Workshop SDR

Cyril DELETRE

Objectifs

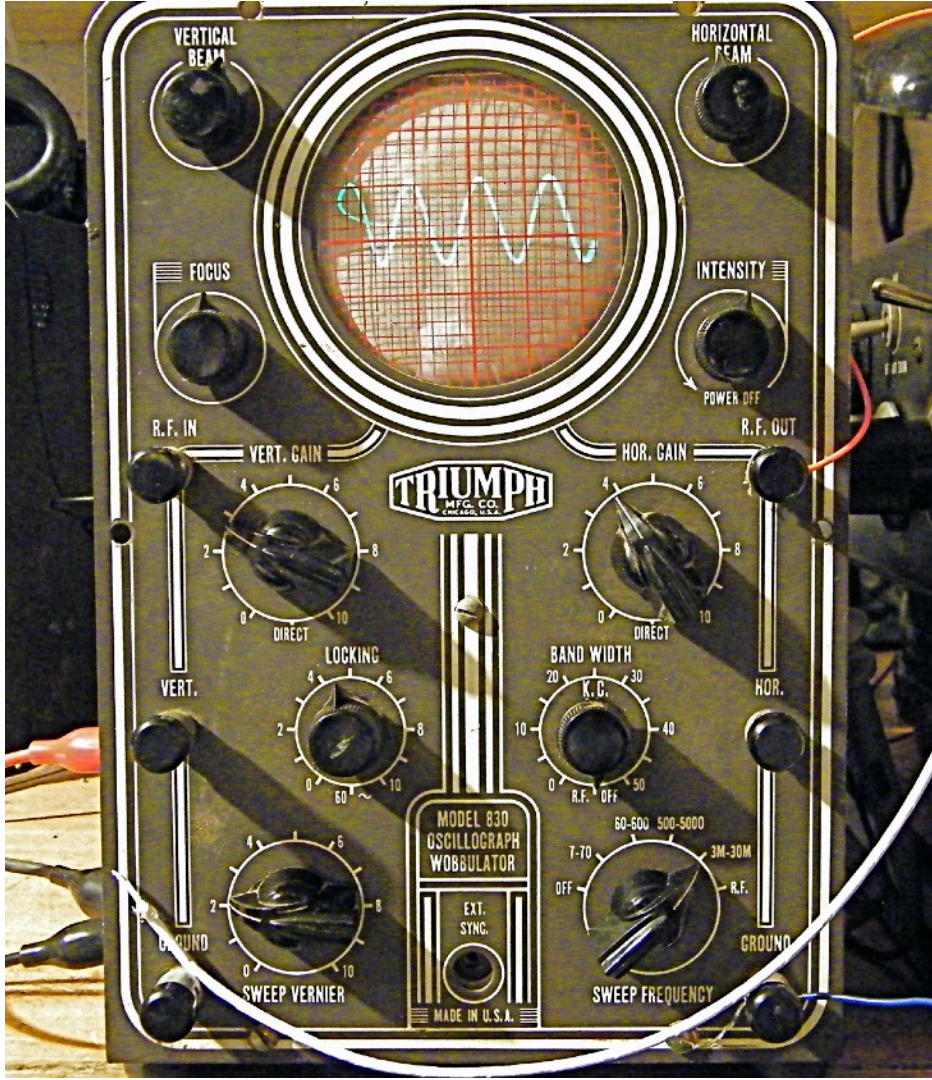
1. Comprendre le principe des transmissions radio
2. Apprivoiser le Software Defined Radio
3. S’amuser :)


ON AIR

Déroulement du Workshop

1. Préface aux ondes radio
2. L'échantillonnage
3. Radio hacking
4. Mise en pratique

Les bases


VERTICAL BEAM
HORIZONTAL BEAM
FOCUS
INTENSITY
POWER OFF
R.F. IN
R.F. OUT
VERT. GAIN
HOR. GAIN
TRIUMPH
MFG. CO.
CHICAGO, U.S.A.
DIRECT
DIRECT
LOCKING
BAND WIDTH
K.C.
R.F. OFF
VERT.
HOR.
MODEL 830
OSCILLOGRAPH
WOBBULATOR
EXT. SYNC.
MADE IN U.S.A.
SWEEP VERNIER
SWEEP FREQUENCY
60-500 500-5000
7-70
3M-30M
OFF
R.F.
GROUND

Préface aux ondes radio
Les bases: débutons avec un petit quizz

Perturber en utilisant une fréquence dans des conditions non conformes aux dispositions de l'article L.34-9 est

- Amusant
- Recommandé
- Puni de six mois d'emprisonnement et de 30000 euros d'amende

Les ondes radio ont été mises en évidence

- 1887 (construction de la Tour Eiffel)
- 1981 (Lancement du réseau 2G)
- 1914 (Première Guerre Mondiale)

Fréquence maximale d'une onde radio

- 60 GHz
- 3000 GHz
- il n'y en a pas

Une onde radio est

- Un rayonnement électrique
- Un rayonnement magnétique
- Un rayonnement électro-magnétique

