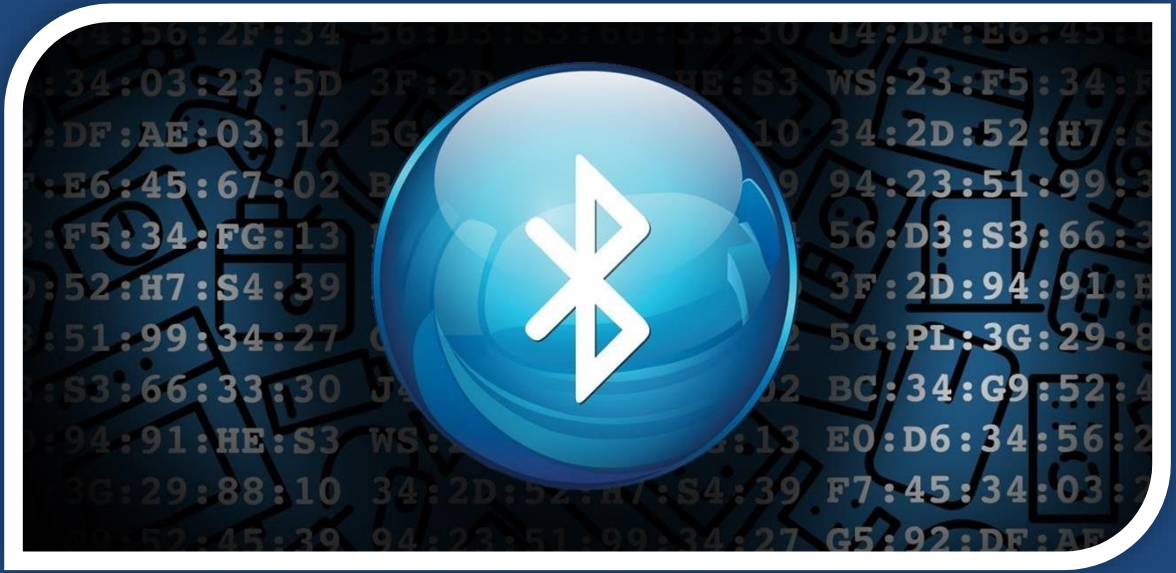


Bluetooth hacking

mongii@grayhash

Bluetooth Hacking 목차

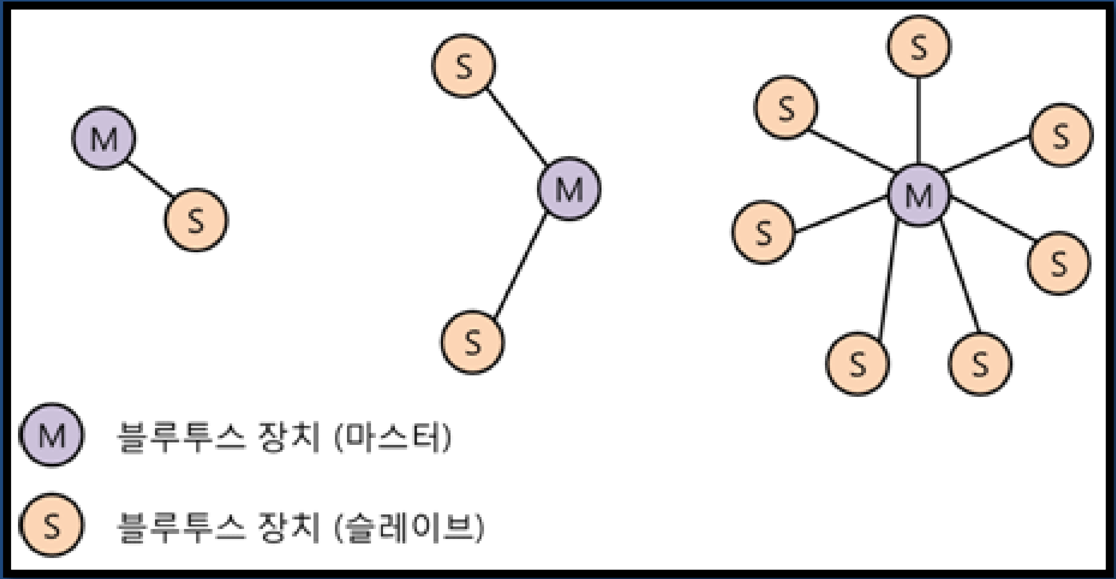
- Bluetooth 기초
- Bluetooth Module 사용 실습
- Bluetooth Packet 분석
- Bluetooth Profile이란?
- 카오디오 장비와 Bluetooth
- 카오디오 Bluetooth의 공격 벡터들
- Bluetooth Packet 변조

Bluetooth 기초

- 무선 데이터 송수신 프로토콜
- 1994년 스웨덴의 에릭슨(Ericsson)사에서 개발
- 10세기 노르웨이와 덴마크를 통일한 바이킹 헤럴드 블루투스(Harald Bluetooth;910~985) 국왕의 이름에서 유래
- 저가, 저전력
- 휴대폰, 노트북, 헤드셋, 차량 등에서 사용
- 통신거리 : 약 10m
- UART Serial 프로토콜의 무선 버전

Master/Slave and Piconet

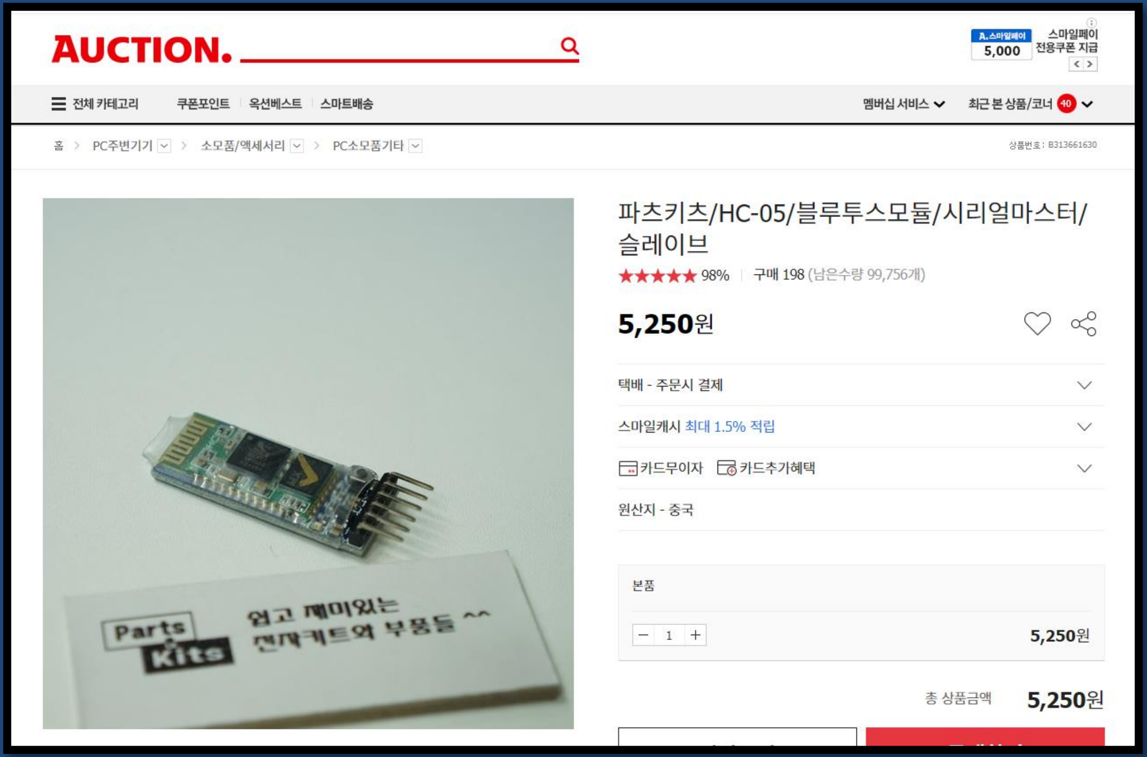
- 하나의 Master에 최대 7개의 Slaves 연결 가능
  - Master : 블루투스 통신의 주체 ex> 휴대폰
  - Slave : 블루투스 기반의 장치 ex> 키보드, 스피커
- Piconet : 하나의 Master를 중심으로 한 Network



Bluetooth Module 사용 실습

Bluetooth Module 소개

- 모델명 : HC-05
- Bluetooth V2.0+EDR (Enhanced Data Rate)
- Master/Slave 겸용
- AT command를 이용하여 제어



상품번호 : B313661630

파츠키츠/HC-05/블루투스모듈/시리얼마스터/슬레이브

★★★★★ 98% | 구매 198 (남은수량 99,756개)

5,250원

택배 - 주문시 결제

스마일캐시 최대 1.5% 적립

카드무이자 카드추가혜택

원산지 - 중국

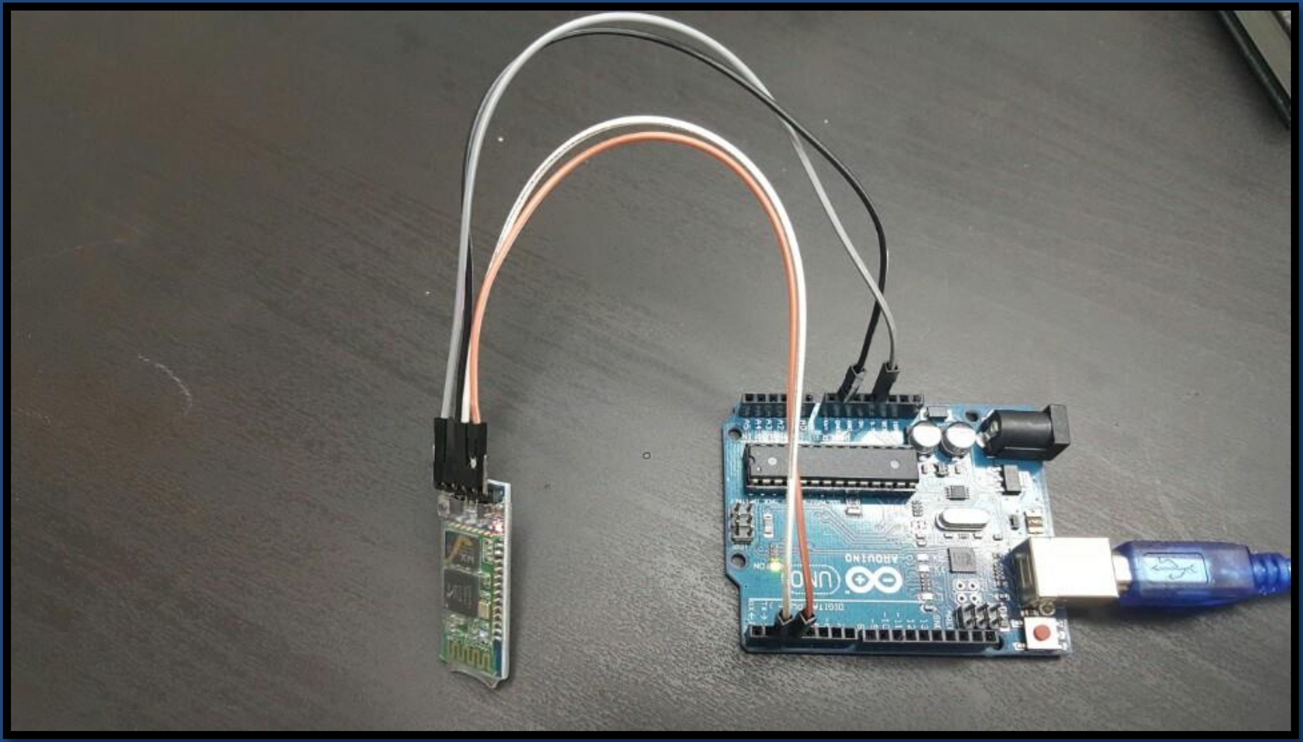
본품

− 1 + 5,250원

총 상품금액 5,250원

Bluetooth Module 연결

- 아두이노 2번핀 → 블루투스 TXD핀
- 아두이노 3번핀 → 블루투스 RXD핀
- 그 외 GND, 3.3V



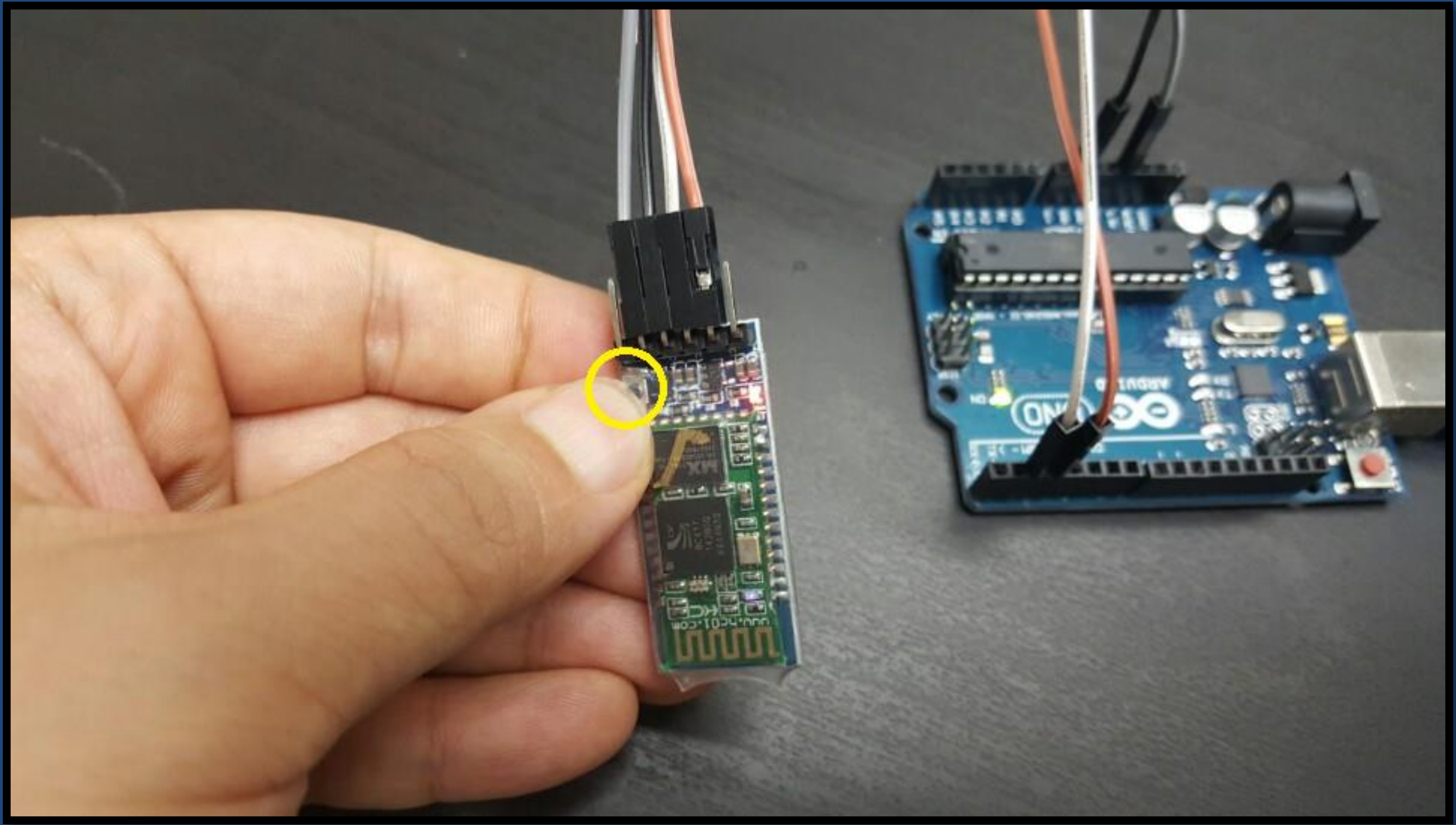
Bluetooth 장치 이름 변경

- 아래 코드의 빨강색 부분을 원하는 대로 변경해 주세요.
- 변경하지 않을 시 기본 이름 : HC-05

```
#include <SoftwareSerial.h>

int ch;
SoftwareSerial BluetoothSerial(2, 3); // RX, TX

void setup()
{
  Serial.begin(9600);
  Serial.println("start");
  BluetoothSerial.begin(9600);

  BluetoothSerial.write("AT+NAME=GOOHONG₩r₩n");
}

void loop()
{
  if(BluetoothSerial.available()){
    ch = BluetoothSerial.read();
    Serial.write(ch);
  }
}
```

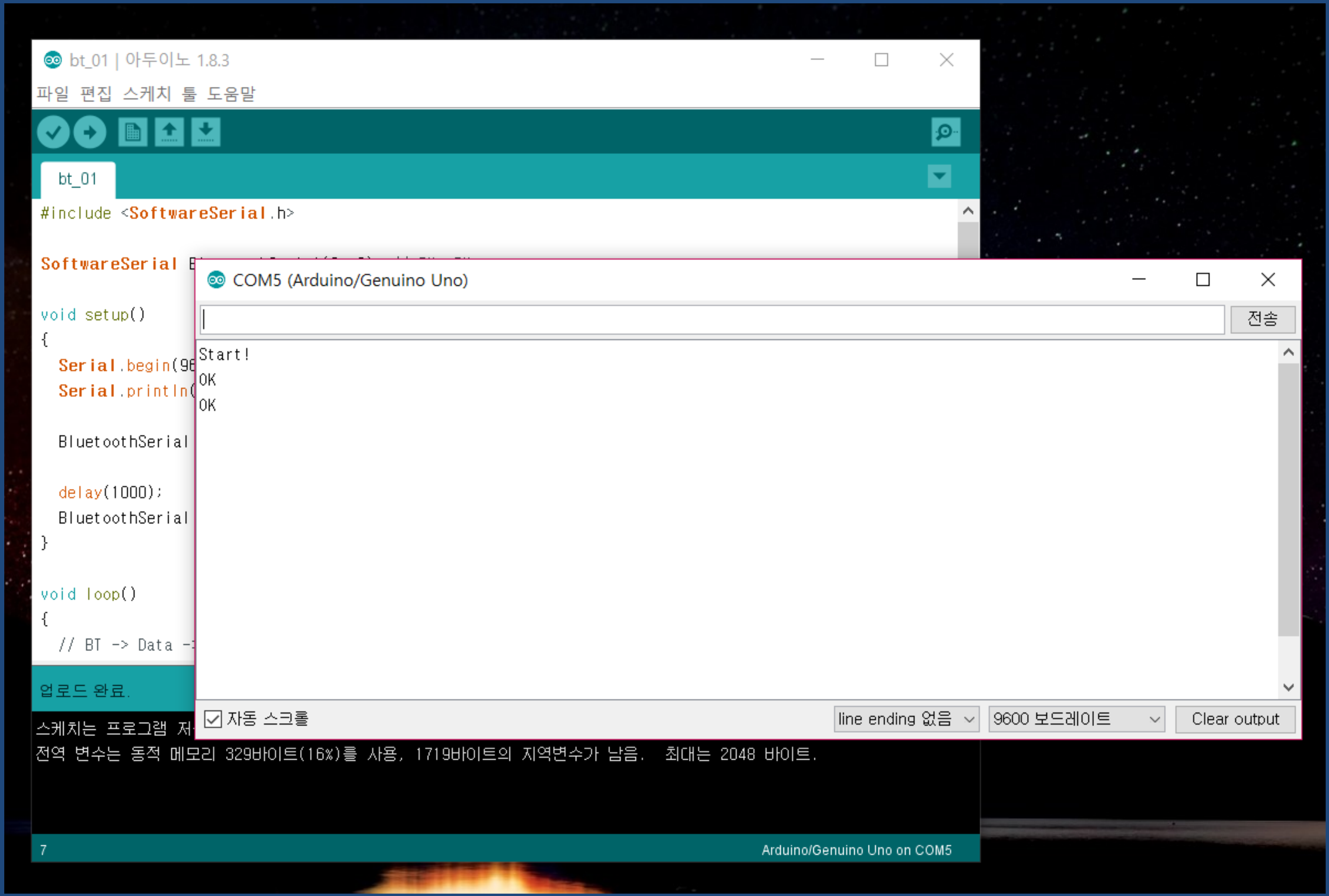
Bluetooth 장치 이름 변경

- 아래 버튼을 눌러 AT 커맨드 수신 모드로 진입
- 동시에 아두이노 -> 툴 -> 시리얼 모니터 실행



Bluetooth 장치 이름 변경

- 아래와 같이 “OK”가 나오면 성공

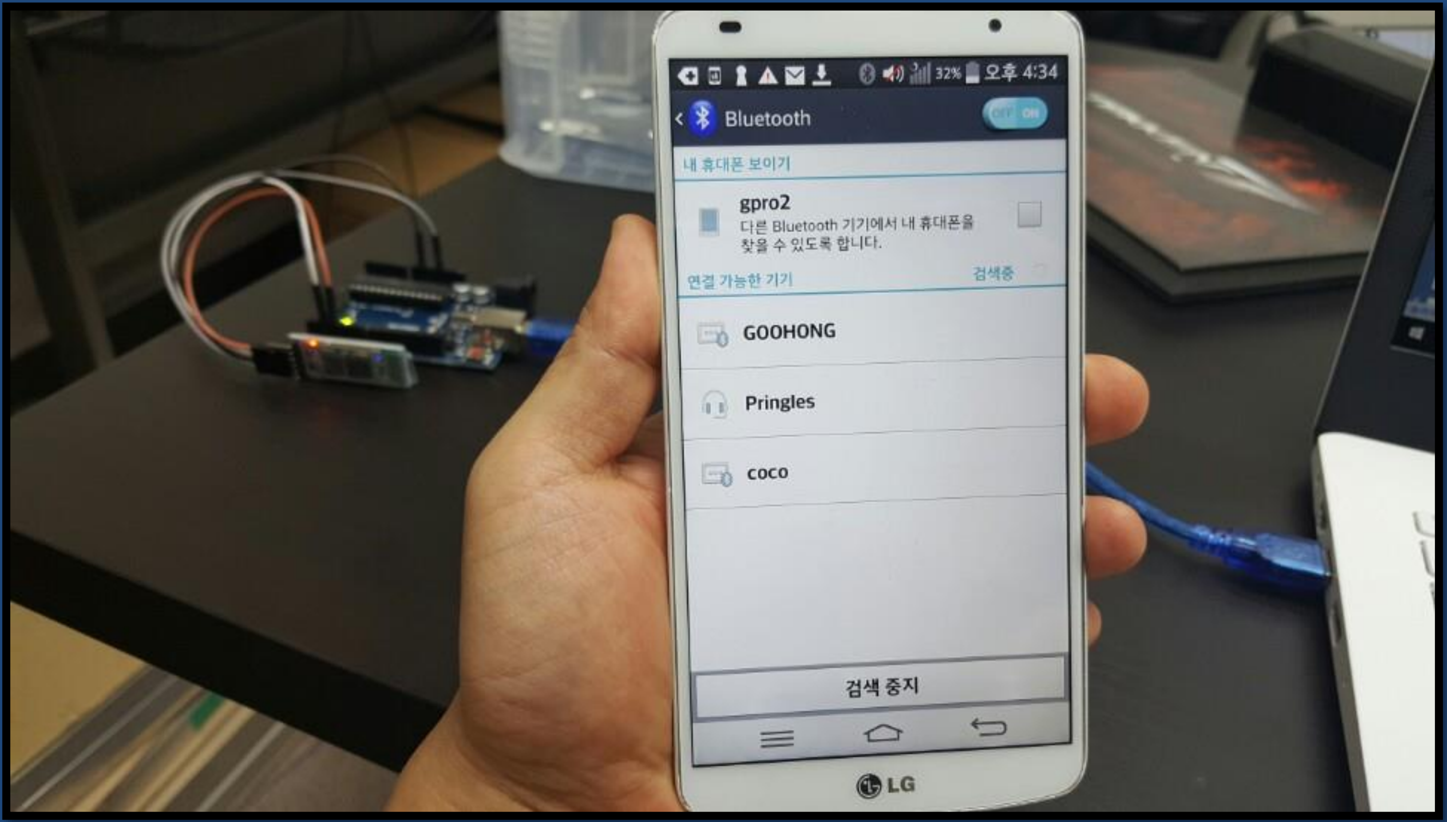


```
#include <SoftwareSerial.h>

SoftwareSerial B

void setup()
{
  Serial.begin(96
  Serial.println(

  BluetoothSerial

  delay(1000);
  BluetoothSerial
}

void loop()
{
  // BT -> Data -
```

```
Start!
OK
OK
```

```
업로드 완료.
스케치는 프로그램 저
전역 변수는 동적 메모리 329바이트(16%)를 사용, 1719바이트의 지역변수가 남음. 최대는 2048 바이트.
```

Bluetooth 장치의 이름 확인



32% 오후 4:34

Bluetooth

내 휴대폰 보이기

gpro2

다른 Bluetooth 기기에서 내 휴대폰을 찾을 수 있도록 합니다. □

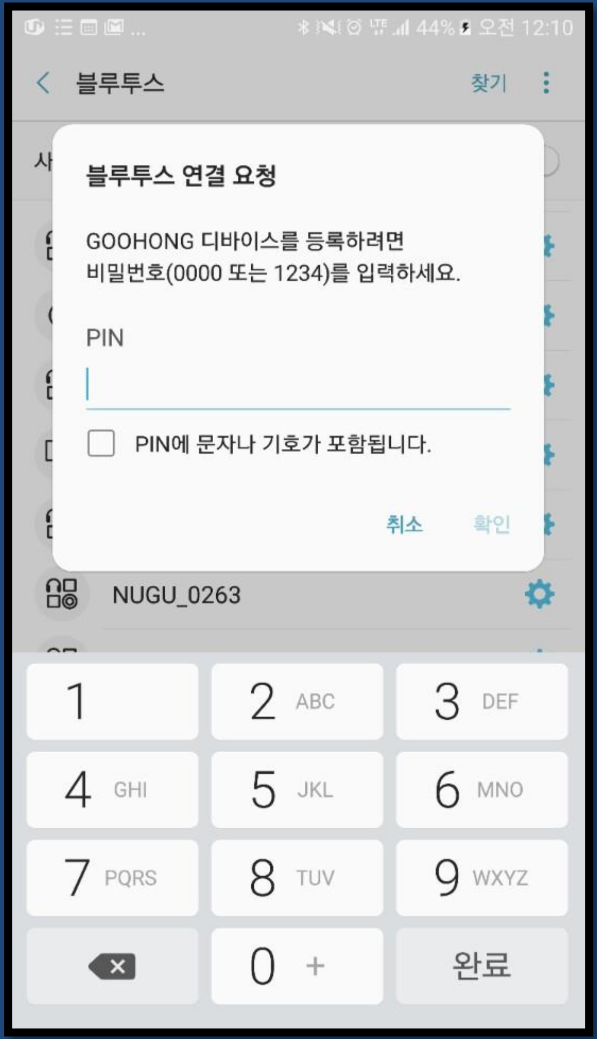
연결 가능한 기기 검색중

GOOHONG

Pringles

coco

장치 연결 (PIN : 1234)

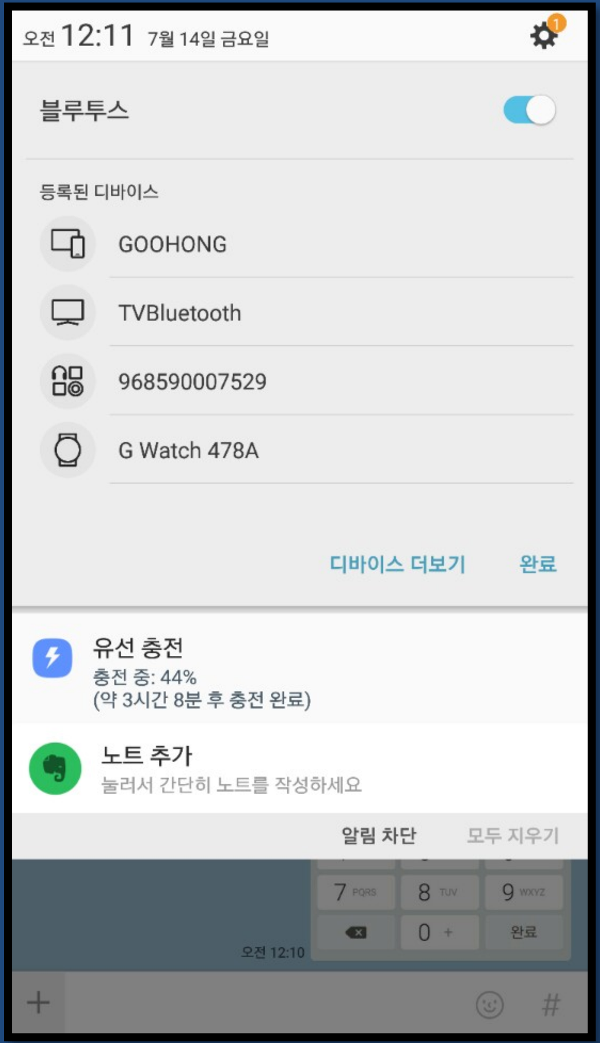


블루투스 연결 요청

GOOHONG 디바이스를 등록하려면
비밀번호(0000 또는 1234)를 입력하세요.

