RF Shadow Plays

Sébastien Dudek

Cyber-ØxOPOSⱭC M¢¢tuP, Avril 22th 2020

Pent Hertz

Who am I

- Sébastien Dudek (@FlUxIuS)
- Founded PentHertz: RF and hardware security company
  - Pentests and Red Team tests
  - Researches
  - Trainings
  - HW & SW tools
- Interests: SDR, Hardware, RFID, Wi-Fi, 2G/3G/4G/5G, Bluetooth, LoRa, mobile networks, etc.

PentHertz

Radio Frequency

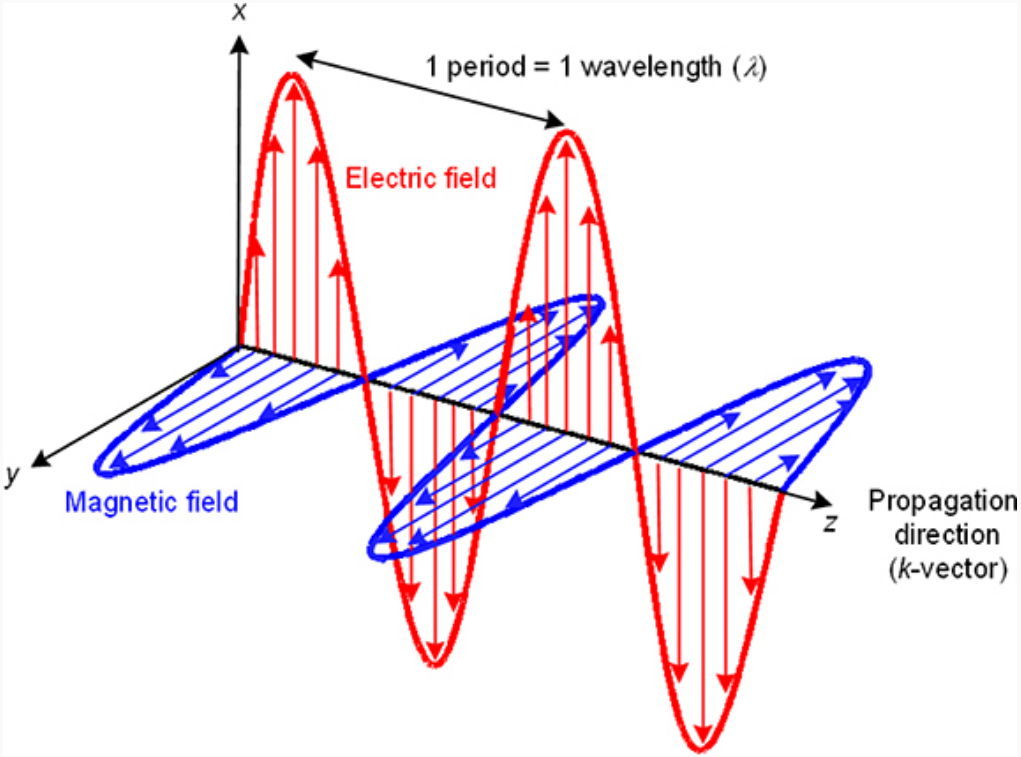
Short introduction

- As a long story (1887, Heinrich Rudolf Hertz generating and detecting radio waves... until these days)
- Used in WWII $\rightarrow$ radar, radio navigation, jamming, talkie walkie, etc
- And then: wireless television, mobile phones, satellite links, access controls systems, etc.
- Today $\rightarrow$ numeric thanks to DSP (Digital Signal Processing)
- Emission and reception $\rightarrow$ regulations of your country $\rightarrow$ better to have your license

Radio wave characteristics

Important:

- λ: wavelength in meter
- c: celerity of light (3.10^8 m.s^{-1})
- T: period in seconds ($\frac{\lambda}{c}$)
- f: frequency in Hz ($\frac{1}{T}$)

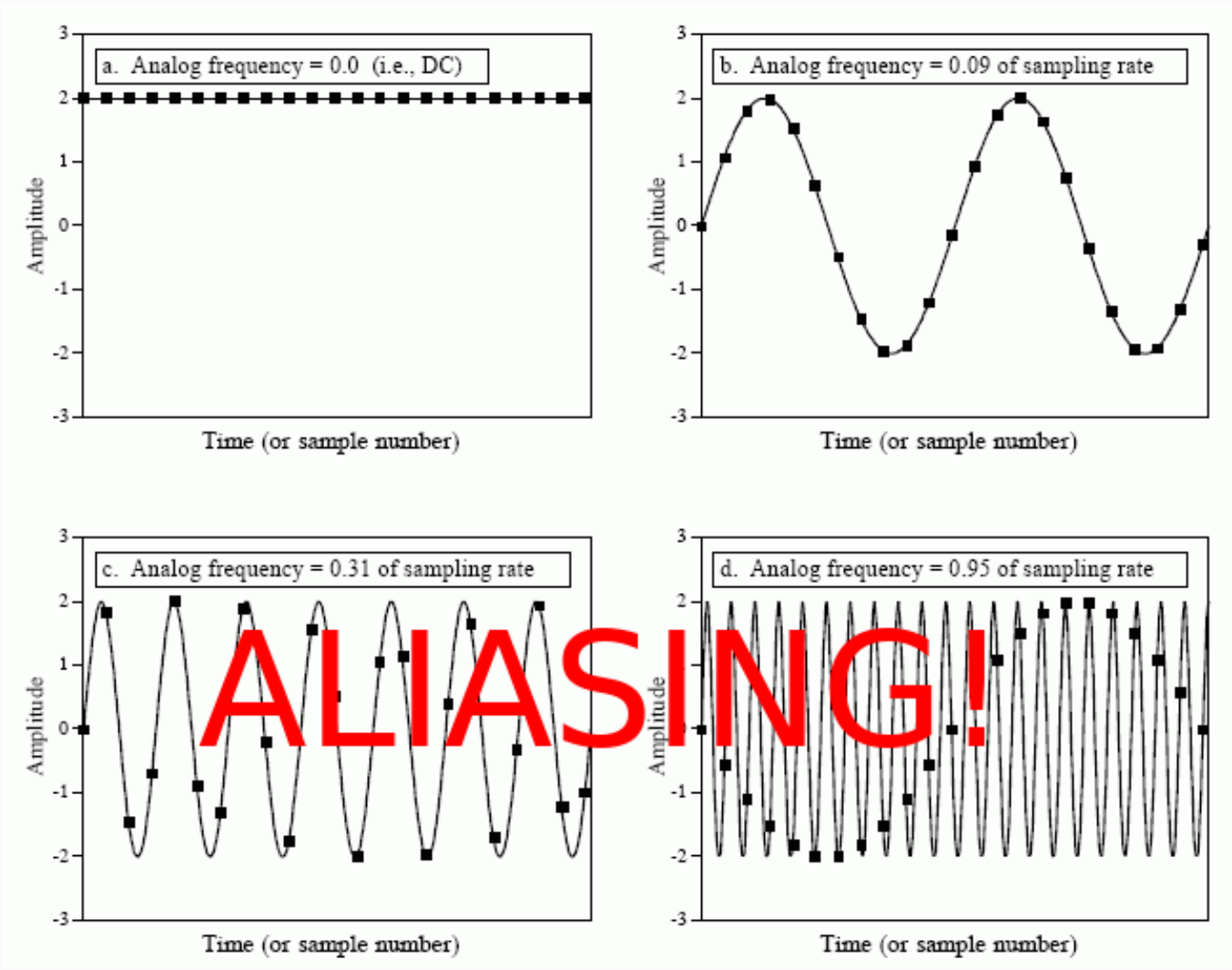


Source: iopscience.com

Process a signal

- Represent it in the time domain
- 2 main steps:
  - Sampling: transform a continuous signal $\rightarrow$ discrete-time signal
  - Quantization: yield a value-discrete binary number $\rightarrow$ generally 32-bit floating number (between “-1.0” and “1”)

Nyquist/Shannon

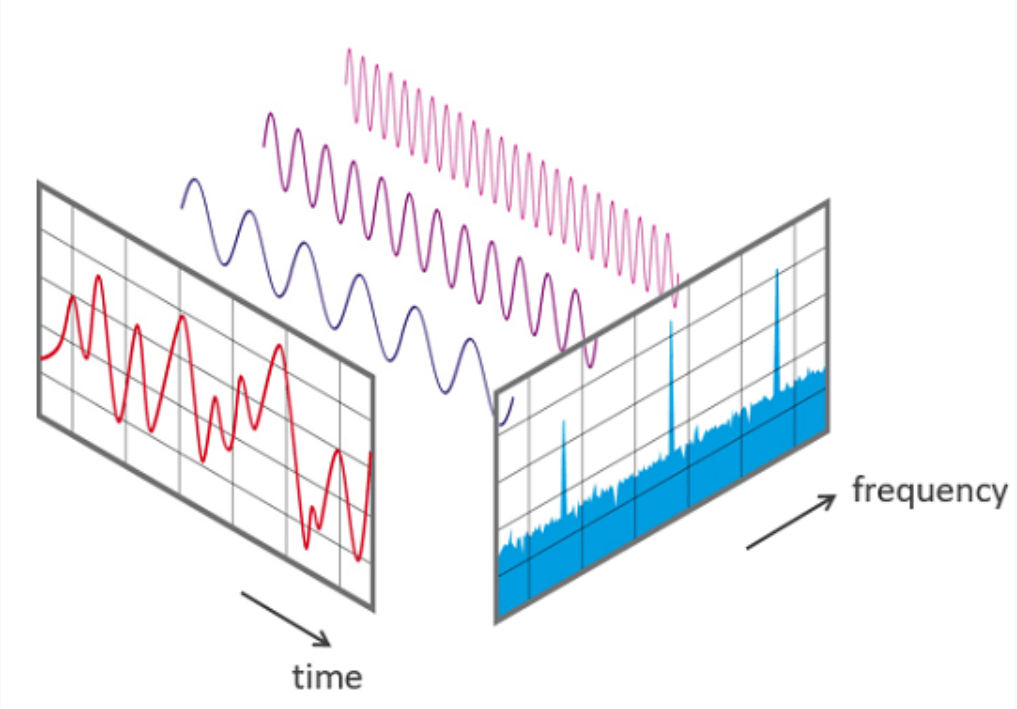


Source: DSP guide To

avoid that $\rightarrow f_{samp} > 2 * f_{max}$

DFT

- Discrete Fourier Transform
- Reveals frequency spectrum structure of a digital signal



What does it reveal? Is there an efficient way to compute it?

