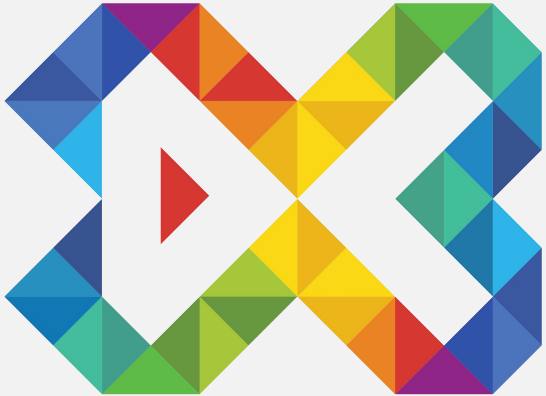
Пишем приложение для вибратора с Алиэкспресс, или Как реверс-инжинирить Bluetooth

Гончаров Даниил (Finch Technologies Ltd.)



UFADEVCONF

Для чего нам Bluetooth?

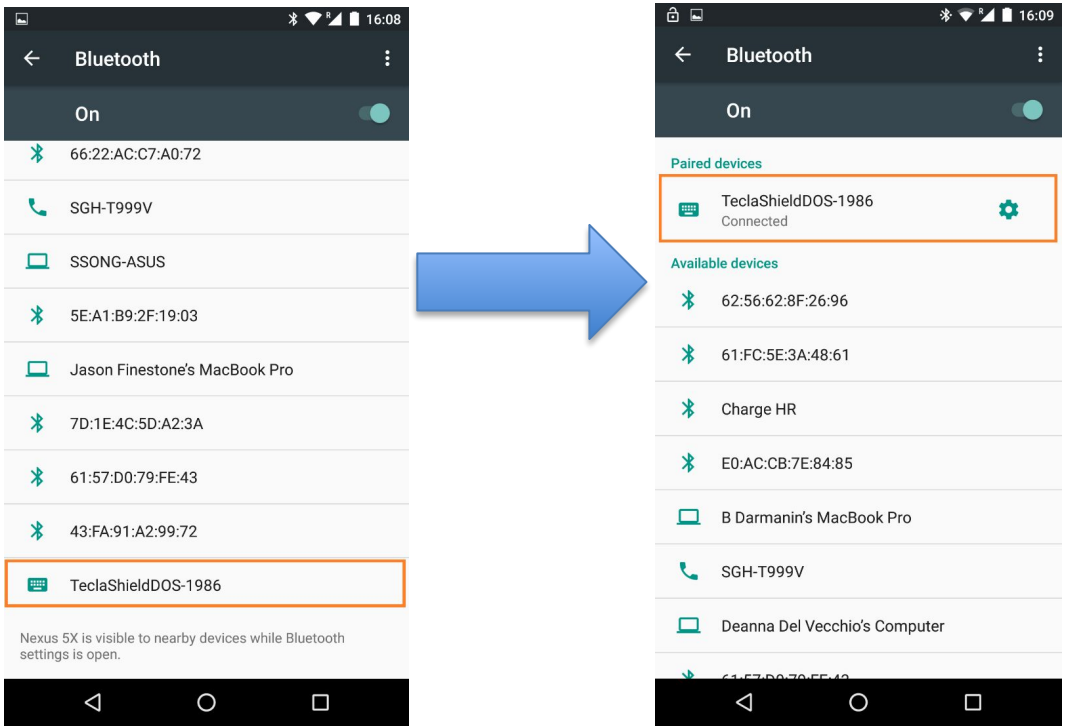
Finch Technologies & Co.

План

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

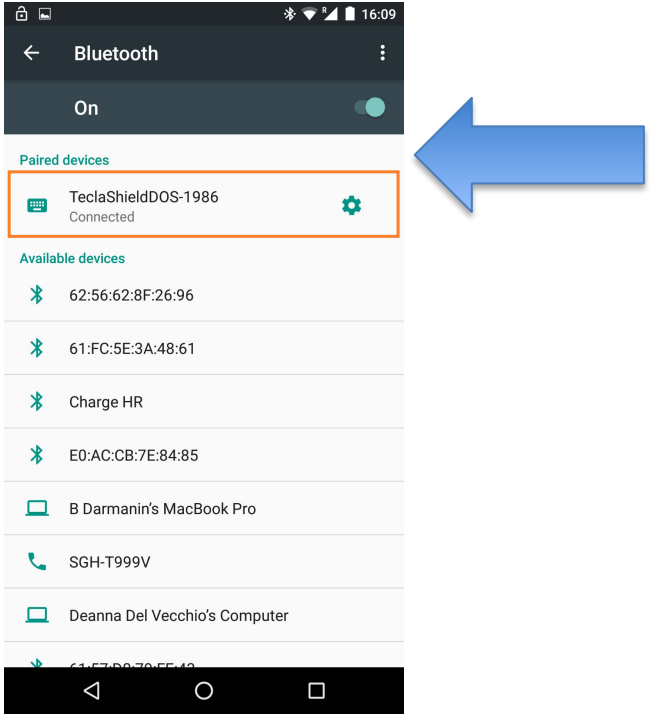
Bluetooth-Device

BLE Connect



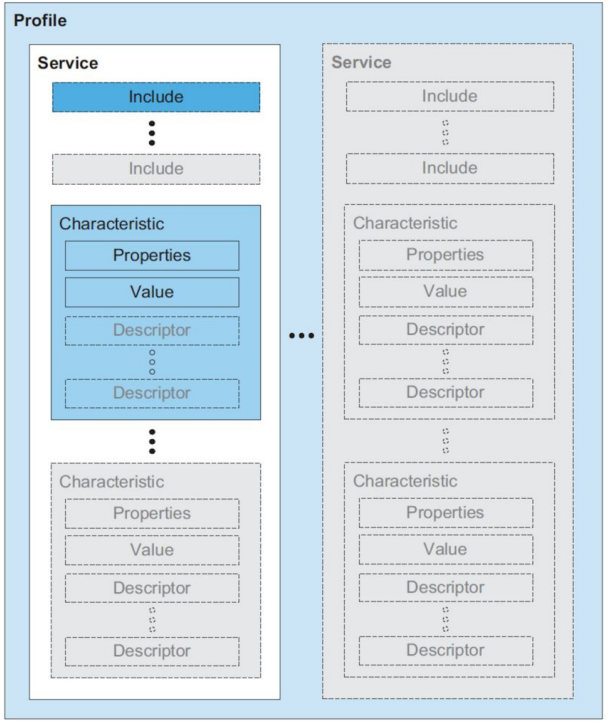
UFADEVCONF

BLE Security



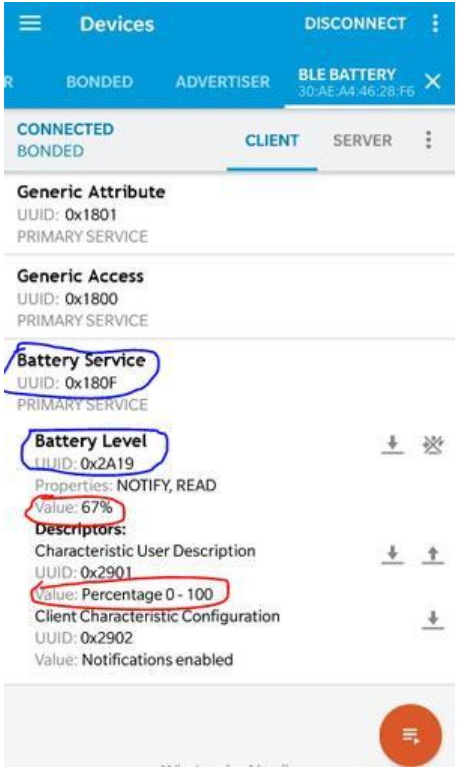
- Pairing – процесс создания парами BLE-устройств секретных ключей для последующего шифрования трафика

BluetoothDevice & BluetoothGatt



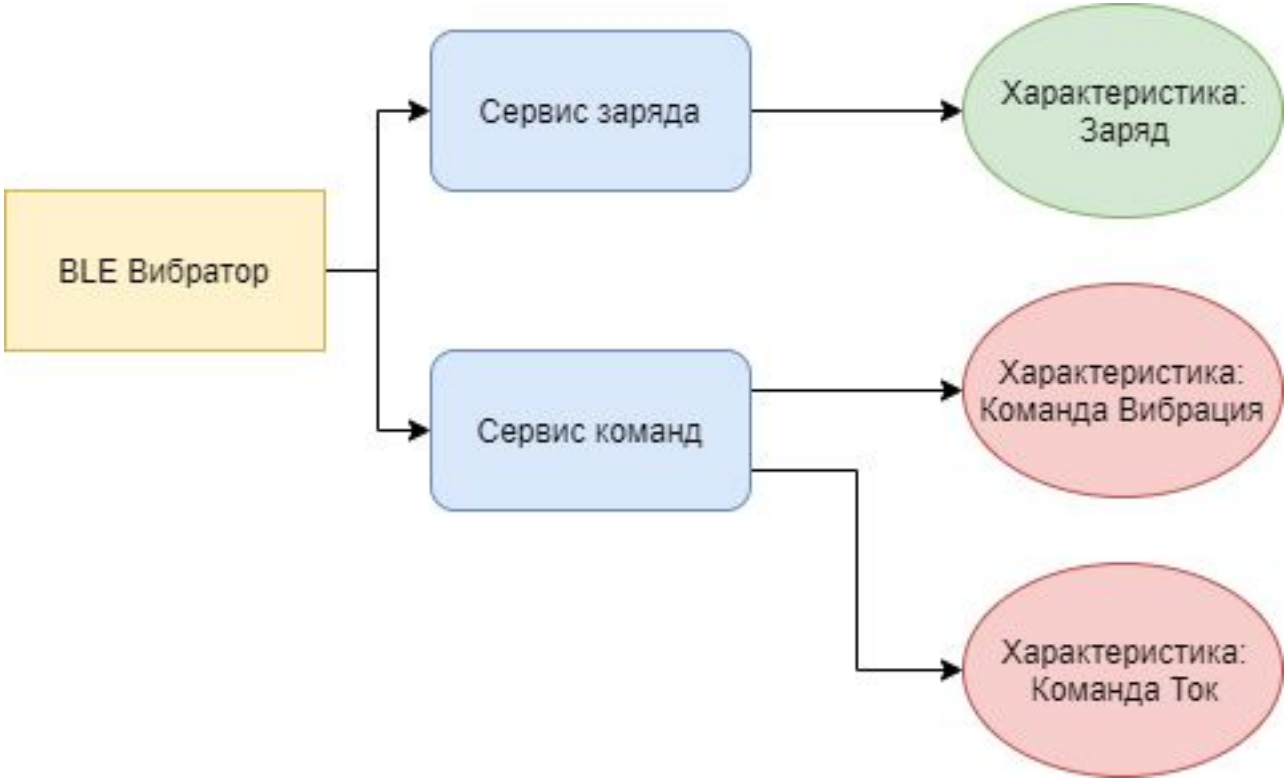
- GATT – профиль Bluetooth, определяющий способ взаимодействия двух устройств и использующий концепцию атрибутов
- GATT Characteristic – контейнер для данных
- GATT Service – совокупность характеристик
- UUID – 128-битный уникальный идентификатор атрибута

