Wireless M-Bus Analyzer

User Guide Version 1.0

Document ID: 4100/40140/0070

IMST GmbH

Carl-Friedrich-Gauß-Str. 2-4 47475 KAMP-LINTFORT GERMANY





Document Information

File name	WMBus_Analyzer_UserGuide_V1_0.docx
Created	2013-06-10
Total pages	27

Revision History

Version	Note
0.1	Created, Initial Version
0.2	Draft Version Created For Review
0.3	Preliminary Version
0.4	New chapters added
1.0	Update to features of version 1.5.0 - Support for hysical Layer C-Mode - Link Layer Frame Format B - Extended Link Leyer Decoding - Encryption Mode 9 (AES-128 GCM + GMAC) - Decrypted Packet Export - Integrated Software Update via HTTPs - Customer specific Feature Extensions

Aim of this Document

This document describes the Wireless M-Bus Analyzer, a Windows application which can be used in combination with the PA-iM871A radio module for capturing and analyzing of wireless M-Bus messages.





Table of Contents

1.		4
	1.1 Overview	4
	1.2 Installation	4
	1.2.1 USB Driver	4
	1.2.2 Installer	4
	1.2.3 Finish Installation	5
2.	GETTING STARTED	6
	2.1 Connected PA-iM871A radio modules	6
	2.2 Capturing wireless M-Bus Messages	7
	2.3 Stop Capture Session	9
	2.4 Load File	10
3.	Data Views	11
	3.1 Table View	11
	3.2 Message View	13
	3.3 Message Tree View & Memory View	14
	3.3.1 Packet Info	14
	3.3.2 Wireless M-Bus Message Blocks	14
	3.3.3 Wireless M-Bus Message Fields	15
	3.4 Traffic Monitor	16
	3.5 AES Key Store	17
	3.6 Settings	18
	3.7 Overview	19
	3.8 Message Filter	19
	3.9 Firmware Update	20
	3.10 Software Update	21
	3.11 Customer specific Feature Extensions	22
4.	APPENDIX	23
	4.1 List of Abbreviations	23
	4.2 List of Figures	23
5.	Regulatory Compliance Information	25





6.	Important Notice	26
	6.1 Disclaimer	26
	6.2 Contact Information	26





1. Introduction

1.1 Overview

The Wireless M-Bus Analyzer is a Windows application which can be used for capturing and analyzing of wireless M-Bus messages. The application uses the PA-871A radio module for message capturing. The Windows GUI offers a comfortable and easy way to configure the connected radio modules and to analyze the captured WM-Bus messages.

1.2 Installation

The Wireless M-Bus Analyzer is shipped with one or two PA-871A radio modules which can be connected to the USB ports of a Host PC. For communication over this USB interface a Virtual COM port (VCP) driver must be installed on the Host PC.

1.2.1 USB Driver

The latest USB/VCP driver can be downloaded from

http://www.silabs.com/products/mcu/pages/usbtouartbridgevcpdrivers.aspx.



Figure 1-1: USB Driver Installation

To verify that the USB driver installation was successful, open the Windows Device Manager ("Start>Control>Panel>System>Hardware>Device Manager" or hit <WIN> + <PAUSE>). A new USB – Serial Port (Silicon Labs CP210x USB to UART Bridge COMxx) entry in section "Ports (COM & LPT)" should appear (see Figure 1-1).

1.2.2 Installer

The Wireless M-Bus Analyzer is based on Qt, a cross-platform application and UI framework, compiled with MinGW and delivered as a zip file. The zip file contains a simple installer program (setup.exe) which guides through the installation procedure.

Note: It might be necessary to install the <u>Microsoft Visual C++ 2008 Redistributable</u> <u>Package (x86)</u> in case the application doesn't start. Click the download button on the Microsoft web page. Double click the vcredist_x86.exe to install runtime components of Visual C++ libraries on a computer that does not have Visual C++ installed.





1.2.3 Finish Installation

Connect one or two PA-iM871A radio modules to your PC. Start WMBus_Analyzer.exe and continue with the following chapter.





2. Getting Started

The Wireless M-Bus Analyzer can be used to capture and analyze wireless M-Bus messages. Capturing of new messages requires at least one connected PA-iM871A radio module.

2.1 Connected PA-iM871A radio modules

The Wireless M-Bus Analyzer provides an automatic PA-iM871A discovery procedure. A new connected radio and its associated serial com port will be displayed in the *Radios* box after successful identification. The tool can operate with a single radio or with two PA-iM871A modules in parallel (Dual Radio Mode).



Figure 2-1: Single Radio Mode, (connected PA-iM871A at COM 87)



Figure 2-2: Dual Radio Mode (connected PA-iM871A at COM 85 + 87)





2.2 Capturing wireless M-Bus Messages

Select **New File** from the main menu or toolbar to start a new capture session. The following dialog will appear which allows selecting the desired Wireless M-Bus Link Mode.

The following **selectable** Link Modes are supported:

- S-Mode
- T-Mode
- R-Mode
- C-Mode

Note: Meter and Other stations which are using the T-/R-/C- Mode are transmitting with different physical link parameters. Due to this it is possible to monitor both link directions with two connected PA-iM871A modules in parallel.

