

# CATC Merlin<sup>TM</sup>

## Bluetooth<sup>TM</sup> Protocol Analyzer

### User's Manual



**For Software Version 2.00**

**Manual Version 2.00**

15 May, 2003

## 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, Merlin's Wand, Merlin Mobile, BTTracer, BTTrainer, Advisor, Chief, FireInspector, Inspector, Detective, Traffic Generator, BusEngine, USB4DOS, UPT, HPT, UHT, IBTracer, and SATracer* are trademarks of Computer Access Technology Corporation.

*Microsoft, Windows NT, Windows 2000, Windows 98SE, Windows Me, and Windows XP* are registered trademarks of Microsoft Inc.

All other trademarks are property of their respective companies.

## Copyright

Copyright © 2003, Computer Access Technology Corporation (CATC); All Rights Reserved.

Portions of this product are supplied courtesy of Richard Herveille. Copyright (c) 2002, 2003 Richard Herveille, rherveille@opencores.org. All rights reserved.

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

## FCC Conference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device and an intentional radiator, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense. The end user of this product should be aware that any changes or modifications made to this equipment

without the approval of CATC could result in the product not meeting the Class A limits, in which case the FCC could void the user's authority to operate the equipment.

**Important Notice:** To comply with FCC RF exposure requirements (sections 1.1307 and 1.310 of the Rules) only the antenna supplied by CATC must be used for this device. The antenna must be located at least 20 cm away from all persons.

FCC Testing applies to FCC ID: KH7BT004APA-X.

## EU Conference Statement

This equipment complies with the R&TT Directive 1999/5/EC. It has been tested and found to comply with EN55022:1994/A1:1995/A2:1997 Class A, EN61000-4-2:1995, EN61000-4-3:1995, EN61000-4-4:1995, EN61000-4-5:1995, EN61000-4-6:1995, EN61000-4-11:1994, EN61010-1:1993, and ESTI EN 300 328-1 V1.2.2 (2000-07).



## TABLE OF CONTENTS

<b>Chapter 1 Overview</b>	<b>1</b>
Bluetooth™ Overview	1
General Description	2
Automation	4
HCI Trace	4
Features	5
General	5
Physical Components	5
Display Options	6
Recording Options	6
Traffic Generation	6
Bluetooth™ BusEngine	6
Specifications	7
Package	7
Power Requirements	7
Environmental Conditions	7
Switches	7
LEDs	7
Recording Memory Size	7
Certification	7
<b>Chapter 2 Installation</b>	<b>9</b>
System Components/Packing List	9
Analyzer LED and Control Descriptions	9
Merlin Rear Panel Description	10
Setting Up the Analyzer	11
Installing the Analyzer Software on the PC	11
Installing the Probe	14
HCI Probe configurations	15
2-port RS232 to USB converter	17
Your First Bluetooth Recording	18
Inquiry Recording	20
External Interface Breakout Board	21
Pin-Outs for the Data In/Out Connector	22
Prototype Rework Area	23
Configuring the Analyzer for the Breakout Board	24
<b>Chapter 3 Updates</b>	<b>25</b>
Software, Firmware, and BusEngine Revisions	25
Software Updates	26
Software License Updates	26
Viewing licensing information	27
Automatic BusEngine and Firmware Updates	27
Manual BusEngine Updates	29
Manual Firmware Updates	30

<b>Chapter 4 Software Overview</b> .....	<b>31</b>
The Main Display Windows. ....	31
Toolbar .....	34
Status Bar .....	35
Recording Progress .....	36
Status Bar Position Definitions: .....	36
Recording Status .....	37
Analyzer Status .....	38
Search Status .....	38
Zoom In .....	38
Zoom Out .....	39
Tool Tips .....	39
Merlin Analyzer Keyboard Shortcuts .....	39
<b>Chapter 5 Recording Wizard</b> .....	<b>41</b>
Starting Recording Wizard .....	41
Recording a Traffic on a New Piconet .....	42
Recording an Existing Piconet .....	52
Recording in Test Mode .....	62
Recording in Reduced Hopping Mode .....	62
Recording in Single Frequency Mode .....	66
<b>Chapter 6 Recording Options</b> .....	<b>69</b>
Recording Modes .....	69
Piconet recording .....	69
Inquiry recording .....	69
IUT:HCI mode .....	70
Opening the Recording Options Dialog Box .....	70
Recording Options - General .....	71
Recording type .....	71
Options .....	72
Buffer Size .....	72
Trigger Position .....	73
Recording Options - Piconet .....	73
Hop Sequence .....	74
Sync Method .....	75
Additional Settings .....	79
Debug .....	80
Recording Options - Inquiry .....	80
Recording Options - HCI .....	82
HCI Window Layout .....	82
Recording HCI Traffic .....	85
Recording Options - Events .....	86
Payload Length Error .....	93
Recording Options - Actions .....	94
Action Buttons - Their Functions .....	95
Blue Dot Menu .....	98

Saving Recording Options .....	102
Recording Bluetooth Traffic .....	103
<b>Chapter 7 Display Options .....</b>	<b>105</b>
General Display Options .....	106
Setting Color, Formatting, and Hiding Options .....	107
Setting Color Display Options .....	107
Changing Field Formats .....	108
Hiding Display Options .....	109
Level Hiding Options .....	109
Level Hiding Parameters .....	109
Saving Display Options .....	111
<b>Chapter 8 Reading a CATC Trace .....</b>	<b>113</b>
Trace View Features .....	113
Interpreting the Displayed Information .....	113
Tooltips .....	114
Set Marker .....	114
Edit or Clear Marker .....	115
Expanded and Collapsed Data Formats .....	116
Hide Frequency Hops .....	118
Hide Nulls and Polls .....	118
Menus in Clicked Fields .....	119
Hide Unassociated Traffic .....	119
<b>Chapter 9 Decoding Protocols .....</b>	<b>121</b>
Introduction .....	121
LMP and L2CAP Messages .....	121
Decoding and Viewing Protocol Data .....	122
Decoding Via the Decoding Toolbar .....	122
Decoding Via the Display Options Dialog Box .....	123
Tooltips .....	124
Viewing Packets in LMP and L2CAP Messages .....	124
Types of LMP and L2CAP Messages .....	124
Viewing L2CAP Channel Connections .....	125
Viewing Protocol Messages and Transactions .....	126
Viewing L2CAP Messages in Protocol Messages .....	127
How to Decode .....	127
Expanding Protocol Messages .....	127
Changing Protocol Assignments .....	128
Using the Decoding Assignments Dialog Box .....	128
Removing User-Assigned Protocol Assignments .....	129
Manually Assigning Protocols .....	130
Other Assignments: OBEX Client/Server Status .....	130
Changing an OBEX Client or Server Status .....	131
Decoding BNEP .....	131
Decoding HID .....	131

---

Other Decoding Options . . . . .	131
<b>Chapter 10 Other Features . . . . .</b>	<b>133</b>
Search . . . . .	133
Go to Trigger . . . . .	133
Go to Packet/Message/Protocol . . . . .	133
Go to Marker . . . . .	134
Go to . . . . .	134
Error . . . . .	138
Soft Bit Error . . . . .	138
Loss of Sync . . . . .	138
Find . . . . .	138
Event Groups . . . . .	140
Union, Intersection, and Exclusion . . . . .	144
Using Find . . . . .	144
Find Next . . . . .	146
Device List . . . . .	147
Edit Comment . . . . .	148
Exporting Data . . . . .	148
File Information . . . . .	149
Error Summary . . . . .	150
Timing Calculations . . . . .	150
Bus Utilization . . . . .	151
Traffic Summary . . . . .	155
Encryption . . . . .	155
Configuring Merlin for Encryption . . . . .	156
<b>Chapter 11 How to Contact CATC . . . . .</b>	<b>159</b>
<b>Chapter 12 Warranty and License . . . . .</b>	<b>159</b>
<b>Index . . . . .</b>	<b>161</b>



# 1. Overview

The CATC Merlin™ Protocol Analyzer is a member in CATC's industry-leading line of high performance, Bluetooth protocol 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 2500 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 with a range of 10 to 100 meters, depending the power of the radio, 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 1.1* for details on the protocol. The Bluetooth™ specification is available from the Bluetooth™ SIG at its web site <http://www.bluetooth.org/>

## 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 conditions, thereby focussing the user's attention on events of interest.

The Merlin Protocol Analyzer functions with any personal computer using the Windows 98SE, Windows 2000, Windows NT 4.0, Windows Me, or Windows XP operating systems and equipped with a functional USB interface. For an updated set of system requirements for the host machine, please refer to the readme file.

The Analyzer is 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. The Analyzer 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 Automation

The Merlin software includes an Application Program Interface (API) for developing testing programs and scripts in C++ and Visual Basic. The API reproduces most of the commands embodied in the Merlin trace viewer software. This API allows users to automate procedures that otherwise have to be run manually via the trace viewer software. The Automation API can be run locally on the PC attached to Merlin or remotely over a network connection.

For further details, refer to the *Automation API for CATC Bluetooth Analyzers* reference manual included in the installation CD-ROM. You can also download the document from the CATC website.

### 1.4 HCI Trace

In addition to the ability to record Bluetooth traffic off-the-air, using the analyzer's hardware and radio module, the Merlin can record serial Bluetooth HCI traffic from Bluetooth devices, or 'IUT's (Implementations Under Test).

While the off-the-air traffic is captured by the analyzers hardware, the HCI Traffic from the IUTs is captured by the analyzer application using an HCI probe (provided by CATC) that is connected directly to the IUT hardware. In a typical setup, the HCI commands and data to transmit are passed from the Bluetooth application to the Bluetooth baseband (Host to Controller), while events and data that was received are passed from the Bluetooth baseband to the Bluetooth application (Controller to Host).

To capture the data, the HCI Probe should be connected to the respective 'Host to Controller' and 'Controller to Host' lines. When the recording of the IUT's HCI is enabled and the application starts a recording, the serial data is captured as incoming serial data. For this, up to two COM ports should be configured for each IUT.

## 1.5 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 79 frequency hop, reduced and fixed frequency.
- Automatic tracking of changes in the hopping scheme.
- Automatic tracking of whitened and non-whitened packets and traffic.
- Supports recording of serial HCI traffic from implementation under test (IUT)
- 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*

**Note** For an updated description of requirements for the host machine, please refer to the readme file.

- Trace viewer software support for Microsoft Windows versions 98SE and above.
- Recording memory of 128MB - enough to record 25 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, HCI, L2CAP, SDP, RFCOMM, TCS, OBEX, HDLC, BNEP, PPP, AT, HCRP, IP, TCP, UDP, HID, AVCTP, and AVDTP.

### *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.
- Support for various piconet characteristics by enabling the user to configure the synchronization method and recording parameters.
- Real-time hardware filtering of captured traffic for optimizing analyzer memory usage.

### *Traffic Generation*

Traffic generation capability is provided by Merlin's Wand.

### *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.

## 1.6 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





## 2. 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.

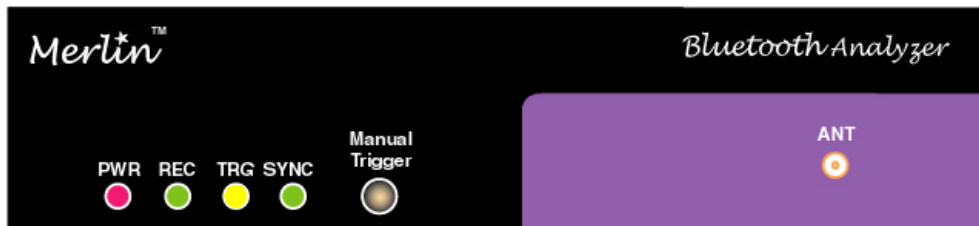
### 2.1 System Components/Packing List

- One stand-alone Merlin Analyzer
- One Antenna
- One External Interface Breakout Board with a 9-pin ribbon cable
- One USB cable
- One RF wired Piconet cable
- One SMA Adapter cable (for changing the polarity from reversed to standard. This cable is used for creating wired piconets.)
- Merlin software program installation CD
- Product documentation

### 2.2 Analyzer LED and Control Descriptions

The Merlin Analyzer has several user-accessible controls and LEDs.

**Figure 1: Front Panel**



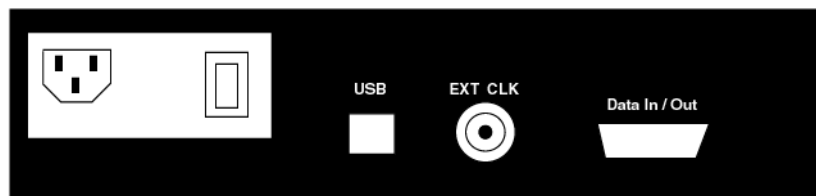
- Red **PWR** (power) indicator LED (lights when the unit power is switched on).
- Green **REC** (recording) LED (lights when the unit is recording).
- Yellow **TRG** (triggered) LED (lights when the unit triggers an event).

**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

## 2.3 Merlin Rear Panel Description

Figure 2: Rear Panel



From left to right, the rear panel has the following connectors and switches:

### *Wide Range AC Connector Module*

The power module is composed of:

- Power on/off switch
- 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.

### *USB type "B" host computer connector*

This is the connector that is used to link the analyzer to the PC that will be administering it.

### *BNC Connectors "Ext. In" and "Ext. Out"*

These connectors allow BNC cables to be attached to the analyzer for the purpose of triggering on external input signals.

### *RS-232 25 pin "Data Output" Connector*

This connector attaches to a 25 pin RS-232 cable that in turn attaches to an External Breakout board. The breakout board allows signals to be sent from the analyzer to an external device such as an oscilloscope.

## 2.4 Setting Up the Analyzer

- Step 1** Attach the Antenna to the ANT connection point. The antenna should point up.
- Step 2** Connect the provided AC power cord to the rear of the analyzer and to a 100-volt to 240-volt, 50 Hz to 60 Hz, 100 W power outlet.

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

**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.

- Step 4** Insert the Merlin CD into the CD ROM drive of the PC that will be administering the analyzer.

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

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

- 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 required USB files are included on the Merlin CD).

## 2.5 Installing the Analyzer Software on the PC

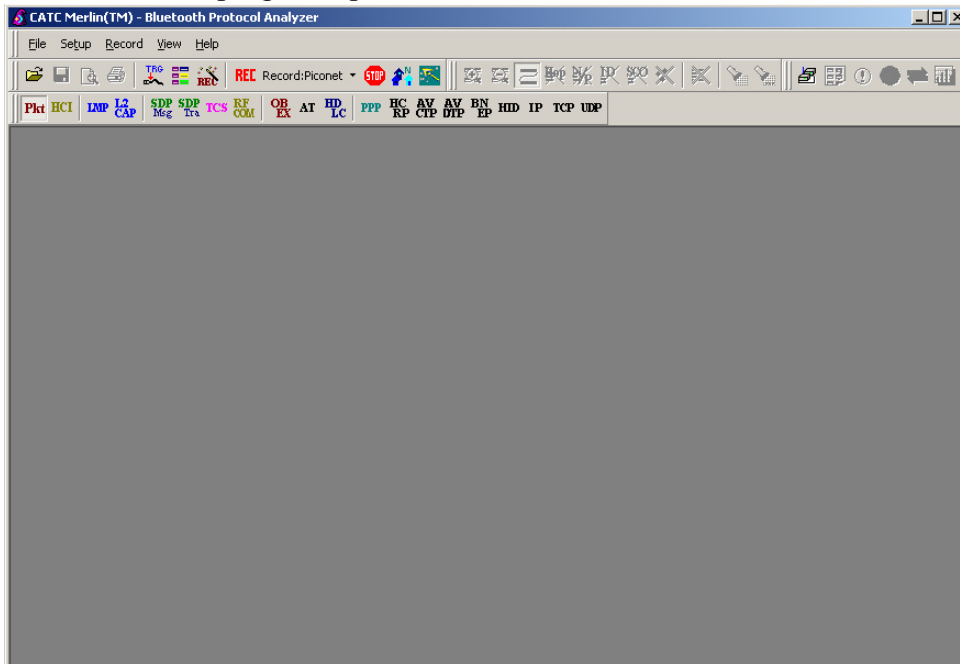
Once Merlin has been recognized as a USB device, install the Merlin software on the PC administering the analyzer.

- Step 1** On the PC, run **setup.exe** on the installation CD and follow the on-screen installation instructions.

The Merlin application will install on the PC hard disk.

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

The Merlin program opens.

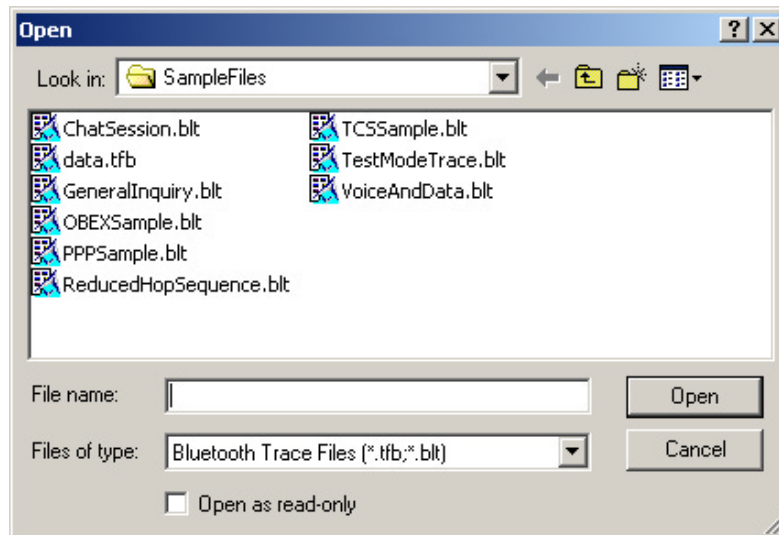


The window shows a menu bar and toolbar at the top, a grey trace viewing area covering most of the window, and a status bar at the bottom.

Opening a sample trace will cause most of the buttons on the toolbar to become active.

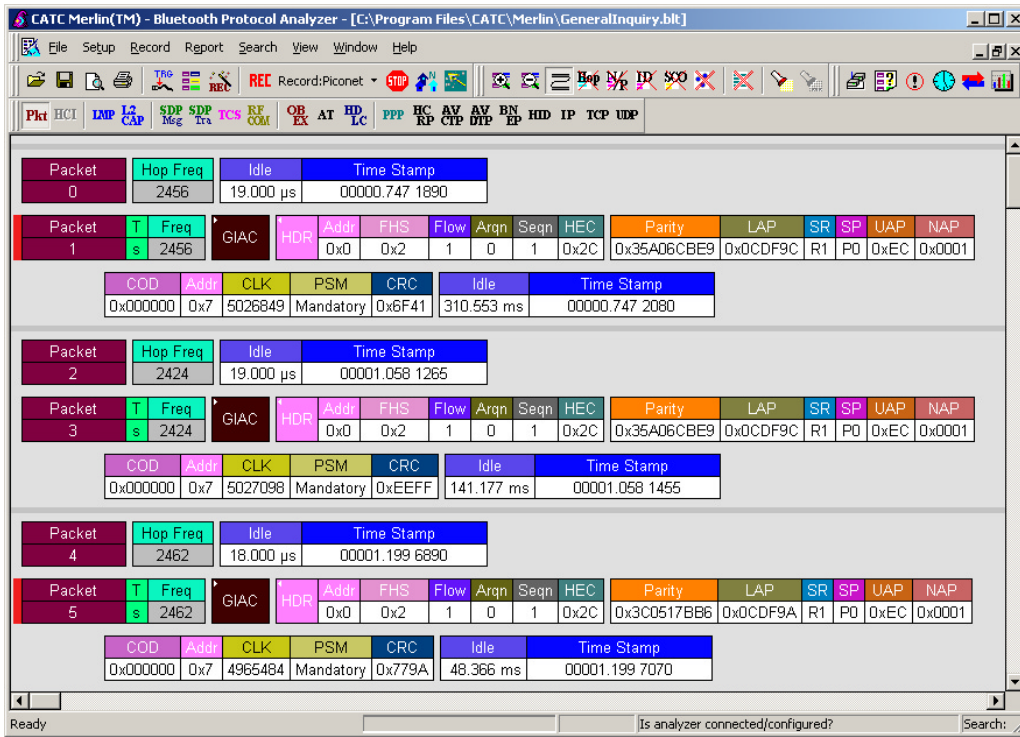
To open a trace,

**Step 1** Select **File > Open** from the menu. A dialog box opens.



**Step 2** Select a file from the dialog box and click **Open**. A trace opens in the main viewing area. When traffic has been

recorded, it will display here.



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

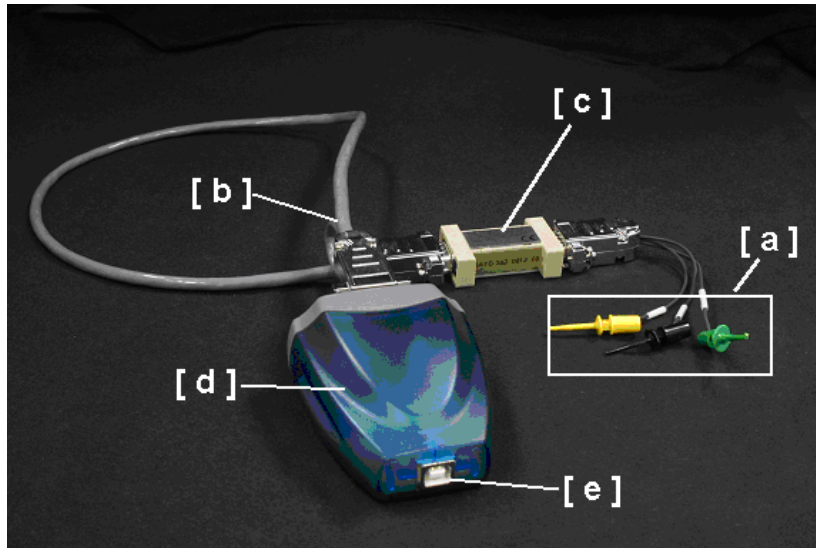
## 2.6 Installing the Probe

If you are planning to record HCI traffic from an Implementation Under Test (IUT), you will need to connect the provided HCI probe to the IUT.

The HCI Probe is used for connecting the analyzer application running on the host machine to a single IUT. If more IUTs are to be monitored (up to three) additional HCI Probes should be used.

The probe is composed of the following components:

- [ a ] HCITrace Probe Cable
- [ b ] HCITrace RS232 Cable
- [ c ] TTL to RS232 converter
- [ d ] 2-port RS232 to USB converter
- [ e ] USB cable



### *HCITrace Probe Cable*

The HCITrace Probe Cable has three probes:

- ‘Gnd’ – Should be connected to the reference/ground wire
- ‘Host’ – Should be connected to the wire that carries the down-link traffic from the host to the controller.
- ‘BTC’ – Should be connected to the wire that carries the up-link traffic from the controller to the host.

### *HCITrace RS232 Cable*

Has three DB-9 connectors:

- *RS-232/Probe* - Should be connected to the **HCITrace Probe Cable** or to the TTL to RS232 converter (depending whether the signal voltage in the IUT is TTL or RS-232).
- *COM A* - Should be connected to one of the serial inputs of the 2-port RS232 to USB converter.
- *COM B* - Should be connected to one of the other serial input of the 2-port RS232 to USB converter.

#### *TTL to RS232 converter*

Should be used only when the signal voltage in the IUT is TTL and not RS-232.

The DB-9 connector marked with 'TTL' should be connected to the **HCITrace Probe Cable**.

The DB-9 connector marked with 'RS-232' should be connected to the 'RS-232/Probe' connector of the **HCITrace RS232 Cable**.

#### *2-port RS232 to USB converter -*

This converter is used so the serial signals can be delivered to the host machine through a USB input.

#### *USB cable –*

Connects the **2-port RS232 to USB converter** to the Host machine USB port.

### **HCI Probe configurations**

The HCI Probe can be used in two configurations:

- For monitoring UART level signals
- For monitoring RS232 level signals

#### *Monitoring UART Level Signals*

For monitoring RS232 level signals, the TTL to RS-232 converter should be used. To assemble the HCI probe for this configuration, perform the following steps. Refer to the photo and component list shown previously for references to components [a] through [e].

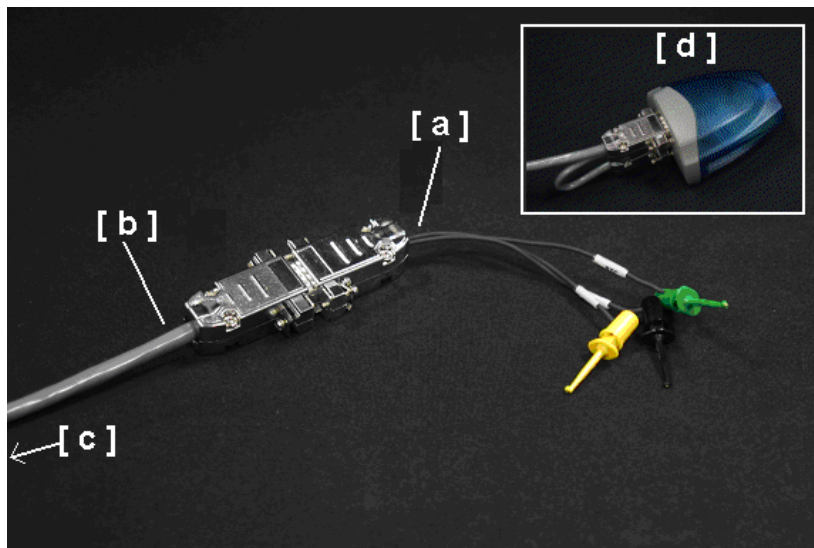
- Step 1** Connect the DB-9 connector of the HCITrace Probe Cable [a] to the connector marked with 'TTL' in the TTL to RS-232 converter [c].
- Step 2** Connect the DB-9 connector marked with 'RS-232' in the TTL to RS-232 converter [c] to the connector marked with 'RS-232/Probe' in the HCITrace RS-232 Cable [b].
- Step 3** Connect the connector marked with 'COM A' in the

HCITrace RS-232 Cable [b] to 'Connector A' in the 2-port RS232 to USB converter [d].

**Step 4** Connect the connector marked with 'COM B' in the HCITrace RS-232 Cable [b] to 'Connector B' in the 2-port RS232 to USB converter [d].

**Step 5** Connect the USB cable to the USB connector of the 2-port RS232 to USB converter [e].

### *Monitoring RS232 level Signals*



Legend for photo:

[a] HCI Probe Cable

[b] HCI Trace RS-232 Cable

[c] Connectors A and B on the other end of the HCI Trace RS-232 Cable

[d] Two-Port RS-232 to USB Converter

For monitoring RS232 level signals do not use the converter. To assemble the HCI probe for this configuration, perform the following steps:

**Step 1** Connect the DB-9 connector of the HCITrace Probe Cable [a] to the connector marked with 'RS-232/Probe' in the HCITrace RS-232 Cable [b].

**Step 2** Connect the connector marked with 'COM A' in the HCITrace RS-232 Cable [c] to 'Connector A' in the 2-port



RS232 to USB converter [d].

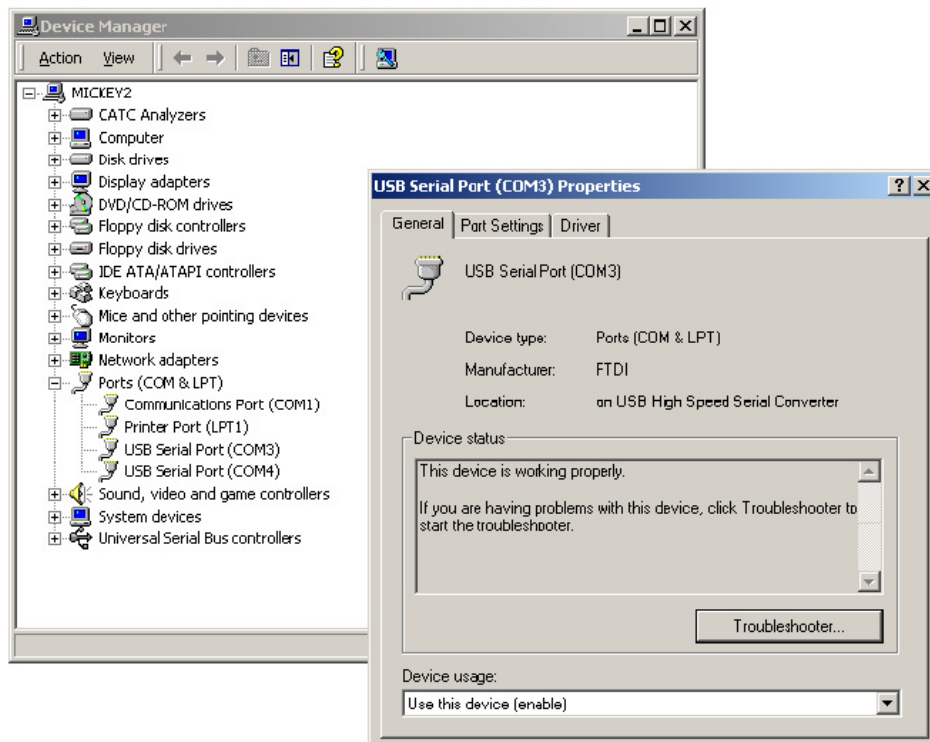
- Step 3** Connect the connector marked with 'COM B' in the HCITrace RS-232 Cable [c] to 'Connector B' in the 2-port RS232 to USB converter [d].
- Step 4** Connect the USB cable [not shown] to the USB connector of the 2-port RS232 to USB converter [d].

## 2-port RS232 to USB converter

The 2-port RS232 to USB converter [d] allows the user to connect two serial connectors to the host machine via a single USB connection. When connected to the host machine the converter emulates two separate virtual COM ports that can be used as other real COM ports. Prior of using this converter as part of the HCI probe several drivers need to be installed. The drivers are provided on the installation CD-ROM in the HCI Probe\Drivers sub directory.

Once the converter is connected to a host machine the user is prompted to provide the place where the system can install the drivers from.

After installing the drivers two new COM ports are going to be available, as seen in the following snapshot of the Device Manager.



## 2.7 Your First Bluetooth Recording

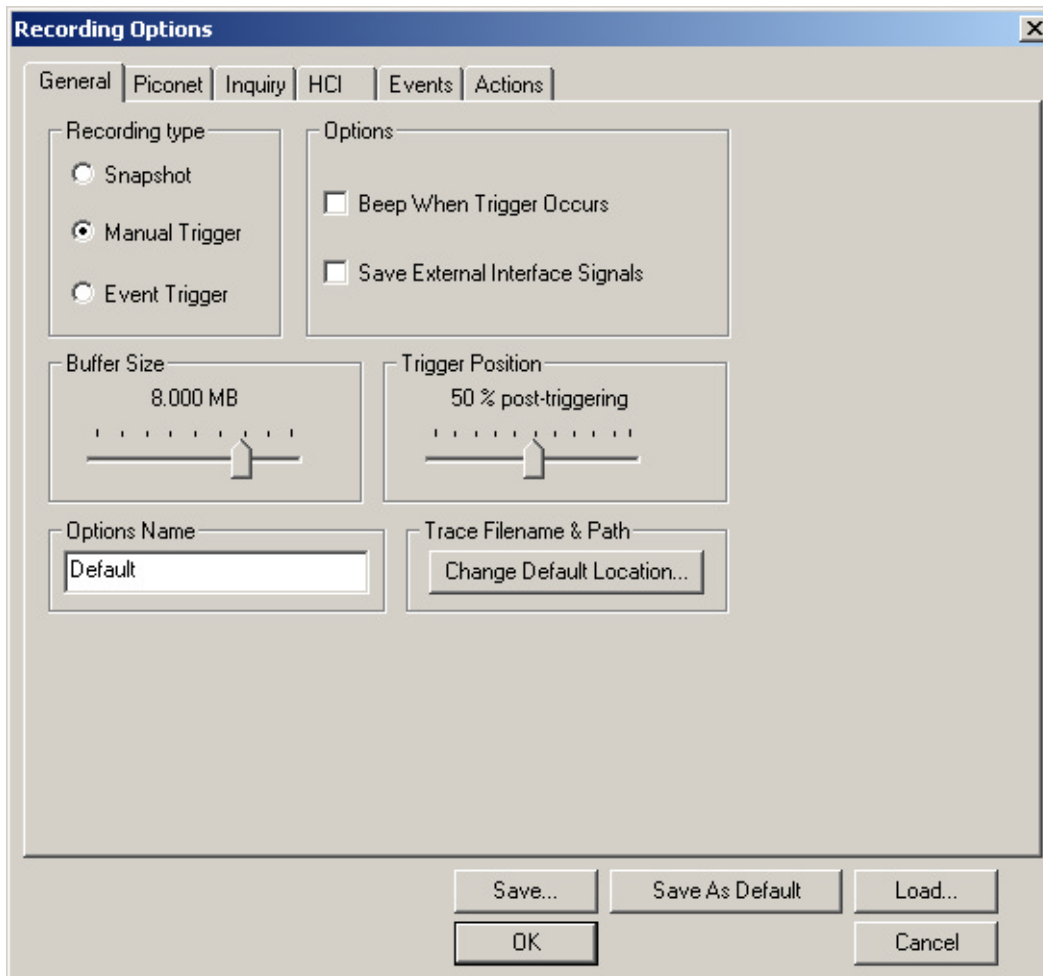
After installing and launching the software, you can test Merlin by synchronizing to a piconet and then recording the inquiry traffic. In this inquiry test, Merlin will issue a General Inquiry that asks local devices to identify themselves. Merlin then records the responses.

**Step 1** Click the down-arrow on the Record button and select **Piconet**.



**Step 2** From the menu, select **Record > Recording Options**.

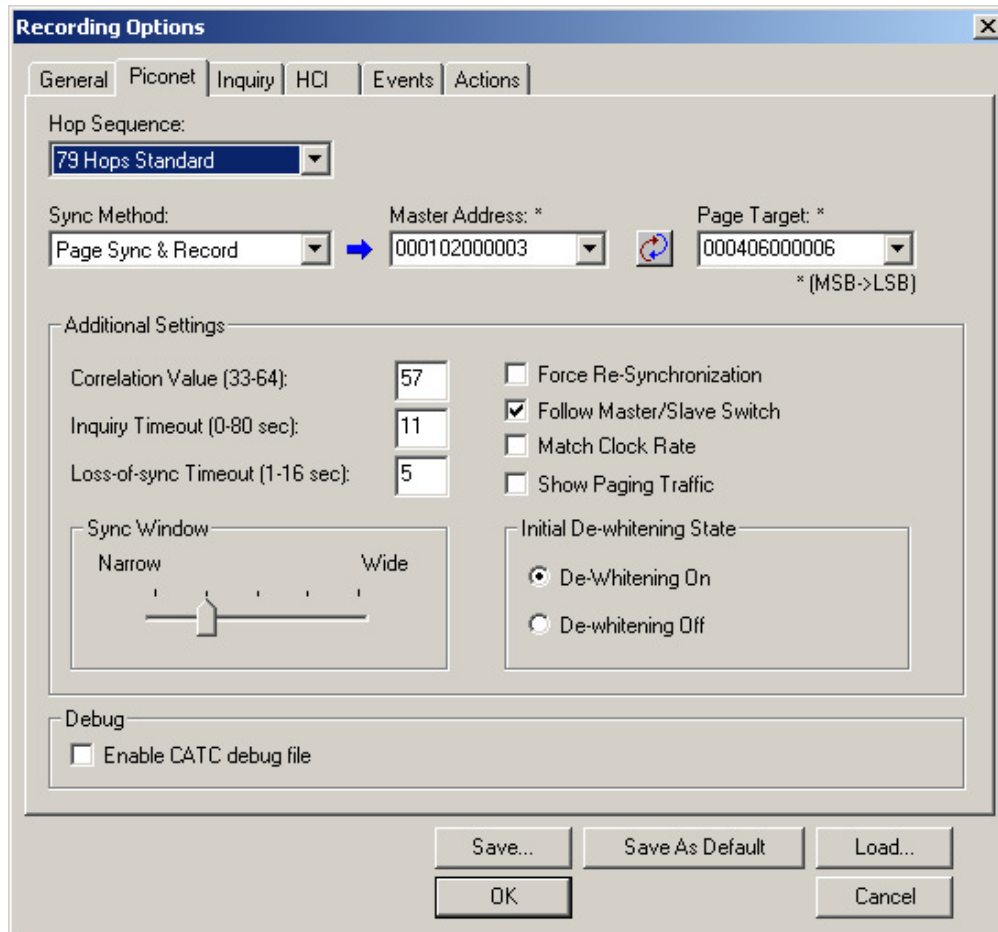
The Recording Options dialog box opens showing factory default settings such as “manual trigger” and 16 MB buffer size. For the General Inquiry recording you are about to create, leave these settings unchanged.



**Step 3** Select the **Piconet** tab.

The following dialog box will open showing factory default settings. Merlin defaults to **"Page Sync & Record."** This setting tells Merlin to perform a General Inquiry and then collect sync information from the specified slave device when the slave responds. Merlin then waits for the Master to begin paging the Slave devices. When paging begins, Merlin synchronizes to the Master and begins recording.

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.



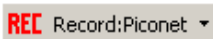
**Step 4** Click OK to close the Recording Options window and activate the recording options you selected.

At this point, Merlin will be ready to record.

## Inquiry Recording

Merlin can also record an inquiry process where the Merlin performs a general inquiry and asks local devices to identify themselves.

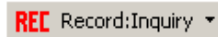
**Step 1** Click the down-arrow on the right side of the

**Record:Piconet** button on the toolbar  .

A sub-menu appears with options for **Piconet Recording Mode**, and **Inquiry Recording Mode**.

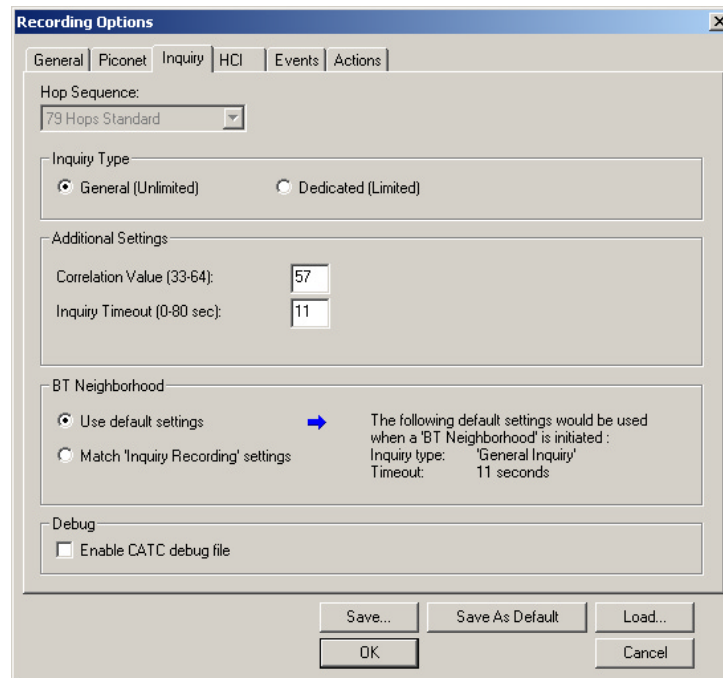
**Step 2** Select **Inquiry Recording Mode**.

The button changes appearance and shows the label **Record: Inquiry**

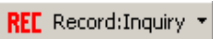


**Step 3** From the menu, select **Setup > Recording Options**.

The Recording Options dialog opens with the **Inquiry** page displaying.



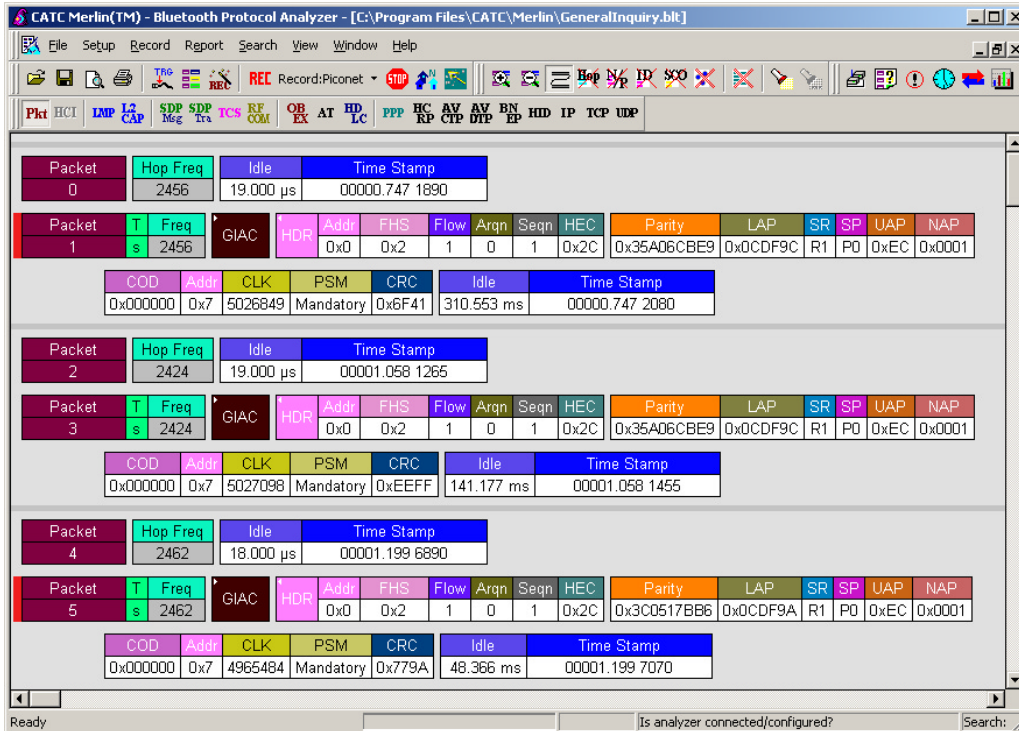
**Step 4** If desired, make any changes to the options, then click **OK**.

**Step 5** Click the  button (i.e. the button itself, and not the down-arrow.)

Merlin starts to record the Bluetooth traffic immediately using the settings from the Piconet page in the Recording Options dialog. The Bluetooth Inquiry process will proceed for whatever amount of time is set for creating an Inquiry action (0 to 80 seconds). After the inquiry time has elapsed, the analyzer will upload the data and displays the packets.


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.tfb** 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 6** 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 7** Give the recording a unique name and save it to the appropriate directory.

