

摩托罗拉 C118 基于 Osmocom-BB & OpenBTS 搭建小型短信基站

0x00 写在前面

大家应该都听说过摩托罗拉 C118 配合 Osmocom-BB 实现 GSM 网络下的短信拦截功能吧，在 14 年左右新出了一种玩法就是 Osmocom-BB 的 [sylvain/testing](#) 分支固件可以配合 OpenBTS，借助周围信号强度较大的 ARFCN 伪造出一个新的基站信号。不过由于摩托罗拉 C118 的问题，无法实现语音通话功能只可以发送短信（默认只可以发送英文短信，修改源码可以实现发送中文短信）

以下内容将会指导你怎样用 Osmocom-bb 兼容的手机(如 c115,c118,c123 等)当作 OpenBTS 的无线收发机。

0x01 环境

已顺利编译运行过 Osmocombb 的可继续往下看,否则请参考[官方链接](#)或[优秀文章](#)

首先安装 libosmo-dsp 库

先下载

```
$ git clone git://git.osmocom.org/libosmo-dsp.git
```

编译前需要安装 fftw3

```
$ apt-get install libfftw3-3 libfftw3-dev libfftw3-doc
```

然后编译

```
$ cd libosmo-dsp
```

```
$ autoreconf -i
```

```
$ ./configure
```

```
$ make
```

```
$ makeinstall
```

0x02 Osmocom-BB

采用 sylvain/testing 分支（具体可看[WIKI](#)）

先下载

```
$ git clone git://git.osmocom.org/osmocom-bb.git
```

再切换分支编译

```
$ cd osmocom-bb
$ git checkout sylvain/testing
```

默认编译出的版本发送信号相关的功能是被注释掉的，用 mobile 启动 layer23 后会一直处于搜信号的过程中，因为无法发送信号。

把 osmocom-bb/src/target/firmware 下的 Makefile 中的 DCONFIG_TX_ENABLE 宏打开：

```
# Uncomment this line if you want to enable Tx (Transmit) Support.
#CFLAGS += -DCONFIG_TX_ENABLE
```

然后到 src 目录下编译

```
$ cd src make HOST_layer23_CONFARGS=--enable-transceiver
```

0x03 OpenBTS

这里使用的 OpenBTS 的版本是 OpenBts-p2.8 (嫌手动编译麻烦的可以找我要 DEB 安装的教程)，首先安装依赖

```
$ sudo apt-get install autoconf libtool libosip2-dev libortp-dev libusb-1.0-0-dev g++ sqlite3
libsqlite3-dev erlang libreadline6-dev libncurses5-dev
```

下载源码

```
$ svn co http://wush.net/svn/range/software/public (svn 版本必须 <= 1.7)
```

然后编译安装 (有不懂的可以前往 [WIKI](#) 查看详细资料)

```
$ cd a53/trunk
```

```
$ make install
```

```
$ cd openbts/trunk
```

```
$ autoreconf -i
```

```
$ ./configure
```

```
$ make
```

```
$ mkdir /etc/OpenBTS
```

```
$ sqlite3 -init ./apps/OpenBTS.example.sql /etc/OpenBTS/OpenBTS.db ".quit"
```

```
$ mkdir -p /var/lib/asterisk/sqlite3dir
```

```

$ cd subscriberRegistry/trunk
$ make
$ sqlite3 -init subscriberRegistry.example.sql /etc/OpenBTS/sipauthserve.db ".quit"

$ cd smqueue/trunk
$ autoreconf -i
$ ./configure
$ make
$ sqlite3 -init smqueue/smqueue.example.sql /etc/OpenBTS/smqueue.db ".quit"

