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

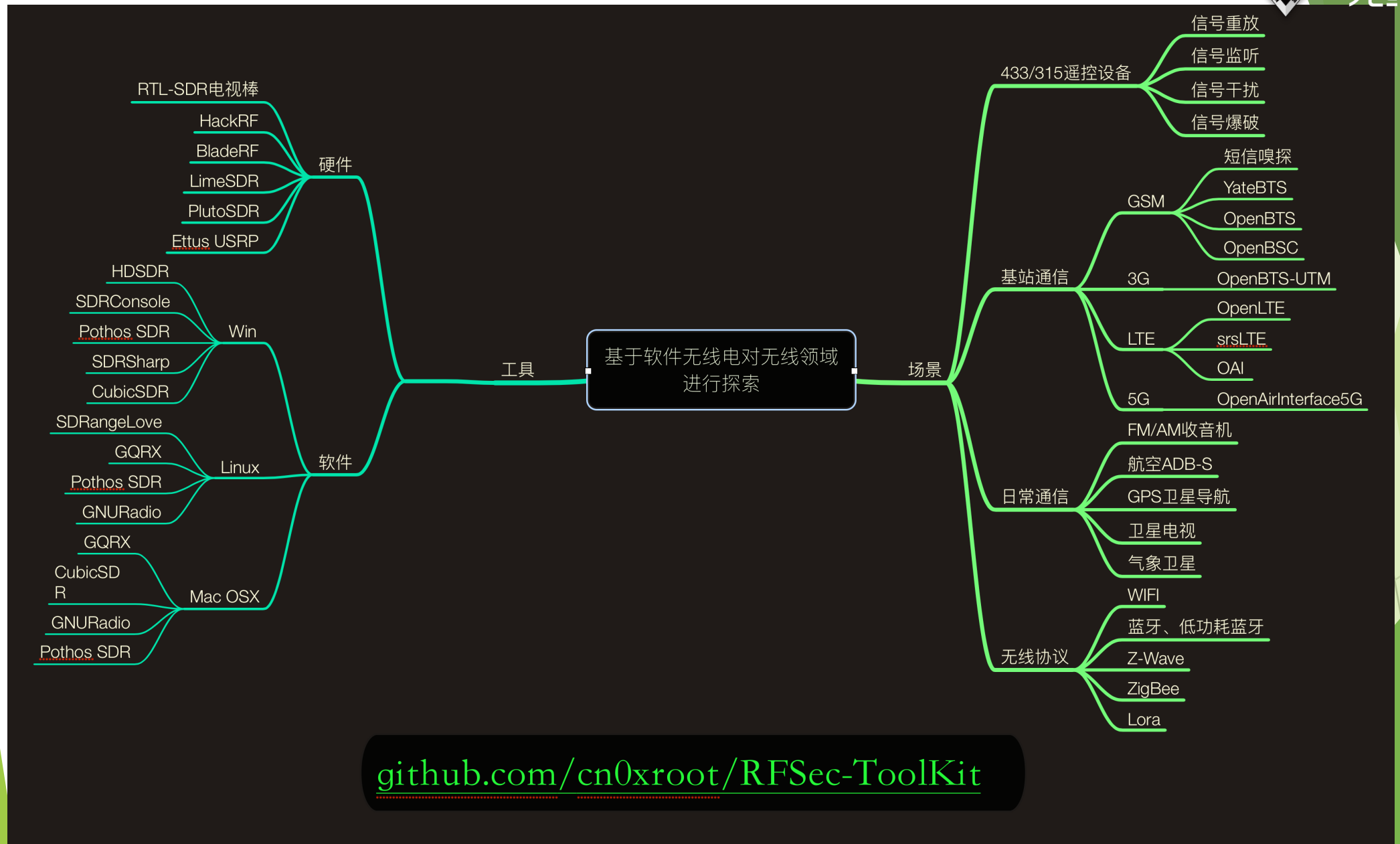
SEE PROFILE

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 0xroot

360
无线电安全研究部



github.com/cn0xroot/RFSec-ToolKit

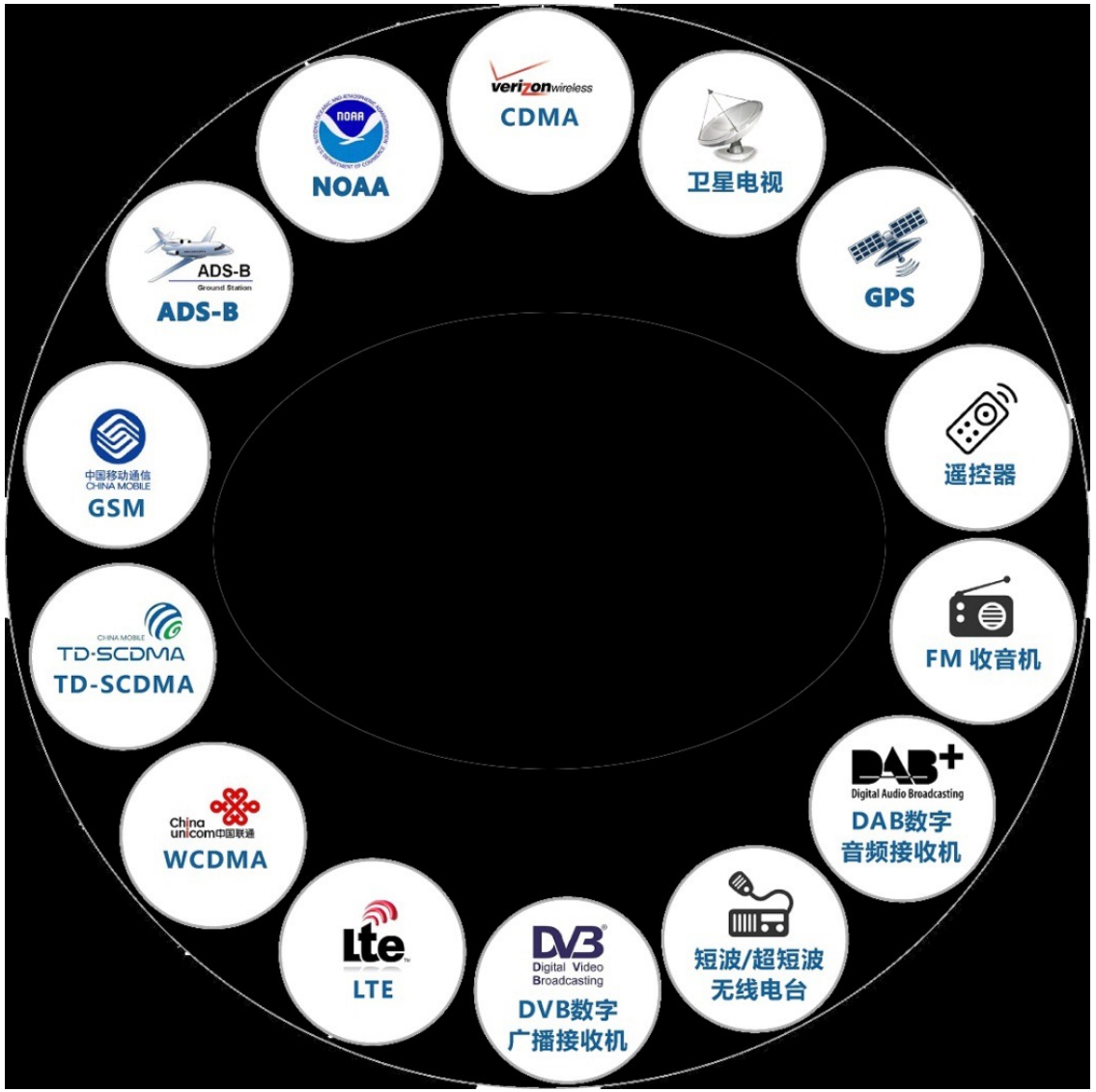
软件无线电硬件

- 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	≈￥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
- **OpenBTS-UTM** https://fairwaves.co/blog/openbts-umts-3g-umtrx/

