你将手机中的文件、

照片甚至是电子名片或日程表信息传输到其他蓝牙设备上，或者把手机作为Modem，利用蓝牙连接其他设备上网。通过蓝牙，你还可以轻松地完成手机与笔记本电脑或台式机的个人信息无线同步。

4、 和你的照片（With Your Picture）

在照片的分享过程中，蓝牙也扮演着重要的角色。不仅是手机，就连数码相机也打起了蓝牙的主意。无论是何种设备，你都可以将其中的照片通过蓝牙发送到其它设备上，例如手机、笔记本电脑，甚至是拥有蓝牙功能的电视机或数码相框，没有任何障碍地实现照片的分享。而蓝牙打印则是另一种应用，不需要借助电脑或存储卡，只需通过蓝牙将照片发送到支持蓝牙数据接收的打印机上就可以自动打印出精美照片。当然不仅仅是打印机，现在就连柯达影像店里面的自助冲印站也都引入了蓝牙打印功能。

5、 和你的音乐（With Your Music）

如果说单声道蓝牙耳机开创了蓝牙音频应用历史的话，那么A2DP的诞生则是真正让无线音乐来到了我们每个人的身边。立体声蓝牙技术依靠稳定的传输以及数字信号处理技术，可以实现高质量的无线立体声音乐。而蓝牙立体声技术也从手机、笔记本电脑、音乐播放器这些个人化的产品扩展到车载音响、家庭影院系统、小型台式音响、便携式扬声器这些的可以众人一起分享的设备上。由于告别了线缆的束缚，使得这些立体声音频设备的摆放更加自由，同时可以实现更灵活、更多样的音频输入、输出过程。

### 1.6 蓝牙的未来

1、 蓝牙的低功耗技术

蓝牙低功耗技术将满足用户对于蓝牙设备拥有更长使用时间的需求。该技术将用于需要超长电池寿命（数年而不是数小时）的设备，例如远程遥控器。蓝牙在这方面具备诸多优势，例如跨行业产品的交互性、更大连接距离等等。无论是电视、DVD播放器、机顶盒或多媒体播放器，这些产品都能够与之匹配。

2、 高速传输标准

2006年，蓝牙技术联盟宣布选择WiMedia联盟的超宽带技术作为蓝牙技术的高速解决方案。目前两大联盟正在携手研发蓝牙与超宽带技术的兼容性。同时蓝牙技术联盟将充分利用IEEE 802.11技术。 在高速蓝牙技术问市后，你无需线缆就可以在自己的设备与好友的可靠的设备之间进行影音娱乐的传输。

3、 助听设备

对于许多老年人而言，助听器是他们必不可少的随身医疗设备。而蓝牙也有望在这类设备上得以应用。蓝牙助听设备可连接到手机或PDA上面，然后清晰地接听到通话或其它音频内容。当然这种设备在日常同样能够扮演起传统助听器的角色，无论是人与人的对话或是收看电视节目或收听音乐都不会有任何问题。

4、 营销广告

手机短信广告已经成为一种成熟的营销模式，在以后你也许还会收到一种新型的蓝牙广告。这种想法正在逐步转化为现实。在购物中心、赛场或是其它公共场合，你会收到来自附近接入点的Push推送服务内容，它们可能是铃声、墙纸或者促销广告。当然相对于短信方式，通过蓝牙要安全得多，因为你可以选择接收或拒绝，甚至可以事先就将蓝牙功能关闭。

5、 白色家电（如电冰箱）

      爱立信与海尔集团宣布，将共同开发蓝牙网络家电。所谓蓝牙网络家电，是一种新一代的网络家电产品，它可以实现 对家电的集中遥控。也就是说用户只需手握一个遥控装置，就能实现对家里所有家用电器比如洗衣机、空调、洗碗机、微波炉、电热水器和冰箱等的遥控。

从目前的情况看，计算机行业、移动通信行业和家电行业都十分青睐蓝牙技术，认为蓝牙技术将对未来的无线移动数据通信业务产生巨大的促进作用。蓝牙技术已被公认为是无线数据通信最为重大的进展之一。当然，蓝牙仍然是一项发展中的技术，其应用目前还处于起步阶段，要真正达到大规模进入商用市场并在用户中普及，还有大量应用技术细节需要解决。

### 1.7蓝牙基本信息设置

1、 蓝牙设备地址 & 名字。地址由6个字段组成，前三个字段表示生产商编号，后三个字段随便分配，出厂之前每台蓝牙设备的地址都是唯一的。6个字段，一个字段8位，用十六进制表示的话就是两个十六进制，一共有248种组合。蓝牙设备的名字最大是30个字节，还加上结束符一共是31个字节。

2、 可见性：可见性的两种模式general mode/limited mode，general mode是设备一直可见的，只要蓝牙开启，其他设备就能搜索到该蓝牙设备；limited mode处于这种模式的蓝牙设备，可见性只是一段时间可见的，比如三分钟，过了三分钟设备又将变为不可见，如果设置过可见性，过了这个时间想重新搜索该设备的话就必须重新设

置可见性。

3、 连接模式 &配对模式：这两种模式主要是就现在的蓝牙耳机而言的。对于像手机这样的产品，当蓝牙开启时，远程设备可以搜索进行配对，也可以在设备列表里连接，也就是说当手机的蓝牙开启了，它就处于连接模式和配对模式了。但对蓝牙耳机而言，这两个模式是分开的，当处于配对模式时，远程蓝牙设备只能对其配对，不能连接，当处于连接状态时只能连接不能配对。

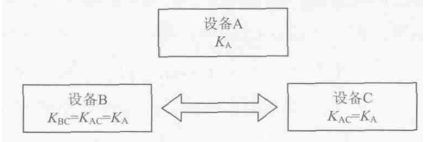
4、 设备状态：slient mode/trusted mode.当设备正忙（正在和其他设备交互并且不允许其他设备再次访问该设备）或者设备是不可见的时候，我们就把这种设备叫做slient设备，这个时候的设备是不能被其他设备搜索到的。Trusted是设备处于受信任模式，这是对绑定过的设备而言，如果绑定过的设备处于受信任模式，当该设备访问本机时就不必再询问，直接访问。设置设备成为受信任模式也叫做授权的过程。

5、 询问模式：general inquiry/limited inquiry. General inquiry询问方式是在搜索设备的时候搜索全部的设备，也就是搜索的时候serviceclass是0xFF;limited inquiry的询问方式是搜索有限的设备，比如audio设备。

6、通信状态下的模式：Active/Sniff/Hold/Park，当设备处于active状态时，每隔1.28s向周围发送信息，它是一串序列，包含了类型，位置，服务等多种消息。当可用范围内的设备监听到主设备发送的信息后，立即做出反应，将自己支持的协议，功能模型回馈到主设备，这样主设备上就能显示出周围可使用的设备。 后面三种模式是为节能而使用的低功耗模式。

## 蓝牙中间人攻击原理

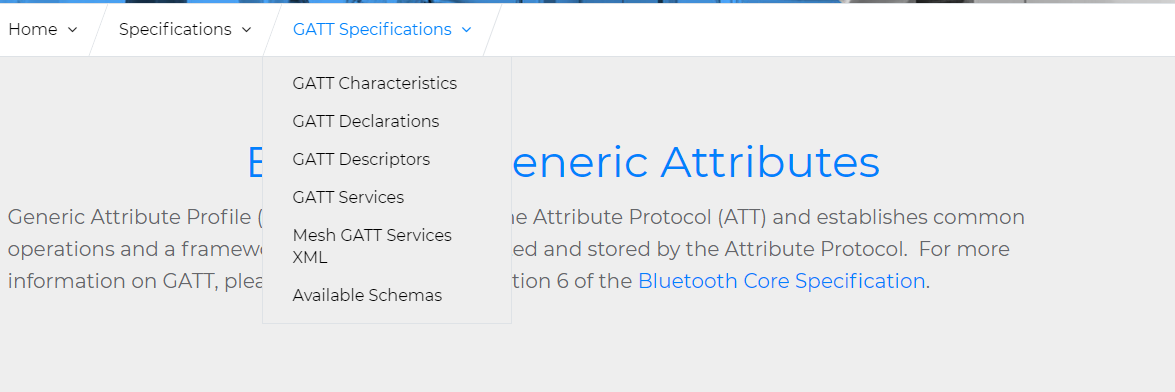
在两个设备之间的攻击者截获数据一方发送的数据后再转发给另一方，可在不影响双方通信的情况下获得双方通信的内容，是一种广泛应用于无线网络的攻击方式。蓝牙 4.0 版本的低功耗蓝牙技术（Bluetooth Low Energy，BLE）在设计初始时有防范中间人攻击的安全措施，但是在产品阶段考虑到产品功耗成本等因素，这方面并没有得到足够的重视，依然容易受到攻击。最常见的是用软硬件结合的蓝牙攻击设备伪造BLE 通信进行中间人攻击。中间人攻击示意图下图所示。