Targets at risk

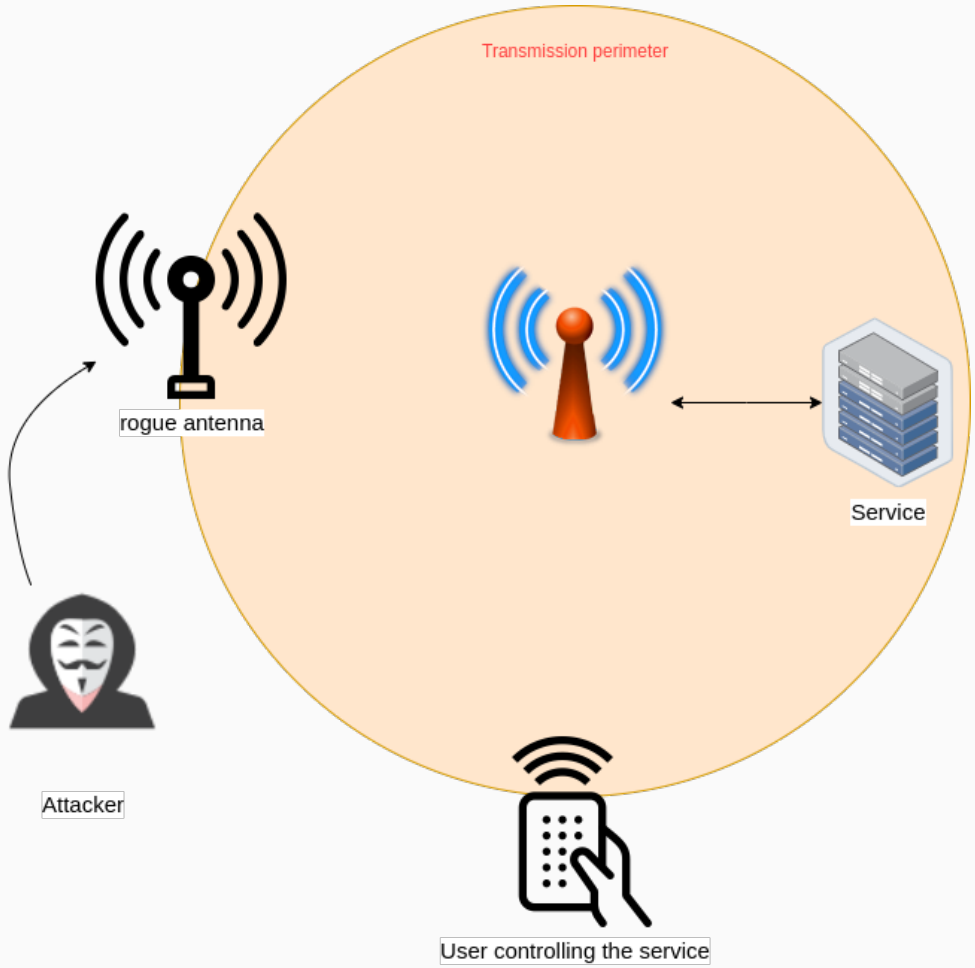
For certain applications, the use of RF may have risks

- Access controls
- Mobile phones
- Navigation
- Autonomous cars
- Industrial systems
- etc.

Risks with the air interface

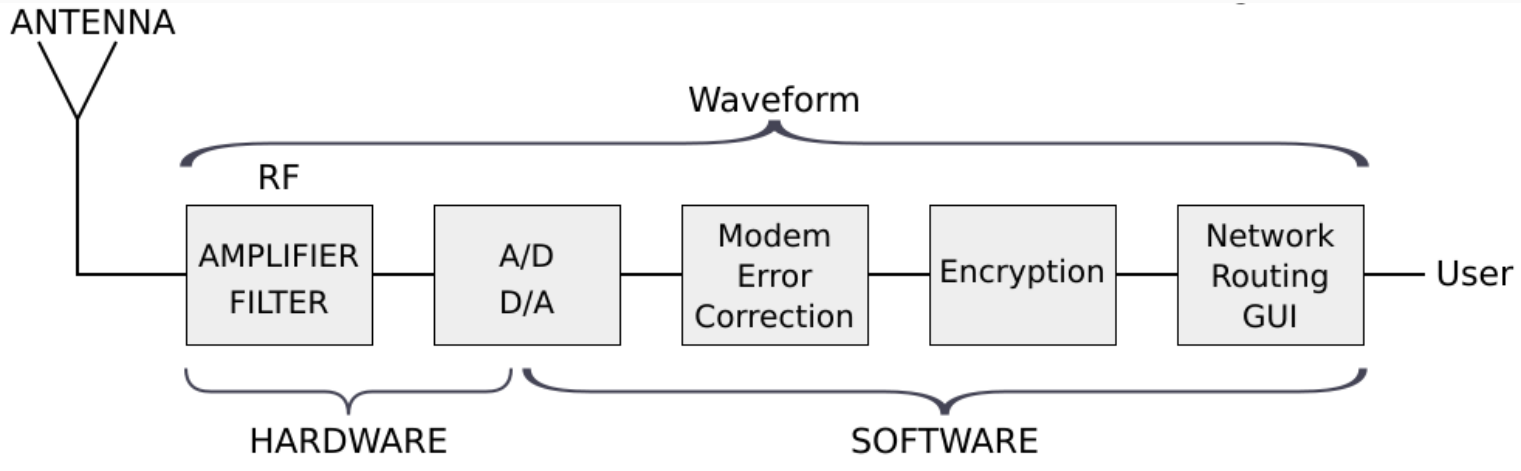
Common vulnerabilities:

- Eavesdropping
- Replay
- Injection
- Relay
- Jamming
- DoS via (very) high amplitude transmission
- etc.



Software-Defined Radio

- Before SDR → difficult to get equipment without $$$
- Made radio more accessible
- ADC/DAC conversion, RF Amp. and filtering performed on RF equipment
- The rest is done in software, generally with a computer:



Source: Wikipedia SDR

More than 100 SDR devices exist → how to make a choice?

Devices: a non-exhaustive list

Device	Tx/Rx	Supported frequencies	Max. samp rate ADC/ DAC (rate, width)	clock stability/pre cision	Tx/Rx channels	Bus / Interface	Price
USRP B2x0	Tx and Rx with Fullduplex	70 Mhz - 6 GHz	61.44 Msps, 12 bits	±2 ppm without GPSDO	- B200 : 1 Tx + 1 Rx - B210 : 2 Tx + 2 Rx	USB 3	~800€ min.
BladeRF 2.0	Tx and Rx with Fullduplex	47MHz - 6GHz	61.44 Msps, 12 bits	±1 ppm	1 Tx + 1 Rx	USB 3	~480€
bladeRF	Tx and Rx with Fullduplex	300 MHz – 3.8 GHz	40 Msps, 12 bits	±1 ppm	1 Tx + 1 Rx	USB 3	~400€ min.
LimeSDR	Tx and Rx with Fullduplex	100 kHz-3.8 GHz	61.44 Msps, 12 bits	±2.5 ppm	2 Tx + 2 Rx	USB 3	~300€ min.
XTRX	Tx and Rx with Fullduplex	30 MHz - 3.7 GHz	120 Msps SISO / 90 Msps MIMO, 12 bits	± 0.5 ppm without GPS / ± 0.01 ppm avec lock GPS	2 Tx + 2 Rx	PCIe x2	~260€ min.
RTL-SDR	Rx only	Different tuners: 52 - 2200MHz; 24 – 1766MHz; 22 - 1100MHz; 22 - 948.6MHz; 146 - 308Mhz and 438 -924 MHz	3.2 Msps, 8 bits	±25 ppm	1 Rx	USB 2	~15€ - 100€
SDRplay	Rx only	10kHz - 2 GHz	10.66 Msps, 12 bits	~0,5ppm	1 Rx	USB 2	150,00 €
HackRF	Tx and Rx Half-duplex	300 MHz - 3.8 GHz	20 Msps, 8 bits	20 ppm	1 Rx	USB 2	> 300€
ADALM-PLUTO SDR	Tx and Rx fullduplex	325MHz – 3.8 GHz; 70MHz – 6.0 GHz conf.	61.44 Msps, 12 bits	±25 ppm	1 Tx + 1 Rx	USB 2	140€

Bigger list: https://en.wikipedia.org/wiki/List_of_software-defined_radios

Antennas

- Antennas are the last link of the chain
- Ensure transmission and reception of symbols
- In general: no distinction between reception (passive) and transmission (active) antennas
- Main characteristics:
  - usage frequency
  - polarisation
  - directivity
  - dimension and shape
  - power mode
  - permissible power to emit
  - mechanical resistance
- Gain $\rightarrow$ directionality and radiation pattern
- Antennas can have different types...

Observations

Spectrum analyzers

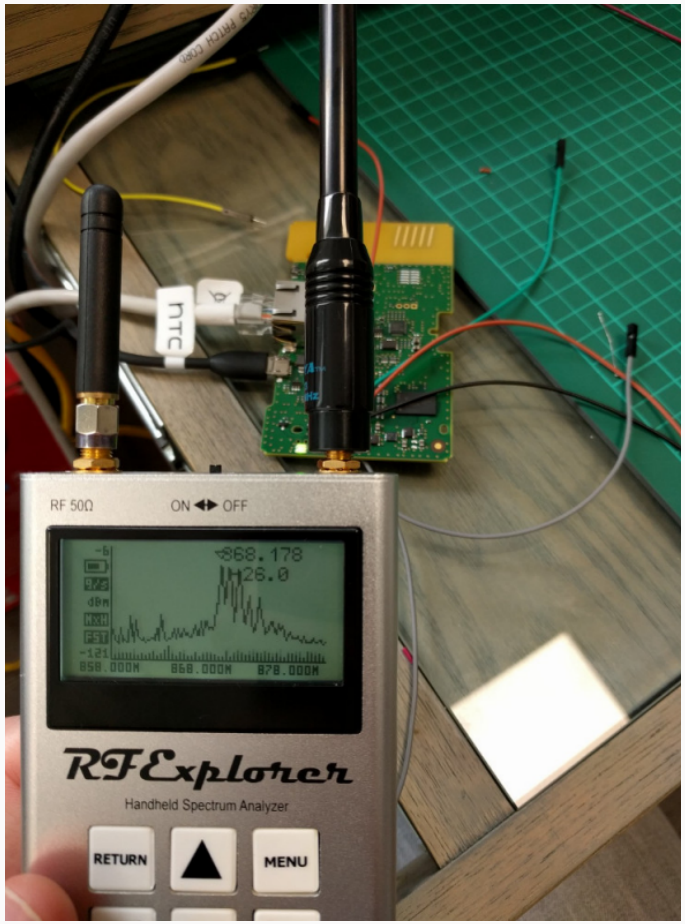
A beast:

- R&S®FSV40
- 10 Hz to 40 GHz freq band
- 160 MHz signal analysis bandwidth
- costs > 43 000€

RF Explorer

A handy gadget for < 300€:

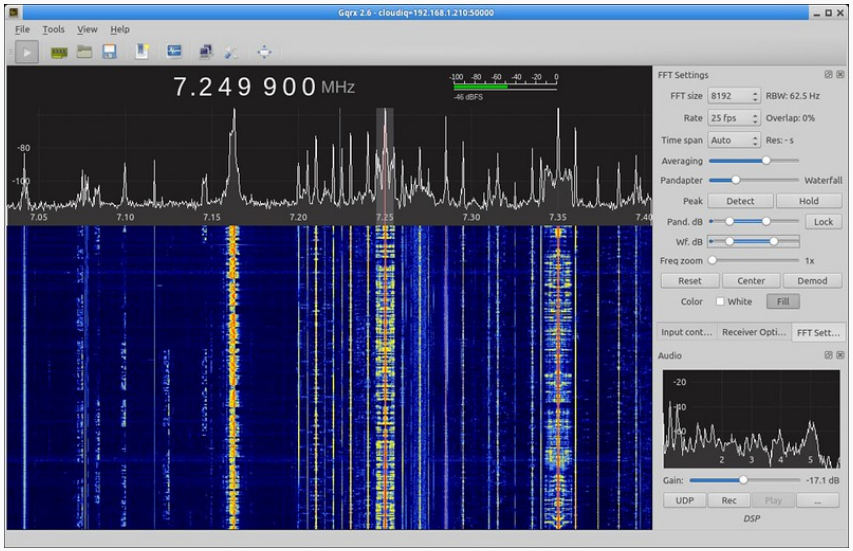
- Left SMA port (WSUB1G): 240-960MHz
- Right SMA port (WSUB3G): 15-2700 MHz
- Resolution bandwidth (RBW): automatic 3Khz to 600Khz