GATT Characteristic

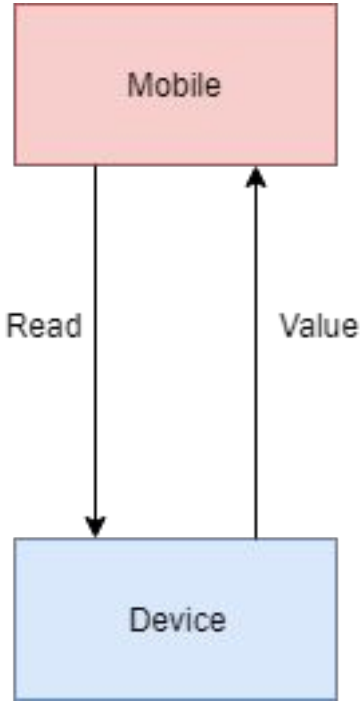


UFADEVCONF

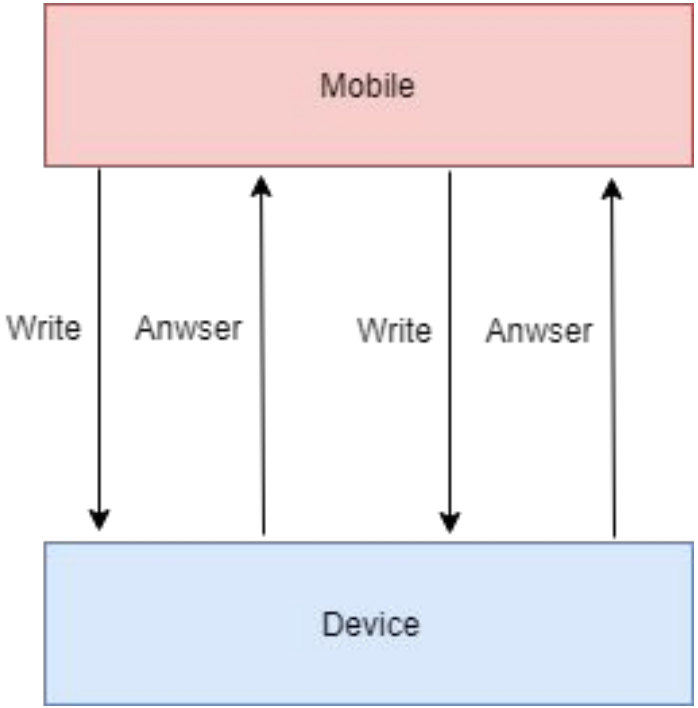
BluetoothGatt



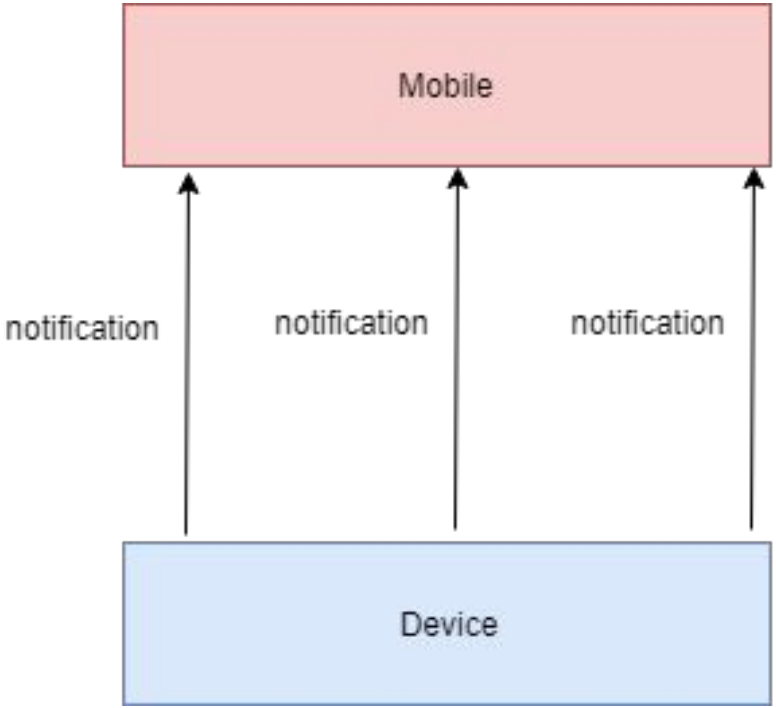
BluetoothGatt read



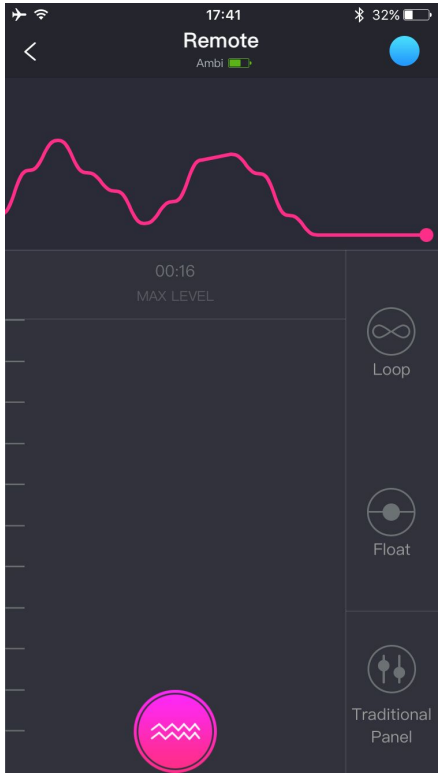
BluetoothGatt write



BluetoothGatt notification



Пример

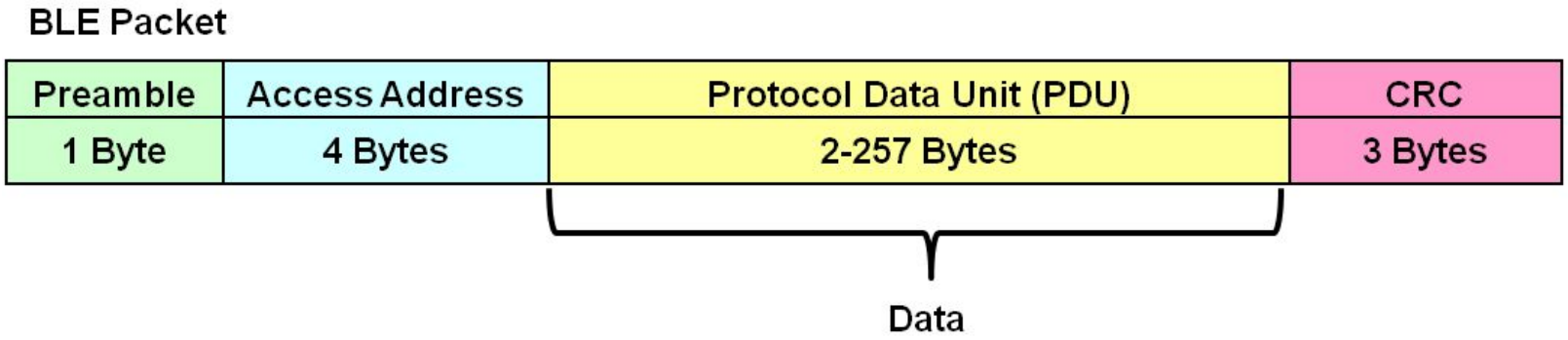


1. Подключение
2. Поиск всех сервисов устройства
3. Список сервисов
4. Отправка команды
5. Результат отправки

