Computer Access Technology Corporation

2403 Walsh Avenue, Santa Clara, CA 95051-1302 Tel: +1/408.727.6600 Fax: +1/408.727.6622

CATC *Merlin*™

Bluetooth™ Protocol Analyzer

User's Manual

Version 1.6

8 June, 2001

Document Disclaimer

The information contained in this document has been carefully checked and is believed to be reliable. However, no responsibility can be assumed for inaccuracies that may not have been detected.

CATC reserves the right to revise the information presented in this document without notice or penalty.

Trademarks and Servicemarks

CATC, Merlin, NetMate, Advisor, Chief, FireInspector, Inspector, Detective, Traffic Generator, BusEngine, USB4DOS, UPT, HPT, UHT, Galaxy, and *Andromeda* are trademarks of Computer Access Technology Corporation.

Microsoft, Windows, and *Windows NT* are registered trademarks of Microsoft Inc.

All other trademarks are property of their respective companies.

Copyright

Copyright © 2001, Computer Access Technology Corporation (CATC); All Rights Reserved.

This document may be printed and reproduced without additional permission, but all copies should contain this copyright notice.

Part number: 730-0017-00

TABLE OF CONTENTS

Chapter 1 Overview. 1
Bluetooth™ Overview 1
General Description 2
Features. 4
General 4
Physical Components 4
Display Options 5
Recording Options 5
Traffic Generation. 5
Bluetooth™ BusEngine 5
Specifications 6
Package 6
Power Requirements. 6
Environmental Conditions 6
Switches 6
LEDs 6
Recording Memory Size. 6
Certification 6

Chapter 2 Quick Installation 7
Setting Up the Analyzer 7
Installing the Software 7
Your First Bluetooth™ Recording 8

Chapter 3 Detailed Installation 11
System Components/Packing List 11
The Installed Merlin Unit 11
Merlin System Setup. 12
AC Power Source 12
External Interface Breakout Board 13
Breakout Board External Output Signalling Pins. 14
Prototype Rework Area 15
PC Connection 15
Antenna Information. 15
Analyzer PC Requirements. 15
Merlin Program Installation 16
Loading the Merlin USB Drivers 16
Installing the Merlin Application Program. 16
Merlin Program Startup 17
Making a Recording 18

Chapter 4 Upgrades. 19

Software, Firmware, and BusEngine Revisions 19
Software Upgrades 20
BusEngine and Firmware Upgrades 20
Automatic Upgrades 20
Manual Upgrades to BusEngine and Firmware 22
Upgrading the BusEngine 22
Upgrading the Firmware 24

Chapter 5 Software Overview 25

The Main Display Windows 25
View Options 27
Tool Bar 27
Status Bar 29
Recording Progress 29
Recording Status 30
Analyzer Status 30
Search Status 31
Zoom In. 31
Zoom Out 31
Tool Tips 31
Merlin Analyzer Keyboard Shortcuts 32

Chapter 6 Recording Wizard 33

Starting Recording Wizard 33
Recording a Traffic on a New Piconet 34
Recording an Existing Piconet 45
Recording in Test Mode 55
Recording in Reduced Hopping Mode 55

Chapter 7 Recording Options. 59

Opening the Recording Options Dialog Box 59
Recording Options - General 60
Recording type 60
Options 61
Buffer Size 61
Trigger Position 61
Recording Options - Modes 62
Recording Mode 63
Inquiry Recording 63
Piconet Recording. 63
Hop Frequency 67
Force Re-synchronization 68
Follow Master/Slave Switch 68
Match Clock Rate 68

Show Paging Traffic 69
Piconet Addresses (MSB -> LSB) 69
Other Parameters. 69
Debug/Test 70
Recording Options - Events 70
Events Options 71
Payload Length Error. 77
Recording Options - Actions 78
Actions Window Layout 78
Action Buttons - Their Functions 79
Counting Buttons - Their Functions 79
Blue Dot Menus 81
Saving Recording Options 87
Recording Bluetooth™ Traffic 88

Chapter 8 Display Options 91

General Display Options. 91
Trace Viewing Level. 92
Creating New Display Options Files 92
Color Display Options 93
Formats Display Options 95
Hiding 96
Saving Display Options 97

Chapter 9 Reading a CATC Trace 99

Trace View Features 99
Interpreting the Displayed Information 99
Tool Tips 100
Set Marker. 100
Edit or Clear Marker 101
Expanded and Collapsed Data Formats 102
Hide Frequency Hops 103
Hide Nulls and Polls 103
Hide Unassociated Traffic 104

Chapter 10 Decoding Higher Protocols 105

Introduction. 105
LMP and L2CAP Messages 105
Decoding and Viewing Higher Protocol Data 106
Decoding Via the Decoding Toolbar. 106
Decoding Via the Display Options Dialog Box 106
Tooltips 107
Viewing Packets in LMP and L2CAP Messages 108
Types of LMP and L2CAP Messages. 108

Viewing L2CAP Channel Connections 109
Viewing Protocol Messages and Transactions 110
Viewing L2CAP Messages in Protocol Messages 110
How to Decode 110
Expanding Protocol Messages 111
Changing Protocol Assignments. 111
Using the Decoding Assignments Dialog Box 112
Removing User-Assigned Protocol Assignments. 112
Manually Assigning Protocols 113
Other Assignments: OBEX Client/Server Status 113
Changing an OBEX Client or Server Status. 114
Decoding BNEP (Bluetooth Network Encapsulation Protocol) 114

Chapter 11 Other Features 115

Search 115
Go to Trigger. 115
Go to Packet/Message/Protocol 115
Go to Marker. 116
Go to 116
Error 119
Soft Bit Error 119
Loss of Sync 119
Find 120
Event Groups 121
Union, Intersection, and Exclusion. 124
Using Find. 124
Find Next 126
Edit Comment 126
Reports 127
File Information 127
Error Summary 127
Timing Calculations 128
Traffic Summary 129
BT Neighborhood 131
Encryption. 131
Configuring Merlin for Encryption. 132

Chapter 12 How to Contact CATC 135

Chapter 13 Warranty and License. 135

1. Overview

The CATC Merlin™ Protocol Analyzer is the newest member in CATC's industry-leading line of high performance, serial bus protocol analyzers. Preceded by CATC's USB Chief™ and IEEE 1394 FireInspector™ Analyzers, Merlin has been designed using the same modular software and hardware architecture that made its predecessors highly successful in the serial bus protocol analyzer market worldwide.

1.1 Bluetooth™ Overview

The Bluetooth™ wireless technology is set to revolutionize the personal connectivity market by providing freedom from wired connections. It is a specification for a small-form factor, low-cost radio solution providing links between mobile computers, mobile phones and other portable handheld devices, and connectivity to the internet.

The Bluetooth™ Special Interest Group (SIG), comprised of leaders in the telecommunications, computing, and network industries, is driving development of the technology and bringing it to market. The Bluetooth™ SIG includes promoter companies 3Com, Ericsson, IBM, Intel, Lucent, Microsoft, Motorola, Nokia and Toshiba, and more than 2000 SIG members.

Bluetooth™ is a radio technology specification designed to transmit both voice and data wirelessly, providing an easier way for a variety of mobile computing, communications and other devices to communicate with one another without the need for cables. Bluetooth™ could make possible what is being called the personal-area network by allowing users to transmit small amounts of data at 1M bit/sec up to 10 meters over the 2.4-GHz radio frequency. The key benefits of the Bluetooth™ technology are robustness, low complexity, low power and low cost. Bluetooth™ employs a rapid frequency hopping mechanism to minimize the effects of *'collisions'* with other protocols and devices operating in the same frequency band. Mechanisms exist for a Bluetooth™ device to determine all devices in range as well as to request connection to a piconet as either a master or a slave.

Please refer to the *Bluetooth™ Specification, version 1.0b* for details on the protocol. The Bluetooth™ specification is available from the Bluetooth™ SIG at its web site **http://www.bluetooth.com/**

1.2 General Description

The Merlin Protocol Analyzer is designed as a stand-alone unit that can be easily configured and controlled by a portable or desktop PC connected via its USB port. Merlin provides customers with the familiar 'CATC Trace' user interface that is the *de facto* industry standard for documenting the performance of high-speed serial protocols.

Merlin supports the functionality required to analyze all levels, including the baseband, of the Bluetooth™ wireless protocol. The featured Radio Interface allows users to probe and analyze transactions at the lowest level within the Bluetooth™ architecture. By creating this "Point of Observation" or probing point within the radio level packet view, the user can analyze all levels of the protocol stack.

Merlin is a non-intrusive testing tool for Bluetooth™ piconets providing network traffic capture and analysis. Hardware triggering allows real-time events to be captured from a piconet. Hardware filtering allows the filtering out of fields, packets, and errors from the recording. Filtering allows users to focus recordings on events of interest and to preserve recording memory so that the recording time can be extended.

Recorded data is presented in colored graphics in a trace viewer application. This application has advanced search and viewing capabilities that allow the user to quickly locate specific data, errors and other desired conditions, thereby focussing the user's attention on events of interest.

The Merlin Protocol Analyzer functions with any personal computer using the Windows 98, Windows 98SE, Windows NT 4.0, or Windows ME operating systems and equipped with a functional USB interface. The Analyzer is a stand-alone unit configured and controlled through a personal computer USB port. It can be used with portable computers for field service and maintenance as well as with desktop units in a development environment. It is easily installed by connecting a cable between the computer's USB port and the Analyzer's USB port.

Sample Bluetooth™ Piconet with Merlin Protocol Analyzer

Merlin provides on-the-fly detection of and triggering on such events as Packet Headers and Errors. Whether recording manually or with a specified trigger condition, Merlin continuously records the bus data in a wrap-around fashion until manually stopped or until the Trigger Event is detected and a specified post-Trigger amount of bus data is recorded.

Upon detection of a triggering event, the analyzer continues to record data up to a point specified by the user. Real-time detection of events can be individually enabled or disabled to allow triggering on events as they happen. This includes predefined exception or error conditions and a

user-defined set of trigger events. The unit can also be triggered by an externally supplied signal. An external DB-9 connector provides a path for externally supplied data or timing data to be recorded along with bus traffic.

This DB-9 connector also provides a path for Merlin to transmit externally two control, timing, or recovered signals for purposes of probing and use by other circuitry.

The Merlin software provides powerful search functions that enable investigation of particular events and allow the software to identify and highlight specific events. In addition to immediate analysis, you can print any part of the data. Use the **Save As** feature to save the data on disk for later viewing. The program also provides a variety of timing information and data analysis reports.

1.3 Features

General

- Flexible design - reconfigurable hardware for future enhancements.
- User friendly - the Graphical User Interface software of Merlin Analyzer is designed to be consistent with the 'CATC Trace' using color and graphics to display Bluetooth™ traffic.
- Radio Level Point of Observation and Capture - traffic capture at the Radio Level for comprehensive analysis.
- Complies with Bluetooth™ v1.1 specification.
- Supports point-to-point and point-to-multipoint Bluetooth™ piconets.
- Supports both 79 frequency hop and 23 frequency hop standards.
- Free non-recording, view-only software available.
- Power-on self-diagnostics.
- Internal 100V to 240 V AC power supply.
- Compliant with FCC class A requirements / meets all CE mark requirements.
- One year warranty and hot-line customer support.

Physical Components

- USB host connection to portable and desktop PCs for analysis of captured information.
- Host software support for Microsoft Windows 98, Windows 98SE, Windows ME, and Windows NT 4.0.
- Trace viewer software support for all of the above plus Windows 95.

- Recording memory of 128MB - enough to record twenty five minutes of high volume traffic.

Display Options

- Analyzes and displays a transaction-level view of piconet traffic with accurate time-stamps and frequency hop information.
- Software analysis and data presentation at several protocol levels: (Baseband, LMP, L2CAP, SDP, RFCOMM, TCS, OBEX, HDLC, BNEP, PPP, and AT Commands).

Recording Options

- Flexible advanced triggering capabilities including - multiple triggering modes, selective views, timing analysis, search functions, protocol packet errors, transaction errors, packet type and destination device, data patterns, or any of these trigger types in combination.
- User defined trigger position.
- Real-time hardware filtering of captured traffic for optimizing analyzer memory usage.