Kireless M-Bus Analyzer			?
New File			
Select a Radio Link Mode for second Radio for monitoring	message capturir of both link direc	ng.The T-Mode, R-Mo tions in parallel !	ode and C-Mode require a
S-Mode	T-Mode	R-Mode	C-Mode
	Radio 1	Ra	dio 2
Status :	connected	COL	nnected
Link Mode :	T-Mode	T-1	1ode
Link Direction :	Meter -> Other	Ot	her -> Meter
Link Frequency :	868.95 MHz	86	8.3 MHz
Coding :	Three-Out-Of-S	ix Ma	nchester
Chiprate :	100000 cps	32	768 cps
Bitrate :	66666 bps	16	384 bps
			Ok Cancel

Figure 2-3: Select Link Mode (Dual Radio Mode Configuration for T-Mode)



Finally a standard file save dialog will open to select a new file for storage purpose.



Figure 2-4: File Save Dialog

The tool proposes a new filename including the current date and time information.

Press Save to enable the radios and to start the capturing process.

a	Wireles	s M-Bus	Analyze	r - C:/Users/Kai_w/Do	ocu						
	File Extr	ras Viev	ws He	elp							
	=	Close	e File	Message View							
	Radios										
	₄ Radio	1									
	Port		COM	189							
	Туре		PA-il	M871A							
	Devi	ce ID	4189								
	Versi	ion	1.4								
	Date		06.10	.2015							
	Link	Mode	T-M	ode							
	Dire	ction	Mete	Meter -> Other							
	Freq	uency	868.9	5 MHz							
	Cod	ing	Thre	Three-Out-Of-Six							
	Chip	orate	1000	100000 cps							
	Bitra	te	0000	b bps							
		2	CON	11.22							
	Tune			11.5Z							
	Devi	e ID	21/1	VIOTA							
	Versi	ion	1.4								
	Date	2	06.10	.2015							
	Link	Mode	T-M	ode							
	Dire	ction	Othe	r -> Meter							
	Freq	uency	868.3	MHz							
	Cod	ing	Man	chester							
	Chip	orate	3276	8 cps							
	Bitra	ite	1638	4 bps							



The new radio configuration will be updated in the radio box on the left side immediately.





2.3 Stop Capture Session

Choose *Close File* from the main menu or toolbar to finish a capture session. The stored file can be opened later again for detailed message analysis.





2.4 Load File

Choose **Open File** or a filename from the recent file list to load an already stored capture session.

候 Wireless M-Bus Ana	lyzer	? ×
Load Fil	e	
File successfully lo	aded.	
Packets: 47 Stations: 7		
		100%
		Close

Figure 2-6: Load File Dialog

A further dialog will display the load progress and amount of captured wireless M-Bus packets and stations.





3. Data Views

This chapter describes the available data views which are provided for further analysis:

- Table View
- Message View
- Message Tree View
- Message Memory View
- Traffic Monitor

3.1 Table View

The Table View displays the captured messages in a standard table format. Each line contains a single message and additional information which is generated by the tool itself (e.g.: Date, Time). The message content is displayed in hexadecimal byte format and if a message is encrypted it is stored and displayed in encrypted format. The format of the message content and the table columns itself can be configured in the **Settings** dialog.