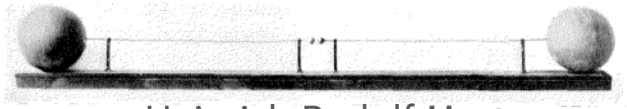
Préface aux ondes radio
Les bases: débutons avec un petit quizz

Perturber en utilisant une fréquence dans des conditions non conformes aux dispositions de l'article L.34-9 est

- ~~Amusant~~
- ~~Recommandé~~
- **Puni de six mois d'emprisonnement et de 30000 euros d'amende**

Les ondes radio ont été mises en évidence

- **1887 (Construction de la Tour Eiffel)**
- ~~1981 (Lancement de la 2G)~~
- ~~1914 (Première Guerre Mondiale)~~



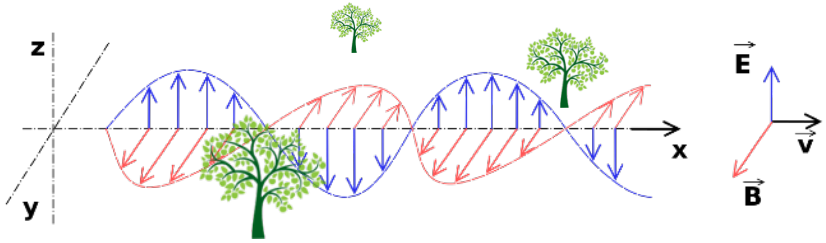
Heinrich Rudolf **Hertz**

Fréquence maximale d'une onde radio

- ~~60 GHz~~
- **3000 GHz**
- ~~il n'y en a pas~~

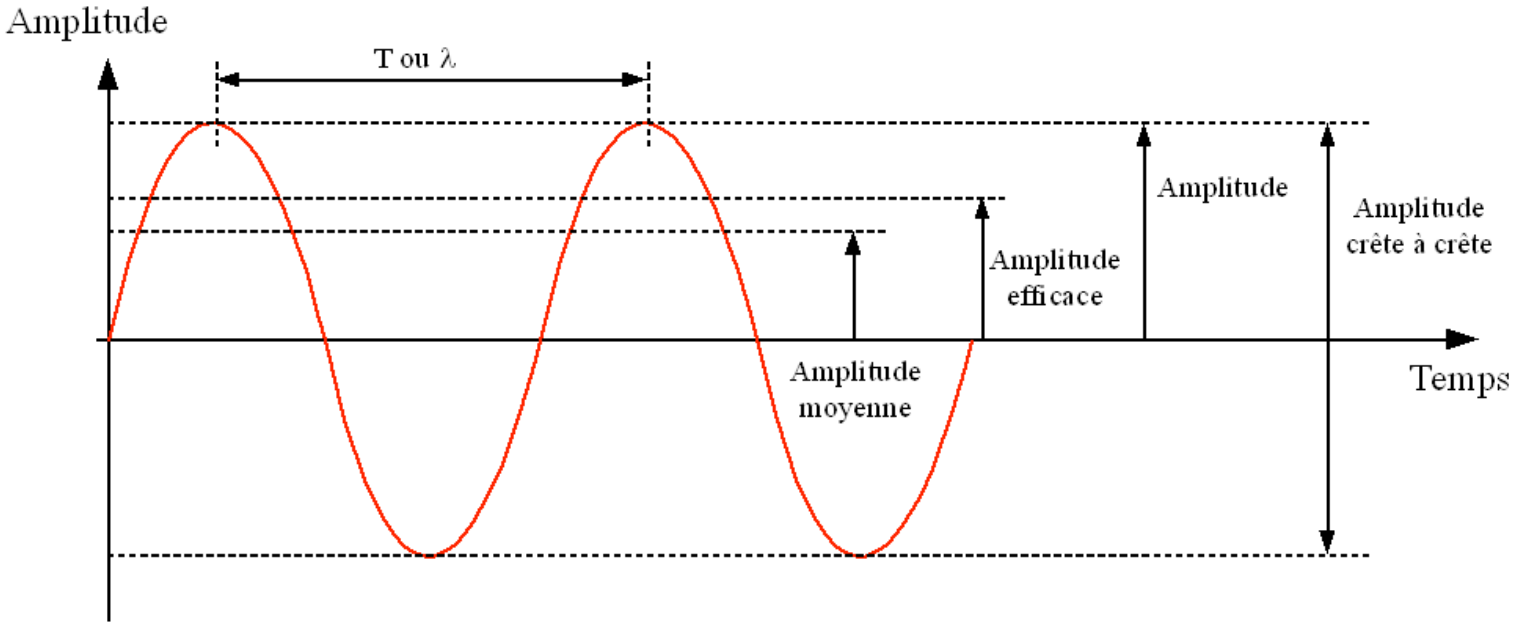
Une onde radio est

- Un rayonnement électrique
- Un rayonnement magnétique
- **Un rayonnement électromagnétique**



