Renifleur BLE

Reconfiguration du dongle USB nRF52840 MDK de makerdiary

Figure 1. Dongle USB MDK nRF52840 de makerdiary.

Figure 2. Le dongle USB.

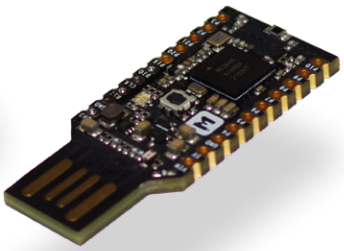

Figure 3. Avec le couvercle enlevé.

Mathias Claußen (Elektor)

Il est toujours marrant de modifier un produit pour remplir une fonction complètement différente de celle pour laquelle il a été conçu à l'origine. Dans ce projet, nous modifions le logiciel d'une carte d'évaluation et la transformons en un renifleur de flux de données BLE utile - un outil pratique pour quiconque développe et teste des applications Bluetooth. La carte d'évaluation en question est le dongle USB nRF52840 bon marché pour le développement IdO de makerdiary.

La visualisation de l'échange de paquets de données en temps réel entre les appareils est utile pour tous ceux qui développent des applications Bluetooth Low Energy (BLE). Elle facilite le débogage. Comme pour l'enregistrement des paquets wifi, un matériel compatible au BLE sera nécessaire. Nous pouvons utiliser une carte d'évaluation prête à l'emploi et à faible coût basée sur le SoC Bluetooth nRF52840 de Nordic qui intègre tous les périphériques de communication nécessaires. Deux exemples sont le dongle USB nRF52840 MDK de makerdiary [1] (**figure 1**) et le dongle nRF52840 de Nordic [2]. Ce SoC est également utilisé comme composant de traitement principal dans d'autres cartes, notamment l'Arduino Nano 33 BLE [3], le BBC micro:bit V2 (ici, le nRF52833 avec moins de capacité mémoire est utilisé) [4], et l'Adafruit CLUE [5].
En plus du module matériel qui traitera les paquets BLE, nous avons également besoin d'un logiciel et d'un PC. Nous pourrions utiliser un PC standard avec un processeur de type AMD64/x86 ou un Raspberry Pi. Le

logiciel utilisé ici est Wireshark, un outil que certains d'entre vous connaissent probablement. L'ensemble constitue un système permettant d'enregistrer et de visualiser le transfert de paquets BLE en temps réel.

Pas à pas

La procédure d'installation et de configuration décrite ici s'applique à un PC AMD64/x86 exécutant Windows 10. Nous utilisons également le dongle USB nRF52840 MDK de makerdiary. Cette petite carte est en fait conçue comme un kit de développement pour le nRF52840 de Nordic et est livrée dans un boîtier de dongle soigné (**figure 2** et **figure 3**) qui se branche directement sur le port USB du PC. En plus de BLE 5.0 et de Bluetooth Mesh, la puce prend en charge les protocoles réseau ZigBee et Thread. Les données techniques se trouvent dans le **tableau 1**. Outre sa capacité à enregistrer des paquets BLE, le dongle pourrait être configuré pour effectuer un travail similaire pour d'autres normes de transmission sans fil.
Dès la fabrication, le dongle USB nRF52840 MDK de makerdiary est équipé du micrologiciel *OpenThread Network Co-Processor* (NCP). Pour notre application, nous utiliserons les communications BLE au lieu de Thread, nous devons donc remplacer le micrologiciel et éventuellement le chargeur d'amorçage (selon la version de la carte que vous possédez). La mise à jour du chargeur d'amorçage (bootloader) d'Open-Bootloader vers le bootloader UF2 facilite la programmation du dongle USB nRF52840 MDK de makerdiary, car il est reconnu comme une clé USB de stockage dans le système. Plus tard, si vous souhaitez changer à nouveau le micrologiciel, par exemple avec CircuitPython [6], vous pouvez le faire très facilement.

