**Guide : Bluetooth LE Sniffing (Interception) avec Dongle nRF52840**

# Introduction

Ce document montre comment configurer le dongle nrf52840 pour réaliser de l’interception de paquets BT entre un dispositif centrale et un périphérique, qui seront ici considérés comme un portable avec l’Application Voltcraft SEM6000 et une prise pour mesure de consommation énergétique Voltcraft SEM6000.

# Prérequis :

* Dongle nRF52840 ou nRF52840 DK
* Prise Voltcraft SEM6000
* App Voltcraft SEM6000 sur un portable
* Wireshark v3.4.1 ou postérieur
* Python v3.6 ou postérieur (v3.9.8 recommandée)
* nRF Connect for Desktop ([Télécharger](https://www.nordicsemi.com/Products/Development-tools/nRF-Connect-for-Desktop/Download#infotabs))

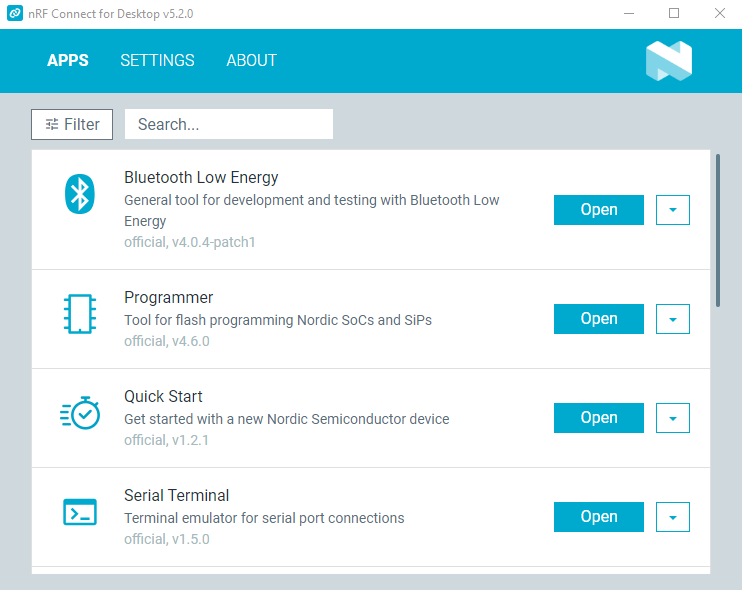
# Installation

Télécharger le firmware [nRF Sniffer for Bluetooth LE](https://www.nordicsemi.com/Products/Development-tools/nrf-sniffer-for-bluetooth-le/download#infotabs) v4.x ou postérieur et extraire les fichiers dans un dossier de votre choix. Dans les sections suivantes, ce dossier sera référencé comme *Sniffer\_Software.*

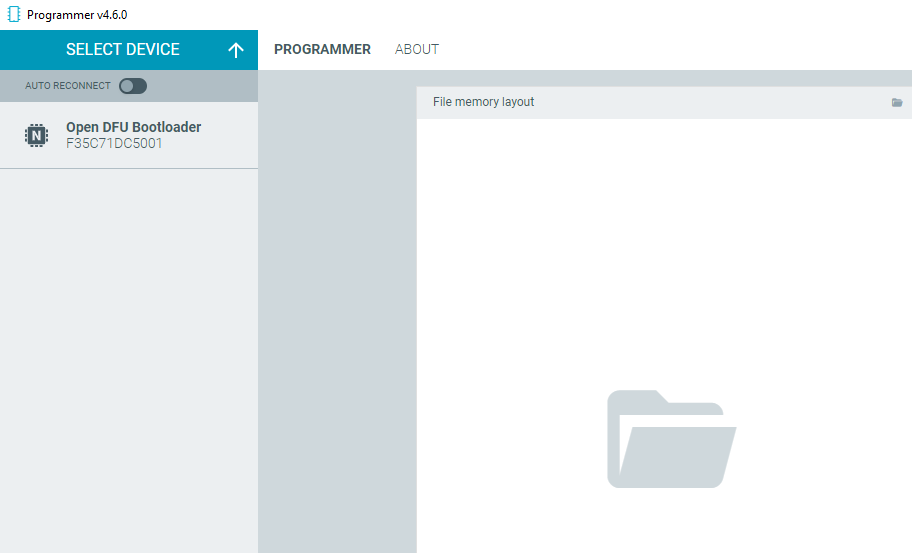
# Programmer le Dongle

Brancher le nRF52840 Dongle ou DK au PC et ouvrir le logiciel nRF Connect for Desktop, puis suivez les étapes :

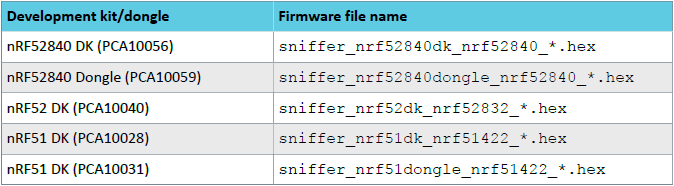
Ouvrir l’outil « Programmer »