Rayonnement électromagnétique

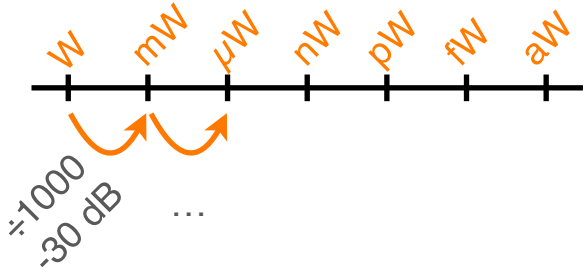
Préface aux ondes radio
Les bases: sinusoïde



source: wikipedia.org

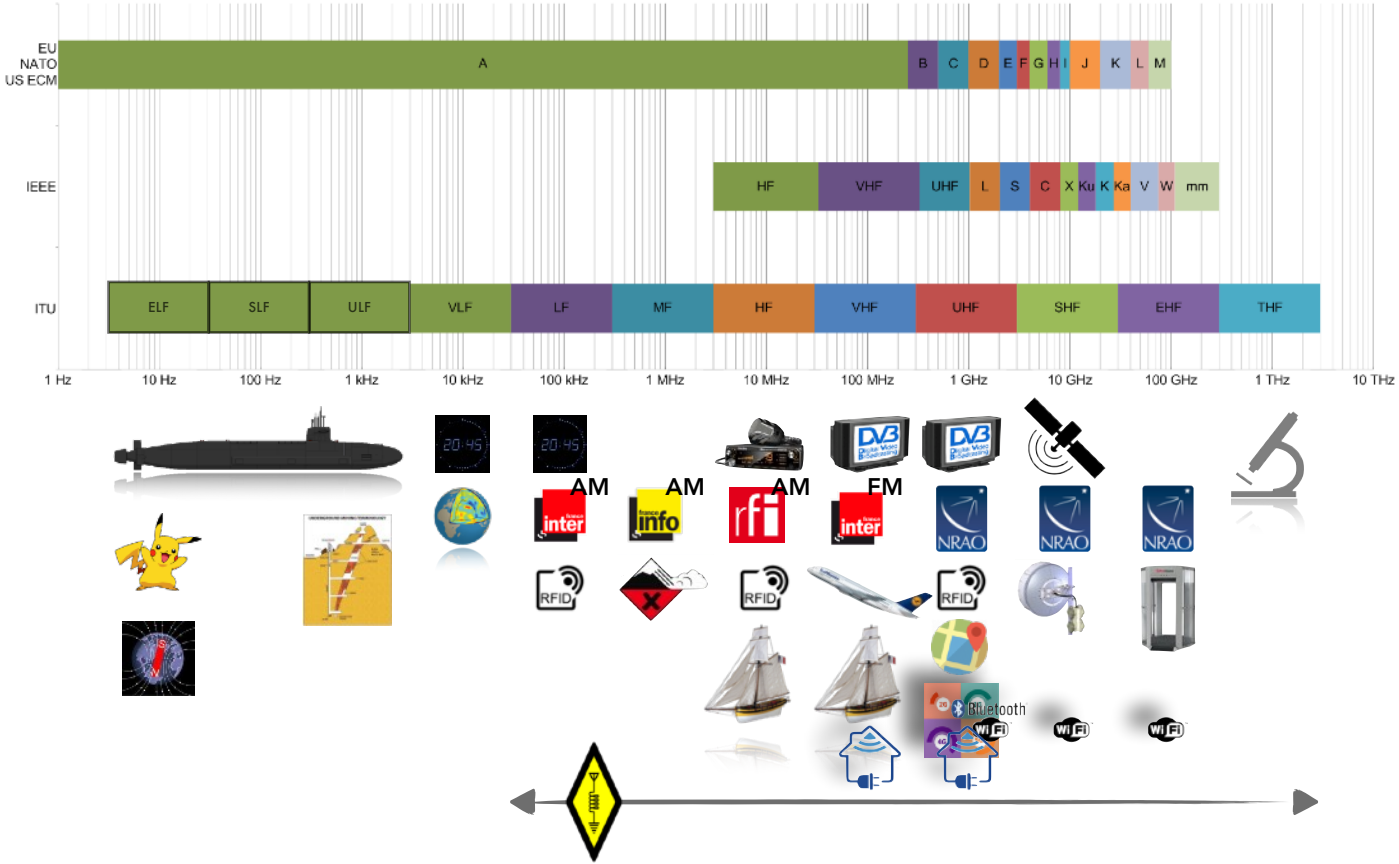
Préface aux ondes radio
Les bases: puissance

- Puissance: P = U.I (Watt, dBm)