## 蓝牙数据包简析

### 3.1 GATT层

关于GATT的一些服务的名称，可通过下面的网址进行查阅：

<https://www.bluetooth.com/specifications/gatt/>

蓝牙协议中包含了许多种GATT规范，每个规范适配一种用户案例，比如FindMe规范适配查找物件的场景，心率传感器规范适配心率测量场景。

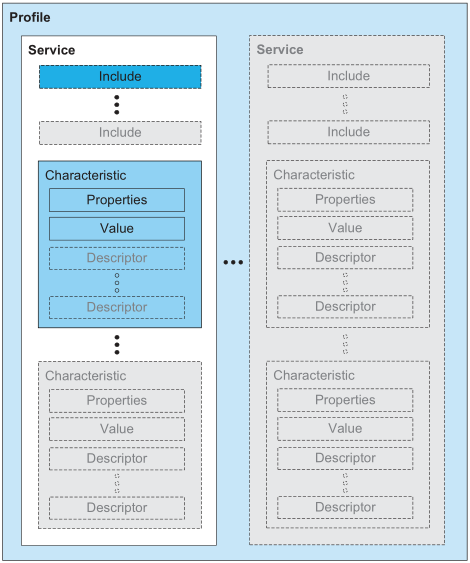
每个规范均中均有若干服务项和特征项，服务项和特征项都属于属性实体，它们携带了通信中传输的数据。

服务项分为主要服务和次要服务，主要服务可以引用（Include）另一个主要服务或次要服务，客户端设备可以通过“主要服务发现过程”获取主要服务信息。

特征项包括一个声明、配置、数据和描述符。描述符用于描述特征项的数据如何被访问和展示。

规范、服务项和特征项之间有明确的包含关系，一个GATT规范中可以包括多个服务项，一个服务项中可以包括多个特征项。

GATT的规范结构框图如下：



#### 2.2.1属性

一个属性包含句柄、UUID(类型)、值，句柄是属性在GATT表中的索引，在一个设备中每一个属性的句柄都是唯一的。UUID包含属性表中数据类型的信息，它是理解属性表中的值的每一个字节的意义的关键信息。在一个GATT表中可能有许多属性，这些属性能可能有相同的UUID。

#### 2.2.2 特性

一个特性至少包含2个属性：一个属性用于声明，一个属性用于存放特性的值。

所有通过GATT服务传输的数据必须映射成一系列的特性，可以把特性中的这些数据看成是一个个捆绑起来的数据，每个特性就是一个自我包容而独立的数据点。 例如，如果几块数据总是一起变化，那么我们可以把它们集中在一个特性里。

#### 2.2.3描述符

任何在特性中的属性不是定义为属性值就是为描述符。描述符是一个额外的属性以提供更多特性的信息，它提供一个人类可识别的特性描述的实例。

然而，有一个特别的描述符值得特别地提起：客户端特性配置描述符(Client Characteristic Configuration Descriptor，CCCD)，这个描述符是给任何支持通知或指示功能的特性额外增加的。

在CCCD中写入“1”使能通知功能，写入“2”使能指示功能，写入“0”同时禁止通知和指示功能。

#### 2.2.4服务

一个服务包含一个或多个特性，这些特性是逻辑上相关的集合体。

GATT服务一般包含几块具有相关的功能，比如特定传感器的读取和设置，人机接口的输入输出。组织具有相关的特性到服务中既实用又有效，因为它使得逻辑上和用户数据上的边界变得更加清晰，同时它也有助于不同应用程序间代码的重用。GATT基于蓝牙技术联盟(SIG)官方而设计，SIG建议根据它们的规范设计自己的profile。

#### 2.2.5 profile（数据配置文件）

一个profile文件可以包含一个或者多个服务，一个profile文件包含需要的服务的信息或者为对等设备如何交互的配置文件的选项信息。设备的GAP和GATT的角色都可能在数据的交换过程中改变，因此，这个文件应该包含广播的种类、所使用的连接间隔、所需的安全等级等信息。

需要注意的是： 一个profile中的属性表不能包含另一个属性表。

#### 2.2.6 标准的定制服务和特性

蓝牙技术联盟(SIG)已经定义一些profile、服务、特性和根据协议栈的GATT层定义的属性。但是，协议栈中只实现了一部分应用的BLE服务，那就意味着，只要协议栈支持GATT，就可能为一个应用建立一个它需要的profile和服务。

既然在一个应用中可以支持profile和服务，那么就可以在这个应用中建立一个定制的服务。

#### 2.2.7 UUID

“GATT层”中定义的所有属性都有一个UUID值，UUID是全球唯一的128位的号码，它用来识别不同的特性。

1. 蓝牙技术联盟 UUID

蓝牙核心规范制定了两种不同的UUID，一种是基本的UUID，一种是代替基本UUID的16位UUID。

所有的蓝牙技术联盟定义UUID共用了一个基本的UUID：

0x0000xxxx-0000-1000-8000-00805F9B34FB

为了进一步简化基本UUID，每一个蓝牙技术联盟定义的属性有一个唯一的16位UUID，以代替上面的基本UUID的‘x’部分。例如，心率测量特性使用0X2A37作为它的16位UUID，因此它完整的128位UUID为：

0x00002A37-0000-1000-8000-00805F9B34FB

虽然蓝牙技术联盟使用相同的基本UUID，但是16位的UUID足够唯一地识别蓝牙技术联盟所定义的各种属性。

蓝牙技术联盟所用的基本UUID不能用于任何定制的属性、服务和特性。对于定制的属性，必须使用另外完整的128位UUID。

1. 供应商特定的UUID

SoftDevice 根据蓝牙技术联盟定义UUID类似的方式定义UUID：先增加一个特定的基本UUID，再定义一个16位的UUID（类似于一个别名），再加载在基本UUID之上。这种采用为所有的定制属性定义一个共用的基本UUID的方式使得应用变为更加简单，至少在同一服务中更是如此。

使用软件nRFgo Studio非常容易产生一个新的基本UUID：

例如，在LED BUTTON示例中，采用0x0000xxxx-1212-EFDE-1523-785FEABCD123作为基本UUID。

蓝牙核心规范没有任何规则或是建议如何对加入基本UUID的16位UUID进行分配，因此你可以按照你的意图来任意分配。

例如，在LED BUTTON示例中，0x1523作为服务的UUID，0x1524作为LED特性的UUID，0x1525作为按键状态特性的UUID。

#### 2.2.8 空中操作和性质

大部分的空中操作事件都是采用句柄来进行的，因为句柄能够唯一识别各个属性。如何使用特性依据它的性质，特性的性质包括：

1）写

2）没有回应的写

3）读

4）通知

5）指示

写和没有回应的写

写和没有回应的写允许GATT客户端写入一个值到GATT服务器的一个特性中。它们之间不同的地方在于没有回应的写事件没有任何应用层上的确认或回应。

读

读性质表明一个GATT客户端可以读取在GATT服务器中特性的值。

通知和指示

通知和指示性质允许GATT服务器在其某个特性改变的时候对GATT客户端进行提醒，通知和指示之间不同之处在于指示有应用层上的确认，而通知没有。

## 针对BLE设备中间人攻击

这是一个有趣的项目，其中介绍了如何对使用蓝牙低功耗（BLE）进行数据交换的测温枪进行中间人攻击。由于测温枪使用低功耗蓝牙（Bluetooth Low Energy）（是蓝牙4.0的子集），因此从理论上讲任何BLE设备都可以控制灯泡。但是要控制灯泡，必须了解与灯泡进行通信的协议，并且本文将向您展示如何使用Bluefruit LE嗅探器和其他工具对蓝牙低功耗小工具进行中间人攻击。

我们需要如下的一些硬件：

* 蓝牙4.0 USB模块。确保模块支持低功耗蓝牙。 4.0版之前的旧版蓝牙不支持BLE！
* PC计算机。最好使用带有Linux系统的计算机，并保证计算机带有USB口，在Linux系统下能够使用一些很好用的小工具，十分便于我们调试，USB口则是其他硬件设备与计算机连接的必备接口。
* 手机（Andriod或IOS），通过手机端的软件与测温枪相连。
* 测温枪，能够测量身体的温度数据，并通过蓝牙连接到app传输温度数据给手机端。
* Bluefruit LE Sniffer。 Bluefruit LE Sniffer是Bluefruit LE friend的特殊版本，可以允许查看来自其他设备的BLE数据包。

### GATT服务初探

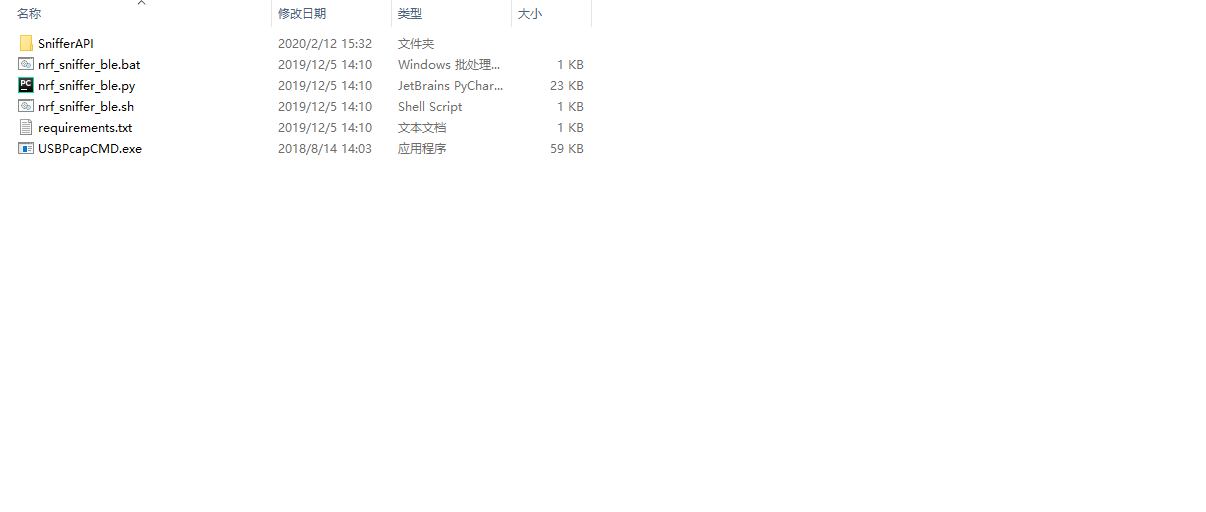
我使用了IOS上的一款名为LightBlue的蓝牙调试软件进行初步测试，这是测试图：



