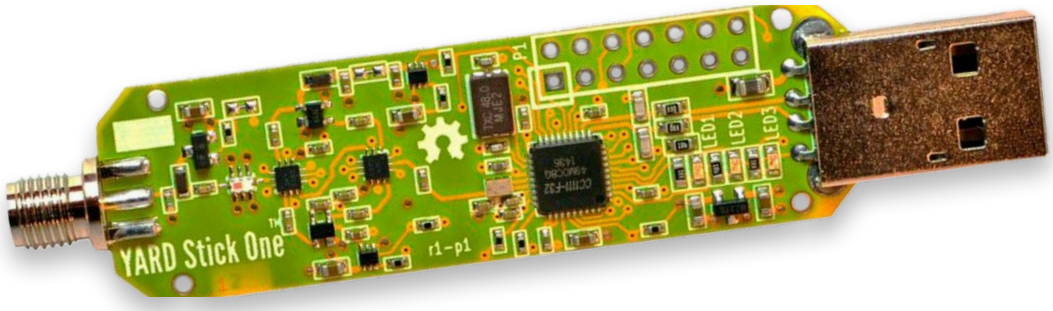
le YARD Stick One

un outil de test sans fil pour les fréquences allant jusqu'à 1 GHz



Wim Ton (Irlande)

Le YARD Stick One est une « radio matérielle » compacte capable d'émettre et de recevoir dans la bande UHF. Il s'agit d'une sorte de carte d'interface USB qui permet de l'utiliser avec des hôtes tels que les PC et les cartes Raspberry Pi. Le YARD Stick One est livré avec un logiciel USB préchargé dans son noyau 8051. La radio est contrôlée avec quelques douzaines de registres de configuration, mais le *middleware* intermédiaire Python permet de résumer de nombreux détails.

L'avantage principal du YARD Stick One de Great Scott Gadgets est qu'il s'agit de l'un des appareils les moins chers (comparé au HackRF [1] ou au LimeSDR [2]), qui peut également émettre et est prêt à l'emploi, alors que les appareils courants et bon marché tels que les dongles RTL SDR ne fonctionnent qu'en réception.
Comme toutes les fonctions de bas niveau sont réalisées par une puce CC1111 [3], l'utilisation de la radio consiste à écrire correctement les registres de configuration. Le CC1111 est destiné aux protocoles complexes de *Layer* 2, avec des fonctions telles que la synchronisation de mots, le cadrage, l'entrelacement et l'embrouillage. Le CC1111 étant un SoC pour les applications RF commerciales, l'utilisation du YARD Stick One pour l'analyse des signaux est très limitée. À moins que le système testé n'utilise un SoC similaire, il est moins frustrant et moins coûteux d'utiliser un SDR.
Le YARD Stick One n'est pris en charge que par *rfcat*, un *middleware* basé sur Python qui résume les options les plus utilisées dans une sorte de méthodes descriptives. Pour un réglage plus fin, *rfcat* offre également un accès brut aux registres.
Tel qu'il est livré, l'appareil est une carte nue et doit être traité avec le soin nécessaire. Des boîtiers provenant d'autres fournisseurs sont disponibles.
Le terme « sub-1 GHz » est un peu large ; le YARD Stick One est limité par son microcontrôleur radio TI CC1111, qui couvre les bandes ISM UHF inférieures de 300 à 928 MHz. La bande 13,56 MHz, utilisée pour la RFID notamment, n'est pas couverte.
Le YARD Stick One fonctionne de manière un peu plus stable sous Linux que sous Windows 10. Windows ne reconnaît souvent pas du tout le dongle, mais vous pouvez vous en sortir en le débranchant et en le réinsérant à plusieurs reprises sous Linux.