Mise à jour avec le bootloader uf2

Nous avons besoin de quelques outils pour mettre à jour le bootloader. Ici, nous utilisons nrfutil [7] pour le faire [8]. Les fichiers de nrfutil et de la mise à jour du bootloader doivent être copiés dans un dossier (ne décompressez pas les fichiers zippés).
Il faut maintenant mettre le dongle USB nRF52840 MDK de makerdiary en mode bootloader. Pour ce faire, maintenez le bouton *reset/user* enfoncé avant de brancher le dongle sur le port USB du PC. Si la LED commence à clignoter en rouge, le dongle

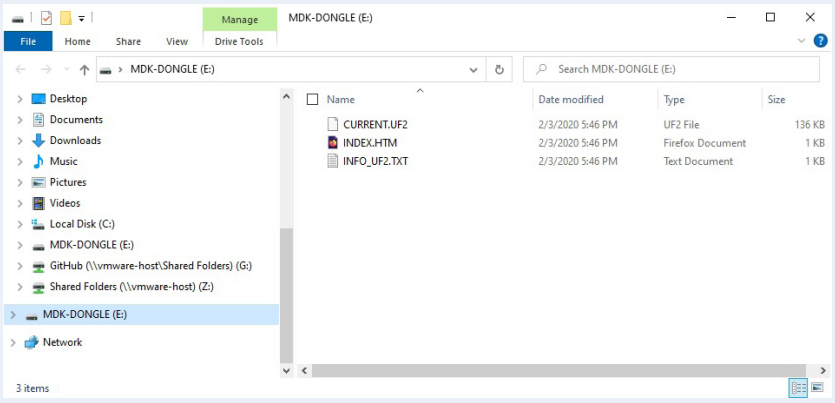

Figure 4. Le nRF52840 est reconnu comme un périphérique de stockage.

Tableau 1. Dongle USB MDK nRF52840 de makerdiary.

- Système sur puce nRF52840 de Nordic
- ARM Cortex M4F
- Optimisé pour ultra-basse consommation
- Bluetooth 5, Bluetooth Mesh
- Thread, IEEE 802.15.4, ANT
- On-chip NFC-A-Tag
- Controleur On-chip USB 2.0 (pleine vitesse)
- Sous-système de sécurité ARM TrustZone Cryptocell 310
- 1 Mo FLASH
- 256 ko RAM
- Jusqu'à 12 GPIO
- Bouton-poussoir et LED RGB
- Antenne 2,4 GHz integrée
- Régulateur 3,3 V avec sortie maximale de 1 A
- Gestion des lignes d'alimentation VBUS et VIN
- Facteur de forme pratique en clé USB
- Compatible avec les platines d'essai avec deux connecteurs à 10 broches

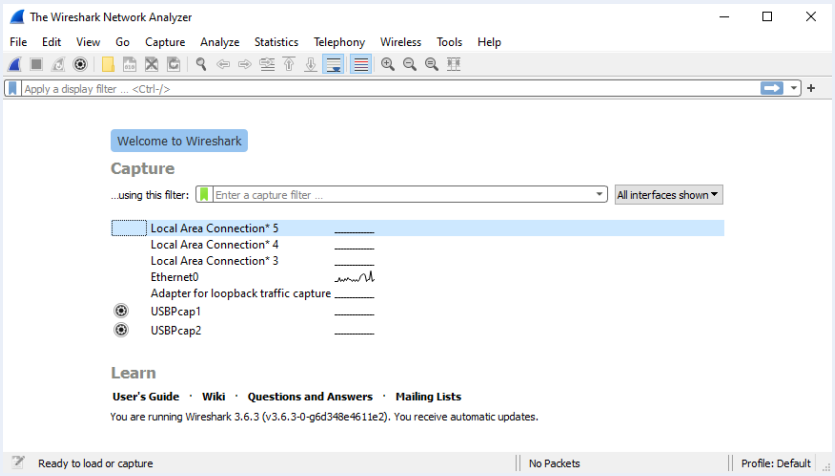

Figure 5. L'interface utilisateur de Wireshark.

USB est en mode bootloader et un nouveau port série doit avoir été identifié par l'ordinateur. Vous devez maintenant ouvrir une fenêtre de terminal/invite de commande afin de pouvoir accéder au dossier dans lequel nrfutil et les nouveaux fichiers du bootloader ont été enregistrés. La ligne de commande suivante doit être saisie ici :

```
nrfutil dfu usb-serial -pkg uf2_
   bootloader-0.2.13-44-gb2b4284-
   nosd_signed.zip -p <serial-port>
```

`<serial-port>` est le nouveau numéro de port série attribué au dongle USB nRF52840 MDK de makerdiary. Une fois cette opération terminée, le dongle USB démarre et un nouveau périphérique de stockage est identifié (**figure 4**).

