

Wireshark ZigBee Sniffer

Configuration and Use

© Z-Smart Systems UK Ltd

Wireshark and the "fin" logo are registered trademarks of the Wireshark Foundation



Table of Contents

Table of Contents	2
Overview	3
Wireshark	3
Dongle Specific Sniffers	4
Texas CC2531	5
Ember NCP Sniffer	5
Software Operation	7
Configuration	7
Getting Started	7
Setting Security Keys	8
Filters	9
Colouring Rules	11
Display Filter Macros	12
Analysing Data	13
IO Graph	13
Protocol Statistics	14
Exporting Selected Packets	14



Overview

A ZigBee sniffer allows capture and display of data frames transmitted between ZigBee devices. It captures the data received with a separate radio from that used by the main system, and can display low level frames that can be useful for debugging problems on the network. Often these low level issues can not be otherwise debugged using higher level APIs that connect to the coordinator as this information is simply not provided.

This document provides information on setting up and using the Wireshark software. Different hardware is available for use with this including the Texas Instruments CC2531 dongle that is commonly available at low cost in online marketplaces such as eBay and AliExpress, and the CEL MeshConnect dongle, or other dongles using the Silabs Ember chipset can also be used.

There are many resources available for using Wireshark, and this document does not intend to replace a good understanding of the software or protocol analyses principals. It does however provide the user with a basic understanding of ZigBee and Wireshark a quick start guide to packet sniffing for the purposes of providing feedback to Z-Smart Systems when reporting ZigBee issues.

Wireshark

Wireshark is a packet capture and analyses tool that can be downloaded freely from the web. It is capable of displaying the contents of ZigBee packets, and allows the debugging of low level protocol issues. Wireshark can be downloaded from <u>https://www.wireshark.org/</u>.



WIRESHARK	NEWS	Get Acquainted 🔻	Get Help 🔻	Develop 🔻	Our Sponsor	SharkFest
Dow The curr	/NO	ad Wires e release of Wireshark	hark			
Stable Release (2.6.2) • July 18, 2018						^
Windows Installer (64-bit) Windows Installer (32-bit) Windows PortableApps® (32-bit) ▲ macOS 10.6 and later Intel 64-bit .dmg Source Code						
Old Stable Release (2.4.8) • July 18, 2018						~ <
Development Release (2.5.1) • March 15, 2018						~
Documentation						~
More downloads and	document	tation can be found or	n the downloa	ds page.		

Dongle Specific Sniffers

Wireshark does not directly interact with ZigBee hardware - it requires a dongle and associated sniffer software to provide it with the data to analyse. The sniffer is very simple - it is only grabbing the low level frames from the dongle and passing them to Wireshark. Note that when used as a sniffer, the dongle is not running in its standard mode and is not used as a node on a ZigBee network. It will normally either run different firmware, or be configured into a specific mode to provide the low level data required.





Sniffer software in Python is available here -: https://github.com/andrewdodd/ccsniffpiper

To install on a Mac OS X -: brew install libusb

easy_install pip pip install pyusb

Note that I haven't tried this software and it may create named pipes that mean Wireshark is started slightly differently than described below.

TBD...

Ember NCP Sniffer

The Z-Smart Systems Ember sniffer software is written in Java so can be run on any computer with a Java VM. It can be used with most standard Ember NCP firmware (any containing the mfglib library), and when running will place the dongle into a special mode where low level frames are provided as required for the sniffer application.

The sniffer application can directly write the Wireshark *pcap* files and Silabs ISD files.