Installation du logiciel

L'utilisation du YARD Stick One nécessite une bonne compréhension des couches OSI 1 et 2. Une certaine connaissance de Python et une familiarité avec le système d'exploitation prévu sont également bénéfiques pour résoudre les problèmes d'installation. Le logiciel recommandé dans sur l'e-choppe Elektor [4] a été installé sur Windows 10, Kali et Ubuntu 18.
L'installation de *rfcat* [5] sur Linux avec Python 3.10 a bien fonctionné. La seule différence par rapport à la documentation est que *rfcat* doit être démarré avec la commande :

```
./rfcat
```

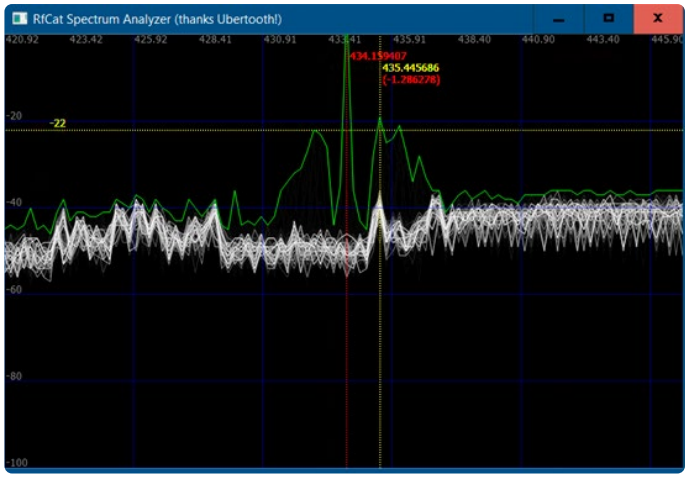


Figure 1. Affichage du spectre Rfcat.

Si vous obtenez un message « Error in resetup() », débranchez et réinsérez la carte.
Windows 10 : N'installez pas Python via Microsoft Store, car cela perturbe les autorisations de fichiers ; installez-le manuellement pour tous les utilisateurs. En plus, vous devez entrer :

```
pip install Cython
```

Dans tous les cas, installez avec les privilèges d'administrateur (vérifiez où les instructions Linux requièrent `sudo`). Et installez une version (MSVC) > 14.
Un ajustement est nécessaire si vous obtenez un message d'erreur à propos de « collections not callable » : ajouter `.abc` dans *C:\Program Files\Python310\Lib\site-packages\pyreadline\py3k_compat.py* sur la ligne 8 :

```
return isinstance(x, collections.abc.Callable)
```

le package *pyreadline* n'est requis que pour Windows uniquement. Installez le pilote *libusb-win32*. Le moyen le plus simple est probablement d'utiliser *Zadig* [6], qui est généralement fourni avec *SDR#*. Si le périphérique est absent, vous obtenez l'exception « No Dongle Found » de *rfcat*. En cas d'exception « ChipconUsbTimeoutException », débranchez et réinsérez le dongle. Dans l'ensemble, l'installation et l'utilisation sous Windows 10 sont un peu plus délicates que sous Linux. Il est obligatoire d'appeler `setmodeIDLE()` à la fin du script, sinon une erreur « device not found » se produira au prochain démarrage.

Le microcontrôleur utilisé dans le CC1111 est une variante MCS51 et nécessite le compilateur SDCC (Small Device C Compiler) [7] version 3.5 ou inférieure. Il nécessite un travail manuel lors de l'installation, car la version actuelle est 4.x. Cependant, de nombreux utilisateurs se contenteront d'utiliser le micrologiciel *rfcat*.

