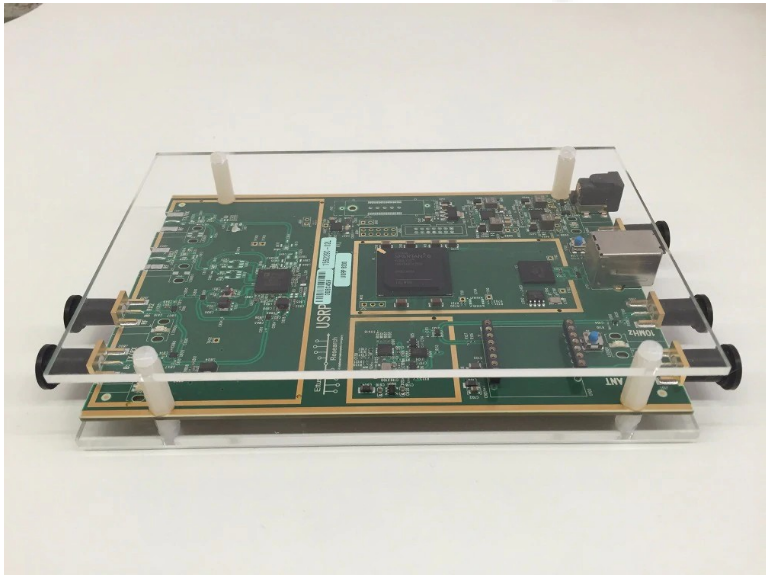
SDR
GUIDE
FOR DUMMIES

.Zhalgas Khassenov
@kruzenshtern2

що це SDR?

RTL-SDR.COM
QUICKSTART SETUP GUIDE: RTL-SDR.COM/QSG
DVB-T+DAB+FM+SDR
RTL2832U R820T2 TCXO+BIAS T+HF
V.3

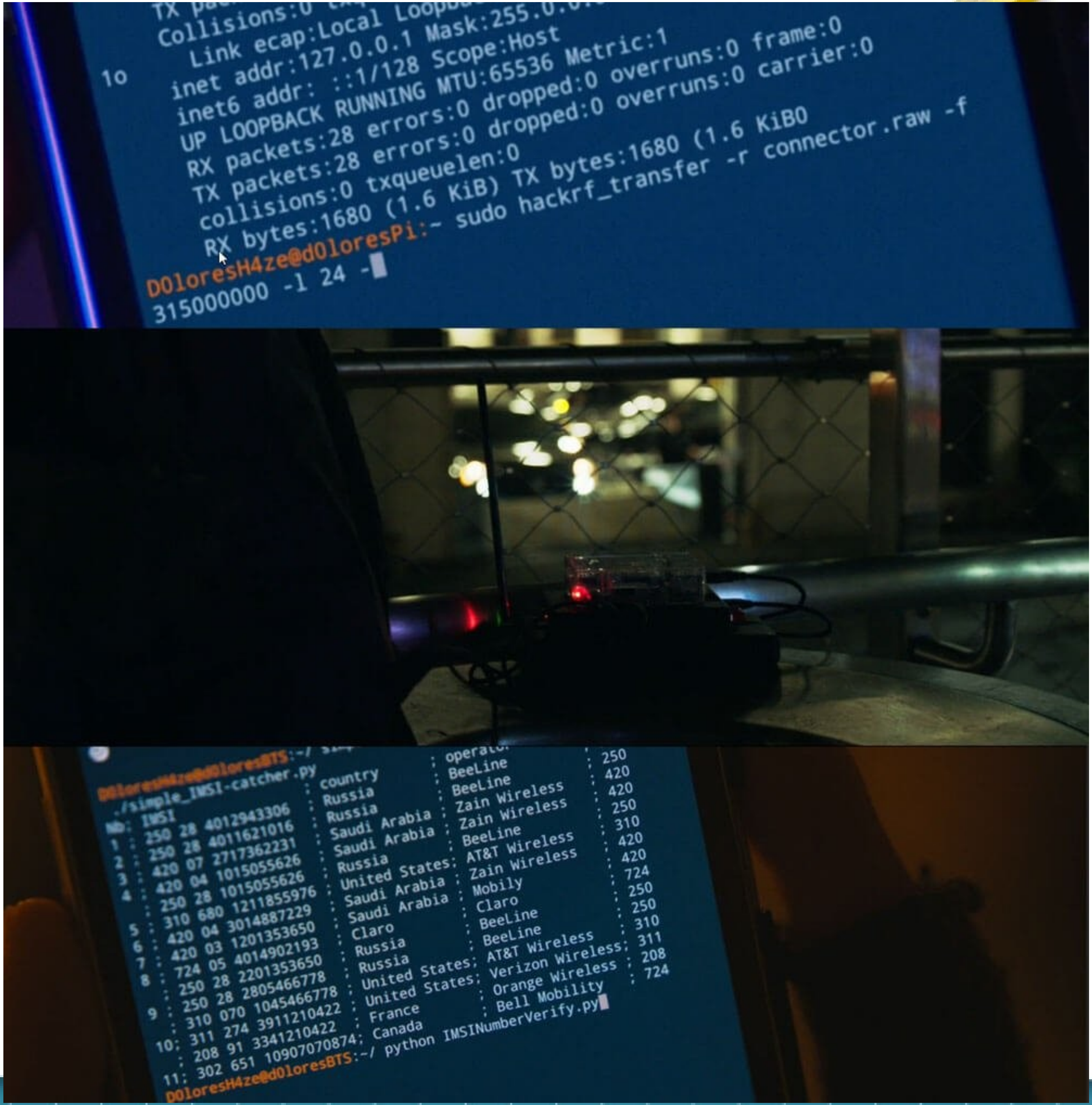

USRP

LimeSDR
ALTERA
Cyclone IV

HackRF One
1MHz-6GHz
HackRF One

nuand

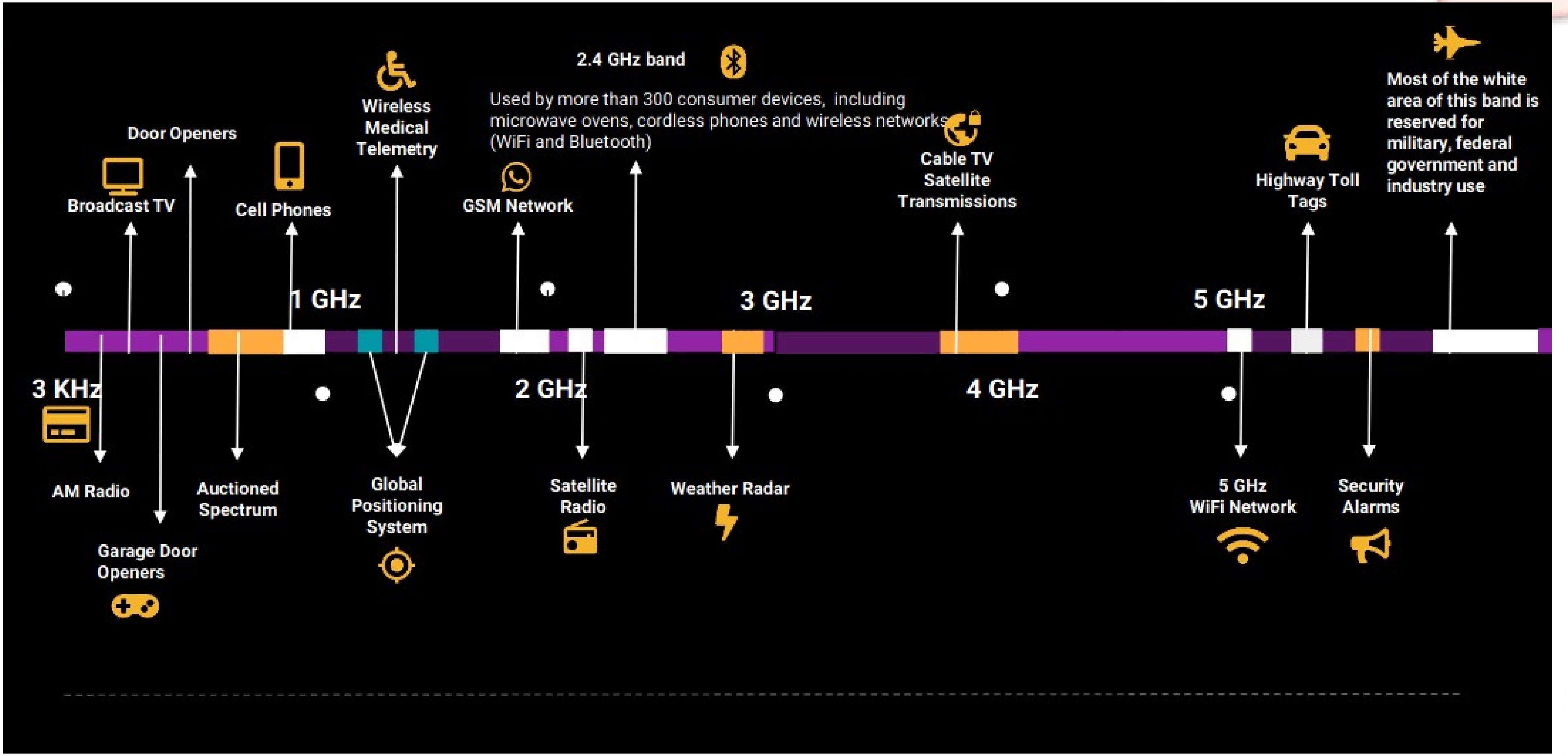
mr.robot



```
        TX pa
        Collisions:0
lo      Link ecap:Local Loopba
        inet addr:127.0.0.1 Mask:255.0.0.
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING MTU:65536 Metric:1
        RX packets:28 errors:0 dropped:0 overruns:0 frame:0
        TX packets:28 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:1680 (1.6 KiB) TX bytes:1680 (1.6 KiB0
D0loresH4ze@d0loresPi:~ sudo hackrf_transfer -r connector.raw -f
315000000 -1 24 -
```

```
D0loresH4ze@d0loresBTS:~/ sim
./simple_IMSI-catcher.py
Nb: IMSI                : country        : operato
1 : 250 28 4012943306   : Russia         : BeeLine
2 : 250 28 4011621016   : Russia         : BeeLine          : 250
3 : 420 07 2717362231   : Saudi Arabia   : Zain Wireless    : 420
4 : 420 04 1015055626   : Saudi Arabia   : Zain Wireless    : 420
  : 250 28 1015055626   : Russia         : BeeLine          : 250
5 : 310 680 1211855976  : United States: AT&T Wireless      : 310
6 : 420 04 3014887229   : Saudi Arabia   : Zain Wireless    : 420
7 : 420 03 1201353650   : Saudi Arabia   : Mobily           : 420
8 : 724 05 4014902193   : Claro          : Claro            : 724
  : 250 28 2201353650   : Russia         : BeeLine          : 250
9 : 250 28 2805466778   : Russia         : BeeLine          : 250
  : 310 070 1045466778  : United States: AT&T Wireless      : 310
10: 311 274 3911210422  : United States: Verizon Wireless: 311
  : 208 91 3341210422   : France         : Orange Wireless  : 208
11: 302 651 10907070874: Canada          : Bell Mobility    : 724
D0loresH4ze@d0loresBTS:~/ python IMSINumberVerify.py
```