Traffic Generation

- Traffic generation capability (when used in future add-on product).

Bluetooth™ BusEngine

CATC's BusEngine™ Technology is at the heart of the new Merlin Analyzer. The revolutionary BusEngine core uses state-of-the-art EPLD technology and incorporates both the real-time recording engine and the configureable building blocks that implement data/state/error detection, triggering, capture filtering, external signal monitoring and event counting & sequencing. And like the flash-memory-based firmware that controls its operation, all BusEngine logic is fully field upgradeable, using configuration files that can be downloaded from the CATC Website.

1.4 Specifications

Package

Dimensions:	9.2 x 8.4 x 2.5 inches (23.4 x 21.3 x 6.4 cm)
Connectors:	AC power connection external clock input (EXT CLK, BNC) host connection (USB, type 'B') data connector (Data In/Out, 9-pin DB)
Weight:	2.8 lbs. (1.2 kg)

Power Requirements

90-264VAC, 47-63Hz (universal input), 100W maximum

Environmental Conditions

Operating Range:	0 to 55 °C (32 to 131 °F)
Storage Range:	-20 to 80 °C (-4 to 176 °F)
Humidity:	10 to 90%, non-condensing

Switches

Power:	on/off
Manual Trigger:	when pressed forces a trigger event

LEDs

Power (PWR):	illuminated when the analyzer is powered on.
Recording (REC):	illuminated when the analyzer is actively recording traffic data.
Triggered (TRG):	illuminated during power-on testing, and when the analyzer has detected a valid trigger condition.
Synchronized (SYNC):	flashes during acquisition of the traffic hop sequence, illuminated when the analyzer is locked to the hop sequence.

Recording Memory Size

128M x 8-bit DRAM for traffic data capture, timing, state and other data.

Certification

FCC (Class A), CE Mark, CSA

2. Quick Installation

The Merlin Protocol Analyzer components and software are easily installed and quickly ready to run on most Windows-based personal computer systems. You can begin making Bluetooth™ recordings after following these initial steps. However, if you are new to personal computers and protocol analyzers, or if you are unsure about what to do after reading the Quick Installation instructions, or if your analyzer does not work after you follow these instructions, read through the subsequent sections in this manual.

2.1 Setting Up the Analyzer

Step 1 Attach the Antenna to the ANT connection point. The antenna should point up.

Step 2 Connect the AC power cable to the rear of the analyzer.

Step 3 Turn on the power switch on the rear of the analyzer.

Step 4 Insert the first Merlin diskette (Disk 1 of 2) into your analyzing PC floppy disk drive.

Step 5 Connect the USB cable between the USB port on the back of the analyzer and a USB port on the analyzing PC.

Step 6 Follow Windows on-screen Plug-and-Play instructions for the automatic installation of the Merlin Analyzer as a USB device on your analyzing PC (the first Merlin diskette includes the required USB files).

2.2 Installing the Software

Step 1 Run the program **a:\setup** and follow the on-screen instructions to install the Merlin application on the analyzing PC hard disk.

Step 2 To start the application, launch the **CATC Merlin** program from the **Start Menu: Start>Programs>CATC>Merlin**.

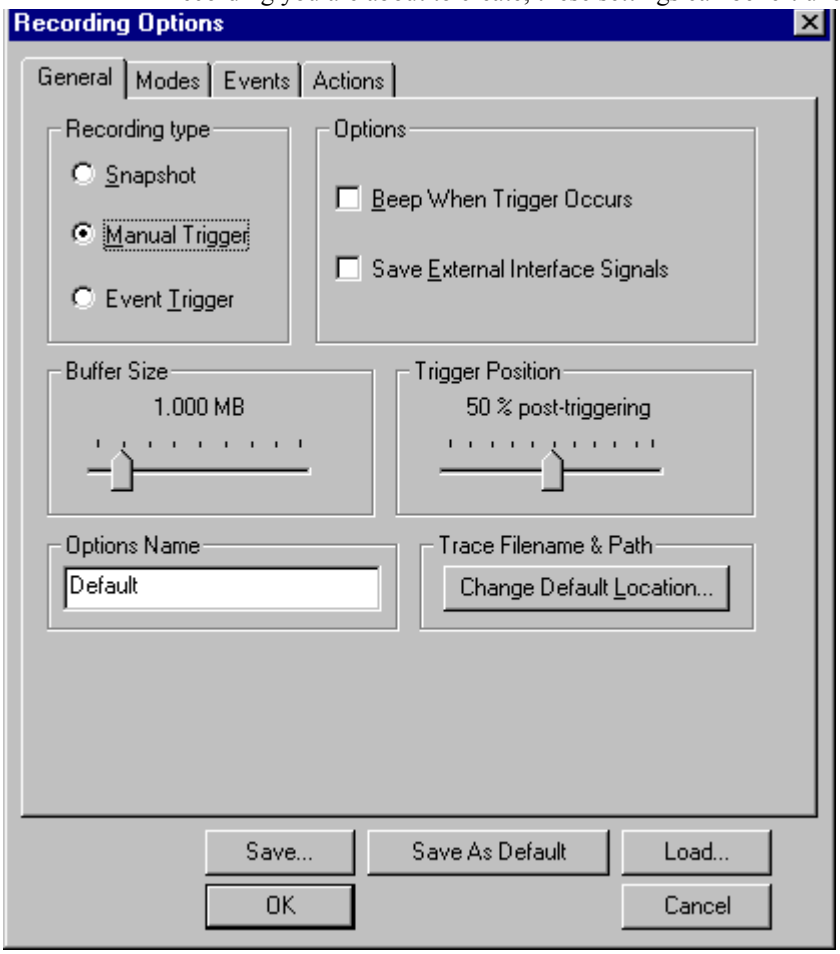
2.3 Your First Bluetooth™ Recording

After installing and launching the software, you can test Merlin by creating a recording of a General Inquiry. In this test, Merlin will issue a General Inquiry that asks local devices to identify themselves. Merlin then records the responses.

Step 1 Select **Recording Options** under **Setup** on the Menu Bar.

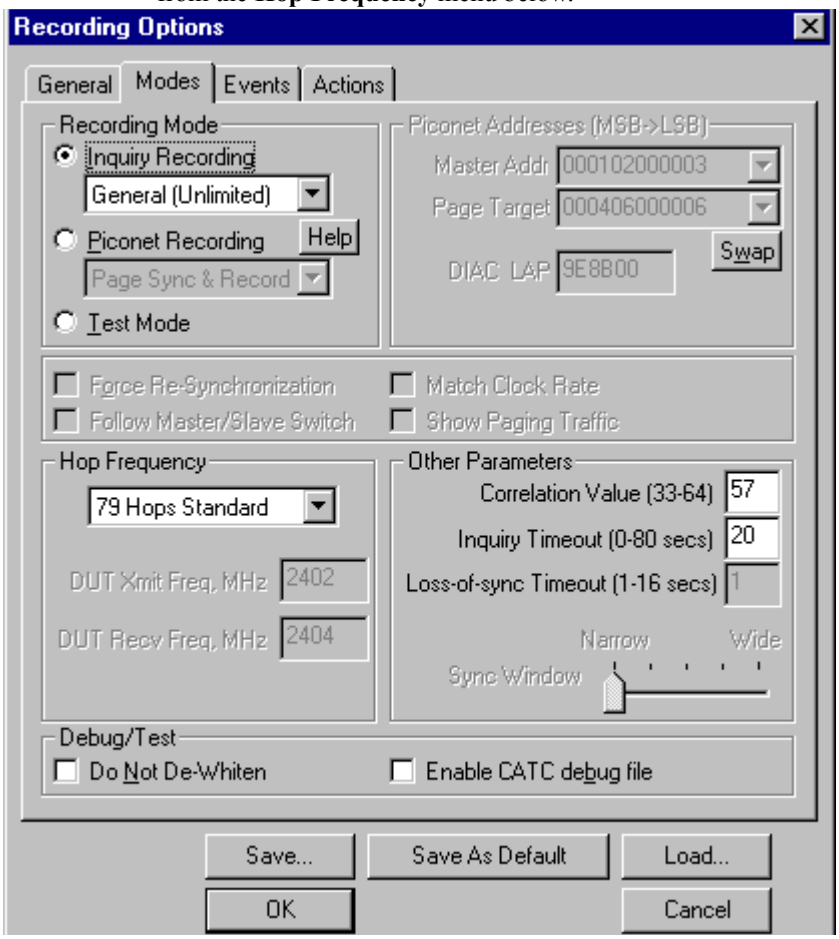
Step 2 Select the **General** tab.

The following dialog box will open showing factory default settings such as "manual trigger" and 1 Mbytes buffer size. For the General Inquiry recording you are about to create, these settings can be left unchanged.



Step 3 Select the **Modes** tab.

The following dialog box will open showing factory default settings. Merlin defaults to "**General Inquiry**." For this recording, leave most of these settings unchanged. If you are recording a Hop Frequency that is not **79 Hops Standard**, you will need to select the appropriate standard from the **Hop Frequency** menu below.



Step 4 Click OK to activate the recording options you selected.

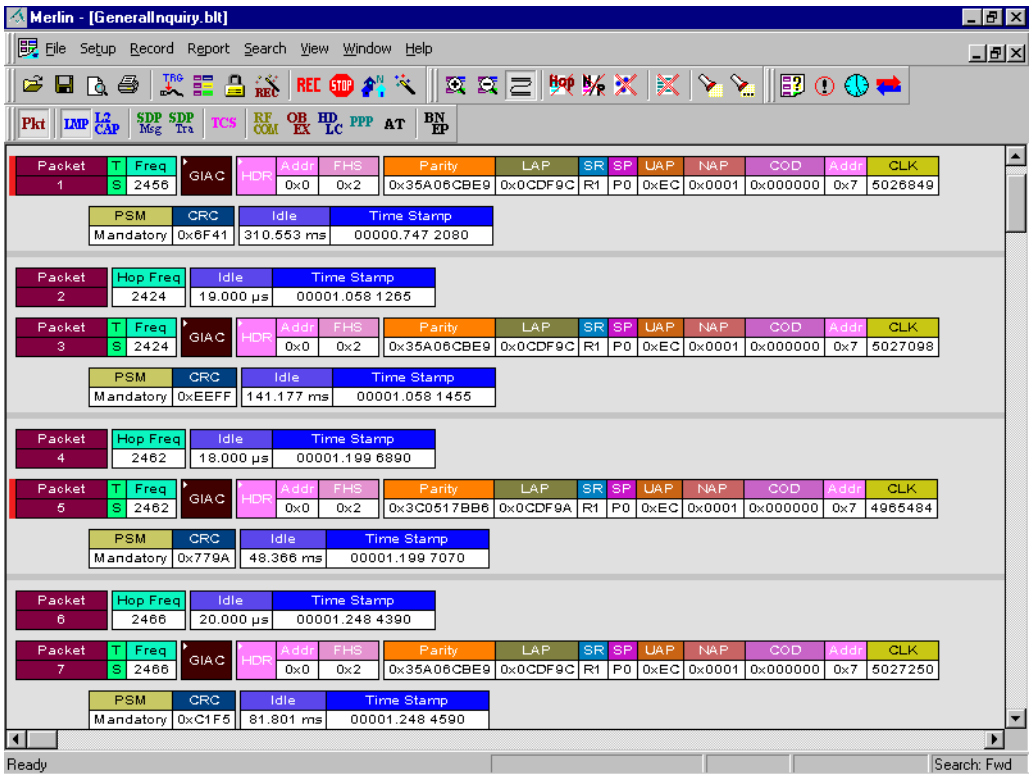
At this point, Merlin will be ready to record.

Step 5 Click REC on the Tool Bar.

Merlin starts to record the Bluetooth™ traffic immediately. The Bluetooth™ Inquiry process will proceed for 20 seconds. After 20 seconds has elapsed, the analyzer uploads the data and displays the packets.

Step 6 If you wish to terminate the recording before the snapshot automatically completes, click STOP on the Tool Bar.

After a few moments, the recording will terminate and the results will display. The screen should look like the sample recording below which shows the FHS packets generated during the Inquiry process.