The sniffer is available on Github

https://github.com/zsmartsystems/com.zsmartsystems.zigbee.sniffer

The sniffer is a console application and requires configuring through the command line -:

usage: ZigBeeSniffer	
-?,help	Print usage information
<pre>-a,ipaddr <remote address="" ip=""></remote></pre>	Set the remote IP address
-b,baud <baud></baud>	Set the port baud rate
<pre>-c,channel <channel id=""></channel></pre>	Set the ZigBee channel ID
-f,flow <type></type>	Set the flow control (none hardware
	software)
-l,local	Log times in local time
-m,maxpcap <length></length>	Maximum filesize for Wireshark files
-p,port <port name=""></port>	Set the port
<pre>-r,ipport <remote ip="" port=""></remote></pre>	Set the remote IP port
<pre>-s,silabs <filename></filename></pre>	Log data to a Silabs ISD compatible
	event log
-t,timeout <seconds></seconds>	NCP restart timeout in seconds
-w,pcap <filename></filename>	Log data to a Wireshark pcap compatible
	log

Note that the IP address will default to the local host on the assumption that you are running Wireshark on the same computer as the sniffer. The *ipport* will default to 17754 which is the port used for the ZigBee Encapsulation Protocol - changing this may stop Wireshark displaying ZigBee data.

Example command line -:

java -jar ZigBeeSniffer.jar -port /dev/tty.SLAB_USBtoUART -baud 115200 -flow hardware

The software will print an output to the console for each packet that is received to allow confirmation it is working. When running Wireshark, these should also be seen in the Wireshark window.

WiresharkZepFrame [sequence=00000000, lqi=255, data={41 88 41 EF CD FF FF 00 00 09 12 FC FF 00 00 01 81 01 00 00 00 08 22 00 28 00 10 01 00 00 00 08 22 00 08 22 00 00 29 88 AC EB 6B 87 FF 80}] WiresharkZepFrame [sequence=00000001, lqi=255, data={41 88 42 EF CD FF FF 00 00 09 12 FC FF 00 00 01 82 01 00 00 00 08 02 20 02 80 11 00 11 00 01 00 00 00 08 22 00 08 20 08

If the NCP fails to receive a valid frame with the timeout period set with the -t command line parameter, then the NCP will be restarted. This will allow the sniffer to recover from serial port or NCP communications problems. The timer defaults to 30 seconds.



Software Operation

Configuration

A few options that may be worth considering to make the software more usable -:

Time format - setting to time of day may help to coordinate different log files, such as the log generated by the Z-Smart Systems ZigBee framework. By default, the time will be in microseconds - milliseconds is probably sufficient.

Date and Time of Day (1970-01-01 01:02:03.123456) Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)	∿₩1
✓ Time of Day (01:02:03.123456)	\\₩2
Seconds Since 1970-01-01	\\#3
Seconds Since Beginning of Capture	~:#4
Seconds Since Previous Captured Packet	∿₩5
Seconds Since Previous Displayed Packet	\7₩6
UTC Date and Time of Day (1970-01-01 01:02:03.123456)	∖⊂₩7
UTC Year, Day of Year, and Time of Day (1970/001 01:02:03.1234	156)
UTC Time of Day (01:02:03.123456)	₹#8
Automatic (from capture file)	
Seconds	
Tenths of a second	
Hundredths of a second	
✓ Milliseconds	
Microseconds	
Nanoseconds	
Display Seconds With Hours and Minutes	

Getting Started

From the Wireshark start screen, you need to start receiving the ZEP (ZigBee Encapsulation Protocol) frames that are sent to port 17754. The filter udp port 17754 will ensure that only ZigBee frames are captured. If you are running the sniffer on the same computer as Wireshark, then you will probably want to use the Loopback interface - otherwise select another suitable interface.

Capture					
using this filter: 📙 udp port 17754	All interfaces shown 🔻				
Loopback: lo0 gif0 stf0 XHC20 © Cisco remote capture: ciscodump © Random packet generator: randpkt					
Learn User's Guide · Wiki · Questions and Answers · Mailing Lists You are running Wireshark 2.6.2 (v2.6.2-0-g1b3cedbc).					

Once Wireshark starts to capture packets, they will be displayed in the main screen as seen below. This is broken into 3 main areas - the list of received packets, the detailed packet information, and the raw packet data.



