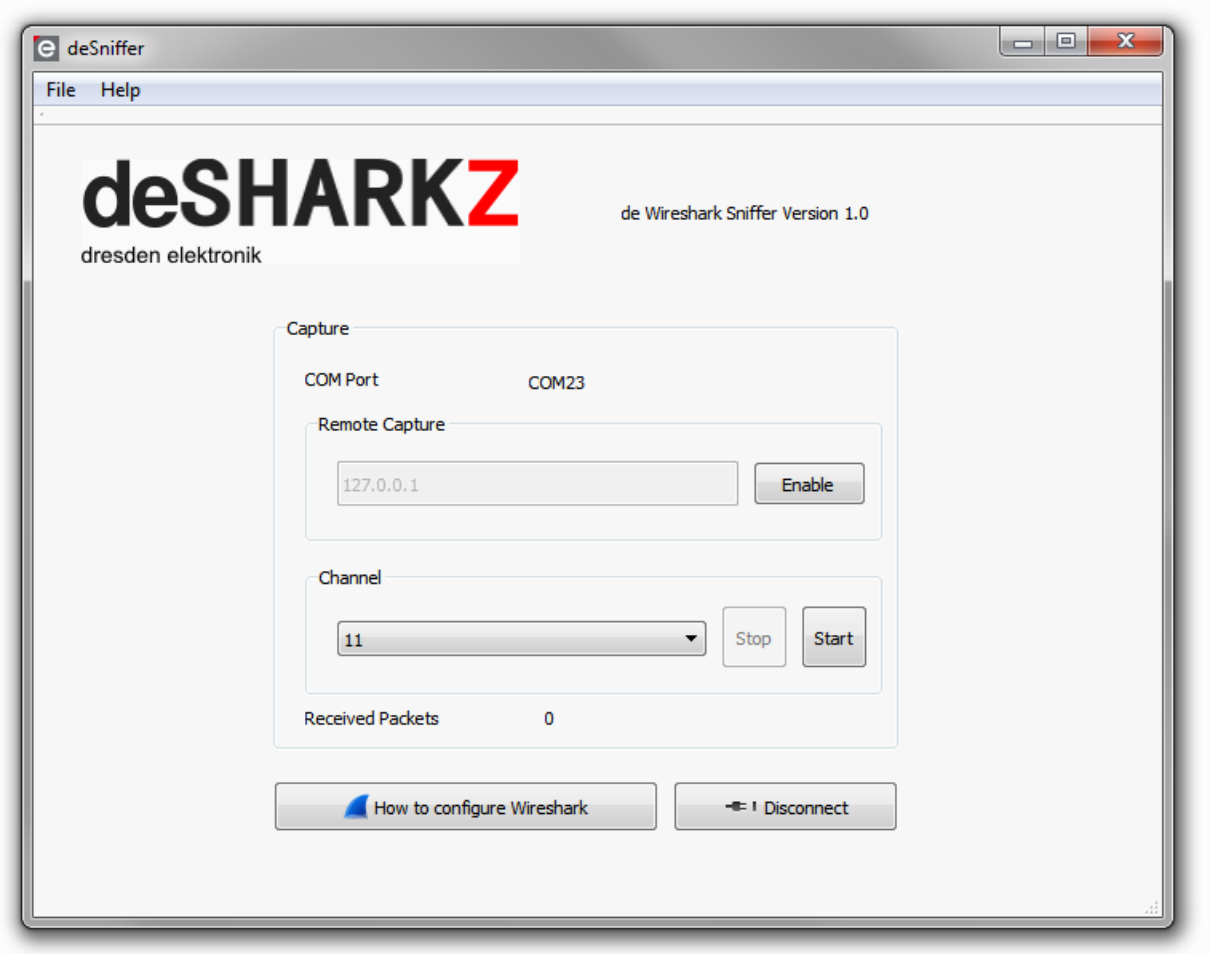
dresden elektronik

User Manual
deSHARKZ



Document Version V1.00
2018-01-10

Table of contents

Document history

Date	Version	Description
2018-01-10	1.00	Initial version

Abbreviations

Abbreviation	Description
GUI	Graphical User Interface
ZigBee	Wireless networking standard targeted at low-power applications

1. Overview

ZigBee is a technology which offers a powerful solution to a wide range of low-power, low-cost wireless sensor network applications. Some popular application profiles are Home Automation, Smart Energy and Health Care; beside them and other public profiles ZigBee PRO provides the possibility to easily develop special purpose applications.