When the recording session is finished, the bus traffic is saved to the hard drive as a file named **data.blt** or whatever name you assign as the default filename. While the file is being saved, you should see a brown progress bar at the bottom of the screen. When the bar turns white, it indicates that the data has been saved to disk.

Step 7 To save a current recording for future reference, Select **Save As** under **File** on the Menu Bar.

OR

Click on the Tool Bar.

You see the standard **Save As** screen.

Step 8 Give the recording a unique name and save it to the appropriate directory.

3. Detailed Installation

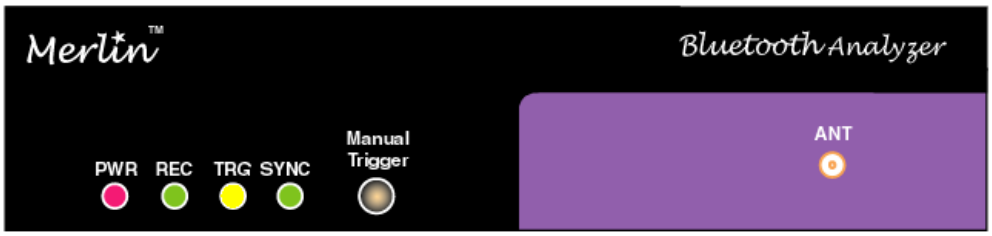
3.1 System Components/Packing List

- One stand-alone Merlin Analyzer module
- One Antenna
- One External Interface Breakout Board with a 9-pin ribbon cable
- One 6-foot (2-meter) USB cable
- Merlin software program installation diskette(s)
- Product documentation

3.2 The Installed Merlin Unit

The Merlin Analyzer has several user-accessible controls and LEDs on its front and rear panels of the OmniBus.

Figure 1: Front Panel

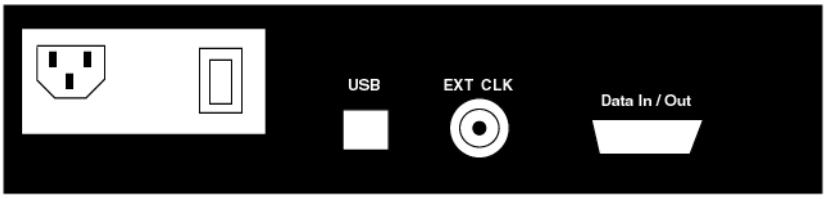


- Red **PWR** (power) indicator LED (lights when the unit power is switched on).
- Green **REC** (recording) LED (lights when the unit is recording).
- Yellow **TRG** (triggered) LED (lights when the unit triggers an event).

Note TRG also lights during power-on testing and will be turned off at the end of the power on cycle. If the LED blinks at the end of this cycle, the hardware is faulty.

- Green **SYNC** (synchronized) LED (lights when the unit is locked onto a specific piconet, based on the Master Address).
- **Manual Trigger** push-button (allows a manual Trace capture)
  - After beginning a recording session, press the **Manual Trigger** switch to force a Trigger condition. The session completes when a specified post-Trigger amount of bus data is recorded or when you manually stop a recording session.
- **ANT** Bluetooth™ Antenna connector

Figure 2: Rear Panel



- Wide range AC connector module
  - — Power socket
  - — Enclosed 5x20 mm 2.0A 250 V fast acting glass fuse

Warning: For continued protection against fire, replace fuse only with the type and rating specified above.

  - — Power on/off switch
- External Clock (**EXT CLK**) input for future enhancement (Note: THIS PORT IS NOT USED)
- USB type "B" host computer connector
- **Data In/Out** DB-9 (9-pin) external interface connector

Warning: Do not open the Merlin Analyzer enclosure. There are no operator servicable parts inside. Refer servicing to CATC.

3.3 Merlin System Setup

The Merlin Analyzer is designed to work with either desktop or laptop computers equipped with a functional USB interface. To set up the system hardware,

- Attach the Antenna to the ANT connector. Set the antenna to point up.
- Connect the Analyzer to an AC power source.
- Connect the External Interface Breakout Board to the **Data In/Out** connector (optional).
- Connect to the analyzing PC via USB.

3.4 AC Power Source

Step 1 Connect the Analyzer box to a 100-volt to 240-volt, 50 Hz to 60 Hz, 100 W power outlet using the provided power cord.

Note The Analyzer is capable of supporting supply voltages between 100-volt and 240-volt, 50 Hz or 60 Hz, thus supporting all known supply voltages around the world.

Step 2 Use the power switch located on the rear panel to turn the analyzer unit on and off.

Note At power-on, the analyzer initializes itself in approximately ten seconds and performs an exhaustive self-diagnostic that lasts about five seconds. The Trigger LED illuminates during the power-on testing and turns off when testing is finished. If the diagnostics fail, the trigger LED blinks continuously, indicating a hardware failure. If this occurs, call CATC Customer Support for assistance.

3.5 External Interface Breakout Board

The External Interface Breakout Board is an accessory that allows convenient access to several potentially useful standard fast TTL output and input signals. It also offers a simple way to connect logic analyzers or other tools to the Merlin Analyzer unit. Four ground pins and one 5-volt pin are provided.

The Breakout Board connects via a ribbon cable to the **Data In/Out** connector located on the rear of the analyzer box. Each pin is isolated by a 100Ω series resistor and a buffer inside the Analyzer box.

Figure 3: Data In/Out Connector

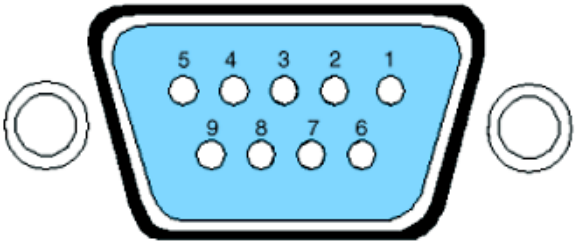


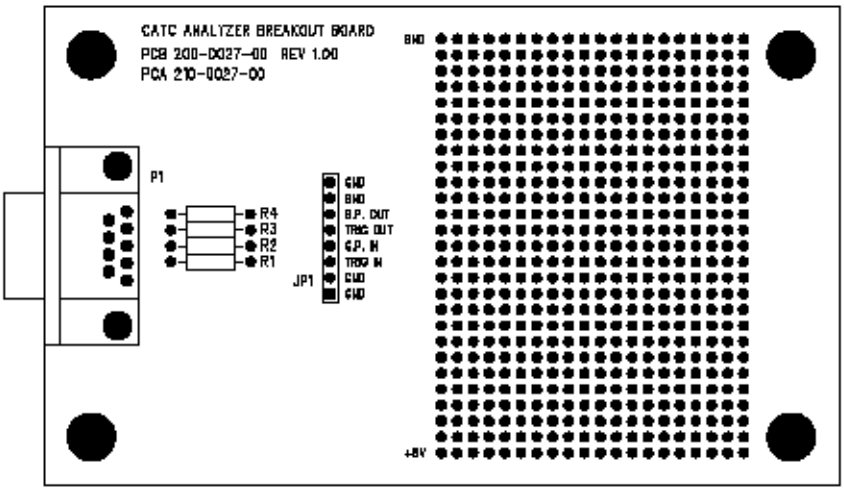
Table 1 lists the pin-out and signal descriptions for the **Data In/Out** connector.

Table 1: Data In/Out Connector – Pin-Out

Pin	Signal Name	Signal Description
1	+5V	+5 Volts, 250mA DC source
2	TRG IN	Trigger Input
3	GP IN	General Purpose Input
4	TRG OUT	Trigger Output
5	GP OUT	General Purpose Output

Pin	Signal Name	Signal Description
6	GND	Ground
7	GND	Ground
8	GND	Ground
9	GND	Ground

Table 2: External Interface Breakout Board



Breakout Board External Output Signalling Pins

The "TRG OUT" and "G.P. OUT" pins found on the Analyzer's Breakout Board have similar functions. Both pins serve to transmit output signals when a trigger event occurs. The main differences between the two pins is in the number of signals that the Analyzer will send through them (TRG OUT will transmit just one signal whereas G.P. OUT may transmit several sequential signals), and in their initial state (TRG OUT is always enabled by the Analyzer whereas G.P. OUT must be enabled in the recording options before it can be utilized).

TRG OUT

When an event trigger occurs, TRG OUT transitions from ground to a continuous 5 V signal on the first instance of a trigger event. TRG OUT is a one-time event: it will not re-signal or change signals with subsequent triggering events. When this first trigger event occurs, the Trigger LED will illuminate (so this pin can be thought of as a reflection of the state of this LED).

G.P. OUT

G.P. OUT needs to be enabled before it will output signalling. See "Blue Dot Menus for the Event Buttons" on page 84 for details on how to enable output signalling.

If enabled, G.P. OUT will provide signalling each time a trigger event is detected by the Analyzer. G.P. OUT's signalling can be set to three different formats - "Pulse High" provides a 16.66 ns (ground to +5V) signal, "Pulse Low" a 16.66 ns (+5 V to ground) signal or "Toggle", a signal with an initial High (+5V) state that alternates with each trigger event between continuous High (+5 V) and continuous Low (Ground). "Pulse High" is the default condition. To change the format, see "Enabling High Pulse, Low Pulse or Pulse Toggle Signal Outputs" on page 84 for details.

Prototype Rework Area

The Breakout Board contains a prototype rework area for making custom circuits for rapid development. The area consists of plated-through holes, 20 columns wide by 27 rows long. The top row of holes is connected to GND and the bottom row is connected to +5V. The remaining holes are not connected. Use the rework area to insert custom components and wire-wrap their respective signal, power, and ground pins.

3.6 PC Connection

Use the USB cable provided to connect the host computer to the Merlin Analyzer.

3.7 Antenna Information

According to the Bluetooth™ specifications, Bluetooth™ Antennas should be placed at least 10 cm apart. It is recommended that Merlin be placed at least 1 meter away from the nearest device in the piconet under observation.

3.8 Analyzer PC Requirements

- USB connection to the computer (unless using the PC only as a viewer)
- Microsoft Windows 98, Windows 98SE, Windows ME, Windows 2000, or Windows NT 4.0 for recording and viewing traffic

Note If installing Merlin software on a Windows NT 4.0 system, you will need a special diskette that is available from CATC.

- Minimum of 16MB physical RAM; 32 MB recommended for viewing transactions
- At least 10 MB hard disk space, plus additional memory for recordings (as much as 200MB when recording a full buffer size)
- Monitor resolution at least 800x600 with thousands of colors

3.9 Merlin Program Installation

The CATC Merlin software is provided on three 3½ inch diskettes and requires a Windows 98, Windows 98SE, Windows 2000 or Windows ME operating system. If you are loading Merlin onto Windows NT 4.0 you will get separate disk and instructions.

You would first need to install Merlin as a USB device and then install the Merlin Windows application program.

Loading the Merlin USB Drivers

Step 1 Insert the Merlin program floppy for your operating system labeled **Disk 1 of 3** into the **a:** drive.

Step 2 Power-on the Merlin Analyzer.

Step 3 Connect the USB cable to the rear of the analyzer and to the personal computer.

The host operating system detects the analyzer and begins to install the USB driver.

Step 4 Follow the installation instructions provided on your screen to complete the installation of the driver.

Note When Windows prompts you for a file, browse to the CATC floppy in the **a:** drive.