О BLE подробнее

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

BLE пакет

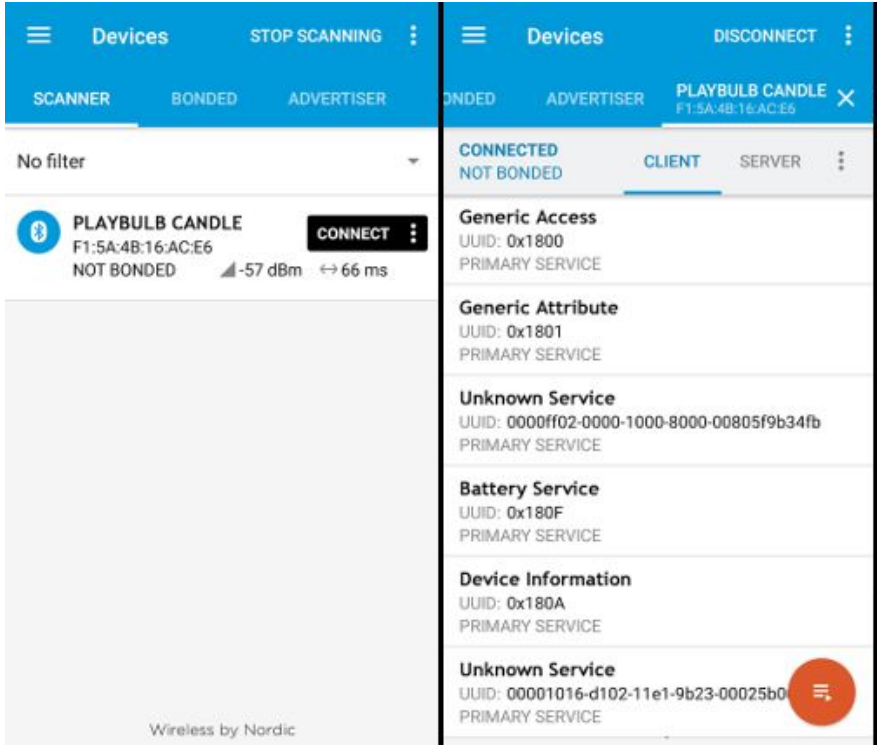


UFADEVCONF

Реверс-инжиниринг BLE-пакета

- Анализ BLE-профиля
- Реверс-инжиниринг приложения
- Анализ трафика

nRF Connect



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

nRF Connect

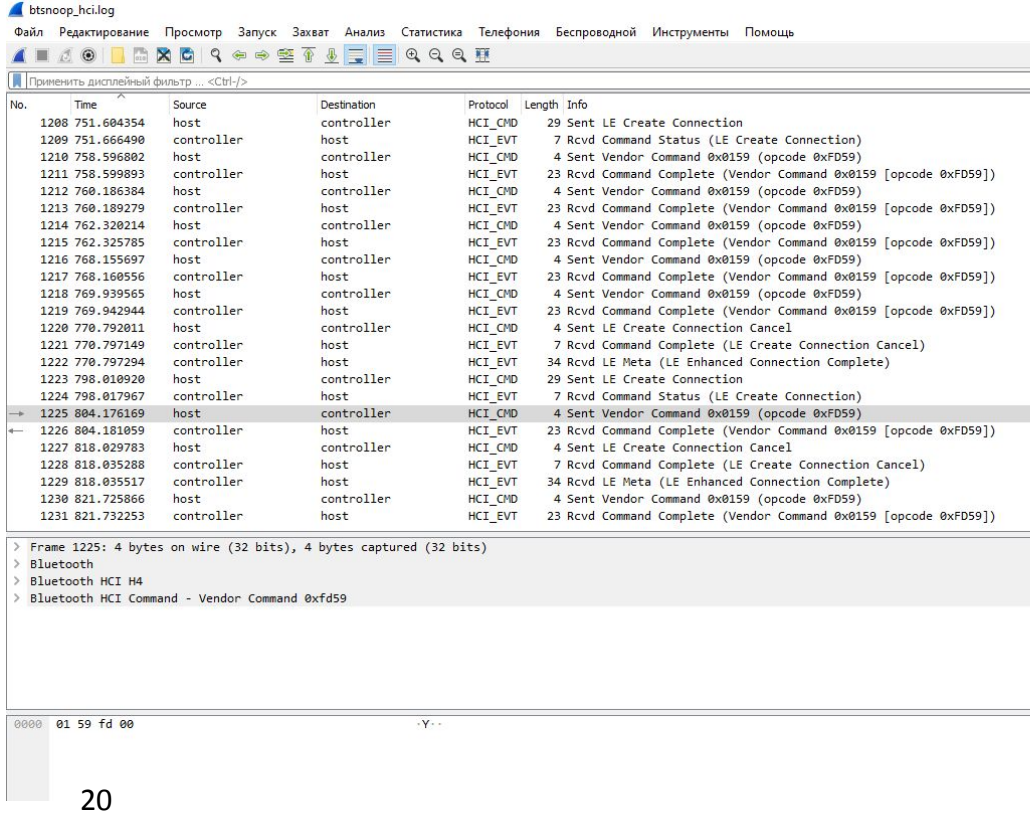
Android

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

iOS

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

Wireshark



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

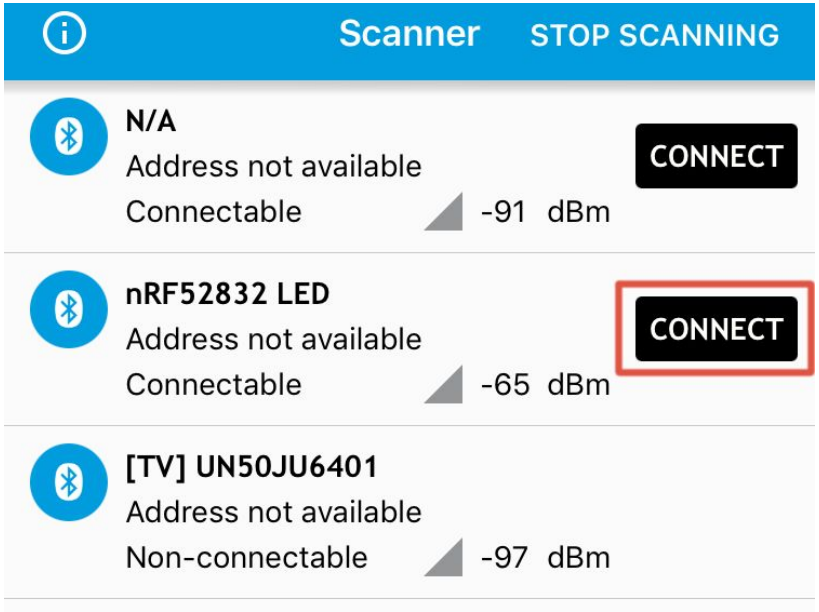
Wireshark

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

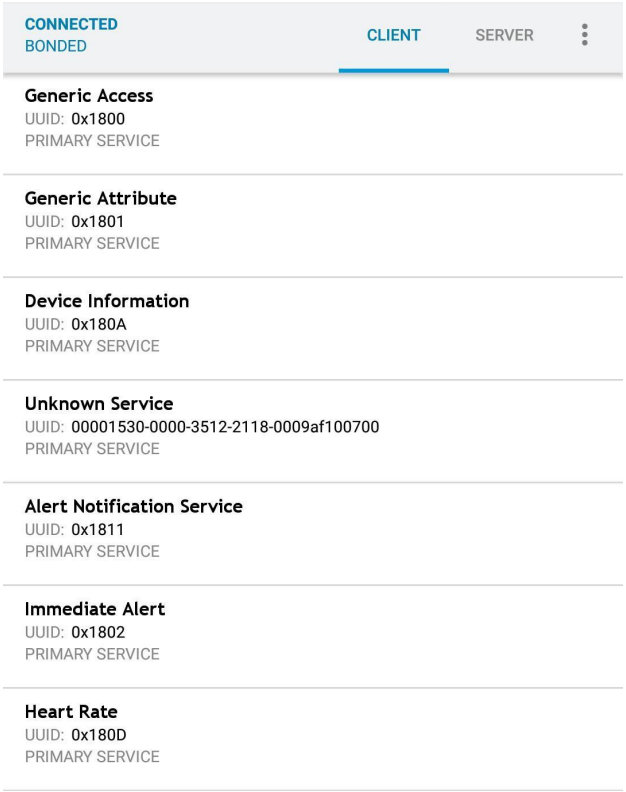
Анализ BLE-профиля