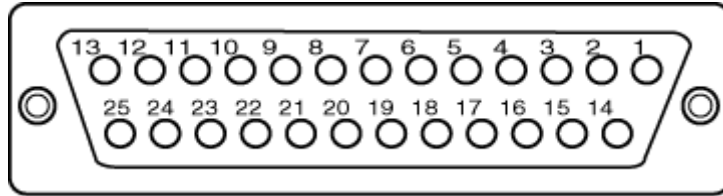
## 2.8 External Interface Breakout Board

The External Interface Breakout Board is an accessory that allows standard, LV TTL signals to be channeled into the analyzer for triggering or out of the analyzer for use by an oscilloscope, logic analyzer or other device. Six ground pins and one 5-volt pin are provided.

Drive strength for all outputs is about 30mA high (@2V) and 60 mA low (@0.5V). Inputs can handle 0 to 5.5V. Inputs above 2V are detected as logic high; inputs below 0.8V are detected as logic low.

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

#### Data In/Out Connector (on cable)



#### Pin-Outs for the Data In/Out Connector

The following table lists the pin-out and signal descriptions for the **Data In/Out** connector on a cable that connects to the Breakout board.

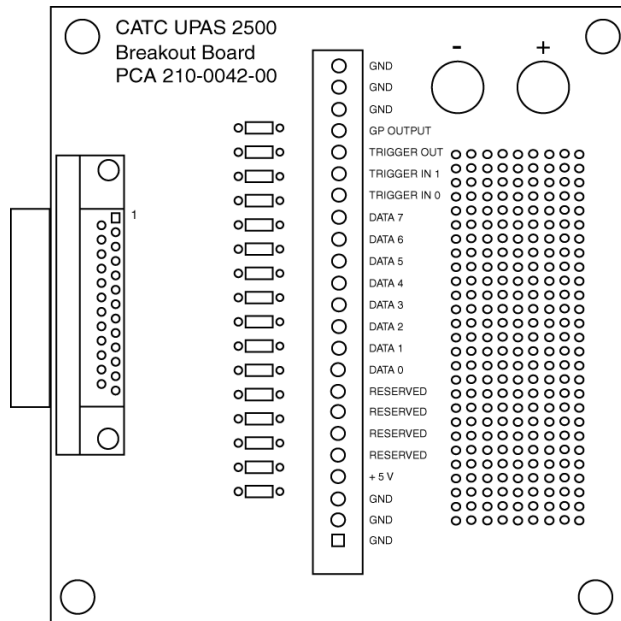
#### Data In/Out Connector – Pin-Out

Pin	Signal Name	Signal Description
1	RSV	Reserved
2	GND	Ground
3	GP OUT	General Purpose Output
4	TRG IN 1	Trigger In 1
5	GND	Ground
6	DATA 6	Data 6
7	DATA 4	Data 4
8	DATA 3	Data 3
9	DATA 1	Data 1
10	GND	Ground
11	RSV	Reserved
12	RSV	Reserved
13	+5V	+5 Volts, 250 mA DC Source
14	RSV	Reserved
15	GND	Ground
16	TRG OUT	Trigger Out
17	TRG IN 0	Trigger In 0
18	DATA 7	Data 7
19	DATA 5	Data 5
20	GND	Ground
21	DATA 2	Data 2
22	DATA 0	Data 0

Pin	Signal Name	Signal Description
23	GND	Ground
24	RSV	Reserved
25	RSV	Reserved

**Note** (\*) Pins 4 and 17 have the same function: they allow external signals to be used to cause triggering or recording. Pins 3 and 16 are used to transmit output signals. Pins 6, 7, 8, 9, 18, 19, 21, and 22 (data pins) are used to define data patterns for external input signals. See External Input Signals in Chapter 6.

### External Interface Breakout Board



### 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.

### External Recordable Signals

**Breakout Board Data 0-1:** These pins let you define an 2 bit Data Pattern that can be recorded in a trace file.

### *External Input Triggers*

You can use either an external input signal or the Trigger button on the front of the UPAS to cause triggering. The following descriptions show what pins or buttons to use:

**Breakout Board Data 7 - Data 0:** Trigger on an 8-bit input pattern (only Data1 - Data0 can be recorded into the trace)

**Breakout Board Trigger In 0:** Selectable Edge triggered inputs. Will trigger on any edge it detects.

**Breakout Board Trigger In 1:** Selectable Edge triggered inputs. Will trigger on any edge it detects.

**BNC Trigger (EXT IN):** Selectable Edge triggered inputs. Will trigger on any edge it detects. Located on the back of the chassis.

**Push Button Trigger.** The Trigger button on the front of the UPAS can be pressed to manually cause a trigger.

### *External Outputs*

The analyzer can be configured to send an external signal anytime a trigger and/or event occurs. The following descriptions show the behavior of these output signals:

**Breakout Board Trigger Out:** Changes from low to high when analyzer triggers (one time per recording only)

**Breakout Board G.P. Output:** Programmable waveform (low or high pulse, toggle). Each event can be programmed to enable this external signal.

**BNC Output (EXT OUT):** Same as Breakout Board G.P. Output. Located on the back of the chassis.

### **Configuring the Analyzer for the Breakout Board**

To configure the analyzer for the breakout board, see See Section "External Input Signals" on page 49, See Section "Setting External Output Options" on page 68, and See Section "Specifying Pulse Signal Outputs" on page 69.



## 3. Updates

Whenever new software is installed, it is possible that the Firmware and/or BusEngine will also need updating. Updates can be performed two ways: either automatically or manually. This chapter describes both procedures. This chapter also describes how to update Merlin software.

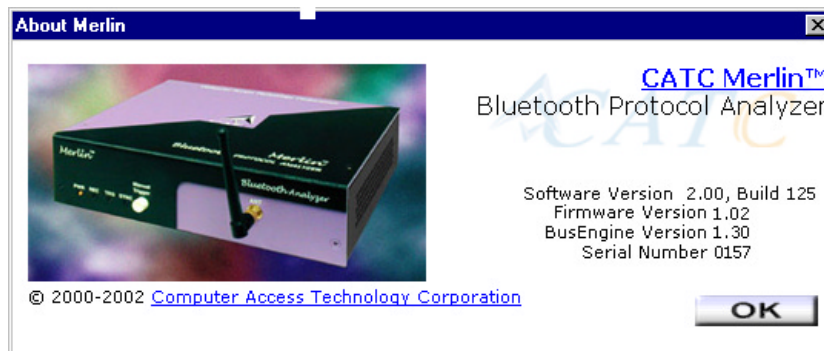
### 3.1 Software, Firmware, and BusEngine Revisions

The **Readme.htm** or **Readme.txt** file on the installation CD 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** file lists the latest versions and informs you if the Firmware or BusEngine needs to be updated.

You can check the current version of the analyzer software, Firmware, and BusEngine by selecting:

- **Help > About Merlin...** from the menu.

You see this screen:



**Note** The Firmware and BusEngine information will not display if the analyzer is not connected to its PC or if the analyzer has just booted up and is still in the process of completing its self diagnostics.

The **About Merlin** box shown above 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.

## 3.2 Software Updates

When a new software release is available, it is posted on the Support page of the CATC website at [www.catc.com/support.html](http://www.catc.com/support.html).

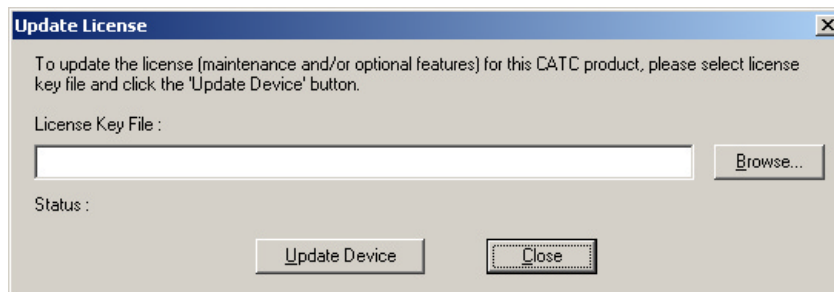
To update the software,

- 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.

## 3.3 Software License Updates

A license key is a file that CATC provides to you when you enter a maintenance agreement. You use this file when you make updates to your CATC software.

- Step 1** From the **Help** menu, select **Update License**.



**Step 2** Type the path and filename to the license key or click the **Browse** button to map to the directory containing the license key.

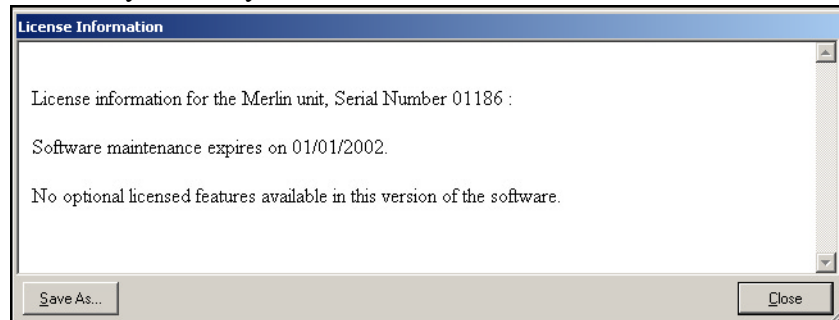
**Step 3** Click **Update Device**.

### Viewing licensing information

You can also view licensing information to see what version of the license you are running.

From the **Help** menu, select **Display License Information**.

The following window appears containing information about the current status of your analyzer's license:




## 3.4 Automatic BusEngine and Firmware Updates

When Merlin's software is updated, the software may become incompatible with the BusEngine and Firmware. When you attempt to record, an error message will appear asking you to update the BusEngine and Firmware.

The following steps describe the update process.

**Step 1** If needed, update the Merlin software using the steps outlined in "Software Updates" described above.

**Step 2** Turn on the Analyzer.

**Step 3** On the toolbar, click the  button.

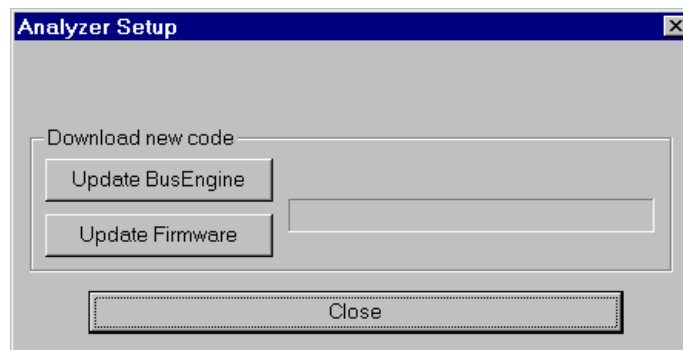
**Step 4** Since the BusEngine and/or the Firmware are incompatible with the current Merlin software version, an error message will appear displaying your current

versions and indicating what versions you need to install.



**Step 5** Click **Yes**.

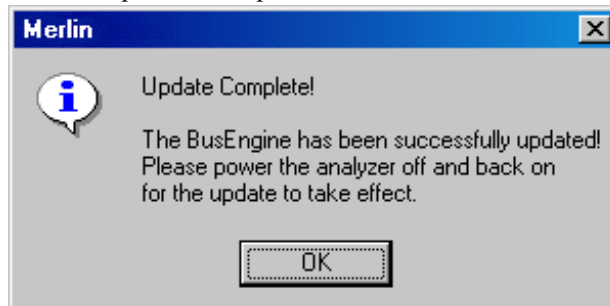
The above window closes and the Analyzer Setup window opens.



**Step 6** 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 update will complete for the first item and then return to the above screen so the second update can be performed.

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



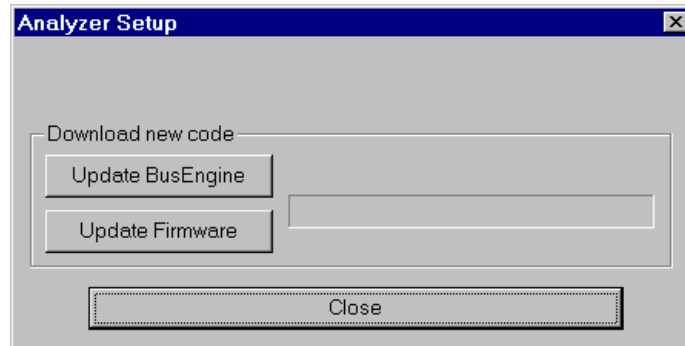
**Step 7** Power cycle Merlin to complete the update.

## 3.5 Manual BusEngine Updates

You can manually update Merlin's BusEngine by performing the following steps:

**Step 1** Select **Setup > Analyzer** from the menu.

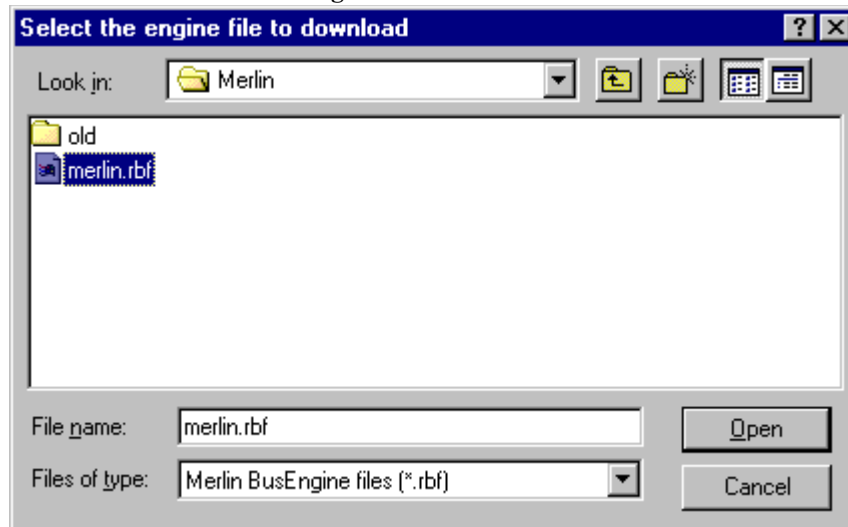
You see the **Analyzer Setup** screen:



**Step 2** Click **Update 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 updateable.

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 3** Click **Open**.

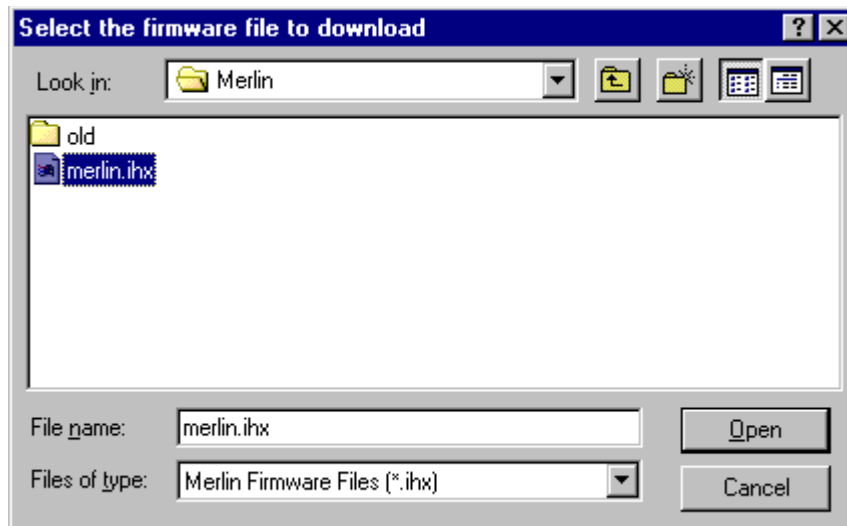
It is not necessary to restart the Analyzer. Once updated, the Analyzer takes approximately 15 seconds to reinitialize, with **Time Remaining** displayed on the screen. During this time the Trigger LED is on, indicating that power-on diagnostics are being run. If there is a hardware failure, the Trigger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

## 3.6 Manual Firmware Updates

To manually update the firmware,

**Step 1** Click **Update 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 updates the Firmware.

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

## 4. Software Overview

### 4.1 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 1: Main Display Pull-Down Windows**

Menu	Function
<b>File</b>	
<u>O</u> pen...	Opens a file
<u>C</u> lose	Closes the current file
Save <u>A</u> s...	Saves all or a specified range of packets from the current file with a specified name
<u>P</u> rint...	Prints part or all of the current traffic data file
<u>P</u> rint <u>P</u> review	Produces an on-screen preview before printing
<u>P</u> rint <u>S</u> etup...	Sets up your current or new printer
<u>E</u> dit <u>C</u> omment...	Creates or edits the Trace file comment field
<u>E</u> xport <u>&gt;</u> <u>P</u> ackets to Text (Packet View Format)	Saves all or part of a trace to a text file
<u>E</u> xport <u>&gt;</u> <u>P</u> ackets to CSV Text	Saves all or part of a trace to a Comma Separated Values (CSV) file suitable for viewing in a spreadsheet application
<u>E</u> xport <u>&gt;&gt;</u> <u>A</u> udio Streams	Saves audio data into a file. Presents options for setting the Audio Source format, Output File format, Stream Direction, and Output Sampling
<i>Last File</i>	Lists the last files that were opened
<u>E</u> xit	Exits the Merlin program
<b>Setup</b>	
<u>D</u> isplay <u>O</u> ptions	Provides the control of various display options such as color, formats, and filters.
<u>R</u> ecording <u>O</u> ptions	Opens a dialog box with checkboxes and drop-down menus for setting up a recording.
Recording <u>W</u> izard	Starts a sequence of interactive dialog boxes that configures Merlin for a recording. This utility provides an alternative to the Recording Options dialog box.
<u>A</u> nalyzer	Allows the operator to reset the Analyzer or update the BusEngine and Firmware.
<b>Record</b>	
<u>S</u> tart	Causes the Analyzer to begin recording Bluetooth activity.
<u>S</u> top	Causes the Analyzer to stop recording.

Menu	Function
Recording <u>M</u> ode	<p>Presents a drop-down menu with options for setting the analyzer's recording mode:</p> <p><b>Piconet Recording Mode</b> -- Causes Merlin to monitor and record piconet traffic. Merlin records the traffic data as specified in the Recording Options, then uploads the data as a Trace file when the recording is complete.</p> <p><b>Inquiry Recording Mode</b> -- Causes Merlin to perform an inquiry to detects and records Bluetooth devices within range. After completing the recording, Merlin uploads the trace to the PC and saves it as a Trace file.</p> <p><b>IUT: HCI Recording Mode</b> -- Causes the Merlin software to record HCI traffic from the IUT. In this mode, the Merlin software on the host PC directly records IUT traffic without first going through the analyzer.</p>
<u>B</u> T Neighborhood Inquiry	Displays Bluetooth Address and clock frequency for devices in range. The expected Bluetooth clock frequency is 3200 Hz +/- 250 ppm.
<b>Report</b>	
<u>F</u> ile Information	Details such information about the recording as number of packets and triggering setup.
<u>E</u> rror 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 <u>C</u> alculation	Starts the calculator dialog for calculating various timing and bandwidth parameters in the recording file.
<u>T</u> raffic Summary	Details the number and type of packets were transferred during the recording, as well as message-level statistics.
<b>Search</b>	
Go to trigger	Positions the display to show the first packet that follows the trigger event.
Go to <u>P</u> acket/Message/Protocol ...	Positions the display to the indicated packet, LMP/L2CAP message, or Protocol Message (RFCOMM, TCS, or SDP protocols).
Go to <u>M</u> arker »	Positions the display to a previously marked packet.
Go to »	Enables quick searching for specific events using a cascade of pop-up windows.
Find	Allows complex searches.
Find <u>N</u> ext	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.













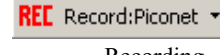









Menu	Function
<b>View</b>	
<u>T</u> oolbars	Presents a sub-menu with options for displaying/hiding the toolbars and an option called Customize which allows the menus and toolbars to be customized or reset to factory default.
<u>S</u> tatus Bar	Switches display of the Status Bar on or off.
<u>U</u> nhide Cells >	Presents a menu of currently hidden cells. Allows you to unhide any cells that were hidden through the Display Options dialog box (View > Display Options > Color/Format/Hiding)
<u>Z</u> oom <u>I</u> n	Increases the size of the displayed elements.
<u>Z</u> oom <u>O</u> ut	Decreases the size of the displayed elements.
<u>W</u> rap	Allows the display to wrap.
<u>D</u> evice List	Displays a list of discovered Bluetooth devices and allows you to add and delete devices and security settings by selecting the device, pressing the security button, and modifying the settings.
<u>R</u> eal-time Statistics	Opens a dialog box with a graphical summary of the traffic currently being recorded by the Analyzer. Real-time monitoring allows continuous monitoring and displaying of traffic and related statistical data in a piconet. This processed data is displayed in a set of configurable graphs.
<u>D</u> ecoding Assignments	Lists current L2CAP decoding assignments.
L2CAP Connections	Lists current L2CAP connections.
RFCOMM Channel Assignments	Lists current RFCOMM assignments.
<u>L</u> evels	Presents a menu of display levels. This menu replicates the Decode/Display buttons in the toolbar such as Packets, L2CAP, TCS etc.)
<b>Window</b>	
<u>N</u> ew Window	Switches display of the Tool Bar on or off.
<u>C</u> ascade	Displays all open windows in an overlapping arrangement.
<u>T</u> ile	Arranges multiple trace windows as a series of strips across the main display area or as a series of side-by-side tiles.
Arrange Icons	Arranges minimized windows at the bottom of the display.
<u>W</u> indows	Displays a list of open windows.























<b>Help</b>	
Online Help	Displays Help topic associated with current Merlin window.
Help Topics...	Displays online help.
Update License...	Opens a dialog box for entering license key information for the analyzer.
Display License Information...	Displays current license information for the analyzer.
About Merlin...	Displays version information about Merlin.

## 4.2 Toolbar

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   |    | View/Hide L2CAP Message Level            |
|   | Save As   |   | View/Hide SDP Message Protocol Level     |
|  | Preview   |  | View/Hide SDP Transaction Protocol Level |
|  | Print...  |  | View/Hide TCS Protocol Level             |
|  | Setup Record Options  |  | View/Hide RFCOMM Protocol Level          |
|  | Start<br>Recording - presents options for recording piconet, inquiry, or IUT:HCI traffic        |  | View/Hide OBEX Protocol Level            |
|  | Stop Recording  |  | View AT Commands Protocol Level          |
|  | Start Recording Wizard  |  | View/Hide HDLC Protocol                  |
|  | Bluetooth Neighborhood. Performs an inquiry and then lists the local devices that it discovered |  | View/Hide PPP                            |
|  | Start Merlin's Wand   |  | View/Hide HCRP                           |

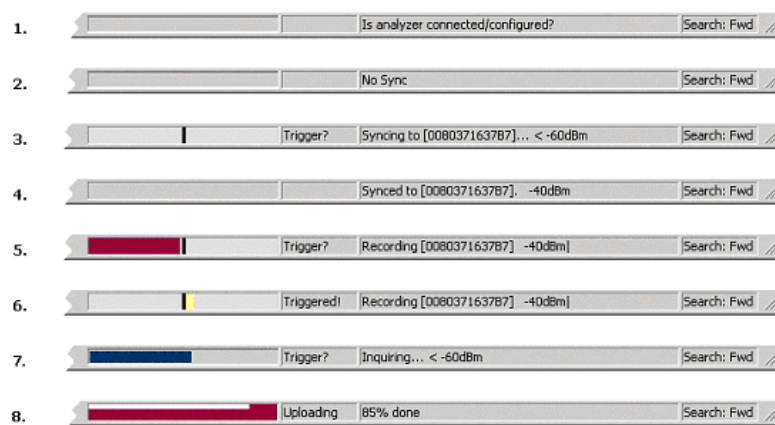
	Setup Display Options		View/Hide AVCTP
	Zoom In		View/Hide AVDTP
	Zoom Out		View/Hide BNEP Protocol
	Wrap		View HID Protocol Layer
	Hide Frequency Hops		View IP Protocol Layer
	Hide Nulls & Polls		View TCP Protocol Layer
	Hide ID Packets		View UDP Protocol Layer
	Hide Voice (SCO) Packets		Display device list
	Hide devices that were specified in the Display Options dialog box		File Information Report
	Hide Unassociated Traffic		Error Summary
	Complex Find		Timing Calculations
	Find Next		Traffic Summary
	View Packet Level (Baseband)		Display Bus Utilization graph
	View/Hide LMP Message Level		Display Real-Time Statistics
			View HCI Protocol layer.

### 4.3 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. The figure below demonstrates the various displays in the status bar.

## Recording Progress

When you begin recording, the left-most segment of the Status Bar displays a Recording Progress Indicator. The following figure displays the various indications of the status bar:



### Status Bar Position Definitions:

The following numbered definitions correspond to the number labels on the above status bars.

- 1 Analyzer is not connected or not configured.
- 2 Idle mode: Analyzer is connected to the host machine, but is not doing any attempts to synchronize to a piconet nor record Bluetooth traffic.
- 3 Analyzer is trying to synchronize to the piconet with the master device that has BD\_Address 00837163787.
- 4 Analyzer is synchronized to the piconet with the master device that has BD\_Address 00837163787.
- 5 Analyzer is recording the traffic of the piconet with the master device that has BD\_Address 00837163787. However, no triggering occurred.
- 6 A trigger event occurred, and the analyzer is recording the traffic of the piconet with the master device that has BD\_Address 00837163787. However, no triggering occurred.
- 7 Analyzer is performing a BT Neighborhood action, where it makes inquiries for Bluetooth devices.
- 8 Merlin application uploads recorded data from the analyzer at the end of a recording session.

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.tfb** or a new name specified in the Recording options.

To abort the upload process,

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. The status will display one of the following:

**No Sync** - the system is not synced to any piconet

**Inquiring...** - The system is performing an Bluetooth Inquiry

**Syncing to [XXX]...** -- The system is attempting to synchronize to a piconet where the device with BD\_Address XXX is the master.

**Synced to [XXX]** - The system is synchronized to a piconet where the device with BD\_Address XXX is the master.

**Recording [XXX]** - system is recording the Bluetooth traffic of the piconet where the device with BD\_Address XXX is the master.

After the analyzer has synchronized to the Bluetooth piconet under observation, the Status Bar will display activity bars and the strength (in dBm) of the radio signal that Merlin is receiving. The activity bars will increase or decrease with activity. The signal strength readings will display as five possible values:

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

The valid range for a signal is between -60 and - 40 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.

## 4.4 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.

## 4.5 Merlin Analyzer Keyboard Shortcuts

Several frequently-used operations are bound to keyboard shortcuts.

**Table 2: 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





## 5. Recording Wizard

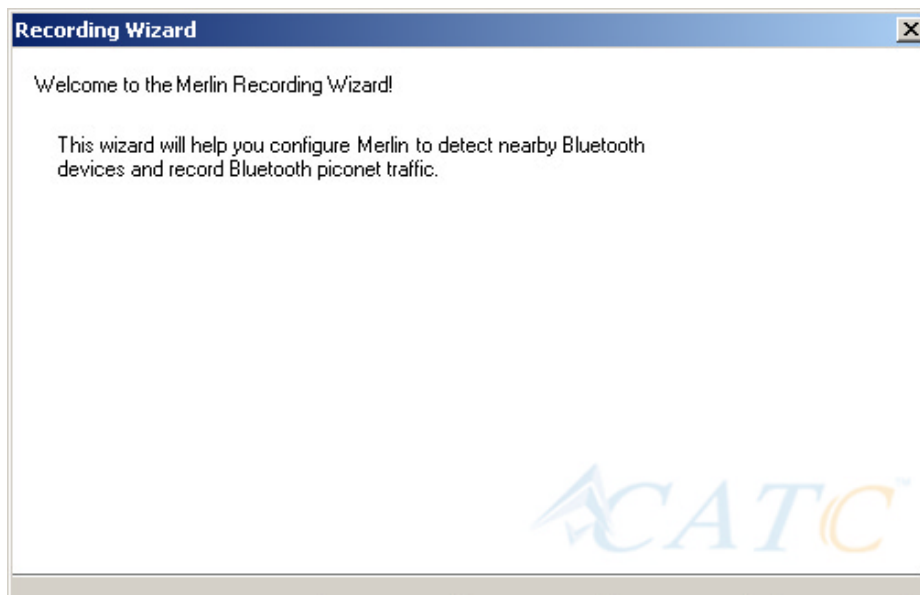
**Recording Wizard** is an interactive utility that presents a series of user-friendly dialog boxes for setting up a recording session. Recording Wizard serves as an alternative method of configuring the Recording Options dialog box. When you are finished using the Wizard, you can view your settings in the Recording Options window. 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:

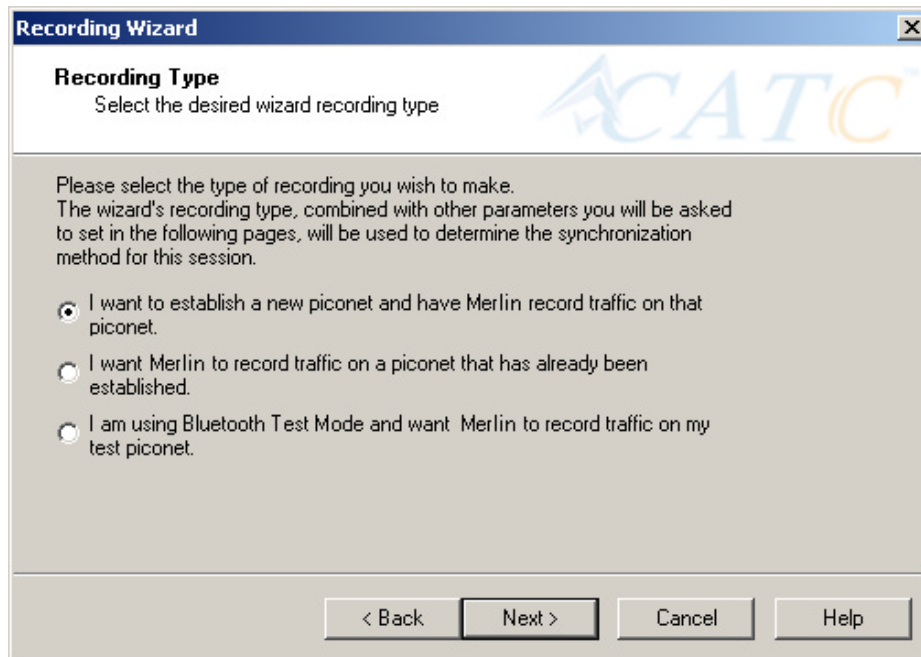


The **Recording Options** window has three buttons marked **Next**, **Back**, and **Cancel** that allow you to move forward or backward through the wizard or to cancel the wizard.

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:



- **I want to 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.

- **I want Merlin to record traffic on a piconet that has already been established.**

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

- **I am using Bluetooth Test Mode and want Merlin to record traffic on my 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.

## 5.1 Recording a Traffic on a New Piconet

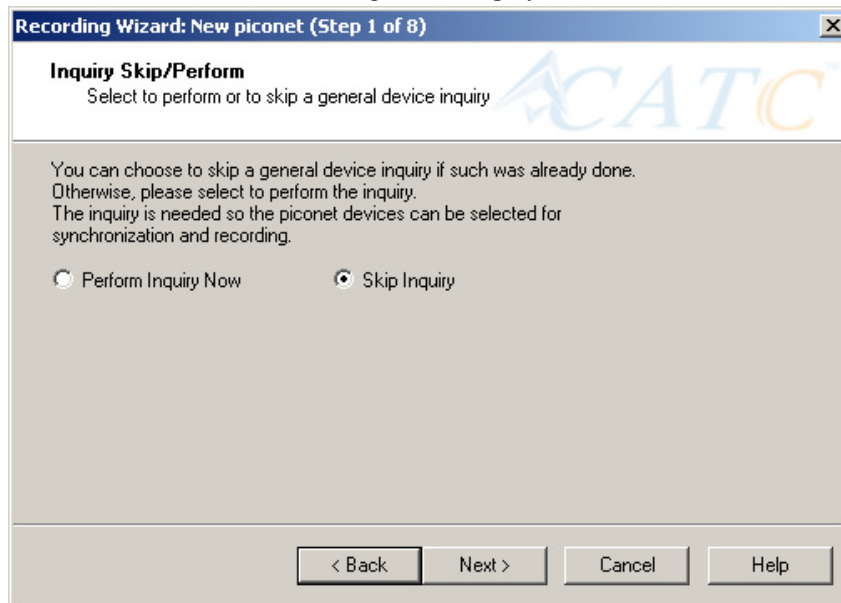
The **New Piconet** option shown in the previous screen presents users with the means of recording the traffic from a new piconet. This option will cause a sequence of screens to prompt you for information such as the piconet Master address.

The following steps show 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**.

I want to establish a new piconet and have Merlin record traffic on that piconet.

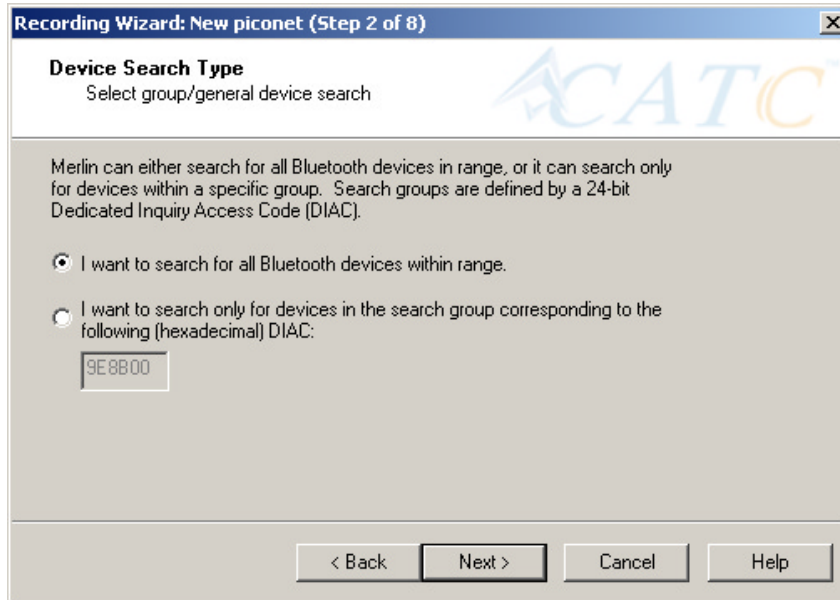
The following screen displays.



- Step 2** 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 6. 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**

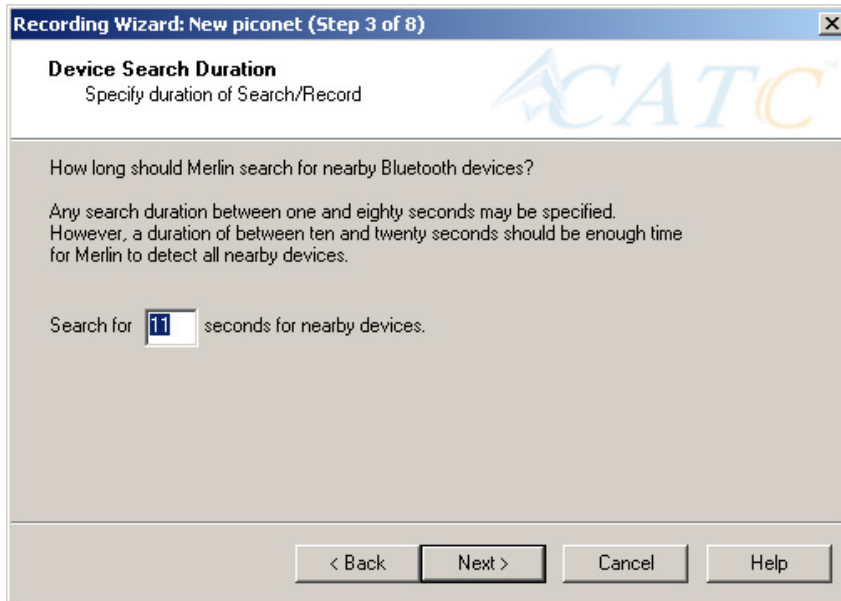
This option will cause Merlin to search for all Bluetooth devices that are in range and ready to transmit and receive data (i.e., in *Inquiry Scan Mode*)

- **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 3** Select the first option: **I want to search for all Bluetooth devices**

**within range**, then press **Next**. The following screen will display.



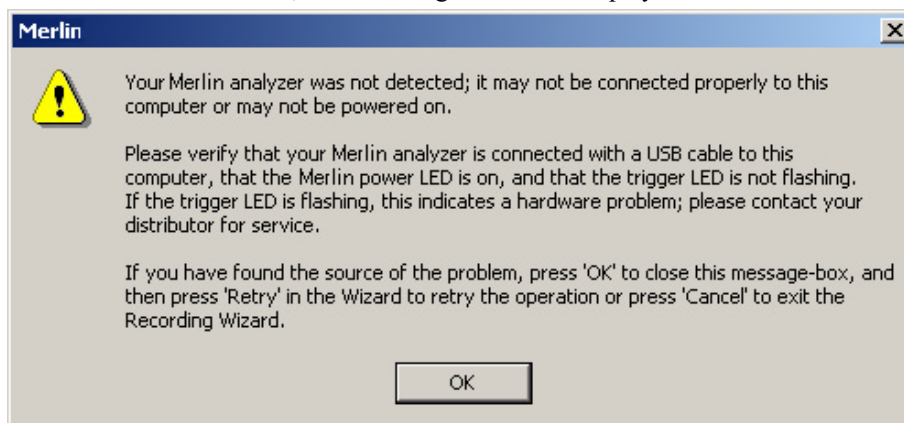
You will see two options:

- Step 4** In the text box, enter the length of time you want Merlin to search for nearby devices.

The default value is **11**. If you do not sure what time value to enter, use the default value.

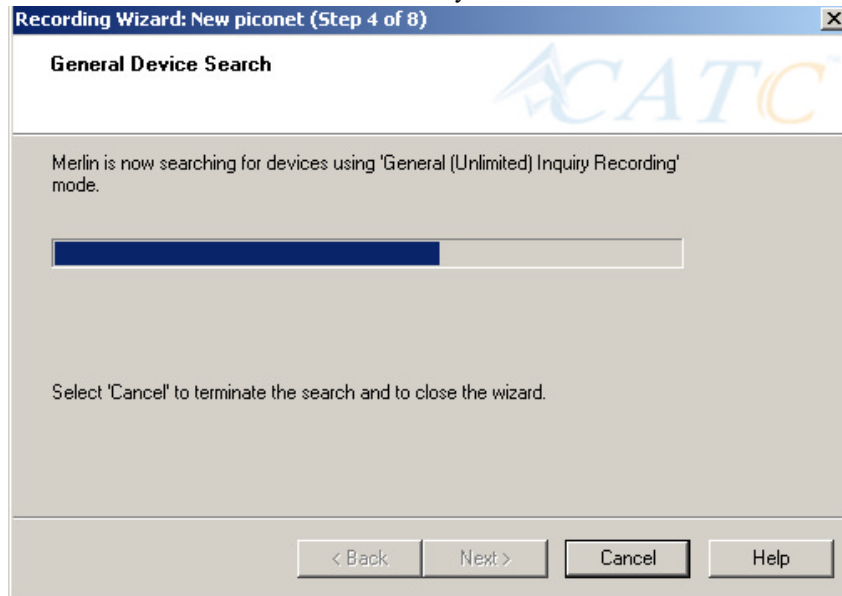
- Step 5** Press **Next**.

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

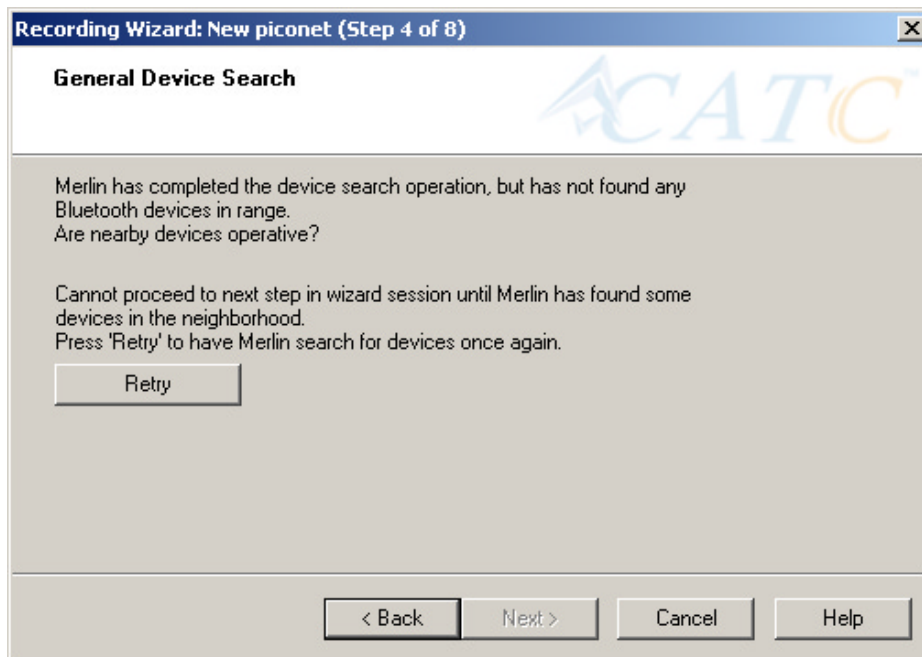


Clicking **OK** will close the message box.