Configuration and Use Sunday, 23 December 2018

	• • • ZigBee Capture.pcapng						
	1 💿 🗖	0 🗙 🚺	२ 🔶 🔿 🖄 🏹	s 👲 🔲 🗐			
	a display filter < %	/>				Expression	+ Leave
No	Time	Source	Destination	Protocol	Length Info		1
219	17:21:59 612750056	300100	Destination	TEEE 902 15 4			
210	17:31:50.612533405	0~000	0,2945	ZicBee	121 ADS: Ack Det Endet: 0 Sec Endet: 0		
215	17:31:58 615232676	0,0000	672045	TEEE 802 15 4	79 Ack		
221	17:31:58.661335604	0x1f75	Broadcast	ZigBee ZDP	131 Device Announcement, Nwk Addr: 7c:25:24:00:00:16:37:62		
222	17:31:58.696167177	0x1f75	0×0000	ZigBee HA	126 ZCL: Report Attributes, Seq: 0		
223				IEEE 802.15.4	79 Ack		
224	17:31:58.696585689	0x3a67	Broadcast	ZigBee ZDP	131 Device Announcement, Nwk Addr: 7c:25:24:00:00:16:6c:fc		
225	17:31:58.743369373	0x1f75	0×0000	ZigBee HA	126 ZCL: Report Attributes, Seq: 1		
226	17:31:58.744050504	0xb465	Broadcast	ZigBee ZDP	131 Device Announcement, Nwk Addr: Quirky_00:00:07:39:01		
227	17:31:58.744704715	0x1f75	0×0000	ZigBee HA	126 ZCL: Report Attributes, Seq: 1		
228	17:31:58.744944665			IEEE 802.15.4	79 Ack		
229	17:31:58.745939209	0xb465	Broadcast	ZigBee ZDP	131 Device Announcement, Nwk Addr: Quirky_00:00:07:39:01		
230	1/:31:58./69/88824	0x5d/2	Broadcast	ZigBee ZDP ZigBee ZDP	131 Device Announcement, Nwk Addr: Quirky_00:00:06:36:10		
231	17:31:30.770204210	0x3407	Broducasc	Zigbee ZDP	131 Device Announcement, NWK Addr: 70:25:24:00:00:10:00:10		
233	17:31:58 986474416	0,0000	670343	TEEE 802 15 4	79 Ack		
234	17:31:58.987056728	0×0000	Øxd545	ZigBee ZDP	121 Link Quality Request		
235	17:31:58.987271754	0,0000	0,40,10	TEEE 802.15.4	79 Ack		
Des Sou [E: 0] Fra ZigBee V ZigBee V Fra Clu Pra Sou	Destination: 8x0808 Source: 7x125524:00:00:16:37:62 (7c:25:24:00:00:16:37:62)] [Drigin: 141] Frame Check Sequence (TI CC24xx format): FCS 0K ZigBee Network Layer Data, Dst: 8x0808, Src: 0x175 ZigBee Network Layer Data, Dst: 0x1075 V JegBee Application Support Layer Data, Dst Endpt: 1, Src Endpt: 1 * Frame Control Field: Data (0x08) 000 = Frame Type: Data (0x08) Destination Endpoint: 1 Cluster: On/Off (0x00806) Frofile: Home Automation (0x0184)						
Counter: 3							
0000 00 0010 00 0020 00 0030 01	0000 <						
Frame (Decryp	Ted Zigbee Payload (15	bytes)				
0 2	Ready to load or capture Packets: 3063 · Displayed: 3063 (100.0%) Profile: Default						

Setting Security Keys

To properly decode ZigBee frames, the keys must be added to Wireshark preferences. If Wireshark doesn't know your keys, it will not display the full packet contents and will effectively be useless for analysing data.

At least the network key is required. Select the preferences, and go to the ZigBee Protocol preferences page. Select the Edit button to change the Pre-configured Keys.