开源基站项目

360
无线电安全研究部

- **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

360
无线电安全研究部

为什么是2G：
攻击的面、范围广

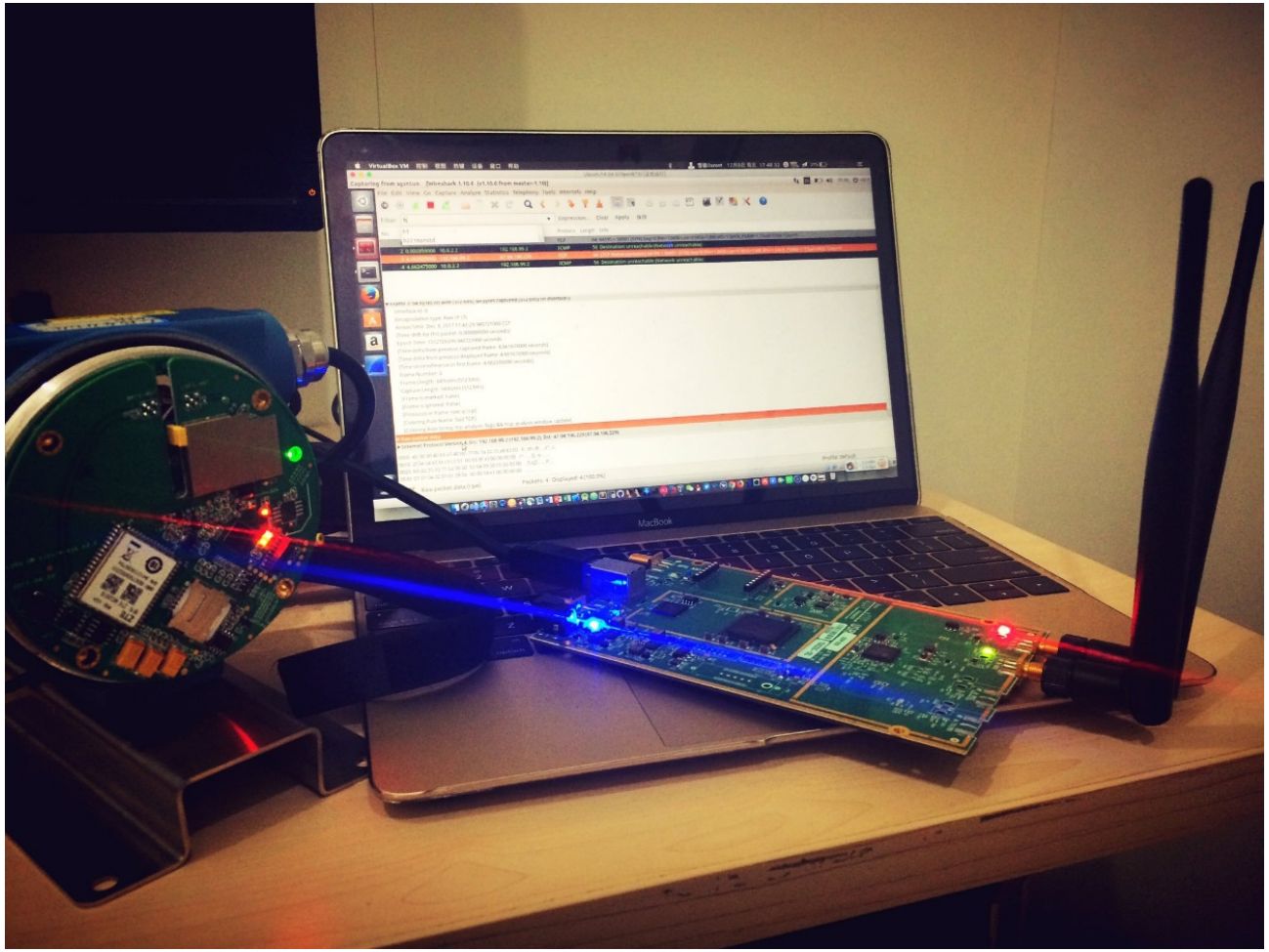
- **鉴权** 2G存在安全缺陷：单向认证、鉴权（3G、4G均为双向认证）导致非法的设备（如基站）可以伪装成合法的成员，从而欺骗用户，轻松将用户拉入伪基站网络；

- **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：

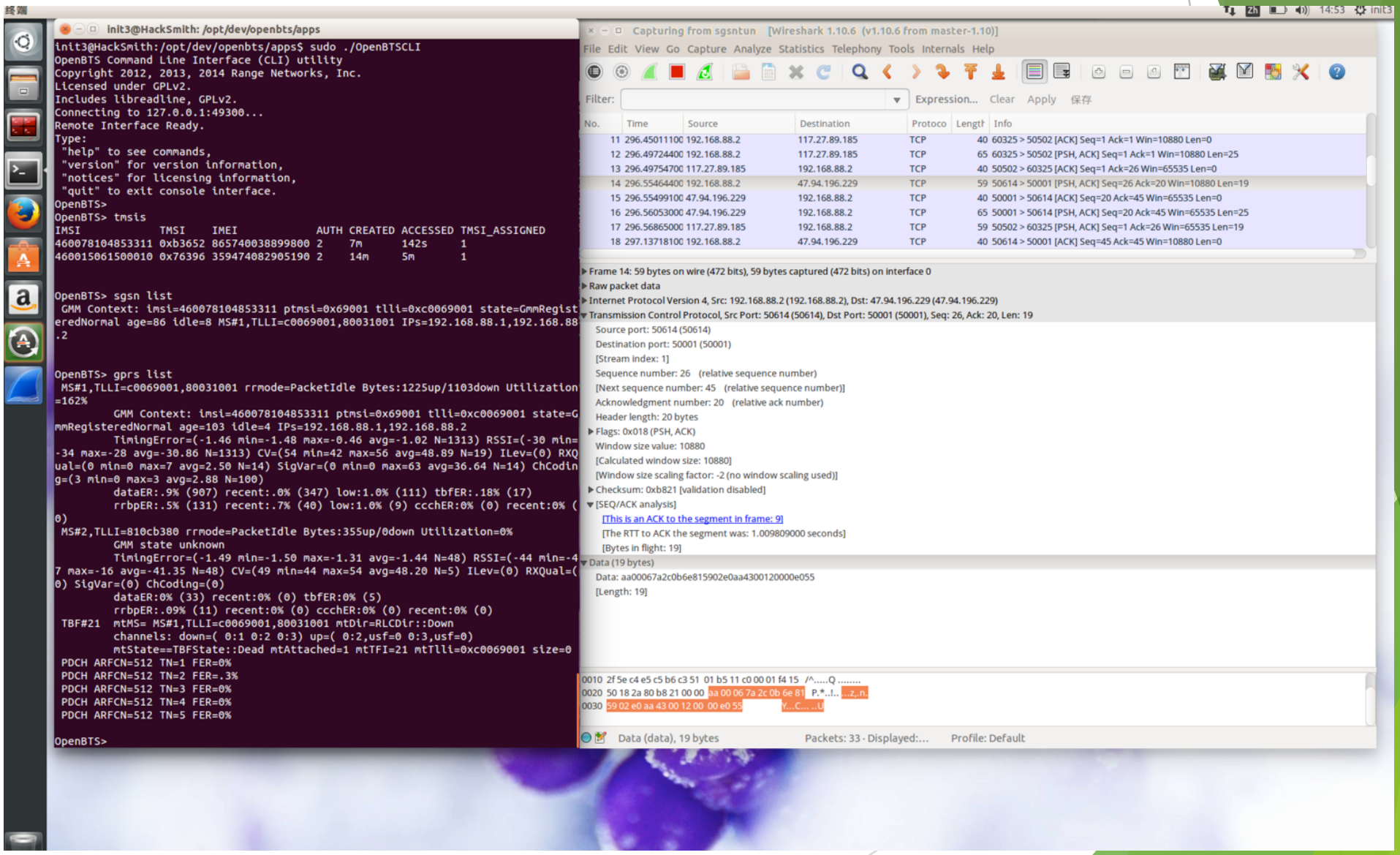
- ✓ OpenBTSCLI命令行功能强大，可玩性高；
- ✓ GSM电话、SMS短信功能稳定；
- ✓ USRP散热性能强；