Radio frequency allocation



Door Openers

Broadcast TV

Cell Phones

Wireless Medical Telemetry

GSM Network

2.4 GHz band

Used by more than 300 consumer devices, including microwave ovens, cordless phones and wireless networks (WiFi and Bluetooth)

Cable TV Satellite Transmissions

Highway Toll Tags

Most of the white area of this band is reserved for military, federal government and industry use

1 GHz

3 GHz

5 GHz

3 KHz

2 GHz

4 GHz

AM Radio

Garage Door Openers

Auctioned Spectrum

Global Positioning System

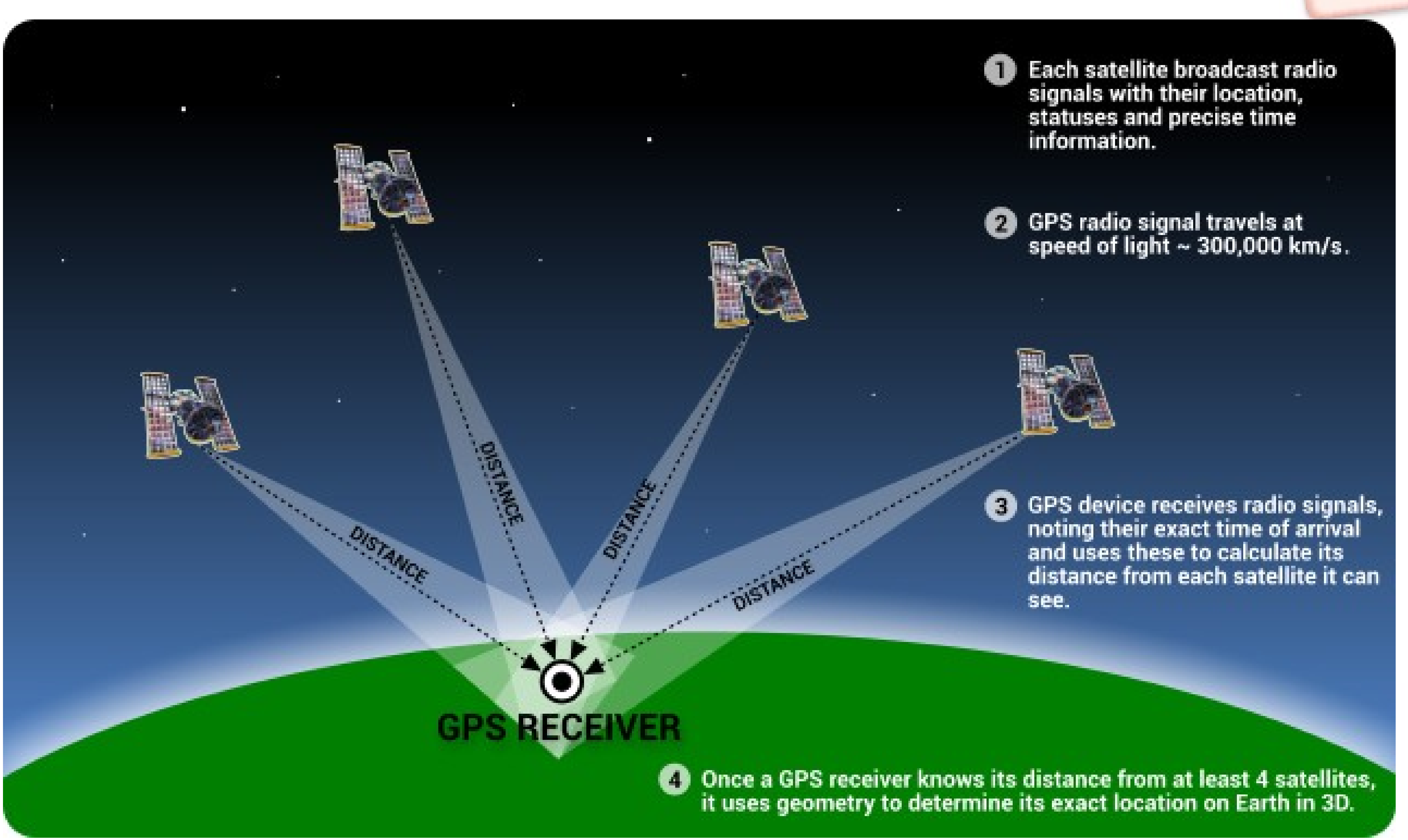
Satellite Radio

Weather Radar

5 GHz WiFi Network

Security Alarms

GPS



1. Each satellite broadcast radio signals with their location, statuses and precise time information.

2. GPS radio signal travels at speed of light ~ 300,000 km/s.

3. GPS device receives radio signals, noting their exact time of arrival and uses these to calculate its distance from each satellite it can see.

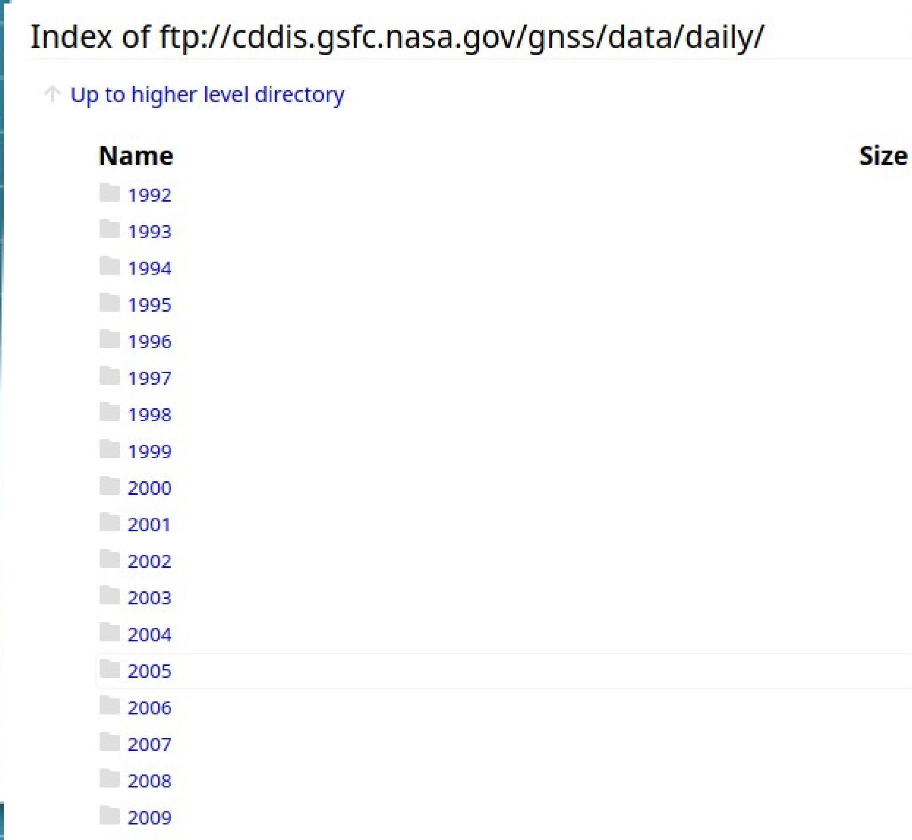
4. Once a GPS receiver knows its distance from at least 4 satellites, it uses geometry to determine its exact location on Earth in 3D.

