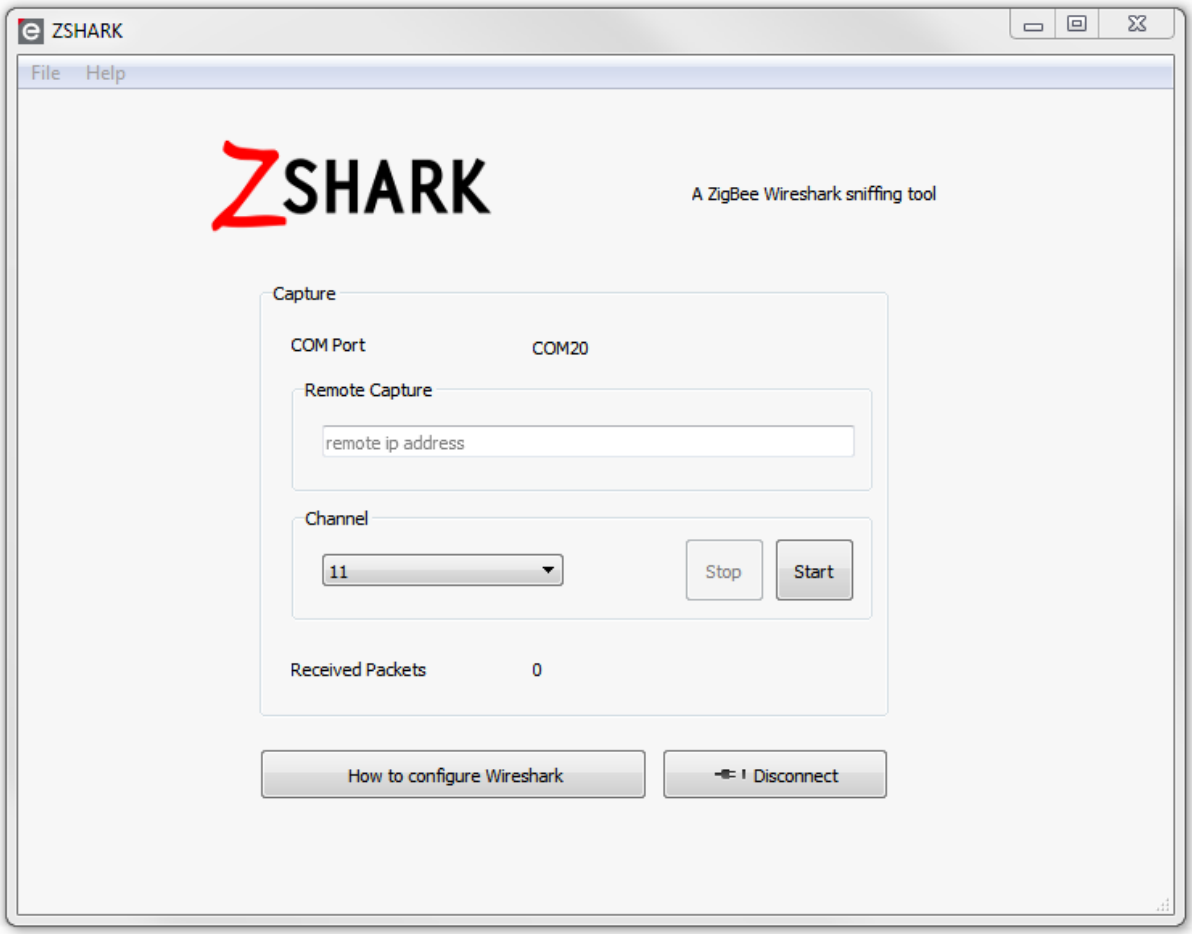
dresden elektronik

User Manual
ZSHARK



Document Version V1.04
2021-06-04

Table of contents

Document history

Date	Version	Description
2018-01-10	1.00	Initial version
2018-07-13	1.01	Added more information and screenshots
2018-09-25	1.02	Fixed some typos
2019-04-12	1.03	Added command line arguments section
2021-06-04	1.04	Added ConBee2 support, updated app functions

Abbreviations

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

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 ZSHARK 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

- **ConBee**
- **ConBee II**
- **RaspBee**

To use the ZSHARK 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. The ConBee II[3] is the successor of the ConBee. The RaspBee module for Raspberry Pi is also supported.

Figure 1: ConBee II USB dongle

2.2 Required Software

The ZSHARK 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 optionally the Npcap[2] library for Windows. On Linux you only need Wireshark (tested with v2.2.6).

