

Kinetis USB-KW41Z Wireless Protocol Sniffer

Quick Start Guide

This document describes the usage of the USB-KW41Z evaluation board with the wireless protocol sniffer firmware, Wireshark adapter and the Wireshark tool itself. The sniffer firmware is also compatible with the NXP Test Tool for Connectivity Products protocol analyzer. This document describes the usage in Bluetooth® Low Energy v4.2 and in the IEEE® 802.15.4 modes with Wireshark. Test Tool specific usage is described separately in the tool's documentation.

Contents

1	Hardware Setup	2
2	Firmware Images	2
3	Flashing the Sniffer Firmware Using External J-Link Probe	3
3.1	Common	3
3.2	Flashing MK22FN512xxx12.....	4
3.3	Flashing MKW41Z512xx4.....	8
4	User Interface – Kinetis Protocol Analyzer Adapter.....	11
4.1	Sniffing Bluetooth® Low Energy v4.2 Wireless Communications	13
4.2	Sniffing IEEE® 802.15.4 Wireless Communications	16



1 Hardware Setup

The hardware setup consists of a USB-KW41Z BLE Sniffer dongle which should be connected to a USB port or to an USB hub connected to a Windows® system capable of running the Wireshark tool.

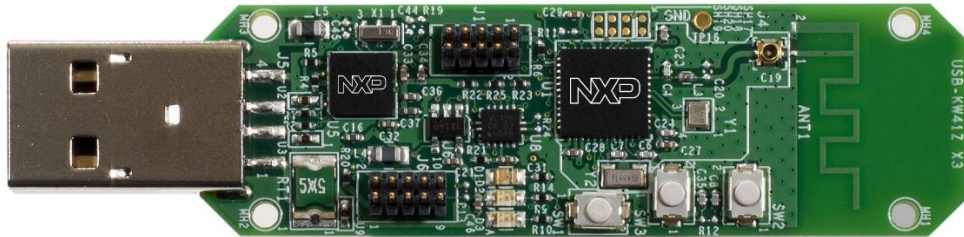


Figure 1: USB-KW41Z dongle

2 Firmware Images

The following firmware images, distributed in the KW41Z connectivity software packages, are necessary for the two microcontrollers residing on the USB-KW41Z evaluation board (KW41Z and K22F):

`<installation_folder>\tools\wireless\binaries\sniffer_usbkw41z_kw41z.bin`

Hybrid (802.15.4 and BLE) sniffer firmware for the KW41Z silicon on the USB-KW41Z board

`<installation_folder>\tools\wireless\binaries\sniffer_usbkw41z_k22f.bin`

Hybrid (802.15.4 and BLE) sniffer firmware for the K22F silicon on the USB-KW41Z board, linked at 0x0 (no OpenSDA bootloader provisioning)

`<installation_folder>\tools\wireless\binaries\sniffer_usbkw41z_k22f_0x8000.bin`

Hybrid (802.15.4 and BLE) sniffer firmware for the K22F silicon on the USB-KW41Z board, linked at 0x8000 (OpenSDA bootloader provisioning)

3 Flashing the Sniffer Firmware Using External J-Link Probe

While the sniffer firmware may come pre-flashed on the USB-KW41Z board, it may need to be re-flashed if the board does not contain it.

The Freescale KW41Z enablement software package includes the sniffer binary firmware images for the two microcontrollers soldered on the USB-KW41Z board: K22F and KW41Z. Both microcontrollers have an exposed 10-pin SWD/JTAG debug interface which can be used to flash these firmware images.

In order to flash the two pieces of firmware needed on the USB-KW41Z, a J-Link probe is needed along with the latest J-Link software from www.segger.com.

Execute **jlink.exe** from the Segger package installation and type the following commands in the command window for flashing the images on the two microcontrollers respectively, while making sure to connect the J-Link probe to the proper microcontroller's debug port (J1 for KW41Z and J6 for K22F). **Make sure that the binary files are in the same folder with the jlink.exe executable.**

3.1 Common

Select the proper emulator connected to USB-KW41 stick.

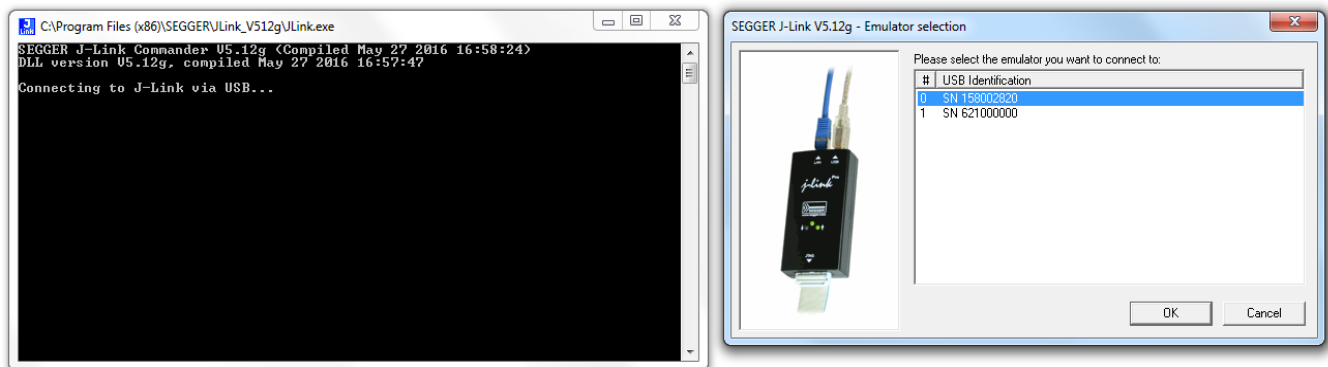
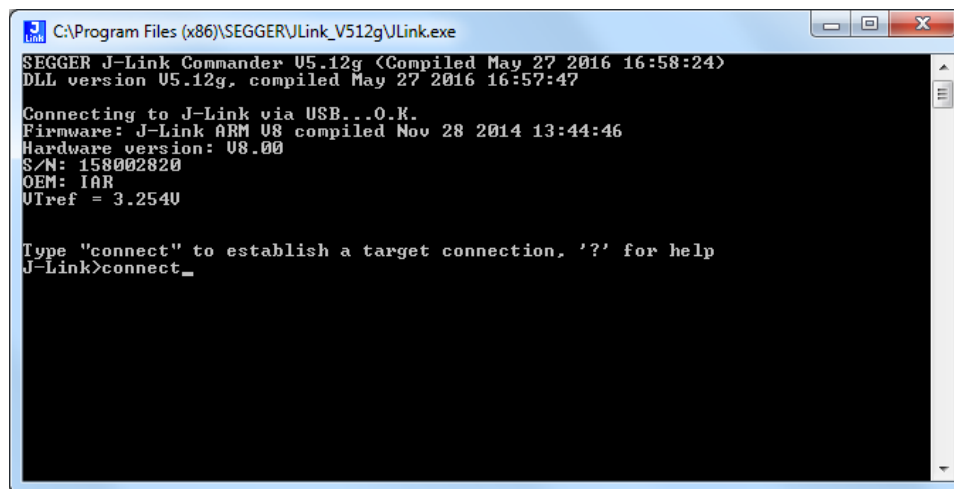


Figure 2: Emulator Selection

Type “connect” in order to establish a target connection.



```
C:\Program Files (x86)\SEGGER\JLink_V512g\JLink.exe
SEGGER J-Link Commander V5.12g (Compiled May 27 2016 16:58:24)
DLL version V5.12g, compiled May 27 2016 16:57:47

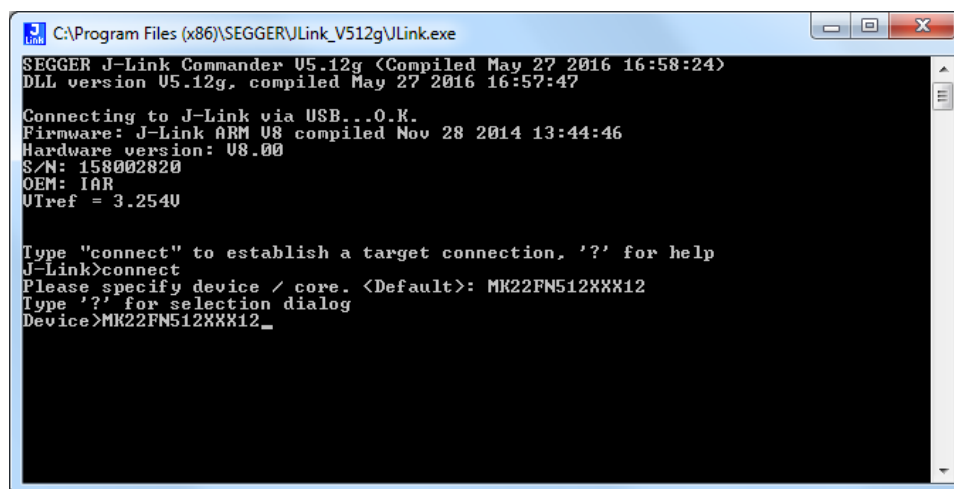
Connecting to J-Link via USB...O.K.
Firmware: J-Link ARM V8 compiled Nov 28 2014 13:44:46
Hardware version: V8.00
S/N: 158002820
OEM: IAR
Vtref = 3.254V

Type "connect" to establish a target connection, '?' for help
J-Link>connect_
```

Figure 3: Connect to target

3.2 Flashing MK22FN512xxx12

Select MK22FN512xxx12 device.



