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. 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.

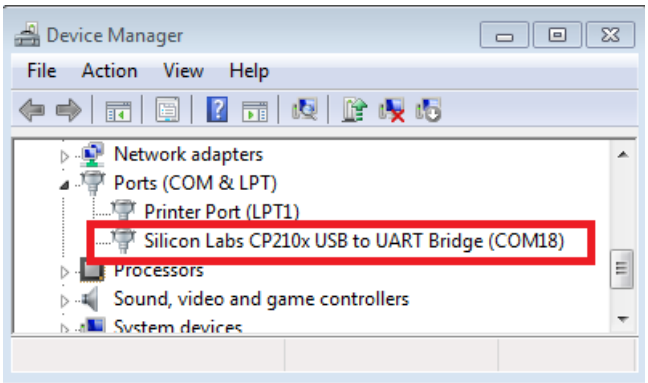

Figure 1-1: USB Driver Installation

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 Microsoft Visual C++ 2008 Redistributable Package (x86) 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).

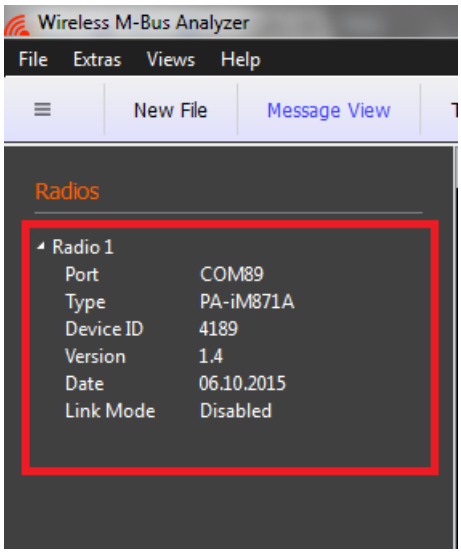

Figure 2-1: Single Radio Mode, (connected PA-iM871A at COM 87)

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.

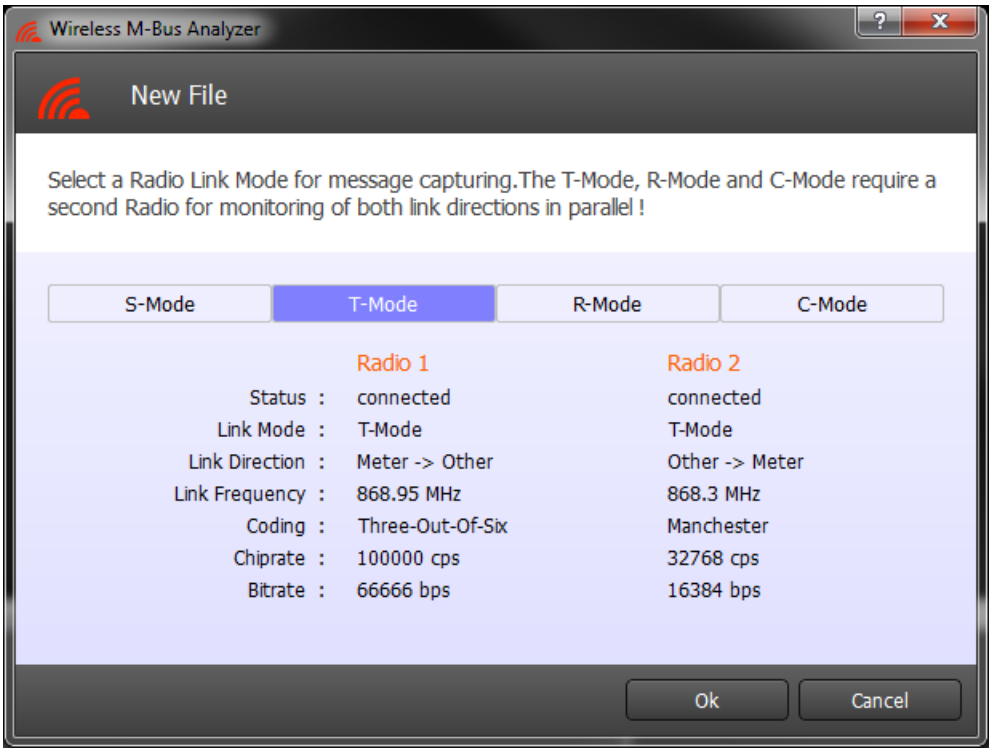

Figure 2-3: Select Link Mode (Dual Radio Mode Configuration for T-Mode)