Micrologiciel du renifleur BLE

L'installation du micrologiciel du renifleur BLE est assez simple. Tout d'abord, nous devons télécharger le micrologiciel approprié [9], qui a une extension de fichier .uf2, depuis le référentiel d'Adafruit. Ensuite, nous le copions sur le dongle. Redémarrez le dongle USB nRF52840 MDK de makerdiary. Il se lancera en exécutant le micrologiciel du renifleur BLE et surveillera les échanges de paquets de données BLE. Il ne reste plus qu'un seul maillon logiciel à ajouter dans la chaîne.

Wireshark et Python 3

Pour commencer, il est nécessaire d'installer Wireshark [10] (**figure 5**) et Python 3 [11] sur un PC. Lors de l'installation de Python 3, il convient de veiller à ce que les variables d'environnement soient correctement enregistrées (**figure 6**) et à ce que le lanceur Python (**figure 7**) soit également disponible. Une fois ceux-ci installés, nous devons installer pyserial qui permet aux applications Python d'accéder aux ports série du système. Pour cela, nous devons ouvrir une invite de commande et taper `pip install pyserial` (**figure 8**).
Wireshark ne peut pas communiquer avec le micrologiciel du renifleur BLE par défaut, il est donc nécessaire d'installer une extension. Pour cela, téléchargez le fichier *nrf_sniffer_for_bluetooth_le_4.1.0.zip* [12] (ou une version plus récente) de Nordic Semiconductor. Le dossier *extcap* se trouve dans ce fichier zip (**figure 9**). Dans le dossier d'installation de Wireshark (sous Windows, c'est généralement *C:\Program Files\Wireshark*), vous devez créer un dossier *extcap* et copier le contenu du dossier *extcap* du fichier zip dedans.

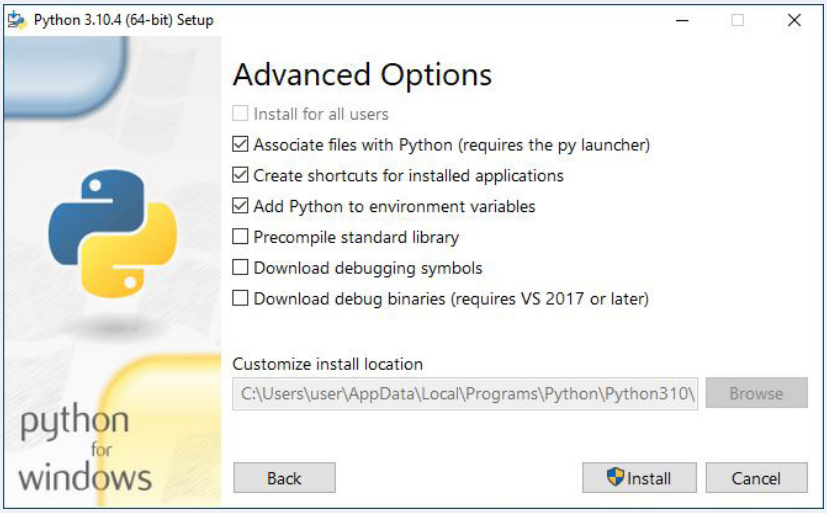

Figure 6: Sélectionnez advanced Options pour Python.

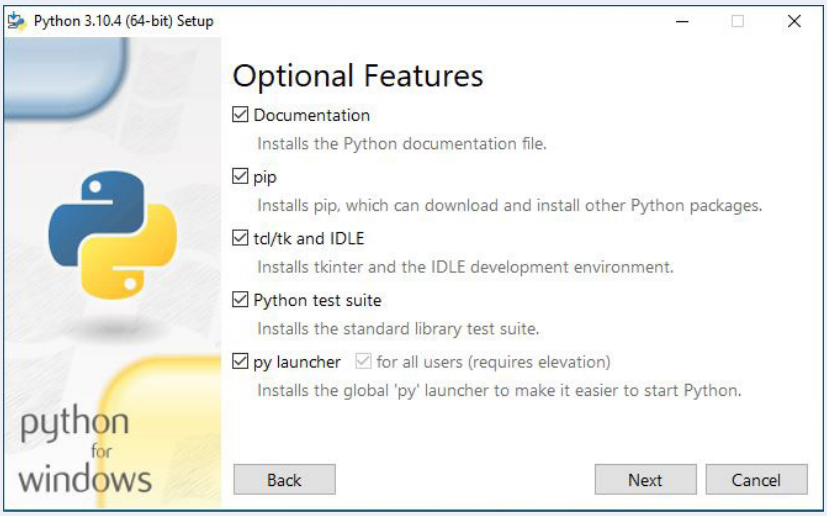

Figure 7. L'option Python launcher doit être sélectionnée.

