

Пишем приложение для вибратора с Алиэкспресс, или Как реверс-инжинирить Bluetooth

Гончаров Даниил (Finch Technologies Ltd.)



UFADEVCONF

Для чего нам Bluetooth?



Finch Technologies & Co.



План

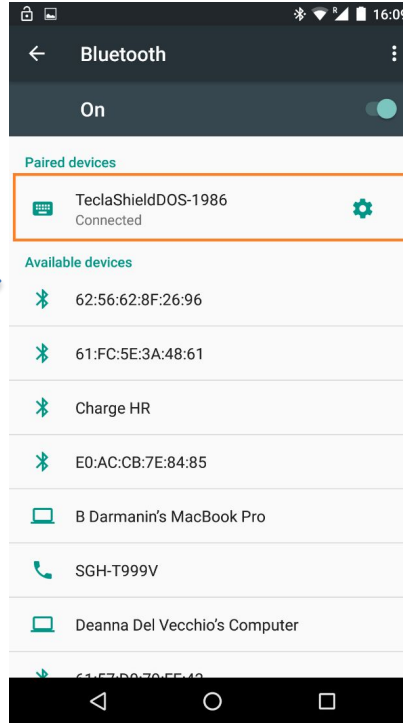
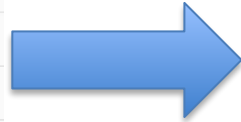
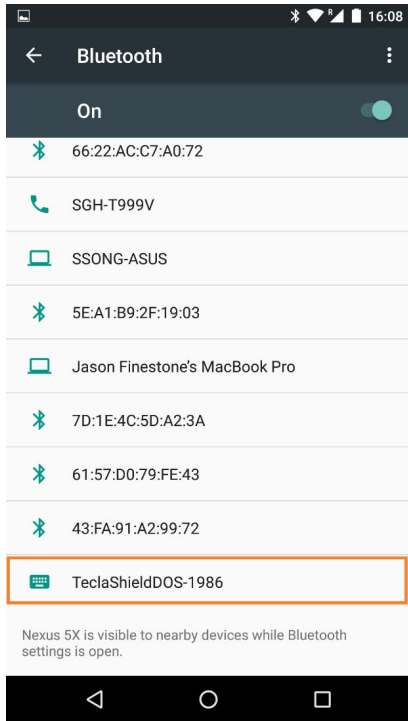
- Основы Bluetooth
- Способы реверс-инжиниринга Bluetooth
- Реверс-инжиниринг вибратора с Алиэкспресс



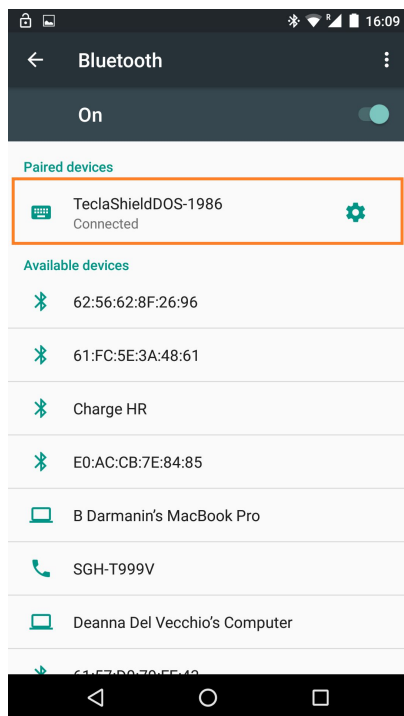
Bluetooth-Device



BLE Connect



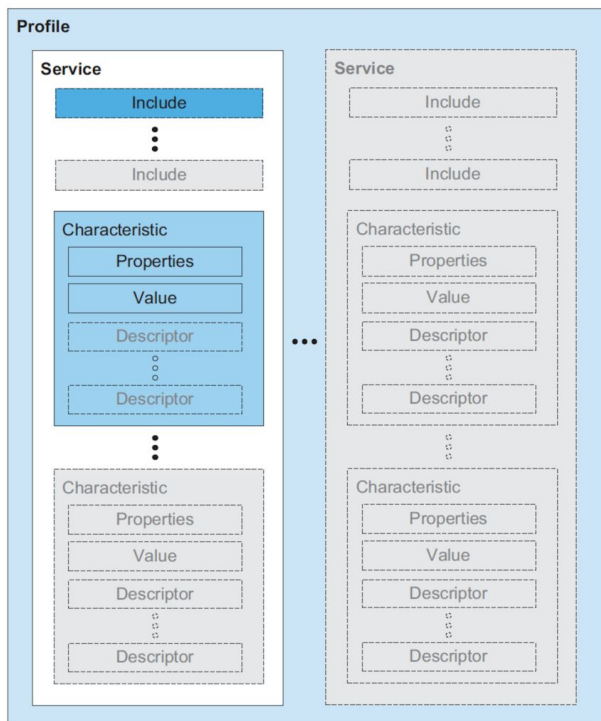
BLE Security



- Pairing – процесс создания парами BLE-устройств секретных ключей для последующего шифрования трафика



BluetoothDevice & BluetoothGatt



- GATT – профиль Bluetooth, определяющий способ взаимодействия двух устройств и использующий концепцию атрибутов
- GATT Characteristic – контейнер для данных
- GATT Service – совокупность характеристик
- UUID – 128-битный уникальный идентификатор атрибута

GATT Characteristic

The screenshot displays a mobile application interface for managing Bluetooth devices. At the top, there is a blue header with a menu icon, the word "Devices", and a "DISCONNECT" button. Below the header, there are tabs for "BONDED", "ADVERTISER", and "BLE BATTERY" (selected). Underneath, there are sub-tabs for "CONNECTED", "BONDED", "CLIENT" (selected), and "SERVER".

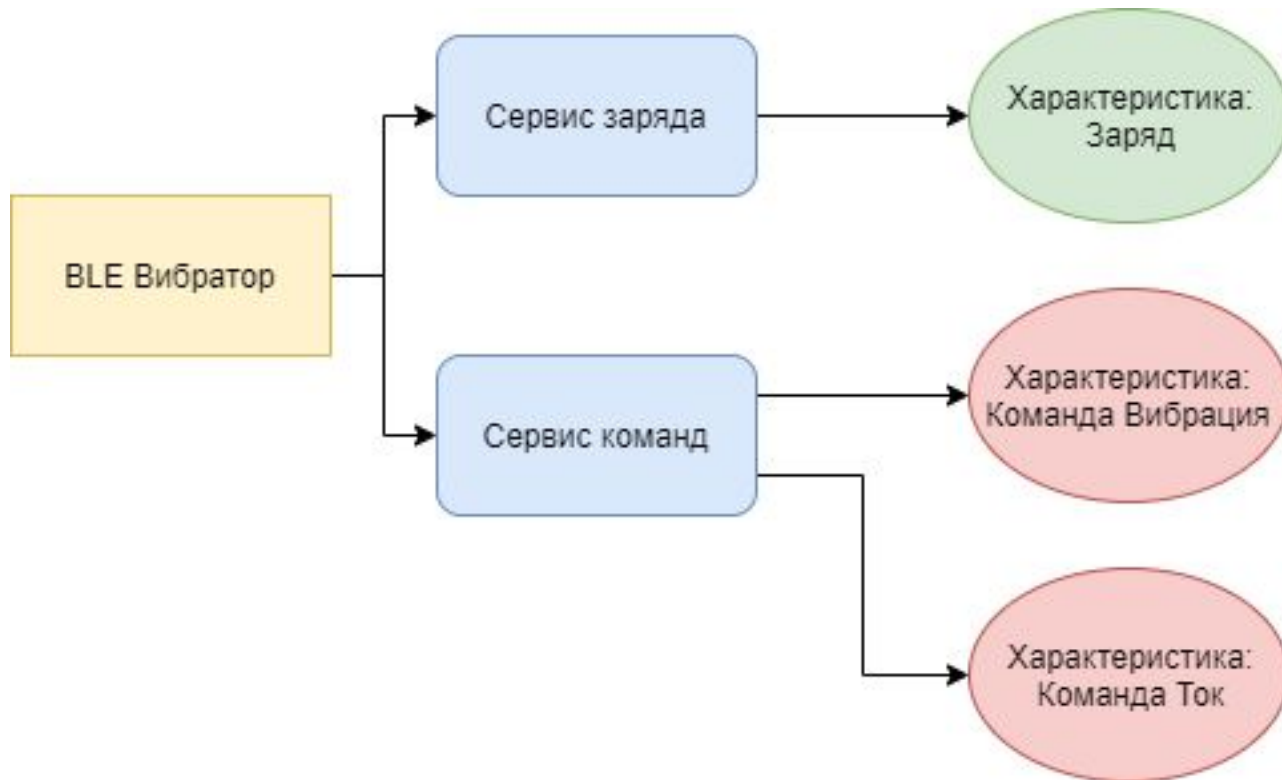
The main content area lists several GATT characteristics:

- Generic Attribute**: UUID: 0x1801, PRIMARY SERVICE
- Generic Access**: UUID: 0x1800, PRIMARY SERVICE
- Battery Service**: UUID: 0x180F, PRIMARY SERVICE
 - Battery Level**: UUID: 0x2A19, Properties: NOTIFY, READ, Value: 67% (circled in red)
 - Descriptors**:
 - Characteristic User Description**: UUID: 0x2901, Value: Percentage 0 - 100 (circled in red)
 - Client Characteristic Configuration**: UUID: 0x2902, Value: Notifications enabled

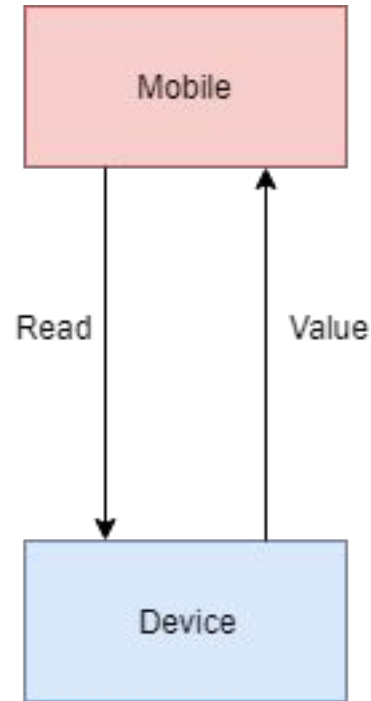
At the bottom right, there is a red circular button with a white menu icon.



