

Open Sniffer 3rd generation

Internet of things packet analyser

tool for 802.15.4 / Zigbee / 6LoWPAN networks

- Multiband 780/868/915/2400 MHz
- Web configuration
- Ethernet remote control and firmware upgrade
- Wireshark based
- HW/SW sources available

Available modes

- Sniffing mode
- Energy Detection scanner
- Injection mode
- Continuous wave & packet generator
- Network scan mode

Sniffing Mode

This is default mode of operation for the Open Sniffer device. Channel, band and modulation need to be selected. All captured frames are feed to Wireshark. Wireshark is the open source cross platform industry-standard software for analyzing wired and wireless networks.

Energy Detection Scanner

In this mode Open Sniffer scan within two seconds all available channels among all supported bands (780/868/915/2400 MHz) and display results to the end user.

Continuous Transmission Mode

This mode is aimed to testing purposes. Sniffer continuously emits packets to selected channel, transmission type, modulation and TX power.

Injection Mode

User defined frames are sent within this mode.

Network Scan

Scan over defined channels is done in order to find networks. Then PANID list is displayed.



1	Getting Started.....	3
1.1	Open Sniffer Settings.....	3
1.2	Setting TCP/IP at the host side.....	3
1.3	Connect to the Open Sniffer probe homepage	4
1.4	Wireshark.....	4
2	Adjusting Wireshark.....	6
2.1	Wireshark columns	6
2.2	Install ZEPv3 plugin	7
2.3	Adjusting Wireshark columns to 802.15.4 frame	7
3	Sniffer configuration.....	10
3.1	Home page	10
3.2	Settings page.....	11
4	ED Scanner page	13
5	Continuous transmission (CT) page	15
6	Injection mode page	17
7	Network scan page	18
8	Further Reading.....	18

1 Getting Started

1.1 Open Sniffer Settings

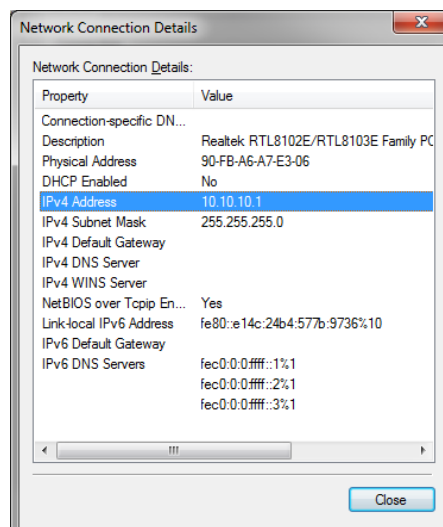
Connect antennas (longer antenna to sub-GHz connector), ethernet cable and finally power cable to Open Sniffer. Plug in other side of ethernet cable and power cable to your host PC.



1.2 Setting TCP/IP at the host side

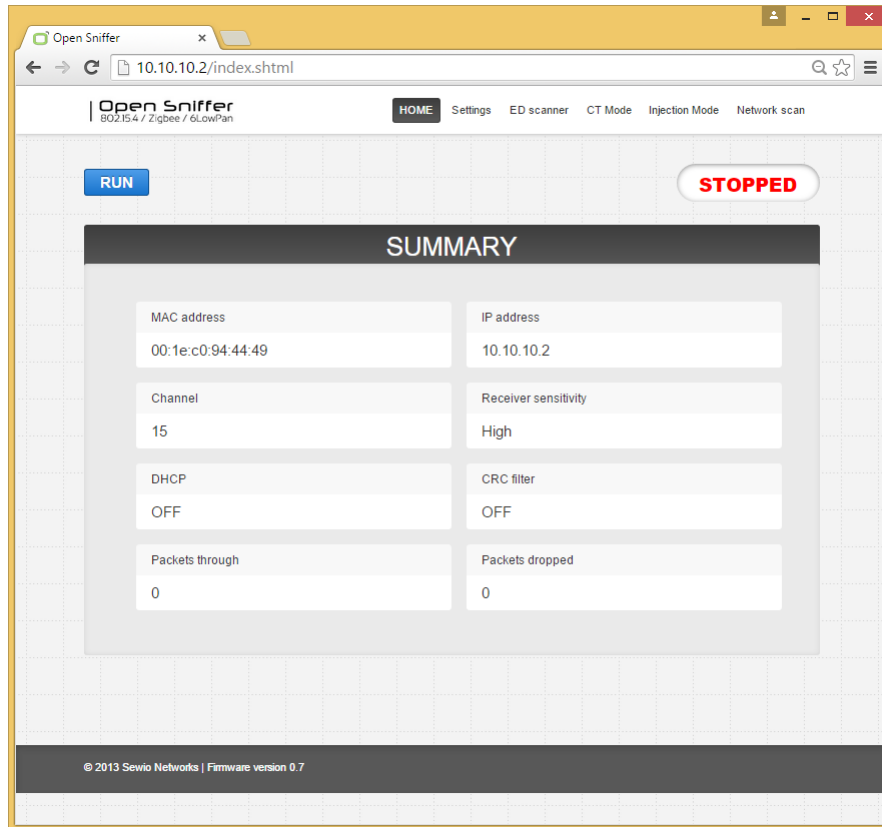
Implicitly Open Sniffer is set to static addressing to **IP address 10.10.10.2** and **mask 255.255.255.0**. Host's IP address must be within the same network scope as the Open Sniffer probe.

Set **host IP to 10.10.10.1** and **network mask to 255.255.255.0**. In Windows this can be done via "Network and Sharing Center". Press CTRL+R and type "ncpa.cpl" Enter. Then you need to select network interface, where you have attached the sniffer and set IP and network address



1.3 Connect to the Open Sniffer probe homepage

Please open an internet browser and point it to probe address <http://10.10.10.2>. Homepage should appear.



1.4 Wireshark

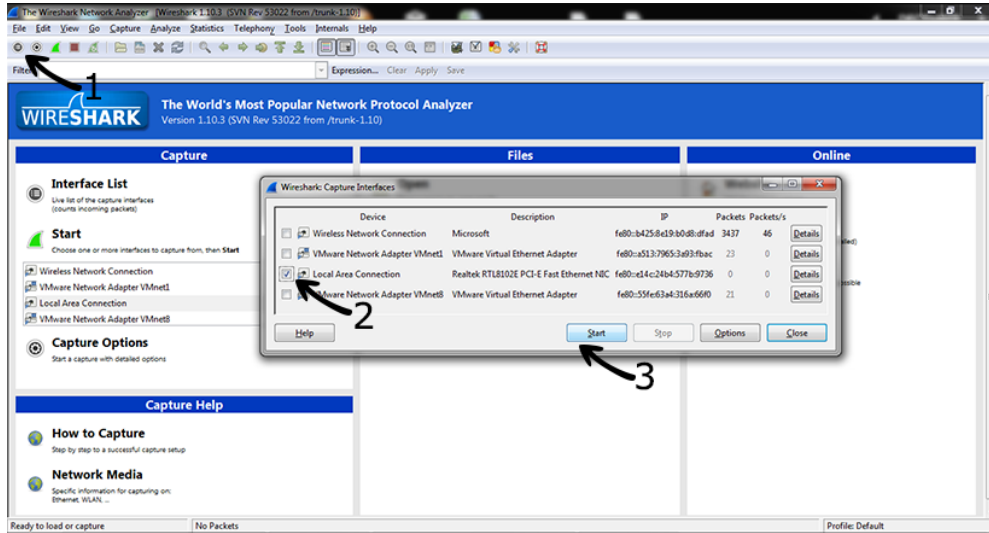
Open Sniffer acts as a probe which capturing 802.15.4 frames and send them to remote host computer. The frames are displayed, filtered and analyzed in Wireshark software.