In many stages of a product development process it is necessary to investigate the network traffic between ZigBee devices. A popular tool for this purpose is the Wireshark[1] network sniffer. dresden elektronik offers compatible hard- and software that will work with Wireshark.

2. Application

The main use case for the deSHARKZ application is sniffing of ZigBee traffic using the popular Wireshark network sniffer. It uses the ZEP packet format and sends received ZigBee frames to the udp port 17754.

2.1 Required Hardware

To use the deSHARKZ application you need appropriate hardware that is capable of communicate with other ZigBee devices. ConBee is a ZigBee capable radio USB dongle that turns any PC or MAC with a free USB port into a ZigBee gateway. Before you can use the deSHARKZ application you have to set up your device and install all required software. A detailed description for this is available for ConBee[2].

Figure 1: ConBee USB dongle

2.2 Required Software

The deSHARKZ installer provides the main application and the GCFFlasher tool which is needed to install and update the firmware to your ConBee USB dongle. Furthermore you have to install the Wireshark[1] application (> v2.2.5) and the Npcap[3] library (> v0.84) for Windows. On Linux you only need Wireshark (tested with v2.2.6).

[1] https://www.wireshark.org
[2] https://www.dresden-elektronik.de/conbee
[3] https://nmap.org/npcap/

2.3 Supported Operating Systems

- Microsoft Windows 7, 8, 8.1 and 10
- Linux (Ubuntu, Raspbian)

3. Getting started

deSHARKZ is shipped with an installer which provides the application and a firmware install tool. Wireshark and Npcap musst be downloaded and installed individually.

After starting the deSHARKZ application you will see the start screen (fig. 2). You can choose a device to connect in the drop down list (1). Press the arrow button (2) to refresh the connected devices list.