Utilisation du YARD Stick One

La puce radio CC1111 fait tout le travail de bas niveau, ajoutant et supprimant les pré- et post-ambules, les mots de synchronisation, le CRC, ainsi que la modulation et la démodulation. La radio doit être entièrement configurée avant d'être utilisée, car la configuration de réinitialisation est inutile. L'écriture d'un petit programme Python tel que décrit dans [8] permet d'économiser du temps de saisie et des erreurs.
Rfcat est également équipé d'un afficheur de spectre. Le qualifier d' « analyseur » est un peu exagéré, la plupart des appareils plus rudimentaires ont une largeur de bande et une plage dynamique limitées, contrairement aux équipements obsolètes tels que le HP141 ou le HP181, qui peuvent afficher une largeur de bande de 1 GHz avec une plage dynamique de 80 dB.
Pour utiliser le YARD Stick One comme récepteur, les propriétés des couches 1 et 2 doivent être configurées correctement, sinon la radio ignorera le paquet. Pour analyser un signal inconnu, une radio SDR supplémentaire est nécessaire, et le matériel le moins cher pour cela sont les dongles RTL. Outre l'utilisation de GNU Radio et d'Audacity comme indiqué dans [9], Universal Radio Hacker [10] fournit un flux de travail plus intégré pour l'analyse et la relecture des signaux. Alternativement, le réglage de la puce radio appairée peut être récupéré à partir de l'interface matérielle si le type de puce est connu, comme illustré dans [11].
L'utilisation du YARD Stick One comme récepteur générique est assez délicate : lorsque les réglages sont trop basiques, beaucoup de bruit se retrouve en réception, et avec des réglages trop précis, tout est filtré. Cela pourrait fonctionner avec un atténuateur variable à l'entrée, mais je n'en avais pas sous la main.
Pour faciliter la configuration des nombreux registres du CC1111, l'utilitaire SmartRF Studio de TI [12] est très utile. Les valeurs calculées peuvent être écrites sur le YARD Stick One avec la fonction `setXxx(value)` appropriée.

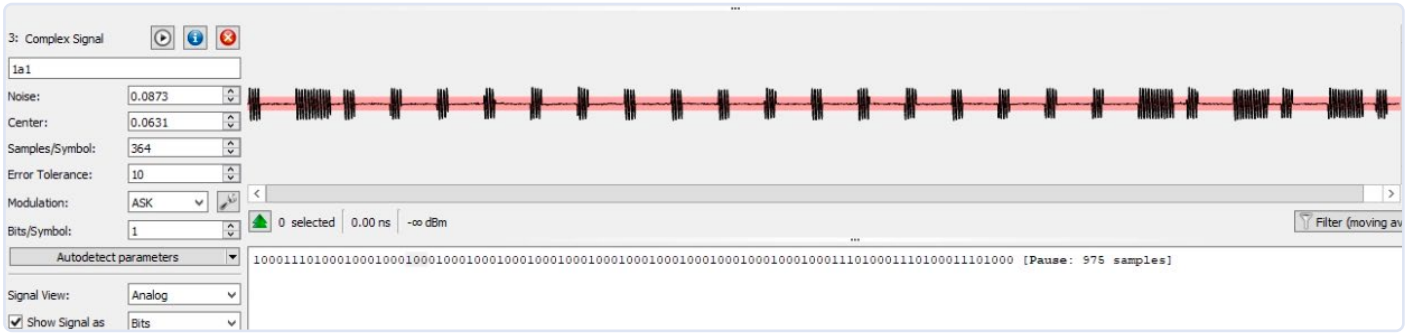


Figure 2. Visualisation du symbole.

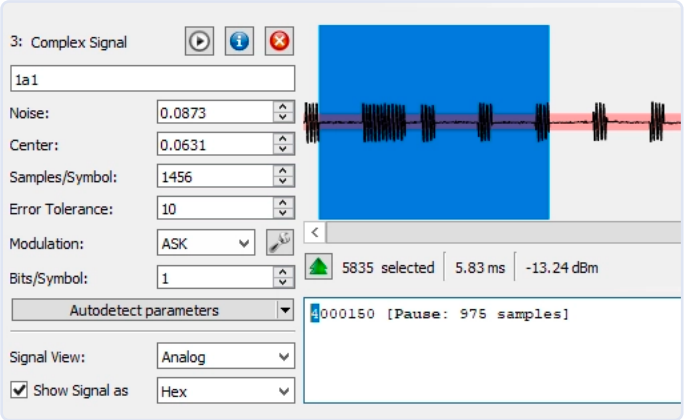


Figure 3. Visualisation des données.