a) Wireshark installation

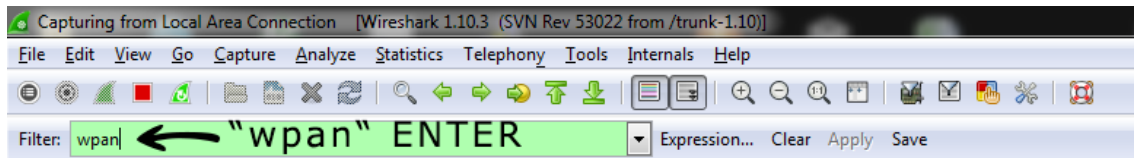
Download, install and run Wireshark, **branch 1.12.x is strongly recommended**. Please select appropriate version for your operating system and architecture.

b) Start Wireshark capture

Select the Ethernet interface (linked to Open Sniffer) from the available network interfaces and start capturing frames.

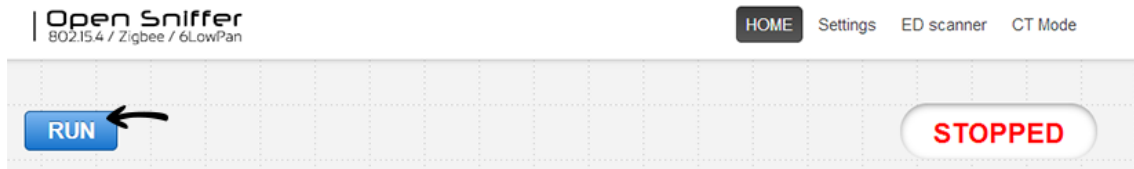


Wireshark implicitly shows all frames from wired and wireless networks delivered to the selected interface. Therefore, it is useful to apply 802.15.4 filter which is referred as "wpan".



c) Start Open Sniffer

Now the host side is prepared and you need to start the Open Sniffer probe via web interface. Point browser to sniffer's IP address (10.10.10.2) and press RUN.



d) Let's sniff some communication

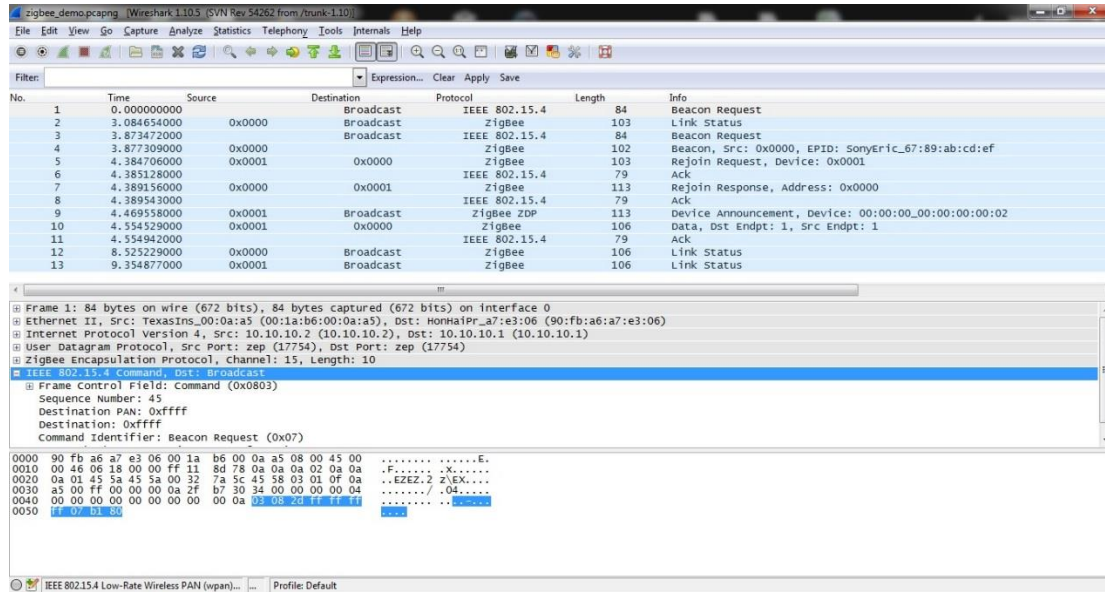
In following example two Zigbee nodes are used to generate some traffic. The Zigbee coordinator with NWK address 0x0000 and Zigbee router with NWK address 0x0001. You may generate your own traffic or [download](#) our captured data zigbee_demo (pcapng).



2 Adjusting Wireshark

2.1 Wireshark columns

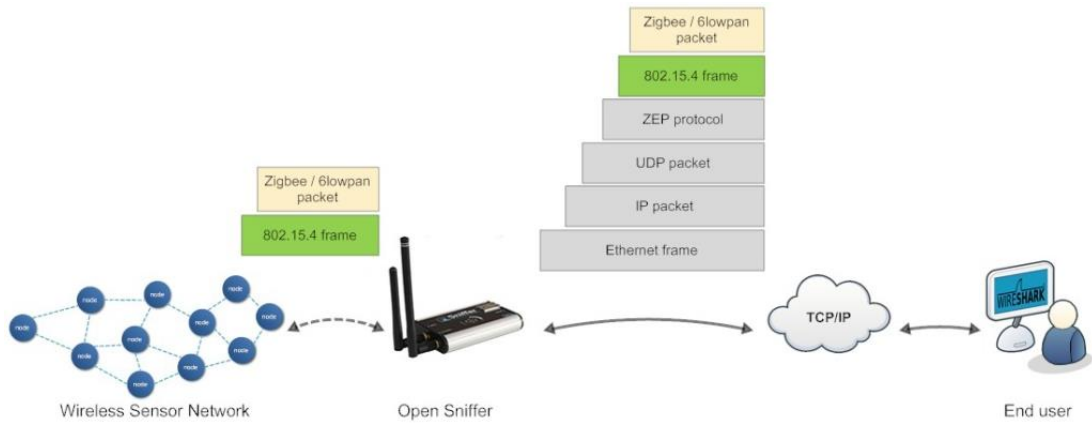
Wireshark has default columns settings for wired Ethernet network, see picture below.