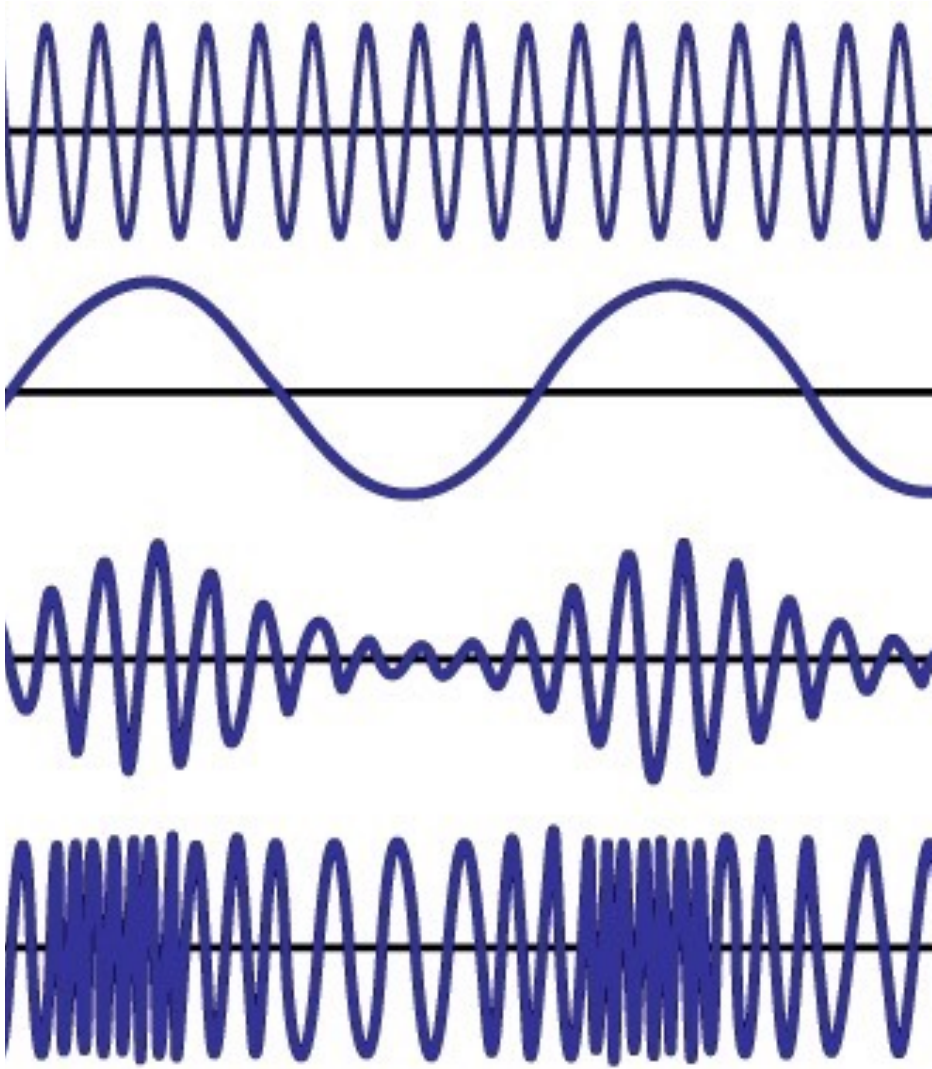


power level	*power*	*example*
80 dBm	100 kW	FM radio station (50km coverage)
60 dBm	1 kW	Microwave oven
33 dBm	2 W	GSM900 handset max. output
30 dBm	1 W	DCS1800 handset max. output
27 dBm	125 mW	UMTS class 4 handset max. output
20 dBm	100 mW	IEEE 802.11b/g max output (EU)
-10 dBm	100 µW	IEEE 802.11b/g received signal
-100 dBm	0.1 pW	IEEE 802.11b/g min. received signal
-127.5 dBm	0.178 fW	Typical received signal power from GPS
-∞ dBm	0 W	not well expressed in dBm

Préface aux ondes radio
Les bases : standards de désignation des bandes



Modulations



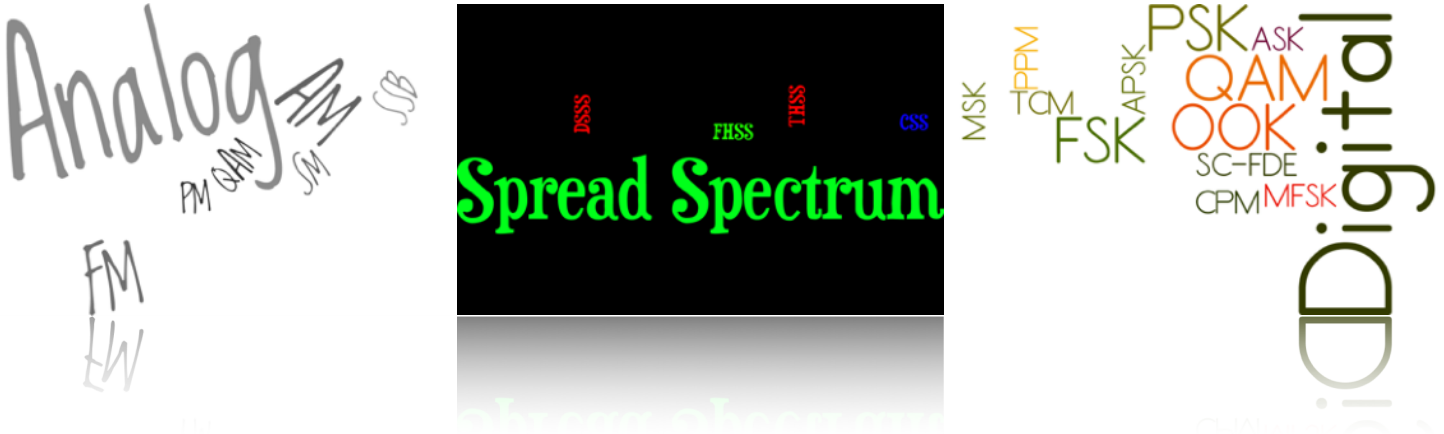
Préface aux ondes radio
Modulations: définition

Modulation du signal

61 langues

Pour les articles homonymes, voir modulation.