Wireless M-Bus J File Extras View	🥷 Wireless M-Bus Analyzer - Cu/Users/Kai_w/Desktop/Projektu/Ester/wmbus_07022014_083402 Dauerlaufraum Wireless Ventil schliessen.log													
≡ New	File Message View	Table View	Traffic Mor	AES Key Sto	ore Set	tings Fim	nware Updat	te D	iscover Radio	os				=
		Packet	Date	Time	RSSI	Station	Mode	Format	Status	Air Time	Length	WM-Bus Message		
		1	07.02.2014	08:56:14.974	-79.2	Meter (P)	T	A	Ok	0.012320 s	98	55 44 93 15 82 81 88 30 40 03 5F 81 7A 5C 00 40 AF B2 3D	Overview	
 Radio 1 		2	07.02.2014	08:58:33.383	-66.9	Meter (P)				0.012320 s		55 44 93 15 84 81 88 30 40 03 A0 7B 7A 5C 00 40 AF 93 8C :	Manufacturers	
Port	COM89	3	07.02.2014	08:59:47.954	-72.8	Meter (P)	T	A	Ok	0.012320 5	98	55 44 93 15 80 81 88 30 40 03 E1 F4 7A 5C 00 40 AF F0 6D	Stations	
Device ID	4189	4	07.02.2014	09:01:05.772		Meter (P)				0.009200 s		3D 44 93 15 21 78 00 31 40 03 86 F4 7A 57 00 00 A0 0D 78	Total Packets	
Version	1.4	5	07.02.2014	09:02:38.814	-58.4	Meter (P)	T	Α	Ok	0.009200 s	72	3D 44 93 15 22 78 00 31 40 03 F9 09 7A 4D 00 00 A0 0D 78	Good Packets	
Date Link Mode	06.10.2015 Disabled	6	07.02.2014	09:03:03.401		Meter (P)				0.012320 s	98	55 44 93 15 79 81 88 30 40 03 E4 40 7A 5C 00 40 AF C0 88	CRC Errors	U 09:56:14 07 02 2014
A Radio 2		7	07.02.2014	09:04:29.455	-81.3	Meter (P)	T	Α	Ok	0.012320 s	98	55 44 93 15 78 81 88 30 40 03 25 C8 7A 5D 00 40 AF 36 93	Capture End	15:04:30 07.02.2014
Port	COM132	8	07.02.2014	09:56:53.187	-83.5	Meter (P)				0.012320 s		55 44 93 15 78 81 88 30 40 03 25 C8 7A 5E 00 40 AF 5F 77	Capture Time	
Device ID	3141	9	07.02.2014	09:58:32.708	-73.9	Meter (P)	т	A	Ok	0.012320 s	98	55 44 93 15 80 81 88 30 40 03 E1 F4 7A 5D 00 40 AF 6E FA	Total Air Time	
Version	1.4	10	07.02.2014	09:59:10.085	-68.5	Meter (P)				0.012320 s		55 44 93 15 84 81 88 30 40 03 A0 7B 7A 5D 00 40 AF 84 36 ;	Media Utilization	
Date Link Mode	06.10.2015 Disabled	11	07.02.2014	10:00:26.520	-57.3	Meter (P)	т	A	Ok	0.009200 s	72	3D 44 93 15 22 78 00 31 40 03 F9 09 7A 4E 00 00 A0 0D 78		
						Meter (P)						55 44 93 15 82 81 88 30 40 03 5F 81 7A 5D 00 40 AF 27 64	Source Address (L	
		13	07.02.2014	10:02:21.518	-57.3	Meter (P)	T	A	Ok	0.009200 s	72	3D 44 93 15 21 78 00 31 40 03 86 F4 7A 58 00 00 A0 0D 78	C-Field	44
		14	07.02.2014	10:03:10.131		Meter (P)						55 44 93 15 79 81 88 30 40 03 E4 40 7A 5D 00 40 AF CD F5	Man ID	B3-25
		15	07.02.2014	10:56:20.949	-72.3	Meter (P)	Т	A	Ok	0.012320 s	98	55 44 93 15 79 81 88 30 40 03 E4 40 7A 5E 00 40 AF AC 3C 2	Device ID	12-34-56-78
		16	07.02.2014	10:57:35.899	-69.1	Meter (P)				0.012320 s		55 44 93 15 84 81 88 30 40 03 A0 7B 7A 5E 00 40 AF 2C 7A	Version	
		17	07.02.2014	11:02:04.969	-79.2	Meter (P)	т	Α	Ok	0.012320 s	98	55 44 93 15 78 81 88 30 40 03 25 C8 7A 5F 00 40 AF E7 C6	🔲 Туре	
		18	07.02.2014	11:02:22.381		Meter (P)				0.009200 s		3D 44 93 15 22 78 00 31 40 03 F9 09 7A 4F 00 00 A0 0D 78	CI-Field	
		19	07.02.2014	11:03:06.515	-73.3	Meter (P)	т	A	Ok	0.012320 s	98	55 44 93 15 80 81 88 30 40 03 E1 F4 7A 5E 00 40 AF 2E 9B		
		20				Meter (P)						3D 44 93 15 21 78 00 31 40 03 86 F4 7A 59 00 00 A0 0D 78	Source Address (L	
		21	07.02.2014	11:59:00.682	-73.3	Meter (P)	т	A	Ok	0.012320 5	98	55 44 93 15 80 81 88 30 40 03 E1 F4 7A 5F 00 40 AF E5 50	C-Field	44
		22	07.02.2014	12:02:05.014		Meter (P)						55 44 93 15 84 81 88 30 40 03 A0 7B 7A 5F 00 40 AF 10 8A	Man ID	
		23	07.02.2014	12:03:29.085	-74.4	Meter (P)	т	A	Ok	0.012320 5	98	55 44 93 15 79 81 88 30 40 03 E4 40 7A 5F 00 40 AF 1D 02 :	Device ID	12-34-56-78
		24	07.02.2014	12:04:07.085	-80.8	Meter (P)	Т		Ok	0.012320 s	98	55 44 93 15 78 81 88 30 40 03 25 C8 7A 60 00 40 AF 5D 27	Version	
		25	07.02.2014	12:06:50.453	-56.8	Meter (P)	т	Α	Ok	0.009200 s	72	3D 44 93 15 22 78 00 31 40 03 F9 09 7A 50 00 00 A0 0D 78	🔲 Туре	
		26	07.02.2014	12:07:21.461		Meter (P)				0.009200 s		3D 44 93 15 21 78 00 31 40 03 86 F4 7A 5A 00 00 A0 0D 78	CI-Field	
		27	07.02.2014	12:56:05.914	-68.0	Meter (P)	т	A	Ok	0.012320 s	98	55 44 93 15 84 81 88 30 40 03 A0 7B 7A 60 00 40 AF B6 CF		
		28	07.02.2014	12:56:09.534		Meter (P)						55 44 93 15 80 81 88 30 40 03 E1 F4 7A 60 00 40 AF 25 C8		
		29	07.02.2014	12:57:21.985	-82.4	Meter (P)	т	A	Ok	0.012320 s	98	55 44 93 15 78 81 88 30 40 03 25 C8 7A 61 00 40 AF C9 7F		
			07.02.2014	12:58:55.026		Meter (P)						55 44 93 15 79 81 88 30 40 03 E4 40 7A 60 00 40 AF D4 5F 2		
		31	07.02.2014	13:00:32.367	-57.3	Meter (P)	т	A	Ok	0.009200 5	72	3D 44 93 15 22 78 00 31 40 03 F9 09 7A 51 00 00 A0 0D 78		
		32	07.02.2014	13:00:52.337	-55.2	Meter (P)	T	Α	Ok	0.009200 s	72	3D 44 93 15 21 78 00 31 40 03 86 F4 7A 5B 00 00 A0 0D 78		
		33	07.02.2014	13:03:24.599	-80.3	Meter (P)	T	Α	Ok	0.012320 s	98	55 44 93 15 82 81 88 30 40 03 5F 81 7A 60 00 40 AF D0 9A 2		
		34	07.02.2014	13:55:36.462		Meter (P)	T		Ok	0.012320 s		55 44 93 15 80 81 88 30 40 03 E1 F4 7A 61 00 40 AF 27 E9		
		35	07.02.2014	13:56:30.885	-79.2	Meter (P)	T	A	Ok	0.012320 s	98	55 44 93 15 79 81 88 30 40 03 E4 40 7A 61 00 40 AF CD 60 2		
		36	07.02.2014	13:57:10.875	-80.8	Meter (P)	T	A	Ok	0.012320 s	98	55 44 93 15 78 81 88 30 40 03 25 C8 7A 62 00 40 AF 65 42		
		37	07.02.2014	13:59:03.816	-68.5	Meter (P)	Т	A	Ok	0.012320 s	98	55 44 93 15 84 81 88 30 40 03 A0 7B 7A 61 00 40 AF D3 06		
		38	07.02.2014	14:02:24.500	-80.3	Meter (P)	T	A	Ok	0.012320 s	98	55 44 93 15 82 81 88 30 40 03 5F 81 7A 61 00 40 AF 95 2A (
	powered by	39	07.02.2014	14:02:49.210	-55.2	Meter (P)	т	A	Ok	0.009200 5	72	3D 44 93 15 21 78 00 31 40 03 86 F4 7A 5C 00 00 A0 0D 78		
www.wir	eless-solutions.de		A100 00 0014	34.05.02.040		M	- 7			0.000000 -	- 0.0			