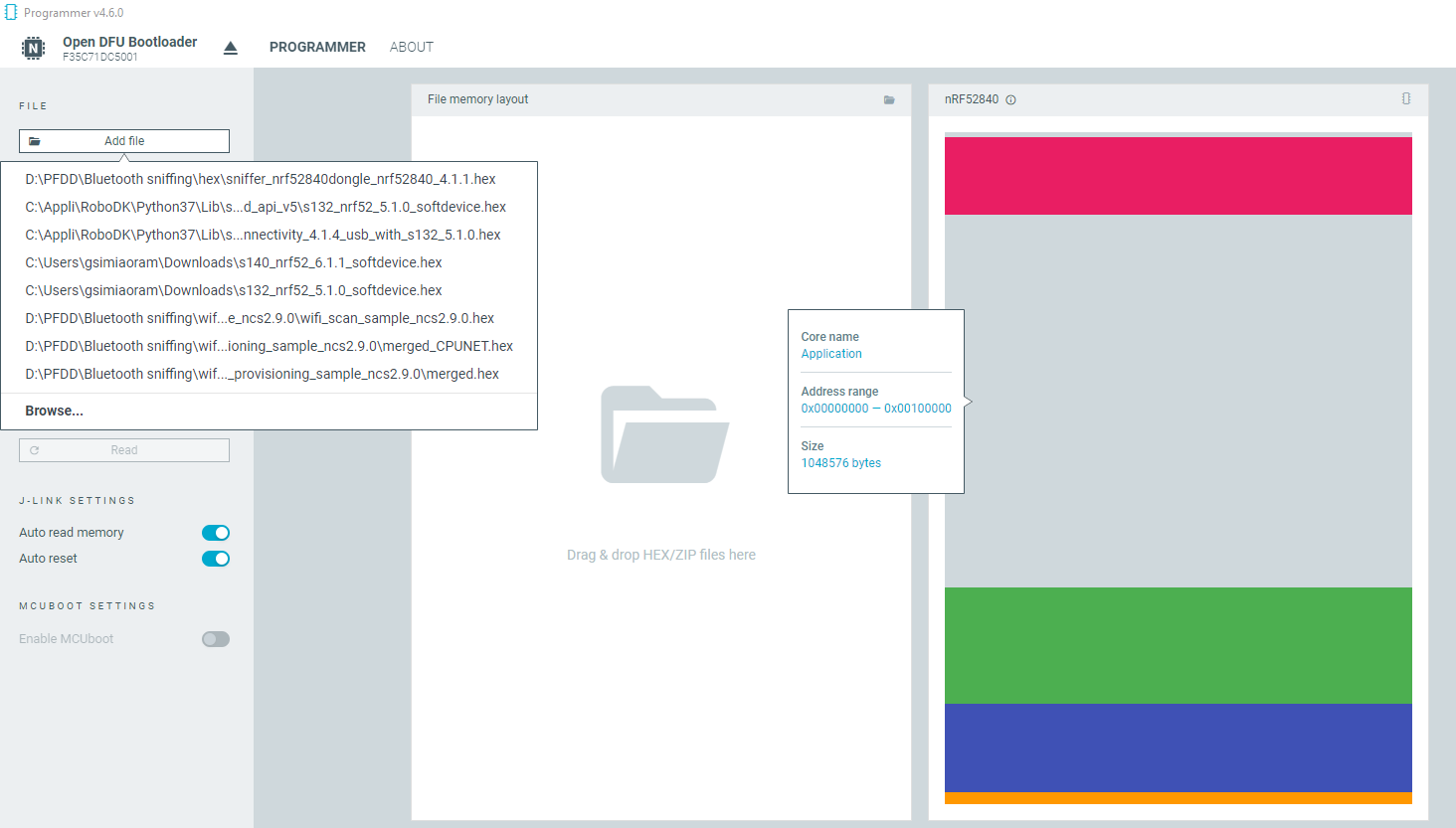


Sélectionner le dispositif dans la liste en haut à gauche

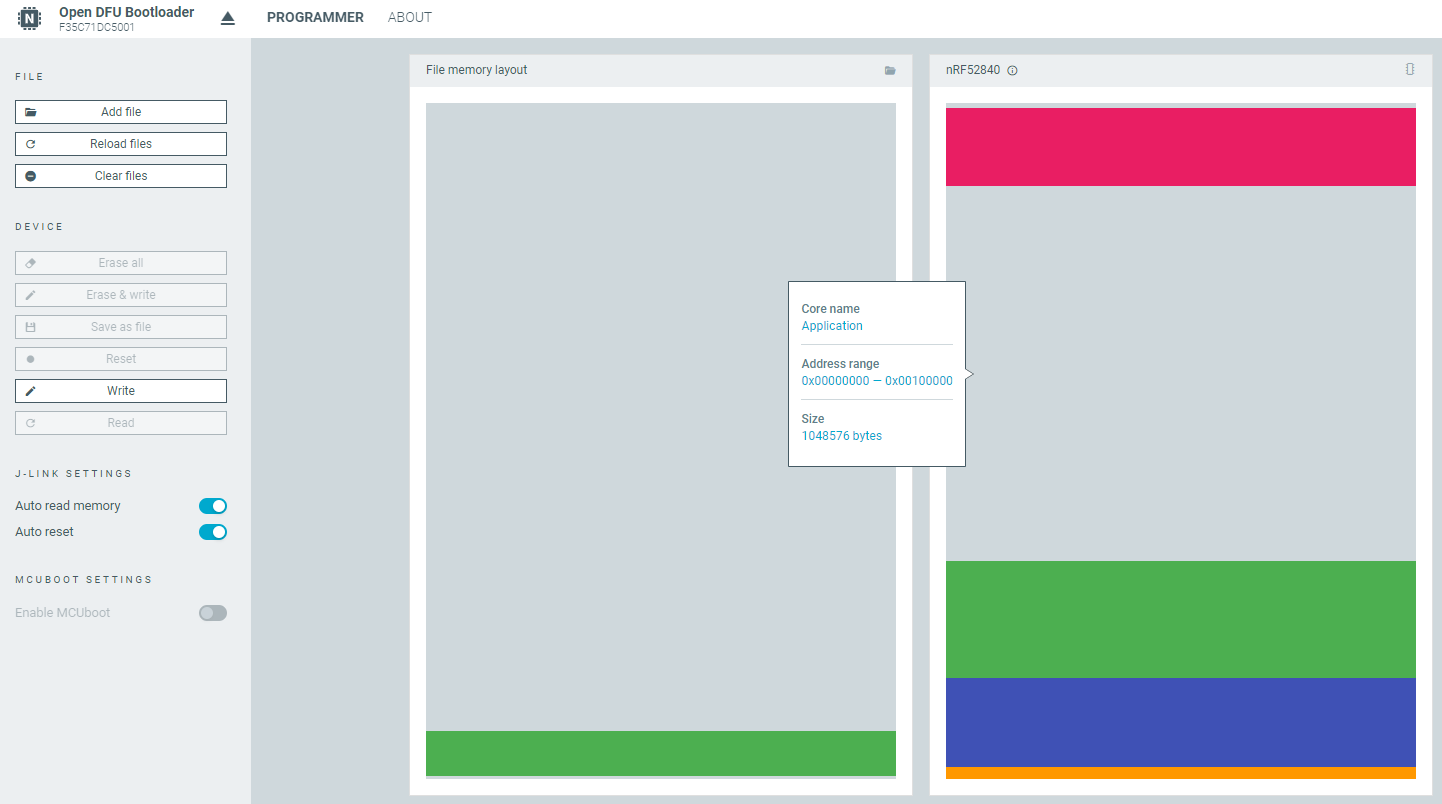


Puis, cliquer sur « Add file », faire « Browse » et sélectionner le fichier correspondant à votre dispositif dans *Sniffer\_Software/hex/.*

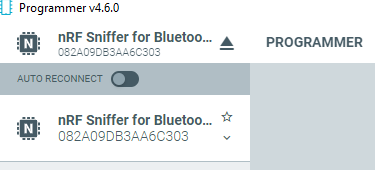




Une fois le fichier *.hex* chargé, cliquer sur « Write » pour télécharger le firmware sur le dongle.



Si tout a été bien fait, le nom du dispositif changera vers le nom du firmware « nRF Sniffer for Bluetooth LE » dans la liste.



