

Initiation RTL-SDR et HackRF One

- 1 - La révolution du mode RTL-SDR en radio-communication
- 2 - Les possibilités radio avec une clé USB pour la TNT
- 3 - Comment hacker une clé TNT en radio scanner
- 4 - Démo et présentation du HackRF One
- 5 - Premier pas avec le HackRF sous Windows et Linux

Présentation de **F1JXQ**
Pour **Passion Radio Shop**

Au salon **Ond'Expo 2015**
28 mars 2015 – Espace Ecully Lyon



Le SDR ?

Software Defined Radio ou Radio Logicielle

- C'est utiliser un **logiciel pour gérer la partie réception et émission** de signaux radio (au lieu d'un matériel)
- Le SDR est par exemple utilisé niveau pro dans les stations de base en **téléphonie GSM**
- Il permet de réduire de manière importante l'investissement en matériel de radio-communication
- Il permet de bénéficier de la puissance d'un PC pour **traiter (presque) n'importe quel signal radio...**
- Une nouvelle activité **grand-public**, qui peut permettre de **re-dynamiser l'activité radioamateur**

La révolution RTL-SDR

Découvert en Mars 2010 par Eric Fry, rejoint par Osmocom et Antti Palosaari qui le popularisent en 2011/2012.

- Une simple clé USB pour recevoir la TNT à moins de **25 euros**
- Devient un véritable scanner radio large bande **HF, VHF et UHF**
- La clé TNT doit avoir le chipset **RTL2832U**
- Et le tuner **R820T, R820T2** (24 – 1766 Mhz sans trou), autres tuners compatibles



RTL-SDR pour radioamateur

en phonie les bandes **VHF, UHF** dans tous
s : **AM, FM, LSB USB**

e morse (CW) et tous les modes : **RTTY,**
TV, ROS, THOR, APRS, etc.

es bandes HF et ondes-courtes (avec un convertier)

si : analyseur de spectre, observer le
catter, chasse au renard, mesurer la SWR,
ballons, réception satellites et plus encore !

Autres application RTL-SDR

- Écoute des tours de contrôle et des avions
- Suivi des positions des avions et décodage **ADSB**
- Décodage des messages courts **ACARS**
- Suivi des bateaux et décodage **AIS**
- Écoute des **téléphones sans fil** et moniteurs de bébé
- Réception des capteurs, ex. capteur température sans fil
- Regarder la **TV analogique**
- Sniffer les **signaux GSM**
- Réception des signaux **GPS** et décodage
- Réception images satellites météorologiques **NOAA**
- L'écoute de satellites et de la station **ISS**
- **Radioastronomie**
- Écoute de la **radio FM**, et décoder les informations **RDS**
- Écoute de la **radio numérique DAB**
- **Reverse engineering** de protocoles radio inconnus
- **Triangulation** de la source d'un signal.
- Recherche de sources de bruit RF, **micro-espion**, etc.

Et plus encore !

Configurer une clé TNT en SDR

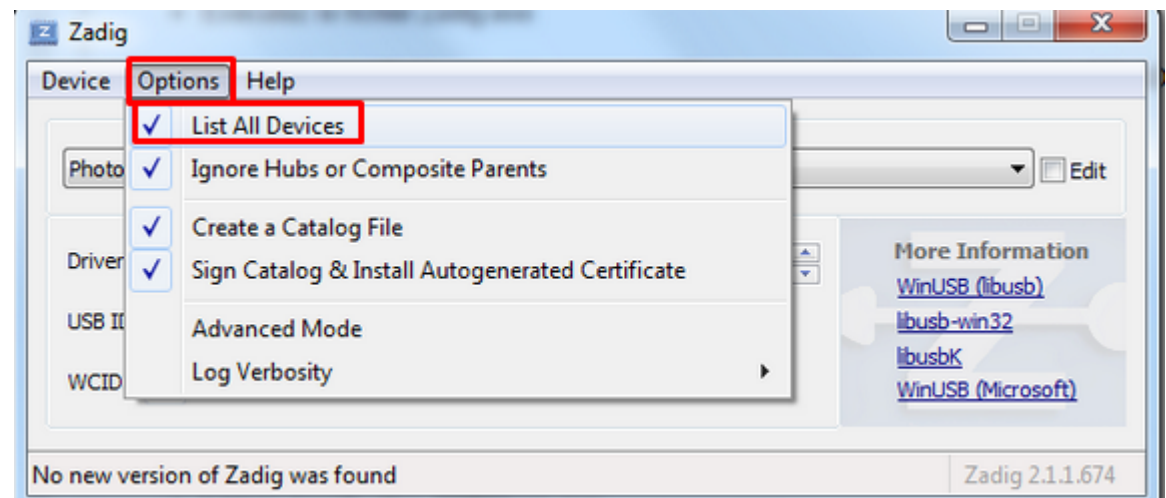
- 1 – N'installez pas les drivers automatiques de la TNT
- 2 – Branchez la clé USB TNT sur un port USB 2.0 et toujours sur le même
- 3 – Télécharger **Zadig** : <http://zadig.akeo.ie/>