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

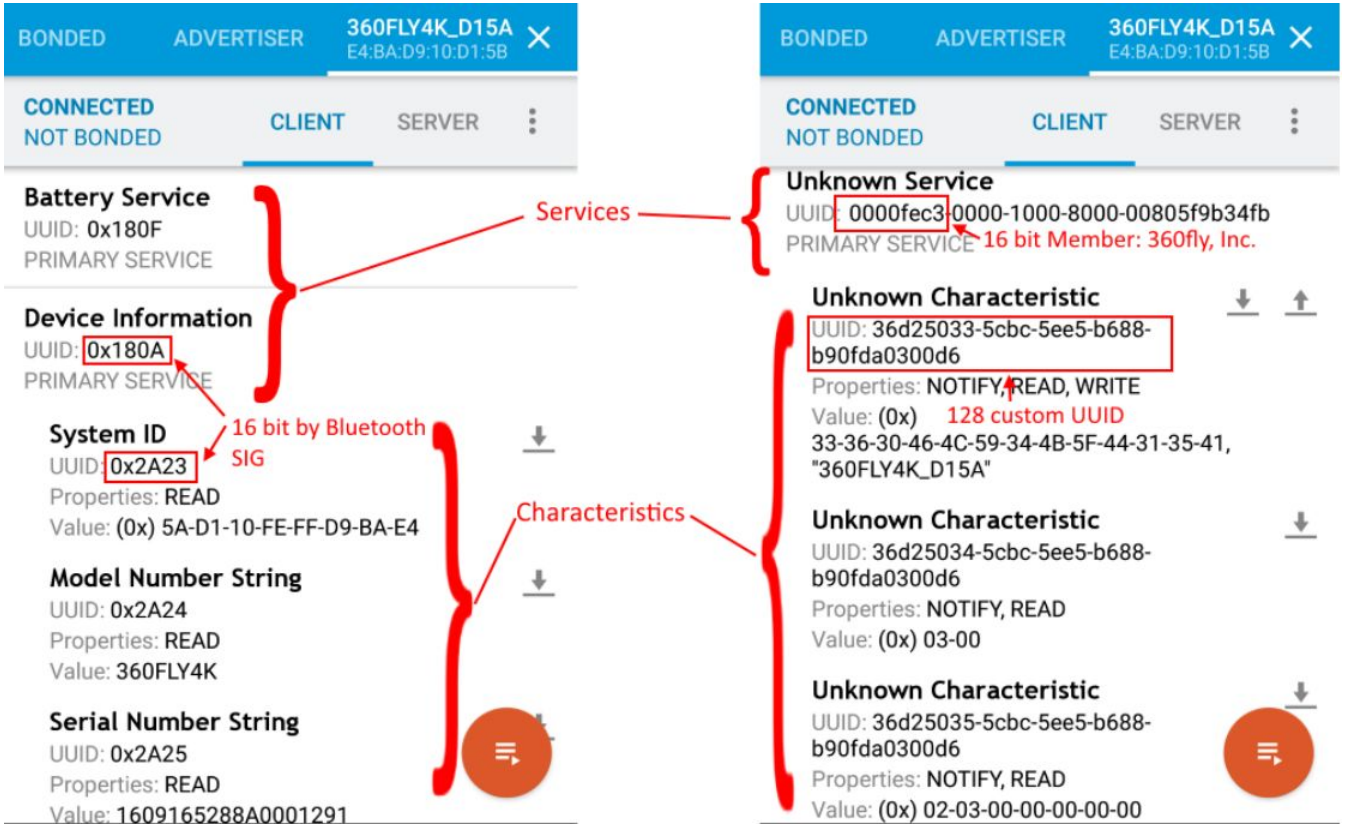
Подключение



Список сервисов

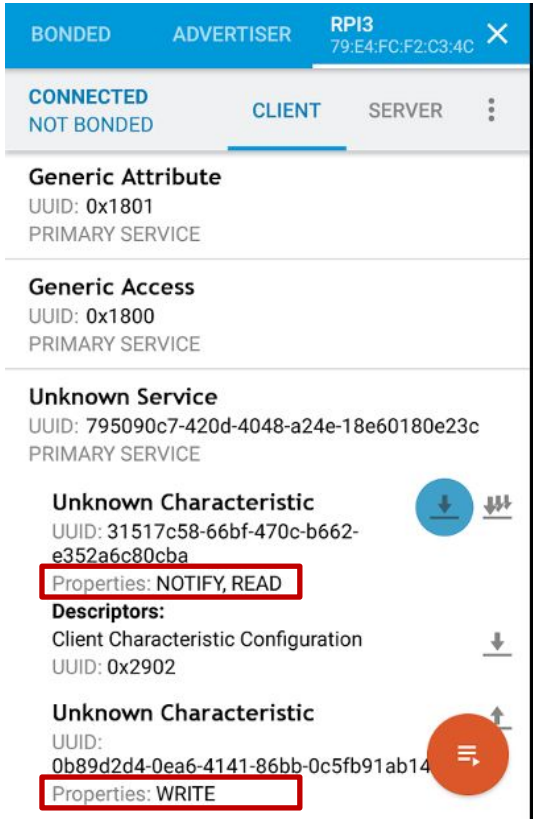


Список характеристик



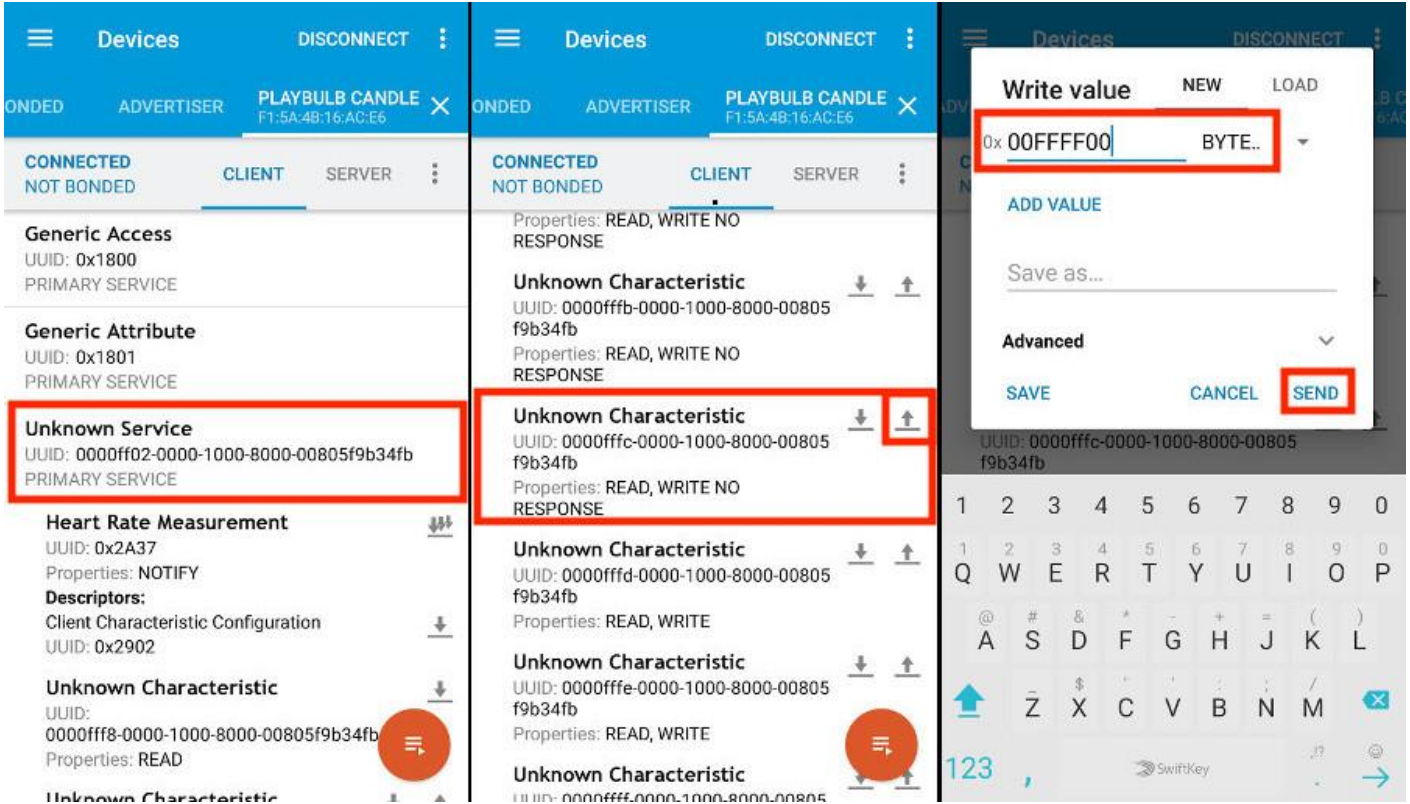
UFADEVCONF

Свойства характеристик



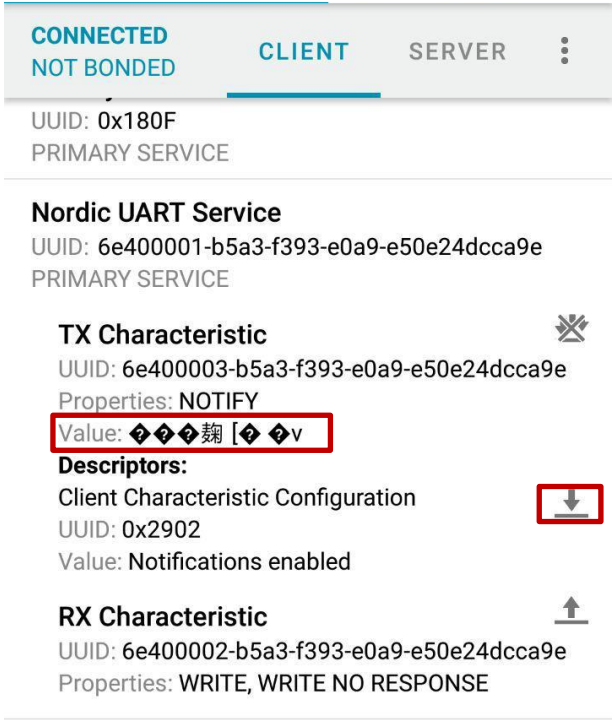
UFADEVCONF

Запись данных



UFADEVCONF

Чтение данных



Резюме

- Первичная информация о девайсе
- Формат данных неизвестен

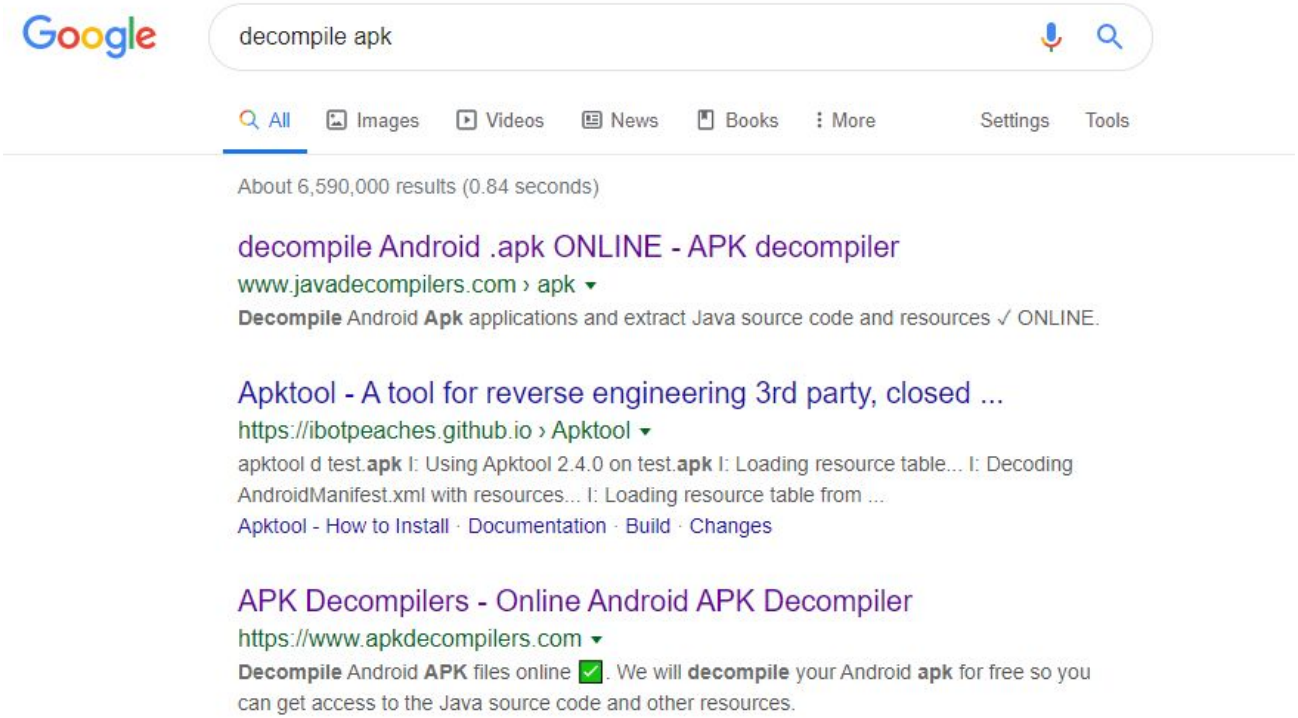
Реверс-инжиниринг приложения

- Декомпиляция бинарников
- Найти сервисы и характеристики
- Формат данных

Получение apk

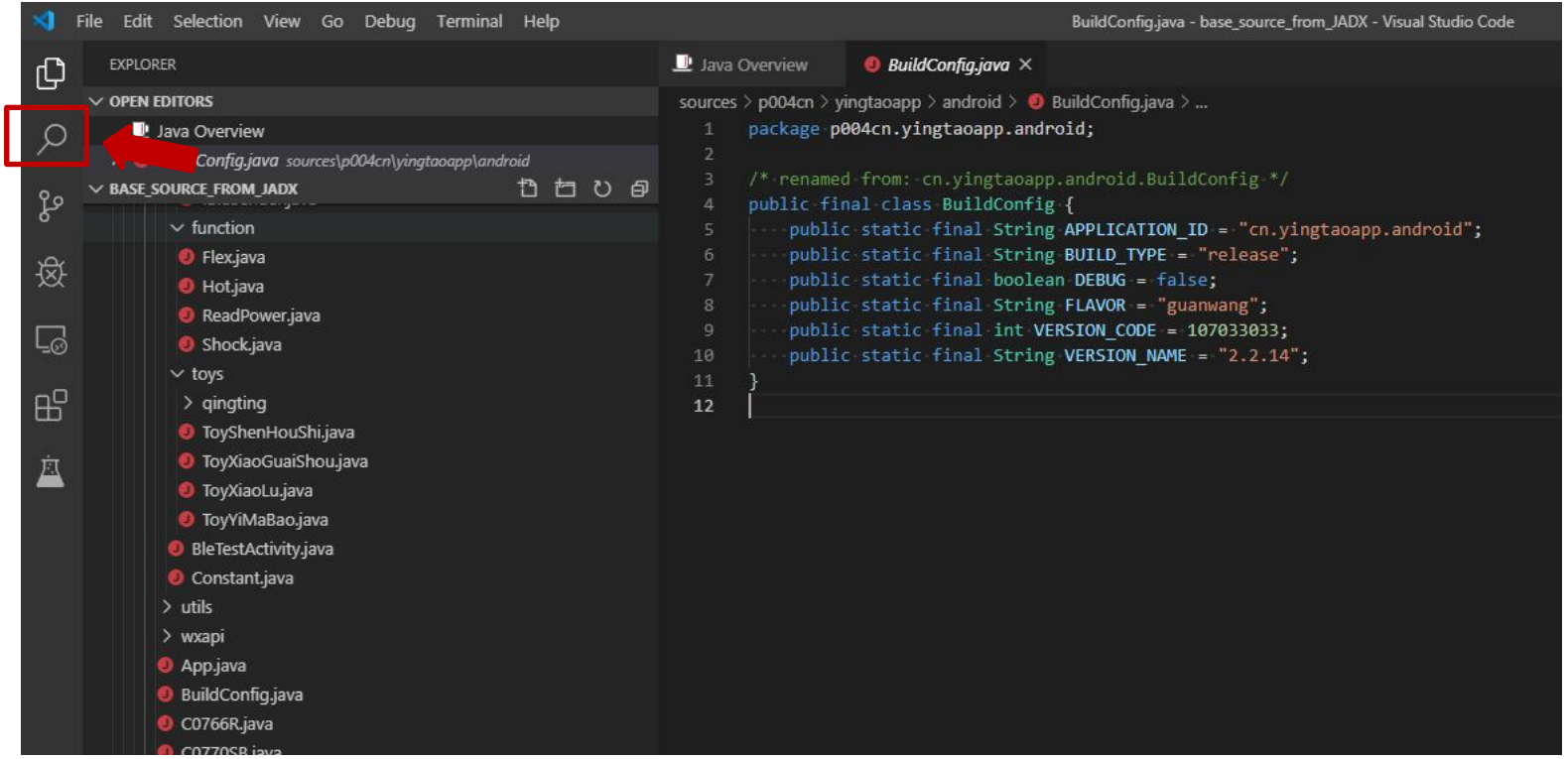
- adb shell pm path package.name
- package:/data/app/package.name/app.apk
- adb pull /data/app/package.name/app.apk