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

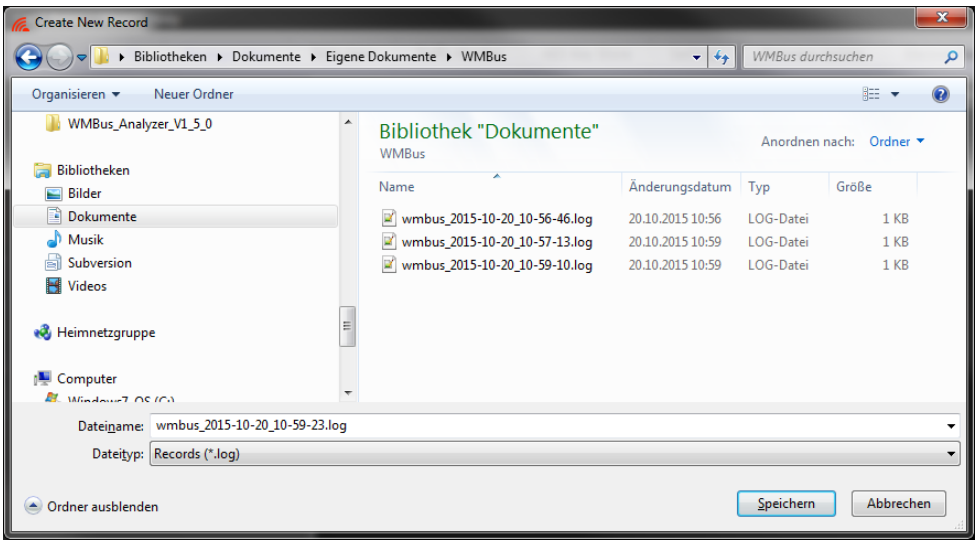

Figure 2-4: File Save Dialog

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.

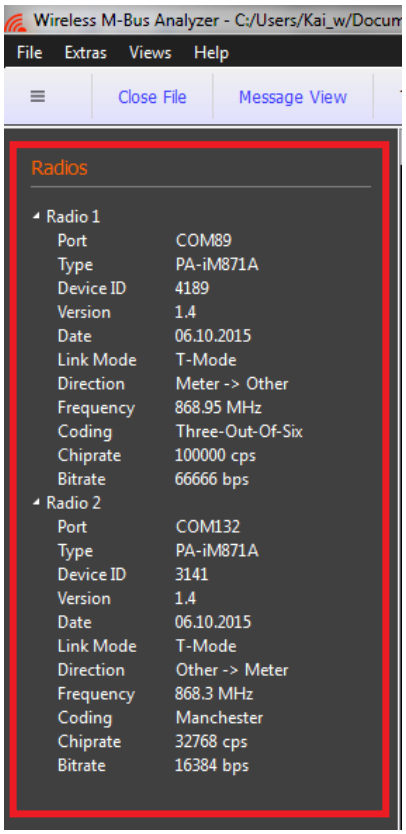

Figure 2-5: File Save Dialog

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.

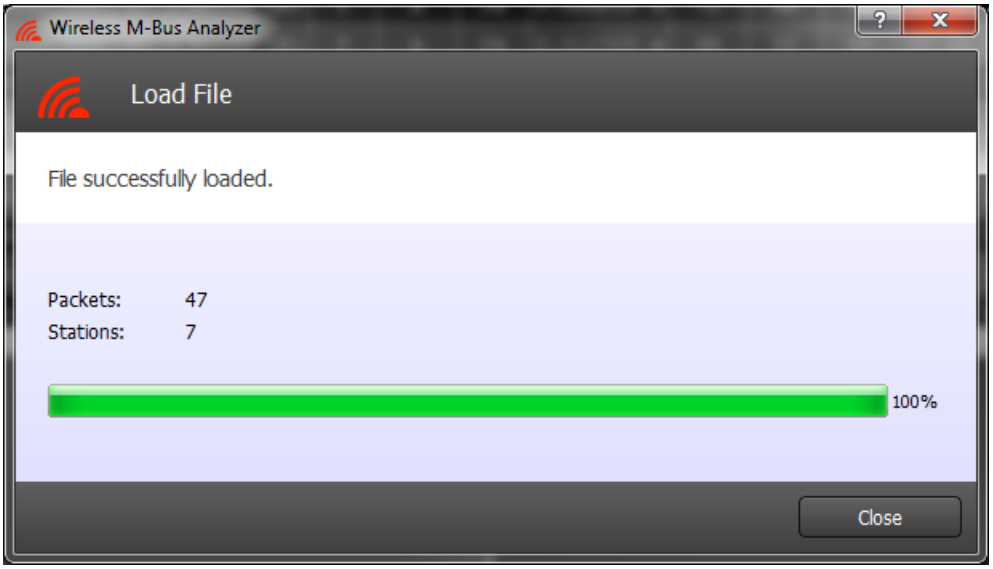

Figure 2-6: Load File Dialog

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.