4 – Lancer l'exécutable



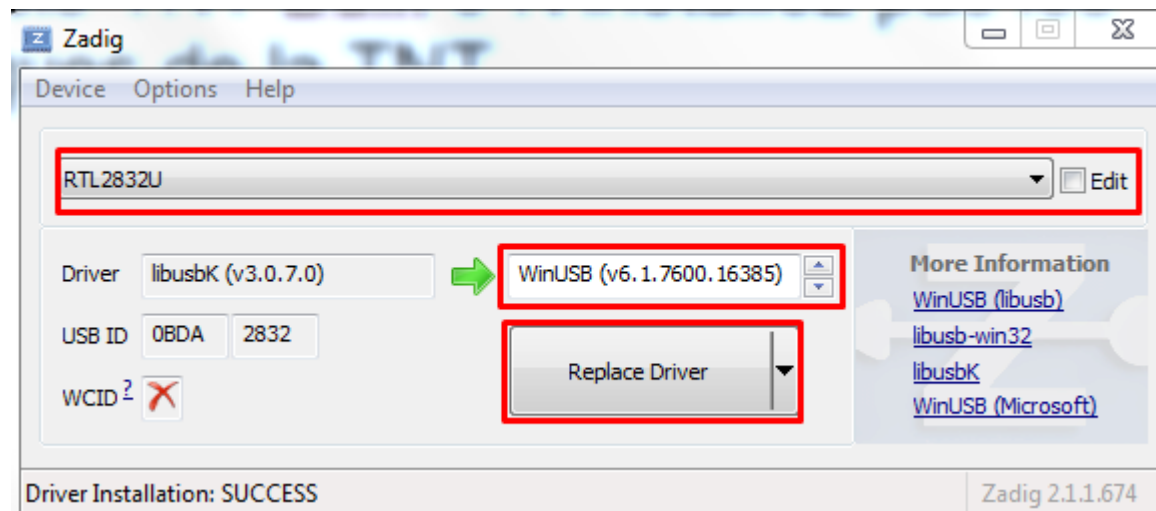
5 – Cocher

« List all devices »



Configurer une clé TNT en SDR

6 – Choisissez la clé TNT « Bulk-In, Interface 0 » ou RTL2832U puis cliquez « Replace Driver »