```

安装 OpenBTS 后按照 [WIKI](#) 的说明配置/etc/OpenBTS/OpenBTS.db

首先安装数据库编译软件

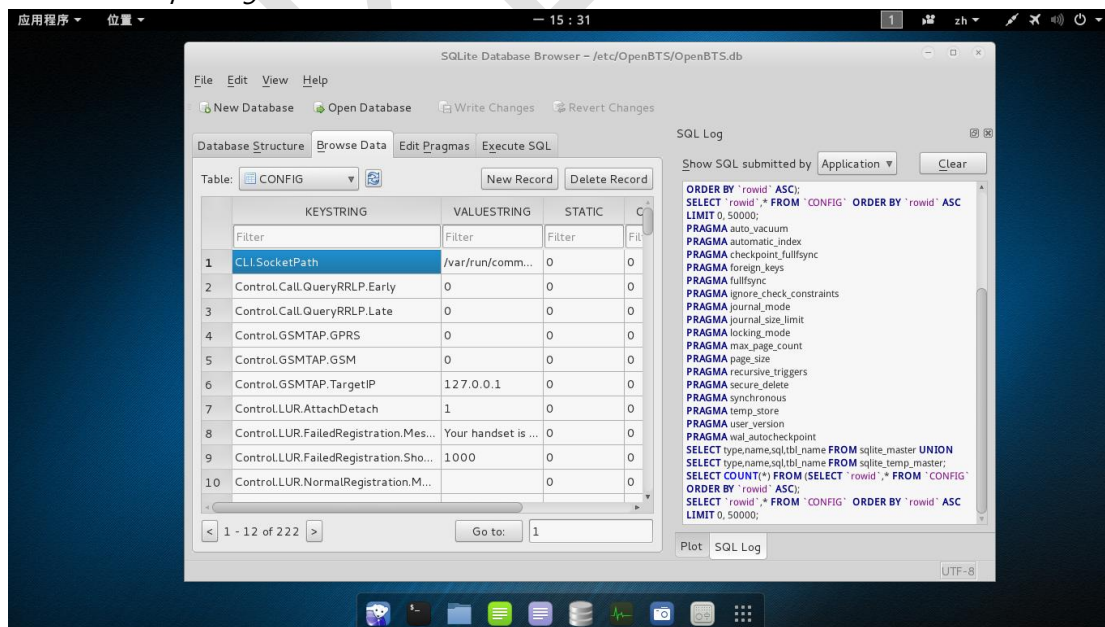
```
$ apt-get install sqlite3 sqliteman ( ubuntu 系统安装 , Kali 自带 sqlitebrowser 无需安装 )
```

然后在终端内输入 sqliteman 启动软件，打开/etc/OpenBTS/目录下的 OpenBTS.db 文件

```

Control.GSMTAP.TargetIP = 127.0.0.1
GSM.Radio.NeedBSIC = 1
GSM.Radio.Band = 900
GSM.CellSelection.Neighbors =(留空)
GSM.RACH.MaxRetrans = 3
GSM.RACH.TxInteger = 8
GSM.Radio.C0 = ( 发射的频点 , 数值1-124之间 )
Control.LUR.OpenRegistration =.*

```



0x04 刷入固件

用 osmocon 程序将 trx.compalam.bin 刷入手机

命令

```
$ sudo ./osmocon -p /dev/ttyUSB0 -m c123xor ../../target/firmware/board/compal_e88/trx.compalam.bin
```

```
root@h4ck0ne: /opt/osmocom-bb2/src/host/osmocon# lsusb
Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 009: ID 10c4:ea60 Cygnal Integrated Products, Inc. CP210x UART Bridge / myAVR mySmartUSB light
Bus 001 Device 004: ID 0a0f:0008 VMware, Inc.
Bus 001 Device 003: ID 0a0f:0002 VMware, Inc. Virtual USB Hub
Bus 001 Device 002: ID 0a0f:0003 VMware, Inc. Virtual Mouse
Bus 001 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
root@h4ck0ne: /opt/osmocom-bb2/src/host/osmocon# ./osmocon -p /dev/ttyUSB0 -m c123xor ../../target/firmware/board/compal_e88/trx.compalam.bin
got 1 bytes from modem, data looks like: ff .
got 2 bytes from modem, data looks like: 04 81 .
got 4 bytes from modem, data looks like: 1b f6 02 00 ....
got 1 bytes from modem, data looks like: 41 A
got 1 bytes from modem, data looks like: 01 .
got 1 bytes from modem, data looks like: 40 @
Received PROMPT1 from phone, responding with CMD
read_file(../../target/firmware/board/compal_e88/trx.compalam.bin): file_size=62880, hdr_len=4, dload_len=62887
got 1 bytes from modem, data looks like: 1b .
got 1 bytes from modem, data looks like: f6 .
got 1 bytes from modem, data looks like: 02 .
got 1 bytes from modem, data looks like: 00 .
got 1 bytes from modem, data looks like: 41 A
got 1 bytes from modem, data looks like: 02 .
got 1 bytes from modem, data looks like: 43 C
Received PROMPT2 from phone, starting download
handle_write(): 4096 bytes (4096/62887)
handle_write(): 4096 bytes (8192/62887)
```

