

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/327971731>

# Hijack IoT devices [GSM GPRS MITM]with SDR

Conference Paper · March 2018

---

CITATIONS

0

READS

4,153

1 author:



[Qiren Gu](#)

10 PUBLICATIONS 423 CITATIONS

[SEE PROFILE](#)

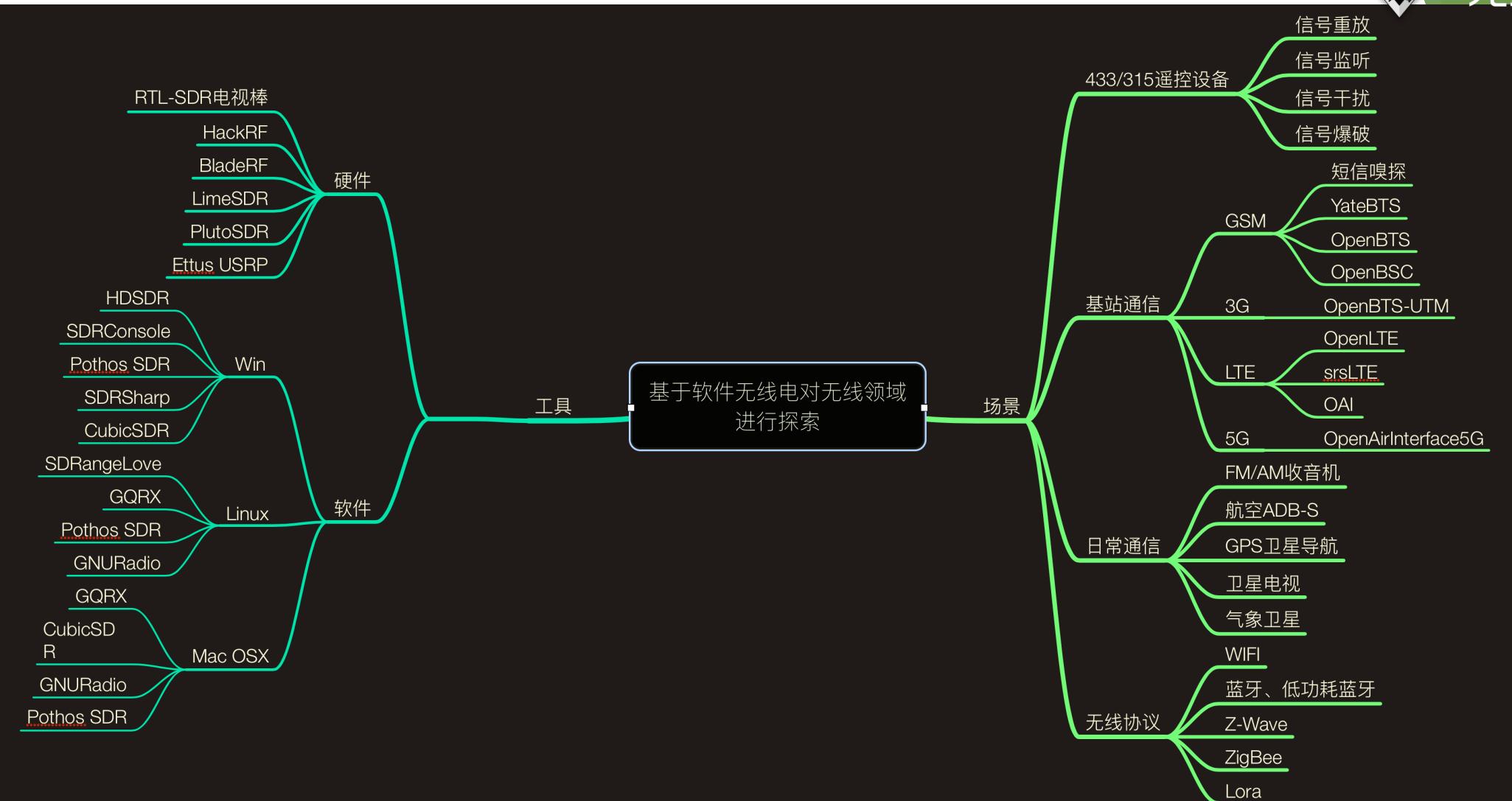
# 通过软件无线电构建自己 的 2-5G 基站

GSM: YateBTS+BladeRF 入门指南

雪碧 Oxroot



360  
无线电安全研究部





# 软件无线电硬件

- HackRF
- BladeRF
- LimeSDR
- PlutoSDR
- USRP



SDR硬件	频率范围	带宽	价格
电视棒	100KHz-1700MHz	2.4MHz	¥几十块；
HackRF	1-6000MHz	10MHz	$\approx$ ¥一千块；
BladeRF	300-3800MHz	40MHz	¥ 2700/4300；
USRP	70-6000MHz	60MHz	¥4600
LimeSDR、PlutoSDR…			



# Hackers – A Big Group of SDR Users



Using wideband SDR tools to analyze many kinds of wireless systems

- Short distance: Bluetooth, RFID, NFC
- Wifi, Zigbee, 315/433MHz
- Cellular: 2G/3G/4G/5G
- Satellite system: GPS, GlobalStar, DVB-S
- Private protocol: private network, links of drones
- Industry control system



# 开源基站项目

- ▶ 2G：
  - ▶ **YateBTS+BladeRF** :支持通过WEB页面配置，容易上手 & 电话、短信、GPRS功能完善；
  - ▶ **OpenBTS+USRP** :支持强大的命令行终端& 安装配置复杂、门槛高、GPRS功能不稳定；
  - ▶ **OpenBSC** :基站组件模块化、基于OsmoTRX可配合使用更多硬件(USRP、Fairwaves UmTRX、LimeSDR)
  
- ▶ 3G:
  - ▶ **Accelerate3g5** [https://osmocom.org/projects/cellular-infrastructure/wiki/Accelerate3g5\\_-\\_unicornteam](https://osmocom.org/projects/cellular-infrastructure/wiki/Accelerate3g5_-_unicornteam)
  - ▶ **OpenBTS-UTM** <https://fairwaves.co/blog/openbts-umts-3g-umtrx/>



# 开源基站项目

- ▶ **4G:**
- ▶ **Open Air Interface (OAI) +USRP** <http://www.ettus.com.cn/SDR/12.html>
- ▶ **OpenLTE (BladeRF USRP)** <https://sourceforge.net/p/openlte/wiki/Home/>
- ▶ **SRSLTE+USRP** <http://www.softwareradiosystems.com/tag/srslte/>
  