Fermer nRF Connect for Desktop.

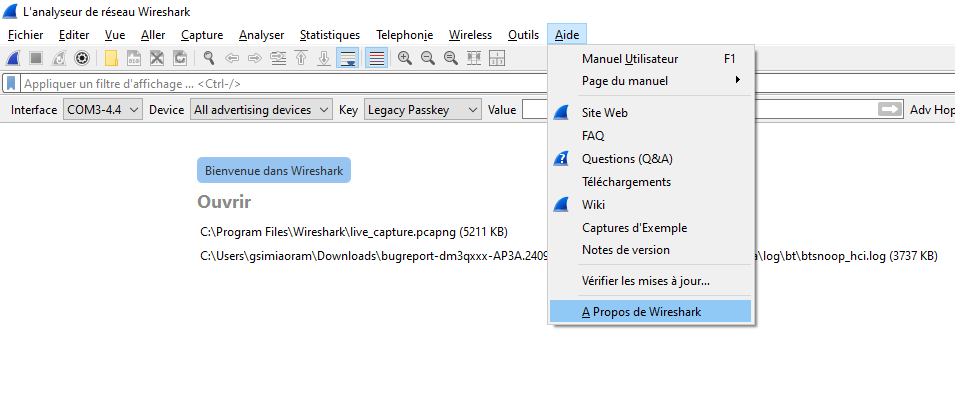
La section suivante a été copiée et traduite en français de la section *2.2* du document [*nRF\_Sniffer\_BLE\_UG\_v4.0.0.pdf*](https://docs.nordicsemi.com/bundle/nrfutil_ble_sniffer_pdf/resource/nRF_Sniffer_BLE_UG_v4.0.0.pdf)

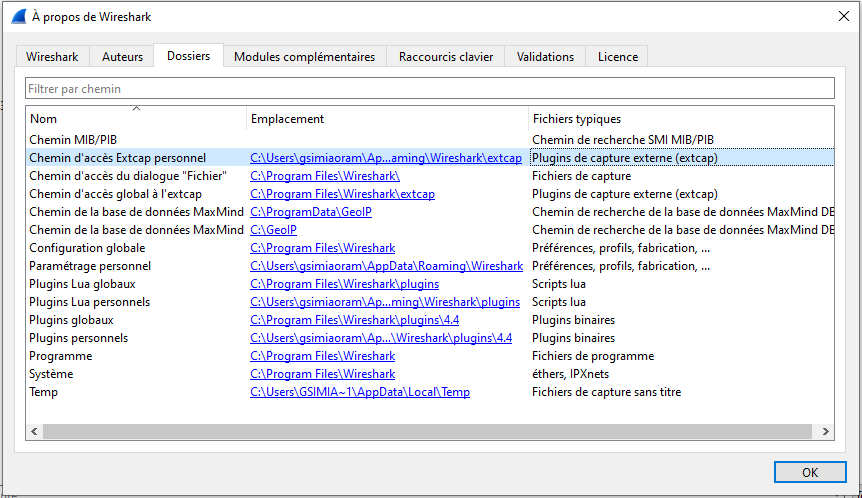
# Installer le nRF Sniffer Capture Tool

Le nRF Sniffer for Bluetooth LE software est installé comme un plugin de capture externe sur Wireshark.

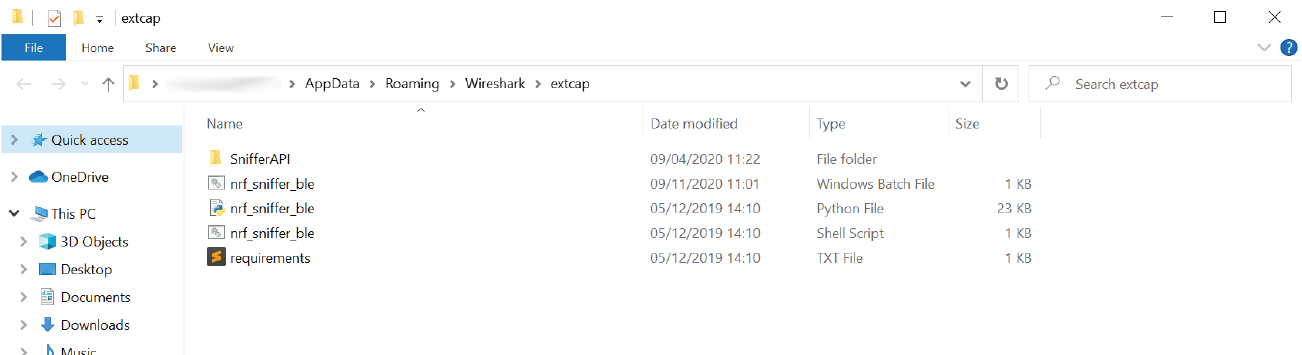
Pour l’installer, suivez les étapes suivantes :

