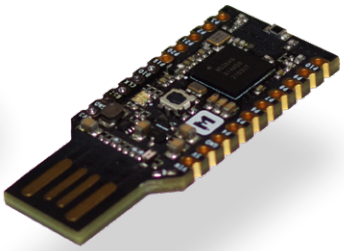
Bluetooth LE-sniffer

hack een makerdiary nRF52840 MDK USB-dongle

Figuur 1. De makerdiary nRF52840 MDK USB-dongle.

Figuur 2. De USB dongle...



Figuur 3. ...zonder de behuizing.

Mathias Claußen (Elektor)

Het is altijd leuk om een kit op een compleet andere manier te gebruiken dan oorspronkelijk bedoeld. Hier reflashen we de software van een evaluatieboard en veranderen het in een handige BLE-datasniffer – een handige tool voor iedereen die Bluetooth-applicaties ontwikkelt en test. Het evaluatieboard in kwestie is de goedkope nRF52840 USB-dongle voor IoT-ontwikkeling van makerdiary.

Iedereen die Bluetooth Low Energy-applicaties (BLE) ontwikkelt, wil graag de uitwisseling van datapakketten tussen apparaten in real time kunnen bekijken, als hulpmiddel bij het debuggen. Net als voor het opnemen van WiFi-pakketjes is geschikte hardware voor BLE nodig. We kunnen daartoe gebruik maken van een low-cost evaluatieboard op basis van de Nordic nRF52840 Bluetooth SoC, die alle noodzakelijke communicatie-periferie aan boord heeft. Twee voorbeelden zijn de makerdiary nRF52840 MDK USB-dongle [1] (**figuur 1**) en de Nordic nRF52840-dongle [2]. Deze SoC wordt ook gebruikt als de primaire processorcomponent op een aantal andere boards, zoals de Arduino Nano 33 BLE [3], de BBC micro:bit V2 (hier wordt de nRF52833 met minder geheugen gebruikt) [4] en de Adafruit CLUE [5].

Naast de hardwaremodule die de BLE-pakketten gaat verwerken, hebben we ook software en een PC nodig. Als computer kunnen we een standaard PC gebruiken, gebaseerd op een AMD64/x86-type processor, of een Raspberry Pi. De software die hier wordt gebruikt is Wireshark, een programma dat je mogelijkerwijs al kent. Alles bij elkaar krijgen we een systeem om de overdracht van BLE-pakketten in real time op te nemen en weer te geven.

Stap voor stap

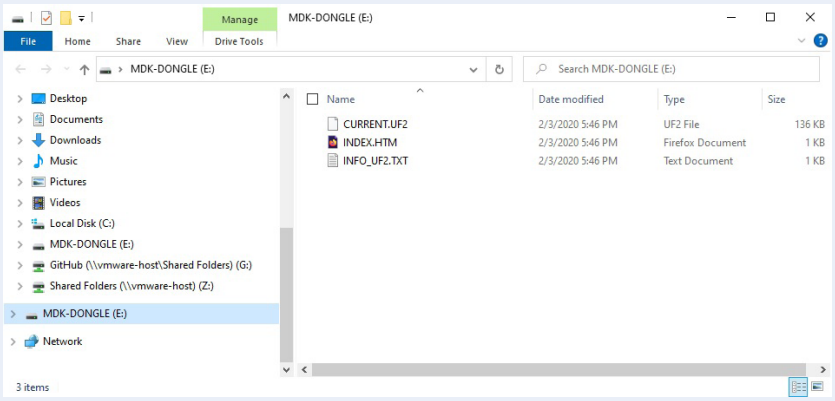
De hier beschreven installatie- en instellingsprocedure betreft een AMD64/x86-PC met Windows 10. We maken ook gebruik van de makerdiary nRF52840 MDK USB-dongle. Dit kleine board is eigenlijk bedoeld als ontwikkelkit voor de Nordic nRF52840 en wordt geleverd in een nette dongle-behuizing (**figuur 2** en **figuur 3**) die rechtstreeks in de USB-poort van de PC wordt geprikt. Naast BLE 5.0 en Bluetooth Mesh ondersteunt de chip ook ZigBee- en Thread-netwerkprotocollen. De technische gegevens zijn te vinden in **tabel 1**. Naast de mogelijkheid om BLE-pakketten op te nemen, kan de dongle ook worden geconfigureerd om dat voor andere draadloze transmissiestandaarden te doen.