缺点：

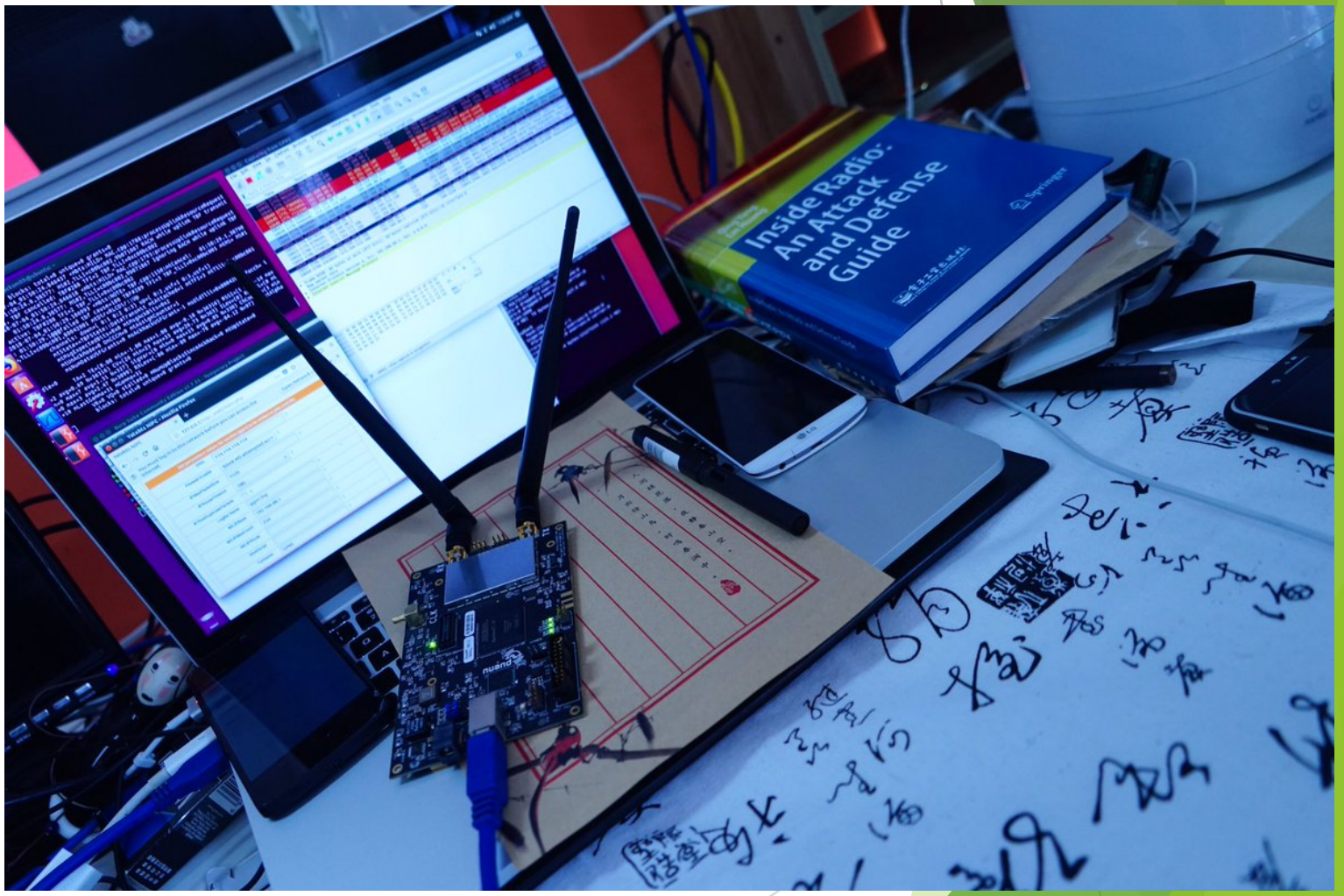
- ◆ 编译难度大：依赖包多、需要翻墙编译；
- ◆ 几百页文档、配置复杂、没有可视化配置页面不适合新手；
- ◆ 运行时需要启动多个组件；
- ◆ GPRS联网功能Bug较多；

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



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)

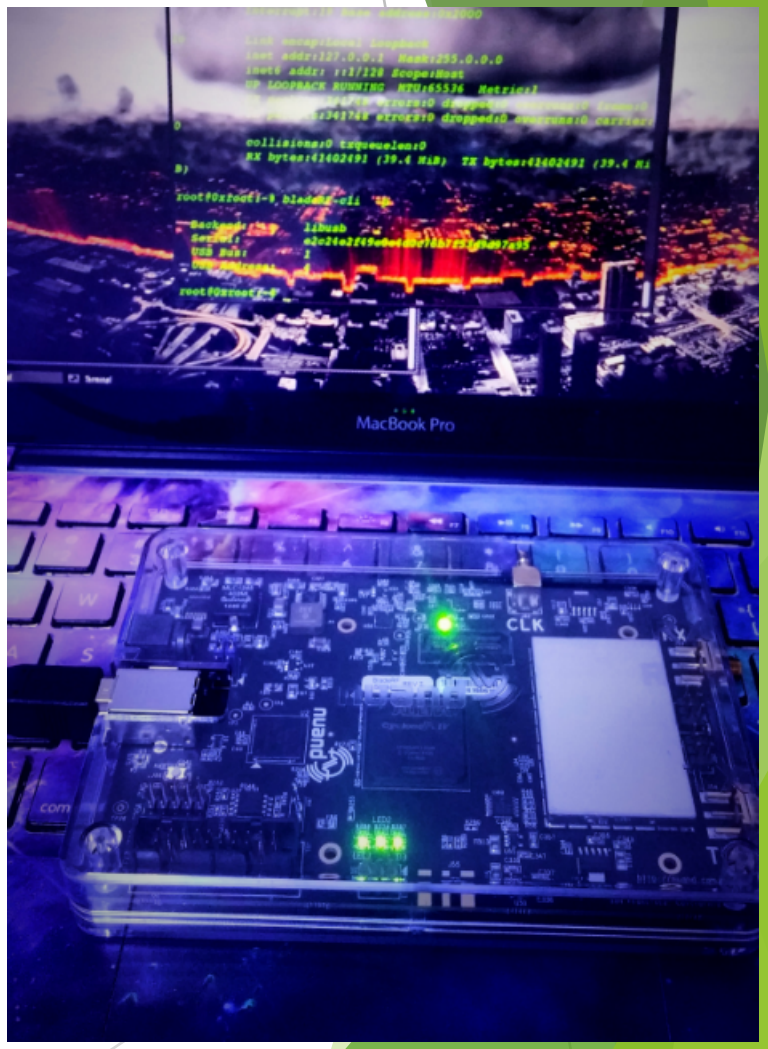
安装依赖 & 编译BladeRF

- 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)