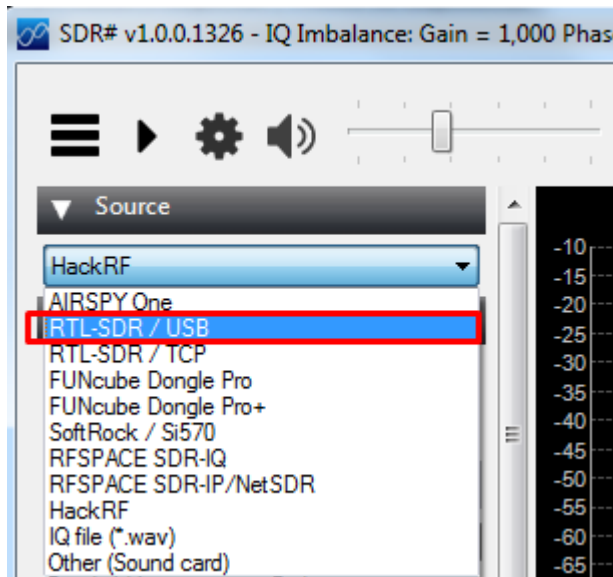


7 – Télécharger le logiciel Windows **SDRsharp**

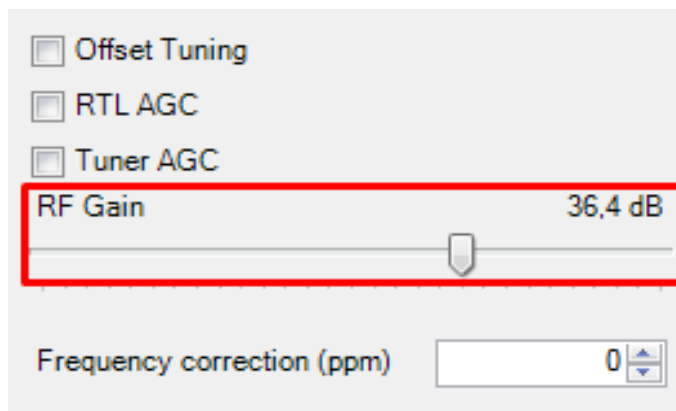
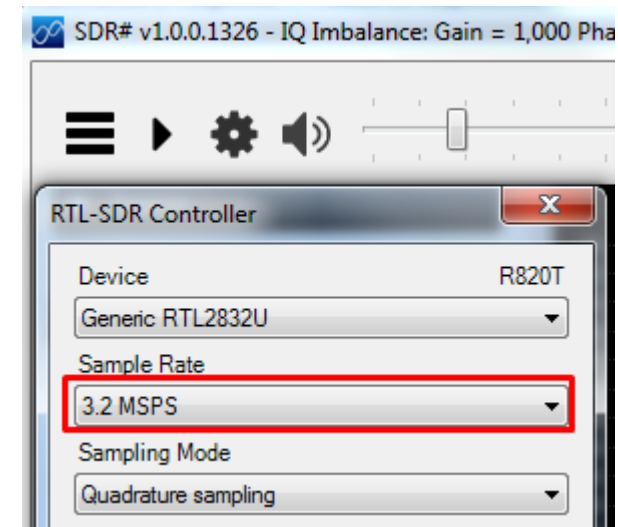
<http://sdrsharp.com/> ou **HDSDR** <http://www.hdsdr.de/>

Configurer SDRSharp

1 - Régler sur RTL-SDR / USB



2 - Choisir la largeur de bande à analyser / écouter



3 - Régler le gain en utilisant RF Gain

Prudence avec les réglages de gain, ne pas pousser tout à fond !

