

Open Sniffer 3nd generation

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

Available modes

Dpen Sniffer

- 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 industrystandard 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.

Internet of things packet analyser

tool for 802.15.4 / Zigbee / 6LoWPAN networks







1		Getting Started	. 3
	1.1	Open Sniffer Settings	. 3
	1.2	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	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	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

v0.1



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

V	etwork Connection Details	;
	Network Connection <u>D</u> etails:	
	Property	Value
	Connection-specific DN Description Physical Address DHCP Enabled	Realtek RTL8102E/RTL8103E Family PC 90-FB-A6-A7-E3-06 No
	IPv4 Address	10.10.10.1
	IPv4 Subnet Mask IPv4 Default Gateway IPv4 DNS Server IPv4 WINS Server	255.255.255.0
	NetBIOS over Tcpip En	Yes
	Link-local IPv6 Address IPv6 Default Gateway	fe80::e14c:24b4:577b:9736%10
	IPv6 DNS Servers	fec0:0:0.ffff::1%1
		fec0:0:0.ffff::2%1
		fec0:0:0:ffff::3%1
	٠ III	•
		Close

v0.1



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.

)pen Sniffer)2.15.4 / Zigbee / 6LowPan	HOME Settings ED scanner CT Mode Injection Mode Network scan
R	UN	STOPPED
		SUMMARY
	MAC address	IP address
	00:1e:c0:94:44:49	10.10.10.2
	Channel	Receiver sensitivity
	15	High
	DHCP	CRC filter
	OFF	OFF
	Packets through	Packets dropped
	0	0

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.



The Weindark Notagek Analyse Winderke 11203 (2001) Ele Edit View So Capture Analyse Statistics Teles	ar 33022 fean frank-3.10) heary Iooks internak Bildp	
Capture	Files	Online
Level for the capture interfaces town for more particular Start Coses one or more interfaces to capture from, then Start Wireless Network Connection Wireless Network Adapter Vinnett Local Area Connection Whater Network Adapter Vinnett Costance Connection Whater Network Adapter Vinnett Costance Connection Costance Connection Costance Connection Costance Connection Costance Connection Costance Connection	Derice Description III Image: Workess Network Connection Microsoft r60:s425.64 Image: Workess Network Adapter VMnett VMware Vistual Ethernet Adapter r60:s425.64 Image: Worker Network Adapter VMnett VMware Vistual Ethernet Adapter r60:s425.64 Image: Worker Network Adapter VMnett VMware Vistual Ethernet Adapter r60:s55663 Holp Sent Sent Sent	Packets Packets/s S940dstoffed 3437 45 Retails S53.ab3/blox 23 0 Details >4537b5/50736 0 Details sobe >4537b6 0 Details sobe >4335b6600 21 0 Details p Options Close
Capture Help Capture Help Mow to Capture Date by major as a societure (aprice singe Deckt, information for paging on Deckt, informat		

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*".

Capturing from Local Area Conr	nection [Wireshark 1.10.3 (SVN Rev 53022 from /trunk-1.10)]	
<u>File Edit View Go</u> Capture	<u>A</u> nalyze <u>S</u> tatistics Telephony <u>T</u> ools <u>I</u> nternals <u>H</u> elp	
🖲 🛞 煮 🔳 🙋 🗎	🕯 🗶 🌮 Q, 🗢 🌳 🗛 🛧 🖢 🗐 🗐 O, Q, Q, 🖻 🖉 🕺 🧩 🎉 -	
Filter: wpan 🔶 "W	pan" ENTER Expression Clear Apply Save	

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.

Op 802.15	en 5.4 / Zig	مد bee / 6	iffer 6LowPar	'n					HOME	Settings	ED scanner	CT Mode	
RUN											STOP	PED)

d) Let's sniff some communication

In following example two Zigbee nodes are used to generate some traffic. The Zigbee coordinator with NWK address 0×0000 and Zigbee router with NWK address 0×0001. You may generate your own traffic or <u>download</u> 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.