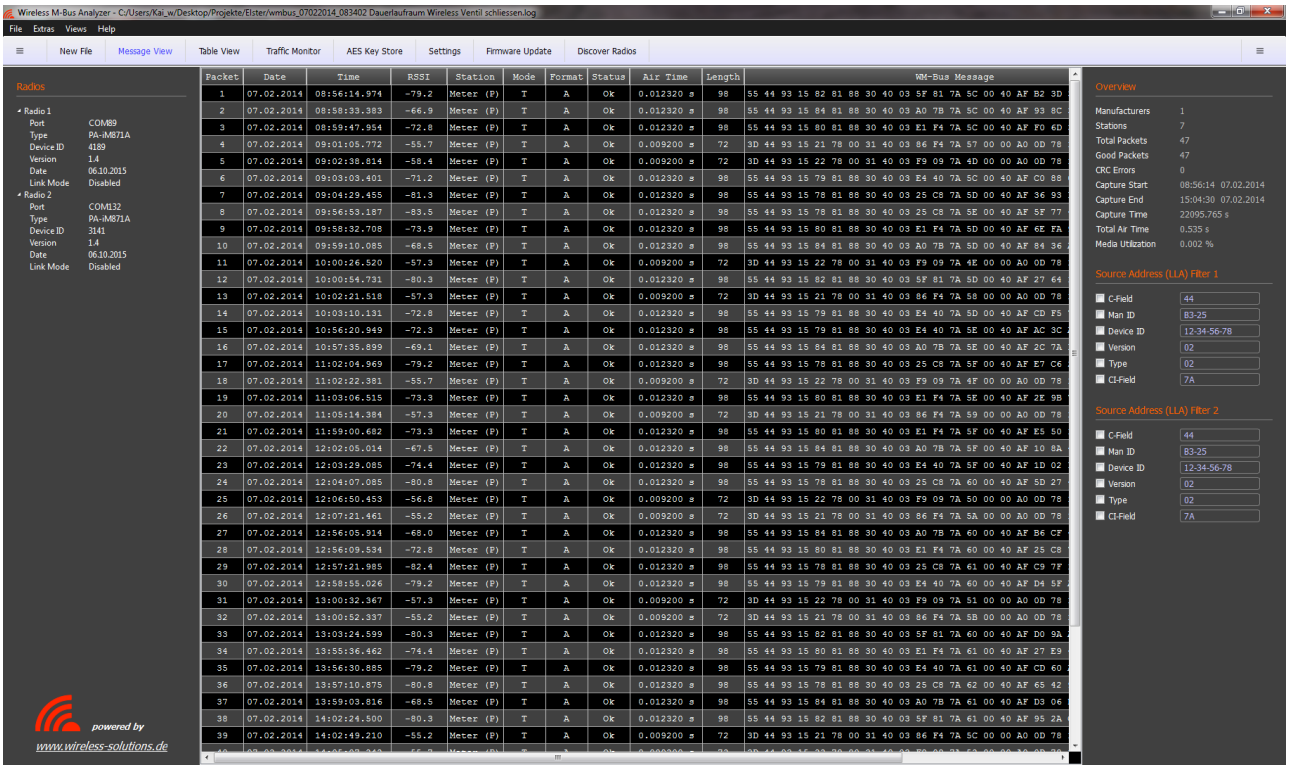

Figure 3-1: Table View

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.