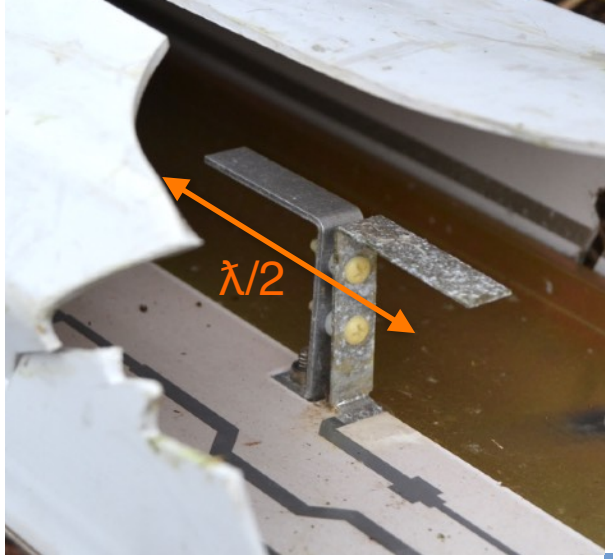
En télécommunications, le signal transportant une information doit passer par un moyen de transmission entre un émetteur et un récepteur. Le signal est rarement adapté à la transmission directe par le canal de communication choisi, hertzien, filaire, ou optique.
La **modulation** peut être définie comme le processus par lequel le signal est transformé de sa forme originale en une forme adaptée au canal de transmission, par exemple en faisant varier les paramètres d'amplitude et d'argument (phase/fréquence) d'une onde sinusoïdale appelée porteuse.
Le dispositif qui effectue cette modulation, en général électronique, est un modulateur (voir modem). L'opération inverse permettant d'extraire le signal de la porteuse est la démodulation.

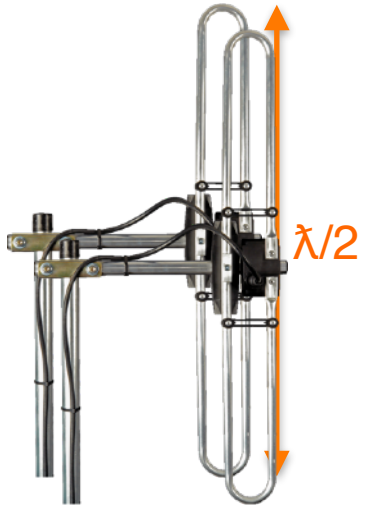


Les antennes

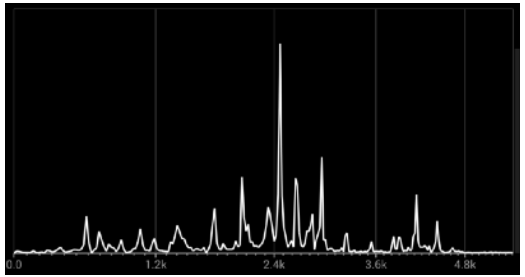
Préface aux ondes radio
Antennes courantes

- Dipôle demi-onde: antenne secteur 2G
- Dipôle replié: radio FM et TV
- Mono-pôle quart d'onde (fouet): radio FM
- Hélicoïdale: sonnette sans fil
- Rubber ducky: WiFi, 2G/3G/4G modem
- Patch: Raspberry Pi Zero W
- Loop cadre: radio AM