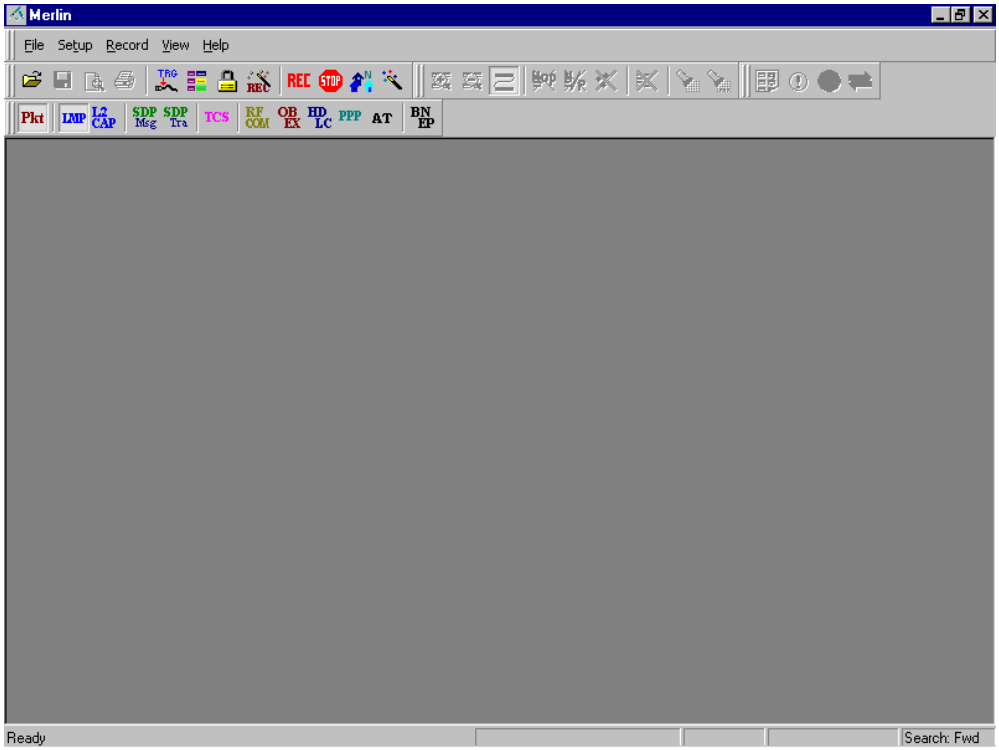
Installing the Merlin Application Program

Run **Setup.exe** from the Merlin floppy disk 1 of 3.

The CATC Merlin Install Wizard automatically installs the necessary files to the computer's hard drive. Merlin software is installed in the **C:\Program Files\CATC\Merlin** directory unless you specify otherwise. Follow the installation instructions on your screen.

3.10 Merlin Program Startup

You can start the Merlin program from the Desktop or from the installed directory. The program always begins with its main screen active:



The software may be used with or without the analyzer box. When used without an analyzer box attached to the computer, the program functions in a Trace Viewer mode to view, analyze, and print captured protocol traffic.

When the program is used with the Merlin Protocol Analyzer attached to the computer, you can set trigger conditions, record, monitor and analyze the activity of your Bluetooth™ device or piconet.

3.11 Making a Recording

After installation, the software is configured to make a manual recording ("Manual Trigger") of General Inquiry traffic.

To make your first recording of this traffic,

Step 1 Click REC on the Tool Bar.

After 20 seconds, Inquiry timeout occurs and the analyzer will upload the data and display the packets.

To terminate the recording before Inquiry timeout occurs,

Step 2 Click STOP on the Tool Bar at any time before recording automatically terminates.

When the recording session is finished, the traffic is saved to the hard drive as a file named **data.blt** or whatever name you assign as the default filename.

To save a current recording for future reference,

Step 3 Select **Save As** under **File** on the Menu Bar.

OR

Click on the Tool Bar.

You see the standard **Save As** screen.

Step 4 Give the recording a unique name and save it to the appropriate directory.

4. Upgrades

From time to time as modifications are made to Merlin, it is necessary to update the Firmware and/or BusEngine for optimal performance. Upgrades can be performed two ways: either automatically or manually. This chapter describes both procedures.

4.1 Software, Firmware, and BusEngine Revisions

The **Readme.txt** file on the first installation disk and in the installed directory gives last-minute updates about the current release. Included with each release are the most recent downloadable images of the Firmware and the BusEngine. The **Readme.txt** file lists the latest versions and informs you if new Firmware or a new BusEngine needs to be updated in your hardware.

Once the Analyzer has completed the self diagnostics and is connected to the PC, you can check the latest revision of the software and BusEngine:

- Selecting **About Merlin…** in the Help Menu.

  You see this screen:

About Merlin details revisions of the following software and hardware:

- Merlin Software Version
- Merlin Firmware Version
- BusEngine Version
- Unit Serial Number

Note When contacting CATC for technical support, please have available all the revisions reported in the **About Merlin** window.

4.2 Software Upgrades

When a new software release is available, it is posted on the Support page of the CATC website at **www.catc.com/support.html**.

To update the software,

Step 1 In the **About Merlin** screen, verify which version of Merlin Software you are currently running.

Step 2 Find the latest released software version on the CATC website under **Support**.

If you are running the latest version of the software, no further action is needed.

If you are **not** running the latest version, continue to Step 3.

Step 3 Click on the first link to download the zipped Disk 1 files for your operating system.

Step 4 Click on the second link to download the zipped Disk 2 files.

Step 5 Unzip the files into your choice of directory.

Step 6 Click **Start**, then **Run**, and browse to where you unzipped the files.

Step 7 Select the program named **Setup** and click **Open**.

Step 8 Click **OK** to run the Setup and begin the installation.

Step 9 Follow the on-screen instructions to complete the installation.

Step 10 Read the Readme file for important information on changes in the release.

4.3 BusEngine and Firmware Upgrades

BusEngine and Firmware upgrades often need to be performed when you update the Merlin software. These upgrades can be performed automatically or manually. Both processes are described.

Automatic Upgrades

When Merlin's software is upgraded, the software may become incompatible with the BusEngine and Firmware. If a recording is attempted, Merlin will display an error message and then automatically

begin an upgrade process for the BusEngine and Firmware. If you prefer, you can abort this upgrade and undertake the steps manually as described later in this chapter.

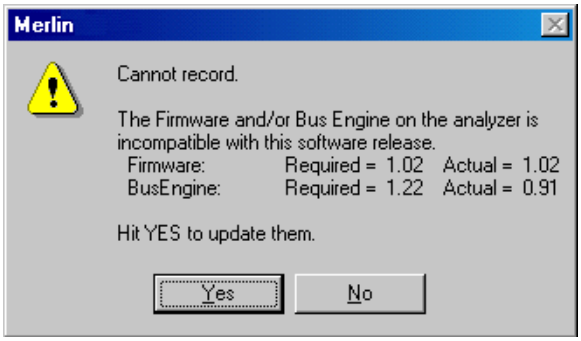
To perform an automatic BusEngine and Firmware upgrade,

Step 1 If needed, upgrade the Merlin software using the steps outlined in "Software Upgrades" described above.

Step 1 Turn on the Analyzer.

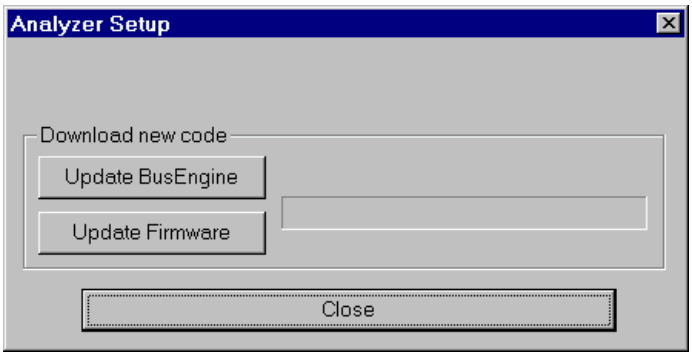
Step 2 On the toolbar, click the REC button.

Since the BusEngine and/or the Firmware are incompatible with the current Merlin software version, an error message will appear displaying your current versions and indicating what versions you need to install.



Step 3 Click Yes.

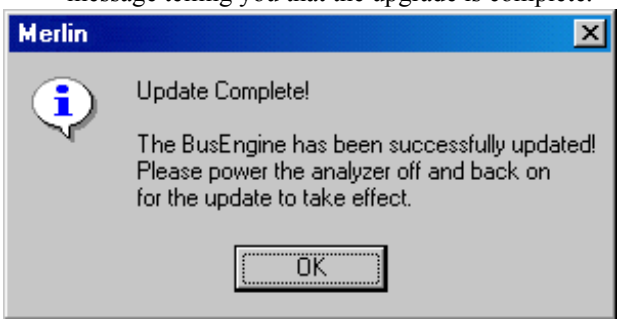
The above window closes and the Analyzer Setup window opens.



Step 4 Click **Update BusEngine** or **Update Firmware** on the **Analyzer Setup** screen.

You can select only one item at this point. If both the BusEngine and the Firmware need to be updated, the upgrade will complete for the first item and then return to the above screen so the second upgrade can be performed.

When the second upgrade has finished, you will see the following message telling you that the upgrade is complete.



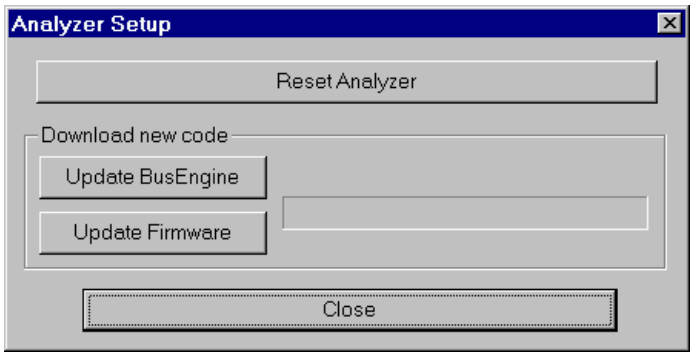
Step 5 Power cycle Merlin to complete the upgrade.

Manual Upgrades to BusEngine and Firmware

You can manually upgrade Merlin's Firmware and/or BusEngine by performing the following steps:

Step 1 Select **Analyzer** under **Setup** on the Menu Bar.

You see the **Analyzer Setup** screen:



Step 2 Click **Reset Analyzer**

The Analyzer resets, performs self-diagnostics, and returns to service.

Note The self-diagnostics should complete about five seconds after the trigger LED lights. If the diagnostics fail, the trigger LED blinks on and off continually, indicating faulty hardware. If this occurs, contact CATC for customer support.

Upgrading the BusEngine

The BusEngine core is the heart of the Merlin Analyzer. Using state-of-the-art PLD technology, it incorporates both the high speed recording engine and the configurable building blocks that implement data/state/error detections, triggering, capture filtering, external signal

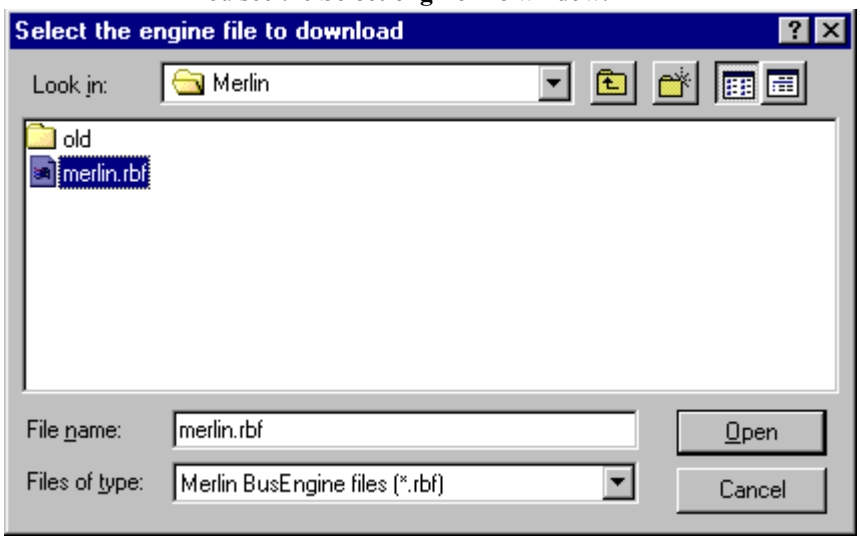
monitoring, and event counting and sequencing. Both the BusEngine program and the Firmware that manages the internal microcontroller are fully field upgradeable.

Within a new software release, it may be necessary to update the Analyzer's BusEngine hardware for proper operation. The Readme file lets you know if this is necessary.

To update the BusEngine,

Step 1 Click **Update BusEngine** on the **Analyzer Setup** screen.

You see the **Select engine file** window:



The program has already automatically searched for the correct file and displays it in the **File name** field.

Note The most current Primary BusEngine file (**Merlin.rbf**) was copied to your **\CATC\Merlin** directory when you installed the program.

Step 2 Click **Open**.

It is not necessary to restart the Analyzer. Once upgraded, the Analyzer takes approximately 15 seconds to reinitialize, with **Time Remaining** displayed on the screen. During this time the Trigger LED is on, indicating that power-on diagnostics are being run. If there is a hardware failure, the Trigger LED continues to blink after initialization is complete. If this occurs, contact CATC for customer support.