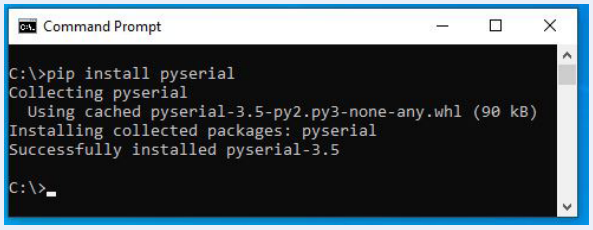

Figure 8. Installation de pyserial.

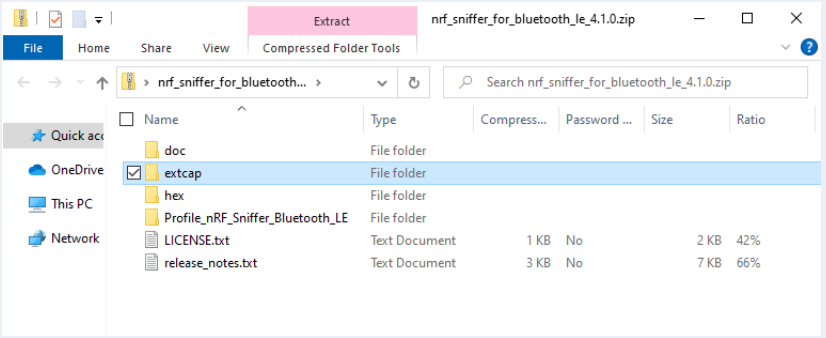

Figure 9. Le dossier extcap dans le Zip.

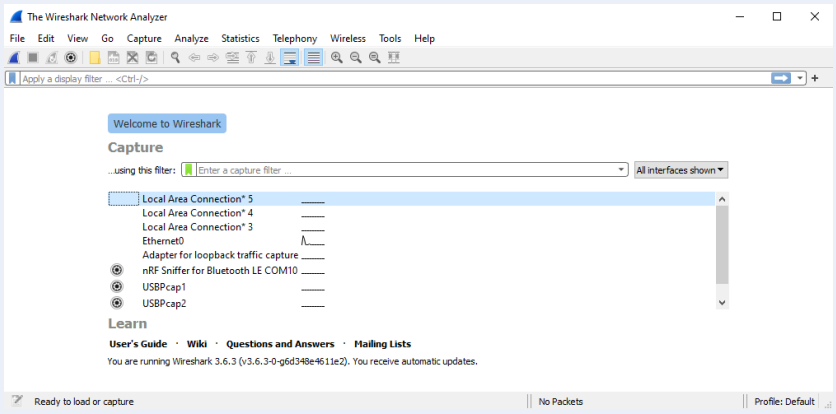

Figure 10. Une nouvelle connexion d'interface dans Wireshark.