- ▶ **5G :**
- ▶ **OAI-5G** <https://gitlab.eurecom.fr/oai/openairinterface5g>

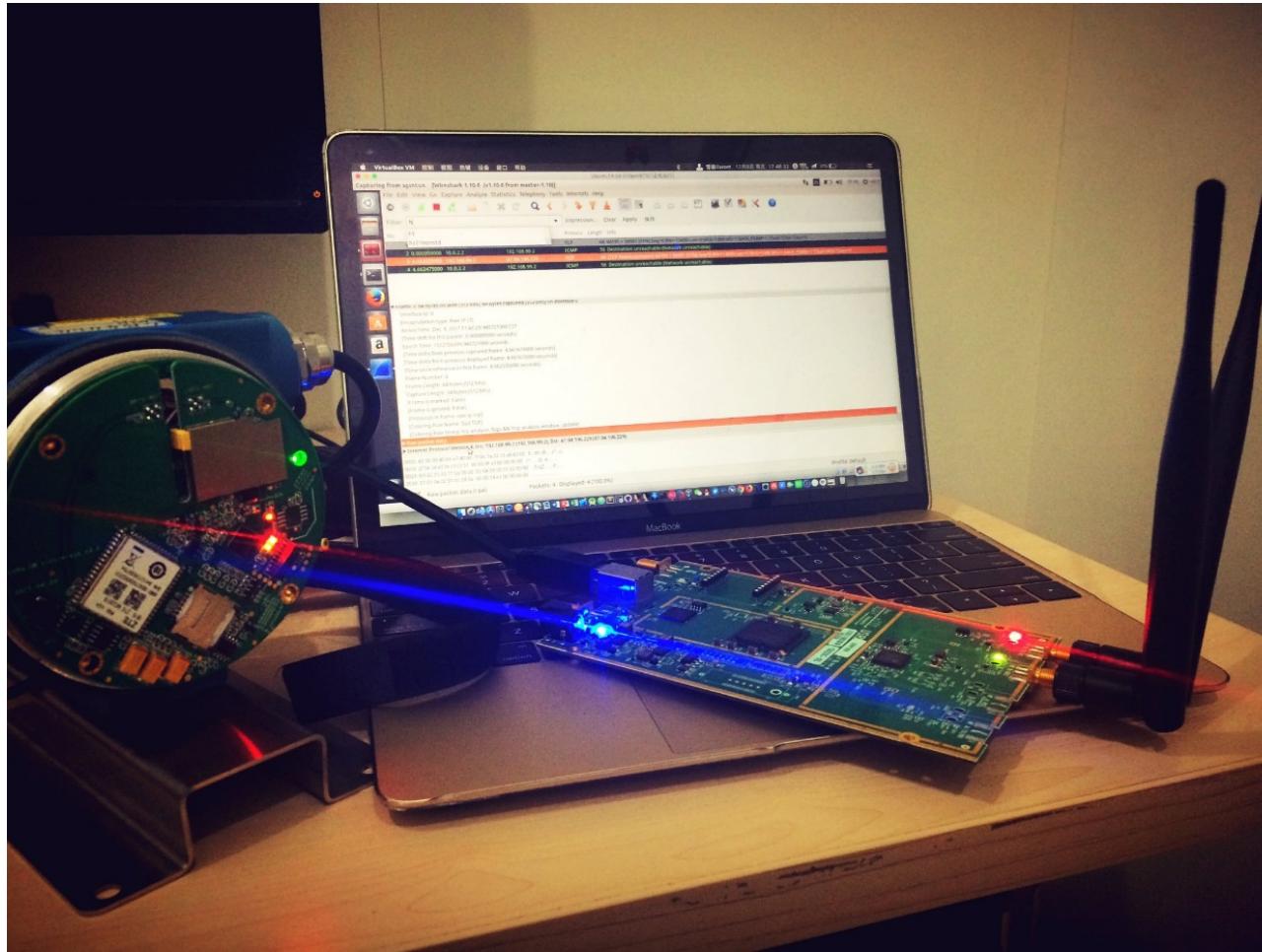


# 为什么是2G： 攻击的面、范围广

- **鉴权** 2G存在安全缺陷：单向认证、鉴权（3G、4G均为双向认证）导致非法的设备（如基站）可以伪装成合法的成员，从而欺骗用户，轻松将用户拉入伪基站网络；
- **兼容** 即使已经进入4G、5G时代，各大品牌手机均支持2G网络；
- **数量体系** 为控制硬件成本，大量物联网设备：共享单车、娃娃机、自动售货机、智能水表、智能电表、车载多媒体等均采用GSM模块；
- **攻击面** SMS-sniff、SMS-fuzz、GSM-MITM、GPRS-MITM、协议Fuzz、参数fuzz、DDoS、重定向、命令执行…



# 方案1：OpenBTS+USRP



## 优点：

- ✓ OpenBTSCLI命令行功能强大，可玩性高；
- ✓ GSM电话、SMS短信功能稳定；
- ✓ USRP散热性能强；

## 缺点：

- ◆ 编译难度大：依赖包多、需要翻墙编译；
- ◆ 几百页文档、配置复杂、没有可视化配置页面不适合新手；
- ◆ 运行时需要启动多个组件；
- ◆ GPRS联网功能Bug较多；

<https://cn0xroot.com/2017/01/10/iot-mode-fuzzing-with-openbt/>

<https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2016/may/gsmgprs-traffic-interception-for-penetration-testing-engagements/>



# 方案1：OpenBTS+USRP

The screenshot shows a terminal window titled "终端" (Terminal) and a Wireshark application window.

**Terminal Output (init3@HackSmith: /opt/dev/openbts/apps):**

```
init3@HackSmith:/opt/dev/openbts/apps$ sudo ./OpenBTSCLI
OpenBTS Command Line Interface (CLI) utility
Copyright 2012, 2013, 2014 Range Networks, Inc.
Licensed under GPLv2.
Includes libreadline, GPLv2.
Connecting to 127.0.0.1:49300...
Remote Interface Ready.
Type:
  "help" to see commands,
  "version" for version information,
  "notices" for licensing information,
  "quit" to exit console interface.
OpenBTS> tmsis
IMSI      TMSI    IMEI        AUTH CREATED ACCESSED TMSI_ASSIGNED
460078104853311 0xb3652 865740038899800 2   7m     142s    1
460015061500010 0x76396 359474082905190 2   14m    5m     1

OpenBTS> sgsn list
GMM Context: imsi=460078104853311 ptmsi=0x69001 tlli=0xc0069001 state=GmmRegisteredNormal age=86 idle=8 MS#1, TLLI=c0069001,80031001 IPs=192.168.88.1,192.168.88.2

OpenBTS> gprs list
MS#1,TLLI=c0069001,80031001 rrmode=PacketIdle Bytes:1225up/1103down Utilization=162%
      GMM Context: imsi=460078104853311 ptmsi=0x69001 tlli=0xc0069001 state=GmmRegisteredNormal age=103 idle=4 IPs=192.168.88.1,192.168.88.2
      TimingError=(-1.46 min=-1.48 max=-0.46 avg=-1.02 N=1313) RSSI=(-30 min=-34 max=-28 avg=-30.86 N=1313) CV=(54 min=42 max=56 avg=48.89 N=19) ILev=(0) RXQual=(0 min=0 max=7 avg=2.50 N=14) SigVar=(0 min=0 max=63 avg=36.64 N=14) ChCoding=(3 min=0 max=3 avg=2.88 N=100)
      dataER:0.9% (907) recent:0.0% (347) low:1.0% (111) tbFER:.18% (17)
      rrbpER:5% (131) recent:.7% (40) low:1.0% (9) ccchER:0% (0) recent:0% (0)
      MS#2,TLLI=810cb380 rrmode=PacketIdle Bytes:355up/0down Utilization=0%
      GMM state unknown
      TimingError=(-1.49 min=-1.50 max=-1.31 avg=-1.44 N=48) RSSI=(-44 min=-47 max=-16 avg=-41.35 N=48) CV=(49 min=44 max=54 avg=48.20 N=5) ILev=(0) RXQual=(0) SigVar=(0) ChCoding=(0)
      dataER:0% (33) recent:0% (0) tbFER:0% (5)
      rrbpER:.09% (11) recent:0% (0) ccchER:0% (0) recent:0% (0)
TBF#21 ntMS= MS#1,TLLI=c0069001,80031001 mtDir=RLCDir::Down
channels: down=( 0:1 0:2 0:3) up=( 0:2,usf=0 0:3,usf=0)
ntState==TBFState::Dead mtAttached=1 mtTFI=21 mtTlli=0xc0069001 size=0
PDCH ARFCN=512 TN=1 FER=0%
PDCH ARFCN=512 TN=2 FER=.3%
PDCH ARFCN=512 TN=3 FER=0%
PDCH ARFCN=512 TN=4 FER=0%
PDCH ARFCN=512 TN=5 FER=0%
```