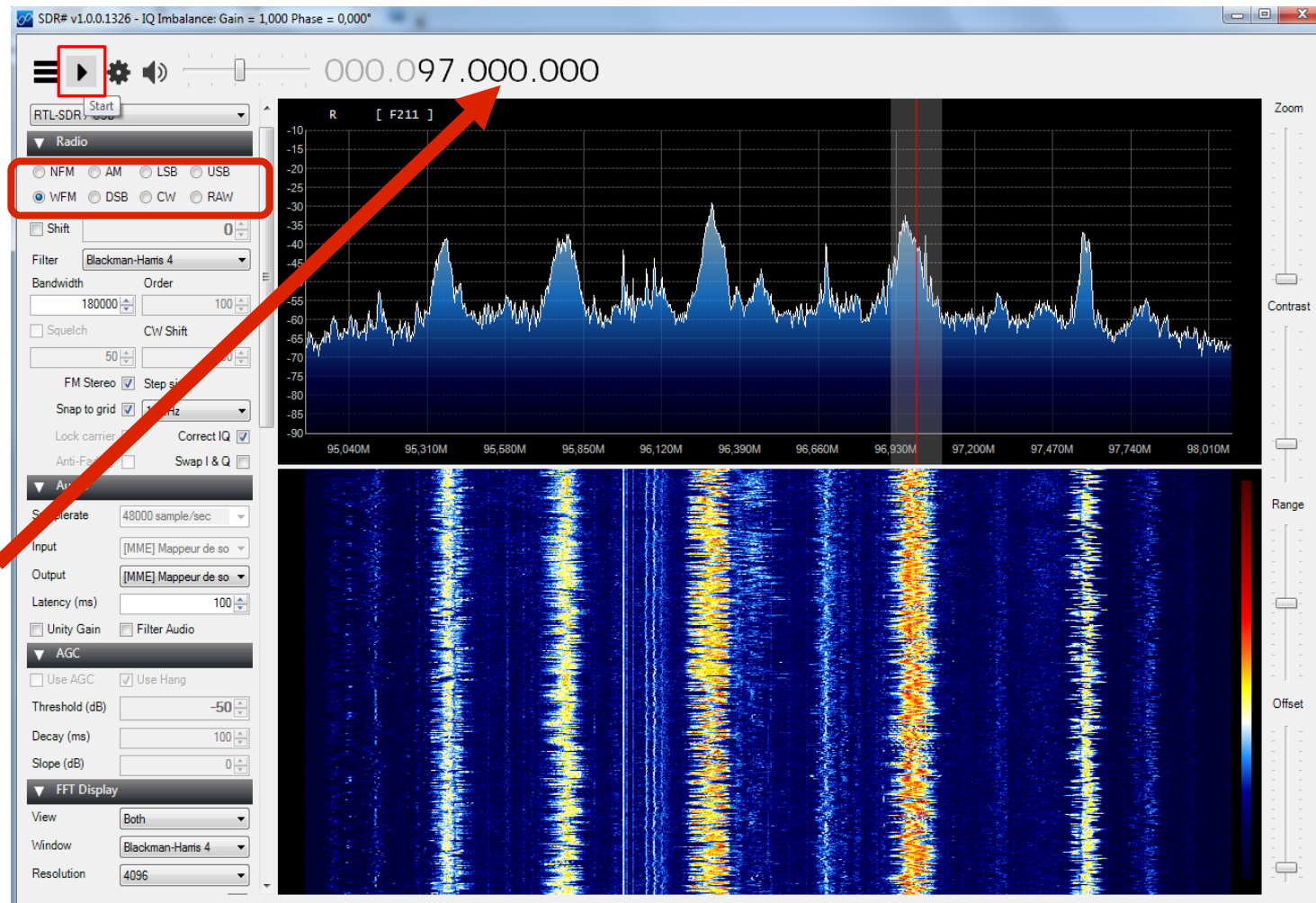
Utiliser SDRSharp

Commencer par tester la réception radio FM 88-108Mhz

Pour lancer la réception

Pour choisir le mode

Pour régler la fréquence

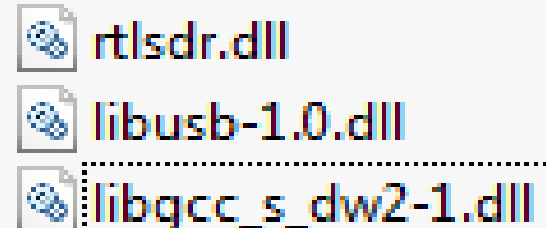


Ajouter (quelques) les bandes HF

Solution #1 (gratuite) par logiciel :

Télécharger le driver RTL-SDR, extension de 13Mhz à 1820Mhz : <https://db.tt/0JuVpWBL>

Dézipper le contenu de l'archive à la racine du répertoire d'installation de SDRsharp et remplacer les 3 fichiers DLL :