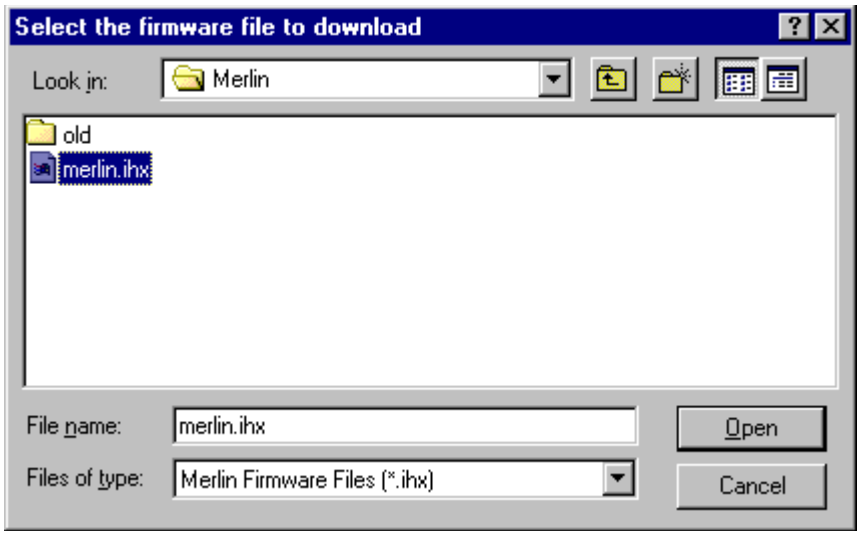
Upgrading the Firmware

Within a new software release, it may also be necessary to upgrade the Analyzer's firmware for proper operation. The Readme file informs you if this is necessary.

To upgrade the firmware,

Step 1 Click **Upgrade Firmware** on the **Analyzer Setup** screen.

You see the **Select firmware file** window:



The program has already automatically searched for the correct file and displays it in the **File name** field.

Step 2 Click **Open**.

The Analyzer upgrades the Firmware.

Step 3 Unplug the USB cable from the back of the Analyzer box and then reinsert it so the new Firmware upgrade can take effect.

5. Software Overview

5.1 The Main Display Windows

While some of the analyzer's Main Display window options are familiar, many contain options specific to the analyzer program.

Table 3: Main Display Pull-Down Windows

Menu	Function
File	
Open…	Opens a file
Close	Closes the current file
Save As…	Saves all or a specified range of packets from the current file with a specified name
Print…	Prints part or all of the current traffic data file
Print Preview	Produces an on-screen preview before printing
Print Setup…	Sets up your current or new printer
Edit Comment…	Creates or edits the Trace file comment field
Export » Packets to Text (Packet View Format)	Saves all or part of a trace to a text file or to a Comma Separated Values (CSV) file suitable for viewing in a spreadsheet application
Export » Packets to CSV Text	Saves all or part of a trace to a Comma Separated Values (CSV) file suitable for viewing in a spreadsheet application
Last File	Lists the last files that were opened
Exit	Exits the Merlin program
Setup	
Display Options…	Provides the control of various display options such as color, formats, and filters.
Recording Options…	Provides setup options for recording, triggering events and filtering events.
Encryption Options ...	Allows a pin code to be assigned to a device to facilitate encryption decoding.
Recording Wizard ...	Starts a sequence of interactive dialog boxes that configures Merlin for a recording. This utility provides an alternative to the Recording Options dialog box.
Analyzer…	Allows the operator to reset the Analyzer or update the BusEngine and Firmware.
Record	
Start	Causes the Analyzer to begin recording Bluetooth™ activity.
Stop	Causes the Analyzer to stop recording.
Inquiry » General	Analyzer initiates General Inquiry to all devices within range and records response packets.
Inquiry » Dedicated	Analyzer initiates inquiry to a class or group of devices specified by the DIAC LAP text box under the Modes tab in Recording Options dialog.

Menu	Function
Piconet » Sync & Record	Used when the Bluetooth™ devices under observation have not established connection.
Piconet » Passive Sync & Record	Used when Bluetooth™ devices under observation are already connected.
Piconet » Page Sync & Record	This mode causes Merlin to perform a General Inquiry and collect sync data from the specified slave device. "Page Sync & Record" is the recommended method of recording. Use this mode when the devices under observation have not established connection.
Test Mode	Allows Merlin's Hop Frequency to be set.
Report	
File Information	Details such information about the recording as number of packets and triggering setup.
Error Summary	Displays an error summary of the current trace file and allows you to go to a specific packet, and save the error file to a uniquely named file.
Timing Calculation	Starts the calculator dialog for calculating various timing and bandwidth parameters in the recording file.
Traffic Summary	Details the number and type of packets were transferred during the recording, as well as message-level statistics.
Search	
Go to trigger	Positions the display to show the first packet that follows the trigger event.
Go to Packet/Message/ Protocol ...	Positions the display to the indicated packet, LMP/L2CAP message, or Protocol Message (RFCOMM, TCS, or SDP protocols).
Go to Marker »	Positions the display to a previously marked packet
Go to »	Enables quick searching for specific events using a cascade of pop-up windows.
Error	Positions the display to the next hard error.
Soft Bit Error	Positions the display to the next soft bit error. A Soft Bit error is an error that is correctable though the Merlin software.
Loss of Sync	Allows searching for loss of sync.
Find	Allows complex searches.
Find Next	Repeats the previous Find operation. Can also use F3 to find next.
Search Direction	Allows you to specify a forward or backward search of a trace file.
View	
Toolbars	Displays list of available toolbars.
Status Bar	Switches display of the Status Bar on or off.
Zoom In	Zoom in increases the size of the displayed elements.
Zoom Out	Zoom out decreases the size of the displayed elements.
Wrap	Allows the display to wrap.

Menu	Function
BT Neighborhood	Displays Bluetooth™ Address and clock frequency for devices in range. The expected Bluetooth™ clock frequency is 3200 Hz +/- 250 ppm.
Decoding Assignments	Displays current decoding assignments and provides options for changing them.
L2CAP connections	Displays current L2CAP connections and provides options for changing them.
RFCOMM Channel Assignments	Displays current RFCOMM Channel Assignments and provides options for changing them.
Window	
New Window	Switches display of the Tool Bar on or off.
Cascade	Displays all open windows in an overlapping arrangement.
Tile	Displays all open windows in a side-by-side arrangement.
Arrange Icons	Arranges minimized windows at the bottom of the display.
Windows	Displays a list of open windows.

Help	
Help Topics	Displays online help.
About Merlin	Displays version information about Merlin.

5.2 View Options

The View feature in the Menu Bar allows you to

- Control the display of the Tool Bar and the Status Bar.

Tool Bar

The Tool Bar provides access to the most popular program functions. Tool tips describe icon functionality as the mouse arrow is moved over the icon/item.

Open file

Save As

Preview

Hide Nulls & Polls

Hide Unassociated Traffic

Complex Find

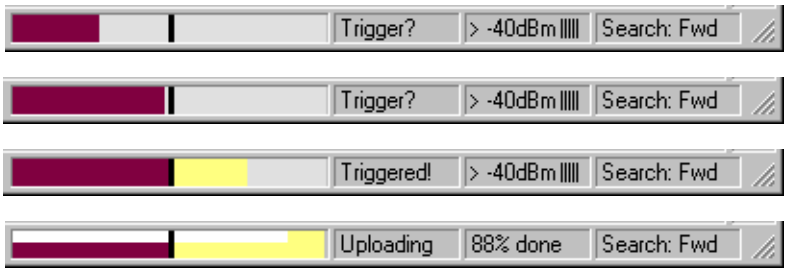
	Print…		Find Next
	Setup Record Options		File Information Report
	Setup Display Options		Traffic Summary
	Start Recording		View Packet Level (Baseband)
	Stop Recording		View/Hide LMP Message Level
	Bluetooth Neighborhood		View/Hide L2CAP Message Level
	Setup Encryption Options		View/Hide SDP Message Protocol Level
	Recording Wizard		View/Hide SDP Transaction Protocol Level
	Zoom In		View/Hide TCS Protocol Level
	Zoom Out		View/Hide RFCOMM Protocol Level
	Wrap		View/Hide OBEX Protocol Level
	Hide Frequency Hops		View/Hide AT Commands
	Error Summary		View/Hide PPP
	Timing Calculations		View/Hide HDLC Protocol
			View/Hide BNEP Protocol

5.3 Status Bar

The Status Bar is located at the bottom of the main display window. Depending on the current activity, the bar can be divided into as many as four segments.

Recording Progress

When you begin recording, the left-most segment of the Status Bar displays a Recording Progress Indicator:



As recording progresses, the Progress Indicator changes to reflect the recording progress graphically:

- In the Progress Indicator, a black vertical line illustrates the location of the Trigger Position you selected in Recording Options.
  - Pre-Trigger progress is displayed in the field to the left of the Trigger Position in the before-Trigger color specified in the Display Options.
  - When the Trigger Position is reached, the progress indicator wiggles as it waits for the trigger.
  - After the trigger occurs, the field to the right of the Trigger Position fills in the post-Trigger color specified in the Display Options.
  - When recording is complete, the upper half of the progress indicator fills in white, indicating the progress of the data upload to the host computer.

You should be aware of two exceptional conditions:

- If a Trigger Event occurs during the before-Trigger recording, the before-Trigger color changes to the after-Trigger color to indicate that not all the expected data was recorded pre-Trigger.
- When you click **Stop** before or after a Trigger Event, the Progress Bar adjusts accordingly to begin uploading the most recently recorded data.

The Progress Bar fills with color in proportion to the specified size and actual rate at which the hardware is writing and reading the recording memory. However, the Progress Indicator is normalized to fill the space within the Status Bar.

Recording Status

During recording activity, the current Recording Status is temporarily displayed in the next segment. When you activate the **Record** function, this segment flashes one of the following messages (depending on the selected Recording Options):

— Trigger?

— Triggered!

— Uploading

After recording stops,

— The flashing message changes to **Uploading data–*x*% done** (**x%** indicates the percentage completion of the data uploading process).

— The traffic data is copied to disk (overwriting any previous version of this file) using the default file name **data.blt** or a new name specified in the Recording options.

To abort the upload process,

- Press **Esc** on your keyboard

  OR

  Again click in the Tool Bar.

  You are prompted to choose whether to keep the partially uploaded data or to throw it away.

When the data is saved, the Recorded Data file appears in the main display window and the Recording Status window is cleared.

- If the recording resulted from a Trigger Event, the first packet following the Trigger (or the packet that caused the Trigger) is initially positioned second from the top of the display.
- If the recording did not result from a Trigger Event, the display begins with the first packet in the traffic file.

Analyzer Status

The third segment in the status bar displays analyzer status. During synchronization, the analyzer status will read:

Inquiring – Merlin is conducting a General Inquiry

Syncing – Merlin is syncing to the Master device

No Sync – Merlin has not yet started syncing to the Master device

After the analyzer has synchronized to the Bluetooth™ piconet under observation, the Status Bar will display activity bars. The activity bars will increase or decrease with activity. If there are no vertical bars, there is no recorded activity.

During uploading, this segment displays the percent of the upload process completed.

Note If packets are filtered from the recording or data are truncated, the recording activity is reduced.

In addition to showing activity, the third segment of the Status Bar will also display the radio signal strength in dBm received by the analyzer. Merlin can display five possible values:

- below -60 dBm
- - 60 dBm
- - 50 dBm
- - 40 dBm
- above - 40 dBm

The valid range for a signal is between -70 and - 20 dBm.

Search Status

The rightmost segment displays the current search direction: **Fwd** (forward) or **Bwd** (backward).

Zoom In

Zoom In increases the size of the displayed elements, allowing fewer (but larger) packet fields per screen.

- Click on the Tool Bar.

Zoom Out

Zoom Out decreases the size of the displayed elements, allowing more (but smaller) packet fields per screen.

- Click on the Tool Bar.

5.4 Tool Tips

Throughout the application, tool tips provide useful information.