Columns are defined for the default Wireshark profile as follows:

Column name	Description
No.	Frame number counted from the start of capture in Wireshark. This is NOT number of packet received from Open Sniffer probe. It includes all packets delivered to the host's Ethernet interface
Time	Ethernet timestamp of the frame assigned by the operating system. This is NOT precise timestamp from Open Sniffer probe.
Source	Source Address
Destination	Destination Address
Protocol	Protocol
Length	Length of entire Ethernet frame including transportation overhead. This is NOT length of 802.15.4 frame
Info	Protocol details

From the table above it is obvious the default column settings are not associated with 802.15.4. Therefore, you can adjust columns to the 802.15.4 frame info. Let's refresh the encapsulation scheme for each 802.15.4 frame delivered to the host (see picture below). While the grey colored protocols are used only to transport the 802.15.4 frame through a network infrastructure, the ZEP – Zigbee Encapsulated Protocol carries all the important information such as sequence number, timestamp or channel number related to every 802.15.4 captured by the Open Sniffer probe.



2.2 Install ZEPv3 plugin

Although, Wireshark natively contains ZEP protocol v2, we provide ZEPv3 which is backwards compatible and brings additional information related to 802.15.4 band, channel page and precise timestamp information.

- a) Download ZEPv3 plugin from [download page](#).
- b) Extract and copy plugin to the Wireshark plugin folder.
- c) Windows c:\Program Files\Wireshark\plugins\1.x.x\,
- d) Linux /usr/local/lib/wireshark/plugins/1.x.x/.
- e) Start Wireshark. menu Analyze -> Enabled Protocols (CTRL+SHIFT+E)
- f) Uncheck ZEP, check ZEPv3
- g) Apply, OK.
- h) If the new dissector is not applied go to menu Analyze -> Decode as -> ZEPv3 -> Apply, OK.

ZEPv3 contains fields illustrated in picture below:

```

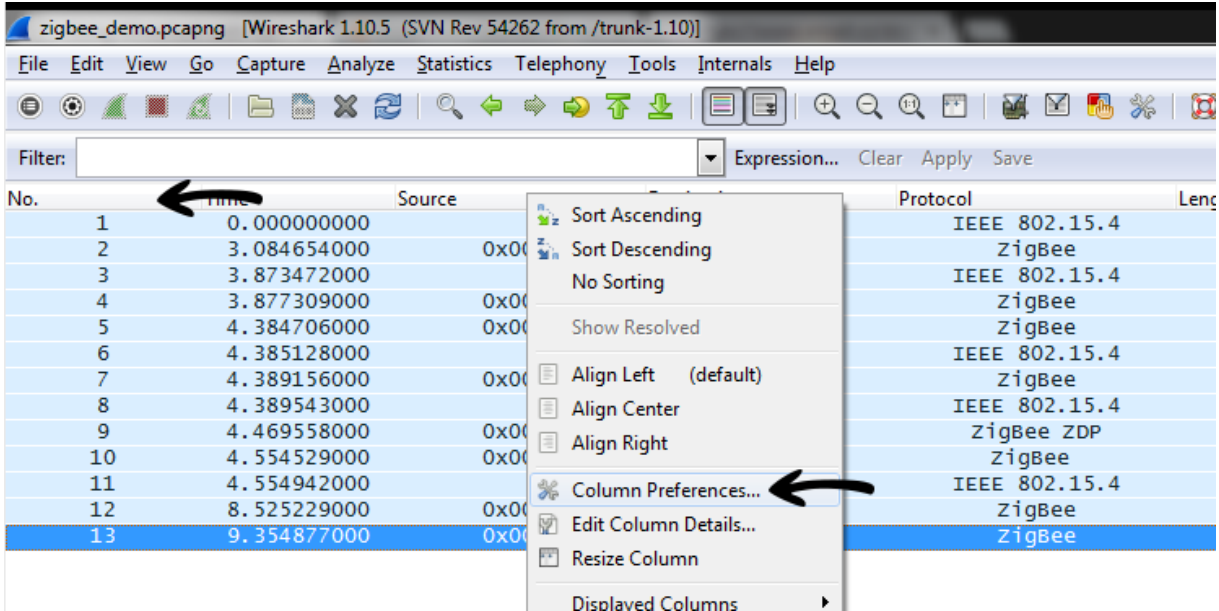
ZigBee Encapsulation Protocol, Channel: 15, Length: 10
Protocol ID String: EX
Protocol Version: 3
Type: 1 (Data)
Channel ID: 15
Device ID: 2725
LQI/CRC Mode: LQI
Link Quality Indication: 255
Sniffer Timestamp: 10.800535000 seconds
Relative Timestamp: 0.000000000 seconds
Absolute Timestamp: Dec 21, 2013 18:46:52.006090000 Central Europe Standard Time
Differential Timestamp: 0.000000000 seconds (This is first packet)
Sequence Number: 0
Frequency band: 2400 MHZ (4)
Channel page: 0
Length: 10 Bytes
    
```

2.3 Adjusting Wireshark columns to 802.15.4 frame

Note: The procedure below describes procedure to adapt Wireshark columns to 802.15.4 frames. You may skip it if you use our Wireshark 802.15.4 [profile](#). Just download the profile, unpack and copy it to the \wireshark\profiles. Finally you need to activate this profile by click on the bottom Wireshark bar "Profile" -> "802.15.4"

Adjusting columns procedure:

- a) Right click on the columns header
- b) Select Column Preferences
- c) Adjust columns to 802.15.4