Figure 3-1: Table View

The Table View provides the following columns:

- Packet
- a unique packet/message number
- Date
- the capture date from the PC
- Time

•

- the capture time from the PC
- Port the associated COM port / radio module





•	RTC	- a timestamp from the radio modules internal real time clock
•	RSSI	- an estimated RSSI value in dBm
•	Station	 the station type of the message sender (Meter, Other, P = Primary, S = Secondary)
•	Mode	- the configured link mode: S, T, R, C
•	Format	- the received message format: A or B
•	Status	- the packet status: OK, CRC Error
•	Air Time	- the packet air time (long packet preambles not included)
•	Length	- the gross packet length, including CRC Fields and Length-Field
•	WM-Bus Message	 the received wireless M-Bus message data as hexadecimal octet stream starting with original L-Field

Note: A received radio message with CRC Error will be marked red.

Selecting a single message allows a more detailed analysis of the message content in the Message Tree & Memory View (see next chapters).





3.2 Message View

The Message View displays the captured messages in a more detailed way. Each message is displayed as a row of several boxes which contain the individual header fields, data blocks and CRC Fields.

Note: A corrupted header block or data block with wrong CRC value is marked with a following red colored CRC Field.



Figure 3-2: Message View

As in the Table View, the message content can be displayed in several ways:

- Simple octet sequence
- Link Layer Header + Blocks and CRCs
- Link Layer Header + higher Layer Protocol Segments

Furthermore it is possible to select a single message for detailed analysis of its content. The selected message will be displayed in the Message Tree & Memory View (see next chapters).





3.3 Message Tree View & Memory View

The Message Tree View and Memory View display a single selected message in more detail.