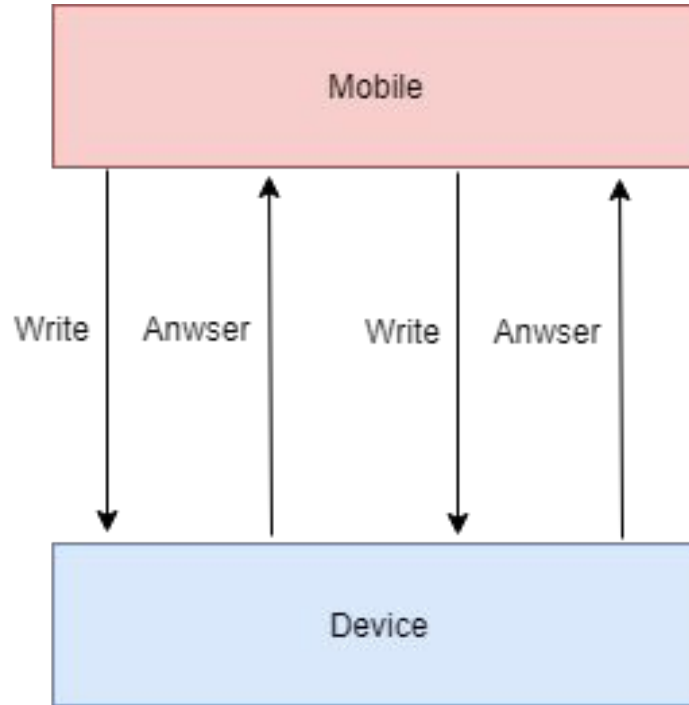
BluetoothGatt



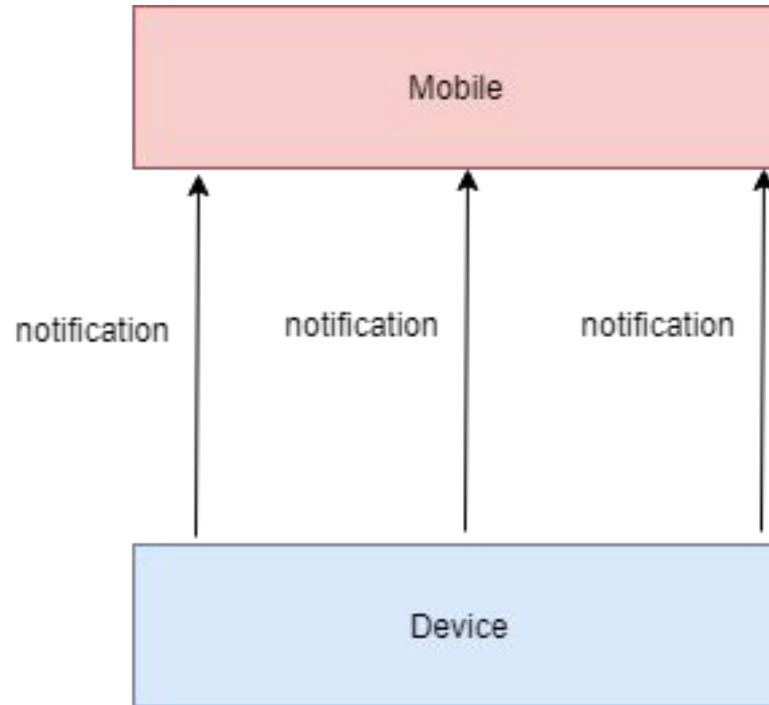
BluetoothGatt read



BluetoothGatt write



BluetoothGatt notification



Пример



1. Подключение

2. Поиск всех сервисов устройства

3. Список сервисов

4. Отправка команды

5. Результат отправки



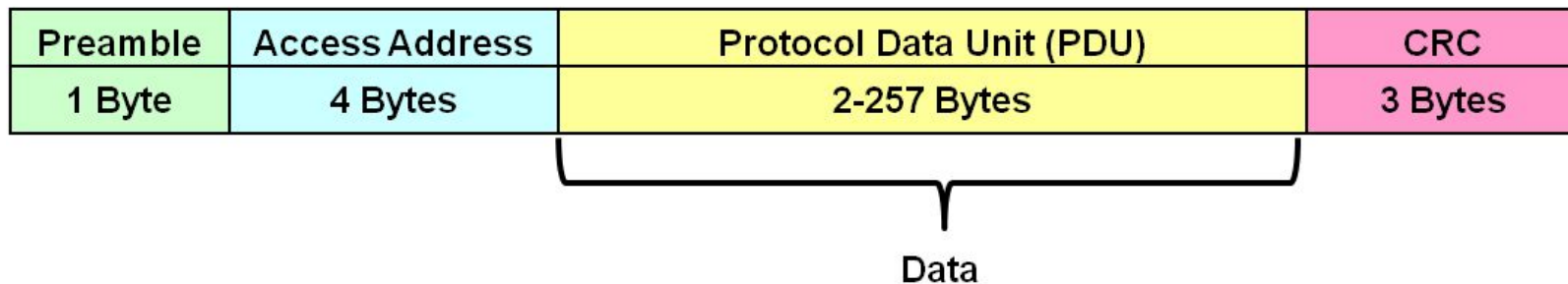
О VLE подробнее

- <http://appsconf.ru/moscow/2019/abstracts/5051>
- https://youtu.be/hpHFo_Lyk0M



BLE пакет

BLE Packet

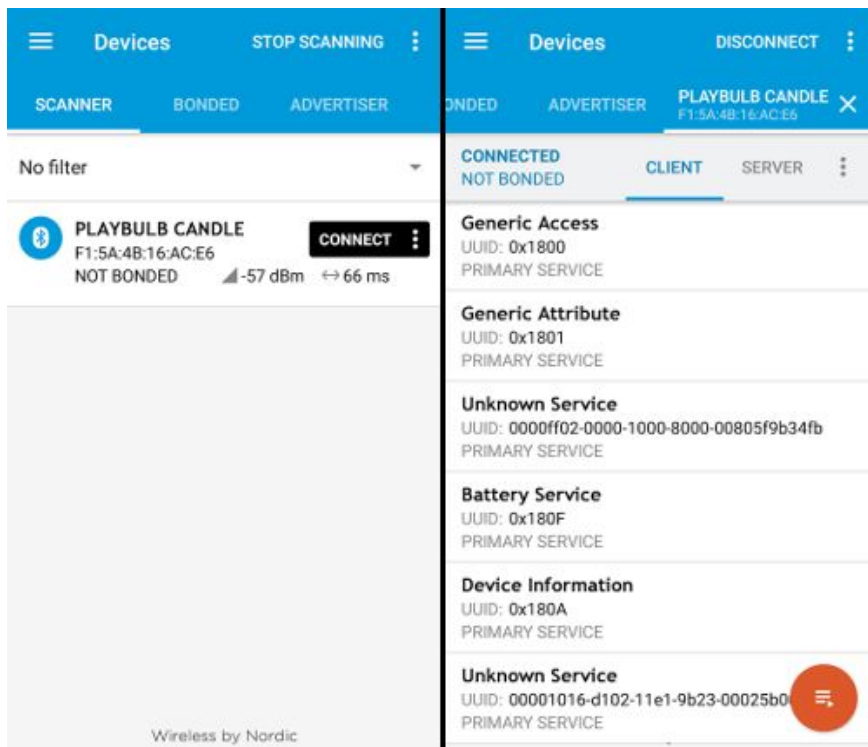


Реверс-инжиниринг VLE-пакета

- Анализ VLE-профиля
- Реверс-инжиниринг приложения
- Анализ трафика



nRF Connect



- Сканирование
- Подключение
- Сервисы
- Характеристики
и
- Чтение и
запись



nRF Connect

Android

- <https://play.google.com/store/apps/details?id=no.nordicsemi.android.mcp>

iOS

- <https://apps.apple.com/ru/app/nrf-connect/id1054362403>



Wireshark

File Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

Применить дисплейный фильтр ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1208	751.604354	host	controller	HCI_CMD	29	Sent LE Create Connection
1209	751.666490	controller	host	HCI_EVT	7	Rcvd Command Status (LE Create Connection)
1210	758.596802	host	controller	HCI_CMD	4	Sent Vendor Command 0x0159 (opcode 0xFD59)
1211	758.599893	controller	host	HCI_EVT	23	Rcvd Command Complete (Vendor Command 0x0159 [opcode 0xFD59])
1212	760.186384	host	controller	HCI_CMD	4	Sent Vendor Command 0x0159 (opcode 0xFD59)
1213	760.189279	controller	host	HCI_EVT	23	Rcvd Command Complete (Vendor Command 0x0159 [opcode 0xFD59])
1214	762.320214	host	controller	HCI_CMD	4	Sent Vendor Command 0x0159 (opcode 0xFD59)
1215	762.325785	controller	host	HCI_EVT	23	Rcvd Command Complete (Vendor Command 0x0159 [opcode 0xFD59])
1216	768.155697	host	controller	HCI_CMD	4	Sent Vendor Command 0x0159 (opcode 0xFD59)
1217	768.160556	controller	host	HCI_EVT	23	Rcvd Command Complete (Vendor Command 0x0159 [opcode 0xFD59])
1218	769.939565	host	controller	HCI_CMD	4	Sent Vendor Command 0x0159 (opcode 0xFD59)
1219	769.942944	controller	host	HCI_EVT	23	Rcvd Command Complete (Vendor Command 0x0159 [opcode 0xFD59])
1220	770.792011	host	controller	HCI_CMD	4	Sent LE Create Connection Cancel
1221	770.797149	controller	host	HCI_EVT	7	Rcvd Command Complete (LE Create Connection Cancel)
1222	770.797294	controller	host	HCI_EVT	34	Rcvd LE Meta (LE Enhanced Connection Complete)
1223	798.010920	host	controller	HCI_CMD	29	Sent LE Create Connection
1224	798.017967	controller	host	HCI_EVT	7	Rcvd Command Status (LE Create Connection)
→ 1225	804.176169	host	controller	HCI_CMD	4	Sent Vendor Command 0x0159 (opcode 0xFD59)
← 1226	804.181059	controller	host	HCI_EVT	23	Rcvd Command Complete (Vendor Command 0x0159 [opcode 0xFD59])
1227	818.029783	host	controller	HCI_CMD	4	Sent LE Create Connection Cancel
1228	818.035288	controller	host	HCI_EVT	7	Rcvd Command Complete (LE Create Connection Cancel)
1229	818.035517	controller	host	HCI_EVT	34	Rcvd LE Meta (LE Enhanced Connection Complete)
1230	821.725866	host	controller	HCI_CMD	4	Sent Vendor Command 0x0159 (opcode 0xFD59)
1231	821.732253	controller	host	HCI_EVT	23	Rcvd Command Complete (Vendor Command 0x0159 [opcode 0xFD59])

> Frame 1225: 4 bytes on wire (32 bits), 4 bytes captured (32 bits)
> Bluetooth
> Bluetooth HCI H4
> Bluetooth HCI Command - Vendor Command 0xfd59

0000 01 59 fd 00

- Просмотр VLE-логов
 - Адреса
 - Запись/Чтение
 - Сервисы
 - Характеристики



Wireshark

- Windows & macOS
- <https://www.wireshark.org/download.html>



Анализ VLE-профиля

- Список всех сервисов и характеристик
- Свойства характеристик
- Чтение/Запись сырых пакетов



Подключение

The screenshot shows a Bluetooth scanner interface with a blue header bar containing an information icon, the text "Scanner", and a "STOP SCANNING" button. Below the header, three devices are listed:

- N/A**: Address not available, Connectable, -91 dBm. A black "CONNECT" button is visible.
- nRF52832 LED**: Address not available, Connectable, -65 dBm. A black "CONNECT" button is visible and highlighted with a red rectangular border.
- [TV] UN50JU6401**: Address not available, Non-connectable, -97 dBm.



Список сервисов

CONNECTED	CLIENT	SERVER	⋮
BONDED			
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			
Immediate Alert UUID: 0x1802 PRIMARY SERVICE			
Heart Rate UUID: 0x180D PRIMARY SERVICE			



Список характеристик

BONDED ADVERTISER 360FLY4K_D15A E4:BA:D9:10:D1:5B

CONNECTED CLIENT SERVER

Battery Service
UUID: 0x180F
PRIMARY SERVICE

Device Information
UUID: 0x180A
PRIMARY SERVICE

System ID
UUID: 0x2A23
Properties: READ
Value: (0x) 5A-D1-10-FE-FF-D9-BA-E4

Model Number String
UUID: 0x2A24
Properties: READ
Value: 360FLY4K

Serial Number String
UUID: 0x2A25
Properties: READ
Value: 1609165288A0001291

BONDED ADVERTISER 360FLY4K_D15A E4:BA:D9:10:D1:5B

CONNECTED CLIENT SERVER

Unknown Service
UUID: 0000fec3
PRIMARY SERVICE 0000-1000-8000-00805f9b34fb
16 bit Member: 360fly, Inc.

Unknown Characteristic
UUID: 36d25033-5cbc-5ee5-b688-b90fda0300d6
Properties: NOTIFY, READ, WRITE
Value: (0x) 128 custom UUID
33-36-30-46-4C-59-34-4B-5F-44-31-35-41, "360FLY4K_D15A"

Unknown Characteristic
UUID: 36d25034-5cbc-5ee5-b688-b90fda0300d6
Properties: NOTIFY, READ
Value: (0x) 03-00

Unknown Characteristic
UUID: 36d25035-5cbc-5ee5-b688-b90fda0300d6
Properties: NOTIFY, READ
Value: (0x) 02-03-00-00-00-00-00

Services

Characteristics

16 bit by Bluetooth SIG



Свойства характеристик

BONDED ADVERTISER RPI3
79:E4:FC:F2:C3:4C

CONNECTED
NOT BONDED CLIENT SERVER

Generic Attribute
UUID: 0x1801
PRIMARY SERVICE

Generic Access
UUID: 0x1800
PRIMARY SERVICE

Unknown Service
UUID: 795090c7-420d-4048-a24e-18e60180e23c
PRIMARY SERVICE

Unknown Characteristic
UUID: 31517c58-66bf-470c-b662-e352a6c80cba
Properties: NOTIFY, READ

Descriptors:
Client Characteristic Configuration
UUID: 0x2902

Unknown Characteristic
UUID: 0b89d2d4-0ea6-4141-86bb-0c5fb91ab14
Properties: WRITE



Запись данных

The image consists of three screenshots from a mobile application interface for managing Bluetooth devices. The first screenshot shows a list of characteristics for a device named 'PLAYBULB CANDLE'. The 'Unknown Service' entry is highlighted with a red box. The second screenshot shows the same list, but the 'Unknown Characteristic' entry with UUID '0000fffc-0000-1000-8000-00805f9b34fb' is highlighted with a red box, and its 'write' icon (an upward arrow) is also highlighted. The third screenshot shows a 'Write value' dialog box where the value '0x 00FFFF00' is entered in a text field, and the 'SEND' button is highlighted with a red box. A keyboard is visible at the bottom of the third screenshot.

Devices DISCONNECT

CONNECTED NOT BONDED

ADVERTISER PLAYBULB CANDLE
F1:5A:4B:16:AC:E6

CLIENT SERVER

Generic Access
UUID: 0x1800
PRIMARY SERVICE

Generic Attribute
UUID: 0x1801
PRIMARY SERVICE

Unknown Service
UUID: 0000ff02-0000-1000-8000-00805f9b34fb
PRIMARY SERVICE

Heart Rate Measurement
UUID: 0x2A37
Properties: NOTIFY
Descriptors:
Client Characteristic Configuration
UUID: 0x2902

Unknown Characteristic
UUID: 0000fff8-0000-1000-8000-00805f9b34fb
Properties: READ

Unknown Characteristic
UUID: 0000fffc-0000-1000-8000-00805f9b34fb
Properties: READ, WRITE NO RESPONSE

Unknown Characteristic
UUID: 0000fffd-0000-1000-8000-00805f9b34fb
Properties: READ, WRITE

Unknown Characteristic
UUID: 0000fffe-0000-1000-8000-00805f9b34fb
Properties: READ, WRITE

Unknown Characteristic
UUID: 0000ffff-0000-1000-8000-00805f9b34fb
Properties: READ, WRITE

Write value NEW LOAD

0x 00FFFF00 BYTE..