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:

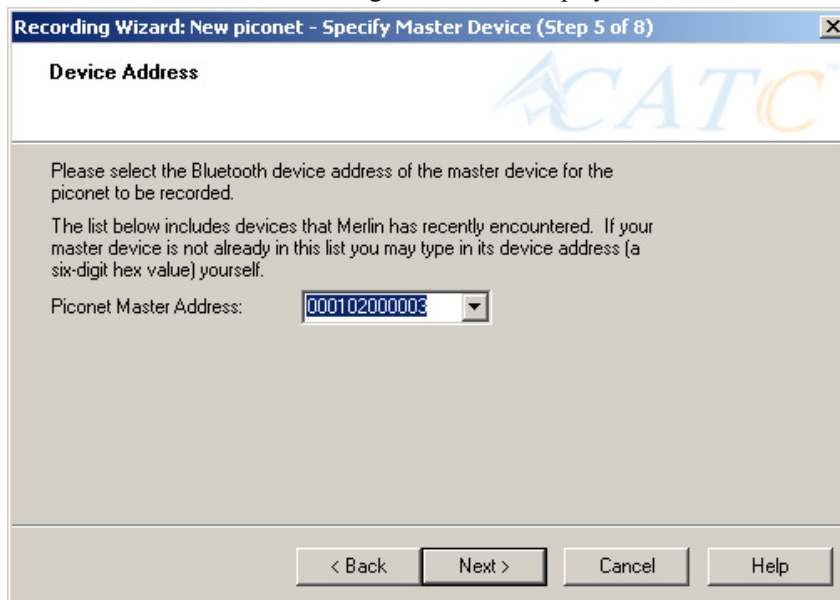


If devices found, the Recording Wizard will display the following screen:



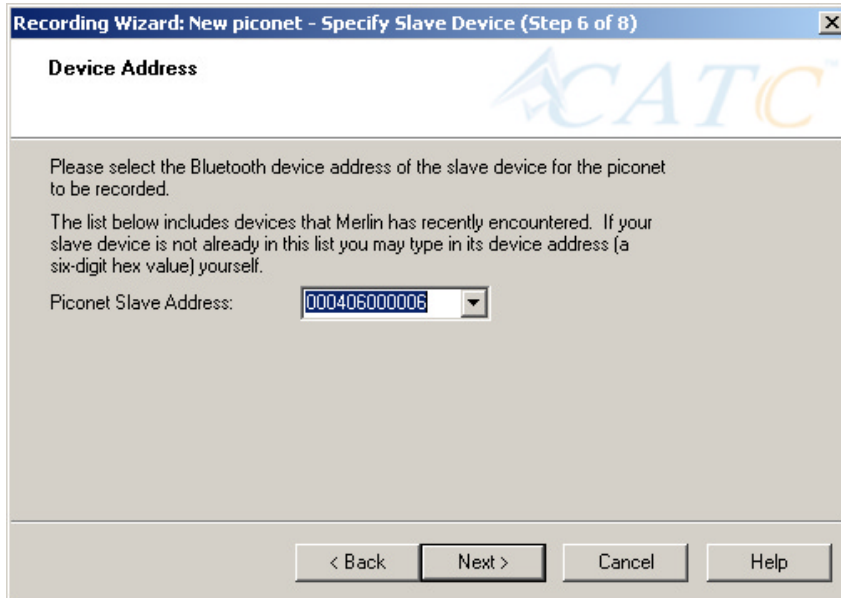
**Step 6 Press Next.**

The following window will display:



**Step 7** 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.

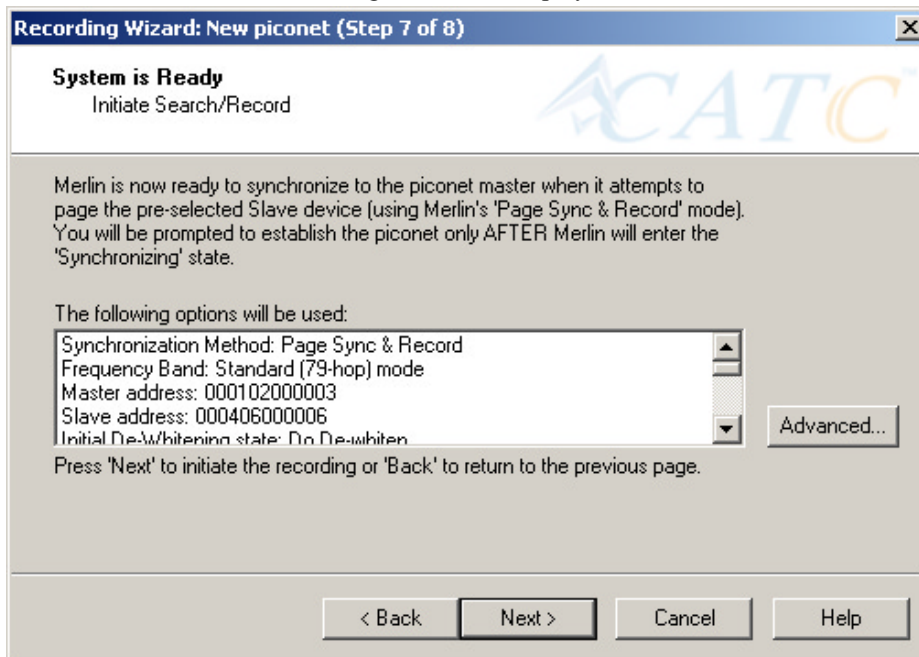
The following window will display:



**Step 8** 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 9** Press **Next**.

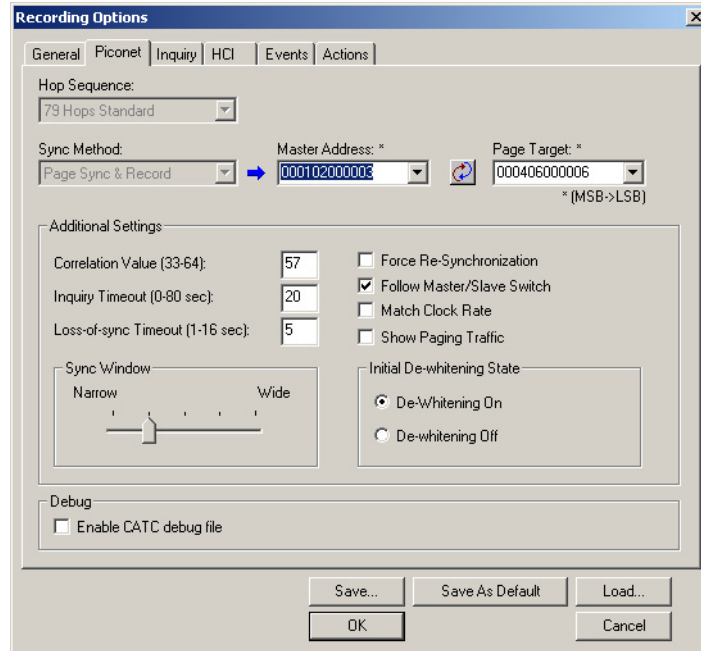
The following screen will display.



This screen displays the settings you selected.

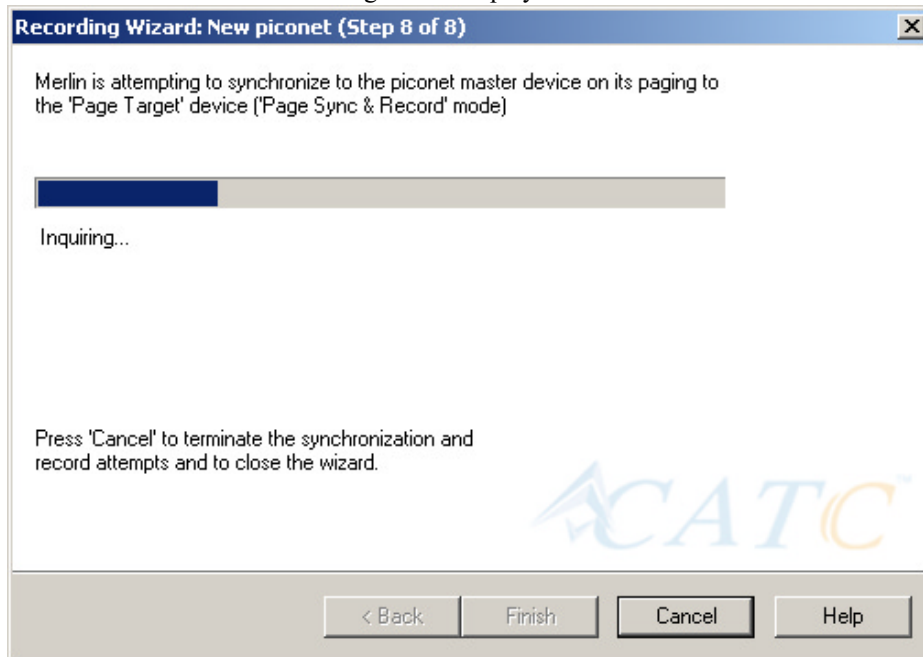


The **Advanced** button on the right will open the Recording Options dialog box shown below. This screen will show the settings you selected through the Recording Wizard have been applied to the Recording Options dialog.



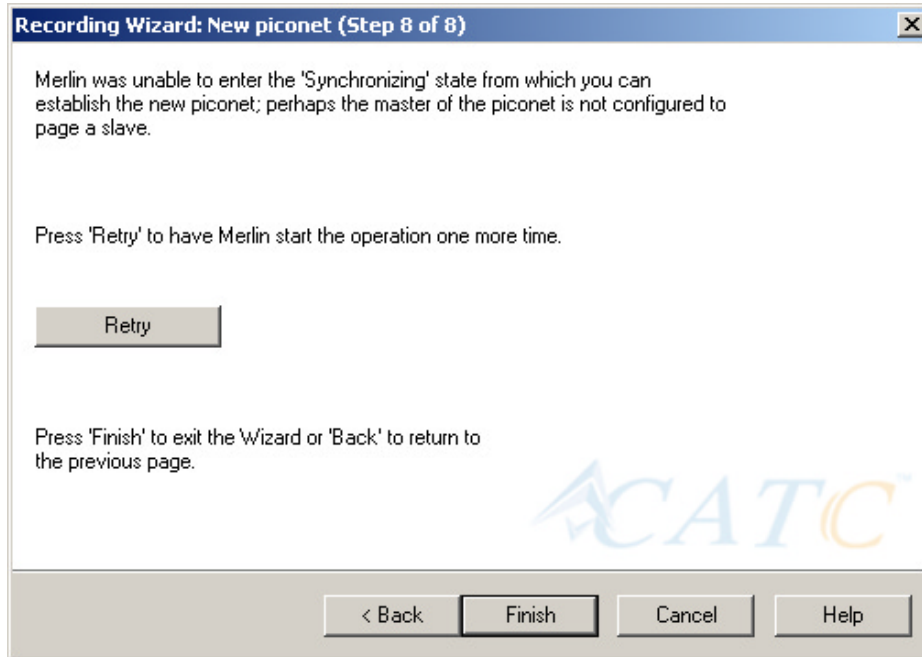
**Step 10** Press **Next** to advance the Recording Wizard to the next screen.

The following screen displays:

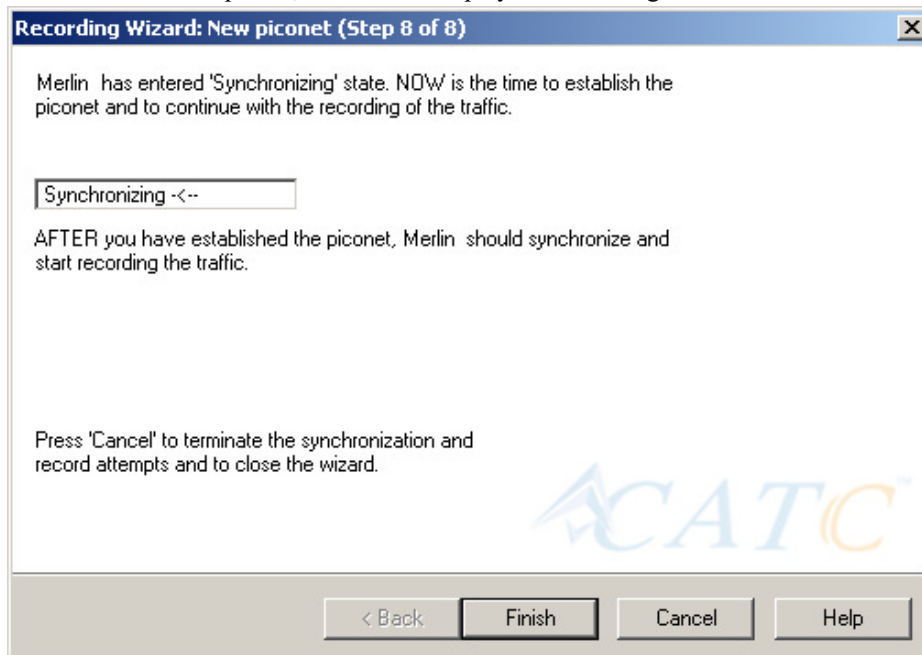


Merlin pages the Master and if specified in Step 8, the Slave devices.

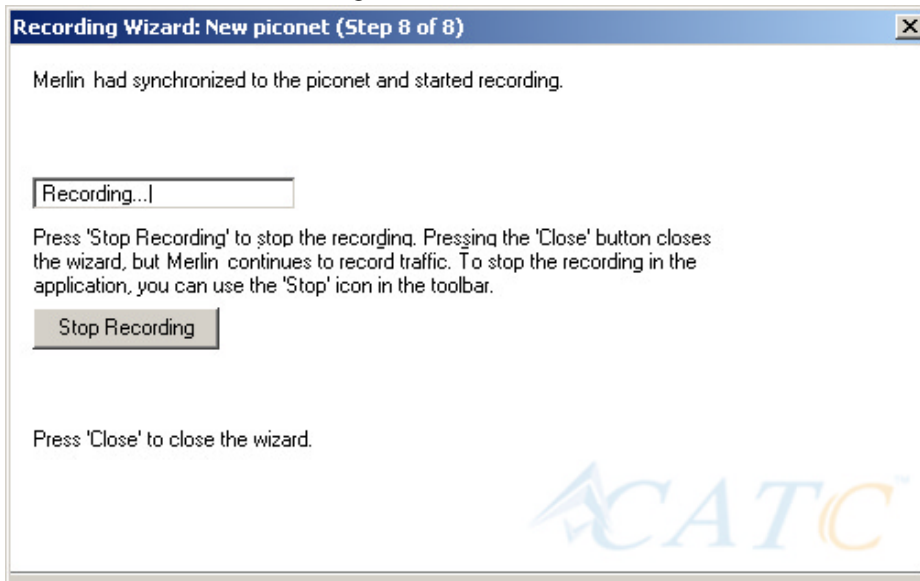
If Merlin is unable to complete its pages, the following screen will display:



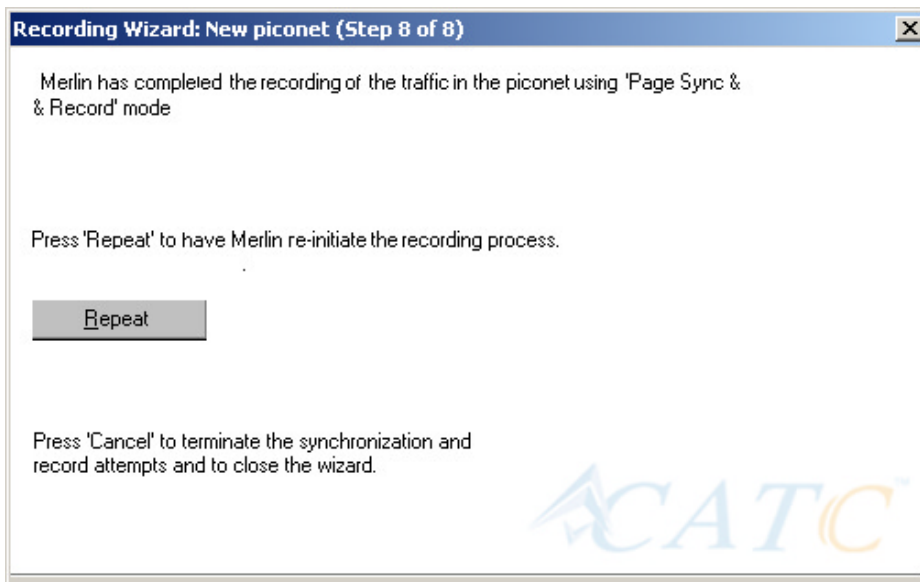
If Merlin is able to complete its pages, it will enter into a synchronizing state and then wait for you to create the piconet. During this waiting period, Merlin will display the following screen:



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



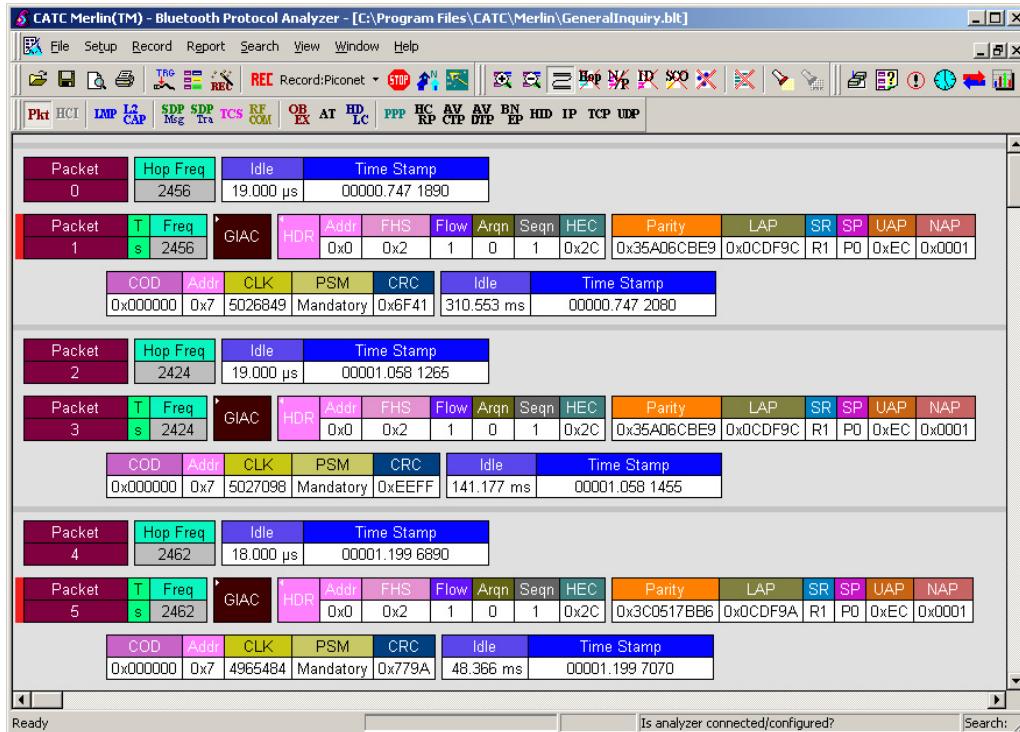
At the completion of the recording, Merlin will display the following screen:



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


**Step 11** To close the wizard, press the **Close** button.

The wizard will close and your trace will display.

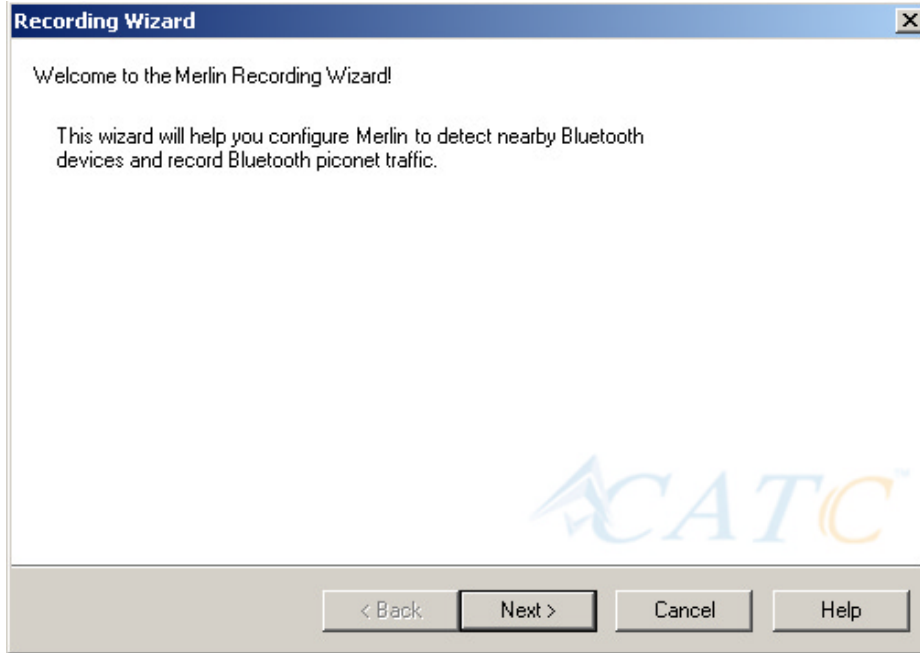


## 5.2 Recording an Existing Piconet

Using Recording Wizard to record an existing piconet is similar to recording a new piconet. The main difference is that you will be asked if your Master device can support multiple slave devices and whether it can respond to pages once it has created a piconet with another device.

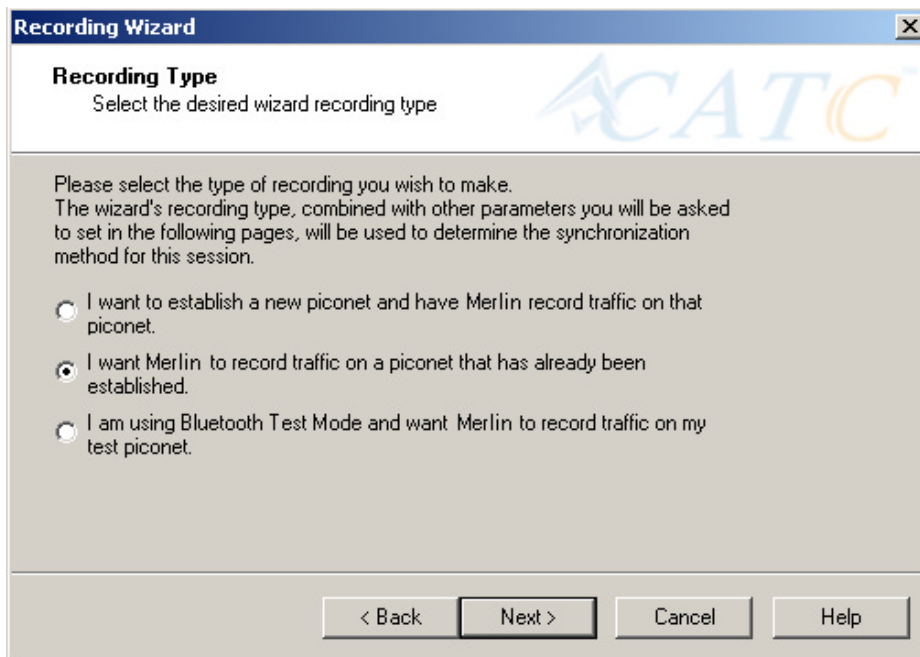
- Step 1** To start the Recording Wizard, press  or select **Setup > Recording Wizard** from the menu.

The Recording Wizard introductory page will open:



**Step 2** Press **Next** to advance to the next screen.

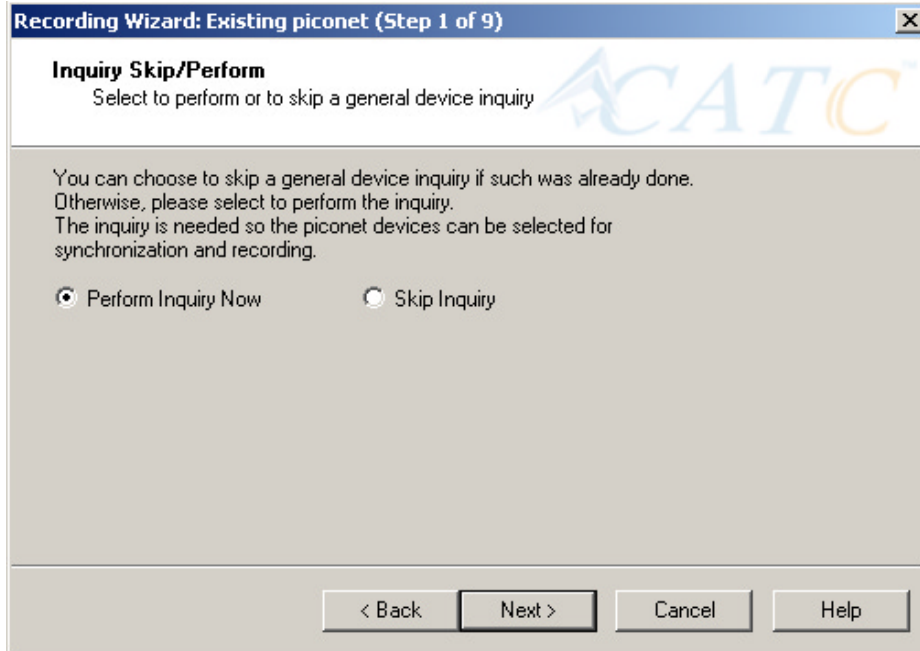
You will see three choices:



**Step 3** Select the second option: **I want Merlin to record traffic on a piconet that has already been established.**

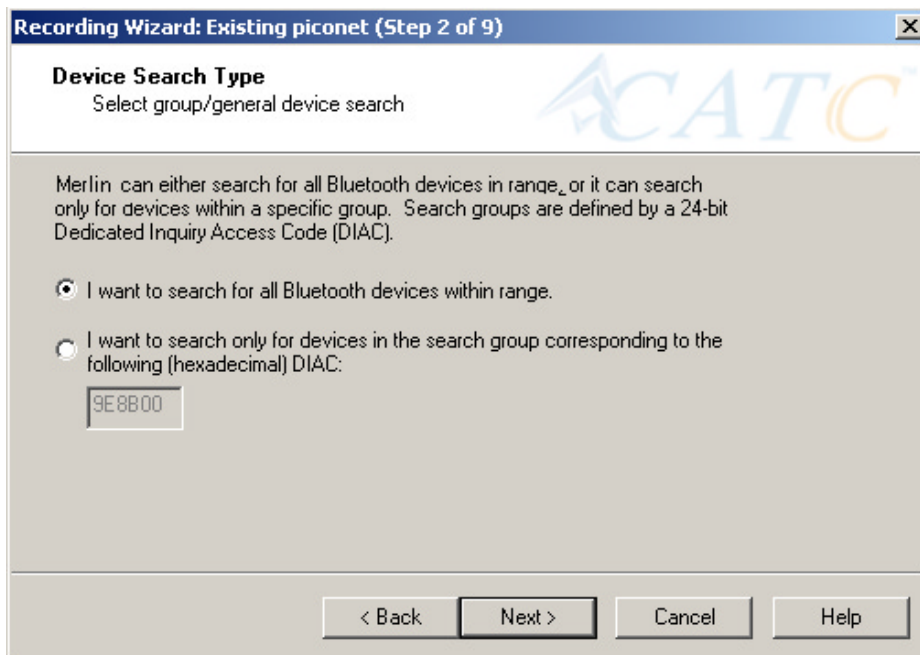
**Step 4** Press **Next**.

You will see two choices:



**Step 5    Select Perform Inquiry Now.**

You will see two choices:

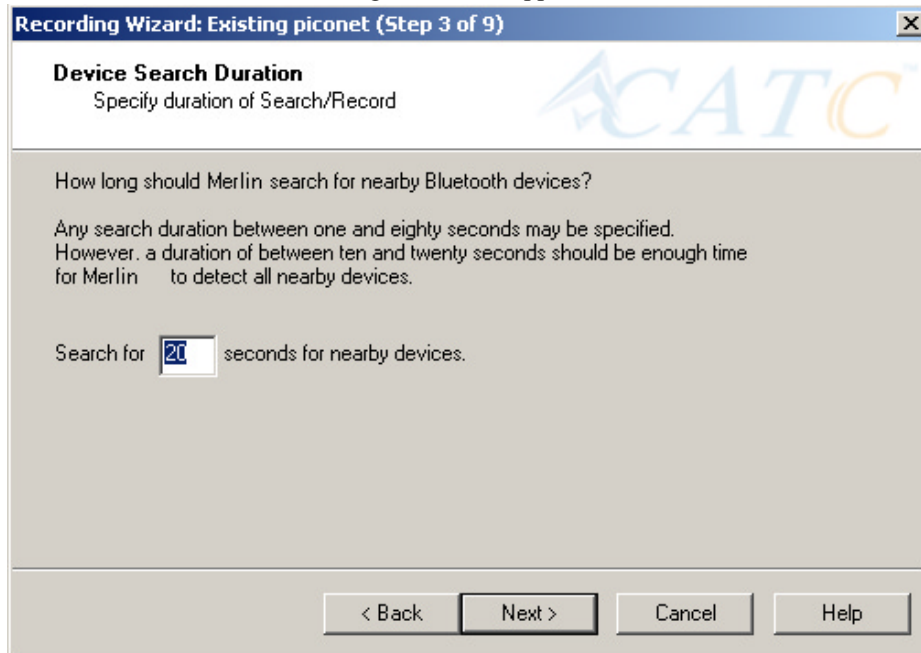


**Step 6    Select the first option: I want Merlin to search for all Bluetooth devices within range.**

If you want to limit the inquiry to a class of devices, select the second option and enter the hexadecimal value for the device class in the text box.

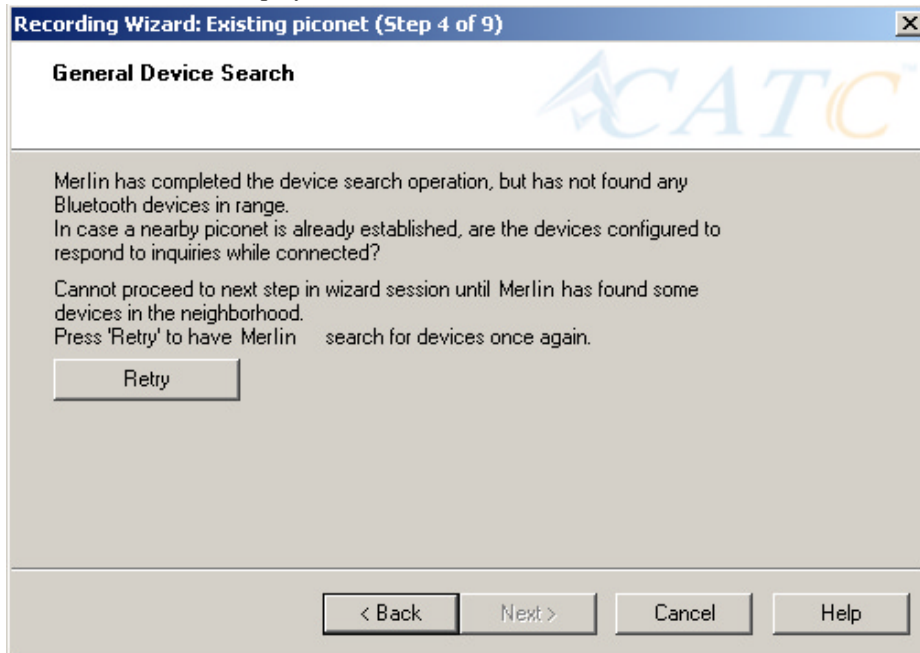
**Step 7** Press **Next**.

The following screen will appear:

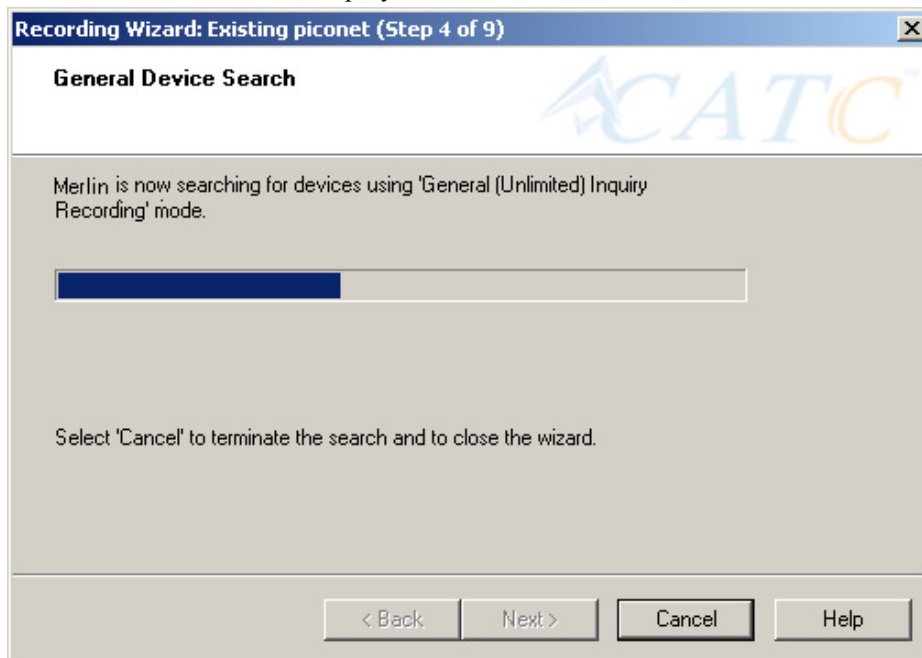


**Step 8** If you want to change the search duration, type in a new value into the text box. Otherwise, use the default value (20 seconds), then press **Next**.

If Merlin cannot detect other devices, the following message will display:



If Merlin passes the hardware test, it will then go on to conduct a General Inquiry to locate local Bluetooth devices.





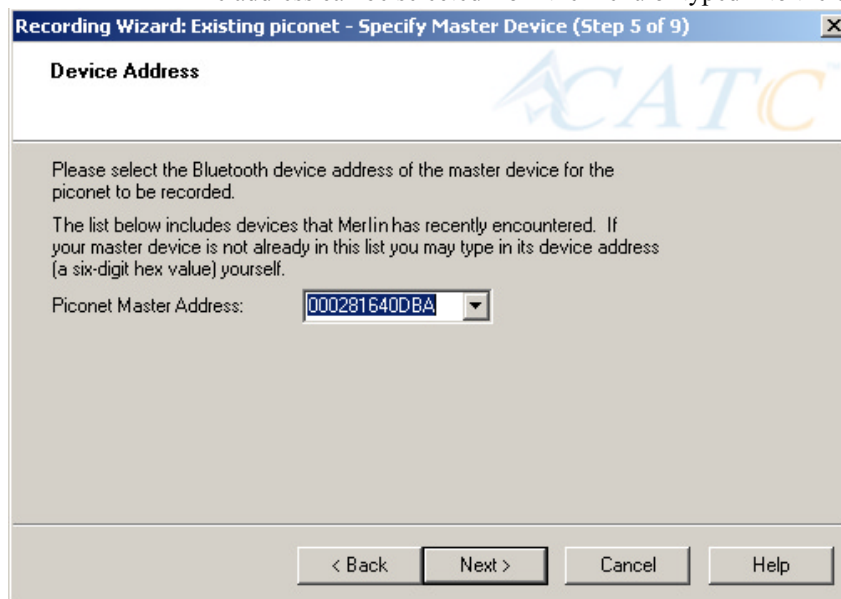
If Merlin finds Bluetooth devices, it will display the following message:



Check the Device List to see if Merlin found all of the devices in your piconet. If you feel that the list is incomplete, you can close this window and press the button marked **Repeat**. This will cause Merlin to repeat the General Inquiry and recollect information on local Bluetooth devices.

**Step 9** Press **Next** to advance to the next screen.

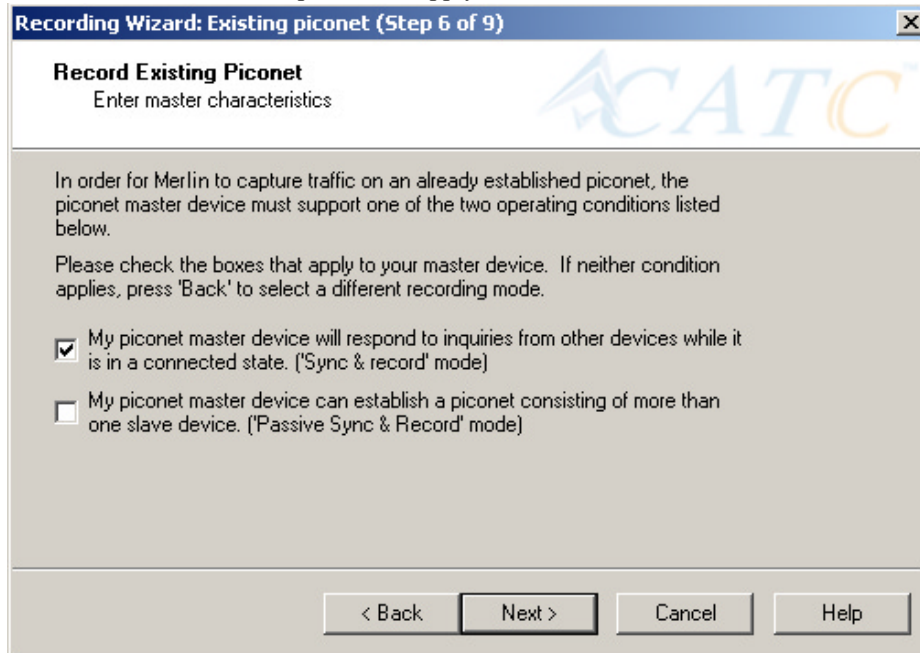
The following screen will prompt you for the Master device's address. The address can be selected from the menu or typed into the box:



**Step 10** Select or type in the Master device's address into the box next to the label **Piconet Master Address**.

**Step 11** Press **Next**.

The following screen will display. This screen asks you which of the following two options apply to your Master device. For some devices, both options will apply.



You can select either or both options. They are not mutually exclusive:

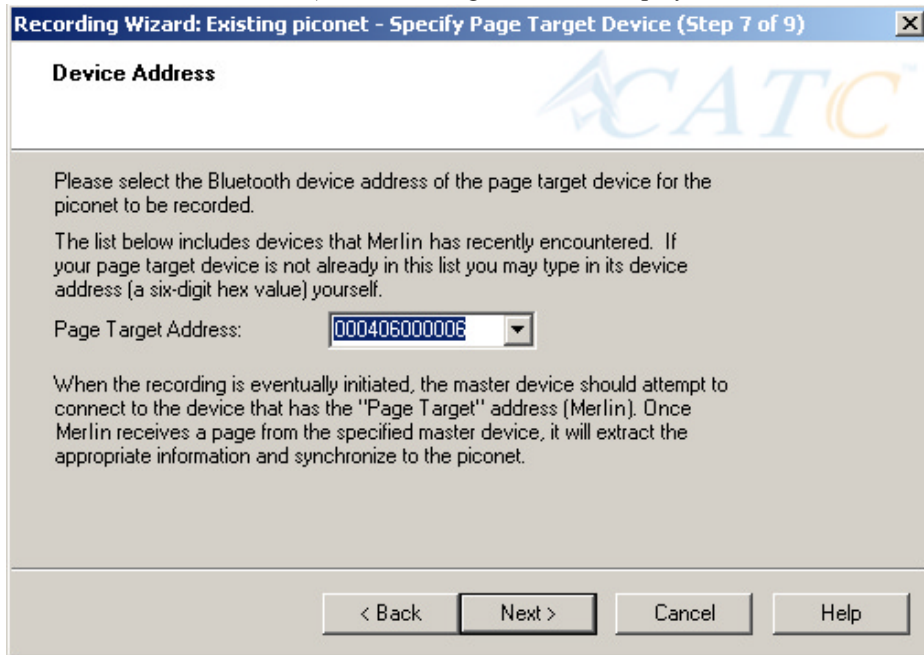
If the Master supports inquiries while in a connected state, select the first option. This will set Merlin to use the 'Sync & Record' mode in its attempts to synchronize to the Master. This will also cause the wizard to skip to step 8.

If the Master can support piconets with multiple slaves, select the second option. If you select this box alone (i.e., you leave the first box unchecked), Merlin will use the 'Passive Sync & Record' mode to synchronize to the Master. The wizard will then advance to Screen 8\*.

If the first checkbox was selected, Merlin will use 'Sync & Record' no matter what was set in the second box.

**Step 12** If you want to skip the Master verification, put a check in the box. If you are in doubt, leave the box unchecked.

If you selected only the second option in Step 12 (= 'Passive Sync & Record'), the following screen will display.



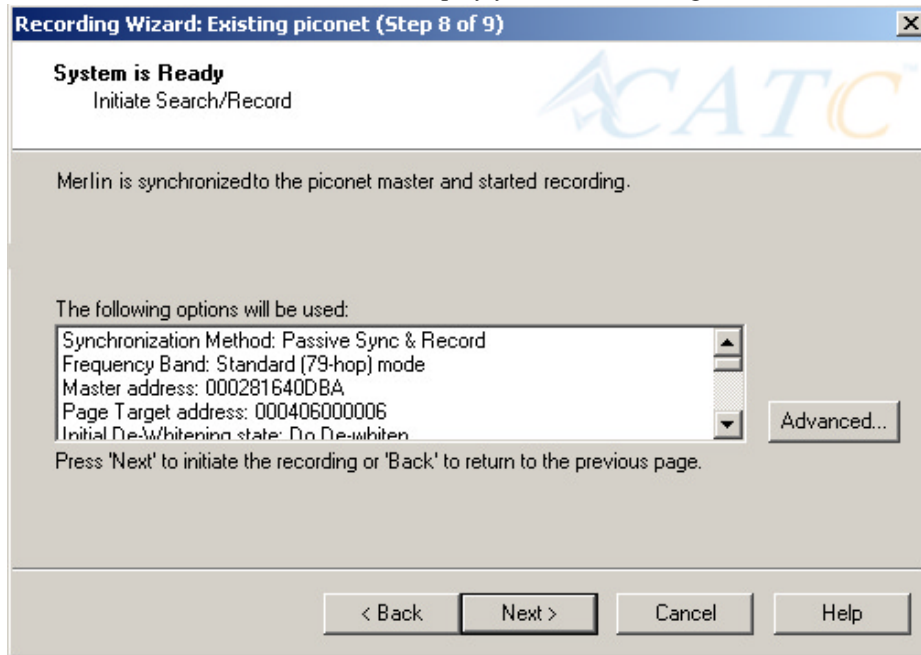
This screen asks you for the address of the Page Target device -- which in this case is Merlin. Since the devices in your piconet are not able to respond to inquiries, Merlin will not be able to page the devices and join the piconet. Instead, you will assign Merlin an address here in this screen, then direct your piconet Master device to connect to Merlin. The Master will attempt to connect to Merlin and therein give Merlin the information it needs to record the Master and slave devices.

**Step 13** Type in an address of your choosing for Merlin (= Page Target).

You are making up an address for Merlin that the Master will use to try to connect to Merlin.