360 无线电安全研究部

- 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

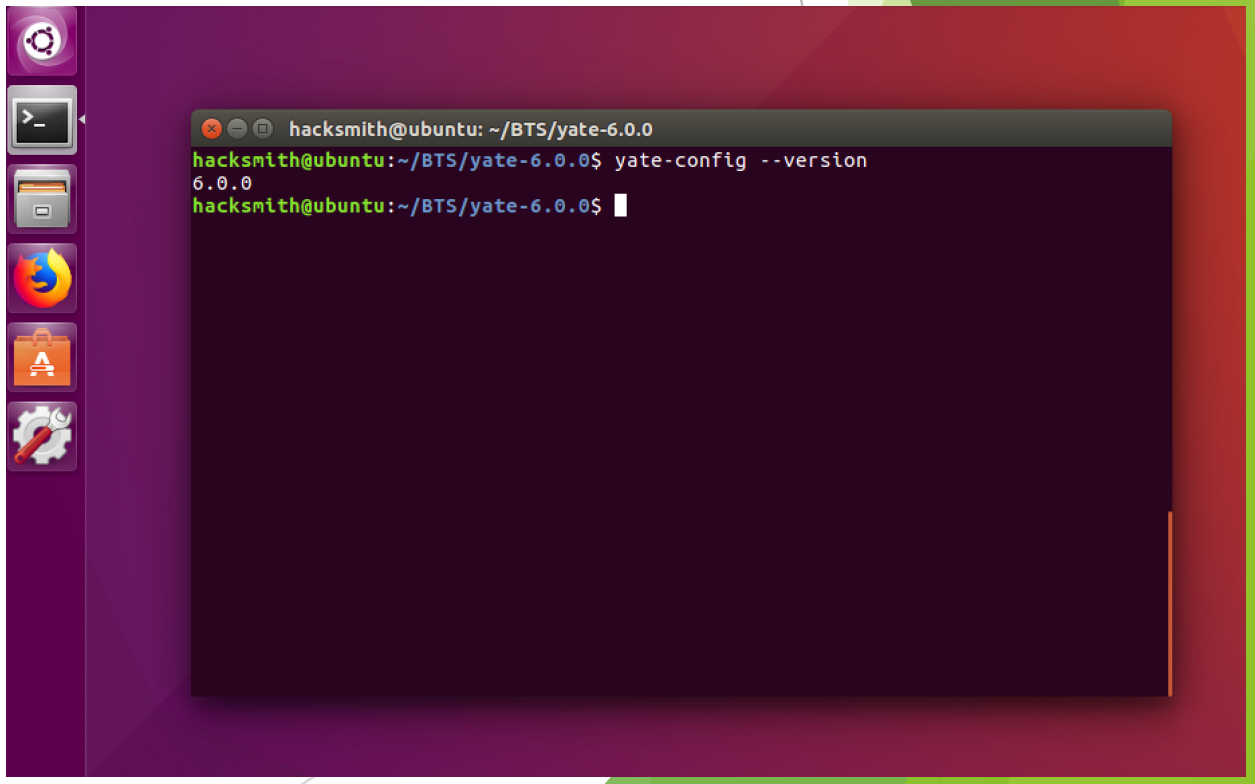
YateBTS+BladeRF 安装指南(Ubuntu 16.04)