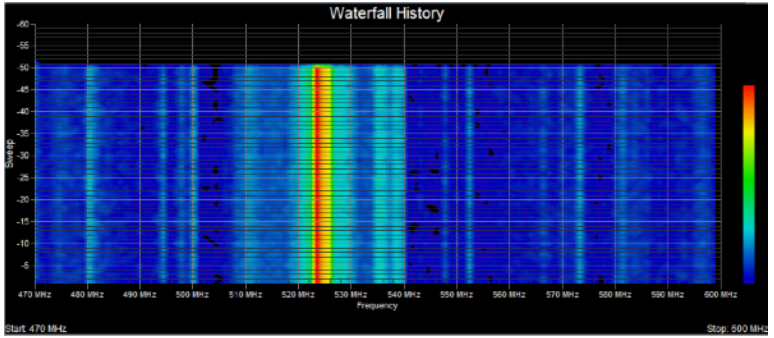




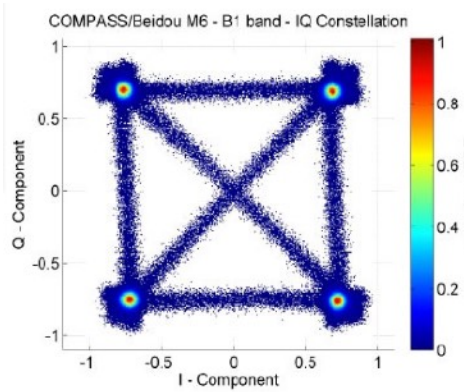
Echantillonnage
Outils de visualisation



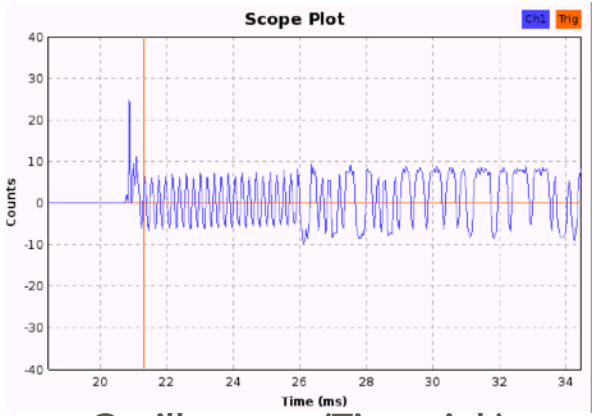
FAST FOURIER TRANSFORM



Waterfall

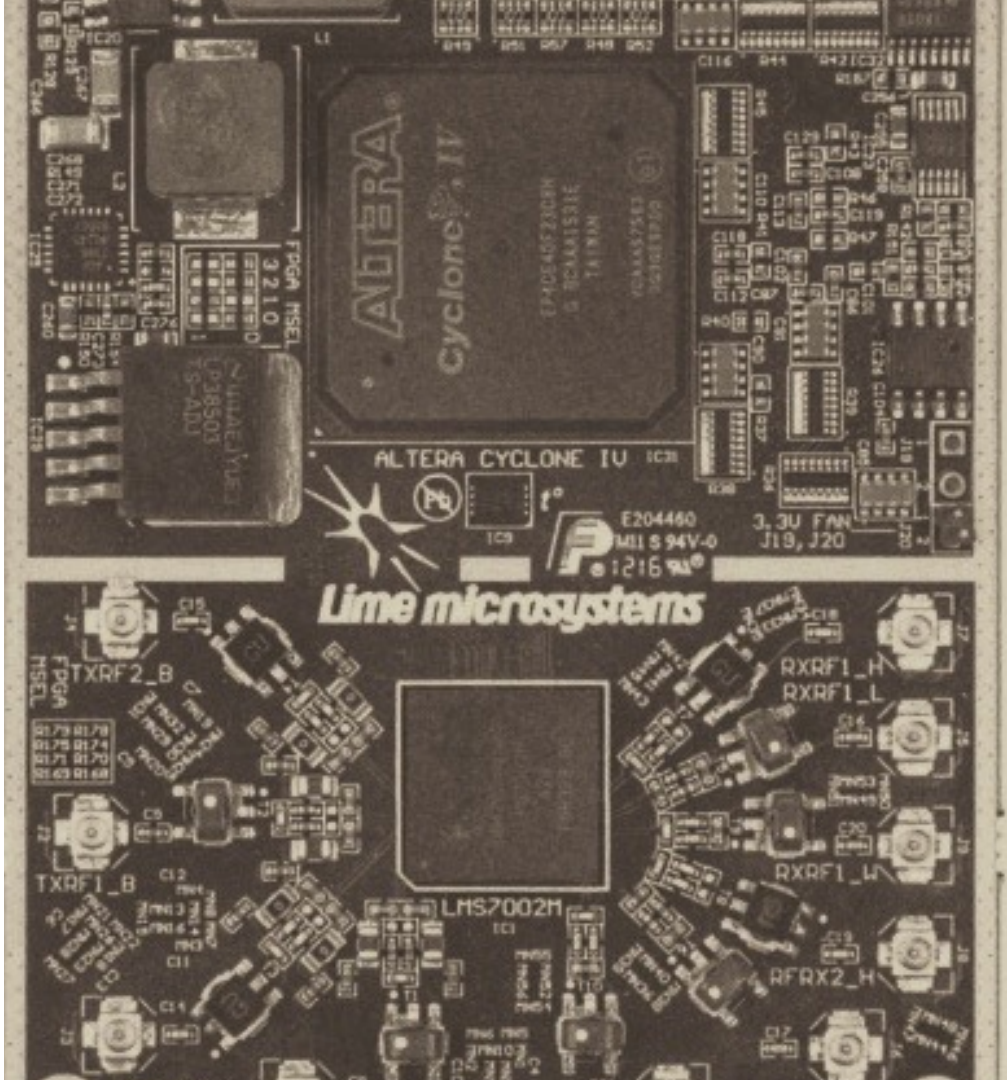


I/Q diagram



Oscilloscope (Time sink)