1. Installer les prérequis Python :
   1. Ouvrez une invite de commande dans le dossier Sniffer\_Software/extcap/
   2. Tapez pip3 install -r requirements.txt pour installer les prérequis
   3. Fermer l’invite de commande
2. Copier le nRF Sniffer capture tool dans le dossier Wireshark « *Chemin d'accès Extcap personnel »:*
   1. Ouvrir Wireshark.
   2. Aller sur Aide > A propos de Wireshark (sur Windows ou Linux) ou Wireshark > A propos de Wireshark (sur macOS).

**

**

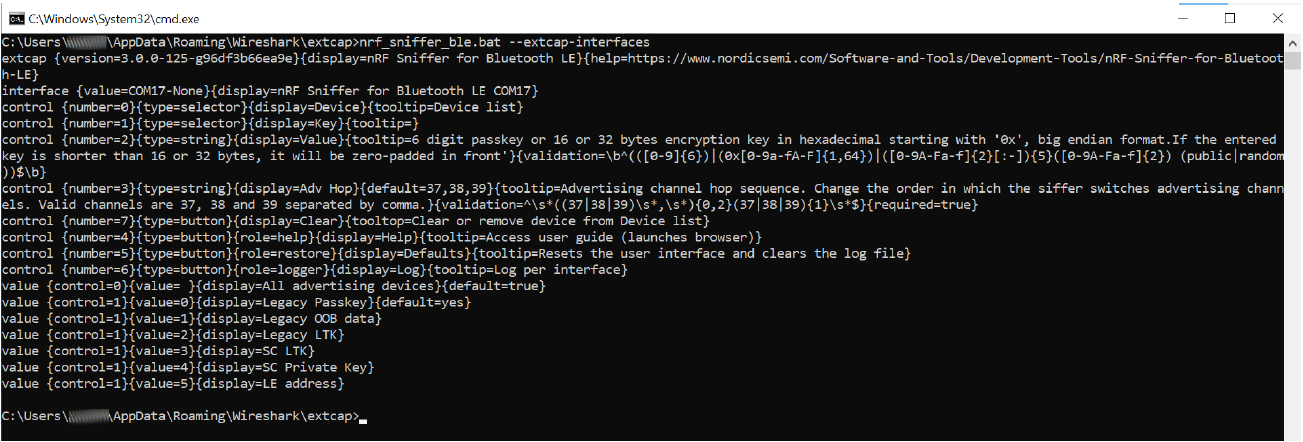
Copier le contenu de *Sniffer\_Software/extcap/* dans ce dossier.



1. Pour vérifier que les fichiers de nRF Sniffer ont été correctement installés, faites :
   1. Ouvrir une invite de commande dans le dossier Wireshark « *Chemin d'accès Extcap personnel »*
   2. Lancer le nRF Sniffer tool pour lister les interfaces disponibles.

Sur Windows, taper nrf\_sniffer\_ble.bat --extcap-interfaces. Sur macOS ou Linux, taper nrf\_sniffer\_ble.sh --extcap-interfaces.

Vous devez avoir une sortie comme la suivante.



* 1. Si la commande précédente retourne un erreur, vérifiez si Python est installé sur la machine.

Sur Windows, tapez python --version. Sur macOS ou Linux, tapez python3. Si la commande ne pas pu être trouvée ou si la version de Python n’est pas la bonne, vérifiez si la version v3.6 ou postérieur est dans le PATH du PC et si elle est la première version dans le PATH.

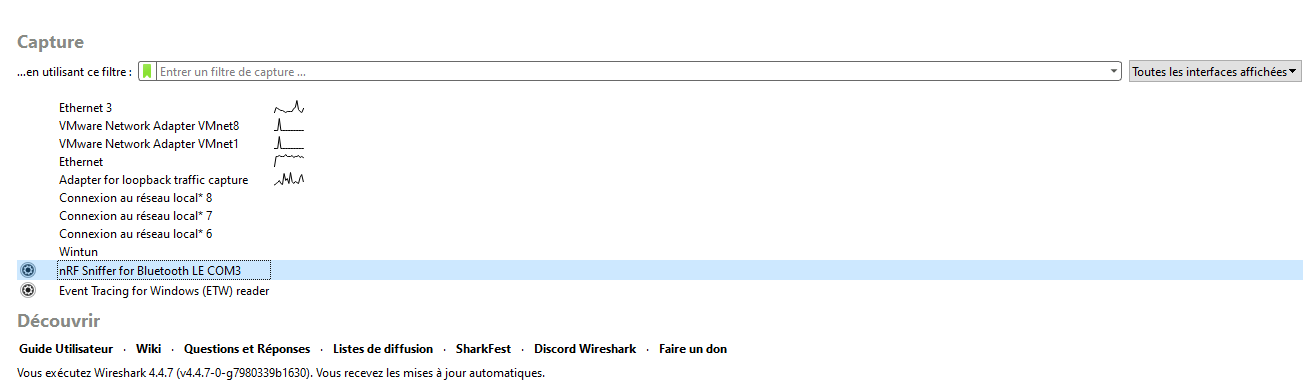
* 1. Pour macOS ou Linux: Vérifiez que le fichier nrf\_sniffer\_ble.sh a la permission x.

Si la permission x est manquante, faites chmod +x nrf\_sniffer\_ble.sh pour l’ajouter.

1. Habiliter nRF Sniffer capture tool dans *Wireshark*:
   1. Actualiser les interfaces dans *Wireshark* en sélectionnant **Capture** > **Actualiser les Interfaces** ou faites **F5**.

You should see that nRF Sniffer is displayed as one of the interfaces on the start page.