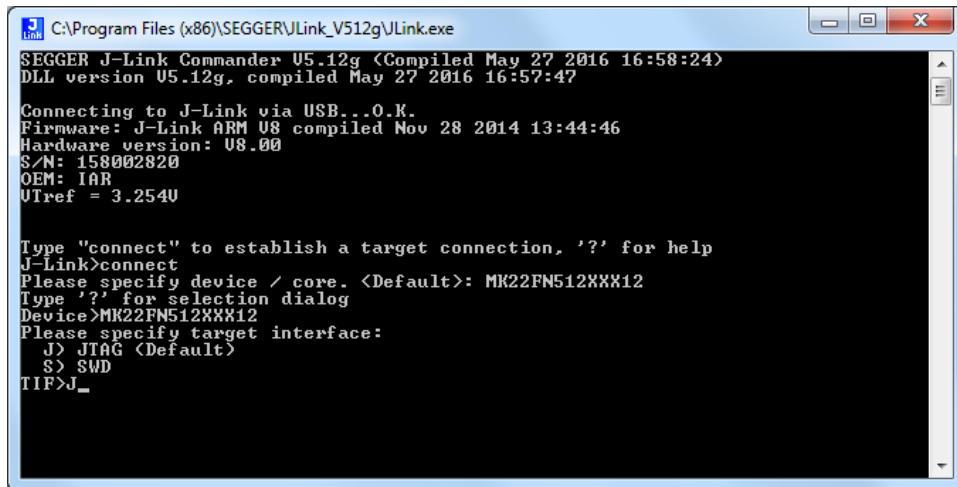
```
C:\Program Files (x86)\SEGGER\JLink_V512g\JLink.exe
SEGGER J-Link Commander V5.12g (Compiled May 27 2016 16:58:24)
DLL version V5.12g, compiled May 27 2016 16:57:47

Connecting to J-Link via USB...O.K.
Firmware: J-Link ARM V8 compiled Nov 28 2014 13:44:46
Hardware version: V8.00
S/N: 158002820
OEM: IAR
Vtref = 3.254V

Type "connect" to establish a target connection, '?' for help
J-Link>connect
Please specify device / core. (Default): MK22FN512XXX12
Type '?' for selection dialog
Device>MK22FN512XXX12_
```

Figure 4: MK22FN512xxx12 device selection

Select JTAG target interface.



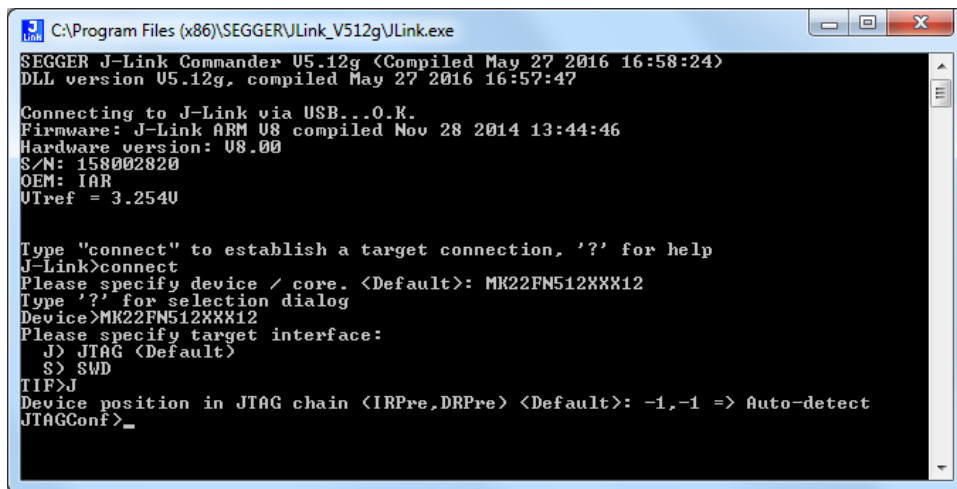
```
C:\Program Files (x86)\SEGGER\JLink_V512g\JLink.exe
SEGGER J-Link Commander V5.12g (Compiled May 27 2016 16:58:24)
DLL version V5.12g, compiled May 27 2016 16:57:47

Connecting to J-Link via USB...O.K.
Firmware: J-Link ARM V8 compiled Nov 28 2014 13:44:46
Hardware version: V8.00
S/N: 158002820
OEM: IAR
Vtref = 3.254V

Type "connect" to establish a target connection, '?' for help
J-Link>connect
Please specify device / core. <Default>: MK22FN512XXX12
Type '?' for selection dialog
Device>MK22FN512XXX12
Please specify target interface:
  J) JTAG <Default>
  S) SWD
TIF>J_
```

Figure 5: JTAG interface selection

Press “Enter” to Auto-detect the device position in JTAG chain.



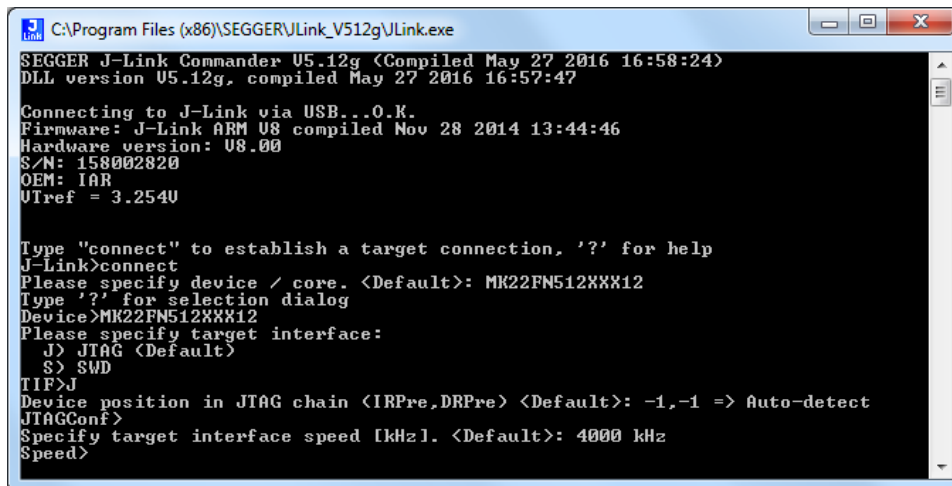
```
C:\Program Files (x86)\SEGGER\JLink_V512g\JLink.exe
SEGGER J-Link Commander V5.12g (Compiled May 27 2016 16:58:24)
DLL version V5.12g, compiled May 27 2016 16:57:47

Connecting to J-Link via USB...O.K.
Firmware: J-Link ARM V8 compiled Nov 28 2014 13:44:46
Hardware version: V8.00
S/N: 158002820
OEM: IAR
Vtref = 3.254V

Type "connect" to establish a target connection, '?' for help
J-Link>connect
Please specify device / core. <Default>: MK22FN512XXX12
Type '?' for selection dialog
Device>MK22FN512XXX12
Please specify target interface:
  J) JTAG <Default>
  S) SWD
TIF>J
Device position in JTAG chain <IRPre,DRPre> <Default>: -1,-1 => Auto-detect
JTAGConf>_
```

Figure 6: JTAG chain device position

Press “Enter” to select the default interface speed.