ADD VALUE

Save as...

Advanced

SAVE CANCEL SEND

1 2 3 4 5 6 7 8 9 0
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
123 , SwiftKey




Чтение данных

CONNECTED
NOT BONDED


CLIENT SERVER ⋮


UUID: 0x180F
PRIMARY SERVICE

Nordic UART Service
UUID: 6e400001-b5a3-f393-e0a9-e50e24dcca9e
PRIMARY SERVICE

TX Characteristic 
UUID: 6e400003-b5a3-f393-e0a9-e50e24dcca9e
Properties: NOTIFY
Value: 00000000 [0000]

Descriptors:

Client Characteristic Configuration 
UUID: 0x2902
Value: Notifications enabled

RX Characteristic 
UUID: 6e400002-b5a3-f393-e0a9-e50e24dcca9e
Properties: WRITE, WRITE NO RESPONSE



Резюме

- Первичная информация о девайсе
- Формат данных неизвестен



Реверс-инжиниринг

приложения

- Декомпиляция бинарников
- Найти сервисы и характеристики
- Формат данных

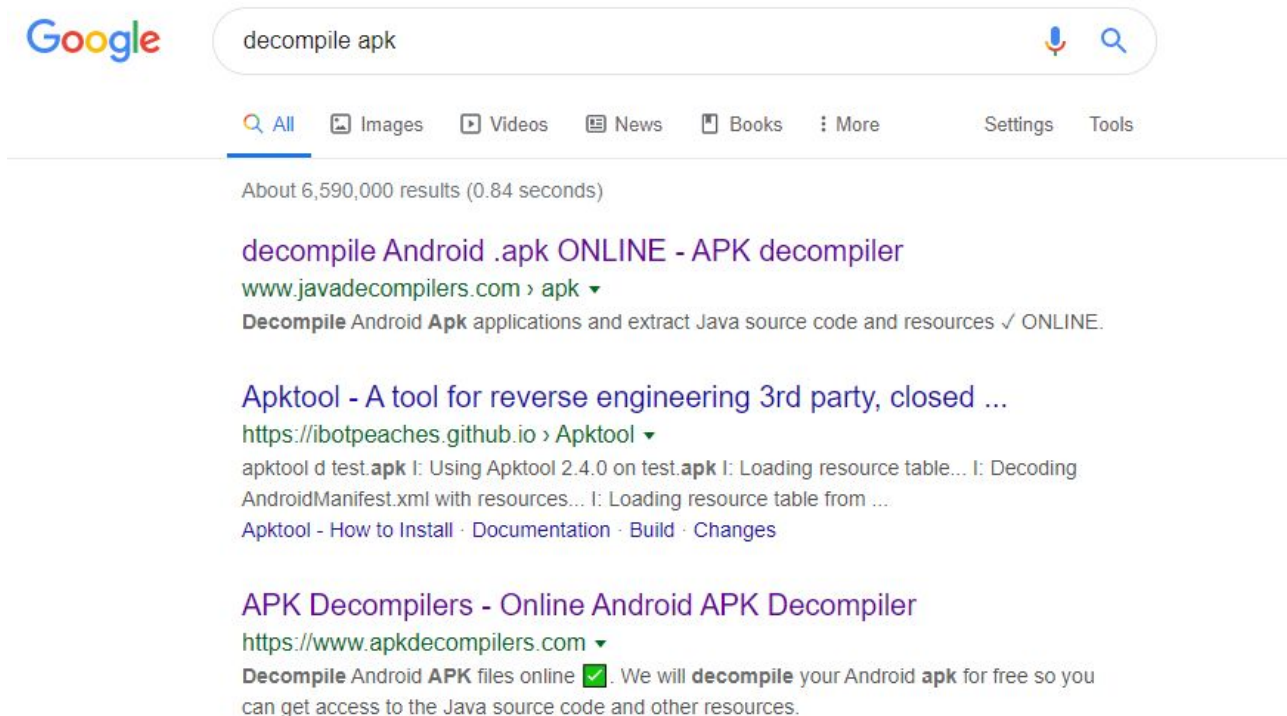


Получение apk

- `adb shell pm path package.name`
- `package:/data/app/package.name/app.apk`
- `adb pull /data/app/package.name/app.apk`



Декомпиляция бинарников



Google

decompile apk

All Images Videos News Books More Settings Tools

About 6,590,000 results (0.84 seconds)

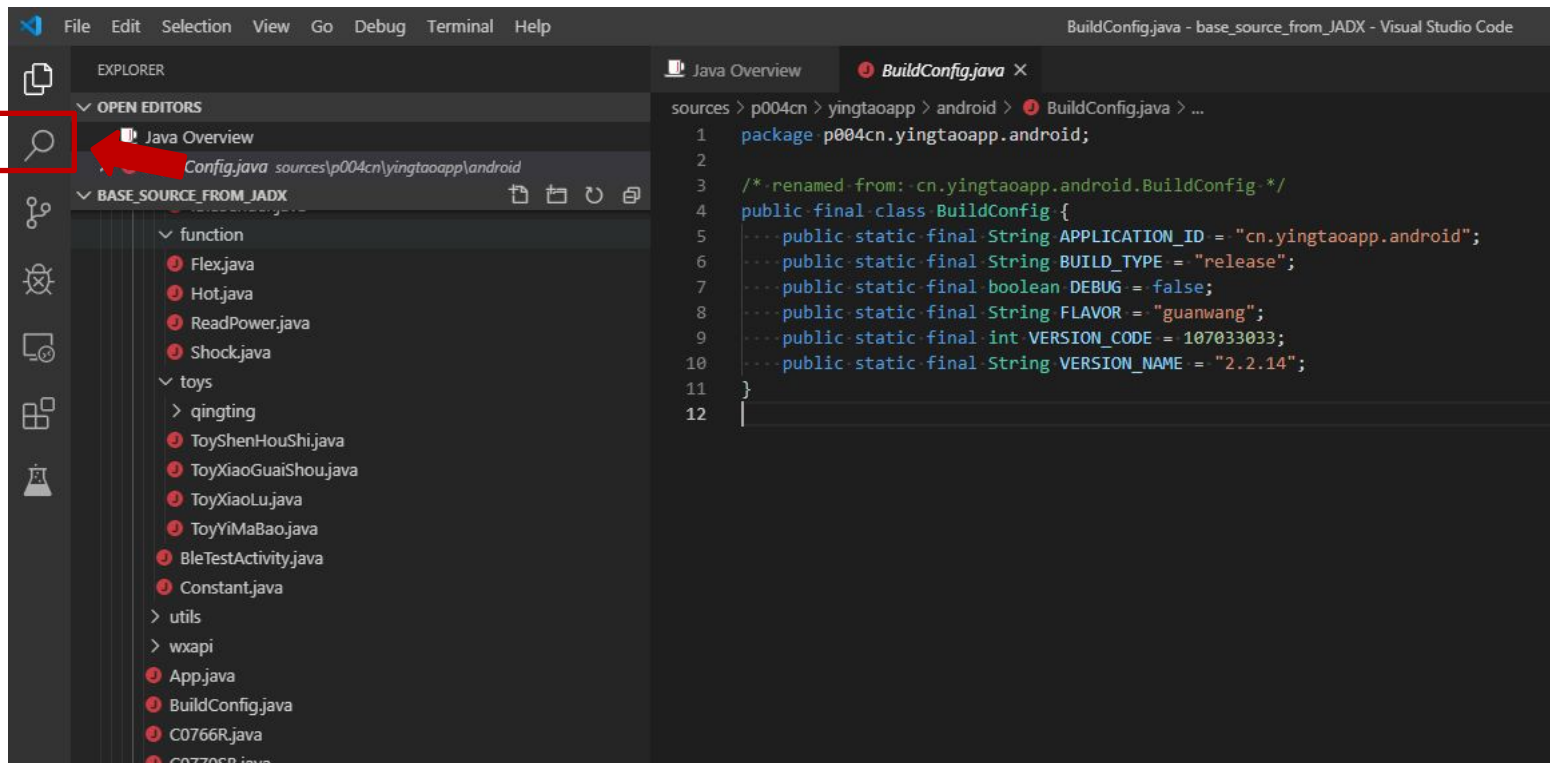
decompile Android .apk ONLINE - APK decompiler
www.javadecompilers.com › apk ▾
Decompile Android **Apk** applications and extract Java source code and resources ✓ ONLINE.