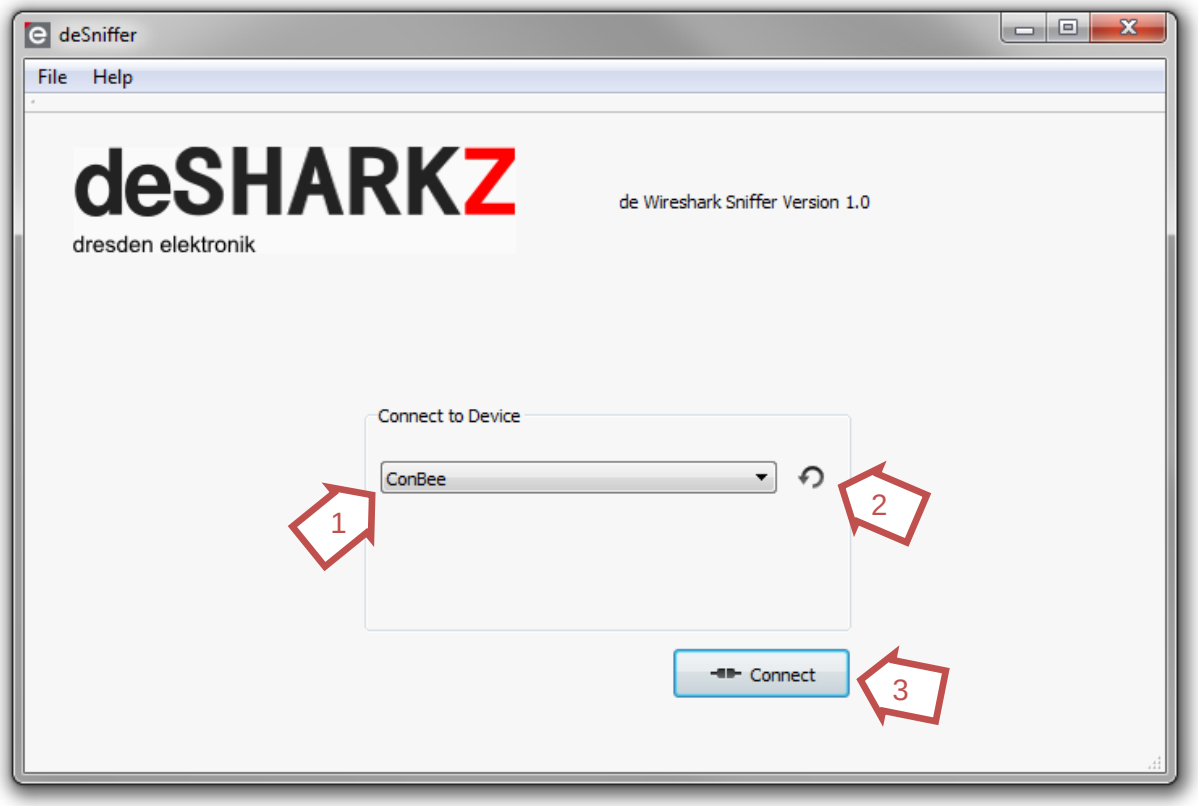


Figure 2: deSHARKZ start screen

3.1 Connect device to PC

Connect the ConBee USB dongle to your pc. If you use the ConBee for the first time Windows will install the USB drivers automatically. If there are problems during the drivers

install please refer to the ConBee user manual[4]. Choose the ConBee from the devices list. Then press the Connect button (3).

3.2 Install firmware

If the USB dongle has no or the wrong firmware installed the install firmware view (fig. 3) will be displayed. Be sure that there is only one USB dongle connected to your pc and then click at the Install Firmware button. After installation is finished it is recommended to replug the USB dongle.

