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"

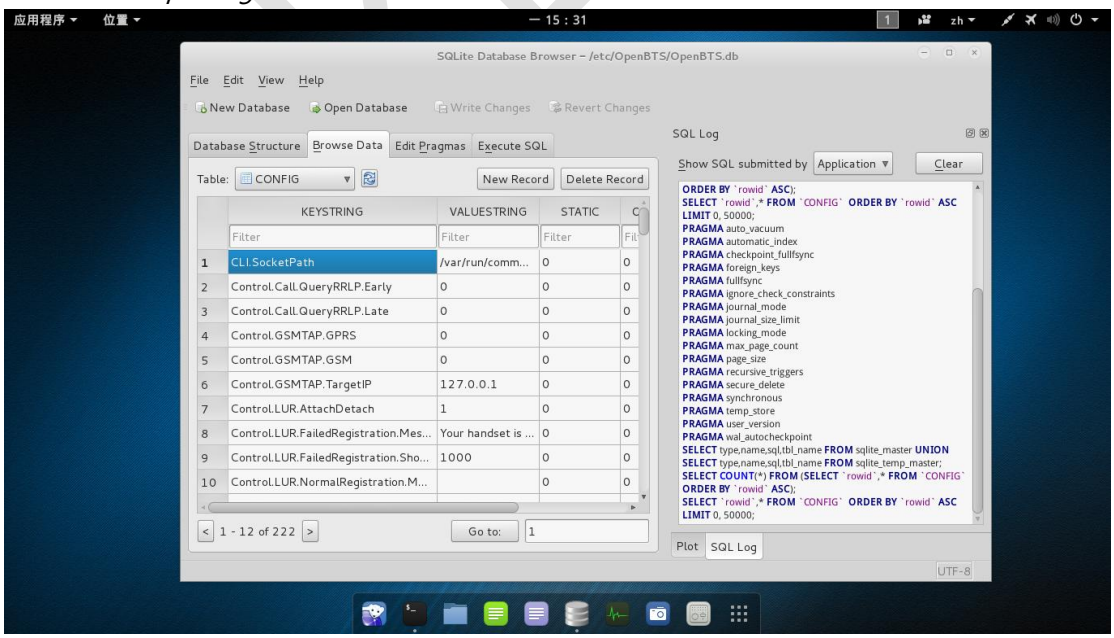
安装 OpenBTS 后按照 WIKI 的说明配置/etc/OpenBTS/OpenBTS.db

