Digianswer A/S

Bluetooth™

Bluetooth Protocol Analyser

Installation & Operation Manual

Contents

CAUTION

FCC Radio-Frequency Exposure Statement

This equipment generates and radiates radio-frequency energy. In order to comply with FCC radio-frequency radiation exposure guidelines for an uncontrolled environment, this equipment has to be installed and operated while maintaining a minimum body-to-antenna distance of 20 cm.

Users are not permitted to make changes or modify the system in any way.

About this manual

This installation and operation manual provides you with the information you need to make maximum use of Digianswer's Bluetooth™ Protocol Analyser. The manual is structured as follows:

- The **Introduction** provides basic information on what the Bluetooth Protocol Analyser is and how it works.
- The sections on **Installation** explain how to connect the USB-based hardware unit, install drivers, and install the software applications. Furthermore, this section contains information on necessary deinstallation of certain programs before the installation of the Bluetooth Protocol Analyser can take place.
- The sections on **Operation** provide instructions in how to use the Data Collector and the Bluetooth Packet Analyser respectively.
- **Technical facts** contains system requirements, upgrade information, and hardware specifications.
- The **Appendices** provide a list of the changes implemented since the previous version of the product. Also, you will find information on the packet format of the Bluetooth Protocol Analyser, allowing developers to build alternatives to Digianswer's Bluetooth Packet Analyser module. Finally, the manual contains various regulatory statements, and information on how to get in contact with Digianswer.

Note: This product has been designed for development purposes and is not to be sold to or used by end users.

Legal disclaimer

Any responsibility or liability for loss or damage in connection with the use of this product and the accompanying documentation is disclaimed. The information in this document is furnished for informational use only, is subject to change without notice, may contain errors or inaccuracies, and represents no commitment whatsoever. This agreement is governed by the laws of Denmark.

Rev: 1.1 – 00-09-08

Unpacking

The Bluetooth Protocol Analyser package contains the following items:

- Bluetooth USB Protocol Analyser
- Cable for Bluetooth USB Protocol Analyser
- Bluetooth Protocol Analyser CD-ROM
- Installation & operation manual

Introduction

Digianswer's Bluetooth Protocol Analyser is a development kit that allows you to view Bluetooth protocol data and carry out fast and effective analysis during the process of developing Bluetooth equipment.

Basically, the Bluetooth Protocol Analyser consists of a USB-based hardware unit and a software application called the Data Collector. With this equipment you can set up a log session during which you can intercept all the data transmitted between devices forming a Bluetooth piconet.

Accompanying the Bluetooth Protocol Analyser is a software application called the Bluetooth Packet Analyser, which is used for analysing the data logged during a session. The Bluetooth Packet Analyser can display all the baseband packets logged, and isolate, decode, and display LMP, L2CAP, RFCOMM, and SDP packets.

The Bluetooth Packet Analyser works as a plug-in for the Data Collector module. This is an open interface, which means that anyone is free to develop alternative Analyser modules for the Bluetooth Protocol Analyser.

The Bluetooth Protocol Analyser can be used in two configurations:

- **As an independent unit:** In this configuration, the Bluetooth Protocol Analyser does not participate in the piconet; it only listens in, logging all baseband packets transmitted between the master and slaves of the piconet.
- **As a participant in the piconet:** In this configuration, the Bluetooth Protocol Analyser is either the master or a slave of the piconet. The Bluetooth Protocol Analyser is attached to a computer running both the Data Collector application and Digianswer's Bluetooth Software Suite*. The Data Collector logs all baseband packets transmitted from the computer to other participants of the piconet as well as the packets received by the computer.

Note: While using the Bluetooth Protocol Analyser, it is advisable not to run any other applications on your computer – the Bluetooth Software Suite being an exception.

---

* Digianswer's Bluetooth Software Suite is automatically installed on your computer at the same time as the Bluetooth Protocol Analyser.

Installation

The installation procedure includes installing hardware, drivers, and software applications for the Bluetooth Protocol Analyser. In addition, Digianswer's Bluetooth Software Suite will be installed.

Note: If the Digianswer Bluetooth Demo Card or a previous version of the Bluetooth Software Suite is installed on your computer, you must uninstall this before you can install the Bluetooth Protocol Analyser. See the subsection "Uninstalling old programs" below.