To display a tool tip, position the mouse pointer over an item. The tool tip displays in a short moment if present. Tool tips can also be found over the Tool Bar and in areas of the packet view screen.

5.5 Merlin Analyzer Keyboard Shortcuts

Several frequently-used operations are bound to keyboard shortcuts.

Table 4: Keyboard Shortcuts

Key Combination	Operation	Key Combination	Operation
Ctrl+O	Open file	Ctrl+P	Print...
Ctrl+Home	Jump to First packet	Ctrl+End	Jump to Last packet
Ctrl+F	Search Forward	Ctrl+B	Search Backward
F3	Find Next	Ctrl+L	Search for Loss of Sync
Shift+I	Goto ID packet	Shift+R	Goto Freq Hop packet
Shift+P	Goto Poll packet	Shift+N	Goto Null packet
Shift+M	Goto DM1 packet	Shift+F	Goto FHS packet
Shift+1	Goto HV1 packet	Shift+H	Goto DH1 packet
Shift+3	Goto HV3 packet	Shift+2	Goto HV2 packet
Shift+A	Goto AUX1 packet	Shift+V	Goto DV packet
Shift+5	Goto DH3 packet	Shift+4	Goto DM3 packet
Shift+7	Goto DH3 packet	Shift+6	Goto DM5 packet
Shift+S	Search for Soft Error	Shift+E	Search Error

6. Recording Wizard

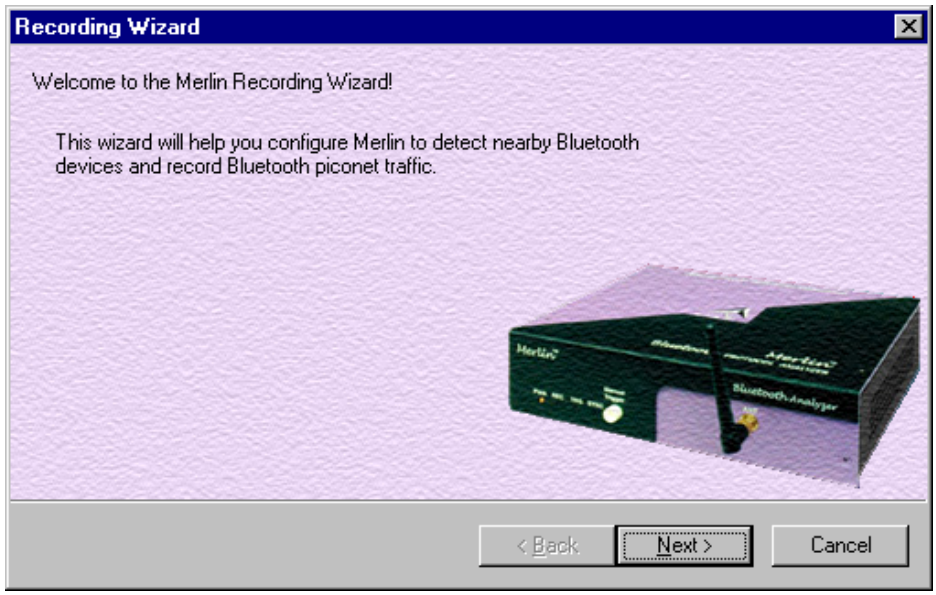
Recording Wizard is an interactive utility that presents a series of user-friendly dialog boxes for setting up a recording session. Recording Wizard serves as an alternative method of configuring the Recording Options dialog box - in fact, when you finish using the Wizard you can see that your settings are . By providing data to the prompts in the Wizard's dialog boxes, you configure Merlin for a recording session.

Starting Recording Wizard

To start the **Recording Wizard**,

- Click on the Tool Bar or select **Recording Wizard** under **Setup** on the Menu Bar.

You see the **Recording Options** window:

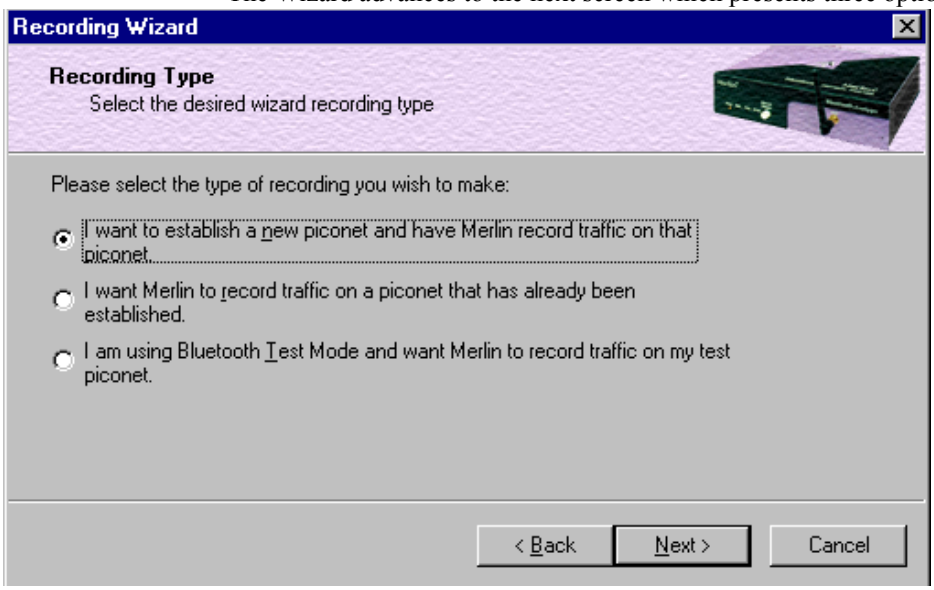


The **Recording Options** window has three buttons marked **Next**, **Back**, and **Cancel** that allow you to move forward or backward through the wizard or to cancel the wizard.

To begin advancing through the wizard,

- Click **Next** to see the options for the three types of recordings that the Recording Wizard can make.

The Wizard advances to the next screen which presents three options:



- **Establish a new piconet and have Merlin record traffic on that piconet.**

  This option causes Merlin to perform an Inquiry so it can discover local devices and then establish a new piconet and record the piconet traffic.

- **Record traffic on a piconet that has already been established.**

  This option lets Merlin record traffic from an already established piconet.

- **Record traffic in Test Mode on a test piconet.**

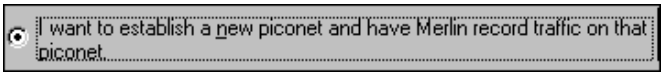
  This option lets Merlin create either a single frequency range recording of a range that you specify or create a recording of a limited hop frequency range consisting of 5 frequency hops.

6.1 Recording a Traffic on a New Piconet

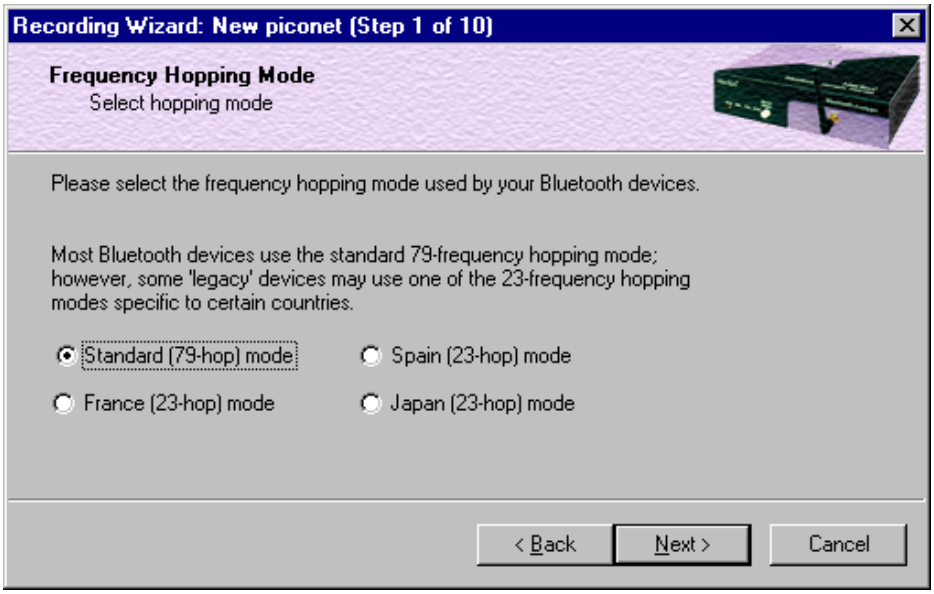
The **New Piconet** option shown in the previous screen presents users with the means of recording the traffic from a new piconet. This option will cause a sequence of screens to prompt you for information such as the piconet Master address.

The following steps shows you how to configure Merlin to record a new piconet.

Step 1 From the screen shown in the previous screenshot, select the first option: **I want to establish a new piconet and have Merlin record traffic on that piconet**, then press **Next**.

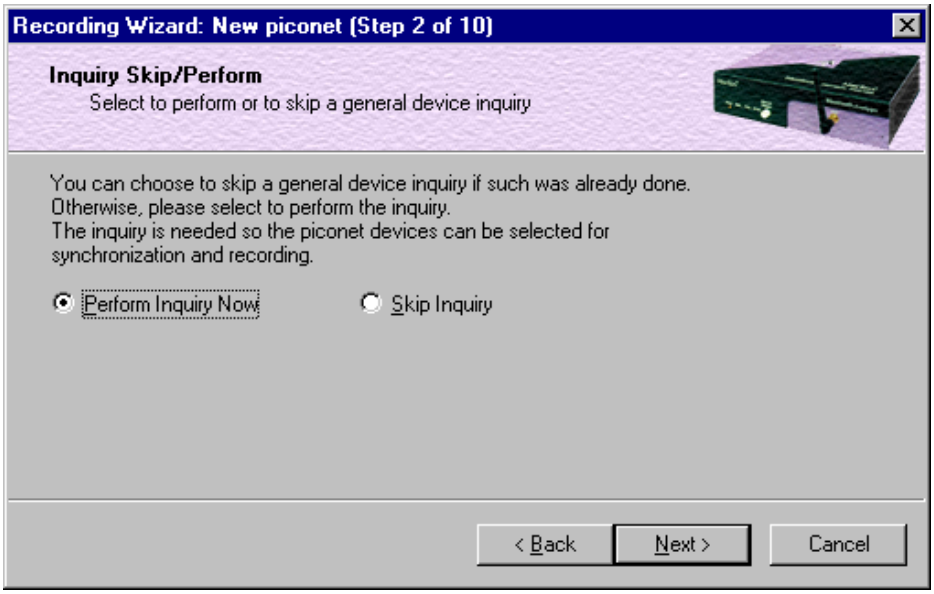


The following screen displays.



Step 2 Select the **Frequency Hopping Mode** for your country, then press **Next**.

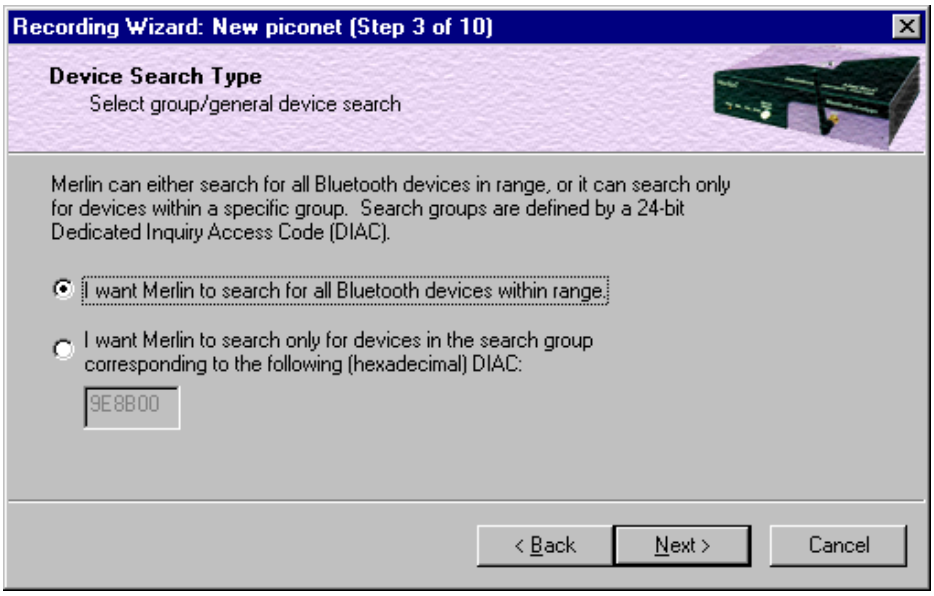
The following screen displays.