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



360
无线电安全研究部

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

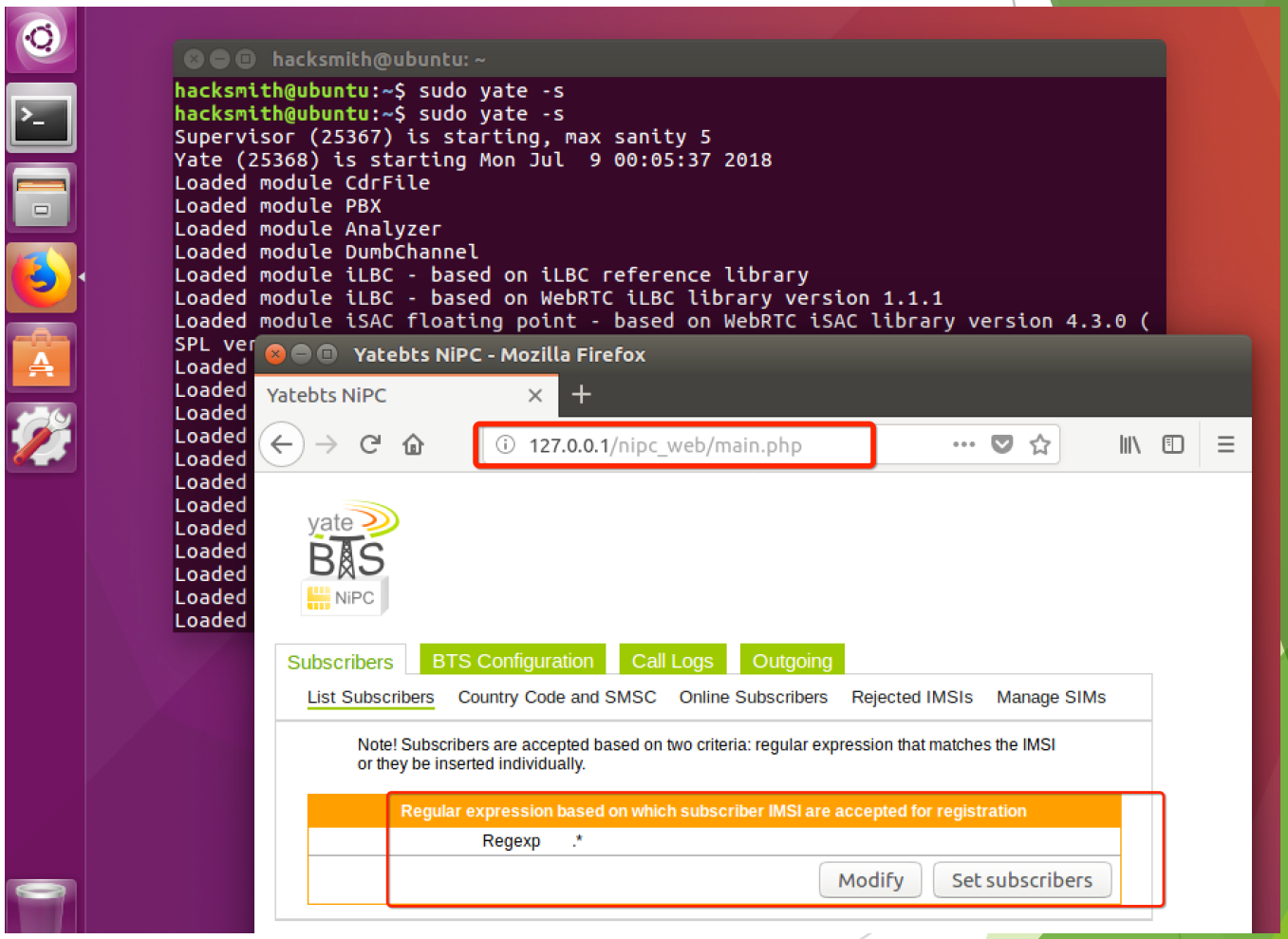
Yate-BTS配置

- sudo yate -s 启动基站
- 在浏览器访问：

localhost/nipc_web

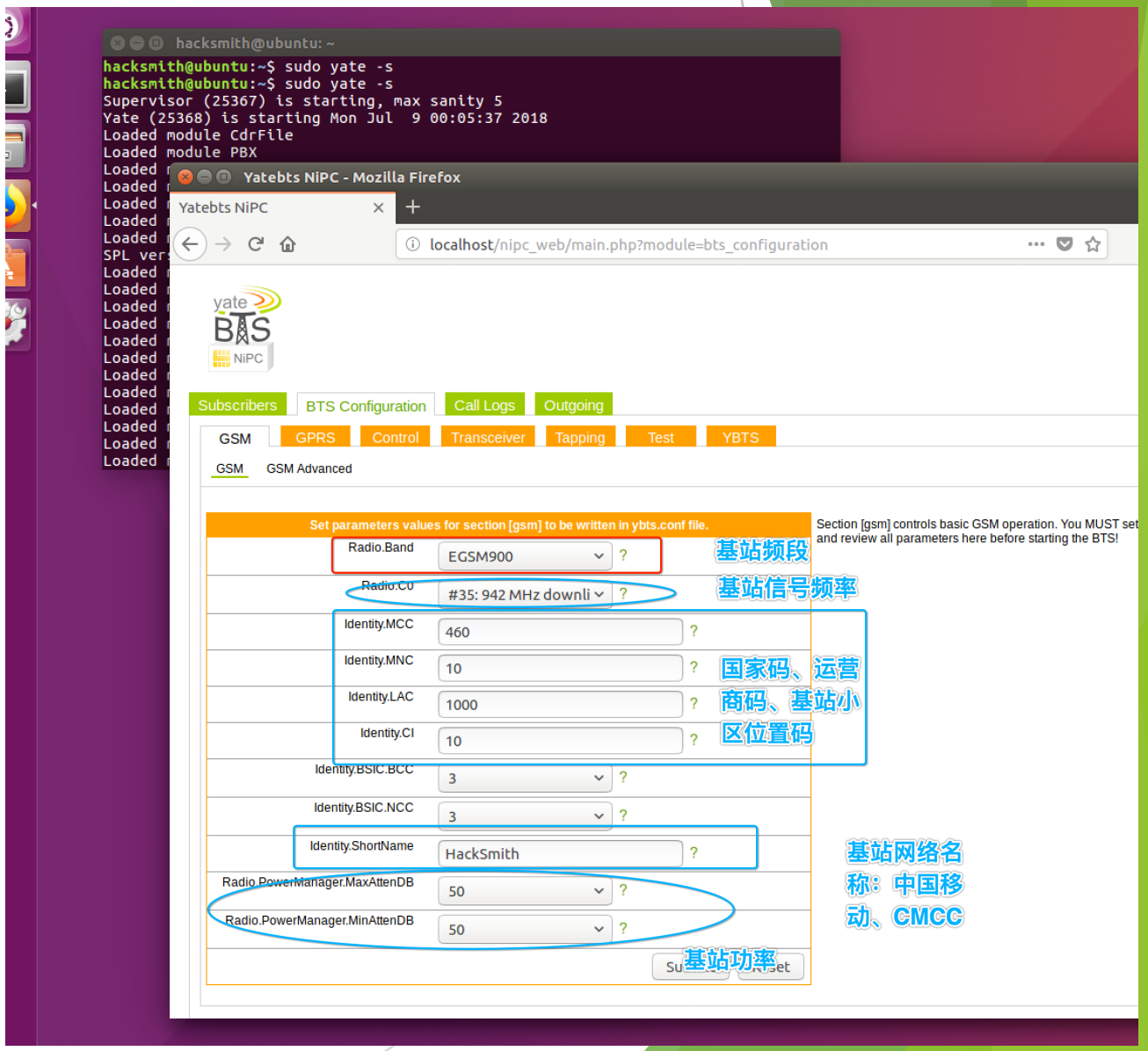
- 修改Regexp的值为：.*

（允许任意用户加入网络）



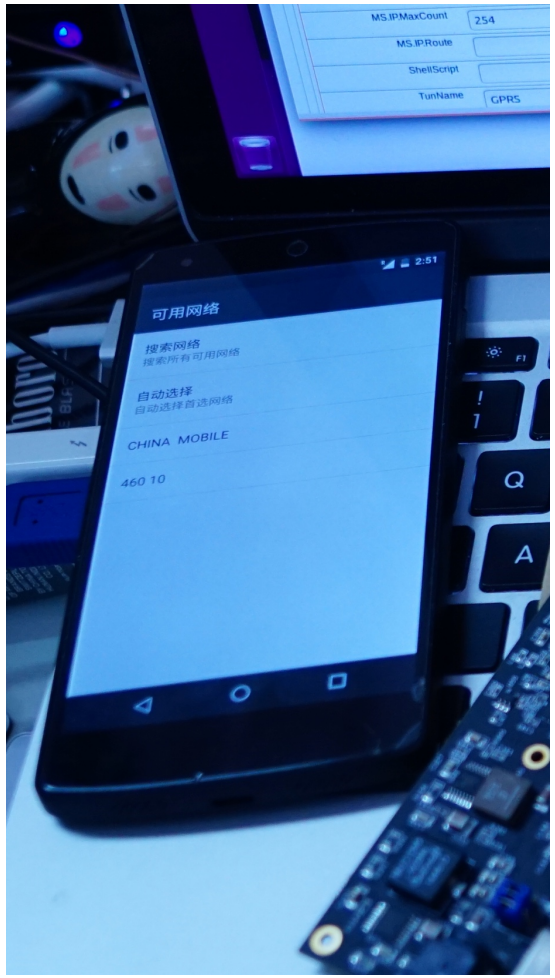
Yate-BTS配置

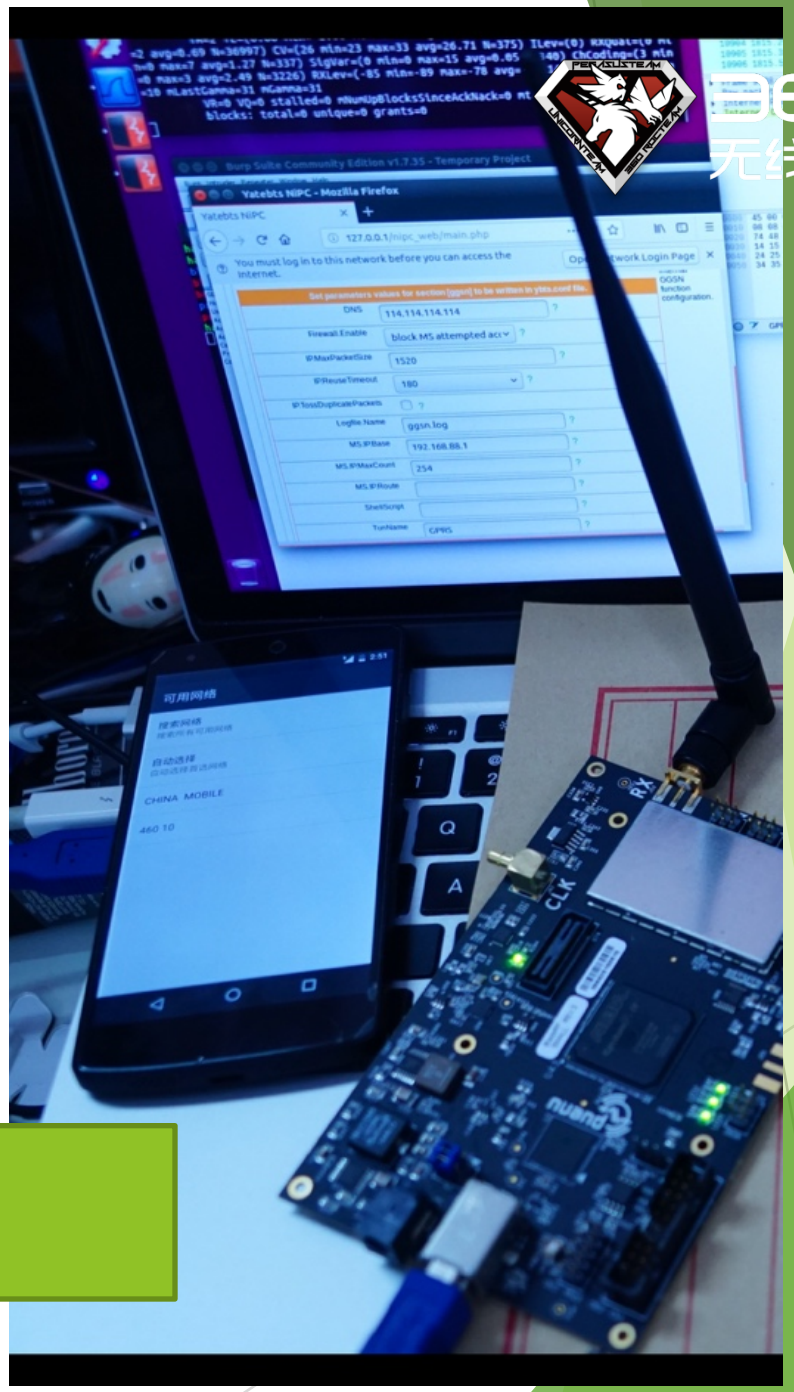
- 配置基站频段：GSM850、或者EGSM900；
- 设定Arfcn值：视实际情况而定；
- MCC：Mobile country code移动设备国家码，中国460；
- MNC：Mobile Network Code移动网络号码，用于识别运营商：中国移动：00、02、04、07；中国联通GSM：01、06、09，
- LAC：Location Area Code，位置区域码
- CI:Cell Identity，基站编号