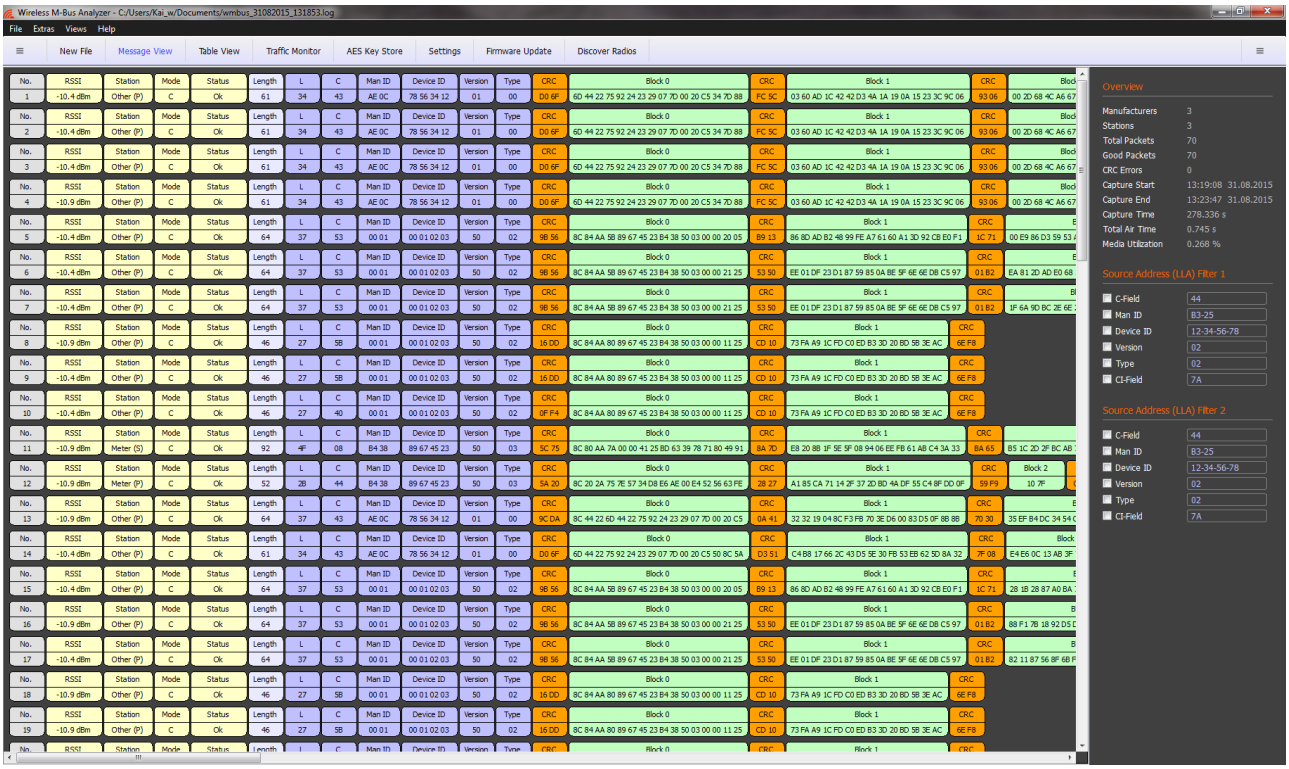

Figure 3-2: Message View

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.