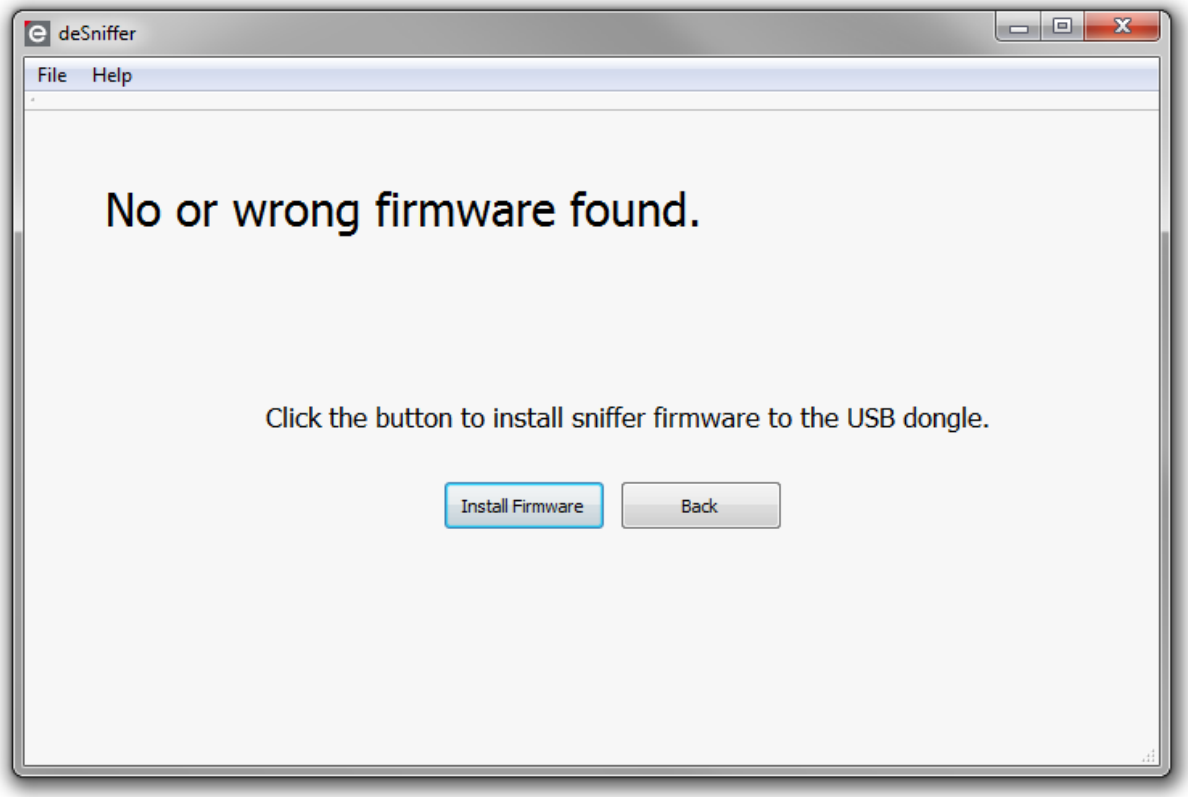


Figure 3: update firmware view

3.3 Configure Wireshark

Windows:

Open the Wireshark application and choose the Npcap Loopback Adapter to start sniffing. To show only ZigBee traffic apply the display filter: **`udp.port==17754`**

[4] https://www.dresden-elektronik.de/funktechnik/solutions/wireless-light-control/gateways/conbee/?eID=dam_frontend_push&docID=5042

Linux:

Open the Wireshark application and choose the Loopback Adapter (lo). A display filter is not needed.

General:

To add ZigBee Keys for decryption go to: Edit/Settings/Protocols/ZigBee.

3.4 Start sniffing

After clicking at the connect button and if the correct firmware is installed the main control view will be visible (fig. 4). The COM port identifier (4) indicates a successful connection to the USB dongle. You can choose a ZigBee channel from the drop down list (5). A click at Start (6) starts sniffing at the chosen channel.