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 =.**

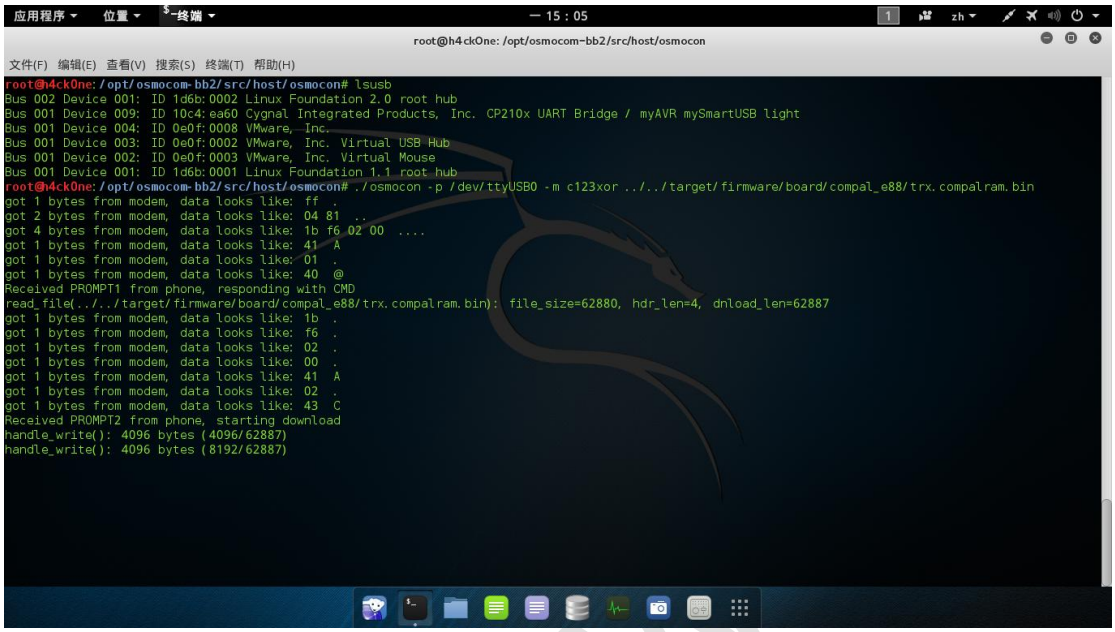


0x04 刷入固件

用 osmocon 程序将 trx.compalram.bin 刷入手机

命令

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