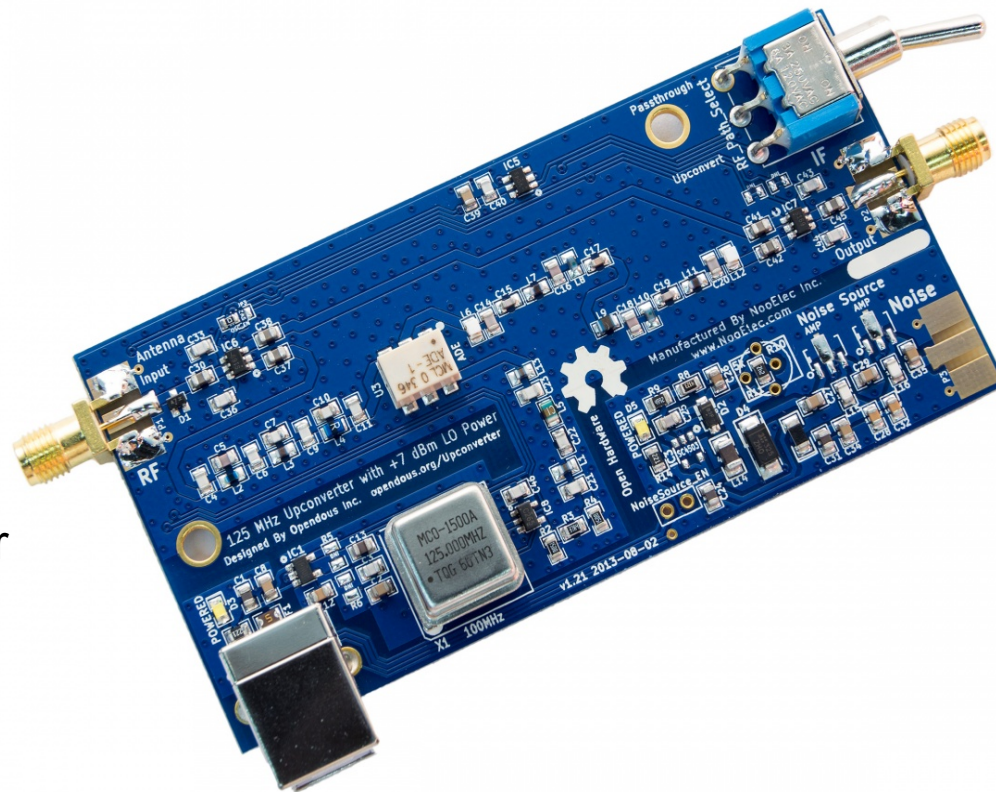


Ajouter les bandes MF et HF

(0.5 à 50Mhz) en RTL-SDR

Solution #2 par matériel (payant) avec la convertir **Ham it Up** (59€) à brancher sur la clé TNT avec un câble MCX <->SMA