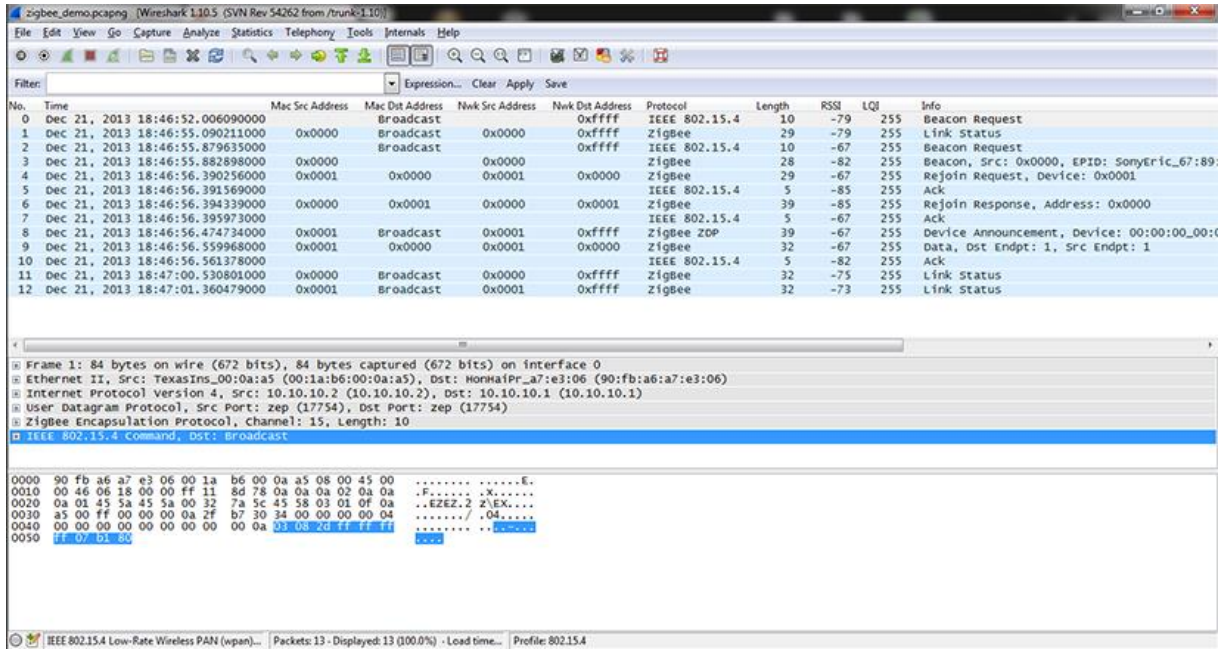
Implicit Wireshark column settings

Displayed Title	Field type
<input checked="" type="checkbox"/> No.	Number
<input checked="" type="checkbox"/> Time	Time (format as specified)
<input checked="" type="checkbox"/> Source	Source address
<input checked="" type="checkbox"/> Destination	Destination address
<input checked="" type="checkbox"/> Protocol	Protocol
<input checked="" type="checkbox"/> Length	Packet length (bytes)
<input checked="" type="checkbox"/> Info	Information

Adjusted columns for 802.15.4

Displayed Title	Field type
<input checked="" type="checkbox"/> No.	Custom (zepv3.seqno)
<input checked="" type="checkbox"/> Time	Custom (zepv3.time)
<input checked="" type="checkbox"/> Mac Src Address	Source address
<input checked="" type="checkbox"/> Mac Dst Address	Destination address
<input checked="" type="checkbox"/> Nwk Src Address	Custom (wpan.src16)
<input checked="" type="checkbox"/> Nwk Dst Address	Custom (wpan.dst16)
<input checked="" type="checkbox"/> Protocol	Protocol
<input checked="" type="checkbox"/> Length	Custom (zepv3.length)
<input checked="" type="checkbox"/> RSSI	Custom (wpan.rssi)
<input checked="" type="checkbox"/> LQI	Custom (zepv3.lqi)
<input checked="" type="checkbox"/> Info	Information

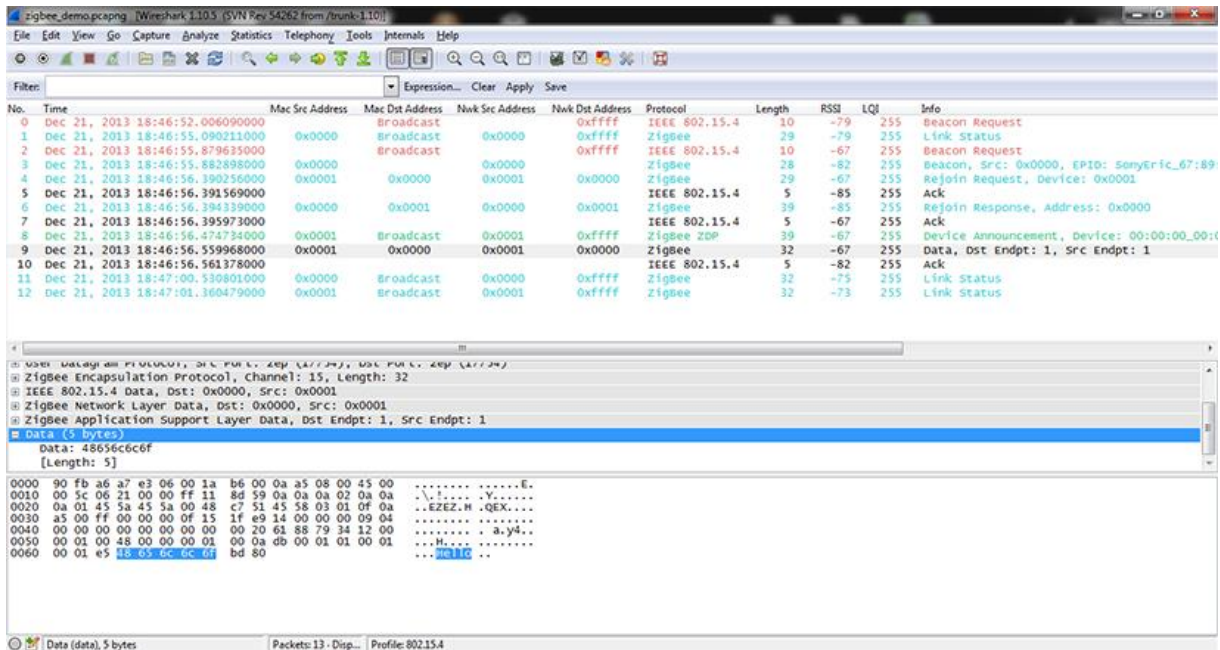
Adjusted Wireshark columns should seem like this:



The screenshot shows a Wireshark capture of Zigbee traffic. The packet list pane displays the following columns: No., Time, Mac Src Address, Mac Dst Address, Nwk Src Address, Nwk Dst Address, Protocol, Length, RSSI, LQI, and Info. The packets are filtered for IEEE 802.15.4. The packet details pane shows the structure of a Zigbee Encapsulation Protocol frame, including the User Datagram Protocol (UDP) and Zigbee Encapsulation Protocol (ZEP) fields.

No.	Time	Mac Src Address	Mac Dst Address	Nwk Src Address	Nwk Dst Address	Protocol	Length	RSSI	LQI	Info
0	Dec 21, 2013 18:46:52.006090000	0x0000	Broadcast	0x0000	0xffff	IEEE 802.15.4	10	-79	255	Beacon Request
1	Dec 21, 2013 18:46:55.090211000	0x0000	Broadcast	0x0000	0xffff	ZigBee	29	-79	255	Link Status
2	Dec 21, 2013 18:46:55.879635000	0x0000	Broadcast	0x0000	0xffff	IEEE 802.15.4	10	-67	255	Beacon Request
3	Dec 21, 2013 18:46:55.882898000	0x0000	0x0000	0x0000	0x0000	ZigBee	28	-82	255	Beacon, Src: 0x0000, EPID: SonyEric_67:89
4	Dec 21, 2013 18:46:56.390256000	0x0001	0x0000	0x0001	0x0000	ZigBee	29	-67	255	Rejoin Request, Device: 0x0001
5	Dec 21, 2013 18:46:56.391569000	0x0000	0x0001	0x0000	0x0001	IEEE 802.15.4	5	-85	255	Ack
6	Dec 21, 2013 18:46:56.394339000	0x0000	0x0001	0x0000	0x0001	ZigBee	39	-85	255	Rejoin Response, Address: 0x0000
7	Dec 21, 2013 18:46:56.395973000	0x0001	Broadcast	0x0001	0xffff	IEEE 802.15.4	5	-67	255	Ack
8	Dec 21, 2013 18:46:56.474734000	0x0001	0x0000	0x0001	0x0000	ZigBee ZDP	39	-67	255	Device Announcement, Device: 00:00:00_00:00:00
9	Dec 21, 2013 18:46:56.559968000	0x0001	0x0000	0x0001	0x0000	ZigBee	32	-67	255	Data, Dst Endpt: 1, Src Endpt: 1
10	Dec 21, 2013 18:46:56.561378000	0x0000	Broadcast	0x0000	0xffff	IEEE 802.15.4	5	-82	255	Ack
11	Dec 21, 2013 18:47:00.530801000	0x0000	Broadcast	0x0000	0xffff	ZigBee	32	-75	255	Link Status
12	Dec 21, 2013 18:47:01.360479000	0x0001	Broadcast	0x0001	0xffff	ZigBee	32	-73	255	Link Status