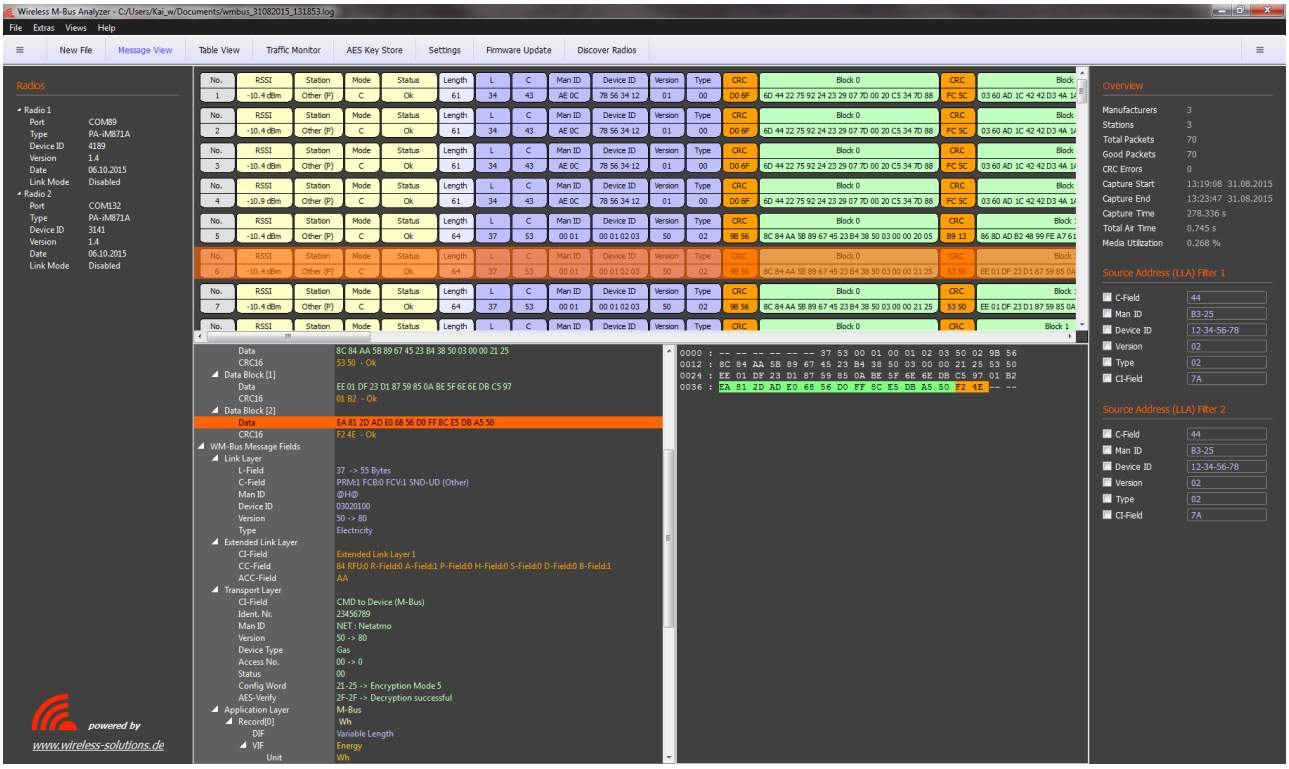

Figure 3-3: Message Tree & Memory View

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

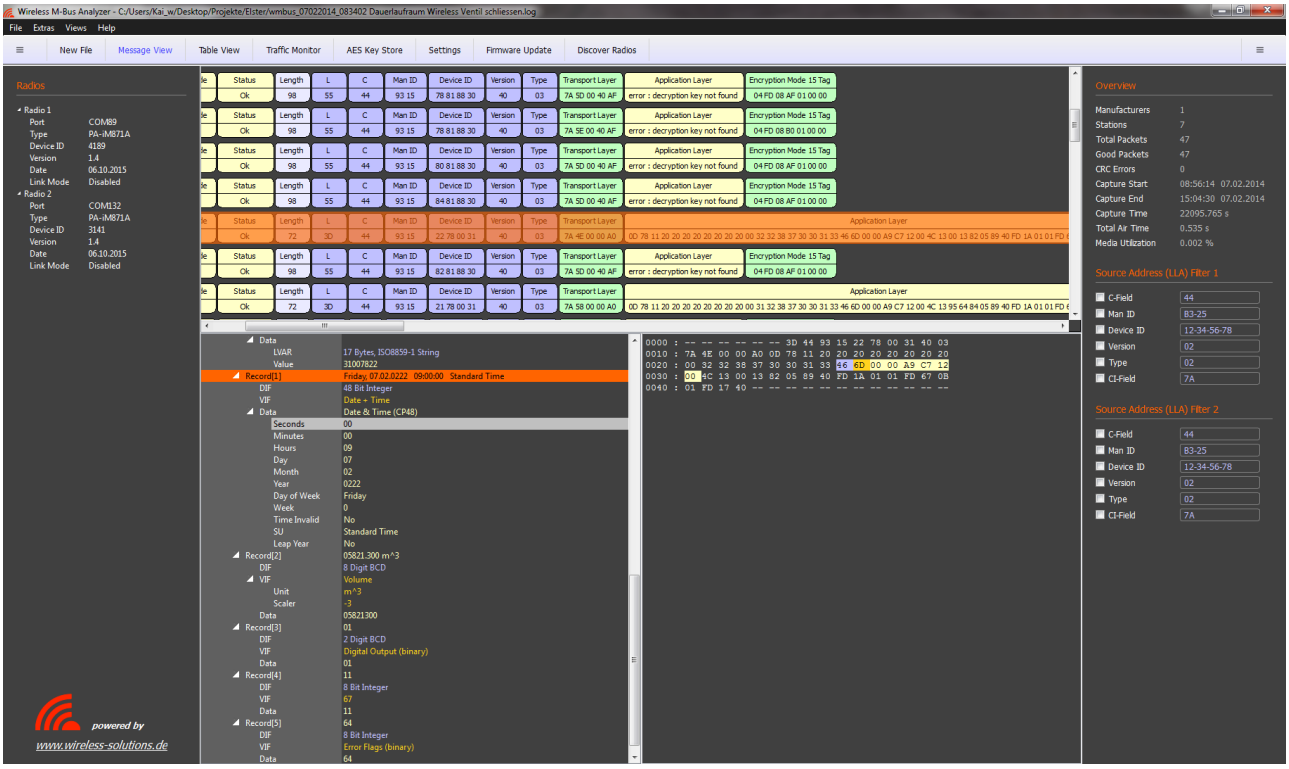

Figure 3-4: Wireless M-Bus Message Fields

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.

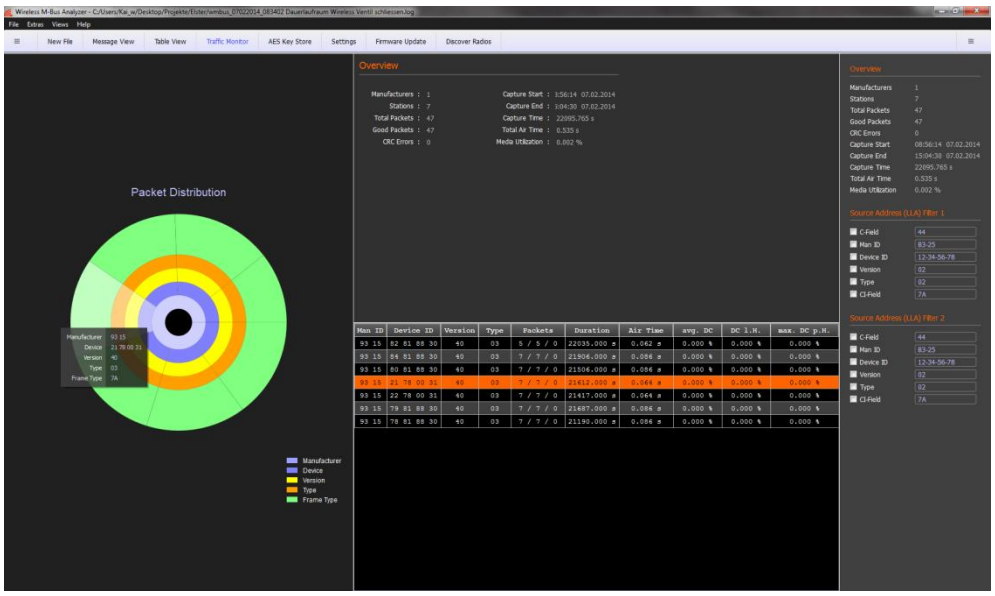

Figure 3-5: Traffic Monitor View

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.