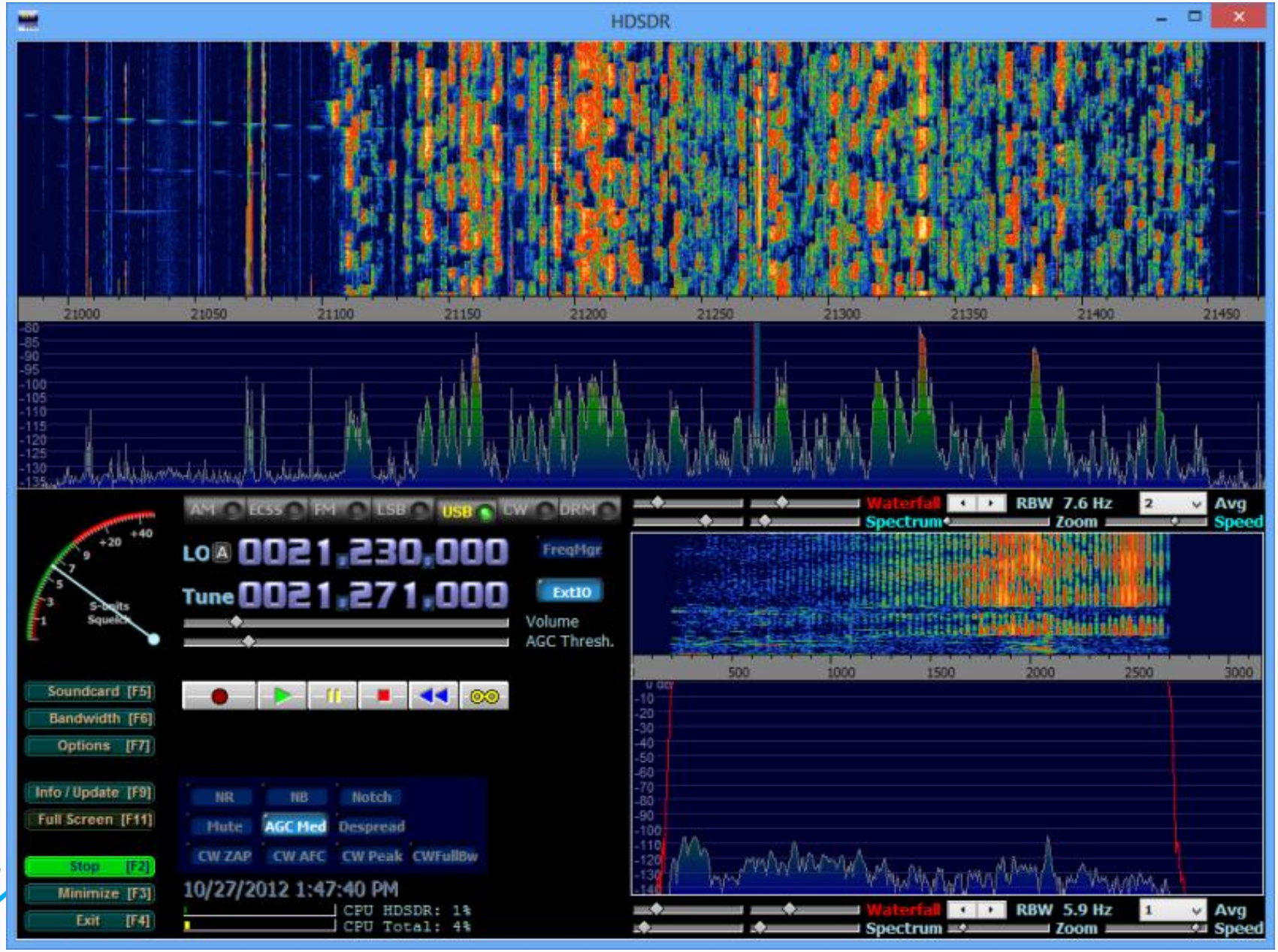
With SDR

Famous software:

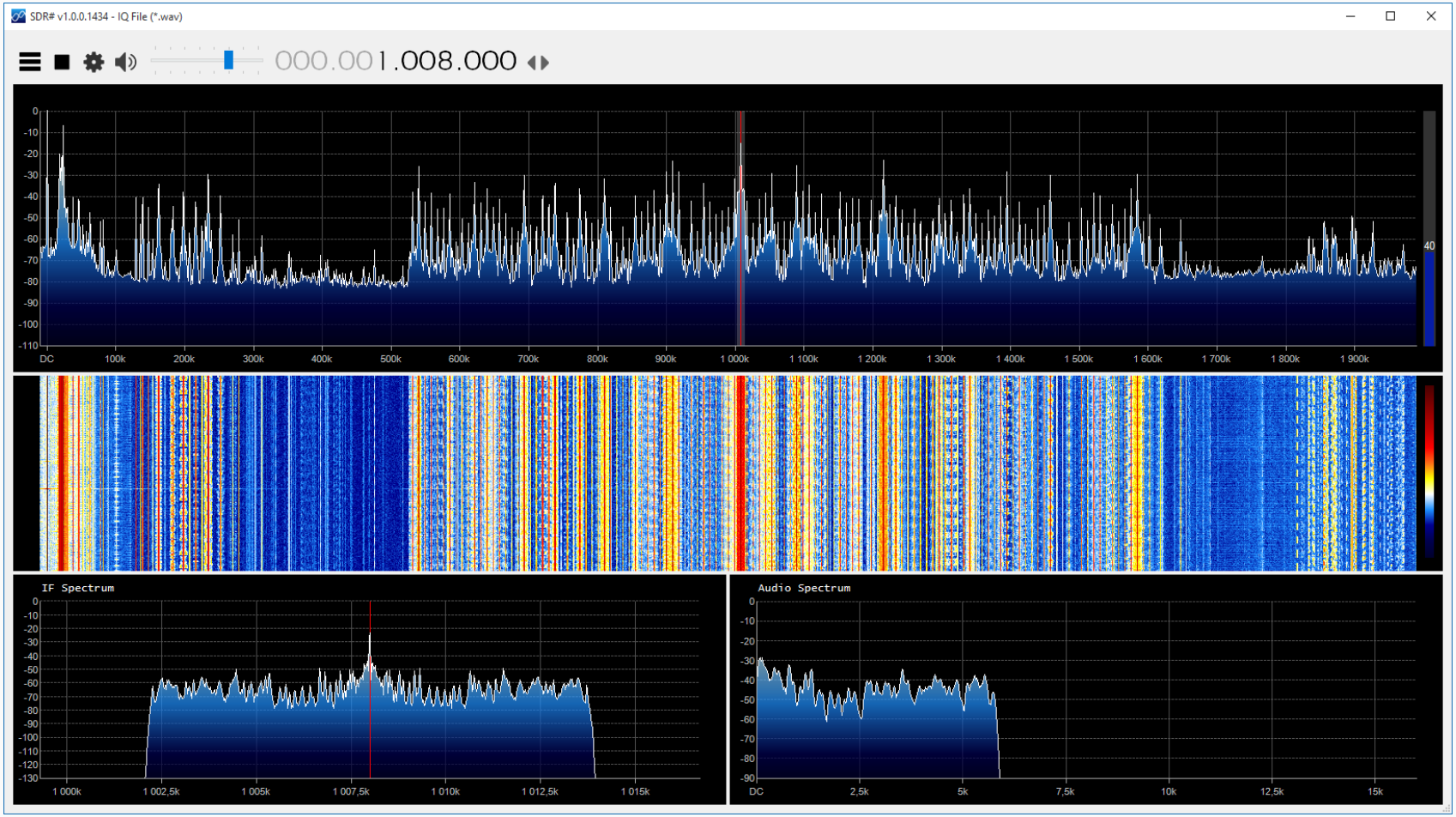
- GQRX on Linux and Mac OS X
- HDSDR on Windows
- SDR# on Windows



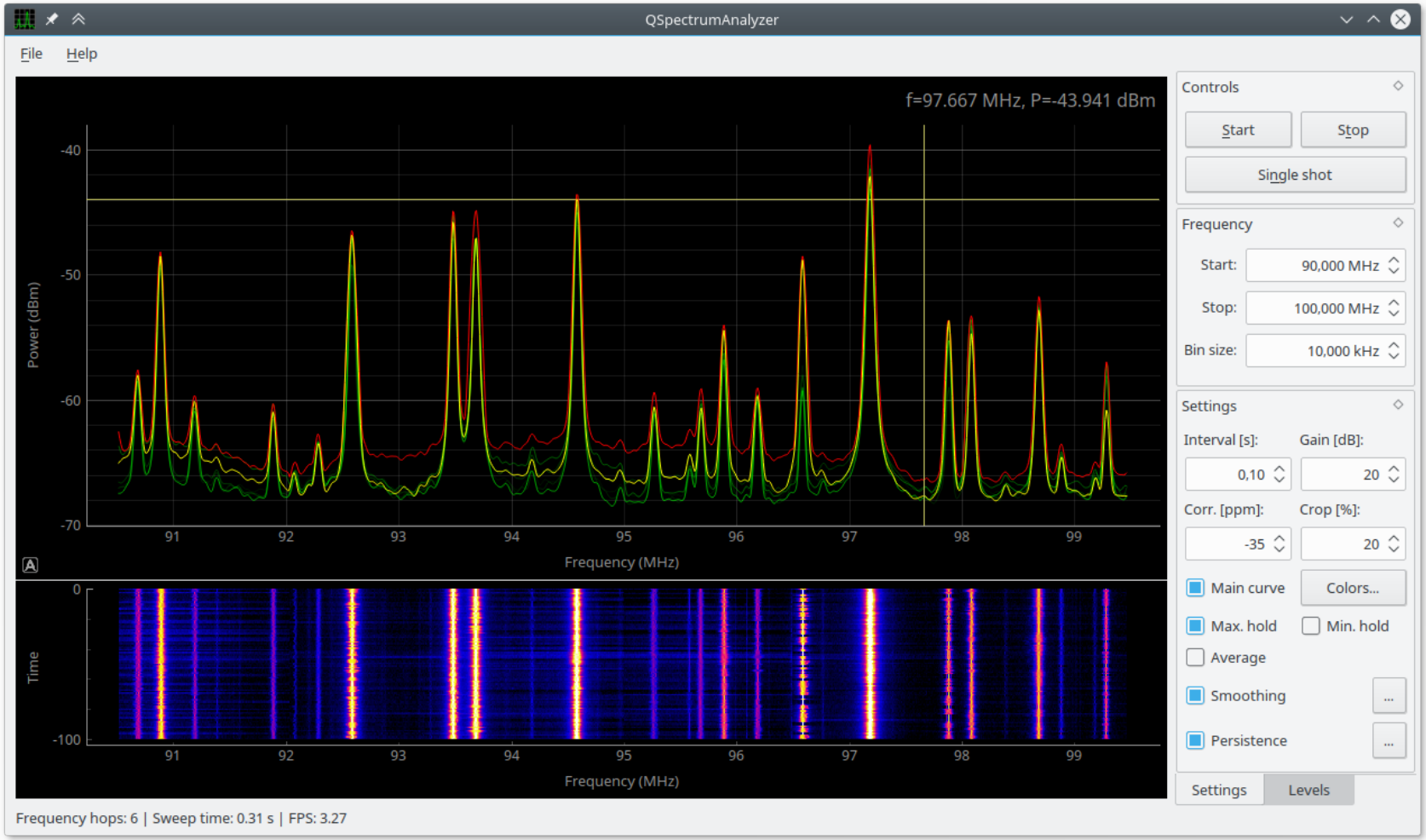
HDSDR


HDSDR
21000
21050
21100
21150
21200
21250
21300
21350
21400
21450
AM
ECSS
FM
LSB
USB
CW
DRM
LO A 0021,230,000
Tune 0021,271,000
FreqMgr
ExtIO
Volume
AGC Thresh.
Waterfall
Spectrum
RBW 7.6 Hz
Zoom
Avg
Speed
Soundcard [F5]
Bandwidth [F6]
Options [F7]
Info / Update [F9]
Full Screen [F11]
Stop [F2]
Minimize [F3]
Exit [F4]
NR
NB
Notch
Mute
AGC Med
Despread
CW ZAP
CW AFC
CW Peak
CWFullBw
10/27/2012 1:47:40 PM
CPU HDSDR: 1%
CPU Total: 4%
RBW 5.9 Hz