	Wireshark · Preferences
WTP X.25	ZigBee Network Layer
X11	Security Level AES-128 Encryption, 32-bit Integrity Protection
X2AP	
XDMCP	Pre-configured Keys Edit
XMCP	
XML	
XMPP	
XOT	
XYPLEX	
YAMI	
YMSG	
ZEDRA	
ZigBee ADS	
ZigBee Green	
ZRTP	
ZVT	
Statistics	
Advanced	
Help	Cancel



Enter your network key, and it is also advisable to enter the ZigBeeAlliance09 key that is normally used to allow ZHA devices to join the network.

5A:69:67:42:65:65:41:6C:6C:69:61:6E:63:65:30:39

Pre-config	ured Keys			
Key AA:AA:AA:AA:AA:AA:AA:AA:AA:AA:AA:AA:AA:	BA:AA:AA N :30:39 N	Byte Order Normal Normal	Label Test Key / ZigBeeAlli	AA ance09
+ - 9 ^ V E	/Users/	/chris/.config,	/wireshark/zig	<u>jbee_pc_key</u>

Filters

Wireshark has a powerful filter system to allow frames to be selectively displayed. The Expression... button in the filter bar will display the Filter Expression box.



• • • Wiresh	ark · Display Filter Expression
Field Name	Relation
 ZCL Shade Configuration · ZigBee ZCL Shade Con ZCL Sub-Ghz · ZigBee ZCL Sub-Ghz ZCL Temperature Meas. · ZigBee ZCL Temperatu ZCL Thermostat · ZigBee ZCL Thermostat ZCL Thermostat User Interface Configuration · Zig ZCL Time · ZigBee ZCL Time ZCL Touchlink · ZigBee ZCL Touchlink ZCL Touchlink · ZigBee ZCL Touneling ZEBRA · Zebra Protocol ZEP · ZigBee Encapsulation Protocol ZigBee · ZigBee Network Layer zbee_beacon.end_dev · End Device Capacity zbee_beacon.profile · Stack Profile Zbee_beacon.profile · Stack Profile zbee_beacon.protocol · Protocol ID zbee_beacon.protocol · Protocol ID zbee_beacon.protocol · Protocol ID zbee_beacon.profile · Stack Profile zbee_beacon.router · Router Capacity zbee_beacon.router · X Offset zbee_beacon.update_id · Update ID zbee_nwk.cmd.cinfo · Capability Information zbee_nwk.cmd.cinfo.alt_coord · Alternate Cooid zbee_nwk.cmd.cinfo.alt_coord · Alternate Cooid zbee_nwk.cmd.cinfo.security · Security Capability zbee_nwk.cmd.cinfo.security · Security Capability zbee_nwk.cmd.cinfo.alt_coord · Alternate Cooid zbee_nwk.cmd.cinfo.alt_coord · Alterest zbee_nwk.cmd.cinfo.alt_coord · Alternate Coo	figurati is present = = l= Relations can be used to restrict fields to specific values. Each relation does the following: gBee Z > e= = in contains field contains, matches Check the field to a specific value. in contains, matches Check the field to a specific set of values expression (matches) value. contains, matches Check the field to a specific set of values Value (Unsigned integer, 2 bytes) 0x0 Predefined Values Network Specific ZigBee Home ZigBee PRO liity ress drinator Range (offset:length) n
zhee beacon profile == $0x0$	
Click OK to insert this filter	
Help	Cancel OK

Buttons can be configured to allow quick access to often used filters

🗽 zbee_beacon.profile == 0x2					
	Filter Buttons Preferences	Label: Enter a description for the filter button Filter: zbee_	<pre>beacon.profile == 0x2</pre>		
		Comment: Enter a comment for the filter button			

The following provides a useful set of filter buttons -:

This file is automatically generated, D0 NOT MODIFY.
"TRUE","Leave","zbee_nwk.cmd.id == 0x4","Filter all LEAVE commands"
"TRUE","Association","wpan.cmd == 0x1 || wpan.cmd == 0x02","Filter ASSOCIATION related commands"

To add these to Wireshark, click the Filter Button Preferences... button above, then click on the link in the bottom right corner of the following window to edit the file. Wireshark must be restarted before the changes will be visible.