手机入站

在手机可用网络中搜寻附近基站，手动选择网络。



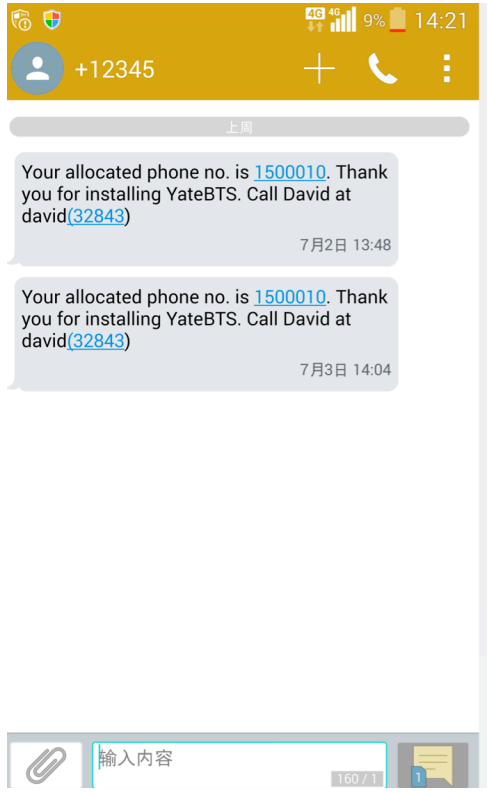


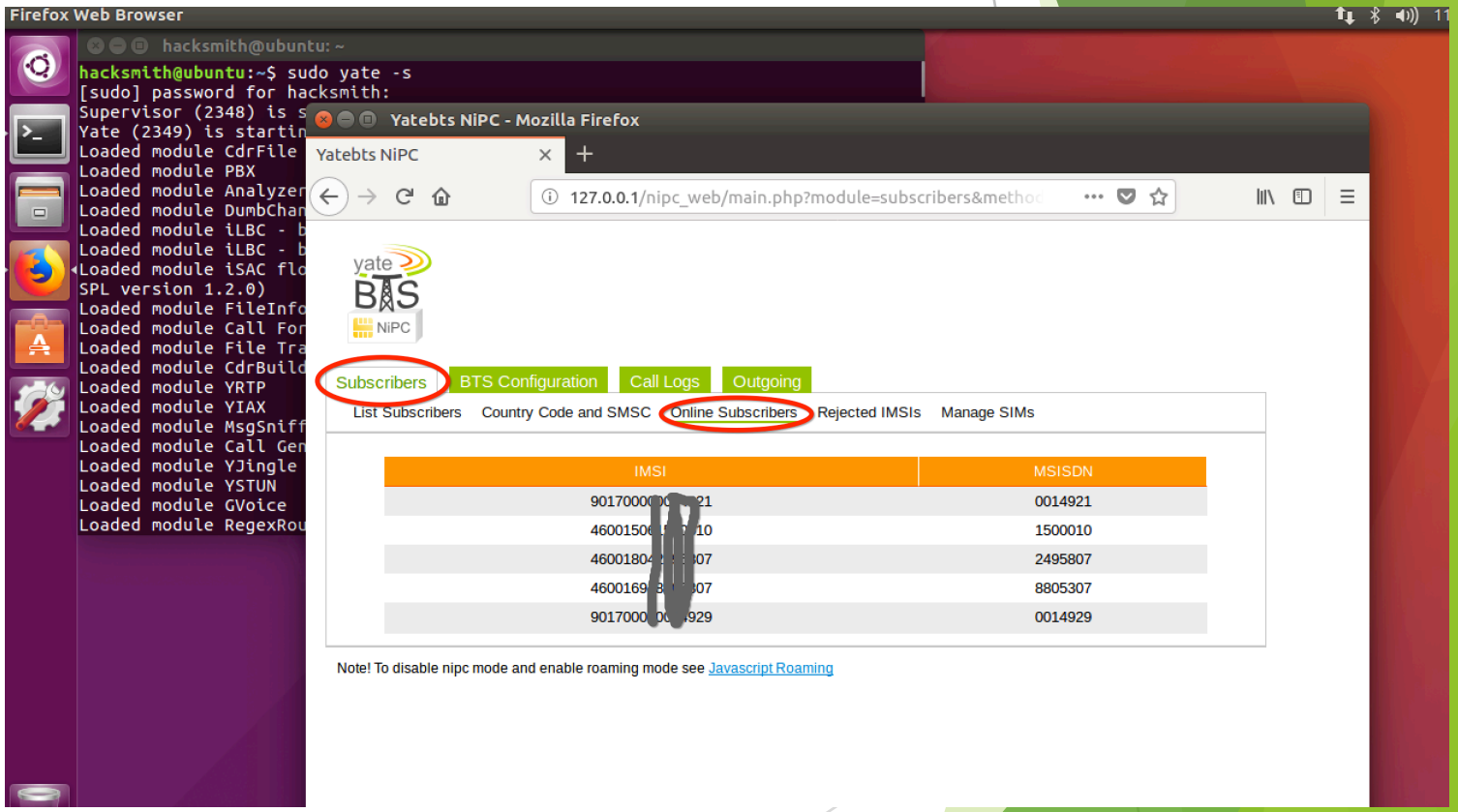
360
无线电安全研究部

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：





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