**Step 14 Press Next**

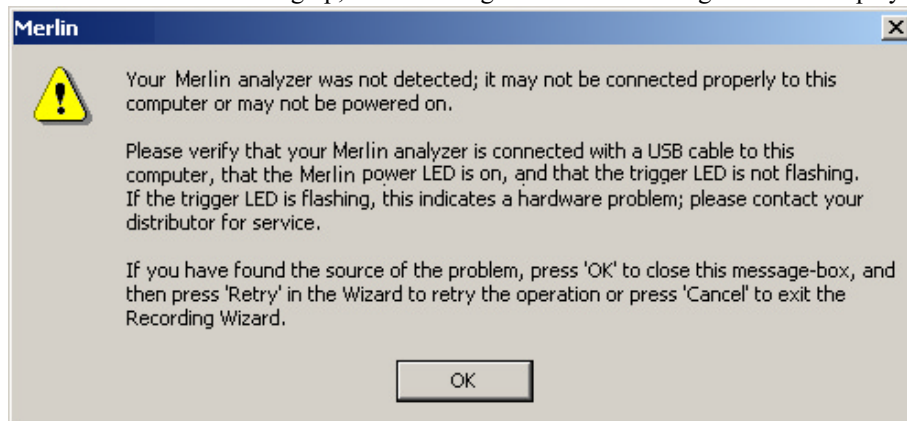
Merlin will then display your current settings.



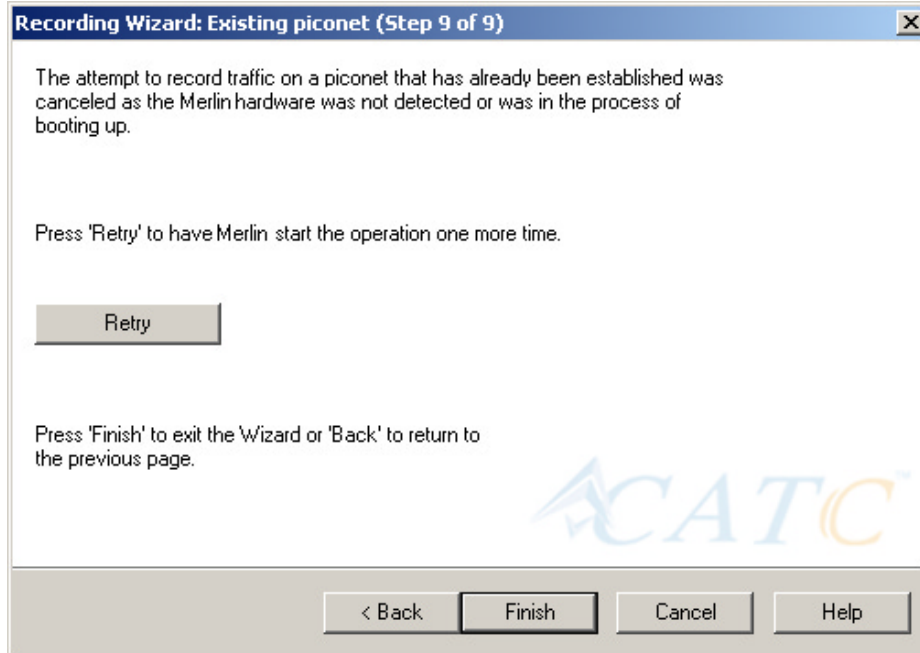
The **Advanced** button will open the Recording Options dialog box shown on page 49 and described in detail in Chapter 7.

**Step 15 Press Next to begin the recording.**

If the Merlin hardware is not ready or connected or is in the process of booting up, the following information message box will display:

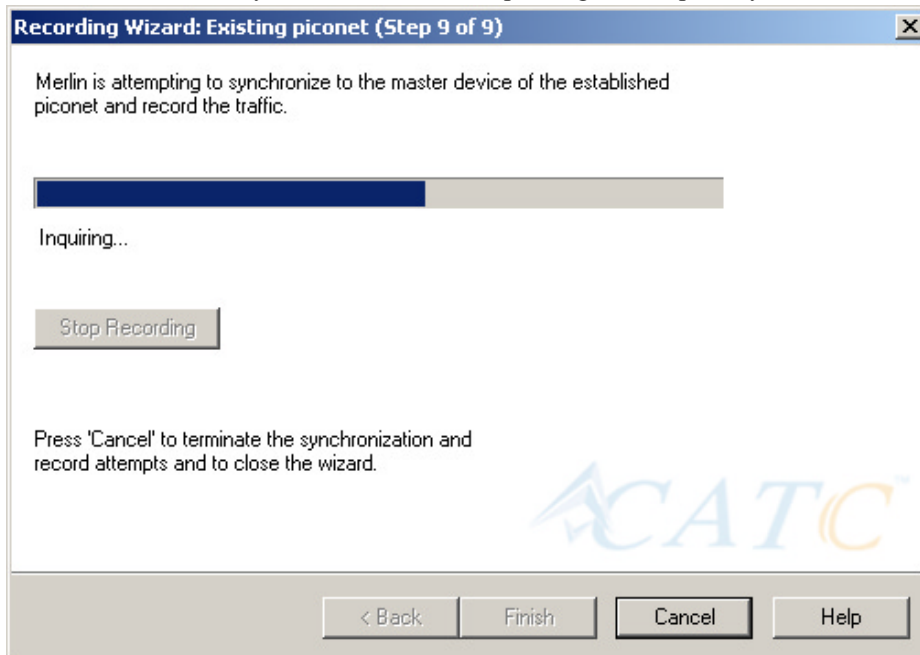
**Step 16 If the above information box opened, press OK to close it.**

The following dialog box will display:



**Step 17** Press **Retry** or **Back** to re-attempt the process.

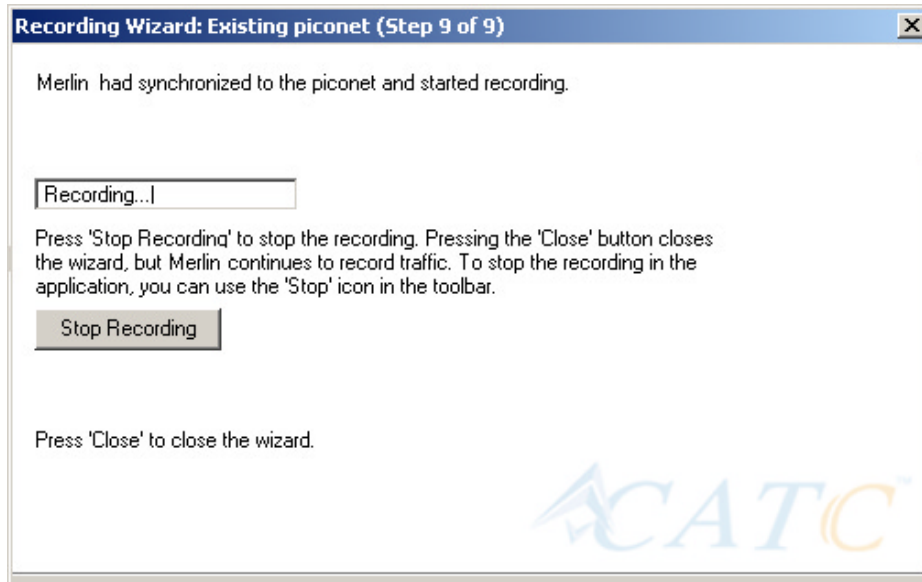
If the hardware failure described above do not occur, Merlin will conduct an inquiry. The screen will show that Merlin is going to attempt a recording in either 'Passive Sync & Record' mode as shown below or in 'Sync & Record' mode depending on the options you selected in Step 15.



**Step 18** If you are recording in 'Passive Sync & Record' mode, you will

need to direct your Master device to attempt a connection to Merlin. This will provide Merlin with the information it needs to record the piconet.

Once Merlin has the information it needs, it will begin recording. The following screen will display:



The recording will end following a trigger event or when you press **Stop Recording** button on the screen shown above or when you press the button on the toolbar.

**Step 19** When finished, press **Close** to close the Recording Wizard.

## 5.3 Recording in Test Mode

A Test Mode recording allows you to limit the frequency hopping range that Merlin will record. Two Test Modes are available: Reduced Hopping Mode and Single Frequency Mode. Reduced Hopping Mode limits Merlin's recording to the five frequency hops that are described in the Bluetooth Specification. Single Frequency Mode limits Merlin's recording to a single frequency range that you specify in the Recording Wizard.

### Recording in Reduced Hopping Mode

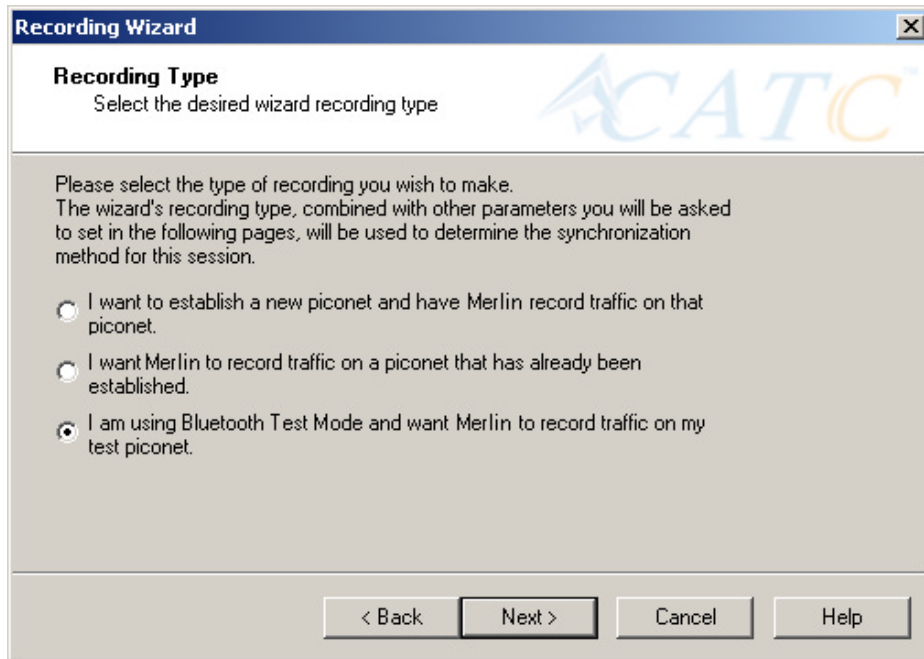
To record in Reduced Hopping Mode, perform the following steps:

**Step 1** Start the Recording Wizard by either pressing the button  or selecting **Setup > Recording Wizard** from the menu.

The Recording Wizard greeting screen will open.

**Step 2** Press **Next** to advance to the **Recording Type** screen.

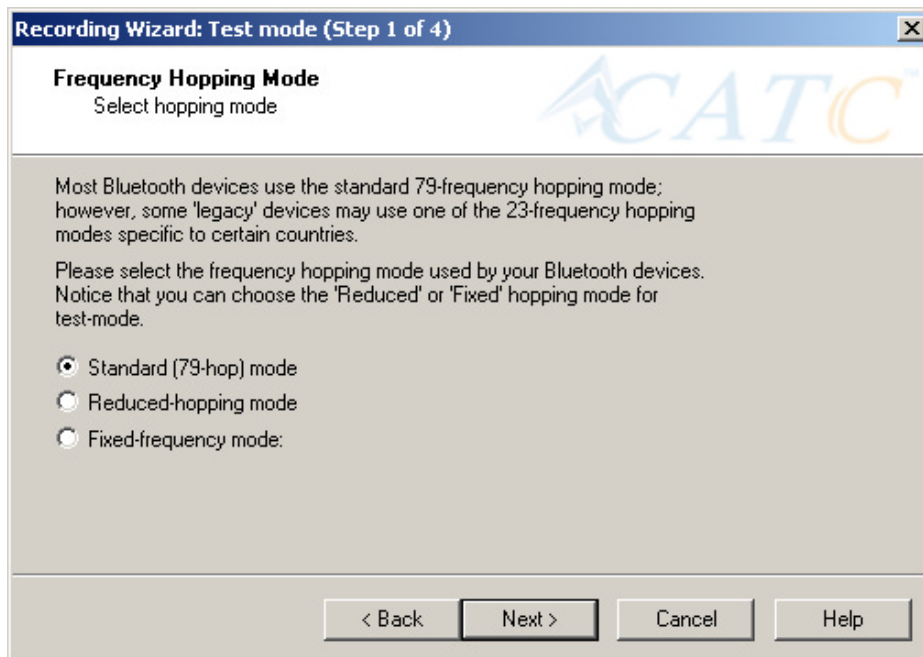
The following screen will display:



**Step 3** Select the third option: **I am using Bluetooth Test Mode and want Merlin to record traffic on my test piconet.**

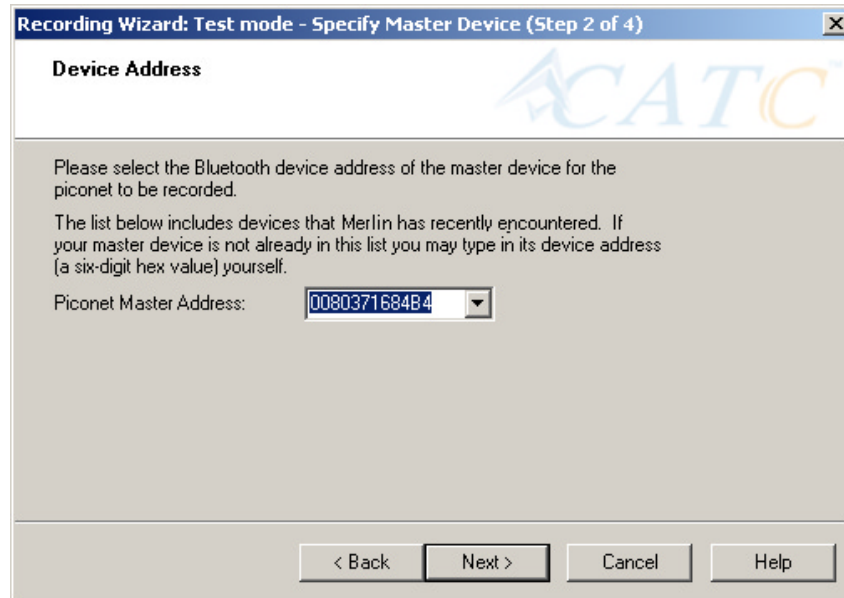
**Step 4** Press **Next**.

The following screen will display:



**Step 5** Select the option **Reduced-hopping mode**, then press **Next**.

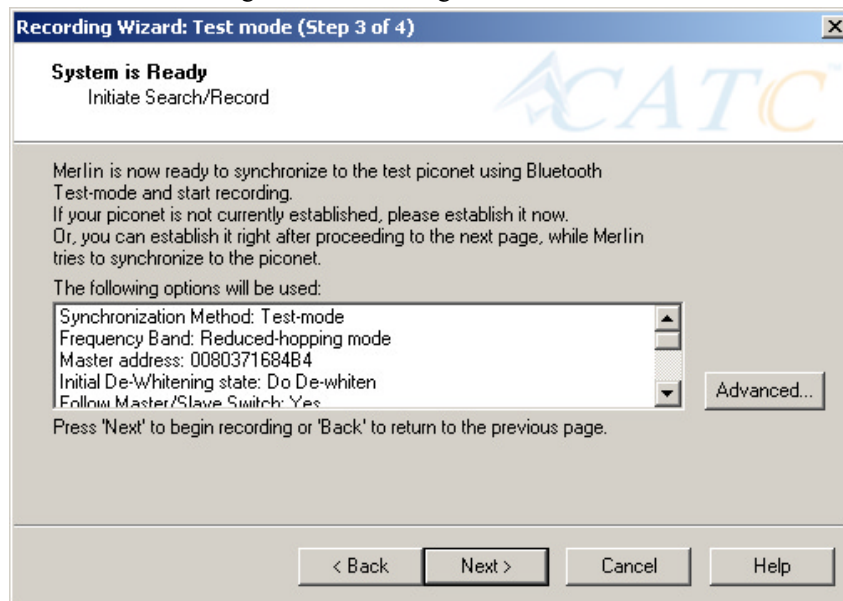
The following screen will display:



**Step 6** Select the address for your piconet's Master device from the drop-down menu. If you prefer, you can type in the address into the box.

**Step 7** Press **Next**.

The following screen will display. This screen will show the current settings for the recording:

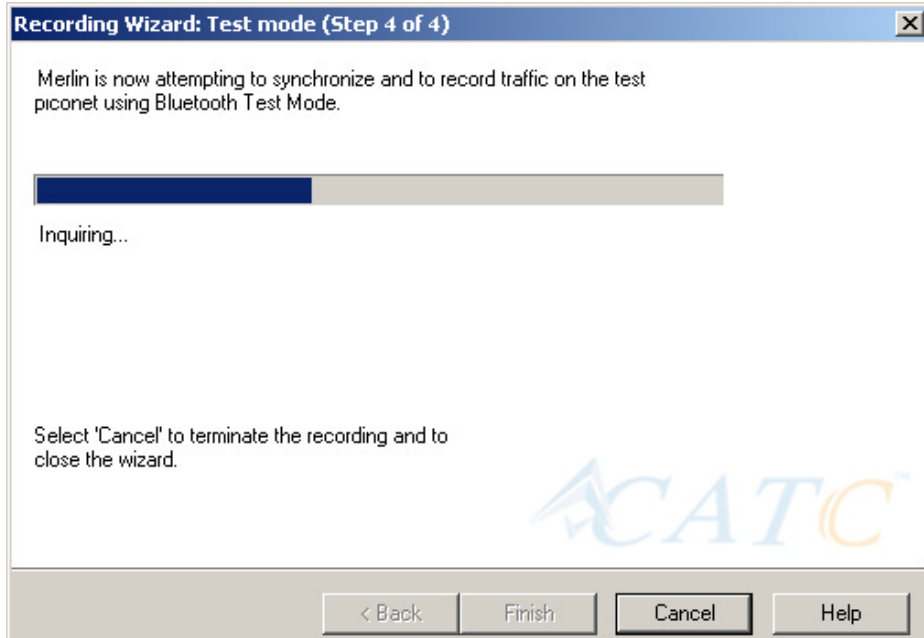




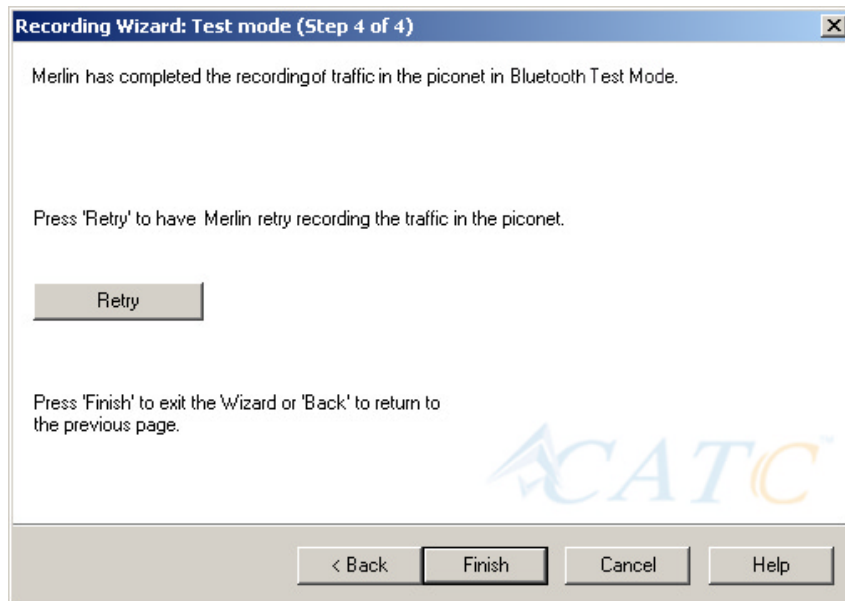
The Advanced button will open the Recording Options dialog box. See Chapter 7 for details on the Recording Options dialog box.

**Step 8** Press **Next** to begin the recording.

The following screen will display:



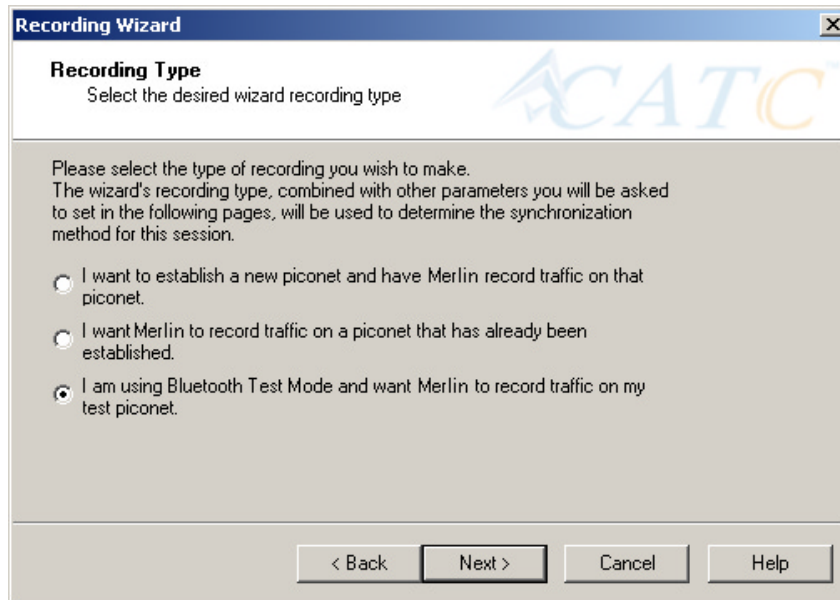
**Step 9** When the recording finishes, the following screen will display. You can repeat the recording by pressing the **Repeat** button.



**Step 10** To close the wizard, press **Finish**.

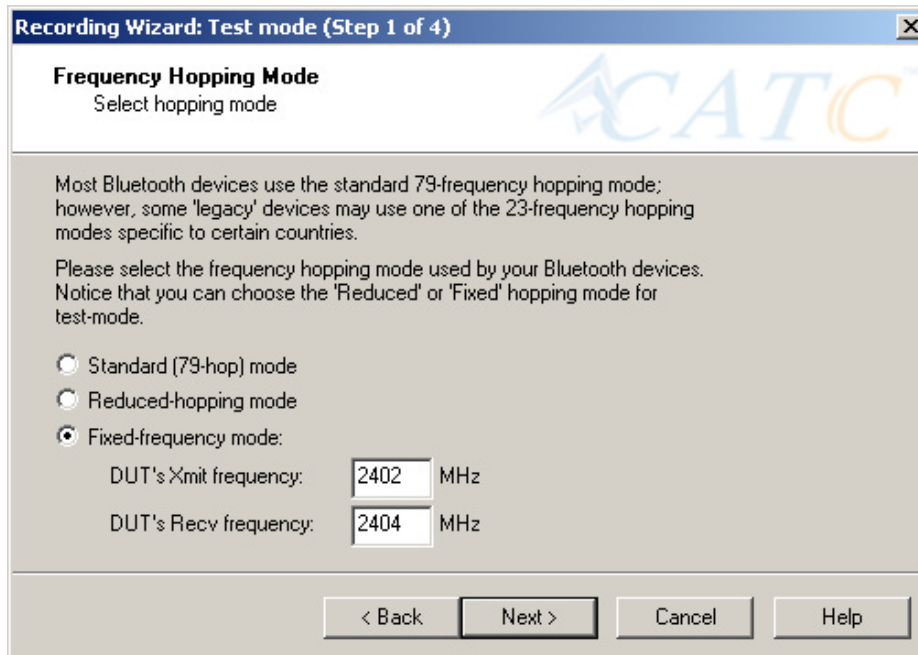
## 5.4 Recording in Single Frequency Mode

**Step 1** In the Recording Type window, select the third radio button



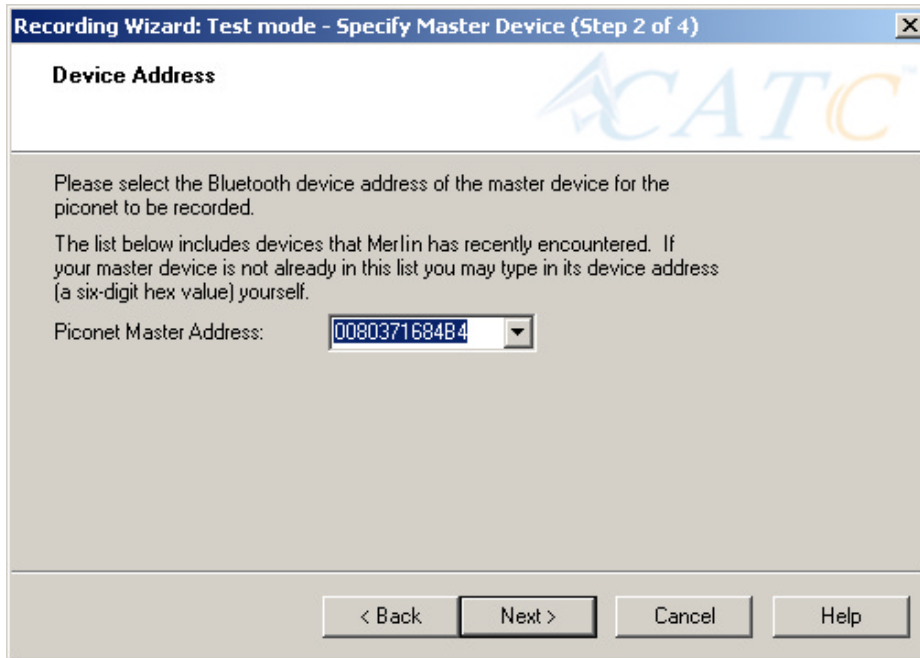
and click **Next**.

**Step 2** In the **Frequency Hopping Mode**, window select the **Fixed-Frequency Mode** radio button, enter the appropriate values in the text boxes, and click **Next**.

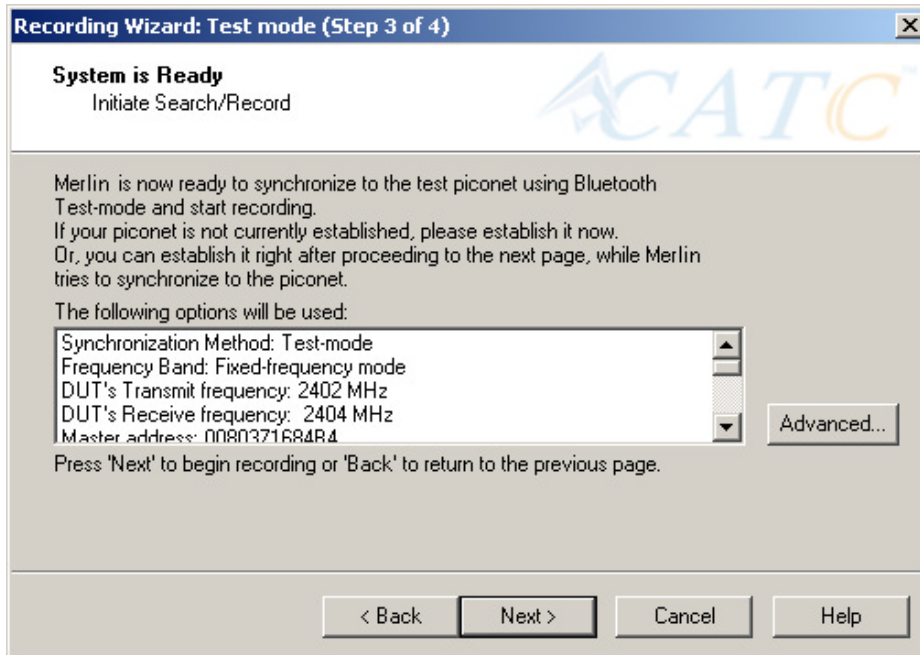


**Step 3** In the Master Device address box, enter the BD Address for

your Master Device.

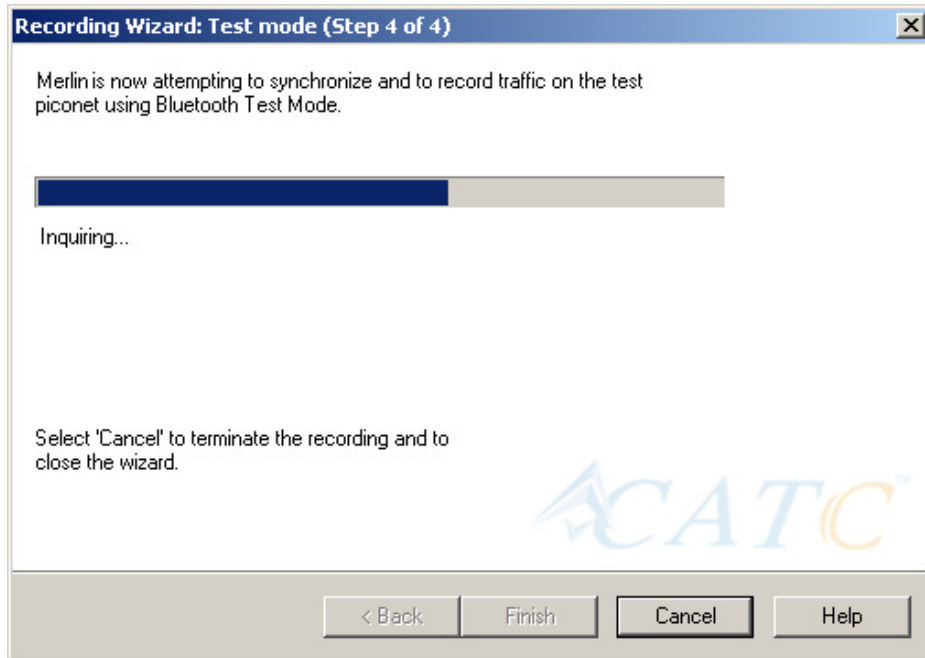


**Step 4 Press Next.**



**Step 5 Press Next.** Merlin then synchronizes with the Master

device and begins recording.

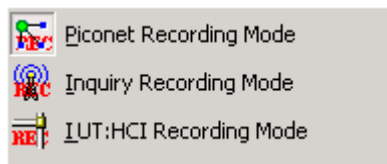


## 6. Recording Options

The **Recording Options** dialog box provides an alternative method of setting up a recording to the Recording Wizard, described in the previous chapter. In this dialog box are all of the settings needed to make a recording. Once you have selected your recording options, you then select the recording mode by clicking the down-arrow on the Record button and selecting from the two mode options: Piconet and Inquiry. Merlin will then use the relevant Recording Options for the selected mode. For example, if you select **Piconet** recording mode, Merlin will use the options from the **Piconet** page in the Recording Options dialog box.

### 6.1 Recording Modes

Pressing the down-arrow on the Record button displays a menu with four Recording Modes:



Selecting one of these modes tells the analyzer what sets of Recording Options it should use when you begin a recording.

**Note:** Selecting a Recording Mode from the menu does not cause the analyzer to begin recording. To begin recording, you must press the Recording button itself.

#### **Piconet recording**

Selecting **Piconet**, configures Merlin to record piconet traffic using the parameters set in the Piconet page in the Recording Options dialog box. When you begin recording in this mode, Merlin will try to synchronize to a piconet that matches the Piconet parameters set in the Recording Options. The recorded traffic is captured off-the-air.

#### **Inquiry recording**

This mode configures Merlin to record Inquiry traffic. When setting the Merlin to Inquiry recording, the system is ready to perform a Bluetooth 'General' or 'Dedicated' inquiry, according to the parameters specified in the


'inquiry' page of the Recording Options. The recorded traffic would consist the transmitted packets as well as the responses received from Bluetooth devices in the area.

### **IUT:HCI mode**

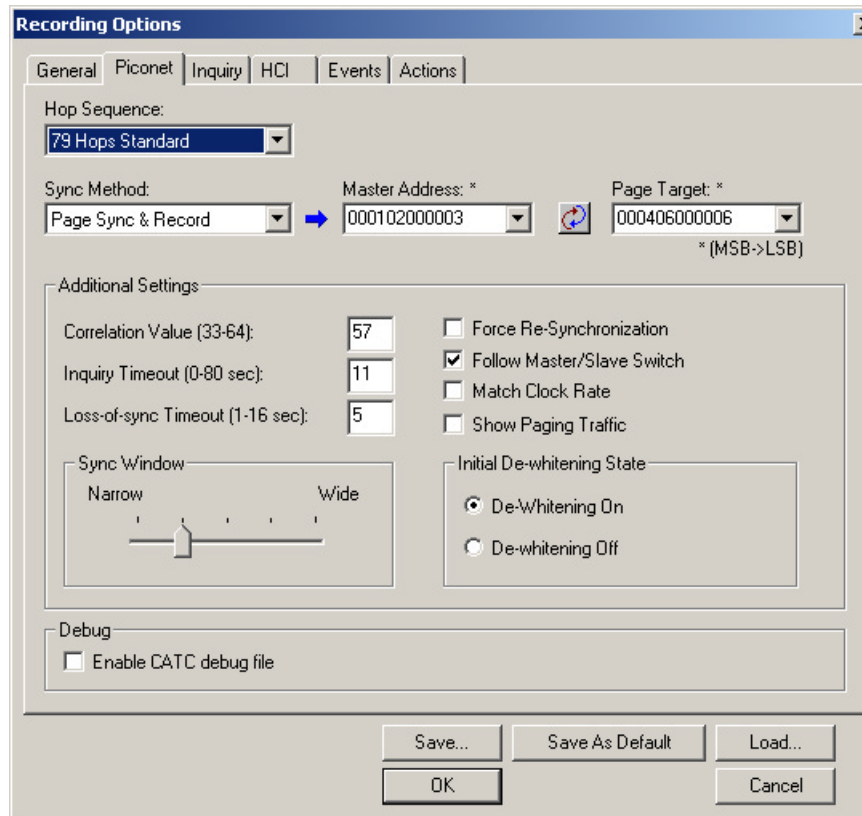
Configures the system to exclusively record HCI traffic from IUTs. This recording mode bypasses the analyzer: HCI traffic from the IUT is recorded directly by the analyzer software without going through the analyzer. This means that you can record HCI traffic even if the analyzer is not turned on.

To record HCI traffic, first enable the recording of HCI traffic from IUTs. You do this in the HCI page of the Recording Options dialog. Then set the recording mode to something other than IUT:HCI. If you want to prevent the recording of HCI traffic from IUTs, disable it in the HCI page of the Recording Options dialog.

## 6.2 Opening the Recording Options Dialog Box

To open the **Recording Options** menu, click  on the Tool Bar or select **Recording Options** under **Setup** on the Menu Bar.

You see the **Recording Options** window. By default, the **Piconet** options page displays:

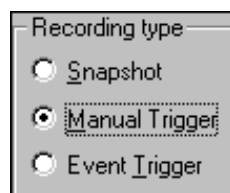


You will need to set options for each of the Recording Options pages. Generally, it is best to begin with the **General** and **Piconet** pages where you can set the type of recording, and then move on to the **Events** and **Actions** pages where you can set triggering events.

## 6.3 Recording Options - General

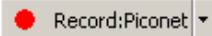
The General page controls the length of a recording and how it begins and ends. It is shown in the previous illustration. The General page displays four boxes marked *Recording Type*, *Buffer Size*, *Trigger Position*, and *Options*.

### Recording type

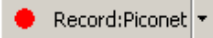



The **Recording Type** box presents options that control how Merlin begins and ends a recording. The options are: *Snapshot*, *Manual Trigger*, and *Event Trigger*.

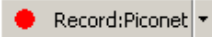
### Snapshot

A Snapshot is a fixed-length recording whose size is determined by the "Buffer Size" box in the Recording Options dialog or by a manual click of the Stop button. Recording begins by clicking  on the Tool Bar and ends when either the selected buffer size is filled or you press the Stop button.

### Manual Trigger

A Manual Trigger recording is a one that is manually begun and ended. Recording is begun by pressing  on the Tool Bar. Recording continues in a circular manner within the limits set by the buffer size. Recording ends when  is clicked on the Tool Bar or the Trigger button is pressed on the analyzer's front panel. If you press the Trigger button, recording will continue until the post-trigger memory has been filled.

### Event Trigger

An Event Trigger recording is one that uses an event trigger to end the recording. Before recording begins, you define the event trigger in the Trigger Options dialog box. You begin the recording by clicking  on the Tool Bar. Recording continues in a circular manner within the limits set by the buffer size. Once the trigger event occurs, some post-trigger recording occurs, then the recording ends.

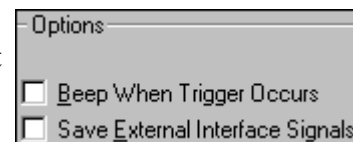
**Note** In this mode, the recording can be stopped manually in the same way as for "manual trigger" mode.

## Options

The Options box contains two options:

### Beep When Trigger Occurs

Will cause the PC to beep when a trigger event has occurred.

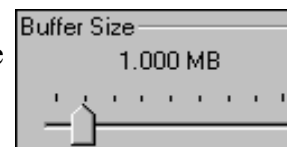


### Save External Interface Signals

Will enable Merlin to record input signals from a breakout board as fields in a trace.

## Buffer Size

The Buffer Size box has a slide bar for adjusting the recording buffer size from 0.4 megabytes to 512 megabytes.



The Recording Type option determines how this buffer is used. Although there are 512 megabytes of physical memory in the analyzer, the efficiency of the recording ranges from 2:1 to 4:1 ratios of physical memory to actual

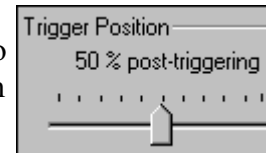


Bluetooth traffic. Shorter Bluetooth packets yield a less efficient recording. The non-traffic portion of physical memory is utilized for control and timing information.

**Note** The scale is not linear and affords more granularity in the smaller buffer sizes.

### Trigger Position

The Trigger Position slide bar sets the amount of post-trigger recording that Merlin will perform. It also allows adjustment of the location of the trigger within the defined buffer. You can adjust the Triggering Position between 1 and 99% post-Trigger. **Trigger Position** is available only when **Manual Trigger** or **Event Trigger** is selected as **Recording type**.



As an example, if the buffer size is set to 16MB, then for the following Trigger Position settings, the amount of pre- and post-Trigger data is

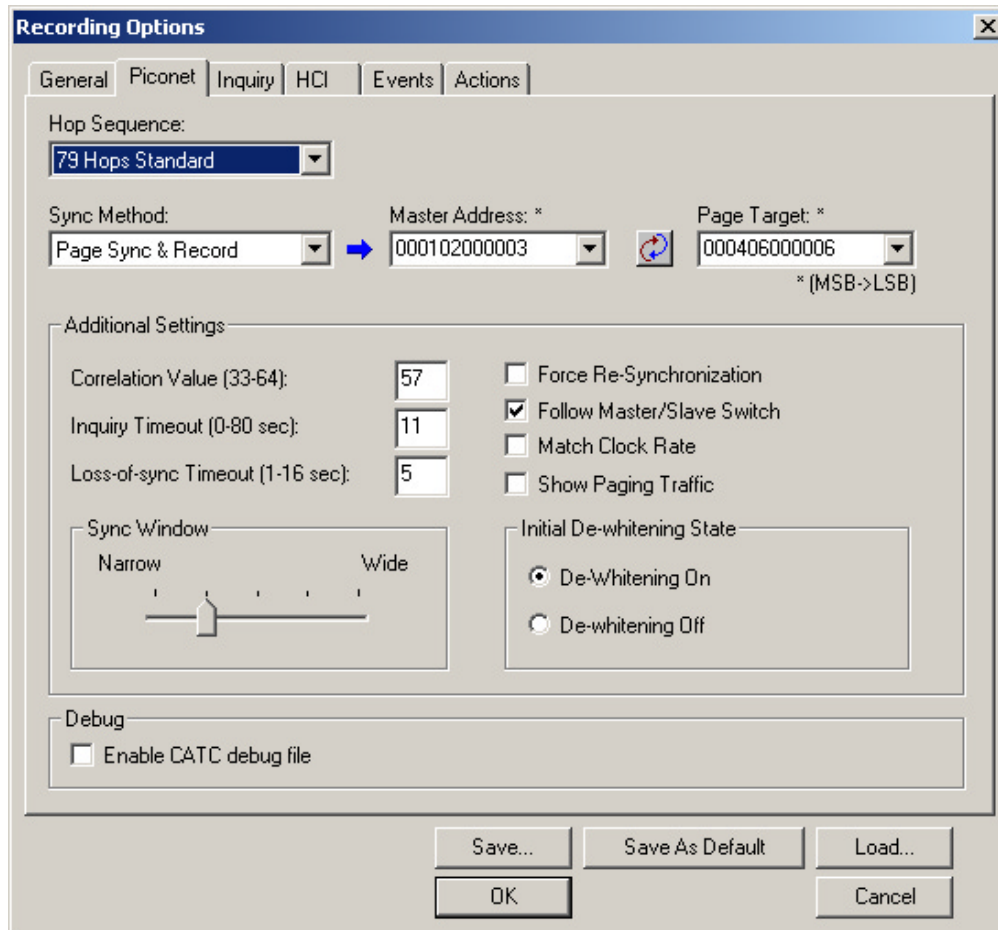
- 95% post-triggering: 0.8MB pre-trigger, 15.2MB post-trigger
- 75% post-triggering: 4MB pre-trigger, 12MB post-trigger
- 50% post-triggering: 8MB pre-trigger, 8MB post-trigger
- 25% post-triggering: 12MB pre-trigger, 4MB post-trigger
- 5% post-triggering: 15.2MB pre-trigger, 0.8MB post-trigger

**Note** When a Trigger occurs, recording continues until the post-Trigger amount of the buffer is filled.

## 6.4 Recording Options - Piconet

The Recording Options dialog box has two pages for configuring how Merlin records Bluetooth traffic: **Piconet**, which configures piconet recording sessions, and **Inquiry** which configures inquiry recording sessions.

For recording in Piconet mode, the **Piconet** page lets you specify the type of piconet you will be recording and how Merlin should synchronize and record the piconet. This window is divided into four boxes marked Hop Sequence, Sync Method, Additional Settings, and Debug.



## Hop Sequence

The **Hop Sequence** menu presents the following three options:

- **79 Hops Standard** - This is the option used for most recordings.
- **Reduced Hop** - Restricts Merlin to five hop frequencies defined in the test mode specification of the Bluetooth Specification. When Reduced Hop or Single Frequency is selected, the Sync method is set to Test Mode and cannot be modified by the user.
- **Fixed Frequency** - Allows the transmit and receive frequency ranges to be specified. Selecting this option highlights the "DUT Xmit" and "DUT Recv" text boxes. When Reduced Hop or Single Frequency is selected, the Sync method is set to Test Mode

and cannot be modified by the user.

Enter values into the two text boxes to set the transmit and receive frequency ranges:

- DUT Xmit Freq, MHz (+2402) – Allows the setting of the transmit signal for the Device Under Test
- DUT Recv Freq, MHz (+2402) – Allows the setting of the receive signal for the Device Under Test

### Sync Method

To record Bluetooth traffic, Merlin needs to synchronize to the piconet under observation. Merlin does not participate in the piconet and behaves as a passive listener. It needs, however, to communicate briefly with the devices in the piconet to learn the Master clock and frequency hopping sequence.