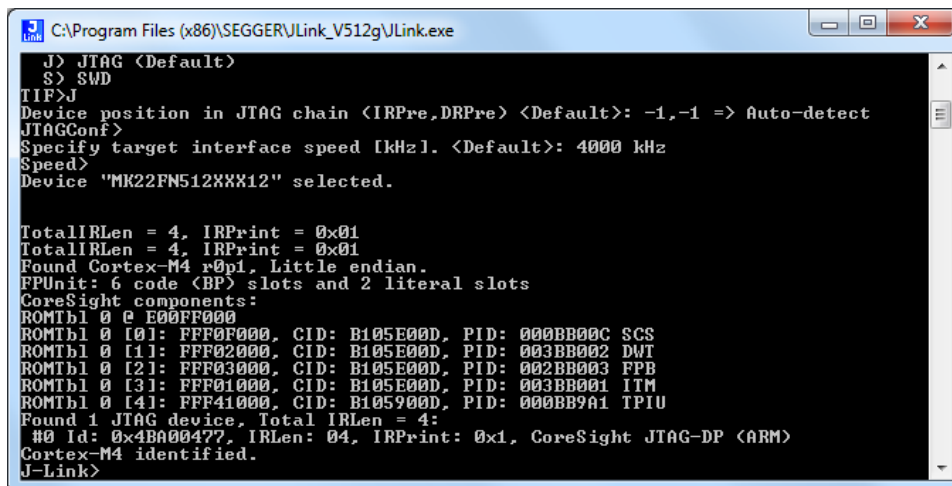


```
C:\Program Files (x86)\SEGGER\JLink_V512g\JLink.exe
SEGGER J-Link Commander V5.12g <Compiled May 27 2016 16:58:24>
DLL version V5.12g, compiled May 27 2016 16:57:47

Connecting to J-Link via USB...O.K.
Firmware: J-Link ARM V8 compiled Nov 28 2014 13:44:46
Hardware version: V8.00
S/N: 158002820
OEM: IAR
Vtref = 3.254V

Type "connect" to establish a target connection, '?' for help
J-Link>connect
Please specify device / core. <Default>: MK22FN512XXX12
Type '?' for selection dialog
Device>MK22FN512XXX12
Please specify target interface:
J> JTAG <Default>
S> SWD
TIF>J
Device position in JTAG chain <IRPre,DRPre> <Default>: -1,-1 => Auto-detect
JTAGConf>
Specify target interface speed [kHz]. <Default>: 4000 kHz
Speed>
```

Figure 7: JTAG interface speed selection

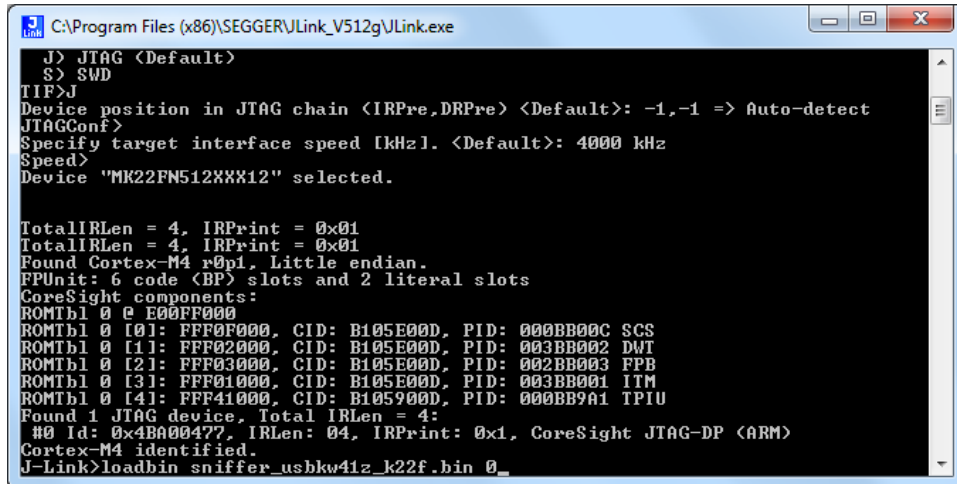


```
J> JTAG <Default>
S> SWD
TIF>J
Device position in JTAG chain <IRPre,DRPre> <Default>: -1,-1 => Auto-detect
JTAGConf>
Specify target interface speed [kHz]. <Default>: 4000 kHz
Speed>
Device "MK22FN512XXX12" selected.

TotalIRLen = 4, IRPrint = 0x01
TotalIRLen = 4, IRPrint = 0x01
Found Cortex-M4 r0p1, Little endian.
FPUnit: 6 code <BP> slots and 2 literal slots
CoreSight components:
ROMTbl 0 @ E00FF000
ROMTbl 0 [0]: FFF0F000, CID: B105E00D, PID: 000BB00C SCS
ROMTbl 0 [1]: FFF02000, CID: B105E00D, PID: 003BB002 DWT
ROMTbl 0 [2]: FFF03000, CID: B105E00D, PID: 002BB003 FPB
ROMTbl 0 [3]: FFF01000, CID: B105E00D, PID: 003BB001 ITM
ROMTbl 0 [4]: FFF41000, CID: B105900D, PID: 000BB7A1 TPIU
Found 1 JTAG device, total IRLen = 4:
#0 Id: 0x4BA00477, IRLen: 04, IRPrint: 0x1, CoreSight JTAG-DP <ARM>
Cortex-M4 identified.
J-Link>
```

Figure 8: Cortex-M4 identified

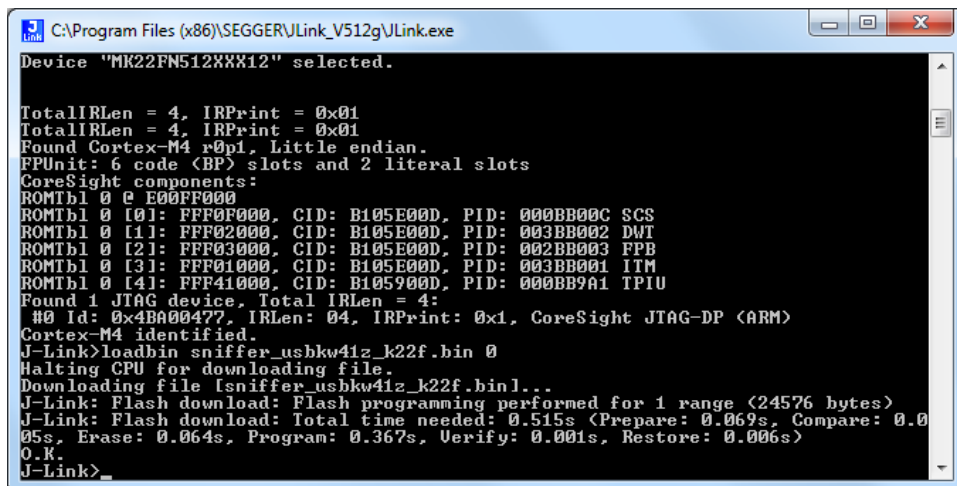
Type `loadbin sniffer_usbkw41z_k22f.bin 0` in order to flash the binary file.



```
C:\Program Files (x86)\SEGGER\JLink_V512g\VLink.exe
J> JTAG (Default)
S> SWD
TIF>J
Device position in JTAG chain (IRPre,DRPre) (Default): -1,-1 => Auto-detect
JTAGConf>
Specify target interface speed [kHz]. (Default): 4000 kHz
Speed>
Device "MK22FN512XXX12" selected.

TotalIRLlen = 4, IRPrint = 0x01
TotalIRLlen = 4, IRPrint = 0x01
Found Cortex-M4 r0p1, Little endian.
FPUnit: 6 code (BP) slots and 2 literal slots
CoreSight components:
ROMTbl 0 @ E00FF000
ROMTbl 0 [0]: FFF0F000, CID: B105E00D, PID: 000BB00C SCS
ROMTbl 0 [1]: FFF02000, CID: B105E00D, PID: 003BB002 DWT
ROMTbl 0 [2]: FFF03000, CID: B105E00D, PID: 002BB003 FPB
ROMTbl 0 [3]: FFF01000, CID: B105E00D, PID: 003BB001 ITM
ROMTbl 0 [4]: FFF41000, CID: B105900D, PID: 000BB9A1 TPIU
Found 1 JTAG device, Total IRLen = 4:
#0 Id: 0x4BA00477, IRLen: 04, IRPrint: 0x1, CoreSight JTAG-DP (ARM)
Cortex-M4 identified.
J-Link>loadbin sniffer_usbkw41z_k22f.bin 0_
```