从这张图我们可以看到我们的测温枪的设备名和使用的服务名以及设备的一些信息以及使用该服务发送的一些值。

### WireShrak抓包

我们继续使用WireShark软件对测温枪的发送数据进行探究，要注意的是，在进行这些活动时，测温枪不能连接其专用的APP，否则将会无法抓包。同时，我在github上上传了名为nrf\_sniffer\_for\_bluetooth\_le\_3.0.0\_129d2b3的wireshark插件，将其中的extcap文件夹复制到wireshark对应的文件夹，即可在wireshark中使用低功耗蓝牙抓取的插件，使抓包过程更为便捷：



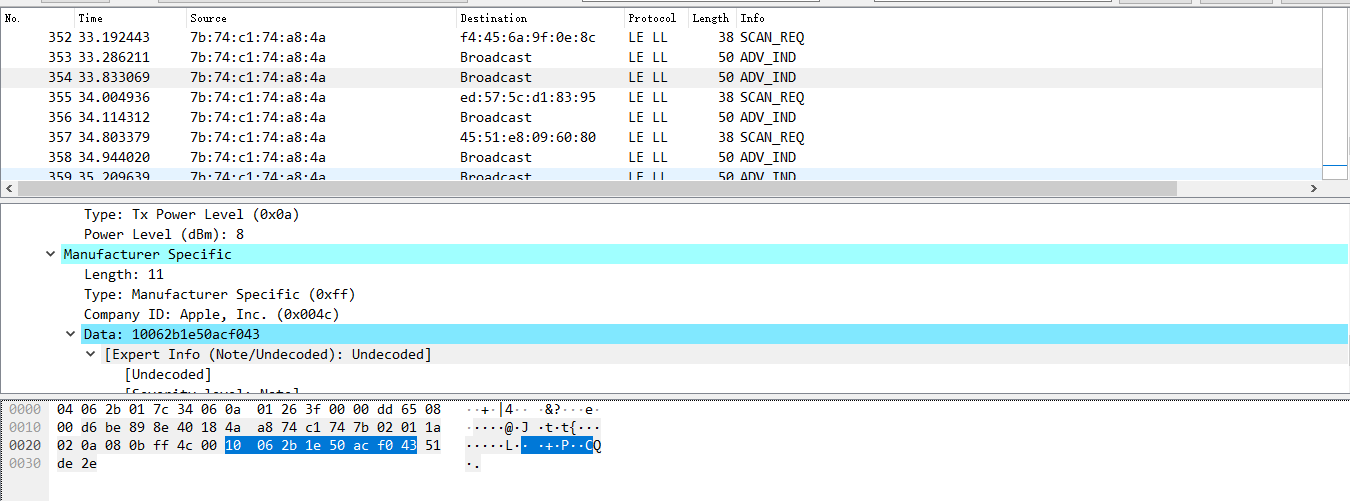
复制后的文件夹



插件示意

下面我们正式开始使用sniffer抓取BLE包，在使用Bluefruit LE sniffer嗅探BLE流量之前，需要注意的一件事是，它可能对来自其他BLE设备的噪声敏感。尝试关闭附近的所有其他BLE设备，例如平板电脑，电话等。还要确保PC上正在运行的程序尽可能少，因为该工具需要尽快从Bluefruit嗅探器获取数据以防止数据包丢失。

Wireshark加载后，很快就会看到大量广告包，例如：

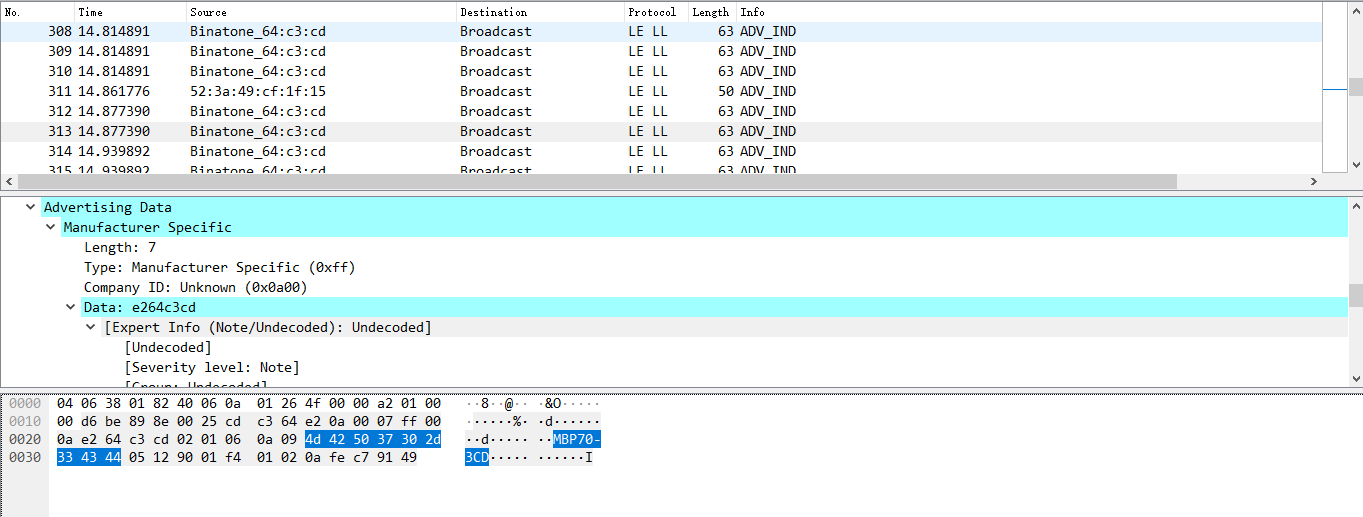


上图所示的窗口可以分为三个部分：

* 前三分之一是已捕获的数据包列表。当wireshark捕获数据包时，此列表将迅速增长。您可以上下滚动查看收到的数据包，也可以单击数据包以查看有关它的更多信息。
* 中间三分之一是已从数据包解码的信息。您可以深入查看数据包中的特定帧，以查看其作用。在这一层我们可以看到一些能够阅读的详细的数据包信息。
* 底部的三分之一是数据包数据的原始十六进制和ASCII表示形式。有趣的是，当您单击中间窗格中的信息时，您会在底部窗格中看到原始信息高亮表示。

在上图中，我选择了一个手机的广告包，并在中间窗格中突出了一些有趣的细节。您可以看到此数据包来自手机，他在不间断的向外发送广播包，同时广播包里面带上了一些自定义的数据。在上面的窗格中我们还可以看到，在app上点击搜索的时候，手机向一些固定的mac地址发送了SCAN\_REQ的广播包。

然后我们启动手机端的app，连接到测温枪，并在这个过程中一直启动sniffer，抓包结果如下图：



可以看到，测温枪一直在发送同一段广播包，里面包含了设备名，以及一段重复的数据，但是从协议端可以看到，我们只能观察到LE LL协议的内容，一直没有抓取到ATT类型的包，而只有那种的包才能识别出对我们有用的信息。到这里wireshark抓包就告一段落了。

### 进行MITM攻击

#### 3.3.1接收

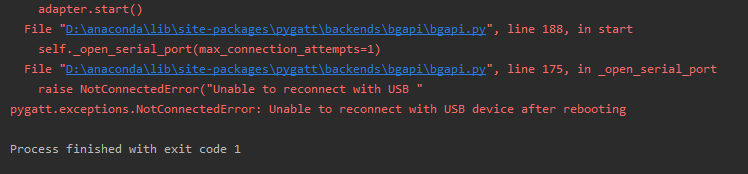
从上面的分析可知，我们这里可以实施较为初级的攻击，即首先将测温枪连接到自己的电脑，同时读取数据，得到测温枪发送的数据格式，但是这一步并不是最重要的。

因为在我们的项目中，测温枪发送温度这一最重要的步骤我们是无法探知的，这不同于其他一些蓝牙设备的交互逻辑，在我们的项目中，从设备（即测温枪）是数据的发送方，所以他发送的数据必须要连接上主设备后才开始发送，所以我们不能达到他发送温度数据的格式。但是如果是一个使用手机蓝牙控制小灯这样的应用中，就算没有连接上小灯，我们仍然可以通过手机发送命令，这就给了我们探究该命令数据格式的机会。但是所幸我们的项目发送数据必须使用规定的服务方式，所以理论上数据格式是固定的。

然后这一步也是没有成功，因为这一步需要使用蓝牙接收器来连接上测温枪接收数据并分析，但是我的电脑当蓝牙接收器连接上的时候没办法识别COM口，所以就没办法搜索设备。：