gps-sdr-sim

```
> $ gps-sdr-sim -e brdc3540.14n -l
30.286502,120.032669,100
```

ephemeris

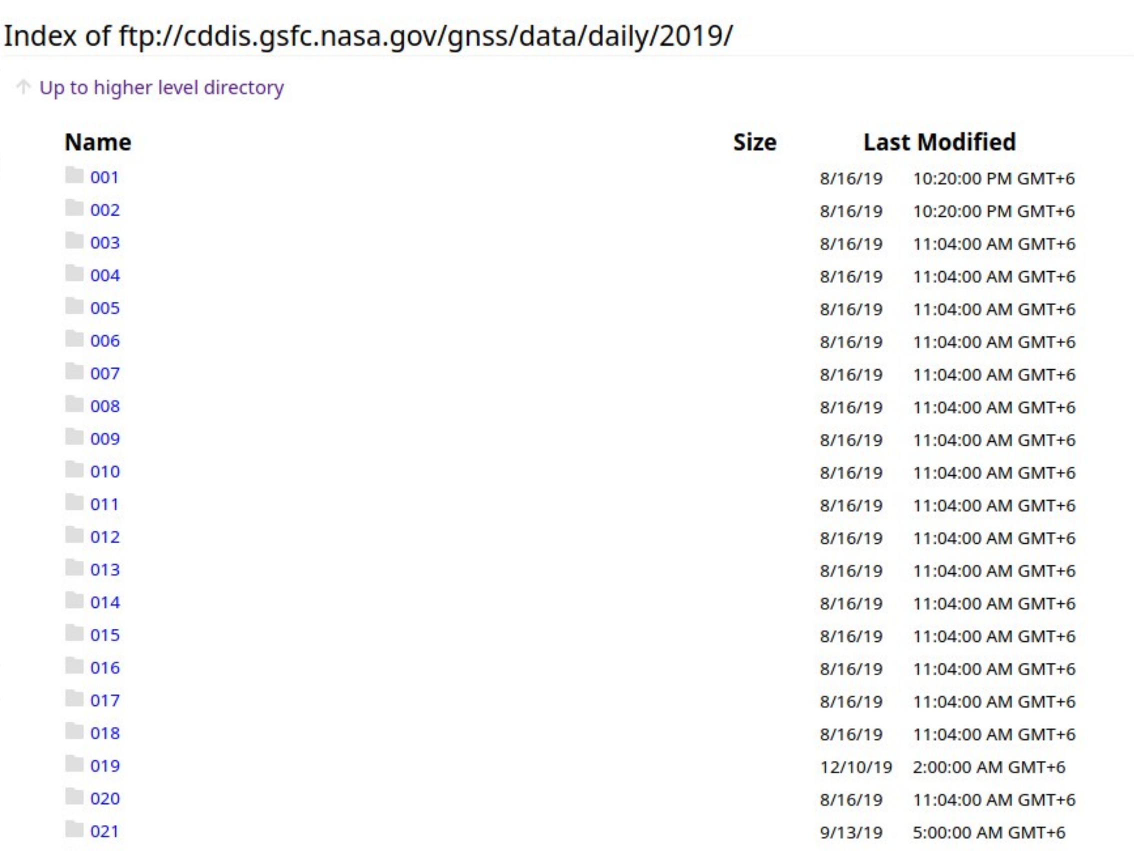
- ephemeris gives the trajectory of naturally occurring astronomical objects as well as artificial satellites in the sky, i.e., the position (and possibly velocity) over time.



Index of ftp://cddis.gsfc.nasa.gov/gnss/data/daily/

↑ Up to higher level directory

Name	Size
1992	
1993	
1994	
1995	
1996	
1997	
1998	
1999	
2000	
2001	
2002	
2003	
2004	
2005	
2006	
2007	
2008	
2009	

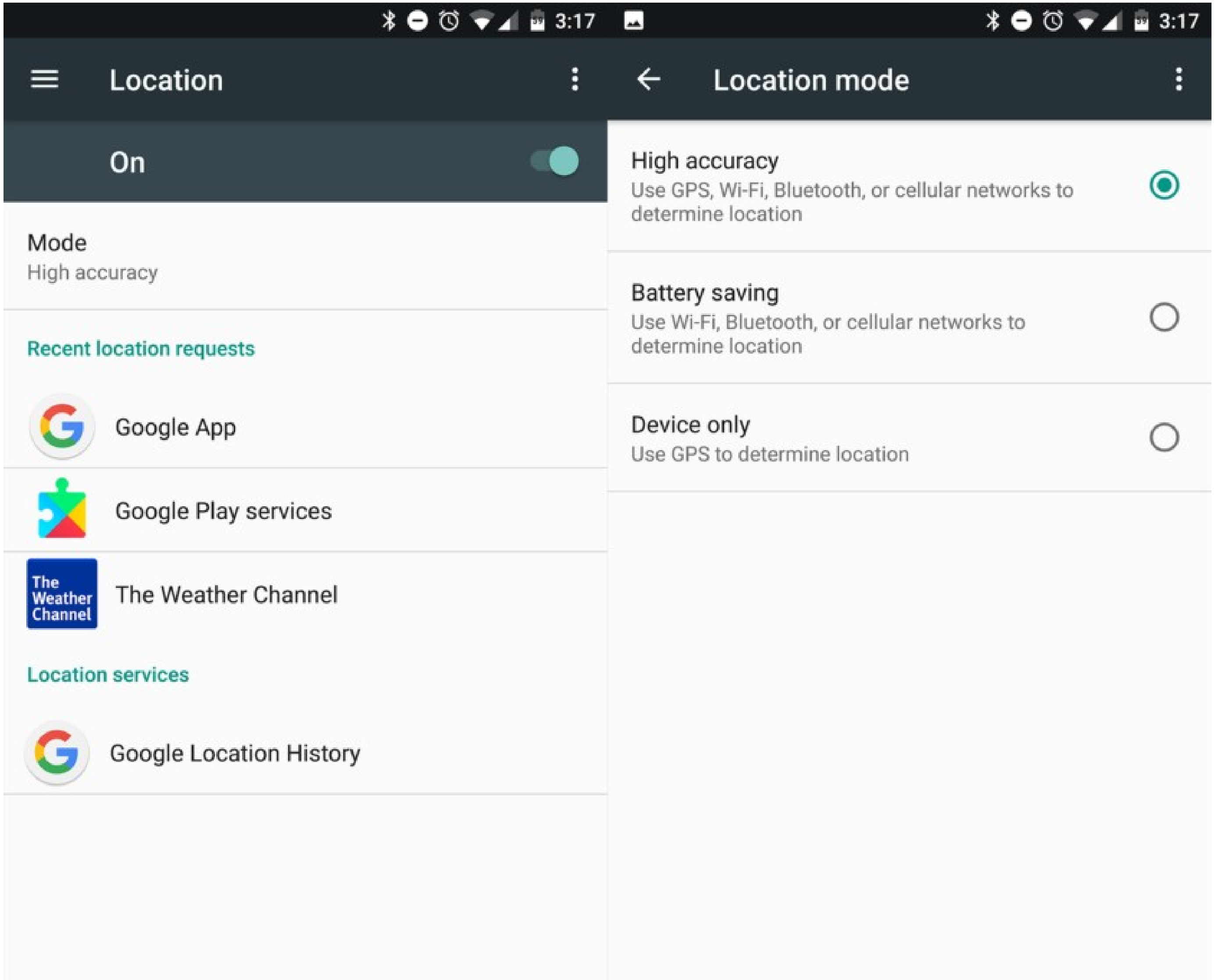


Index of ftp://cddis.gsfc.nasa.gov/gnss/data/daily/2019/

↑ Up to higher level directory

Name	Size	Last Modified	
001		8/16/19	10:20:00 PM GMT+6
002		8/16/19	10:20:00 PM GMT+6
003		8/16/19	11:04:00 AM GMT+6
004		8/16/19	11:04:00 AM GMT+6
005		8/16/19	11:04:00 AM GMT+6
006		8/16/19	11:04:00 AM GMT+6
007		8/16/19	11:04:00 AM GMT+6
008		8/16/19	11:04:00 AM GMT+6
009		8/16/19	11:04:00 AM GMT+6
010		8/16/19	11:04:00 AM GMT+6
011		8/16/19	11:04:00 AM GMT+6
012		8/16/19	11:04:00 AM GMT+6
013		8/16/19	11:04:00 AM GMT+6
014		8/16/19	11:04:00 AM GMT+6
015		8/16/19	11:04:00 AM GMT+6
016		8/16/19	11:04:00 AM GMT+6
017		8/16/19	11:04:00 AM GMT+6
018		8/16/19	11:04:00 AM GMT+6
019		12/10/19	2:00:00 AM GMT+6
020		8/16/19	11:04:00 AM GMT+6
021		9/13/19	5:00:00 AM GMT+6

