Softwarově definované rádio

Jan Hrach

http://jenda.hrach.eu/
CD98 5440 4372 0C6D 164D A24D F019 2F8E 6527 282E

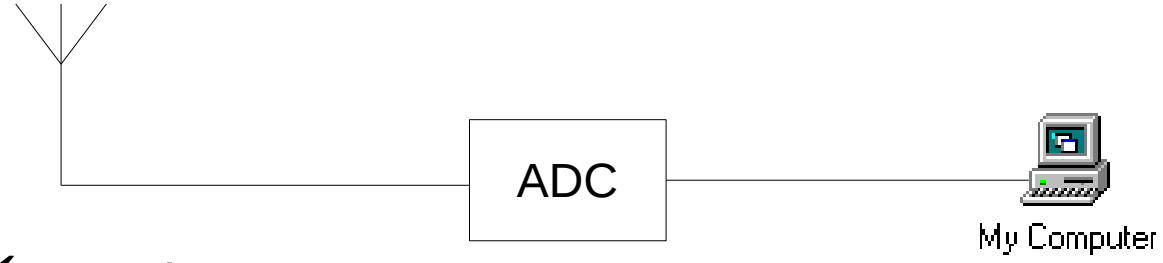
Tahejte: http://jenda.hrach.eu/f2/sdr-linuxdays-2014.pdf

URL

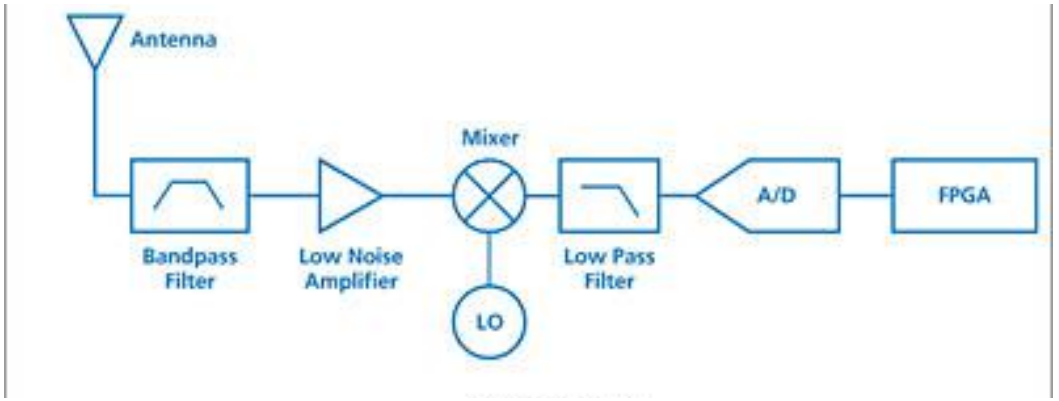
- Slidy: http://jenda.hrach.eu/f2/sdr-linuxdays-2014.pdf
- Podobná přednáška, zaměřená víc na dekódování a bezpečnost: http://nat.brmlab.cz/talks/2014-09-13-postavte-si-vlastni-nsa.mkv

SDR?

- Ideál:



- Skutečnost:

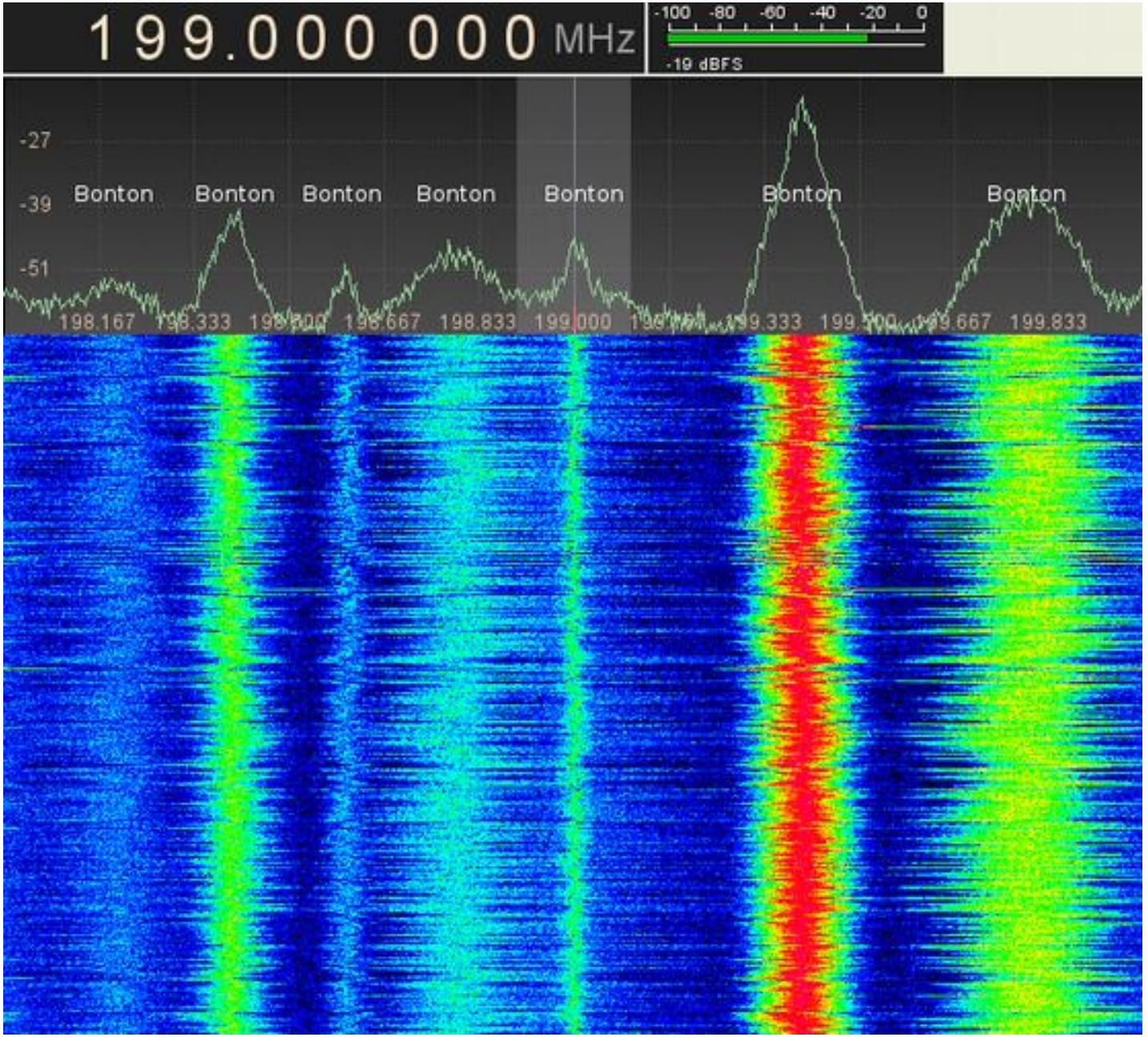


zdroj: http://urgentcomm.com/cognitivesoftware-defined-radio/software-defined-radio-simply-better-way-do-radio

Hardware

- rtl-sdr (200 Kč)

- 2 MHz, 48 dB, RFI/IMP


199.000 000 MHz
-100 -80 -60 -40 -20 0
-19 dBFS
-27
-39
-51
Bonton
Bonton
Bonton
Bonton
Bonton
Bonton
Bonton
198.167
198.333
198.667
198.833
199.000
199.333
199.667
199.833