Af fabriek is de makerdiary nRF52840 MDK USB-dongle uitgerust met firmware voor de OpenThread Network Co-Processor (NCP). Hier gebruiken we BLE-communicatie in plaats van Thread, dus moeten we de firmware en eventueel de bootloader vervangen (afhankelijk van welke versie van het board je hebt). Het achteraf actualiseren van de bootloader van Open-Bootloader naar de UF2-bootloader maakt het programmeren van de makerdiary nRF52840 MDK USB-dongle werkelijk simpel omdat het door het systeem wordt herkend als een USB-apparaat voor massaopslag (vergelijkbaar met een Raspberry Pi Pico). Als je later de firmware weer wilt verwisselen, bijvoorbeeld met CircuitPython [6], dan gaat dat heel gemakkelijk.

Updaten met de UFf2-bootloader

Er zijn een paar tools nodig om de bootloader te actualiseren. Hier gebruiken we *nrfutil* [7] voor dat doel [8]. De *nrfutil*- en bijgewerkte bootloader-bestanden moeten naar één map gekopieerd worden (pak de gezipte bestanden niet uit).

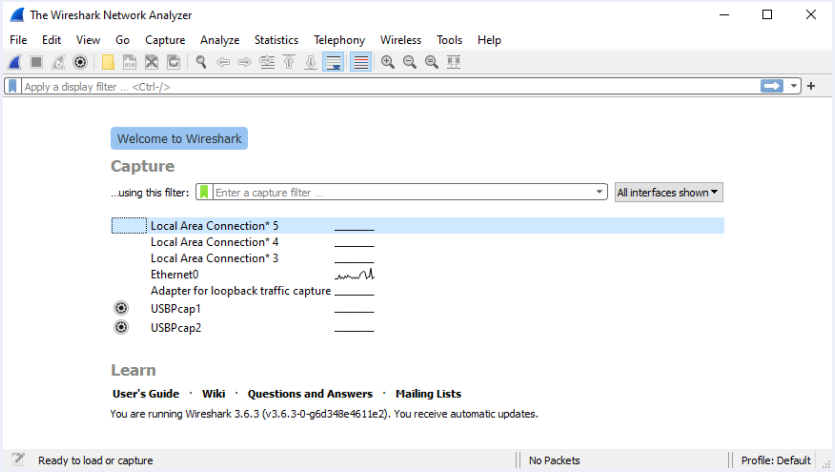
Nu moeten we de makerdiary nRF52840 MDK USB-dongle in bootloader-modus zetten. Hiertoe hou je de reset/user-knop ingedrukt voordat de dongle in de USB-poort van de PC wordt gestoken. Als de LED rood gaat knipperen, is de USB-dongle in bootloader-modus en hoort er een nieuwe seriële poort te zijn geïdentificeerd door de computer. Nu moet je een terminalvenster/commandoprompt openen zodat je naar de map kunt navigeren waar de *nrfutil* en de nieuwe bootloader-bestanden zijn opgeslagen. Hier moet nu de volgende



Figuur 4. De nRF52840 wordt herkend als extern massageheugen.

Tabel 1. De makerdiary nRF52840 MDK USB Dongle.

- Nordic nRF52840 System-on-Chip
- ARM Cortex M4F
- Geoptimaliseerd voor ultra low power
- Bluetooth 5, Bluetooth Mesh
- Thread, IEEE 802.15.4, ANT
- On-chip NFC-A-Tag
- On-chip USB 2.0-controller (full speed)
- ARM TrustZone Cryptocell 310 beveiligings-subsysteem
- 1 MB FLASH
- 256 kB RAM
- Max. 12 GPIO's
- Druktoets en RGB-LED
- On-board 2.4G-antenne
- 3,3V-regelaaruitgang (1 A max)
- VBUS & VIN Power Path Management
- Handige USB-dongle vormfactor
- Breadboard-vriendelijk met dubbele 10-polige headers



Figuur 5. De Wireshark-GUI.

opdrachtregel worden ingevoerd:

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

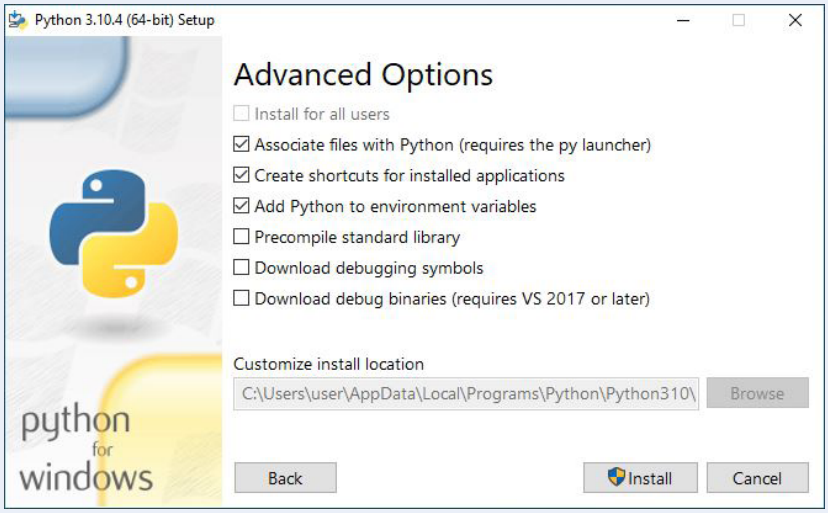
`<serial-port>` is het nieuwe seriële poortnummer dat is toegewezen aan de makerdiary nRF52840 MDK USB-dongle. Zodra dit is voltooid start de USB-dongle en wordt een nieuw station voor massa-opslag geïdentificeerd (**figuur 4**).

De BLE sniffer-firmware

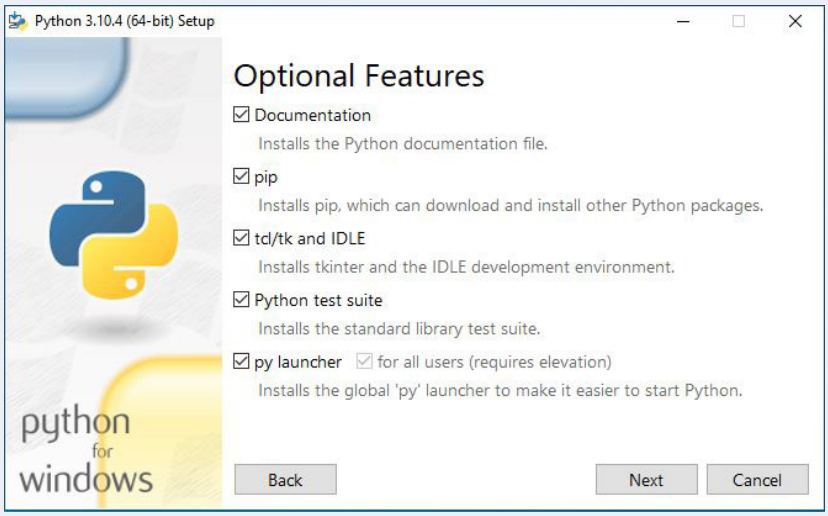
Het installeren van de firmware voor de BLE-sniffer is vrij eenvoudig. Eerst moeten we de juiste firmware [9], die een *.uf2*-bestandsextensie heeft, downloaden uit de Adafruit-repository. Vervolgens kopiëren we die naar de dongle, die nu is herkend als een station voor massa-opslag. Na het herstarten zal de makerdiary nRF52840 MDK USB-dongle opstarten met de Bluetooth LE sniffer-firmware en zal BLE dataverkeer monitoren. Slechts één software-schakel in de keten moet nog worden toegevoegd.