**Wireshark Capture (Capturing from sgsntun [Wireshark 1.10.6]):**

The Wireshark capture shows several TCP connections between the local host (192.168.88.2) and a destination IP (192.168.88.1). The traffic includes ACKs, PSHs, and data frames. A detailed analysis of one specific TCP segment is shown:

- Frame 14:** 59 bytes on wire (472 bits), 59 bytes captured (472 bits) on interface 0
- Raw packet data:** 0x0010 2f 5e c4 e5 c5 b6 c3 51 01 b5 11 c0 00 01 f4 15 ...
- Internet Protocol Version 4, Src: 192.168.88.2 (192.168.88.2), Dst: 47.94.196.229 (47.94.196.229)**
- Transmission Control Protocol, Src Port: 50614 (50614), Dst Port: 50001 (50001), Seq: 26, Ack: 20, Len: 19**
- Source port: 50614 (50614)**
- Destination port: 50001 (50001)**
- [Stream index: 1]**
- Sequence number: 26 (relative sequence number)**
- [Next sequence number: 45 (relative sequence number)]**
- Acknowledgment number: 20 (relative ack number)**
- Header length: 20 bytes**
- Flags: 0x108 (PSH, ACK)**
- Window size value: 10880**
- [Calculated window size: 10880]**
- [Window size scaling factor: -2 (no window scaling used)]**
- Checksum: 0xb821 [validation disabled]**
- [SEQ/ACK analysis]**
- This is an ACK to the segment in frame: 9**
- [The RTT to ACK the segment was: 1.009809000 seconds]**
- [Bytes in flight: 19]**
- Data (19 bytes): aa00067a2c0b6e815902e0aa4300120000e055**
- [Length: 19]**

Below the Wireshark capture, there is a hex dump of the data payload:

```
0010 2f 5e c4 e5 c5 b6 c3 51 01 b5 11 c0 00 01 f4 15 /.....Q .....
0020 50 18 2a 80 b2 21 00 00 3a 00 06 7a 2c 0b 6e 81 P.*...l...z,n.
0030 59 02 e0 aa 43 00 12 00 00 e0 55 Y...C...U
```

At the bottom of the Wireshark window, it says "Data (data), 19 bytes" and "Packets: 33 - Displayed:...".



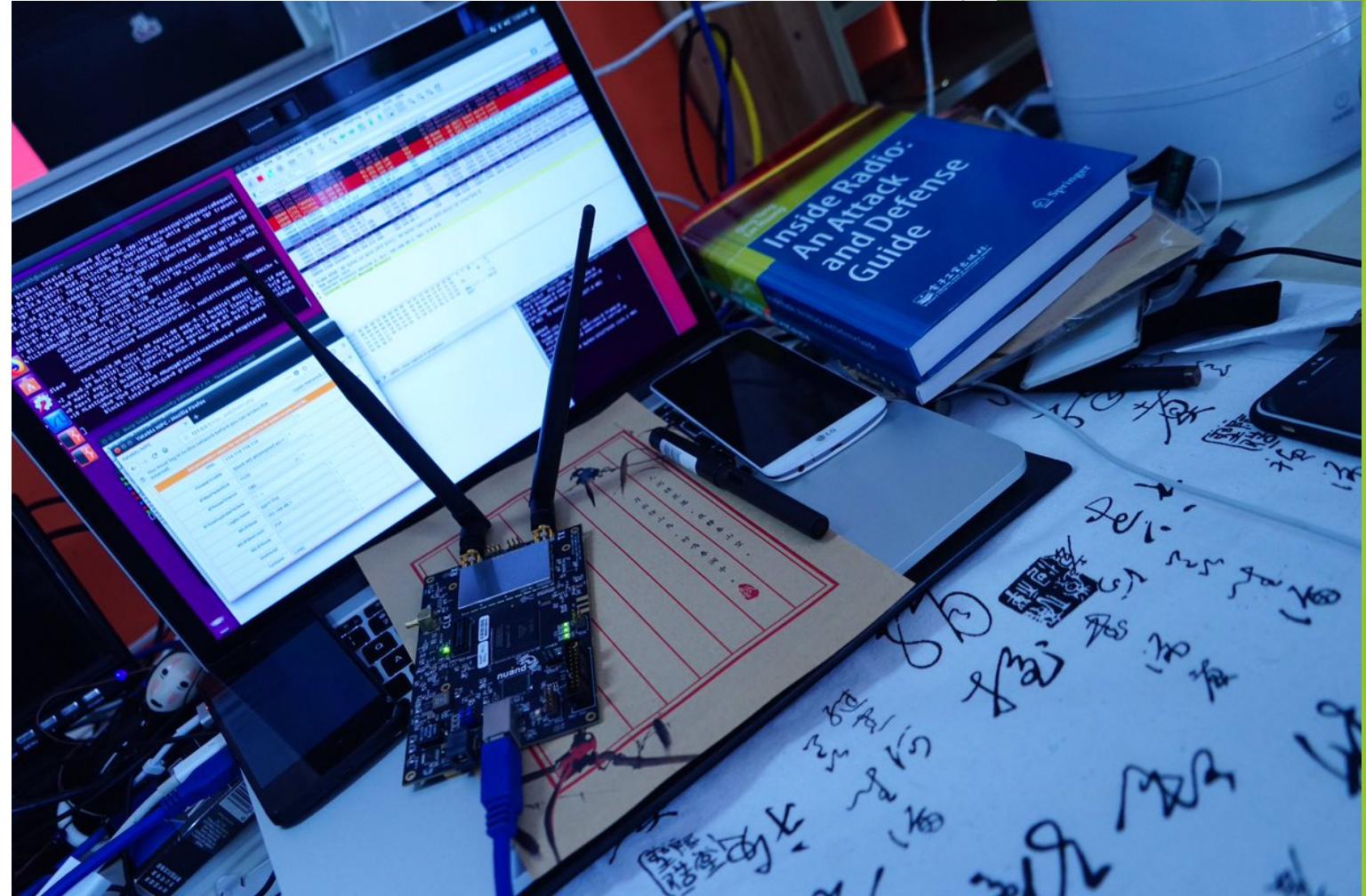
## 方案2：YateBTS+BladeRF

### 优点：

- ✓ 源码编译比OpenBTS容易；
- ✓ 启动简单 (`sudo yate -s`)；
- ✓ 支持WEB页面配置基站、上手简单；
- ✓ 电话、短信、GPRS功能完善、稳定；
- ✓ BladeRF精度高（相对USRP而言）