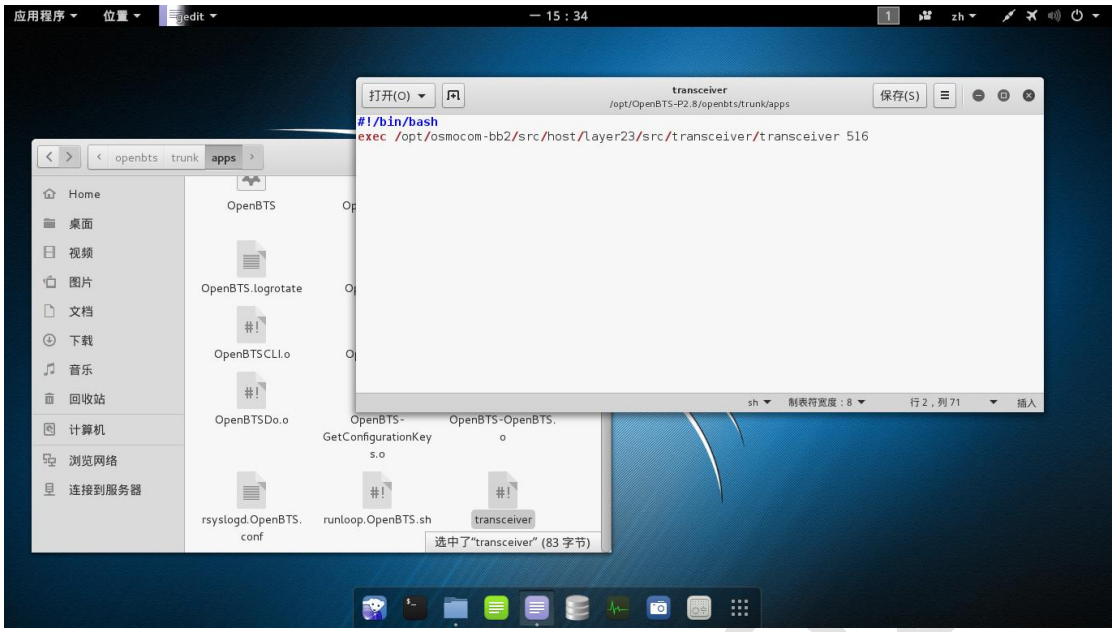


0x05 开始执行

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



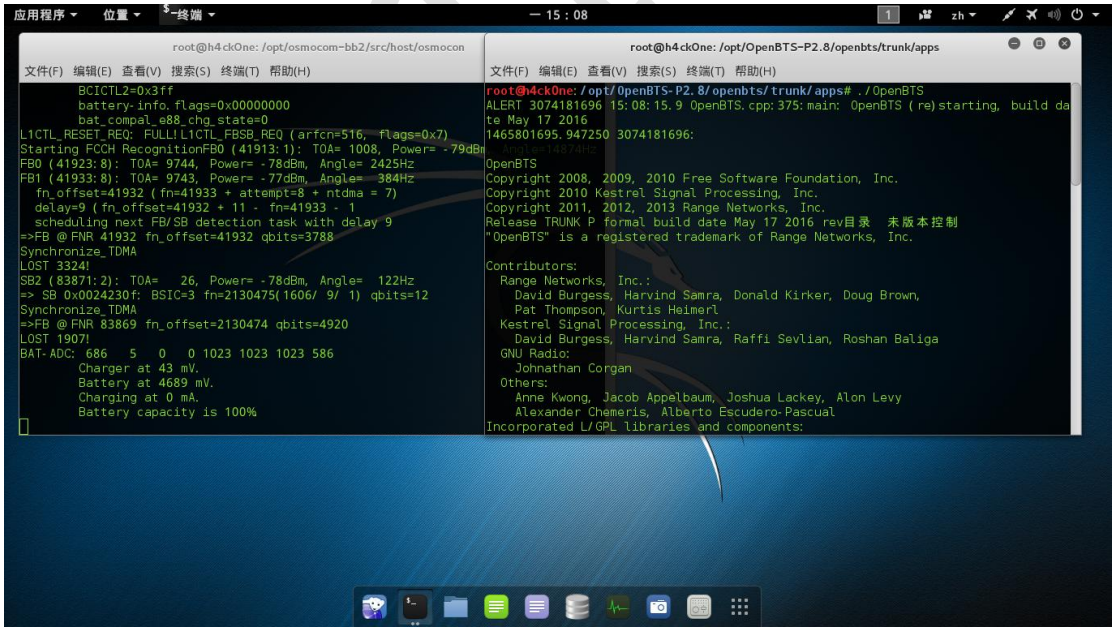
赋予执行权限

chmod +x transceiver

然后开 4 个终端窗口分别执行

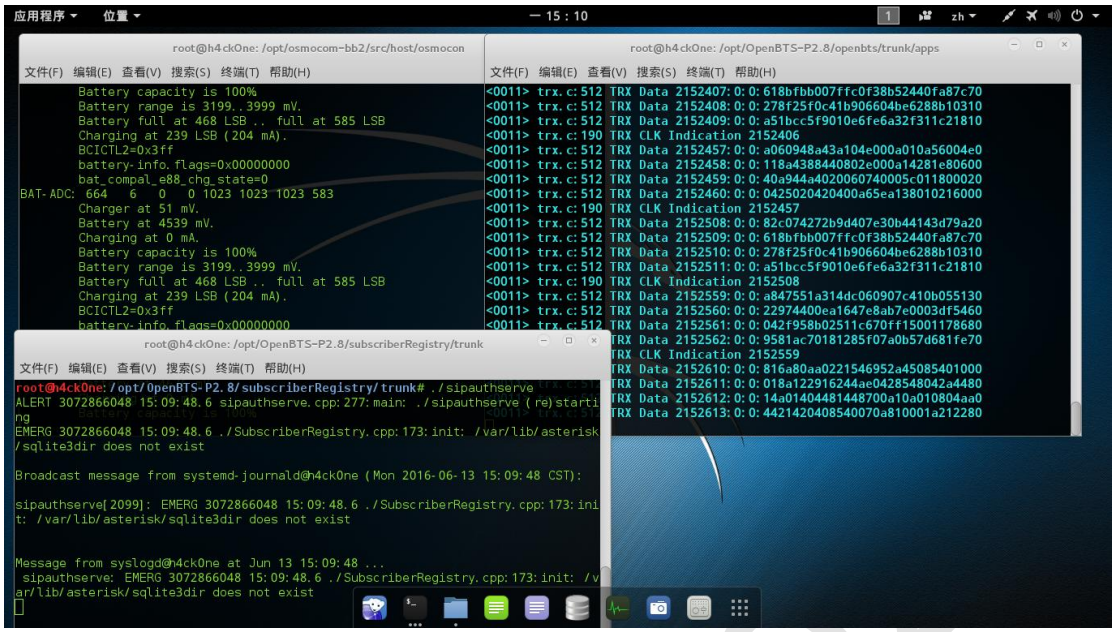