Декомпиляция бинарников



UFADEVCONF

Анализ исходников



UFADEVCONF

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);
```

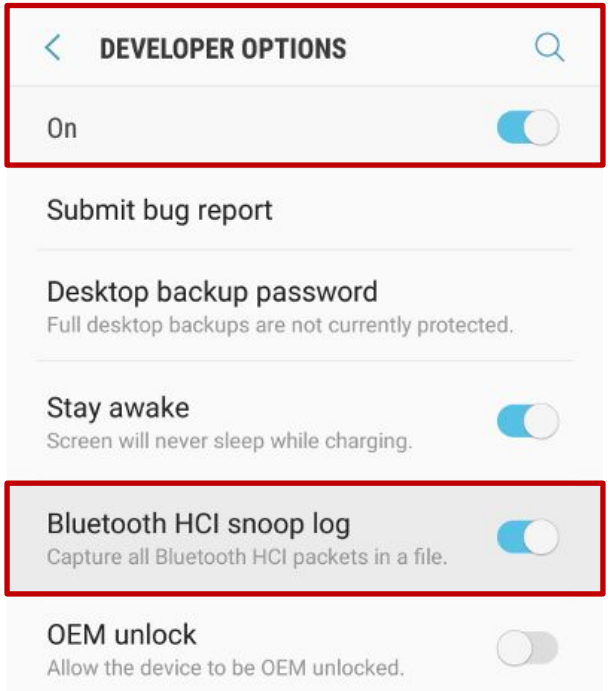
Резюме

- Не все приложения можно реверс-инжинирить

Анализ трафика приложения

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

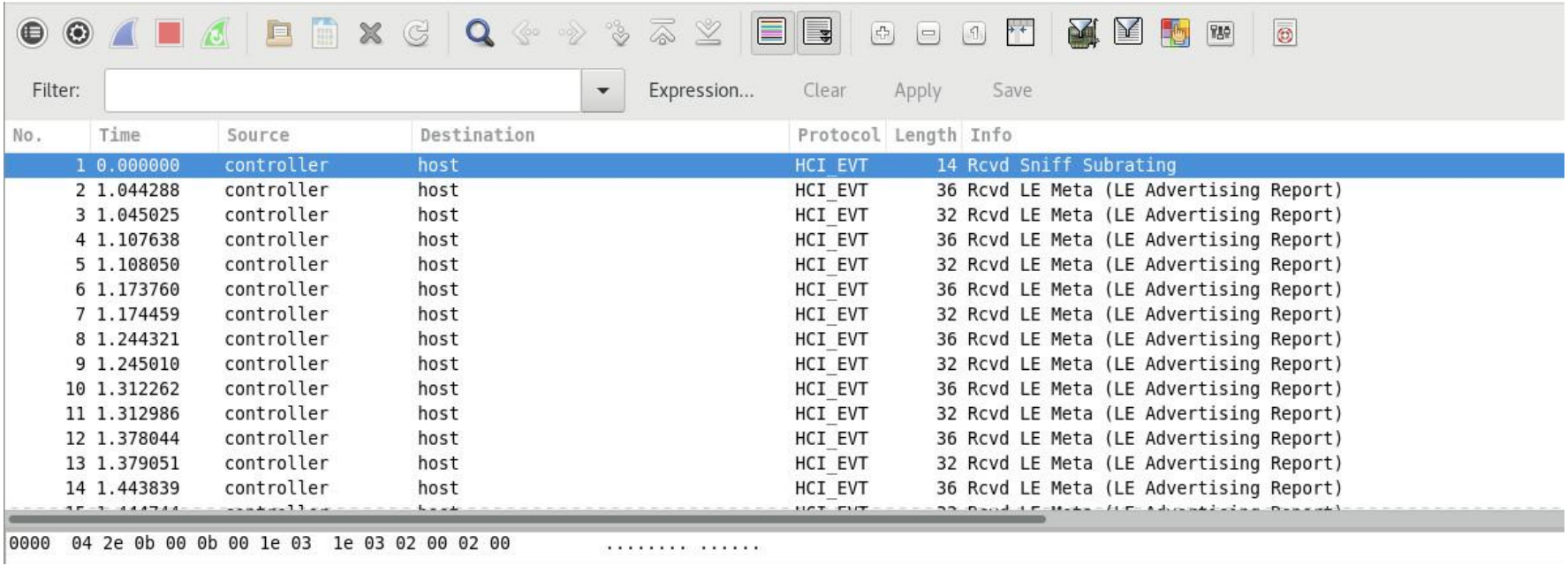
Включения логов трафика



Получаем трафик приложения

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

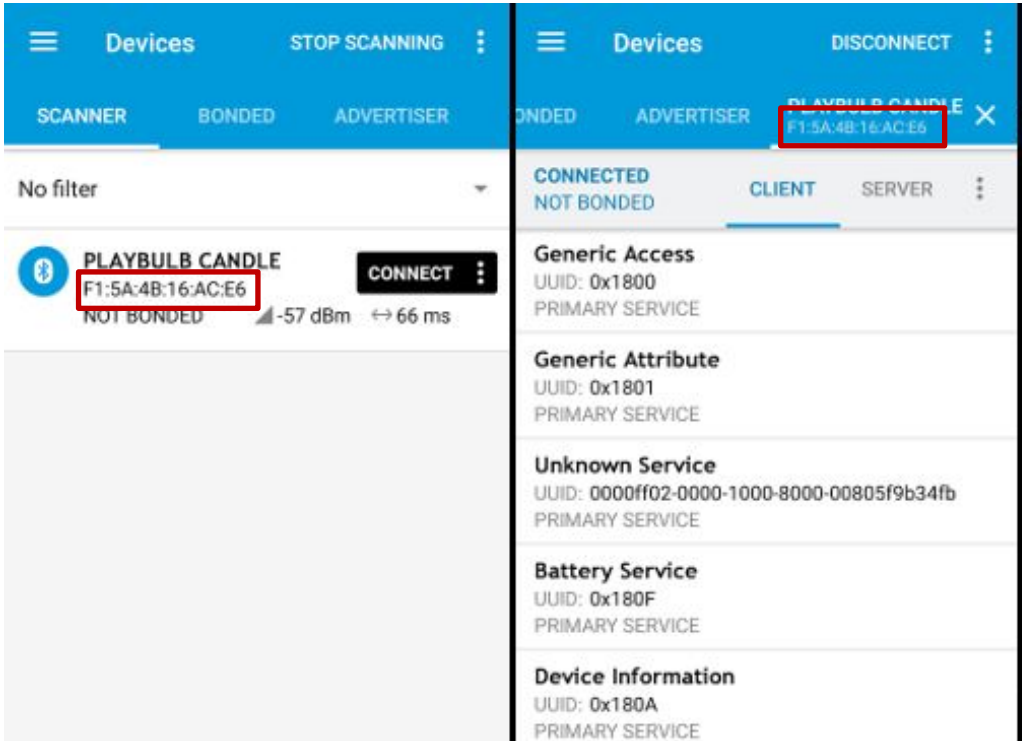
Анализ трафика



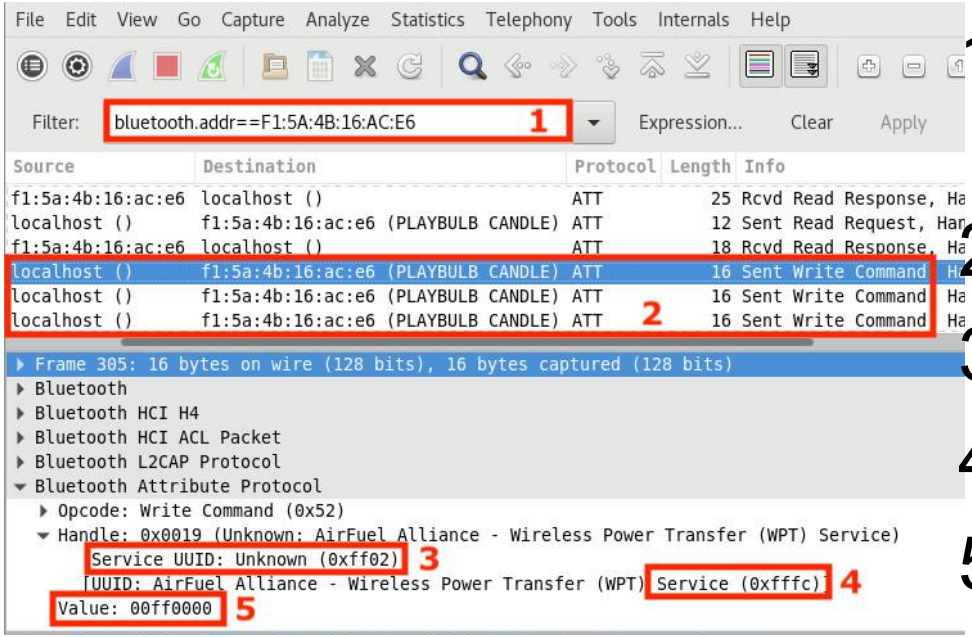
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	controller	host	HCI_EVT	14	Rcvd Sniff Subrating
2	1.044288	controller	host	HCI_EVT	36	Rcvd LE Meta (LE Advertising Report)
3	1.045025	controller	host	HCI_EVT	32	Rcvd LE Meta (LE Advertising Report)