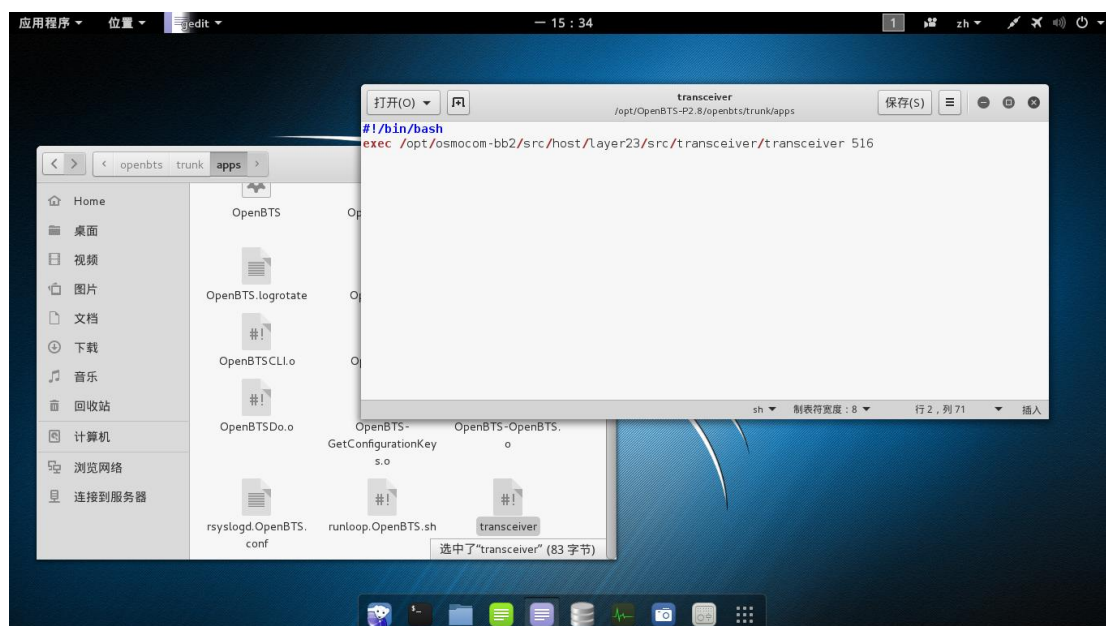
0x05 开始执行

到 OpenBTS/apps 目录下,将 transceiver 重命名为 transceiver.bak 新建脚本文件 transceiver 内容如下

```
#!/bin/bash exec <your path to osmocom-bb>/src/host/layer23/src/transceiver/transceiver <ARFCN>
```