蓝牙接收器adapter

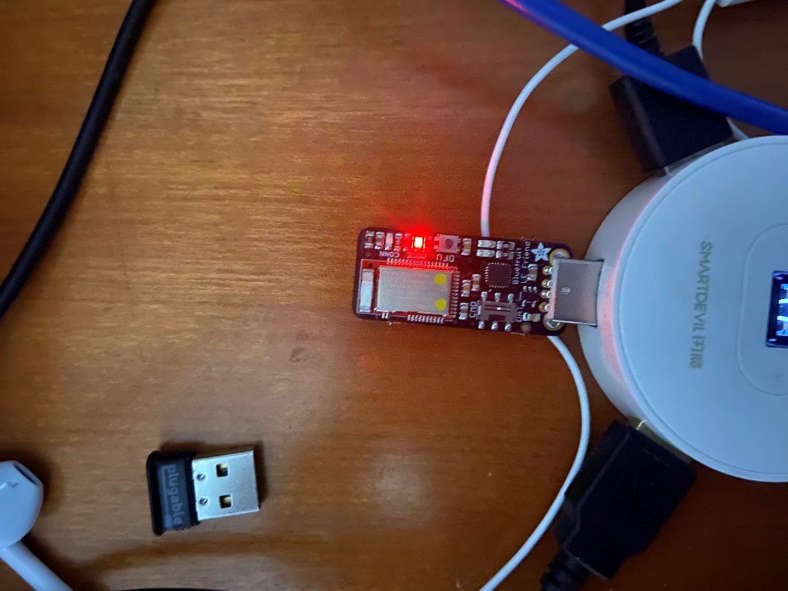


代码运行失败截图

这个部分属于硬件问题，可能出问题的地方是这个蓝牙接收器、或者是windows下这个代码的问题，因为我现在没有Linux系统的环境，所以这个问题暂时是无解的。

#### 3.3.2发送

接收到了数据，接下来我们分析一下这个数据就将它发送出去，发送的时候使用LE Friend：



LE friend

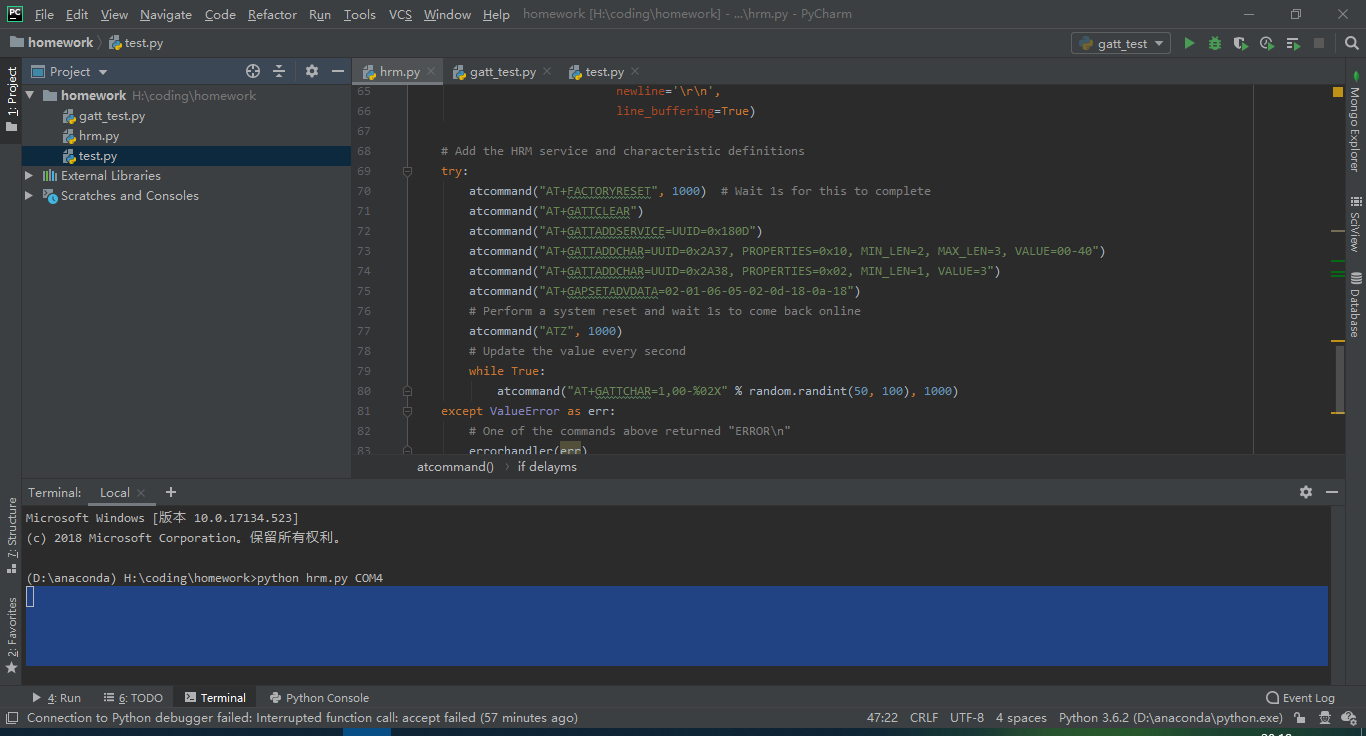
同样的，这个LE friend也是亮红灯，无法工作，但是你给的那个sniffer和这个LE friend是一模一样的东西，然后它可以使用，所以我用了你给的sniffer：