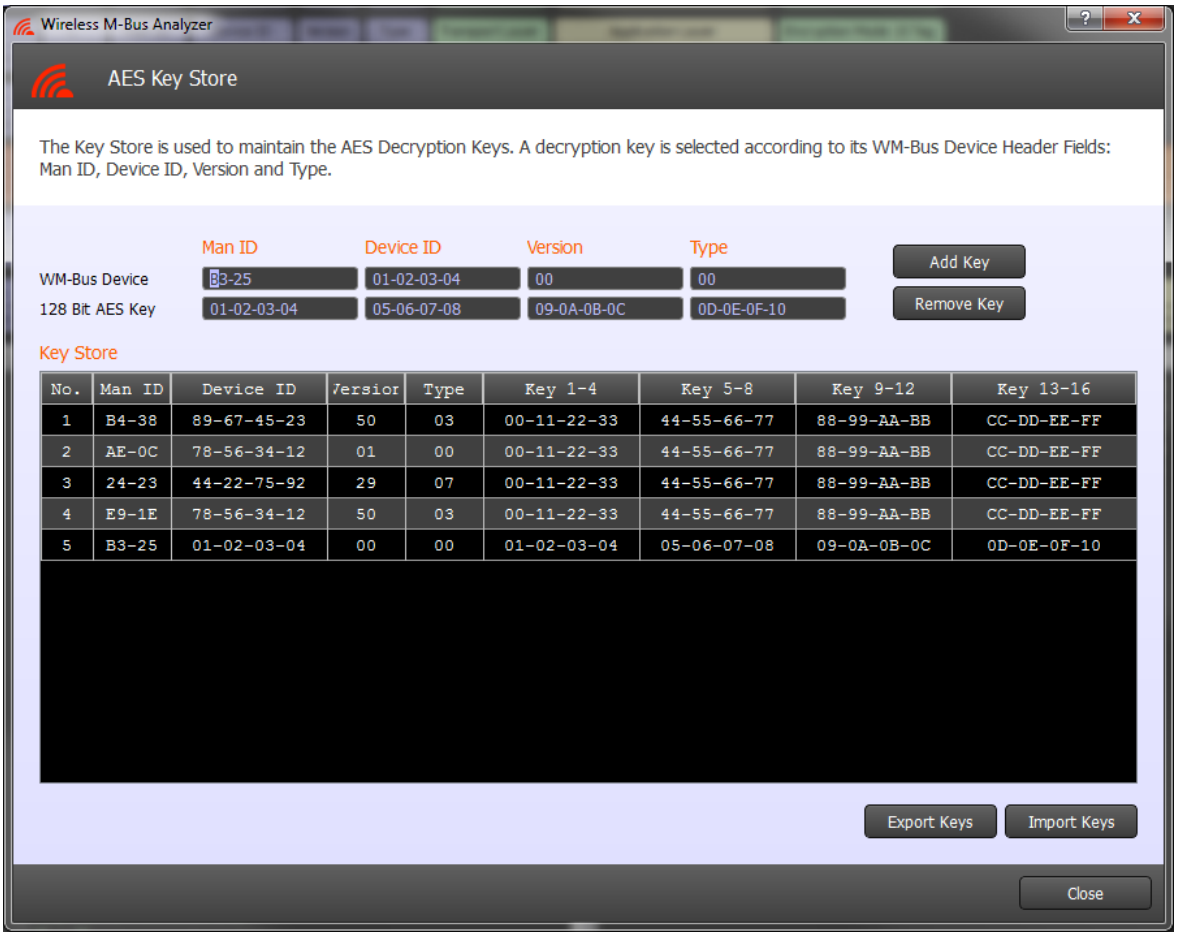

Figure 3-6: AES Key Store

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.

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.

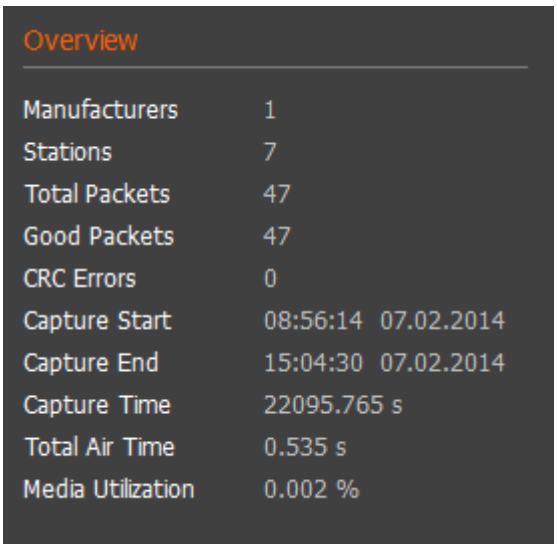

Figure 3-8: Overview

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.

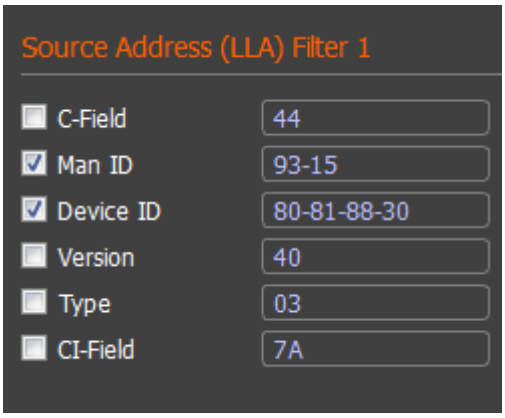

Figure 3-9: Message Filter

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.