SDR#

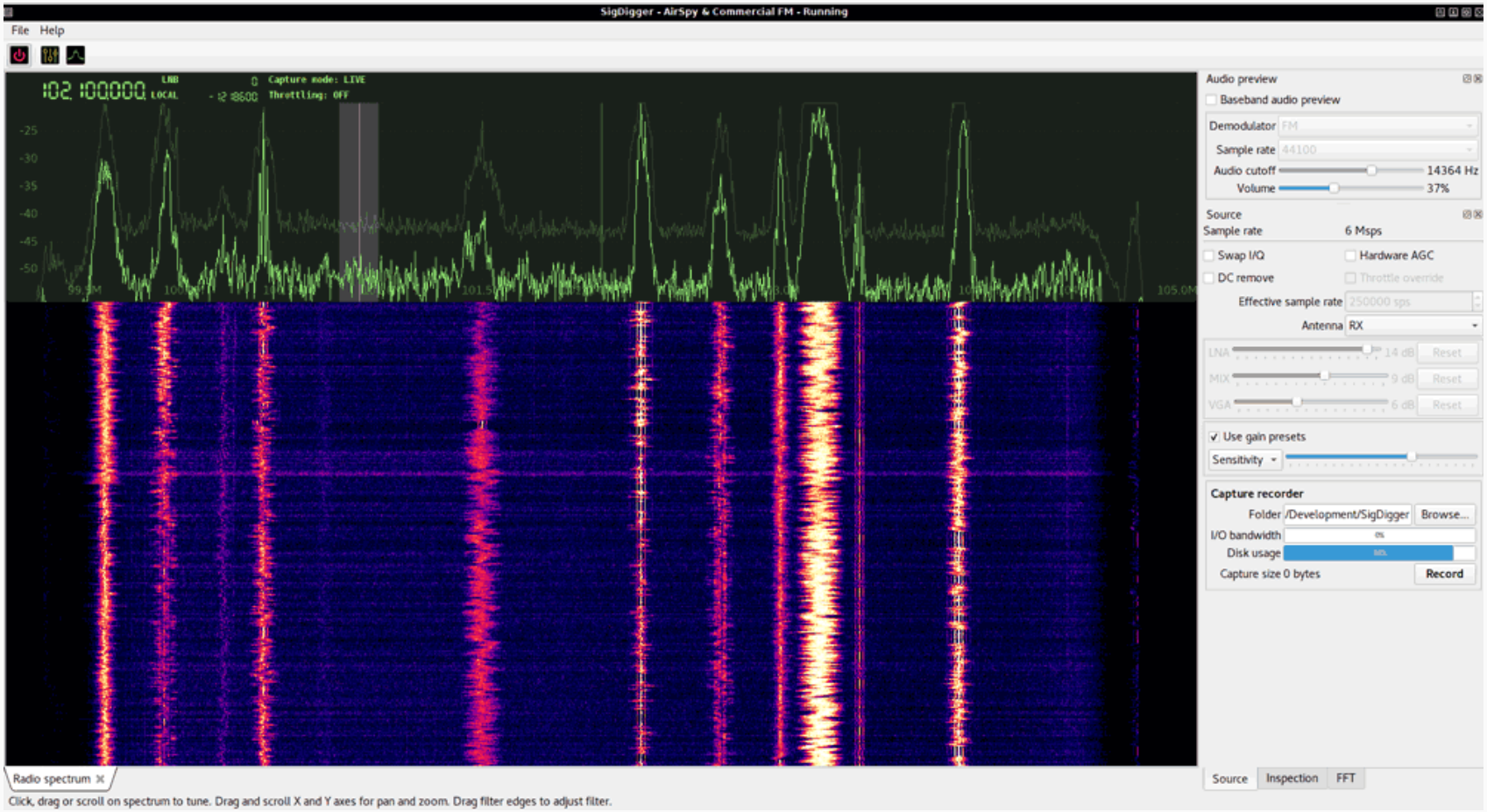

SDR# v1.0.0.1434 - IQ File (*.wav)
000.001.008.000
IF Spectrum
Audio Spectrum

But also: QSpectrumAnalyzer



Helpful with → Automatic peak detection

But also: SigDigger

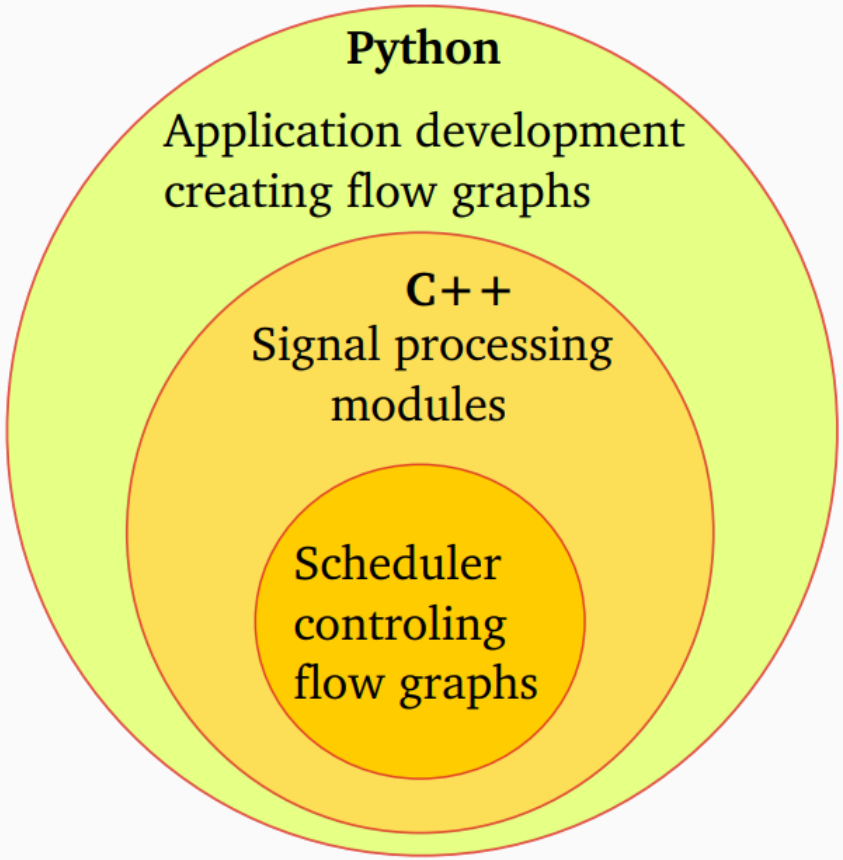


Designed for reverse engineering

GNU Radio Companion

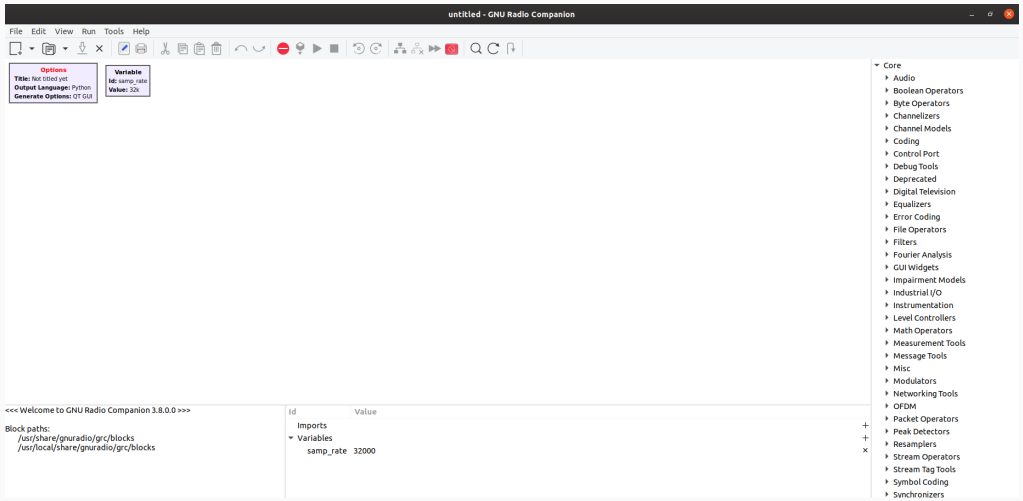
3 tier architecture

- Python → creates signal flow graphs
- C++/Python to create blocks
- Scheduler to control operations → ‘start’, ‘stop’ and ‘wait’ operations



GNU Radio Companion

- Graphical tool
- Create signal flow graphs and generate flow-graph source code



Analyzing a signals

Classic process

1. Determine the frequency
2. Look at the shape → which modulation does it use (ASK, FSK, ...)
3. Sometimes the shape is complicated to see → go deeper by look to device's transmitter specs
4. Use the blocks you need to process the signal
5. etc.

At the end you'll have to decode it (NRZ, Manchester, etc.)