PIN

□ PIN에 문자나 기호가 포함됩니다.



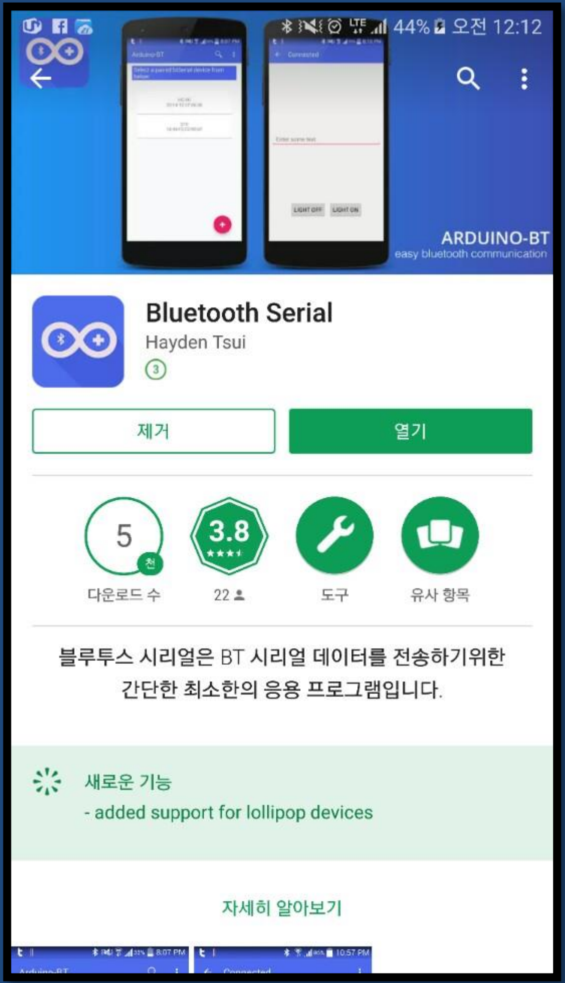
등록된 디바이스

- GOOHONG
- TVBluetooth
- 968590007529
- G Watch 478A

유선 충전
충전 중: 44%
(약 3시간 8분 후 충전 완료)

노트 추가
눌러서 간단히 노트를 작성하세요

Bluetooth Serial 앱 다운로드



44% 오전 12:12

ARDUINO-BT
easy bluetooth communication

Bluetooth Serial
Hayden Tsui

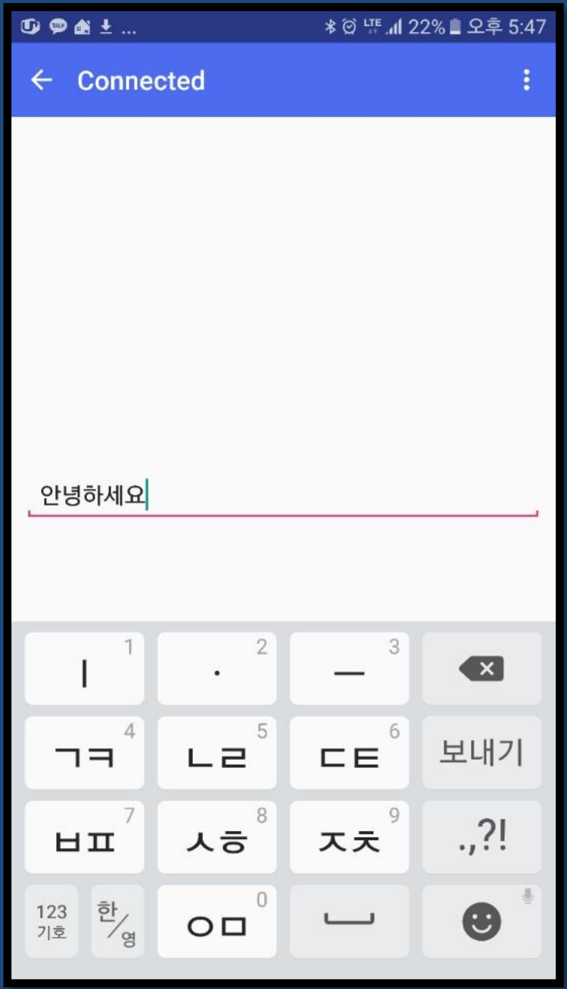
제거 | 열기

5 천 다운로드 수
3.8 22
도구
유사 항목

블루투스 시리얼은 BT 시리얼 데이터를 전송하기위한 간단한 최소한의 응용 프로그램입니다.

새로운 기능
- added support for lollipop devices

자세히 알아보기

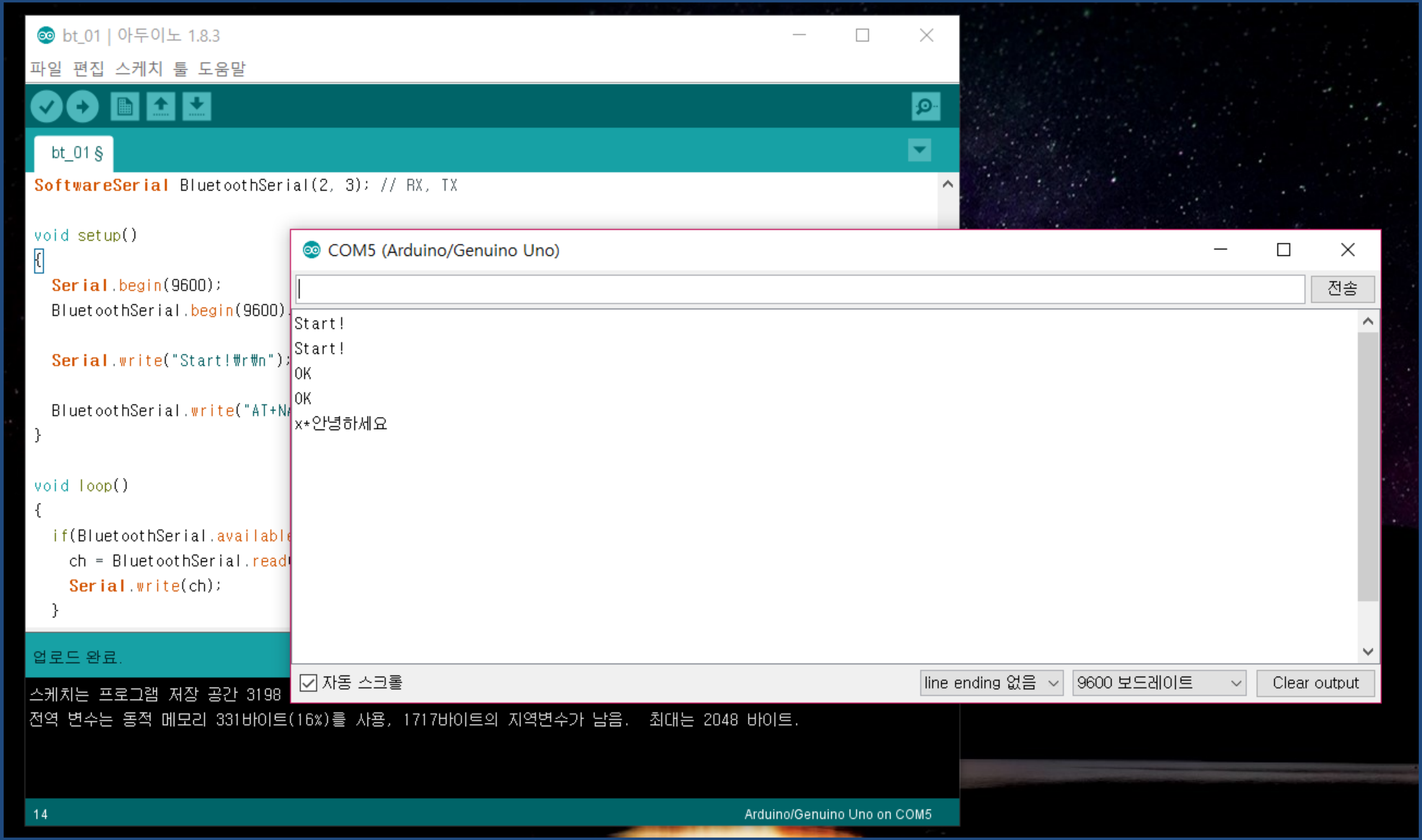


22% 오후 5:47

Connected

안녕하세요

Bluetooth 데이터 송신 테스트



```
SoftwareSerial BluetoothSerial(2, 3); // RX, TX

void setup()
{
  Serial.begin(9600);
  BluetoothSerial.begin(9600).

  Serial.write("Start!₩r₩n");

  BluetoothSerial.write("AT+N
}

void loop()
{
  if(BluetoothSerial.availabl
    ch = BluetoothSerial.read(
    Serial.write(ch);
  }
```

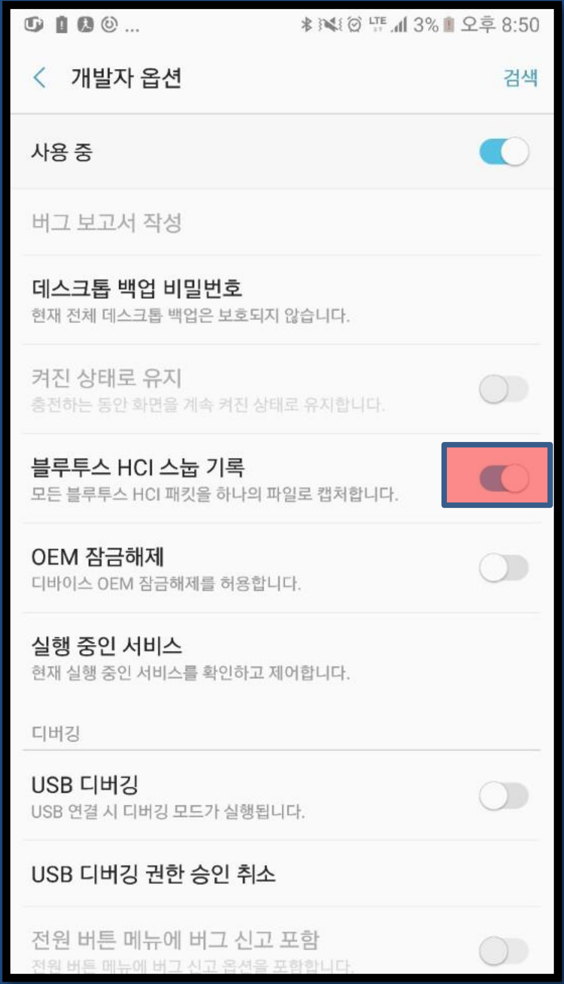
```
Start!
Start!
OK
OK
x*안녕하세요
```

```
업로드 완료.
스케치는 프로그램 저장 공간 3198
전역 변수는 동적 메모리 331바이트(16%)를 사용, 1717바이트의 지역변수가 남음.  최대는 2048 바이트.
```

14   Arduino/Genuino Uno on COM5

Bluetooth Packet 분석

Bluetooth Packet Sniffing



3% 오후 8:50

< 개발자 옵션 검색

사용 중 ●

버그 보고서 작성

데스크톱 백업 비밀번호
현재 전체 데스크톱 백업은 보호되지 않습니다.

켜진 상태로 유지 ○
충전하는 동안 화면을 계속 켜진 상태로 유지합니다.

블루투스 HCI 스눕 기록 ●
모든 블루투스 HCI 패킷을 하나의 파일로 캡처합니다.

OEM 잠금해제 ○
디바이스 OEM 잠금해제를 허용합니다.

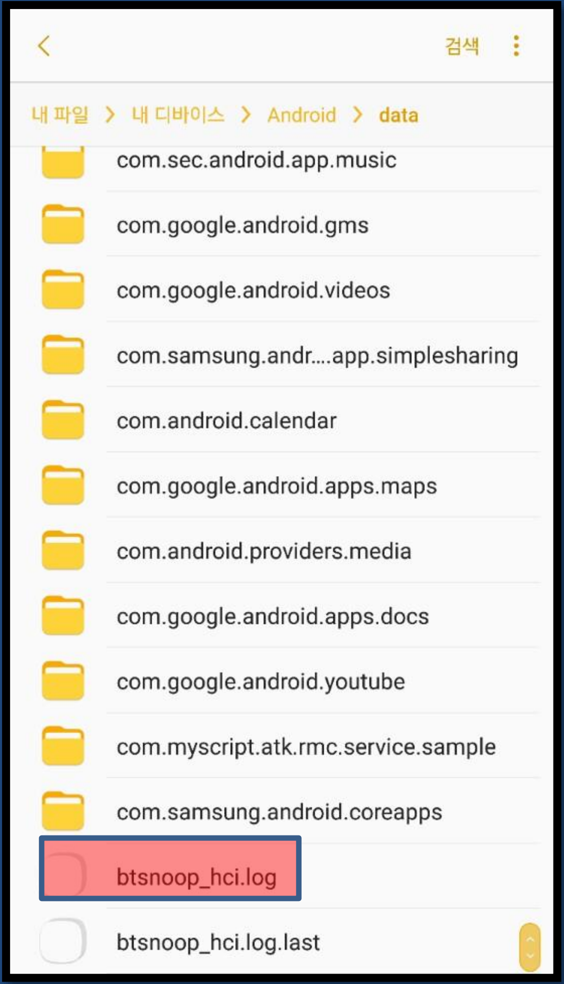
실행 중인 서비스
현재 실행 중인 서비스를 확인하고 제어합니다.

디버깅

USB 디버깅 ○
USB 연결 시 디버깅 모드가 실행됩니다.

USB 디버깅 권한 승인 취소

전원 버튼 메뉴에 버그 신고 포함 ○
전원 버튼 메뉴에 버그 신고 옵션을 포함합니다.

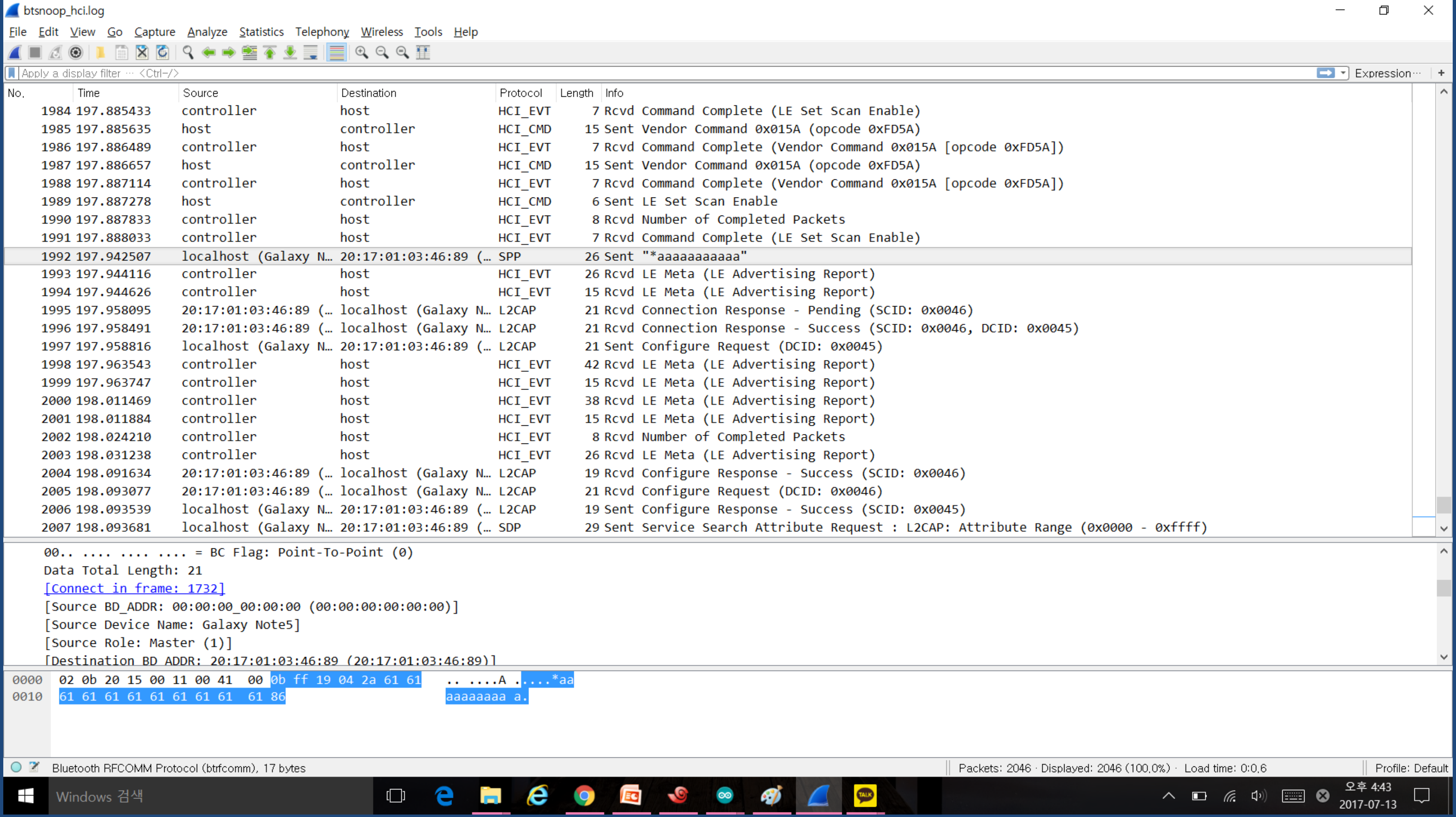


< 검색

내 파일 > 내 디바이스 > Android > data

- com.sec.android.app.music
- com.google.android.gms
- com.google.android.videos
- com.samsung.andr....app.simplesharing
- com.android.calendar
- com.google.android.apps.maps
- com.android.providers.media
- com.google.android.apps.docs
- com.google.android.youtube
- com.myscript.atk.rmc.service.sample
- com.samsung.android.coreapps
- btsnoop_hci.log
- btsnoop_hci.log.last

Bluetooth Packet Sniffing



```
No.  Time        Source                Destination           Protocol  Length Info
1984 197.885433  controller            host                  HCI_EVT      7 Rcvd Command Complete (LE Set Scan Enable)
1985 197.885635  host                  controller            HCI_CMD     15 Sent Vendor Command 0x015A (opcode 0xFD5A)
1986 197.886489  controller            host                  HCI_EVT      7 Rcvd Command Complete (Vendor Command 0x015A [opcode 0xFD5A])
1987 197.886657  host                  controller            HCI_CMD     15 Sent Vendor Command 0x015A (opcode 0xFD5A)
1988 197.887114  controller            host                  HCI_EVT      7 Rcvd Command Complete (Vendor Command 0x015A [opcode 0xFD5A])
1989 197.887278  host                  controller            HCI_CMD      6 Sent LE Set Scan Enable
1990 197.887833  controller            host                  HCI_EVT      8 Rcvd Number of Completed Packets
1991 197.888033  controller            host                  HCI_EVT      7 Rcvd Command Complete (LE Set Scan Enable)
1992 197.942507  localhost (Galaxy N…  20:17:01:03:46:89 (…  SPP         26 Sent "*aaaaaaaaaaa"
1993 197.944116  controller            host                  HCI_EVT     26 Rcvd LE Meta (LE Advertising Report)
1994 197.944626  controller            host                  HCI_EVT     15 Rcvd LE Meta (LE Advertising Report)
1995 197.958095  20:17:01:03:46:89 (…  localhost (Galaxy N…  L2CAP       21 Rcvd Connection Response - Pending (SCID: 0x0046)
1996 197.958491  20:17:01:03:46:89 (…  localhost (Galaxy N…  L2CAP       21 Rcvd Connection Response - Success (SCID: 0x0046, DCID: 0x0045)
1997 197.958816  localhost (Galaxy N…  20:17:01:03:46:89 (…  L2CAP       21 Sent Configure Request (DCID: 0x0045)
1998 197.963543  controller            host                  HCI_EVT     42 Rcvd LE Meta (LE Advertising Report)
1999 197.963747  controller            host                  HCI_EVT     15 Rcvd LE Meta (LE Advertising Report)
2000 198.011469  controller            host                  HCI_EVT     38 Rcvd LE Meta (LE Advertising Report)
2001 198.011884  controller            host                  HCI_EVT     15 Rcvd LE Meta (LE Advertising Report)
2002 198.024210  controller            host                  HCI_EVT      8 Rcvd Number of Completed Packets
2003 198.031238  controller            host                  HCI_EVT     26 Rcvd LE Meta (LE Advertising Report)
2004 198.091634  20:17:01:03:46:89 (…  localhost (Galaxy N…  L2CAP       19 Rcvd Configure Response - Success (SCID: 0x0046)
2005 198.093077  20:17:01:03:46:89 (…  localhost (Galaxy N…  L2CAP       21 Rcvd Configure Request (DCID: 0x0046)
2006 198.093539  localhost (Galaxy N…  20:17:01:03:46:89 (…  L2CAP       19 Sent Configure Response - Success (SCID: 0x0045)
2007 198.093681  localhost (Galaxy N…  20:17:01:03:46:89 (…  SDP         29 Sent Service Search Attribute Request : L2CAP: Attribute Range (0x0000 - 0xffff)
```

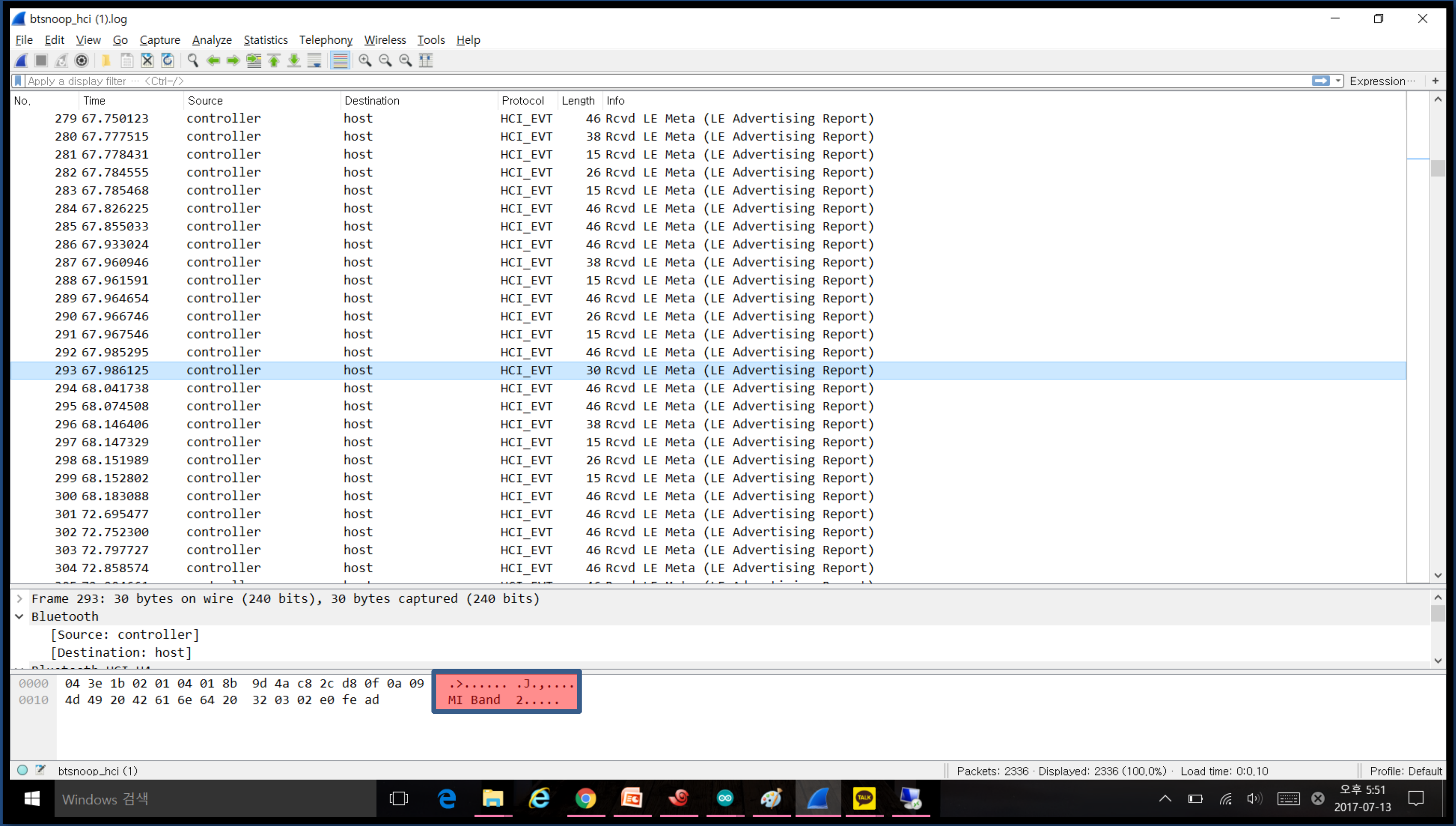
```
    00.. .... .... .... = BC Flag: Point-To-Point (0)
    Data Total Length: 21
    [Connect in frame: 1732]
    [Source BD_ADDR: 00:00:00_00:00:00 (00:00:00:00:00:00)]
    [Source Device Name: Galaxy Note5]
    [Source Role: Master (1)]
    [Destination BD_ADDR: 20:17:01:03:46:89 (20:17:01:03:46:89)]
```

```
0000  02 0b 20 15 00 11 00 41  00 0b ff 19 04 2a 61 61   .. ....A .....*aa
0010  61 61 61 61 61 61 61 61  61 86                     aaaaaaaa a.
```

Bluetooth RFCOMM Protocol (btrfcomm), 17 bytes | Packets: 2046 · Displayed: 2046 (100.0%) · Load time: 0:0.6 | Profile: Default