### 缺点：

- ◆ BladeRF散热性差、需要加小风扇；
- ◆ 功能（参数配置）不如OpenBTS强大；



<https://www.evilsocket.net/2016/03/31/how-to-build-your-own-rogue-gsm-bts-for-fun-and-profit/>  
<https://github.com/Nuand/bladeRF/wiki/Setting-up-Yate-and-YateBTS-with-the-bladeRF>



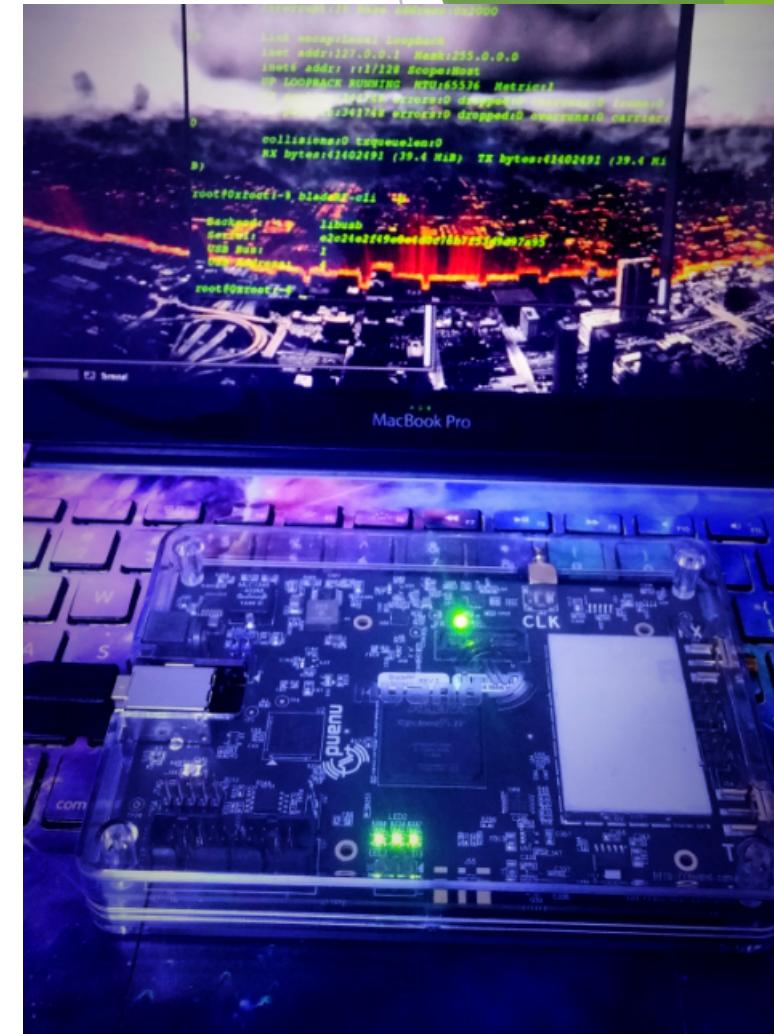
# YateBTS+BladeRF 安装指南(Ubuntu 16.04) 安装依赖 & 编译BladeRF

- ▶ 安装依赖包:
- ▶ Sudo apt install git cmake **automake libusb-1.0.0-dev** apache2 php libapache2-mod-php php-mcrypt php-mysql
- ▶ 源码编译BladeRF:
- ▶ wget <https://github.com/Nuand/bladeRF/archive/2016.06.zip>
- ▶ unzip 2016.06.zip
- ▶ cd bladeRF-2016.06/host
- ▶ mkdir build && cd build
- ▶ cmake ..
- ▶ make -j4 && sudo make install
- ▶ sudo ldconfig



# YateBTS+BladeRF 安装指南(Ubuntu 16.04)

- ▶ 测试BladeRF是否正常工作:
- ▶ wget http://www.0xroot.cn/hostedx40.rbf
- ▶ bladeRF-cli -l hostedx40.rbf //加载BladeRF FPGA镜像
- ▶ bladeRF-cli -p //列出硬件设备





# YateBTS+BladeRF 安装指南(Ubuntu 16.04)

## Yate

Yate 的全名是 Yet Another Telephony Engine，是开放源代码的 VoIP 网络电话引擎。  
可以作为网络电话服务器、也可以作为网络电话客户端使用。

Yate

<http://yate.ro>

Yate 最早是 2004 年由 NullTeam 所推出。

YateBTS

<https://yatebts.com>



# YateBTS+BladeRF 安装指南(Ubuntu 16.04) 源码编译Yate (>= 6.0)

- ▶ wget <https://github.com/vir/yate/archive/6.0.0.zip>
- ▶ unzip 6.0.0.zip
- ▶ cd yate-6.0.0
- ▶ ./autogen.sh
- ▶ ./configure --prefix=/usr/local
- ▶ make -j4
- ▶ sudo make install
- ▶ sudo ldconfig

➤ 检测是否安装成功：  
yate-config --version

```
hacksmith@ubuntu: ~/BTS/yate-6.0.0
hacksmith@ubuntu:~/BTS/yate-6.0.0$ yate-config --version
6.0.0
hacksmith@ubuntu:~/BTS/yate-6.0.0$
```



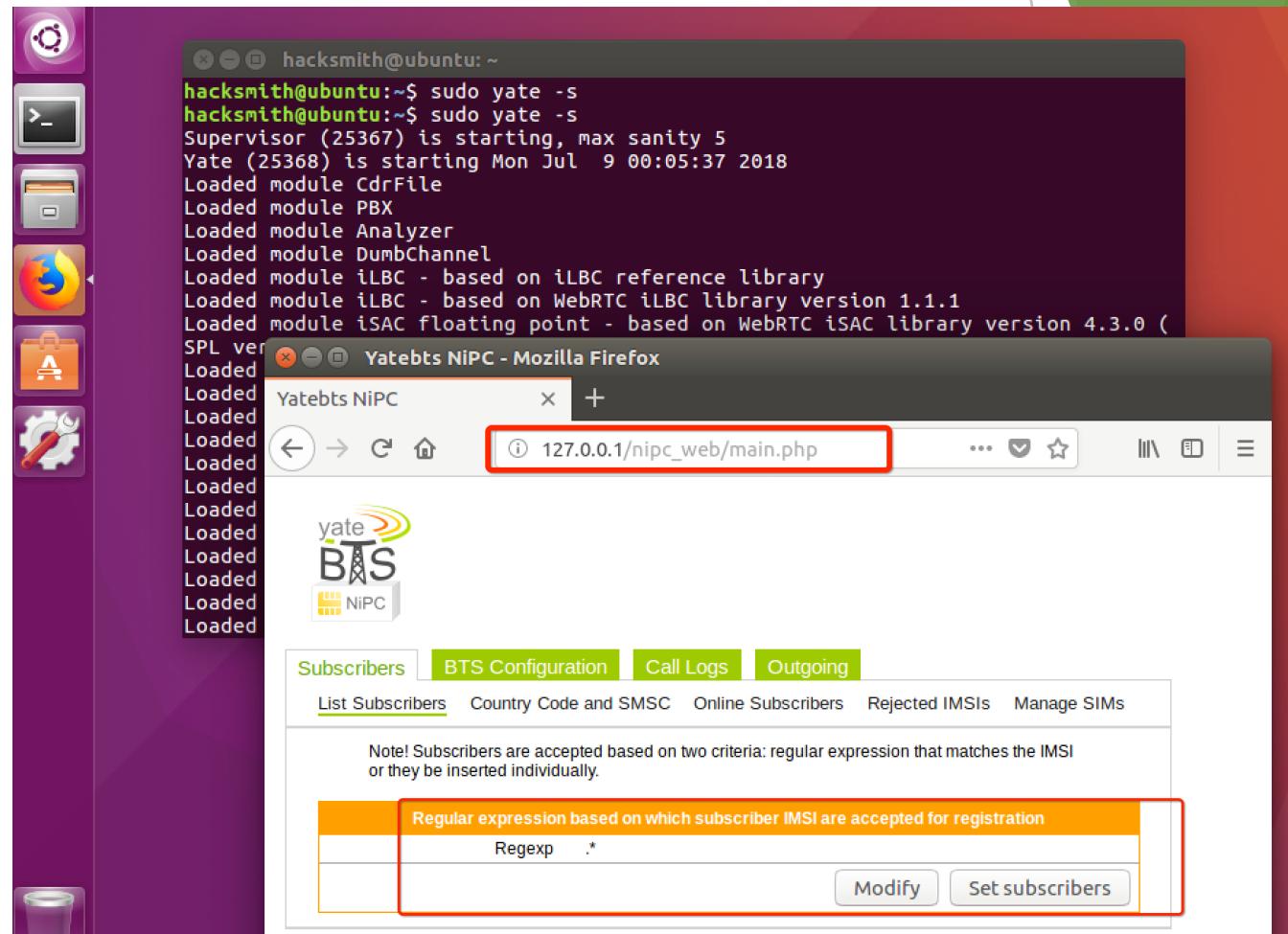
# YateBTS+BladeRF 安装指南(Ubuntu 16.04) 源码编译Yate-BTS