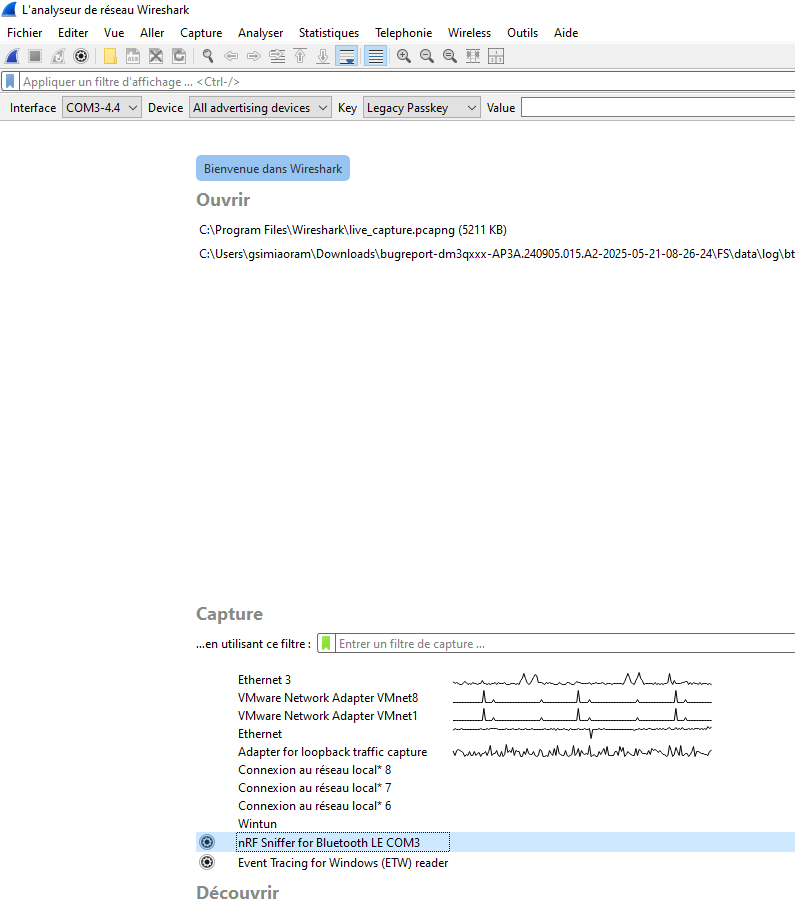
* 1. Select **View** > **Interface Toolbars** > **nRF Sniffer for Bluetooth LE** to enable the nRF Sniffer interface.



Vous pouvez aussi ajouter un profil de capture personnalisé pour le nRF Sniffer pour montrer de façon personnalisée les données capturées, pour faire cela, suivez la section *2.3* du document *nRF\_Sniffer\_BLE\_UG\_v4.0.0.pdf.*

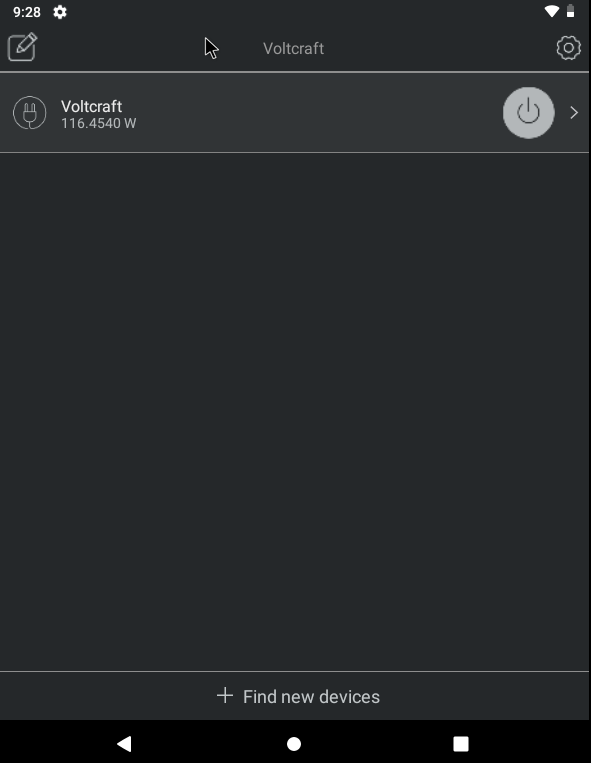
# Capturer des paquets avec nRF52840 et Wireshark

Enfin, pour capturer les paquets BT LE échangés entre l’appli et la prise, sur Wireshark, sélectionnez l’interface *nRF Sniffer for Bluetooth LE COMX* et cliquez sur *Capturer* en haut à gauche.

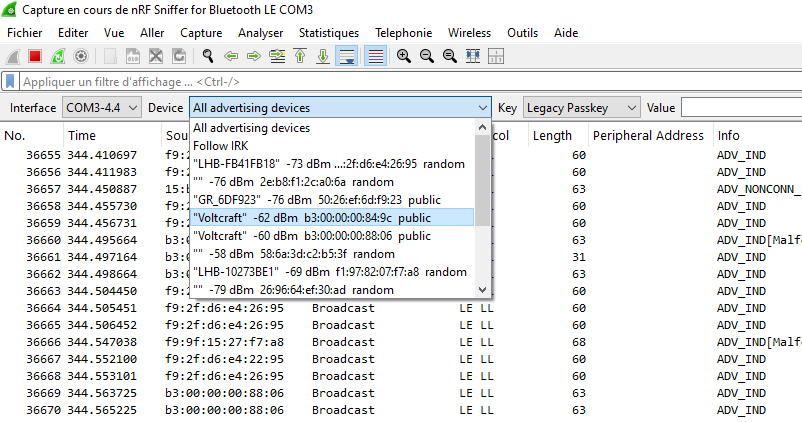


La fenêtre de capture ira s’ouvrir et tous les paquets BT proches du dongle seront affichés, maintenant il faut les filtrer pour montrer juste les paquets de la prise.