$ cd openbts/trunk/apps

$ ./OpenBTS



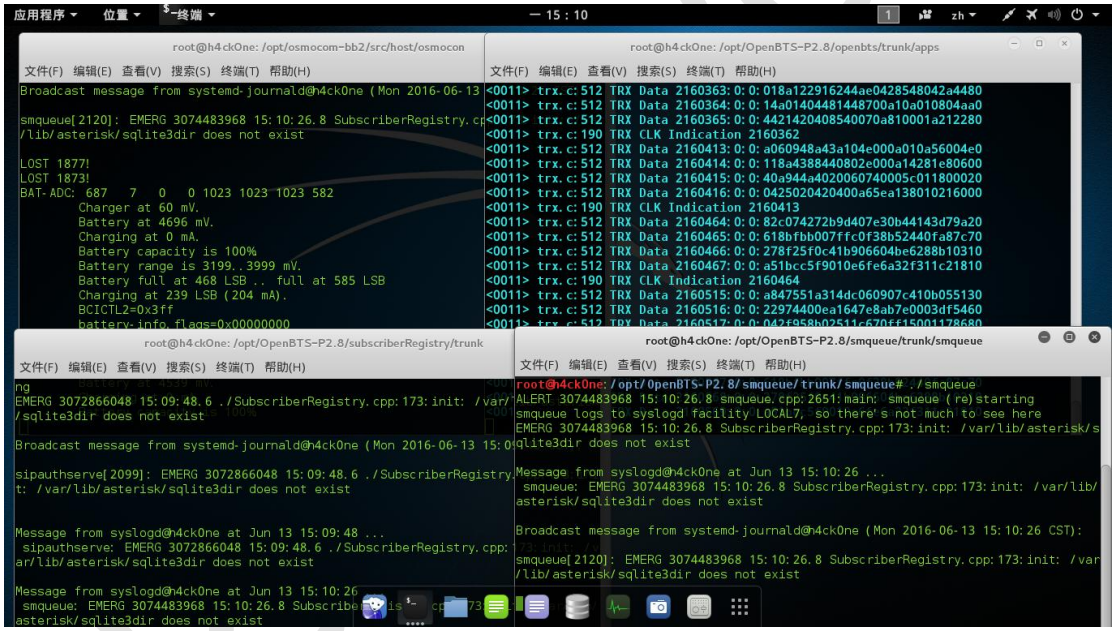
$ cd subscriberRegistry/trunk

$ ./sipauthserve(开启注册服务)



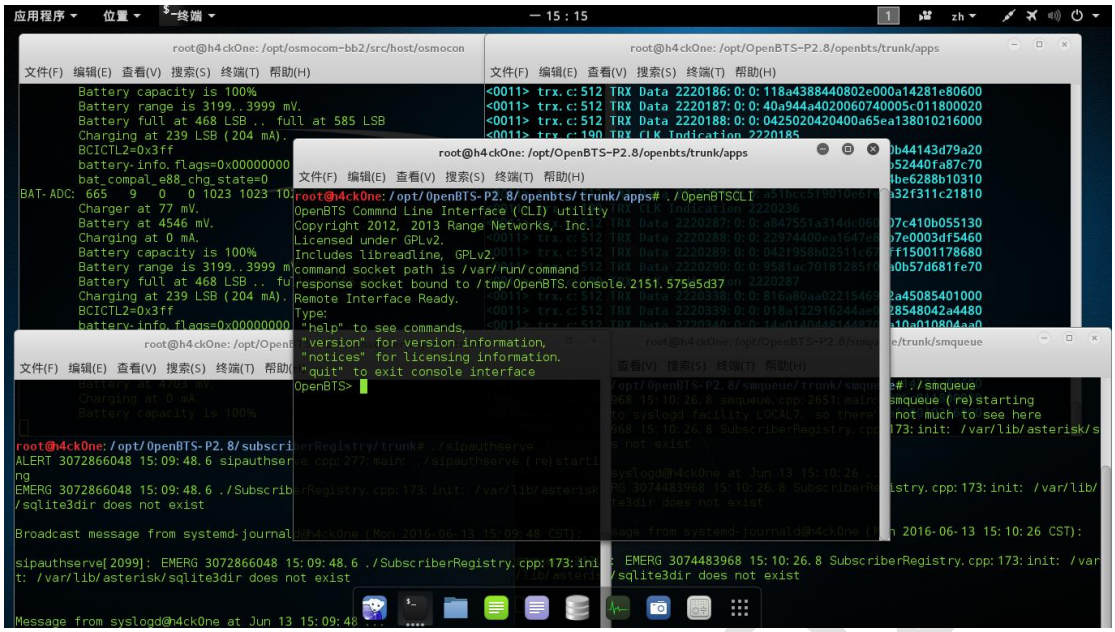
$ cd smqueue/trunk/smqueue/

$ ./smqueue(开启短信功能)