Step 3 Select **Perform Inquiry Now**, then press **Next**.

Selecting **Perform Inquiry Now** will cause Merlin to perform a General Inquiry and collect addresses and other details about local Bluetooth devices. If you already have address information for your Bluetooth devices you can choose **Skip Inquiry**. Choosing **Skip Inquiry** will cause the Recording Wizard to advance to Step 8. If you are not sure what option to select, choose **Perform Inquiry Now**.

The following screen will display.



You will see two options:

- **I want to search for all Bluetooth devices within range**

  This option will cause Merlin to search for all Bluetooth devices that are in range and ready to transmit and receive data (i.e., in *Inquiry Scan Mode*)

- **I want to search only for devices corresponding to the following (hexadecimal) DIAC:**

  This option will cause Merlin to search for the class of devices that you specify in the DIAC text box. DIAC stands for *Device Inquiry Access Code*. Values are entered in hexadecimal format. You can get DIAC values from the Bluetooth Specification.

Step 4 Select the first option: **I want to search for all Bluetooth devices within range**, then press **Next**.The following screen

will display.

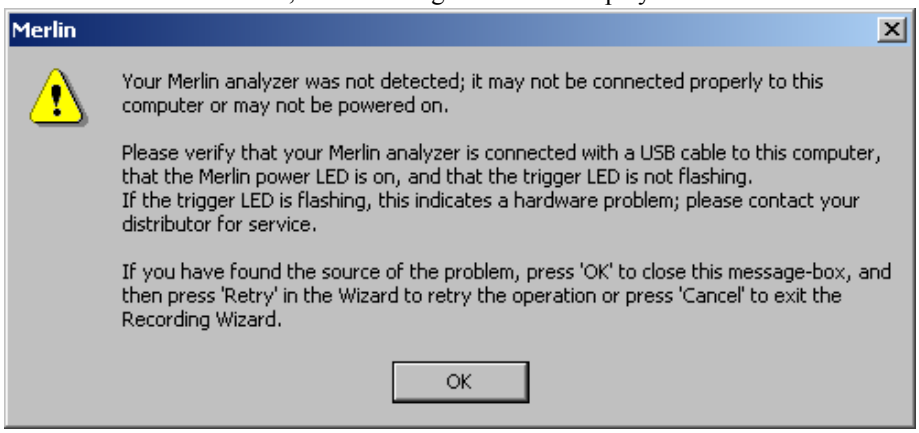
You will see two options:

Step 5 In the text box, enter the length of time you want Merlin to search for nearby devices.

The default value is **20**. If you do not sure what time value to enter, use the default value.

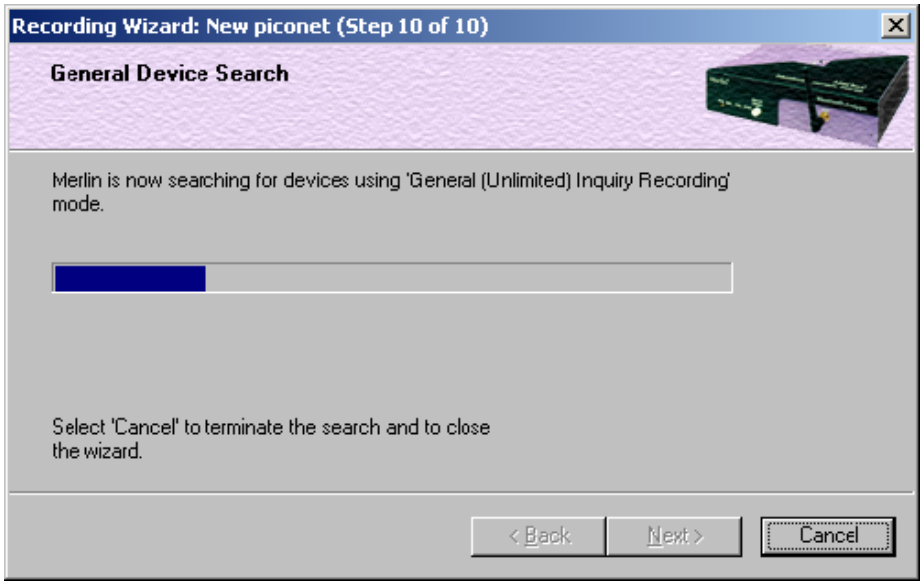
Step 6 Press **Next**.

Before the Inquiry, Merlin tests the hardware connection. In the case of failure, the following screen will display.

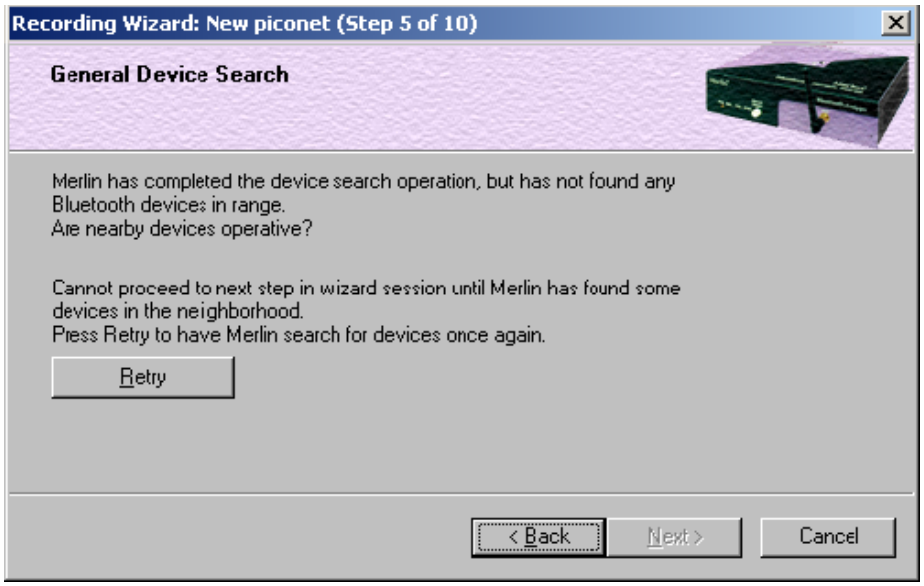


Clicking **OK** will close the message box.

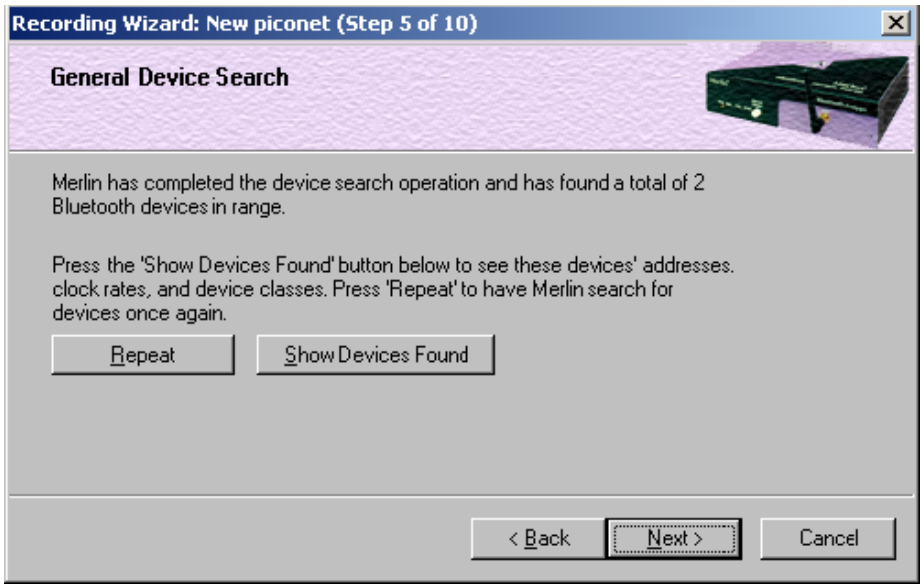
If Merlin passes the hardware test, it will search for devices. The Recording Wizard will display a progress bar and a message telling you that a search is under way:



If no device is found, the Recording Wizard will display the following screen:



If devices found, the Recording Wizard will display the following screen:

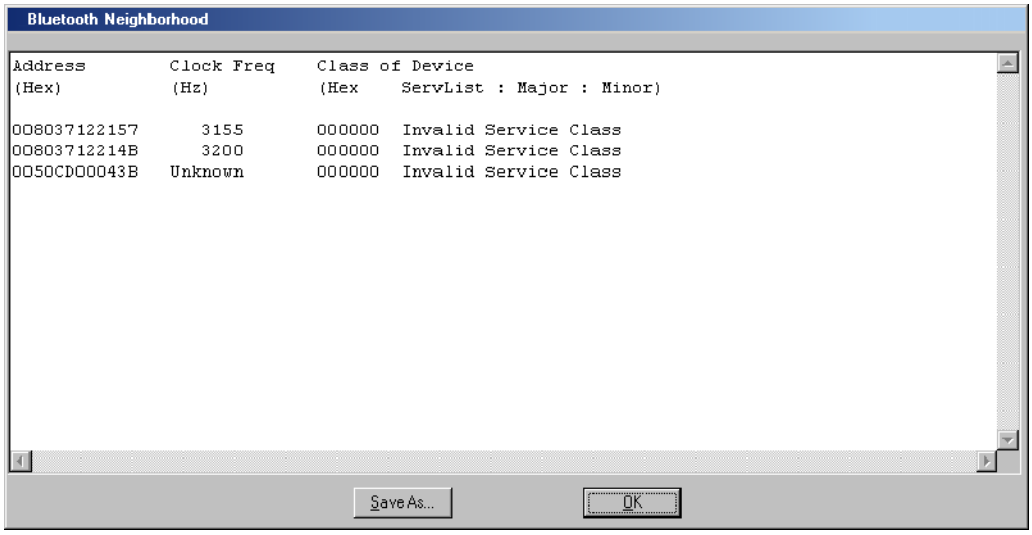


Two buttons will display:

- **Repeat** - This button will cause Merlin to repeat the General Inquiry
- **Show Devices Found** - This button will cause a window to open and display details about the found devices.

Step 7 Press the button marked **Show Devices Found**.

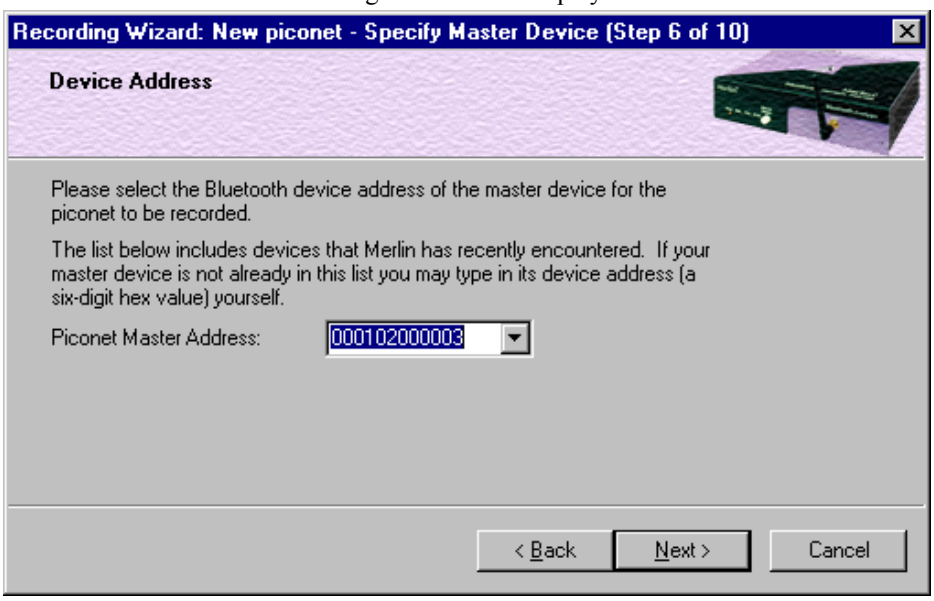
The following screen will display:



Step 8 Click **OK** to close the window.