<your path to osmocom-bb>替换成你自己的路径,<ARFCN>替换成附近信号最强的

ARFCN 号



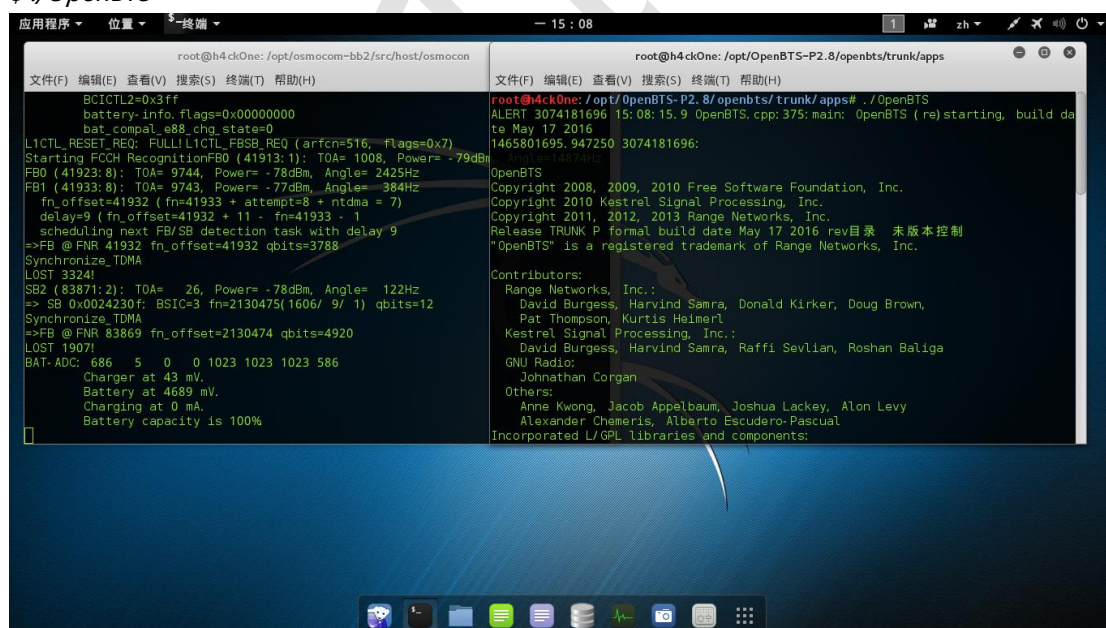
赋予执行权限

`chmod +x transceiver`

然后开 4 个终端窗口分别执行

`$ cd openbts/trunk/apps`

`$ ./OpenBTS`



`$ cd subscriberRegistry/trunk`

`$ ./sipauthserve(开启注册服务)`

```

root@h4ckOne: /opt/osmocom-bb2/src/osmocom
Battery capacity is 100%
Battery range is 3199..3999 mV.
Battery full at 468 LSB ... full at 585 LSB
Charging at 239 LSB (204 mA).
BCICL2=0x3ff
battery.info.flags=0x00000000
bat_compall_e88_chg_state=0
BAT-ADC: 664 6 0 0 1023 1023 1023 583
Charger at 51 mV.
Battery at 4539 mV.
Charging at 0 mA.
Battery capacity is 100%
Battery range is 3199..3999 mV.
Battery full at 468 LSB ... full at 585 LSB
Charging at 239 LSB (204 mA).
BCICL2=0x3ff
battery.info.flags=0x00000000

root@h4ckOne: /opt/OpenBTS-P2.8/subscriberRegistry/trunk
root@h4ckOne: /opt/OpenBTS-P2.8/subscriberRegistry/trunk# ./sipauthserve
ALERT 3072866048 15:09:48.6 sipauthserve.cpp:277:main: ./sipauthserve (re)starting
EMERG 3072866048 15:09:48.6 ./SubscriberRegistry.cpp:173:init: /var/lib/asterisk/
/sqlite3dir does not exist

Broadcast message from systemd-journald@h4ckOne (Mon 2016-06-13 15:09:48 CST):

sipauthserve[2099]: EMERG 3072866048 15:09:48.6 ./SubscriberRegistry.cpp:173:ini
t: /var/lib/asterisk/sqlite3dir does not exist

Message from syslogd@h4ckOne at Jun 13 15:09:48 ...
sipauthserve: EMERG 3072866048 15:09:48.6 ./SubscriberRegistry.cpp:173:init: /v
ar/lib/asterisk/sqlite3dir does not exist

root@h4ckOne: /opt/OpenBTS-P2.8/subscriberRegistry/trunk/apps