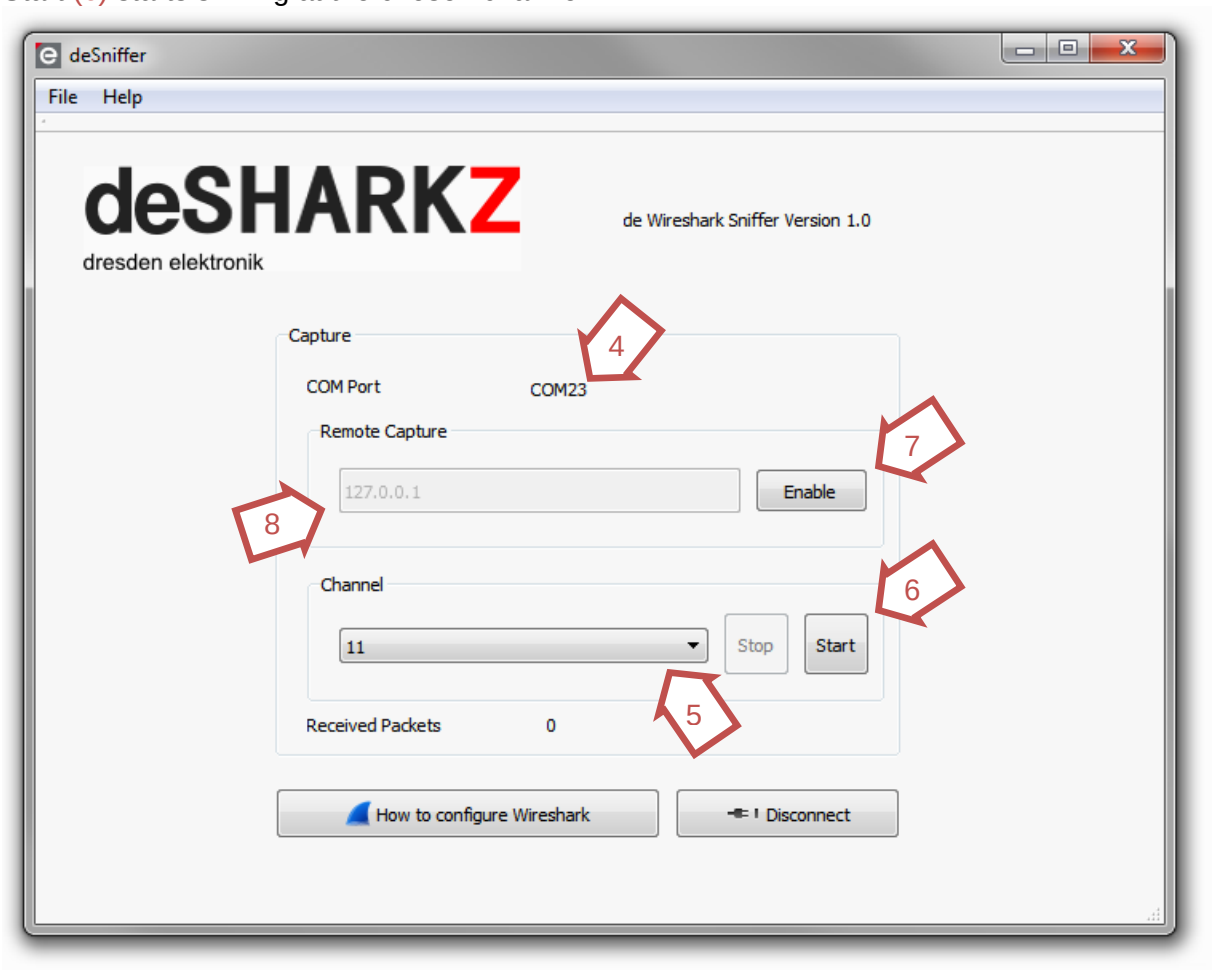


Figure 4: main control view

3.5 Remote Capture

You can run deSHARKZ on one pc or Raspberry Pi to capture traffic and send the data to Wireshark which runs on another system in the same network. To do so, enable remote capturing by clicking at the enable button (7). Then enter the ip address (without http or port number) in the input field (8). On the other system configure Wireshark as follows:
Connect to the LAN adapter. Use the display filter **`udp.port==17754`**. In the Ethernet settings (Edit/Settings/Protocols/Ethernet) disable: **Assume packets have FCS** and **Validate the Ethernet checksum if possible**.

4. Firmware update

To start a firmware update manually you can use the command line tool GCFFlasher which is shipped with the deSHARKZ installer. Open a command promt and enter “GCFFlasher” followed by these arguments: “-d <device to use> -f <file to use>”. You can enter “GCFFlasher –h” to print a list of all functions.

A detailed description of the GCFFlasher tool can be found in the ConBee user manual[5] in section 5.

5. Known problems

In Wireshark:

- Don’t read the LQI value from the ZEP tab. Read the value from the IEEE 802.15.4/Frame Check Sequence tab instead.
- The RSSI value from the IEEE 802.15.4/Frame Check Sequence tab is not the correct one.

[5] https://www.dresden-elektronik.de/funktechnik/solutions/wireless-light-control/gateways/conbee/?eID=dam_frontend_push&docID=5042

dresden elektronik ingenieurtechnik gmbh
Enno-Heidebroek-Straße 12
01237 Dresden
GERMANY

Phone +49 351 - 31850 0
Fax +49 351 - 31850 10
Email wireless@dresden-elektronik.de

Trademarks and acknowledgements

• ZigBee is a registered trademark of the ZigBee Alliance.

• IEEE 802.15.4 is a trademark of the Institute of Electrical and Electronics Engineers (IEEE).

These trademarks are registered by their respective owners in certain countries only. Other brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such.

Disclaimer

This note is provided as-is and is subject to change without notice. Except to the extent prohibited by law, dresden elektronik ingenieurtechnik gmbh makes no express or implied warranty of any kind with regard to this guide, and specifically disclaims the implied warranties and conditions of merchantability and fitness for a particular purpose. dresden elektronik ingenieurtechnik gmbh shall not be liable for any errors or incidental or consequential damage in connection with the furnishing, performance or use of this guide.