Apktool - A tool for reverse engineering 3rd party, closed ...
<https://ibotpeaches.github.io> › Apktool ▾
apktool d test.apk I: Using Apktool 2.4.0 on test.apk I: Loading resource table... I: Decoding AndroidManifest.xml with resources... I: Loading resource table from ...
Apktool - How to Install · Documentation · Build · Changes

APK Decompilers - Online Android APK Decompiler
<https://www.apkdecompilers.com> ▾
Decompile Android **APK** files online ✓. We will **decompile** your Android **apk** for free so you can get access to the Java source code and other resources.



Анализ исходников



Поиск нужного сервиса

```
UART_UUID = UUID.fromString("6E400001-B5A3-F393-E0A9-E50E24DCCA9E");
```

```
TX_UUID = UUID.fromString("6E400002-B5A3-F393-E0A9-E50E24DCCA9E");
```

```
RX_UUID = UUID.fromString("6E400003-B5A3-F393-E0A9-E50E24DCCA9E");
```



Поиск чтения данных

```
class Clazz extends BluetoothGattCallback
{
    @Override
    public void onCharacteristicRead(...)
    { ... }
}
```



Поиск формата данных

```
onCharacteristicRead(... Characteristic c)
{
    receivedData(c.getValue());
}
```



Поиск формата данных

```
private static void receivedData(byte[] dataBytes)
{
    byte[] temp = { dataBytes[2], dataBytes[3] };
    boolean[] bits = byteArray2BitArray(temp);

    Inputs.buttonA.key = bits[0];
    ...
    Inputs.forward2.key = bits[13];
    ...
}
```



Поиск записи данных

```
service = gatt.getService(s);  
char = service.getCharacteristic(c);  
char.setValue(value);  
gatt.writeCharacteristic(char);
```



Резюме

- Не все приложения можно реверс-инжинирить

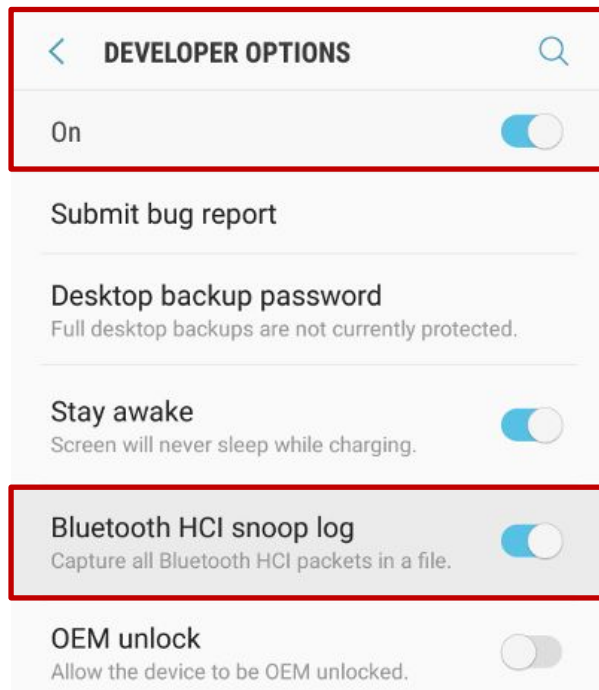


Анализ трафика приложения

- Протокол работы с девайсом
 - Сервисы и характеристики
 - Данные чтения/записи
 - Адреса, пароли, явки



Включения логов трафика

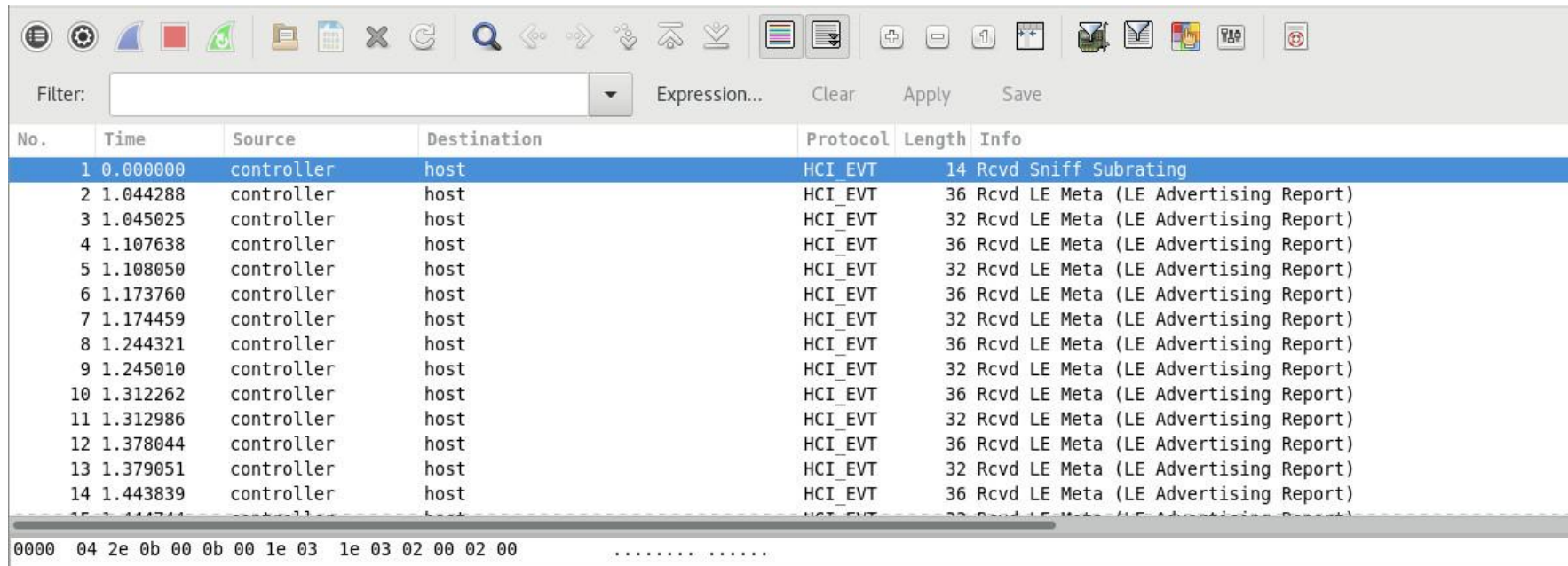


Получаем трафик приложения

- Делаем некие действия в приложение
- `adb pull /sdcard/btsnoop_hci.log`



Анализ трафика



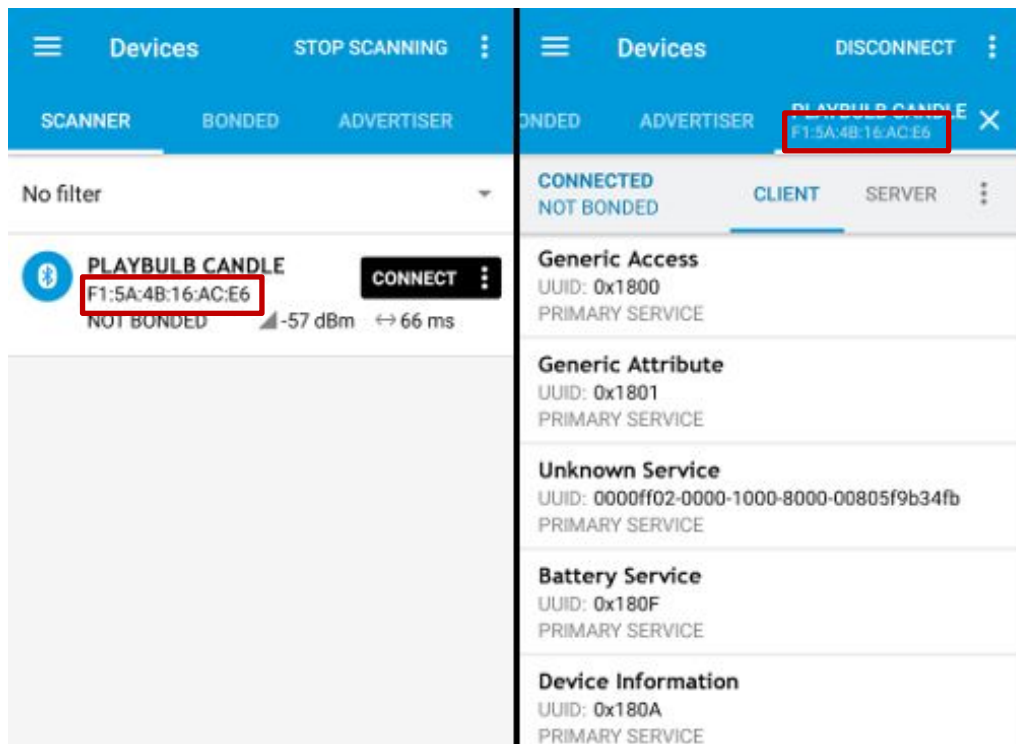
Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	controller	host	HCI_EVT	14	Rcvd Sniff Subrating
2	1.044288	controller	host	HCI_EVT	36	Rcvd LE Meta (LE Advertising Report)
3	1.045025	controller	host	HCI_EVT	32	Rcvd LE Meta (LE Advertising Report)
4	1.107638	controller	host	HCI_EVT	36	Rcvd LE Meta (LE Advertising Report)
5	1.108050	controller	host	HCI_EVT	32	Rcvd LE Meta (LE Advertising Report)
6	1.173760	controller	host	HCI_EVT	36	Rcvd LE Meta (LE Advertising Report)
7	1.174459	controller	host	HCI_EVT	32	Rcvd LE Meta (LE Advertising Report)
8	1.244321	controller	host	HCI_EVT	36	Rcvd LE Meta (LE Advertising Report)
9	1.245010	controller	host	HCI_EVT	32	Rcvd LE Meta (LE Advertising Report)
10	1.312262	controller	host	HCI_EVT	36	Rcvd LE Meta (LE Advertising Report)
11	1.312986	controller	host	HCI_EVT	32	Rcvd LE Meta (LE Advertising Report)
12	1.378044	controller	host	HCI_EVT	36	Rcvd LE Meta (LE Advertising Report)
13	1.379051	controller	host	HCI_EVT	32	Rcvd LE Meta (LE Advertising Report)
14	1.443839	controller	host	HCI_EVT	36	Rcvd LE Meta (LE Advertising Report)
15	1.444744	controller	host	HCI_EVT	32	Rcvd LE Meta (LE Advertising Report)