problems



3:17

Location

On

Mode
High accuracy

Recent location requests

Google App

Google Play services

The Weather Channel

Location services

Google Location History

3:17

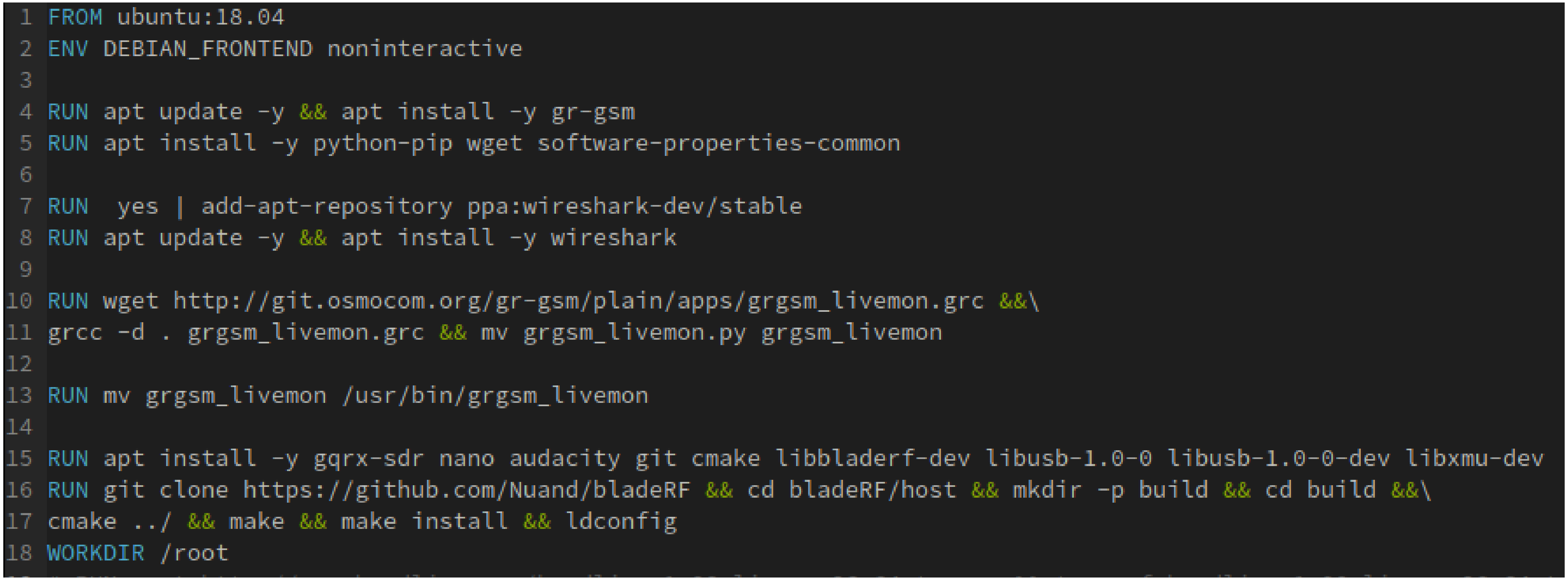
Location mode

● High accuracy
Use GPS, Wi-Fi, Bluetooth, or cellular networks to determine location

○ Battery saving
Use Wi-Fi, Bluetooth, or cellular networks to determine location

○ Device only
Use GPS to determine location

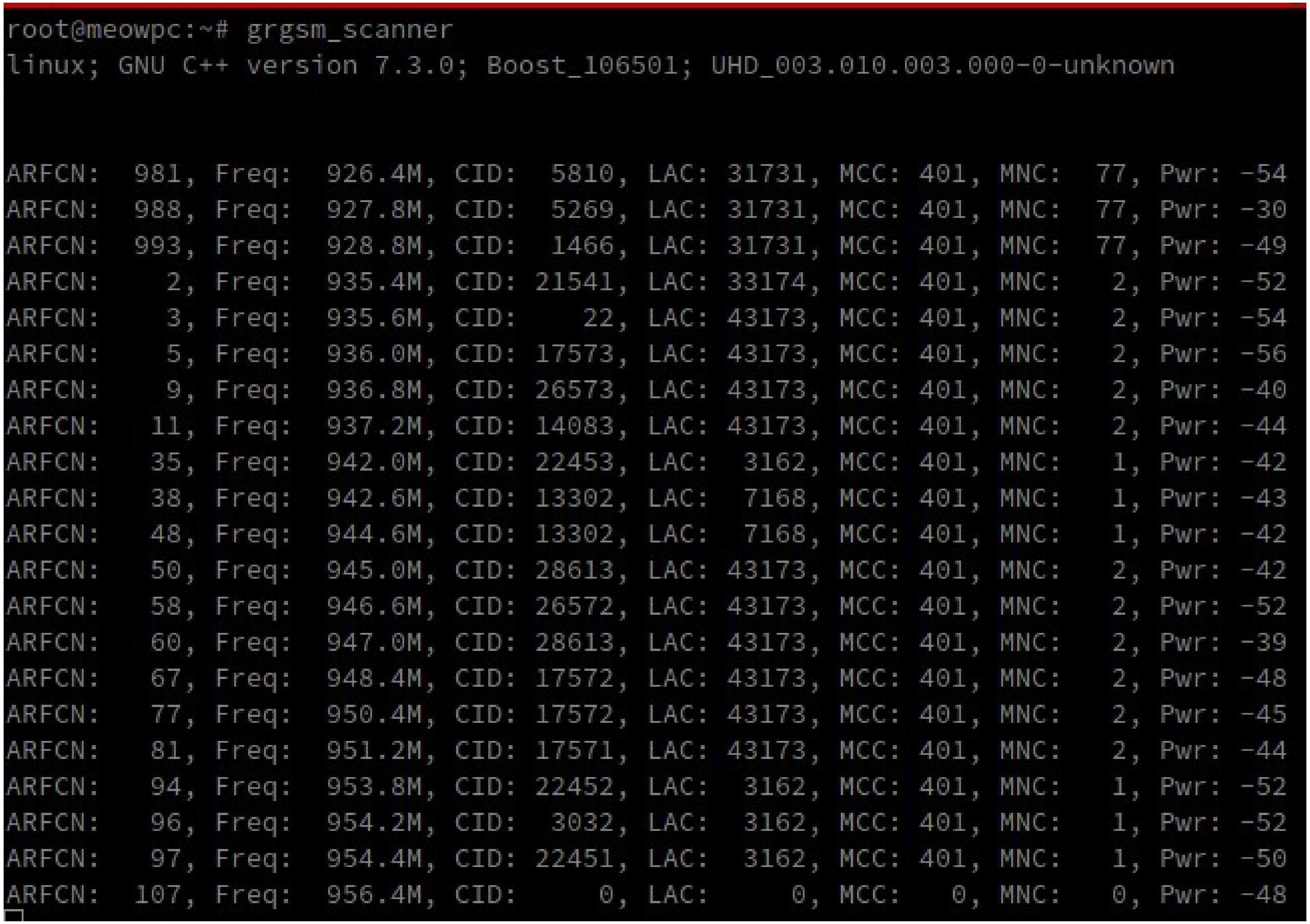
GSM



```
FROM ubuntu:18.04
ENV DEBIAN_FRONTEND noninteractive

RUN apt update -y && apt install -y gr-gsm
RUN apt install -y python-pip wget software-properties-common

RUN  yes | add-apt-repository ppa:wireshark-dev/stable
RUN apt update -y && apt install -y wireshark

RUN wget http://git.osmocom.org/gr-gsm/plain/apps/grgsm_livemon.grc &&\
grcc -d . grgsm_livemon.grc && mv grgsm_livemon.py grgsm_livemon

RUN mv grgsm_livemon /usr/bin/grgsm_livemon

RUN apt install -y gqrx-sdr nano audacity git cmake libbladerf-dev libusb-1.0-0 libusb-1.0-0-dev libxmu-dev
RUN git clone https://github.com/Nuand/bladeRF && cd bladeRF/host && mkdir -p build && cd build &&\
cmake ../ && make && make install && ldconfig
WORKDIR /root
```

gr-gsm: scanning

- > $ grgsm_scanner



```
root@meowpc:~# grgsm_scanner
linux; GNU C++ version 7.3.0; Boost_106501; UHD_003.010.003.000-0-unknown



ARFCN:  981, Freq:  926.4M, CID:  5810, LAC: 31731, MCC: 401, MNC:  77, Pwr: -54
ARFCN:  988, Freq:  927.8M, CID:  5269, LAC: 31731, MCC: 401, MNC:  77, Pwr: -30
ARFCN:  993, Freq:  928.8M, CID:  1466, LAC: 31731, MCC: 401, MNC:  77, Pwr: -49
ARFCN:    2, Freq:  935.4M, CID: 21541, LAC: 33174, MCC: 401, MNC:   2, Pwr: -52
ARFCN:    3, Freq:  935.6M, CID:    22, LAC: 43173, MCC: 401, MNC:   2, Pwr: -54
ARFCN:    5, Freq:  936.0M, CID: 17573, LAC: 43173, MCC: 401, MNC:   2, Pwr: -56
ARFCN:    9, Freq:  936.8M, CID: 26573, LAC: 43173, MCC: 401, MNC:   2, Pwr: -40
ARFCN:   11, Freq:  937.2M, CID: 14083, LAC: 43173, MCC: 401, MNC:   2, Pwr: -44
ARFCN:   35, Freq:  942.0M, CID: 22453, LAC:  3162, MCC: 401, MNC:   1, Pwr: -42
ARFCN:   38, Freq:  942.6M, CID: 13302, LAC:  7168, MCC: 401, MNC:   1, Pwr: -43
ARFCN:   48, Freq:  944.6M, CID: 13302, LAC:  7168, MCC: 401, MNC:   1, Pwr: -42
ARFCN:   50, Freq:  945.0M, CID: 28613, LAC: 43173, MCC: 401, MNC:   2, Pwr: -42
ARFCN:   58, Freq:  946.6M, CID: 26572, LAC: 43173, MCC: 401, MNC:   2, Pwr: -52
ARFCN:   60, Freq:  947.0M, CID: 28613, LAC: 43173, MCC: 401, MNC:   2, Pwr: -39
ARFCN:   67, Freq:  948.4M, CID: 17572, LAC: 43173, MCC: 401, MNC:   2, Pwr: -48
ARFCN:   77, Freq:  950.4M, CID: 17572, LAC: 43173, MCC: 401, MNC:   2, Pwr: -45
ARFCN:   81, Freq:  951.2M, CID: 17571, LAC: 43173, MCC: 401, MNC:   2, Pwr: -44
ARFCN:   94, Freq:  953.8M, CID: 22452, LAC:  3162, MCC: 401, MNC:   1, Pwr: -52
ARFCN:   96, Freq:  954.2M, CID:  3032, LAC:  3162, MCC: 401, MNC:   1, Pwr: -52
ARFCN:   97, Freq:  954.4M, CID: 22451, LAC:  3162, MCC: 401, MNC:   1, Pwr: -50
ARFCN:  107, Freq:  956.4M, CID:     0, LAC:     0, MCC:   0, MNC:   0, Pwr: -48
```