Installing hardware and drivers

To install the Bluetooth Protocol Analyser hardware and the drivers for it:

1. Insert the Bluetooth Protocol Analyser CD-ROM.
2. Plug the USB cable of the Bluetooth Protocol Analyser into an available USB port on the computer. Windows now finds the new hardware and asks for drivers.
3. Follow the on-screen steps to complete the installation of the drivers, which are located on the CD-ROM at **D:\Drivers** (where **D:** is your CD-ROM drive).

Note: When you have installed the drivers, Windows will ask if you want to restart your computer. However, it is not necessary to restart the computer before installing the application software.

Note: When you have installed the drivers, your computer may appear frozen for some 30 seconds.

Note: Do not remove the Bluetooth Protocol Analyser CD-ROM from your computer until you have installed the application software.

Installing application software

Having connected the Bluetooth USB Protocol Analyser and installed the drivers, your are now ready to install the application software for the Bluetooth Protocol Analyser: the Data Collector and the Bluetooth Packet Analyser. At the same time you will be installing Digianswer's Bluetooth Software Suite.

1. Run **D:\Setup.exe** (where **D:** is your CD-ROM drive, where the Bluetooth Protocol Analyser CD-ROM is present).

2. Follow the on-screen instructions to complete the installation of the application software.

3. Restart your computer.

You are now ready to operate your Bluetooth Protocol Analyser.

Uninstalling old programs

If the Digianswer Bluetooth Demo Card or a previous version of the Bluetooth Software Suite is installed on your computer, you must uninstall this before you can install the Bluetooth Protocol Analyser.

To uninstall the Bluetooth Demo Card:

1. Insert the Demo Card.
2. Insert the Bluetooth Protocol Analyser CD-ROM.
3. Run **D:\deinstaller.exe** (where **D:** is your CD-ROM drive).
4. Follow the on-screen instructions.
5. Remove the Demo Card.
6. Restart your computer.

To uninstall the Bluetooth Software Suite:

To uninstall the application software:

1. From the **Start** menu, find and select **Uninstall** / **Digianswer Bluetooth Software Suite.**

2. Follow the on-screen instructions.

3. Restart your computer.

To uninstall the drivers:

1. Enter **System Properties** / **Device Manager.**

2. Locate and remove the **Digianswer Bluetooth Demo Card Controller** and the **Digianswer Bluetooth Ethernet Adapter.**

3. Click **OK.**

Note: At this stage, you may need the original Windows installation CD-ROM.

Note: The computer may ask if you want to restart your computer. However, you need to delete the system files listed below. Therefore, **DO NOT RESTART THE COMPUTER NOW!**

---

4. Start **Explorer**, enter your **\windows\system** directory, and delete the following files:

Dgahci.vxd	Dgapcc.sys *and* Dgapcc32.vxd
Dgal2cap.vxd	Dgarfcom.vxd
Dganat.vxd	Dgasdp.vxd
Dgandis.vxd	Dgausb.vxd *and* Dgavcomm.vxd

5. Enter the **\windows\inf** directory and delete the following files:

Dgahub.inf	Dgahub.inf
Dganet.inf	Dgausb.inf
Dgapcc.inf	Drvdata.bin *and* Drvidx.bin

6. Enter the **\windows\system32\drivers** directory and delete the following files:

Digiusb.sys	Dgamap.sys

7. Restart your computer.

You can now install the Bluetooth Protocol Analyser, including the Bluetooth Software Suite as described in the sections “Installing hardware and drivers” and “Installing application software” above.

Data Collector operation

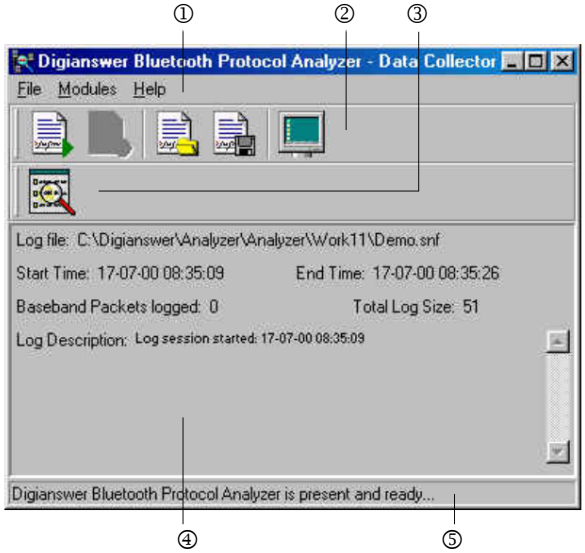
Features

The purpose of the Data Collector is, basically, to listen in on the Bluetooth piconet to which it is connected, and create a log containing all the baseband packets transmitted between the Bluetooth devices participating in the piconet. With the Data Collector, you can:

- Capture all baseband packets transmitted within a Bluetooth piconet – including packets that are normally not visible for the host such as retransmitted packets – and view the status of each packet (access error, packet header error, etc.), estimated clock and hop frequency.
- Transmit and receive on a single user-defined frequency.
- Turn data whitening on and off.
- Select any specified hopping pattern: Europe/USA, Japan, France, or Spain.
- Start/stop log sessions manually.

Main window

In this section, we will take a look at the Data Collector main window. In the following sections, we will go into detail with the various functions of the program.



① **File**, **Modules**, and **Help** menus. The **File** menu contains an item for each of the functions that you can use the Data Collector for: Opening logged files, saving files, starting log sessions, stopping log session, and quitting the Data Collector. These functions are described in the following sections. From the **Modules** menu, it is possible to add icons for alternative packet Analysers to the Data Collector window – see the description of ③ below. Finally, the **Help** menu offers easy access to the Digianswer homepage.

② Five icons representing the functions of the Data Collector. These functions are also accessible from the **File** menu. The functions are described below.

③ Bluetooth Packet Analyser icon. When you have logged a new file, or opened an old file from the Data Collector, clicking this icon will conveniently open the corresponding file in Digianswer's Bluetooth Packet Analyser. During the installation of the Bluetooth Protocol Analyser, the icon is placed in the registry:

KEY_LOCAL_MACHINE\Software\Digianswer\Bluetooth Protocol Analyser\Data Collector\Modules\Digianswer

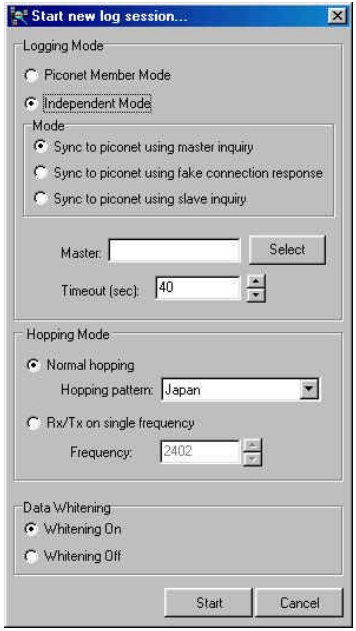
If you want to use an alternative packet Analyser, placing an icon for it in the Data Collector window is easily done via the **Modules** menu.

④ Various information on the current log file: Location, start and end times, number of baseband packets logged, log size, and date.

⑤ Status bar.

Starting log session

Click this icon to open the **Start new log session** dialog box:



We will now take a look at the three main items of this dialog box: **Logging Mode**, **Hopping Mode**, and **Data Whitening**.

Logging Mode:

Piconet Member Mode is to be used in connection with the Bluetooth Software Suite. When a log session is started, the Bluetooth Protocol Analyser logs all baseband packets sent from and received by your computer.

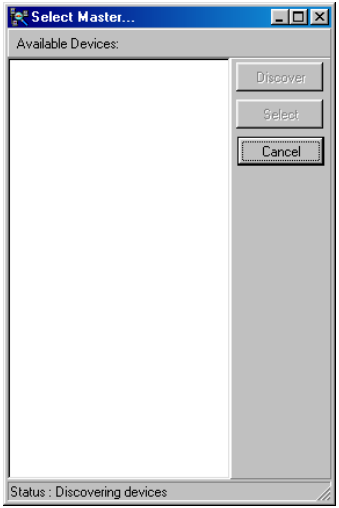
In **Independent Mode**, the Bluetooth Protocol Analyser works as a stand-alone unit. Three kinds of synchronization modes can be selected:

- *Sync to piconet using master inquiry:* In this mode the synchronization is obtained by performing an inquiry and using the clock information returned by the master to set the clock of the Protocol Analyser. (The master is chosen in a dialog box opened by clicking **Select**.) As in some Bluetooth devices the clock drifts away when the device is not in connect mode, this synchronization mode can be troublesome if it is desirable to monitor negotiations during the connect phase. This is due to the fact that there are often several seconds' delay from the time when the Protocol Analyser obtains the master clock information until the master actually connects to the slave. Likewise, if the inquiry scan mode on the Bluetooth device is not implemented or disabled during the connection, this mode cannot be used for synchronization.