File Extras Vie	ws Help																		
≡ New	File Message View	Table Viev	w Traffic	Monitor	AES Key	Store Se	ettings	Firmwa	are Updat	e Dis	cover Radios								=
Radios		No.	RSSI	Station	Mode	Status	Length	L	С	Man ID	Device ID	Version	Type	CRC	Block 0	CRC	Block 🔶		
Raulus		1	-10.4 dBm	Other (P)	с	Ok	61	34	43	AE OC	78 56 34 12	01	00	D0 6F	6D 44 22 75 92 24 23 29 07 7D 00 20 C5 34 7D 88	FC SC	03 60 AD 1C 42 42 D3 4A 1/		
 Radio 1 		No.	RSSI	Station	Mode	Status	Length	L	С	Man ID	Device ID	Version	Туре	CRC	Block 0	CRC	Block	Manufacturers	
Port Type	PA-iM871A	2	-10.4 dBm	Other (P)	c	Ok	61	34	43	AE OC	78 56 34 12	01	. 00	D0 6F	6D 44 22 75 92 24 23 29 07 7D 00 20 C5 34 7D 88	FC SC	03 60 AD 1C 42 42 D3 4A 1/	Stations	
Device ID	4189	No.	RSSI	Station	Mode	Status	Length		C	Man ID	Device ID	Version	Type	CRC	Block 0	CRC	Block	Total Packets	
Version	1.4	3	-10.4 dBm	Other (P)	с	Ok	61	34	43	AE OC	78 56 34 12	01	00	D0 6F	6D 44 22 75 92 24 23 29 07 7D 00 20 C5 34 7D 88	FC 5C	03 60 AD 1C 42 42 D3 4A 1/	GOOD Packets	
Link Mode	Disabled	No	RSST	Station	Mode	Status	Length	Ē		Map ID	Device ID	Version	Type	CRC	Block 0	CRC	Block	Capture Start	13:19:08 31.08.2015
✓ Radio 2		4	-10.9 dBm	Other (P)	c	Ok	61	34	43	AE OC	78 56 34 12	01	00	D0 6F	6D 44 22 75 92 24 23 29 07 7D 00 20 C5 34 7D 88	FC SC	03 60 AD 1C 42 42 D3 4A 1/	Capture End	
Type	PA-iM871A		Deet	Challen		Chabas	1 and 1			Mars 10	Davies 1D				Plate a	-	Diada (Capture Time	
Device ID		NO.	-10.4 dBm	Other (P)	Mode	Ok	64	37	53	00.01	00.01.02.03	50	02	08.56	BIOLK U BIC 84 AA 58 89 67 45 23 84 38 50 03 00 00 20 05	R0 13	86 8D AD 82 48 99 FE A7 61	Total Air Time	
Version	1.4		201 1 0011	Outer (r)													CO CO NO DE NO DOTE NO D	Media Utilization	
Link Mode	Disabled	No.	RSSI	Station	Mode	Status	Length	L		Man ID	Device ID	Version	Type		Block 0		Block :		
		6	-10.4 d8m	Other (P)	C C	Ok	64	37	53	00 01	00 01 02 03	50	02	98 56	8C 84 AA 58 89 67 45 23 84 38 50 03 00 00 21 25	53 50	EE 01 DF 23 D1 87 59 85 0A		
		No.	RSSI	Station	Mode	Status	Length	L	С	Man ID	Device ID	Version	Type	CRC	Block 0	CRC	Block :	C-Field	
		7	-10.4 dBm	Other (P)	С	Ok	64	37	53	00 01	00 01 02 03	50	02	98 56	8C 84 AA 5B 89 67 45 23 B4 38 50 03 00 00 21 25	53 50	EE 01 DF 23 D1 87 59 85 0A	III Man ID	
		No.	RSSI	Station	Mode	Status	Length	L	С	Man ID	Device ID	Version	Туре	CRC	Block 0	CRC	Block 1	Device ID	
			Data	80	C 84 AA 58	3 89 67 45 23 B4	38 50 03 0	0 00 21 25				A 0			97 59 00 01 00 01 02	09 50 1	02.08.56	Version	
			CRC16	53 50 - Ok										C 84 A	A 5B 89 67 45 23 B4 38 50 03 00	00 21 3	25 53 50	🔲 Туре	
		▲ Data Block [1]										0	024 : 1	E 01 E	F 23 D1 87 59 85 0A BE 5F 6E 6E	DB C5 1	97 01 B2	CI-Field	
			CRC66 01 82 -04																
		🔺 Da	ta Block [2]																
			Data CRC16	E	A 81 2D AD	D E0 68 56 D0 FF	8C E5 DB	A5 50										C.F.MI	
		🔺 WM-В	us Message Fiel															Man TD	
		🔺 Lin	k Layer															Device ID	12-34-56-78
			C-Field	PI	37 -> >> bytes PRM:1 FCB:0 FCV:1 SND-UD (Other)												Version		
				G														Type	
			Device ID Verrion	03	3020100													CI-Field	
			Туре	EI	lectricity														
		🔺 Ext	ended Link Lay									E							
			CI-held CC-Field	84 84	xtended Li 4 RFU:0 R-I	nk Layer 1 Field:0 A-Field:1													
		🔺 Tra	nsport Layer			ice (M. Pire)													
			Ident. Nr.	23	3456789	nce (m-bus)													
Man ID NET : Netatmo						19													
			Version Device Type	50	U -> 80 ias														
				00															
			Status Cooffic Wood	00	0														
			AES-Verify	21	F-2F -> De	cryption wode cryption succe	ssful												
		🔺 Ap	plication Layer	M	1-Bus														
	powered by		Record[0]	V V	Wh ariable Len	hoth													
www.win	eless-solutions.de		⊿ VIF	E	nergy Vh														

Figure 3-3: Message Tree & Memory View

The Tree View contains three top level sections which can be expanded to display the more information:

- Packet Info
- WM-Bus Message Blocks
- WM-Bus Message Fields

3.3.1 Packet Info

This section contains general packet information e.g. Date, Time RSSI, Air Time.