Sniffer

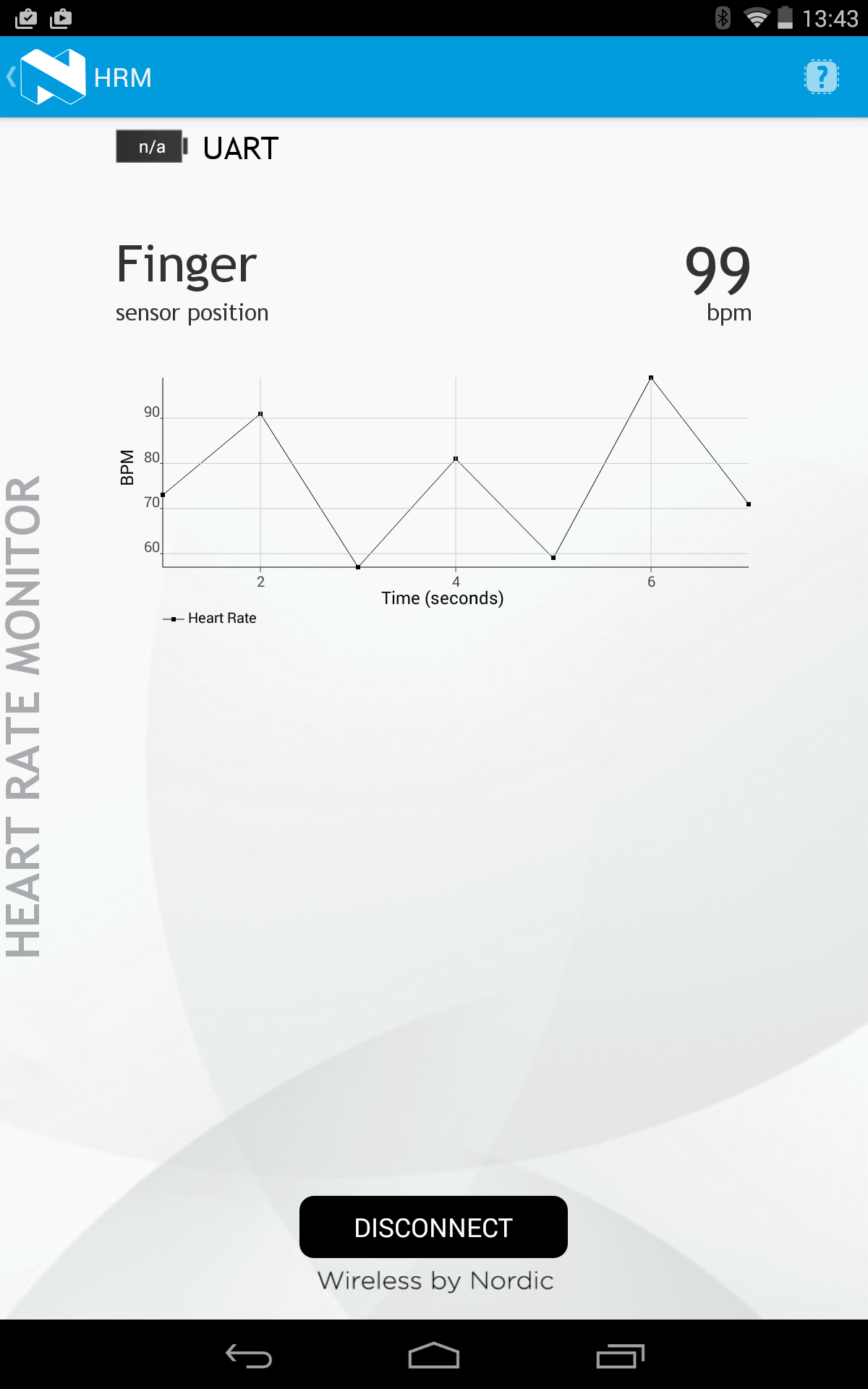
可以看到，sniffer蓝灯的部分是在进行嗅探，而黄灯的地方是在向外发送数据。

程序的运行时如下：



程序运行截图

同时，在手机端我们使用一款名叫nRF Toolbox的软件，可以看到我们自己修改的值被发送出来：



这就是在发端我们做的工作，到这里，一个完整的中间人攻击就结束了。

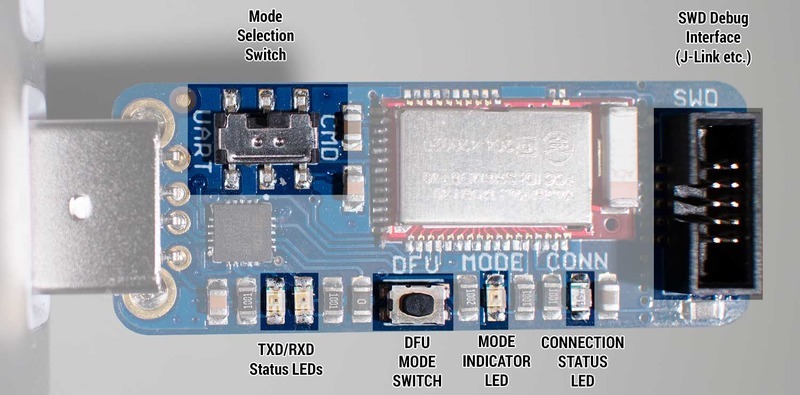
新：

接下来我们在Linux上做一下这些动作，下面的操作使用了LE friend ，因为按照官方的教程，直接使用LE friend也是可以的，所以我想试一试。

1. LE friend介绍

这是LE friend的硬件示意图，从上面我们可以清楚的看到各个指示灯的含义

后面的那个口（即SWD Debug）我们不需要用，本身硬件也没有，所以不用管，DFU是用于烧写LE friend固件的，也不用管。



Mode Selection Switch

可以在“ CMD”（命令模式）和“ UART”（数据模式）之间切换此开关，这将改变设备在终端仿真器中的行为方式。

TXD/RXD Status LEDs

提供这两个LED主要用于调试目的，以帮助您可视化USB CDC接口上的传入和传出字符。Mode Indicator LED

该指示灯用于指示设备当前正在运行的模式（数据，命令或DFU）。

Connection Status LED

当BLEFriend已成功与另一个BLE设备建立连接时，此LED将启用，并且对于调试目的很有用。

1. 操作模式

数据模式

数据模式使用BLE UART服务，并将BLEFriend变成BLE中央设备（您的手机或平板电脑）与您的PC或支持USB的设备之间的HW UART桥接器。 要使用数据模式，只需将BLEFriend模块连接到PC的USB端口，将模式选择开关设置为UART，然后使用您喜欢的终端软件以9600 bps的速度开始发送或接收数据。

如果MODE LED闪烁两次，然后延迟三秒钟，则您处于数据模式：

（视频演示了如何亮灯）

命令模式用于将配置命令发送到模块或检索有关模块本身或BLE连接另一端连接的设备的信息。 要使用命令模式，请确保将模式选择开关设置为CMD，然后使用您喜欢的终端仿真器以9600 bps的速度输入有效的Hayes AT样式命令（例如，使用``ATI''显示有关该模块的一些基本信息）。 如果MODE LED闪烁三下，然后延迟三秒钟，则您处于命令模式：



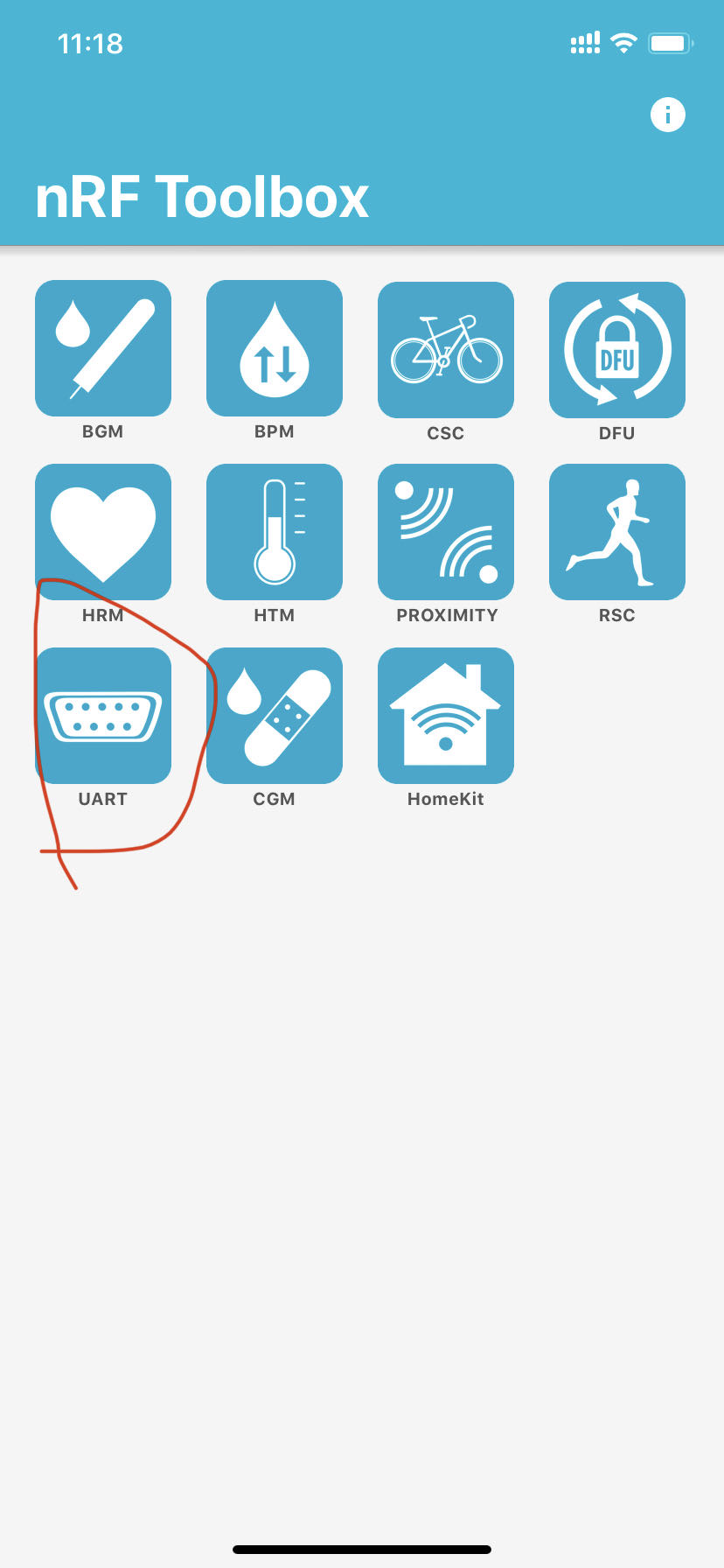
1. 测试操作（这一步只是进行测试，和我们最后做的没关系，所以这些工具可以只是作为了解或是写在论文中，不必强求能够运行）

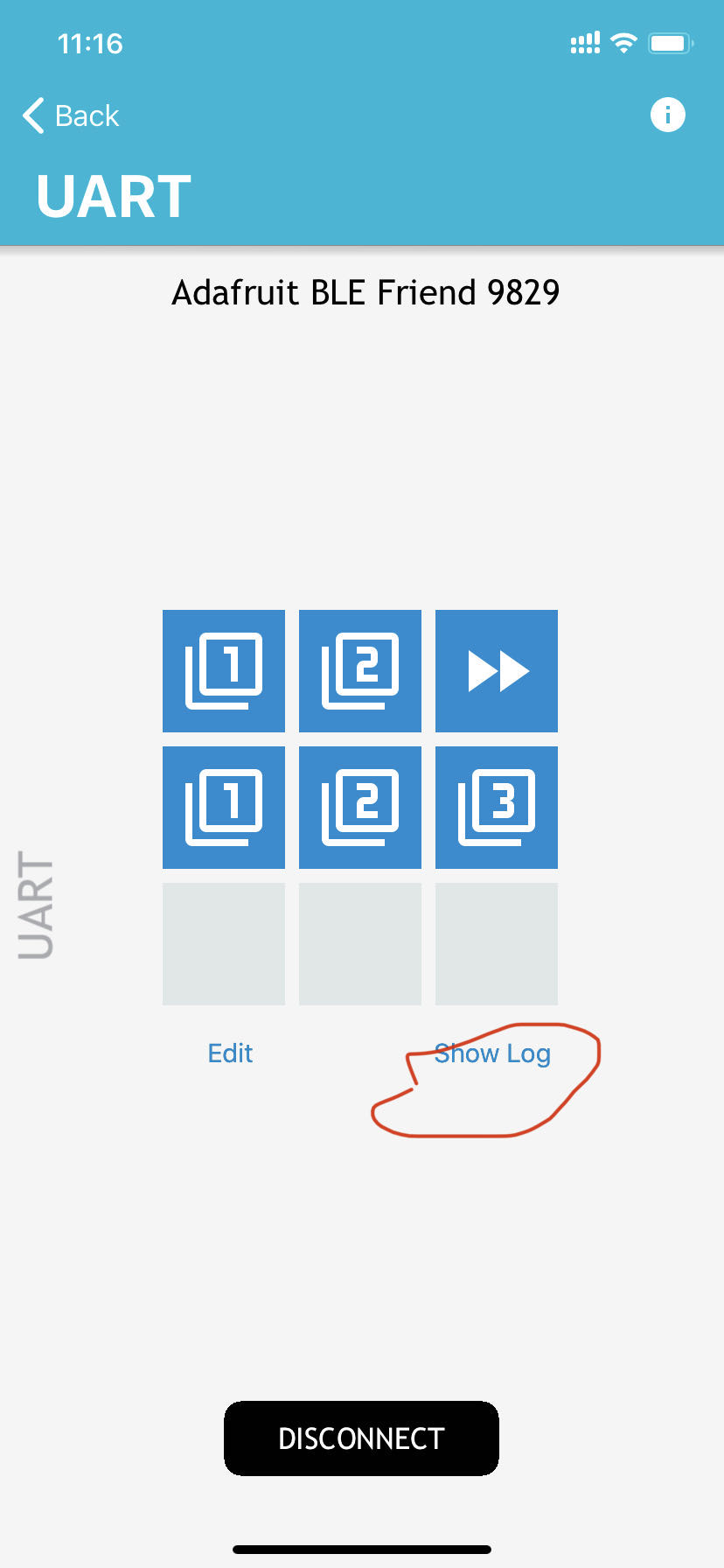
首先需要在电脑端安装CoolTerm，这是一个免费且功能齐全的终端仿真器软件包。<http://freeware.the-meiers.org/>