- ▶ wget <https://yate.null.ro/tarballs/yatebts6/yate-bts-6.0.0-1.tar.gz> --no-check-certificate
- ▶ tar zxvf yate-bts-6.0.0-1.tar.gz
- ▶ cd yate-bts
- ▶ ./autogen.sh
- ▶ ./configure --prefix=/usr/local
- ▶ make -j4
- ▶ sudo make install
- ▶ sudo ldconfig
- ▶ sudo ln -s /usr/local/share/yate/nipc\_web/ /var/www/html/ (WEB控制台页面软链接到Apache服务器)



# Yate-BTS配置

- ▶ sudo yate -s 启动基站
- ▶ 在浏览器访问：  
localhost/nipc\_web
- ▶ 修改Regexp的值为：.\*  
*(允许任意用户加入网络)*





# Yate-BTS配置

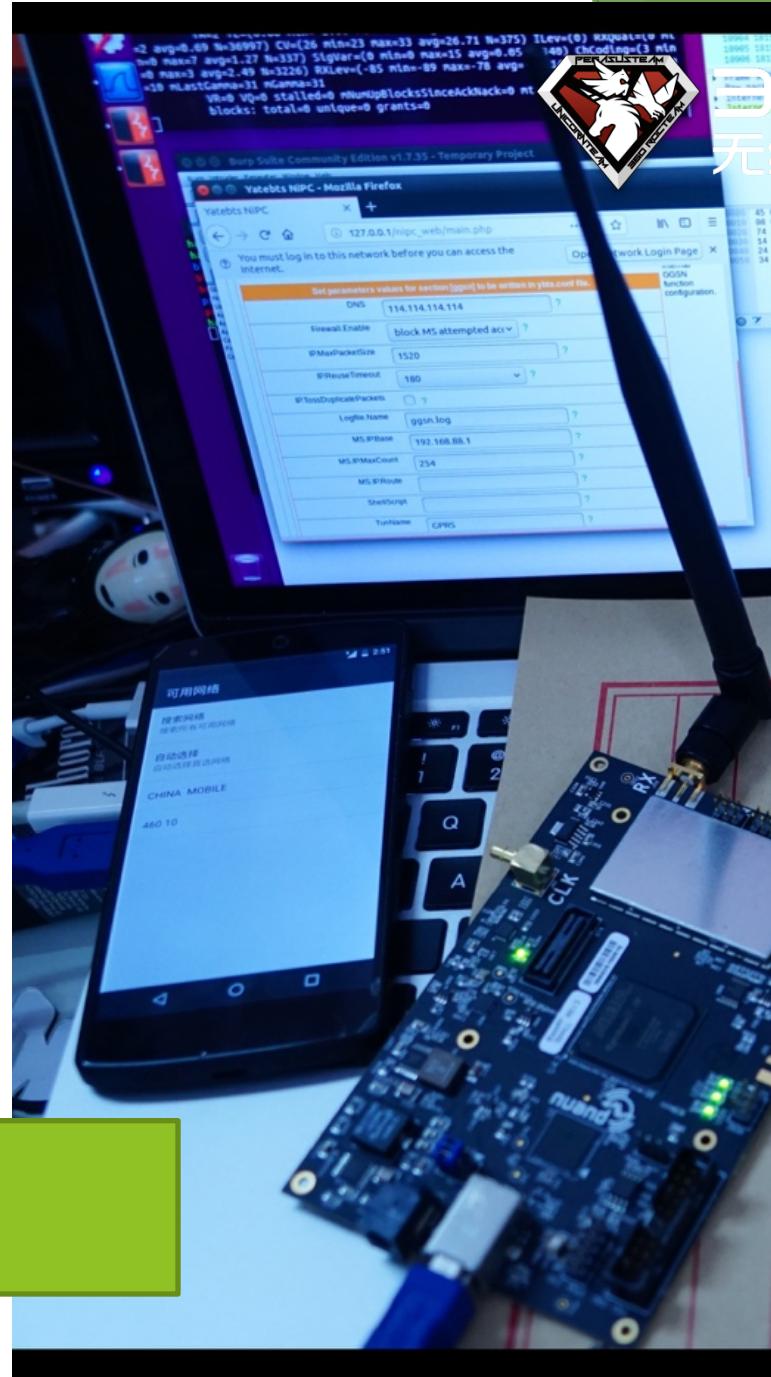
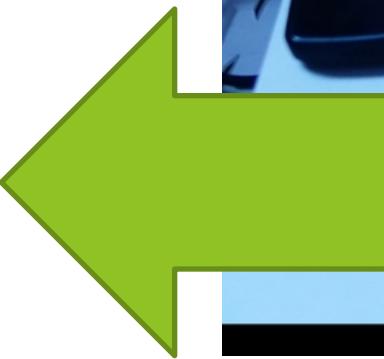
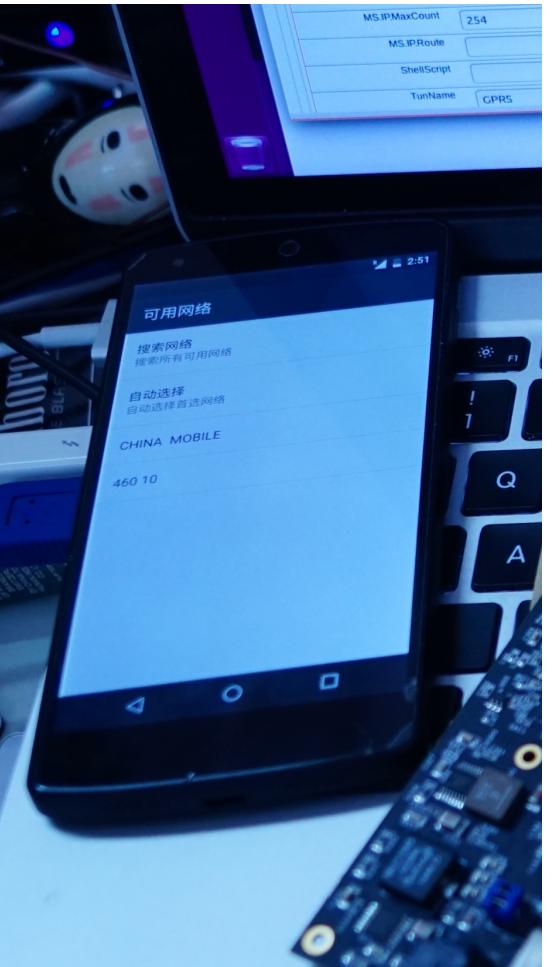
- 配置基站频段：GSM850、或者EGSM900；
- 设定Arfcn值：视实际情况而定；
- MCC：Mobile country code移动设备国家码，中国460；
- MNC：Mobile Network Code移动网络号码，用于识别运营商：中国移动：00、02、04、07；中国联通GSM：01、06、09；
- LAC：Location Area Code，位置区域码
- CI:Cell Identity，基站编号