Figure 9: Load binary file



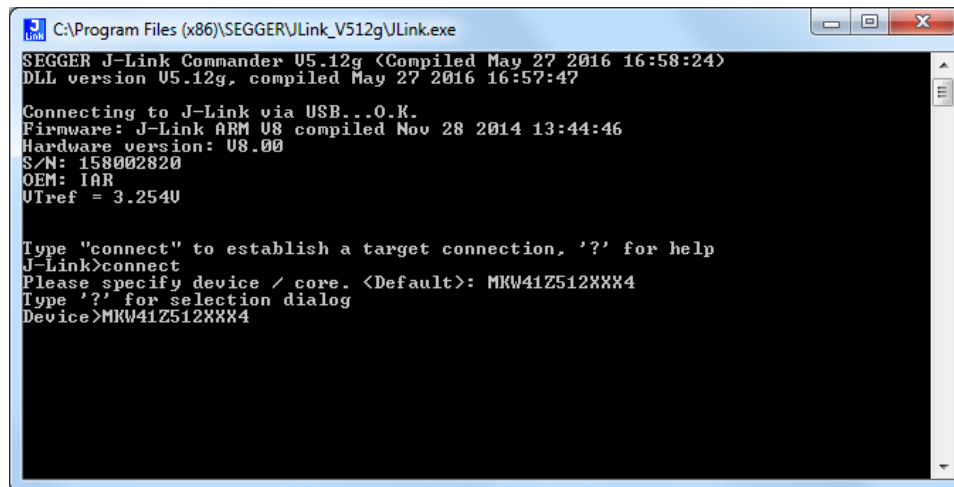
```
C:\Program Files (x86)\SEGGER\JLink_V512g\VLink.exe
Device "MK22FN512XXX12" selected.

TotalIRLlen = 4, IRPrint = 0x01
TotalIRLlen = 4, IRPrint = 0x01
Found Cortex-M4 r0p1, Little endian.
FPUnit: 6 code (BP) slots and 2 literal slots
CoreSight components:
ROMTbl 0 @ E00FF000
ROMTbl 0 [0]: FFF0F000, CID: B105E00D, PID: 000BB00C SCS
ROMTbl 0 [1]: FFF02000, CID: B105E00D, PID: 003BB002 DWT
ROMTbl 0 [2]: FFF03000, CID: B105E00D, PID: 002BB003 FPB
ROMTbl 0 [3]: FFF01000, CID: B105E00D, PID: 003BB001 ITM
ROMTbl 0 [4]: FFF41000, CID: B105900D, PID: 000BB9A1 TPIU
Found 1 JTAG device, Total IRLen = 4:
#0 Id: 0x4BA00477, IRLen: 04, IRPrint: 0x1, CoreSight JTAG-DP (ARM)
Cortex-M4 identified.
J-Link>loadbin sniffer_usbkw41z_k22f.bin 0
Halting CPU for downloading file.
Downloading file [sniffer_usbkw41z_k22f.bin]...
J-Link: Flash download: Flash programming performed for 1 range (24576 bytes)
J-Link: Flash download: Total time needed: 0.515s (Prepare: 0.069s, Compare: 0.005s, Erase: 0.064s, Program: 0.367s, Verify: 0.001s, Restore: 0.006s)
O.K.
J-Link>_
```

Figure 10: Download completed successfully

3.3 Flashing MKW41Z512xx4

Select MKW41Z512xxx4 device.



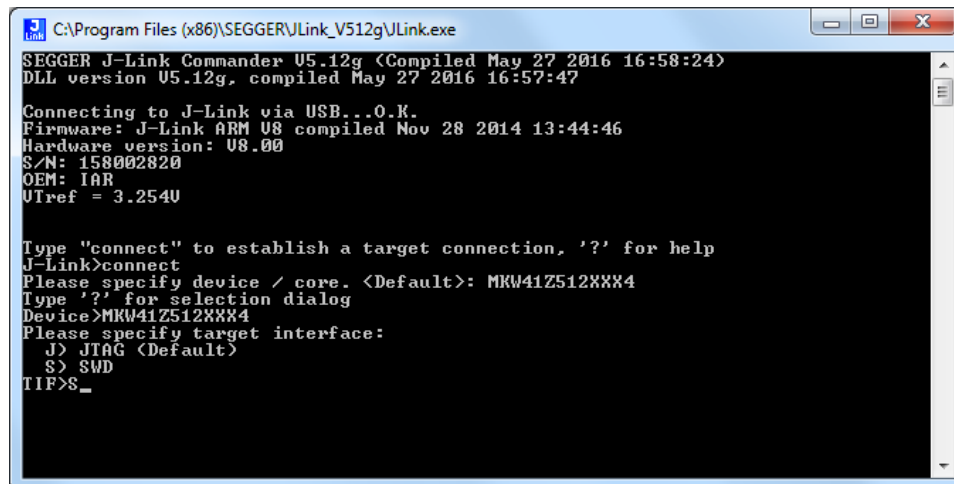
```
C:\Program Files (x86)\SEGGER\JLink_V512g\JLink.exe
SEGGER J-Link Commander V5.12g (Compiled May 27 2016 16:58:24)
DLL version V5.12g, compiled May 27 2016 16:57:47

Connecting to J-Link via USB...O.K.
Firmware: J-Link ARM V8 compiled Nov 28 2014 13:44:46
Hardware version: V8.00
S/N: 158002820
OEM: IAR
Vtref = 3.254V

Type "connect" to establish a target connection, '?' for help
J-Link>connect
Please specify device / core. (Default): MKW41Z512XXX4
Type '?' for selection dialog
Device>MKW41Z512XXX4
```

Figure 11: MKW41Z512xxx4 device selection

Select SWD target interface.



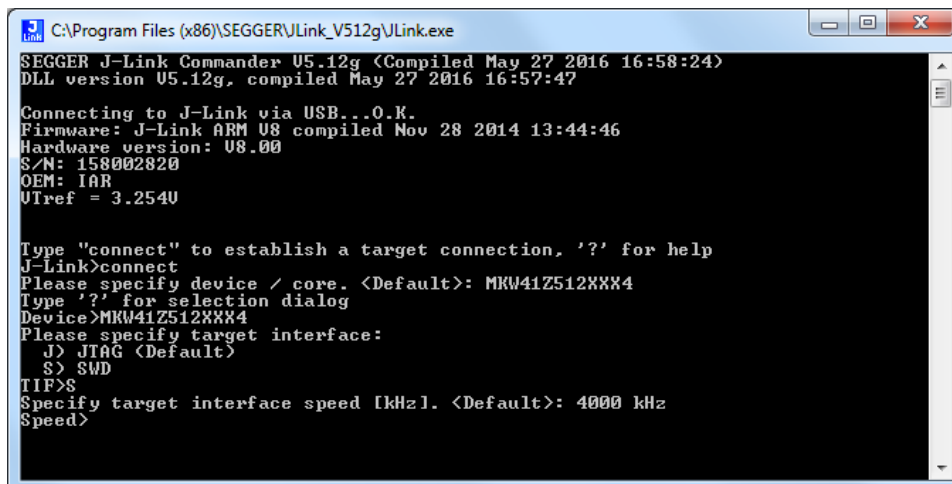
```
C:\Program Files (x86)\SEGGER\JLink_V512g\JLink.exe
SEGGER J-Link Commander V5.12g (Compiled May 27 2016 16:58:24)
DLL version V5.12g, compiled May 27 2016 16:57:47

Connecting to J-Link via USB...O.K.
Firmware: J-Link ARM V8 compiled Nov 28 2014 13:44:46
Hardware version: V8.00
S/N: 158002820
OEM: IAR
Vtref = 3.254V

Type "connect" to establish a target connection, '?' for help
J-Link>connect
Please specify device / core. (Default): MKW41Z512XXX4
Type '?' for selection dialog
Device>MKW41Z512XXX4
Please specify target interface:
J) JTAG (Default)
S) SWD
TIF>S_
```

Figure 12: SWD interface selection

Press “Enter” to select the default interface speed.