3.3.2 Wireless M-Bus Message Blocks

Within this section a single message is displayed according to its wireless M-Bus Link Layer Blocks:

- one single Header Block + CRC Field (16 Bit)
- up-to 16 Data Blocks + individual CRC Fields (16 Bit)

Each block is displayed as a row of data bytes in hexadecimal format and a separate row of CRC bytes. In case of a CRC Error the complete block is displayed in red.

Selecting a single row within a block of the tree structure highlights the corresponding data bytes and CRC bytes in the Memory View on the right side.





3.3.3 Wireless M-Bus Message Fields

Error free messages with correct CRC values are also displayed according to the logical layer structure of the wireless M-Bus specification:

- Link Layer
- Extended Link Layer
- Transport Layer
- Application Layer



Figure 3-4: Wireless M-Bus Message Fields

The Application Layer Fields are only displayed if the message is not encrypted or if it is possible to decrypt the message successfully. The message decryption is triggered automatically when a message is selected. The decryption process looks for a configured AES key in the *AES Key Store* (see next chapter) and decrypts the Application Layer message content according to the signalled and supported decryption algorithm. On successful decryption, the Application Layer Fields will be parsed and the data in the Memory View will be displayed in a decrypted state.





3.4 Traffic Monitor

The Traffic Monitor View allows to inspect the amount of captured radio packets and corresponding traffic in terms of air time and duty cycle per wireless M-Bus node.

File Extres Views Help											
New File Nessage View Table View Traffic Monitor AES	Key Store Setting	s Firmware Update	Discover Radios								=
		Overview								Övervana	
Packet Distribution		Hendeturens : 1 Soziona : 7 Tech Packets : 47 Gele Packets : 47 GRC Brows : 0	c c y me	aeture Start († 155 Gepture End († 154 Gapture Time († 25 tal Ar Time († 0.5 de Utilization († 0.0	614 07.02.2014 139 07.02.2014 85.765 s 35 s 262 %					Manufacturers Stations Total Pickels Geod Packets ORC Errors Capture Start Capture Start Capture Time Total Ar Time Meda Utikation Source Address C Frield Han ID E Dence ID E Venson Type C Frield	1 7 47 47 47 47 47 47 47 47 47 59423 47542304 42080578 8 6.0325 8 6.0325 8 6.0325 4 44 49 49 2285578 9 6.032 4 12335678 12335678 12335678 12335678 1235578 1235778 1235778 1235778 123578 12357778 123577778 1235777777777777777777777777777777777777
Andrew B 15 De B 20 De D 10 Teacher B 20 De D 10 De	Manufacturer Device Vession Frame Type	Heat ID Device ID 33 10 24 21 85 35 33 34 24 21 85 35 33 34 24 21 86 35 33 34 24 71 00 11 33 35 22 78 00 31 33 35 22 78 00 31 34 35 22 78 00 31 35 36 35 76 81 68 30 31 37 61 68 30 30 31 76 61 68 30	Variation Type 40 03 40 03 40 03 41 03 42 03 44 03 46 03 46 03 46 03 46 03 47 03 48 03 49 03	Bobbts 5 / 9 7 7 9 7 7 0 7 7 10 7 7 7 10 7 7 7 10 7 7 7 10 7 7 10 7 7 7 10 7 7 10 7 7 7 10 7 7 10 7 7 7 10 7 7 7 10 7 7 7 10 7 7 7 17 10 7 7 10 7 7 10 7 7 10 7 7 10 7 7 10 7 7 10 7 7 10 7 7 10 7 7 10 7 7 10 7 7 10 7 7 10 7 10 7 10 10 10 10 <th10< th=""> <th10< th=""> <th10< th=""></th10<></th10<></th10<>	Duration 2203.000 s 2150.000 s 2150.000 s 2150.000 s 2117.000 s 2117.000 s 2117.000 s 2119.000 s	Air Time 0.062 5 0.066 5 0.066 5 0.066 3 0.066 3 0.066 5	awg. DC 0.000 % 0.000 % 0.000 % 0.000 % 0.000 % 0.000 %	DC 1.8. 0.000 % 0.000 % 0.000 % 0.000 % 0.000 %	www.DC.p.H. 0.000 % 0.000 % 0.000 % 0.000 % 0.000 % 0.000 %	Correct Address (Creat) The Dorese 20 Creat 20 Type Creat 20 Type Creat 20 Creat 20 Cr	LU 1987 2 44 1925 1 1234 5678 1 192 192 192 192 192

Figure 3-5: Traffic Monitor View

For every discovered wireless M-Bus node the following information is presented:

- Man ID, Device ID, Version, Type
 - the device identifying bytes from the wireless M-Bus message header
- Packets
 - the number of total packets, error free (good) packets and CRC error packets
- Duration

the time span between the start of the first and last received packet, used for the average duty cycle calculation

- Air Time the cumulated air time of all captured packets per node
- Average Duty Cycle (avg. DC) the average duty cycle based on the cumulated air time and measurement duration
- Duty Cycle last Hour the duty cycle based on all captured packets within the last hour
- Max. Duty Cycle per Hour the max. duty cycle observed in a time span of one hour

Notes:

- The air time calculation does not include the long preambles which are use for nodes which operate in Link Mode S1.
- The packet arrival time stamp is derived from the Host PCs clock and may jitter according to other application (processes) which run in parallel to this program.