- *Sync to piconet using fake connection response:* This mode can only be used during the connect phase, i.e. when the piconet master connects to a new slave. The Protocol Analyser pretends it is the slave unit chosen in the **Select ...** dialog box and obtains the master clock information by initiating a new connection as if it were that slave. Immediately after the clock information has been retrieved, the Protocol Analyser stops transmitting, and the piconet master continues the connection attempt with the true slave.

- *Sync to piconet using slave inquiry:* This mode can only be used during the connect phase and is based on the same principle as the method mentioned above in connection with *Sync to piconet using fake connection response*. Instead of pretending to be the slave unit chosen in the **Select ...** dialog box, the Protocol Analyser listens for the clock information sent in the connect phase to the new piconet slave and therefore does not interfere with the piconet in any way. To be able to catch the clock information on the right frequency, it is necessary to obtain the slave clock. This is done by performing an inquiry to the slave.

To select master or slave, click **Select**. The following dialog box opens:



The Bluetooth Protocol Analyser will now carry out device discovery, and then display a list of all active Bluetooth devices within range. To select the master or slave you want to connect to, highlight the desired device in the above dialog box and click **Select**.

You can edit the MAC address in the edit field, thus changing to a different address.

Selecting **Independent Mode** also involves setting the number of seconds allowed to pass when there is no activity in the piconet. On timeout, the Bluetooth Protocol Analyser will inform you of the lack of activity.

Note: When you use the Bluetooth Protocol Analyser in connection with the Bluetooth Software Suite, it has to be in piconet mode, i.e. working as a participant in a piconet. When the Bluetooth Protocol Analyser is in independent mode, i.e. working as a stand-alone unit, you cannot use it in connection with the Bluetooth Software Suite.

Hopping Mode:

Here you can select **Normal hopping**, specifying the hopping pattern of the geographical area. Or you can select **Rx/Tx on single-frequency**, including specifying the desired frequency.

Data Whitening:

Data whitening can be turned on or off. By default, the function is set to on.

Stopping log session

Click this icon to stop the current log session. The Data Collector main window will now display information on the start and end times of the log session, number of baseband packets logged, and log size.

Opening old log session

Click this icon to browse in Windows Explorer and open a previously stored log session.

Saving log session

Click this icon to save the current log session. The Bluetooth Protocol Analyser will save two versions of the log file: A **.snf** file to be opened from the Data Collector, and a **.data** file to be opened from the Bluetooth Packet Analyser.

Exit

Click this icon to quit the Data Collector.

Bluetooth Packet Analyser operation

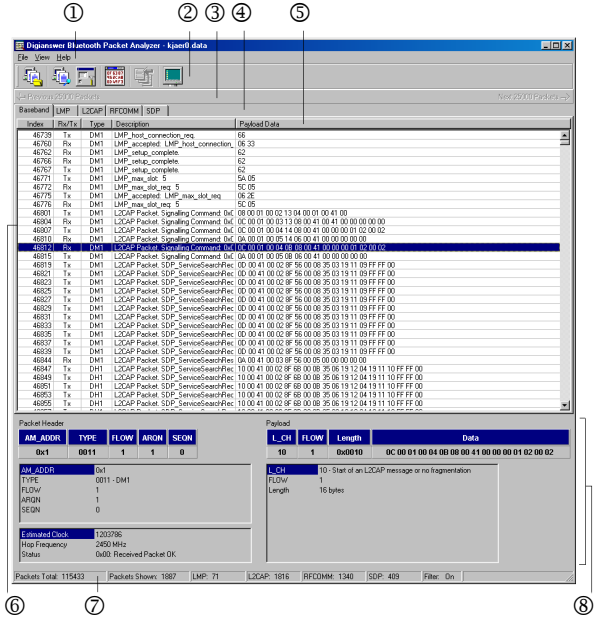
Features

The purpose of the Bluetooth Packet Analyser is, basically, to analyse and display the contents of log files created by means of the Data Collector. The Bluetooth Packet Analyser can:

- Analyse baseband packets and display ID, IQ, NULL, POLL, FHS, DMx, DHx, HVx, and DV Packets.
- Isolate, decode, and display LMP, L2CAP, RFCOMM, SDP commands, events and data packets.
- Export to .CSV files with ':' as separator. These files are readable with e.g. Microsoft Excel.