**Sync Method** options let you configure how Merlin synchronizes to the piconet under observation. There are three options:

- Sync and Record
- Passive Sync & Record
- Page Sync & Record

**Note** If the selected Hop Sequence is "Reduced Hop" or "Single Frequency," the Sync Method is set to "Test Mode" and cannot be modified by the user.

To the right of the Sync Method menu are two menus which let you select or enter address for the devices in the piconet:

**Master Address** - Presents a drop-down list of Master devices found previously. You can also enter address values in this box.

**Page Target** -- Presents a drop-down list of Page Target devices found previously. You can also enter address values in this box.

Between the two text boxes is the following button:



- Swaps the Master and Page Target addresses.

### *When to Use the Different Piconet Recording Modes*

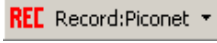
Page Sync & Record is the preferred option and should be used whenever possible. If Page Sync & Record can not be used, then Sync & Record should be used. Passive Sync and Record should be used only if the first two options can not be used.

### *Sync & Record*

Sync and Record works just like "Page Sync and Record" except that Merlin takes its sync data directly from the Master instead of the Slave devices. With Sync and Record, Merlin conducts a General Inquiry to get hop frequency and clock information from the Master. Merlin then waits to detect piconet traffic from the Master device's piconet. When the piconet is established, Merlin is able to synchronize to the Master and begin recording. In contrast to "Page Sync and Record", "Sync and Record" can be run with or without an established piconet.

**Note** This mode can only be used with master devices that support Inquiry Scan.

To perform a "Sync and Record", follow the steps below:

- Step 1** Turn on the Bluetooth devices under observation, and set up the master device so it is ready to respond to Inquiry scan. For a typical recording, ensure that the Master and Slave device(s) are not yet connected.
- Step 2** In the Modes tab under Recording Options, enter the Master Device's address.
- Step 3** Start Merlin recording by pressing the  Record button on the toolbar.
- Step 4** When the analyzer is able to Sync up to the Piconet Master Clock, the Green **Sync** LED in the Merlin front panel will start blinking.
- Step 5** Establish connection between the Bluetooth devices under analysis.
- Step 6** When Merlin senses Piconet traffic, the Green **Sync** light goes ON solid, recording starts and the status bar in the bottom of the analyzer screen shows activity.

Recording may be stopped manually or when the recording buffer is filled.

**Note** After the Sync light starts blinking, a connection between the Bluetooth devices should be established within one (1) minute.

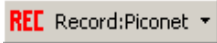
### *Passive Sync & Record*

Passive Sync and Record is used in situations where the Master device and slave devices do not support Inquiry Scan mode. When selected, Merlin enters Inquiry Scan and Page Scan mode and waits for a page from the Master device. When the piconet Master pages Merlin, Merlin obtains the information necessary for synchronization and then attempts to synchronize to the piconet controlled by that Master.

"Passive Sync and Record" is designed to be used with established piconets or *private device networks*.

#### *Running "Passive Sync and Record" with Established Piconets*

For most situations, "Passive Sync and Record" will be run after a piconet has been established. The steps are as follows:

- Step 1** Establish a connection between two or more Bluetooth devices.
- Step 2** Under General Recording Options, select "Passive Sync & Record."
- Step 3** Under the Modes tab in Recording Options, enter the address for the piconet's master device.
- Step 4** Make up an address for Merlin and enter it into the Page Target address in the Modes tab in Recording Options. Make sure you do not select an address for any other local device.
- Step 5** Press the record button on the toolbar in Merlin  to start a recording session.
- Step 6** If necessary, have Master "discover" Merlin through a General Inquiry.
- Step 7** From the Master device, initiate a page to Merlin's address. This action will enable Merlin to synchronize to the piconet. However, the analyzer will not complete the page sequence from the Master. This will cause the Master to time out in this request.
- Step 8** At the end of this sequence, the green **Sync** light will go on solid, recording will begin and activity will be displayed on the status bar in the bottom of the analyzer screen.

#### *Running "Passive Sync and Record" with Private Device Piconets*

Because *private device networks* do not allow other devices to join the network, Merlin needs to temporarily assume the identity of a slave in the network in order to join that network. To do this requires disabling the slave and beginning the operation without an established piconet. The following steps show the process.

- Step 1** Turn the Master device on and the slave device off. You need the slave device turned off so that Merlin can take its place in the piconet.
- Step 2** Enter the slave's address into Merlin's "Page Target" field in the Modes tab in the Recording Options dialog box.
- Step 3** Run "Passive Sync and Record." The Master will then page the slave's address and Merlin will be able to sync.


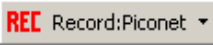
- Step 4** When Merlin synchronizes to the Master, turn the slave back on. When the Master re-pages the address the slave is admitted into the private network. Since Merlin is passive in this mode, the slave and Merlin do not conflict over the shared address. Merlin is then able to record the traffic between the Master and slave.

### *Page Sync & Record*

"Page Sync and Record" is the recommended method of recording. "Page Sync and Record" should be implemented before a piconet is established. This mode causes Merlin to perform a General Inquiry and collect sync information from the specified slave device when it responds. Merlin then waits for the Master to begin paging the Slave devices. When paging begins, Merlin synchronizes to the Master and begins recording.

**Note** In order for this mode to work, the intended Slave must support "inquiry scan".

The following steps describe the simplest way to use this mode:

- Step 1** Place both the "intended master" as well as its first "intended slave" into inquiry scan mode.
- Step 2** Have Merlin perform a General Inquiry. You do this by pressing the BT Neighborhood button 
- Step 3** After the General Inquiry completes, the addresses will populate the menus marked **Master Device** and **Page Target**. Select or enter the addresses for both your Master Device and Page Target.
- Step 4** Click **OK** at the bottom of the window to close the Recording Options dialog box.
- Step 5** Press the  button found on Merlin's toolbar. After approximately 20 seconds, the "SYNC" light on the front of Merlin will begin to flash, meaning that Merlin has acquired all the information it needs to fully synchronize with the piconet about to be established. At this point, you should establish the piconet using the devices previously defined as master and slave.

**Note** Inquiry Timeout is configurable (0 to 80 seconds) in the Recording Options General page.

- Step 6** When the piconet is established, the "Sync" light on the front of Merlin will change from flashing to solid, indicating that Merlin is fully synchronized to the piconet and is currently recording all traffic within that piconet.

**Note** If the "sync" light on the front of Merlin does not change from flashing to solid it means that Merlin did not synchronize with the piconet when it was established.

## **Additional Settings**

### *Force Re-synchronization*

"Force Re-Synchronization" forces Merlin to re-synchronize at the beginning of each "Sync & Record," "Passive Sync & Record," or "Sync & Record" operation. By default, "Force Re-Synchronization" is disabled (i.e., unchecked).

Unchecking the "Force Re-Synchronization" checkbox tells Merlin to use its existing data on Bluetooth devices, thereby bypassing the synchronization process and saving a few seconds from the beginning of the trace. If you know that Merlin's data is correct, you can uncheck this checkbox and cause Merlin to use the existing data. If the data is incomplete or incorrect, however, Merlin will automatically perform a refresh.

To examine Merlin's Bluetooth data, open Device List: **View >Device List**.

### *Follow Master/Slave Switch*

If enabled, this option allows Merlin to follow a role switch between a Master and Slave. This capability allows Merlin to keep track of changes in a device's role when it changes from one role to another.

### *Match Clock Rate*

Match Clock Rate is a useful option if the Master device's clock is inaccurate. Match Clock Rate causes Merlin to do a General Inquiry to determine the Page Target's clock rate prior to synchronizing to the piconet. If unchecked, Merlin will begin piconet synchronization without first doing a General Inquiry.

This option only works with Page Sync and Record mode.

### *Show Paging Traffic*

Show Paging Traffic causes Merlin to capture paging traffic between the Master and Page Target devices. This option is used only with Page Sync and Record Mode.

### *Correlation Value (33-64)*

This value tells Merlin how many bits in the sync word of each received packet must be matched in order for Merlin to consider the packet valid and start recording.

Recommended value: 57.

*Inquiry Timeout (0-80 secs)*

Default value is 20 seconds.

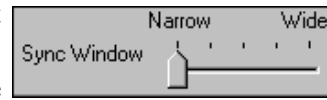
This value specifies how long Merlin should perform the Inquiry process for the General (unlimited) and Dedicated (limited) recording modes. After the specified time has elapsed, Merlin will illuminate the trigger light on the front of the analyzer.

*Loss of Sync Timeout (1-30 secs)*

This value specifies the amount of time that Merlin will wait for piconet traffic before determining that synchronization has been lost.

*Sync Window*

The Sync Window slide bar controls the amount of time that Merlin should wait between receiving an Inquiry Response (which will cause the Sync LED to blink) and detecting Master-Slave piconet traffic (which will cause the Sync LED to turn solid.)



A "Narrow" setting means that the wait time will be minimal, a "Wide" setting means it will be "maximal." The default is "Narrow" and this is suitable for most recordings. However, if significant drift occurs between Merlin's clock and that of the Master, Merlin may not be able to sync properly to the piconet. Under these conditions, you should move the slide bar towards the "Wide" Setting. The slide bar has five discrete settings.

After sync is established, Merlin will remain in sync as long as there is piconet traffic.

**Debug***Enable CATC debug file*

Checking this box enables the creation of a file that can be used by CATC Support to aid in debugging. This option should always be disabled unless you are requested to enable it by CATC personnel.

## 6.5 Recording Options - Inquiry

The **Inquiry** page configures how Merlin should perform an inquiry. Two main options are presented in the radio buttons: General (Unlimited) Inquiry and Dedicated (Limited) Inquiry. These options tell Merlin what kind of Inquiry it should do. This mode records the inquiry responses from devices.

This page includes settings only for Inquiry recording and BT Neighborhood.



*General (Unlimited)*

"General" means "General Inquiry" and is used to search for ALL Bluetooth devices that are within range, for the amount of time specified in the Inquiry Timeout field. Completion of the inquiry process is indicated by illumination of the "trigger" light on the front of the analyzer. All responding packets will be displayed when data upload from the analyzer completes.

*Dedicated (Limited)*

"Dedicated" means a specific class or group of Bluetooth devices (designated by the DIAC field of the Recording Options dialog). Selecting "Dedicated" causes Merlin to search for all devices from a specific class or group that are within range, for the amount of time specified in the Inquiry Timeout field. Completion of the inquiry process is indicated by illumination of the "trigger" light on the front of the analyzer. All responding packets will be displayed when stop is selected.

*BT Neighborhood*

These options configure how the BT Neighborhood command behaves. BT Neighborhood is a utility that performs an Inquiry and then lists the local devices that it discovered.

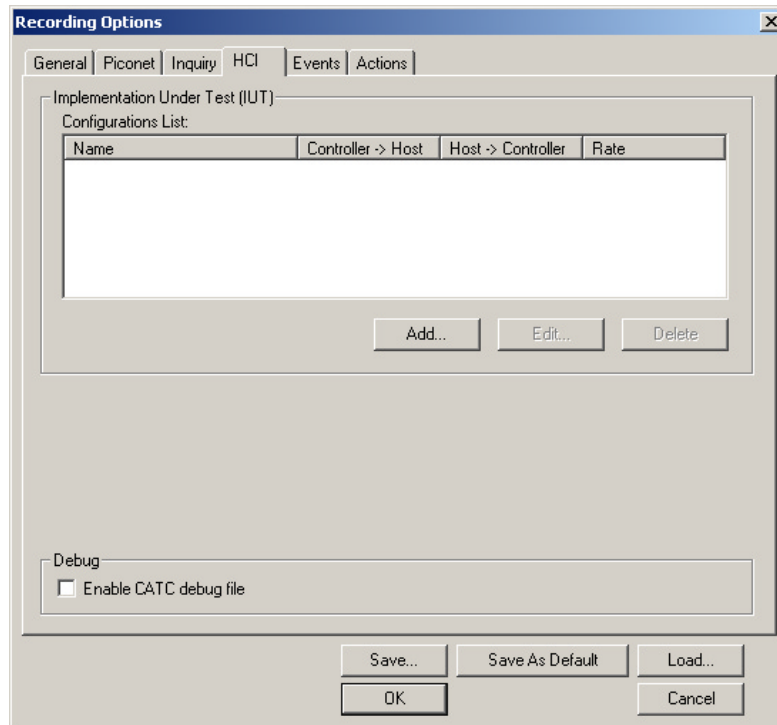
- **Use Default settings** -- Sets the analyzer to record a General Inquiry with an Inquiry Timeout of 11 seconds.
- **Match 'Inquiry' Recording Settings** -- Sets the analyzer to use the settings you chose above under Hop Sequence, Inquiry Type, and Additional Settings.

*Debug*

Enables the creation of a file that can be used by CATC Support to aid in debugging.

## 6.6 Recording Options - HCI

The HCI property page lets you include HCI traffic from IUTs into the trace. HCI traffic consists of commands and other traffic that are sent by the IUT to generate Bluetooth traffic. By default, this option is disabled - meaning that HCI traffic is not shown in the trace.



HCI Traffic from the IUTs is captured by the analyzer application using an HCI probe (provided by CATC) that is connected directly to the IUT hardware. In a typical setup, the HCI commands and data to transmit are passed from the Bluetooth application to the Bluetooth baseband (Host to Controller), while events and data that was received are passed from the Bluetooth baseband to the Bluetooth application (Controller to Host).

To capture the data, the HCI Probe should be connected to the respective 'Host to Controller' and 'Controller to Host' lines. When the recording of the IUT's HCI is enabled and the application starts a recording, the serial data is captured as incoming serial data. For this, up to two COM ports should be configured for each IUT.

### HCI Window Layout

The HCI page displays a Debug checkbox, a Configurations List that is made up of IUTs that were added via the **Add** button, and buttons labeled **Add**, **Edit**, and **Delete**.

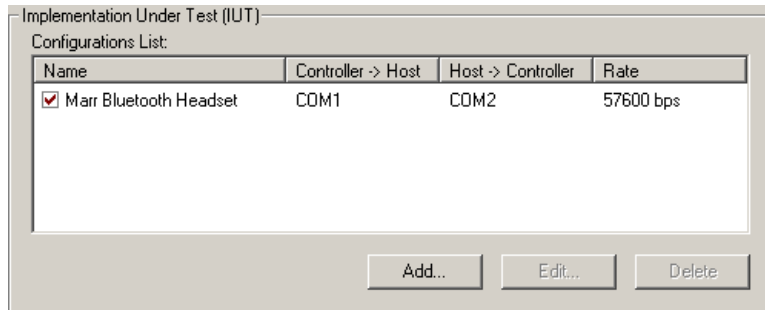
### Debug

Enables the creation of a file that can be used by CATC Support to aid in debugging.

### Configurations List

The Configurations List displays the COM settings for the ports used to connect the IUT to the host PC.

The Configurations List allows you to manage as list of up to three IUTs to be recorded and set the parameters for each one. It also allows you to enable or disable a specific IUT from being recorded. The settings are stored in the recording options file, like the rest of the recording options.



The Configurations List is made up of the following fields:

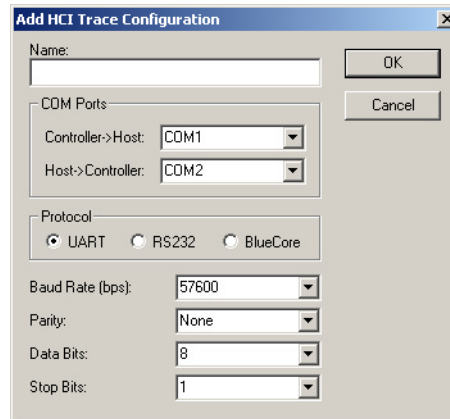
- **Name** - Symbolic name of the IUT given by the user, for easy identification.
- **Controller => Host** COM port - The port that is used for the capturing of the up-link traffic.
- **Host => Controller** COM port - The port that is used for the capturing of the down-link traffic.
- **Rate** - the bits per second rate the COM ports are configured for.

The list displays three possible states for each one of the entries:

- **Enabled** - The HCI traffic from the IUT is going to be recorded.
- **Disabled** - The HCI traffic from the IUT is not going to be recorded.
- **Invalid** - The analyzer failed in opening the COM port for accessing the IUT, with the listed parameters. In this case, you should refer to Windows configuration of the COM ports or check whether the same COM port(s) is (are) used by other applications in the host machine or that the parameters are set correctly.

*Add ...*

The **Add** button lets you add devices to the Configurations List. Clicking **Add** causes the following dialog box to open:



**Name** - Symbolic name for easy identification of the device and connector.

**Controller -> Host** - COM port used for monitoring the HCI traffic from the application to the bluetooth baseband.

**Host -> Controller** - COM port used for monitoring the HCI traffic from the Bluetooth baseband (Controller) to the application (Host).

**Rate** - Sets the maximum rate in bits per second (bps) that you want data to be transmitted through this port.

**Data Bits** - Changes the number of data bits you want to use for each character that is transmitted and received. The computer or device you are communicating with must have the same setting that you choose here. Most characters are transmitted in seven or eight data bits.

**Parity** - Changes the type of error checking you want to use for the selected port. The computer or device you are communicating with must have the same setting that you choose here. You must choose one of the following:

- **None** - No parity bit will be added to the data bits sent from this port. This will disable error checking.
- **Even** - Parity bit is set to 1 if it is needed to make the number of ones in the data bits even. This will enable error checking.
- **Odd** - Parity bit is added if it is needed to make the number of ones in the data bits odd. This will enable error checking.
- **Mark** - Parity bit is added but is always set to 1.

**Stop Bits** - Changes the time between each character being transmitted (where time is measured in bits).

**Protocol** - Sets the protocol for the ports used to connect the IUT to the host PC. There are three choices:

UART

RS232

Bluecore - a special HCI transport

### *Edit*

The Edit button reopens the **Add HCI Configurations** dialog box so you can edit your settings. Be sure to select an entry in the HCI Configurations list before clicking **Edit**.

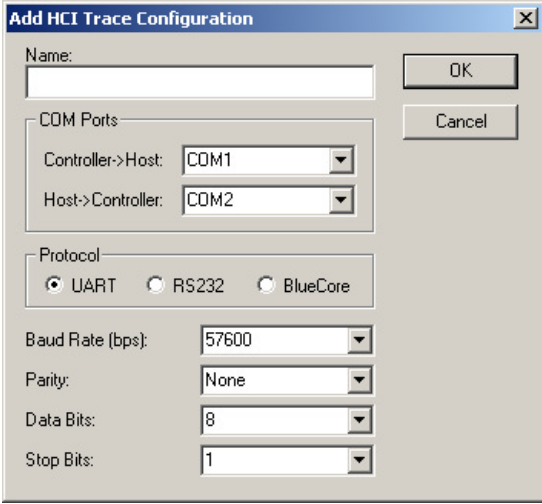
### *Delete*

The Delete button allows entries to be deleted from the Configurations List.

## 6.7 Recording HCI Traffic

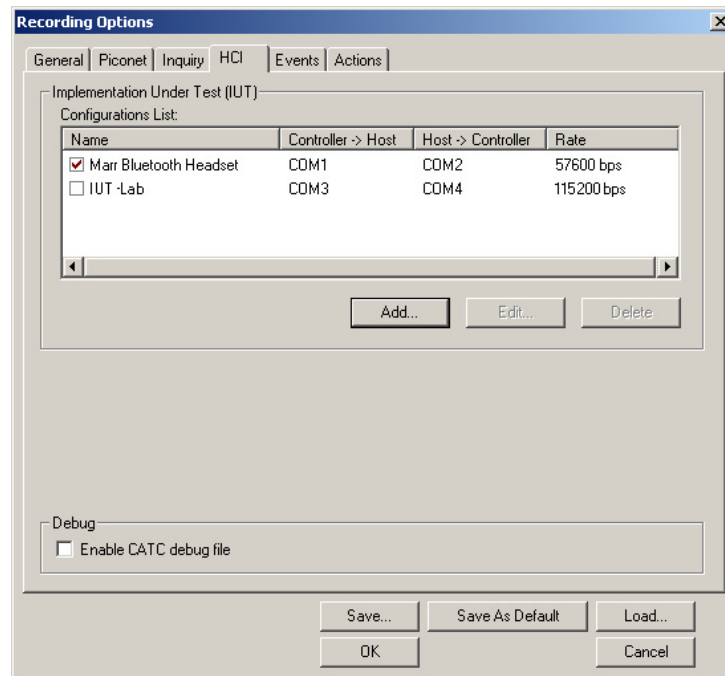
To record HCI traffic from an IUT, enter data in the HCI window.

**Step 1** In Recording Options, go to the HCI page, and click **Add**. The Add HCI Trace Configuration dialog appears.



**Step 2** Enter the pertinent data in the data fields, and click OK. The HCI configuration is shown in the HCI page of Recording

options.



To edit an entry in the Configurations List,

- Step 1** In the HCI page of Recording Options, click **Edit**. The Edit HCI Trace Configuration dialog appears.
- Step 2** Change the data in the data fields according to your desired changes, and click **OK**. The changes are reflected in the Extern page of Recording Options.

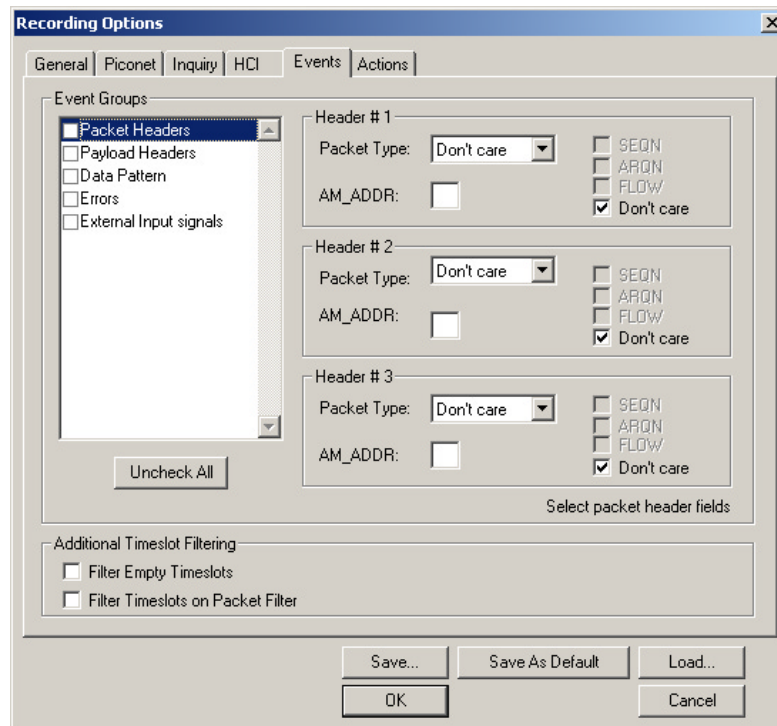
## 6.8 Recording Options - Events

If you have selected **Event Trigger** mode under the **General** tab in the Recording Options screen, you may now select specific Bluetooth events using the **Events** tab on the **Recording Option** Screen. You can also use the **Actions** tab to define specific event sequences that will trigger Merlin to record a Bluetooth session.

In addition, the **Events** and **Actions** screens allow you to specify which packets you want to include or exclude from the recording.

- Click the **Events** tab on the **Recording Options** screen.

You see the **Event Groups** window:



The Event triggering and filtering options allow you to set event conditions for errors and/or a variety of packet characteristics.

Clicking a check box causes further options to display in the right side of the window.

#### *Additional Timeslot Filtering*

By default, Merlin records frequency hop and timestamp information for all time slots in the Piconet under analysis, regardless of whether the time slot contained a Bluetooth packet. This means that in instances where there is little piconet traffic, Merlin will display row after row of empty packets -- each representing an empty time slot. Through the use of timeslot filtering, these empty packets can be filtered out. Filtering out this information has the benefit of freeing memory so that more traffic can be recorded.

#### **Filter Empty Slots**

If "Filter Empty Slots" is checked, Merlin will exclude all empty time slots from a recording except for those that lie immediately in front of Bluetooth communications packets. These remaining empty packets are preserved to give timestamp and frequency hop reference data to the packets that follow.

### Filter Slots on Packet Filter

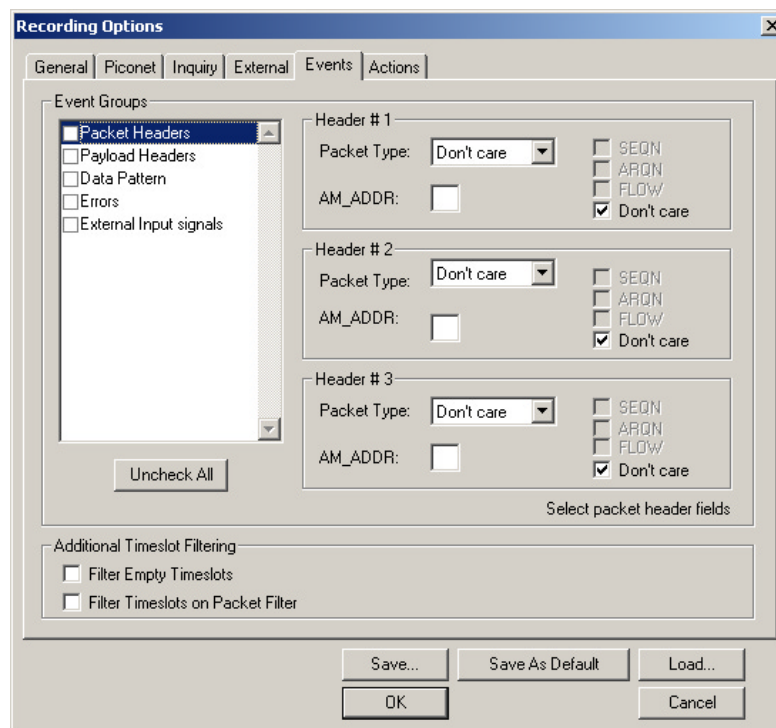
If filters are used to exclude FHS, DM1 or other packets, Merlin will exclude these packets from a trace and mark their locations with empty packets. The result can be rows and rows of empty packets. The option "Filter Empty Slots" will not exclude these empty slots because they lie immediately in front of Bluetooth communications packets - even though those packets were not recorded. To eliminate these empty packets, select "Filter Slots on Packet Filter."

### Packet Headers

Clicking "Packet Headers" opens three sets of check boxes and menus on the right that represent fields within packet headers: Packet Type, Active Member Address, Flow Control, Acknowledgment, and Sequence Number.

- Select **Packet Headers** under **Event Groups**.

You see the **Packet Headers** window:



### Packet Type

The Packet Type drop down menu lets you select the following packet types for filtering or triggering: NULL, POLL, FHS, DM1, DH1, HV1, HV2, HV3, DV, AUX1, DM3, DH3, 1100, 1101, DM5, or DH5.

Select "Don't Care" if you want Merlin to ignore this field.



**AM\_ADDR**

(Active Member Address) The AM\_ADDR is a three bit slave address. To select packets from a particular slave device for filtering or triggering, enter an address into the AM\_ADDR text box. You can target up to three devices using the three text boxes.

**SEQN, ARQN, and Flow Control Bits**

To set event conditions on SEQN, ARQN, and Flow control, uncheck "Don't Care." Unchecking "Don't Care" sets the event condition to SEQN=0 AND ARQN=0 AND Flow=0. This action also puts a checkmark in the box marked "Packet Headers." A checkmark next to SEQN, ARQN, or Flow changes the value of this field from zero to one. For example, if SEQN is checked, the event condition becomes "SEQN=1 AND ARQN=0 AND Flow=0."

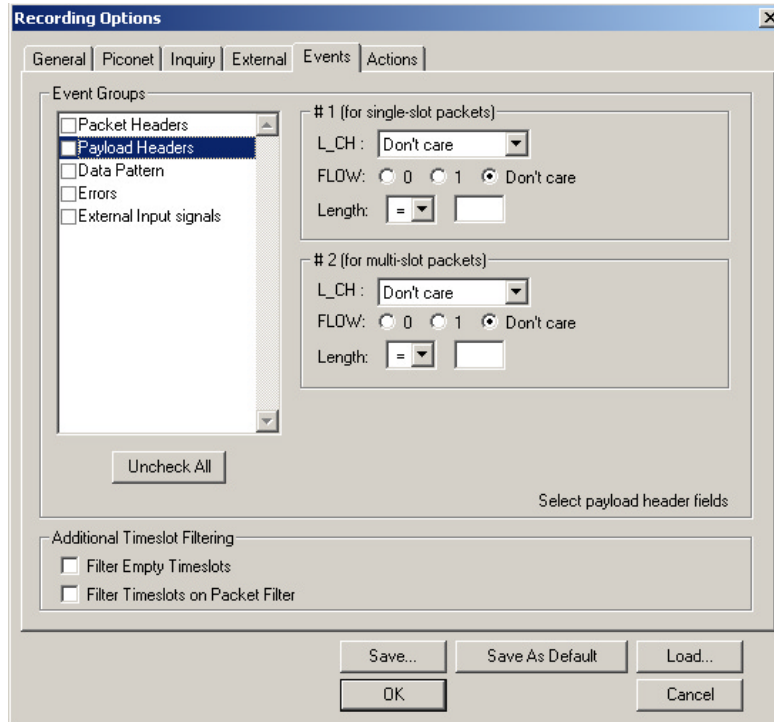
To cause Merlin to ignore this set of check boxes, choose "don't care."

*Payload Headers*

Clicking "Payload Headers" causes a series of options to display on the right for setting conditions on payload headers. You will see two sets of options - one for single slot packets such as DM1 packets and a second for multi-slot packets such as DM3 packets. Within each set is a menu for the Logical Channel and sub-options for Flow Control, and Payload length. These latter two options allow you to modify searches based on the Logical Channel. An example would be "Trigger on a start L2CAP message whose flow control bit is 1 and whose data field length is less than 20."

- Select **Payload Headers** under **Event Groups**.

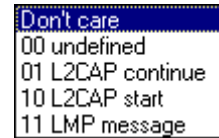
You see the **Payload Headers** window



### L\_CH (Logical Channel)

The "L\_CH" drop down menu presents five options for setting conditions on the Logical Channel:

- Don't care
- 00 Undefined
- 01 L2CAP continue
- 10 L2CAP start
- 11 LMP message



Select "Don't care" if you do not want to set conditions on Logical Channel.

### Flow

Three "radio buttons" are presented for setting conditions based on L2CAP Flow control:



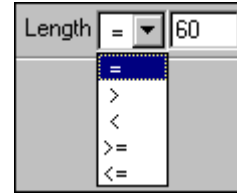
- 0
- 1
- Don't care

Flow works in conjunction with the Logical Channel (L\_CH) menu - you select an option from the L\_CH menu and then select an option under Flow.

Select "Don't care" if you do not want to set conditions on Flow control.

### Length (in bytes)

Using both the drop down menu and the text box, you can set conditions based on data field length. The maximum length for a single slot packet is 29 bytes. The maximum length for multi-slot packets is 339 bytes.

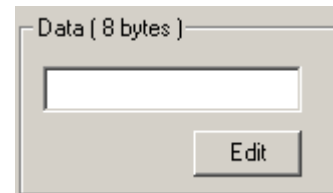


The drop-down menu gives you options for selecting operators such as "greater than" and "equal to." The text box to the right of the drop-down menu lets you enter values.

The Length option works in conjunction with the Logical Channel (L\_CH) menu - you first select an option from the L\_CH menu and then select an option under Length.

### Data Patterns

Clicking "Data Patterns" causes a text box to appear for entering patterns to be matched in the raw payload data. Patterns of up to eight hexadecimal bytes can be entered.

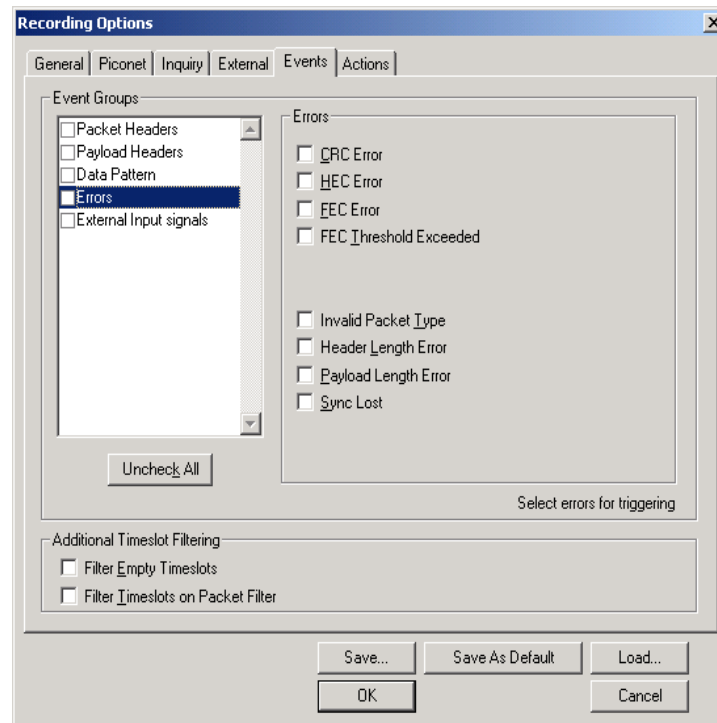


### Errors

Clicking "Errors" causes check boxes to appear for setting conditions for triggering or filtering based on packet/signaling/protocol errors. You can select one or a combination of errors.

- Select **Errors** under **Event Groups**.

You see the **Errors** window:



Use any combination of the listed packet/signaling/protocol errors as a Trigger.

### **CRC Error**

A CRC error in the packet data payload of the previous Bluetooth data packet.

### **HEC Error**

An HEC (header error check) error in the packet header for the previous Bluetooth data packet.

### **FEC Error**

An uncorrectable FEC (Forward Error Correction) error in the packet header for the previous Bluetooth data packet.

### **Threshold Exceeded**

Indicates that the number of single-bit FEC errors detected since the current recording started has exceeded the specified value.

### **Invalid Packet Type**

An invalid value was detected in the 'packet type' field of the packet header for the previous Bluetooth data packet.

**Header Length Error**

Indicates that a received Bluetooth data packet was terminated before all bits of the packet header were received.

**Payload Length Error**

Indicates that the payload of a received Bluetooth data packet was either longer than expected, or that a Bluetooth data packet terminated before the expected end of the payload data.

**Sync Loss**

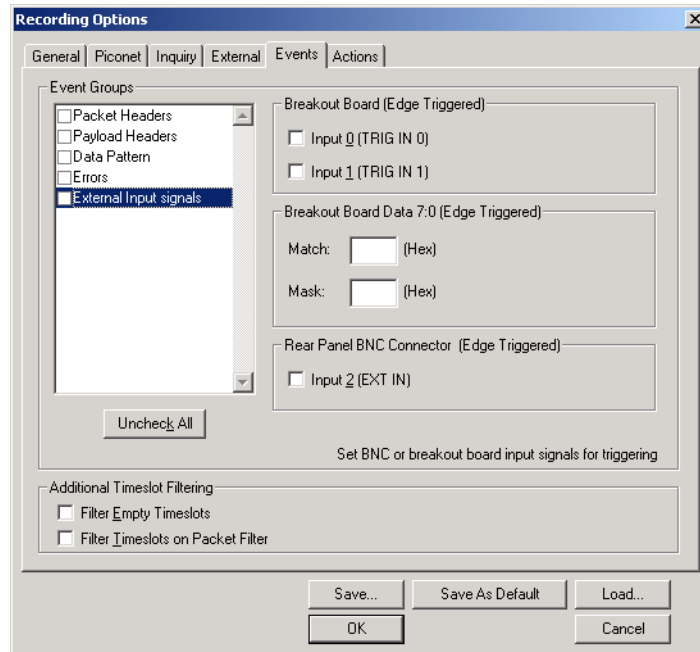
When set, indicates that a loss of piconet synchronization occurred during the frequency slot prior to this slot.

*External Input Signals*

Clicking "External Input Signals" causes two check boxes to appear for setting conditions based on breakout board input signals. The names of the two check boxes are the same ones you will find on the break out board:

- Input 0 [TRIG IN 0]
- Input 1 [TRIG IN 1]

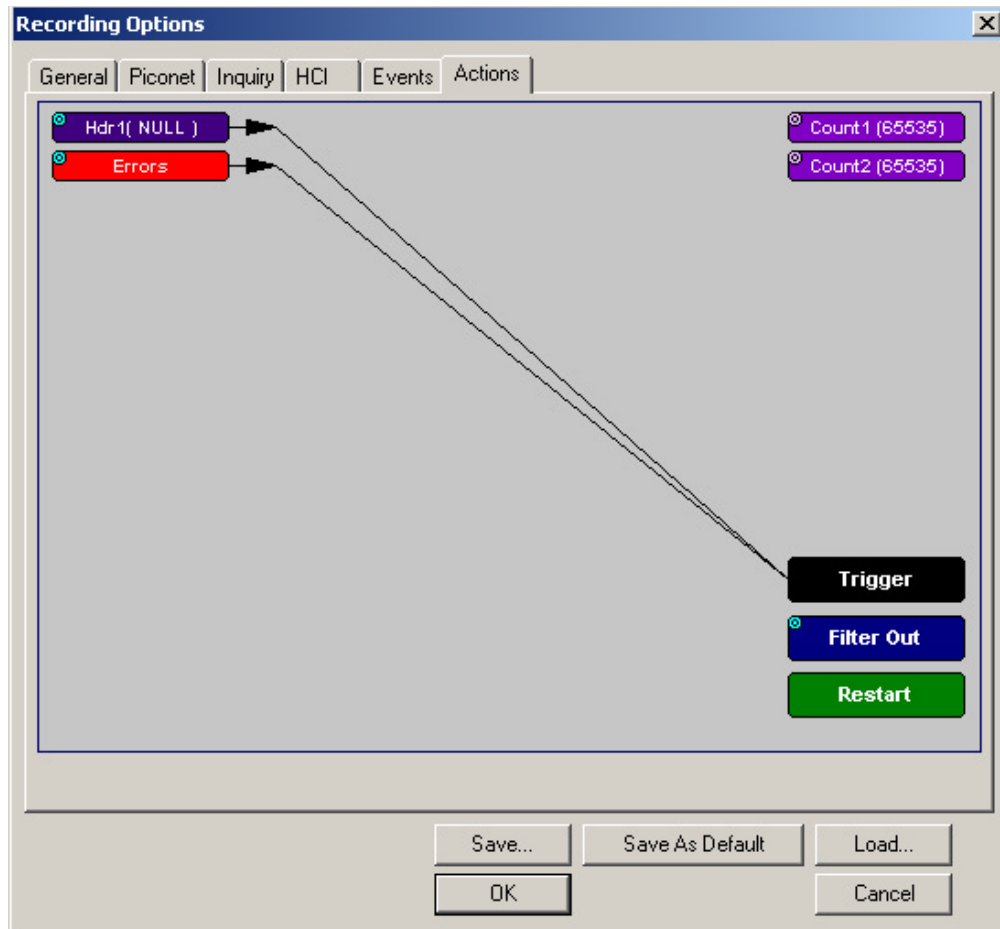
- Data 7:0
- BNC Input



## 6.9 Recording Options - Actions

The **Actions** screen allows you to specify the type of action that Merlin should perform when it encounters the events specified in the **Events**

window.



### Action Buttons - Their Functions

The **Action** buttons in the right side of the window provide the means of setting triggers, filters, and restarts. To set an action, you simply drag your mouse from an Event to an Action. As described further on, this movement will link the two via an arrow.

#### *Trigger*

The **Trigger** button enables event triggering.

#### *Filter In/Out*

The **Filter In/Out** button allows events to be filtered in or out of the recording. Filtering provides a useful method of excluding data from the trace so you can conserve recording memory.

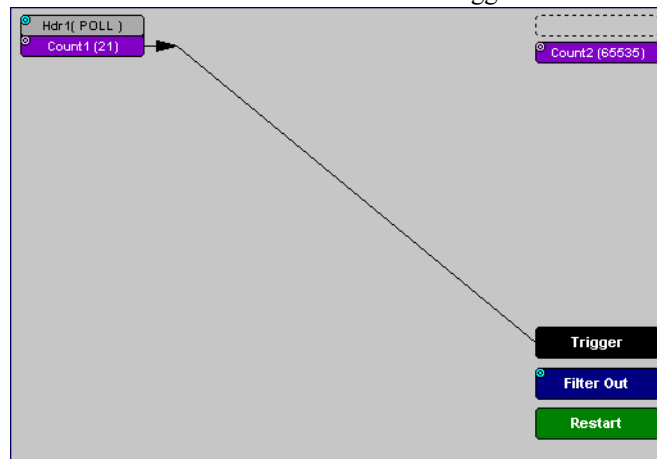
*Restart*

The **Restart** button causes the two counters Count1 and Count2 to be reset to zero. It also causes the search for *event sequences* to restart. Event sequences are sequences of events that trigger the end of the recording. Restart buttons provide you with a way of saying "If you see a sequence of A, B, C, and D, then trigger. However, if you see *X* anywhere during the sequence, restart your search."

*Count1, Count2*

Count1 and Count2 are counters for specifying how many events must occur before an event can cause a trigger. Counters allow conditions to be made such as "Trigger after the 21st Poll packet" (see screenshot below).

The Actions window showing a condition based on a Poll packet and a counter. This condition reads "Trigger after the 21st Poll packet."

*Connecting Events to Counters*

To connect an event to a counter, click an Event button, then click one of the two counter buttons. The Counter will reposition itself immediately below the event. A line will connect the counter to the Trigger button.

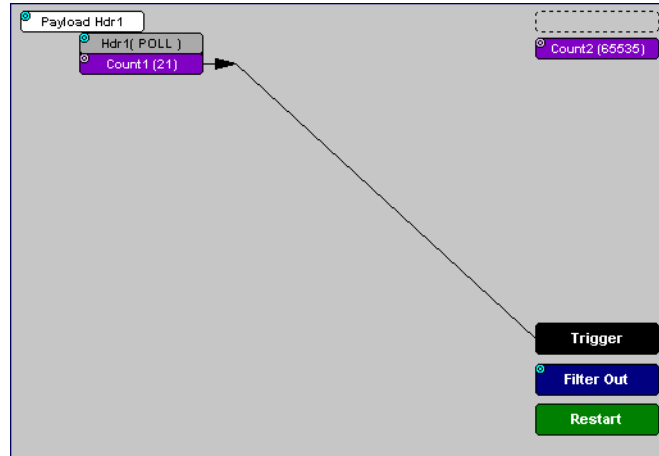
This latter connection between the Counter button and the Trigger button occurs because counters always work in association with triggers. Counters act as assistants to triggers.