Colouring Rules

Wireshark can highlight packets in the packet window based on colouring rules. These use the same rules as the filters and can be configured in the View menu, Colouring Rules... option.

lam	le	Filter			
~	ZigBee Link Record	zbee_nwk.cmd.id == 0x5			
~	ZigBee Link State	zbee_nwk.cmd.id == 0x8			
~	ZigBee Link Response	zbee_nwk.cmd.id == 0x2			
~	ZigBee Link Request	zbee_nwk.cmd.id == 0x1			
~]	ZigBee APS Ack	zbee_aps.type == 0x2			
\checkmark	IEEE 802.15.4 ACK	wpan.frame_type == 0x2			
/	ZigBee Announce Commands	zbee_aps.zdp_cluster == 0x13			
/	ZigBee Association Response	wpan.cmd == 0x2			
/	ZigBee Association Request	wpan.cmd == 0x1			
/	ZigBee Cluster Library Commands	zbee_zcl			
	ZigBee Leave Commands	zbee_nwk.cmd.id == 0x4			
/	ZigBee invalid beacon protocol	zbee_beacon.profile==0			
/	ZigBee Beacon allowing joins	zbee_beacon.router==true			
	ZigBee Beacon	zbee_beacon.profile==0x2			
	ZigBee Beacon Request	wpan.cmd == 0x7			
	ZigBee	zep			
	ZigBee Beacon ZigBee Beacon Request ZigBee	zbee_beacon.profile==0x2 wpan.cmd == 0x7 zep			
ZigBee zep Double click to edit. Drag to move. Rules are processed in order until a match is found.					
÷	- Pa				



The following provides a useful set of colouring rules that may be imported into Wireshark -:

```
# D0 NOT EDIT THIS FILE! It was created by Wireshark
@ZigBee Link Record@zbee_nwk.cmd.id == 0x5@[65535,52428,26214][0,39321,39321,39321]
@ZigBee Link Response@zbee_nwk.cmd.id == 0x2@[65535,52428,26214][26214,0,0]
@ZigBee Link Response@zbee_nwk.cmd.id == 0x2@[65535,52428,26214][0,13107,39321]
@ZigBee Link Request@zbee_nwk.cmd.id == 0x2@[65535,55428,26214][0,13107,39321]
@ZigBee APS Ack@zbee_aps.type == 0x2@[65535,65535][3921,39321,39321]
@IEEE 802.15.4 ACK@wpan.frame_type == 0x2@[65535,65535][52428,52428,52428]
@ZigBee Announce Commands@zbee_aps.zdp_Cluster == 0x13@[26214,65535,26214][65535,26214,26214]
@ZigBee Association Response@wpan.cmd == 0x2@[26214,65535,26214][0,13107,65535]
@ZigBee Cluster Library Commands@zbee_zcl@[26214,65535,65535][0,0,0]
@ZigBee Leave Commands@zbee_nwk.cmd.id == 0x4@[13107,13107,13107][65535,39321,39321]
@ZigBee invalid beacon protocol@zbee_beacon.profile==0@[64764,0,7196][0,0,65535]
@ZigBee Beacon allowing joins@zbee_beacon.ruter==true@[52428,52428,52428][0,65535,0]
@ZigBee Beacon.erofile==0x2@[52428,52428,52428][0,65535,0]
@ZigBee Beacon Request@wpan.cmd == 0x7@[52428,52428,52428][0,0,65535]
@ZigBee Beacon Request@wpan.cmd == 0x7@[52428,52428][0,0,65535]
!@ZigBee Beacon Request@wpan.cmd == 0x7@[52428,52428][0,0,65535]
!@ZigBee Beacon Request@wpan.cmd == 0x7@[52428,52428][0,0,65535]
```

Display Filter Macros

Display Filter Macros are a mechanism to create shortcuts for complex filters.