ter:			 Expression 	Clear Apply Save			
	Time Sour	ce	Destination	Protocol	Length	Info	
1	0.00000000		Broadcast	IEEE 802.15.4	84	Beacon Request	
2	3.084654000	0x0000	Broadcast	ZigBee	103	Link Status	
3	3.873472000		Broadcast	IEEE 802.15.4	84	Beacon Request	
4	3.877309000	0x0000		ZigBee	102	Beacon, Src: 0x0000, EPID: SonyEric_67:89:ab:cd:ef	
5	4.384706000	0x0001	0x0000	ZigBee	103	Rejoin Request, Device: 0x0001	
6	4.385128000			IEEE 802.15.4	79	Ack	
7	4.389156000	0x0000	0x0001	ZigBee	113	Rejoin Response, Address: 0x0000	
8	4.389543000			IEEE 802.15.4	79	Ack	
9	4.469558000	0x0001	Broadcast	ZigBee ZDP	113	Device Announcement, Device: 00:00:00_00:00:00:00:02	
10	4.554529000	0x0001	0x0000	ZigBee	106	Data, Dst Endpt: 1, Src Endpt: 1	
11	4 554942000			IEEE 802.15.4	79	Ack	
	11 33 13 12000					0.LV	
12	8.525229000	0x0000	Broadcast	ZiaBee	106	Link Status	
12 13 rame 1: thernet nternet ser Data	8.525229000 9.354877000 84 bytes on wire (6 II, Src: TexasIns_0 Protocol version 4, gram Protocol, Src	0x0000 0x0001 72 bits), 84 b 0:0a:a5 (00:1a Src: 10.10.10 Port: zep (177	Broadcast Broadcast bytes captured (672 k s:b6:00:0a:a5), bst: 0.2 (10.10.2), bst 54), bst Port: zep (ZigBee ZigBee " bits) on interface 0 HonHaiPr_a7:e3:06 (90: :: 10.10.10.1 (10.10.10 (17754)	106 106 fb:a6:a7:e3: .1)	Link Status Link Status	
12 13 rame 1: thernet internet igBee En ter 802. Frame C Sequenc	8.525229000 9.354877000 84 bytes on wire (6 II, Src: TexasIns.0 Protocol Version 4, ugram Protocol, Src icapsulation Protoco 15.4 Command, Dst; iontrol Field: Comma e Number: 45	0x0000 0x0001 72 bits), 84 b 0:0a:a5 (00:1a Src: 10.10.10 Port: zep (177 1, channel: 15 Broadcast nd (0x0803)	Broadcast Broadcast hytes captured (672 b 1:b6:00:0a:a5), DSt:), 2 (10.10.10.2), DSt 54), DSt Port: zep (, Length: 10	ZigBee ZigBee m bits) on interface 0 HonHalfPr_J2:83:06 (90: :: 10.10.10.1 (10.10.10 (17754)	106 106 fb:a6:a7:e3: .1)	Link Status Link Status	
12 13 Frame 1: Ethernet Internet User Data ZigBee En IEEE 802. E Frame C Sequenc Destina Destina Command	8:525229000 9:354877000 84 bytes on wire (6 II, Src: TexasIns_0 Protocol version 4, gram Protocol, Src Lagualation Protocol 15:4 CommanG, Dott 15:4 CommanG, Dott 15:	0x0000 0x0001 72 bits), 84 b 0:0a:a5 (00:1a Src: 10.10.10 Port: zep (177 1, channel: 17 1, channel: 17 BF00dCast nd (0x0803)	Broadcast Broadcast hytes captured (672 b h:b6:00:0a:a5), Db5 (2 (10.10.10.2), Db5 (34), Db5 Port: zep (, Length: 10	ZigBee ZigBee m bits) on interface 0 HonHalfP_J7:e3:06 (90: : 10.10.10.1 (10.10.10 (17754)	106 106 fb:a6:a7:e3: .1)	Link Status Link Status	

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 <u>profile</u>. 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"

Dpen Sniffer



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
V	No.	Number
V	Time	Time (format as specified)
V	Source	Source address
V	Destination	Destination address
v	Protocol	Protocol
v	Length	Packet length (bytes)
V	Info	Information

Adjusted columns for 802.15.4

Displayed	Title	Field type
V	No.	Custom (zepv3.seqno)
v	Time	Custom (zepv3.time)
v	Mac Src Address	Source address
1	Mac Dst Address	Destination address
v	Nwk Src Address	Custom (wpan.src16)
V	Nwk Dst Address	Custom (wpan.dst16)
1	Protocol	Protocol
1	Length	Custom (zepv3.length)
1	RSSI	Custom (wpan.rssi)
1	LQI	Custom (zepv3.lqi)
V	Info	Information



Adjusted Wireshark columns should seem like this:

		10	6.	Curto			Carteral		Lucini,		CALLON I		Liste.				_	_		
ine .	Cost	Xiew	20	7-abrun	e Ana	iyze	Seacesco	s ie	sepnon	Y 1	oois p	nternais	Teib	200200110						
			A		2 20	8	19	\$4 H		Ŧ	2		Q	Q Q 2	📓 🖾 😼 %					
iter	-										1	Express	ion	Clear Apply	Save					
a,	Time							Mac 3	Sec Add	śress	Mac	Dist Addres	s Nv	k Src Address	Nwk Dst Address	Protocol	Length	RSSI	LQI	Info
0	Dec	21.	2013	18:4	6:52.0	0060	90000				Br	oadcast	t		Oxffff	IEEE 802.15.4	10	-79	255	Beacon Request
1	Dec	21,	2013	18:4	6:55.0	0902	11000		0x000	00	Br	oadcast	τ	0x0000	Oxffff	ZigBee	29	-79	255	Link Status
2	Dec	21.	2013	18:4	6:55.1	8796	35000				8r	oadcast	t		0xffff	IEEE 802.15.4	10	-67	255	Beacon Request
3	Dec	21.	2013	18:4	6:55.1	8828	98000	10	0x000	00				0x0000		ZigBee	28	-82	255	Beacon, Src: 0x0000, EPID: SonyEric_67:
4	Dec	21,	2013	18:4	6:56.	3902	56000		0x000	01	1	0x0000		0x0001	0x0000	ZigBee	29	-67	255	Rejoin Request, Device: 0x0001
5	Dec	21,	2013	18:4	6:56.	3915	69000									IEEE 802.15.4	5	-85	255	Ack
6	Dec	21.	2013	18:4	6:56.	3943	39000	- 3	0x000	00		0x0001		0x0000	0x0001	zigBee	39	-85	255	Reioin Response, Address: 0x0000
7	Dec	21.	2013	18:4	6:56.	3959	73000									IEEE 802.15.4	5	-67	255	Ack
8	Dec	21.	2013	18:4	6:56.4	4747	34000	30	0x000	01	Br	oadcast	t	0x0001	Oxffff	ZioBee ZOP	39	-67	255	Device Announcement, Device: 00:00:00 0
9	Dec	21.	2013	18:4	6:56	\$500	68000	- 3	0x000	01		0x0000	<u> </u>	0x0001	0x0000	ZioBee	32	-67	255	Data, Ost Endot: 1 Src Endot: 1
10	Dec	21.	2013	18:4	6:56	5613	78000									TEEE 802.15.4	5	-82	255	Ack
11	Dec	21	2013	18:4	7:00	5308	01000		0x000	00	R/	oadcast		0x0000	Oxffff	ZigRee	32	-75	255	Link Status
12	Dac	21	2012	18.4	7-01	2604	79000	1	0×000	11		oadcast	2	0x0001	Overer	710840	22	-72	255	Lick Status
_													-	1						
En	me 1	· 84	byt	les on	wire	(67	2 hit	s)	84 hv	tes	capt	ured (6	= 72 hi	ts) on in	rerface 0					
Fra	ime () herni	: 84 et Il	byt	es on	wire xasIn	(67 s_00	2 bit :0a:a	s), 5 (0	84 by 0:1a:	ytes :b6:(capt 00:0a	ured (6 :a5), D	— 72 bi st: н	ts) on in onHaiPr_a	terface 0 7:e3:06 (90:ft	a6:a7:e3:06)				
Fra	ine () ierni	t II t Pr	byt , Sr	ces on c: Te cl Ve	wire xasIn rsion	(67 s_00 4.	2 bit :0a:a Src:	s), 5 (0 10.1	84 by 0:1a: 0.10.	ytes :b6:0	capt 00:0a	ured (6 :a5), D .10.2),	72 bi st: H Dst:	ts) on in onHaiPr_a 10.10.10	terface 0 7:e3:06 (90:ft 1 (10.10.10.1	:a6:a7:e3:06))				
Fr: Eti Int Usi	ime) ierni ierni ir Di	t 11 t Pr tagr	byt , Sr otor	tes on c: Te c] Ve Protoc	wire xasIn rsion ol, S	(67 s_00 4, rc P	2 bit :0a:a Src: ort: . cha	s), 5 (0 10.1 zep	84 by 0:1a: 0.10. (1775	ytes :b6:(.2 () 54),	capt 00:0a 10.10 Dst	ured (6 :a5), D .10.2), Port: Z	72 bi st: H Dst: ep (1	ts) on in onHaiPr_a 10.10.10 7754)	terface 0 7:e3:06 (90:ft 1 (10.10.10.1	::a6:a7:e3:06))				