*Setting Multiple Conditions with Counters*

You can create multiple event conditions by linking a counter to multiple events or by linking two counters to two or more events.

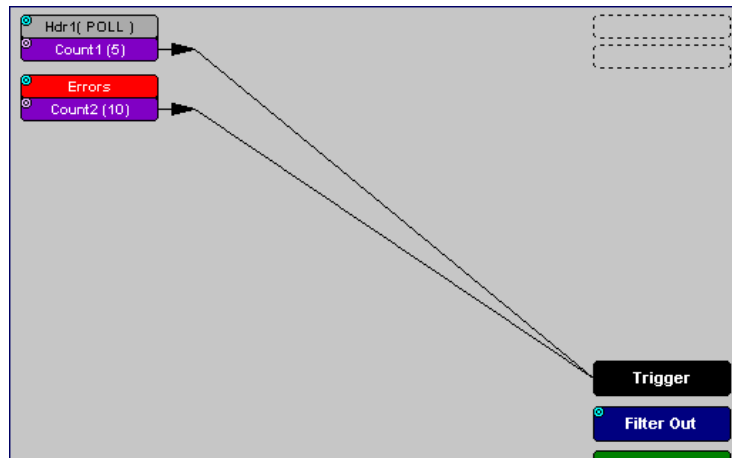


**Linking Multiple Events to One Counter** - When two or more Events are strung together and then connected to a counter, the event button that is touching the counter gets counted. The example below reads "Trigger after you see a sequence of a packet with the specified payload followed by a 21 null packets."



**Linking Two Events to Two or More Counters** - If an Event is linked to **Count1** and a second event is linked to **Count2**, it creates an "or" statement. This statement reads "Trigger when Count1 OR Count2 has reached their specified values."

This example reads "Trigger when Count1 has counted 5 Poll packets or Count2 has counted 10 errors."



## Blue Dot Menus

**Count1**, **Count2** and a few other buttons in the **Actions** window have blue dots in their top left-hand corners that indicate the presence of context-sensitive menus. These menus let you set the button's values and/or operations. Click the left mouse button on a dot to open the menu.



### Counters Blue Dot Menu

The **Count1** and **Count2** blue dot menus allow the value of their counters to be changed. The value you specify here tells Merlin how many instances of an event must take place before a trigger occurs. The counter can be set between 1 and 65,535.

To set a Counter,

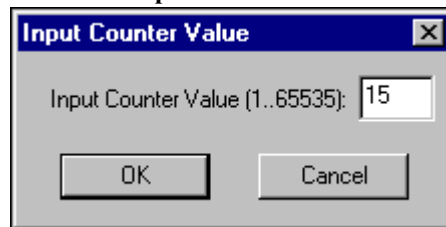
- Step 1** Click on the blue dot in the upper left corner of the **Count** button.

You see the **Change Counter Value** menu:



- Step 2** Click **Change Counter Value**

You see the **Input Counter Value** menu



- Step 3** Enter an input value to tell the Analyzer how many times this event must occur before triggering the end of a recording
- Step 4** Click **OK**.

### Filter Out/In Blue Dot Menu

The **Filter Out/In** button toggles between "**Filter Out**" and "**Filter In**".

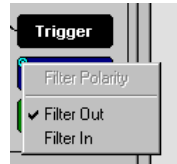
- **Filter In** records ONLY those packets related to the specified event.
- **Filter Out** records all packets EXCEPT those related to the

specified event.

To filter an event in or out of a recording,

- Step 1** Click the blue dot on **Filter Out**. (Note: the button may say **Filter In** depending on the last action specified.)

You see the **Filter Out/In** menu:



Use this menu to toggle the selection between **Filter Out** and **Filter In**.

- Step 2** Select "**Filter In**".

The button changes to read "Filter In".

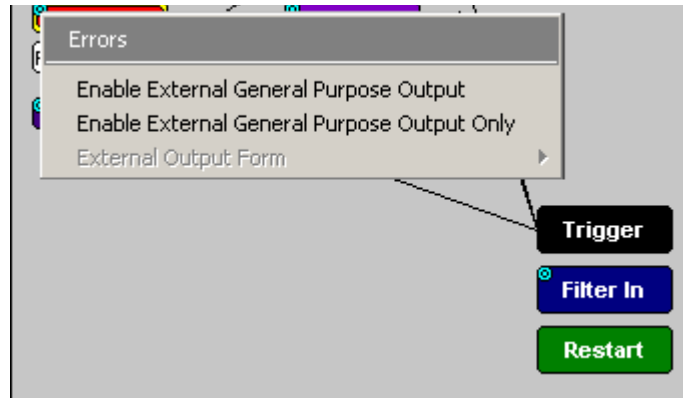
### *Blue Dot Menus for the Event Buttons*

The **Errors** button and the first Headers button (marked "**Hdr1**") have the same Blue Dot menus. These menus allow Merlin to trigger external output.

To enable or disable external trigger output,

- Step 1** Click the Blue Dot on an Event button such as **Hdr1** or **Errors**.

A menu similar to the one below will open. Your menu may say "Disable" instead of "Enable."



- Step 2** Select "**Enable External Trigger Output**" (or "**Disable External Trigger Output**" if that is the choice presented.)

If you have chosen "**Enable External Trigger Output**", a small arrow will appear on the right side of the button. This arrow indicates that a condition has been set for creating an external output signal.

Choosing "**Disable External Trigger**" will cause the arrow to disappear.



### *Enabling High Pulse, Low Pulse or Pulse Toggle Signal Outputs*

Once External Trigger Output has been enabled, you can configure the output signal to one of three formats:

**Pulse High** - This is the default format. The Pulse High setting causes the Analyzer to transmit a 5 volt, 16.66 nanosecond signal.

**Pulse Low** - This format causes the Analyzer to transmit a -5 volt, 16.66 nanosecond signal.

**Toggle** - This format causes the Analyzer to transmit a signal that will toggle with each trigger event between a continuous 5 volt signal and a continuous -5 volt signal.

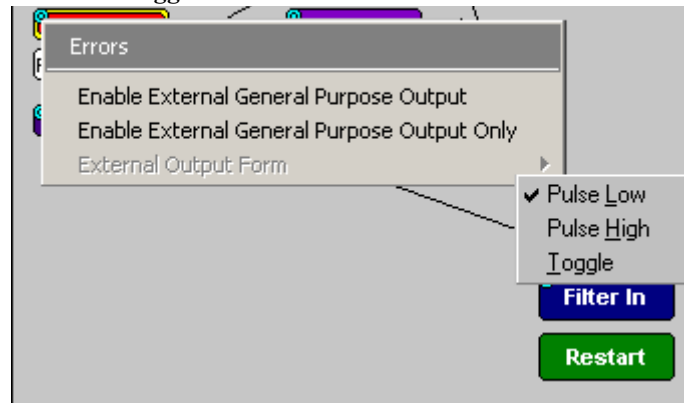
To configure the output signal,

**Step 1** Click the blue dot on an Event button that has a small arrow attached to it like the one shown above.

A Blue Dot Menu will open. "**External Trigger Form**" should be a choice available. If it is not, you will need to choose "**Enable External Trigger**" and then reopen the menu.

**Step 2** Choose "**External Trigger Form**"

A menu will appear with choices for "**Pulse Low**", "**Pulse High**", and "**Toggle**".



**Step 3** Choose an option not currently selected.

The menu closes.

**Step 4** Reopen the menu.

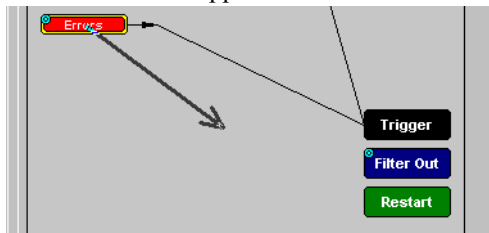
Note that your new selection is now checked.

### Elastic Arrow

Elastic arrows allow you to associate Events, Counters, and Actions. To make an association,

- Step 1** Click the left mouse button on an Event button such as **Hdr1** or **Errors**.

The elastic arrow appears.

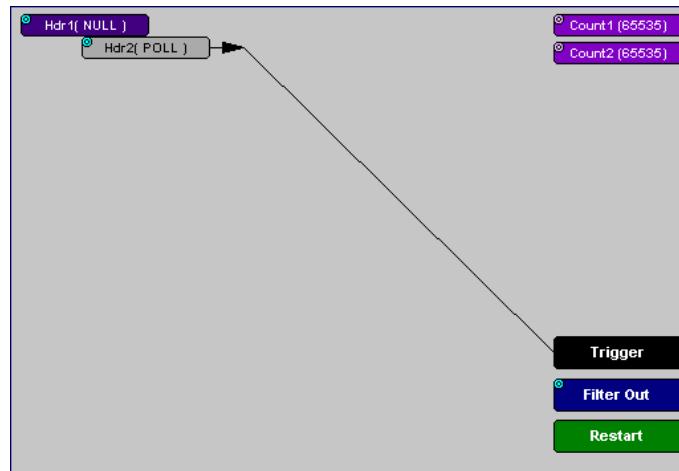


- Step 2** Drag the arrow to the desired Action button.
- Step 3** With the pointer over an Actions button, click again the left mouse button again.

The arrow is replaced with a black line connecting the Event button to the Action button.

### Event Sequencing

If you drag your mouse from one event button to another, you will create a compound condition known as an *Event Sequence*. An event sequence is a condition that says "Trigger when you see the following sequence of packets." The example below may help to clarify.



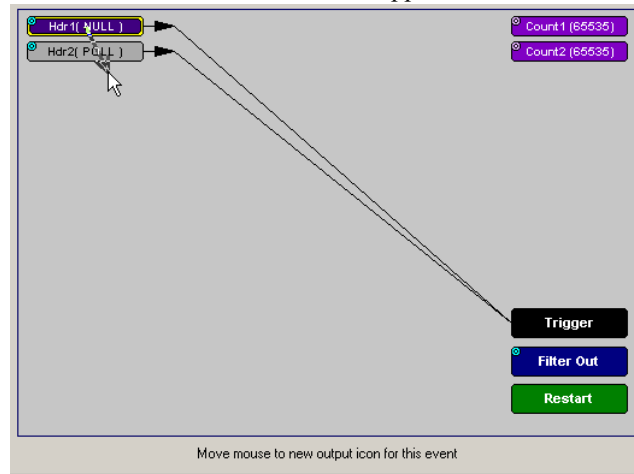
This example means "Trigger when you see a packet with a Null Header followed by a packet with a Poll Header."

To create an event sequence, perform the following steps:

- Step 1** Select two events from the Events window

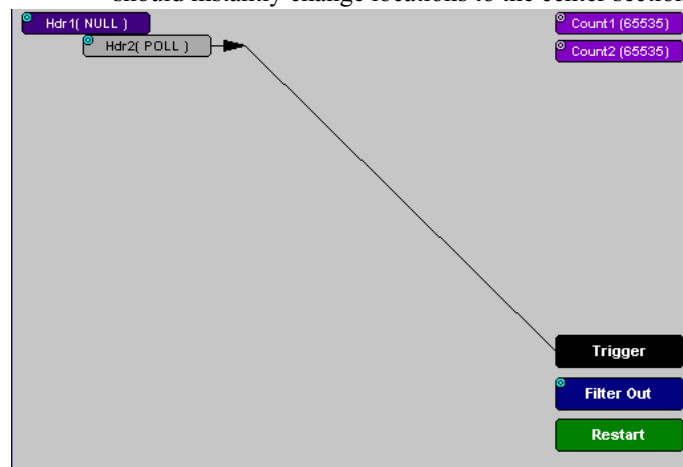
- Step 2** Open the Actions window and click on one of the two Event buttons.

An elastic arrow should appear.



- Step 3** Click on the other event.

The arrow should connect to the second button and the second button should instantly change locations to the center section of the window.



## 6.10 Saving Recording Options

To complete your Recording Options settings, use the features at the bottom of the **Recording Options** screen. These features remain the same no matter which of the three Recording Options screens you are working in.

- Click **Save** to save the currently specified Recording Options for use in future recording sessions. Any file name can be specified, though use of the **.rec** is recommended; if no extension is

specified, **.rec** is added by default.

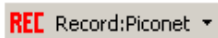
- Click **Load** to load a previously saved **\*.rec** file, thus restoring a previous set of Recording Options.
- The **Save as Default** function is equivalent to the **Save** function, specifying the file name **default.rec**. Whenever you start up the Analyzer, it automatically loads the **default.rec** file if one exists.
- Click **OK** to apply any changes and close this dialog box.
- Click **Cancel** to cancel any immediate changes you have made and exit the Recording Options menu.


## 6.11 Recording Bluetooth Traffic

To start recording Bluetooth traffic once the appropriate Recording Options have been set,

**Step 1** Select **Start** under **Record** on the Menu Bar

OR


Click  on the Tool Bar.

Your recording session can continue until it has finished naturally or you may need to stop manually by clicking  on the Tool Bar, depending on how you set the Recording Options.

To manually stop recording,

**Step 2** Select **Stop** under **Record** on the Menu Bar

OR

Click  on the Tool Bar.

**Note** The manual Stop Recording feature is primarily of use when recording low-volume traffic, which can take a long time to fill the recording buffer.


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

If you have enabled the recording of serial HCI traffic from IUT, then a second trace file is created called **data\_hci.tfb**.

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.

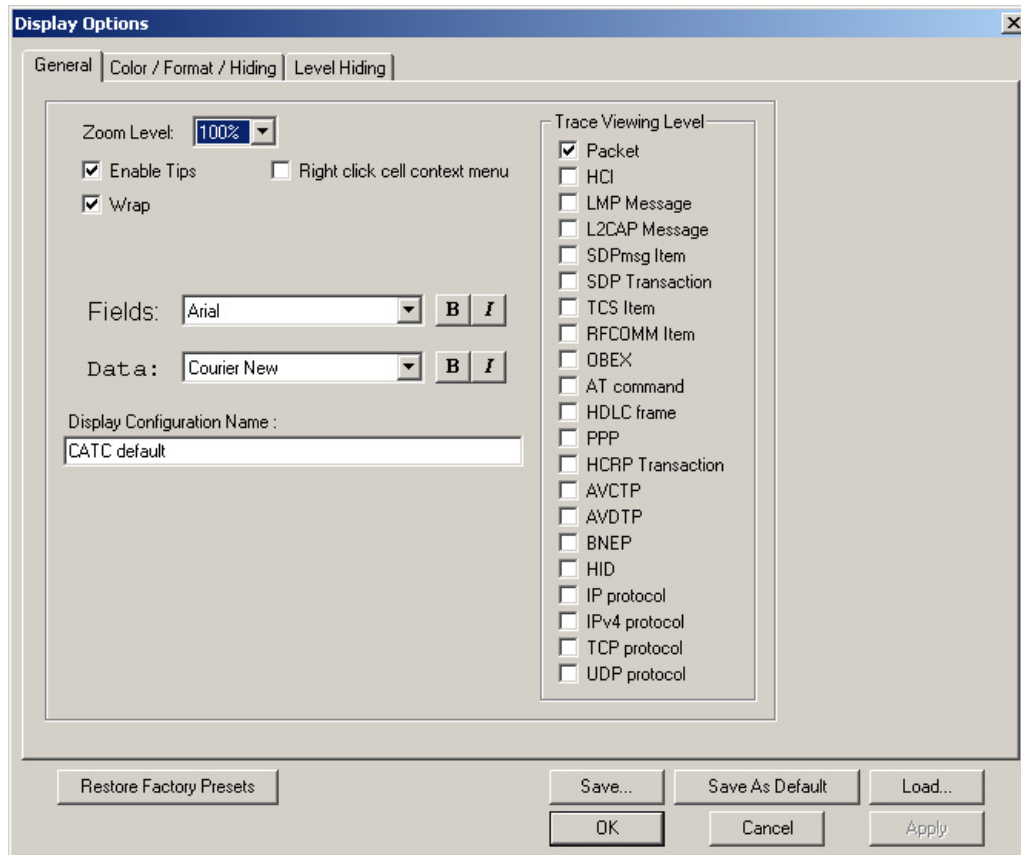
**Step 4** Give the recording a unique name and save it to the appropriate directory.



## 7. Display Options

Use the **Display Options** menu to specify the way CATC Trace information is displayed.

From the **Setup** menu, select **Display Options**.



## 7.1 General Display Options

Use the General Display Options to specify the basic appearance of a Trace view.

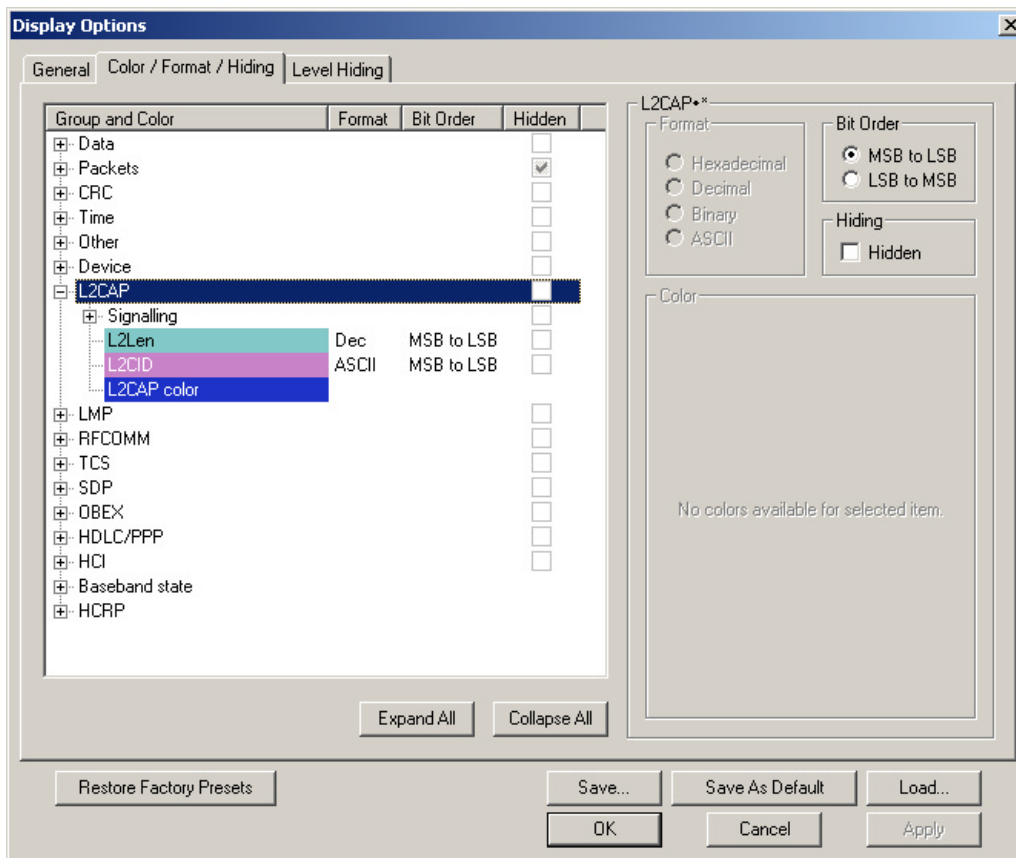
- **Zoom Level:** Adjustable in discrete increments from 10% to 200% percent.
- **Enable Tips:** Select to enable Tool Tips with explanation text to pop up when you position your cursor over various fields in the Trace View.
- **Wrap:** Causes packets to wrap within the window if their length exceeds the width of the window.
- **Right click cell context menu:** Activates the right mouse button for opening cell context menus.
- **Trace Viewing Level:** Allows you to select the hierarchical level at which traffic is displayed.
- **Fields:** Configures the appearance of field text within the trace.
- **Data:** Configures the appearance of data within the trace.
- **Display Configuration Name:** Comment field associated with the \*.opt file containing the current Display Options values. You can also create and store your unique Display Options for future use.

To create a new Display Options file, follow these steps:

- Step 1** Enter a comment for the new file in the **Display Configuration Name** field.
- Step 2** Click **Save...**
- Step 3** Specify a filename (\*.opt).
- Step 4** Click **Save**.

## 7.2 Setting Color, Formatting, and Hiding Options

Click the **Color/Format/Hiding** tab on the Display Options screen.



Use this window to customize the colors and formats associated with each field in the Trace view. You can also use this window to hide fields within the trace.

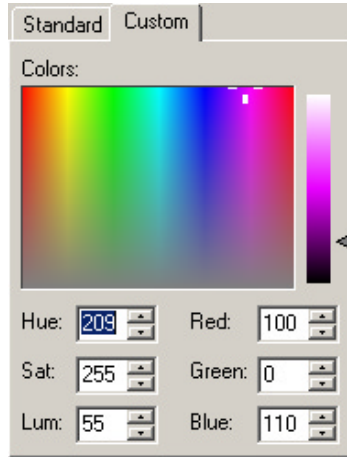
### Setting Color Display Options

To change the colors of elements in the trace, select an item in the Group and Color column and use the color pallet screen on the right to make the desired changes.

**Note** The color of an Invalid Data (packet error) field cannot be changed; it is permanently set to red.

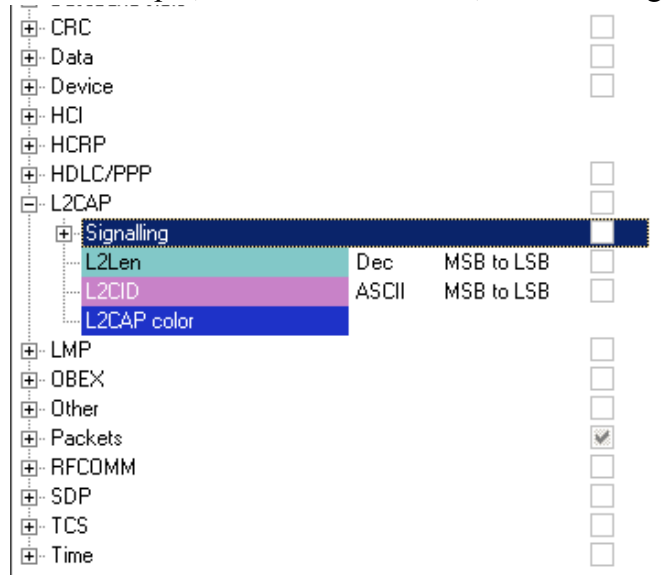
Use this window to customize the colors associated with each field in the trace. You can experiment with these options to achieve the color combination best suited to a particular graphic system.

You can also customize the colors by using the options in the Custom tab.

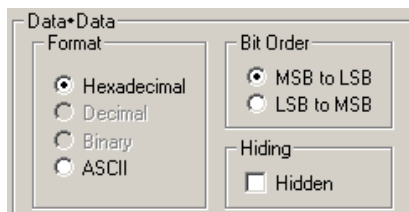


### Changing Field Formats

To change field formats, select an item under the Group and Color column. This action will enable the formats radio buttons on the right. The format types change with respect to the item selected under the Group and Color column. For example, if L2CAP is selected, the following displays:



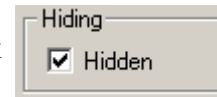
The following formats are available:



**Note** Not every format is available for every item.

## Hiding Display Options

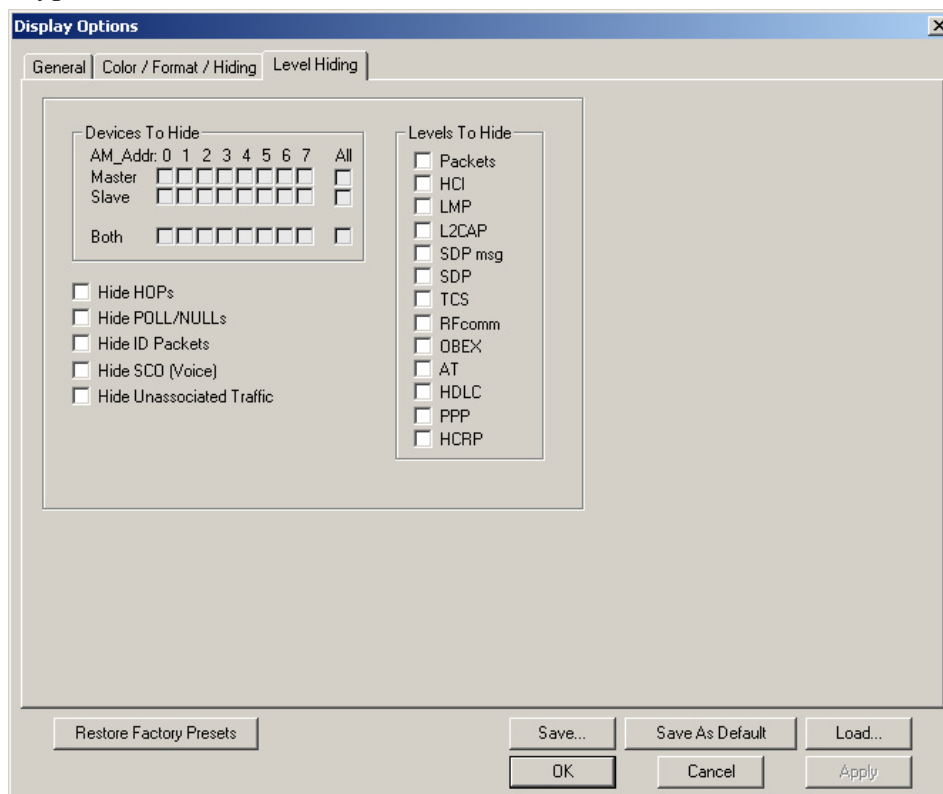
To hide one or more fields in the trace, select the appropriate item from the Group and color column, click the checkbox marked **Hidden**, and click the **Save** button.



You can also hide Sequences from a trace by selecting the desired options from the checkboxes.

## 7.3 Level Hiding Options

The Level Hiding tab allows you to hide FISs, Idle Sequences and other types of traffic. To hide traffic, select one or more items, then click **Save**.



### Level Hiding Parameters

Use the Hiding window to hide various fields, packets, messages, and protocols from the Trace View screen. You can modify these settings at will to display a specific area of a Trace.

#### *Hiding Fields*

The "Hide Fields" checkboxes allow individual fields to be hidden within a trace. Click the checkbox(es) of your choice to hide one or more fields.

### Hiding Packets, Messages, and Protocols

The "Hide Packets and Transactions" box contains two grids of checkboxes for hiding whole packets, messages, protocols, and traffic from individual devices. The grids are labeled "Devices to Hide" and "Levels to Hide".

#### Devices to Hide

The "Devices to Hide" grid lets you hide traffic according to device address. The grid divides into columns which represent different devices.

Devices To Hide									
AM_Addr:	0	1	2	3	4	5	6	7	All
Master	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Slave	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Both	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Columns labeled "0" through "7" and "All" represent the **Active Member Address** of a device. By checking one of the boxes in a column, you hide the traffic of the selected device (or traffic from all devices if you have selected **All**.)

The row in which you place your checkmark determines whether you are hiding traffic going to or from a device.

- Master - Hide traffic from a Master to selected Slaves
- Slave - Hide traffic from selected Slaves to the Master
- Both - Hide all traffic between the Master and selected Slave

Example: to hide all traffic from a Master *to* a Slave device with an address of six, click the checkbox under column **6** on the row marked **Master**.

#### Levels to Hide

The "Levels to Hide" grid divides into rows which represent the different packet, message, and protocol levels. Clicking a checkbox will cause Merlin to hide all traffic of a selected level.

Levels To Hide	
<input type="checkbox"/>	Packets
<input type="checkbox"/>	LMP
<input type="checkbox"/>	L2CAP
<input type="checkbox"/>	SDP msg
<input type="checkbox"/>	SDP
<input type="checkbox"/>	TCS
<input type="checkbox"/>	RFcomm
<input type="checkbox"/>	OBEX
<input type="checkbox"/>	AT
<input type="checkbox"/>	HDLC
<input type="checkbox"/>	PPP

#### Hiding Packets

At the bottom of the Hiding tab of the Display Options window, check boxes are available for hiding HOPs, POLLS, NULLs, and other kinds of traffic.

<input type="checkbox"/>	Hide HOPs
<input type="checkbox"/>	Hide POLL/NULLs
<input type="checkbox"/>	Hide ID Packets
<input type="checkbox"/>	Hide SCO (Voice)
<input type="checkbox"/>	Hide Unassociated Traffic

## 7.4 Saving Display Options

To complete your display options settings, use the features at the bottom of the **Display Options** window. These features remain the same no matter which of the four **Display Options** windows you are working in.

- Click **Save** to save the currently specified display options for use in future sessions. Any file name can be specified, but you must use the **.opt** extension. If no extension is specified, **.opt** is added by default.
- Click **Load** to load a previously saved **\*.opt** file, thus restoring a previous set of display options.
- The **Save as Default** function is equivalent to the **Save** function, specifying the file name **default.opt**. Whenever you start up the Analyzer, it automatically loads the **default.opt** file if one exists.
- Click **OK** to apply any changes you have made to **Display Options** and close this dialog box.
- Click **Cancel** to cancel any immediate changes you have made and exit the **Display Options** menu.
- Click **Apply** to apply your changes while keeping the **Display Options** window open.





## 8. Reading a CATC Trace

Packet	Hop Freq	Idle	Time Stamp										
0	2456	4.383 sec	00003.193 3643										
Packet	Hop Freq	Idle	Time Stamp										
1	2478	88.000 µs	00007.575 8643										
Packet	T Freq	CA C	HDR	Addr	POLL	Idle	Time Stamp						
2	M 2478			0x1	0x1	1.518 ms	00007.575 9523						
Packet	Hop Freq	Idle	Time Stamp										
3	2408	7.000 µs	00007.577 5961										
Packet	T Freq	CA C	HDR	Addr	NULL	Idle	Time Stamp						
4	S 2408			0x1	0x0	492.000 µs	00007.577 6031						
Packet	Hop Freq	Idle	Time Stamp										
5	2419	5.000 µs	00007.578 2211										
Packet	T Freq	CA C	HDR	Addr	DM1	L_CH	L2FL	Len	Data	CRC	Ack'd	Idle	Time Stamp
6	M 2419			0x1	0x3	LM	1	1	66	0x02E8	Yes	424.000 µs	00007.578 2261

### 8.1 Trace View Features

- The Merlin packet view display makes extensive use of color and graphics to fully document the captured traffic.
- Packets are shown on separate rows, with their individual fields both labeled and color coded.
- Packets are numbered (sequentially, as recorded), time-stamped, and highlighted to show the device status (master or slave).
- Display formats can be named and saved for later use.
- Pop-up Tool Tips annotate packet fields with detailed information about their contents.
- Data fields can be collapsed to occupy minimal space in the display (which can in turn be zoomed in and out to optimize screen utilization).
- The display software can operate independent of the hardware and so can function as a stand-alone Trace Viewer that may be freely distributed.

### 8.2 Interpreting the Displayed Information

Packet	T Freq	Pre	CA C	Trail	Addr	DM1	Flow	Arqn	Seqn	HEC	L_CH	L2FL	Len	Data
2	M 2452	0xA	0xB00012488AC3A74C	0xA	0x1	0x3	1	0	1	0x2D	LM	1	1	66
CRC	Ack'd	Idle	Time Stamp											
0x02E8	Yes	1.458 ms	00006.135 9825											

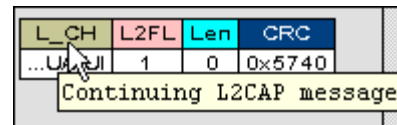
The following table describes the abbreviations used in the Merlin display. Packet #0 is described from left to right:

<b>Packet:#</b>	<b>Packet/Event Number</b>
T/M, T/S	M =Master Device Transmitting S = Slave Device Transmitting
Freq	Current Hop Frequency (in MHz)
Pre	Preamble of the Sync word

Packet:#	Packet/Event Number
CAC	Channel Access Code
Trail	Access Code Trailer of the Sync word
Addr	Active Member Address
DM1	DM1 Packet Type
Flow	ACL Link Flow Control
Arqn	Acknowledgment Indication Flag
Seqn	Sequential Numbering
HEC	Header Error Correction Code
L_CH	LMP Message
L2FL	L2CAP Flow Control Flag
Len	Message Length in Bytes including Opcode
TID	LMP Transition initiated by Master
Opcode	LMP-host_connection_req
CRC	Cyclic Redundancy Check
Ack'd	Packet Acknowledgment based on subsequent packet's ARQN with same AM_ADDR
Idle	Idle Time in nanoseconds
Time Stamp	Decimal in Seconds.Milliseconds.Microseconds*10 This is the analyzer internal clock as a reference with resolution of 100 ns.

### 8.3 Tooltips

You can get additional information about each field in a trace by holding your mouse pointer over a field. A tooltip will appear with details about the field.



### 8.4 Set Marker

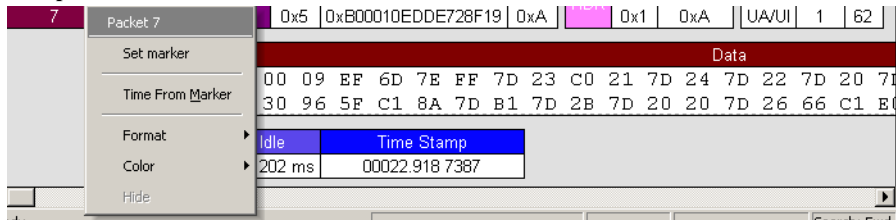
**Note** **Set Marker** works in conjunction with the **Go to Marker** feature.

You can define a unique Marker for each packet.

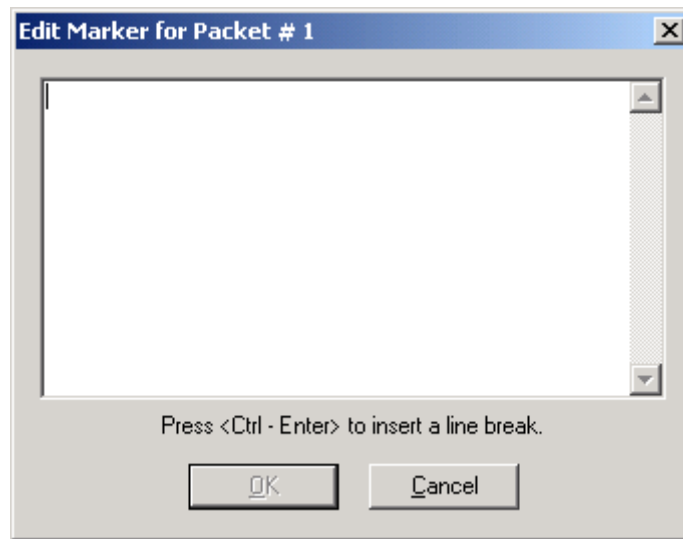
To place a marker on a packet,

**Step 1** Left-click on **Packet #** for the packet you wish to mark.

**Step 2 Select Set Marker.**



You see the **Edit Marker Comment** window where you can enter a unique comment about this packet.:



**Step 3** Enter your comment.

**Step 4** Click **OK**.

A marked packet is indicated by a vertical red bar along the left edge of the packet # block:

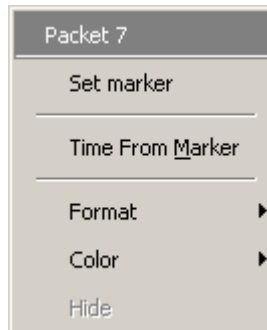
Packet#	T	Freq	Pre	CAC	Trail	Addr	NULL	Flow	Arqn	Seqn	HEC	Time Stamp
1681	S	13	0x5	0xB00010EDDE728F19	0xA	0x1	0x0	1	1	1	0x0B	00060.128 5315

## 8.5 Edit or Clear Marker

To clear or edit the comments associated with a packet marker,

**Step 1** Left-click on **Packet #** for the chosen packet.

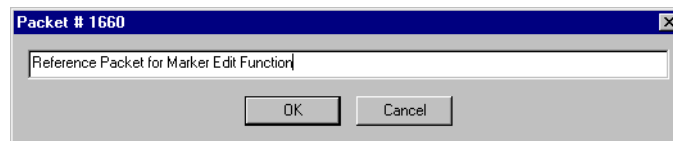
You see the **Packet** menu:



To edit the Marker Comment,

**Step 2** Select **Edit marker**.

You see the **Edit marker comment** window:



**Step 3** Edit the comment as desired.

**Step 4** Click **OK**.

To clear a Marker,

**Step 5** Click **Clear marker**.

The vertical red Marker bar disappears.

## 8.6 Expanded and Collapsed Data Formats

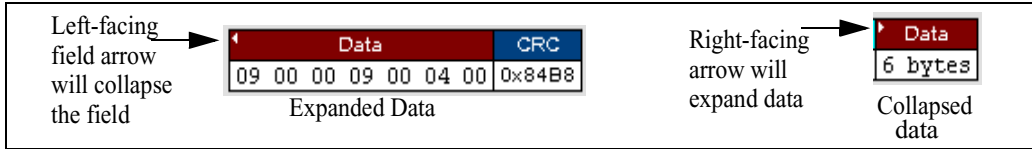
The data field can be expanded to display greater detail or collapsed to a compact view. The Expand/Collapse Data feature operates as a toggle. There are three ways to toggle between the two views.

### *Double-Clicking*

You can expand or collapse a Data field by double-clicking anywhere in the Data field of a packet.

### Left-clicking a Field Arrow

Many fields have small arrows in the top left corner. If you left-click this arrow, the field will toggle back and forth between collapsed and expanded views.



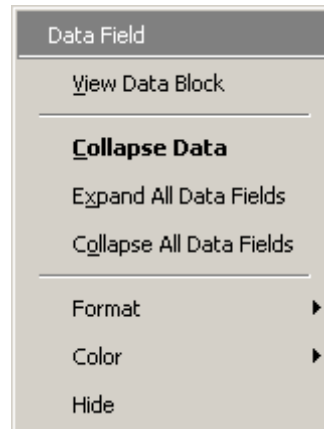
If you click and hold down the left mouse button on one of these arrows, you can collapse or expand the field for *ALL* packets, messages or protocols.

### Using the Shortcut Menu

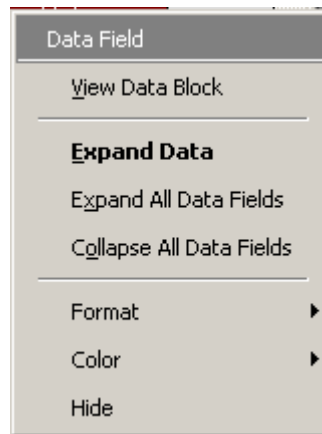
If you left-click on a **Data** field, a menu will open for expanding or collapsing data fields.

**Step 1** Left-click on **Data** in the Data packet you want to expand or collapse.

If your Data Trace View is currently expanded, you see the **Collapse Data** menu:



If your Data Trace View is currently collapsed, you see the **Expand Data** menu:



Note that you can choose to expand or collapse

- **Only** the Data in the selected Data packet
- OR
- **All** Data Fields in the Trace View.


**Step 2** Select the desired Expand Data or Collapse Data menu item.

The Trace View is repositioned with the selected packet(s) adjusted in the format you have specified.

## 8.7 Hide Frequency Hops

You can hide Frequency Hops (Hops) from a trace by pressing the **Hide Hops** button on the Tool Bar:


From the Tool Bar

- Click  to hide all Hop packets.

## 8.8 Hide Nulls and Polls

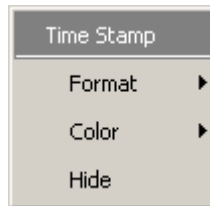
You can hide Nulls and Polls from a trace by pressing the **Hide Nulls and Polls** button on the Tool Bar.

From the Tool Bar

- Click  to hide all Nulls and Polls.

## 8.9 Menus in Clicked Fields



You can display the following menu when you click in a field in a trace.



## 8.10 Hide Unassociated Traffic

You can hide all traffic that is not associated with the current decode level by pressing the **Hide Unassociated Traffic** button on the Tool Bar.

### From the Tool Bar

- First, click one or more decode buttons such as the **View L2CAP Messages** . This button will cause Merlin to decode the trace and display selected level of decode.
- Next, click  to hide all unassociated traffic.

The **Hide Unassociated Traffic** button will cause Merlin to hide all traffic except for the selected decode messages or protocols. In the example above, all packets would be hidden and only L2CAP messages would display.





# 9. Decoding Protocols

SDPmsg	T	Addr	PDU ID	Trans ID	ParLength	SrvSearchPat	MaxSrvReqCount	Continuation	Time					
0	M	0x1	SrvSearchReq	0xAABB	8	0x1101	8	end	8.314s					
SDPmsg	T	Addr	PDU ID	Trans ID	ParLength	TotSrvReqCount	CurSrvReqCount	Data	Continuation	Time				
1	S	0x1	SrvSearchResp	0xAABB	9	1	1	00 01 00 02	end	8.318s				
L2CAP	T	Addr	Packets	L2Len	L2CID	A	Data		Time					
15	S	0x1	1	14	Dyn: 0x0041	S	0000: 03 AA BB 00 09 00 01 00 0008: 01 00 01 00 02 00		8.318s					
Packet	T	Freq	CAC	HDR	Addr	DM1	L_CH	L2FL	Len	Data	CRC	Ack'd	Idle	Time Stamp
1330	S	2429			0x1	0x4	UA/UI	1	18	0000: 0E 00 41 00 03 AA BB 00 09 00 01 00 01 00 01 00 0016: 02 00	0xA858	Yes	314.000 μs	00008.318 8476

## 9.1 Introduction

Merlin can decode HCI, LMP and L2CAP messages, and RFCOMM, SDP, TCS, HDLC, PPP, OBEX, HCRP, BNEP, HID, IP, TCP, and UDP protocols. The default is *packet level* decoding, which means that baseband packets will be displayed when you first view a trace. If these packets are carrying LMP, L2CAP or other protocols, the protocols will display as undecoded fields such as the L2CAP packet below.

←Undecoded L2CAP fields→														
Packet	T	Freq	CAC	HDR	Addr	DM1	L_CH	L2FL	Len	Data	CRC	Ack'd	Idle	Time Stamp
1318	M	2420			0x1	0x3	UA/UI	1	17	17 bytes	0x7E98	Yes	243.800 μs	00008.314 4708

By issuing a decode command, Merlin can decode these LMP and other fields and display the data in summary statements called *LMP/L2CAP Messages*, *Protocol Messages*, and *Protocol Transactions*.