4	1.107638	controller	host	HCI_EVT	36	Rcvd 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)

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

Фильтрация по адресу



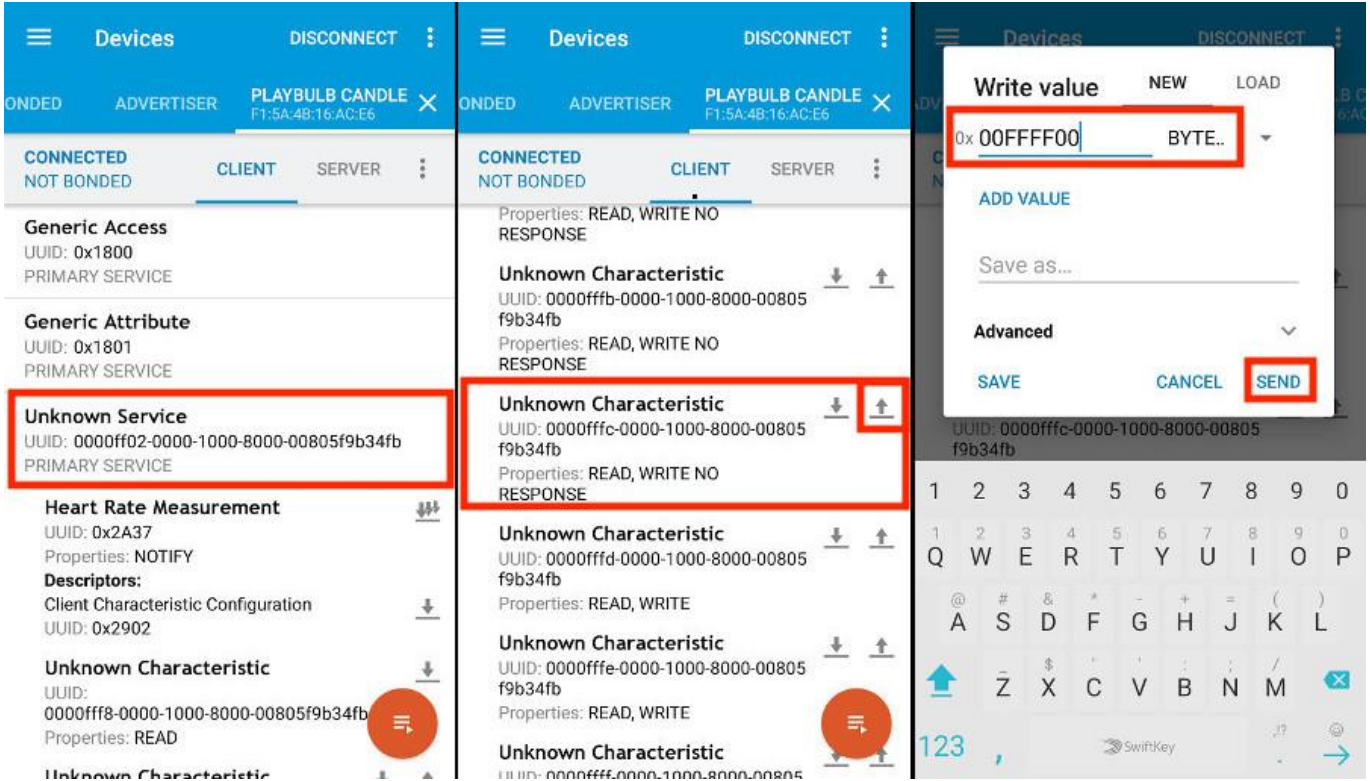
Анализ трафика



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

UFADEVCONF

Проверка

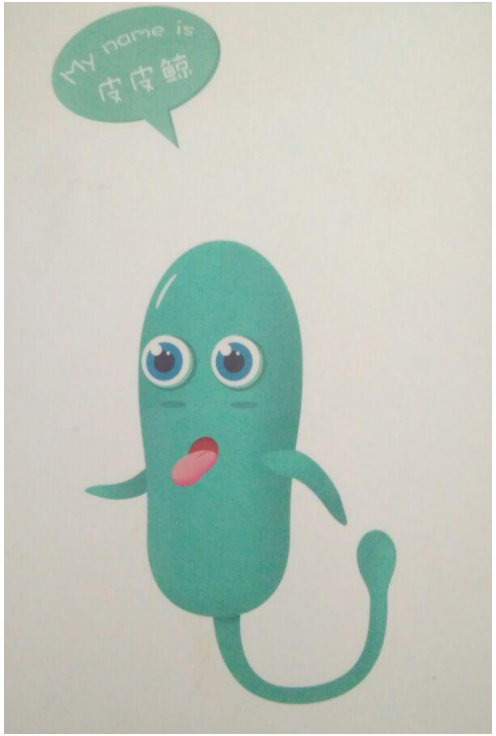


UFADEVCONF

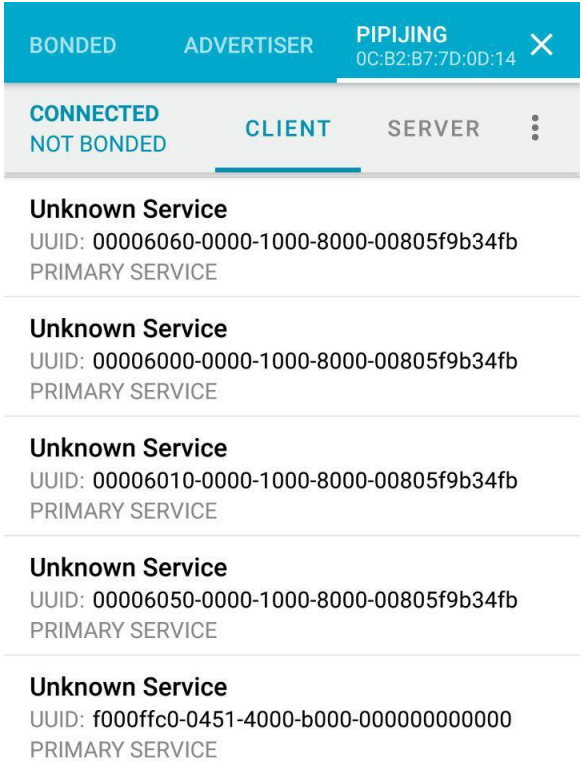
Резюме

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

Реверс вибратора



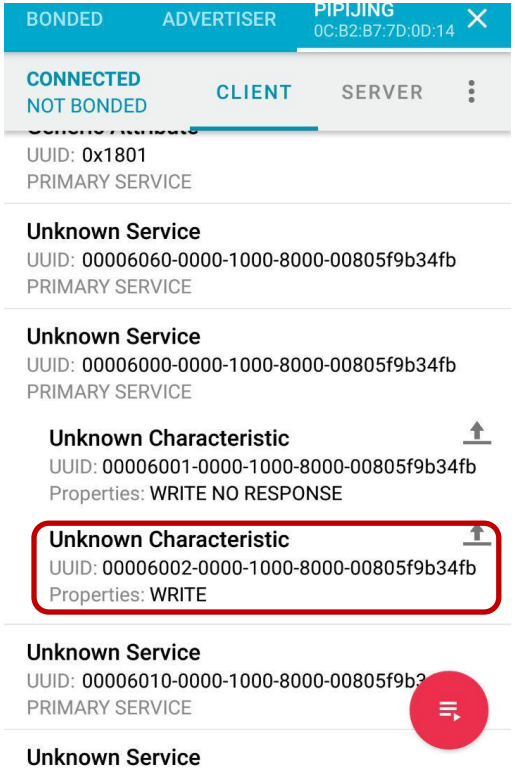
Сервисы девайса



Брутфорс?

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

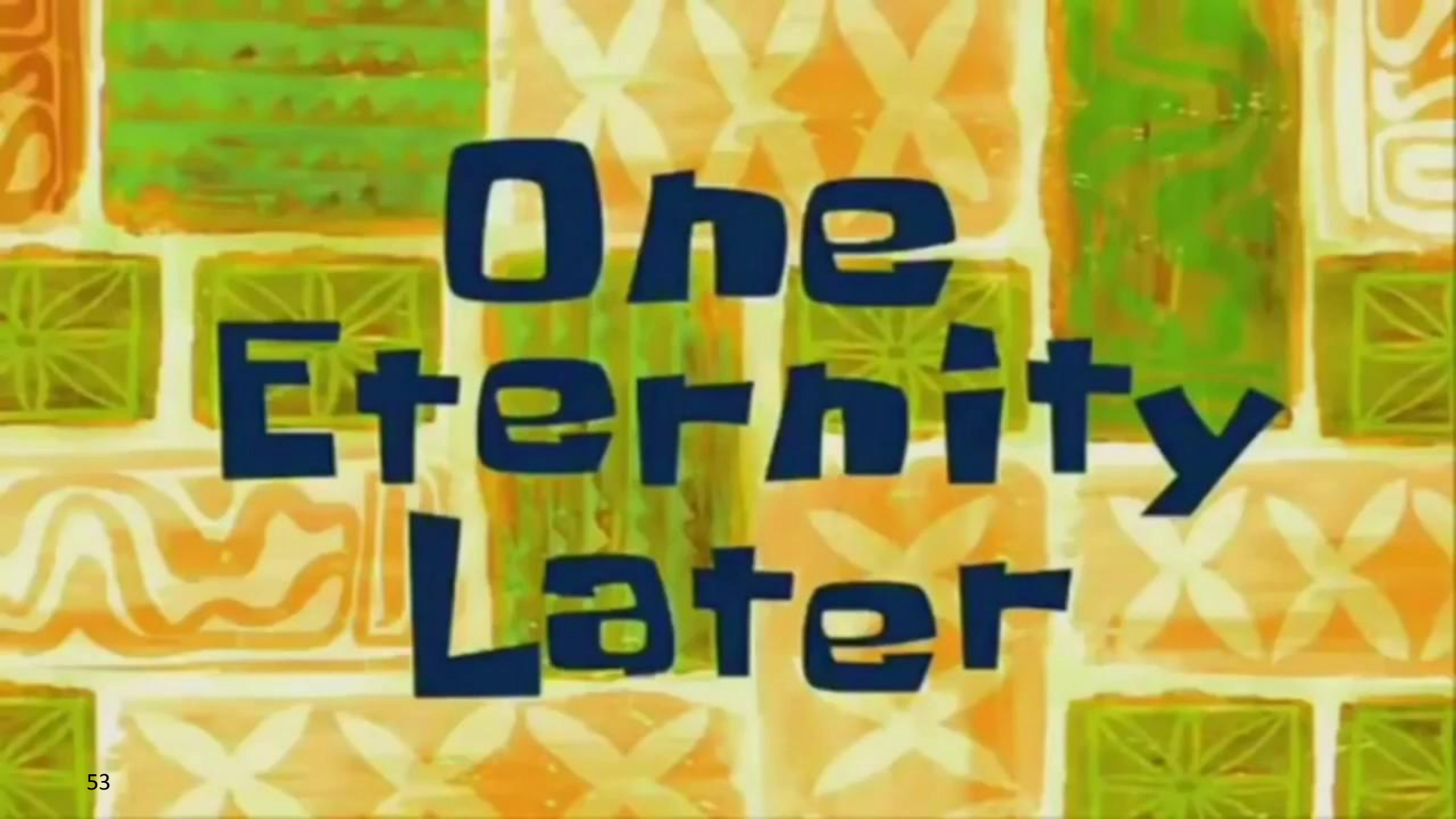
Характеристика для команд



- 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
}
```