Wireshark en Python 3

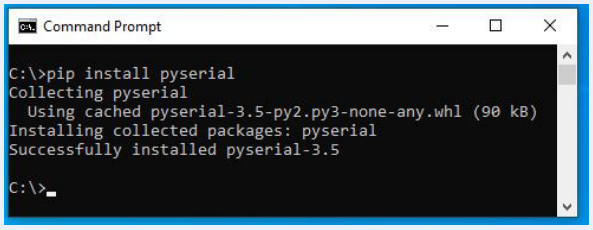
Ter voorbereiding moeten eerst Wireshark [10] (**figuur 5**) en Python 3 [11] op de PC worden geïnstalleerd. Bij de installatie van Python 3 moet erop worden gelet dat de omgevingsvariabelen correct zijn geregistreerd (**figuur 6**) en dat ook de Python launcher (**figuur 7**) beschikbaar is. Zodra deze zijn geïnstalleerd, moeten we *pyserial* installeren, waarmee Python-applicaties toegang kunnen krijgen tot de seriële poorten van het systeem. Hiervoor moeten we een opdrachtprompt openen en `pip install pyserial` intypen (**figuur 8**). Wireshark kan standaard niet communiceren met de BLE sniffer-firmware, dus is het nodig om een extensie te installeren. Hiervoor is het nodig om de *nrf_sniffer_for_bluetooth_le_4.1.0.zip* [12] (of een nieuwere versie) van Nordic Semiconductor te downloaden. De *extcap*-map kan in dit zip-bestand worden gevonden (**figuur 9**). In de Wireshark-installatiemap (onder Windows is dit meestal C:\Program Files\Wireshark) moet je een *extcap*-map aanmaken, waarin je de inhoud van de *extcap*-map uit het zip-bestand moet kopiëren. Nu hebben we alles wat we nodig hebben om BLE-datapakketten te kunnen monitoren. Wanneer Wireshark nu wordt gestart, is een andere interface te zien (**figuur 10**),



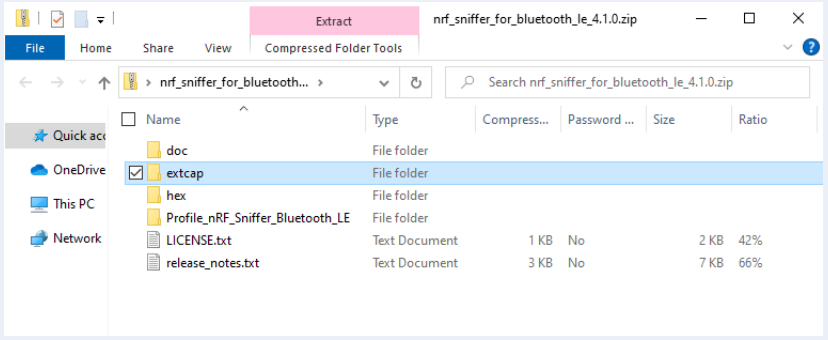
Figuur 6. Selecteer Advanced Options voor Python.



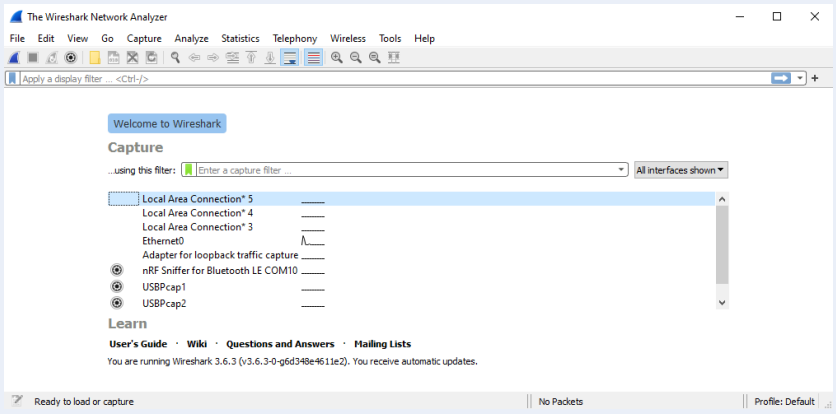
Figuur 7. De Python launcher-optie moet worden geselecteerd.