🛑 🔘 🛑 🧧 Display Filter Macros			
Nai	me	Text	
	zigbee_address	zbee_nwk.src == \$1 zb	ee_nwk.dst == \$1
	-		
+	- 10 ^		/Users/chris/.config/wireshark/dfilter_macros
H	lelp		Cancel OK

For example defining a display filter macro named *zigbee_address* defined as *zbee_nwk.src* == $\$1 \parallel zbee_nkw.dst$ == \$1 could be used as $\${zigbee_address:0x1234}$ to display all packets to or from address 0x1234.

Масто	Content
zigbee_address	wpan.dst16 == \$1 wpan.src16 == \$1



Wireshark ZigBee Sniffer Configuration and Use Sunday, 23 December 2018

IO Graph

Wireshark provides a very useful facility to graph events. Any expression can be used to graph the number of events per second.





Protocol Statistics

11010001		Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packet
Frame		100.0	3063	100.0	337806	54 k	0
Ethernet		100.0	3063	12.7	42882	6906	0
Interr	et Protocol Version 4	100.0	3063	18.1	61260	9866	0
▼ Us	er Datagram Protocol	100.0	3063	7.3	24504	3946	0
▼	ZigBee Encapsulation Protocol	100.0	3063	29.0	98016	15 k	0
	IEEE 802.15.4 Low-Rate Wireless PAN	100.0	3063	32.9	111144	17 k	994
	 ZigBee Network Layer 	59.5	1824	23.4	79105	12 k	400
	 ZigBee Application Support Laye 	er 46.5	1424	6.5	21899	3527	502
	ZigBee Device Profile	28.1	860	3.0	10093	1625	860
	ZigBee Cluster Library	2.0	62	0.1	414	66	62
	ZigBee Beacon	8.0	245	1.1	3675	591	245

Exporting Selected Packets

It may be necessary to export a select few packets to illustrate a problem you have identified. To do this, you can select the packets, and export them as follows.

Mark packets using the Edit menu options -:

🛒 V	Wireshark	File	Edit View Go Capture	Analyze	Statistics	Telephony	Wirele	ess Tools	Help	0			D :	* 🗟 🕇	100% 🛃	Sat 11:12	ର ≔
		- 1	Сору	•		📕 Loopbac	k: lo0 (u	dp port 177	54)								
			S Find Packet	ЖF				\oplus \ominus		E							
			Find Next	ЖN		∠ _		44	~ <u>1</u>	E							
Apply	a display filte	r <{	Find Previous	ЖΒ										Expression	+ Le	ave Associat	tion Announce
No.	Time	Sou	Mark/Linmark Packet	₩M	Protoc	ol	Length	Destination	Infe	D							
9618	3 22:54:08.568	8 0x41	Mark All Displayed	A 9€ M	ZigBee	00 15 4	111	0×0000	Re	join Requ	est, De	vice: 0>	(48†5				
9628	22:54:08.92	0×41	Mark All Displayed		TEEE 8	02.15.4	76	0×0000	Dat	a Request	+						
9621	22:54:08.928	B N/A	Unmark All Displayed	₹ ₩	IEEE 8	02.15.4	69	0,0000	Acl	<							
9622	22:54:08.934	0×01	Next Mark	企業N	ZigBee		121	0x48f5	Re	join Resp	onse, N	ew Addre	ess: 0x4	8f5			
9623	3 22:54:08.934	N/A	Previous Mark	企業B	IEEE 8	02.15.4	69		Ac								
9624	22:54:09.177	0x41			IEEE 8	02.15.4	76	0×0000	Dat	ta Reques	t						
9625	5 22:54:09.178	B N/A	Ignore/Unignore Packet	жD	IEEE 8	02.15.4	69		Acl								
9626	5 22:54:09.429	0x41	Ignore All Displayed	介留D	IEEE 8	02.15.4	76	0×0000	Dat	ta Reques	t						
9627	22:54:09.430) N/A	Upignoro All Displayed	7-980	IEEE 8	02.15.4	69	0	Aci	<							
9628	22:54:09.68	N/A	Unighore All Displayed	C 36 D	TEEE 8	02.15.4	/4	OXTTTT	Bea	acon keque	est						
		0x1	Sat/Upgat Time Deference	φT			92				• 0x145						
9631	22:54:09.83	0x4	Set/Unset Time Reference	æ i	ZigBee		111	0×0000	Re	ioin Requ	est. De	vice: 0	48f5		05.54		
9632	22:54:09.835	N/A	Unset All Time References	72 % T	IEEE 8	02.15.4	69		Ac	<	,						
9633	3 22:54:10.194	0x41	Next Time Reference	-Σ [#] N	IEEE 8	02.15.4	76	0×0000	Dat	ta Request	t						
9634	22:54:10.194	N/A	Previous Time Reference	77 # B	IEEE 8	02.15.4	69		Acl								
9635	5 22:54:10.202	2 0×01			ZigBee		121	0x48f5	Re	join Resp	onse, N	ew Addre	ess: 0x4	8f5			
9636	5 22:54:10.203	B N/A	Time Shift	Ω₩T	IEEE 8	02.15.4	69		Acl								
9637	22:54:10.445	6 0x41			IEEE 8	02.15.4	76	0×0000	Dat	ta Reques	t						
9638	3 22:54:10.445	N/A	Packet Comment	77 #C	IEEE 8	02.15.4	69		Aci								
9639	22:54:10.694	0X41	Delete All Backet Comments		TEEE 8	02.15.4	/0	0X0000	Dat	ca keques	τ						
► Frame	9665: 69 byte	5 00 1	Delete All Facket Comments	5) on interface	02.15.4	05		ACI	\							
Null/L	_oopback		Configuration Profiles	☆₩A	, on incertace	U III											
User D	Datagram Proto	col, S	Emoji & Symbols	ЖSpace													
TEFE 8	302.15.4 Ack.	Sequenc	e Number: 25														
▼ Fra	ame Control Fi	eld: 0	0002, Frame Type: Ack, Destinati	on Address	ing Mode: None	e, Frame Versio	n: IEEE	Std 802.15.4	-2003, Sou	urce Addre	essing M	Mode: No	one				
		010	= Frame Type: Ack (0x2)														
		. 0	= Security Enabled: False														
		0	= Frame Pending: False														
)	= Acknowledge Request: False														
	0.	• • • • • •	= PAN 1D Compression: False														