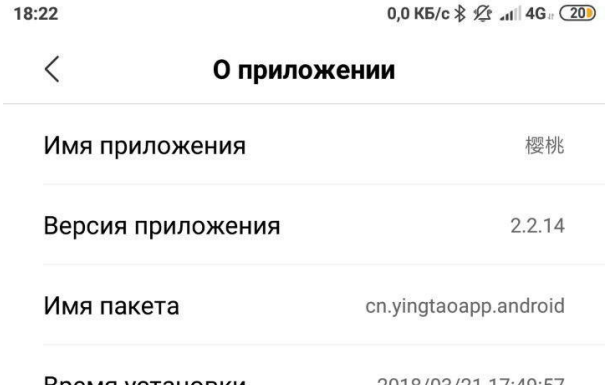

One
Eternity
Later

Брутфорс?

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

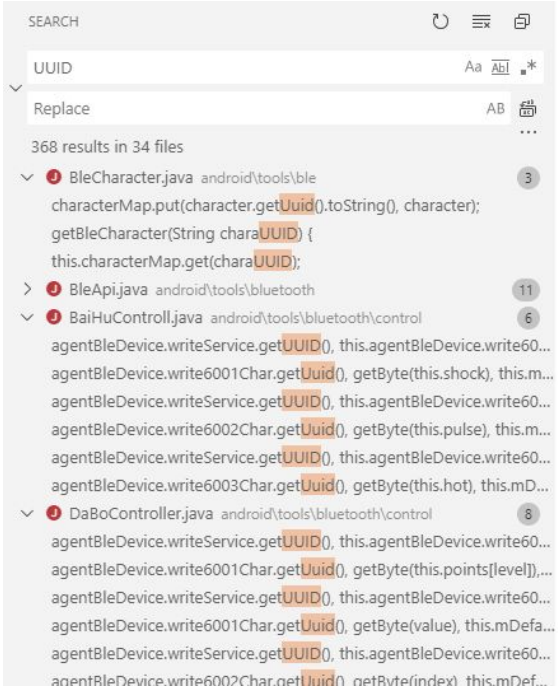
Реверс-инжиниринг apk

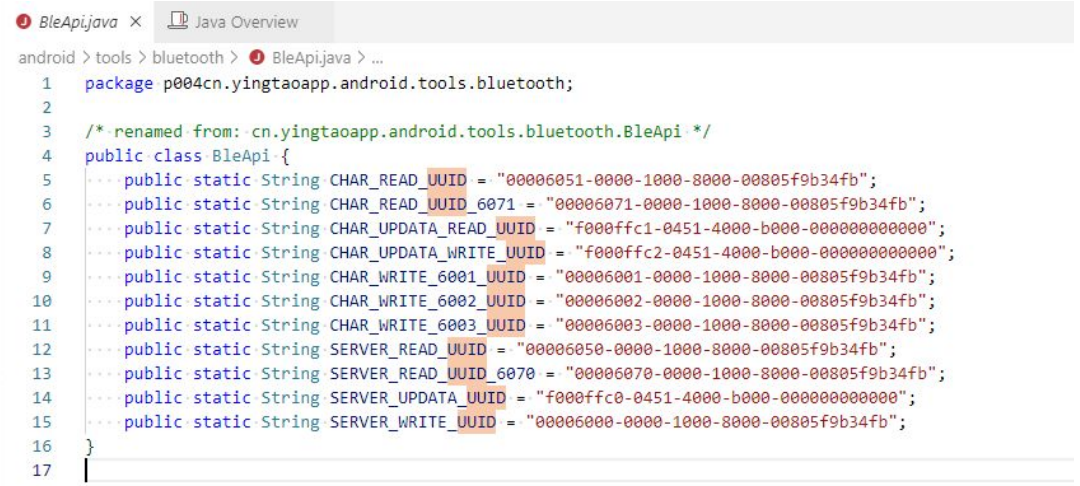
- adb shell pm path cn.yingtaoapp.android
- package:/data/app/cn.yingtaoapp.android/base.apk
- adb pull /data/app/cn.yingtaoapp.android/base.apk
- Декомпиляция apk



UFADEVCONF

Поиск нужного сервиса





UFADEVCONF

Поиск нужного сервиса

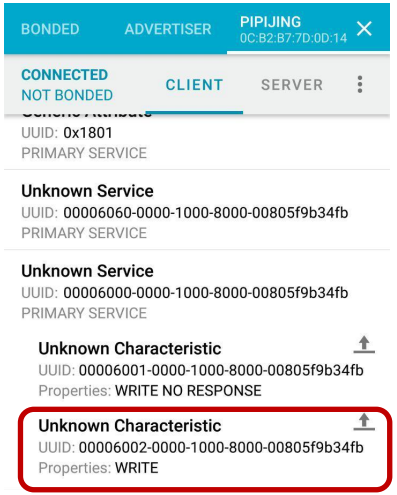
i.java × Java Overview

> 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_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_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";
}
```

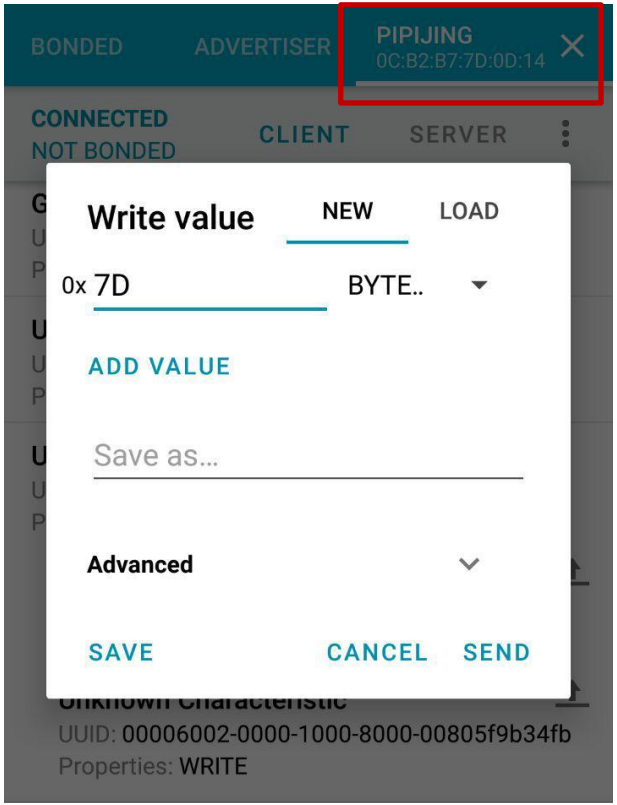
- Характеристики с “Write”



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;
}
```