Applying our 802.15.4 profile with predefined color rules:



The screenshot shows the same Wireshark capture as above, but with color rules applied. The packet list pane shows the IEEE 802.15.4 protocol column highlighted in blue for packets 0, 2, 4, 6, 8, 10, and 12. The packet details pane shows the structure of a Zigbee Encapsulation Protocol frame, including the User Datagram Protocol (UDP) and Zigbee Encapsulation Protocol (ZEP) fields. The packet bytes pane shows the raw data of the frame.

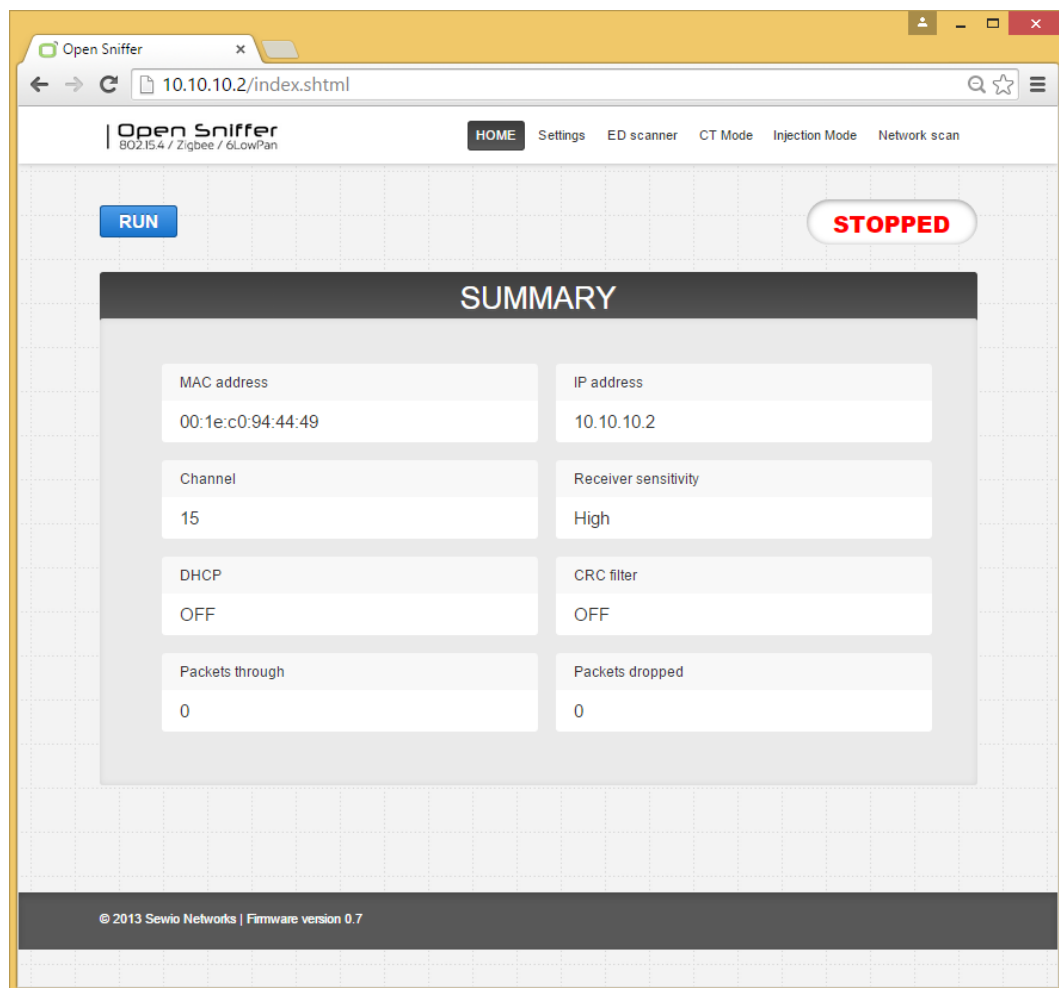
No.	Time	Mac Src Address	Mac Dst Address	Nwk Src Address	Nwk Dst Address	Protocol	Length	RSSI	LQI	Info
0	Dec 21, 2013 18:46:52.006090000	0x0000	Broadcast	0x0000	0xffff	IEEE 802.15.4	10	-79	255	Beacon Request
1	Dec 21, 2013 18:46:55.090211000	0x0000	Broadcast	0x0000	0xffff	ZigBee	29	-79	255	Link Status
2	Dec 21, 2013 18:46:55.879635000	0x0000	Broadcast	0x0000	0xffff	IEEE 802.15.4	10	-67	255	Beacon Request
3	Dec 21, 2013 18:46:55.882898000	0x0000	0x0000	0x0000	0x0000	ZigBee	28	-82	255	Beacon, Src: 0x0000, EPID: SonyEric_67:89
4	Dec 21, 2013 18:46:56.390256000	0x0001	0x0000	0x0001	0x0000	ZigBee	29	-67	255	Rejoin Request, Device: 0x0001
5	Dec 21, 2013 18:46:56.391569000	0x0000	0x0001	0x0000	0x0001	IEEE 802.15.4	5	-85	255	Ack
6	Dec 21, 2013 18:46:56.394339000	0x0000	0x0001	0x0000	0x0001	ZigBee	39	-85	255	Rejoin Response, Address: 0x0000
7	Dec 21, 2013 18:46:56.395973000	0x0001	Broadcast	0x0001	0xffff	IEEE 802.15.4	5	-67	255	Ack
8	Dec 21, 2013 18:46:56.474734000	0x0001	0x0000	0x0001	0x0000	ZigBee ZDP	39	-67	255	Device Announcement, Device: 00:00:00_00:00:00
9	Dec 21, 2013 18:46:56.559968000	0x0001	0x0000	0x0001	0x0000	ZigBee	32	-67	255	Data, Dst Endpt: 1, Src Endpt: 1
10	Dec 21, 2013 18:46:56.561378000	0x0000	Broadcast	0x0000	0xffff	IEEE 802.15.4	5	-82	255	Ack
11	Dec 21, 2013 18:47:00.530801000	0x0000	Broadcast	0x0000	0xffff	ZigBee	32	-75	255	Link Status
12	Dec 21, 2013 18:47:01.360479000	0x0001	Broadcast	0x0001	0xffff	ZigBee	32	-73	255	Link Status

3 Sniffer configuration

3.1 Home page

RUN/STOP button and status field are located below the top menu. RUN/STOP button is present on every sub-page and always refers to sniffer mode.