[1] https://www.wireshark.org
[2] https://nmap.org/npcap/
[3] https://phoscon.de/de/conbee2/

2.3 Supported Operating Systems

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

3. Getting started

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

After starting the ZSHARK 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.

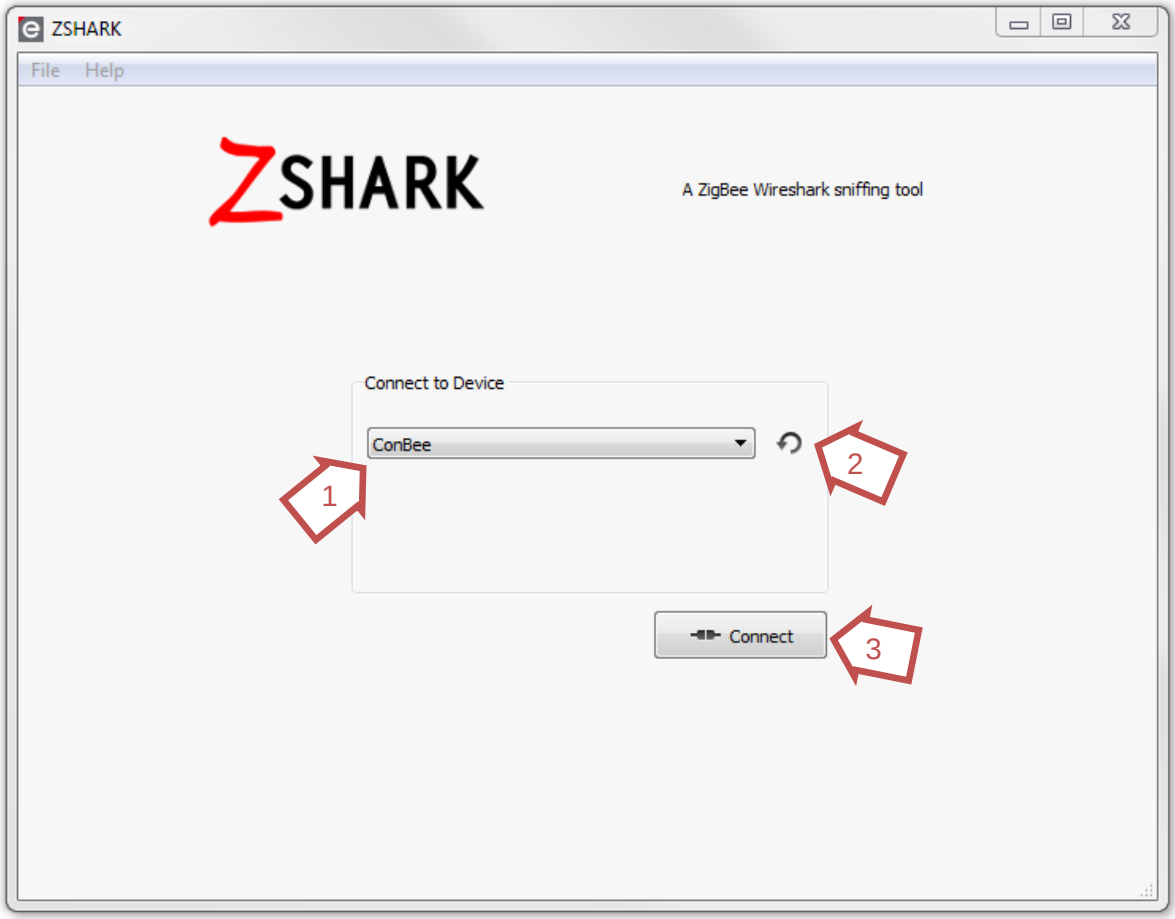


Figure 2: ZSHARK start screen

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[3]. 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.