Fr: Eth Int Use Zie	ime) ierni ierni ir Di jBee	t II t Pr tagr	byt , Sr otoc am F apsu	tes on c: Te col ve Protoc lation	wire xasIn rsion ol, S Prot	(67 s_00 4, rc P ocol	2 bit :0a:a Src: ort: , Cha	s), 5 (0 10.1 zep nnel	84 by 0:1a: 0.10. (1775 : 15,	ytes :b6:(.2 (1 54), , Ler	capt 00:0a LO.10 Dst ngth:	ured (6 :a5), D .10.2), Port: Z 10	72 bi st: H Dst: cep (1	ts) on im onHaiPr_a 10.10.10 7754)	terface 0 7:e3:06 (90:ft 1 (10.10.10.1	::a6:a7:e3:06))				
Fra Eti Int Uso Zio	ime (erni erni Bee	t S4 et II et Pr etagr Enca	byt (, Sr otoc am f apsu	tes on c: Te col ve Protoc lation	wire xasIn rsion ol, s Prot	(67 s_00 4, rc P ocol	2 bit :0a:a Src: ort: , Cha	s), 5 (0 10.1 zep nnel	84 by 0:1a: 0.10. (1775 : 15,	ytes :b6:(.2 () 54), Ler	capt 00:0a 10.10 Dst ngth:	ured (6 :a5), D .10.2), Port: Z 10	= 72 bi st: H Dst: rep (1	ts) on im onHaiPr_a 10.10.10 7754)	terface 0 7:e3:06 (90:ft 1 (10.10.10.1	::a6:a7:e3:06))				
Fr: Eti Int Uso Zig	ime i ierni ierni jBee E 8	t S4 et II et Pr tagr Enca	byt (, Sr otoc am F apsul	es on c: Te c) ve Protoc lation	wire xasIn rsion ol, s Prot	(67 s_00 4, rc P ocol	2 bit :0a:a Src: ort: . cha	s), 5 (0 10.1 zep nnel 350	84 by 0:1a: 0.10. (1775 : 15,	ytes :b6:0 .2 (1 54), . Ler	caption 00:0a 10.10 Dst ngth:	ured (6 :a5), D .10.2), Port: z 10	= 72 bi st: H Dst; ep (1	ts) on im onHaiPr_a 10.10.10. 7754)	terface 0 7:e3:06 (90:fb 1 (10.10.10.1	1:a6:a7:e3:06))				
Fr: Eti Uso Zio 000	ine i ierni ierni Bee 90 00	t 11 t Pr tagr Enca fb a	byt , Sr otor am f apsul	es on c: Te c) ve Protoc lation	wire xasIn rsion ol, s Prot d, Ds 6 00 0 ff	(67 s_00 4, rc P ocol	2 bit :0a:a Src: ort: , Cha rootdo b6 00 8d 78	s), 5 (0 10.1 zep nnel	84 by 0:1a: 0.10. (1775 : 15.	ytes :b6:(.2 (1 54), . Ler 5 00 1 02	capt) 00:0a 10.10 Dst ngth: 45 00 0a 0	ured (6 :a5), D .10.2), Port: z 10	= 72 bi st: H Dst: ep (1	ts) on in onHaiPr_a 10.10.10, 7754)	terface 0 7:e3:06 (90:fb 1 (10.10.10.1	::a6:a7:e3:06))				
Fr: Eti Uso Zio 100 000 010 020	ine i erni erni Bee E 8 90 00 00	fb ad fb ad	byt (, Sr otor am F apsul 5 6 18 5 5a	es on c: Te clation e3 0 6 00 0 45 5	wire xasIn rsion ol, s Prot d, Ds 6 00 1 6 00 ff a 00	(67 s_00 4. rc P ocol t: E 1a 11 32	2 bit :0a:a Src: ort: . Cha rootdo b6 00 8d 78 7a 5c	s), 5 (0 10.1 zep nnel 45	84 by 0:1a: 0.10. (1775 : 15. a5 08 0a 0a 58 03	ytes :b6:(2 () 54), , Ler 5 00 1 02 3 01	capt) 00:0a 10.10 Dst ngth: 45 00 0a 0: 0f 0:	ured (6 (a5), D 10.2), Port: 2 10	= 72 bi st: H Dst: ep (1	ts) on inn onHaiPr_a 10.10.10, 7754)	terface 0 7:e3:06 (90:ft 1 (10.10.10.1	::a6:a7:e3:06))				