Home page contains following summary information about an analyzer: MAC address, IP address, current channel, sensitivity, DHCP client mode, CRC filter option, number of 802.15.4 packets received and dropped. At the bottom of the home page firmware version is located.



3.2 Settings page

Radio parameters, network configuration and host settings are done via this page.

Radio Settings contains following options

- Available Frequency and modulation

Freq / Channel	Modulation
780/0	OQPSK-RC-250
782/1	OQPSK-RC-250
784/2	OQPSK-RC-250
786/3	OQPSK-RC-250
868/0	BPSK-20
906/1	BPSK-40/OQPSK-SIN-250
908/2	BPSK-40/OQPSK-SIN-250
910/3	BPSK-40/OQPSK-SIN-250
912/4	BPSK-40/OQPSK-SIN-250
914/5	BPSK-40/OQPSK-SIN-250
916/6	BPSK-40/OQPSK-SIN-250
918/7	BPSK-40/OQPSK-SIN-250
920/8	BPSK-40/OQPSK-SIN-250
922/9	BPSK-40/OQPSK-SIN-250
924/10	BPSK-40/OQPSK-SIN-250
2405/11	OQPSK-250
2410/12	OQPSK-250
2415/13	OQPSK-250
2420/14	OQPSK-250
2425/15	OQPSK-250
2430/16	OQPSK-250
2435/17	OQPSK-250
2440/18	OQPSK-250
2445/19	OQPSK-250
2450/20	OQPSK-250
2455/21	OQPSK-250
2460/22	OQPSK-250
2465/23	OQPSK-250
2470/24	OQPSK-250
2475/25	OQPSK-250
2480/26	OQPSK-250

- Receiver Sensitivity:
 - High - lower than -101 dBm
 - Medium - lower than -79 dBm
 - Low - lower than -64dBm
 - Lowest - lower than -48 dBm

- CRC filter On/Off:
 - IEEE 802.15.4 frames with wrong CRC are discarded

IPv4 settings related to Open Sniffer device contains:

- IP mode – DHCP client / Static IP address
- IP address
- Netmask
- Gateway

Host settings block contains:

- Host IP address – IP address of the host computer where Wireshark is running
- Host UDP port – should be set 17754, this identifies 802.15.4 data flow in Wireshark

Open Sniffer
802.15.4 / Zigbee / 6LoWPan
HOME **Settings** ED scanner CT Mode Injection Mode Network scan

RUN
STOPPED

RADIO SETTINGS

Frequency / Channel
2425/15 MHz/-

Receiver sensitivity
High (< -91dBm)

LQI/CRC mode
 LQI CRC

Modulation
O-QPSK_250 (compliant)

CRC filter

SUBMIT & RUN

IPV4 SETTINGS

IP mode
 DHCP Static

Netmask
255.255.255.0

IP address
10.10.10.2

Gateway
10.10.10.1

SUBMIT

HOST SETTINGS

Host IP address
10.10.10.1

Host UDP port
17754

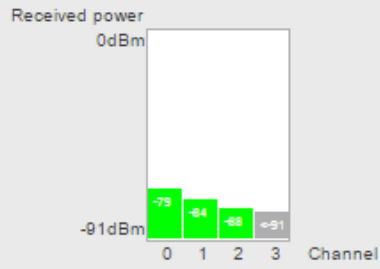
SUBMIT

4 ED Scanner page

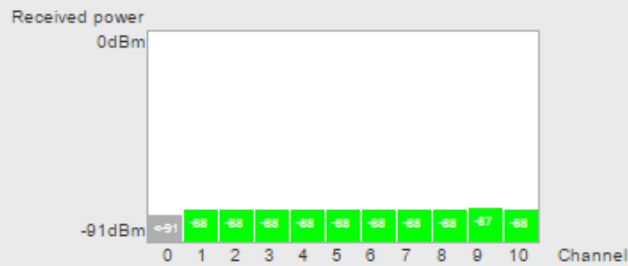
This page provides Energy Detection measurement for the all 31 channels during 2s period. Results are shown in graph separated for each frequency band.