평상시의 Bluetooth 패킷들

- 자신을 알리는(Advertising) 다수의 기기들



btsnoop_hci (1).log
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

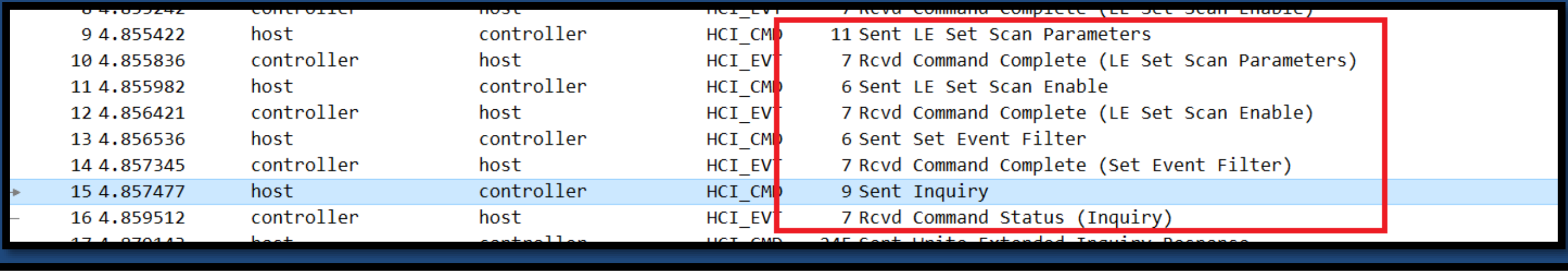
```
No.  Time       Source      Destination  Protocol  Length  Info
 279 67.750123  controller  host         HCI_EVT       46  Rcvd LE Meta (LE Advertising Report)
 280 67.777515  controller  host         HCI_EVT       38  Rcvd LE Meta (LE Advertising Report)
 281 67.778431  controller  host         HCI_EVT       15  Rcvd LE Meta (LE Advertising Report)
 282 67.784555  controller  host         HCI_EVT       26  Rcvd LE Meta (LE Advertising Report)
 283 67.785468  controller  host         HCI_EVT       15  Rcvd LE Meta (LE Advertising Report)
 284 67.826225  controller  host         HCI_EVT       46  Rcvd LE Meta (LE Advertising Report)
 285 67.855033  controller  host         HCI_EVT       46  Rcvd LE Meta (LE Advertising Report)
 286 67.933024  controller  host         HCI_EVT       46  Rcvd LE Meta (LE Advertising Report)
 287 67.960946  controller  host         HCI_EVT       38  Rcvd LE Meta (LE Advertising Report)
 288 67.961591  controller  host         HCI_EVT       15  Rcvd LE Meta (LE Advertising Report)
 289 67.964654  controller  host         HCI_EVT       46  Rcvd LE Meta (LE Advertising Report)
 290 67.966746  controller  host         HCI_EVT       26  Rcvd LE Meta (LE Advertising Report)
 291 67.967546  controller  host         HCI_EVT       15  Rcvd LE Meta (LE Advertising Report)
 292 67.985295  controller  host         HCI_EVT       46  Rcvd LE Meta (LE Advertising Report)
 293 67.986125  controller  host         HCI_EVT       30  Rcvd LE Meta (LE Advertising Report)
 294 68.041738  controller  host         HCI_EVT       46  Rcvd LE Meta (LE Advertising Report)
 295 68.074508  controller  host         HCI_EVT       46  Rcvd LE Meta (LE Advertising Report)
 296 68.146406  controller  host         HCI_EVT       38  Rcvd LE Meta (LE Advertising Report)
 297 68.147329  controller  host         HCI_EVT       15  Rcvd LE Meta (LE Advertising Report)
 298 68.151989  controller  host         HCI_EVT       26  Rcvd LE Meta (LE Advertising Report)
 299 68.152802  controller  host         HCI_EVT       15  Rcvd LE Meta (LE Advertising Report)
 300 68.183088  controller  host         HCI_EVT       46  Rcvd LE Meta (LE Advertising Report)
 301 72.695477  controller  host         HCI_EVT       46  Rcvd LE Meta (LE Advertising Report)
 302 72.752300  controller  host         HCI_EVT       46  Rcvd LE Meta (LE Advertising Report)
 303 72.797727  controller  host         HCI_EVT       46  Rcvd LE Meta (LE Advertising Report)
 304 72.858574  controller  host         HCI_EVT       46  Rcvd LE Meta (LE Advertising Report)
```

```
> Frame 293: 30 bytes on wire (240 bits), 30 bytes captured (240 bits)
v Bluetooth
    [Source: controller]
    [Destination: host]
```

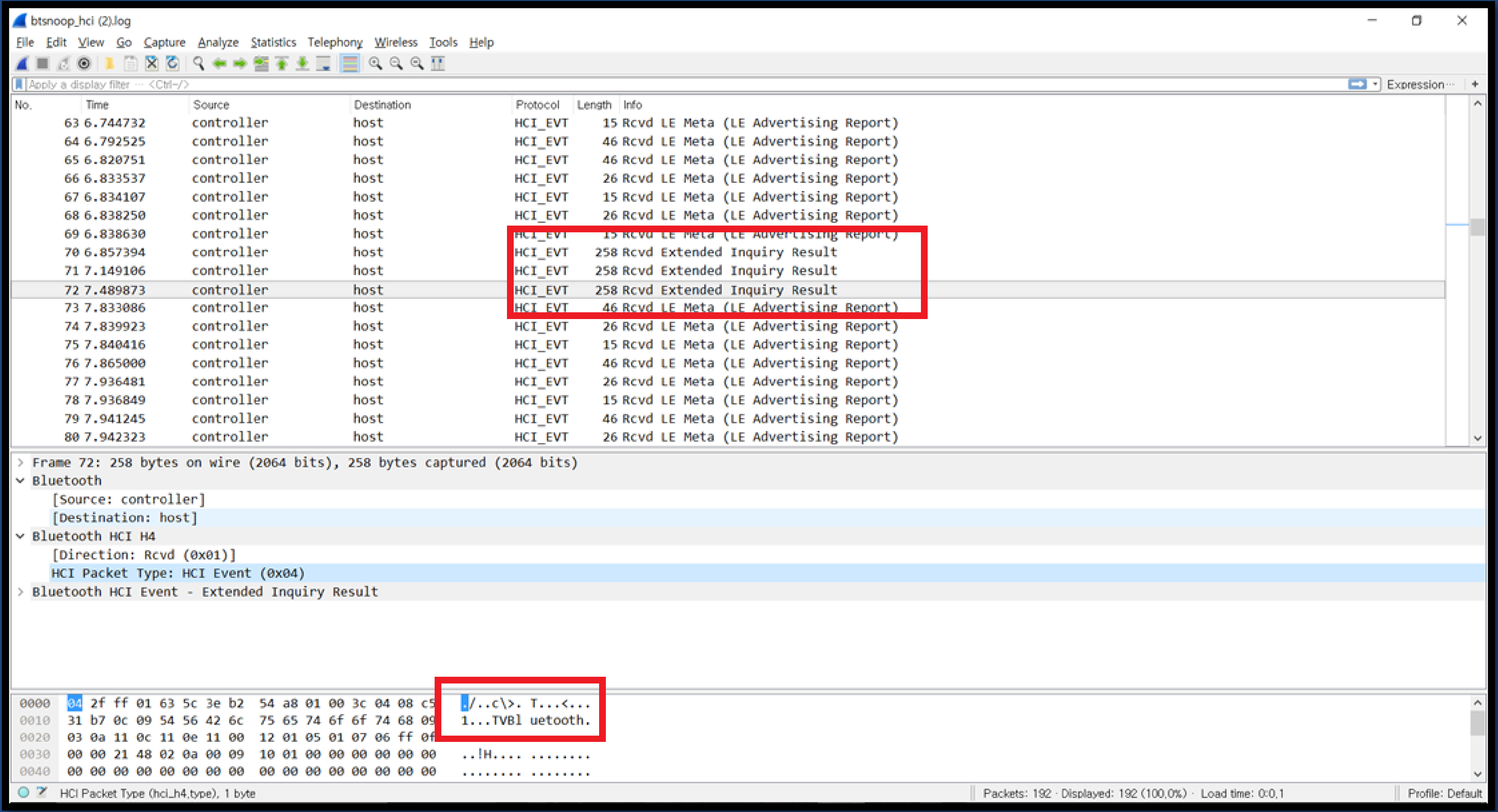
```
0000  04 3e 1b 02 01 04 01 8b  9d 4a c8 2c d8 0f 0a 09   .>...... .J.,....
0010  4d 49 20 42 61 6e 64 20  32 03 02 e0 fe ad         MI Band  2.....
```

btsnoop_hci (1) | Packets: 2336 · Displayed: 2336 (100.0%) · Load time: 0:0.10 | Profile: Default

주변 장치 Scanning



```
 8 4.855242  controller  host        HCI_EVT   7 Rcvd Command Complete (LE Set Scan Enable)
 9 4.855422  host        controller  HCI_CMD  11 Sent LE Set Scan Parameters
10 4.855836  controller  host        HCI_EVT   7 Rcvd Command Complete (LE Set Scan Parameters)
11 4.855982  host        controller  HCI_CMD   6 Sent LE Set Scan Enable
12 4.856421  controller  host        HCI_EVT   7 Rcvd Command Complete (LE Set Scan Enable)
13 4.856536  host        controller  HCI_CMD   6 Sent Set Event Filter
14 4.857345  controller  host        HCI_EVT   7 Rcvd Command Complete (Set Event Filter)
15 4.857477  host        controller  HCI_CMD   9 Sent Inquiry
16 4.859512  controller  host        HCI_EVT   7 Rcvd Command Status (Inquiry)
17 4.870143  host        controller  HCI_CMD 245 Sent Write Extended Inquiry Response
```



btsnoop_hci (2).log

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…

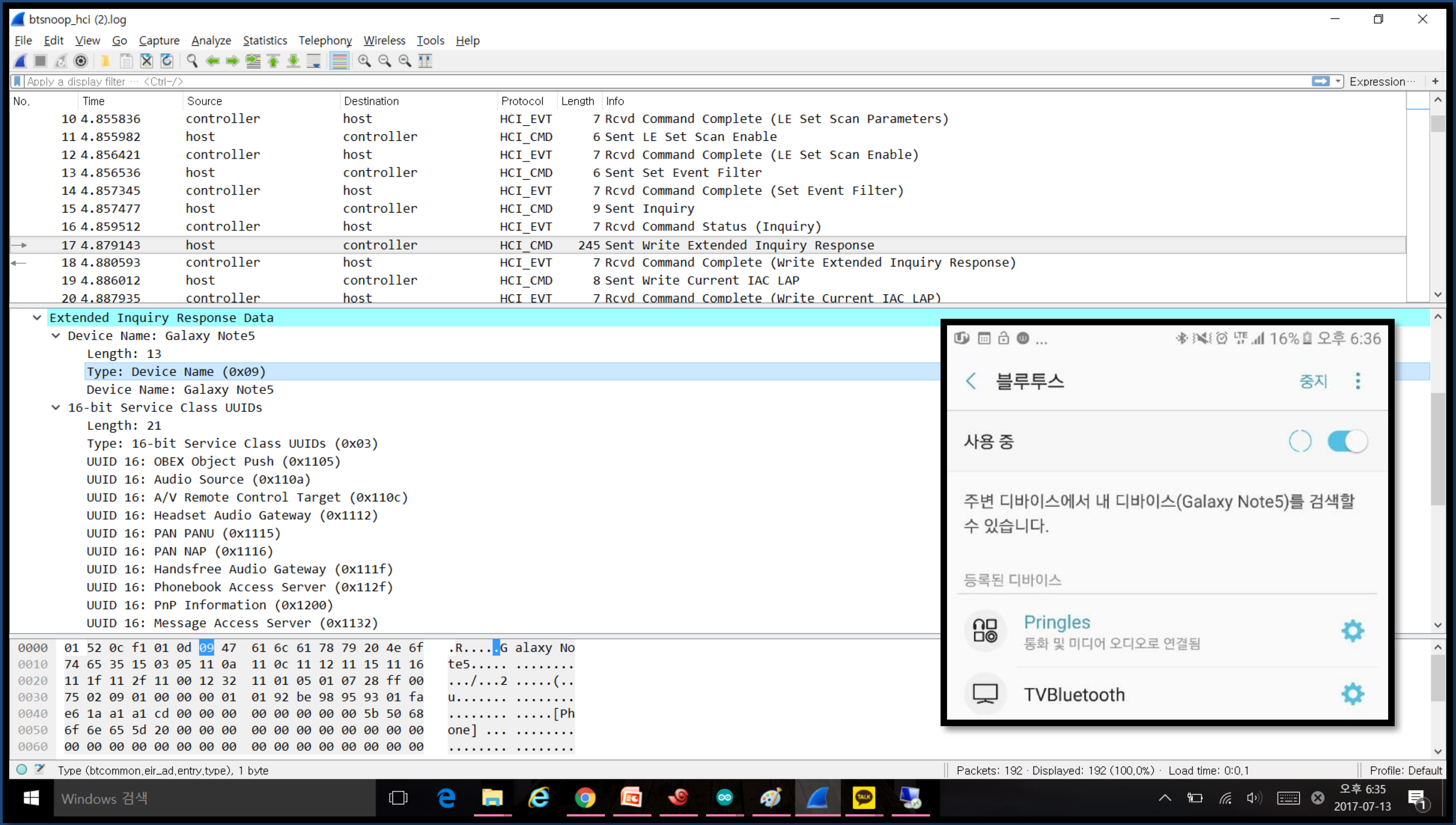
```
No.  Time      Source      Destination  Protocol  Length  Info
63 6.744732   controller  host         HCI_EVT    15 Rcvd LE Meta (LE Advertising Report)
64 6.792525   controller  host         HCI_EVT    46 Rcvd LE Meta (LE Advertising Report)
65 6.820751   controller  host         HCI_EVT    46 Rcvd LE Meta (LE Advertising Report)
66 6.833537   controller  host         HCI_EVT    26 Rcvd LE Meta (LE Advertising Report)
67 6.834107   controller  host         HCI_EVT    15 Rcvd LE Meta (LE Advertising Report)
68 6.838250   controller  host         HCI_EVT    26 Rcvd LE Meta (LE Advertising Report)
69 6.838630   controller  host         HCI_EVT    15 Rcvd LE Meta (LE Advertising Report)
70 6.857394   controller  host         HCI_EVT   258 Rcvd Extended Inquiry Result
71 7.149106   controller  host         HCI_EVT   258 Rcvd Extended Inquiry Result
72 7.489873   controller  host         HCI_EVT   258 Rcvd Extended Inquiry Result
73 7.833086   controller  host         HCI_EVT    46 Rcvd LE Meta (LE Advertising Report)
74 7.839923   controller  host         HCI_EVT    26 Rcvd LE Meta (LE Advertising Report)
75 7.840416   controller  host         HCI_EVT    15 Rcvd LE Meta (LE Advertising Report)
76 7.865000   controller  host         HCI_EVT    46 Rcvd LE Meta (LE Advertising Report)
77 7.936481   controller  host         HCI_EVT    26 Rcvd LE Meta (LE Advertising Report)
78 7.936849   controller  host         HCI_EVT    15 Rcvd LE Meta (LE Advertising Report)
79 7.941245   controller  host         HCI_EVT    46 Rcvd LE Meta (LE Advertising Report)
80 7.942323   controller  host         HCI_EVT    26 Rcvd LE Meta (LE Advertising Report)
```

```
> Frame 72: 258 bytes on wire (2064 bits), 258 bytes captured (2064 bits)
v Bluetooth
    [Source: controller]
    [Destination: host]
v Bluetooth HCI H4
    [Direction: Rcvd (0x01)]
    HCI Packet Type: HCI Event (0x04)
> Bluetooth HCI Event - Extended Inquiry Result
```

```
0000  04 2f ff 01 63 5c 3e b2  54 a8 01 00 3c 04 08 c5   ./..c\>. T...<...
0010  31 b7 0c 09 54 56 42 6c  75 65 74 6f 6f 74 68 09   1...TVBl uetooth.
0020  03 0a 11 0c 11 0e 11 00  12 01 05 01 07 06 ff 0f
0030  00 00 21 48 02 0a 00 09  10 01 00 00 00 00 00 00   ..!H.... ........
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

HCI Packet Type (hci_h4.type), 1 byte | Packets: 192 · Displayed: 192 (100.0%) · Load time: 0:0.1 | Profile: Default

자신의 정보를 보내는 부분


btsnoop_hci (2).log
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…

```
No.  Time      Source      Destination  Protocol  Length  Info
  10 4.855836  controller  host         HCI_EVT        7  Rcvd Command Complete (LE Set Scan Parameters)
  11 4.855982  host        controller   HCI_CMD        6  Sent LE Set Scan Enable
  12 4.856421  controller  host         HCI_EVT        7  Rcvd Command Complete (LE Set Scan Enable)
  13 4.856536  host        controller   HCI_CMD        6  Sent Set Event Filter
  14 4.857345  controller  host         HCI_EVT        7  Rcvd Command Complete (Set Event Filter)
  15 4.857477  host        controller   HCI_CMD        9  Sent Inquiry
  16 4.859512  controller  host         HCI_EVT        7  Rcvd Command Status (Inquiry)
→ 17 4.879143  host        controller   HCI_CMD      245  Sent Write Extended Inquiry Response
← 18 4.880593  controller  host         HCI_EVT        7  Rcvd Command Complete (Write Extended Inquiry Response)
  19 4.886012  host        controller   HCI_CMD        8  Sent Write Current IAC LAP
  20 4.887935  controller  host         HCI_EVT        7  Rcvd Command Complete (Write Current IAC LAP)
```

```
∨ Extended Inquiry Response Data
  ∨ Device Name: Galaxy Note5
      Length: 13
      Type: Device Name (0x09)
      Device Name: Galaxy Note5
  ∨ 16-bit Service Class UUIDs
      Length: 21
      Type: 16-bit Service Class UUIDs (0x03)
      UUID 16: OBEX Object Push (0x1105)
      UUID 16: Audio Source (0x110a)
      UUID 16: A/V Remote Control Target (0x110c)
      UUID 16: Headset Audio Gateway (0x1112)
      UUID 16: PAN PANU (0x1115)
      UUID 16: PAN NAP (0x1116)
      UUID 16: Handsfree Audio Gateway (0x111f)
      UUID 16: Phonebook Access Server (0x112f)
      UUID 16: PnP Information (0x1200)
      UUID 16: Message Access Server (0x1132)
```

```
0000  01 52 0c f1 01 0d 09 47  61 6c 61 78 79 20 4e 6f   .R.....G alaxy No
0010  74 65 35 15 03 05 11 0a  11 0c 11 12 11 15 11 16   te5..... ........
0020  11 1f 11 2f 11 00 12 32  11 01 05 01 07 28 ff 00   .../...2 .....(..
0030  75 02 09 01 00 00 00 01  01 92 be 98 95 93 01 fa   u....... ........
0040  e6 1a a1 a1 cd 00 00 00  00 00 00 00 00 5b 50 68   ........ .....[Ph
0050  6f 6e 65 5d 20 00 00 00  00 00 00 00 00 00 00 00   one] ... ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

Type (btcommon.eir_ad.entry.type), 1 byte | Packets: 192 · Displayed: 192 (100.0%) · Load time: 0:0.1 | Profile: Default

사용 중

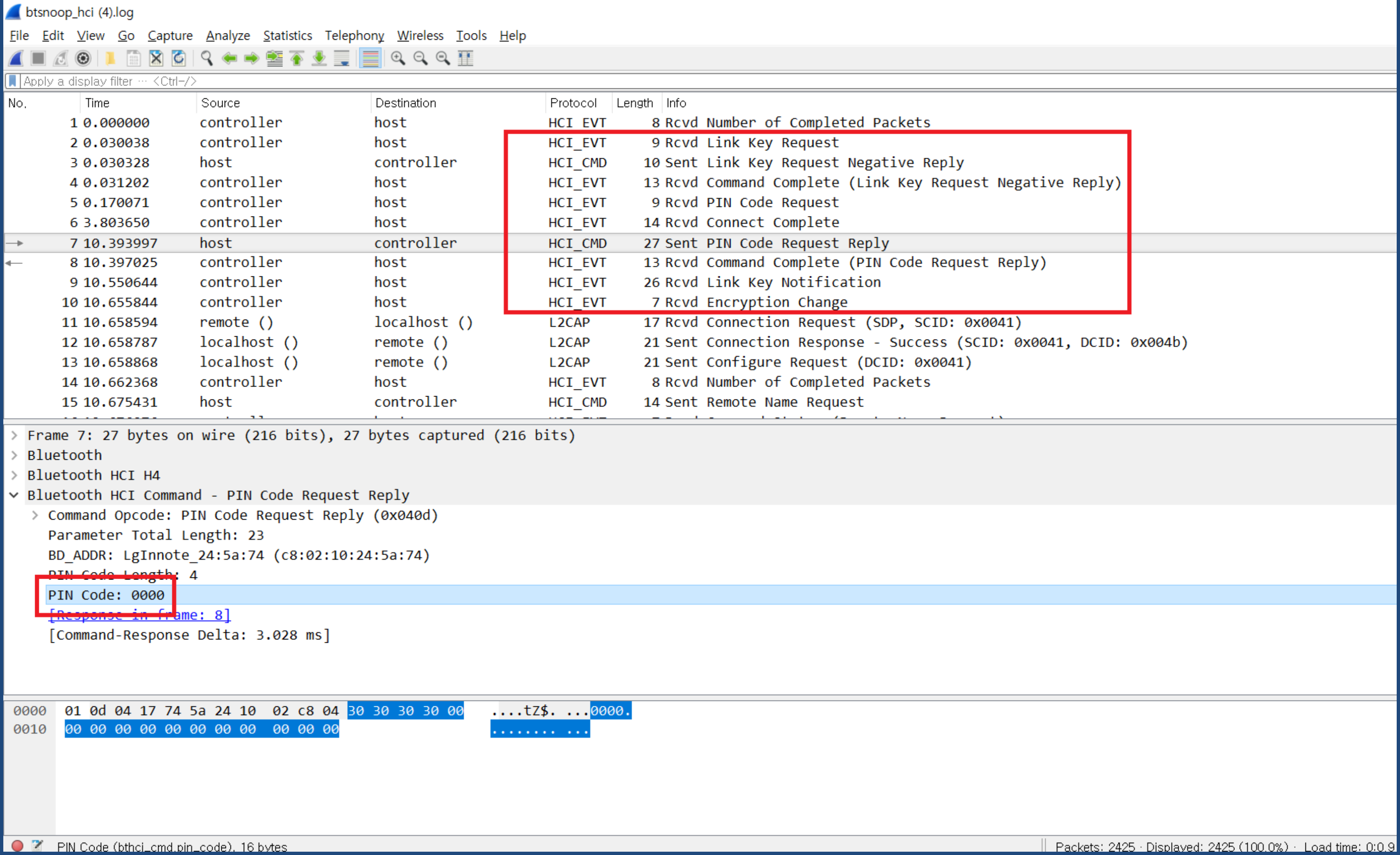
주변 디바이스에서 내 디바이스(Galaxy Note5)를 검색할 수 있습니다.

등록된 디바이스

Pringles
통화 및 미디어 오디오로 연결됨

TVBluetooth

Bluetooth Paring


btsnoop_hci (4).log
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

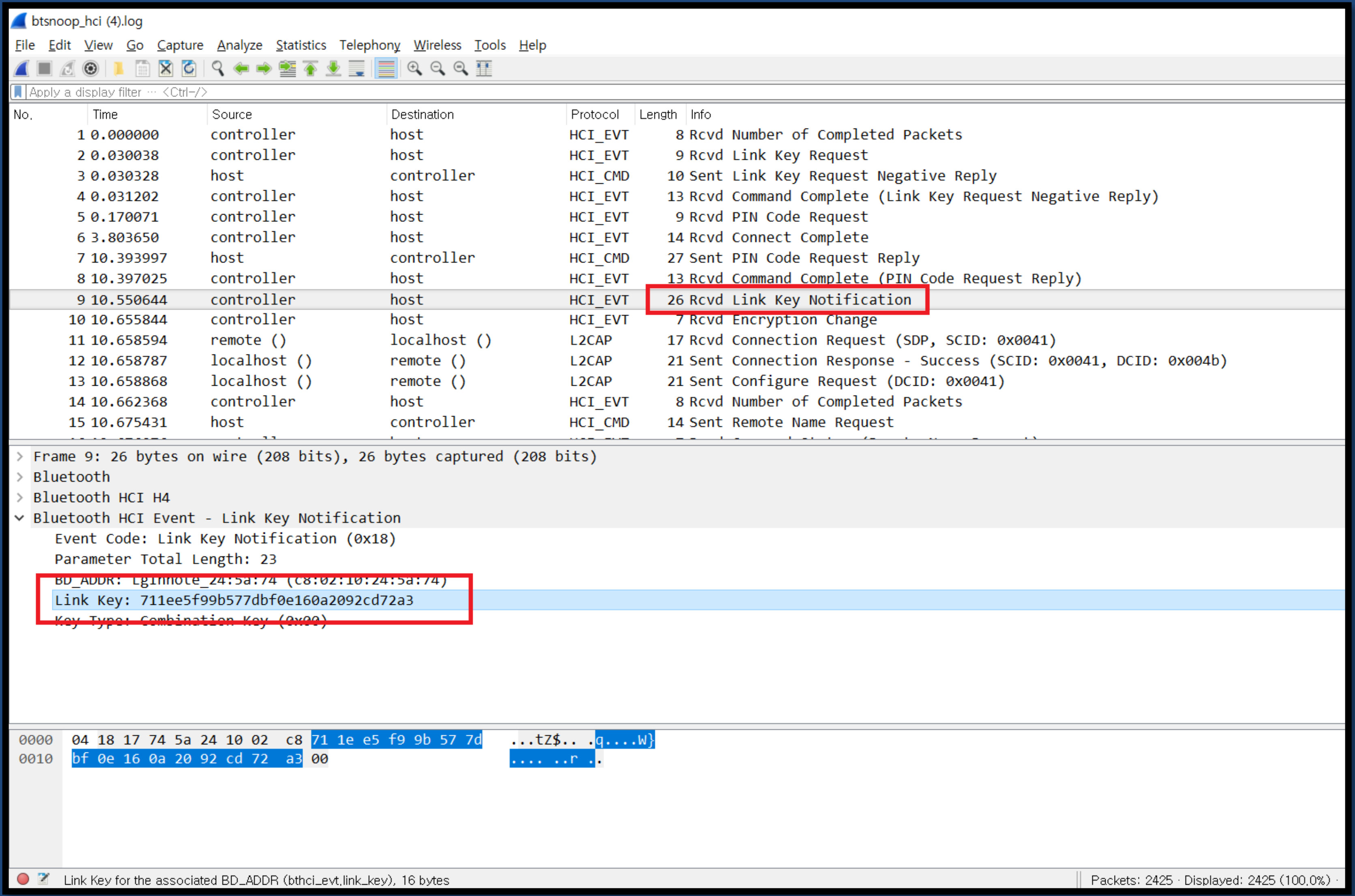
```
No.   Time        Source        Destination   Protocol  Length  Info
    1 0.000000    controller    host          HCI_EVT        8  Rcvd Number of Completed Packets
    2 0.030038    controller    host          HCI_EVT        9  Rcvd Link Key Request
    3 0.030328    host          controller    HCI_CMD       10  Sent Link Key Request Negative Reply
    4 0.031202    controller    host          HCI_EVT       13  Rcvd Command Complete (Link Key Request Negative Reply)
    5 0.170071    controller    host          HCI_EVT        9  Rcvd PIN Code Request
    6 3.803650    controller    host          HCI_EVT       14  Rcvd Connect Complete
    7 10.393997   host          controller    HCI_CMD       27  Sent PIN Code Request Reply
    8 10.397025   controller    host          HCI_EVT       13  Rcvd Command Complete (PIN Code Request Reply)
    9 10.550644   controller    host          HCI_EVT       26  Rcvd Link Key Notification
   10 10.655844   controller    host          HCI_EVT        7  Rcvd Encryption Change
   11 10.658594   remote ()     localhost ()  L2CAP         17  Rcvd Connection Request (SDP, SCID: 0x0041)
   12 10.658787   localhost ()  remote ()     L2CAP         21  Sent Connection Response - Success (SCID: 0x0041, DCID: 0x004b)
   13 10.658868   localhost ()  remote ()     L2CAP         21  Sent Configure Request (DCID: 0x0041)
   14 10.662368   controller    host          HCI_EVT        8  Rcvd Number of Completed Packets
   15 10.675431   host          controller    HCI_CMD       14  Sent Remote Name Request
```

```
> Frame 7: 27 bytes on wire (216 bits), 27 bytes captured (216 bits)
> Bluetooth
> Bluetooth HCI H4
v Bluetooth HCI Command - PIN Code Request Reply
  > Command Opcode: PIN Code Request Reply (0x040d)
    Parameter Total Length: 23
    BD_ADDR: LgInnote_24:5a:74 (c8:02:10:24:5a:74)
    PIN Code Length: 4
    PIN Code: 0000
    [Response in frame: 8]
    [Command-Response Delta: 3.028 ms]
```

```
0000  01 0d 04 17 74 5a 24 10  02 c8 04 30 30 30 30 00   ....tZ$. ...0000.
0010  00 00 00 00 00 00 00 00  00 00 00                  ........ ...
```