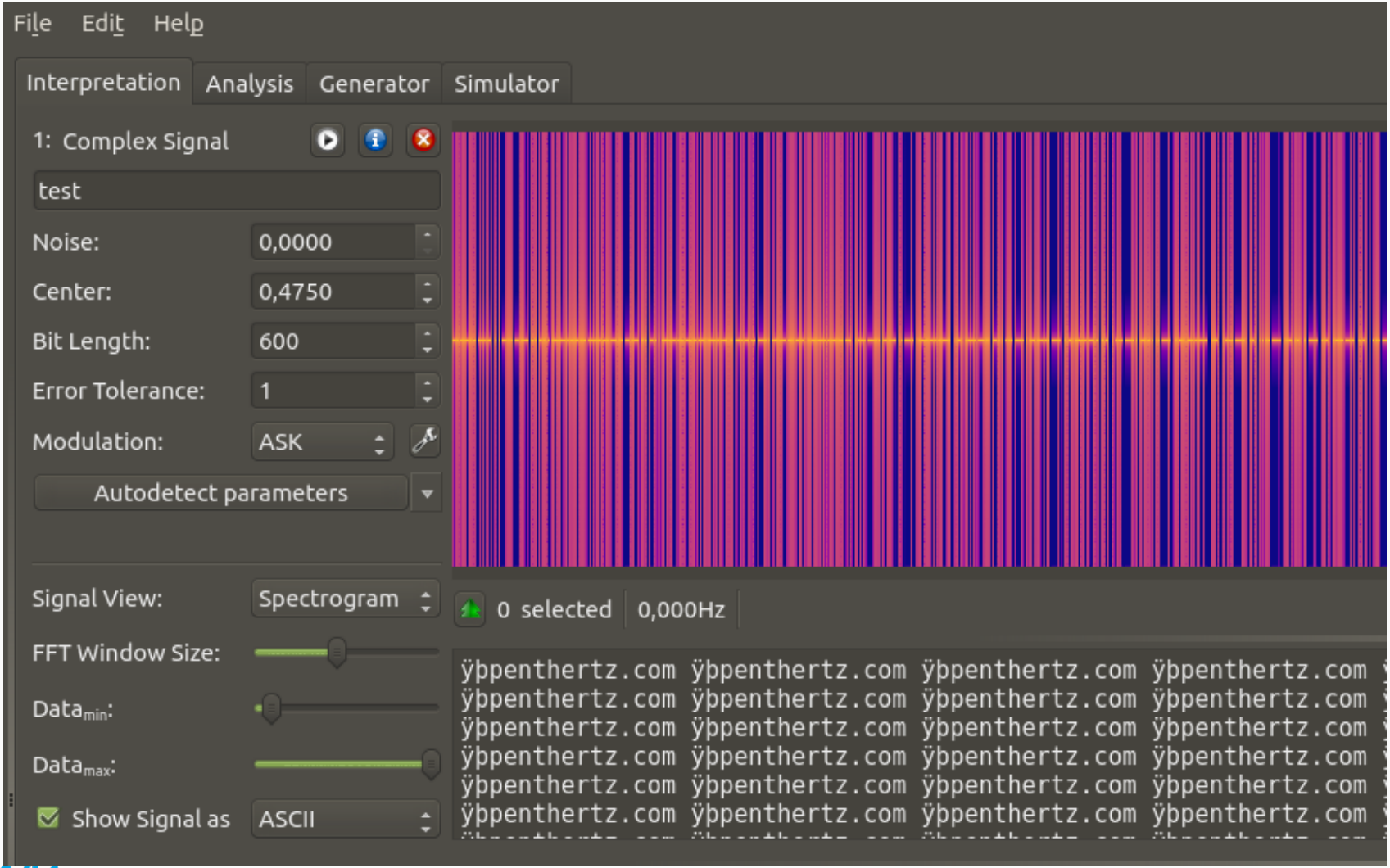
Why should I do that?

Like said before:

- Tons of targets use RF communications
- Attacking them can be interesting (remember that signal broadcast in the air)

Useful tools: Universal Radio Hacker

There is Inspetrum, but also URH (my favorite)



Examples of targets

subGhz devices

- Industrial, Scientific, and Medical (ISM) frequency bands
  $\rightarrow$ unlicensed
- Present in:
  - Power Meter
  - Doorbells
  - Alarms
  - Door remotes
  - Medical Device
  - Car remotes
  - Industrial systems
  - etc.
- Cheap transceiver

subGhz devices (2)

Sub-GHz ISM bands

Band	Range	Central frequency	Countries
300 MHz			US
433 MHz	433.050 – 434.790 MHz	433.92 MHz	Europe, Africa, the former Soviet Union, Mongolia, and the Middle East west of the Persian Gulf, including Iraq.
868 MHz	863 – 870 MHz	868 MHz	Europe, Africa, the former Soviet Union, Mongolia, and the Middle East west of the Persian Gulf, including Iraq.
915 MHz	902 – 928 MHz	915 MHz	Americas including Greenland, and some of the eastern Pacific Islands, non-FSU Asia east of and including Iran, and most of Oceania

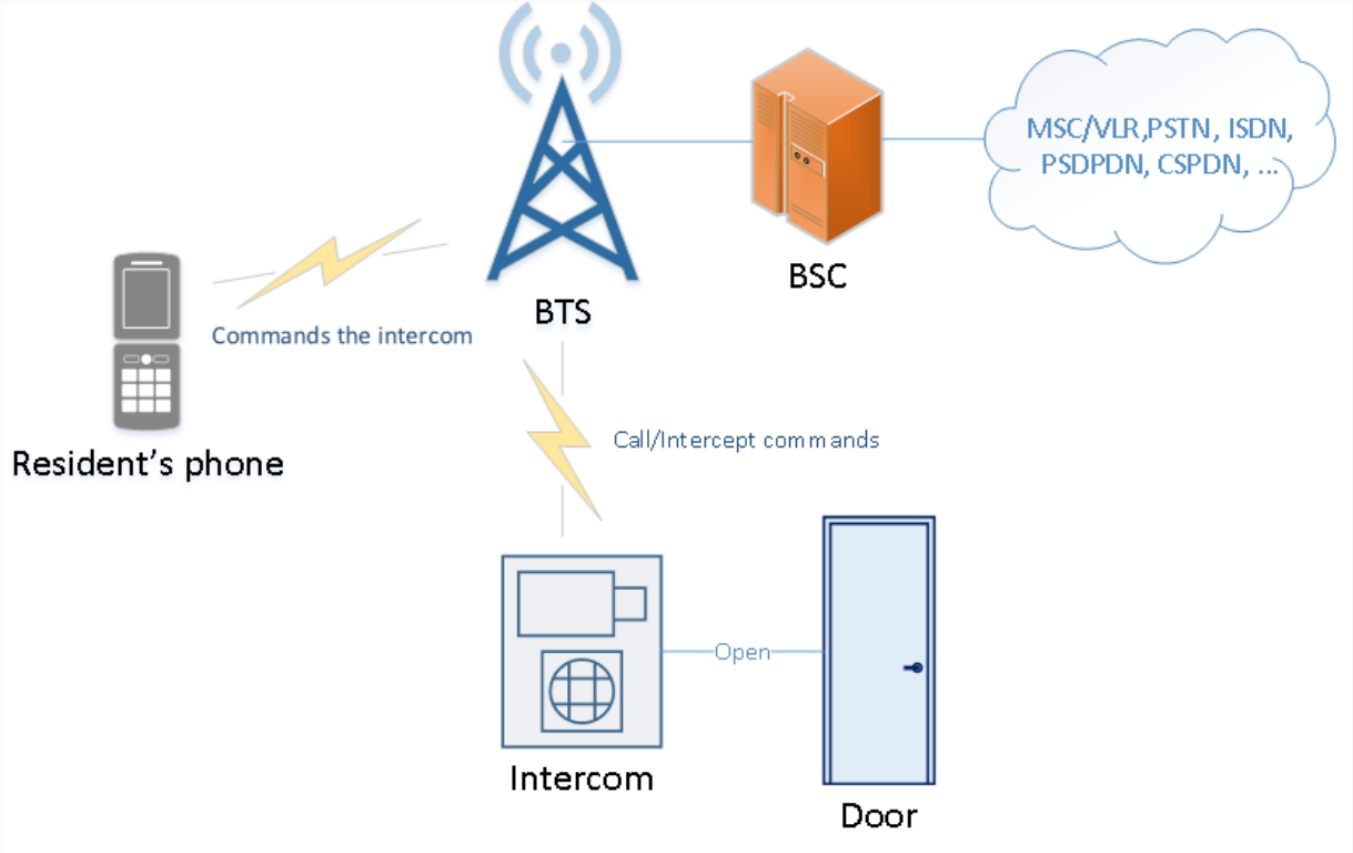
Use of mobile network

- Current use of the mobile network:
  - intercoms
  - delivery pick-up stations
  - electric counters
  - cameras
  - alarms
  - cars...

Targets: intercoms

- No wire for each resident
- Replaced by:
  - GSM, 3G, or 4G
  - Wi-Fi
  - …

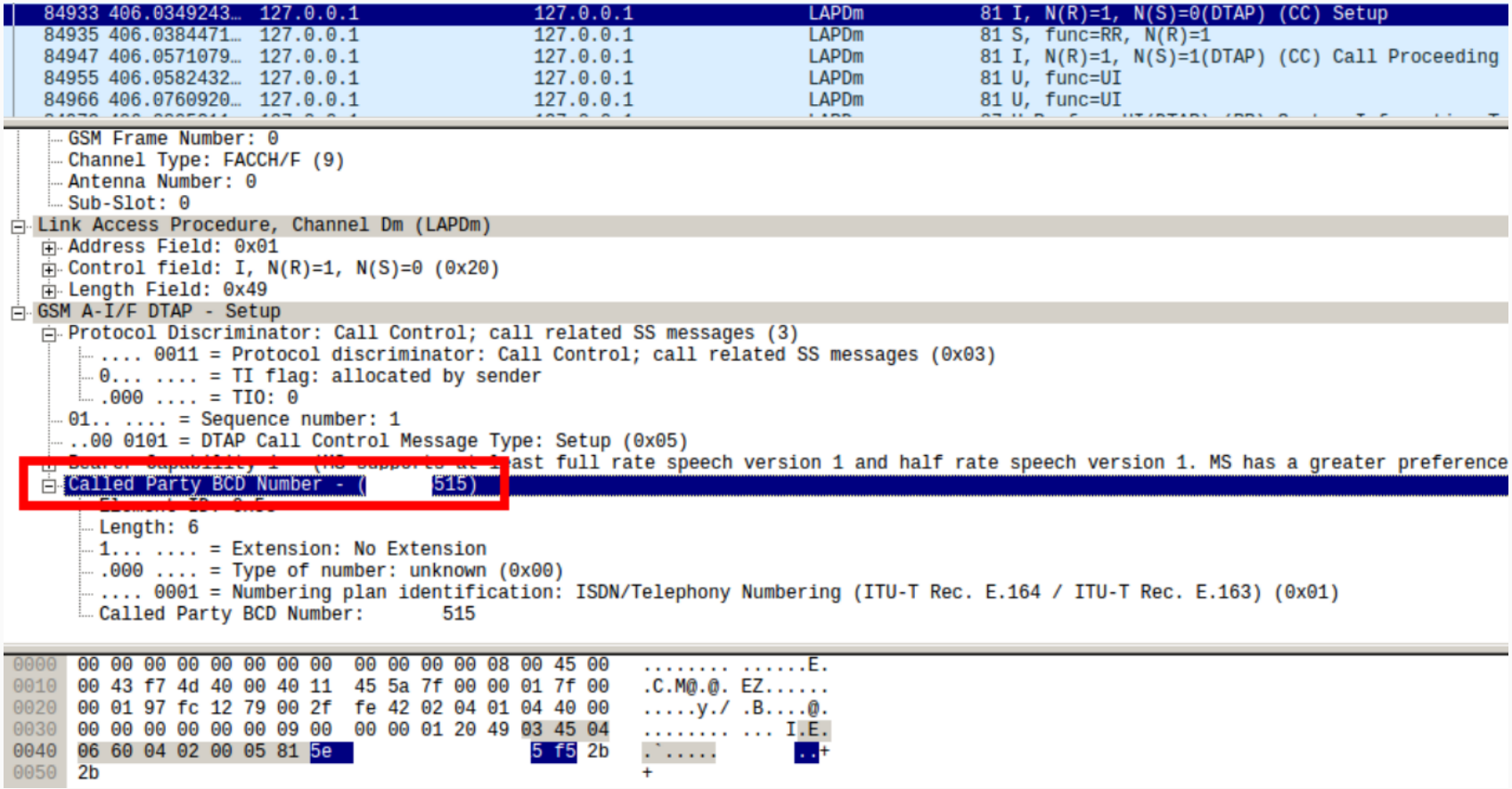
Intercom in the network



How to catch it? Let's introduce the handover first

Spotting a mobile module

Capture resident's number



Impresonate the number

In YateBTS, by modifying *tmsidata.conf* as follows:

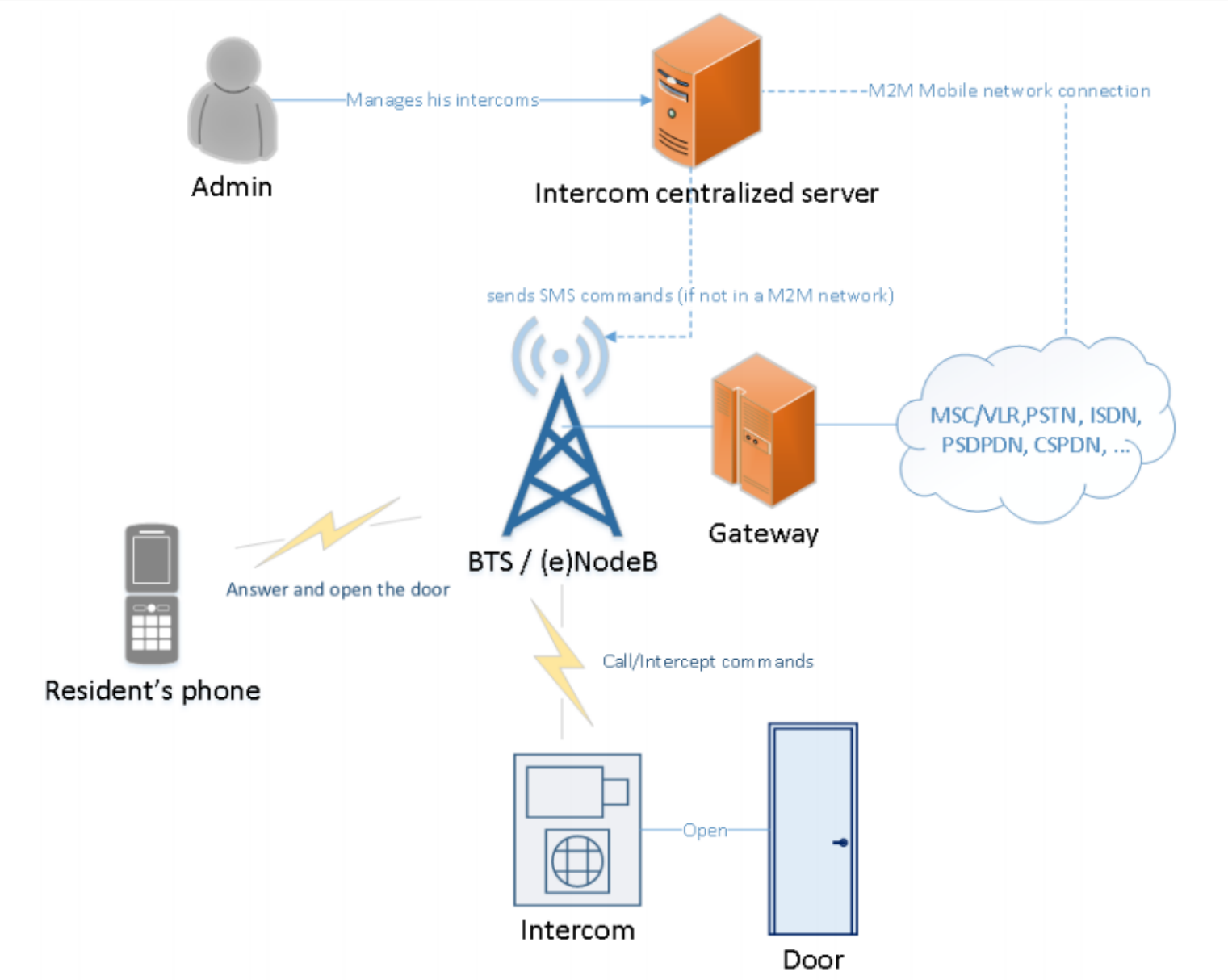
```
[tmsi]
last=007b0005
[ues]
20820XXXXXXXXXX=007b0003,35547XXXXXXXXXX,XXXXXX
515,1460XXXXXX,ybts/TMSI007b0003
# associating attacker IMSI with a resident number
[...]
```

We can then open the door or use SMS commands!

Our alarm station

Let’s see how different it is with our alarm station...

3G or 4G targets



3G or 4G targets (2)

- Mutual authentication → difficult to spawn a station at this level
- We have to downgrade the communication to GSM

3G or 4G targets (2)

- Mutual authentication $\rightarrow$ difficult to spawn a station at this level
- We have to downgrade the communication to GSM

Jamming with portable Chinese jammer

Cheap and can be reworked by disabling 2G antenna and jam only 3G and 4G

Pent Hertz

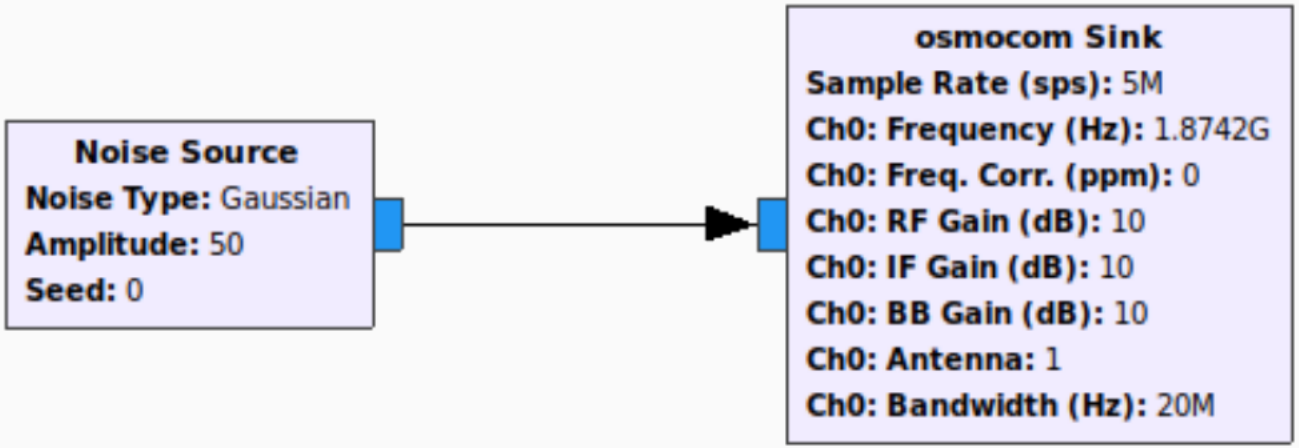
But signal strength poor

Jamming with portable desktop jammer

Strong signal and can be reworked too

But heavy and expensive.

Jamming the SDR way



It’s just noise… But you are limited in bandwidth and speed!

Jamming with Modmodjam

Concept of ”smart”-jamming:

- Uses results from a scanner like Modmodmap
- Then jam frequencies with adapted bandwidth

`https://github.com/PentHertz/Modmobjam`

Intercepting cars' IVI

Pent Hertz

Intercepting cars' IVI (2)

A lot of clear-text traffic!

10	1.459318826	192.168.99.2	192.168.99.254	HTTP	913	POST /Service/InitSession/[redacted] HTTP/1.1 (applicat
19	7.536599505	192.168.99.2	10.91.80.203	HTTP	52	HEAD http://master.coyoterts.com HTTP/1.1
26	13.660617735	192.168.99.2	10.91.80.203	HTTP	52	HEAD http://master.coyoterts.com HTTP/1.1
65021	922.704281910	192.168.99.2	10.91.80.203	HTTP	52	HEAD http://master.coyoterts.com HTTP/1.1
66923	946.703883356	192.168.99.2	10.91.80.203	HTTP	52	HEAD http://master.coyoterts.com HTTP/1.1
69066	974.461373298	192.168.99.254	192.168.99.2	HTTP	173	HTTP/1.0 404 File not found
69093	974.818419668	192.168.99.2	192.168.99.254	HTTP	52	HEAD http://master.coyoterts.com HTTP/1.1
70396	990.503915759	192.168.99.2	192.168.99.254	HTTP	406	POST /api/app/call HTTP/1.1 (application/x-protobuf)
70401	990.504770592	192.168.99.254	192.168.99.2	HTTP	390	HTTP/1.0 501 Unsupported method ('POST') (text/html)
70459	991.484062985	192.168.99.2	192.168.99.254	HTTP	406	POST /api/app/call HTTP/1.1 (application/x-protobuf)
70462	991.484923306	192.168.99.254	192.168.99.2	HTTP	390	HTTP/1.0 501 Unsupported method ('POST') (text/html)
70530	992.483719425	192.168.99.2	192.168.99.254	HTTP	406	POST /api/app/call HTTP/1.1 (application/x-protobuf)
70533	992.484544176	192.168.99.254	192.168.99.2	HTTP	390	HTTP/1.0 501 Unsupported method ('POST') (text/html)
1048…	1590.1445388…	192.168.99.2	192.168.99.254	HTTP	406	POST /api/app/call HTTP/1.1 (application/x-protobuf)
1048…	1590.1450970…	192.168.99.254	192.168.99.2	HTTP	390	HTTP/1.0 501 Unsupported method ('POST') (text/html)
1048…	1591.0455681…	192.168.99.2	192.168.99.254	HTTP	406	POST /api/app/call HTTP/1.1 (application/x-protobuf)
1048…	1591.0462935…	192.168.99.254	192.168.99.2	HTTP	390	HTTP/1.0 501 Unsupported method ('POST') (text/html)
1049…	1591.8855224…	192.168.99.2	192.168.99.254	HTTP	406	POST /api/app/call HTTP/1.1 (application/x-protobuf)

Intercepting cars' IVI (3)

Old Android → choice of your public sploit!

```
▾ Hypertext Transfer Protocol
  ▸ POST /api/app/call HTTP/1.1\r\n
    Content-Type: application/x-protobuf; charset=utf-8\r\n
    Accept-Encoding: gzip\r\n
    User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.0.4; ARM2-MX6DQ Build/UNKNOWN)\r\n
    Host: fr·           .aw.atos.net\r\n
    Connection: Keep-Alive\r\n
  ▸ Content-Length: 91\r\n
    \r\n
    [Full request URI: http://fr-           .aw.atos.net/api/app/call]
    [HTTP request 1/1]
    [Response in frame: 70533]
    File Data: 91 bytes
▸ Media Type
```

AddJavascriptInterface (CVE-2012-6636/CVE-2013-4710) RCE by example? :)

Attacking mobile network

- Software to emulate User Equipment exist:
  - srsLTE $\rightarrow$ srsUE
  - srsUE allows testing a eNodeB
  - But also to connect as a legit UE

Smart Grids

- Mainly to avoid issues in the past → power outage (e.g Northeast blackout of 2003[1])
- Many issues:
  - Cable expansion due to heat rise → sags between supporting structure → flashover
  - Flashover → triggers protection relays
  - If the other lines do not have enough spare capacity → cascading failure
- Need to use efficiently "smart" technologies for:
  - Wide variety of generation sources
  - Distribution assets coordination
  - Predict and control power consumption
  - Use energy storages for renewable energy production systems...