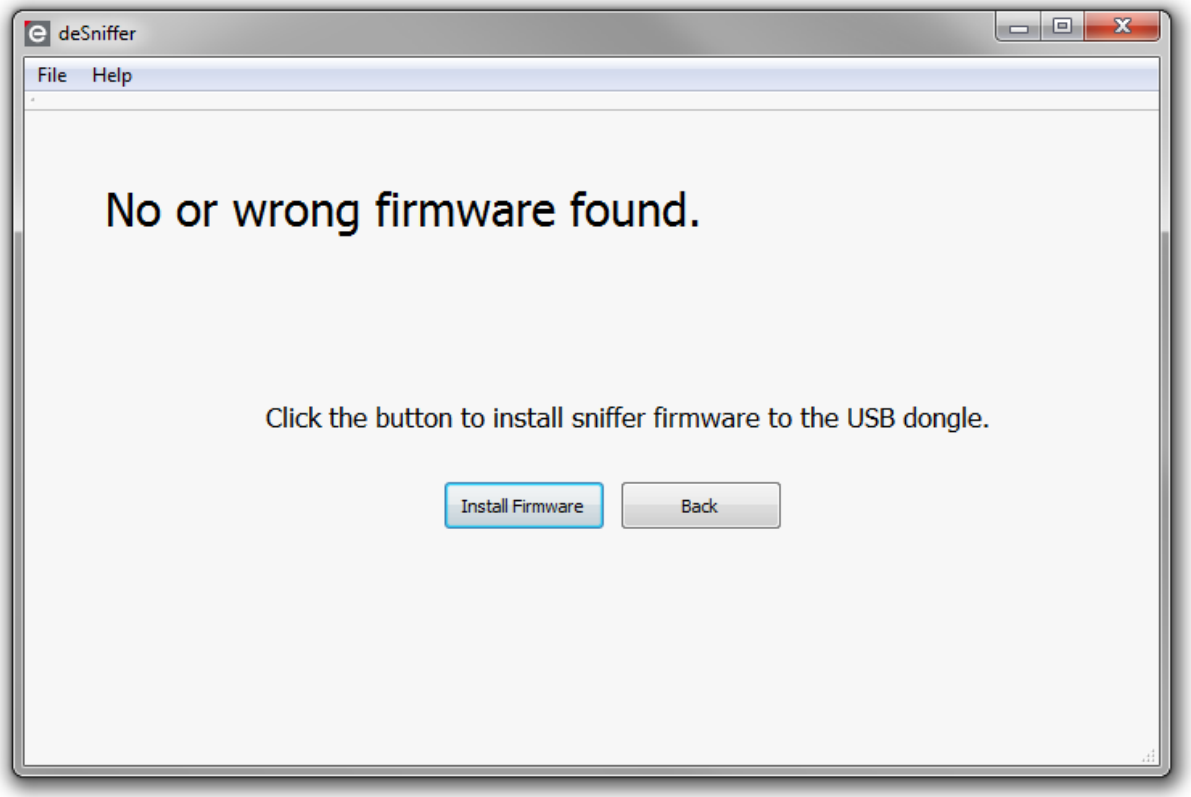


Figure 3: update firmware view

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

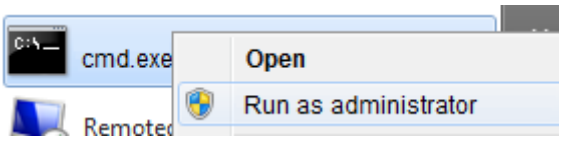
3.3 Configure Wireshark

Windows:

By default ZSHARK sends ZigBee packets to the loopback address of your machine. On Windows you can't capture on the local loopback address 127.0.0.1 with a Windows packet capture driver like WinPcap which is used by Wireshark. In this section two methods are introduced to configure Wireshark so it can work together with the ZSHARK application. You can find more information about this issue in the Wireshark wiki at https://wiki.wireshark.org/CaptureSetup/Loopback.

Variant a) Using Wireshark without the Npcap library (recommended)

To receive traffic in Wireshark from your local machine without a loopback adapter you have to add a route from your machine to your default gateway. To do so open a terminal in windows with administrator rights (press the windows key and type cmd then right click)



and enter the following:

```
route add <your_ip> mask 255.255.255.255 <default_gateway_ip>
```

you can find out your IP and the IP of the default gateway by typing: `ipconfig /all`

(The route will only exist up to the next reboot of your machine). Open Wireshark and double click at your LAN adapter to start sniffing. Because of the added route Wireshark will receive duplicated packets. To filter ZigBee traffic and remove duplicate packets apply the display filter (1) (the !icmp entry is optional but suitable for most networks).

```
udp.port==17754 && ip.ttl==128 && !icmp
```

In the ZSHARK application enable Remote Capture and enter the IP of your PC (see 3.5).