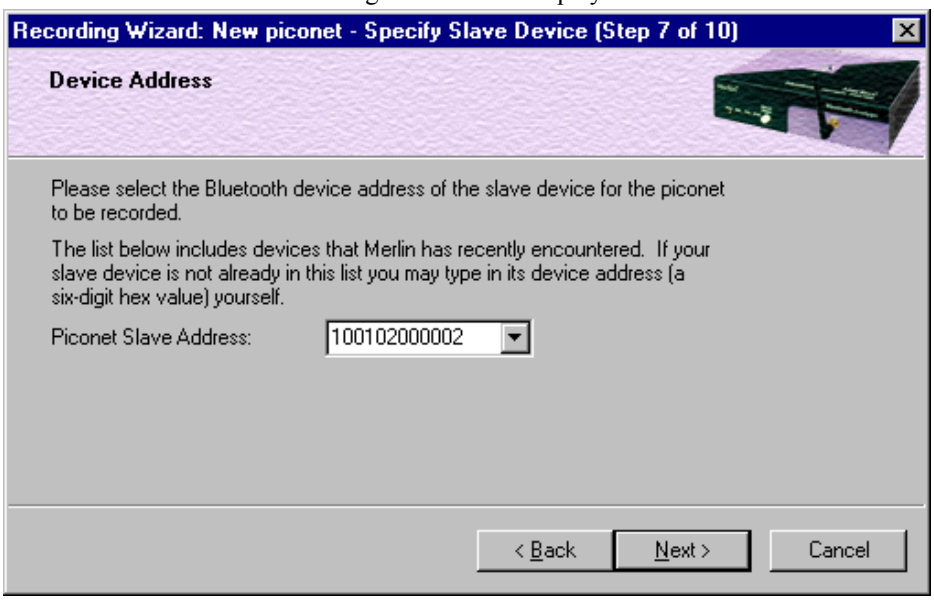
Step 9 Press **Next**.

The following window will display:



Step 10 Select from the drop-down menu the hexadecimal address for your Master device. If you do not see your device's address, you may type it into the text box yourself.

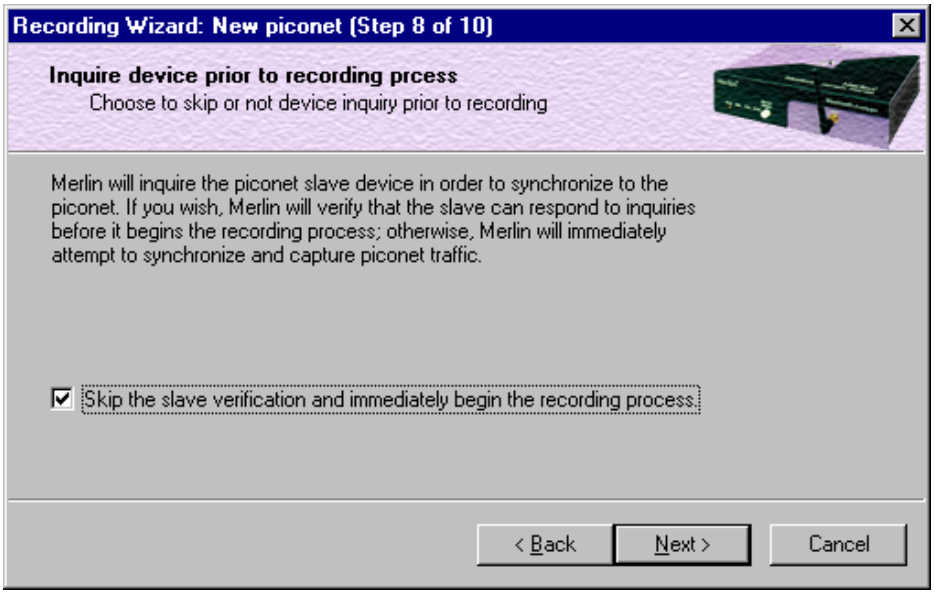
The following window will display:



Step 11 Select from the drop-down menu the hexadecimal address for your slave device into the box labeled **Piconet Slave Address**. If you do not see your slave's address, you can type it into the box.

Step 12 Press **Next**.

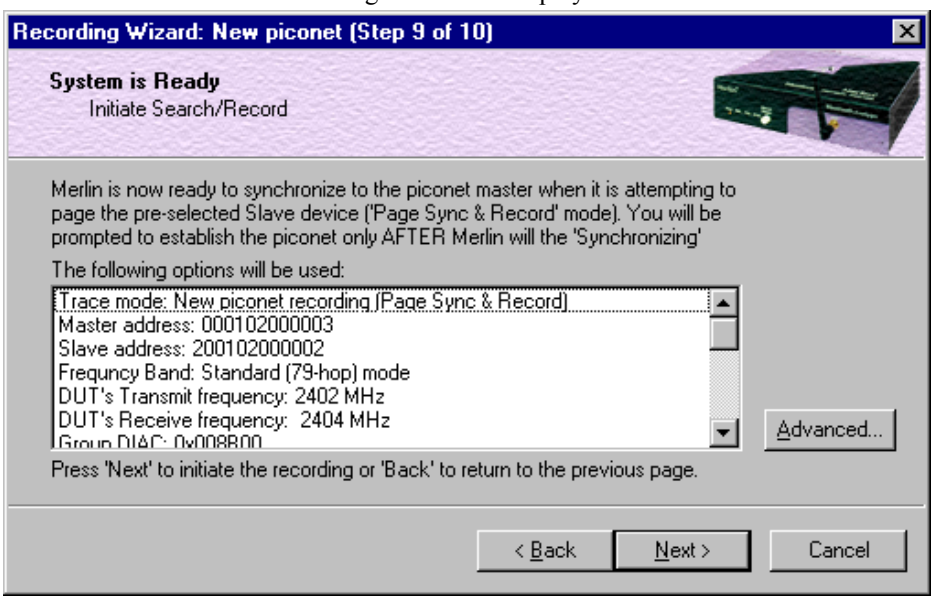
The following screen displays.



You will see a checkbox marked **Skip the verification and immediately begin the recording process**. If you uncheck this box, Merlin will perform a device inquiry on the slave device in Step 10 before it attempts to synchronize to the piconet.

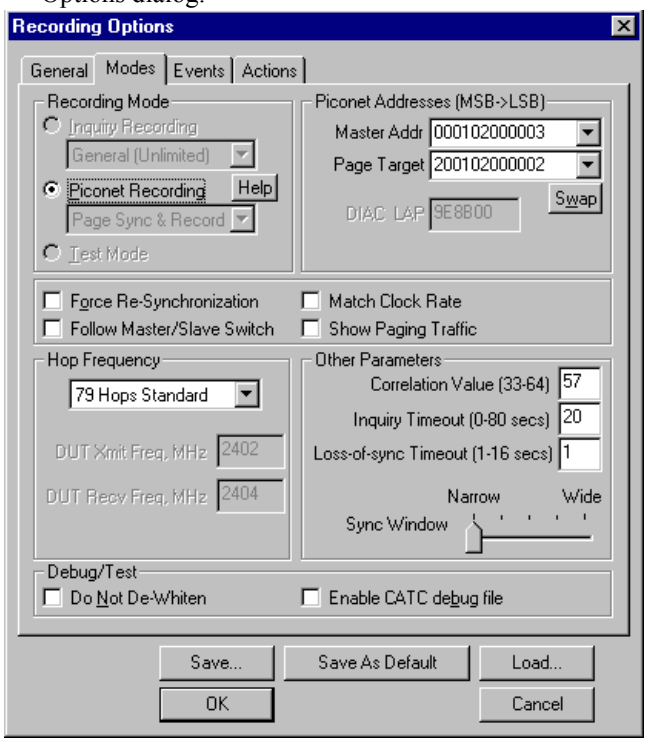
Step 13 Press **Next**.

The following screen will display.



This screen displays the settings you selected.

The **Advanced** button on the right will open the Recording Options dialog box shown below. This screen will show the settings you selected through the Recording Wizard have been applied to the Recording Options dialog.



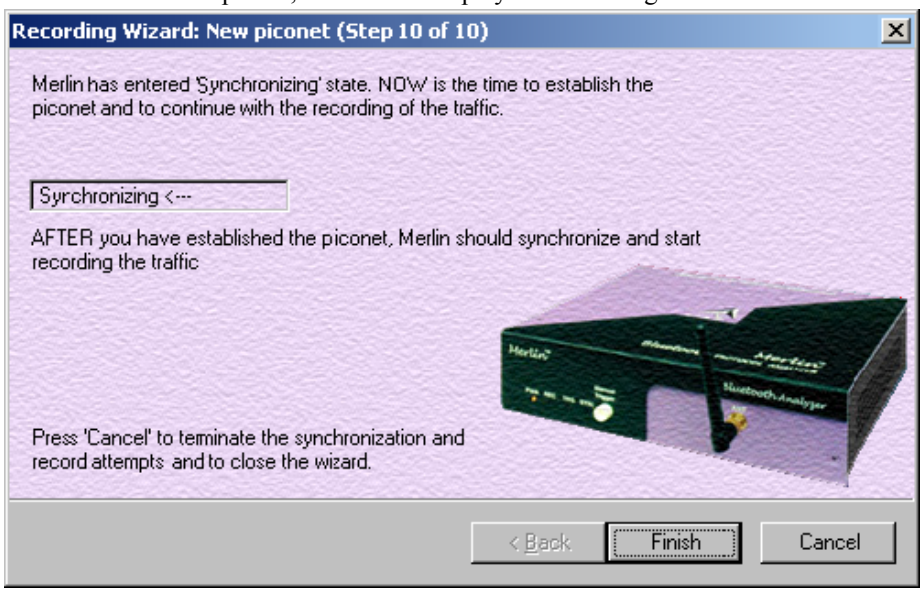
Step 14 Press **Next** to advance the Recording Wizard to the next screen.

The following screen displays:

Merlin pages the Master and if specified in Step 8, the Slave devices.

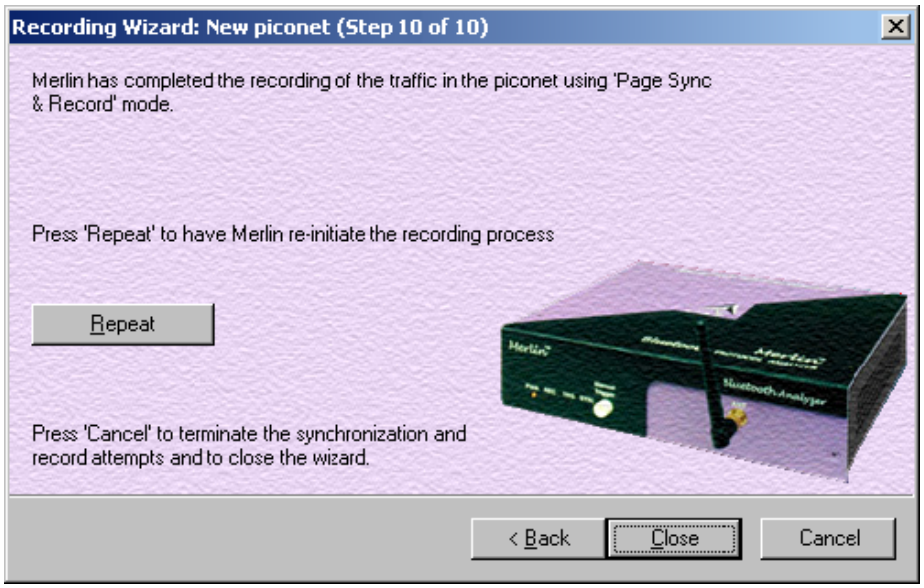
If Merlin is unable to complete its pages, the following screen will display:

If Merlin is able to complete its pages, it will enter into a synchronizing state and then wait for you to create the piconet. During this waiting period, Merlin will display the following screen:



Once you have created the piconet, Merlin will synchronize to the piconet and begin recording. During the recording, Merlin will display the following screen:

At the completion of the recording, Merlin will display the following screen:



You can repeat the recording by pressing the **Repeat** button.

Step 15 To close the wizard, press the **Close** button.