Fr: Eth Use Zie 200 000 000 000 000 000 000 000 000 00	serni erni gBee 90 00 0a a5	fb a 46 00 00 f	byt (, Sr otoc am (ipsu) 6 18 5 5a f 00	es on c: Te clation e3 0 6 00 0 45 5	wire xasIn rsion ol, s Prot d, Ds 6 00 0 0 ff a 00 0 0a	(67 s_00 4. rc P ocol t: E 1a 11 32 2f	2 bit :0a:a Src: , Cha roado b6 00 8d 78 7a 5c b7 30	s), 5 (0 10.1 zep nnel 351 0a 45 34	84 by 0:1a: 0.10. (1775 : 15. a5 08 0a 0a 58 03 00 00	ytes :b6:(2 (1 54), 1 Ler 5 00 1 02 3 01 0 00	capt: 00:0a 0.10.10 Dst ngth: 45 00 0a 0: 0f 0: 00 0	ured (6 (a5), 0 (10.2), Port: 2 10 F. E	= 72 bi st: H Dst: ep (1 	ts) on im onHaiPr_a 10.10.10, 7754) E. .x z\EX 04	terface 0 7:e3:06 (90:fb .1 (10.10.10.1	1:a6:a7:e3:06))				
Fr: Etl Use Zie 2000 200 200 200 200 200 200 200 200 2	90 00 00 00 00 00	fb a fb a 46 0 01 4 00 f	byt , Sr otoc am F ipsul 6 18 5 5a f 00	es on c: Te col ve Protoc lation 6 00 0 45 5 00 0 00 0	wire xasIn rsion ol, s Prot d, Ds 6 00 0 ff a 00 0 0a 0 00	(67 s_00 4, rc P ocol 13 11 32 2f 00	2 bit :0a:a src: , Cha roado b6 00 8d 78 7a 5c b7 30 00 0a	s), 5 (0 10.1 zep nnel 35t 0a 45 34 34	84 by 0:1a: 0.10. (1775 : 15. a5 08 0a 0a 58 03 00 00 05 20	ytes (b6:0 2 (1 54), Let 8 00 2 01 0 00	capt; 00:0a 0.10.10 Dst ngth: 45 00 0a 0; 00 0; 00 0;	ured (6 (a5), 0 (10.2), Port: 2 10	= 72 bi st: H Dst: ep (1	ts) on int onHaiPr_ai 10.10.10, 7754)	cerface 0 7:e3:06 (90:fb 1 (10.10.10.1	1:a6:a7:e3:06))			,	
Fr: Eti Ini Usi Zii 2ii 2ii 000 000 000 000 000 000 000 0	sme) erni gBee 6 8 90 00 00 03 a5 00 ff	t: 84 t II t Pr tagr Enca 2.11 fb a 46 0 01 4 00 f 00 0	byt , Sr otor am \$ apsul 6 18 5 5a f 00 0 00	es on c: Te col ve Protoc lation 6 00 0 45 5 00 0 00 0	wire xasIn rsion ol, S Prot d, Ds 6 00 0 ff a 00 0 0a 0 00	(67 s_00 4. rc P ocol 11 11 32 2f 00	2 bit :0a:a Src: ort: , Cha r0300 86 78 78 76 56 00 86 78 76 57 30 00 0a	s), 5 (0 10.1 zep nnel 350 0a 45 34 03	84 by 0:1a: 0.10. (1775 : 15, a5 08 0a 0a 58 03 00 00 03 20	ytes (b6:0 2 (1 54), Let 8 00 8 02 3 01 0 00	capt) 00:0a 0.10 0st 0a 0: 0a 0: 0f 0: 00 0-	ured (6 :a5), D 10.2), Port: Z 10	= 72 bi st: H Dst: ep (1	ts) on int onHaiPr_ai 10.10.10, 7754) E. .x 2\EX .04	terface 0 7:e3:06 (90:fb 1 (10.10.10.1	::a6:a7:e3:06))				
Fr: Etl US- Zi- 2i- 0000 010 020 030 030 030 030	erni erni Bee Bee 90 00 03 a5 00	t: 84 et 11 et Pr Enca 2,15 fb a 46 0 01 4 00 f 00 0 07 5	i byt (, Sr otoc am F spsu 5.4 0 6 18 5 5a f 00 00 00 0 1 80	es on c: Te col ve Protoc lation 6 00 0 45 5 000 0 000 0	wire xasIn rsion ol, S Prot d, Ds 6 00 0 ff a 00 0 0a 0 00	(67 s_00 4, rc P ocol t: B 1a 11 32 2f 00	2 bit :0a:a Src: ort: . Cha roado 86 78 7a Sc b7 30 00 0a	s), 5 (0 10.1 zep nnel ast 0a 45 34	84 by 0:1a: 0.10. (1775 : 15. a5 08 0a 0a 58 03 00 00	ytes :b6:(2 () 54), Ler 5 00 1 00 1 11	capt) 00:0a 0.10 Dst ngth: 45 00 0a 0. 0f 0. 00 0-	ured (6 :a5), D :10.2), Port: 2 10	= 72 bi st: H Dst: rep (1 	ts) on ini onHaiPr_ai 10.10.10 7754)	terface 0 7:e3:06 (90:ft 1 (10.10.10.1	a:a6:a7:e3:06))				