Le *firmware* livré avec le YARD Stick One dans l'e-choppe Elektor agit comme un pont entre les registres du CC1111 et l'interface USB. Après une exception Python, le YARD Stick One doit être débranché et réinséré, sinon la *rflib* ne le trouve plus. L'exemple suivant montre un signal PWM avec modulation ASK, ce qui est très courant pour les télécommandes simples. Les captures d'écran proviennent de URH.

Chaque bit de données se compose de quatre symboles, un 0 est transmis sous la forme 1000 et un 1 sous la forme 1110, ce qui doit être envoyé au YARD Stick One sous la forme `8e88888888888888888e8e8e8`. Un symbole dure 0,484 ms, le débit en bauds doit donc être réglé sur 2744.

Documentation

La documentation [4] fournie par l'e-choppe Elektor est très succincte. Le forum indiqué par Great Scott Gadgets est d'une utilité limitée. Le dépôt *git rfcat* donne beaucoup d'informations sur la construction et le téléchargement du firmware du YARD Stick One. Il y a quelques tutoriels sur Internet, voir par exemple [13]. Veuillez vous conformer à la règlementation locale pour la bande ISM.

Verdict

Le YARD Stick One n'est pas bon marché pour ce qu'il offre et sa phase d'apprentissage est plutôt difficile. Le logiciel n'est pas parfait et la documentation est un peu légère. Pour l'analyse uniquement, un simple récepteur SDR est un bien meilleur choix. Pour la transmission, vous avez un transceiver SDR générique pour 150 € de plus (par exemple, HackRF One ou Adalm Pluto).

Le YARD Stick One peut être utile si vous vous concentrez sur les protocoles spécifiques supportés par cette famille de SoCs radio (voir IM-Me [14] comme mentionné sur le site Elektor). Pour des applications dédiées, on peut envisager une carte d'interface CC111x [15] de Chine connectée à un Arduino, ce qui évite la communication USB peu pratique.

VF : Laurent Rauber — 230388-04

Questions ou commentaires ?

Contactez Elektor (redaction@elektor.fr).

Produits

- **Great Scott Gadgets YARD Stick One – Outil de test sans fil sub-1 GHz**
  https://elektor.fr/20088
- **Great Scott Gadgets radio logicielle HackRF One (1 MHz à 6 GHz)**
  https://elektor.fr/18306
- **Great Scott Gadgets GreatFET One Universal USB**
  https://elektor.fr/19114
- **Kit Raspberry Pi RTL-SDR d'Elektor**
  https://elektor.fr/19518

LIENS

[1] Denis Meyer, "HackRF One SDR Transceiver," elektormagazine.com: https://elektormagazine.com/news/hack-rf-one-sdr-transceiver
[2] Jan Buiting, "LimeSDR Mini," elektormagazine.com: https://elektormagazine.com/news/digital-tv-transmitter-based-on-raspberry-pi-zero-and-limesdr-mini
[3] CC1110Fx / CC1111Fx fiche technique: https://ti.com/lit/gpn/cc1110-cc1111
[4] YARD Stick One logiciel et documentation: https://github.com/greatscottgadgets/yardstick
[5] RfCat GitHub: https://github.com/atlas0fd00m/rfcat
[6] Zadig: https://zadig.akeo.ie/
[7] SDCC: http://sdcc.sourceforge.net/
[8] YARD Stick One notes: https://bit.ly/3ql6mjo
[9] Tout pirater avec la RF et la radio logicielle- Part 1: https://bit.ly/3qpIGuI
[10] Piratage radio universel: https://github.com/jopohl/urh
[11] Analyse des communications radio à l'aide de RfCat: https://bit.ly/42kxvAj
[12] SmartRF Studio de Texas Instruments: https://ti.com/tool/smartrftm-studio
[13] Tout pirater avec la RF et la radio logicielle - Part 2: https://bit.ly/43ITm5D
[14] Analyseur de spectre de poche à 16$: https://ossmann.blogspot.com/2010/03/16-pocket-spectrum-analyzer.html
[15] Carte d'interface pour CC111x: https://www.aliexpress.com/item/32963409008.html