gr-gsm: capture

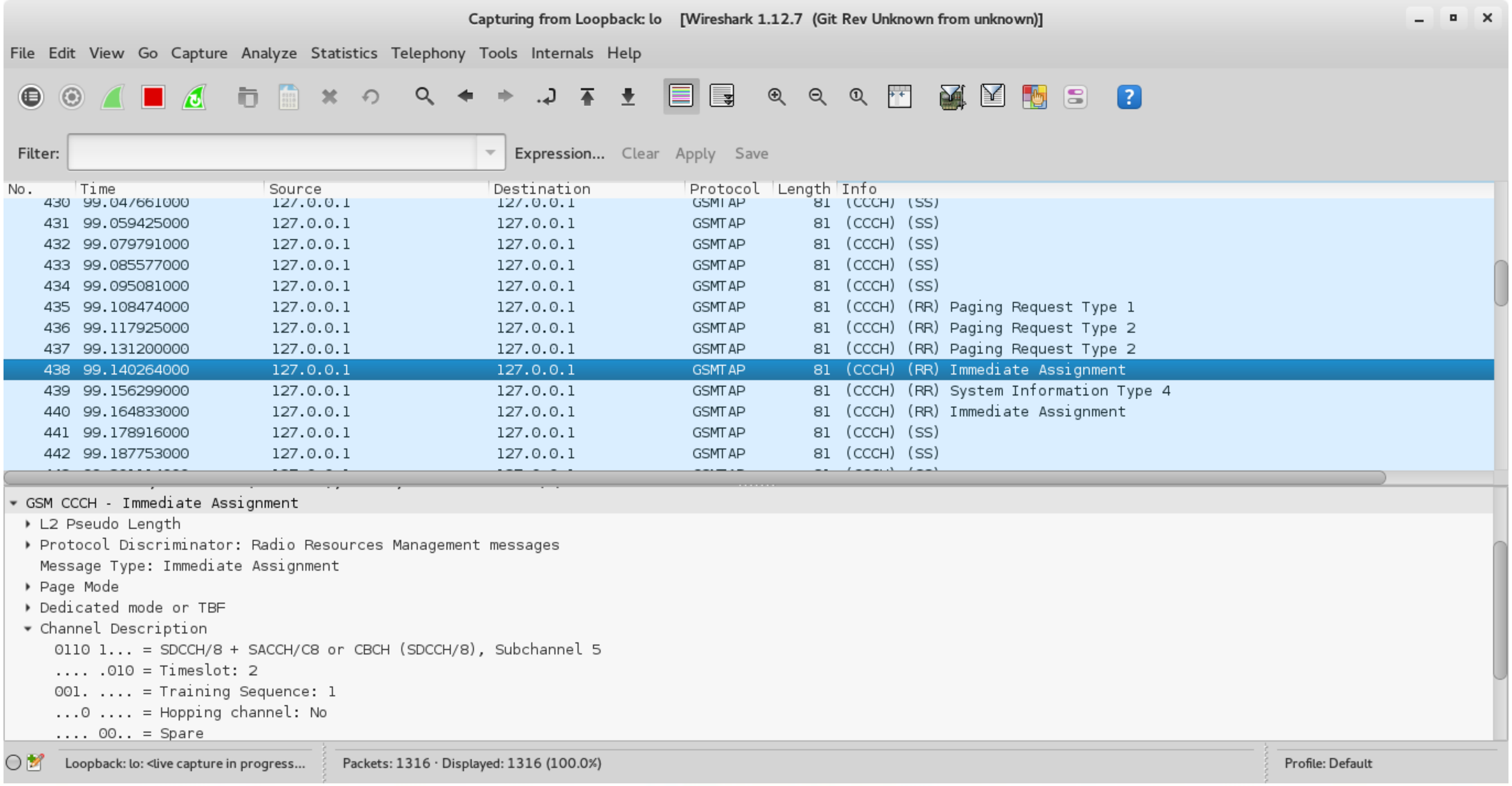
-
  ```
  > $ grgsm_capture -f *downlink_frequency*
  -c capture.cfile -T 60
  ```

gr-gsm:decode

- TMSI - Temporary Mobile Subscriber Identity
- A5 – encoding algorithm
- KC – encryption key

gr-gsm:decode

- > $ grgsm_decode -c capture.cfile -f *downlink_frequency* -m BCCH


Capturing from Loopback: lo [Wireshark 1.12.7 (Git Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.  Time          Source     Destination  Protocol  Length  Info
430  99.047661000  127.0.0.1  127.0.0.1    GSMTAP        81  (CCCH) (SS)
431  99.059425000  127.0.0.1  127.0.0.1    GSMTAP        81  (CCCH) (SS)
432  99.079791000  127.0.0.1  127.0.0.1    GSMTAP        81  (CCCH) (SS)
433  99.085577000  127.0.0.1  127.0.0.1    GSMTAP        81  (CCCH) (SS)
434  99.095081000  127.0.0.1  127.0.0.1    GSMTAP        81  (CCCH) (SS)
435  99.108474000  127.0.0.1  127.0.0.1    GSMTAP        81  (CCCH) (RR) Paging Request Type 1
436  99.117925000  127.0.0.1  127.0.0.1    GSMTAP        81  (CCCH) (RR) Paging Request Type 2
437  99.131200000  127.0.0.1  127.0.0.1    GSMTAP        81  (CCCH) (RR) Paging Request Type 2
438  99.140264000  127.0.0.1  127.0.0.1    GSMTAP        81  (CCCH) (RR) Immediate Assignment
439  99.156299000  127.0.0.1  127.0.0.1    GSMTAP        81  (CCCH) (RR) System Information Type 4
440  99.164833000  127.0.0.1  127.0.0.1    GSMTAP        81  (CCCH) (RR) Immediate Assignment
441  99.178916000  127.0.0.1  127.0.0.1    GSMTAP        81  (CCCH) (SS)
442  99.187753000  127.0.0.1  127.0.0.1    GSMTAP        81  (CCCH) (SS)
```

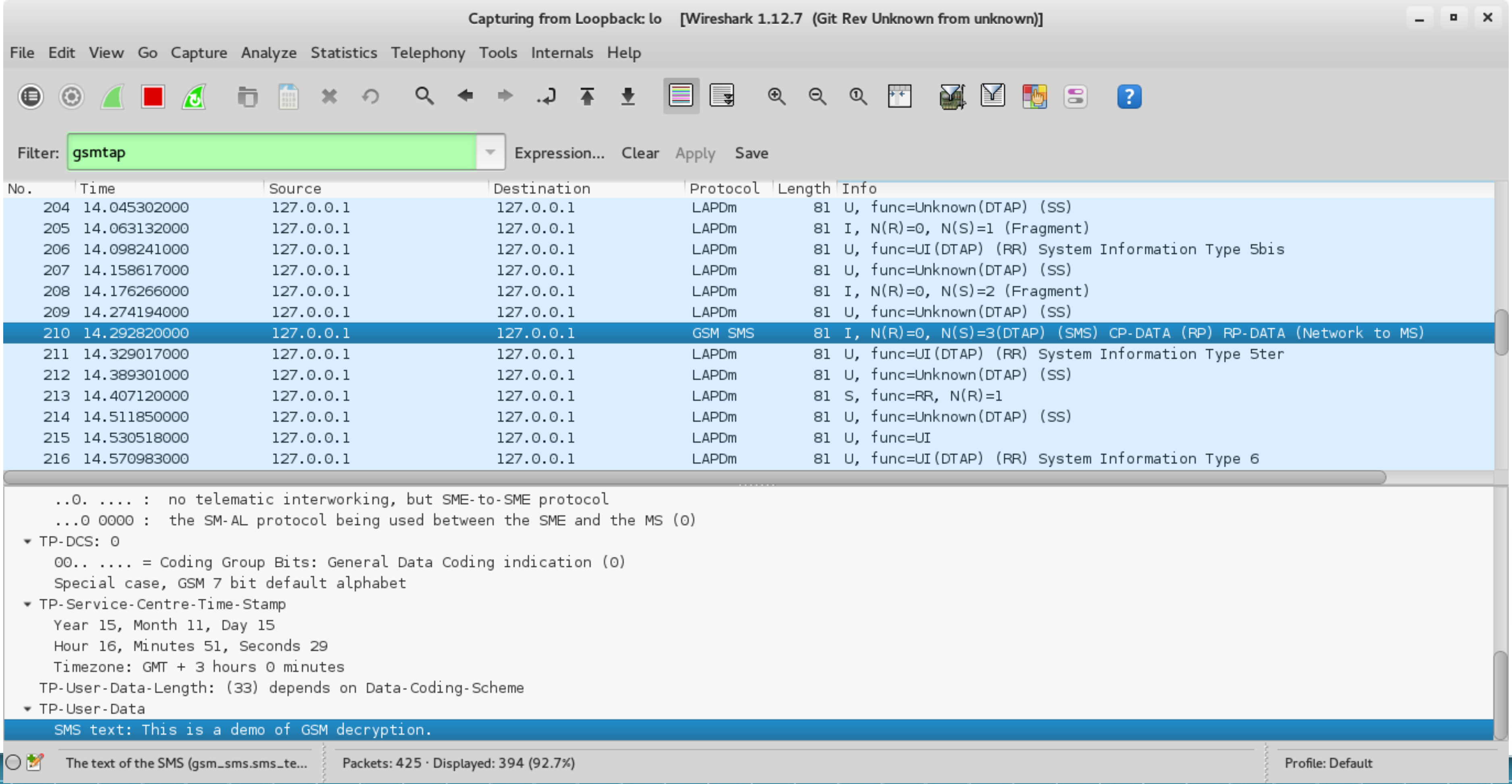
```
▾ GSM CCCH - Immediate Assignment
  ▸ L2 Pseudo Length
  ▸ Protocol Discriminator: Radio Resources Management messages
    Message Type: Immediate Assignment
  ▸ Page Mode
  ▸ Dedicated mode or TBF
  ▾ Channel Description
      0110 1... = SDCCH/8 + SACCH/C8 or CBCH (SDCCH/8), Subchannel 5
      .... .010 = Timeslot: 2
      001. .... = Training Sequence: 1
      ...0 .... = Hopping channel: No
      .... 00.. = Spare
```

Loopback: lo: <live capture in progress... Packets: 1316 · Displayed: 1316 (100.0%) Profile: Default

gr-gsm:decode

- > $ grgsm_decode -c capture.cfile

  -f *downlink_frequency* -m SDCCH8 -t 2


Capturing from Loopback: lo [Wireshark 1.12.7 (Git Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

Filter: gsmtap