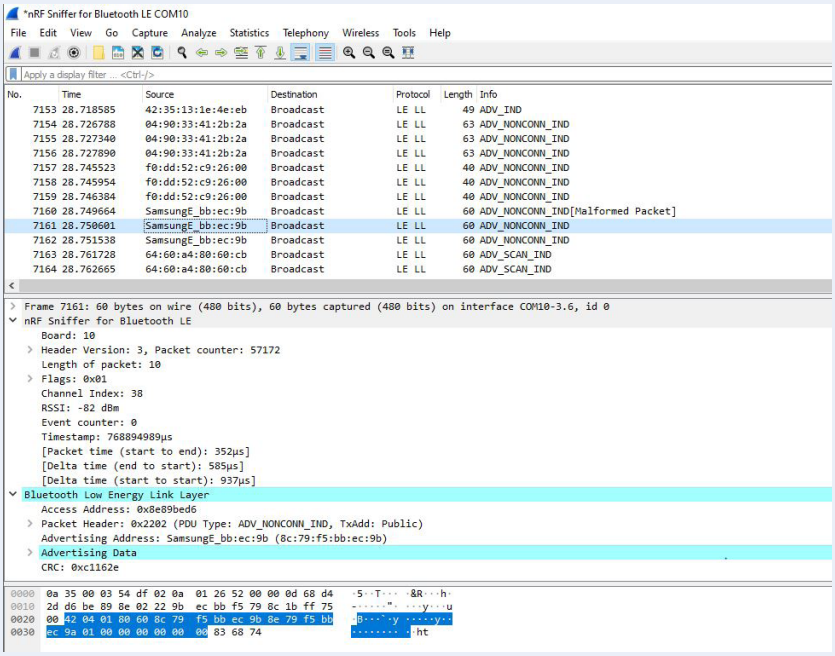

Figure 11. Affichage montrant les paquets de données BLE.

LIENS

[1] Dongle USB MDK nRF52840 de makerdiary: https://wiki.makerdiary.com/nrf52840-mdk-usb-dongle/
[2] Dongle nRF52840: www.nordicsemi.com/Products/Development-hardware/nrf52840-dongle
[3] Arduino Nano 33 BLE: https://docs.arduino.cc/hardware/nano-33-ble
[4] BBC micro:bit V2: https://microbit.org/new-microbit/
[5] T. Hanna, « CLUE d'Adafruit : Une solution intelligente pour les projets IdO », Elektormagazine.fr: www.elektormagazine.fr/news/clue-dadafruit-une-solution-intelligente-pour-les-projets-iot
[6] CircuitPython : https://circuitpython.org/board/makerdiary_nrf52840_mdk_usb_dongle/
[7] Nordic nrfutil: https://github.com/NordicSemiconductor/pc-nrfutil/releases
[8] Bootloader UF2: https://bit.ly/3atr9JI
[9] Micrologiciel du renifleur BLE: https://bit.ly/3LTMEQP
[10] Page d'accueil de Wireshark: www.wireshark.org/
[11] Page d'accueil de Python: www.python.org/
[12] Interface Wireshark dans nrf_sniffer_for_bluetooth_le_4.1.0.zip: https://bit.ly/3Gq 0yZQ

PRODUITS

- **makerdiary nRF52840 MDK USB Dongle with case (SKU 19252)**
  www.elektor.fr/19252
- **Adafruit CLUE – nRF52840 Express with Bluetooth LE (SKU 19512)**
  www.elektor.fr/19512
- **ESP-C3-12F-Kit Development Board with 4 MB Flash (SKU 19855)**
  www.elektor.fr/19855
- **Adafruit Feather nRF52840 Express (SKU 20114)**
  www.elektor.fr/20114

Nous avons à ce stade tout ce dont nous avons besoin pour commencer à capturer les paquets BLE.
Lorsque vous démarrez Wireshark, une autre interface appelée *nRF Sniffer for Bluetooth LE COMxx* apparait (**figure 10**), où *xx* indique le numéro du port Com utilisé par le dongle USB nRF52840 MDK de makerdiary. Pour enregistrer des paquets, sélectionnez cette interface et commencez l'enregistrement. S'il y a des appareils BLE à proximité, Wireshark commencera à recevoir des données (**figure 11**).

Un renifleur BLE pratique

En quelques étapes simples, le dongle USB nRF52840 MDK de makerdiary peut être transformé en un renifleur BLE vraiment utile. C'est désormais un outil inestimable pour les développeurs travaillant sur des applications BLE, en particulier lors de la configuration d'ESP32 et d'autres cartes. Non seulement vous pouvez confirmer que les données sont échangées entre les appareils, mais avec Wireshark, vous pouvez même lire le contenu des paquets. En plus des communications BLE, il est possible de reconfigurer le même dongle pour fonctionner avec d'autres protocoles de communication standard.

220248-04

Des questions, des commentaires ?

Envoyez un courriel à l'auteur (mathias.claussen@elektor.com) ou contactez Elektor (redaction@elektor.fr). Vous pouvez également regarder Mathias sur le livestream mensuel Elektor Lab Talk (www.elektormagazine.com/elt) sur YouTube, et poser vos questions en direct !