0000 04 2e 0b 00 0b 00 1e 03 1e 03 02 00 02 00



Фильтрация по адресу



Анализ трафика

The screenshot shows the Wireshark interface with a filter applied: `bluetooth.addr==F1:5A:4B:16:AC:E6`. The packet list shows several Bluetooth ATT packets. The selected packet (Frame 305) is a Write Command (opcode 0x52) for the 'AirFuel Alliance - Wireless Power Transfer (WPT) Service' with a Service UUID of 0xff02 and a value of 00ff0000.

Source	Destination	Protocol	Length	Info
f1:5a:4b:16:ac:e6	localhost ()	ATT	25	Rcvd Read Response, Ha
localhost ()	f1:5a:4b:16:ac:e6 (PLAYBULB CANDLE)	ATT	12	Sent Read Request, Har
f1:5a:4b:16:ac:e6	localhost ()	ATT	18	Rcvd Read Response, Ha
localhost ()	f1:5a:4b:16:ac:e6 (PLAYBULB CANDLE)	ATT	16	Sent Write Command, Ha
localhost ()	f1:5a:4b:16:ac:e6 (PLAYBULB CANDLE)	ATT	16	Sent Write Command, Ha
localhost ()	f1:5a:4b:16:ac:e6 (PLAYBULB CANDLE)	ATT	16	Sent Write Command, Ha

Frame 305: 16 bytes on wire (128 bits), 16 bytes captured (128 bits)

- Bluetooth
- Bluetooth HCI H4
- Bluetooth HCI ACL Packet
- Bluetooth L2CAP Protocol
- Bluetooth Attribute Protocol
 - Opcode: Write Command (0x52)
 - Handle: 0x0019 (Unknown: AirFuel Alliance - Wireless Power Transfer (WPT) Service)
 - Service UUID: Unknown (0xff02)
 - UUID: AirFuel Alliance - Wireless Power Transfer (WPT) Service (0xfffc)
 - Value: 00ff0000

1. Фильтрация по адресу
2. Лог записи/чтения
3. Сервис
4. Характеристика
5. Значения



Проверка

The image displays three screenshots from a mobile application interface for managing Bluetooth devices. The device shown is 'PLAYBULB CANDLE' with MAC address 'F1:5A:4B:16:AC:E6'.

Left Screenshot: Shows the 'Generic Attribute' section with a red box highlighting an 'Unknown Service' entry with UUID '0000ff02-0000-1000-8000-00805f9b34fb'.

Middle Screenshot: Shows the 'Unknown Characteristic' section with a red box highlighting an entry with UUID '0000fffc-0000-1000-8000-00805f9b34fb'.

Right Screenshot: Shows a 'Write value' dialog box with a red box around the input field containing '0x 00FFFF00' and a 'SEND' button.

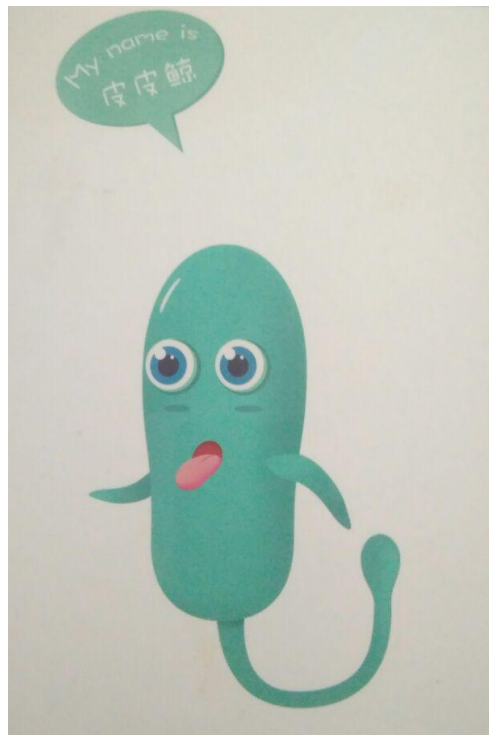


Резюме

- Информация о работе приложения без его реверс-инжиниринга
- Неявный формат данных



Реверс вибратора



Сервисы девайса

BONDED		ADVERTISER	PIPIJING 0C:B2:B7:7D:0D:14	×
CONNECTED	NOT BONDED	CLIENT	SERVER	⋮

Unknown Service
UUID: 00006060-0000-1000-8000-00805f9b34fb
PRIMARY SERVICE

Unknown Service
UUID: 00006000-0000-1000-8000-00805f9b34fb
PRIMARY SERVICE

Unknown Service
UUID: 00006010-0000-1000-8000-00805f9b34fb
PRIMARY SERVICE

Unknown Service
UUID: 00006050-0000-1000-8000-00805f9b34fb
PRIMARY SERVICE

Unknown Service
UUID: f000ffc0-0451-4000-b000-000000000000
PRIMARY SERVICE



Брутфорс?

- Нужно найти сервис для отправки команд
- Отправлять туда байты
- Фиксировать результат



Характеристика для команд

The screenshot shows a Bluetooth interface for a device named 'PIPIJING' with MAC address '0C:B2:B7:D:0D:14'. It lists several services and characteristics:

- CONNECTED** (status)
- NOT BONDED** (status)
- CLIENT** / **SERVER** (roles)
- Unknown Service** (UUID: 0x1801, PRIMARY SERVICE)
- Unknown Service** (UUID: 00006060-0000-1000-8000-00805f9b34fb, PRIMARY SERVICE)
- Unknown Service** (UUID: 00006000-0000-1000-8000-00805f9b34fb, PRIMARY SERVICE)
- Unknown Characteristic** (UUID: 00006001-0000-1000-8000-00805f9b34fb, Properties: WRITE NO RESPONSE)
- Unknown Characteristic** (UUID: 00006002-0000-1000-8000-00805f9b34fb, Properties: WRITE) - This entry is highlighted with a red box.
- Unknown Service** (UUID: 00006010-0000-1000-8000-00805f9b34fb, PRIMARY SERVICE)
- Unknown Service** (bottom entry)

- Находим характеристики для записи
 - Properties: Write



Приложение для брутфорса

```
char = service.getCharacteristic(uuid);  
while (true) {  
    char.setValue(rand_byte_array);  
    gatt.writeCharacteristic(char);  
    // Смотрим на результат  
}
```





**One
Eternity
Later**

Брутфорс?