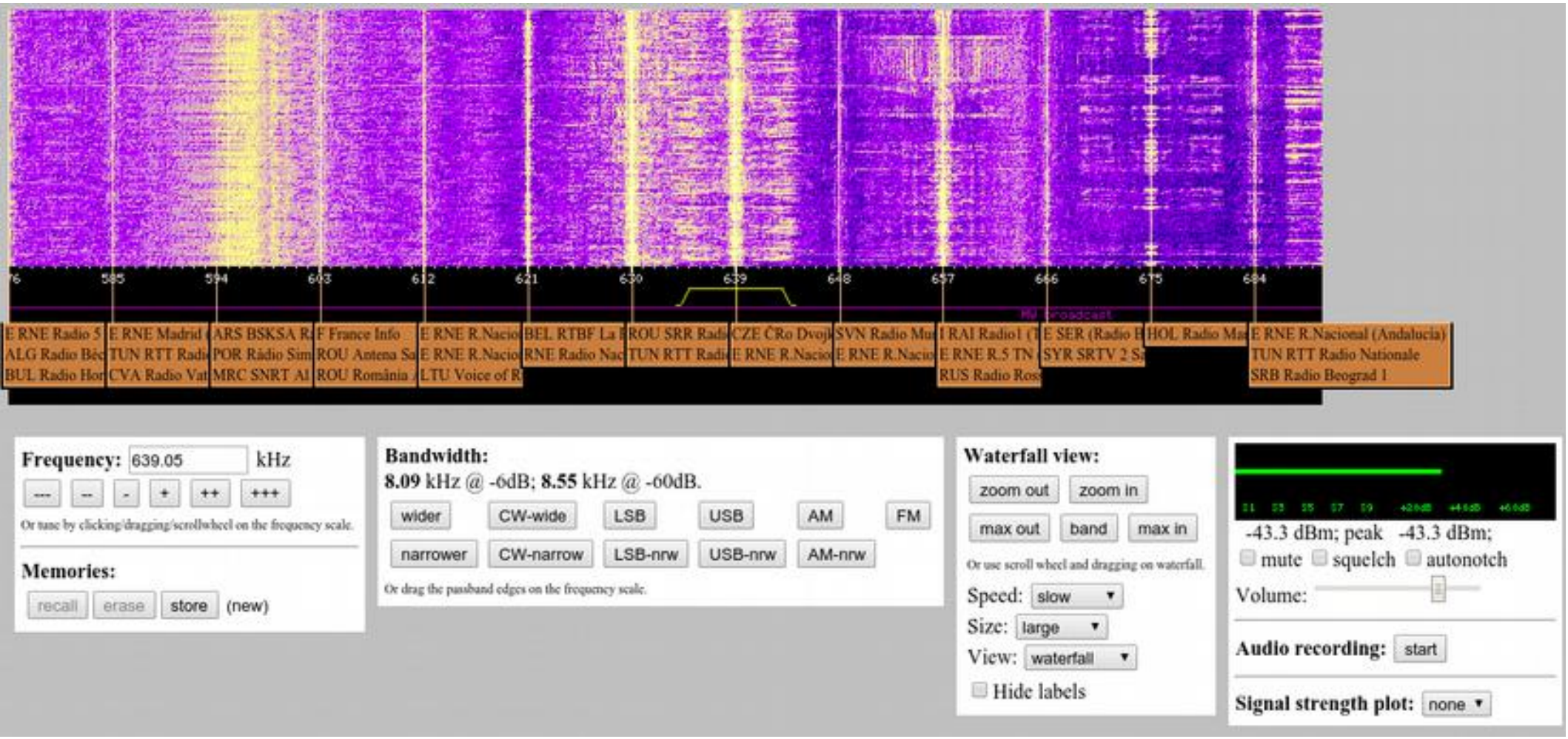
Hardware

- rtl-sdr + filtr + alobal (500 Kč)