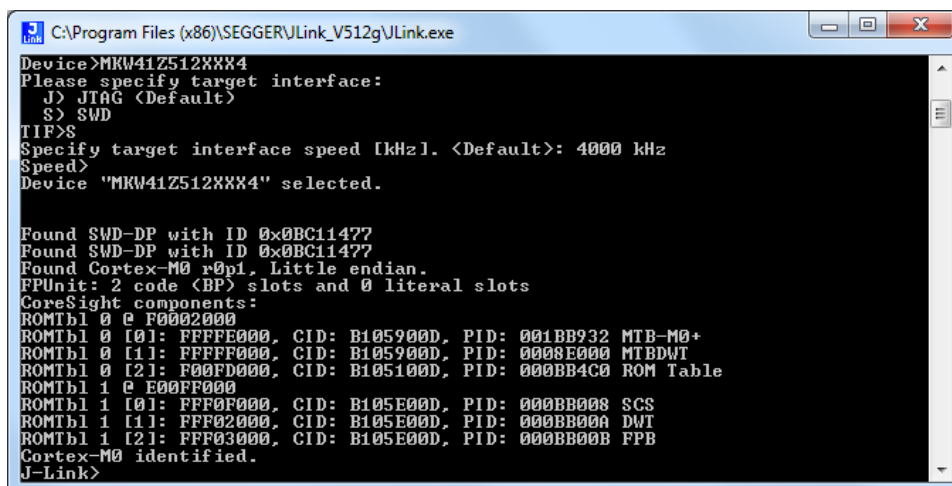


```
C:\Program Files (x86)\SEGGER\JLink_V512g\JLink.exe
SEGGER J-Link Commander V5.12g <Compiled May 27 2016 16:58:24>
DLL version V5.12g, compiled May 27 2016 16:57:47

Connecting to J-Link via USB...O.K.
Firmware: J-Link ARM V8 compiled Nov 28 2014 13:44:46
Hardware version: V8.00
S/N: 158002820
OEM: IAR
Vtref = 3.254V

Type "connect" to establish a target connection, '?' for help
J-Link>connect
Please specify device / core. <Default>: MKW41Z512XXX4
Type '?' for selection dialog
Device>MKW41Z512XXX4
Please specify target interface:
  J> JTAG <Default>
  S> SWD
TIF>S
Specify target interface speed [kHz]. <Default>: 4000 kHz
Speed>
```

Figure 13: SWD interface speed selection

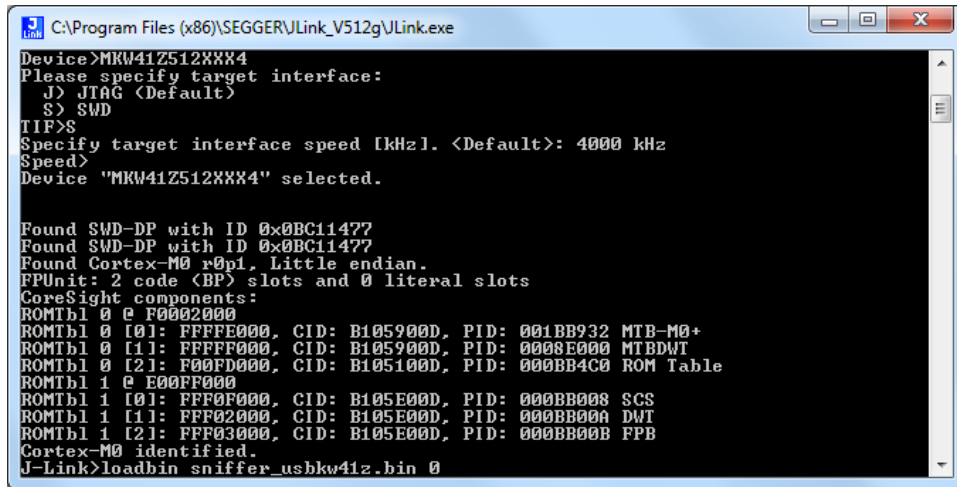


```
Device>MKW41Z512XXX4
Please specify target interface:
  J> JTAG <Default>
  S> SWD
TIF>S
Specify target interface speed [kHz]. <Default>: 4000 kHz
Speed>
Device "MKW41Z512XXX4" selected.

Found SWD-DP with ID 0x0BC11477
Found SWD-DP with ID 0x0BC11477
Found Cortex-M0 r0p1, Little endian.
FPUnit: 2 code <BP> slots and 0 literal slots
CoreSight components:
ROMTbl 0 @ F0002000
ROMTbl 0 [0]: FFFF0000, CID: B105900D, PID: 001BB932 MTB-M0+
ROMTbl 0 [1]: FFFF0000, CID: B105900D, PID: 0008E000 MTBDWT
ROMTbl 0 [2]: F00FD000, CID: B105100D, PID: 000BB4C0 ROM Table
ROMTbl 1 @ E00FF000
ROMTbl 1 [0]: FFF0F000, CID: B105E00D, PID: 000BB008 SCS
ROMTbl 1 [1]: FFF02000, CID: B105E00D, PID: 000BB00A DWI
ROMTbl 1 [2]: FFF03000, CID: B105E00D, PID: 000BB00B FPB
Cortex-M0 identified.
J-Link>
```

Figure 14: Cortex-M0 identified

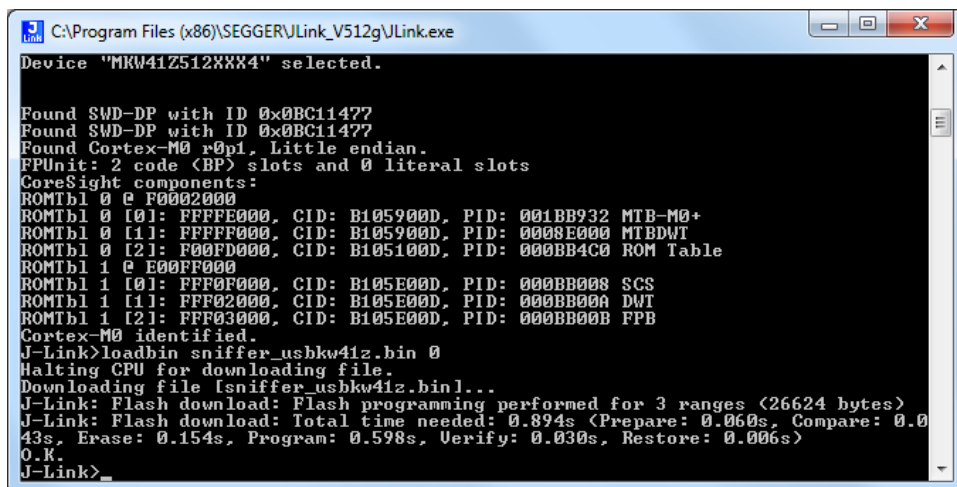
Type `loadbin sniffer_usbkw41z_kw41z.bin 0` in order to flash the binary file.



```
C:\Program Files (x86)\SEGGER\JLink_V512g\JLink.exe
Device>MKW41Z512XXX4
Please specify target interface:
J> JTAG <Default>
S> SWD
TIF>S
Specify target interface speed [kHz]. <Default>: 4000 kHz
Speed>
Device "MKW41Z512XXX4" selected.

Found SWD-DP with ID 0x0BC11477
Found SWD-DP with ID 0x0BC11477
Found Cortex-M0 r0p1, Little endian.
FPUnit: 2 code <BP> slots and 0 literal slots
CoreSight components:
ROMTbl 0 @ F0002000
ROMTbl 0 [0]: FFFFE000, CID: B105900D, PID: 001BB932 MTB-M0+
ROMTbl 0 [1]: FFFFF000, CID: B105900D, PID: 0008E000 MTBDWT
ROMTbl 0 [2]: F00FD000, CID: B105100D, PID: 000BB4C0 ROM Table
ROMTbl 1 @ E00FF000
ROMTbl 1 [0]: FFF0F000, CID: B105E00D, PID: 000BB008 SCS
ROMTbl 1 [1]: FFF02000, CID: B105E00D, PID: 000BB00A DWT
ROMTbl 1 [2]: FFF03000, CID: B105E00D, PID: 000BB00B FPB
Cortex-M0 identified.
J-Link>loadbin sniffer_usbkw41z.bin 0
```