- Брутфорс возможен для несложного пакета команд
- Но занимает много времени и внимания



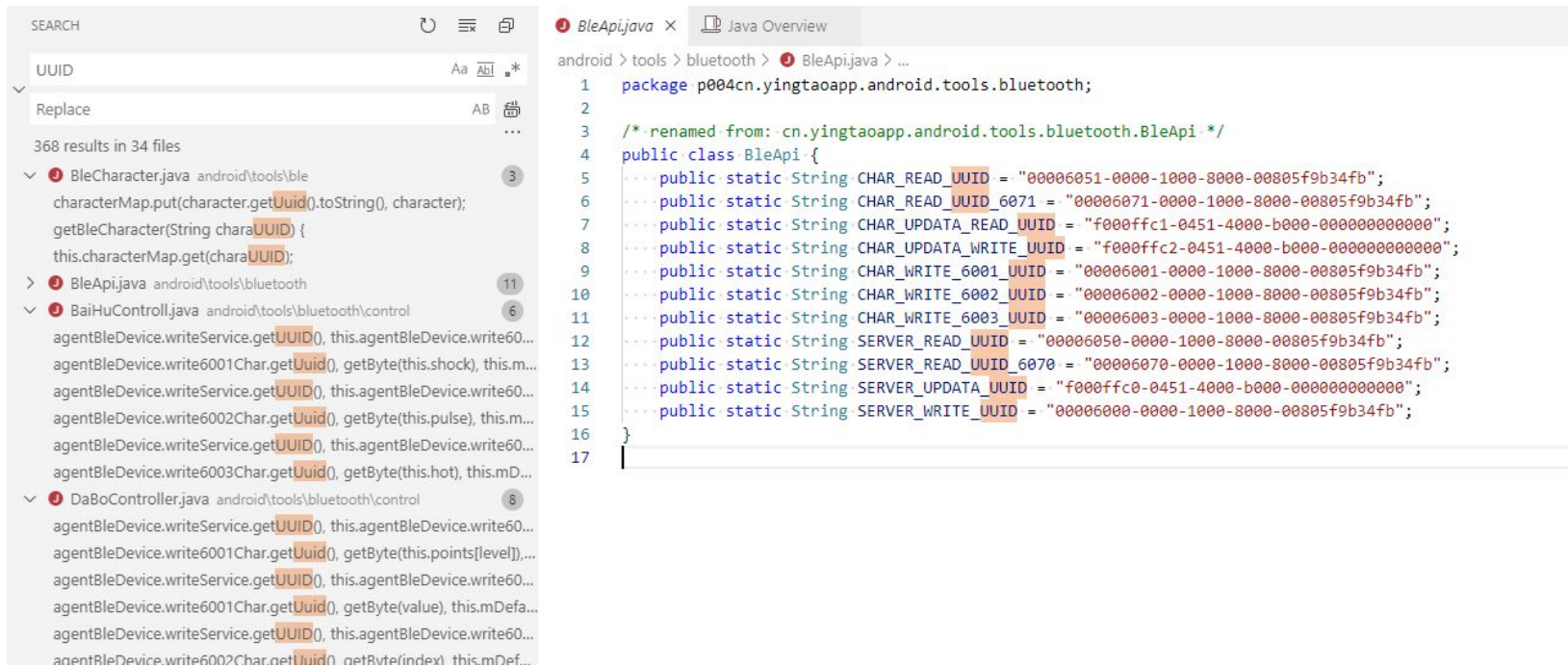
Реверс-инжиниринг apk

- `adb shell pm path cn.yingtaoapp.android`
- `package:/data/app/cn.yingtaoapp.android/base.apk`
- `adb pull /data/app/cn.yingtaoapp.android/base.apk`
- Декомпиляция apk

18:22	0,0 КБ/с	4G	20
<	0 приложений		
Имя приложения	樱桃		
Версия приложения	2.2.14		
Имя пакета	cn.yingtaoapp.android		
Время установки	2018/02/21 17:40:57		



Поиск нужного сервиса



The image shows a screenshot of an IDE with a search window on the left and a code editor on the right. The search window shows the results of a search for 'UUID' across 34 files, with 368 results. The files listed are BleCharacter.java, BleApi.java, BaiHuControll.java, and DaBoController.java. The code editor shows the content of BleApi.java, which is a Java class containing several public static strings representing UUIDs for various Bluetooth services. The strings are: CHAR_READ_UUID, CHAR_READ_UUID_6071, CHAR_UPDATA_READ_UUID, CHAR_UPDATA_WRITE_UUID, CHAR_WRITE_6001_UUID, CHAR_WRITE_6002_UUID, CHAR_WRITE_6003_UUID, SERVER_READ_UUID, SERVER_READ_UUID_6070, SERVER_UPDATA_UUID, and SERVER_WRITE_UUID. The strings are all in the format of a 128-bit UUID (e.g., "00006051-0000-1000-8000-00805f9b34fb").

```
SEARCH
UUID
Replace
368 results in 34 files
3 BleCharacter.java android\tools\ble
characterMap.put(character.getUuid(),toString(), character);
getBleCharacter(String charaUUID) {
this.characterMap.get(charaUUID);
11 BleApi.java android\tools\bluetooth
6 BaiHuControll.java android\tools\bluetooth\control
agentBleDevice.writeService.getUUID(), this.agentBleDevice.write60...
agentBleDevice.write6001Char.getUuid(), getByte(this.shock), this.m...
agentBleDevice.writeService.getUUID(), this.agentBleDevice.write60...
agentBleDevice.write6002Char.getUuid(), getByte(this.pulse), this.m...
agentBleDevice.writeService.getUUID(), this.agentBleDevice.write60...
agentBleDevice.write6003Char.getUuid(), getByte(this.hot), this.mD...
8 DaBoController.java android\tools\bluetooth\control
agentBleDevice.writeService.getUUID(), this.agentBleDevice.write60...
agentBleDevice.write6001Char.getUuid(), getByte(this.points[level]),...
agentBleDevice.writeService.getUUID(), this.agentBleDevice.write60...
agentBleDevice.write6001Char.getUuid(), getByte(value), this.mDefa...
agentBleDevice.writeService.getUUID(), this.agentBleDevice.write60...
agentBleDevice.write6002Char.getUuid(), getByte(index) this.mDef...

BleApi.java x Java Overview
android > tools > bluetooth > BleApi.java > ...
1 package p004cn.yingtaoapp.android.tools.bluetooth;
2
3 /*-renamed from: cn.yingtaoapp.android.tools.bluetooth.BleApi */
4 public class BleApi {
5     public static String CHAR_READ_UUID = "00006051-0000-1000-8000-00805f9b34fb";
6     public static String CHAR_READ_UUID_6071 = "00006071-0000-1000-8000-00805f9b34fb";
7     public static String CHAR_UPDATA_READ_UUID = "f000ffc1-0451-4000-b000-000000000000";
8     public static String CHAR_UPDATA_WRITE_UUID = "f000ffc2-0451-4000-b000-000000000000";
9     public static String CHAR_WRITE_6001_UUID = "00006001-0000-1000-8000-00805f9b34fb";
10    public static String CHAR_WRITE_6002_UUID = "00006002-0000-1000-8000-00805f9b34fb";
11    public static String CHAR_WRITE_6003_UUID = "00006003-0000-1000-8000-00805f9b34fb";
12    public static String SERVER_READ_UUID = "00006050-0000-1000-8000-00805f9b34fb";
13    public static String SERVER_READ_UUID_6070 = "00006070-0000-1000-8000-00805f9b34fb";
14    public static String SERVER_UPDATA_UUID = "f000ffc0-0451-4000-b000-000000000000";
15    public static String SERVER_WRITE_UUID = "00006000-0000-1000-8000-00805f9b34fb";
16 }
17
```



Поиск нужного сервиса

```
ijava x Java Overview
> tools > bluetooth > BleApi.java > ...
package p004cn.yingtaoapp.android.tools.bluetooth;

/*-renamed from: cn.yingtaoapp.android.tools.bluetooth.BleApi-*/
public class BleApi {
    ... public static String CHAR_READ_UUID = "00006051-0000-1000-8000-00805f9b34fb";
    ... public static String CHAR_READ_UUID_6071 = "00006071-0000-1000-8000-00805f9b34fb";
    ... public static String CHAR_UPDATA_READ_UUID = "f000ffc1-0451-4000-b000-000000000000";
    ... public static String CHAR_UPDATA_WRITE_UUID = "f000ffc0-0451-4000-b000-000000000000";
    ... public static String CHAR_WRITE_6001_UUID = "00006001-0000-1000-8000-00805f9b34fb";
    ... public static String CHAR_WRITE_6002_UUID = "00006002-0000-1000-8000-00805f9b34fb";
    ... public static String CHAR_WRITE_6003_UUID = "00006003-0000-1000-8000-00805f9b34fb";
    ... public static String SERVER_READ_UUID = "00006000-0000-1000-8000-00805f9b34fb";
    ... public static String SERVER_READ_UUID_6070 = "00006070-0000-1000-8000-00805f9b34fb";
    ... public static String SERVER_UPDATA_UUID = "f000ffc0-0451-4000-b000-000000000000";
    ... public static String SERVER_WRITE_UUID = "00006000-0000-1000-8000-00805f9b34fb";
}
```

- Характеристики с “Write”

Bluetooth scanner interface showing a list of services. The top bar indicates the device is bonded and the advertiser is PIPIJING (0C:B2:B7:7D:0D:14). The scanner is currently in CLIENT mode. The list includes:

- CONNECTED** (NOT BONDED) | CLIENT | SERVER
- Unknown Service**
UUID: 00006060-0000-1000-8000-00805f9b34fb
PRIMARY SERVICE
- Unknown Service**
UUID: 00006000-0000-1000-8000-00805f9b34fb
PRIMARY SERVICE
- Unknown Characteristic**
UUID: 00006001-0000-1000-8000-00805f9b34fb
Properties: WRITE NO RESPONSE
- Unknown Characteristic** (highlighted)
UUID: 00006002-0000-1000-8000-00805f9b34fb
Properties: WRITE