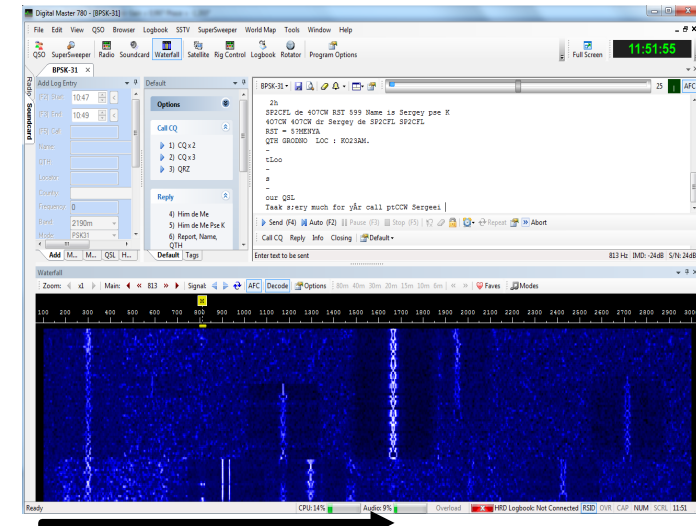
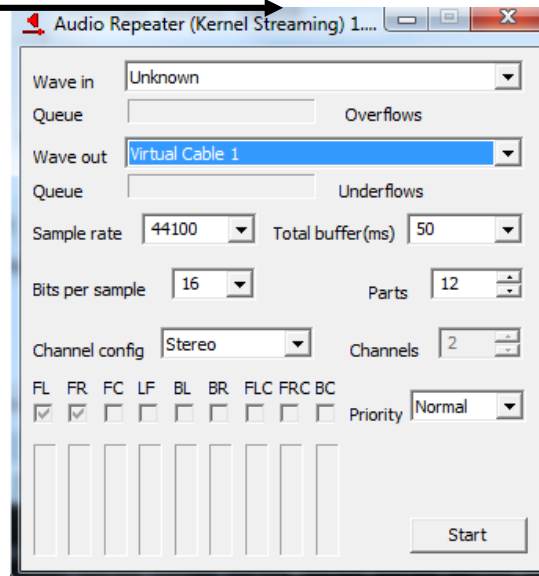
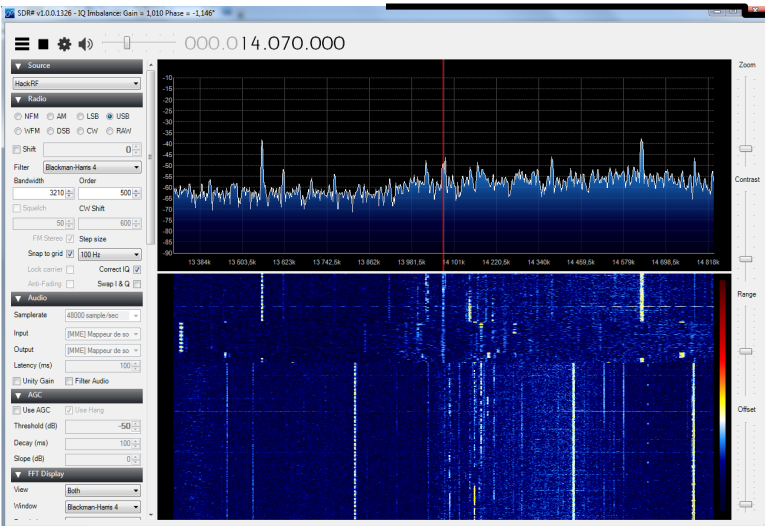
Vers une antenne externe **ET** accordée sur la bande à écouter