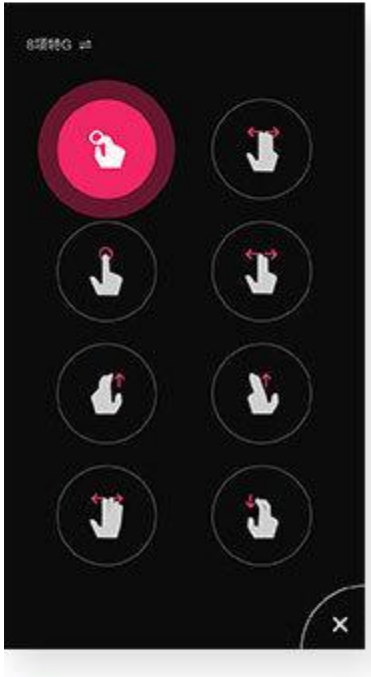
Проверим


BONDED
ADVERTISER
PIPIJING
0C:B2:B7:7D:0D:14
CONNECTED
NOT BONDED
CLIENT
SERVER
Write value
NEW
LOAD
0x 7D
BYTE..
ADD VALUE
Save as...
Advanced
SAVE
CANCEL
SEND
UUID: 00006002-0000-1000-8000-00805f9b34fb
Properties: WRITE

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

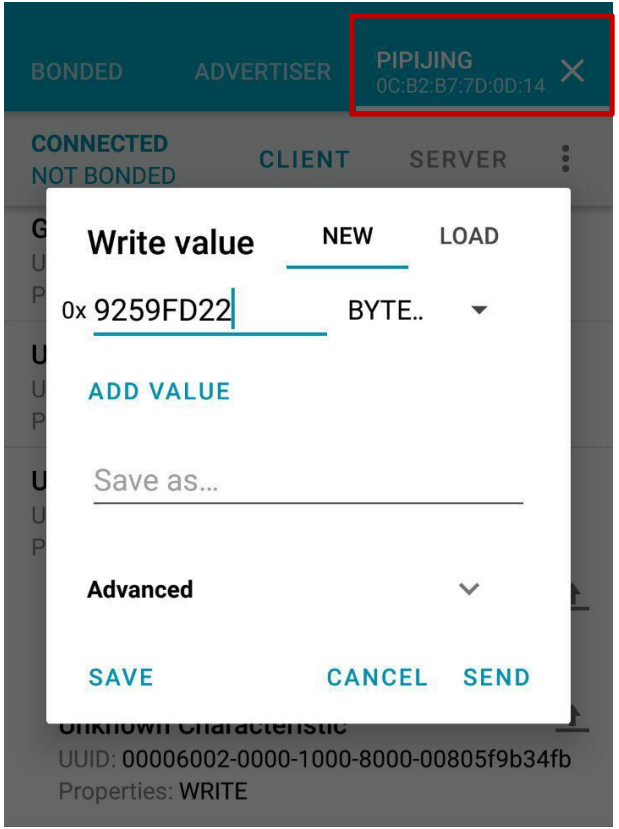
Анализ трафика

1223	798.010920	host	controller	HCI_CMD	29 Sent LE Create Connectio
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 Connectio
1228	818.035288	controller	host	HCI_EVT	7 Rcvd Command Complete (L
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

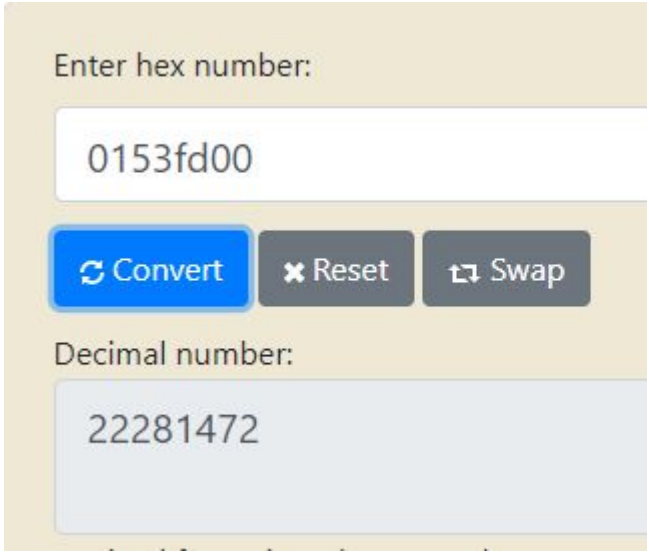
```
> Frame 1225: 4 bytes on wire (32 bits), 4 bytes captured (32 bits)
> Bluetooth
> Bluetooth HCI H4
> Bluetooth HCI Command - Vendor Command 0xfd59
```

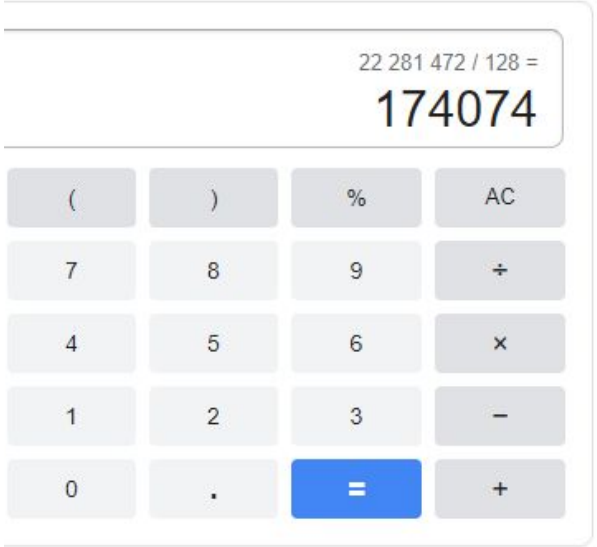
```
0000  01 59 fd 00                                        ·Y··
```

Проверим


BONDED
ADVERTISER
PIPIJING
0C:B2:B7:7D:0D:14
CONNECTED
NOT BONDED
CLIENT
SERVER
Write value
NEW
LOAD
0x 9259FD22
BYTE..
ADD VALUE
Save as...
Advanced
SAVE
CANCEL
SEND
UUID: 00006002-0000-1000-8000-00805f9b34fb
Properties: WRITE

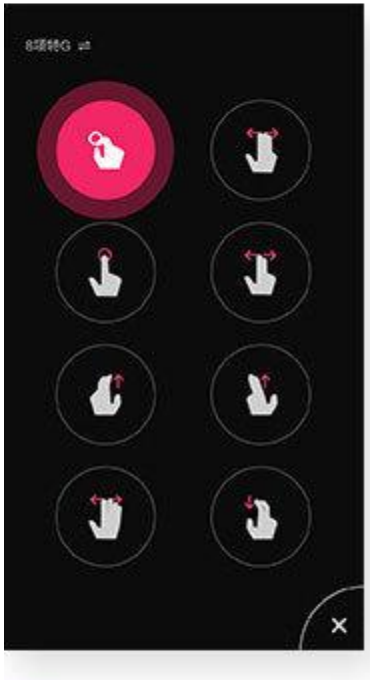
Что за формат?





UFADEVCONF

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,
    private static int[] classicMode6 = {0, 0, 0,
    private static int[] classicMode7 = {0, 100,
    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

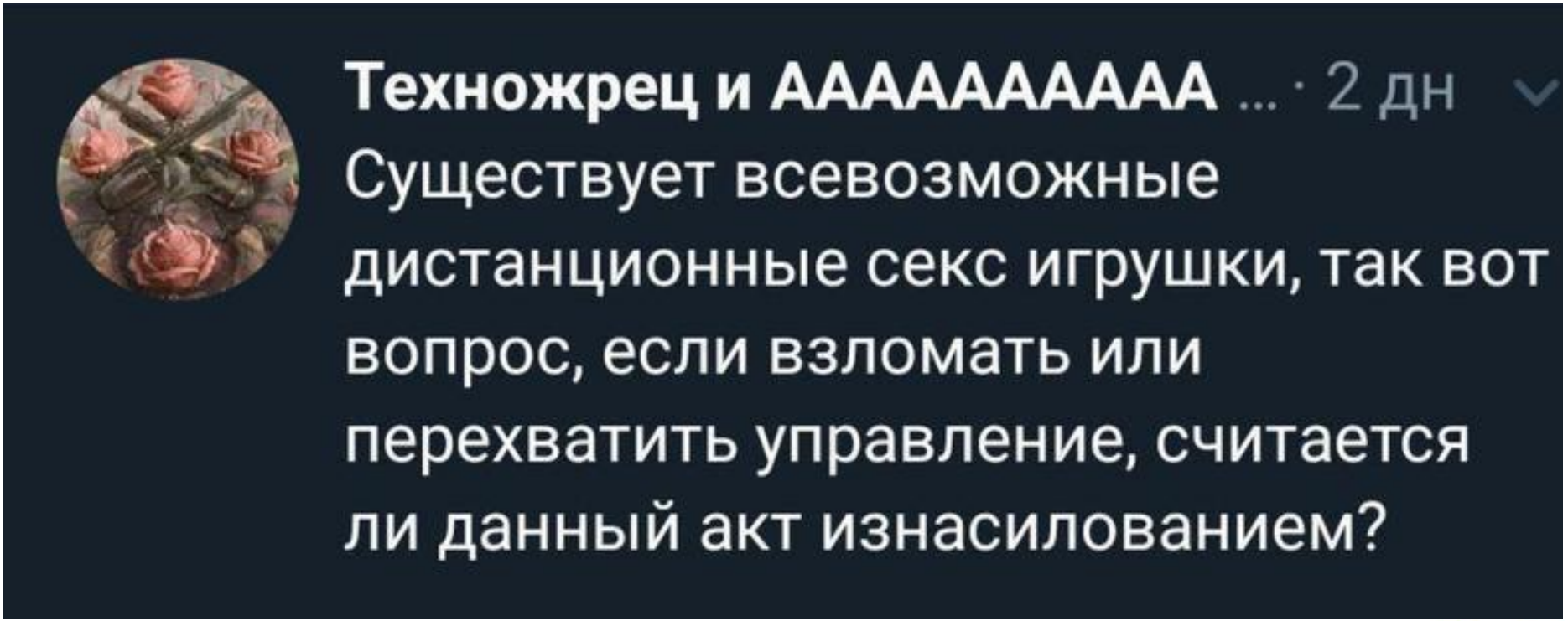
Заключение

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

Спасибо за внимание

Контакты:

- telegram @neargye


Техножрец и АААААААААА ... · 2 дн
Существует всевозможные дистанционные секс игрушки, так вот вопрос, если взломать или перехватить управление, считается ли данный акт изнасилованием?