Fr: Etil Usi 210 310 320 310 320 330 340 350	erni erni gee 8 90 00 03 a5 00 ff	1: 84 et 11 et Pr tragr Enca 2:15 fb a 46 0 01 4 00 f 00 0 07 b	5 byt (, Sr otoc am F apsu ¹ 5.4 C 6 18 5 Sa 7 OC 0 OC 1 80	es on c: Te ol ve rotoc lation 6 00 0 45 5 00 0 00 0	wire xasIn rsion ol, S Prot d, DS 6 00 0 ff a 00 0 0a 0 00	(67 s_00 4, rc P ocol 11 11 32 2f 00	2 bit :0a:a src: . cha roado b6 00 8d 78 7a 5c b7 30 00 0a	s), 5 (0 10.1 zep 0a 45 34 93	84 by 0:1a: 0.10. (1775 : 15. a5 08 0a 0a 58 03 00 00 05 23	ytes :b6: 2 ((54), , Les 5 00 8 02 3 01 0 00	capti 00:0a 10.10 Dst i ngth: 45 00 0a 0: 00 0 01 1	ured (6 :a5), D 10.2), Port: 2 10 	= 72 bi st: H Ost: rep (1 	ts) on im onHaiPr_a 10.10.10. 7754) E. .x 2\EX .04 	terface 0 7:e3:06 (90:ft	::a6:a7:e3:06))				
Fr: Eti Usi Zii 2000 200 200 200 200 200 200 200 200	ime ; erni gBee 90 00 0a a5 00	1: 84 et I) et Pr tragr Enca 2:15 fb a 46 0 01 4 00 f 00 0 07 b	5 byt (, Sr otoc am F apsu ¹ 5.4 C 6 18 5 Sa 7 OC 0 OC 1 80	es on c: Te col ve Protoc lation 00 0 45 5 00 0 00 0	wire xasIn rsion ol, 55 Prot d, D5 6 00 0 ff a 00 0 0 0 ff 0 00 0 00	(67 s_00 4, rc P ocol 11 11 11 32 2f 00	2 bit :0a:a src: . Cha roadd b6 00 8d 78 7a 5c b7 30 00 0a	s), 5 (0 10.1 2ep nnel 35 0 45 34 34 34	84 by 0:1a: 0.10. (1775 : 15. a5 08 0a 0a 58 03 00 00 08 20	ytes :b6:c .2 (1 54), . Les \$ 00 \$ 01 \$ 01 \$ 01	capt 00:0a 10.10 Dst 10 01 01 01 01 01 01 01	ured (6 (a5), 0 10,2), Port: 2 10	= 72 bi st: H Dst: ep (1 ZEZ.2	ts) on inn onHalPr_ai 10.10.10. 7754)	terface 0 ?:e3:06 (90:ft	a:a6:a7:e3:06))				
Fr: Eti Usi Zii 000 100 200 300 400 500	ime ; erni gBee 90 00 0a a5 00	1: 84 et 11 et Pr Enca 2:11 fb a 46 0 00 f 00 0 00 f	i byt (, Sr otoc am F apsul 5.4 C 6 18 5 5 6 0 00 0 00 0 00 0 1 80	es on c: Te c) ve Protoc lation 6 00 0 45 5 00 0 00 0	wire xasIn rsion ol, s Prot 0 ff a 00 0 ff a 00 0 0a 0 00	(67 s_00 4, rc P ocol 11 11 11 32 2f 00	2 bit :0a:a src: ort: . Cha roudo 86 78 7a 5c b7 30 00 0a	s), 5 (0 10.1 2ep nnel 34 45 34 23	84 by 0:1a: 0.10. (1775 : 15. a5 08 0a 0a 58 03 00 00 08 20	ytes :b6:c .2 (1 54), . Les 5 00 8 02 3 01 0 1 1	capt 00:00 Dst ngth: 45 00 00 0 00 0 01 1	ured (6 (a5), 0 (10.2), Port: 2 10	= 72 bi st: H Dst: ep (1	ts) on im onha/Pr_a: 10.10.10. 7754) E. 	terface 0 7:e3:06 (90:fb 1 (10.10.10.1	a:a6:a7:e3:06))				