RUN

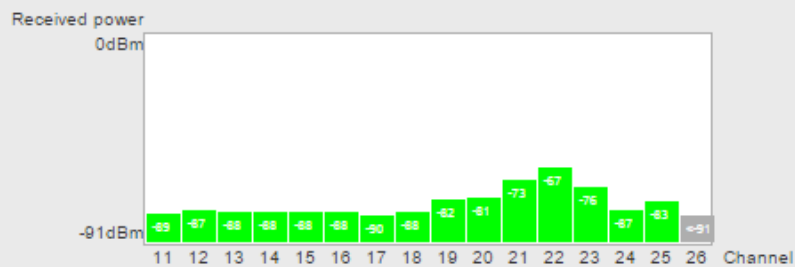
STOPPED

ENERGY SCAN SUCCESSFULLY FINISHED
780MHZ BAND


SCAN AGAIN

868MHZ AND 915MHZ BAND


SCAN AGAIN

2.4GHZ BAND


SCAN AGAIN

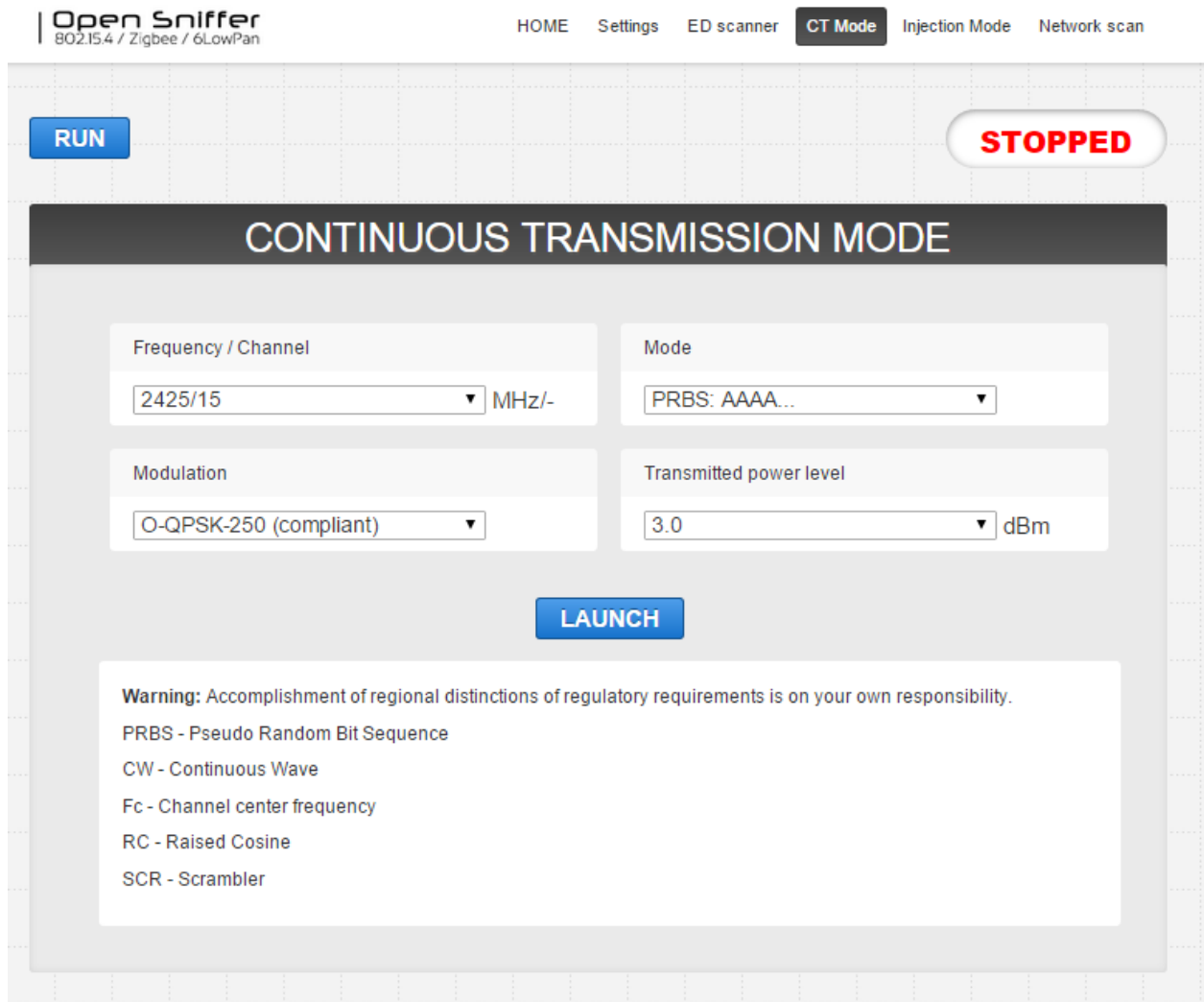
Open Sniffer

Datasheet

5 Continuous transmission (CT) page

This mode allows to transmit single tone signal (CW – Continuous Wave) or random signals (PRBS – Pseudo Random Binary Sequence). It is useful for RF related measurements (TX power, harmonics) and other test purposes such as generating RF noise on the particular channel.

CT mode is started by click on the LAUNCH button.



CW mode has 6 different frequencies:

- $F_c + 0.50$ MHz
- $F_c - 0.50$ MHz
- $F_c + 0.25$ MHz
- $F_c - 0.25$ MHz
- $F_c + 0.10$ MHz
- $F_c - 0.10$ MHz

F_c stands for the channel center frequency.

Note that in CW mode it is not possible to transmit a RF signal directly on the channel center frequency.

PBRS mode transmits payload bytes continuously in the infinite loop.

There are 3 payloads available:

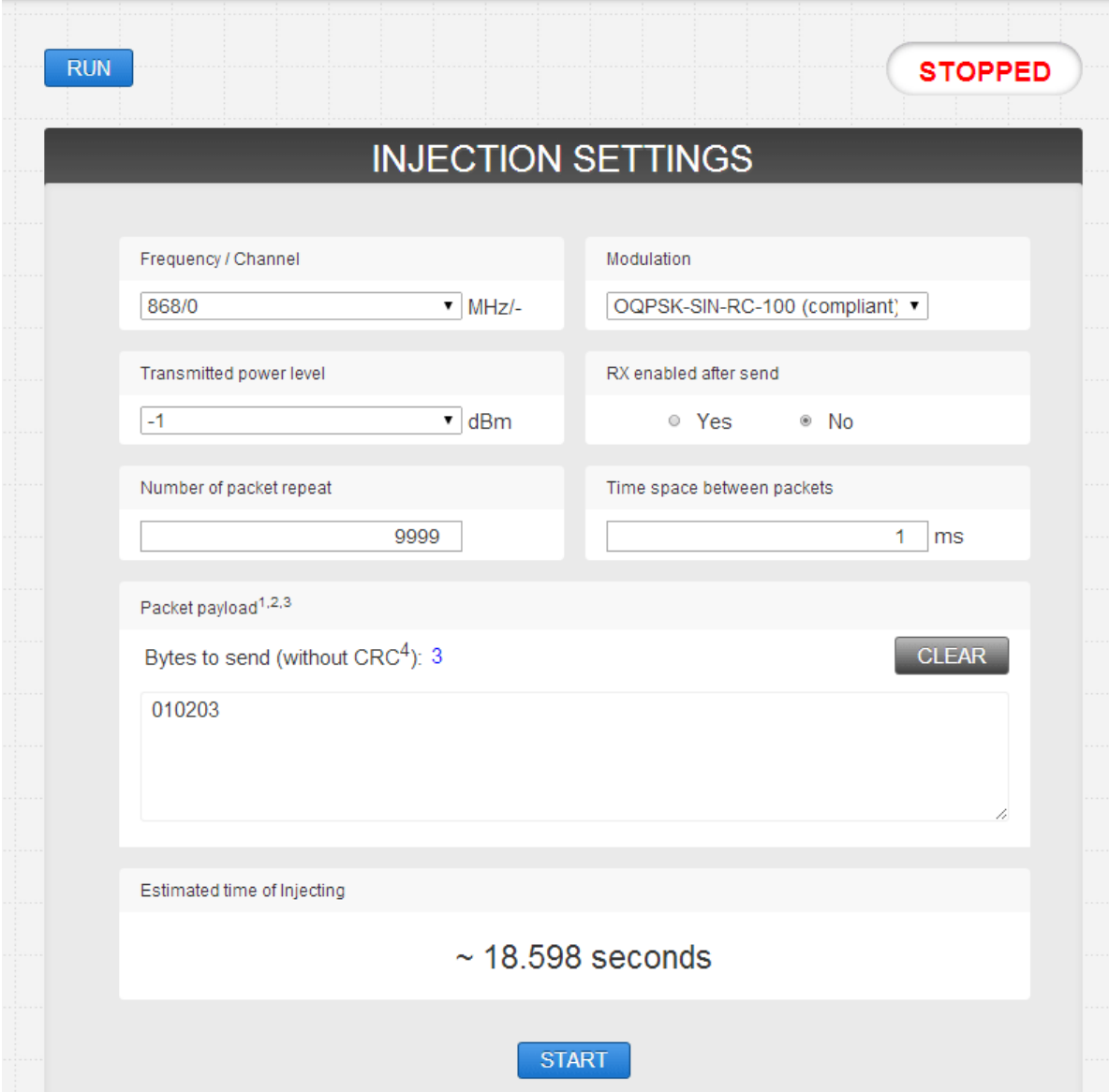
- PRBS: 0xAAAA... – Repeated hexadecimal value A (1010 binary).
- PRBS: 0x0000... – Repeated hexadecimal value 0 (0000 binary).
- PRBS: 0xFFFF... – Repeated hexadecimal value F (1111 binary).