tip: kalibrate rtl

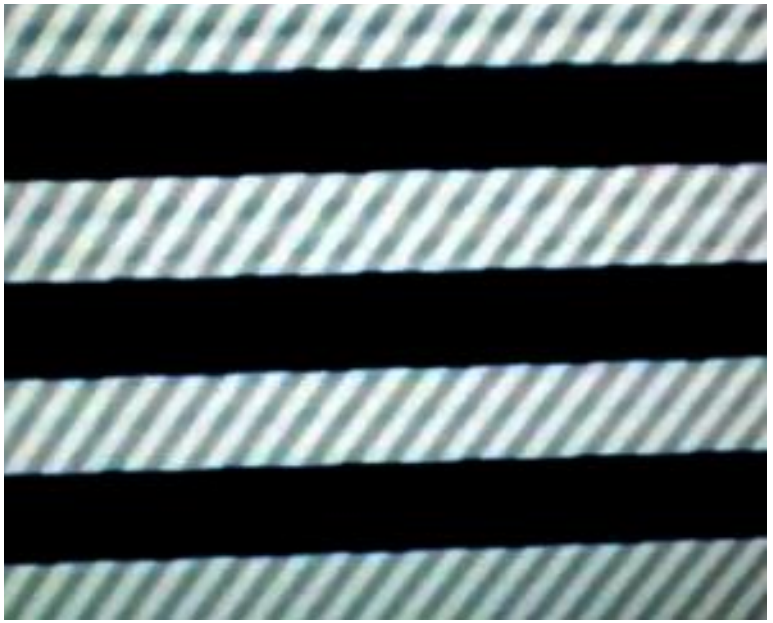
WebSDR

- Např. http://websdr.ewi.utwente.nl:8901/



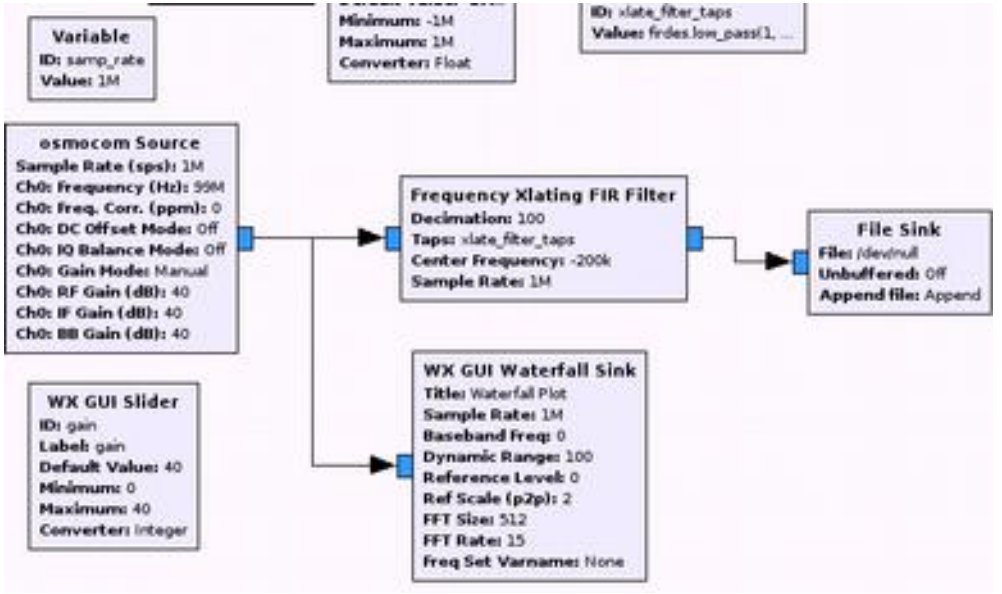
Hardware

- TX: bladeRF (10000 Kč), RaspberryPi, GPU (https://www.brmlab.cz/project/gctx)



Software

- GQRX (demo)
- GnuRadio
  - „funkční bloky“
  - klikátor, Python, C++
  - nekompatibilní samo se sebou
  - zítra workshop
- software obecně nic moc



Co přijímat

- FM hlas
  - 150-180, 440-480 MHz
  - taxi, messengeři
  - ochranky
  - zásahovka…
  - metro (https://www.brmlab.cz/project/metro)
  - bezdrátové mikrofony (670-800 MHz) - konference…
  - chůvičky (stále zapnuté)
  - hobby, HAM
  - SW: rtl_fm, gqrx, https://www.brmlab.cz/project/sdr/szdc

Meteosondy

- http://www.radiosonda.sk/
- https://www.brmlab.cz/project/weathersonde/start

GSM

- Airprobe, OsmocomBB
- nešifrovaná preambule (IMSI!), pak šifrováno
- šifra A5/1, zlomena
  - SMS cracknutelné, hovory obtížně
  - (https://www.brmlab.cz/project/gsm/deka)
  - https://brmlab.cz/event/codenight
- 3G → A5/3
- GSM-R

Tetra

- “GSM pro průmysl”
- Městská policie, DPP, krizový štáb…
  - spousta komunikace o ničem
  - má to skupiny, ale je to všelijaké
- Šifrování: módy 0-3, většina sítí mód 0
- Software: Osmo-tetra
  - gr3.6 (http://jenda.hrach.eu/brm/rad/tetra-3.6-3.7.patch)
  - Dekóduje rámce, je potřeba přidat dumpování provozu…
  - …a pustit na to referenční kodek
  - lze chytat celá síť paralelně (vyrobí roky audia)
- V uplinku polohy, obtížná synchronizace