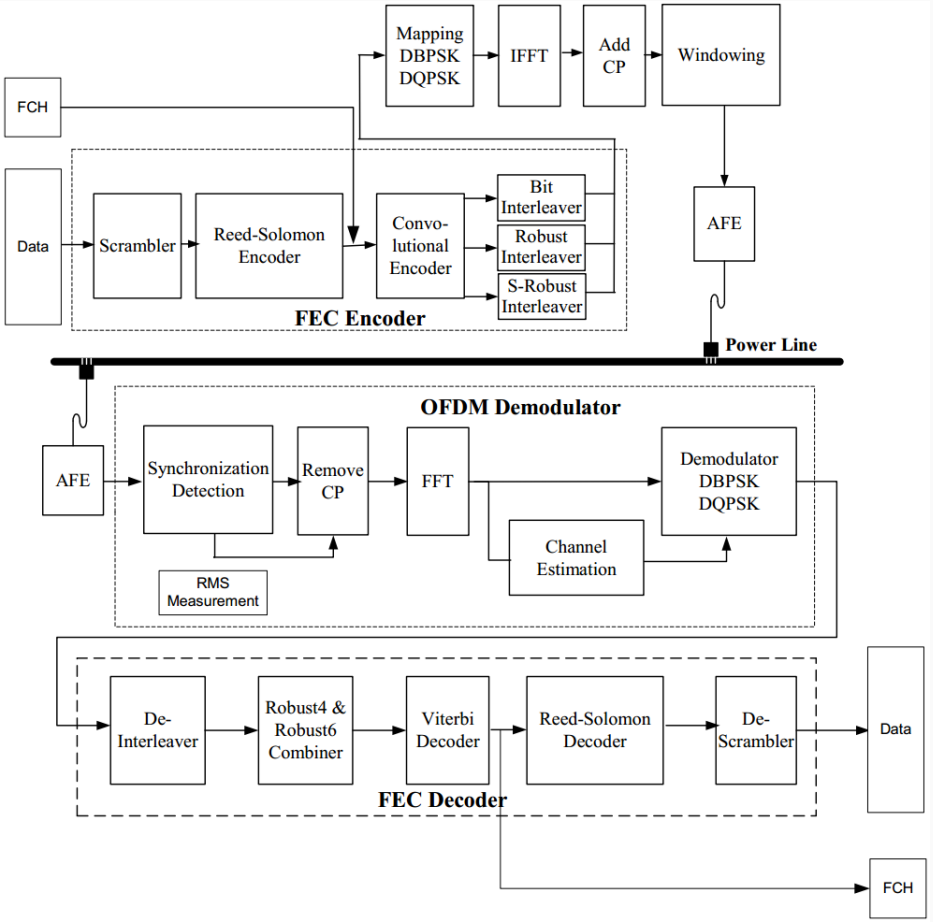
[1] https://www.scientificamerican.com/article/2003-blackout-five-years-later/

Smart grids

- Aims to manage small scale energy production nodes
- Manages the storage and distribution
- Use these nodes effectively
- Includes:
  - smart meters
  - smart appliances
  - renewable energy resources
  - and energy-efficient resources

Data propagation: DSP

1. data scrambling
2. turbo encoding
3. modulation of control and data frames
4. form OFDM symbols
5. windowing
6. etc.



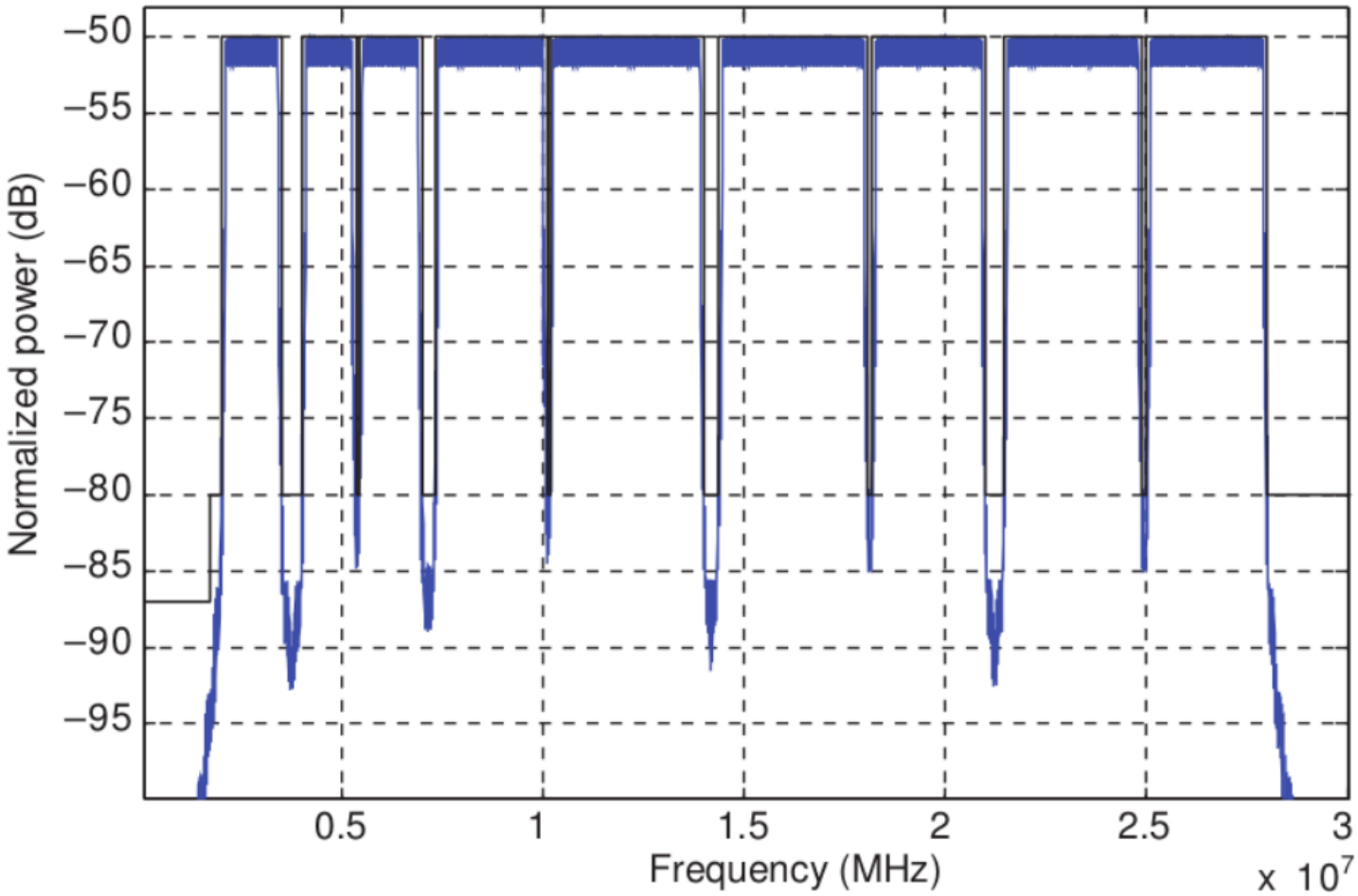
Some PoC: V2G Injector

Using a PLC:

- Available: https://github.com/FlUxIuS/V2GInjector
- Paper, slides and recording: click here (SSTIC 2019)

Our attempts on HPAV

Different bands can be observed depending on the transmission quality and QoS $\rightarrow$ 1.8 - 30 MHz:



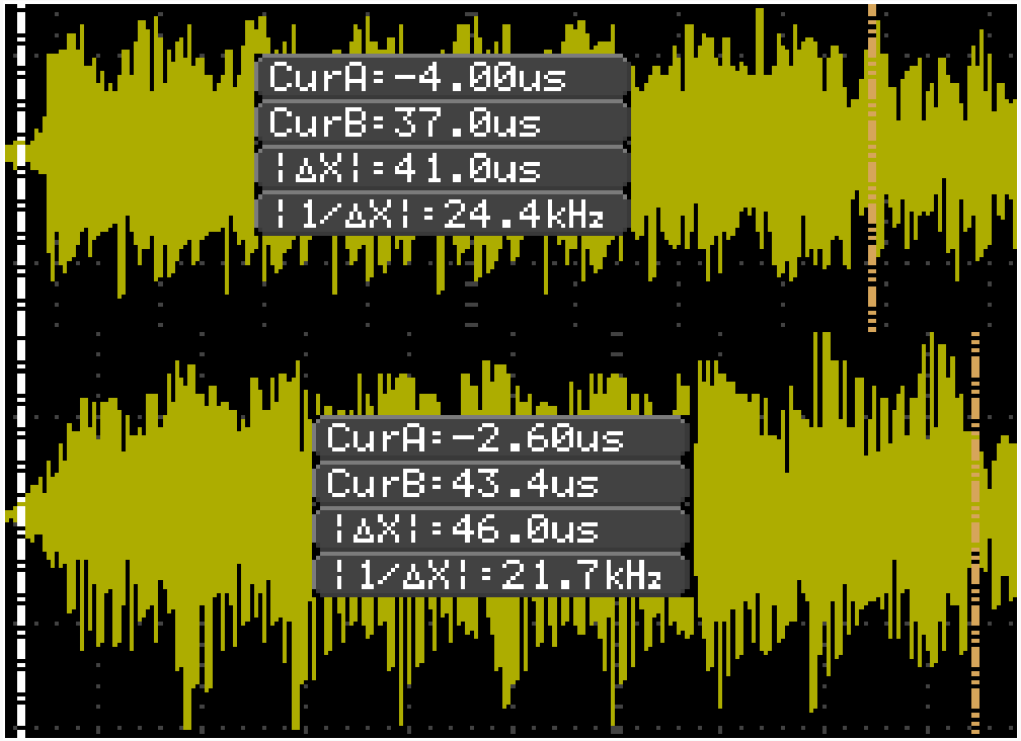
Customization

Customize an old PLC to be directly plugged in the line.