The screenshot shows two windows related to Yate-BTS configuration:

- Terminal Window:** Shows the command `sudo yate -s` being run twice, followed by the supervisor and Yate processes starting up.
- Web Browser (Mozilla Firefox):** Displays the Yatebts NiPC web interface at [localhost/nipc\\_web/main.php?module=bts\\_configuration](http://localhost/nipc_web/main.php?module=bts_configuration). The interface has tabs for Subscribers, BTS Configuration, Call Logs, and Outgoing. Under the BTS Configuration tab, the GSM section is selected. A specific configuration section is highlighted with a blue border and labeled with its parameter names and their meanings:
  - Radio.Band:** EGSM900 (基站频段)
  - Radio.CU:** #35: 942 MHz downli (基站信号频率)
  - Identity.MCC:** 460 (国家码、运营商)
  - Identity.MNC:** 10 (国家码、运营商)
  - Identity.LAC:** 1000 (商码、基站小)
  - Identity.CI:** 10 (区位置码)
  - Identity.BSIC.BCC:** 3
  - Identity.BSIC.NCC:** 3
  - Identity.ShortName:** HackSmith
  - Radio.PowerManager.MaxAttenDB:** 50
  - Radio.PowerManager.MinAttenDB:** 50
- Text Labels on the right:** 基站网络名称：中国移动、CMCC (BTS network name: China移 CMCC)

# 手机入站

在手机可用网络中搜寻附近基站，手动选择网络。

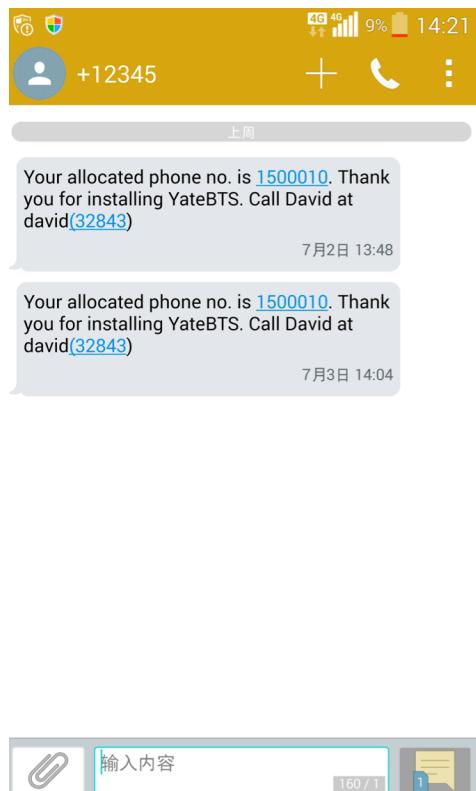




# 手机入站

手机加入基站后，可在管理页面找到已注册SIM卡的IMSI：基站会自动给手机分配号码跟IP地址。

手机同时也会收到基站的欢迎短信：



Firefox Web Browser

hacksmith@ubuntu:~

[sudo] password for hacksmith:

Yate (2348) is starting

Loaded module CdrFile

Loaded module PBX

Loaded module Analyzer

Loaded module DumbChan

Loaded module iLBC - b

Loaded module iLBC - b

Loaded module isAC fl

SPL version 1.2.0)

Loaded module FileInfo

Loaded module Call For

Loaded module File Tra

Loaded module CdrBuild

Loaded module YRTP

Loaded module YIAX

Loaded module MsgSniff

Loaded module Call Gen

Loaded module YJingle

Loaded module YSTUN

Loaded module GVoice

Loaded module RegexRou

Yatebts NIPC - Mozilla Firefox

127.0.0.1/nipc\_web/main.php?module=subscribers&method=

yate  
BTS  
NIPC

Subscribers BTS Configuration Call Logs Outgoing

List Subscribers Country Code and SMSC Online Subscribers Rejected IMSIs Manage SIMs

IMSI	MSISDN
9017000000000021	0014921
4600150000000010	1500010
4600180000000007	2495807
4600169000000007	8805307
9017000000000029	0014929

Note! To disable nipc mode and enable roaming mode see [Javascript Roaming](#)



# Yate-BTS配置Tips

通过软件无线电工具扫描获取附近基站信息：

```
init3@HackSmith:~/sdr/gr-gsm/apps$ sudo ./grgsm_scanner
linux; GNU C++ version 4.8.4; Boost_105400; UHD_003.010.001.001-release
```

```
ARFCN: 24, Freq: 939.8M, CID: 5997, LAC: 4421, MCC: 460, MNC: 0, Pwr: -46
ARFCN: 25, Freq: 940.0M, CID: 0, LAC: 0, MCC: 0, MNC: 0, Pwr: -58
ARFCN: 27, Freq: 940.4M, CID: 41285, LAC: 4421, MCC: 460, MNC: 0, Pwr: -47
ARFCN: 29, Freq: 940.8M, CID: 64215, LAC: 4421, MCC: 460, MNC: 0, Pwr: -46
ARFCN: 31, Freq: 941.2M, CID: 64214, LAC: 4421, MCC: 460, MNC: 0, Pwr: -60
ARFCN: 34, Freq: 941.8M, CID: 0, LAC: 4421, MCC: 460, MNC: 0, Pwr: -54
ARFCN: 35, Freq: 942.0M, CID: 0, LAC: 4421, MCC: 460, MNC: 0, Pwr: -61
ARFCN: 37, Freq: 942.4M, CID: 41285, LAC: 4421, MCC: 460, MNC: 0, Pwr: -53
ARFCN: 39, Freq: 942.8M, CID: 64215, LAC: 4421, MCC: 460, MNC: 0, Pwr: -46
init3@HackSmith:~/sdr/gr-gsm/apps$
```

46000（中国移动）的基站数量比46001（中国联通）的多

```
init3@HackSmith:~/sdr/gr-gsm/apps$ sudo ./grgsm_scanner -b DCS1800
linux; GNU C++ version 4.8.4; Boost_105400; UHD_003.010.001.001-release
```

```
ARFCN: 512, Freq: 1805.2M, CID: 11327, LAC: 4219, MCC: 460, MNC: 0, Pwr: -79
ARFCN: 518, Freq: 1806.4M, CID: 17032, LAC: 4421, MCC: 460, MNC: 0, Pwr: -77
ARFCN: 640, Freq: 1830.8M, CID: 51418, LAC: 4301, MCC: 460, MNC: 1, Pwr: -68
ARFCN: 650, Freq: 1832.8M, CID: 0, LAC: 4301, MCC: 460, MNC: 1, Pwr: -70
```