Variant b) Using the Npcap library with loopback adapter

You can download the Npcap library from https://nmap.org/npcap/
During installation of Npcap make sure to select to install the loopback adapter. Open the Wireshark application and double click the Npcap Loopback Adapter (2) to start sniffing. To show only ZigBee traffic apply the display filter: **`udp.port==17754 && !icmp`** (1)
Press the arrow button right of the input field or press enter to apply the filter. You can also apply the filter while the sniffer is running.
Notice: Npcap was tested with the versions 0.84 to 0.97. The versions 0.99r1 and above seem not to work.

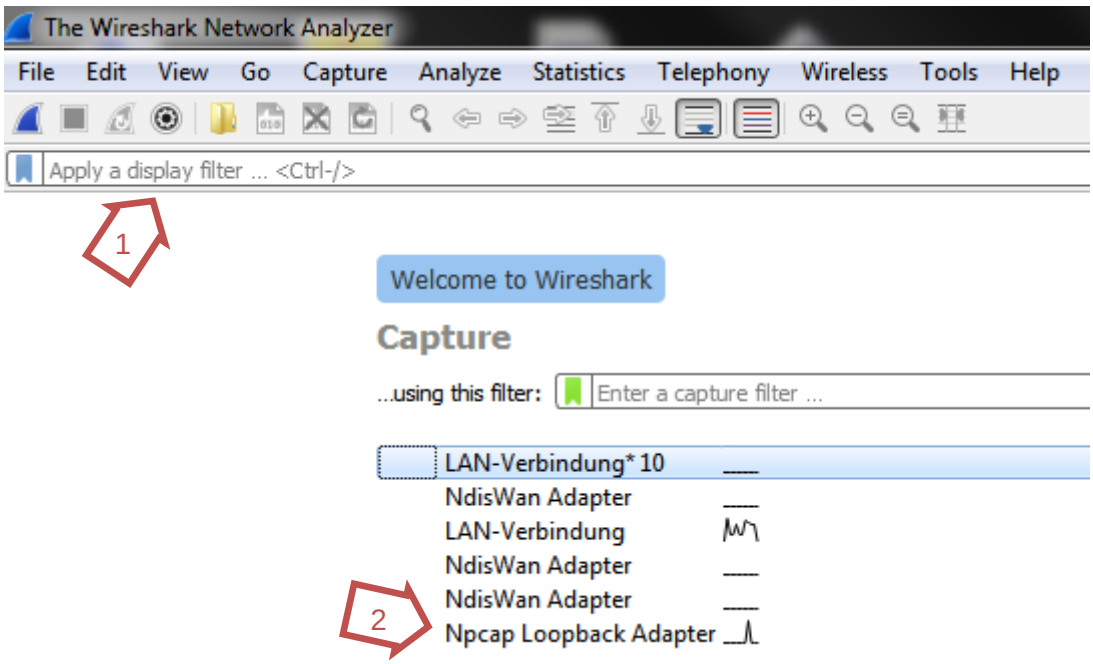


Figure 4: Wireshark start screen (v2.6.1)

Linux:

Open the Wireshark application and choose the Loopback Adapter (lo). Apply the display filter (1)

```
udp.port==17754 && !icmp
```

3.3.1 Add ZigBee Keys to Wireshark:

To add ZigBee Keys for decryption of ZigBee packets go to: *Edit/Preferencs/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. 5). The COM port identifier (1) indicates a successful connection to the USB dongle. You can choose a ZigBee channel from the drop down list (2). A click at Start (3) starts sniffing at the chosen channel. In Wireshark you will see a list of received packets that will fill over time (fig. 6). For more information how to use and configure Wireshark please consult the official Wireshark homepage *www.wireshark.org*.