Pent Hertz

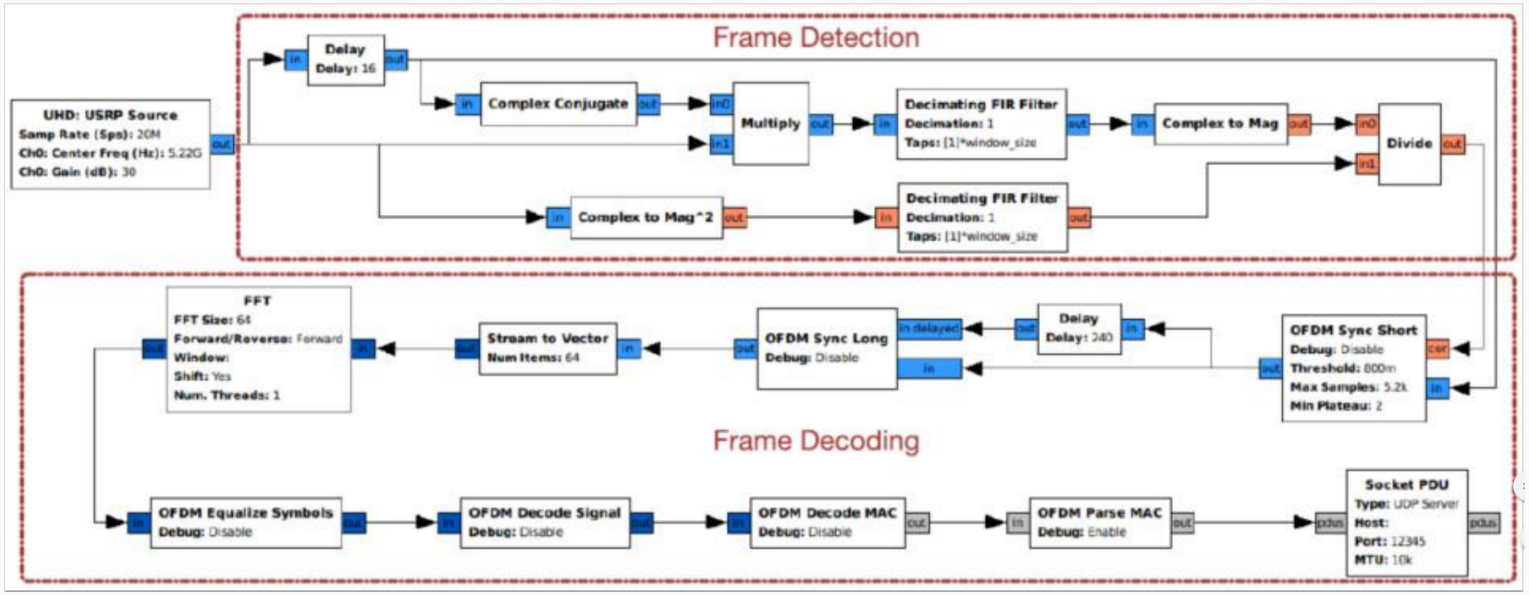
HP vs HPAV

With an oscilloscope → tiny differences: used preamble in HP ↔ HPAV



Decoding OFDM

Wi-Fi shares the same OFDM underpinnings:



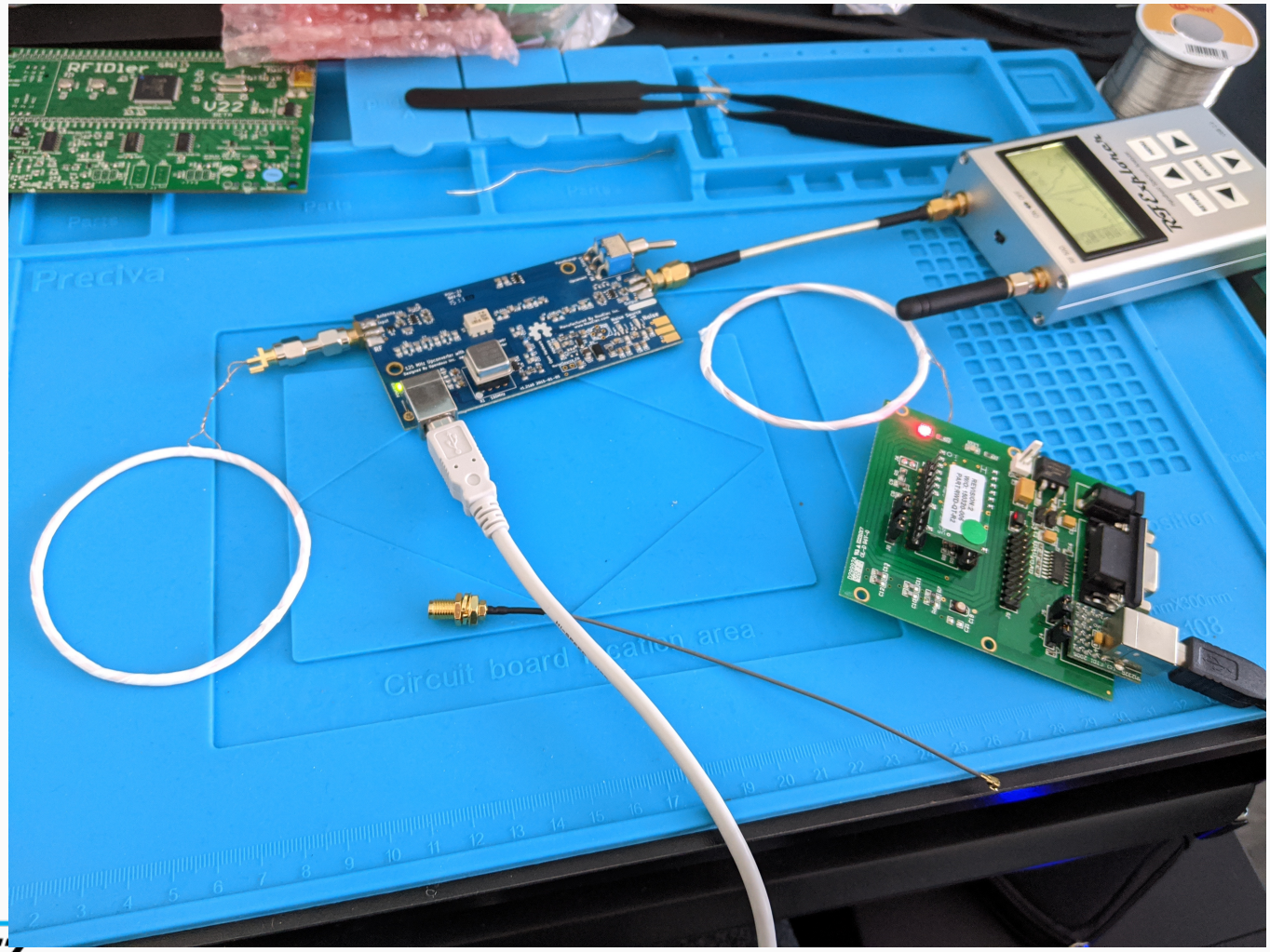
Sources of blocks: `https://www.wime-project.net/`

But could not manage to get all symbols with a USRP v1[2]

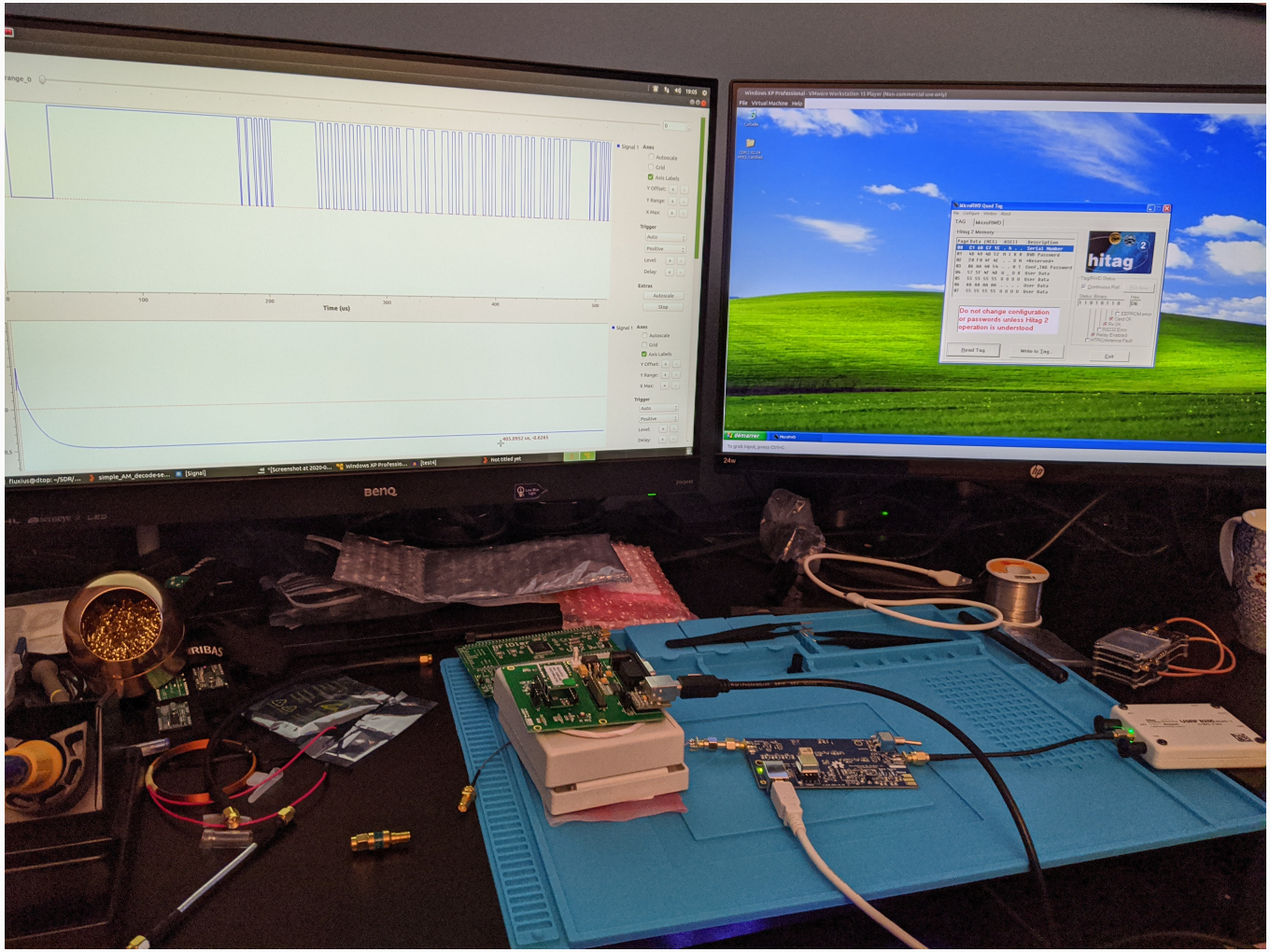
[2] `https://www.usenix.org/system/files/sec19-baker.pdf`

RFID

- Need to deal with low frequencies: 125 kHz - 13.56 MHz → need of upconverter sometimes → use of heterodyne



RFID


hitag
Do not change configuration or passwords unless Hitag 2 operation is understood
Time (us)
BenQ

Conclusion

Conclusion

R4D!O start

Questions?

Pent Hertz

Thanks!


THANK
YOU
GRACIAS
ARIGATO
SHUKURIA
BOLZÏN
MERCI
BÏYAN
SHUKRIA
DANKSCHEEN
TASHAKKUR ATU
YAQHANYELAY
SUKSAMA
EKHMET
MEHRBANI
GRAZIE
MAAKE
KOMAPSUMNIDA
JUSPAXAR
GOZAIMASHITA
EFCHARISTO
PALDIES
TINGKI
SPASSIBO
SNACHALHUYA
NUHUN
CHALTU
WABEEJA
MAITEKA
YUSPAGABÀTAM
HUI
DHANYABAAD
ANIHA
ATTO
LAH
SANCO
MERASTAWHY
GAEJTHO
AGUYJE
FAKAAUE
TAVTAPUCH
MEDAWAGSE
BANYA
GU
HATUR
EKOJU
SIKOMO
MAKETAJ
MIMMONCHAR
MERSI
SPASIBO
DENKAUJA
NEMACHALHYA
UNALCHÉESH