D’abord, connectez la prise au portable en utilisant l’appli Voltcraft SEM6000 pour Android/Apple.

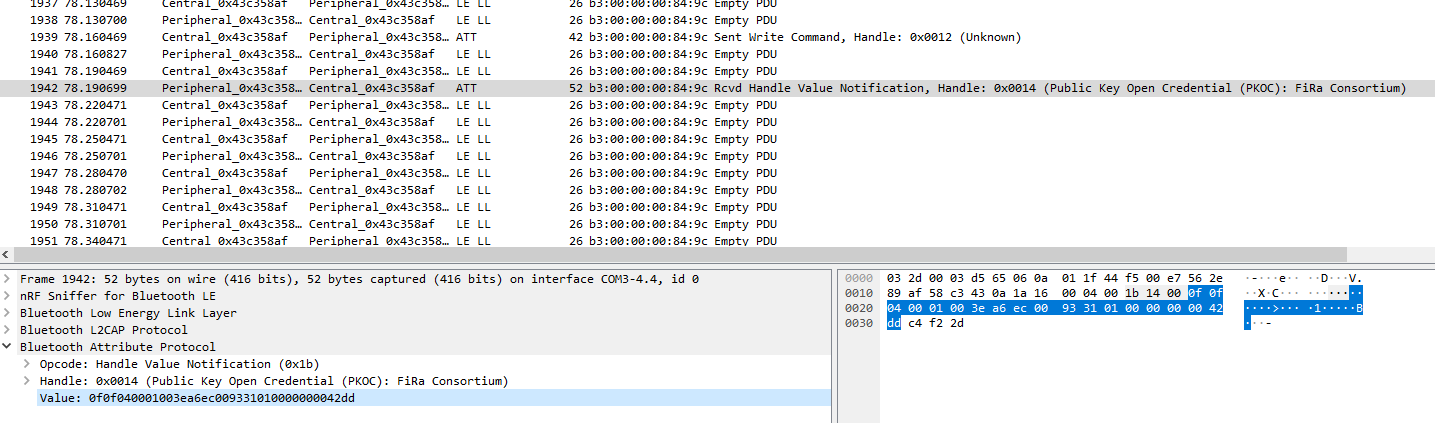


Puis, Dans la liste *Device* sélectionnez *« Voltcraft … »* , si il n’apparaît pas, fermez l’appli sur le portable et faites *Rafraichir* et après réouvrez l’appli, répétez cela jusqu’à ce que le dispositif soit affiché dans la liste.



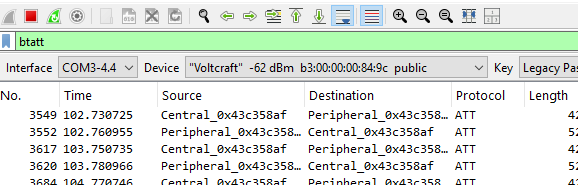
Une fois que le dispositif a été sélectionnez dans la liste, vous verrez plusieurs paquets du type *LE LL* que sont les des paquets d’avertissement émis par la prise mais qui ne contiennent pas les valeurs de consommation cherchées.

Les paquets qui contiennent ces valeurs sont du type *ATT*, s’ils ne sont pas présents dans la liste, fermez l’appli sur le portable et le réouvrez, répétez cela jusqu’à voir les paquets dans la liste.



Le paquet *Rcvd Handle Value Notification, Handle 0x0014* contient les valeurs de consommation en format Hexadécimal.

(Optionnel) Appliquer le filtre *btatt* pour n’afficher que les paquets *ATT* dans la liste.



Pour capture des paquets d’autres prises Voltcraft, il faudra un dongle par prise, puis, sur Wireshark, sélectionner un *Device* pour chaque interface (dongle).

# Script Python pour envoyer les données BT LE à Node-Red sur OPCUA

Un script python capture\_wireshark\_ble.py a été écrit pour permettre la lecture des paquets *ATT, Handle 0x0014* provenant de Wireshark avec les informations de consommation énergétique.

Avant de lancer ce script, ouvrez une invite de commande dans le dossier contenant le script python et tapez la commande wireshark --update-interval 25 -i COM<X>-4.4 -k -w live\_capture.pcapng en remplaçant <X> par le nombre du port du dispositif branché, pour plus de détails sur comment lancer cette commande avec plusieurs dongles, voir le script python.

Cette commande lancera Wireshark et ira commencer à capturer les paquets BT LE et les enregistrer dans un fichier appelé live\_capture.pcapng, filtrez les paquets en utilisant la liste *Device* pour afficher que les paquets des prises et vérifiez que les paquets *ATT* sont présents.

Après cela, il faut lancer le script python avec l’IDE de votre choix, le scriptama ira ouvrir le fichier *.pcapng*, lire que les paquets *ATT, Handle 0x0014* (Infos de consommation), ouvrir un serveur OPCUA et publier les infos sur ce serveur.

# Simuler Android sur PC (Machine Virtuelle)

Le souci que nous rencontrons en utilisant l’appli sur un portable c’est que le même devient inutilisable pour d’autres tâches, vu que si l’appli est fermée les paquets seront plus échangés.