Mototrbo/DMR

- DMR: standard podobný Tetře
- Mototrbo: proprietární rozšížení od Motoroly
- Software: DMRDecode, dsd
- Šifrování:
  - None
  - Basic (8-bit key + 16-bit LFSR)
  - Enhanced (40-bit RC-4, IV in LSBs, unknown)
  - 2014 AES-256 update
- Městská policie, průmysl, ČEZ

Tetrapol/Matra

- Další trunková síť
- Policie, armáda
- Šifrování: částečné, neznámé
- Software: žádný
- Specifikace (bez šifrování) volně dostupná

Paging

- Software: multimon-ng
- Záchanky – info typu
  - “Bubenská 1, úraz elektickým proudem”
  - “Bubenská 1, nemoc z ozáření”

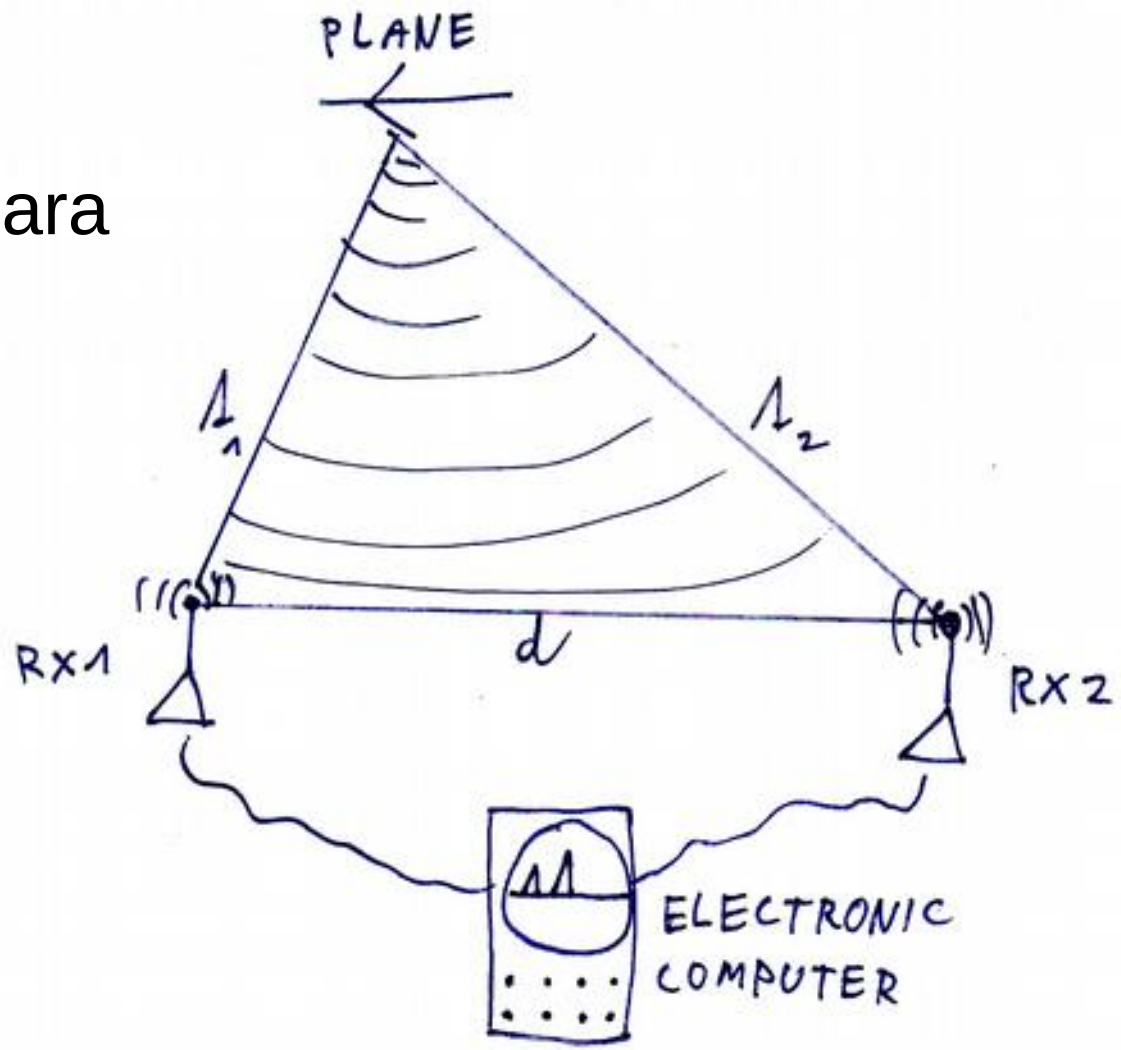
Letadýlka

- ACARS, ADS-B
- Software: acarsdec, dump1090
- Aplikace: http://www.flightradar24.com/
- Mají hezké multilateration
- Jde to vysílat…

- (zbyl čas? pasivní radar →)

Planes

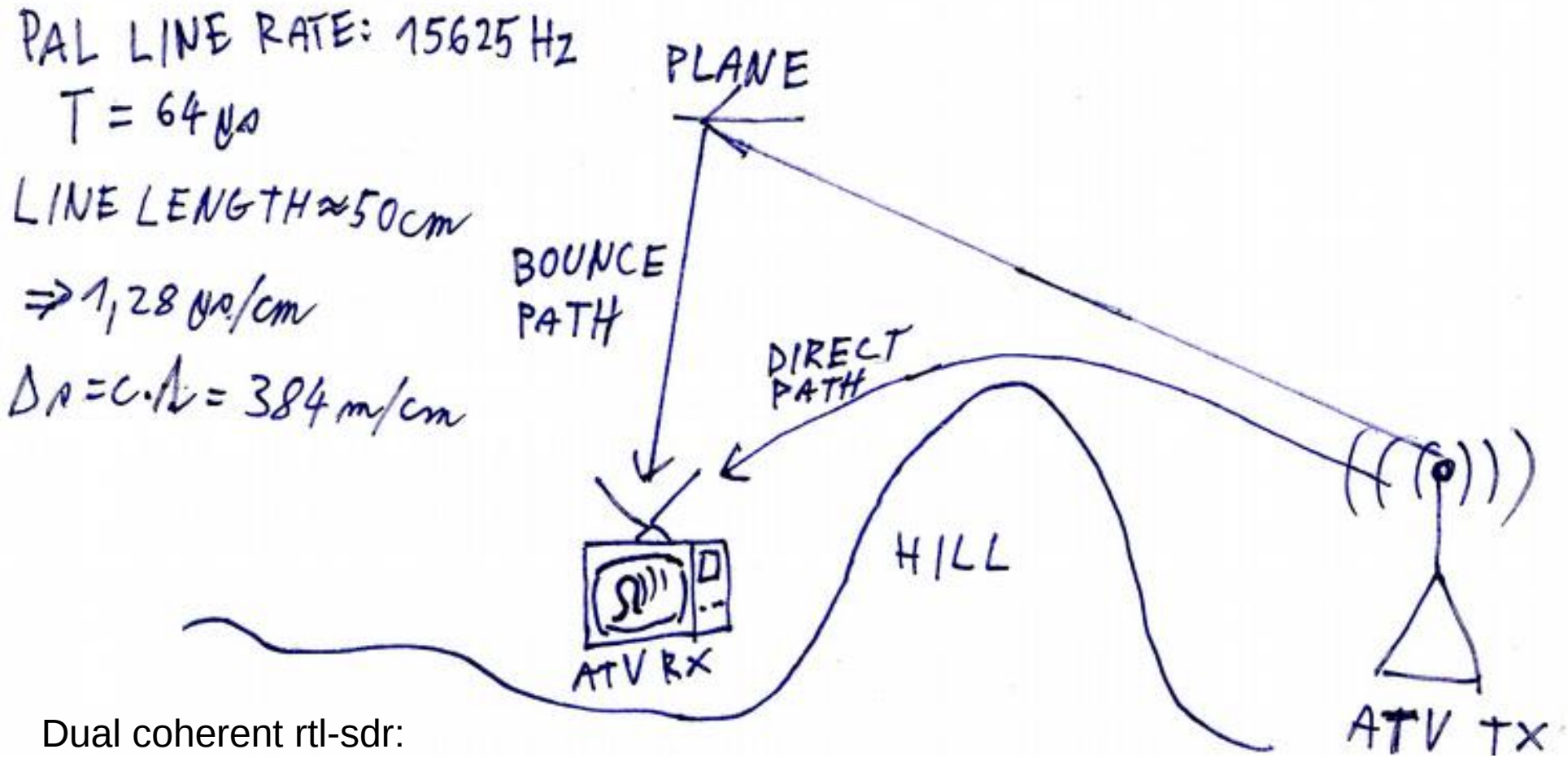
- Active-passive:
  - Kopáč/Ramona/Tamara
  - Flightradar24 MLAT