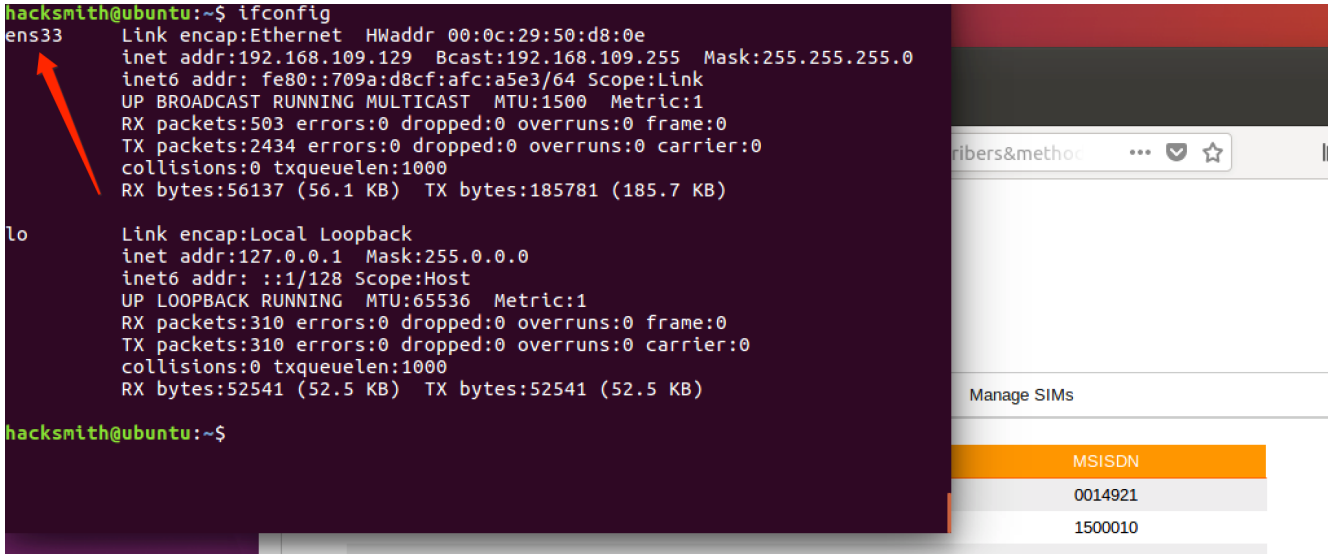
- 开启数据转发：

sudo su

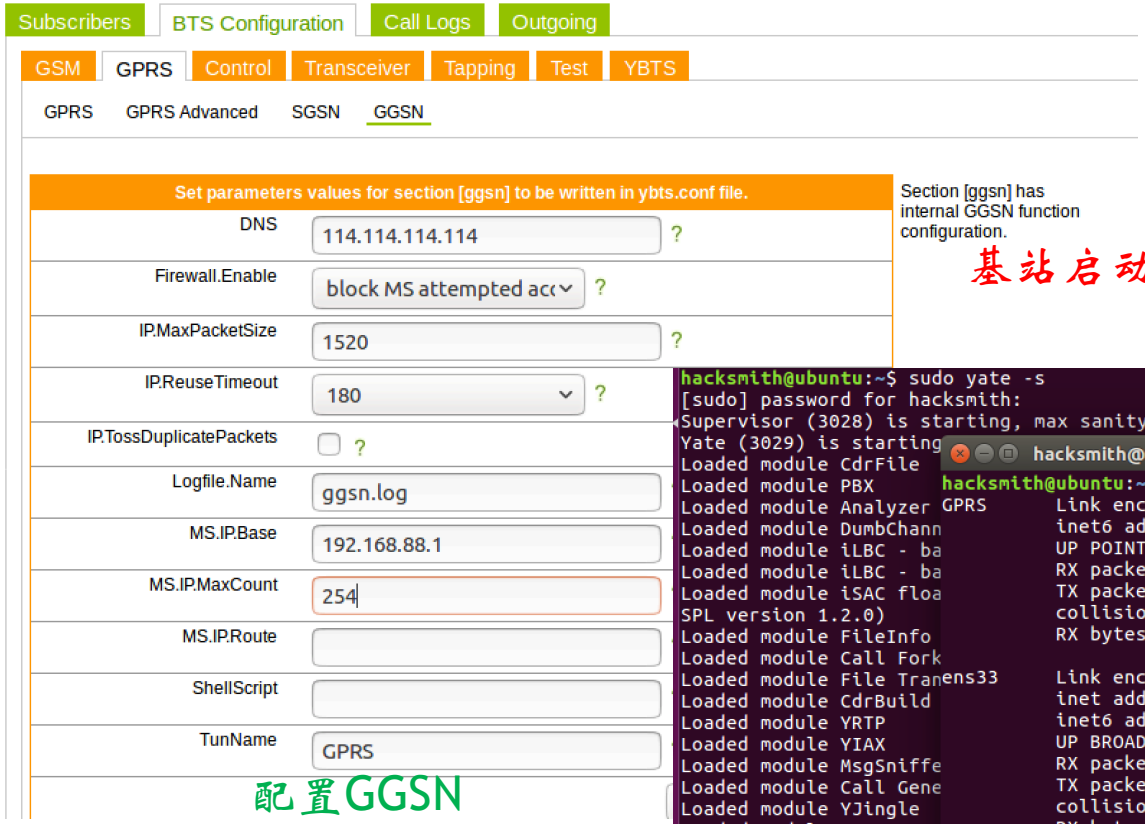
echo 1 >> /proc/sys/net/ipv4/ip_forward

- Iptable映射：

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

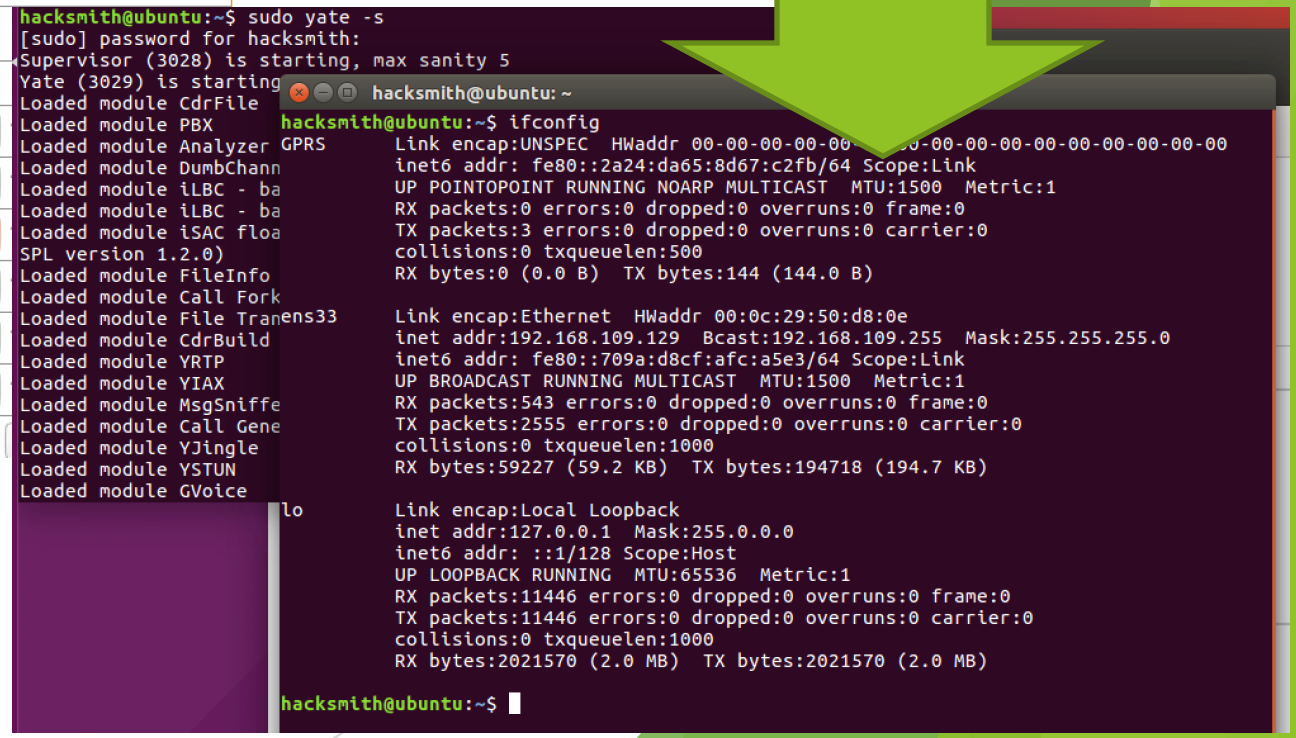


手机上网 GPRS