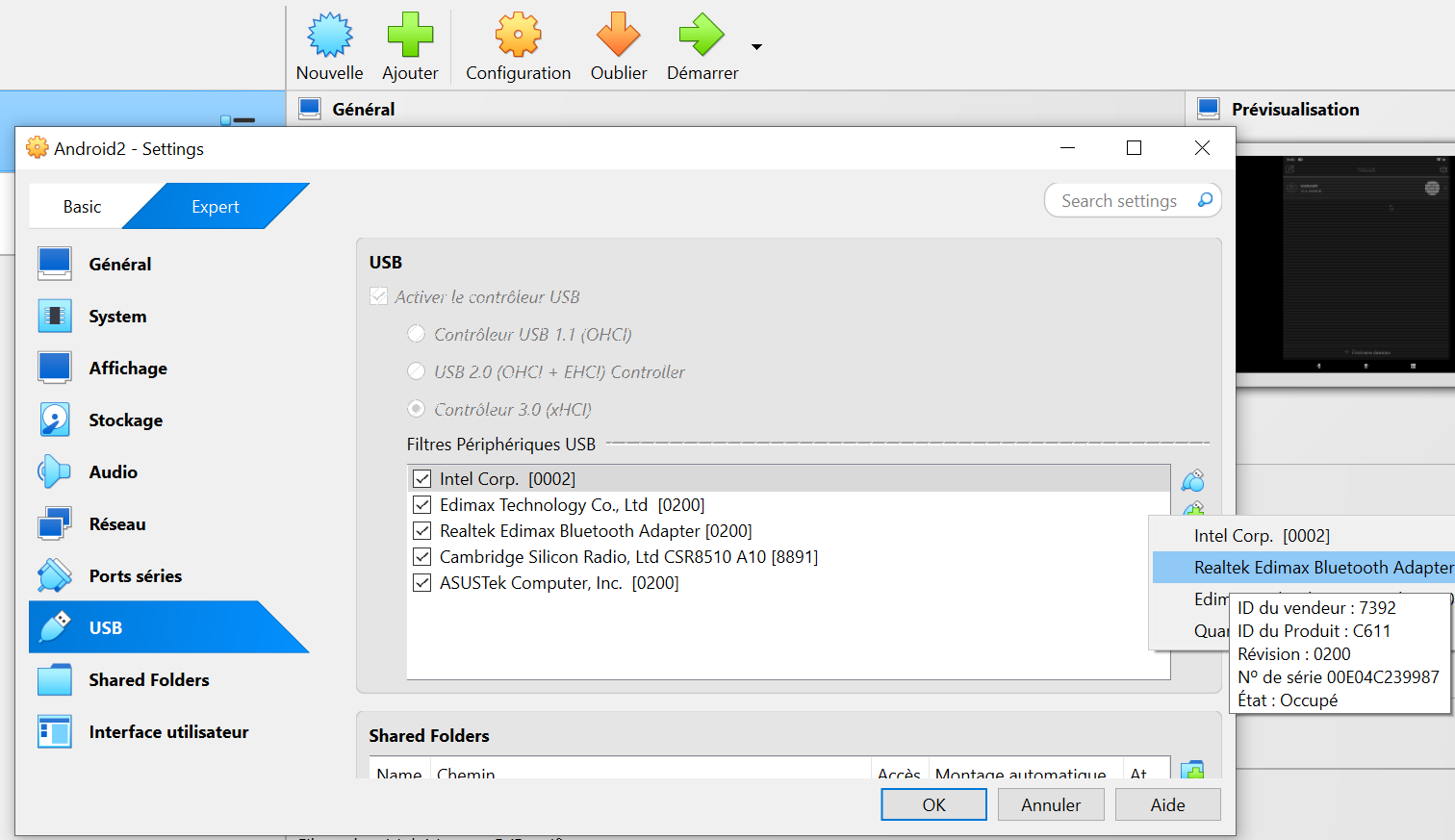
Pour contourner ce problème, vous pouvez simuler une tablette Android sur le PC à l’aide d’une Machine Virtuelle et un adaptateur USB pour bluetooth. Le logiciel pour VM utilisé ici sera l’Oracle VirtualBox (<https://www.virtualbox.org/wiki/Downloads>) avec un ISO android téléchargeable sur (<https://www.osboxes.org/android-x86/>). De plus, comme les VM n’ont pas de Bluetooth intégré, il faudra utiliser un adaptateur USB-Bluetooth pour installer le driver BT sur l’appareil, les adaptateurs compatibles recommandés sont :

* EDIMAX BT-8500
* Renkforce 4.0 +EDR

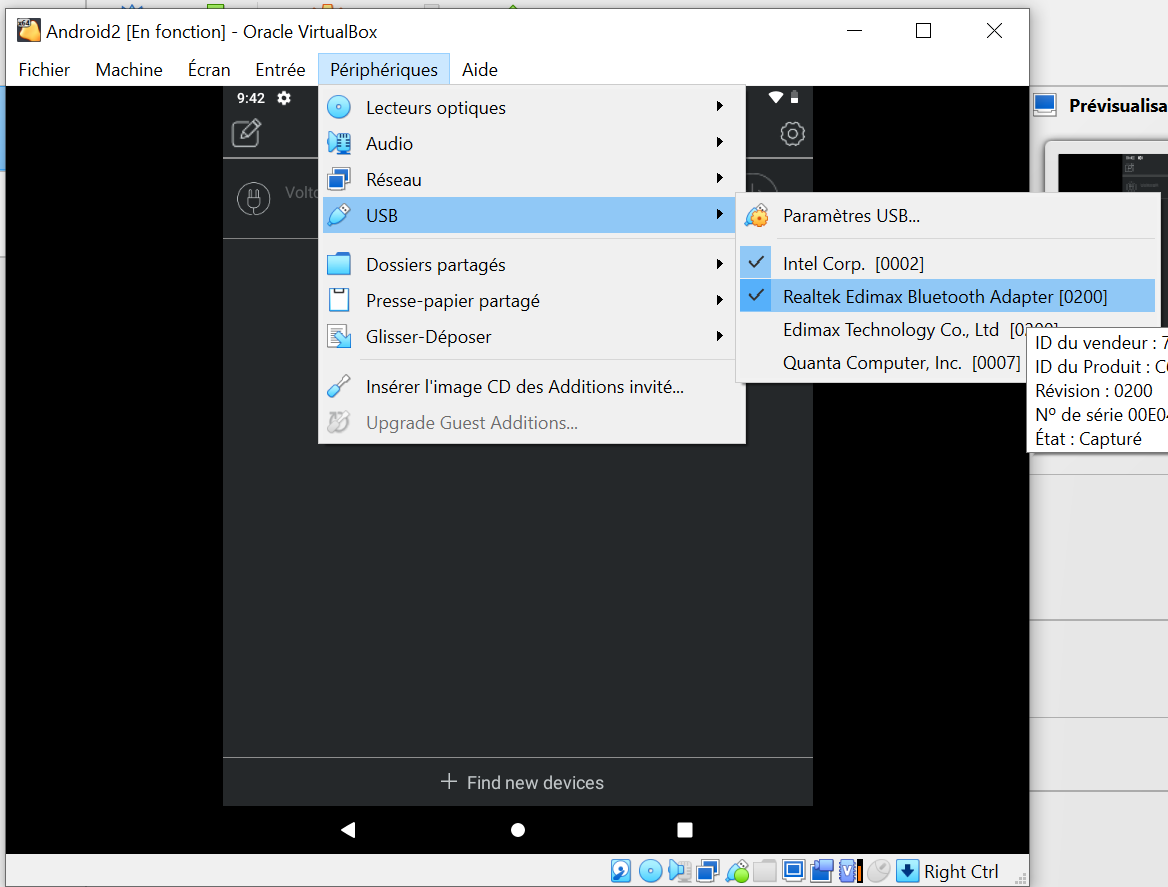
Ouvrez Oracle VM, si la VM « Android2 » n’est pas déjà installée, suivez les instructions de la vidéo [2] pour installer l’ISO Android et la configurer pour pouvoir utiliser l’appli Voltcraft SEM6000.