Main window

In this section we will take a look at the main window of the Bluetooth Packet Analyser. In the following sections, we will go into detail with the various functions of the program.



① **File**, **View**, and **Help** menus. From the **File** menu you can open files, view the properties of the current log file, and quit the program. From the **View** menu, you can view the filter and view setups; go directly to any packet number you want; search; and open the **Packet Hex View** window (see the section "Hex view" below). Finally, the **Help** menu offers easy access to the Digianswer homepage.

② Icons representing the various functions of the Bluetooth Packet Analyser. These are described below.

③ View the last/next 25,000 packets (baseband packets are shown at intervals of 25,000).

④ Tabs for selecting which packets of the current log file you want to see – all baseband packets or specific types/levels of packets: LMP, L2CAP, RFCOMM, and SDP.

⑤ Tabs indicating which items you have selected in the view setup, where you can decide which elements you want the list view to show.

⑥ List view displaying the contents of the current log file as a list of the packets the file contains.

⑦ Status bar.

⑧ Various information on the packet currently highlighted in the list view. The nature of this information depends on the type and contents of the packet.

Opening a file

This function – **Load Log session from file** – will open a dialog box that allows you to browse and open a log file.

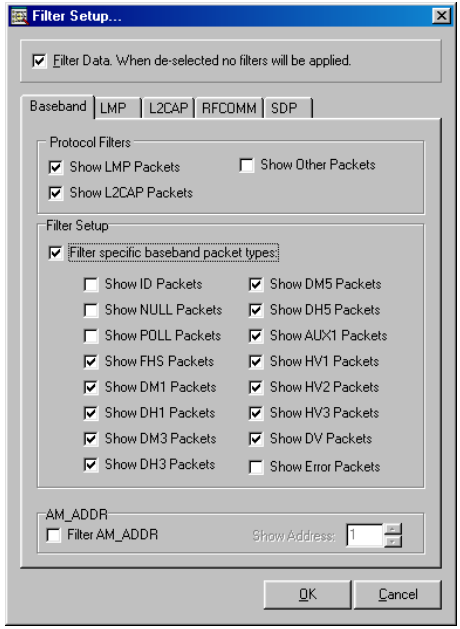
The Protocol Analyser features especially fast load of files of sizes up to the available physical and virtual memory limitations. Files exceeding that size will be loaded less fast.

Filter setup

The filter function allows you to reduce the amount of data displayed in the list view. In **Baseband**, for instance, you can choose to view only LMP and L2CAP packets, rather than *all* the packets transmitted. This function can greatly reduce the number of packets on a list, making the list much easier to work with.

The filter function needs to be selected for each of the lists – **Baseband, LMP, L2CAP, RFCOMM**, or **SDP**; applying the function to one of these lists will not affect the others.

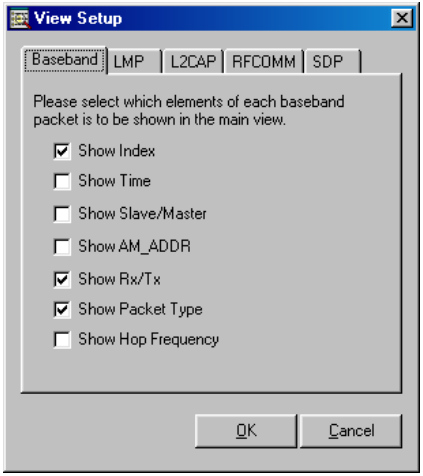
In the **Filter Setup** dialog box, you can select which list of packets the filter function should be applied to, and which data should be filtered. The choice of data varies depending on which list of packets is selected. The following example shows the dialog box as it appears when selected from **Baseband**:



Although **Baseband** is, in principle, a list of all the packets logged in the current log file, these are filtered by default so that only LMP and L2CAP packets are shown in **Baseband**. However, you can change the settings as your desire.