```
No.   Time          Source       Destination  Protocol  Length Info
  204 14.045302000  127.0.0.1    127.0.0.1    LAPDm         81 U, func=Unknown(DTAP) (SS)
  205 14.063132000  127.0.0.1    127.0.0.1    LAPDm         81 I, N(R)=0, N(S)=1 (Fragment)
  206 14.098241000  127.0.0.1    127.0.0.1    LAPDm         81 U, func=UI(DTAP) (RR) System Information Type 5bis
  207 14.158617000  127.0.0.1    127.0.0.1    LAPDm         81 U, func=Unknown(DTAP) (SS)
  208 14.176266000  127.0.0.1    127.0.0.1    LAPDm         81 I, N(R)=0, N(S)=2 (Fragment)
  209 14.274194000  127.0.0.1    127.0.0.1    LAPDm         81 U, func=Unknown(DTAP) (SS)
  210 14.292820000  127.0.0.1    127.0.0.1    GSM SMS       81 I, N(R)=0, N(S)=3(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
  211 14.329017000  127.0.0.1    127.0.0.1    LAPDm         81 U, func=UI(DTAP) (RR) System Information Type 5ter
  212 14.389301000  127.0.0.1    127.0.0.1    LAPDm         81 U, func=Unknown(DTAP) (SS)
  213 14.407120000  127.0.0.1    127.0.0.1    LAPDm         81 S, func=RR, N(R)=1
  214 14.511850000  127.0.0.1    127.0.0.1    LAPDm         81 U, func=Unknown(DTAP) (SS)
  215 14.530518000  127.0.0.1    127.0.0.1    LAPDm         81 U, func=UI
  216 14.570983000  127.0.0.1    127.0.0.1    LAPDm         81 U, func=UI(DTAP) (RR) System Information Type 6
```

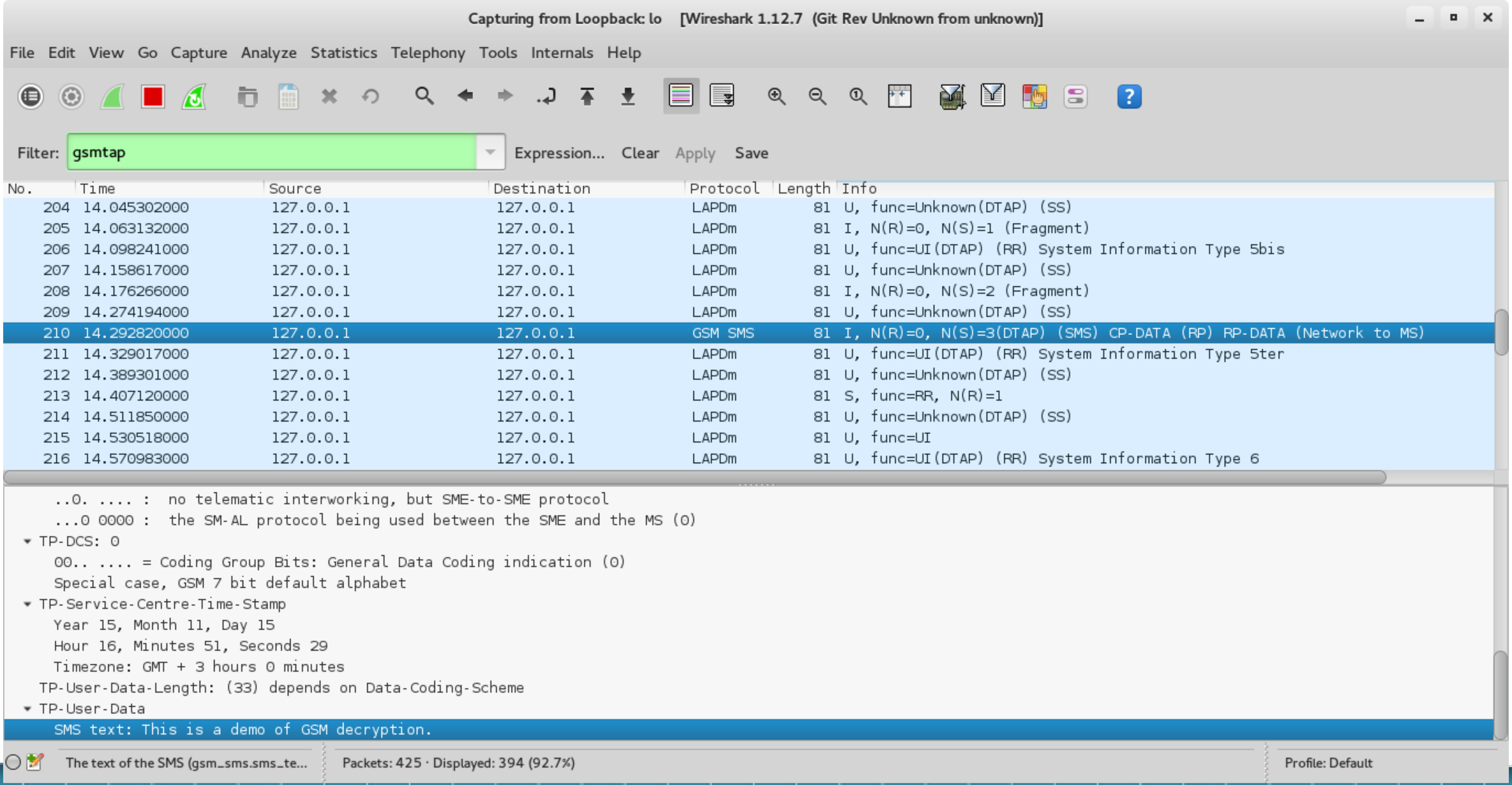
```
    ..0. .... :  no telematic interworking, but SME-to-SME protocol
    ...0 0000 :  the SM-AL protocol being used between the SME and the MS (0)
  ▾ TP-DCS: 0
    00.. .... = Coding Group Bits: General Data Coding indication (0)
    Special case, GSM 7 bit default alphabet
  ▾ TP-Service-Centre-Time-Stamp
    Year 15, Month 11, Day 15
    Hour 16, Minutes 51, Seconds 29
    Timezone: GMT + 3 hours 0 minutes
  TP-User-Data-Length: (33) depends on Data-Coding-Scheme
  ▾ TP-User-Data
    SMS text: This is a demo of GSM decryption.
```

The text of the SMS (gsm_sms.sms_te... Packets: 425 · Displayed: 394 (92.7%) Profile: Default

gr-gsm:decode

- > $ grgsm_decode -c capture.cfile

  -f *downlink_frequency* -m SDCCH8 -t 2 -e 1 -k 0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00


Capturing from Loopback: lo [Wireshark 1.12.7 (Git Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: gsmtap