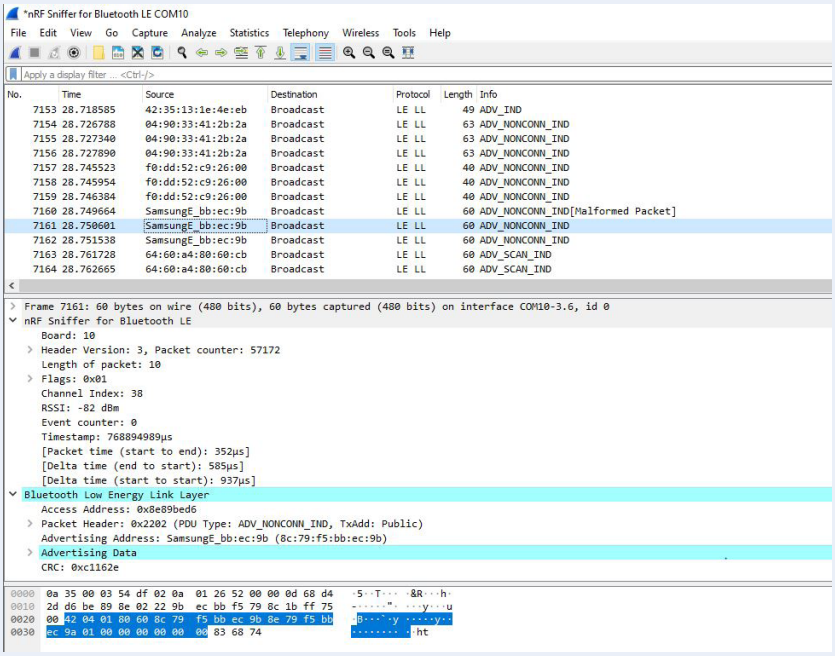
Figuur 8. Installatie van pyserial.



Figuur 9. De extcap map in het zip-bestand.



Figuur 10. Een nieuwe interfaceverbinding in Wireshark.



Figuur 11. De BLE-gegevenspakketten zijn zichtbaar.

WEBLINKS

[1] makerdiary nRF52840 MDK USB-dongle: https://wiki.makerdiary.com/nrf52840-mdk-usb-dongle/
[2] nRF52840-dongle: 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, "De CLUE van Adafruit: een slimme oplossing voor IoT-projecten", elektormagazine.nl: www.elektormagazine.nl/news/clue-van-adafruit-een-slimme-oplossing-voor-iot-projecten
[6] CircuitPython : https://circuitpython.org/board/makerdiary_nrf52840_mdk_usb_dongle/
[7] Nordic nrfutil: https://github.com/NordicSemiconductor/pc-nrfutil/releases
[8] UF2-bootloader: https://bit.ly/3atr9JI
[9] BLE sniffer-firmware: https://bit.ly/3LTMEQP
[10] Wireshark-homepage: www.wireshark.org/
[11] Python-homepage: www.python.org/
[12] Wireshark Interface in het nrf_sniffer_for_bluetooth_le_4.1.0.zip-bestand: https://bit.ly/3Gq0yZQ

GERELATEERDE PRODUCTEN

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

die *nRF Sniffer for Bluetooth LE COMxx* heet (waarbij xx het nummer aangeeft van de Com-poort die wordt gebruikt door de makerdiary nRF52840 MDK USB-dongle). Om pakketten op te nemen, selecteer je gewoon die interface en begin je met opnemen. Als er BLE-apparaten in de buurt zijn, zal Wireshark nu data gaan ontvangen (**figuur 11**).

Een handige BLE-sniffer

Met een paar eenvoudige handelingen kan de makerdiary nRF52840 MDK USB-dongle worden omgebouwd tot een echt nuttige BLE-sniffer. Het is nu een hulpmiddel van onschatbare waarde voor ontwikkelaars die aan BLE-toepassingen werken, vooral bij het opzetten van ESP32 en Co. Je kunt niet alleen bevestigen dat er gegevens worden uitgewisseld tussen apparaten, maar met Wireshark kun je ook de inhoud van de pakketten lezen. Naast BLE-communicatie kan dezelfde dongle ook worden geconfigureerd om met een aantal andere standaard-communicatieprotocollen te werken.

220248-03

Vragen of opmerkingen?

Hebt u vragen of opmerkingen naar aanleiding van dit artikel? Stuur een e-mail naar de auteur via mathias.claussen@elektor.com of naar de redactie van Elektor via redactie@elektor.com. U kunt Mathias ook volgen op de maandelijkse Elektor Lab Talk-livestream (www.elektormagazine.com/elt) op YouTube, waar u live uw vragen kunt stellen!