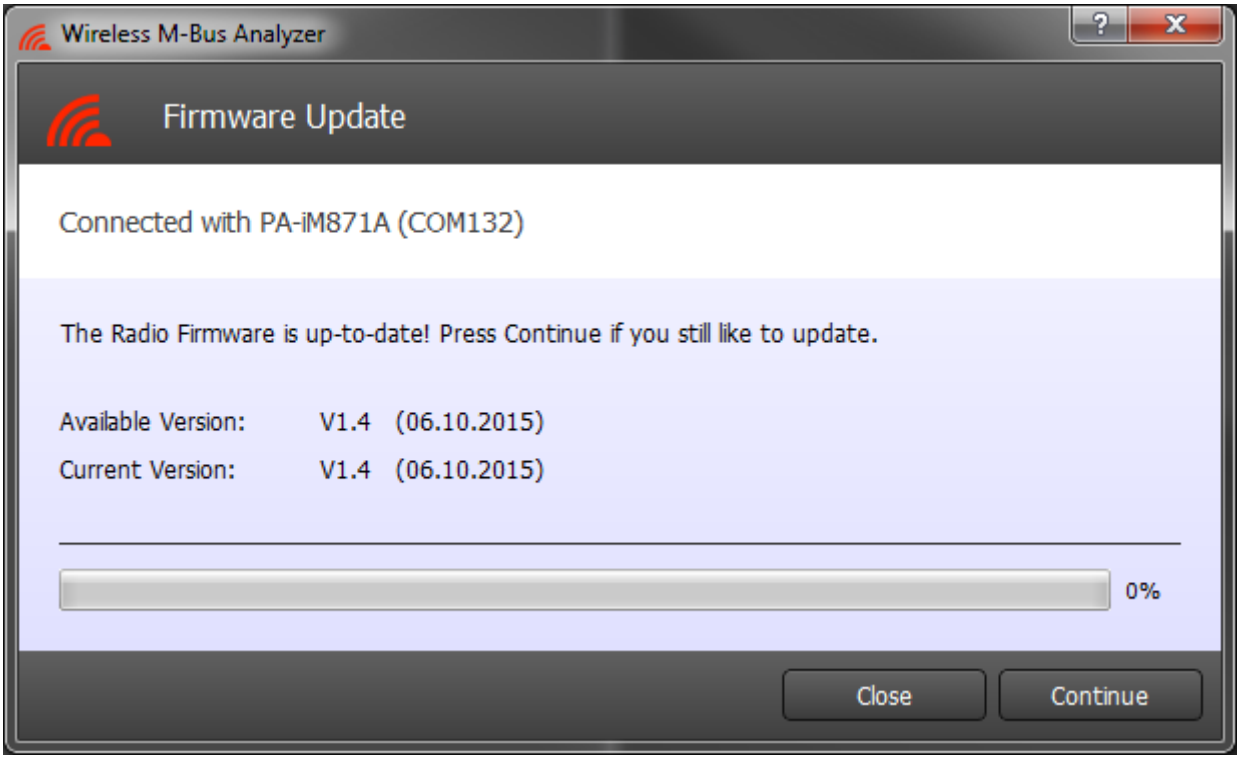

Figure 3-10: Firmware Update

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.