```
No.   Time               Source          Destination     Protocol  Length Info
  204 14.045302000       127.0.0.1       127.0.0.1       LAPDm         81 U, func=Unknown(DTAP) (SS)
  205 14.063132000       127.0.0.1       127.0.0.1       LAPDm         81 I, N(R)=0, N(S)=1 (Fragment)
  206 14.098241000       127.0.0.1       127.0.0.1       LAPDm         81 U, func=UI(DTAP) (RR) System Information Type 5bis
  207 14.158617000       127.0.0.1       127.0.0.1       LAPDm         81 U, func=Unknown(DTAP) (SS)
  208 14.176266000       127.0.0.1       127.0.0.1       LAPDm         81 I, N(R)=0, N(S)=2 (Fragment)
  209 14.274194000       127.0.0.1       127.0.0.1       LAPDm         81 U, func=Unknown(DTAP) (SS)
  210 14.292820000       127.0.0.1       127.0.0.1       GSM SMS       81 I, N(R)=0, N(S)=3(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)
  211 14.329017000       127.0.0.1       127.0.0.1       LAPDm         81 U, func=UI(DTAP) (RR) System Information Type 5ter
  212 14.389301000       127.0.0.1       127.0.0.1       LAPDm         81 U, func=Unknown(DTAP) (SS)
  213 14.407120000       127.0.0.1       127.0.0.1       LAPDm         81 S, func=RR, N(R)=1
  214 14.511850000       127.0.0.1       127.0.0.1       LAPDm         81 U, func=Unknown(DTAP) (SS)
  215 14.530518000       127.0.0.1       127.0.0.1       LAPDm         81 U, func=UI
  216 14.570983000       127.0.0.1       127.0.0.1       LAPDm         81 U, func=UI(DTAP) (RR) System Information Type 6
```

```
    ..0. .... :  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: 0
    00.. .... = Coding Group Bits: General Data Coding indication (0)
    Special case, GSM 7 bit default alphabet
  ▾ TP-Service-Centre-Time-Stamp
    Year 15, Month 11, Day 15
    Hour 16, Minutes 51, Seconds 29
    Timezone: GMT + 3 hours 0 minutes
  TP-User-Data-Length: (33) depends on Data-Coding-Scheme
  ▾ TP-User-Data
    SMS text: This is a demo of GSM decryption.
```

The text of the SMS (gsm_sms.sms_te... Packets: 425 · Displayed: 394 (92.7%) Profile: Default

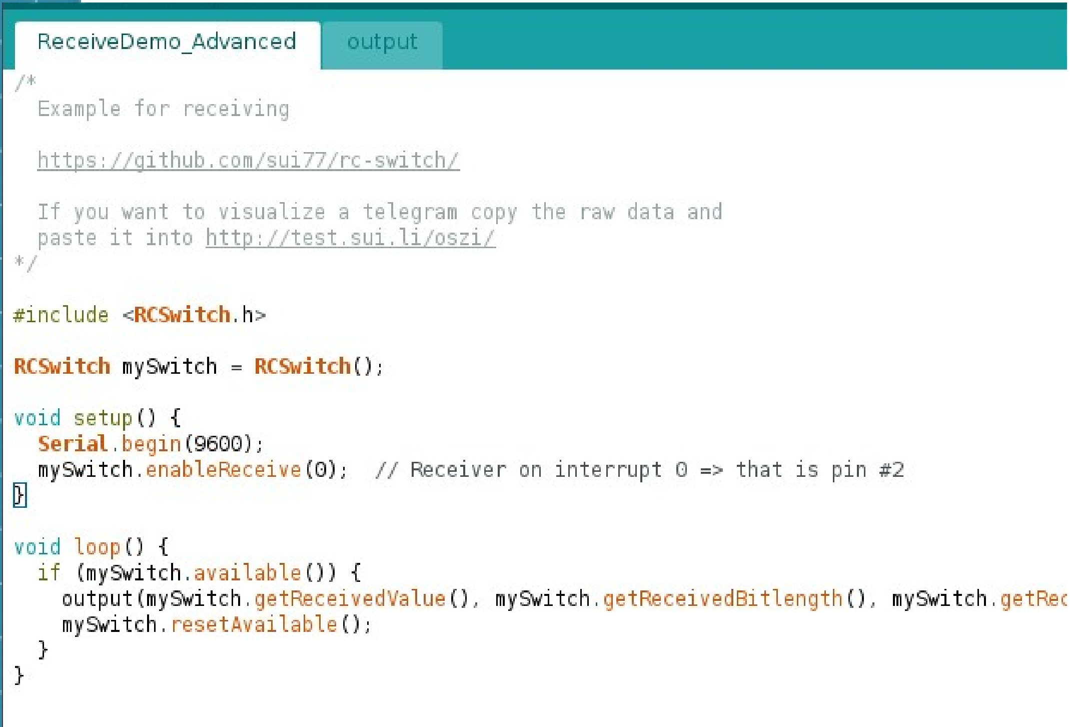
problems

- GSM in 2k19 :/
- KC
- Bruteforce with Kraken (2TB rainbow tables)

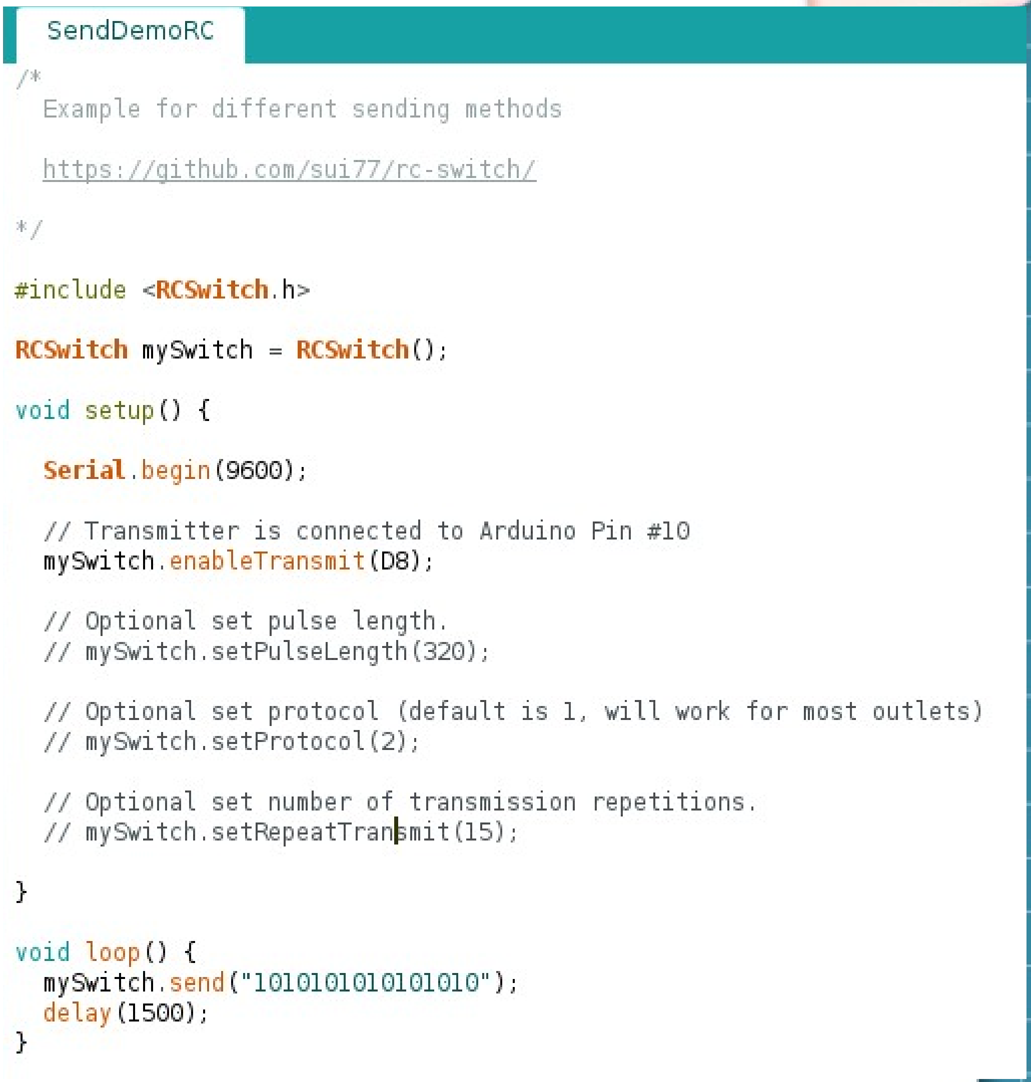
rf433

- how about doing something yourself?

Arduino code

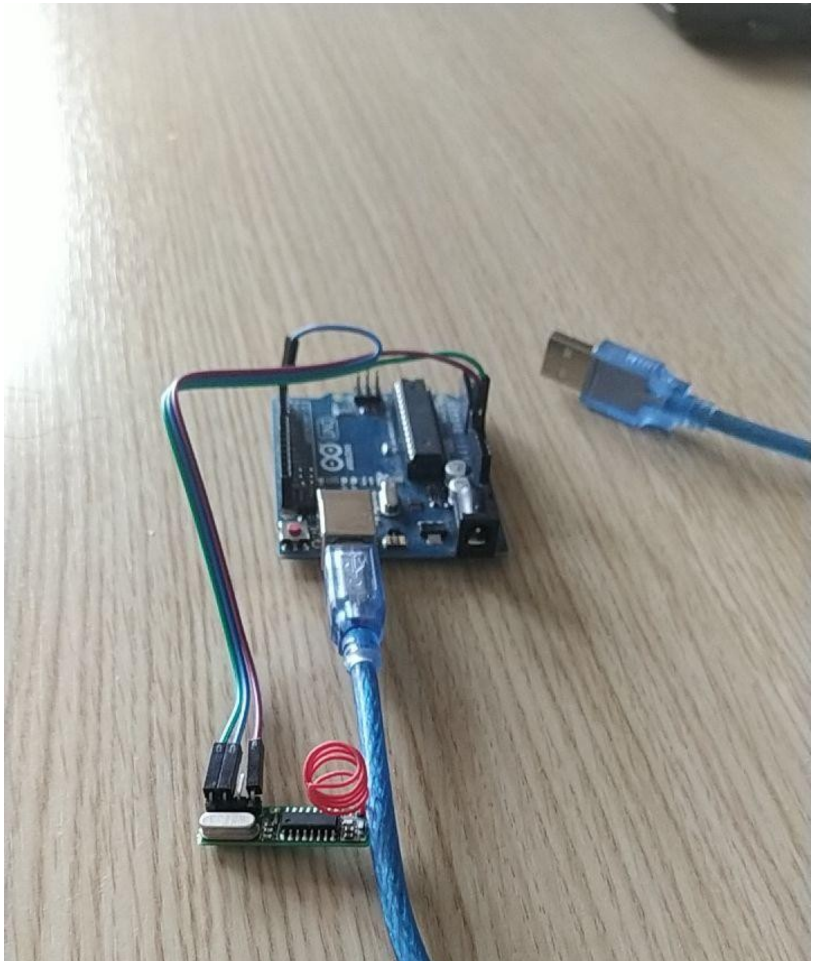


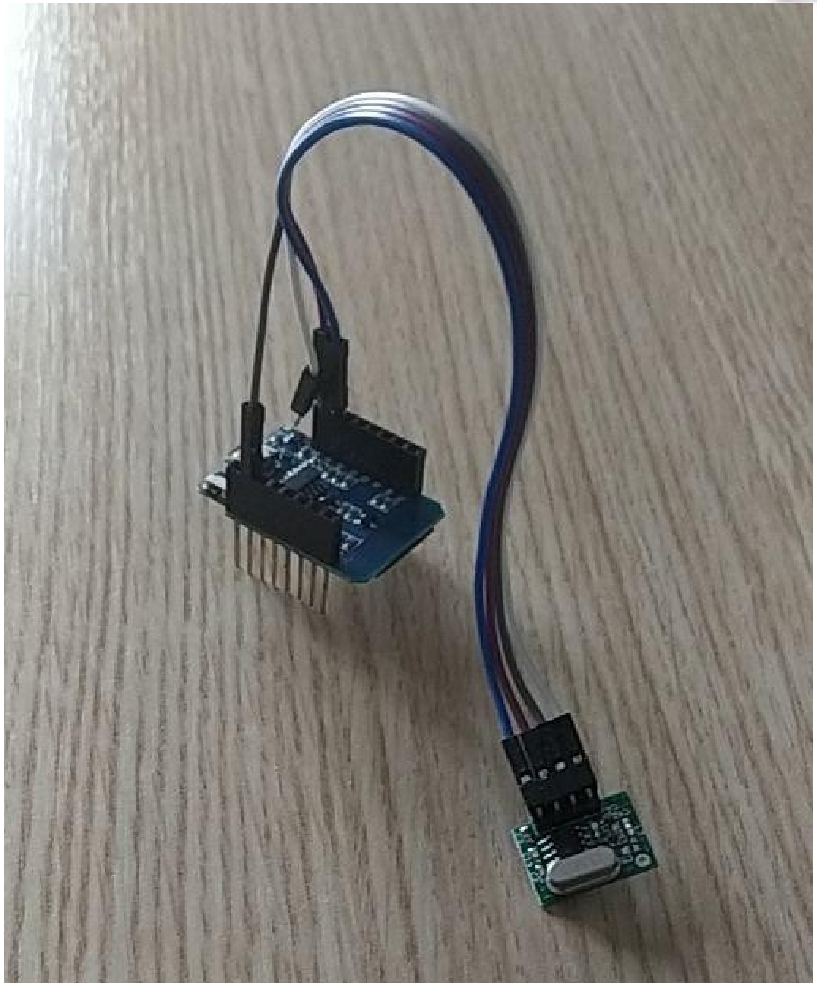
```
/*
  Example for receiving