# 手机上网 GPRS

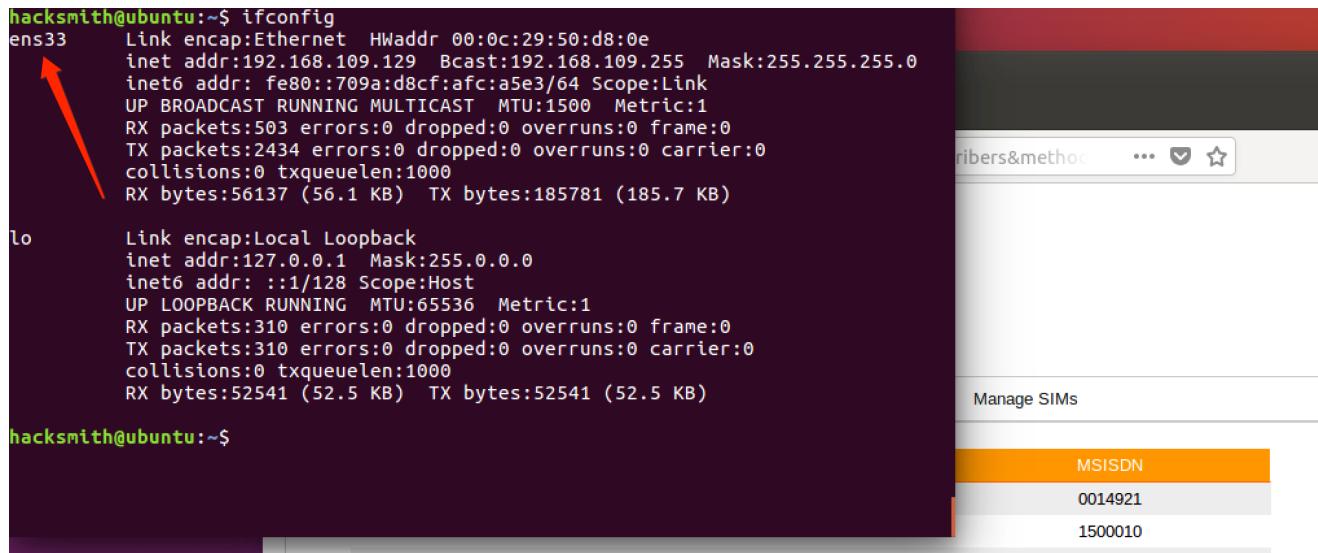
- ▶ 开启数据转发:

```
sudo su
```

```
echo 1 >> /proc/sys/net/ipv4/ip_forward
```

- ▶ Iptable 映射:

```
sudo iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE (虚拟机网卡 ens33  
物理机eth0)
```



The image shows a composite screenshot. On the left, a terminal window displays the output of the 'ifconfig' command. An arrow points from the top of this window to the right, where a smaller window titled 'Manage SIMs' is visible. This window lists three SIM cards: 'MSISDN 0014921' and '1500010'. The background of the entire image features a green and white abstract geometric pattern.

```
hacksmith@ubuntu:~$ ifconfig
ens33      Link encap:Ethernet HWaddr 00:0c:29:50:d8:0e
            inet addr:192.168.109.129 Bcast:192.168.109.255 Mask:255.255.255.0
            inet6 addr: fe80::709a:d8cf:afc:a5e3/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:503 errors:0 dropped:0 overruns:0 frame:0
            TX packets:2434 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:56137 (56.1 KB) TX bytes:185781 (185.7 KB)

lo        Link encap:Local Loopback
            inet addr:127.0.0.1 Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:65536 Metric:1
            RX packets:310 errors:0 dropped:0 overruns:0 frame:0
            TX packets:310 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:52541 (52.5 KB) TX bytes:52541 (52.5 KB)

hacksmith@ubuntu:~$
```

# 手机上网 GPRS

Subscribers BTS Configuration Call Logs Outgoing

GSM GPRS Control Transceiver Tapping Test YBTS

GPRS GPRS Advanced SGSN GGSN

Set parameters values for section [gprs] to be written in ybts.conf

Enable  ?

RAC 0 ?

RA COLOUR 7 ?

启用GPRS功能

Subscribers BTS Configuration Call Logs Outgoing

GSM GPRS Control Transceiver Tapping Test YBTS

GPRS GPRS Advanced SGSN GGSN

Set parameters values for section [ggsn] to be written in ybts.conf file.

DNS 114.114.114.114 ?

Firewall.Enable block MS attempted acc? ?

IP.MaxPacketSize 1520 ?

IP.ReuseTimeout 180 ?

IP.TossDuplicatePackets  ?

Logfile.Name ggsn.log

MS.IP.Base 192.168.88.1

MS.IP.MaxCount 254

MS.IP.Route

ShellScript

TunName GPRS

Section [ggsn] has internal GGSN function configuration.