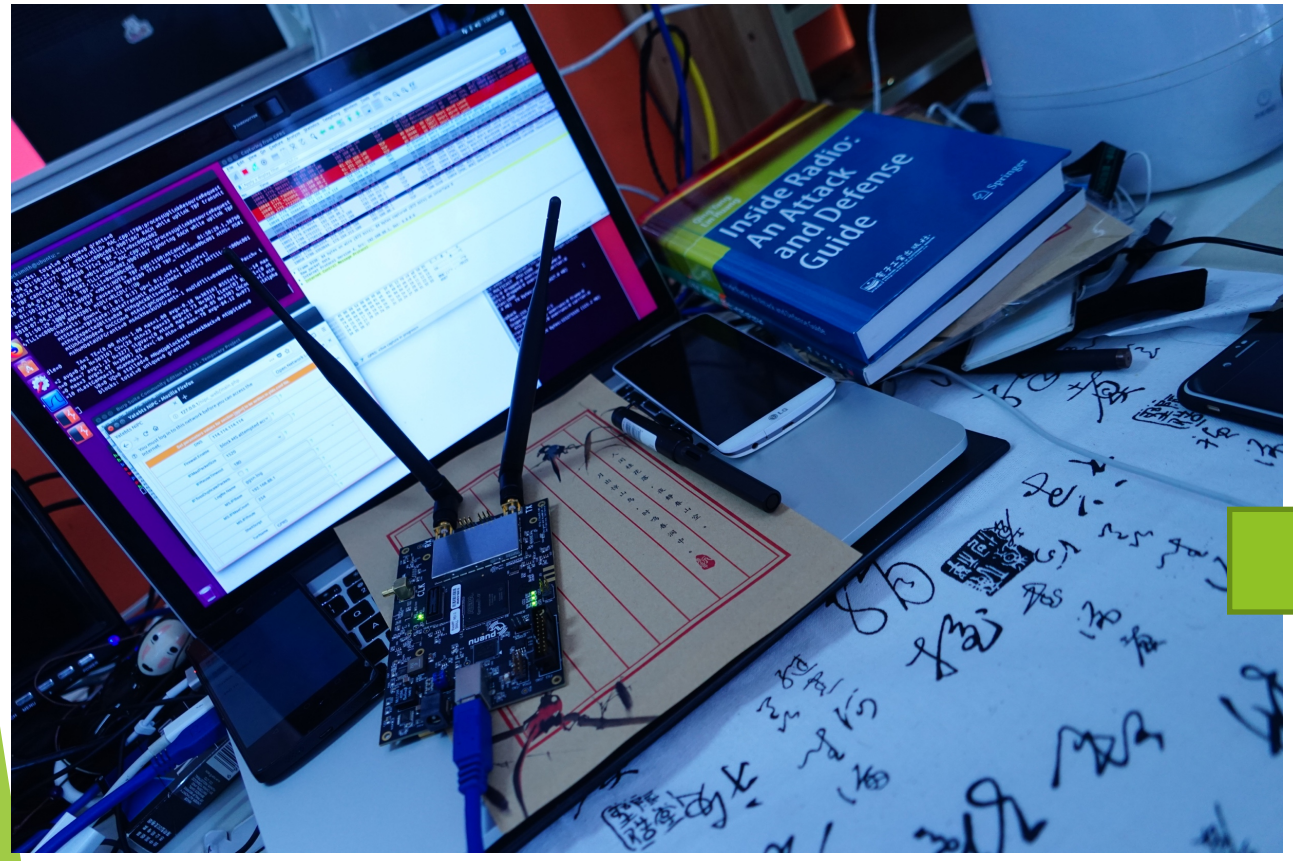
Section [ggsn] has internal GGSN function configuration.

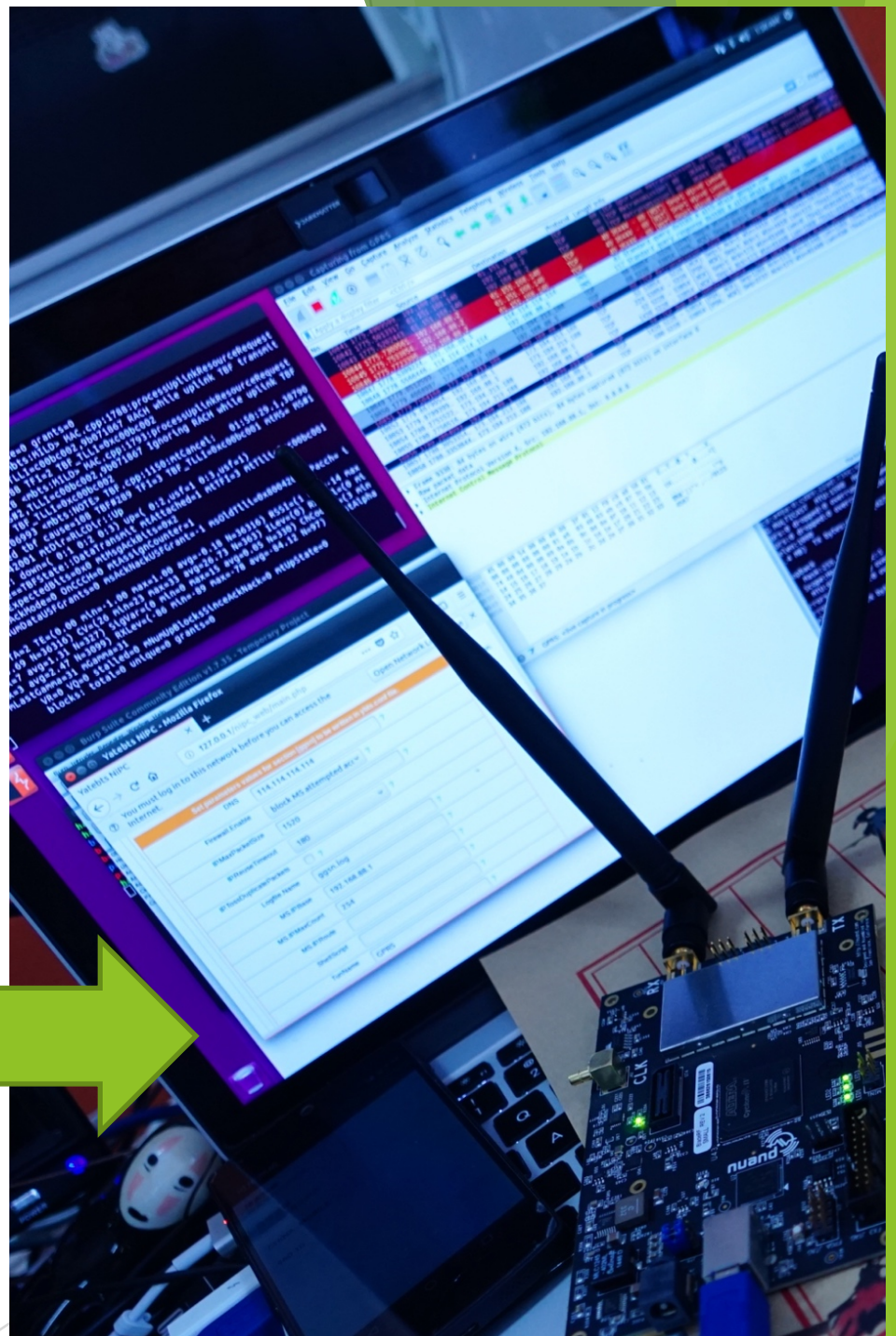
基站启动后，主机多出一块虚拟网卡：



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
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