Pour ajouter le BT sur la machine, après installer le driver de l’adaptateur, sur Oracle VM, suivez les étapes suivantes :

Dans les configurations de la VM crée, dans l’onglet « USB », activez le contrôleur USB et puis ajoutez le périphérique correspondant à l’adaptateur dans la liste, ici Edimax, et faites OK.

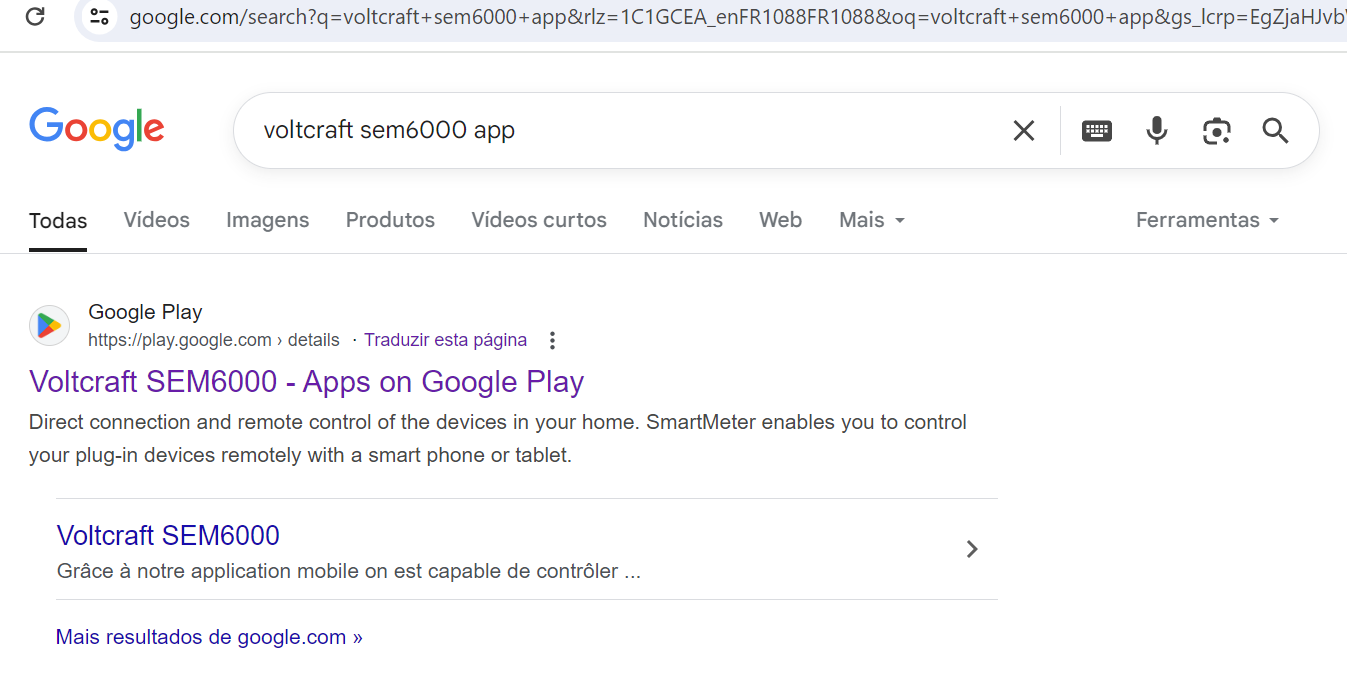


Puis, après lancer la VM « Android2 », dans le menu Périphériques, activez le driver USB.



Vous avez alors du Bluetooth sur votre VM, il faut maintenant installer l’appli Voltcraft SEM6000 s’il n’est pas déjà installé.

Pour l’installer, utilisez l’App Store sur la VM ou, comme des fois l’App Store ne fonctionne pas, vous pouvez chercher « Voltcraft SEM6000 app » sur Google pour installer avec le premier lien.



Voilà, la machine virtuelle est totalement configurée et vous pouvez l’utiliser pour se connecter avec les prises et intercepter les paquets avec Wireshark.

# Références :

[1] DIY Bluetooth Low Energy (BLE) Sniffing: Debug Your Projects Like a Pro! <https://www.youtube.com/watch?v=gvxqg0vxhrQ>, Elektor TV

[2] Meu video sobre Live CD VESA

[3] *nRF\_Sniffer\_BLE\_UG\_v4.0.0.pdf* <https://docs.nordicsemi.com/bundle/nrfutil_ble_sniffer_pdf/resource/nRF_Sniffer_BLE_UG_v4.0.0.pdf>