配置GGSN

基站启动后，主机多出一块虚拟网卡：

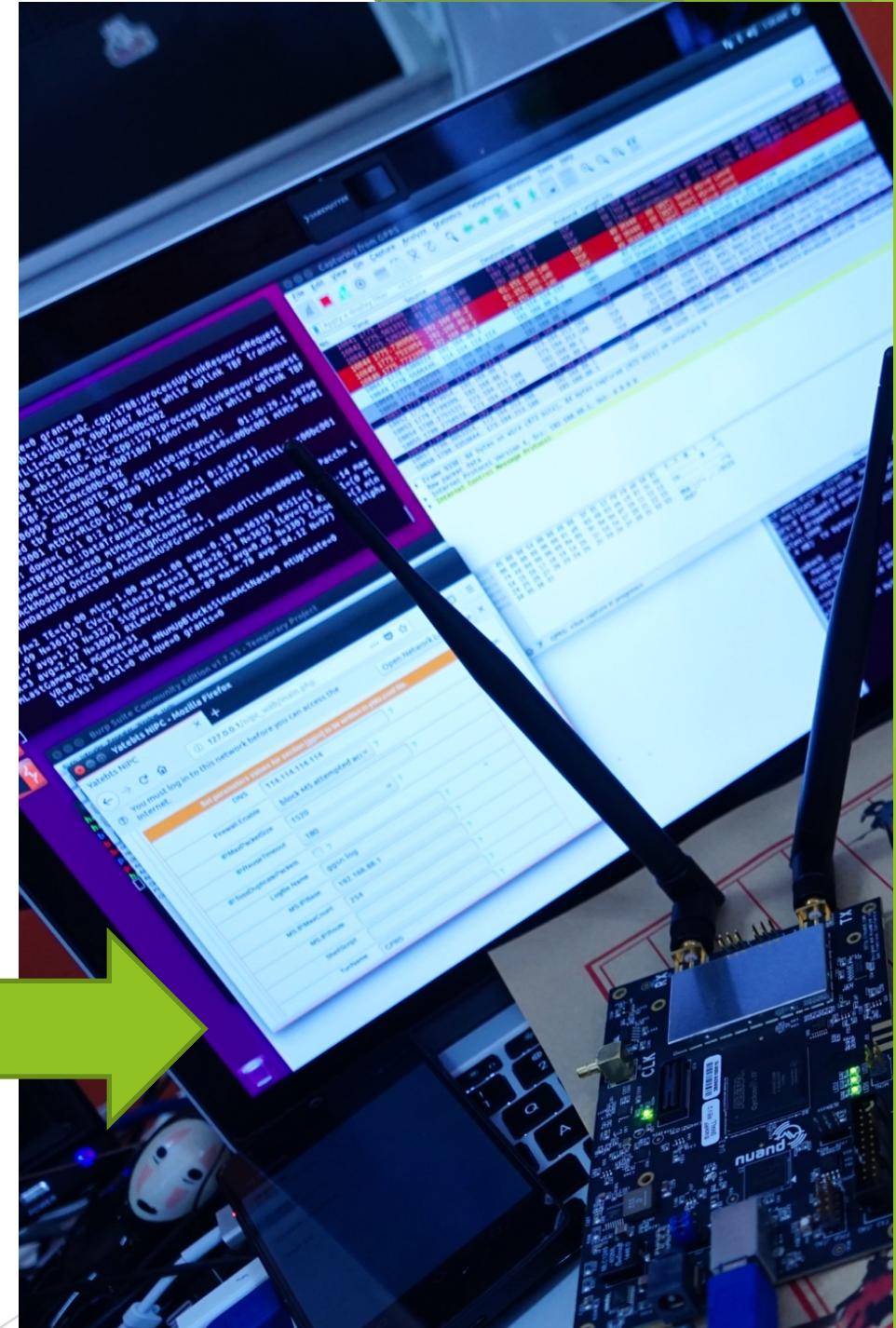
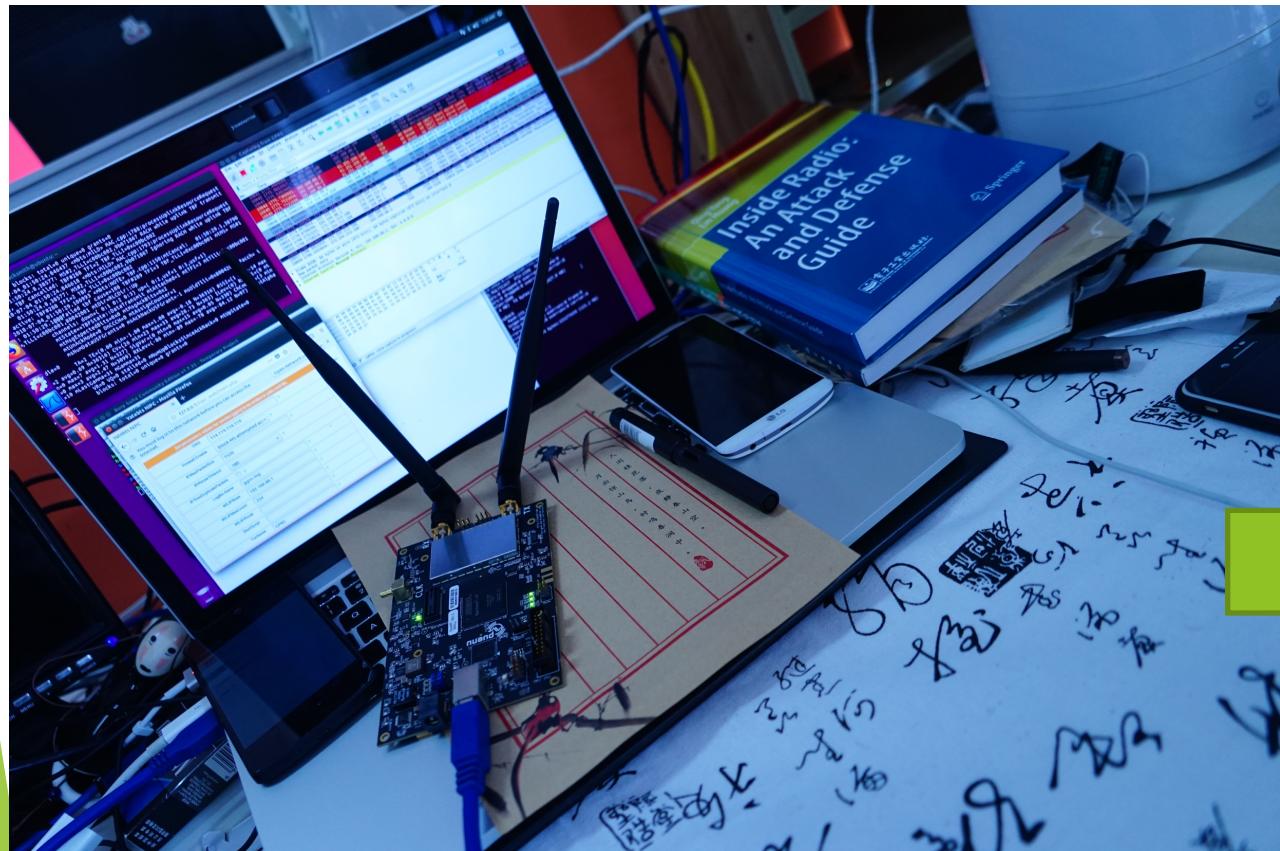
```
hacksmith@ubuntu:~$ sudo yate -s
[sudo] password for hacksmith:
Supervisor (3028) is starting, max sanity 5
Yate (3029) is starting
Loaded module CdrFile
Loaded module PBX
Loaded module Analyzer
Loaded module DumbChann
Loaded module iLBC - ba
Loaded module iLBC - ba
Loaded module isAC floa
SPL version 1.2.0)
Loaded module FileInfo
Loaded module Call Fork
Loaded module File Tranens33
Loaded module CdrBuild
Loaded module YRTP
Loaded module YIAX
Loaded module MsgSniffe
Loaded module Call Gene
Loaded module YJingle
Loaded module YSTUN
Loaded module GVoice
Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
inet6 addr: fe80::2a24:da65:8d67:c2f/64 Scope:Link
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:3 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:500
RX bytes:0 (0.0 B) TX bytes:144 (144.0 B)

Link encap:Ethernet HWaddr 00:0c:29:50:d8:0e
inet addr:192.168.109.129 Bcast:192.168.109.255 Mask:255.255.255.0
inet6 addr: fe80::709a:d8cf:afc:a5e3/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:543 errors:0 dropped:0 overruns:0 frame:0
TX packets:2555 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:59227 (59.2 KB) TX bytes:194718 (194.7 KB)

Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:11446 errors:0 dropped:0 overruns:0 frame:0
TX packets:11446 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:2021570 (2.0 MB) TX bytes:2021570 (2.0 MB)
```

# 手机、IOT设备流量嗅探

通过wireshark捕获虚拟网卡的流量，  
从而实现对基站内所有设备的流量进行嗅探。必要时可进行GPRS-MITM



# 参 考 资 料

[https://wiki.yatebts.com/index.php/Main\\_Page](https://wiki.yatebts.com/index.php/Main_Page)

[http://openbts.org/site/wp-content/uploads/ebook/Getting\\_Started\\_with\\_OpenBTS\\_Range\\_Networks.pdf](http://openbts.org/site/wp-content/uploads/ebook/Getting_Started_with_OpenBTS_Range_Networks.pdf)

<http://openbts.org/site/wp-content/uploads/2014/07/OpenBTS-4.0-Manual.pdf>



@cnxroot

<https://cn0xroot.com>