PIN Code (bthci_cmd.pin_code), 16 bytes   Packets: 2425 · Displayed: 2425 (100.0%) · Load time: 0:0.9

Bluetooth Paring



```
No.   Time        Source         Destination    Protocol  Length  Info
    1 0.000000    controller     host           HCI_EVT        8  Rcvd Number of Completed Packets
    2 0.030038    controller     host           HCI_EVT        9  Rcvd Link Key Request
    3 0.030328    host           controller     HCI_CMD       10  Sent Link Key Request Negative Reply
    4 0.031202    controller     host           HCI_EVT       13  Rcvd Command Complete (Link Key Request Negative Reply)
    5 0.170071    controller     host           HCI_EVT        9  Rcvd PIN Code Request
    6 3.803650    controller     host           HCI_EVT       14  Rcvd Connect Complete
    7 10.393997   host           controller     HCI_CMD       27  Sent PIN Code Request Reply
    8 10.397025   controller     host           HCI_EVT       13  Rcvd Command Complete (PIN Code Request Reply)
    9 10.550644   controller     host           HCI_EVT       26  Rcvd Link Key Notification
   10 10.655844   controller     host           HCI_EVT        7  Rcvd Encryption Change
   11 10.658594   remote ()      localhost ()   L2CAP         17  Rcvd Connection Request (SDP, SCID: 0x0041)
   12 10.658787   localhost ()   remote ()      L2CAP         21  Sent Connection Response - Success (SCID: 0x0041, DCID: 0x004b)
   13 10.658868   localhost ()   remote ()      L2CAP         21  Sent Configure Request (DCID: 0x0041)
   14 10.662368   controller     host           HCI_EVT        8  Rcvd Number of Completed Packets
   15 10.675431   host           controller     HCI_CMD       14  Sent Remote Name Request
```

```
> Frame 9: 26 bytes on wire (208 bits), 26 bytes captured (208 bits)
> Bluetooth
> Bluetooth HCI H4
v Bluetooth HCI Event - Link Key Notification
    Event Code: Link Key Notification (0x18)
    Parameter Total Length: 23
    BD_ADDR: LgInnote_24:5a:74 (c8:02:10:24:5a:74)
    Link Key: 711ee5f99b577dbf0e160a2092cd72a3
    Key Type: Combination Key (0x00)
```

```
0000  04 18 17 74 5a 24 10 02  c8 71 1e e5 f9 9b 57 7d   ...tZ$.. .q....W}
0010  bf 0e 16 0a 20 92 cd 72  a3 00                     .... ..r ..
```

Link Key for the associated BD_ADDR (bthci_evt.link_key), 16 bytes

Packets: 2425 · Displayed: 2425 (100.0%)

Bluetooth Profile

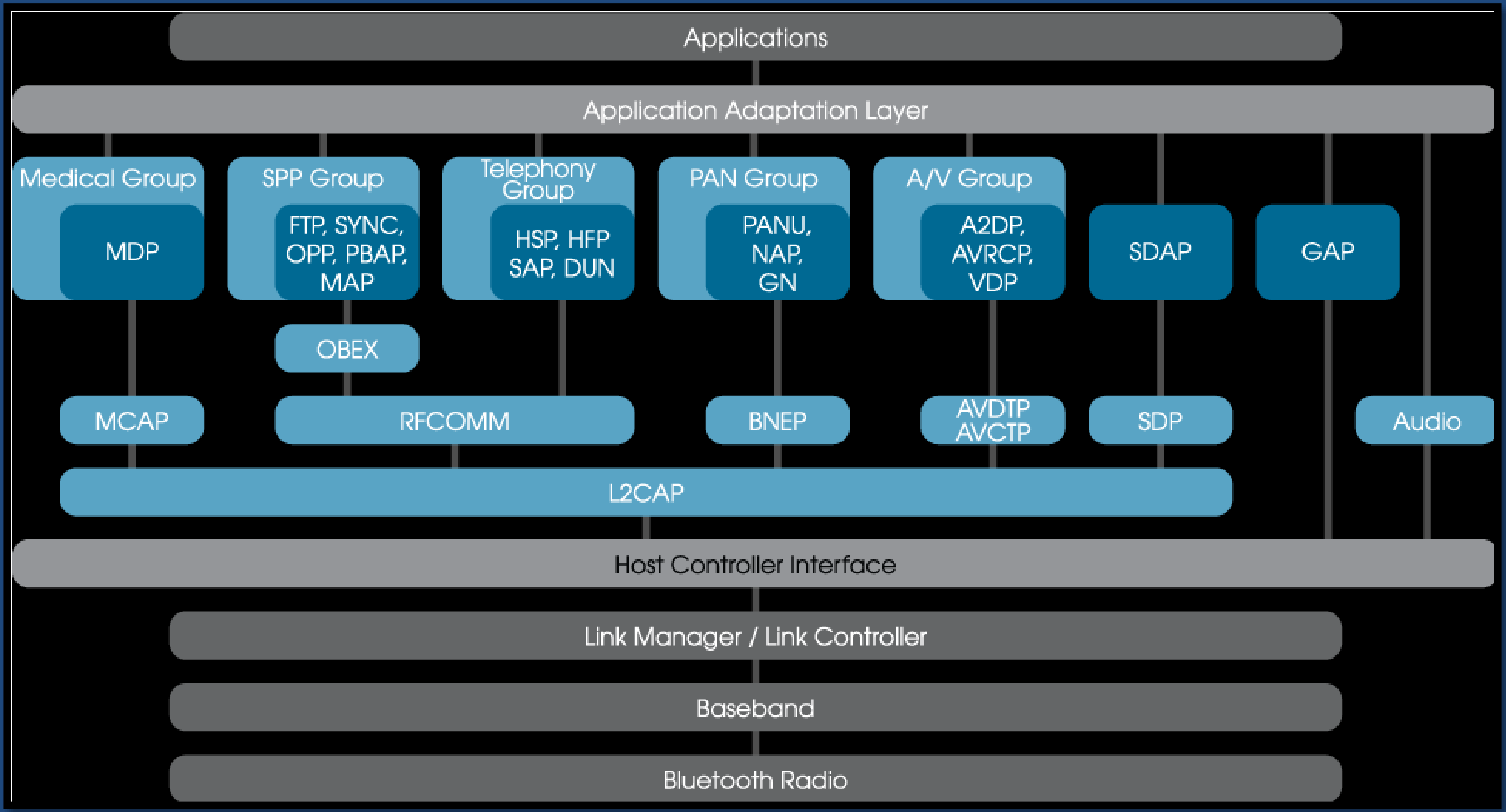
Bluetooth Profile이란?

- 통신 데이터의 종류를 나타내는 규격
  - 오디오 데이터, 전화 통화 데이터, 전화번호부 등
  - 서로 다른 제조사의 제품들에 대한 호환성 확보를 위함
- 장치가 연결되었을 때 어떻게 동작할지를 결정
- 특정 프로파일에 데이터를 실어 보낼 수 있음
- 블루투스 통신 주체들이 해당 프로파일에 대한 정보를 가지고 있고, 해석할 수 있어야 함

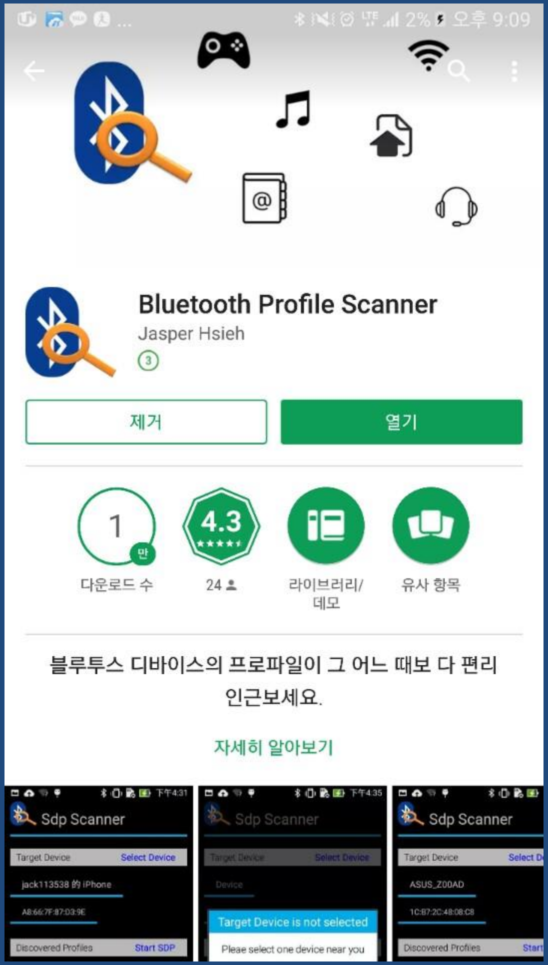
주요 Bluetooth Profiles

- SPP (Serial Port Profile)
  - 시리얼 통신 프로파일 (RX, TX)
- HID (Human Interface Device)
  - 사용자 입력장치 프로파일 (키보드, 마우스 등)
- Hands-Free Profile (HFP) / Headset Profile (HSP)
  - 전화 통화를 하기 위한 프로파일
- A2DP (Advanced Audio Distribution Profile)
  - 오디오 전송 프로파일 (SBC, MPEG-1, MPEG-2, AAC 등 지원)
- AVRCP (Audio/Video Remote Control Profile)
  - 장치 무선 제어(리모컨) 프로파일
- PBAP (Phone Book Access Profile)
  - 전화번호부 전송 프로파일
- OPP (Object Push Profile) / OBEX (Object Exchange) / FTP
  - 기기간 Data Object 및 파일 전송 프로파일
- PAN (Personal Area Networking Profile)
  - 인터넷 연결에 사용되는 프로파일

Profile이 표현된 Stack 구조



Bluetooth Profile Scanning



Bluetooth Profile Scanner

Jasper Hsieh

블루투스 디바이스의 프로파일이 그 어느 때보 다 편리 인근보세요.

jack113538 的 iPhone

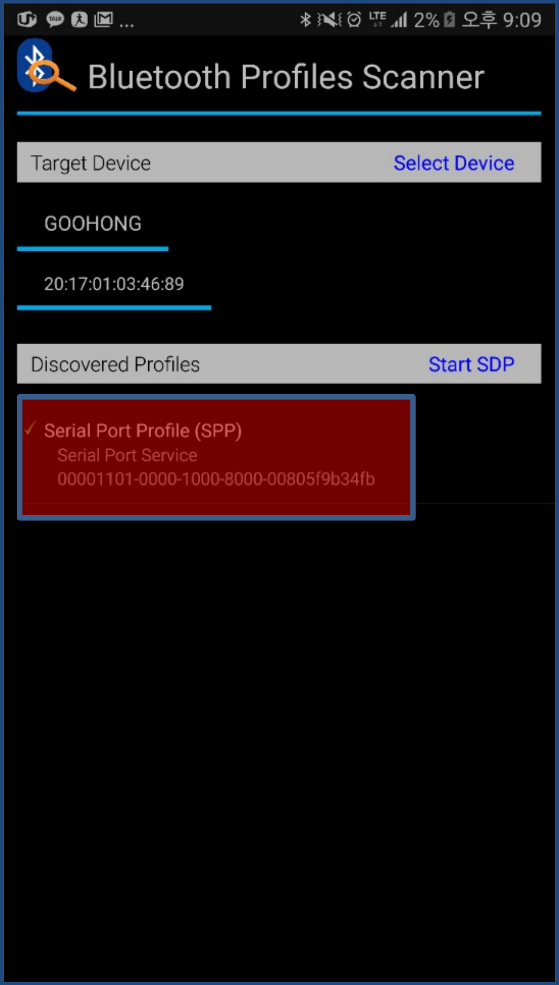
A8:66:7F:87:D3:9E

Target Device is not selected

Pleae select one device near you

ASUS_Z00AD

1C:B7:2C:48:08:C8



Bluetooth Profiles Scanner

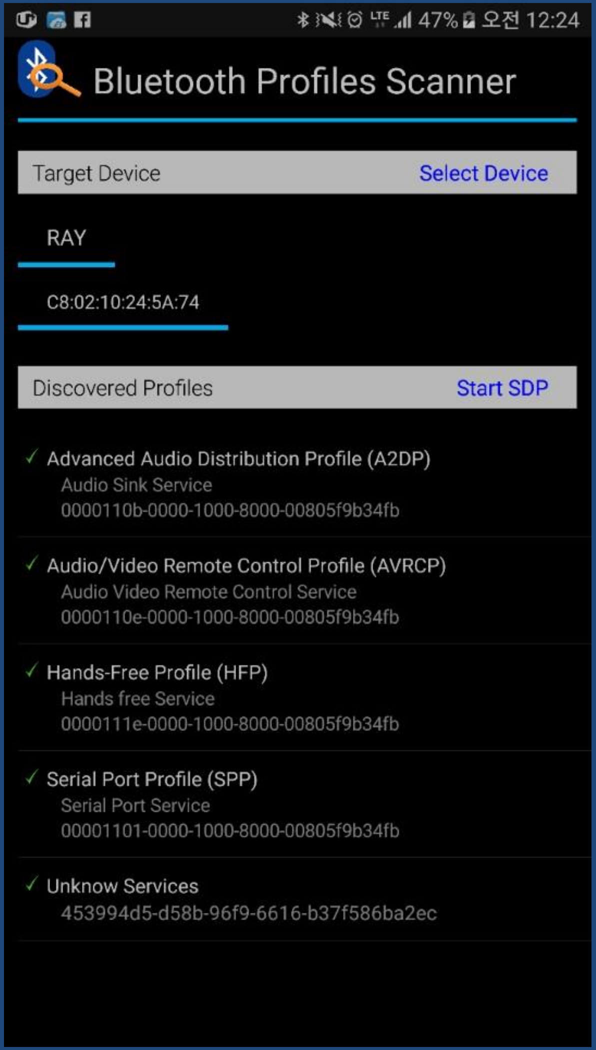
GOOHONG

20:17:01:03:46:89

✓ Serial Port Profile (SPP)
Serial Port Service
00001101-0000-1000-8000-00805f9b34fb

차량 장비의 Profiles

- A2DP
- AVRCP
- HFP
- SPP



47% 오전 12:24

Bluetooth Profiles Scanner

Target Device Select Device

RAY

C8:02:10:24:5A:74

Discovered Profiles Start SDP

✓ Advanced Audio Distribution Profile (A2DP)
Audio Sink Service
0000110b-0000-1000-8000-00805f9b34fb

✓ Audio/Video Remote Control Profile (AVRCP)
Audio Video Remote Control Service
0000110e-0000-1000-8000-00805f9b34fb

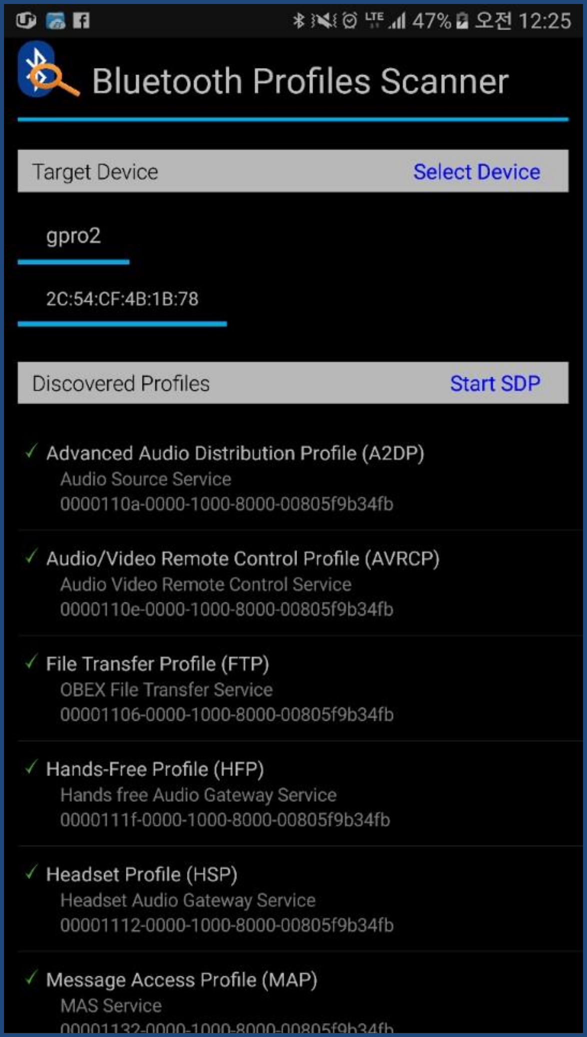
✓ Hands-Free Profile (HFP)
Hands free Service
0000111e-0000-1000-8000-00805f9b34fb

✓ Serial Port Profile (SPP)
Serial Port Service
00001101-0000-1000-8000-00805f9b34fb

✓ Unknow Services
453994d5-d58b-96f9-6616-b37f586ba2ec

스마트폰의 Profiles

- A2DP
- AVRCP
- FTP
- HFP
- HSP
- MAP
- OPP
- PBAP
- PAN



Bluetooth Profiles Scanner

Target Device — Select Device

gpro2

2C:54:CF:4B:1B:78

Discovered Profiles — Start SDP

✓ Advanced Audio Distribution Profile (A2DP)
Audio Source Service
0000110a-0000-1000-8000-00805f9b34fb

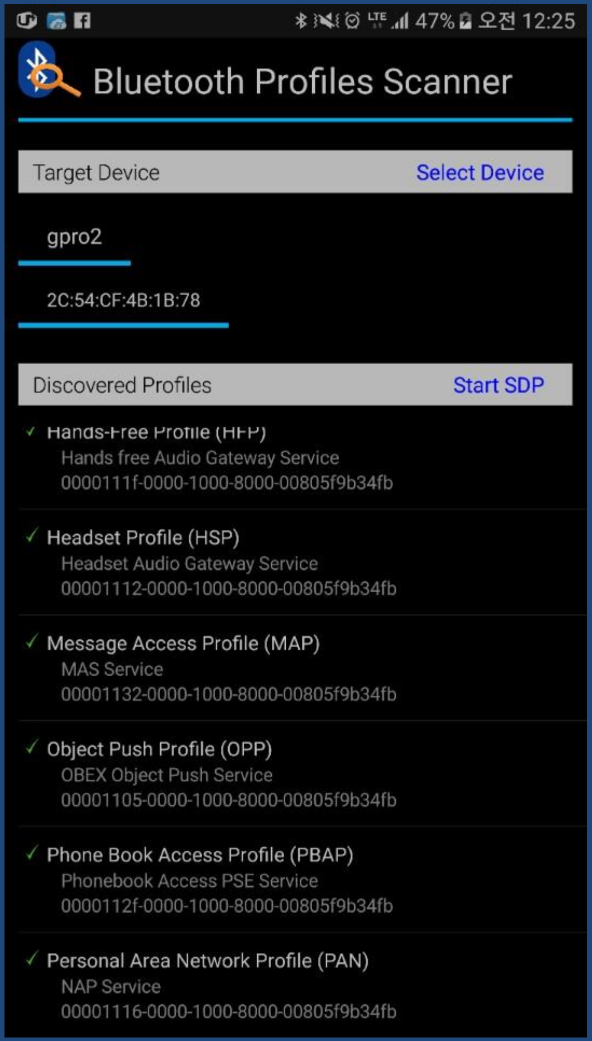
✓ Audio/Video Remote Control Profile (AVRCP)
Audio Video Remote Control Service
0000110e-0000-1000-8000-00805f9b34fb

✓ File Transfer Profile (FTP)
OBEX File Transfer Service
00001106-0000-1000-8000-00805f9b34fb

✓ Hands-Free Profile (HFP)
Hands free Audio Gateway Service
0000111f-0000-1000-8000-00805f9b34fb

✓ Headset Profile (HSP)
Headset Audio Gateway Service
00001112-0000-1000-8000-00805f9b34fb

✓ Message Access Profile (MAP)
MAS Service
00001132-0000-1000-8000-00805f9b34fb



Bluetooth Profiles Scanner

Target Device — Select Device

gpro2

2C:54:CF:4B:1B:78

Discovered Profiles — Start SDP

✓ Hands-Free Profile (HFP)
Hands free Audio Gateway Service
0000111f-0000-1000-8000-00805f9b34fb

✓ Headset Profile (HSP)
Headset Audio Gateway Service
00001112-0000-1000-8000-00805f9b34fb

✓ Message Access Profile (MAP)
MAS Service
00001132-0000-1000-8000-00805f9b34fb

✓ Object Push Profile (OPP)
OBEX Object Push Service
00001105-0000-1000-8000-00805f9b34fb

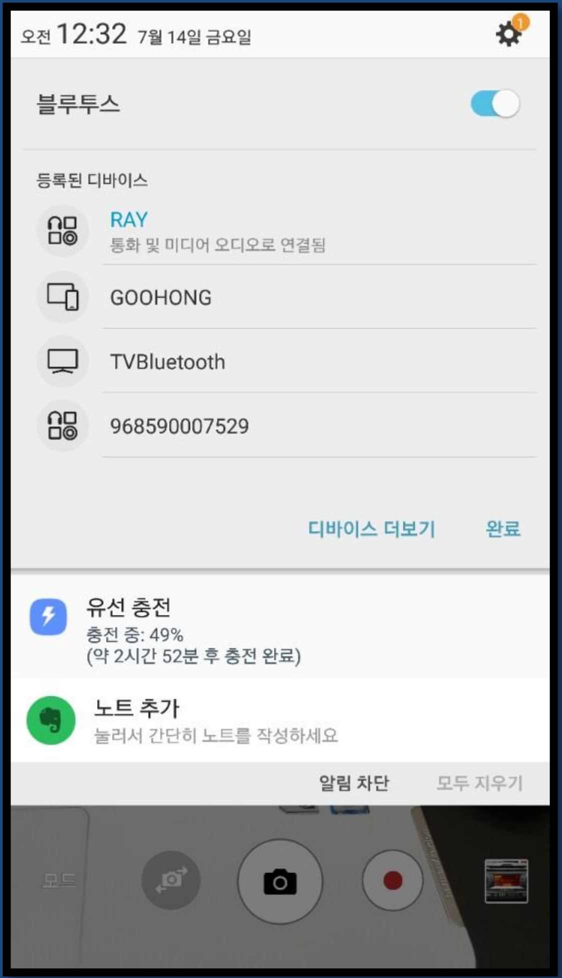
✓ Phone Book Access Profile (PBAP)
Phonebook Access PSE Service
0000112f-0000-1000-8000-00805f9b34fb

✓ Personal Area Network Profile (PAN)
NAP Service
00001116-0000-1000-8000-00805f9b34fb

Bluetooth Packet 변조 예시

- 카오디오 장비와 Bluetooth -

Bluetooth 등록



오전 12:32 7월 14일 금요일

블루투스

등록된 디바이스

RAY
통화 및 미디어 오디오로 연결됨

GOOHONG

TVBluetooth

968590007529

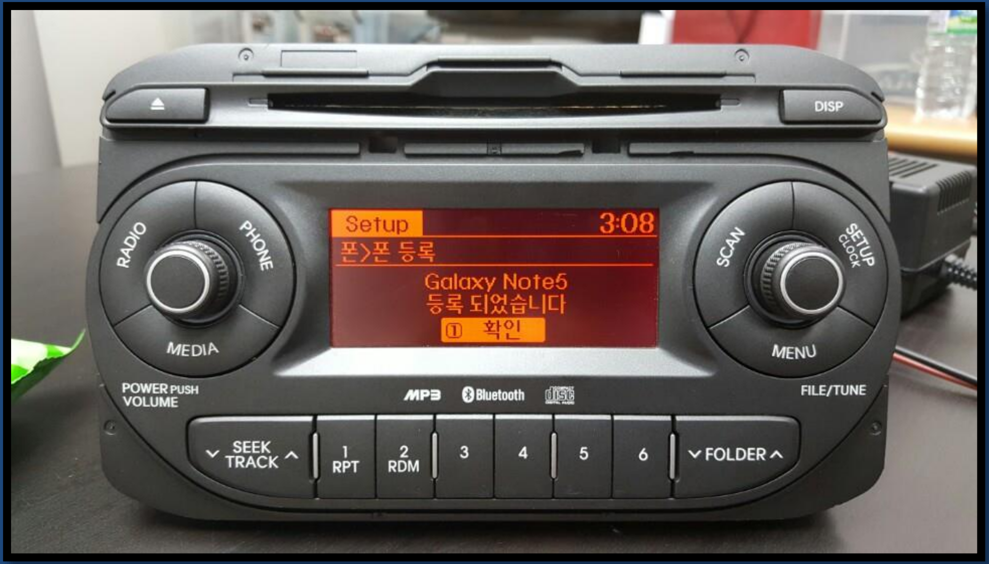
디바이스 더보기 완료

유선 충전
충전 중: 49%
(약 2시간 52분 후 충전 완료)