ATV signal ghosting

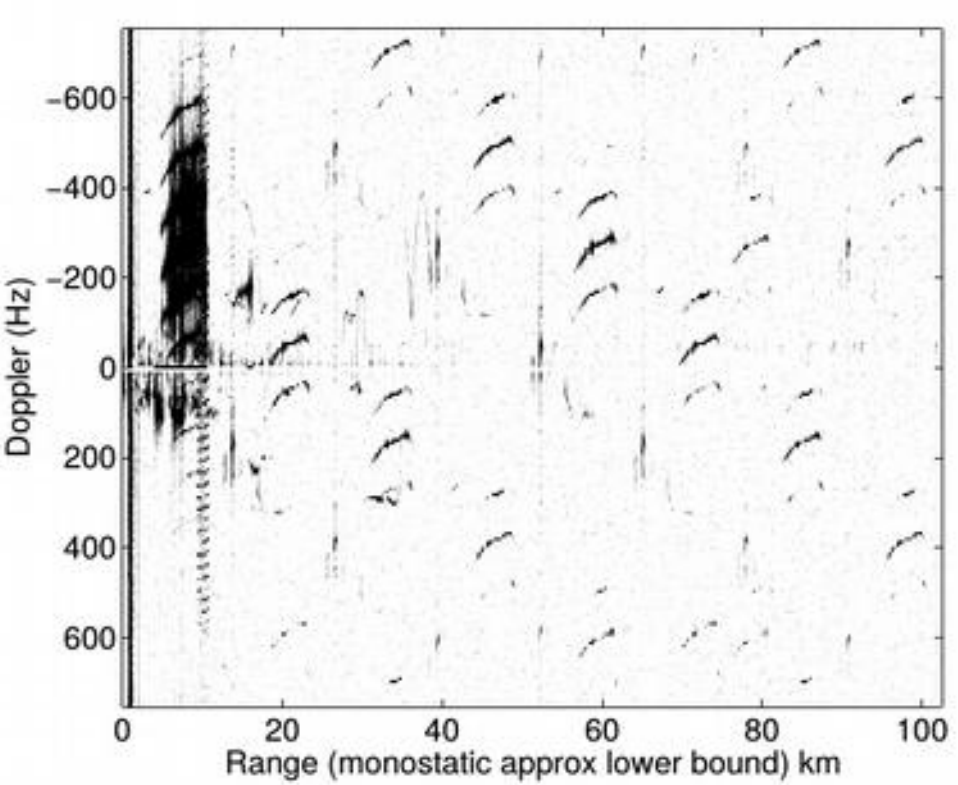
source: http://www.rsm.govt.nz/cms/consumers/reception-problems/what-does-interference-look-like

- Fully passive
  - VERA (Věra)
  - http://people.duke.edu/~hah16/papers/passive-radar-processing-preprint.pdf
    - Anyone knows the math for this^?



Dual coherent rtl-sdr:
https://www.youtube.com/watch?v=KRqtqtCVRR0

http://www.armadninoviny.cz/cesky-tichy-strazce-vidi-i-neviditelna-letadla-.html
http://clanekvera.sweb.cz/



ASMKS

- ASMKS (Automatic system for frequency spectrum monitoring) by ČTÚ
- Coherent scanners + MLAT
- DYI: SDR + GPS, SDR + FM?
- Anyone?

EOF

- kthxbye