Applying our 802.15.4 profile with predefined color rules:

zig	bee_c	lemo.	pcapng	Wires	hark 110.5	SVN Re	v 5426	2 from	/trunk	-1.10	1	-	-							
Eile	Edit	Yiev	v <u>G</u> o	⊆apture	: Analyze	t Statisti	ics To	elephor	ny I	ools	Internals	Help								
0	•		10	8		10	4	¢ 🔹	3	2		Q	990	1	i 🖾 🥵 %	1				
Filter											· Expres	sion	Clear Apply	Save	e					
No.	Time						Mac	Src Ad	dress	Ma	c Dst Addre	ss Ni	wk Sec Addres	s N/	wk Dst Address	Protocol	Length	RSSI	LQI	Info
0	Dec	21.	2013	18:4	5:52.00	6090000)			1	Broadcas	ť.			Oxffff	IEEE 802.15.4	10	-79	255	Beacon Request
1	Dec	21,	2013	18:4	5:55.09	0211000	0	0x00	00	. 8	sroadcas	τ	0x0000		Oxffff	Zigsee	29	-79	255	Link Status
2	Dec	21,	2013	18:4	5:55.87	9635000	0			1	troadcas	τ			Oxffff	IEEE 802.15.4	10	-67	255	Beacon Request
3	Dec	21.	2013	18:4	5:55.88	2898000	0	0x00	00				0x0000			zigsee	2.8	~82	255	Beacon, Src: 0x0000, EPID: SonyEric_67:89
-4	Dec	21,	2013	18:4	5:56.39	0256000	0	0x00	01		0x0000		0x0001		0x0000	zigőée	29	-67	255	Rejoin Request, Device: 0x0001
5	Dec	21,	2013	18:4	5:56.39	1569000	0									IEEE 802.15.4	5	-85	255	Ack
6	Dec	21	2013	18:4	5:56.39	4339000	0	0x00	00		0x0001		0x0000		0x0001	Zigsee	39	-85	255	Rejoin Response, Address: 0x0000
7	Dec	21	2013	18:4	5:56.39	5973000	D C									IEEE 802.15.4	5	-67	255	Ack
8	Dec	21	2013	18:4	5:56.47	4734000	0	0x00	01	1	Iroadcas	£.	0x0001		Oxffff	ZigSee ZDP	39	~67	255	Device Announcement, Device: 00:00:00_00:
9	Dec	21,	2013	18:4	5:56.55	9968000	0	0x00	01		0x0000		0x0001		0x0000	Zigsee	32	-67	255	Data, Dst Endpt: 1, Src Endpt: 1
10	Dec	21	2013	18:4	5:56.56	1378000	0									IEEE 802.15.4	5	-82	255	Ack
11	Dec	21	2013	18:4	7:00.53	0801000	0	0x00	00	. 8	troadcas	τ	0x0000		Oxffff	ZigBee	32	-75	255	Link Status
12	Dec	21	2013	18:4	7:01.36	0479000	0	0x00	01		eroadcas	τ	0x0001		Oxffff	ziosee	-32	-73	255	Link Status
	98e0 98e0 98e0 98e0	En 802.1 Net Ap	capsul 15.4 (twork plicat	lation Data, Layer tion S	Protoc Dst: 0x Data, upport	ol, Ch 0000, Dst: 0 Layer	annel Src: x0000 Data,	: 15 0x00 , Sr Dst	, Le 01 c: 0 End	x000 pt:	: 32 1 1, Src E	indpt	: 1							
∎ Da	ta	5 b	ytes)	est.																
	[Ler	gth	: 5]	1001																
0000 0010 0020 0030 0040 0050 0060	90 00 00 00 00 00	fb 5c 01 00 00 01	a6 a7 06 21 45 52 ff 00 00 48 e5	e3 0 00 0 45 5 0 00 0 00 0 00 0	6 00 1a 0 ff 11 a 00 48 0 0f 15 0 00 00 0 00 01 c 6c 6f	b6 00 8d 5 c7 5 1f e 00 20 00 0 bd 80	0 0a 9 0a 1 45 9 14 0 61 a db	a5 00 0a 00 58 0 00 00 88 79 00 00	8 00 a 02 3 01 0 00 9 34 1 01	45 0 0f 0 09 0 12 0	00 0a 0a 04 01	ZEZ.I	E. YE. 							
0.*	Date	(dat	a) Shee				Part	ato 12	Dire	De	of Jac 202 15									