노트 추가
눌러서 간단히 노트를 작성하세요

알림 차단 모두 지우기

모드

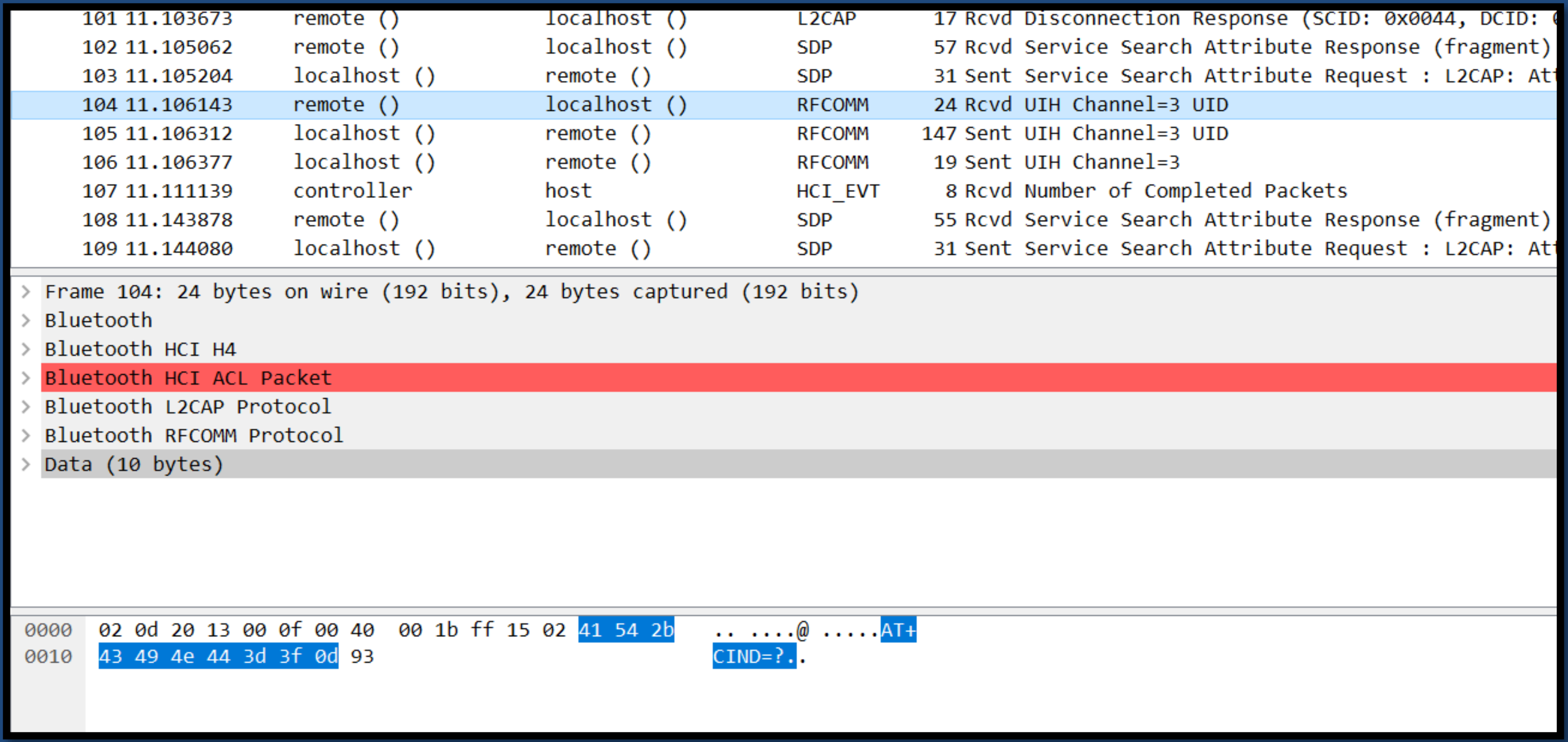


Bluetooth 관련 기능들

- 연락처 목록 수신
- 최근 통화 목록 수신
- 전화 통화
- 문자 확인
- 음악 재생

Bluetooth Packet Sniffing

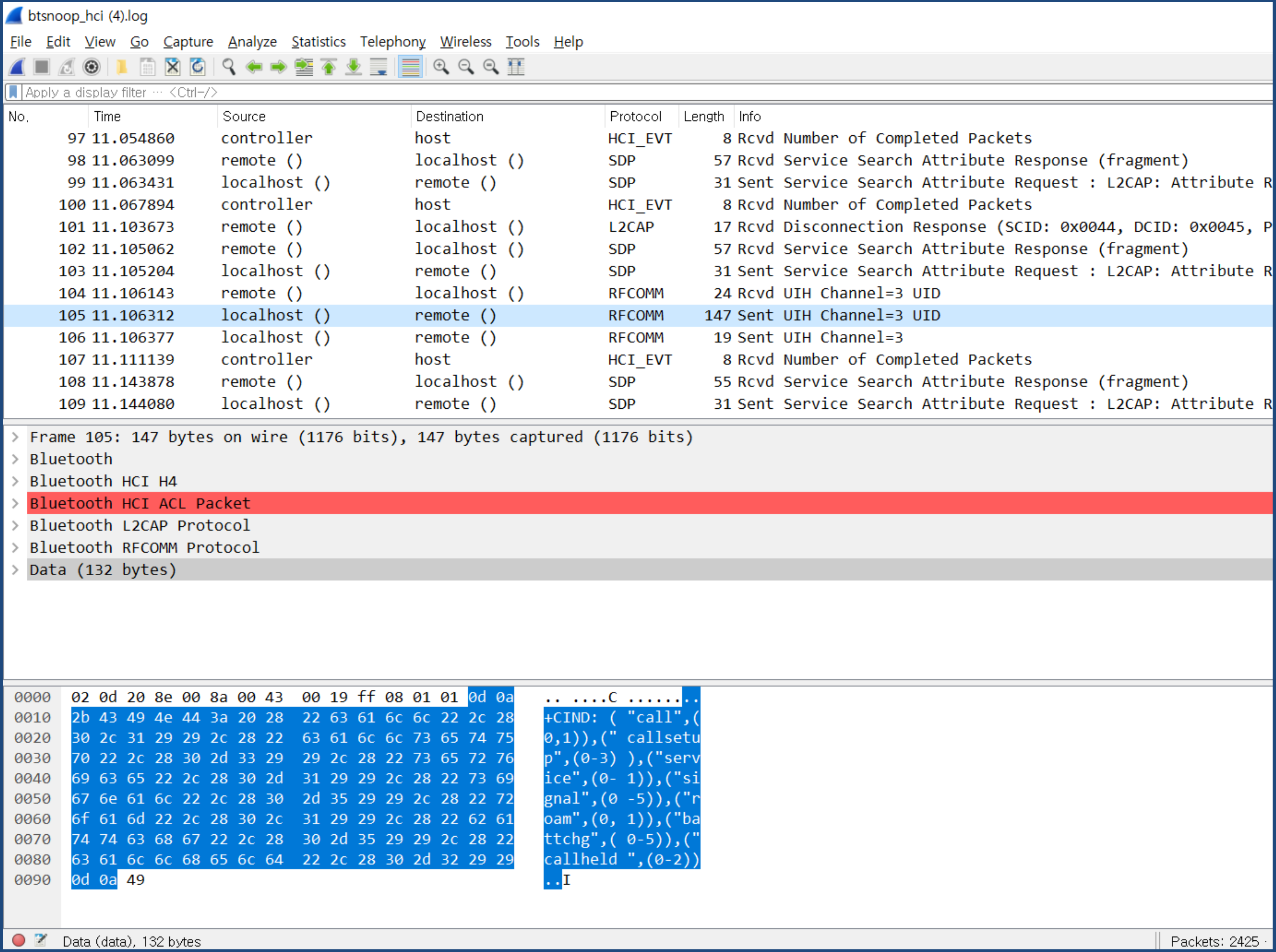
- 휴대폰과 연결 시의 패킷들



```
101 11.103673   remote ()      localhost ()   L2CAP      17 Rcvd Disconnection Response (SCID: 0x0044, DCID: 
102 11.105062   remote ()      localhost ()   SDP        57 Rcvd Service Search Attribute Response (fragment)
103 11.105204   localhost ()   remote ()      SDP        31 Sent Service Search Attribute Request : L2CAP: At
104 11.106143   remote ()      localhost ()   RFCOMM     24 Rcvd UIH Channel=3 UID
105 11.106312   localhost ()   remote ()      RFCOMM    147 Sent UIH Channel=3 UID
106 11.106377   localhost ()   remote ()      RFCOMM     19 Sent UIH Channel=3
107 11.111139   controller     host           HCI_EVT     8 Rcvd Number of Completed Packets
108 11.143878   remote ()      localhost ()   SDP        55 Rcvd Service Search Attribute Response (fragment)
109 11.144080   localhost ()   remote ()      SDP        31 Sent Service Search Attribute Request : L2CAP: At
```

```
> Frame 104: 24 bytes on wire (192 bits), 24 bytes captured (192 bits)
> Bluetooth
> Bluetooth HCI H4
> Bluetooth HCI ACL Packet
> Bluetooth L2CAP Protocol
> Bluetooth RFCOMM Protocol
> Data (10 bytes)
```

```
0000  02 0d 20 13 00 0f 00 40  00 1b ff 15 02 41 54 2b   .. ....@ .....AT+
0010  43 49 4e 44 3d 3f 0d 93                            CIND=?..
```


btsnoop_hci (4).log
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.     Time      Source        Destination   Protocol  Length Info
     97 11.054860 controller    host          HCI_EVT        8 Rcvd Number of Completed Packets
     98 11.063099 remote ()     localhost ()  SDP           57 Rcvd Service Search Attribute Response (fragment)
     99 11.063431 localhost ()  remote ()     SDP           31 Sent Service Search Attribute Request : L2CAP: Attribute R
    100 11.067894 controller    host          HCI_EVT        8 Rcvd Number of Completed Packets
    101 11.103673 remote ()     localhost ()  L2CAP         17 Rcvd Disconnection Response (SCID: 0x0044, DCID: 0x0045, P
    102 11.105062 remote ()     localhost ()  SDP           57 Rcvd Service Search Attribute Response (fragment)
    103 11.105204 localhost ()  remote ()     SDP           31 Sent Service Search Attribute Request : L2CAP: Attribute R
    104 11.106143 remote ()     localhost ()  RFCOMM        24 Rcvd UIH Channel=3 UID
    105 11.106312 localhost ()  remote ()     RFCOMM       147 Sent UIH Channel=3 UID
    106 11.106377 localhost ()  remote ()     RFCOMM        19 Sent UIH Channel=3
    107 11.111139 controller    host          HCI_EVT        8 Rcvd Number of Completed Packets
    108 11.143878 remote ()     localhost ()  SDP           55 Rcvd Service Search Attribute Response (fragment)
    109 11.144080 localhost ()  remote ()     SDP           31 Sent Service Search Attribute Request : L2CAP: Attribute R
```

```
> Frame 105: 147 bytes on wire (1176 bits), 147 bytes captured (1176 bits)
> Bluetooth
> Bluetooth HCI H4
> Bluetooth HCI ACL Packet
> Bluetooth L2CAP Protocol
> Bluetooth RFCOMM Protocol
> Data (132 bytes)
```

```
0000  02 0d 20 8e 00 8a 00 43  00 19 ff 08 01 01 0d 0a   .. ....C ........
0010  2b 43 49 4e 44 3a 20 28  22 63 61 6c 6c 22 2c 28   +CIND: ( "call",(
0020  30 2c 31 29 29 2c 28 22  63 61 6c 6c 73 65 74 75   0,1)),(" callsetu
0030  70 22 2c 28 30 2d 33 29  29 2c 28 22 73 65 72 76   p",(0-3) ),("serv
0040  69 63 65 22 2c 28 30 2d  31 29 29 2c 28 22 73 69   ice",(0- 1)),("si
0050  67 6e 61 6c 22 2c 28 30  2d 35 29 29 2c 28 22 72   gnal",(0 -5)),("r
0060  6f 61 6d 22 2c 28 30 2c  31 29 29 2c 28 22 62 61   oam",(0, 1)),("ba
0070  74 74 63 68 67 22 2c 28  30 2d 35 29 29 2c 28 22   ttchg",( 0-5)),("
0080  63 61 6c 6c 68 65 6c 64  22 2c 28 30 2d 32 29 29   callheld ",(0-2))
0090  0d 0a 49                                           ..I
```

Data (data), 132 bytes

Packets: 2425

수신 AT Command 목록

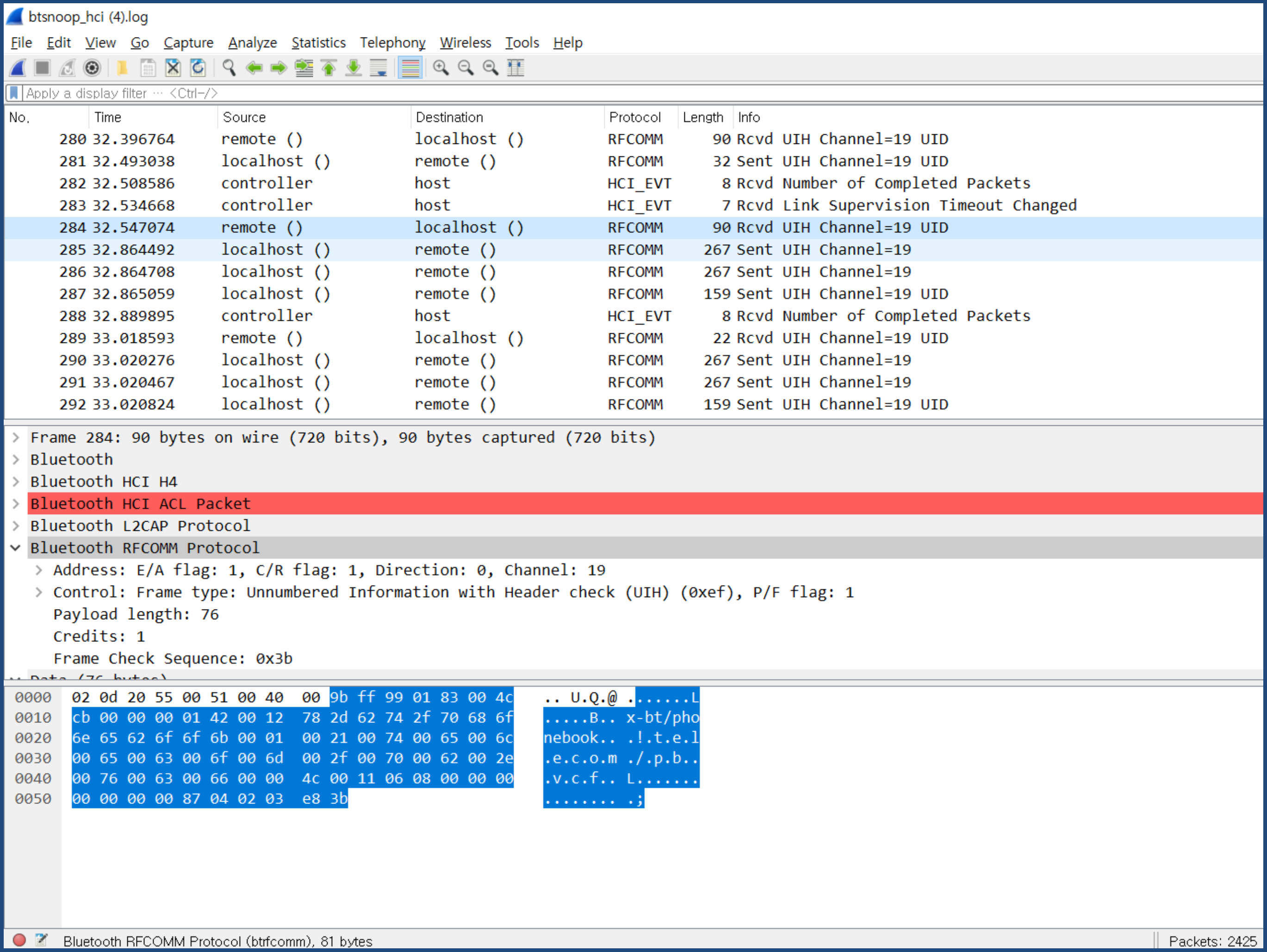
- AT+CIND=?
- AT+CMER=3, 0, 0, 1
- AT+CHLD=?
- AT+CLIP=1
- AT+CCWA=1
- AT+NREC=0
- AT+VGS=15
- AT+VGM=10
- AT+CGMI=?
- AT+BSRF=39

수신 AT Command 목록

- AT+CIND=?
- AT+CMER=3, 0, 0, 1
- AT+CHLD=?
- AT+CLIP=1
- AT+CCWA=1
- AT+NREC=0
- AT+VGS=15
- AT+VGM=10
- AT+CGMI=?
- AT+BSRF=39

응답으로 Evil Packet 전송 시도 가능

PhoneBook 요청 Packet
x-bt/phonebook!telecom/pb.vcf

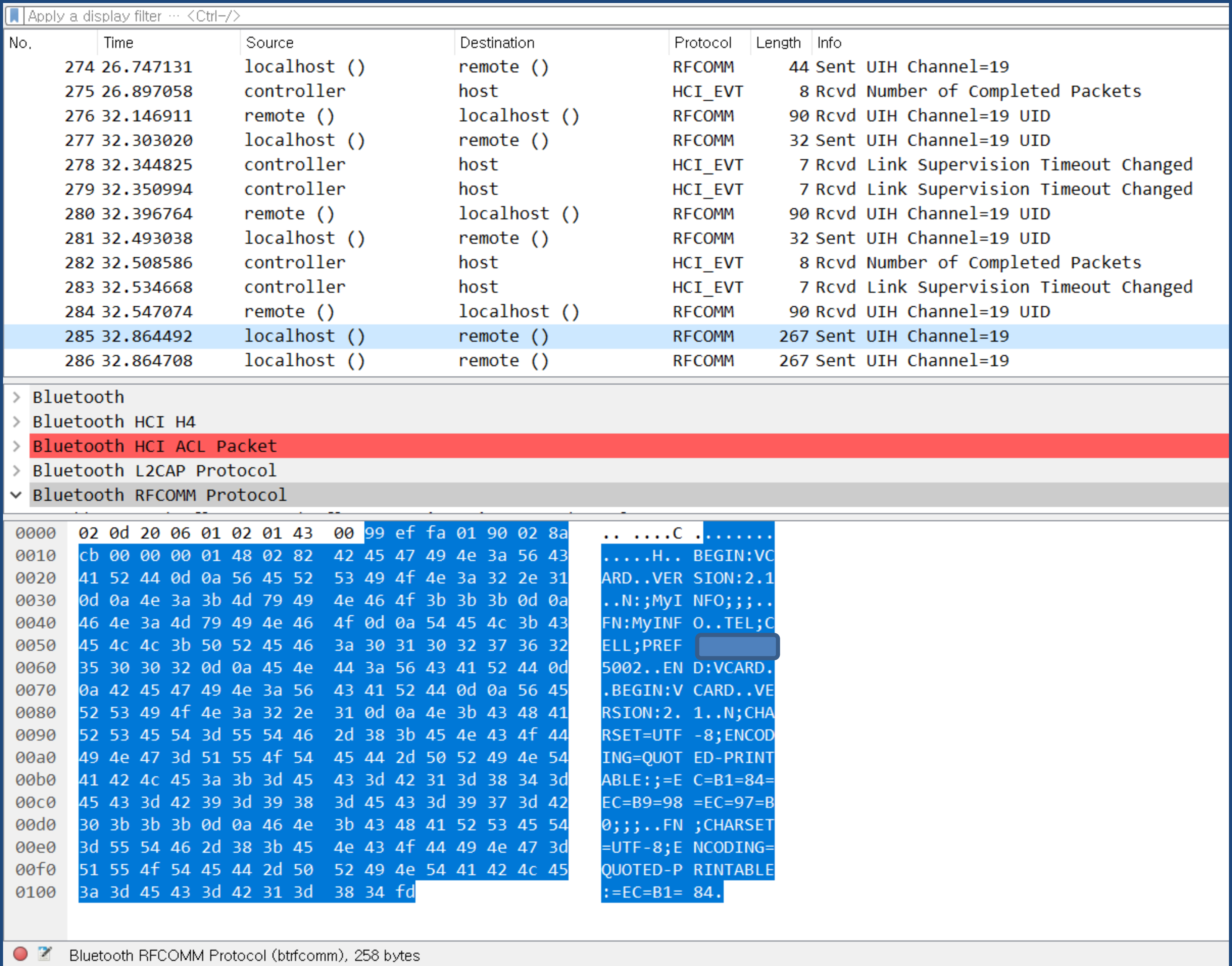

btsnoop_hci (4).log
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.    Time       Source          Destination     Protocol Length Info
   280 32.396764  remote ()       localhost ()    RFCOMM       90 Rcvd UIH Channel=19 UID
   281 32.493038  localhost ()    remote ()       RFCOMM       32 Sent UIH Channel=19 UID
   282 32.508586  controller      host            HCI_EVT       8 Rcvd Number of Completed Packets
   283 32.534668  controller      host            HCI_EVT       7 Rcvd Link Supervision Timeout Changed
   284 32.547074  remote ()       localhost ()    RFCOMM       90 Rcvd UIH Channel=19 UID
   285 32.864492  localhost ()    remote ()       RFCOMM      267 Sent UIH Channel=19
   286 32.864708  localhost ()    remote ()       RFCOMM      267 Sent UIH Channel=19
   287 32.865059  localhost ()    remote ()       RFCOMM      159 Sent UIH Channel=19 UID
   288 32.889895  controller      host            HCI_EVT       8 Rcvd Number of Completed Packets
   289 33.018593  remote ()       localhost ()    RFCOMM       22 Rcvd UIH Channel=19 UID
   290 33.020276  localhost ()    remote ()       RFCOMM      267 Sent UIH Channel=19
   291 33.020467  localhost ()    remote ()       RFCOMM      267 Sent UIH Channel=19
   292 33.020824  localhost ()    remote ()       RFCOMM      159 Sent UIH Channel=19 UID
```

```
> Frame 284: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
> Bluetooth
> Bluetooth HCI H4
> Bluetooth HCI ACL Packet
> Bluetooth L2CAP Protocol
v Bluetooth RFCOMM Protocol
  > Address: E/A flag: 1, C/R flag: 1, Direction: 0, Channel: 19
  > Control: Frame type: Unnumbered Information with Header check (UIH) (0xef), P/F flag: 1
    Payload length: 76
    Credits: 1
    Frame Check Sequence: 0x3b
v Data (76 bytes)
```

```
0000  02 0d 20 55 00 51 00 40  00 9b ff 99 01 83 00 4c   .. U.Q.@ .......L
0010  cb 00 00 00 01 42 00 12  78 2d 62 74 2f 70 68 6f   .....B.. x-bt/pho
0020  6e 65 62 6f 6f 6b 00 01  00 21 00 74 00 65 00 6c   nebook.. .!.t.e.l
0030  00 65 00 63 00 6f 00 6d  00 2f 00 70 00 62 00 2e   .e.c.o.m ./.p.b..
0040  00 76 00 63 00 66 00 00  4c 00 11 06 08 00 00 00   .v.c.f.. L.......
0050  00 00 00 00 87 04 02 03  e8 3b                     ........ .;
```

```
Bluetooth RFCOMM Protocol (btrfcomm), 81 bytes                    Packets: 2425
```



```
No.   Time        Source         Destination    Protocol  Length Info
  274 26.747131   localhost ()   remote ()      RFCOMM        44 Sent UIH Channel=19
  275 26.897058   controller     host           HCI_EVT        8 Rcvd Number of Completed Packets
  276 32.146911   remote ()      localhost ()   RFCOMM        90 Rcvd UIH Channel=19 UID
  277 32.303020   localhost ()   remote ()      RFCOMM        32 Sent UIH Channel=19 UID
  278 32.344825   controller     host           HCI_EVT        7 Rcvd Link Supervision Timeout Changed
  279 32.350994   controller     host           HCI_EVT        7 Rcvd Link Supervision Timeout Changed
  280 32.396764   remote ()      localhost ()   RFCOMM        90 Rcvd UIH Channel=19 UID
  281 32.493038   localhost ()   remote ()      RFCOMM        32 Sent UIH Channel=19 UID
  282 32.508586   controller     host           HCI_EVT        8 Rcvd Number of Completed Packets
  283 32.534668   controller     host           HCI_EVT        7 Rcvd Link Supervision Timeout Changed
  284 32.547074   remote ()      localhost ()   RFCOMM        90 Rcvd UIH Channel=19 UID
  285 32.864492   localhost ()   remote ()      RFCOMM       267 Sent UIH Channel=19
  286 32.864708   localhost ()   remote ()      RFCOMM       267 Sent UIH Channel=19
```

```
> Bluetooth
> Bluetooth HCI H4
> Bluetooth HCI ACL Packet
> Bluetooth L2CAP Protocol
v Bluetooth RFCOMM Protocol
```

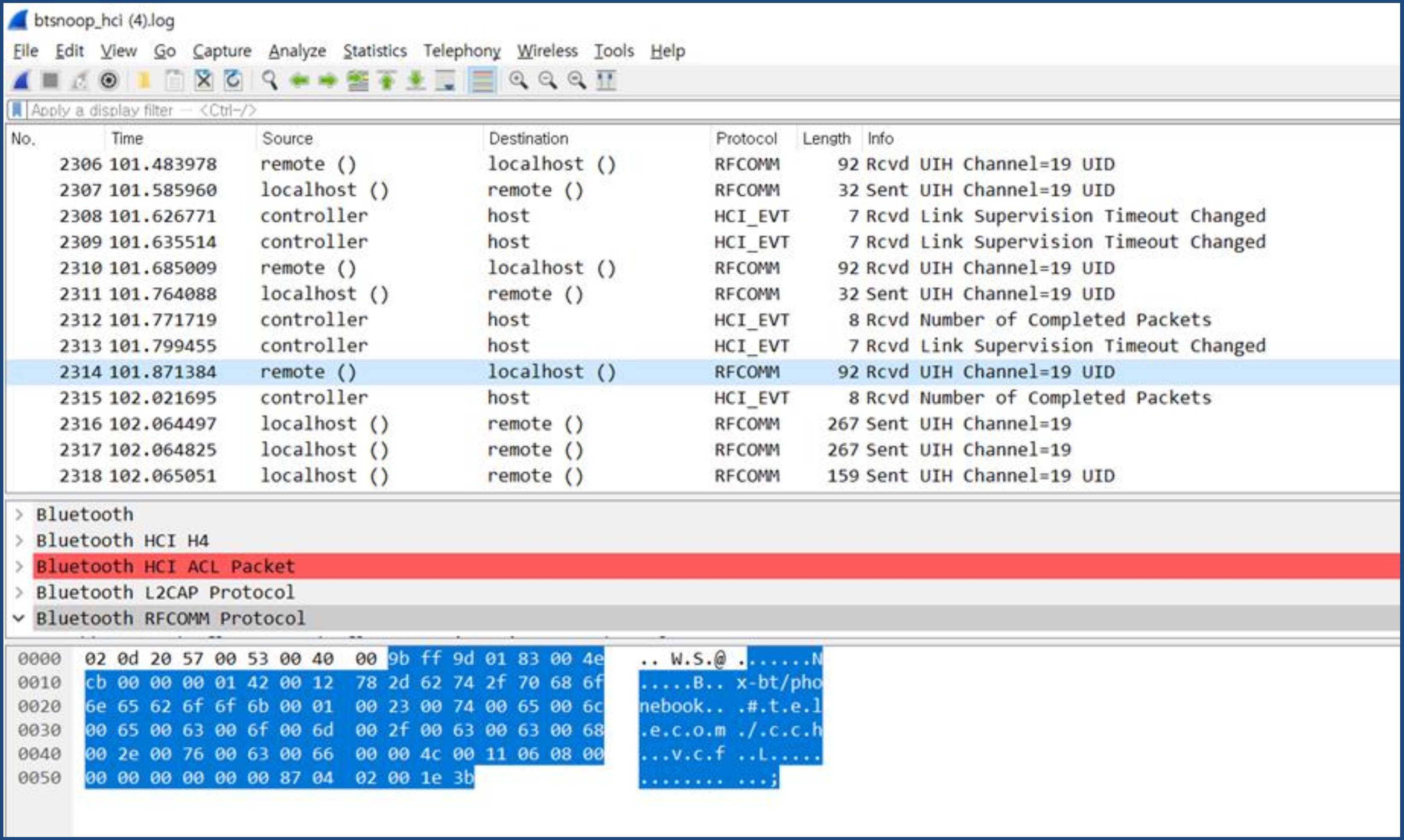
```
0000  02 0d 20 06 01 02 01 43  00 99 ef fa 01 90 02 8a   .. ....C ........
0010  cb 00 00 00 01 48 02 82  42 45 47 49 4e 3a 56 43   .....H.. BEGIN:VC
0020  41 52 44 0d 0a 56 45 52  53 49 4f 4e 3a 32 2e 31   ARD..VER SION:2.1
0030  0d 0a 4e 3a 3b 4d 79 49  4e 46 4f 3b 3b 3b 0d 0a   ..N:;MyI NFO;;;..
0040  46 4e 3a 4d 79 49 4e 46  4f 0d 0a 54 45 4c 3b 43   FN:MyINF O..TEL;C
0050  45 4c 4c 3b 50 52 45 46  3a 30 31 30 32 37 36 32   ELL;PREF [redacted]
0060  35 30 30 32 0d 0a 45 4e  44 3a 56 43 41 52 44 0d   5002..EN D:VCARD.
0070  0a 42 45 47 49 4e 3a 56  43 41 52 44 0d 0a 56 45   .BEGIN:V CARD..VE
0080  52 53 49 4f 4e 3a 32 2e  31 0d 0a 4e 3b 43 48 41   RSION:2. 1..N;CHA
0090  52 53 45 54 3d 55 54 46  2d 38 3b 45 4e 43 4f 44   RSET=UTF -8;ENCOD
00a0  49 4e 47 3d 51 55 4f 54  45 44 2d 50 52 49 4e 54   ING=QUOT ED-PRINT
00b0  41 42 4c 45 3a 3b 3d 45  43 3d 42 31 3d 38 34 3d   ABLE:;=E C=B1=84=
00c0  45 43 3d 42 39 3d 39 38  3d 45 43 3d 39 37 3d 42   EC=B9=98 =EC=97=B
00d0  30 3b 3b 3b 0d 0a 46 4e  3b 43 48 41 52 53 45 54   0;;;..FN ;CHARSET
00e0  3d 55 54 46 2d 38 3b 45  4e 43 4f 44 49 4e 47 3d   =UTF-8;E NCODING=
00f0  51 55 4f 54 45 44 2d 50  52 49 4e 54 41 42 4c 45   QUOTED-P RINTABLE
0100  3a 3d 45 43 3d 42 31 3d  38 34 fd                  :=EC=B1= 84.
```