## 9.2 LMP and L2CAP Messages

LMP and L2CAP Messages are lines in a trace that summarize LMP and L2CAP actions such as an *LMP connection request*. LMP and L2CAP Messages summarize the type of action, the number of packets involved in

the action, and the device performing the action. If the message is carrying other protocol data such as RFCOMM, TCS, OBEX or SDP data, the message displays this data in an undecoded format that can be decoded later.

L2CAP	T	Addr	Packets	L2Len	L2CID	A	Data	Time
14	M	0x1	1	13	Dyn: 0x0041	S	0000: 02 AA BB 00 08 35 03 19 0008: 11 01 00 08 00	8.314s

Undecoded protocol data

## 9.3 Decoding and Viewing Protocol Data

Protocol data can be decoded two ways: by clicking a decode button on the toolbar or by selecting a decode command from a pull down menu.

### Decoding Via the Decoding Toolbar




The Decoding Toolbar has ten buttons for decoding packets, messages, and protocols:

- **Pkt** (Display Packets)
- **HCI** (Display HCI Protocol)
- **LMP** (Display LMP Messages)
- **L2CAP** (Display L2CAP Messages)
- **SDP Msg** (Display SDP Protocol Messages)
- **SDP Tra** (Display SDP Transactions)
- **TCS** (Display TCS Protocol messages)
- **RFCOMM** (Display RFCOMM Protocol)
- **OBEX** (Display OBEX Protocol)
- **AT** (Display AT Commands Protocol)
- **HDLC** (Display HDLC Protocol)
- **PPP** (Display PPP)
- **HCRP** (Display HCRP)
- **AVCTP** (Display AVCTP)
- **AVDTP** (Display AVDTP)
- **BNEP** (Display Bluetooth Network Encapsulation Protocol)
- **HID** (Display HID Protocol)
- **IP** (Display IP)

- **TCP** (Display TCP)
- **UDP** (Display UDP)

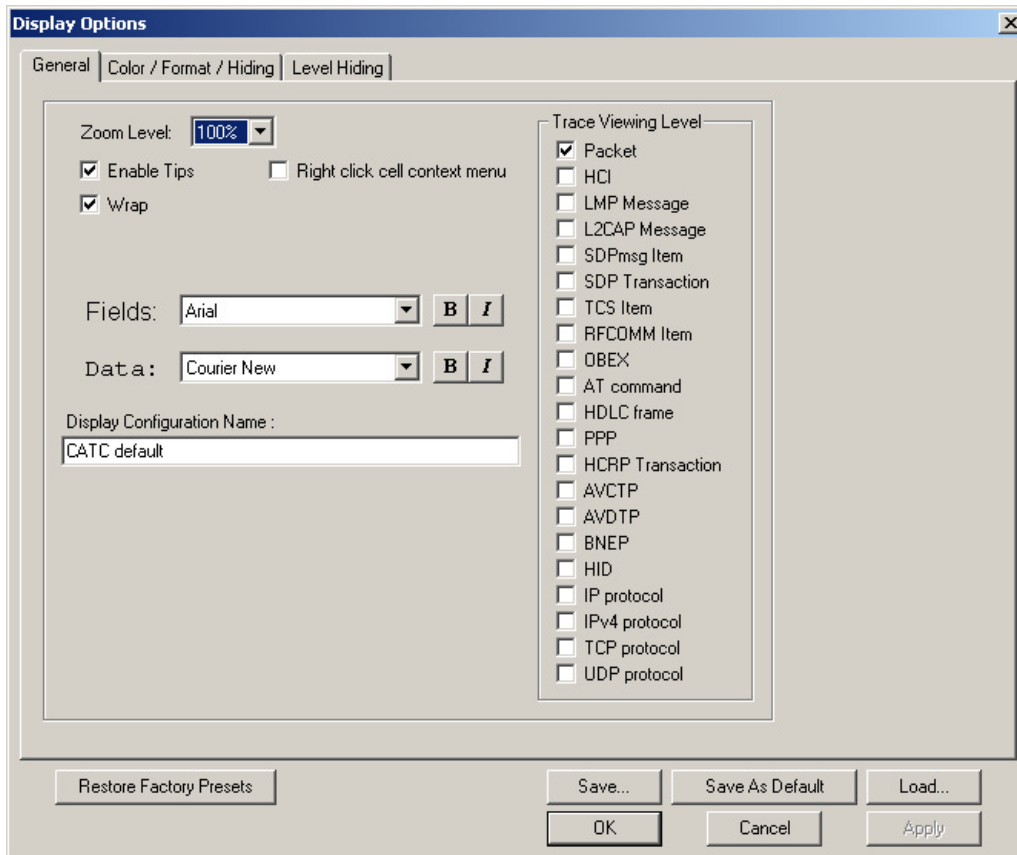
For example, to display LMP messages, click .

**Note** Once a decode has been performed, it will probably be necessary to scroll through the display to find the decoded messages or protocols. You can shorten your search by first clicking the Hide Unassociated Traffic button .

### Decoding Via the Display Options Dialog Box

The Display Options dialog box has three options for issuing decode commands. To issue a command,

**Step 1** From the menu bar, select **Setup>Decoding Options**



**Step 2** Select the option for the desired level of decoding.

**Step 3** Click **OK** or **Apply**.

## 9.4 Tooltips

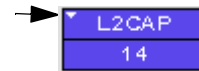
Additional information about fields can be attained by positioning your mouse pointer over a field of interest. A tooltip will appear that will provide details about the field. In some cases, there can be a considerable amount of information available.

Code	Ident	SigLen	DestnCID	SrcCID	Result
ConnReq	0x03	8	0x0041	0x0040	0x0000

Connection Request Signalling Command Code 0x3

## 9.5 Viewing Packets in LMP and L2CAP Messages

LMP and L2CAP Messages can be "opened" to reveal their constituent packets by double-clicking the first cell in of the message or clicking once on the small arrow on that same cell. The packets will then display below the message. The following screenshot shows an example of a message and its packets.



L2CAP	T	Freq	Packets	L2Len	L2CID	A	Data	Time
19	S	0x1	2	41	Dyn: 0x0041	S	0000: 05 AA BB 00 24 00 21 36 00 1E 09 00 04 35 10 35 0016: 05 1A 00 00 01 00 35 07 1A 00 00 00 03 08 01 09 0032: 01 00 25 04 43 4F 4D 35 00	8.3273

Packet	T	Freq	CAC	DR	DH	L_CH	L2FL	Len	Data
1356	S	2406	0x1	0x4	UA/UA	1	27	0000: 29 00 41 00 05 AA BB 00 24 00 21 36 00 1E 0	
								0016: 04 35 10 35 05 1A 00 00 01 00 35	

Packet	T	Freq	CAC	DR	DH	L_CH	L2FL	Len	Data
1380	S	2465	0x1	0x4	UA/UA	1	18	0000: 07 1A 00 00 00 03 08 01 09 01 00 25 04 43	
								0016: 35 00	

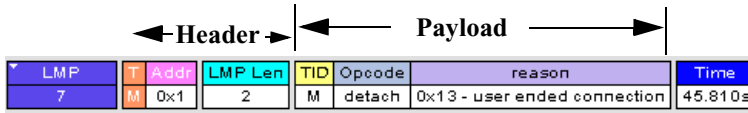
## 9.6 Types of LMP and L2CAP Messages

If you scroll through a trace, you will see three kinds of message:

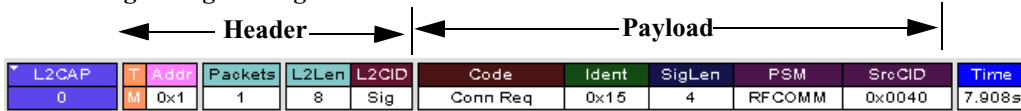
- LMP Signalling Message
- L2CAP signalling Message
- L2CAP Data Transfer Message

Each message has the same basic message header but differs in its payload.

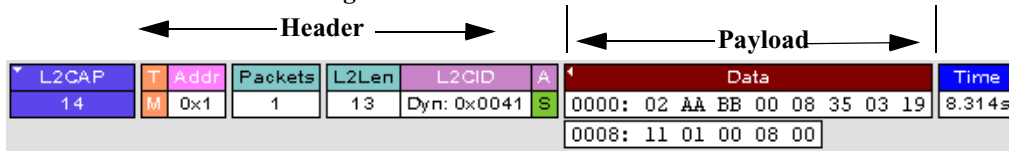
**LMP Signalling Message**



**L2CAP Signalling Message**



**L2CAP Data Transfer Message**



LMP and L2CAP Signalling messages have payloads of commands for establishing LMP and L2CAP channels. L2CAP Data-Transfer messages have a payload that may include RFCOMM, SDP, or TCS data. In order to view this protocol data, you will need to decode the messages (shown in the next section). The decoded data will appear as new lines in the trace called "Protocol Messages."

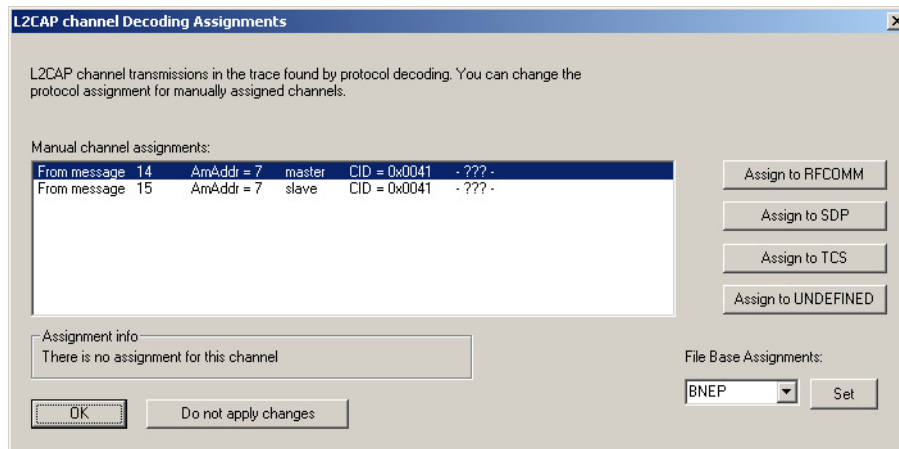
## 9.7 Viewing L2CAP Channel Connections

Once L2CAP messages have been decoded and displayed, you can check or change their L2CAP channel connections by opening the L2CAP Decoding Connections dialog box.

To view or change an L2CAP channel connection,

- Step 1 Select from the menu bar  
**View>Decoding Assignments**

The following dialog box will open.



- Step 2** Click on a channel assignment and then look at the Connect and Disconnect buttons on the far right of the dialog box.



If the Connect and Disconnect buttons are grayed-out, it means that Merlin made the channel assignments using data in the trace. You can verify that Merlin performed the assignments by looking at the text in the "Slave Channel" box in the lower left corner of the dialog box. If you see "Connection Recorded" it means that Merlin performed the channel assignments.

If Merlin was not able to make these channel assignments, then the Connect and Disconnect buttons on the right side of the dialog box will be active. You can then assign and edit channel connections.


- Step 3** Open the drop-down menu labeled AM\_Addr (Active Member Address). If possible, select an address other than the currently displayed address.

The connections for the 'new' device should now display.

## 9.8 Viewing Protocol Messages and Transactions

By pressing a button such as  or , you can cause Merlin to decode the protocol data contained within L2CAP messages and display them as packet-like rows called *Protocol Messages*. Protocol Messages have headers marked "protocol" and fields that vary in appearance and content depending on the type of protocol.

Some Protocol Messages can be grouped into an entity called a *Protocol Transaction*. A Protocol Transaction is a row in a trace that summarizes the higher level protocol data that is transmitted between a Master and Slave

device when one sends a request and the other sends back a response. For example, if you press , Merlin will locate SDP requests and responses between a Master and Slave device summarize their data.

### Viewing L2CAP Messages in Protocol Messages

If the protocol heading is double-clicked, the L2CAP data-transfer messages that make up the protocol will display below the protocol. You can also expand the protocol by left-clicking the small downward pointing arrow on the protocol header.

L2CAP	T	Addr	Packets	L2Len	L2CID	Code	Ident	SigLen	DestnCID	Flags	Data
10	M	0x1	1	12	Sig	Conf Req	0x19	8	0x0041	0x0000	01 02 00 00

Packet	T	Freq	CAC	HDR	Addr	DM1	L_CH	L2FL	Len	Data	CRC
779	M	2476			0x1	0x3	UA/UI	1	16	0000: 0C 00 01 00 04 19 08 00 0008: 41 00 00 00 01 02 00 02	0xEFA5

### How to Decode

Decoding Protocol messages is the same process as decoding LMP and L2CAP messages.

**Using the Toolbar** - To decode using the Toolbar, press one of the protocol decode buttons such as:   .


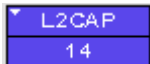
**Using the Menu** - To decode using the menu, select:  
**Setup>Display Options**

Then select one of the decode checkboxes.

Once a decode command has been issued, Merlin will create Protocol Messages in the trace. You will probably have to hide hops, polls, and null packets and then scroll through the trace in order to find Protocol messages.


### Expanding Protocol Messages

Protocol messages can be expanded to reveal their constituent packets using any of the following methods:

- Left-click the small downward pointing arrow in the message/protocol header  
- Double-click a message/protocol header
- Left-click the message/protocol header and choose "Expand Transaction" from the short-cut menu

## 9.9 Changing Protocol Assignments

If a sequence of messages is assigned the wrong protocol, errors will display. To change or remove a protocol assignment, you will need to access the **Assignment** menu and issue an Add Assignment command.

**Step 1** Click  to display L2CAP messages.

**Note** You need to view L2CAP Messages in order to have access to the "A" field that permits reassigning protocols.

**Step 2** Scroll through the trace until you have located an L2CAP message with a field marked "A."

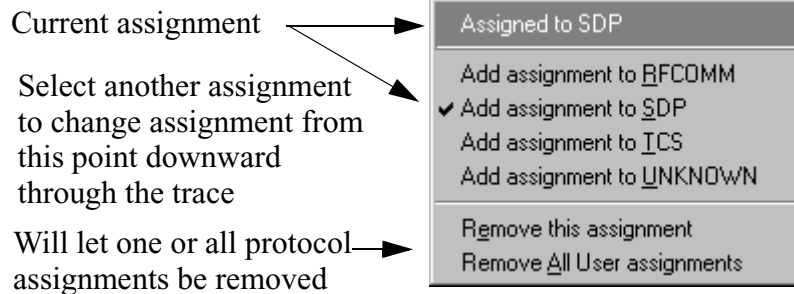
**Step 3** Left-click the field marked "A."

Left-click  
↓

Message	L2CAP	T Addr	L2Len	L2CID	A	Data	Time
40	3 Pkts	S 0x7	4	0x0040 (Dyn)	R	09 53 01 D9	154.711s

An **Assignment** menu will open for assigning, re-assigning, or un-assigning protocols to messages. This menu is context-sensitive and will vary in content depending on the protocols in the trace.

### The Assignment Menu



**Step 4** From the menu, select one of the "Add Assignment" options not already selected.

At this point, the protocol assignment will change to your selection.

### Using the Decoding Assignments Dialog Box

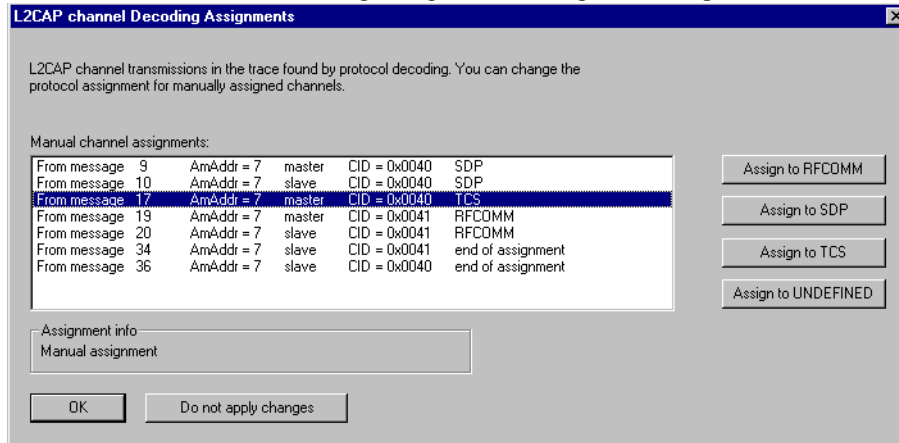
You can get a complete list of all protocol assignments by opening the Decoding Assignments dialog box. This dialog box will tell you which protocol assignments were made by Merlin and which are user-assigned. User-assigned protocols can be reassigned if need be using this dialog box.



To open the Decoding Assignments dialog box and reassign a protocol,

- Step 1** Select from the menu  
**View>Decoding assignments**

The Decoding Assignments dialog box will open. A status message in



the bottom left corner of the dialog box will indicate who assigned the protocol.

- Step 2** Click on one of the displayed assignments.

If the protocol was assigned by Merlin, the Assign buttons on the right will be grayed out and unavailable. If you want to change these assignments, you will have to use the pop-up menus described in the previous section. If a protocol has been manually assigned by a user, the Assign buttons will become active and allow you to make a change in assignment.

- Step 3** If possible, click the appropriate Assign button.

### Removing User-Assigned Protocol Assignments

As you practice assigning and reassigning protocols, you will find that one of the more useful commands is "Remove All User Assignments." This command allows you to undo all of your assignments.

To remove some or all user-assigned protocol assignments,

- Step 1** Double-click any Protocol Message header to open view L2CAP messages.
- Step 2** Locate a message with a field marked "A."
- Step 3** Left-click on the "A" field to open the Assignment menu.
- Step 4** Select "Remove All User assignments" or "Remove this assignment."

### Manually Assigning Protocols

If a recording does not capture the beginning of a dialog between a Master and Slave devices, Merlin may not have the L2CAP messages it needs to determine the correct protocol assignments. In this case, L2CAP messages will display an "N" in the Assignment field that means "Not Assigned."

Message	L2CAP	T	Addr	L2Len	L2CID	A	Data	Time
16	4 Pkts	S	0x7	14	Dyn: 0x0040	N	0000: 03 00 01 00 09 00 01 00 0008: 01 00 01 00 00 00	26.971s

↑  
N=Protocol not assigned





**An L2CAP message without a protocol assignment for protocol data within the message.**

If you know what the protocol assignment should be for the missing assignments, you can manually add them by right-clicking your mouse over the A field shown above and selecting from the pop-up Assignment menu shown on the previous page.

### Other Assignments: OBEX Client/Server Status

OBEX messages carry a status that indicates whether the transmitting device is an OBEX client or OBEX server.

To view an OBEX message's client/server status,

- Step 1 Open an OBEX trace file such as the sample file "OBEXsample.tfb" in C:\Program files\CATC\Merlin.
- Step 2 Press  , , and  to hide Hops, NAKs, and unassociated traffic.
- Step 3 Press  to decode OBEX.
- Step 4 Left-click your mouse over the field marked Type.

A pop-up menu will appear indicating whether the message was produced by an OBEX client or server. If the menu items appear

OBEX	TYPE	T	Addr	respon
1	req			
OBEX	TYPE			
2	req			
OBEX	TYPE			


Left-click over the Type field to open the OBEX Client/Server Assign menu.

grayed-out (as they do in this example) it means that Merlin assigned the client or server status based on data it found in the trace. If the menu items appear in black, it means that the user assigned the status and is therefore free to change the assignment.

### Changing an OBEX Client or Server Status

If the beginning sequence of traffic is not recorded in a trace, the client/server status of the transmitting devices will not be preserved in the trace. In this case, the OBEX Client/Server pop-up menu will become active and you will be able to change the assignment.


### Decoding BNEP

BNEP (Bluetooth Network Encapsulation Protocol) is a protocol that allows devices to encapsulate network protocols such as IP. Since BNEP can carry different types of network protocols, you need to tell Merlin what protocol the BNEP is going to be carrying. You do this via a script file called *bnep.dec* that is read during the initialization of the Merlin software. This file tells Merlin how to decode BNEP fields. Once read, BNEP can be correctly decoded by pressing the  button on the toolbar. If the decode file is not read at initialization, Merlin will display the data in an undecoded format.

For more information on BNEP decoding, see a supplemental document on BNEP in the support directory on the CATC web site:

[http://www.catc.com/products/support/sup\\_Merlinbluetooth.html](http://www.catc.com/products/support/sup_Merlinbluetooth.html)

### Decoding HID

HID (Human Interface Device) is a profile associated with traffic from devices such as a mouse or a keyboard. To decode HID traffic, you will need to tell Merlin what types of HID traffic it will be recording. You do this by editing a script file called *hid.dec*. Merlin reads this file during the initialization of the Merlin software. This file tells Merlin how to decode the HID fields. Once read, HID can be correctly decoded by pressing the  button. If the decode file is not read at initialization, Merlin will display the data in an undecoded format.

### Other Decoding Options

Other decoding options include the following:

- IP
- TCP
- UDP
- AVCTP
- AVDTP
- HCRP



## 10. Other Features

This chapter describes how to conduct searches and to create reports on errors, bus utilization, and other features.

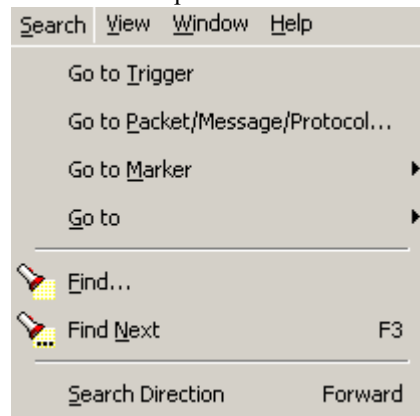
### 10.1 Search

The Search feature provides several options for searching through recorded traffic, allowing you to find specific packets based on triggering status, packet number, marking, or content.

To view the Search options,

- Click **Search** in the Menu bar.

You see the Search drop-down menu:



#### Go to Trigger

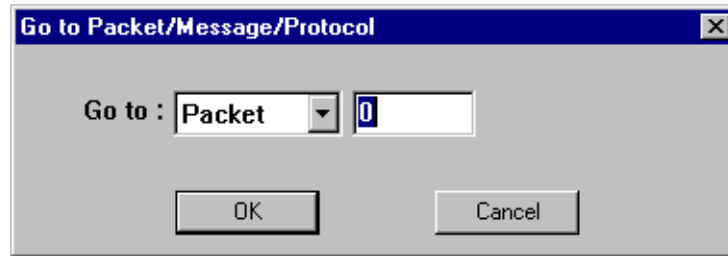
To display a triggering event, select **Go to Trigger** under **Search** on the Menu bar. The **Trace Viewer** display will reposition the trace to show the triggering event at the top of the screen.

#### Go to Packet/Message/Protocol

To display a specific packet, Message or Protocol

- Step 1** Select **Go to Packet/Message/Protocol** under **Search** on the Menu Bar.

You see the **Go to Packet/Message/Protocol** window:



**Step 2** Enter the number of the packet, message or protocol you want to display.

**Step 3** Click **OK**.

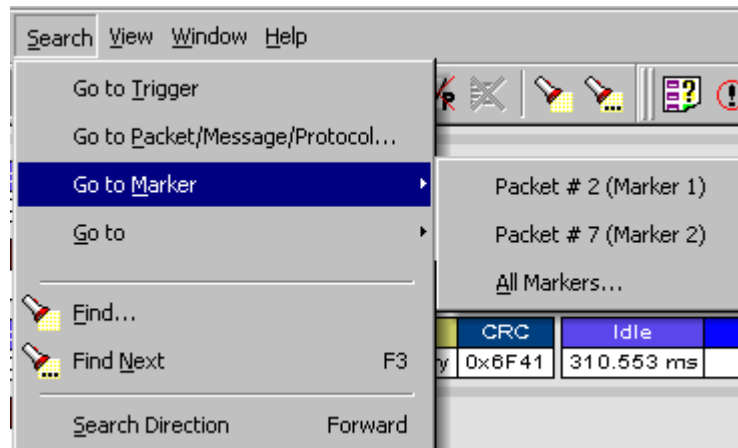
The Trace View repositions to show the packet at the top of your screen.

## Go to Marker

To instruct the analyzer to display a marked packet,

**Step 1** Select **Go to Marker** under **Search** on the Menu Bar.

You see a drop-down menu listing the marked packets in that Trace View:



**Step 2** Select the desired packet from the displayed list.

The Trace View repositions to show the packet at the top of your screen.

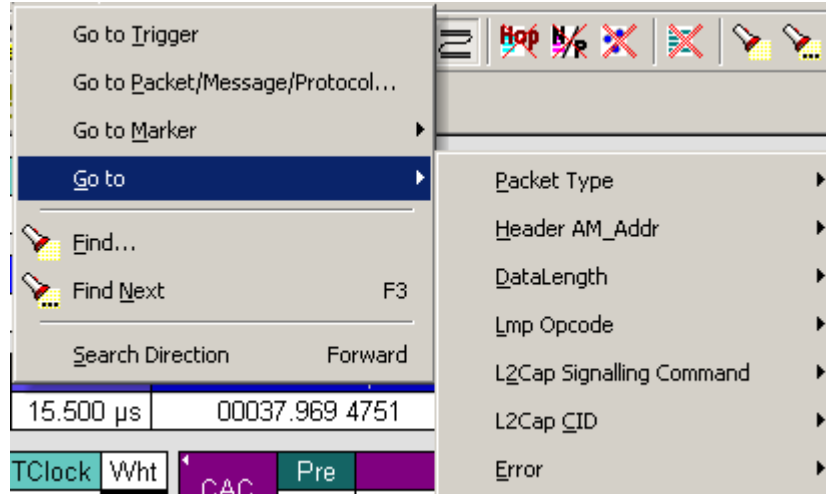
**Note** The **Go to Marker** feature functions in conjunction with the **Set Marker** feature. The comments within the parentheses following each marked packet are added or edited with the **Set Marker** feature.

## Go to

The **Go To** feature takes you directly to an event in a Trace.

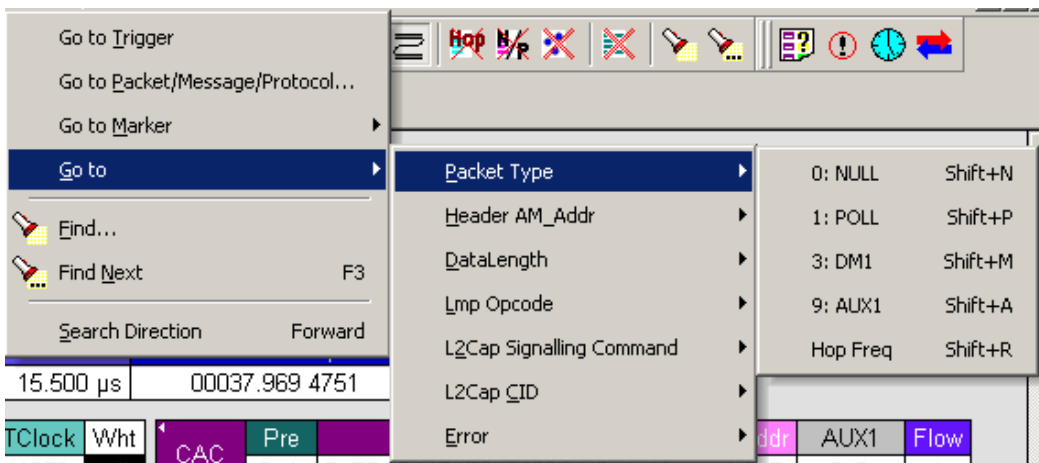
**Step 1** Select **Go To** under **Search** on the Menu Bar.

You see the **Go To** drop-down menu:



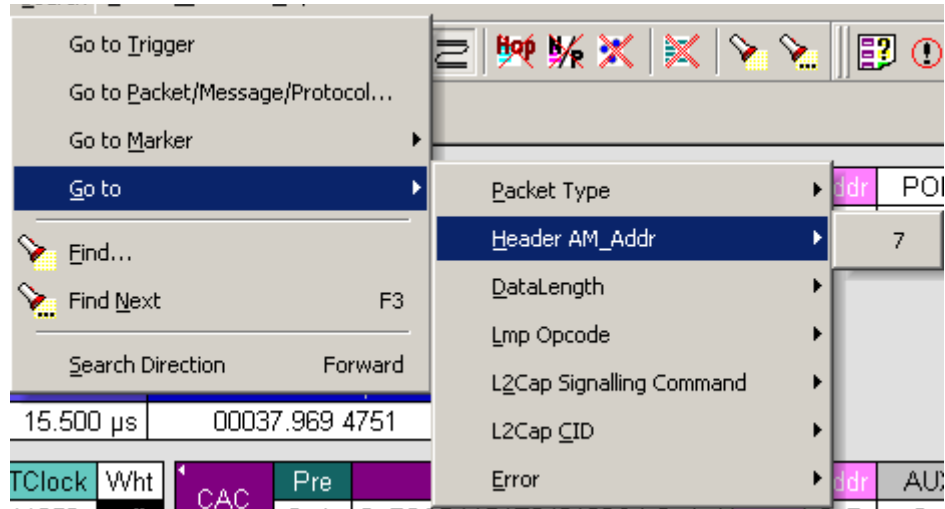
**Step 2** Select the event you want to go to and enter the necessary information.

*Packet Types*



Select the type of packet you want to go to.

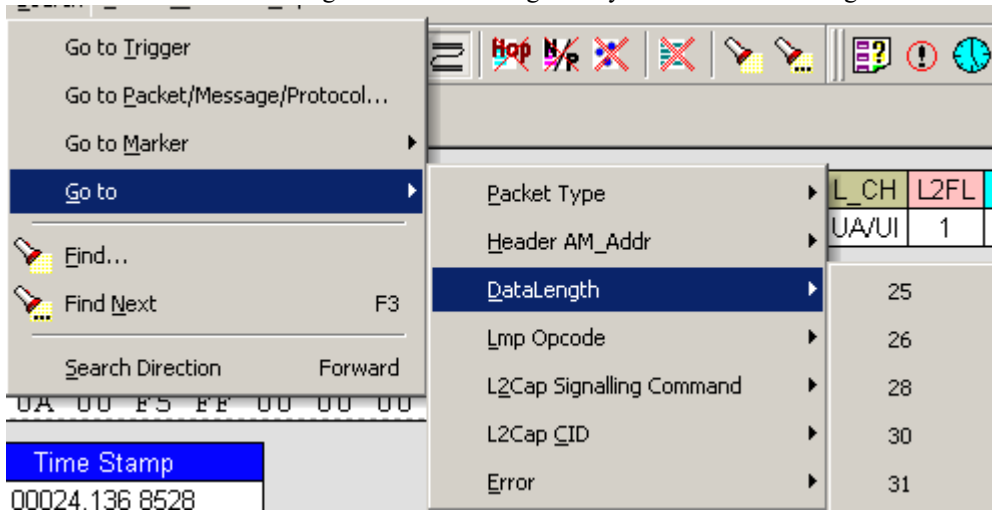
*Header AM\_Addr*



Select an Active Member Address from the list.

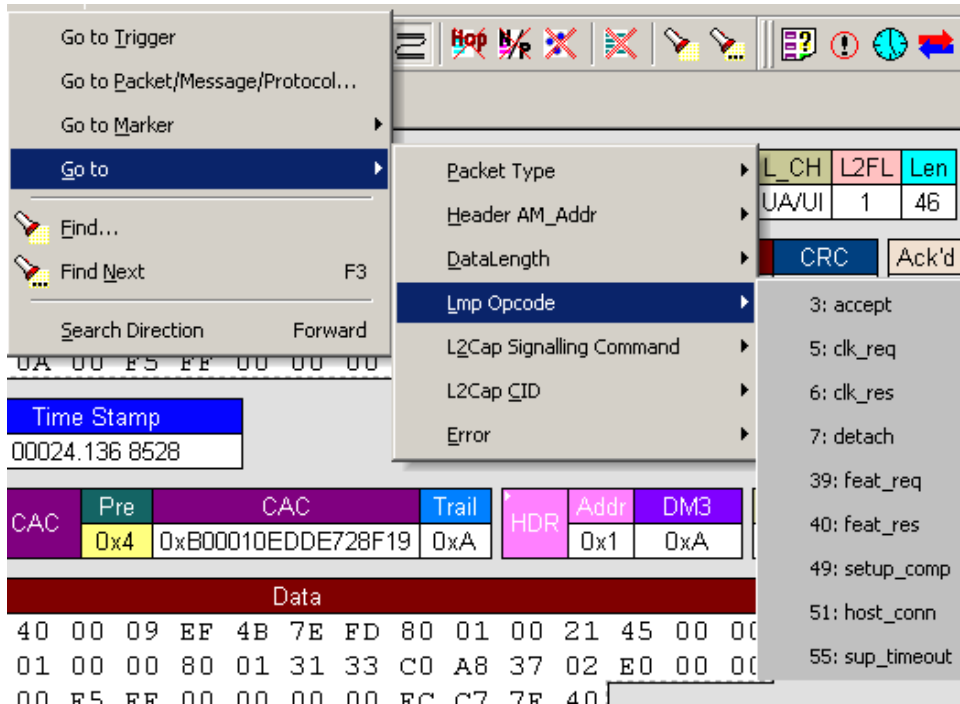
*DataLength*

Allows searching based on data length in bytes from the recording.



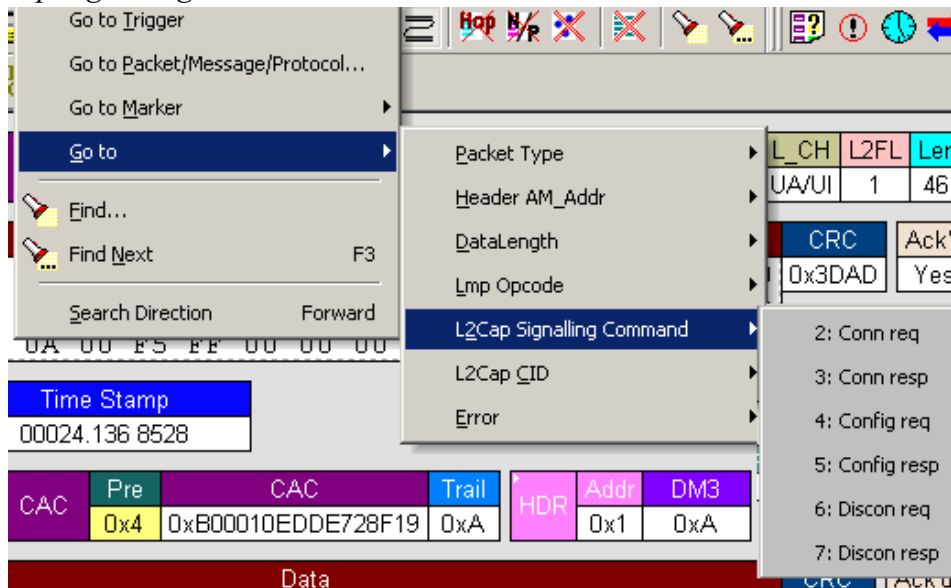


*Lmp Opcode*

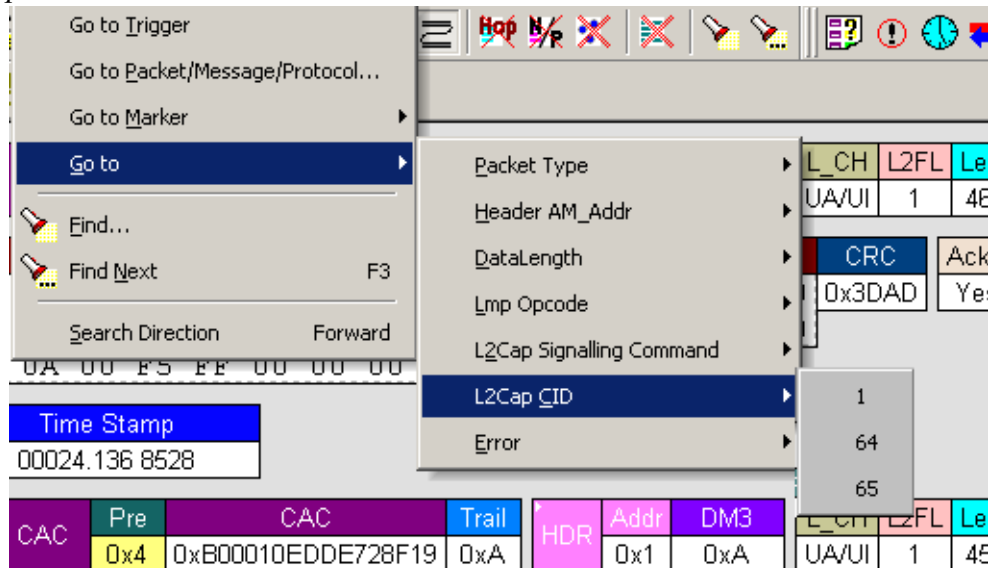


Select the Link Management Protocol Operational Code (Lmp Opcode) that you want to go to.

*L2Cap Signalling Command*



Select the type of L2Cap Signalling Command that you want to go to.

*L2Cap CID*

Select the L2Cap Channel ID (L2 Cap CID) that you want to go to.

**Error**

Moves trace view to next uncorrected error.

**Soft Bit Error**

Moves trace view to next soft (corrected) error.

**Loss of Sync**

Moves trace viewer to the next loss of sync.


**Find**

**Find** is a utility that allows you to conduct searches of one or more events within a trace. Find allows you to search different hierarchical levels within the trace - packets, LMP Messages, L2CAP messages etc.

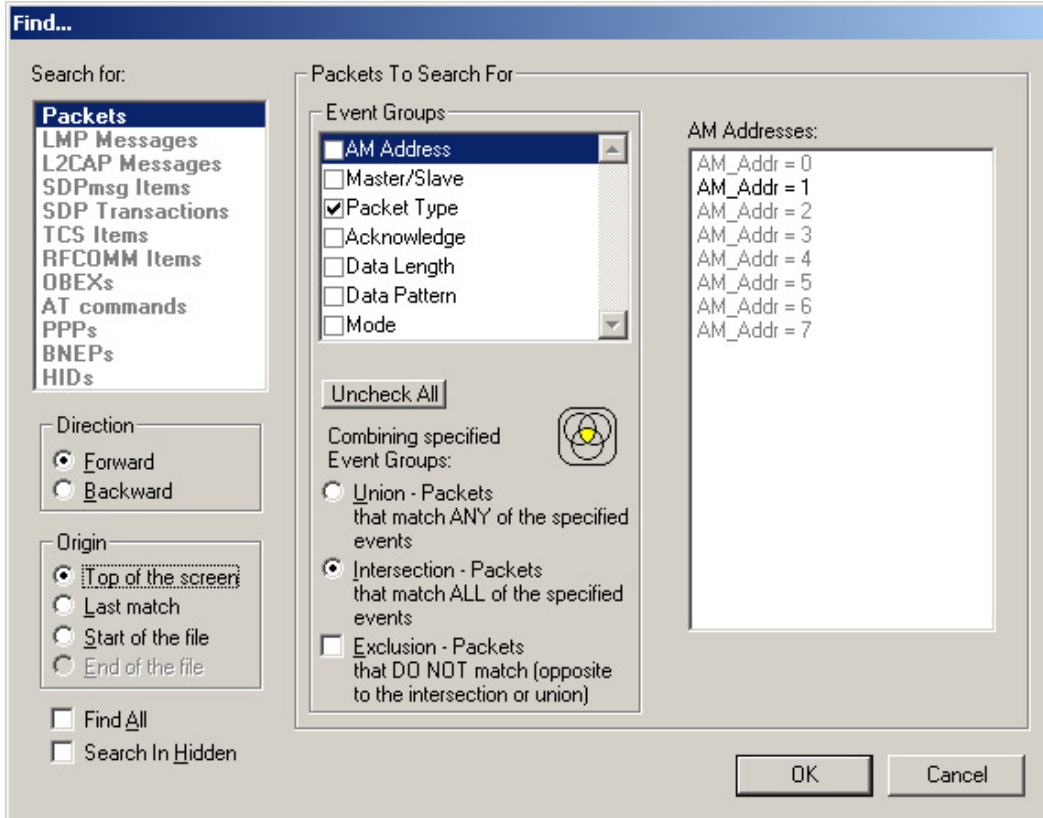
To start find,

- Select **Find...** under **Search** on the Menu Bar

OR

Click  in the Tool Bar.

You see the **User-Defined Find Events** screen:



The **Find** window divides into three areas:

**Left area** -- Controls the search level, search direction and search origin.

**Find All** - Extracts the results and place them in a separate trace.

**Search In Hidden** - Searches all packets including packets that have been hidden.

**Center area** -- Controls the event groups to be searched. The selection you make will display further choices on the right side of the Find window. At the bottom are three options called Union, Intersection, and Exclusion that are used with multi-criteria searches. These options are explained below.

**Right area** -- Controls the specific events to be searched within the trace. The box in this right section displays events from the selected Event Group.

The right area is context sensitive -- the Event Group selected in the Center area will determine what events will display on the right. For example, if you select **Packet Type**, the Right area will show you a list of packet types. Bold entries in the list represent items that actually occurred in the trace.

In the screenshot shown above, for example, AM Address is selected. On the right, you see that only Address 1 is in bold. This indicates that only a single device was transmitting traffic in the displayed trace.

### Event Groups

Event Groups are categories of events that can occur in a trace. Clicking on an Event Group will display a list of Event types on the right side of the Find window that occur within each Event Group.

#### *AM Address*

Contains a list of seven Active Member addresses. Bold entries represent devices that occur in the trace.

#### *Master/Slave*

Contains two options labeled **Master** and **Slave**. Selecting an option will cause Merlin to search for traffic based on the selected role.

#### *Packet Type*

Contains a list of all Bluetooth packet types. If a packet type occurs in the trace, it will appear in bold.

#### *Acknowledge*

Contains a list of three Acknowledge types: **Explicit NAK**, **Implicit NAK**, and **ACK**. The three Acknowledge types are responses a device can issue to attempts to transmit packets to it.

A device can send an Acknowledgment in two ways: through setting the ARQN field to 0 (= explicitly not acknowledged), to 1 (explicitly acknowledged) or by sending an empty packet that does not have an ARQN field (= implicitly not acknowledged).

**Explicit NAK** - Explicitly not acknowledged. An Explicit NAK is an explicit response by a device that it did not receive a data packet. The Explicit NAK is transmitted in the ARQN field (=Acknowledgment Request Negotiation field). ARQN=0 means 'Explicit NAK.'

**Implicit NAK** - Implicitly not acknowledged. An Implicit NAK is a NAK that is implied rather than explicitly stated. If a device responds to a data packet by sending an empty packet, the NAK is implied.