3.5 AES Key Store

The AES Key Store dialog can be used to configure several AES Keys for decryption purpose. According to the wireless M-Bus specification the Application Layer message content might be encrypted.

Important Note: all captured messages are stored in encrypted format! The decryption is only triggered if a message is selected in one of the provided Message Views.

🌈 Wirele	ess M-Bus An	alyzer	-		-			? **							
	AES Ke	y Store													
			150.0												
Man I	Man ID, Device ID, Version and Type.														
		Man ID	Devic	e ID	Version	Туре	Ad	d Key							
WM-B	us Device	B 3-25	01-0	2-03-04	00	00	Bomo								
128 B	t AES Key	01-02-03-04	05-0	6-07-08	09-0A-0B-0C	OD-0E-0F-10	Kemo	JVE Key							
Key S	itore														
No.	Man ID	Device ID	7ersior	Type	Key 1-4	Кеу 5-8	Key 9-12	Key 13-16							
1	B4-38	89-67-45-23	50	03	00-11-22-33	44-55-66-77	88-99-AA-BB	CC-DD-EE-FF							
2	AE-0C	78-56-34-12	01	00	00-11-22-33	44-55-66-77	88-99-AA-BB	CC-DD-EE-FF							
3	24-23	44-22-75-92	29	07	00-11-22-33	44-55-66-77	88-99-AA-BB	CC-DD-EE-FF							
4	E9-1E	78-56-34-12	50	03	00-11-22-33	44-55-66-77	88-99-AA-BB	CC-DD-EE-FF							
5	B3-25	01-02-03-04	00	00	01-02-03-04	05-06-07-08	09-0A-0B-0C	0D-0E-0F-10							
							Export K	eys Import Keys							
								Close							

Figure 3-6: AES Key Store

For message decryption purpose an AES key is selected according to its wireless M-Bus Device Header Fields: Man ID, Device ID Version and Type.

Important Note: All AES Keys which are visible in the Key Store will be stored in: C:\Users\USERNAME\AppData\Local\IMST\WMBus Analyzer\WMBus Analyzer.ini ¹⁾

¹⁾ USERNAME is a placeholder for your windows user name

Export Keys / Import Keys

The content of the AES Key store can be exported and re-imported on another PC by means of this feature.





3.6 Settings

The Settings dialog provides an easy configuration mean for several options.

Kireless M-Bus Analyzer	2		? x
Settings			
You can change some	e options here.		
Display Options for Me	essage Columns		
Date	Time	Port	
RTC	RSSI	Station	
Mode	Format	V Status	
Air Time	Length		
WM-Bus Message Dist	olav Format		
Simple Octet Sequer	nce		
💿 Detailed Link Layer H	leader + Blocks + CRCs		
Oetailed Link Layer H	leader + Higher Protocol Layer	Segments	
Scrol Behaviour			
Scroll to last line on r	nessage reception		
GUI Theme			
Manhattan			
Montreal			
			Grand
		OK	Cancel

Figure 3-7: Settings

Message Columns

The column layout which is used in the Table View and Message View can be adapted by checking/unchecking the corresponding column title.

WM-Bus Message Display Format

The content of a message can be displayed in three different ways:

- Simple octets sequence
- Detailed Link Layer Header + Blocks with CRCs
- Detailed Link Layer Header + higher Protocol Layer Segments

Scroll Behaviour

The automatic scroll behaviour of Table View and Message View while capturing messages can be enabled / disabled here.





3.7 Overview

The Overview box gives a short overview about the number of captured packets, CRC errors, discovered wireless M-Bus stations and capture session time.

Overview	
Manufacturers	1
Stations	7
Total Packets	47
Good Packets	47
CRC Errors	0
Capture Start	08:56:14 07.02.2014
Capture End	15:04:30 07.02.2014
Capture Time	22095.765 s
Total Air Time	0.535 s
Media Utilization	0.002 %

Figure 3-8: Overview

3.8 Message Filter

The Message Filter box provides an easy mean to reduce the amount of displayed wireless M-Bus messages. Only those messages are displayed, which Link Layer Header Fields (LLA) matches to the configured and enabled (checked) filter settings.

Source Address (LLA) Filter 1		
C-Field	44	
🗹 Man ID	93-15	
🗹 Device ID	80-81-88-30	
Version	40	
🔲 Туре	03	
🔲 CI-Field	7A	

Figure 3-9: Message Filter

Note: A right mouse click on a particular row in the Table View, Message View or Traffic Monitor provides a simple mean to copy the address fields of the selected row directly to the filter box.





3.9 Firmware Update

To enable further feature enhancements of this tool and the required PA-iM871A radio modules a firmware update support is provides. The update dialog verifies the available and currently used version of the radio modules firmware and guides through the update process.

🌈 Wireless M-Bus Analyzer				? <u>×</u>
Firmware Upda	te			
Connected with PA-iM871	A (COM132)			
The Radio Firmware is up-to-	date! Press Continue i	f you still like to	update.	
Available Version: V1.4	(06.10.2015)			
Current Version: V1.4	(06.10.2015)			
				0%
		(Close	Continue

Figure 3-10: Firmware Update





3.10 Software Update

The Analyzer PC application itself can be updated via HTTPs. Select **SoftwareUpdate** from the main menu to query for a new software version.