  https://github.com/sui77/rc-switch/

  If you want to visualize a telegram copy the raw data and
  paste it into http://test.sui.li/oszi/
*/

#include <RCSwitch.h>

RCSwitch mySwitch = RCSwitch();

void setup() {
  Serial.begin(9600);
  mySwitch.enableReceive(0);  // Receiver on interrupt 0 => that is pin #2
}

void loop() {
  if (mySwitch.available()) {
    output(mySwitch.getReceivedValue(), mySwitch.getReceivedBitlength(), mySwitch.getRec
    mySwitch.resetAvailable();
  }
}
```



```
/*
  Example for different sending methods

  https://github.com/sui77/rc-switch/

*/

#include <RCSwitch.h>

RCSwitch mySwitch = RCSwitch();

void setup() {

  Serial.begin(9600);

  // Transmitter is connected to Arduino Pin #10
  mySwitch.enableTransmit(D8);

  // Optional set pulse length.
  // mySwitch.setPulseLength(320);

  // Optional set protocol (default is 1, will work for most outlets)
  // mySwitch.setProtocol(2);

  // Optional set number of transmission repetitions.
  // mySwitch.setRepeatTransmit(15);

}

void loop() {
  mySwitch.send("1010101010101010");
  delay(1500);
}
```

Arduino setup

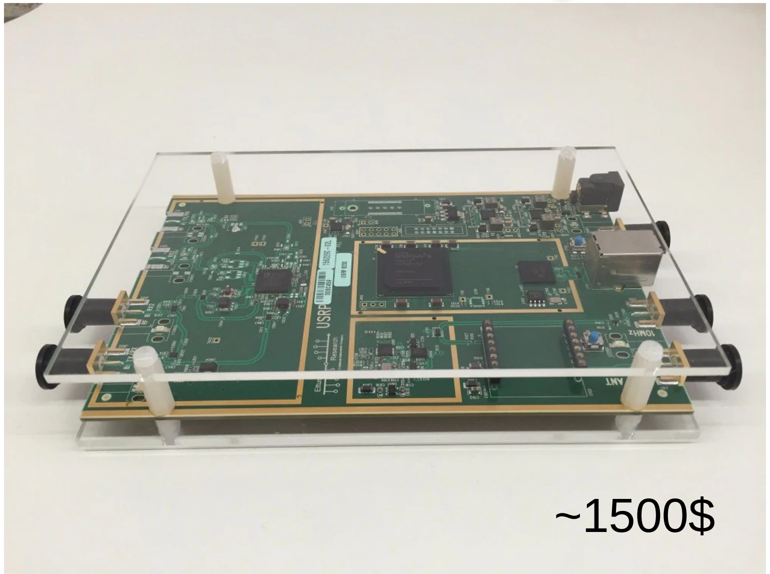




what to choose?

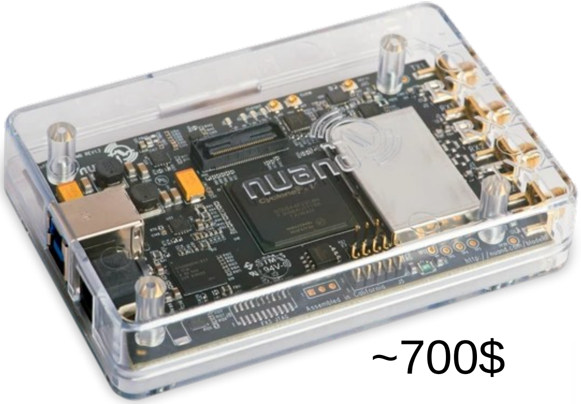
RTL-SDR.COM
QUICKSTART SETUP GUIDE: RTL-SDR.COM/QSG
DVB-T+DAB+FM+SDR
RTL2832U R820T2 TCXO+BIAS T+HF

~20$



~1500$

~300$



~700$

Materials

- https://github.com/Nuand/gps-sdr-sim
- https://github.com/osqzss/gps-sdr-sim
- https://osmocom.org/projects/gr-gsm/wiki/Installation
- https://www.ckn.io/blog/2015/11/29/gsm-sniffing-sms-traffic/
- https://www.youtube.com/channel/UClg0eyJTbAZaYuz3mhwfBBQ/featured

  (Crazy Danish Hacker youtube channel)
- https://zeta-two.com/radio/2015/06/23/ook-ask-sdr.html
- https://nccgroup.github.io/RFTM/fsk_receiver.html
- https://calebmadrigal.com/editing-radio-signals-with-audacity/

QUESTIONS?