Available modulation for PRBS mode is based on the selected channel:

- Channels 0 – 3 (780 Band): Modulation O-QPSK_250.
- Channel 0 (868 Band): Modulations BPSK_20 and modulation O-QPSK_100.
- Channels 1 – 10 (915 Band): Modulations BPSK_40 and O-QPSK_250.
- Channels 11 – 26 (2400 Band): Modulation O-QPSK_250.

6 Injection mode page

This mode is dedicated for packet transmitting. Several parameters such as payload, number of repetitions or delay among packets might be set.



Open Sniffer
802.15.4 / Zigbee / 6LowPan

HOME Settings ED scanner CT Mode **Injection Mode** Network scan

RUN **STOPPED**

INJECTION SETTINGS

Frequency / Channel 868/0 MHz/-	Modulation OQPSK-SIN-RC-100 (compliant)
Transmitted power level -1 dBm	RX enabled after send <input type="radio"/> Yes <input checked="" type="radio"/> No
Number of packet repeat 9999	Time space between packets 1 ms

Packet payload^{1,2,3}
Bytes to send (without CRC⁴): 3 **CLEAR**

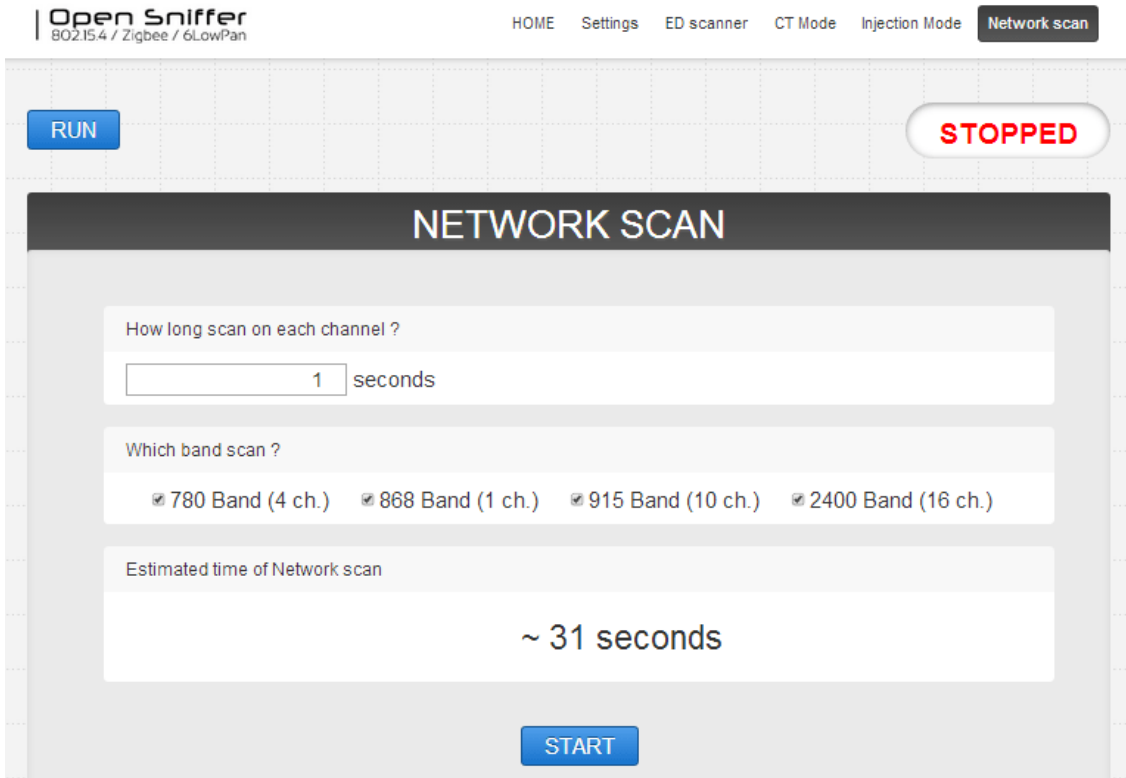
010203

Estimated time of Injecting
~ 18.598 seconds

START

7 Network scan page

Network scan search for frames among specified channels and bands. If 802.15.4 network is found network PANID is displayed otherwise "unknown" network or no frame is shown.



The screenshot shows the 'Open Sniffer' web interface. At the top, there is a navigation menu with 'HOME', 'Settings', 'ED scanner', 'CT Mode', 'Injection Mode', and 'Network scan'. The 'Network scan' tab is active. Below the navigation, there is a 'RUN' button on the left and a 'STOPPED' button on the right. The main content area is titled 'NETWORK SCAN' and contains the following controls:

- A text input field for 'How long scan on each channel?' with the value '1' and the unit 'seconds'.
- A section titled 'Which band scan?' with four radio button options: '780 Band (4 ch.)', '868 Band (1 ch.)', '915 Band (10 ch.)', and '2400 Band (16 ch.)'. All options are currently selected.
- A section titled 'Estimated time of Network scan' displaying '~ 31 seconds'.
- A 'START' button at the bottom.

8 Further Reading

How to control sniffer programmatically via HTTP protocol, Frequently Asked Questions or how to write your own Wireshark protocol dissector can be found at Open Sniffer [product page](#).

EVALUATION BOARD

Sewio provides the enclosed product under the following conditions:

This evaluation board/kit is intended for use for ENGINEERING DEVELOPMENT, DEMONSTRATION, OR EVALUATION PURPOSES ONLY and is not considered by Sewio to be a finished end-product fit for general consumer use. Persons handling the product(s) must have electronics training and observe good engineering practice standards. As such, the goods being provided are not intended to be complete in terms of required design-,marketing-, and/or manufacturing-related protective considerations, including product safety and environmental measures typically found in end products that incorporate such semiconductor components or circuit boards. This evaluation board/kit does not fall within the scope of the European Union directives regarding electromagnetic compatibility, restricted substances (RoHS), recycling (WEEE), FCC, CE or UL, and therefore may not meet the technical requirements of these directives or other related directives.

The user assumes all responsibility and liability for proper and safe handling of the goods. Further, the user indemnifies Sewio from all claims arising from the handling or use of the goods.

EXCEPT TO THE EXTENT OF THE INDEMNITY SET FORTH ABOVE, NEITHER PARTY SHALL BE LIABLE TO THE OTHER FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES.

Sewio assumes no liability for applications assistance, customer product design, software performance, or infringement of patents or services described herein.

No license is granted under any patent right or other intellectual property right of Sewio covering or relating to any machine, process, or combination in which such Sewio products or services might be or are used.

FCC Warning. This evaluation board/kit is intended for use for ENGINEERING DEVELOPMENT, DEMONSTRATION, OR EVALUATION PURPOSES ONLY and is not considered by Sewio to be a finished end-product fit for general consumer use. It generates, uses, and can radiate radio frequency energy and has not been tested for compliance with the limits of computing devices pursuant to part 15 of FCC rules, which are designed to provide reasonable protection against radio frequency interference. Operation of this equipment in other environments may cause interference with radio communications, in which case the user at his own expense will be required to take whatever measures may be required to correct this interference.