Boite à outils



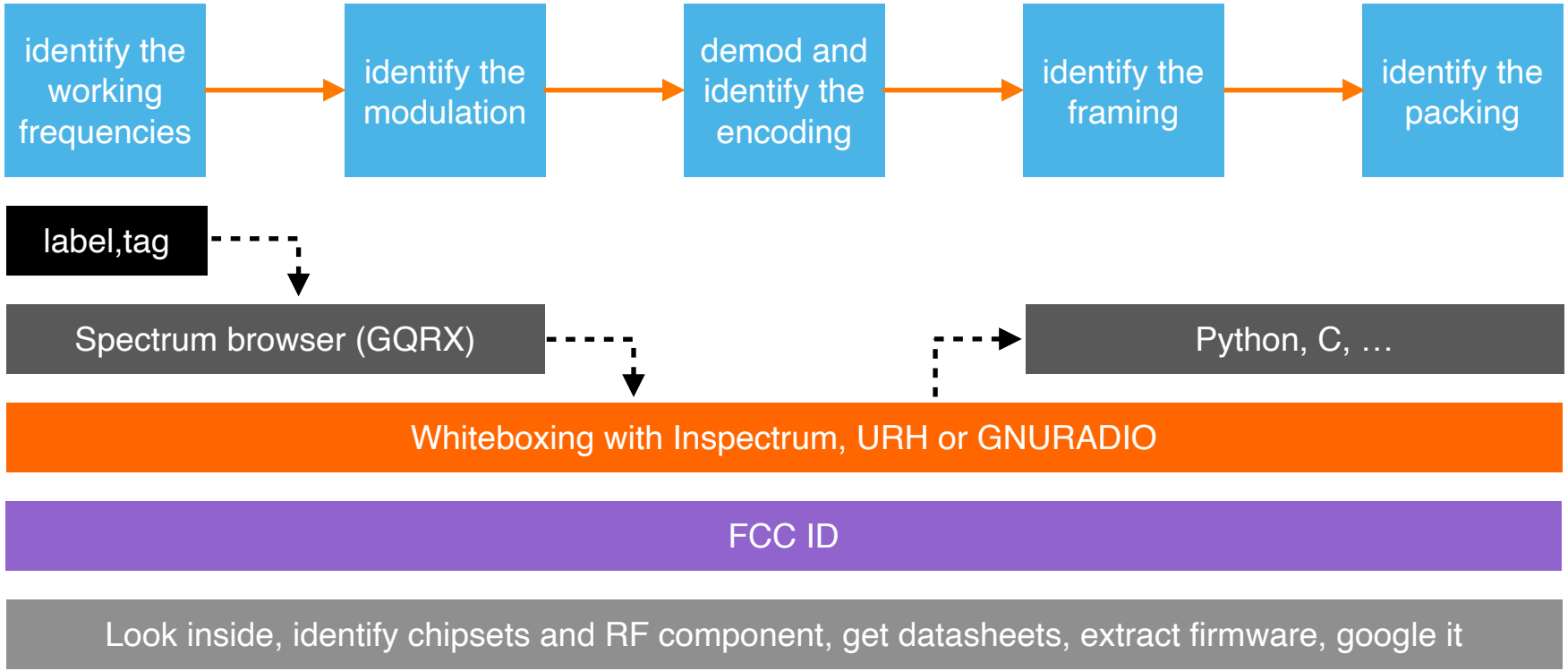
Echantillonnage
Boite à outils: exemples

Echantillonnage
Boite à outils: performances

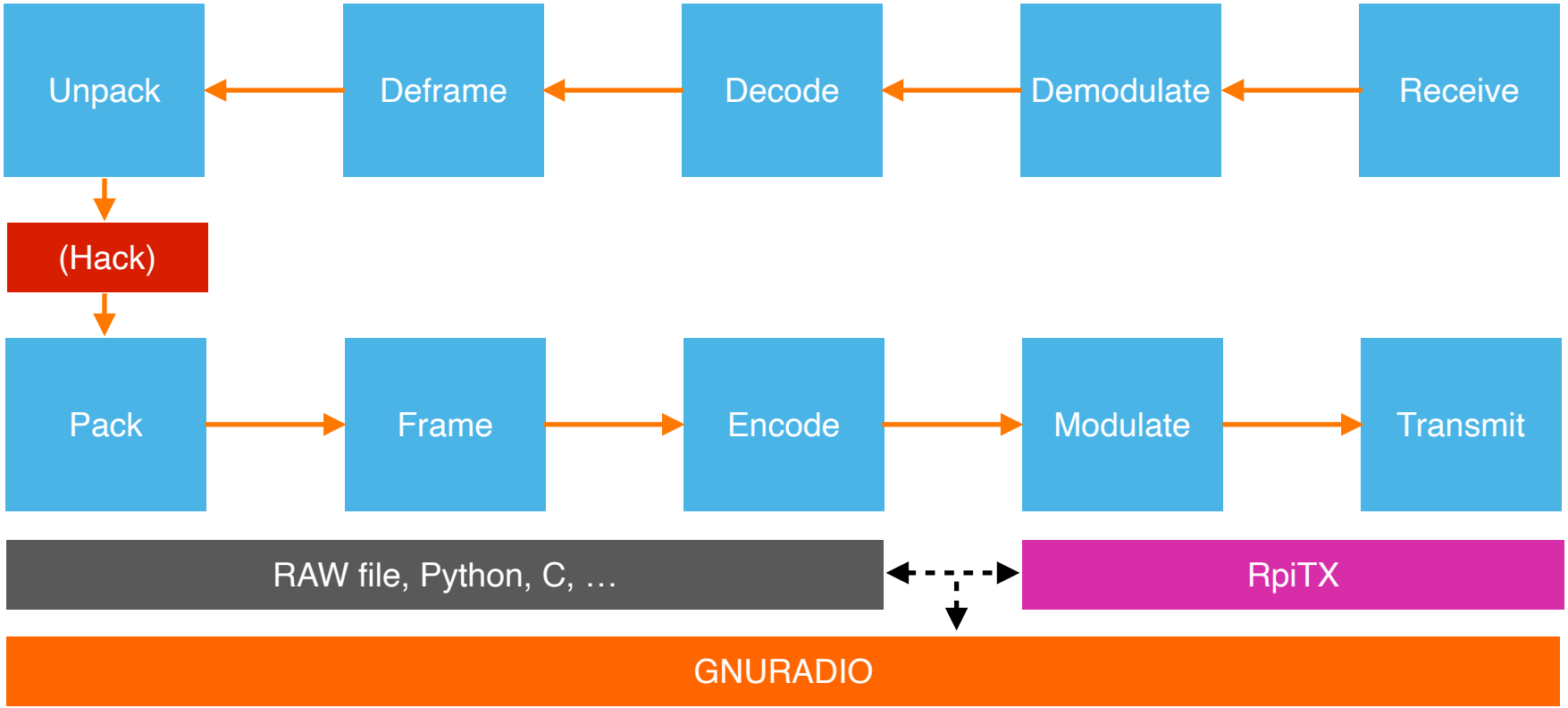
	HackRF One	Ettus B210	BladeRF x40	RTL-SDR	LimeSDR
Frequency Range	1MHz-6GHz	70MHz-6GHz	300MHz-3.8GHz	22MHz-2.2GHz	100kHz-3.8GHz
RF Bandwidth	20MHz	61.44MHz	40MHz	3.2MHz	61.44MHz
Sample Depth	8 bits	12 bits	12 bits	8 bits	12 bits
Sample Rate	20MSPS	61.44MSPS	40MSPS	3.2MSPS	61.44MSPS
Transmitter Channels	1	2	1	0	2
Receivers	1	2	1	1	2
Duplex	Half	Full	Full	N/A	Full
Interface	USB 2.0	USB 3.0	USB 3.0	USB 2.0	USB 3.0
Chipset	MAX5864, MAX2837, RFFC5072	AD9361	LMS6002M	RTL2832U	LMS7002M
Oscillator Precision	+/-20ppm	+/-2ppm	+/-1ppm	?	+/-1ppm initial, +/-4ppm stable
Transmit Power	15dBm @ 2.4GHz	10dBm+	6dBm	N/A	0 to 10dBm (depending on frequency)
Price	$299	$1,119	$420 ($650)	~$10	$299 ($289 pre-order)