<0011> trx.c:512 TRX Data 2152407: 0: 0: 618bfbb007ffc0f38b52440fa87c70
<0011> trx.c:512 TRX Data 2152408: 0: 0: 278f25f0c41b906604be6288b10310
<0011> trx.c:512 TRX Data 2152409: 0: 0: a51bcc5f9010e6fe6a32f311c21810
<0011> trx.c:190 TRX CLK Indication 2152406
<0011> trx.c:512 TRX Data 2152457: 0: 0: a060948a43a104e000a010a56004a0
<0011> trx.c:512 TRX Data 2152458: 0: 0: 118a4388440802e000a14281e80600
<0011> trx.c:512 TRX Data 2152459: 0: 0: 40a944a420060740005c011800020
<0011> trx.c:512 TRX Data 2152460: 0: 0: 0425020420400a65ea138010216000
<0011> trx.c:190 TRX CLK Indication 2152457
<0011> trx.c:512 TRX Data 2152508: 0: 0: 82c074272b9d407e30b44143d79a20
<0011> trx.c:512 TRX Data 2152509: 0: 0: 618bfbb007ffc0f38b52440fa87c70
<0011> trx.c:512 TRX Data 2152510: 0: 0: 278f25f0c41b906604be6288b10310
<0011> trx.c:512 TRX Data 2152511: 0: 0: a51bcc5f9010e6fe6a32f311c21810
<0011> trx.c:190 TRX CLK Indication 2152508
<0011> trx.c:512 TRX Data 2152559: 0: 0: a847551a314d060907c410b055130
<0011> trx.c:512 TRX Data 2152560: 0: 0: 22974400ea1647e8ab7e0003df5460
<0011> trx.c:512 TRX Data 2152561: 0: 0: 042f958b02511c670f1f1500178680
<0011> trx.c:512 TRX Data 2152562: 0: 0: 9581ac70181285f07a0b57d681fe70
<0011> trx.c:190 TRX CLK Indication 2152559
<0011> trx.c:512 TRX Data 2152610: 0: 0: 816a80aa0221546952a45085401000
<0011> trx.c:512 TRX Data 2152611: 0: 0: 018a122916244ae0428548042a4480
<0011> trx.c:512 TRX Data 2152612: 0: 0: 14a01404481448700a10a010804aa0
<0011> trx.c:512 TRX Data 2152613: 0: 0: 4421420408540070a810001a212280