$ cd openbts/trunk/apps

$ ./OpenBTSCLI (打开 OpenBTS 控制台)

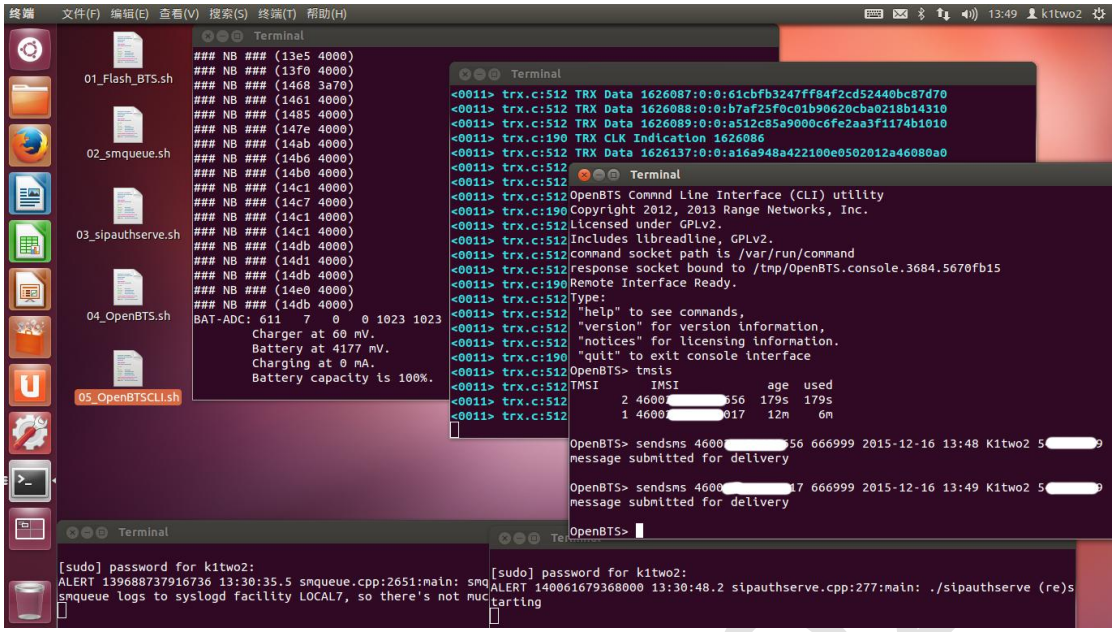


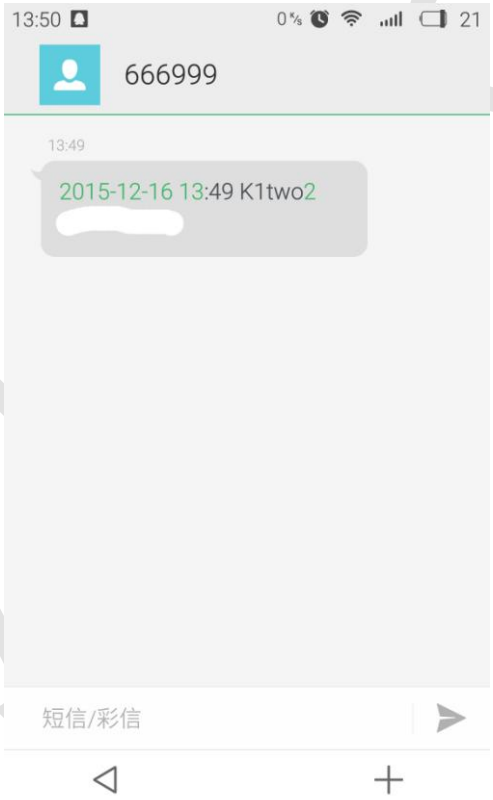
如果一切运行顺利打开手机进入 *设置-移动网络-网络运营商* 即可看到我们创建的基站

在 OpenBTSCLI 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





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