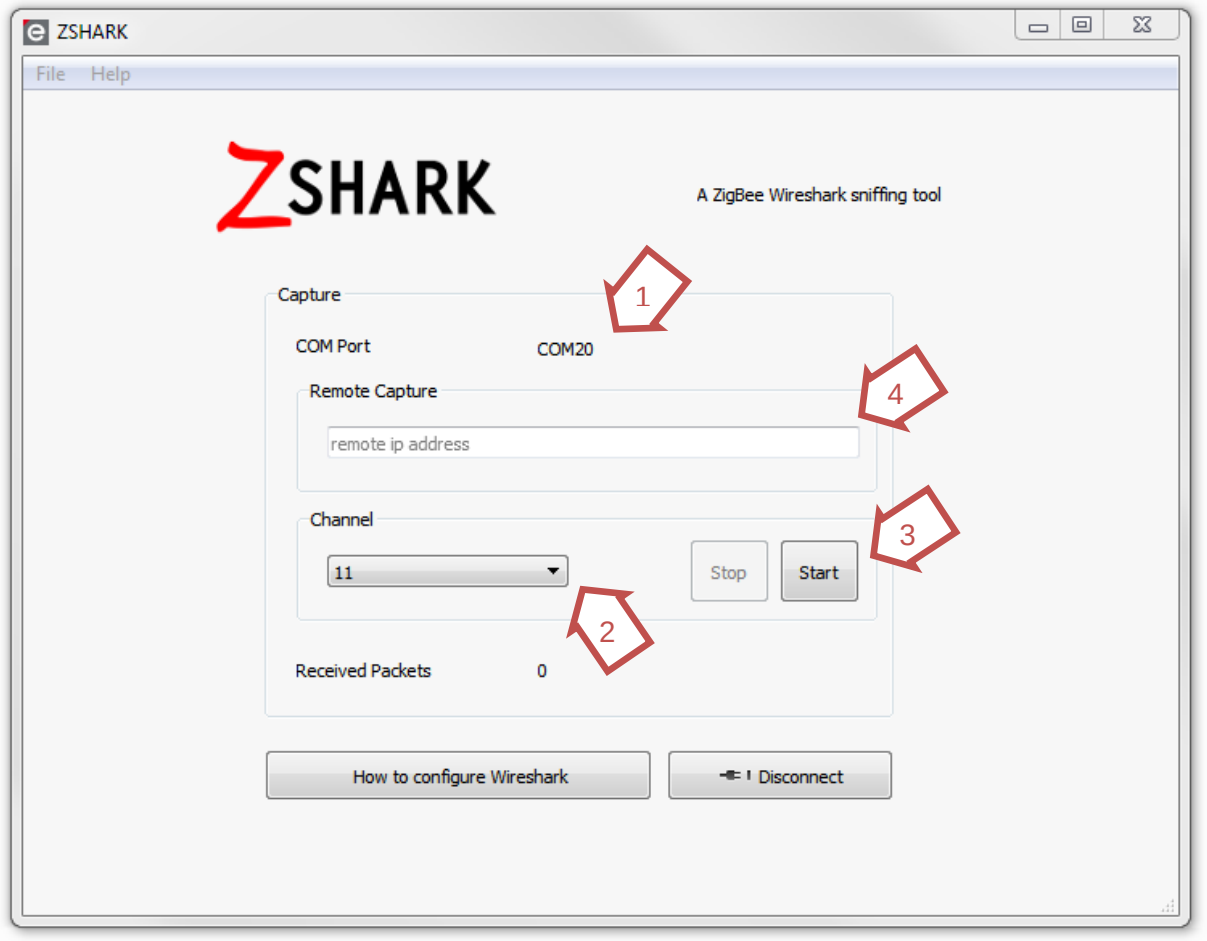


Figure 5: main control view

Figure 6: Wireshark view of received packets

3.5 Remote Capture

You can run ZSHARK 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, just enter the IP address of the receiving machine on which Wireshark runs in the remote capture input field (4). On the other system configure Wireshark as follows:
Connect to the LAN adapter. Use the display filter **`udp.port==17754 && !icmp`**. In the Ethernet settings (Edit/Settings/Protocols/Ethernet) disable both: **Assume packets have FCS** and **Validate the Ethernet checksum if possible**.

3.6 Command line arguments

Following command line arguments are supported. The format is <argument>=<value>.
Multiple arguments are separated by spaces.

argument	value	Description
`--auto-connect`	`0 | 1`	Auto connect to the connected hardware
`--com-port`	`COM[0..n]`	Use COM port for auto-connect e.g. COM8
`--auto-start`	`[11, 12, .., 26]`	Automatic start sniffing on the specified channel
`--remote-ip`	`Ip address`	Specifies the ip address of the machine where tha data will be sent (where Wireshark is running)

Example:

```
zshark --auto-connect=1 --auto-start=15 --remote-ip=192.168.192.20
```

4. Firmware update

To start a firmware update manually you can use the command line tool GCFFlasher which is shipped with the ZSHARK installer. Open a terminal (cmd) in the GCFFlasher directory and enter “GCFFlasher” followed by these arguments: “-d <device to use> -f <file to use>”.
-l will list all devices and -h will print a list of all functions.

A detailed description of the GCFFlasher tool can be found in the ConBee user manual[4] in section 5.

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

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.

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

Disclaimer

any errors or incidental or consequential damage in connection with the furnishing, performance or use of this guide.