3 Sniffer configuration

3.1 Home page

Open Sniffer

RUN/STOP button and status field are located below the top menu. RUN/STOP button is present on every subpage 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.

🖸 Open Sniffer	×	± - □ ×
← → C 🗅	10.10.10.2/index.shtml	ର ଛ] ≡
802.15.4	HOME Se	ttings ED scanner CT Mode Injection Mode Network scan
RUN		STOPPED
	SUMM	ARY
	MAC address	IP address
	00:1e:c0:94:44:49	10.10.10.2
	Channel	Receiver sensitivity
	15	High
	DHCP	CRC filter
	OFF	OFF
	Packets through	Packets dropped
	0	0
© 2013 Se	wio Networks Firmware version 0.7	



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
 - \circ Medium lower than -79 dBm
 - Low lower than -64dBm
 - o 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

Open Sniffer

• 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



			STOPP
	RADIO S	ETTINGS	
Frequency / Channel		Modulation	
2425/15	▼ MHz/-	O-QPSK_250 (compliant)	¥
Receiver sensitivity		CRC filter	
High (< -91dBm)	T		
LQI/CRC mode			
* LQI •	CRC		
	SUBM	IT & RUN	
	IPV4 SE	TTINGS	
IP mode		ID arkiness	
• DHCP	 Static 	10.10.10.2	
Netmask		Gateway	
200.200.200.0		10.10.10.1	
	SU	BMIT	
		TTINGS	
	HOST SE	ETTINGS	
Host IP address	HOST SI	ETTINGS Host UDP part	
Host IP address	HOST SI	Host UDP port	

Open Sniffer

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.







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.

802.15.4 / Zigbee / 6LowPan	HOME Se	ettings E	ED scanner	CT Mode	Injection Mode	Network scan	1
RUN					ST	OPPED)
CONTINUOUS	TRAN	ISM	ISSIO	N MO	DE		
Frequency / Channel		Mode					
2425/15 ▼ N	1Hz/-	PRB	S: AAAA		•		
Modulation		Transi	mitted powe	rlevel			
O-QPSK-250 (compliant) ▼		3.0			▼ dE	Bm	
	LAUI	NCH					
Warning: Accomplichment of regional distinct	iono of roquia	ton, roqui	iromonto io c		roopopoibility		
PRBS - Pseudo Random Bit Sequence	ions of regula	atory requi	irements is c	ni your own	responsibility.		
CW - Continuous Wave							
Fc - Channel center frequency							
RC - Raised Cosine							
SCR - Scrambler							

CW mode has 6 different frequencies:

- Fc + 0.50 MHz
- Fc 0.50 MHz
- Fc + 0.25 MHz
- Fc 0.25 MHz
- Fc + 0.10 MHz
- Fc 0.10 MHz

Fc 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.



<u>PBRS mode</u> transmits payload bytes continuously in the infinite loop.

There are 3 payloads available:

- PRBS: 0xAAAA... Repeated hexadecimal value A (1010 binary).
- PRBS: 0×0000... 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.

802.15.4 / Zigbee / 6LowPan	HOME	Settings	ED scanner	CT Mode	Injection Mode	Network scan
RUN					S	TOPPED
INJEC	CTION	SET	TINGS			
Frequency / Channel] MHz/-	Modu	lation PSK-SIN-RC)-100 (co	mpliant) 🔻	
Transmitted power level	dBm	RX er	nabled after s O Yes	end ®	No	
Number of packet repeat]	Time	space betwe	en packets	1 n	ns
Packet payload ^{1,2,3}						
Bytes to send (without CRC ⁴): 3 010203					CL	EAR
Estimated time of Injecting						
	~ 18.59	8 sec	onds			
	ST	TART				

Open Sniffer



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.

Den Sniffer 02.15.4 / Zigbee / 6LowPan HOME Settings ED scanner CT Mode Injection Mode Network scan								
)							
 NETWORK SCAN								
How long scan on each channel ?								
1 seconds								
Which band scan ?								
Estimated time of Network scan								
~ 31 seconds								
START								

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 endproduct 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.

v0.1