Bluetooth RFCOMM Protocol (btrfcomm), 258 bytes

vCARD(연락처)의 Format

```
BEGIN:VCARD
VERSION:2.1
FN;CHARSET=UTF-8:홍길동
N;CHARSET=UTF-8:홍길동
TEL;TYPE=CELL:01012341234
X-IRMC-CALL-DATETIME;TYPE=RECEIVED:20170710T151235
END:VCARD
```

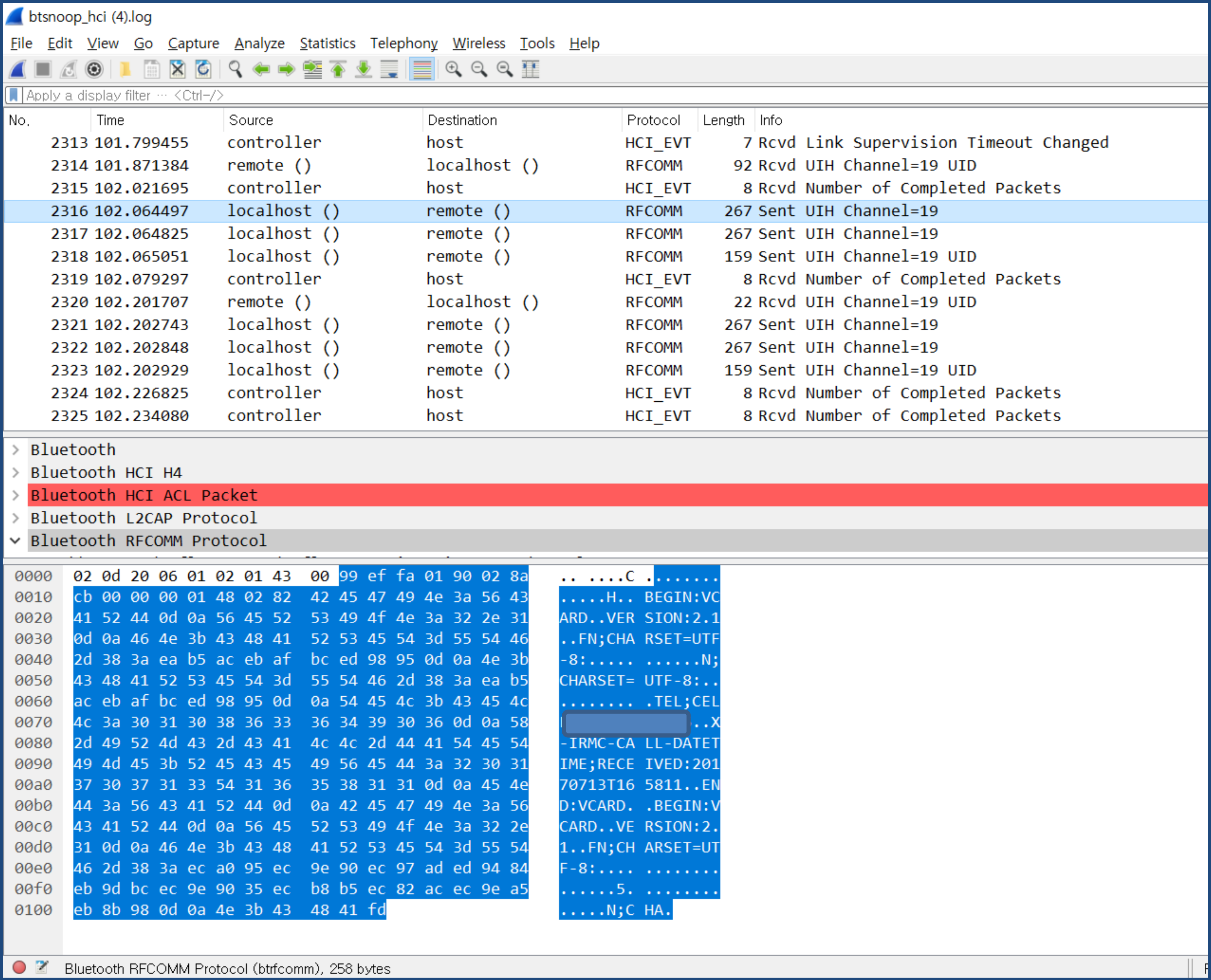
최근 통화 목록 요청
x-bt/phonebook!telecom/cch.vcf


btsnoop_hci (4).log
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter — <Ctrl-/>

```
No.   Time        Source         Destination    Protocol  Length Info
 2306 101.483978  remote ()      localhost ()   RFCOMM       92 Rcvd UIH Channel=19 UID
 2307 101.585960  localhost ()   remote ()      RFCOMM       32 Sent UIH Channel=19 UID
 2308 101.626771  controller     host           HCI_EVT       7 Rcvd Link Supervision Timeout Changed
 2309 101.635514  controller     host           HCI_EVT       7 Rcvd Link Supervision Timeout Changed
 2310 101.685009  remote ()      localhost ()   RFCOMM       92 Rcvd UIH Channel=19 UID
 2311 101.764088  localhost ()   remote ()      RFCOMM       32 Sent UIH Channel=19 UID
 2312 101.771719  controller     host           HCI_EVT       8 Rcvd Number of Completed Packets
 2313 101.799455  controller     host           HCI_EVT       7 Rcvd Link Supervision Timeout Changed
 2314 101.871384  remote ()      localhost ()   RFCOMM       92 Rcvd UIH Channel=19 UID
 2315 102.021695  controller     host           HCI_EVT       8 Rcvd Number of Completed Packets
 2316 102.064497  localhost ()   remote ()      RFCOMM      267 Sent UIH Channel=19
 2317 102.064825  localhost ()   remote ()      RFCOMM      267 Sent UIH Channel=19
 2318 102.065051  localhost ()   remote ()      RFCOMM      159 Sent UIH Channel=19 UID
```

```
> Bluetooth
> Bluetooth HCI H4
> Bluetooth HCI ACL Packet
> Bluetooth L2CAP Protocol
v Bluetooth RFCOMM Protocol
```

```
0000  02 0d 20 57 00 53 00 40  00 9b ff 9d 01 83 00 4e   .. W.S.@ .......N
0010  cb 00 00 00 01 42 00 12  78 2d 62 74 2f 70 68 6f   .....B.. x-bt/pho
0020  6e 65 62 6f 6f 6b 00 01  00 23 00 74 00 65 00 6c   nebook.. .#.t.e.l
0030  00 65 00 63 00 6f 00 6d  00 2f 00 63 00 63 00 68   .e.c.o.m ./.c.c.h
0040  00 2e 00 76 00 63 00 66  00 00 4c 00 11 06 08 00   ...v.c.f ..L.....
0050  00 00 00 00 00 00 87 04  02 00 1e 3b               ........ ...;
```



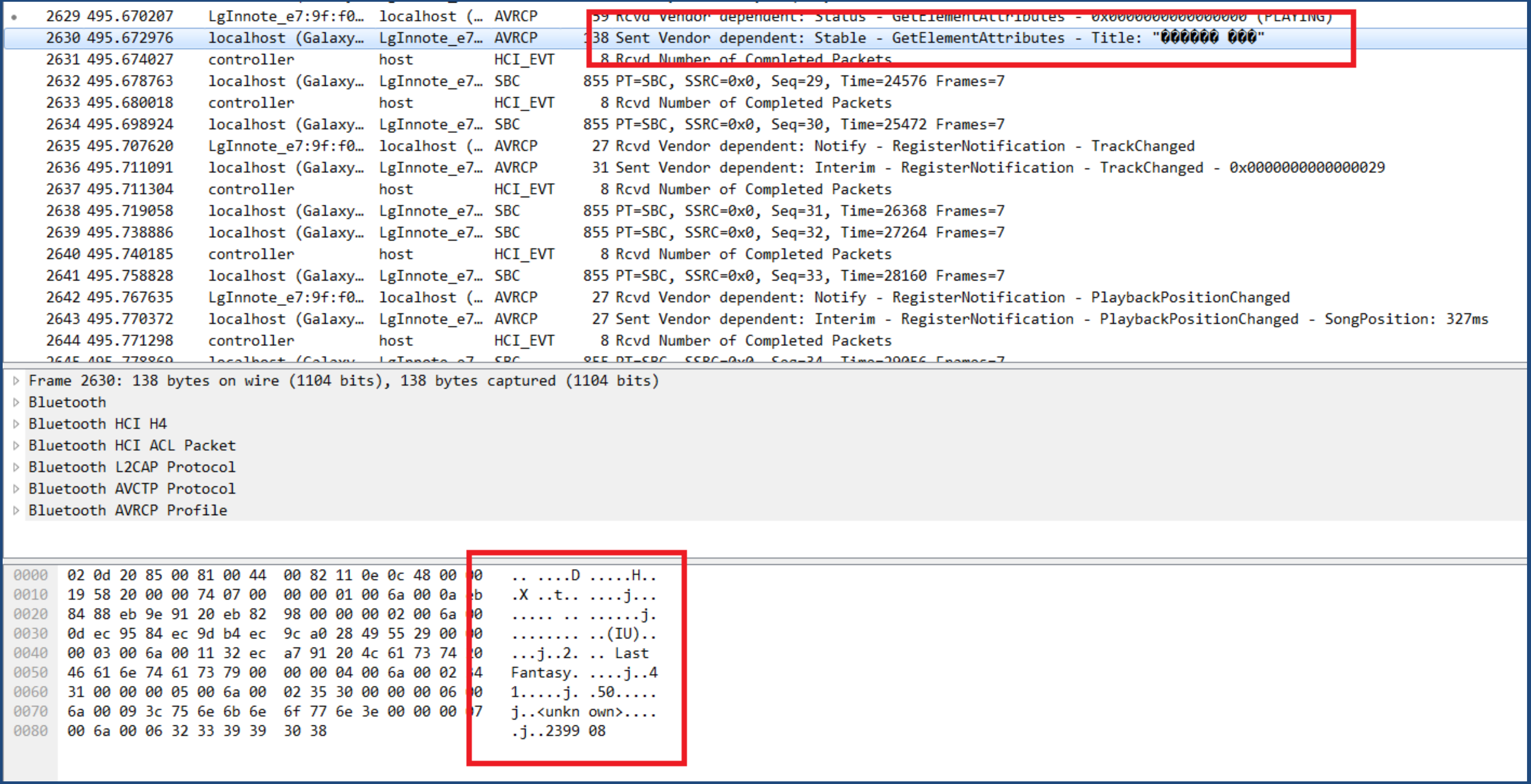
```
No.   Time        Source         Destination    Protocol  Length Info
 2313 101.799455  controller     host           HCI_EVT        7 Rcvd Link Supervision Timeout Changed
 2314 101.871384  remote ()      localhost ()   RFCOMM        92 Rcvd UIH Channel=19 UID
 2315 102.021695  controller     host           HCI_EVT        8 Rcvd Number of Completed Packets
 2316 102.064497  localhost ()   remote ()      RFCOMM       267 Sent UIH Channel=19
 2317 102.064825  localhost ()   remote ()      RFCOMM       267 Sent UIH Channel=19
 2318 102.065051  localhost ()   remote ()      RFCOMM       159 Sent UIH Channel=19 UID
 2319 102.079297  controller     host           HCI_EVT        8 Rcvd Number of Completed Packets
 2320 102.201707  remote ()      localhost ()   RFCOMM        22 Rcvd UIH Channel=19 UID
 2321 102.202743  localhost ()   remote ()      RFCOMM       267 Sent UIH Channel=19
 2322 102.202848  localhost ()   remote ()      RFCOMM       267 Sent UIH Channel=19
 2323 102.202929  localhost ()   remote ()      RFCOMM       159 Sent UIH Channel=19 UID
 2324 102.226825  controller     host           HCI_EVT        8 Rcvd Number of Completed Packets
 2325 102.234080  controller     host           HCI_EVT        8 Rcvd Number of Completed Packets
```

```
> Bluetooth
> Bluetooth HCI H4
> Bluetooth HCI ACL Packet
> Bluetooth L2CAP Protocol
v Bluetooth RFCOMM Protocol
```

```
0000  02 0d 20 06 01 02 01 43  00 99 ef fa 01 90 02 8a   .. ....C ........
0010  cb 00 00 00 01 48 02 82  42 45 47 49 4e 3a 56 43   .....H.. BEGIN:VC
0020  41 52 44 0d 0a 56 45 52  53 49 4f 4e 3a 32 2e 31   ARD..VER SION:2.1
0030  0d 0a 46 4e 3b 43 48 41  52 53 45 54 3d 55 54 46   ..FN;CHA RSET=UTF
0040  2d 38 3a ea b5 ac eb af  bc ed 98 95 0d 0a 4e 3b   -8:..... ......N;
0050  43 48 41 52 53 45 54 3d  55 54 46 2d 38 3a ea b5   CHARSET= UTF-8:..
0060  ac eb af bc ed 98 95 0d  0a 54 45 4c 3b 43 45 4c   ........ .TEL;CEL
0070  4c 3a 30 31 30 38 36 33  36 34 39 30 36 0d 0a 58   [redacted]..X
0080  2d 49 52 4d 43 2d 43 41  4c 4c 2d 44 41 54 45 54   -IRMC-CA LL-DATET
0090  49 4d 45 3b 52 45 43 45  49 56 45 44 3a 32 30 31   IME;RECE IVED:201
00a0  37 30 37 31 33 54 31 36  35 38 31 31 0d 0a 45 4e   70713T16 5811..EN
00b0  44 3a 56 43 41 52 44 0d  0a 42 45 47 49 4e 3a 56   D:VCARD. .BEGIN:V
00c0  43 41 52 44 0d 0a 56 45  52 53 49 4f 4e 3a 32 2e   CARD..VE RSION:2.
00d0  31 0d 0a 46 4e 3b 43 48  41 52 53 45 54 3d 55 54   1..FN;CH ARSET=UT
00e0  46 2d 38 3a ec a0 95 ec  9e 90 ec 97 ad ed 94 84   F-8:.... ........
00f0  eb 9d bc ec 9e 90 35 ec  b8 b5 ec 82 ac ec 9e a5   ......5. ........
0100  eb 8b 98 0d 0a 4e 3b 43  48 41 fd                  .....N;C HA.
```

Bluetooth RFCOMM Protocol (btrfcomm), 258 bytes

음원 Meta-data 전송



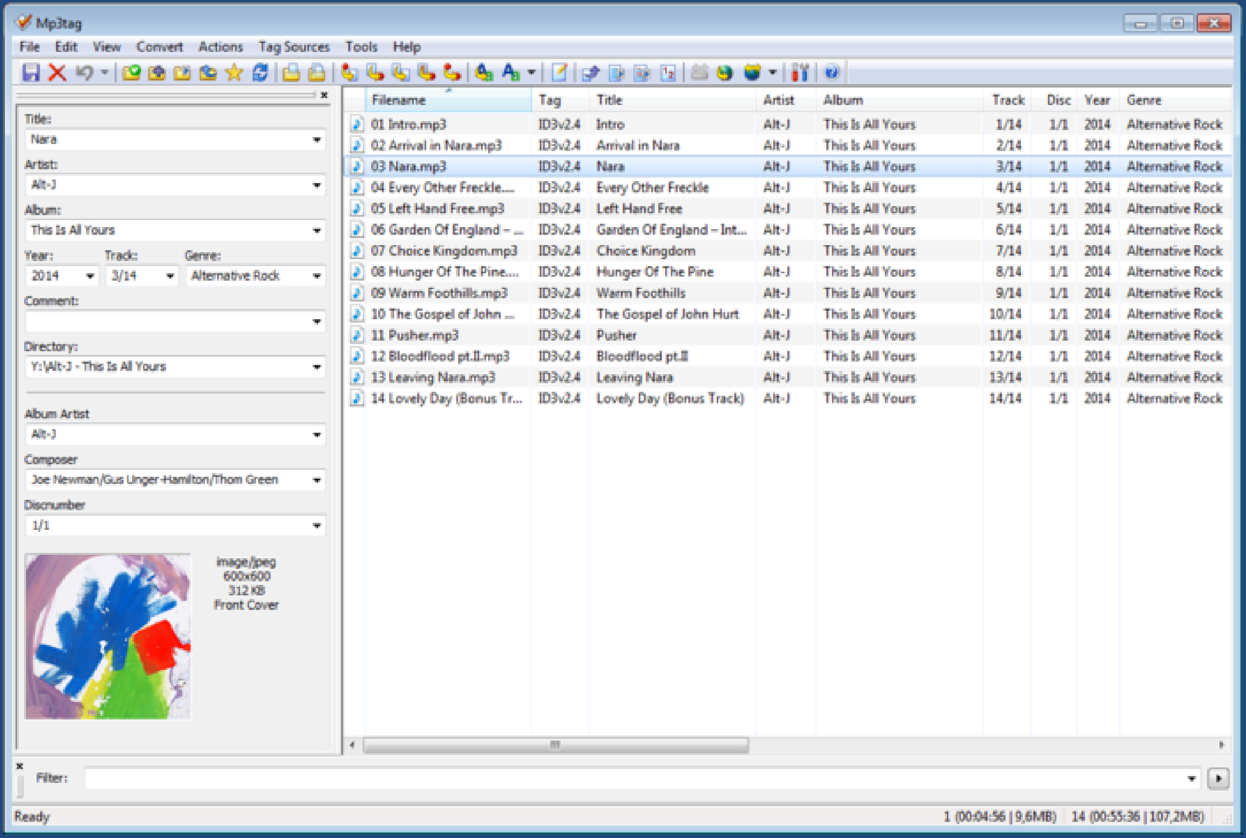
```
• 2629 495.670207   LgInnote_e7:9f:f0…  localhost (…   AVRCP     59 Rcvd Vendor dependent: Status - GetElementAttributes - 0x0000000000000000 (PLAYING)
  2630 495.672976   localhost (Galaxy…  LgInnote_e7…   AVRCP    138 Sent Vendor dependent: Stable - GetElementAttributes - Title: "������ ���"
  2631 495.674027   controller          host           HCI_EVT    8 Rcvd Number of Completed Packets
  2632 495.678763   localhost (Galaxy…  LgInnote_e7…   SBC      855 PT=SBC, SSRC=0x0, Seq=29, Time=24576 Frames=7
  2633 495.680018   controller          host           HCI_EVT    8 Rcvd Number of Completed Packets
  2634 495.698924   localhost (Galaxy…  LgInnote_e7…   SBC      855 PT=SBC, SSRC=0x0, Seq=30, Time=25472 Frames=7
  2635 495.707620   LgInnote_e7:9f:f0…  localhost (…   AVRCP     27 Rcvd Vendor dependent: Notify - RegisterNotification - TrackChanged
  2636 495.711091   localhost (Galaxy…  LgInnote_e7…   AVRCP     31 Sent Vendor dependent: Interim - RegisterNotification - TrackChanged - 0x0000000000000029
  2637 495.711304   controller          host           HCI_EVT    8 Rcvd Number of Completed Packets
  2638 495.719058   localhost (Galaxy…  LgInnote_e7…   SBC      855 PT=SBC, SSRC=0x0, Seq=31, Time=26368 Frames=7
  2639 495.738886   localhost (Galaxy…  LgInnote_e7…   SBC      855 PT=SBC, SSRC=0x0, Seq=32, Time=27264 Frames=7
  2640 495.740185   controller          host           HCI_EVT    8 Rcvd Number of Completed Packets
  2641 495.758828   localhost (Galaxy…  LgInnote_e7…   SBC      855 PT=SBC, SSRC=0x0, Seq=33, Time=28160 Frames=7
  2642 495.767635   LgInnote_e7:9f:f0…  localhost (…   AVRCP     27 Rcvd Vendor dependent: Notify - RegisterNotification - PlaybackPositionChanged
  2643 495.770372   localhost (Galaxy…  LgInnote_e7…   AVRCP     27 Sent Vendor dependent: Interim - RegisterNotification - PlaybackPositionChanged - SongPosition: 327ms
  2644 495.771298   controller          host           HCI_EVT    8 Rcvd Number of Completed Packets
  2645 495.778869   localhost (Galaxy…  LgInnote_e7…   SBC      855 PT=SBC, SSRC=0x0, Seq=34, Time=29056 Frames=7
```

```
▷ Frame 2630: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits)
▷ Bluetooth
▷ Bluetooth HCI H4
▷ Bluetooth HCI ACL Packet
▷ Bluetooth L2CAP Protocol
▷ Bluetooth AVCTP Protocol
▷ Bluetooth AVRCP Profile
```

```
0000  02 0d 20 85 00 81 00 44  00 82 11 0e 0c 48 00 00   .. ....D .....H..
0010  19 58 20 00 00 74 07 00  00 00 01 00 6a 00 0a eb   .X ..t.. ....j...
0020  84 88 eb 9e 91 20 eb 82  98 00 00 00 02 00 6a 00   ..... .. ......j.
0030  0d ec 95 84 ec 9d b4 ec  9c a0 28 49 55 29 00 00   ........ ..(IU)..
0040  00 03 00 6a 00 11 32 ec  a7 91 20 4c 61 73 74 20   ...j..2. .. Last 
0050  46 61 6e 74 61 73 79 00  00 00 04 00 6a 00 02 34   Fantasy. ....j..4
0060  31 00 00 00 05 00 6a 00  02 35 30 00 00 00 06 00   1.....j. .50.....
0070  6a 00 09 3c 75 6e 6b 6e  6f 77 6e 3e 00 00 00 07   j..<unkn own>....
0080  00 6a 00 06 32 33 39 39  30 38                     .j..2399 08
```

음원 Meta-data

- 제목
- 아티스트
- 앨범
- 제작년도
- 작곡가
- 트랙
- 장르
- 설명



Title: Nara

Artist: Alt-J

Album: This Is All Yours

Year: 2014 Track: 3/14 Genre: Alternative Rock

Comment:

Directory: Y:\Alt-J - This Is All Yours

Album Artist: Alt-J

Composer: Joe Newman/Gus Unger-Hamilton/Thom Green

Discnumber: 1/1

image/jpeg
600x600
312 KB
Front Cover

Filename	Tag	Title	Artist	Album	Track	Disc	Year	Genre
01 Intro.mp3	ID3v2.4	Intro	Alt-J	This Is All Yours	1/14	1/1	2014	Alternative Rock
02 Arrival in Nara.mp3	ID3v2.4	Arrival in Nara	Alt-J	This Is All Yours	2/14	1/1	2014	Alternative Rock
03 Nara.mp3	ID3v2.4	Nara	Alt-J	This Is All Yours	3/14	1/1	2014	Alternative Rock
04 Every Other Freckle....	ID3v2.4	Every Other Freckle	Alt-J	This Is All Yours	4/14	1/1	2014	Alternative Rock
05 Left Hand Free.mp3	ID3v2.4	Left Hand Free	Alt-J	This Is All Yours	5/14	1/1	2014	Alternative Rock
06 Garden Of England – ...	ID3v2.4	Garden Of England – Int...	Alt-J	This Is All Yours	6/14	1/1	2014	Alternative Rock
07 Choice Kingdom.mp3	ID3v2.4	Choice Kingdom	Alt-J	This Is All Yours	7/14	1/1	2014	Alternative Rock
08 Hunger Of The Pine....	ID3v2.4	Hunger Of The Pine	Alt-J	This Is All Yours	8/14	1/1	2014	Alternative Rock
09 Warm Foothills.mp3	ID3v2.4	Warm Foothills	Alt-J	This Is All Yours	9/14	1/1	2014	Alternative Rock
10 The Gospel of John ...	ID3v2.4	The Gospel of John Hurt	Alt-J	This Is All Yours	10/14	1/1	2014	Alternative Rock
11 Pusher.mp3	ID3v2.4	Pusher	Alt-J	This Is All Yours	11/14	1/1	2014	Alternative Rock
12 Bloodflood pt.II.mp3	ID3v2.4	Bloodflood pt.II	Alt-J	This Is All Yours	12/14	1/1	2014	Alternative Rock
13 Leaving Nara.mp3	ID3v2.4	Leaving Nara	Alt-J	This Is All Yours	13/14	1/1	2014	Alternative Rock
14 Lovely Day (Bonus Tr...	ID3v2.4	Lovely Day (Bonus Track)	Alt-J	This Is All Yours	14/14	1/1	2014	Alternative Rock

Ready 1 (00:04:56 | 9,6MB) 14 (00:55:36 | 107,2MB)

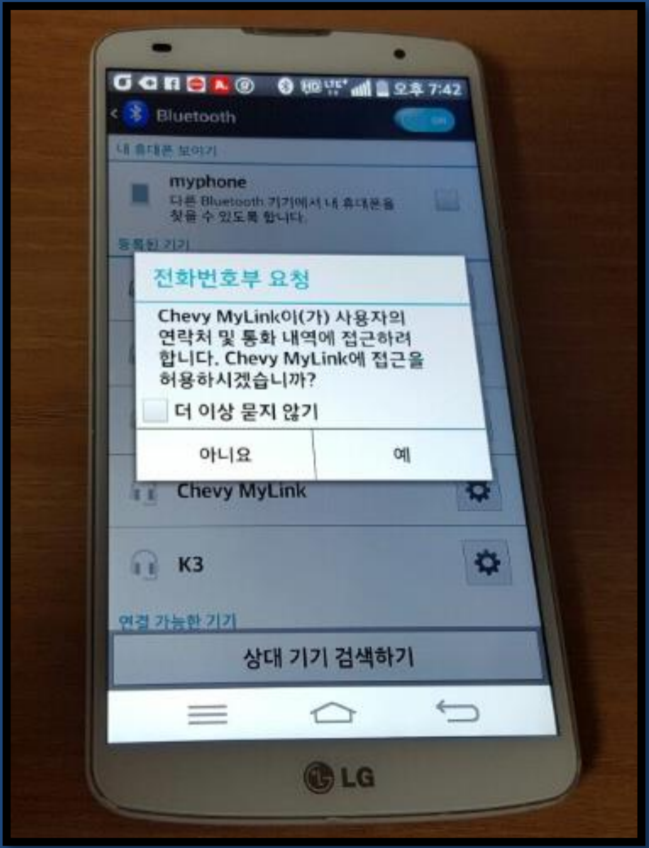
Mp3tag.exe

차량 Bluetooth 공격 벡터들

- AT 커맨드에 대한 응답
  - AT+CNUM, AT+CIND, AT+COPS 등
- 최근 통화 목록, 연락처
  - 이름, 전화번호, 시간정보 등
- 음원 Meta-data
  - 곡명, 작곡가, 발매년도 등
- 휴대폰 이름

Bluetooth Packet 변조

- 스마트폰을 이용한 Bluetooth Packet 변조



전화번호부 요청

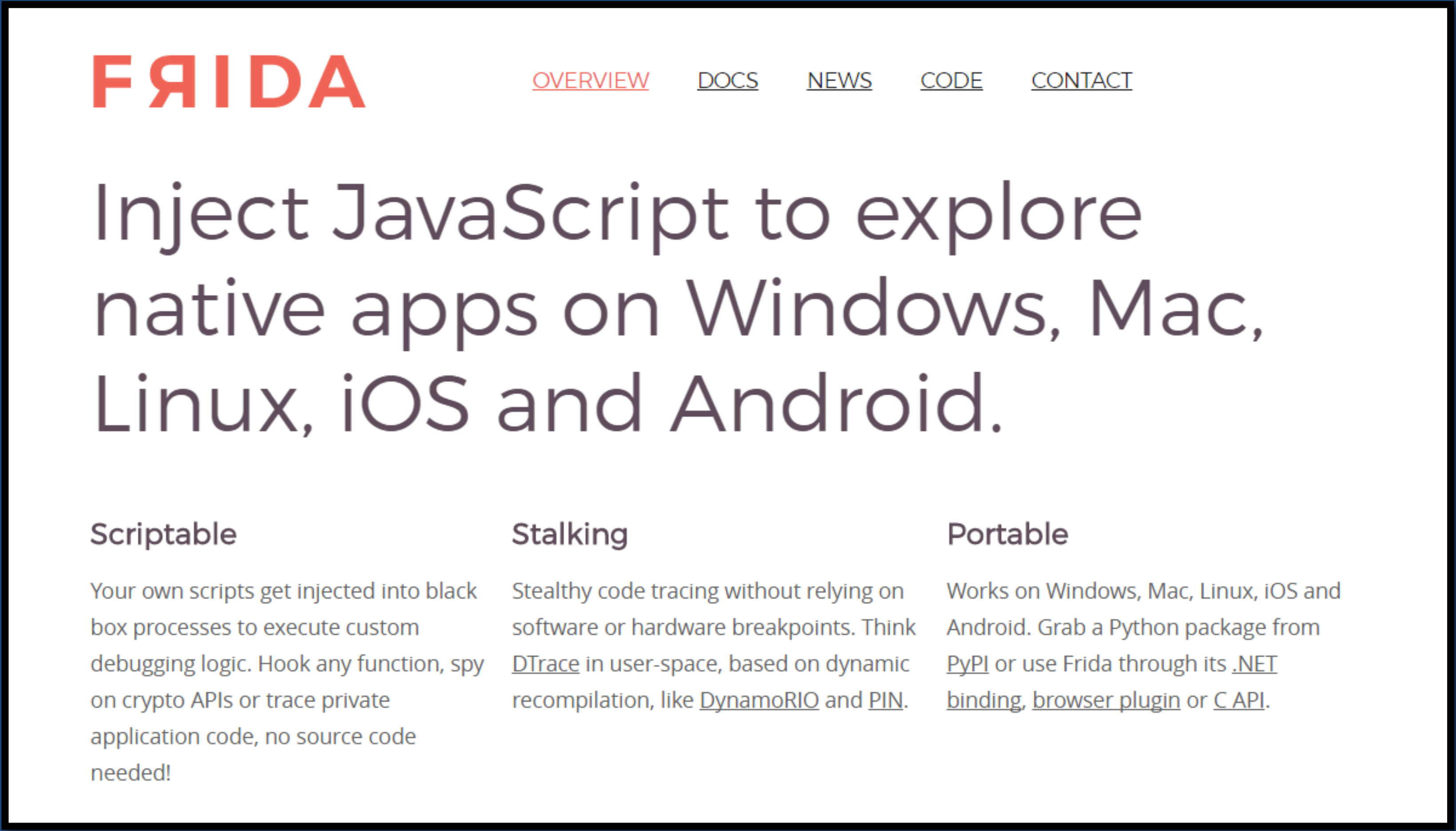
Chevy MyLink이(가) 사용자의 연락처 및 통화 내역에 접근하려 합니다. Chevy MyLink에 접근을 허용하시겠습니까?