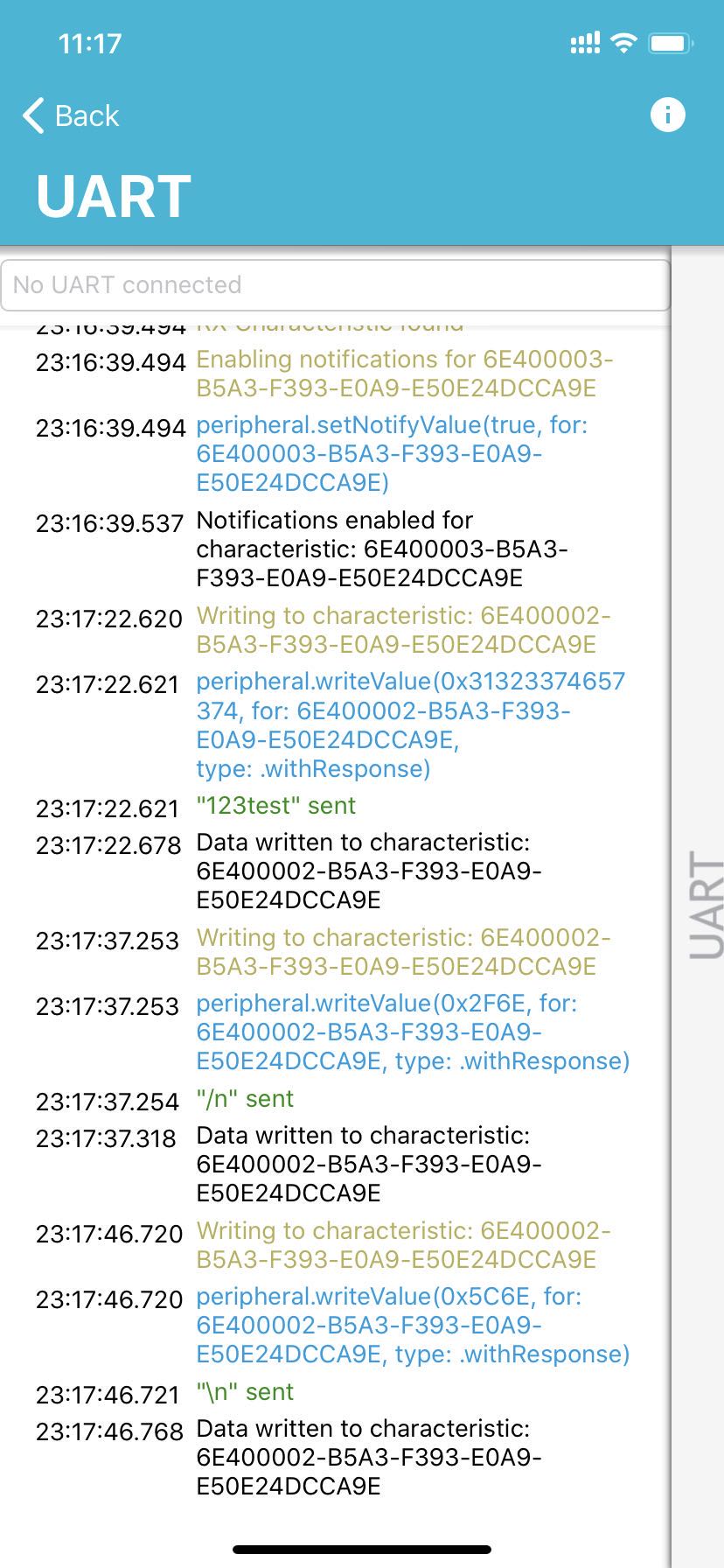
这里可以进行下载

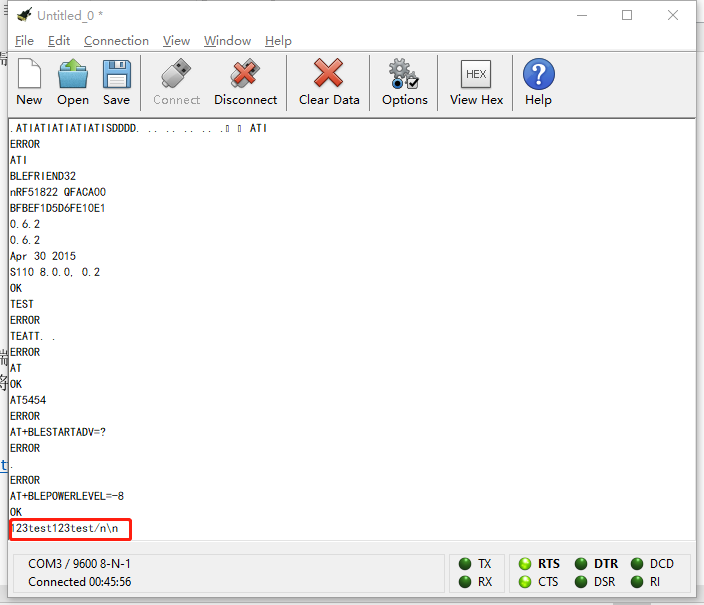
手机端需要安装

然后将LE friend设置为数据模式，手机端发送的数据就能在电脑端看到了：









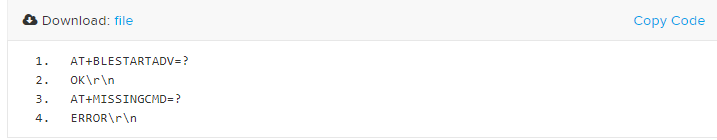
将LE friend调至cmd模式，输入命令可以看到上面的一些消息打印出来

**Hayes/AT Commands简介**

AT样式命令集的优点是它易于在机器间通信中使用，同时仍然对用户友好。

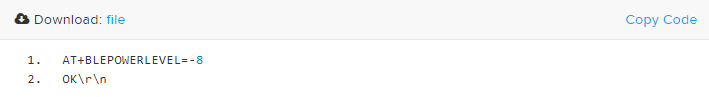
Test Command Mode '=?'

“测试”模式用于检查系统上是否存在指定的命令。 某些固件版本或配置可能包含也可能不包含特定命令，您可以通过使用命令名称并附加'=？'来确定该命令是否存在。如下图所示：



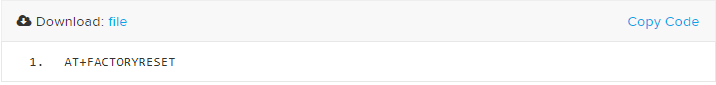
Write Command Mode '=xxx'

“写入”模式用于为命令分配特定的值，例如使用我们上面使用的命令来更改无线电的发射功率电平。 要向命令中写入值，只需在命令后附加一个'='符号，然后加上您要写入的任何参数（除了一个单独的'？'字符，它将被解释为tet模式）：



Execute Mode

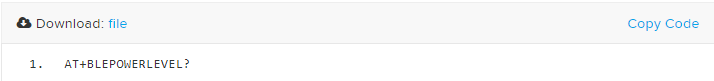
“执行”模式将运行合法的特定命令，并且在输入命令名称而没有其他参数时将使用该模式。



您可以使用执行模式来执行出厂重置，就像上面那样通过执行AT + FACTORYRESET命令来实现。

Read Command Mode '?'