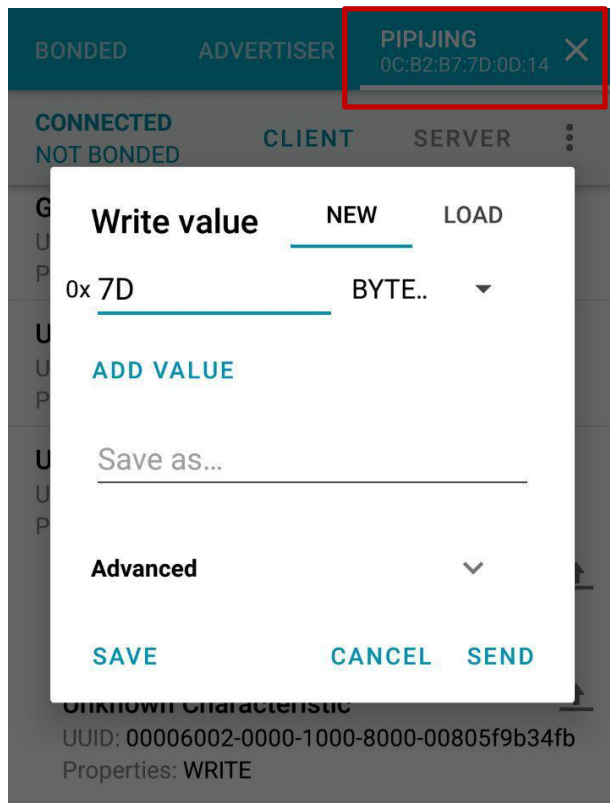


Поиск отправки данных

```
public void doClick(int value) {  
    case 0:  
        this.mToy.BLE.write(value * 128);  
        return;  
    case 1:  
        this.mToy.BLE.write(value * 64);  
        return;  
    default:  
        return;  
}
```



Проверим

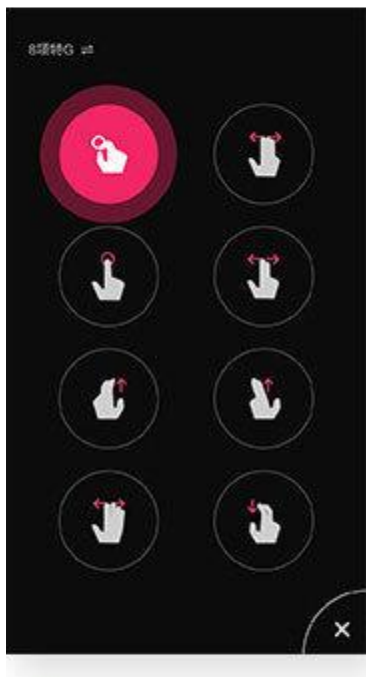


Стоит ли доверять?

```
c void postGameRecords(final String body, final Callback<Integer> callback) {  
f (callback != null) {  
.. this.mThreadPool.execute(new Runnable() {  
.. .. public void run() {  
.. .. .. try {  
.. .. .. .. HttpRequest request = HttpRequest.post((CharSequence) "http://api.bianquejia.cn:8777/v1/re");  
.. .. .. .. request.header("appversion", ToolsApi.this.getVersion());  
.. .. .. .. int code = request.code();  
.. .. .. .. if (code == 200) {  
.. .. .. .. .. callback.onResult(Integer.valueOf(code));  
.. .. .. .. } else {  
.. .. .. .. .. callback.onFail(code);  
.. .. .. .. }  
.. .. .. } catch (Exception e) {  
.. .. .. .. e.printStackTrace();  
.. .. .. .. callback.onFail(-1);  
.. .. .. }  
.. .. }  
.. }  
.. });
```



Анализ приложения



- Включим логи
- Отправим команду
- Посмотрим логи



Анализ трафика

1223	798.010920	host	controller	HCI_CMD	29	Sent LE Create Connection	
1224	798.017967	controller	host	HCI_EVT	7	Rcvd Command Status (LE)	
→	1225	804.176169	host	controller	HCI_CMD	4	Sent Vendor Command 0x01
←	1226	804.181059	controller	host	HCI_EVT	23	Rcvd Command Complete (V)
	1227	818.029783	host	controller	HCI_CMD	4	Sent LE Create Connection
	1228	818.035288	controller	host	HCI_EVT	7	Rcvd Command Complete (LI)
	1229	818.035517	controller	host	HCI_EVT	34	Rcvd LE Meta (LE Enhance)
	1230	821.725866	host	controller	HCI_CMD	4	Sent Vendor Command 0x01
	1231	821.732253	controller	host	HCI_EVT	23	Rcvd Command Complete (V)

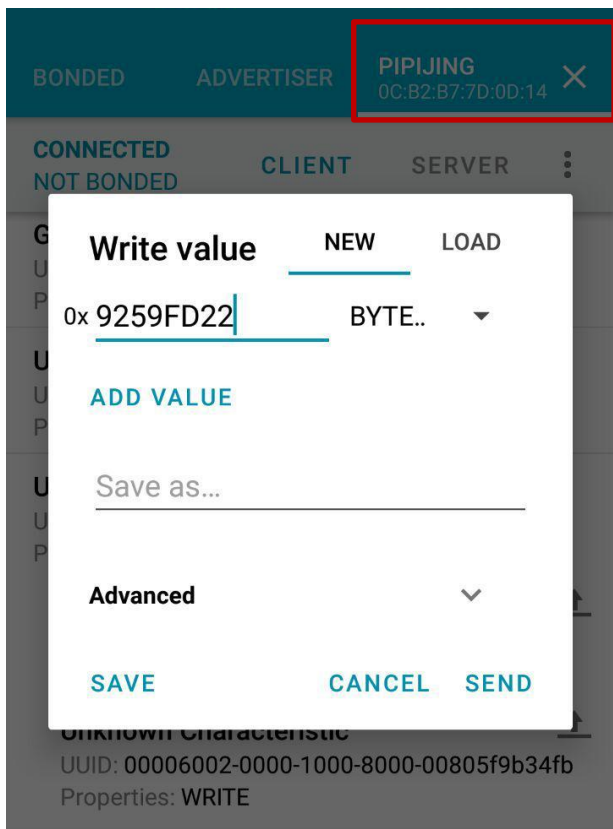
> Frame 1225: 4 bytes on wire (32 bits), 4 bytes captured (32 bits)
> Bluetooth
> Bluetooth HCI H4
> Bluetooth HCI Command - Vendor Command 0xfd59

0000 01 59 fd 00

-Y..



Проверим



Что за формат?

Enter hex number:

↻ Convert **✖ Reset** **↕ Swap**

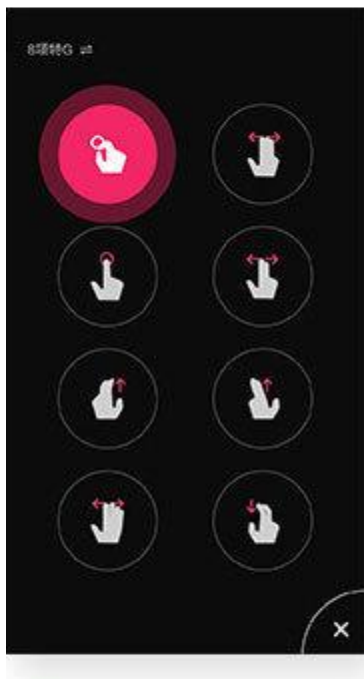
Decimal number:

22 281 472 / 128 =
174074

()	%	AC
7	8	9	+
4	5	6	×
1	2	3	-
0	.	=	+



Получим команды



- 0153fd00
- 3200
- ...



Поиск в приложении

```
public class WaveDataTransformer {  
    private static int[] classicMode1 = {30};  
    private static int[] classicMode2 = {60};  
    private static int[] classicMode3 = {100};  
    private static int[] classicMode4 = {0, 0, 0};  
    private static int[] classicMode5 = {60, 60, 0};  
    private static int[] classicMode6 = {0, 0, 0};  
    private static int[] classicMode7 = {0, 100, 0};  
    private static int[] classicMode8 = {0, 100};  
}
```



Резюме

Формат команд
+
UUID сервисов и характеристик
=
Свое приложение



BLE Security?

- и Да и Нет
- Шифрование передачи данных между устройствами



Немного методов защиты

- Спрятать парс данных в C++, etc
- Аутентификация устройства и приложения
- Дополнительное шифрование трафика



Заключение

- Bluetooth просто – протокол передачи данных
- Не стоит забывать о безопасности!



Спасибо за внимание

Контакты:

- telegram [@neargye](#)