□ 더 이상 묻지 않기

방법 1 : 스마트폰 앱 코드 변조
 - repackaging 작업에 긴 시간 소요

방법 2 : 스마트폰 앱 함수 Hooking
 - 동적으로 Packet 변조 가능

FRIDA를 이용한 BT Packet 변조



FRIDA

OVERVIEW DOCS NEWS CODE CONTACT

Inject JavaScript to explore native apps on Windows, Mac, Linux, iOS and Android.

Scriptable

Your own scripts get injected into black box processes to execute custom debugging logic. Hook any function, spy on crypto APIs or trace private application code, no source code needed!

Stalking

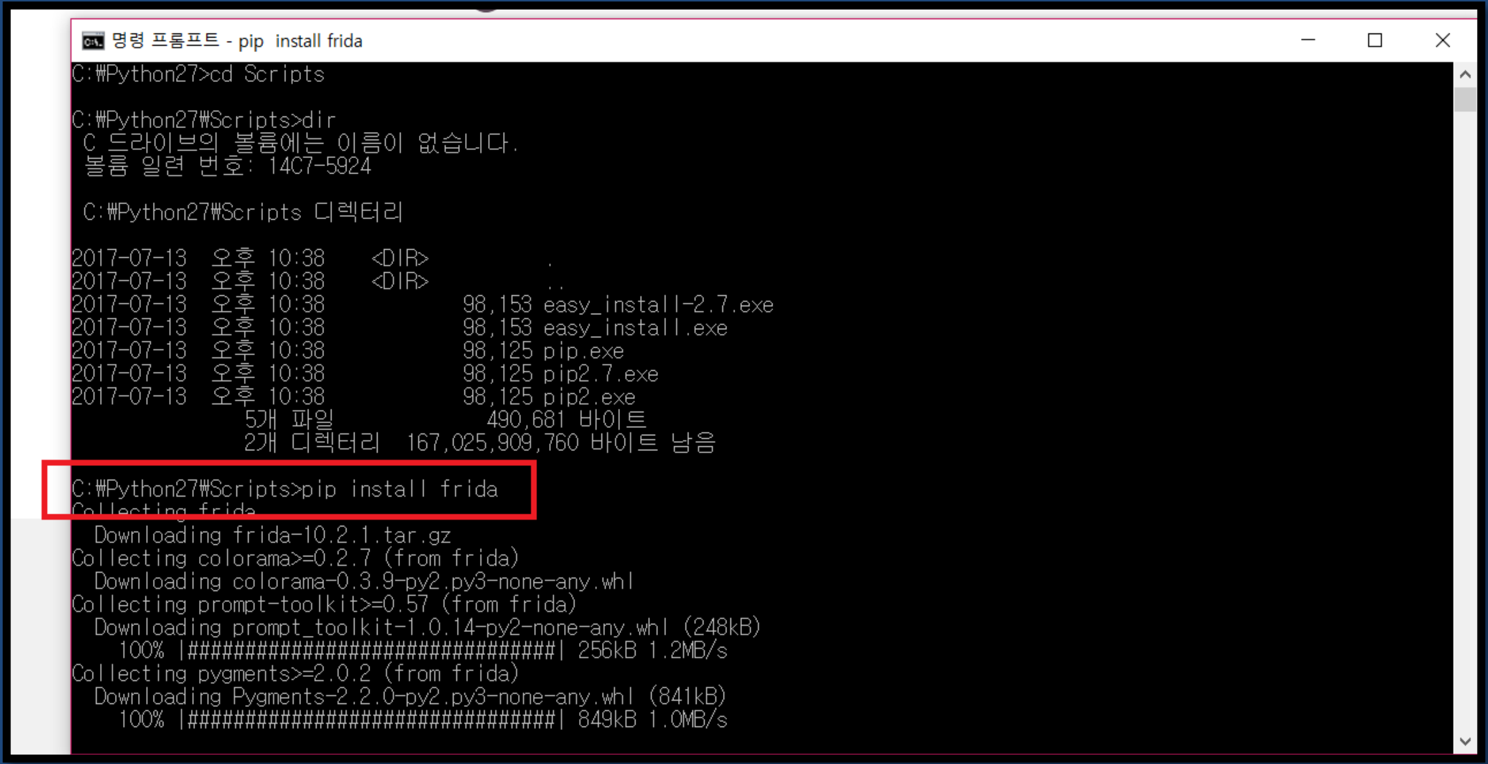
Stealthy code tracing without relying on software or hardware breakpoints. Think DTrace in user-space, based on dynamic recompilation, like DynamoRIO and PIN.

Portable

Works on Windows, Mac, Linux, iOS and Android. Grab a Python package from PyPI or use Frida through its .NET binding, browser plugin or C API.

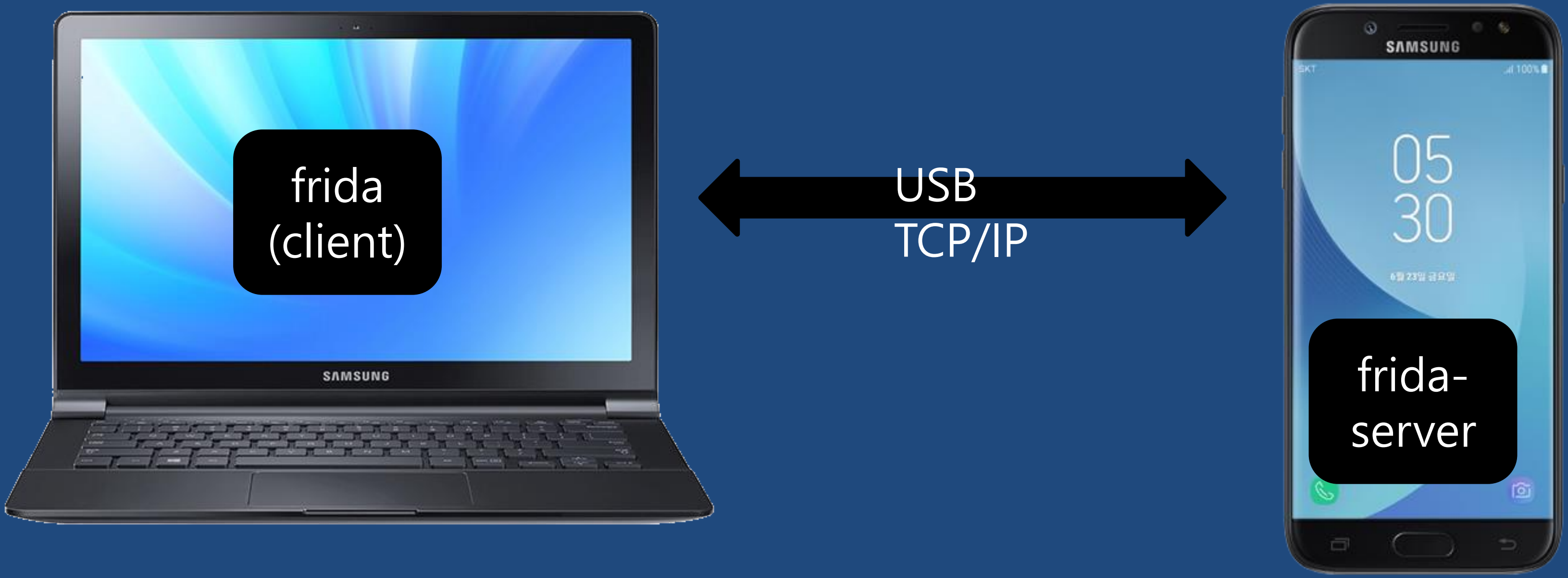
FRIDA 설치

- Python 설치
  - https://www.python.org/ftp/python/2.7.13/python-2.7.13.amd64.msi



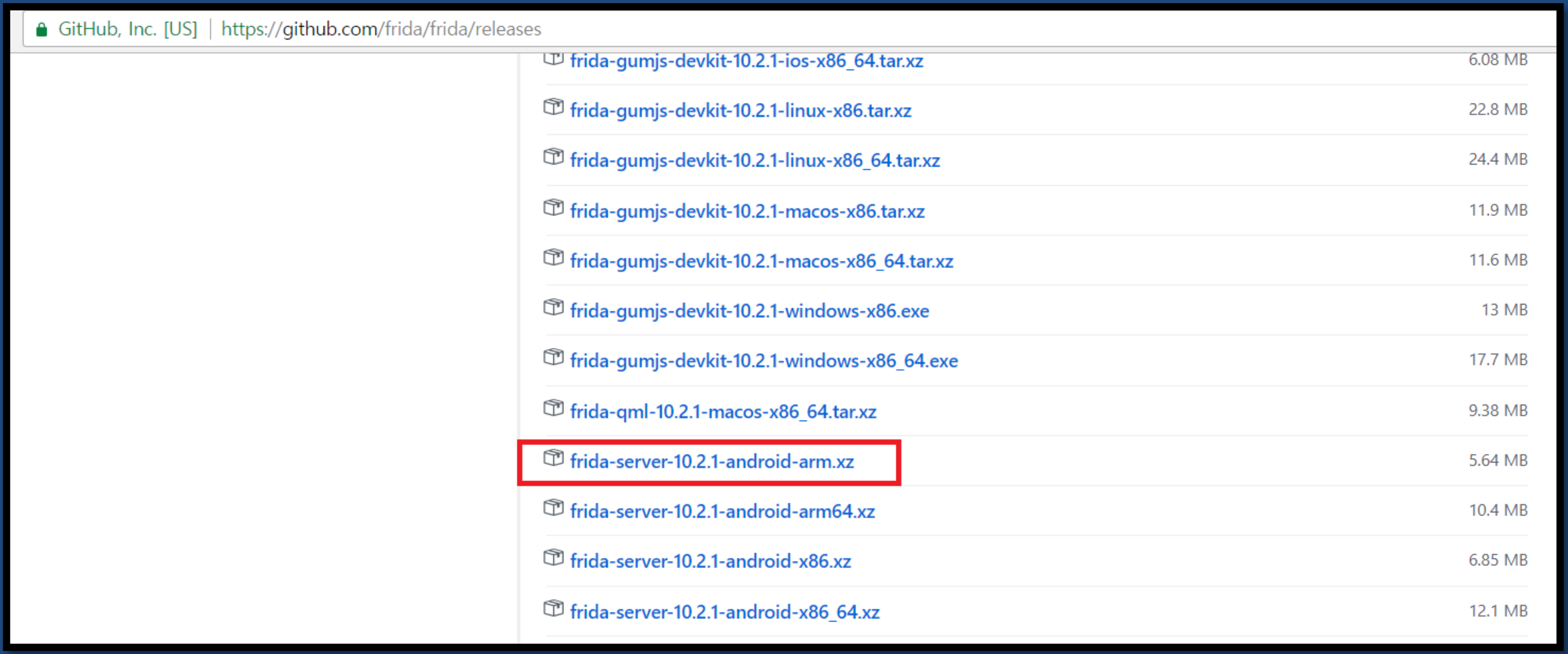
```
C:₩Python27>cd Scripts

C:₩Python27₩Scripts>dir
 C 드라이브의 볼륨에는 이름이 없습니다.
 볼륨 일련 번호: 14C7-5924

 C:₩Python27₩Scripts 디렉터리

2017-07-13  오후 10:38    <DIR>          .
2017-07-13  오후 10:38    <DIR>          ..
2017-07-13  오후 10:38            98,153 easy_install-2.7.exe
2017-07-13  오후 10:38            98,153 easy_install.exe
2017-07-13  오후 10:38            98,125 pip.exe
2017-07-13  오후 10:38            98,125 pip2.7.exe
2017-07-13  오후 10:38            98,125 pip2.exe
               5개 파일             490,681 바이트
               2개 디렉터리  167,025,909,760 바이트 남음

C:₩Python27₩Scripts>pip install frida
Collecting frida
  Downloading frida-10.2.1.tar.gz
Collecting colorama>=0.2.7 (from frida)
  Downloading colorama-0.3.9-py2.py3-none-any.whl
Collecting prompt-toolkit>=0.57 (from frida)
  Downloading prompt_toolkit-1.0.14-py2-none-any.whl (248kB)
    100% |################################| 256kB 1.2MB/s
Collecting pygments>=2.0.2 (from frida)
  Downloading Pygments-2.2.0-py2.py3-none-any.whl (841kB)
    100% |################################| 849kB 1.0MB/s
```

FRIDA의 작동 구조



Frida-server 다운로드

- https://github.com/frida/frida/releases
- http://grayhash.com/training/frida-server.zip



GitHub, Inc. [US] | https://github.com/frida/frida/releases

frida-gumjs-devkit-10.2.1-ios-x86_64.tar.xz	6.08 MB
frida-gumjs-devkit-10.2.1-linux-x86.tar.xz	22.8 MB
frida-gumjs-devkit-10.2.1-linux-x86_64.tar.xz	24.4 MB
frida-gumjs-devkit-10.2.1-macos-x86.tar.xz	11.9 MB
frida-gumjs-devkit-10.2.1-macos-x86_64.tar.xz	11.6 MB
frida-gumjs-devkit-10.2.1-windows-x86.exe	13 MB
frida-gumjs-devkit-10.2.1-windows-x86_64.exe	17.7 MB
frida-qml-10.2.1-macos-x86_64.tar.xz	9.38 MB
frida-server-10.2.1-android-arm.xz	5.64 MB
frida-server-10.2.1-android-arm64.xz	10.4 MB
frida-server-10.2.1-android-x86.xz	6.85 MB
frida-server-10.2.1-android-x86_64.xz	12.1 MB

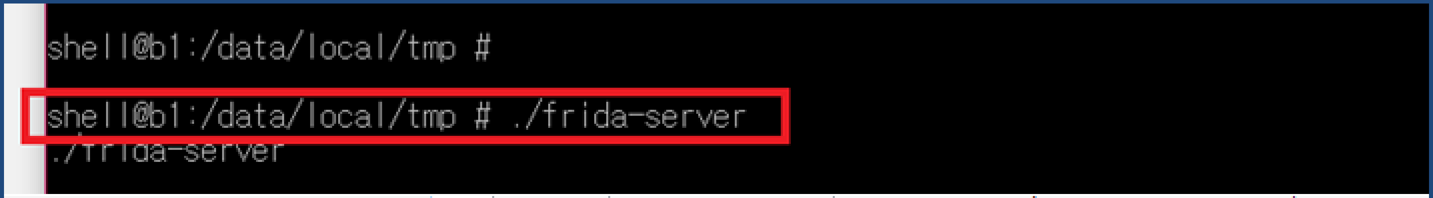
adb 설치 및 실행

- google : adb download
  - http://adbshell.com/downloads

Frida-server 실행

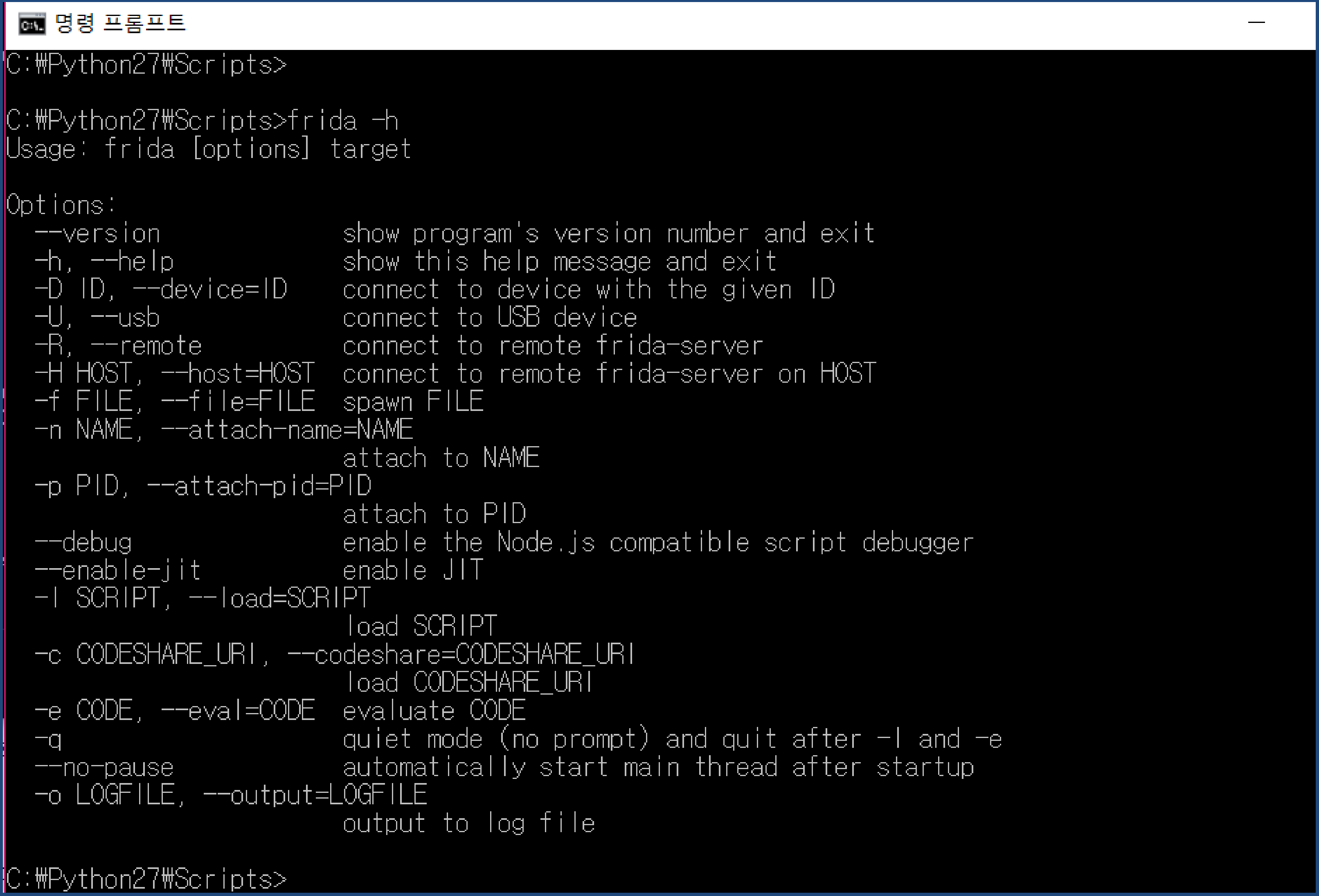
- http://grayhash.com/training/frida-server.zip
- 휴대폰에 업로드 후 root로 실행
  - adb push frida-server /data/local/tmp

- C:₩…₩adb₩ adb shell
- $ su
- # cd /data/local/tmp
- # chmod 777 frida-server
- # ./frida-server



```
shell@b1:/data/local/tmp #
shell@b1:/data/local/tmp # ./frida-server
./frida-server
```

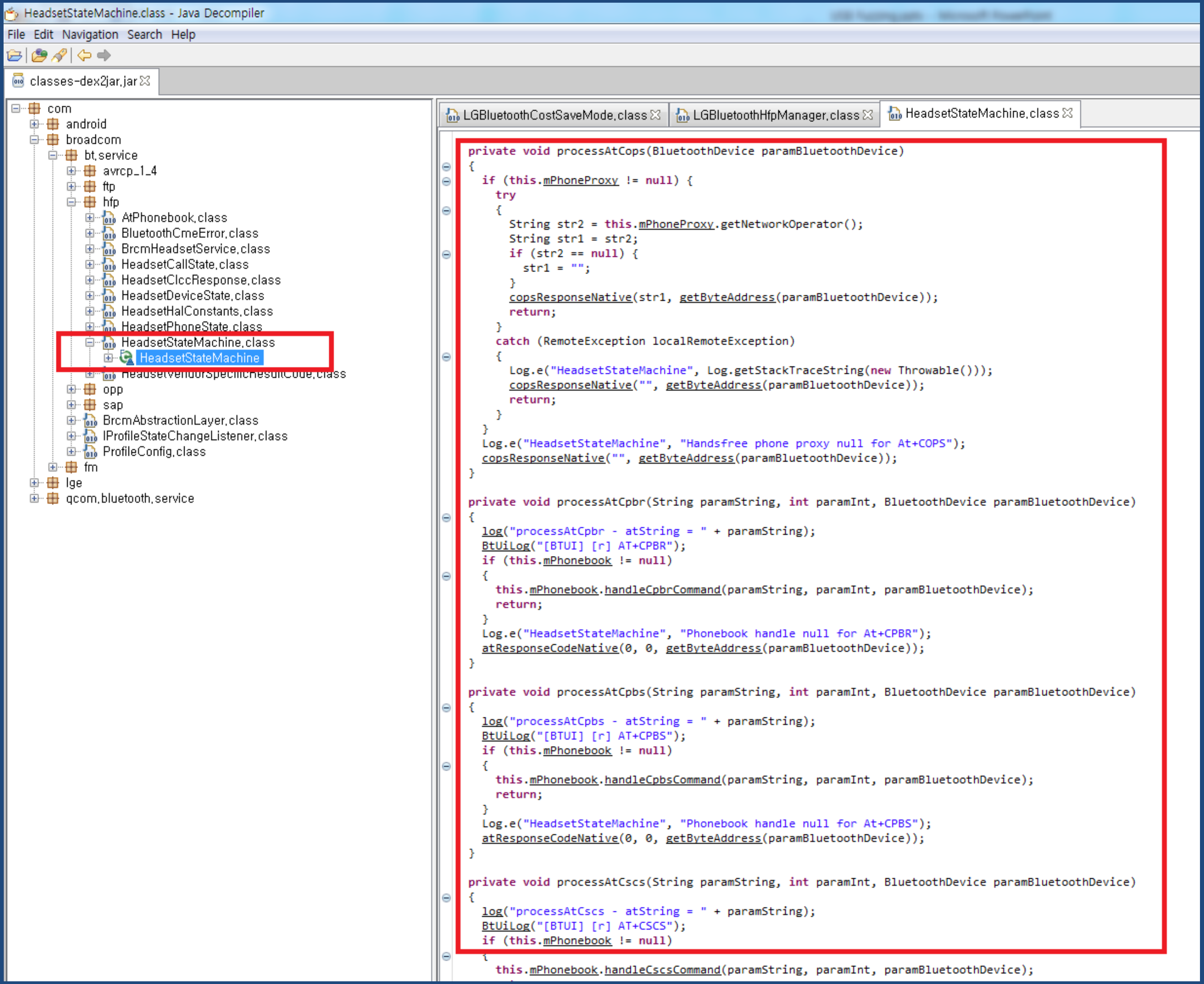
Frida 사용법



```
C:\Python27\Scripts>

C:\Python27\Scripts>frida -h
Usage: frida [options] target

Options:
  --version             show program's version number and exit
  -h, --help            show this help message and exit
  -D ID, --device=ID    connect to device with the given ID
  -U, --usb             connect to USB device
  -R, --remote          connect to remote frida-server
  -H HOST, --host=HOST  connect to remote frida-server on HOST
  -f FILE, --file=FILE  spawn FILE
  -n NAME, --attach-name=NAME
                        attach to NAME
  -p PID, --attach-pid=PID
                        attach to PID
  --debug               enable the Node.js compatible script debugger
  --enable-jit          enable JIT
  -l SCRIPT, --load=SCRIPT
                        load SCRIPT
  -c CODESHARE_URI, --codeshare=CODESHARE_URI
                        load CODESHARE_URI
  -e CODE, --eval=CODE  evaluate CODE
  -q                    quiet mode (no prompt) and quit after -l and -e
  --no-pause            automatically start main thread after startup
  -o LOGFILE, --output=LOGFILE
                        output to log file

C:\Python27\Scripts>
```