```

\$ cd smqueue/trunk/smqueue/

\$./smqueue(开启短信功能)

```

root@h4ckOne: /opt/osmocom-bb2/src/osmocom
Broadcast message from systemd-journald@h4ckOne (Mon 2016-06-13 15:09:48 CST):

smqueue[2120]: EMERG 3074483968 15:10:26.8 SubscriberRegistry.cpp:173:init: /var/
/lib/asterisk/sqlite3dir does not exist

LOST 1877!
LOST 1877!
BAT-ADC: 687 7 0 0 1023 1023 1023 582
Charger at 60 mV.
Battery at 4696 mV.
Charging at 0 mA.
Battery capacity is 100%
Battery range is 3199..3999 mV.
Battery full at 468 LSB ... full at 585 LSB
Charging at 239 LSB (204 mA).
BCICL2=0x3ff
battery.info.flags=0x00000000

root@h4ckOne: /opt/OpenBTS-P2.8/subscriberRegistry/trunk
root@h4ckOne: /opt/OpenBTS-P2.8/subscriberRegistry/trunk# ./sipauthserve
ALERT 3074483968 15:10:26.8 smqueue.cpp:2651:main: smqueue (re)starting
smqueue logs to syslogd facility LOCAL7, so there's not much to see here
EMERG 3074483968 15:10:26.8 SubscriberRegistry.cpp:173:init: /var/lib/asterisk/s
qlite3dir does not exist

Broadcast message from systemd-journald@h4ckOne (Mon 2016-06-13 15:10:26 CST):

sipauthserve[2099]: EMERG 3072866048 15:09:48.6 ./SubscriberRegistry.cpp:173:ini
t: /var/lib/asterisk/sqlite3dir does not exist

Message from syslogd@h4ckOne at Jun 13 15:09:48 ...
sipauthserve: EMERG 3072866048 15:09:48.6 ./SubscriberRegistry.cpp:173:init: /v
ar/lib/asterisk/sqlite3dir does not exist

Message from syslogd@h4ckOne at Jun 13 15:10:26 ...
smqueue: EMERG 3074483968 15:10:26.8 SubscriberRegistry.cpp:173:init: /var/lib/
asterisk/sqlite3dir does not exist

Broadcast message from systemd-journald@h4ckOne (Mon 2016-06-13 15:10:26 CST):

smqueue[2120]: EMERG 3074483968 15:10:26.8 SubscriberRegistry.cpp:173:init: /var/
/lib/asterisk/sqlite3dir does not exist

root@h4ckOne: /opt/OpenBTS-P2.8/smqueue/trunk/smqueue
root@h4ckOne: /opt/OpenBTS-P2.8/smqueue/trunk/smqueue# ./smqueue
ALERT 3074483968 15:10:26.8 smqueue.cpp:2651:main: smqueue (re)starting
smqueue logs to syslogd facility LOCAL7, so there's not much to see here
EMERG 3074483968 15:10:26.8 SubscriberRegistry.cpp:173:init: /var/lib/asterisk/s
qlite3dir does not exist

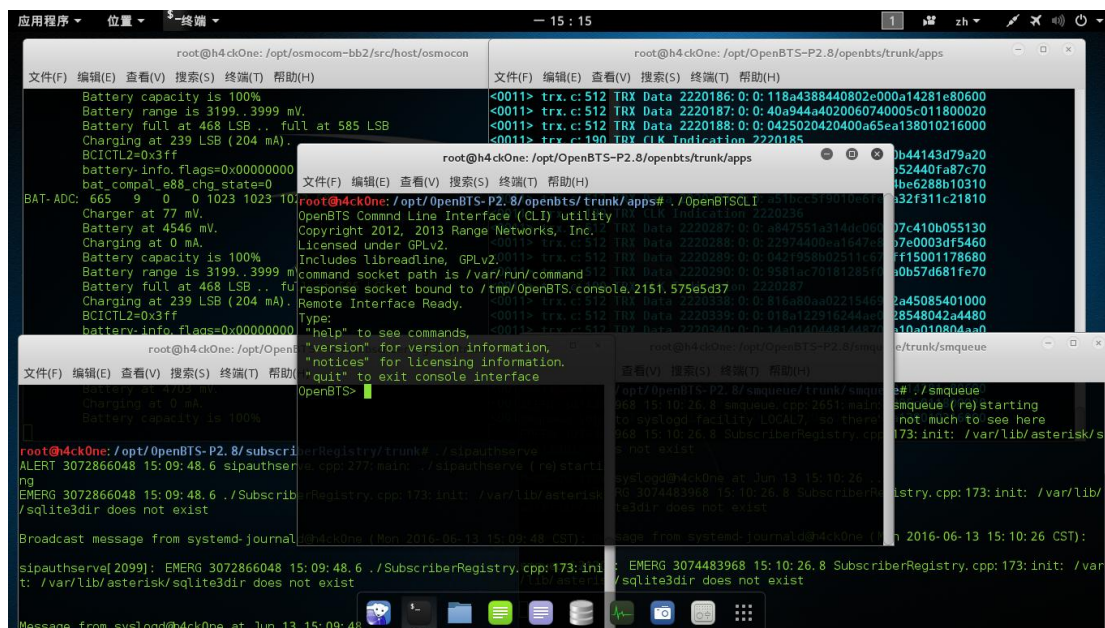
Broadcast message from systemd-journald@h4ckOne (Mon 2016-06-13 15:10:26 CST):

smqueue[2120]: EMERG 3074483968 15:10:26.8 SubscriberRegistry.cpp:173:init: /var/
/lib/asterisk/sqlite3dir does not exist

```

\$ cd openbts/trunk/apps

\$./OpenBTCLI (打开 OpenBTS 控制台)