“读取”模式用于读取命令的当前值。 并非每个命令都支持读取模式，但是通常您可以通过添加'？'来使用它来检索信息，例如无线电的当前发射功率水平。如下所示：



1. 模拟蓝牙

通过上面的测试我们能够知道，将LE FRIEND设置为cmd模式，我们就可以通过输入命令的方式模拟一个蓝牙设备。

这些代码是通过AT+命令的形式来将LE friend模拟为一个心率设备的，下面是代码的详细信息：

# Perform a factory reset to make sure we get a clean start

AT+FACTORYRESET

OK

# Add the Heart Rate service entry

AT+GATTADDSERVICE=UUID=0x180D

1

OK

# Add the Heart Rate Measurement characteristic

AT+GATTADDCHAR=UUID=0x2A37, PROPERTIES=0x10, MIN\_LEN=2, MAX\_LEN=3, VALUE=00-40

1

OK

# Add the Body Sensor Location characteristic

AT+GATTADDCHAR=UUID=0x2A38, PROPERTIES=0x02, MIN\_LEN=1, VALUE=3

2

OK

# Create a custom advertising packet that includes the Heart Rate service UUID

AT+GAPSETADVDATA=02-01-06-05-02-0d-18-0a-18

OK

# Reset the device to start advertising with the custom payload

ATZ

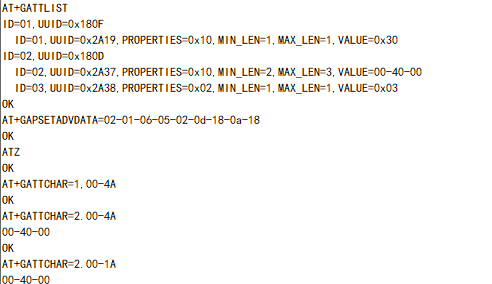
OK

# Update the value of the heart rate measurement (set it to 0x004A)

AT+GATTCHAR=1,00-4A

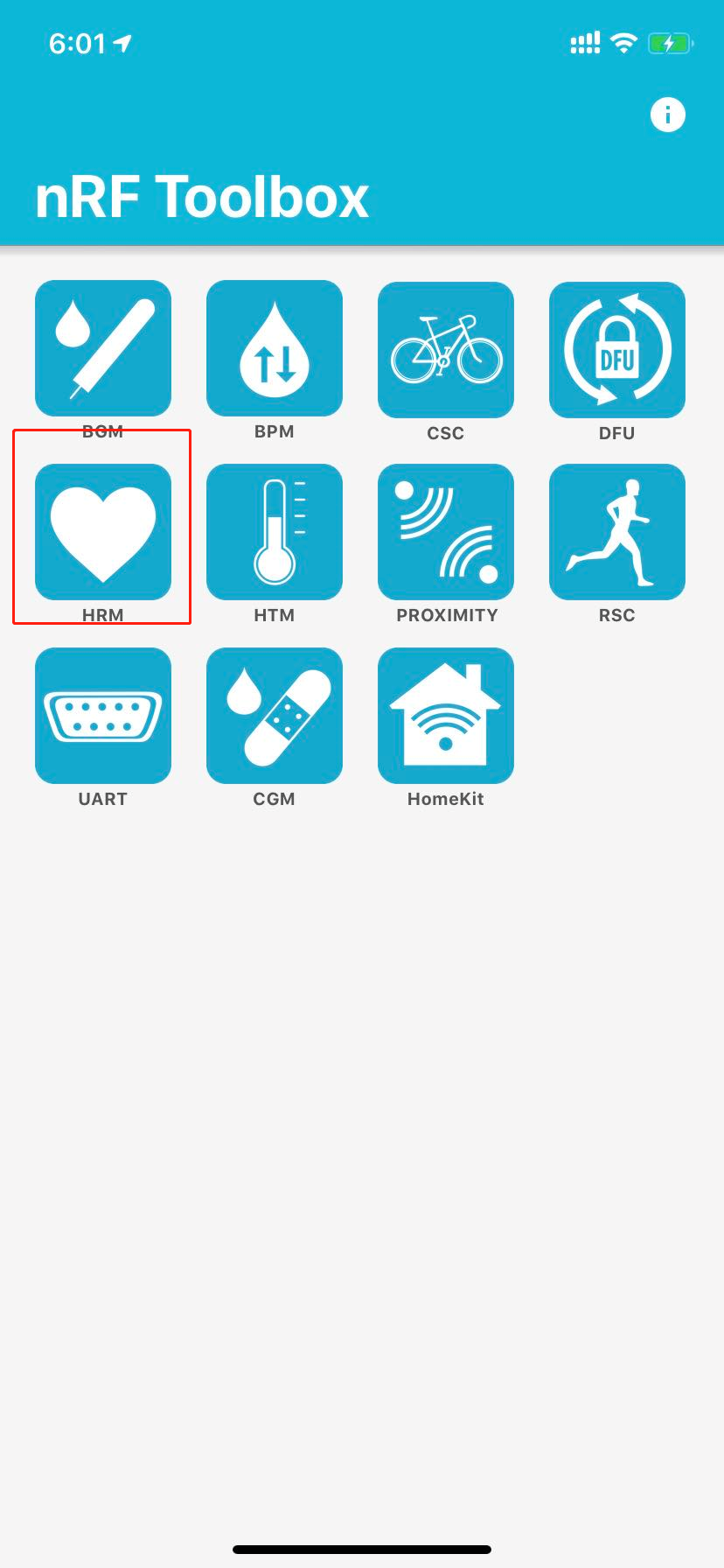
OK

这是我在CoolTerm上输入的部分指令：

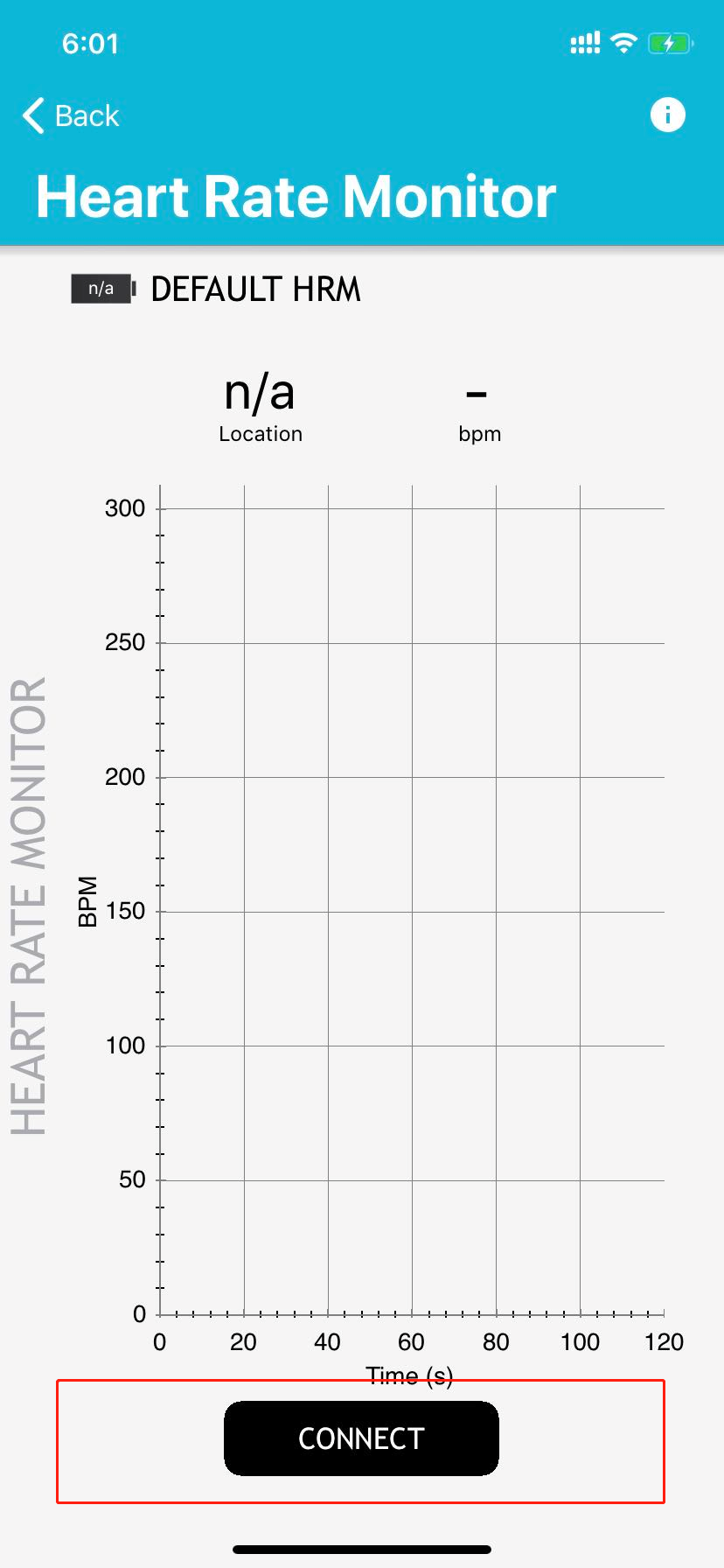


这是运行的效果图：

首先打开软件，进入心率测量的选项：



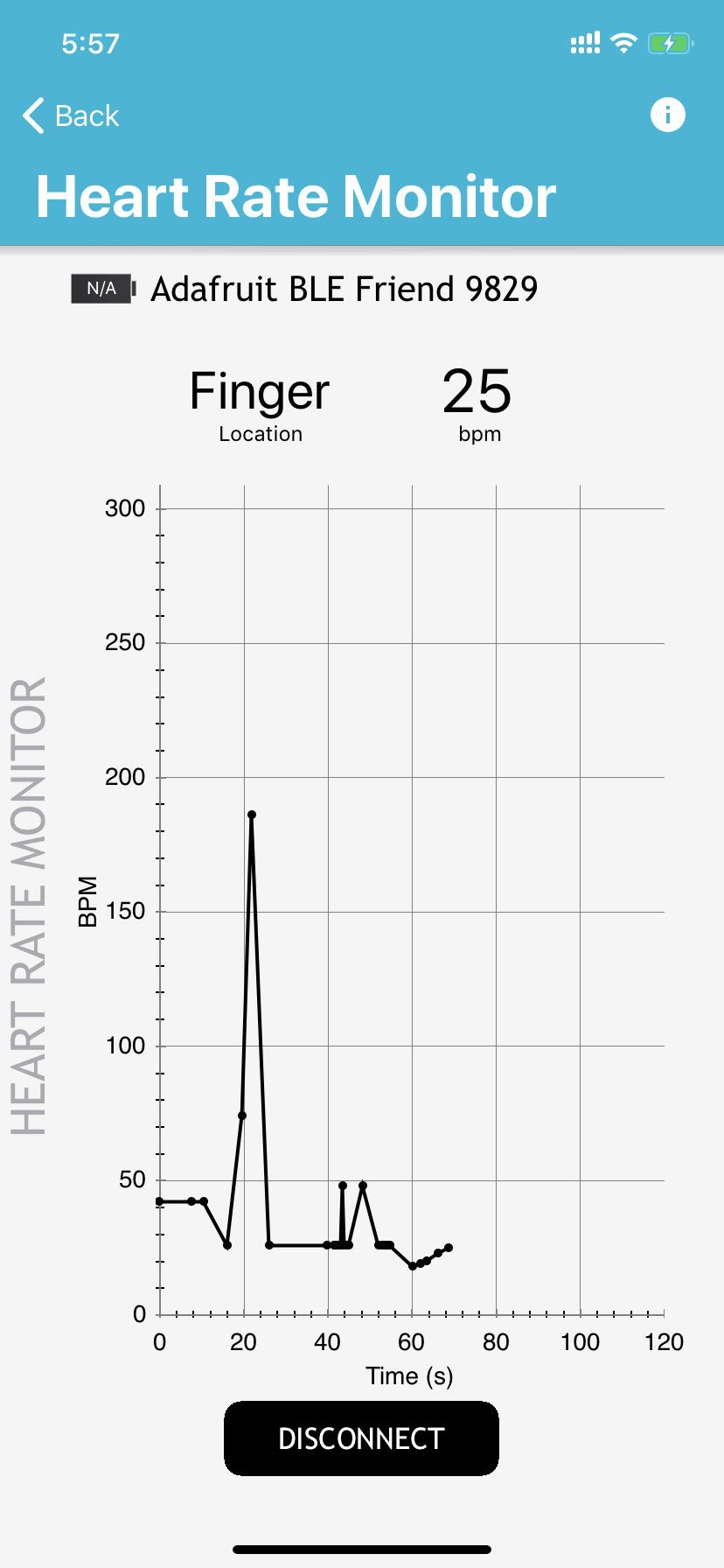
点进去后点connect：



找到你的LE friend，连接上：（这个名字也是可以改的）



输入上面的命令之后就可以看到效果了：



使用linux系统

我们在这里想要使用bluez平台，接下来我们将纤细介绍这个工具，它包含了许多实用的蓝牙工具并且便于使用。不幸的是，没有跨Windows，Mac，Linux等平台的跨平台蓝牙协议栈或API。因此，如果想使用其他平台，则需要查看该平台的蓝牙低能耗协议栈和API。

Bluez