Figure 3-11: Software Update





3.11 Customer specific Feature Extensions

The new About dialog provides a list of features which are supported or not supported in the installed version.

Kireless M-Bus Analyzer		? ×
About Wireless M-Bus Analyzer		
Version: 1.5.0 (30.10.2015)		
Customer ID: 00-00-00-00-00-00-00		
Supported Features	License	
Feature	Status	
- Physical Laver S/T/R-Mode	supported	
- Physical Layer C-Mode	supported	
- Link Layer Frame Format B	supported	
- Extended Link Layer Decoder	supported	
- Encryption Mode 5 (AES-128 CBC)	supported	
- Encryption Mode 9 (AES-128 GCM + GMAC)	not supported	
- Encryption Mode 15 (Customer specific)	not supported	
- Source Address (LLA) Filtering	supported	
- Traffic Monitor (Packet Statistics)	supported	
 Integrated Software Update over HTTPs 	supported	
- Decrypted Packet Export	supported	
		Close

Figure 3-12: About Dialog – Supported Features





4. Appendix

4.1 List of Abbreviations

- FW Firmware
- GUI Graphical User Interface
- HW Hardware
- RSSI Received Signal Strength Indicator
- RTC Real Time Clock
- SW Software
- UART Universal Asynchronous Receiver/Transmitter

4.2 List of Figures

Figure 1-1: USB Driver Installation	4
Figure 2-1: Single Radio Mode, (connected PA-iM871A at COM 87)	6
Figure 2-2: Dual Radio Mode (connected PA-iM871A at COM 85 + 87)	6
Figure 2-3: Select Link Mode (Dual Radio Mode Configuration for T-Mode)	7
Figure 2-4: File Save Dialog	8
Figure 2-5: File Save Dialog	8
Figure 2-6: Load File Dialog	10
Figure 3-1: Table View	11
Figure 3-2: Message View	13
Figure 3-3: Message Tree & Memory View	14
Figure 3-4: Wireless M-Bus Message Fields	15
Figure 3-5: Traffic Monitor View	16
Figure 3-6: AES Key Store	17
Figure 3-7: Settings	18
Figure 3-8: Overview	19
Figure 3-9: Message Filter	19
Figure 3-10: Firmware Update	20





WiMC





5. Regulatory Compliance Information

The use of radio frequencies is limited by national regulations. The radio module has been designed to comply with the European Union's R&TTE (Radio & Telecommunications Terminal Equipment) directive 1999/5/EC and can be used free of charge within the European Union. Nevertheless, restrictions in terms of maximum allowed RF power or duty cycle may apply.

The radio module has been designed to be embedded into other products (referred as "final products"). According to the R&TTE directive, the declaration of compliance with essential requirements of the R&TTE directive is within the responsibility of the manufacturer of the final product. A declaration of conformity for the radio module is available from IMST GmbH on request.

The applicable regulation requirements are subject to change. IMST GmbH does not take any responsibility for the correctness and accuracy of the aforementioned information. National laws and regulations, as well as their interpretation can vary with the country. In case of uncertainty, it is recommended to contact either IMST's accredited Test Center or to consult the local authorities of the relevant countries.





6. Important Notice

6.1 Disclaimer

IMST GmbH points out that all information in this document is given on an "as is" basis. No guarantee, neither explicit nor implicit is given for the correctness at the time of publication. IMST GmbH reserves all rights to make corrections, modifications, enhancements, and other changes to its products and services at any time and to discontinue any product or service without prior notice. It is recommended for customers to refer to the latest relevant information before placing orders and to verify that such information is current and complete. All products are sold and delivered subject to "General Terms and Conditions" of IMST GmbH, supplied at the time of order acknowledgment.

IMST GmbH assumes no liability for the use of its products and does not grant any licenses for its patent rights or for any other of its intellectual property rights or third-party rights. It is the customer's duty to bear responsibility for compliance of systems or units in which products from IMST GmbH are integrated with applicable legal regulations. Customers should provide adequate design and operating safeguards to minimize the risks associated with customer products and applications. The products are not approved for use in life supporting systems or other systems whose malfunction could result in personal injury to the user. Customers using the products within such applications do so at their own risk.

Any reproduction of information in datasheets of IMST GmbH is permissible only if reproduction is without alteration and is accompanied by all given associated warranties, conditions, limitations, and notices. Any resale of IMST GmbH products or services with statements different from or beyond the parameters stated by IMST GmbH for that product/solution or service is not allowed and voids all express and any implied warranties. The limitations on liability in favor of IMST GmbH shall also affect its employees, executive personnel and bodies in the same way. IMST GmbH is not responsible or liable for any such wrong statements.

Copyright © 2011, IMST GmbH

6.2 Contact Information

IMST GmbH

Carl-Friedrich-Gauss-Str. 2-4 47475 Kamp-Lintfort Germany

T +49 2842 981 0 F +49 2842 981 299 E <u>wimod@imst.de</u> I <u>www.wireless-solutions.de</u>