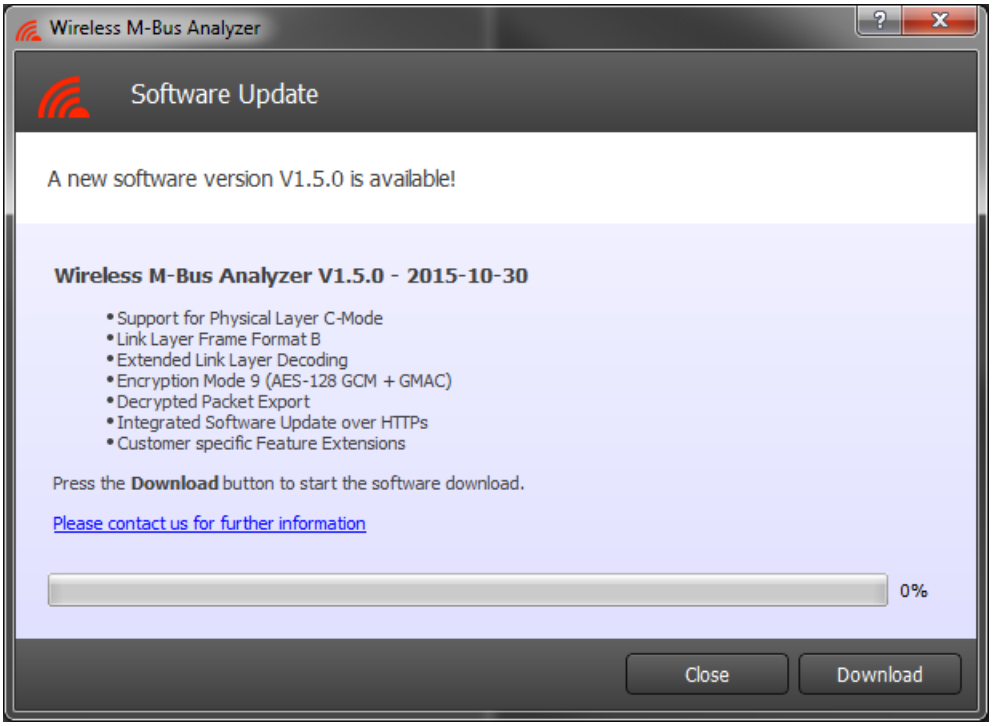

Figure 3-11: Software Update

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.

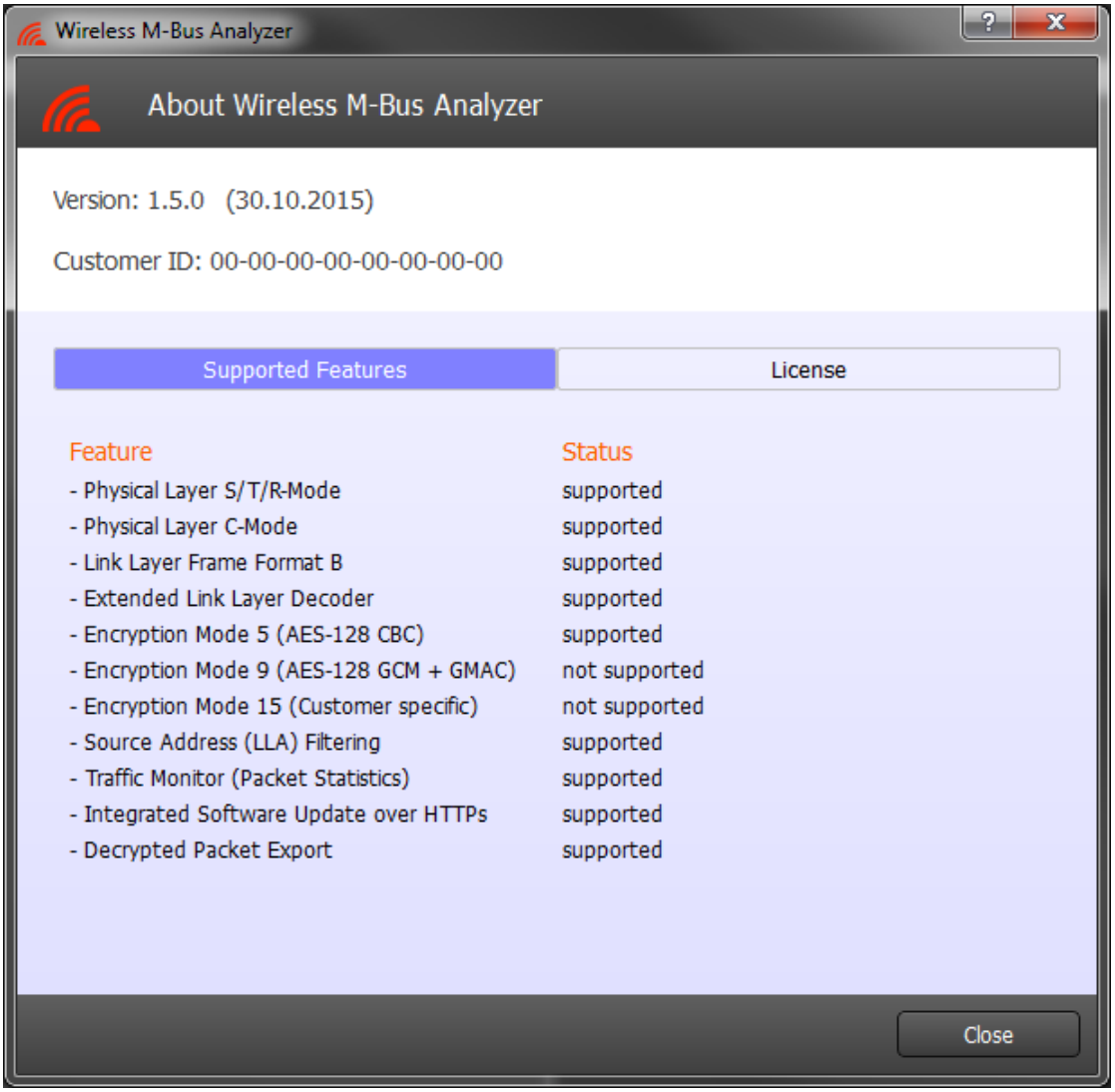

Figure 3-12: About Dialog – Supported Features

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

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.

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 wimod@imst.de
I www.wireless-solutions.de