Vers la clé USB TNT ou le HackRF, puis écouter à partir de 125Mhz qui devient le point 0,500Mhz de la bande HF

Décoder avec SDRsharp et HRD

Installer un câble audio virtuel : <http://software.muzychenko.net/eng/vac.htm>



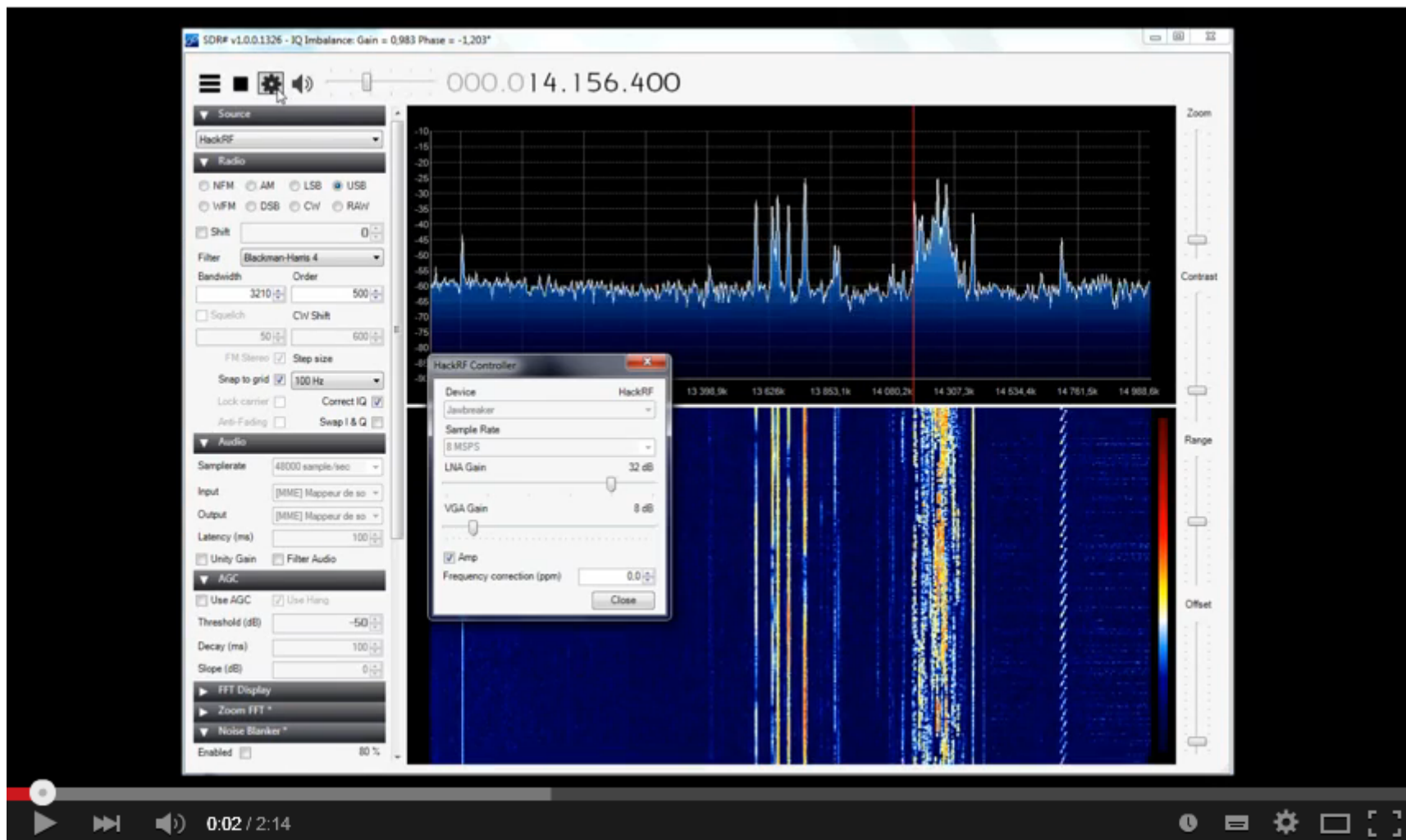
HackRF One

- Réception et émission de 10Mhz à 6Ghz
- Jusqu'à 20Mps de bande passante à l'écran
- Puissance de 3mW à 30mW
- Compatible avec le converter Ham it up 0.5 à 50Mhz réception et émission !



HackRF One avec SDRcharp

Réception en phonie SSB sur la bande des 20 mètres (14Mhz)
HackRF est « plug and play » avec #SDRCharp, seul le gain est à régler
https://www.youtube.com/watch?v=6tP_m497mU4



HackRF + #SDR + VAC + HRD

Décodage PSK31 avec SDR, un câble audio virtuel (VAC) et Digital Master 780, sous Windows : <https://www.youtube.com/watch?v=zfe2GI74ezw>

The screenshot displays the Digital Master 780 software interface, which is used for digital signal processing and decoding. The main window is titled "Digital Master 780 - [BPSK-31]". The interface is divided into several sections:

- Top Panel:** Contains a menu bar (File, Edit, View, QSO, Browser, Logbook, SSTV, SuperSweeper, World Map, Tools, Window, Help) and a toolbar with icons for various functions. A digital clock shows "11:49:30".
- Left Panel:** Features an "Add Log Entry" section with fields for "PSK Start", "PSK End", "PSK Call", "Name", "QTH", "Locator", "Country", "Frequency", "Band", "Mode", "Serv", "Flow", and "Flow". Below these are "Add (F7)", "Reset (F4)", and "Add M...", "M...", "QSL H..." buttons.
- Center Panel:** Contains "Options" (Call CQ, Reply, Info, Closing) and "Info" sections. The "Call CQ" section lists "1) CQx2", "2) CQx3", and "3) QRZ". The "Reply" section lists "4) Him de Me", "5) Him de Me Pse K", "6) Report, Name, QTH", and "7) Station". The "Info" section lists "8) MFSK Picture".
- Right Panel:** Displays a terminal window with the following text:

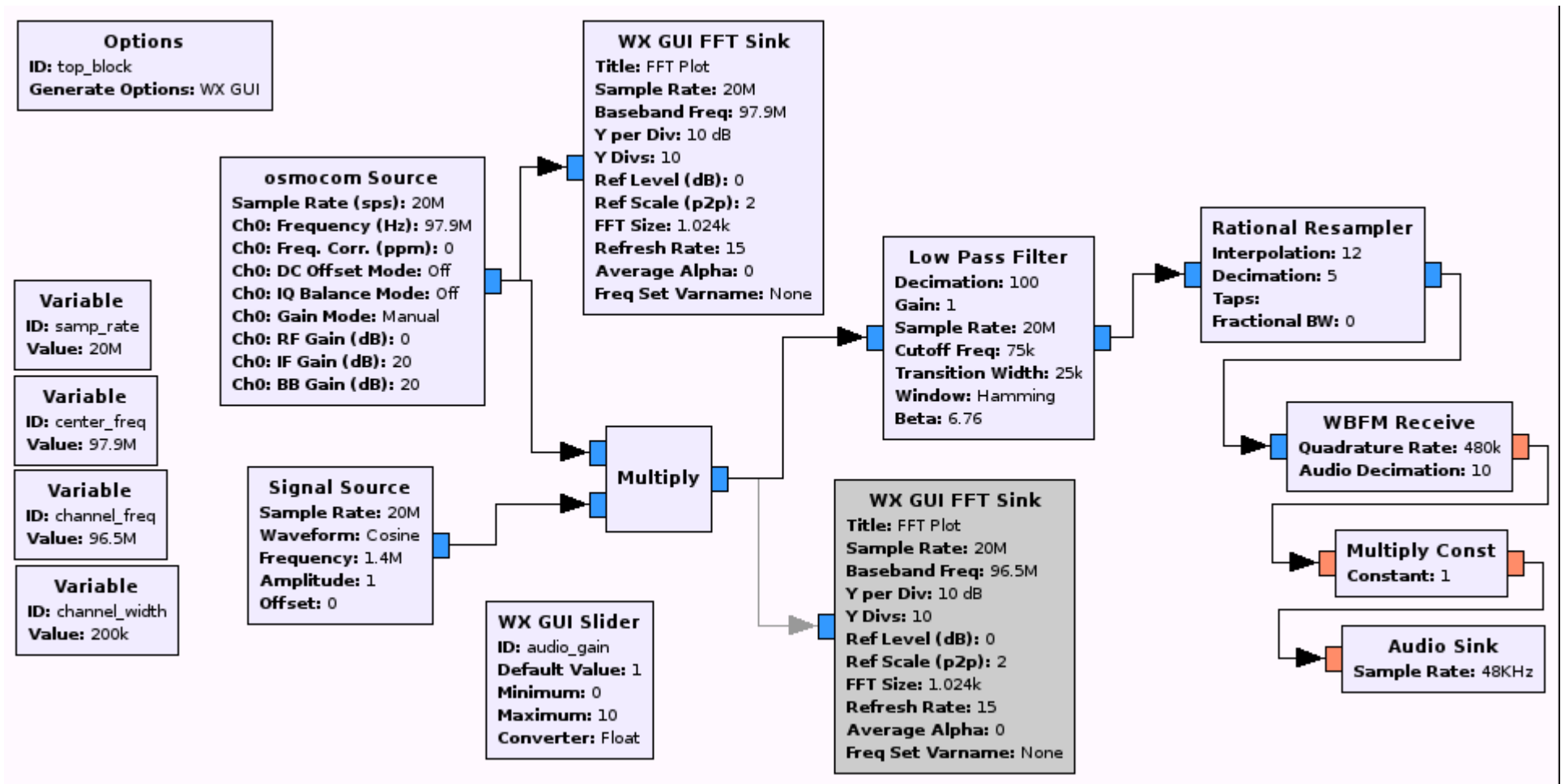
```
11:47:20> Main
FTX .....: Ham Radio Deluxe
FTX .....:
Input ....: Line 1
Output ...: Realtek High Definition Audio

11:47:20> Main
CQ
Q be2de En S12ee/4 EAS1JF/4 EAS1JF/4 CQ K
CQ CQ CQ de EAS1JF
```
- Bottom Panel:** Shows a "Waterfall" display with a frequency axis from 100 to 3000 kHz. A signal is visible at approximately 1295 kHz. A yellow box highlights the decoded text: "h2Eae atm te fa-a", "aa l11el aH a ahtl l eD aea etl l Va a-a a a", and "x1 eD a".
- Status Bar:** Displays "Ready", "CPU: 12%", "Audio: 10%", "Overload", "HRD Logbook: Not Connected", "PSD", "OVR", "CAP", "NUM", "SCRL", and "11:49".

The video player interface at the bottom shows a progress bar at 0:51 / 1:57 and standard playback controls.

HackRF avec GNU Radio (Linux)

Pentoo ou Kali + GNU Radio + GRC assistant graphique
pour créer les scripts (à voir les tutos de [F4GMU](#))



Le SDR vous intéresse ?

Suivez nous !



Le blog : <http://www.passion-radio.org/>

La boutique : <https://www.passion-radio.com/>

Twitter : @radioamateur et @F1JXQ

Facebook, Youtube et Slideshare