BlueZ是Linux官方蓝牙协议栈。它是一个基于GNU General Public License (GPL)发布的开源项目，从Linux2.4.6开始便成为Linux 内核的一部分。其基础代码均是由就职于Qualcomm(高通)的Maxim Krasnyansky完成的。包括：HCI，L2CAP，RFCOMM和基本socket的实现。Marcel Holtmann开发层的协议和应用，包括：BNEP, CMTP等。当然，这些中也有Maxim Krasnyansky的参预。有部分代码由Nokia提供的。

1. BlueZ支持蓝牙核心层和协议，它灵活、高效，以模块化方式实现，具有以下特点：

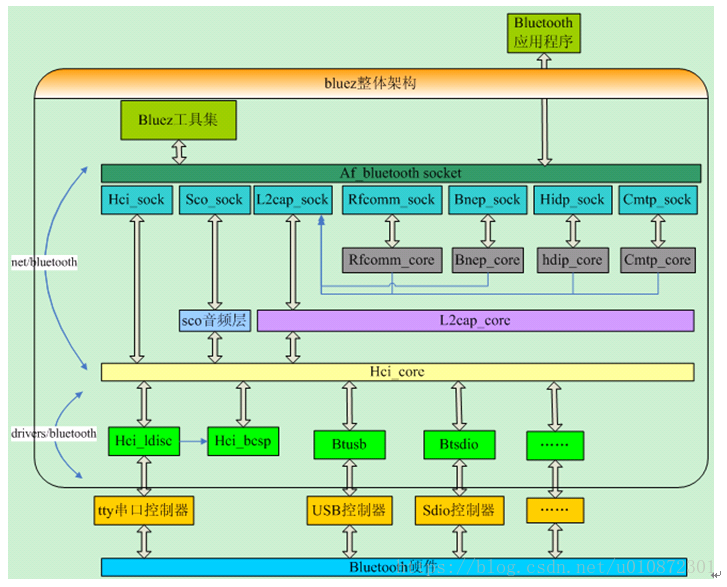
* 完整的模块化实现
* 均衡的多处理安全
* 支持多线程数据处理
* 支持多个蓝牙设备
* 硬件抽象
* 提供所有层的标准socket接口
* 支持设备级和服务级安全保证

1. BlueＺ包含多个相互独立的模块：

* Linux内核蓝牙子系统核心
* L2CAP 和 SCO 音频内核层
* RFCOMM, BNEP, CMTP 和 HIDP内核实现
* HCI UART, USB, PCMCIA 和虚拟设备驱动
* 通用的蓝牙和SDP库及守护进程
* 配置和测试小工具
* 协议解析和分析工具

我们主要使用了上面标红的这些模块

下图是bluez的一个架构示意图：



Bluez的安装

在ubuntu14.04 下编译安装Bluez-5.52

1、安装相关依赖库：

sudo apt-get install libusb-dev libdbus-1-dev libglib2.0-dev automake libudev-dev libical-dev libreadline-dev

2、下载Bluez-5.28压缩包并解压:

wget http://www.kernel.org/pub/linux/bluetooth/bluez-5.52.tar.xz

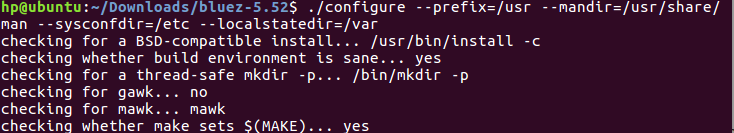
tar xvf bluez-5.52.tar.xz

进入解压后的目录：

cd bluez-5.52

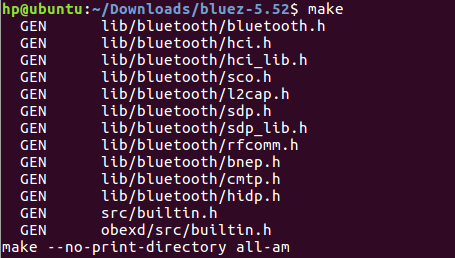
3、执行配置文件

./configure --prefix=/usr --mandir=/usr/share/man --sysconfdir=/etc --localstatedir=/var

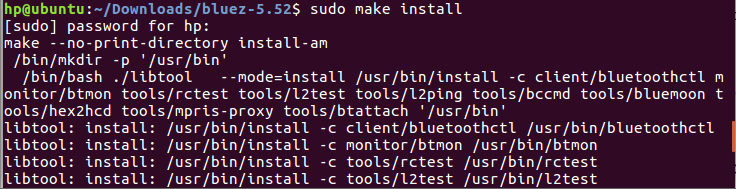


4、执行make和install

make



sudo make install



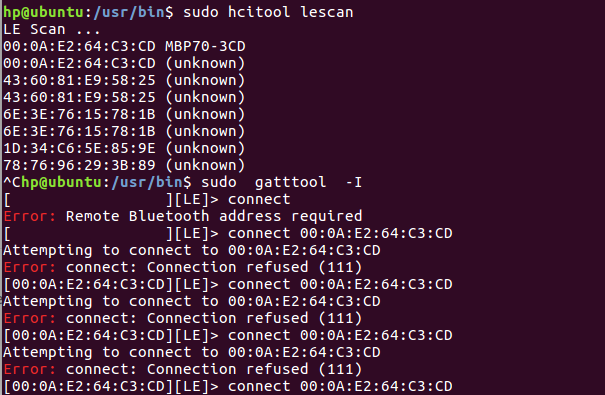
没有提示任何错误的话，安装完毕。

Bluez的使用

1. lescan扫描低功耗蓝牙设备

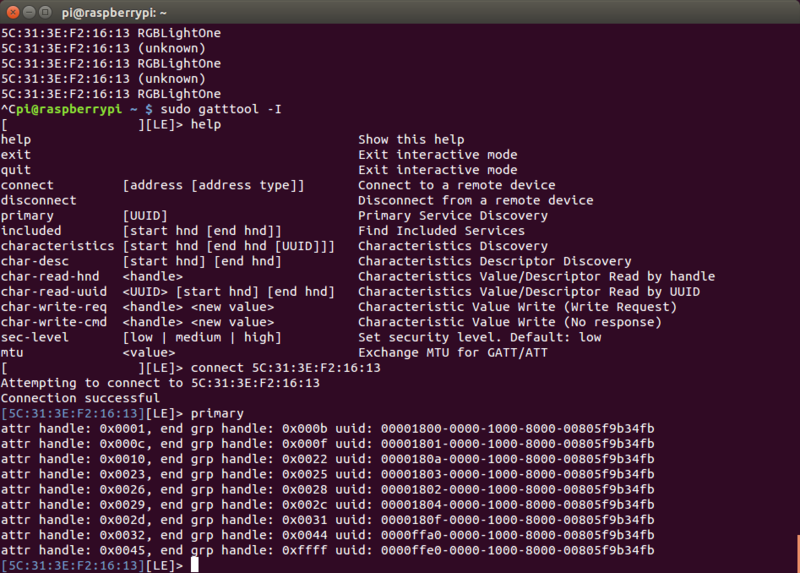


1. connect   //连接低功耗设备



1. primary

在连接成功后输入这个命令，可以看到该低功耗蓝牙设备能够支持的服务，和uuid



1. char-desc 0x0028 0x0028

可以运行的另一个命令是char-desc命令，以获取有关特定特征的详细信息。我运行以下命令来查询0x0028特性：