Marked pa	ckets will bec	ome hic	hlighted	and ca	an be	expo	orte	d with tl	he File m	enu optio	on -:	
🗯 Wireshark	File Edit View Go	Capture An	alyze Statistic	Telephony	Wireles	ss Tools	Help	p () 📥		3 🔶 🛋 100%	5 🕼 Sat 11:14	. <u>२</u> ≔
	Open	жо		📕 Loopbac	k: lo0 (ud	p port 177	'54)					
	Open Recent	▶	-			Ð Ð		11				
	Merge			∠ _			9	11				
Apply a display filt	Import from Hex Dump.									Expression +	Leave Associa	tion Announce
No. Time	Close	жw	Proto	col	Length D	Destination		Info				
9667 22:54:13.2	Sava	900	IEEE	802.15.4	69			Ack				
9668 22:54:13.4	Save Save Ac	#3 A990	IEEE ZigB	802.15.4	74 (92	Øxffff		Beacon Request Beacon, Src: 0x0	1000. EPTD: 00:00:0	0 09:87:65:43:21		
9670 22:54:13.5	Save AS	1	ZigB	e	92			Beacon, Src: 0x1	457, EPID: df:2e:e	e:27:24:1f:03:3a		
9671 22:54:13.6	File Set	•	ZigB	e 000 15 4	111 (3×0000		Rejoin Request,	Device: 0x48f5			
9673 22:54:13.8	E 10 10 10 1		ZigB	ee	111 (ðxffff		Command, Dst: Br	oadcast, Src: 0x14	57		
9674 22:54:13.9	Export Specified Packe	ts	IEEE	802.15.4	76 6	0000x8		Data Request				
9675 22:54:13.9	Export Packet Dissectio	ons 🕨	IEEE ZiaB	802.15.4	69 121 (ax48f5		Ack Reigin Response.	New Address: 0x48	f5		
9677 22:54:13.9	Export Packet Bytes	ፕቋጀ	IEEE	802.15.4	69			Ack				
9678 22:54:14.2	Export SSL Session Ko	10	IEEE	802.15.4	76 6	3×0000		Data Request				
9680 22:54:14.4	Export Objects	·S	IEEE	802.15.4	76 6	0000×8		Data Request				
9681 22:54:14.4	Export Objects	•	IEEE	802.15.4	69			Ack				
9682 22:54:14.7	Print	ЖР	ZiaB	802.15.4	74 t 92	ØXTTTT		Beacon Request Beacon, Src: 0x0	0000. EPID: 00:00:0	0 09:87:65:43:21		
9684 22:54:14.8	1 0x1457	N/A	ZigB	e	92			Beacon, Src: 0x1	457, EPID: df:2e:e	e:27:24:1f:03:3a		
9685 22:54:14.8	08 0x48f5	0×0000	ZigB	ee	111 6	3×0000		Rejoin Request,	Device: 0x48f5			
9687 22:54:15.2	53 0x48f5	0×0000	IEEE	802.15.4	76 (0×0000		Data Request				
9688 22:54:15.2	53 N/A	N/A	IEEE	802.15.4	69			Ack				
9689 22:54:15.2 ► Frame 9665: 69 byt	es on wire (552 bits), 69 bv1	0X48T5 tes_captured (55)	Zigs 2 bits) on interfa	e 0	121 (8X48T5		Rejoin Response,	New Address: 0X48	175		
Null/Loopback			,									
Internet Protocol	Version 4, Src: 127.0.0.1, Ds	st: 127.0.0.1										
 ZigBee Encapsulati 	on Protocol, Channel: 11, Ler	ngth: 5										
▼ IEEE 802.15.4 Ack,	Sequence Number: 25											
▼ Frame Control F	<pre>ield: 0x0002, Frame Type: Ac 010 = Frame Type: Ack (0</pre>	k, Destination A	ddressing Mode: No	ne, Frame Versi	on: IEEE S	td 802.15.4	1-2003,	Source Addressin	ig Mode: None			
	0 = Security Enabled:	False										
	.0 = Frame Pending: Fal	.se										
) = PAN ID Compression	: False										
0000 02 00 00 00 45	0 00 41 28 2a 00 00 40 11 0		(*··@···									
0010 7f 00 00 01 7f	00 00 01 45 5a 45 5a 00 2d f	e 40	EZEZ – @									
0030 d0 00 00 26 85	0 00 00 00 00 00 00 00 00 00 00	0 05										
0040 02 00 19 00 00												
🔵 🏹 wireshark_lo	0_20181018211400_Znw1Cs.pcap	png		_	_	_	_	Pack	ets: 11975 · Displaye	d: 11975 (100.0%) · N	Marked: 32 (0.3%)	Profile: Default

The Export dialog provides an option to select the packet range to be exported - to export just the required packets, select the *Marked packets only* option -:

		【 Wireshark · E:	kport Specified I	Packets		
Look in:	/Users			\$		2
Computer	Name		Size	Kind	Date Modified	V
	🏫 chris			Folder	14/10/28 10:7	12
Chins	Shared			Folder	19/01/28 19:	58
	Guest			Folder	23/07/27 11:.	27
						Save
File name:						Cancel
Export as: Wire	shark/tondumn/	- 0020				
	sindi k/topdump/	- pcap			`	Help
Packet Range				Comp	ress with gzip	
		Captured	 Displayed 			
All packets		11975	11975			
Selected participation	ckets only	1	1			
 Marked pac 	kets only	32	32			
First to last	marked	32	32			
Range:		0	0			
Remove ign	ored packets	0	0			

Note that in order to export the specified packets, live capture must be stopped.