Méthodes

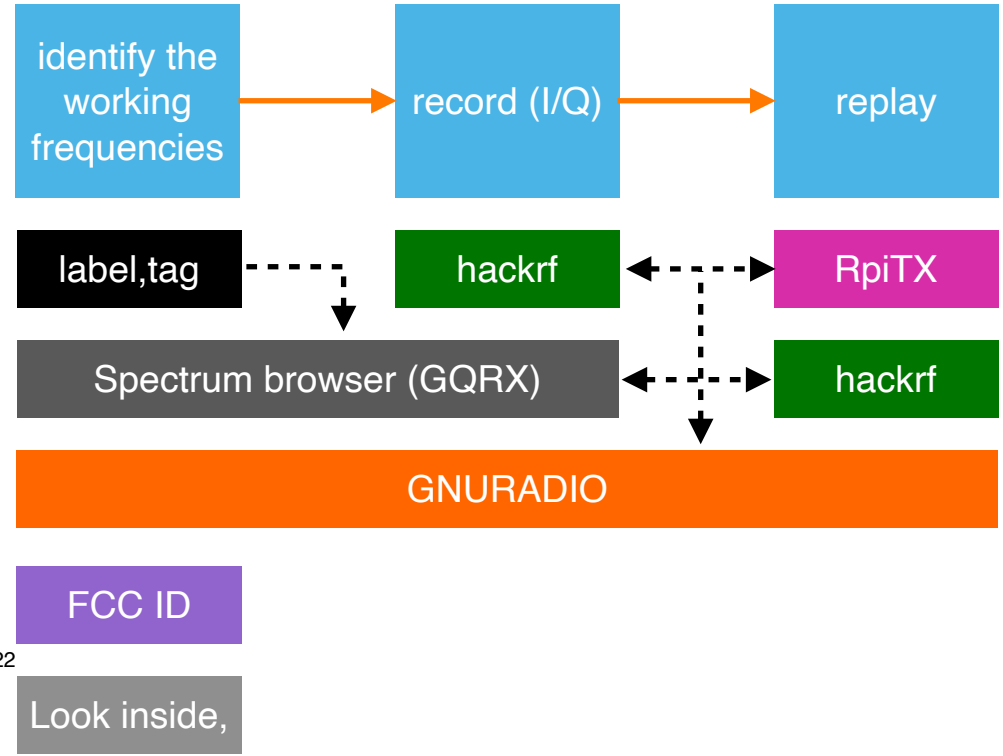
Radio HACKING
Méthode: écouter la cible



Radio HACKING
Méthode: parler à la cible



Radio HACKING
Méthode: simplifiée



I/Q format: complex 32-bit floating, complex 16-bit signed integer, complex 8-bit signed integer, complex 8-bit unsigned integer