Figure 15: Load binary file



```
C:\Program Files (x86)\SEGGER\JLink_V512g\JLink.exe
Device "MKW41Z512XXX4" selected.

Found SWD-DP with ID 0x0BC11477
Found SWD-DP with ID 0x0BC11477
Found Cortex-M0 r0p1, Little endian.
FPUnit: 2 code <BP> slots and 0 literal slots
CoreSight components:
ROMTbl 0 @ F0002000
ROMTbl 0 [0]: FFFFE000, CID: B105900D, PID: 001BB932 MTB-M0+
ROMTbl 0 [1]: FFFFF000, CID: B105900D, PID: 0008E000 MTBDWT
ROMTbl 0 [2]: F00FD000, CID: B105100D, PID: 000BB4C0 ROM Table
ROMTbl 1 @ E00FF000
ROMTbl 1 [0]: FFF0F000, CID: B105E00D, PID: 000BB008 SCS
ROMTbl 1 [1]: FFF02000, CID: B105E00D, PID: 000BB00A DWT
ROMTbl 1 [2]: FFF03000, CID: B105E00D, PID: 000BB00B FPB
Cortex-M0 identified.
J-Link>loadbin sniffer_usbkw41z.bin 0
Halting CPU for downloading file.
Downloading file [sniffer_usbkw41z.bin]...
J-Link: Flash download: Flash programming performed for 3 ranges (26624 bytes)
J-Link: Flash download: Total time needed: 0.894s (Prepare: 0.060s, Compare: 0.043s, Erase: 0.154s, Program: 0.598s, Verify: 0.030s, Restore: 0.006s)
O.K.
J-Link>
```

Figure 16: Download completed successfully

4 User Interface – Kinetis Protocol Analyzer Adapter

NOTE

In order to be able to use the USB-KW41Z BLE and IEEE® 802.15.4 sniffer, **Kinetis Protocol Analyzer Adapter** software have to be installed on the Windows® machine. This software is available for download on the NXP website. Please follow the installation instructions in the respective package.

Launch **Kinetis Protocol Analyzer Adapter** software. It will automatically start to detect the connected Sniffer interfaces.

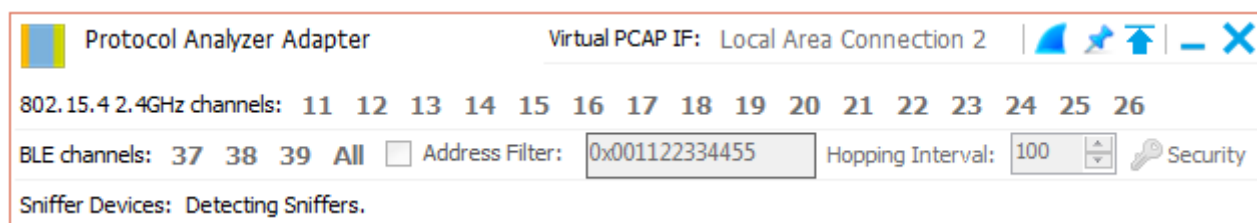


Figure 17: Kinetis Protocol Analyzer Adapter

After the detection is complete the connected device name will appear in Sniffer Devices row.

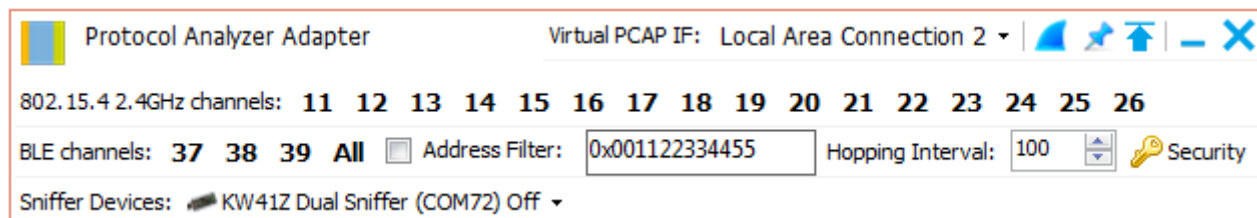


Figure 18: Sniffer Detection completed

Start the Wireshark Network Analyzer by clicking the icon in upper right corner.

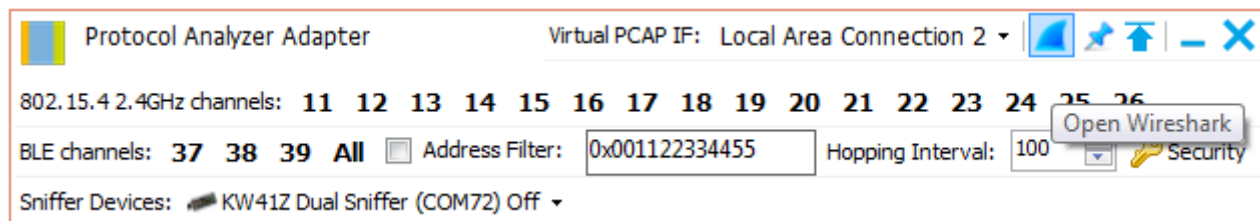


Figure 19: Wireshark Network Analyzer Shortcut

Start the Wireshark Capture session on the Local Area Connection created by the Kinetis Protocol Analyzer Adapter.

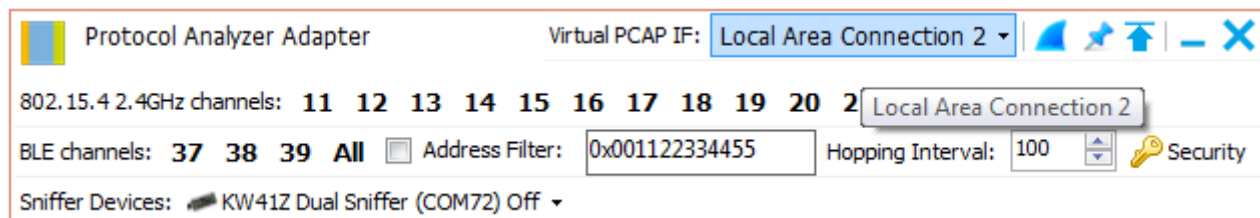


Figure 20: Local Area Connection virtual interface

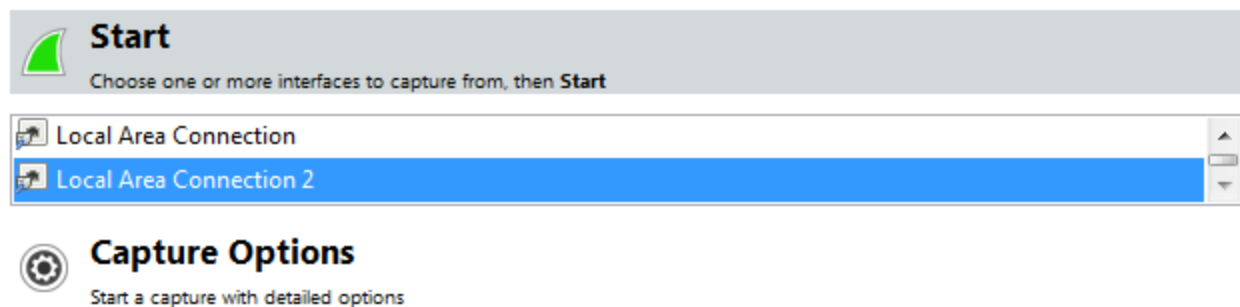


Figure 21: Start Wireshark on the required network interface

4.1 Sniffing Bluetooth® Low Energy v4.2 Wireless Communications

Start the capture by pressing one (or many) Advertising Channel button(s).