如果一切运行顺利打开手机进入 **设置-移动网络-网络运营商** 即可看到我们创建的基站



在 OpenBTSLI 的终端窗口可以输入 **help** 查看命令帮助

输入 **tmsis** 可以查看当前基站用户的 IMSI

输入 **sendsms IMSI 电话 短信内容** 即可发送任意显示号码的短信

```
### NB ### (13e5 4000)
### NB ### (13f0 4000)
### NB ### (1468 3a70)
### NB ### (1461 4000)
### NB ### (1485 4000)
### NB ### (147e 4000)
### NB ### (14ab 4000)
### NB ### (14b6 4000)
### NB ### (14b0 4000)
### NB ### (14c1 4000)
### NB ### (14c7 4000)
### NB ### (14c1 4000)
### NB ### (14c1 4000)
### NB ### (14db 4000)
### NB ### (14d1 4000)
### NB ### (14db 4000)
### NB ### (14e0 4000)
### NB ### (14db 4000)

BAT-ADC: 611 7 0 0 1023 1023
Charger at 60 mV.
Battery at 4177 mV.
Charging at 0 mA.
Battery capacity is 100%.

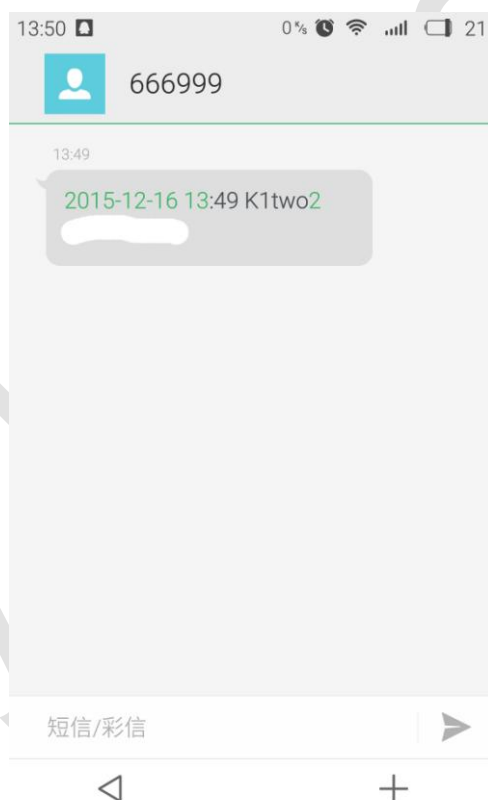
<0011> trx.c:512 TRX Data 1626087:0:0:61cbfb3247ff84f2cd52440bc87d70
<0011> trx.c:512 TRX Data 1626088:0:0:b7af25f0c01b90620cba0218b14310
<0011> trx.c:512 TRX Data 1626089:0:0:a512c85a9000c6fe2aa3f1174b1010
<0011> trx.c:190 TRX CLK Indication 1626086
<0011> trx.c:512 TRX Data 1626137:0:0:a16a948a422100e0502012a46080a0
<0011> trx.c:512
<0011> trx.c:512 OpenBTS Command Line Interface (CLI) utility
<0011> trx.c:190 Copyright 2012, 2013 Range Networks, Inc.
<0011> trx.c:512 Licensed under GPLv2.
<0011> trx.c:512 Includes readline, GPLv2.
<0011> trx.c:512 command socket path is /var/run/command
<0011> trx.c:512 response socket bound to /tmp/OpenBTS.console.3684.5670fb15
<0011> trx.c:190 Remote Interface Ready.
<0011> trx.c:512 Type:
<0011> trx.c:512 "help" to see commands,
<0011> trx.c:512 "version" for version information,
<0011> trx.c:512 "notices" for licensing information.
<0011> trx.c:190 "quit" to exit console interface
<0011> trx.c:512 OpenBTS> tmsi
<0011> trx.c:512 TMSI age used
2 4600 56 179s 179s
1 4600 017 12m 6m

OpenBTS> sendSMS 4600 56 666999 2015-12-16 13:48 Kitwo2 5
message submitted for delivery

OpenBTS> sendSMS 4600 17 666999 2015-12-16 13:49 Kitwo2 5
message submitted for delivery

OpenBTS>

[sudo] password for kitwo2:
ALERT 139688737916736 13:30:35.5 smqueue.cpp:2651:main: smq
smqueue logs to syslogd facility LOCAL7, so there's not muc
taring
```



0x06 结语

一入 GSM 深似海，作者不是学通信的，只是业余爱好，第一次写文章，文中不免纰漏和不妥之处。有任何建议或意见欢迎留言！

0x07 参考资料

<http://osmocom.org/projects/baseband/wiki/Transceiver>

<https://wush.net/trac/rangepublic/wiki/BuildInstallRun>

<https://wush.net/trac/rangepublic/wiki/DebOpenBTS>

<http://bb.osmocom.org/trac/blog/PHD2012>

<http://www.h-online.com/open/news/item/29C3-Budget-mobile-turns-into-GSM-base-station-1775204.html>

<http://blog.0x7678.com/2014/03/osmocombbopenbtsgsmcalypso.html>