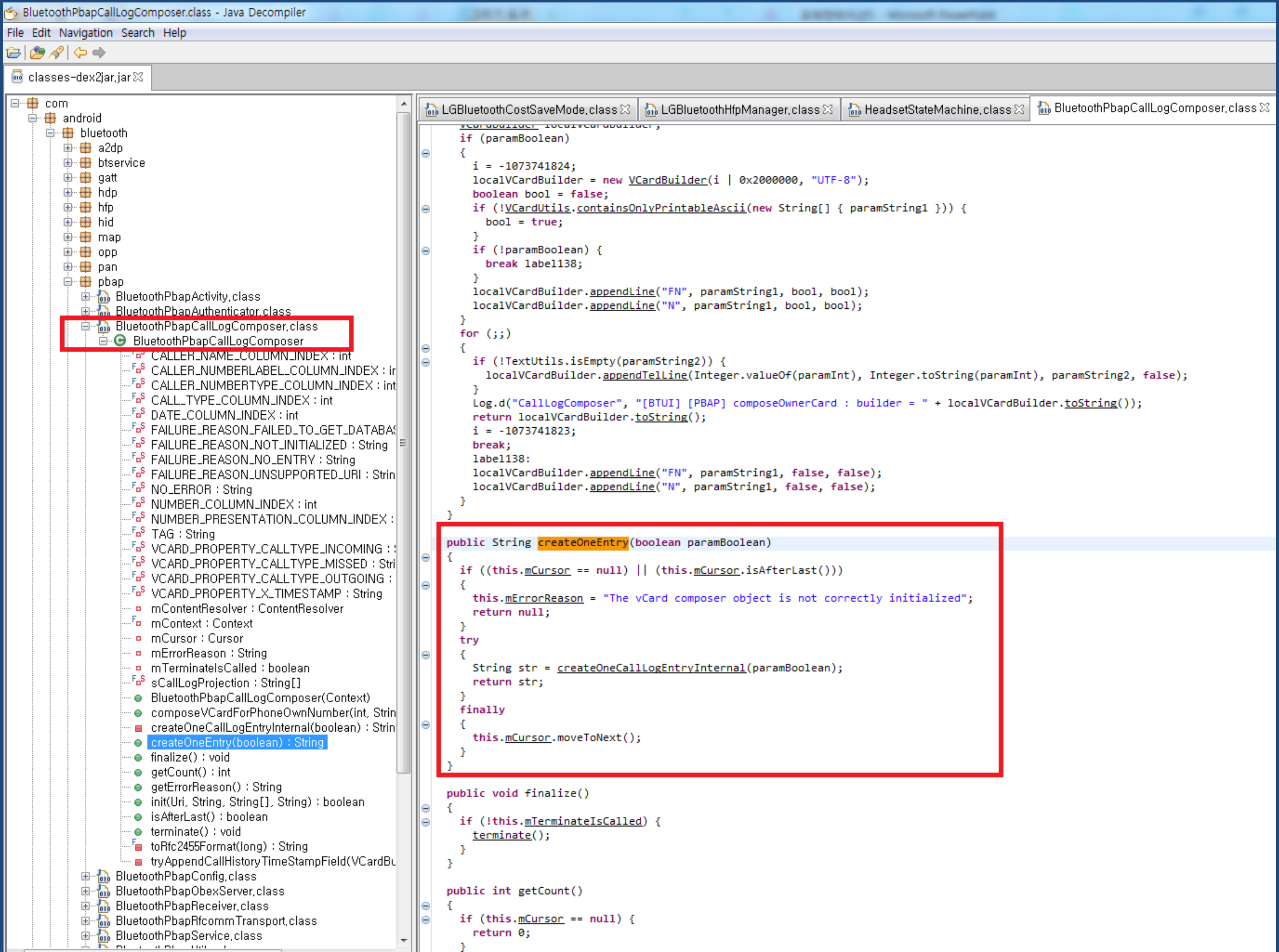
Hooking 구간 파악
- com.android.bluetooth Reversing

AT 커맨드 변조 대상


HeadsetStateMachine.class - Java Decompiler
File Edit Navigation Search Help
classes-dex2jar.jar
com
android
broadcom
bt.service
avrcp_1_4
ftp
hfp
AtPhonebook.class
BluetoothCmeError.class
BrcmHeadsetService.class
HeadsetCallState.class
HeadsetClccResponse.class
HeadsetDeviceState.class
HeadsetHalConstants.class
HeadsetPhoneState.class
HeadsetStateMachine.class
HeadsetStateMachine
HeadsetVendorSpecificResultCode.class
opp
sap
BrcmAbstractionLayer.class
IProfileStateChangeListener.class
ProfileConfig.class
fm
lge
qcom.bluetooth.service
LGBluetoothCostSaveMode.class
LGBluetoothHfpManager.class
HeadsetStateMachine.class

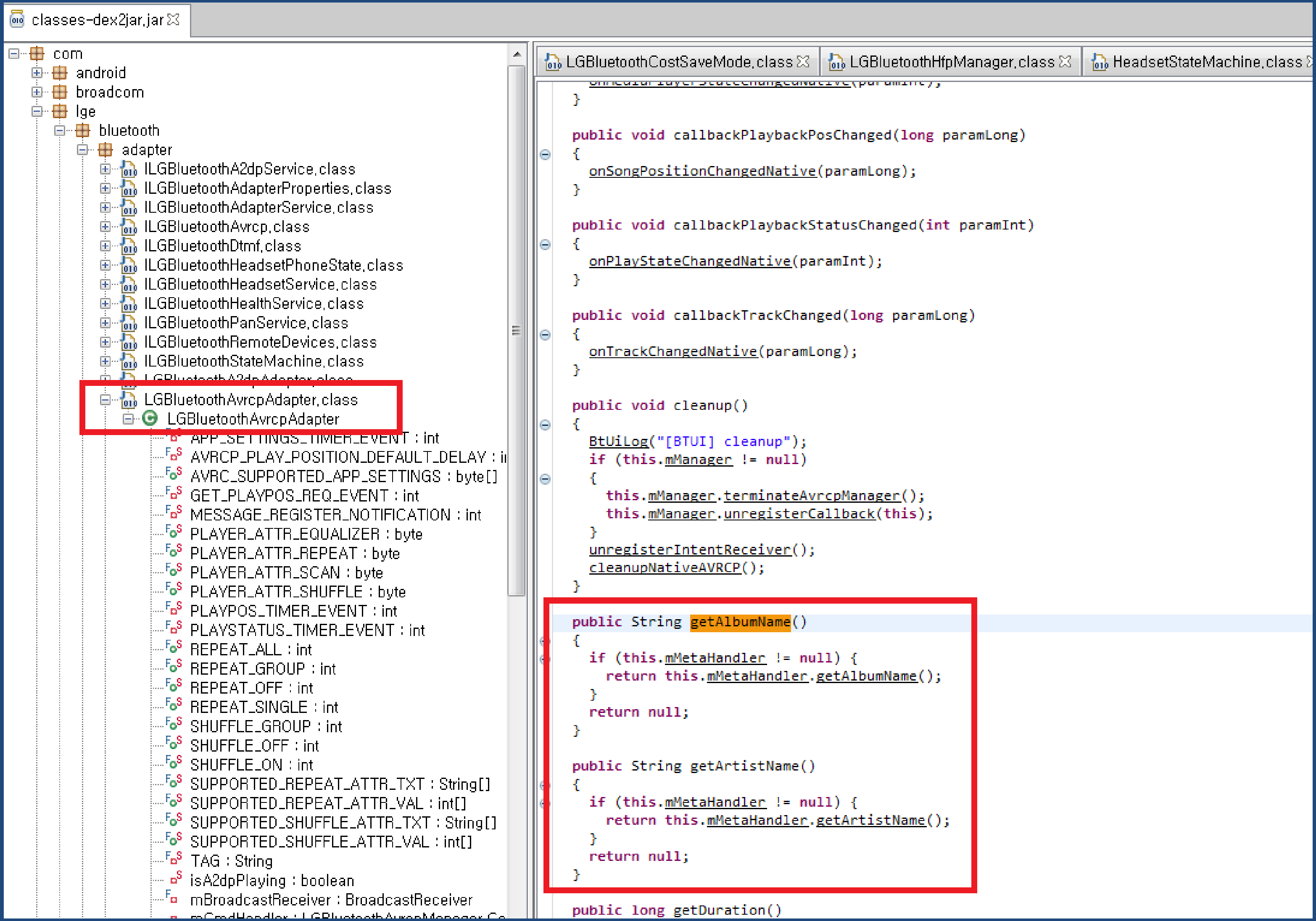
```java
private void processAtCops(BluetoothDevice paramBluetoothDevice)
{
  if (this.mPhoneProxy != null) {
    try
    {
      String str2 = this.mPhoneProxy.getNetworkOperator();
      String str1 = str2;
      if (str2 == null) {
        str1 = "";
      }
      copsResponseNative(str1, getByteAddress(paramBluetoothDevice));
      return;
    }
    catch (RemoteException localRemoteException)
    {
      Log.e("HeadsetStateMachine", Log.getStackTraceString(new Throwable()));
      copsResponseNative("", getByteAddress(paramBluetoothDevice));
      return;
    }
  }
  Log.e("HeadsetStateMachine", "Handsfree phone proxy null for At+COPS");
  copsResponseNative("", getByteAddress(paramBluetoothDevice));
}

private void processAtCpbr(String paramString, int paramInt, BluetoothDevice paramBluetoothDevice)
{
  log("processAtCpbr - atString = " + paramString);
  BtUiLog("[BTUI] [r] AT+CPBR");
  if (this.mPhonebook != null)
  {
    this.mPhonebook.handleCpbrCommand(paramString, paramInt, paramBluetoothDevice);
    return;
  }
  Log.e("HeadsetStateMachine", "Phonebook handle null for At+CPBR");
  atResponseCodeNative(0, 0, getByteAddress(paramBluetoothDevice));
}

private void processAtCpbs(String paramString, int paramInt, BluetoothDevice paramBluetoothDevice)
{
  log("processAtCpbs - atString = " + paramString);
  BtUiLog("[BTUI] [r] AT+CPBS");
  if (this.mPhonebook != null)
  {
    this.mPhonebook.handleCpbsCommand(paramString, paramInt, paramBluetoothDevice);
    return;
  }
  Log.e("HeadsetStateMachine", "Phonebook handle null for At+CPBS");
  atResponseCodeNative(0, 0, getByteAddress(paramBluetoothDevice));
}

private void processAtCscs(String paramString, int paramInt, BluetoothDevice paramBluetoothDevice)
{
  log("processAtCscs - atString = " + paramString);
  BtUiLog("[BTUI] [r] AT+CSCS");
  if (this.mPhonebook != null)
  {
    this.mPhonebook.handleCscsCommand(paramString, paramInt, paramBluetoothDevice);
```

최근 통화 목록 변조 대상


BluetoothPbapCallLogComposer.class - Java Decompiler
File Edit Navigation Search Help
classes-dex2jar.jar
LGBluetoothCostSaveMode.class
LGBluetoothHfpManager.class
HeadsetStateMachine.class
BluetoothPbapCallLogComposer.class
com
android
bluetooth
a2dp
btservice
gatt
hdp
hfp
hid
map
opp
pan
pbap
BluetoothPbapActivity.class
BluetoothPbapAuthenticator.class
BluetoothPbapCallLogComposer.class
BluetoothPbapCallLogComposer
CALLER_NAME_COLUMN_INDEX : int
CALLER_NUMBERLABEL_COLUMN_INDEX : ir
CALLER_NUMBERTYPE_COLUMN_INDEX : int
CALL_TYPE_COLUMN_INDEX : int
DATE_COLUMN_INDEX : int
FAILURE_REASON_FAILED_TO_GET_DATABA
FAILURE_REASON_NOT_INITIALIZED : String
FAILURE_REASON_NO_ENTRY : String
FAILURE_REASON_UNSUPPORTED_URI : Strin
NO_ERROR : String
NUMBER_COLUMN_INDEX : int
NUMBER_PRESENTATION_COLUMN_INDEX :
TAG : String
VCARD_PROPERTY_CALLTYPE_INCOMING :
VCARD_PROPERTY_CALLTYPE_MISSED : Stri
VCARD_PROPERTY_CALLTYPE_OUTGOING :
VCARD_PROPERTY_X_TIMESTAMP : String
mContentResolver : ContentResolver
mContext : Context
mCursor : Cursor
mErrorReason : String
mTerminateIsCalled : boolean
sCallLogProjection : String[]
BluetoothPbapCallLogComposer(Context)
composeVCardForPhoneOwnNumber(int, Strin
createOneCallLogEntryInternal(boolean) : Strin
createOneEntry(boolean) : String
finalize() : void
getCount() : int
getErrorReason() : String
init(Uri, String, String[], String) : boolean
isAfterLast() : boolean
terminate() : void
toRfc2455Format(long) : String
tryAppendCallHistoryTimeStampField(VCardBu
BluetoothPbapConfig.class
BluetoothPbapObexServer.class
BluetoothPbapReceiver.class
BluetoothPbapRfcommTransport.class
BluetoothPbapService.class

```java
    VCardBuilder localVCardBuilder;
    if (paramBoolean)
    {
      i = -1073741824;
      localVCardBuilder = new VCardBuilder(i | 0x2000000, "UTF-8");
      boolean bool = false;
      if (!VCardUtils.containsOnlyPrintableAscii(new String[] { paramString1 })) {
        bool = true;
      }
      if (!paramBoolean) {
        break label138;
      }
      localVCardBuilder.appendLine("FN", paramString1, bool, bool);
      localVCardBuilder.appendLine("N", paramString1, bool, bool);
    }
    for (;;)
    {
      if (!TextUtils.isEmpty(paramString2)) {
        localVCardBuilder.appendTelLine(Integer.valueOf(paramInt), Integer.toString(paramInt), paramString2, false);
      }
      Log.d("CallLogComposer", "[BTUI] [PBAP] composeOwnerCard : builder = " + localVCardBuilder.toString());
      return localVCardBuilder.toString();
      i = -1073741823;
      break;
      label138:
      localVCardBuilder.appendLine("FN", paramString1, false, false);
      localVCardBuilder.appendLine("N", paramString1, false, false);
    }
  }

  public String createOneEntry(boolean paramBoolean)
  {
    if ((this.mCursor == null) || (this.mCursor.isAfterLast()))
    {
      this.mErrorReason = "The vCard composer object is not correctly initialized";
      return null;
    }
    try
    {
      String str = createOneCallLogEntryInternal(paramBoolean);
      return str;
    }
    finally
    {
      this.mCursor.moveToNext();
    }
  }

  public void finalize()
  {
    if (!this.mTerminateIsCalled) {
      terminate();
    }
  }

  public int getCount()
  {
    if (this.mCursor == null) {
      return 0;
    }
```

음원 meta-data 변조 대상



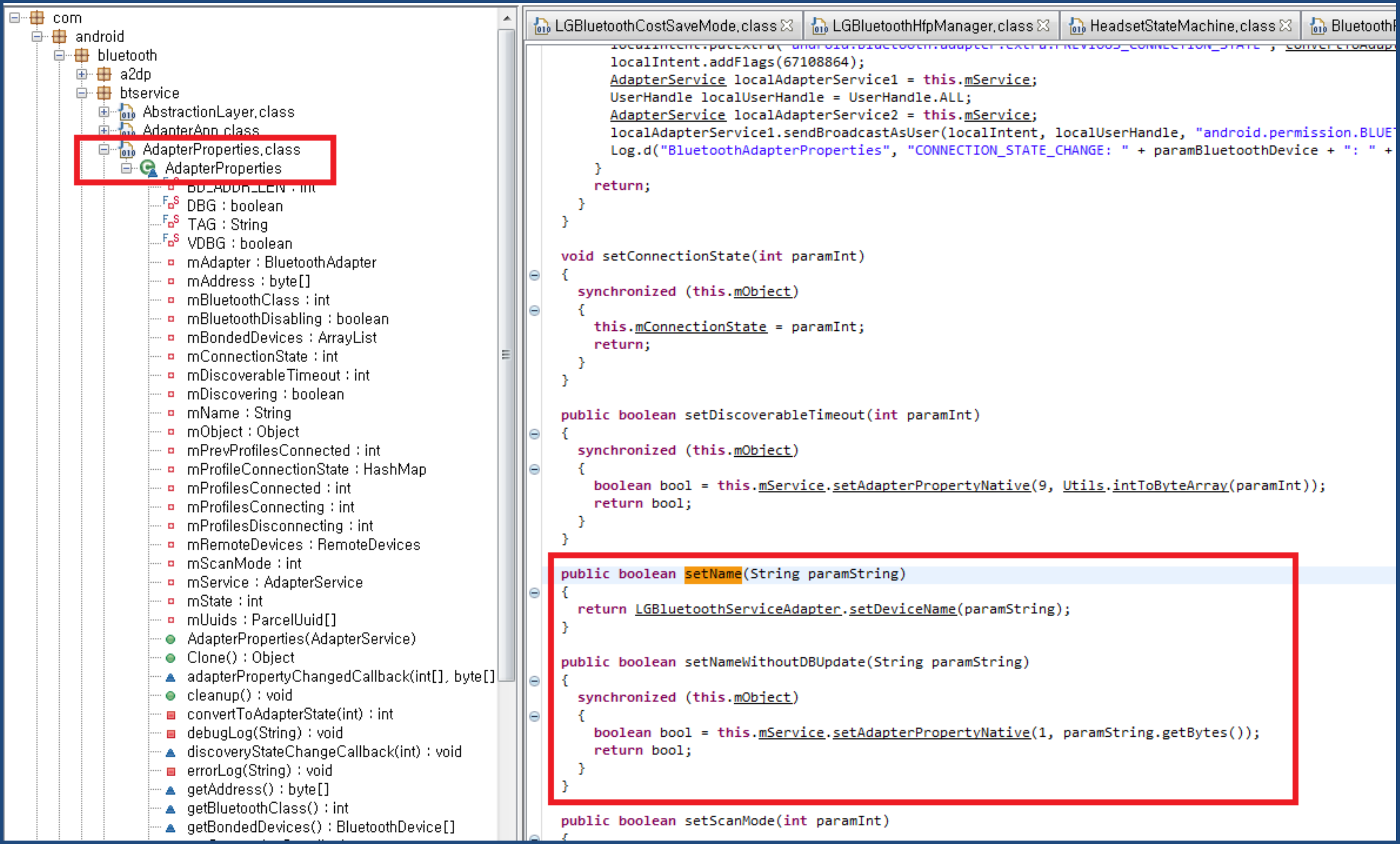
classes-dex2jar.jar

```
com
  android
  broadcom
  lge
    bluetooth
      adapter
        ILGBluetoothA2dpService.class
        ILGBluetoothAdapterProperties.class
        ILGBluetoothAdapterService.class
        ILGBluetoothAvrcp.class
        ILGBluetoothDtmf.class
        ILGBluetoothHeadsetPhoneState.class
        ILGBluetoothHeadsetService.class
        ILGBluetoothHealthService.class
        ILGBluetoothPanService.class
        ILGBluetoothRemoteDevices.class
        ILGBluetoothStateMachine.class
        LGBluetoothA2dpAdapter.class
        LGBluetoothAvrcpAdapter.class
          LGBluetoothAvrcpAdapter
            APP_SETTINGS_TIMER_EVENT : int
            AVRCP_PLAY_POSITION_DEFAULT_DELAY : i
            AVRC_SUPPORTED_APP_SETTINGS : byte[]
            GET_PLAYPOS_REQ_EVENT : int
            MESSAGE_REGISTER_NOTIFICATION : int
            PLAYER_ATTR_EQUALIZER : byte
            PLAYER_ATTR_REPEAT : byte
            PLAYER_ATTR_SCAN : byte
            PLAYER_ATTR_SHUFFLE : byte
            PLAYPOS_TIMER_EVENT : int
            PLAYSTATUS_TIMER_EVENT : int
            REPEAT_ALL : int
            REPEAT_GROUP : int
            REPEAT_OFF : int
            REPEAT_SINGLE : int
            SHUFFLE_GROUP : int
            SHUFFLE_OFF : int
            SHUFFLE_ON : int
            SUPPORTED_REPEAT_ATTR_TXT : String[]
            SUPPORTED_REPEAT_ATTR_VAL : int[]
            SUPPORTED_SHUFFLE_ATTR_TXT : String[]
            SUPPORTED_SHUFFLE_ATTR_VAL : int[]
            TAG : String
            isA2dpPlaying : boolean
            mBroadcastReceiver : BroadcastReceiver
            mCmdHandler : LGBluetoothAvrcpManager.Ca
```

LGBluetoothCostSaveMode.class | LGBluetoothHfpManager.class | HeadsetStateMachine.class

```java
  onPlayerStateChangedNative(paramInt);
}

public void callbackPlaybackPosChanged(long paramLong)
{
  onSongPositionChangedNative(paramLong);
}

public void callbackPlaybackStatusChanged(int paramInt)
{
  onPlayStateChangedNative(paramInt);
}

public void callbackTrackChanged(long paramLong)
{
  onTrackChangedNative(paramLong);
}

public void cleanup()
{
  BtUiLog("[BTUI] cleanup");
  if (this.mManager != null)
  {
    this.mManager.terminateAvrcpManager();
    this.mManager.unregisterCallback(this);
  }
  unregisterIntentReceiver();
  cleanupNativeAVRCP();
}

public String getAlbumName()
{
  if (this.mMetaHandler != null) {
    return this.mMetaHandler.getAlbumName();
  }
  return null;
}

public String getArtistName()
{
  if (this.mMetaHandler != null) {
    return this.mMetaHandler.getArtistName();
  }
  return null;
}

public long getDuration()
```

휴대폰 이름 변조 대상


LGBluetoothCostSaveMode.class
LGBluetoothHfpManager.class
HeadsetStateMachine.class
BluetoothF

```
com
  android
    bluetooth
      a2dp
      btservice
        AbstractionLayer.class
        AdapterApp.class
        AdapterProperties.class
          AdapterProperties
            BD_ADDR_LEN : int
            DBG : boolean
            TAG : String
            VDBG : boolean
            mAdapter : BluetoothAdapter
            mAddress : byte[]
            mBluetoothClass : int
            mBluetoothDisabling : boolean
            mBondedDevices : ArrayList
            mConnectionState : int
            mDiscoverableTimeout : int
            mDiscovering : boolean
            mName : String
            mObject : Object
            mPrevProfilesConnected : int
            mProfileConnectionState : HashMap
            mProfilesConnected : int
            mProfilesConnecting : int
            mProfilesDisconnecting : int
            mRemoteDevices : RemoteDevices
            mScanMode : int
            mService : AdapterService
            mState : int
            mUuids : ParcelUuid[]
            AdapterProperties(AdapterService)
            Clone() : Object
            adapterPropertyChangedCallback(int[], byte[]
            cleanup() : void
            convertToAdapterState(int) : int
            debugLog(String) : void
            discoveryStateChangeCallback(int) : void
            errorLog(String) : void
            getAddress() : byte[]
            getBluetoothClass() : int
            getBondedDevices() : BluetoothDevice[]
```

```java
        localIntent.putExtra("android.bluetooth.adapter.extra.PREVIOUS_CONNECTION_STATE", convertToAdap
        localIntent.addFlags(67108864);
        AdapterService localAdapterService1 = this.mService;
        UserHandle localUserHandle = UserHandle.ALL;
        AdapterService localAdapterService2 = this.mService;
        localAdapterService1.sendBroadcastAsUser(localIntent, localUserHandle, "android.permission.BLUE
        Log.d("BluetoothAdapterProperties", "CONNECTION_STATE_CHANGE: " + paramBluetoothDevice + ": " +
      }
      return;
    }
  }

  void setConnectionState(int paramInt)
  {
    synchronized (this.mObject)
    {
      this.mConnectionState = paramInt;
      return;
    }
  }

  public boolean setDiscoverableTimeout(int paramInt)
  {
    synchronized (this.mObject)
    {
      boolean bool = this.mService.setAdapterPropertyNative(9, Utils.intToByteArray(paramInt));
      return bool;
    }
  }

  public boolean setName(String paramString)
  {
    return LGBluetoothServiceAdapter.setDeviceName(paramString);
  }

  public boolean setNameWithoutDBUpdate(String paramString)
  {
    synchronized (this.mObject)
    {
      boolean bool = this.mService.setAdapterPropertyNative(1, paramString.getBytes());
      return bool;
    }
  }

  public boolean setScanMode(int paramInt)
  {
```

최근 통화 목록 변조 예제

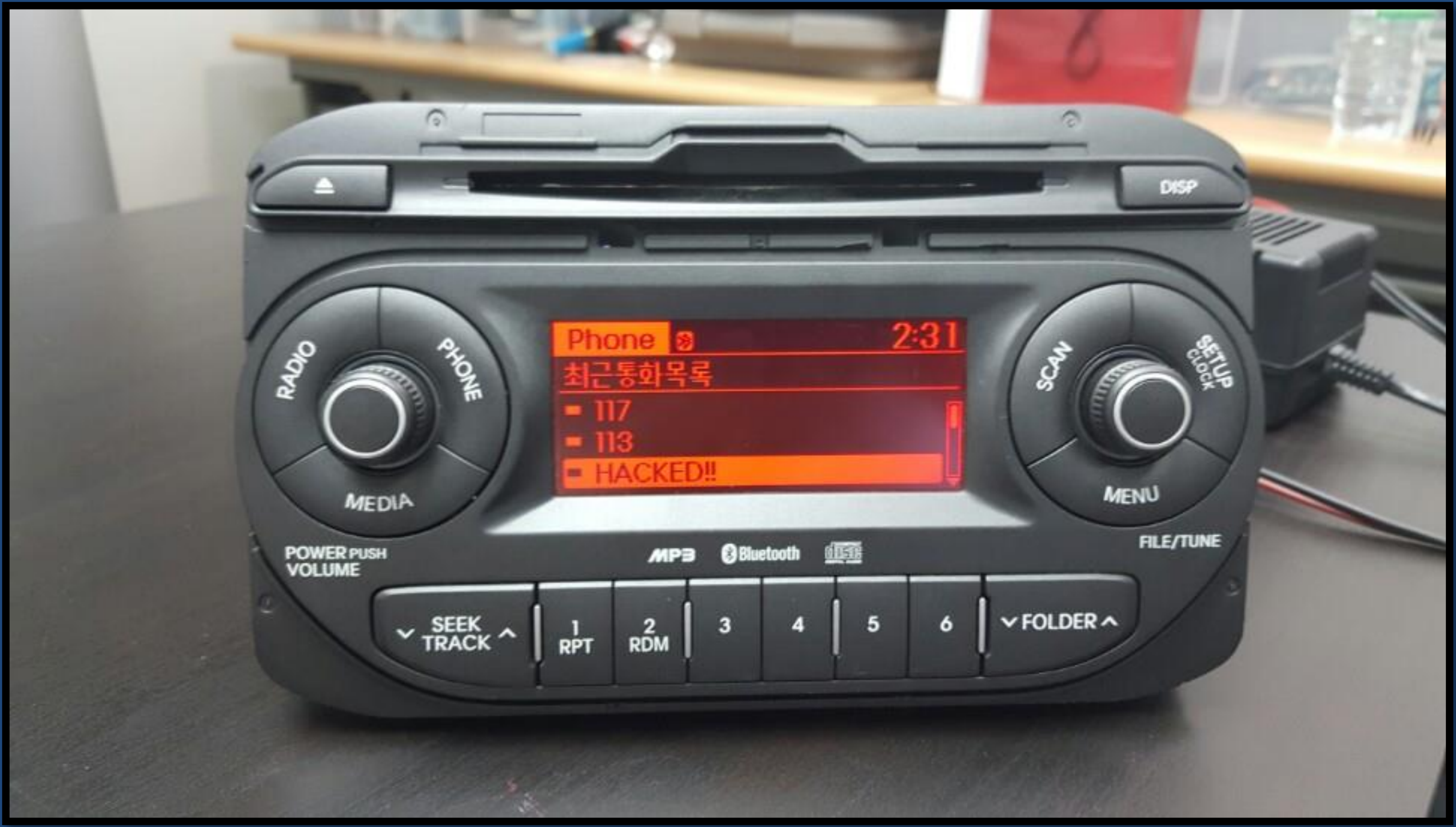
```
Java.perform(function(){
        var cls = Java.use("com.android.bluetooth.pbap.BluetoothPbapCallLogComposer");

        cls.createOneEntry.implementation = function(arg){
          pbcall =  this.createOneEntry.call(this, arg);

          console.log("createOneEntry called");

          pbcall = pbcall.replace(/112/gi, "HACKED!!");
          return pbcall;
        };
});
```

[hook_test.js]

```
Scripts₩frida -U -l hook_test.js com.android.bluetooth
```

-U : USB 디바이스 연결
-l : 스크립트 실행
com.android.bluetooth : 후킹 대상 프로세스

최근 통화 목록 변조 예시


Phone
2:31
최근통화목록
117
113
HACKED!!
DISP
RADIO
PHONE
MEDIA
SCAN
SETUP
CLOCK
MENU
POWER PUSH
VOLUME
MP3
Bluetooth
FILE/TUNE
SEEK
TRACK
1
RPT
2
RDM
3
4
5
6
FOLDER

Bluetooth Hacking 결론

- 최신 장비들은 블루투스 통신을 이용하여 다양한 정보들을 주고받을 수 있음

- 스마트폰이 장비로 송신하는 Bluetooth Packet을 변조하여 취약점 유발 가능

- Bluetooth는 공격자에게 굉장히 좋은 Remote Attack Surface가 될 수 있음

Q/A

감사합니다.