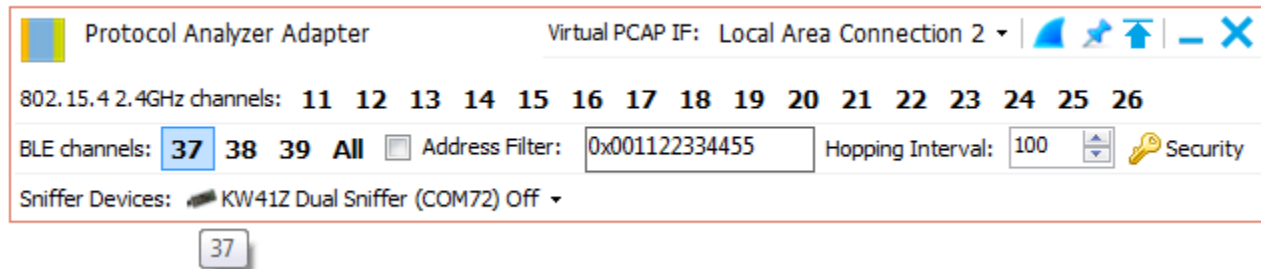


Figure 22: Advertising Channel selection

The incoming advertising data will be displayed in the Wireshark Network Analyzer's capture window.

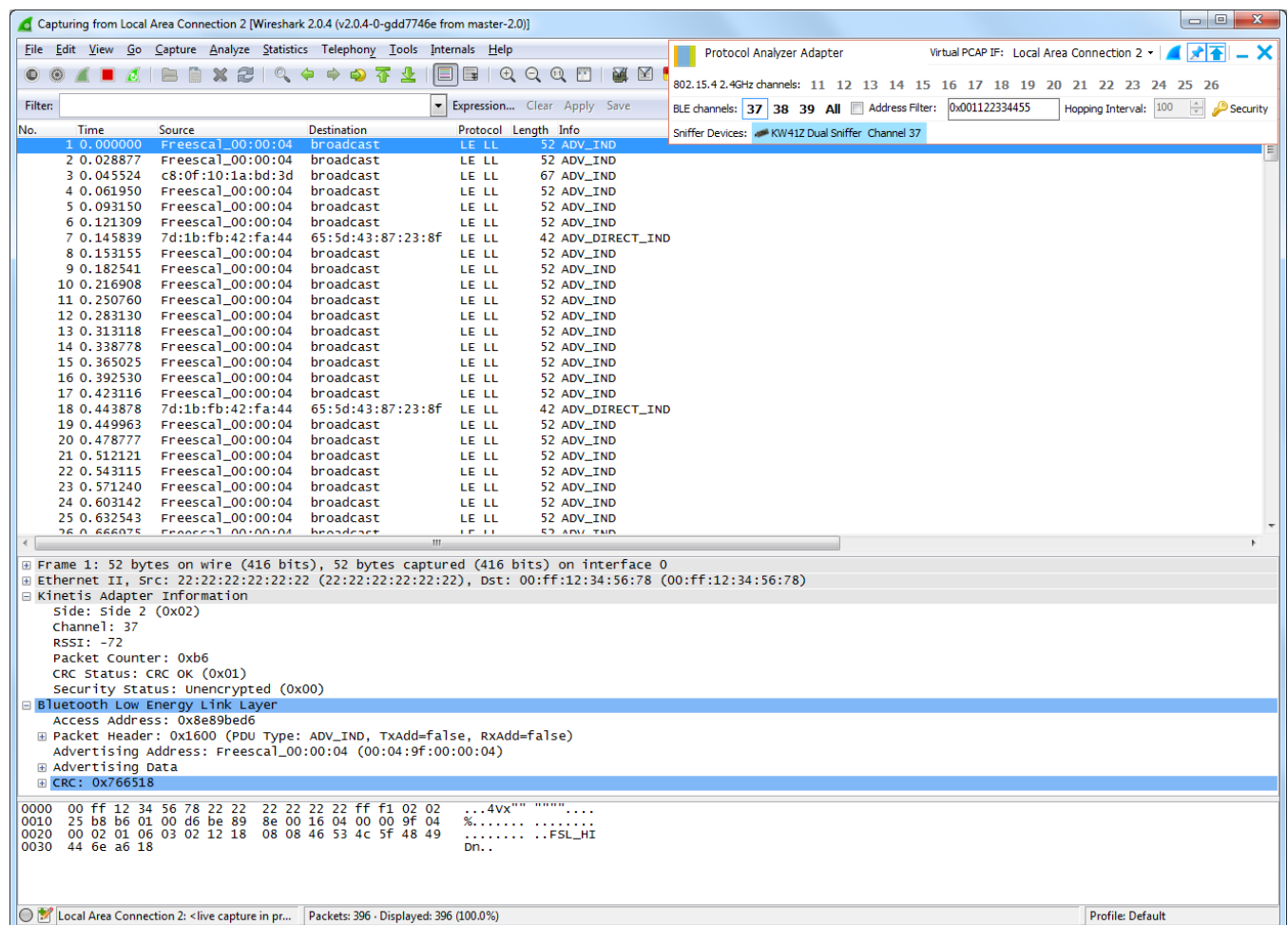


Figure 23: Wireshark Capture window

In order to filter the packets by Advertising Address, the Address Filter have to be set.

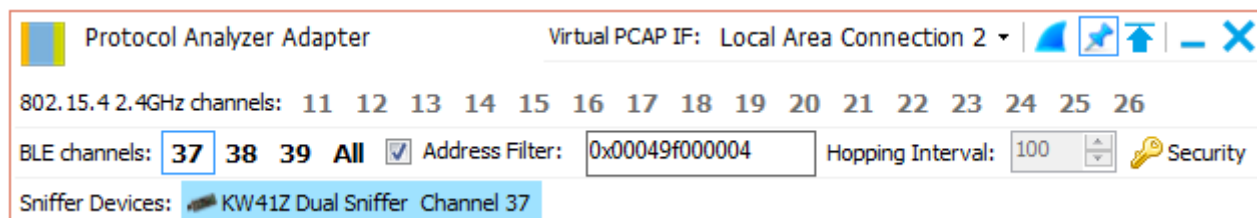


Figure 24: Advertising Address Filtering

If the Advertising Address is not known or not taken into consideration, an advertising channel dwell or hop interval for the advertising channels can be defined. The hopping interval is in milliseconds and is used if no Address was set to be filtered and more than 2 advertising channels were selected.

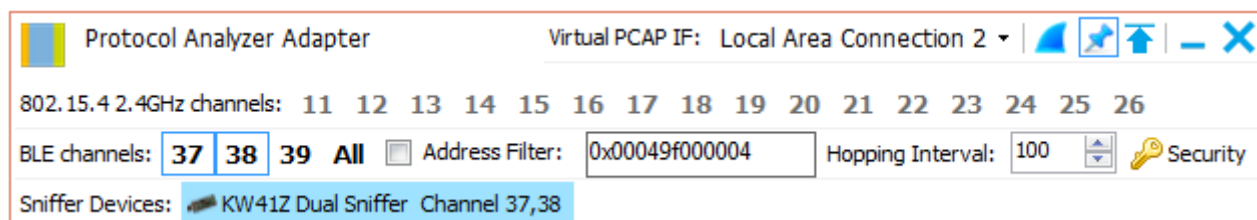


Figure 25: Advertising Hop Interval

For the encrypted connections the PIN and Long Term key values can be set from the “Security” window in order to successfully decrypt the received frames.