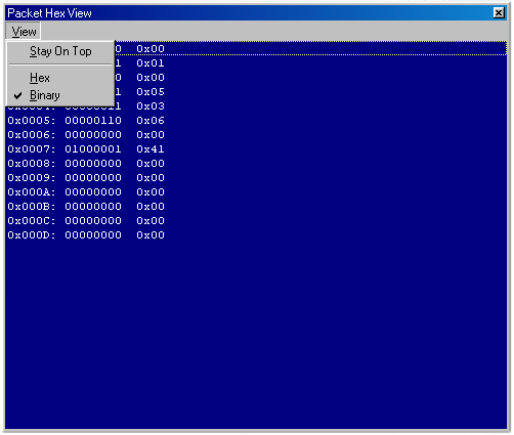
View setup

For each of the tabs representing a list of packets – **Baseband, LMP, L2CAP, RFCOMM**, or **SDP** – you can select which elements should be displayed in the list view. This is done in the **View Setup** dialog box. In the example below, the following elements have been selected for **Baseband: Index, Rx/Tx,** and **Packet Type**.



Hex view

The main window only shows part of what a packet contains (except at the RFCOMM and SDP level). However, you can view the entire contents of a packet – including packets that were fragmented during transmission – by opening the **Packet Hex View** dialog box. Here you can select **Hex** or **Binary**. Furthermore, selecting **Stay On Top** will keep the dialog box in front of any other Bluetooth Packet Analyser windows that you open.



Back to Baseband

Click this icon to return to the list of baseband packets from any of the other lists of packets.

One level up/down

When a packet is highlighted in the list view, you can navigate from one level of information to another by means of ***Enter*** (one level down) and ***Backspace*** (one level up). For instance, in **Baseband**, highlight an L2CAP packet, and press ***Enter***. This will take you to the L2CAP level of the same packet. You can now return to **Baseband** by pressing ***Backspace***, or proceed to the RFCOMM/SDP level (depending on the packet) by pressing ***Enter***:

Navigating from one level to another in the Bluetooth Packet Analyser:

Exit

Click this icon to quit the Bluetooth Packet Analyser.

Technical facts

System requirements

- Computer with a 266 MHz or higher processor; Pentium II recommended
- Microsoft Windows 95 or later operating system (excluding Windows NT)
- 64 MB RAM
- Free hard-disk space required: Approx. 100 MB (depending on the amount of data logged)
- Monitor resolution: 1024 by 768 pixels or higher

Upgrades

The Bluetooth Protocol Analyser is upgradeable via computer software. Information about new upgrades will be available from our web site: www.digianswer.com

Hardware specifications

- Compliant with the USB specification version 1.1
- Powered by the computer
- Standby power consumption: <20mA
- Active power consumption: <350mA

Bluetooth radio specifications

- Designed in accordance with the Bluetooth specification version 1.0B
- Transmit power: +20dBm (100mW)
- Receiver sensitivity:<-80dBm
- Frequency range: 2.402 - 2.480 GHz

Bluetooth Protocol Analyser packet format

The definition of the Bluetooth Protocol Analyser packet format is shown in Appendix B.

Appendix A: Changes implemented since v1.0

The following is a list of the new features implemented in the Bluetooth Protocol Analyser version 1.1 (i.e. features not implemented in version 1.0, known as the ”Bluetooth Sniffer”):

Data Collector

- Three sync modes.
- It is now possible to edit a selected master MAC address in the *Start new session* dialog box *Master* edit field. The format is 6 bytes in hex notation, values are separated by a colon (00:50:CD:01:00:04).
- Support of correct selection of hop frequency for Europe/USA, France, Spain, and Japan.

Packet Analyser

- Export to .CSV files.
- Faster file load with file sizes up to the available physical and virtual memory limitations.
- Decoding of SDP packets across page boundaries.
- Better recognition of SDP packets.

Appendix B: Packet format

The following table shows the packet format of the Bluetooth Protocol Analyser. Each [xx] represents one byte.

Byte position	Name	Description
[01]	Sync word	The Digianswer specified sync word for the Protocol Analyser packet is 0xFF.
[02]	Protocol Analyser packet type	Currently there is only one Protocol Analyser packet type: 0 (the one shown in this table). It provides a description of how to decode the packet from byte position 7 and onward. In the future, there may be additional packet types.
[03]	Packet counter (15-8)	The packet counter can be used to detect missing packets. Please note that packets are deleted if the host interface is too slow.
[04]	Packet counter (7-0)	-
[05]	Total length (7-0)	The total length of the Protocol Analyser packet, not including the first six bytes.
[06]	Total length (15-8)	-
[07]	Status byte	**Receive direction** 0x00 = Received packet OK Bit 0 = Access error Bit 1 = Packet header error (FEC 1/3) Bit 2 = Packet header error (HEC) Bit 3 = Payload recoverable error (FEC 1/3 or FEC 2/3) Bit 4 = Payload nonrecoverable error (FEC 2/3) Bit 5 = Payload error (CRC) Bit 6 = Type <> Length error **Transmit direction** 0x80 = Packet transmitted