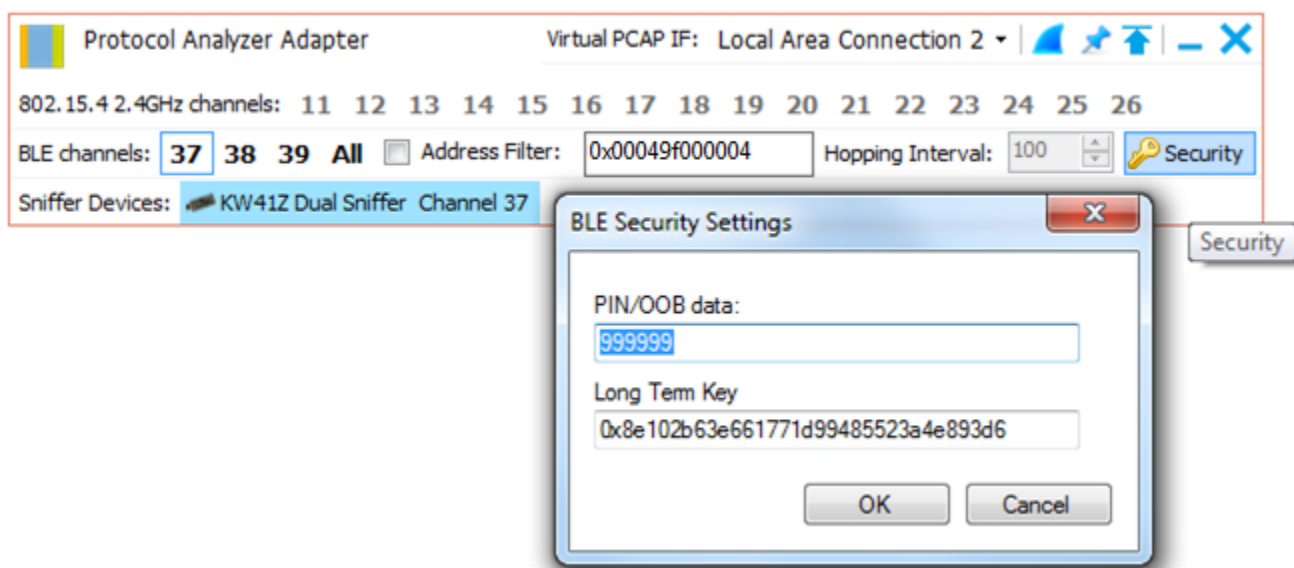


Figure 26: Security Settings

4.2 Sniffing IEEE® 802.15.4 Wireless Communications

4.2.1 Wireshark Protocol Analyzer Adapter

Start the capture by pressing one of the 802.15.4 Channel buttons when the sniffer is idle.

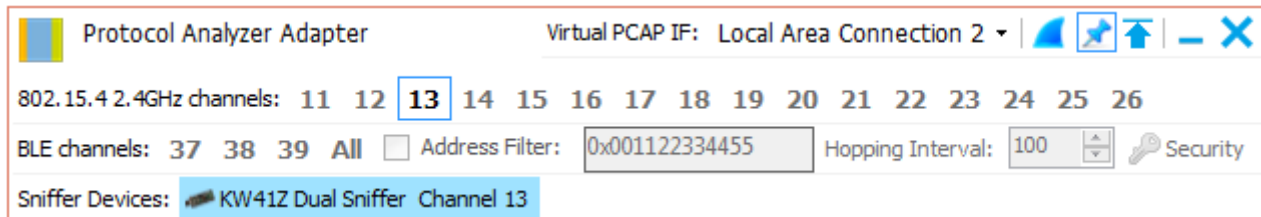


Figure 28: 802.15.4 Channel selection

The incoming data will be displayed in the Wireshark Network Analyzer's capture window.

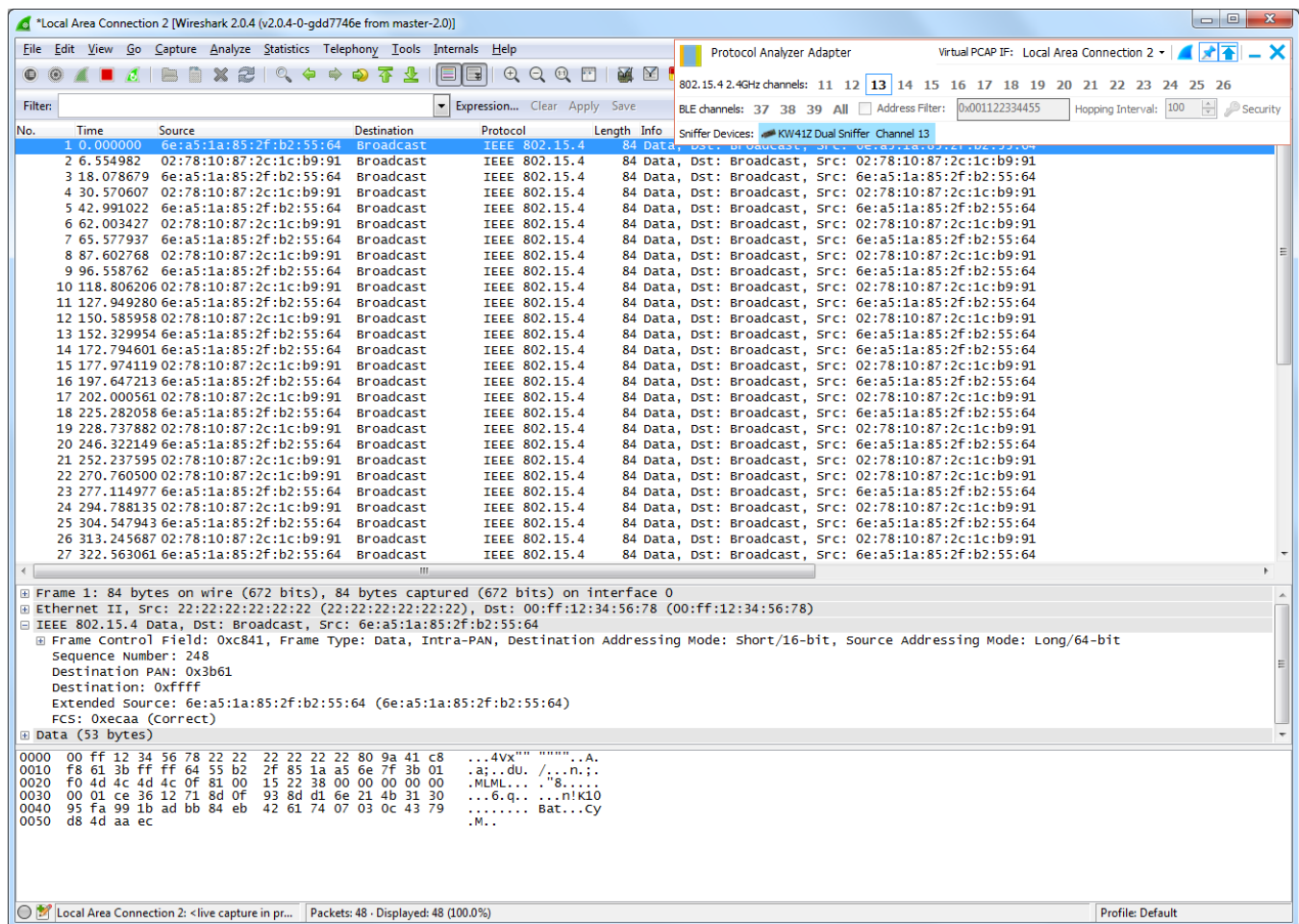


Figure 29: Wireshark capture window

4.2.2 Test Tool for Connectivity Products

The USB-KW41Z sniffer is compatible with the Test Tool for Connectivity Products IEEE 802.15.4 protocol analyzer, starting with version 12.6 of the tool. For more information, please refer chapter 6 of NXP Test Tool User's Guide (*TTUG.pdf*).

5 Revision history

This table summarizes revisions to this document.

Table 1. Revision history		
Revision number	Date	Substantive changes
0	04/2016	Initial release
1	7/2016	Updated J-Link commands
2	09/2016	Added test tool information

How to Reach Us:

Home Page:

www.nxp.com

Web Support:

www.nxp.com/support

Information in this document is provided solely to enable system and software implementers to use Freescale products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits based on the information in this document.

Freescale reserves the right to make changes without further notice to any products herein. Freescale makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does Freescale assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. "Typical" parameters that may be provided in Freescale data sheets and/or specifications can and do vary in different applications, and actual performance may vary over time. All operating parameters, including "typicals," must be validated for each customer application by customer's technical experts. Freescale does not convey any license under its patent rights nor the rights of others. Freescale sells products pursuant to standard terms and conditions of sale, which can be found at the following address: nxp.com/SalesTermsandConditions.

Freescale, the Freescale logo, and Kinetis are trademarks of Freescale Semiconductor, Inc., Reg. U.S. Pat. & Tm. Off. IEEE 802.15.4 is a trademark of the Institute of Electrical and Electronics Engineers, Inc. (IEEE). This product is not endorsed or approved by the IEEE. All other product or service names are the property of their respective owners. ARM, the ARM powered logo, and Cortex are registered trademarks of ARM Limited (or its subsidiaries) in the EU and/or elsewhere. ZigBee is a registered trademark of ZigBee Alliance, Inc. All rights reserved.

© 2016 Freescale Semiconductor, Inc.

Document number: MKW41ZSNIFFERQSG
Rev. 1
09/2016