[08]	Estimated clock (27-24)	Piconet master clock
[09]	Estimated clock (23-16)	-
[10]	Estimated clock (15-8)	-
[11]	Estimated clock (7-0)	-
[12]	Hop frequency	The frequency offset “k” used for this packet F = (2402 + k) MHz
[13]	Header info: AM address (bit 2-0)	If packet type is ID or IQ, this parameter is not valid
[14]	Header info: Type (bit 3-0)	If packet type is ID: 255
[15]	Header info: FLOW (bit 0)	If packet type is ID or IQ, this parameter is not valid
[16]	Header info: ARQN (bit 0)	-
[17]	Header info: SEQN (bit 0)	-
[18]	Payload info: L_CH (bit 1-0)	If packet type is ID, IQ, NULL, POLL, HV1, HV2, HV3 or FHS, this parameter is not valid
[19]	Payload info: FLOW (bit 0)	-
[20]	Payload info: Length (bit 8)	-
[21]	Payload info: Length (bit 7-0)	-
[22]	1st payload data byte	Tx/Rx payload data bytes. Note that Tx data bytes are bit-reversed
[23]	2nd payload data byte	-
...	...	-
...	...	-
...	...	-
[359]	338th payload data byte	-

Appendix C: Regulatory statements

General

This product complies with any mandatory product specification in any country where the product is sold. In addition, the product complies with the following.

United States of America and Canada

Tested To Comply With FCC Standards FOR HOME OR OFFICE USE. See FCC 47CFR part 15.19(b)(2).

This device complies with part 15 of the FCC rules and with RSS-210 / RSS-139 of the Industry Canada. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

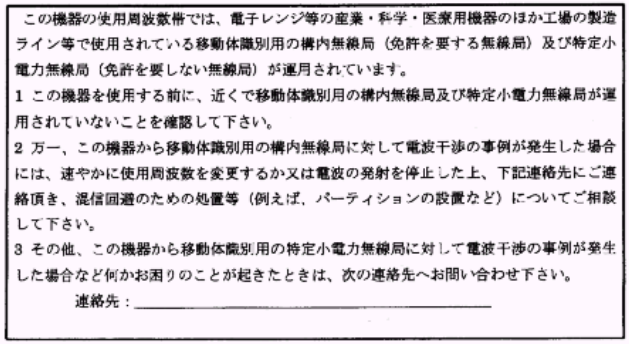
Note that any changes or modifications to this equipment not expressly approved by the manufacturer may void the FCC authorization to operate this equipment.

European Union (EU) and EFTA

This equipment complies with the R&TTE directive and has been provided with the CE mark accordingly.

Note that the radio frequency band used by this equipment has not been harmonized in all of the EU.

Japan


この機器の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用されている移動体識別用の構内無線局（免許を要する無線局）及び特定小電力無線局（免許を要しない無線局）が運用されています。
1 この機器を使用する前に、近くで移動体識別用の構内無線局及び特定小電力無線局が運用されていないことを確認して下さい。
2 万一、この機器から移動体識別用の構内無線局に対して電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか又は電波の発射を停止した上、下記連絡先にご連絡頂き、混信回避のための処置等（例えば、パーティションの設置など）についてご相談して下さい。
3 その他、この機器から移動体識別用の特定小電力無線局に対して電波干渉の事例が発生した場合など何かお困りのことが起きたときは、次の連絡先へお問い合わせ下さい。
連絡先：

Japan office:

Address:	BIA Inc. No. 202 Gobancho House 4-22 Gobancho Chiyoda-Ku, Tokyo 102-0076
Phone	03 5276 5984
Fax:	03 5276 0625
E-mail:	biasib@gol.com

Appendix D:
Digianswer contact information

Digianswer A/S

Skalhuse 5
DK-9240 Nibe
Denmark
Phone: +45 9671 0000
Fax: +45 9835 0052
E-mail: BluetoothPA@Digianswer.com
Web site: www.digianswer.com

Digianswer A/S

Bluetooth™

Bluetooth Protocol Analyser