**ACK** - Acknowledged. If a data packet is successfully transmitted to a target device, the target device acknowledges the received packet by setting the ARQN field to 1.

Acknowledgments are easily seen in Merlin traces because Merlin adds an **Ack'd** field on data packets of the transmitting device. This means that you do not have to hunt through the trace to see if the packet was acknowledged.

The following screenshot shows two examples of Acknowledgments.

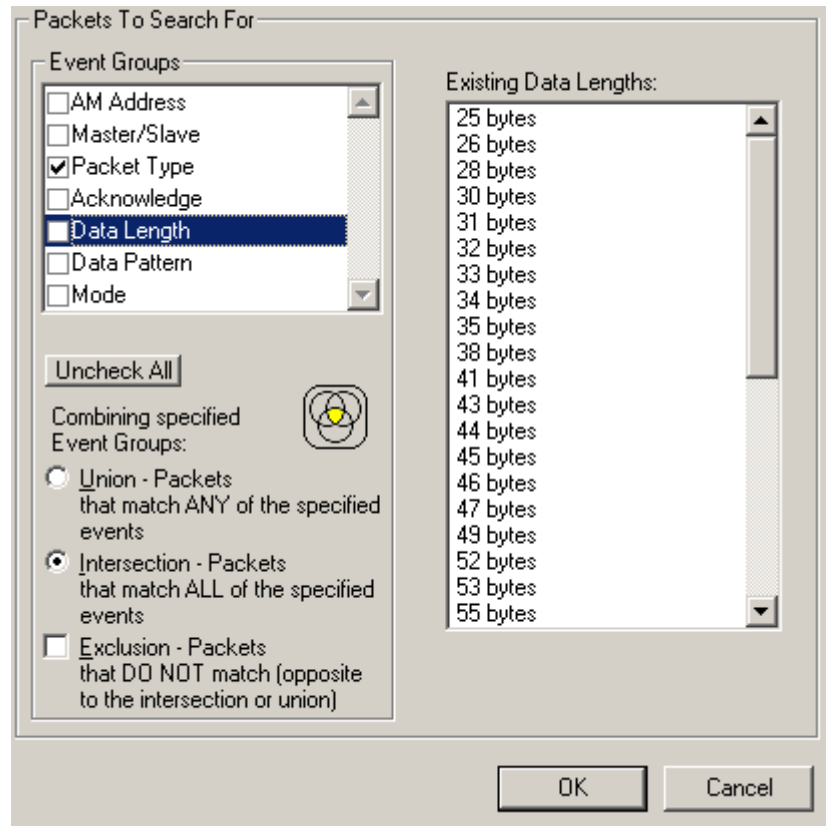
Packet	T	Freq	BTClock	CA/C	HDR	Addr	DM1	L_CH	L2FL	Len	Data	CRC	Ack'd	Idle
14577	M	2444	5949588		0x1	0x3	UA/UI	1	12	0000: 08 00 01 00 02 24 04 00	0xF963	Imp Nak	303.600	
0008: 05 00 40 00														
Packet	Hop Freq	Idle	Time Stamp											
14578	2459	625.000 μs	00009.195 8818											
Packet	Hop Freq	Idle	Time Stamp											
14579	2446	15.400 μs	00009.196 3068											
Packet	T	Freq	BTClock	CA/C	HDR	Addr	DM1	L_CH	L2FL	Len	Data	CRC	Ack'd	Idle
14580	M	2446	5949592		0x1	0x3	UA/UI	1	12	0000: 08 00 01 00 02 24 04 00	0xF963	Yes	303.700 μs	
0008: 05 00 40 00														
Packet	Hop Freq	Idle	Time Stamp											
14581	2480	14.800 μs	00009.196 9319											
Packet	T	Freq	BTClock	CA/C	HDR	Addr	NULL	Flow	Arqn	Seqn	HEC	Idle	Time Stamp	
14582	S	2480	5949594		0x1	0x0		1	1	1	0x7A	484.200 μs	00009.196 9467	

**Implicit NAK** - Packet 14577 is a data packet sent by the piconet Master device. Packet 14579 should have been a data packet with an acknowledgment. Instead, it is an empty packet. This Master interprets this empty packet as an **Implicit NAK** (i.e., implicitly not acknowledged). Merlin summarizes this packet exchange by adding an **Ack'd** field to the Master's data packet and setting the **Ack'd** field to **Imp Nak**.

**ACK** - Packet 14580 is the Master's retransmission of the data sent in packet 14577. Packet 14582 is the reply by the Slave device. This reply contains an ARQN field with a value of (= Acknowledge). Merlin summarizes this packet exchange by setting the **Ack'd** field on packet 14580 to **Ack**.

### *Data Length*

Contains a list of all data lengths that occur in the trace.



### Data Pattern

Searches for the next packet that has a specified data pattern.

Packets To Search For

Event Groups

- AM Address
- Master/Slave
- Packet Type
- Acknowledge
- Data Length
- Data Pattern

Combining specified Event Groups:

- Union - Packets that match ANY of the specified events
- Intersection - Packets that match ALL of the specified events
- Exclusion - Packets that DO NOT match (opposite to the intersection or union)

	Bitmask	Mask (hex)	Match (hex)
0	XXXXXXXXXX	00	00
1	XXXXXXXXXX	00	00
2	XXXXXXXXXX	00	00
3	XXXXXXXXXX	00	00
4	XXXXXXXXXX	00	00
5	XXXXXXXXXX	00	00
6	XXXXXXXXXX	00	00
7	XXXXXXXXXX	00	00
8	XXXXXXXXXX	00	00
9	XXXXXXXXXX	00	00
10	XXXXXXXXXX	00	00
11	XXXXXXXXXX	00	00
12	XXXXXXXXXX	00	00
13	XXXXXXXXXX	00	00
14	XXXXXXXXXX	00	00
15	XXXXXXXXXX	00	00

### Searching for Bit Patterns

You search for a bit pattern by using the box labeled **Bitmask**. Enter one of the three following values:

- X = 'Don't care,'
- 0 = 'Match a 0',
- 1 = 'Match a 1.'

Example -- xxxxxx01 means 'Look for a data pattern where the first 6 bits can be any value but the last two bits must be 01.'

### Searching for Long Patterns

You can search for long pattern sequences by entering patterns into multiple rows within the editor. Entering a pattern on one row and skipping several rows before entering the second pattern tells Merlin to search for the entire pattern between the two specified rows.

Example - Enter xxxxxx01 in row 1 and 11xxxxxx in row 2. This pattern means 'Look for the pattern xxxxxx0111xxxxxx.'

Example - If you enter `xxxxxx01` into row 0 and `11xxxxxx` into row 4, it means 'Look for the pattern `xxxxxx01 xxxxxxxx xxxxxxxx xxxxxxxx 11xxxxxx`.'

	Bitmask	Mask (hex)	Match (hex)
0	XXXXXX01	03	01
1	XXXXXXXX	00	00
2	XXXXXXXX	00	00
3	XXXXXXXX	00	00
4	1XXXXXX	C0	C0

### Searching for Hexadecimal Patterns

The columns marked Match and Mask allow you to specify a pattern in hex. You enter the pattern you want to match in the column marked Match, and enter the mask in the column marked Mask. The Mask column allows you to specify which bits you are searching for.

	Bitmask	Mask (hex)	Match (hex)
0	XXXX0011	0F	03

Example - A Match of `03` and a Mask of `'0F'` tells Merlin that you are looking for the hex pattern of `03` occurring in the last four bits of the pattern. If you enter these values in the Match and Mask columns, the Bitmask section will automatically display the equivalent bit values: `XXXX0011`.

### Union, Intersection, and Exclusion

If you select multiple events, you will need to use the options Union or Intersection to conduct the search.

**Union** is used to search for any selected event: "Find x or y." Union lets you tell the analyzer to search the trace for any of any of the selected items.

**Intersection** is used to search for all selected events: "Find x and y." Intersection lets you tell the analyzer to search the trace for any packet having all of the selected events.

**Exclusion** is used to exclude selected traffic from the trace. Exclusion is used with Union and Intersection --i.e., you select Exclusion with Union or Intersection.

- **Exclusion + Union** -- tells Merlin to exclude packets with any of the specified events.
- **Exclusion + Intersection** -- tells Merlin to exclude packets with all of the specified events.

### Using Find

**Step 1** Select the display level to be searched from the **Search For** box on the left side of the window.

For example, to search through L2CAP messages, select L2CAP. The display level that you select will affect options presented in the Events Group box.



**Step 2** Select a search direction and origin.

**Step 3** Select one or more events from the **Events Group** box.

Your choices will affect options presented in the box on the right side of the screen.

**Step 4** If you have selected two or more criteria, then select either :

- **Union:** Find all packets that match ANY of the specified events. An



example would be to find packets with either X or Y.

- **Intersection:** Find all packets that match ALL of the specified events. An example would be to find all packets with X and Y.



If you want to selected events from the trace, then select:

- **Exclusion:** Exclude all packets that match any of the specified events. This option works in conjunction with Union and Intersection. Select an exclusion plus one of the other two options. If you select Exclusion and Union, it means Exclude packets in any of the following events. An example would be to exclude packets with either X or Y.



**Step 5** Click **OK**.

The search will then occur. Afterwards, the packets meeting the search criteria will display.

### *Some Find Examples*

*Search for all DM1 and Poll packets with an Active Member Address of 7.*

**Step 1** From the Event Group, select **Packet Types**.

**Step 2** From the box on the right, select **DM1** and **Poll**.

**Step 3** From the Event Group, select **Header AM\_Addr**.

**Step 4** From the box on the right, select **AM\_Addr=7**.

**Step 5** From the Center area, select **Intersection**.

Selecting Intersection tells Merlin to find packets with ALL of the selected traits.

**Step 6** Press **OK**.

The trace should reposition to the first DM1 or Poll packet that has an Active Member address of 7.

*Exclude all DM1 and Poll Packets with Active Member Addresses of 7.*

**Step 1** Select **Packet Types** from the From the Event Group

**Step 2** Select **DM1** and **Poll** from the box on the right.

**Step 3** Select **Header AM\_Addr** from the Event Group.

**Step 4** Select **AM\_Addr=7** from the box on the right.

**Step 5** From the Center area, select **Intersection and Exclusion**

**Step 6** Press **OK**.

The trace will redisplay so that it excludes *DM1 packets with AM\_Addr=7* and *Poll packets with AM\_Addr=7*.

*Exclude all packets with ANY of the following attributes: DM1, Poll, or AM\_Addr=7.*

**Step 1** Select **Packet Types** from the Event Groups.

**Step 2** Select DM1 and Poll from the box on the right.

**Step 3** Select **Header AM\_Addr** from Event Group.

**Step 4** Select **AM\_Addr=7** from the box on the right

**Step 5** Select **Union and Exclusion**.

Selecting Union causes the analyzer to search for any of the selected events.

**Step 6** Press **OK**.


The trace will redisplay so that it excludes *DM1s, Polls, or any packet with AM\_Addr=7*.

## Find Next

To apply the previous **Find** parameters to the next search,

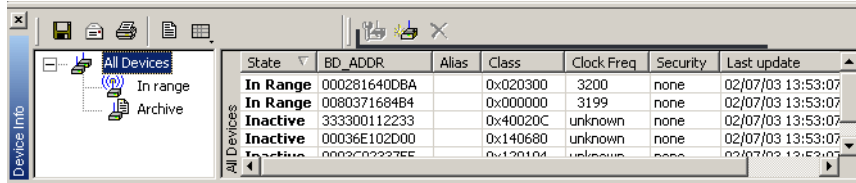
- Select **Find Next** under **Search** on the Menu Bar

OR

Click  on the Tool Bar.

## 10.2 Device List

Device List describes devices discovered in a previous inquiry or was entered by the user. The list is stored in a file from one session to the next, so the information on a device that was collected in previous sessions or was manually entered can always be viewed.



State	BD_ADDR	Alias	Class	Clock Freq	Security	Last update
In Range	000281640DBA		0x020300	3200	none	02/07/03 13:53:07
In Range	0080371684B4		0x000000	3199	none	02/07/03 13:53:07
Inactive	333300112233		0x40020C	unknown	none	02/07/03 13:53:07
Inactive	00036E102D00		0x140680	unknown	none	02/07/03 13:53:07
Inactive	0003C02222FE		0x120104	unknown	none	02/07/03 13:53:07

By default, Device List appears at the bottom of the Merlin application window. If it is not open, you can open it by selecting **View > Device List**.

### Fields in the Device List

- **State** -- Device State
- **BD\_ADDR** -- Bluetooth Device Address
- **Alias** -- Whatever alias you entered for the device in the Add New Device dialog
- **Class** -- The device class for each listed device
- **Clock Freq** -- Shows the device's Clock Frequency
- **Security** -- If Encryption is enabled, then this field will be marked with a "Yes." You enter Encryption by clicking the Add Devices button, and then clicking Options
- **Last Update** -- Shows when device information was last updated
- **User Notes** -- User comments. You add notes by clicking Add Devices and entering text into the dialog box

### Buttons



**Edit Device** -- Opens a dialog box for editing the device settings in the Device List.



**Add New Device** -- Opens a dialog box for adding new devices to the list. (You can also enter devices by performing an Inquiry.) This dialog box lets you enter information that will appear in the device list: device names, addresses, aliases, and comments.



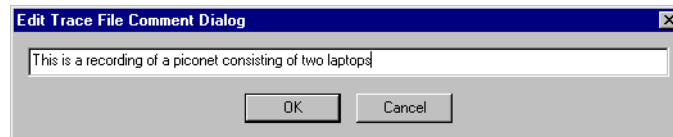
**Remove Device** -- Removes the selected device from the Device List.

## 10.3 Edit Comment

You can create, view, or edit the 100-character comment field associated with each Trace file.

**Step 1** Select **Edit Comment** under **File** on the Menu Bar.

You see the **Edit comment for trace file** window:



**Step 2** Create, view, or edit the comment.

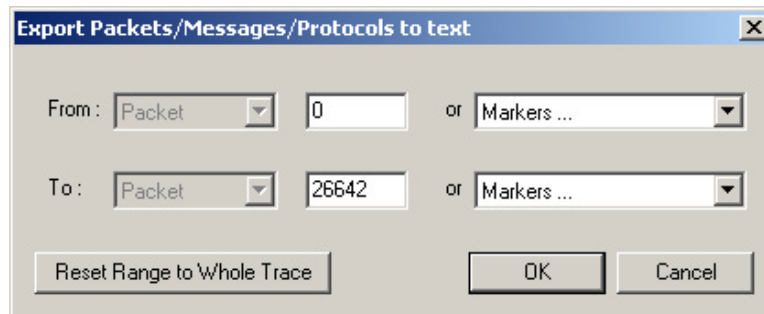
**Step 3** Click **OK**.

## 10.4 Exporting Data

The Export command under the File menu allows you to export trace data for use in a spreadsheet, text editor or other utility. The Export command supports three formats:

### **Export »Packets toText (Packet View Format)**

Saves all or part of a trace to a text file. Selecting this option opens a dialog box that prompts you for a range. Enter the range, then click **OK**. The data is then exported to a text file.

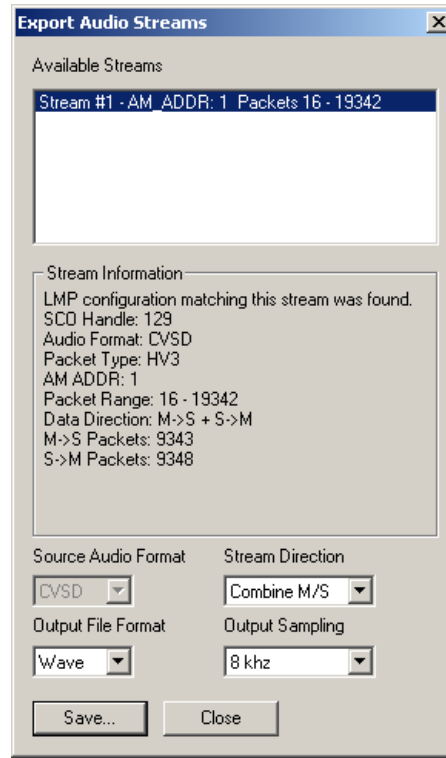


### **Export »Packets to CSV Text**

Saves all or part of a trace to a Comma Separated Values (CSV) file suitable for viewing in a spreadsheet application. The steps are the same as those described above.

### Export>>Audio Streams

Saves audio data into a file.  
Opens a dialog box with options for setting the Audio Source format, Output File format, Stream Direction, and Output Sampling.




## 10.5 File Information

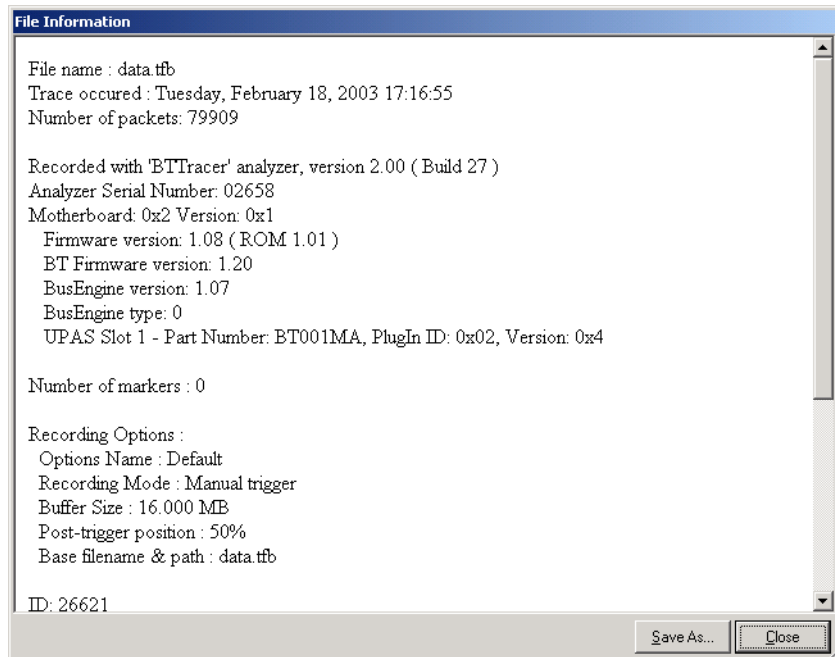
To display a File Information report,

- Select **File Information** under **Report** in the Menu Bar

OR

Click  in the Tool Bar.

You see the File Information screen:



The File Information report provides valuable information about how the recording was made, what the buffer settings were, what the trigger options were, and what version of all the analyzer hardware was used to make the recording.

## 10.6 Error Summary

The Error Summary command opens the **Traffic Summary** dialog box and displays an error summary of the current trace file. The dialog box allows you to go to a specific packet, and save the error file to a uniquely named file. See the discussion below on **Traffic Summary** for more information.


## 10.7 Timing Calculations

Starts the modeless calculator dialog for calculating various timing and bandwidth parameters in the recording file.

To display a File Information report,

- Select **Timing Calculations** under **Report** in the Menu Bar

OR

Click  in the Tool Bar.

You see the Timing and Bus Usage Calculator screen:

The screenshot shows the 'Timing Calculator' dialog box. It has a title bar with 'Timing Calculator' and standard window controls. The main area is divided into several sections. At the top, there are two rows of controls for selecting the start and end points of the calculation. Each row starts with 'From beginning of:' or 'To beginning of:', followed by a 'Packet' dropdown menu, a text box containing the number '0', and the word 'or', followed by another 'Packet # 0 (Trigger)' dropdown menu. Below this, there is a 'Total Time:' label and a dropdown menu currently set to 'nanoseconds'. A section titled 'Air traffic calculations' contains an 'AM Address:' label with a dropdown menu set to 'ALL', and labels for 'Throughput:' and 'Bit Error Rate:'. At the bottom of the dialog is a 'Calculate' button.


To calculate bus usage and bit rate errors,

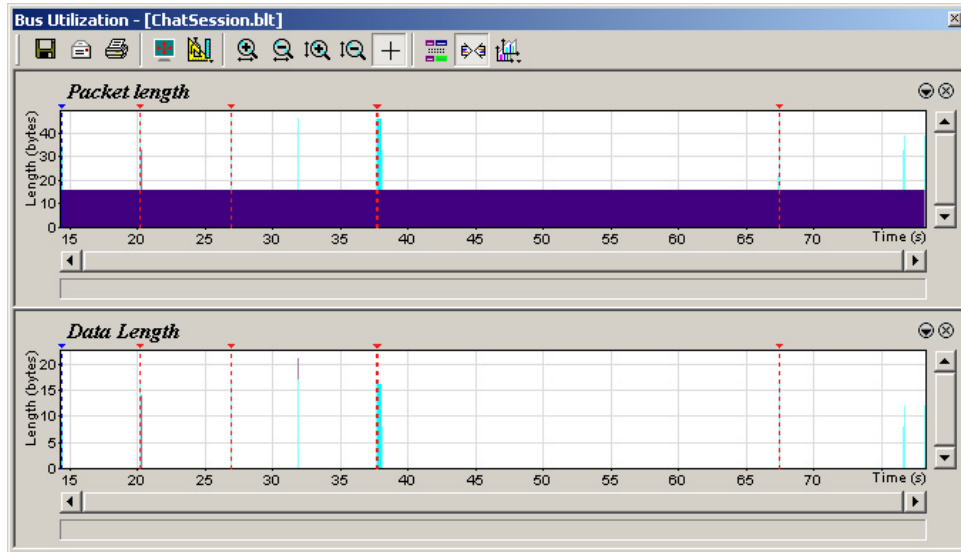
- Step 1** Enter the range of packets to be examined in the text boxes marked "From packet" and "To packet."
- Step 2** If you wish to limit your calculations to a single device, select the device's address from the AM Address drop-down menu.
- Step 3** Click the "Calculate" button.

At this point, bus usage will be calculated.

## 10.8 Bus Utilization

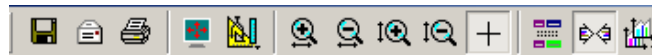
The **Bus Utilization** window displays a graph of bandwidth use within a displayed trace.

To open the Bus Utilization window, select **Report > Bus Utilization** or click the button marked . A window will open with graphs of Link Utilization, Data Throughput, and Packet Counts:













*Bus Utilization Buttons*

The Bus Utilization window has a row of buttons for changing the format of the displayed data and for exporting data:



The buttons have the following functions:

- |   |   |   |   |
|---|---|---|---|
|  | Save As - Saves the graphs as a bitmap file (*.bmp)   |  | Vertical zoom in  |
|  | Email - Creates an email with a *.bmp file attachment of the graphs                                       |  | Vertical zoom out   |
|  | Print   |  | Click and Drag zoom - Click diagonally to select and zoom in on part of the graph   |
|  | Full Screen   |  | Select Range  |
|  | View Settings - opens a sub-menu with options for formatting the display. See "View Settings Menu" below. |  | Sync and Graph areas - If two or more graphs are displayed, this button will synchronize the graphs to one another. Once synchronized, the positioning slider of one graph will move the other graphs |





Horizontal zoom in




Graph Areas - Presents options for displaying additional graphs of data lengths, packet lengths, and percentage of bus utilized.

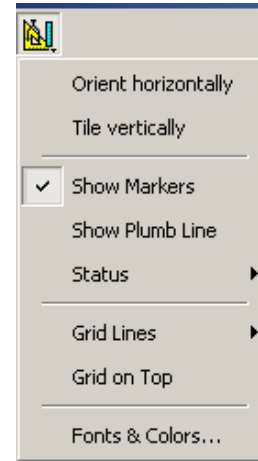


Horizontal zoom out

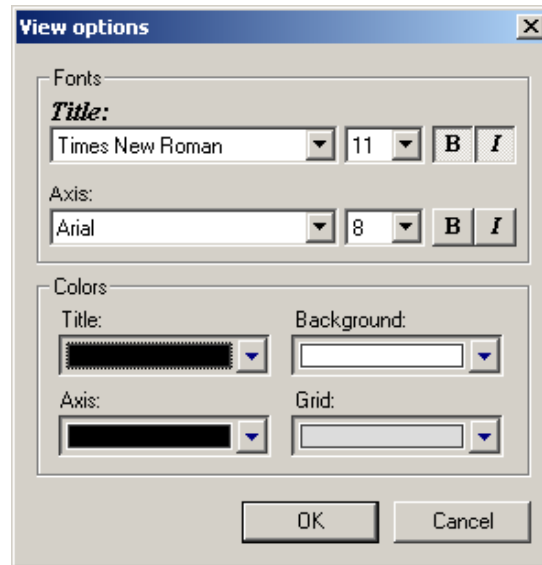
### View Settings Menu

Clicking the View settings button  causes a menu to open with options for formatting the display.

- **Orient Horizontally** - changes the orientation of bus usage to horizontal. After selecting this option, the menu will say "Orient Vertically."
- **Tile Vertically** - tiles the two graphs vertically (i.e., side by side).
- **Show Markers** - Places "tick" marks along the x axis of each graph.
- **Show Plumb Line** - Displays a vertical line that connects your cursor to the horizontal axis. As the mouse is moved, the status bar will show the packet and time frame to which the cursor is pointing.
- **Status** - Opens a sub-menu with the following options:
  - Bar - Displays a status bar at bottom of graph.
  - Tooltip - Causes a tooltip to appear if you position your mouse pointer over part of the graph and leave it there for a couple of seconds.
  - None - Turns off tooltips and the status bar.
- **Grid Lines** - Opens a sub-menu with the following options:
  - Both - Displays both X and Y axis gridlines.
  - X Axis - Displays X axis gridlines.
  - Y Axis - Display Y axis gridlines.
  - None - Turns off gridlines.
- **Grid on Top** - Moves the grid lines above the graph.




- **Fonts and Colors** - Opens a dialog box for setting the colors and fonts used in the graphs:

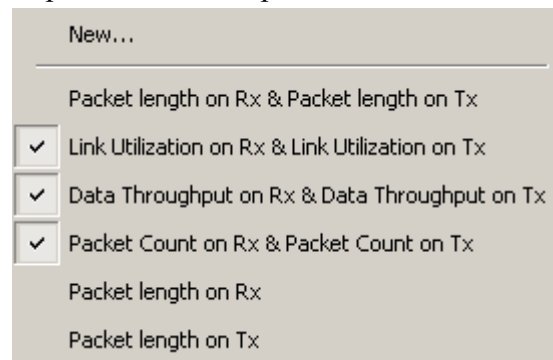


### *Graph Areas Menu*

The Graph Areas menu allows you to view different information in the Bus Utilization window.

Step 1 Click the  button.

*The Graph Areas menu opens.*



Step 2 Select the data you want to appear in the Graph Areas window.

To change the properties in the Bus Utilizations graph, follow these steps:

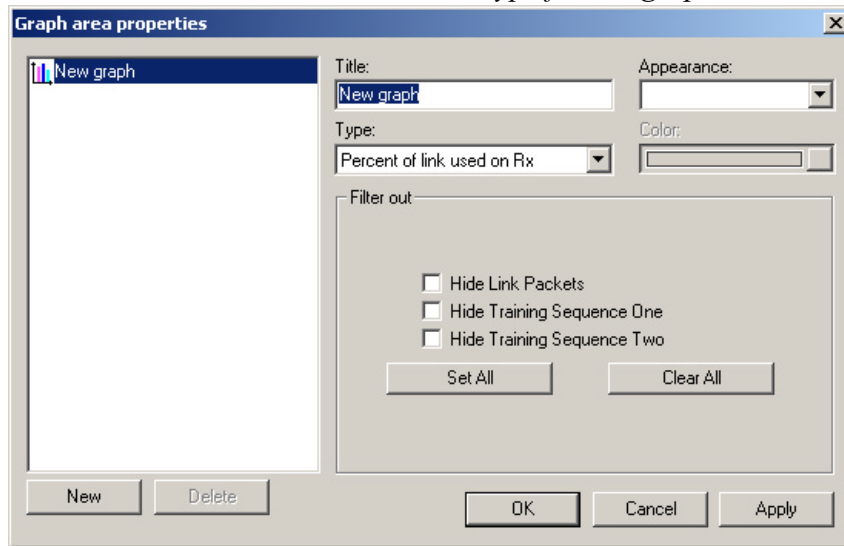
Step 1 In the **Graph Areas** menu, select the type of data to be displayed.

Step 2 Click **OK**.

Or

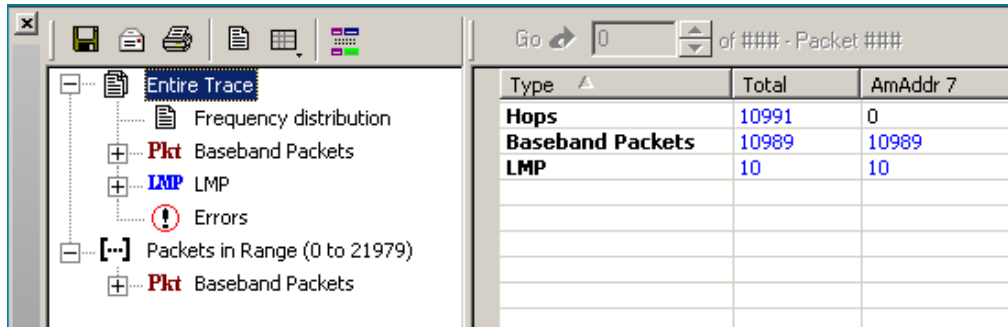
To make a new graph, click **New**.


The following dialog box will open. It will display options for setting the title, data, color, and line type for the graph.



## 10.9 Traffic Summary

The Traffic Summary dialog box displays a text summary of traffic captured in the current trace.



To open the Traffic Summary window, press .

The left pane displays a tree of the different protocol levels. Click the plus symbol (+) to expand the tree. The example above is fully expanded. The right pane displays a summary of the traffic for the selected level.

## 10.10 Encryption

Bluetooth encryption is a multi-staged process that provides devices with secure, encrypted communications. The process begins with a device prompting the user for a Personal Identification Number (PIN). When the

right PIN is entered, the Slave begins an encryption setup dialogue with the Master. At the beginning of this dialogue, the Slave and the Master agree on a *Link Key*. A Link Key is a 128-bit value that the two devices use for authentication. When the Slave and Master agree on a Link Key, the Slave then negotiates for the transfer of the *Encryption Key* from the Master device. The Encryption Key is used to encrypt and decrypt messages. Once the Encryption Key is transferred, both devices use it to encrypt all subsequent communications.

In order for Merlin to decode encrypted traffic, it needs the *Link Key* for each Master-Slave connection for which encryption will be used. If you know the Link Key, you can enter the Key into the Encryption Options dialog box. If you do not know it, you give Merlin the PIN for a device and allow Merlin to discover the Link Key on its own. Once Merlin has the Link Key, it can capture the rest of what it needs by listening to the Master and Slave devices as they negotiate for the Encryption Key.

### Configuring Merlin for Encryption

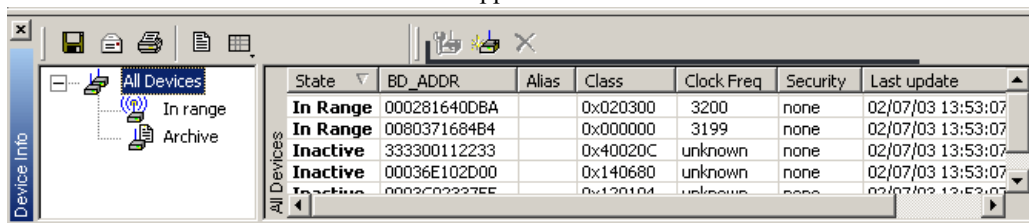
For Merlin to successfully decrypt traffic Merlin needs to be given the PIN or Link Key for each Master-Slave connection before the Link Key is created. If recording is begun prior to the creating the Master-Slave connection, Merlin will be able to obtain the encryption key and decode encrypted traffic.

The following steps show how to configure Merlin for encrypted traffic.

**Note** Be sure to begin the following process *prior* to connecting your Slave device to the Master or Merlin will not be able to capture the Link Key.

#### Step 1 Select **View >Device List**

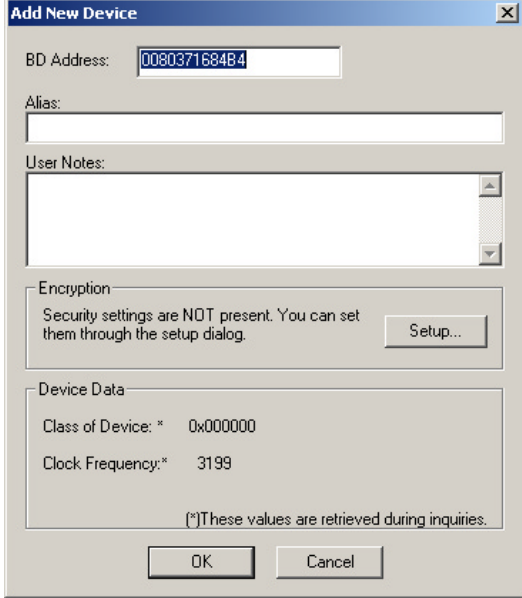
The Device List appears.



**Step 2** Click in the row for the device of interest.

**Step 3** Click the Edit Devices button 

The following dialog box opens.

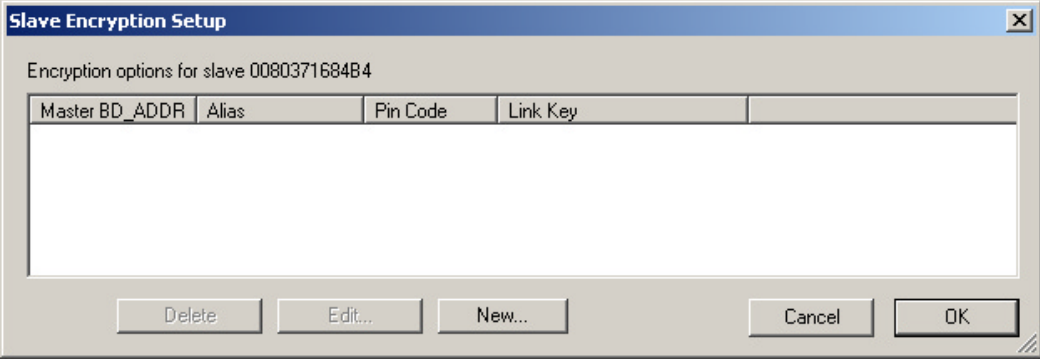


The dialog box titled "Add New Device" contains the following fields and sections:

- BD Address:** A text field containing "0080371684B4".
- Alias:** An empty text field.
- User Notes:** A large empty text area with scrollbars.
- Encryption:** A section with the text "Security settings are NOT present. You can set them through the setup dialog." and a "Setup..." button.
- Device Data:** A section with the following values:
  - Class of Device: \* 0x000000
  - Clock Frequency:\* 3199
- A note at the bottom: "(\*)These values are retrieved during inquiries.
- Buttons: "OK" and "Cancel".

**Step 4** Click the **Setup ...** button.

The following dialog box opens:



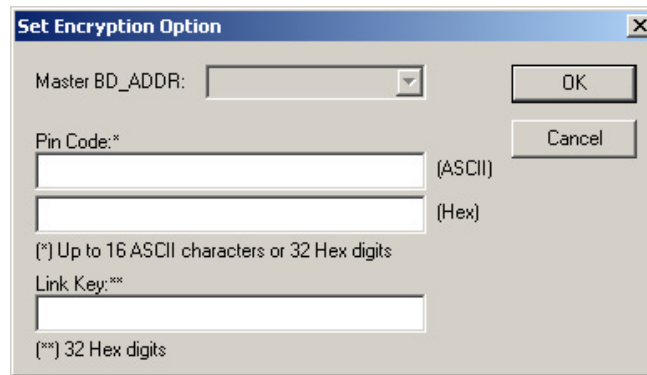
The dialog box titled "Slave Encryption Setup" displays encryption options for slave 0080371684B4. It features a table with the following columns:

Master BD_ADDR	Alias	Pin Code	Link Key

At the bottom of the dialog, there are buttons for "Delete", "Edit...", "New...", "Cancel", and "OK".

**Step 5** Click the button marked **New**.

The following dialog box appears.



The dialog box titled "Set Encryption Option" contains the following fields and controls:

- Master BD\_ADDR: A dropdown menu.
- Pin Code:\* Two text input fields. The first is labeled "(ASCII)" and the second is labeled "(Hex)".
- Link Key:\*\* A text input field.
- Buttons: "OK" and "Cancel" buttons are located on the right side.
- Footnote: "(\*) Up to 16 ASCII characters or 32 Hex digits" is located below the Pin Code fields.
- Footnote: "(\*\*) 32 Hex digits" is located below the Link Key field.

**Step 6** Enter the appropriate Personal Identification Number (PIN) for the selected device to the box marked **PIN Code**. This PIN allows Merlin to learn the Link Key. If you do not have the PIN, skip to Step 5.

**Note** The PIN you provide should be the same used by the Slave. For example, if your Slave device requires a PIN of "1234", then enter the same PIN in the dialog box shown above.

**Step 7** If you do not have the PIN, or if the Master and Slave have already agreed upon the Link Key, manually enter a Link Key as a 128 bit (sixteen byte) hex value into the box marked **Current Link Key**. If you have the PIN, you can skip this step.

**Note** If the Master and Slave were previously connected, they may already agree on the Link Key. In this case, you will need to provide Merlin with the Link Key and not simply the PIN.

**Step 8** Click **OK**

The changes you have made are applied and the information is displayed in the **Slave Encryption Setup** dialog box as shown previously.

**Step 9** Click **OK**.

The **Slave Encryption Setup** dialog box closes. Within the Device List, you should see a "Yes" in the Security field for the selected device.

## How to Contact CATC

Type of Service	Contact
Call for technical support...	US and Canada: 1 (800) 909-2282 Worldwide: 1 (408) 727-6600
Fax your questions...	Worldwide: 1 (408) 727-6622
Write a letter...	Computer Access Technology Corp. Customer Support 2403 Walsh Avenue Santa Clara, CA 95051-1302
Send e-mail...	support@CATC.com
Visit CATC's web site...	<a href="http://www.CATC.com/">http://www.CATC.com/</a>

## Warranty and License

Computer Access Technology Corporation (hereafter CATC) warrants this product to be free from defects in material, content, and workmanship, and agrees to repair or replace any part of the enclosed unit that proves defective under these terms and conditions. Parts and labor are warranted for one year from the date of first purchase.



The CATC software is licensed for use on a single personal computer. The software may be copied for backup purposes only.

This warranty covers all defects in material or workmanship. It does not cover accidents, misuse, neglect, unauthorized product modification, or acts of nature. Except as expressly provided above, CATC makes no warranties or conditions, express, implied, or statutory, including without limitation the implied warranties of merchantability and fitness for a particular purpose.

CATC shall not be liable for damage to other property caused by any defects in this product, damages based upon inconvenience, loss of use of the product, loss of time or data, commercial loss, or any other damages, whether special, incidental, consequential, or otherwise, whether under theory of contract, tort (including negligence), indemnity, product liability, or otherwise. In no event shall CATC's liability exceed the total amount paid to CATC for this product.

CATC reserves the right to revise these specifications without notice or penalty.





## INDEX

### Symbols

### Numerics

1100 packet 90

1101 packet 90

### A

Abort upload 40

Acknowledge 142

Action buttons 36, 97

Actions tab 96

Addr 116

### Addresses

AM\_ADDR 91

Bluetooth 60

slave device 50

target 61

AM Address 142

### Analyzer

describing Bluetooth 2

set up 9

status 40

### API 4

Application installation 11

Architecture of Piconet 3

Arqn 116

ARQN condition 91

AT 124

Authentication 159

Automation Feature 4

AUX1 packet 90

### B

Basic installation 9

Bit pattern, searching 145

Blue dot menus 100

### Bluetooth

BusEngine 6

described 1

device address 60

first recording 18

limited search 83

recording traffic 105

search for device 56

- searching for devices 46
- target address 61
- BNEP 124
- Bubble help 41
- Buffer size 18, 74
- Bus utilization 152
- BusEngine
  - Bluetooth 6
- Buttons
  - bus utilization 153
  - graph area 155
  - toolbar 36
- C
- CAC 116
- Calculations, timing 151
- CATC Technical Support 163
- Certification 7
- Channel connections, L2CAP 127
- Clicked fields, menus in 121
- Clock rate, match 81
- Collapse data 118
- Comments, editing 150
- Components, physical 5
- Configuring encryption 159
- Connecting events 98
- Connectors
  - data 7
  - physical 7
- Correlation Value 82
- Counters
  - connecting events 98
  - value 100
- CRC 116
- CRC error 94
- D
- Data
  - decoding 124
  - expand, collapse 118
  - filename 18
  - length 93
  - pattern 88, 93
  - searching by length 138
  - searching by pattern 145

- transfer message 126
- Debug file 19, 83
- Decoding 124
- Dedicated inquiry 19
- Description of Merlin 2
- Device
  - Bluetooth address 60
  - general search 48
  - search 46
  - search for Bluetooth 56
  - slave address 50
- DH1, 2, 3 packet 90
- Displaying information 115, 150
- DM1 116
- DM1, 2, 3 packet 90
- Duration of search 56
- DUT Recv/Xmit Freq 77
- DV packet 90
- E
- Editing comments 150
- Enable
  - debug file 83
- Encryption 159
- Environmental Conditions 7
- Error summary 151
- Errors
  - CRC 94
  - FEC 94
  - header length 95
  - HEC 94
  - invalid packet 94
  - payload length 95
  - Searching for 140
  - setting conditions for 94
  - sync loss 95
  - threshold exceeded 94
  - types of 88
- Established Piconets 79
- Events
  - conditions 91
  - connecting 98
  - sequencing 103
  - tab 88

- trigger 18, 74
- Exclusion search 146
- Existing Piconet, recording 54
- Expand data 118
- Explicit NACK 142
- External
  - input signals 88, 95
  - trigger form 102
- F
- Features 5
- FEC Error 94
- FHS packet 90
- File information, displaying 150
- File menu 33
- Filename and data 18
- Filter In/Out button 97
- Filter Out/In 100
- Filtering 89, 90
- Find feature, using 146
- Finding 140
- Finding devices 46
- Flow 116
- Fonts 155
- Force resynchronization 81
- Frequencies, DUT 77
- Frequency hops, hiding 120
- G
- General description 2
- General features 5
- General inquiry 19, 80, 83
- General options
  - recording 71
- General purpose output 102
- Go to
  - DataLength 138
  - error 140
  - Header AM\_Addr 138
  - L2Cap CID 140
  - Lmp Opcode 139
  - marker 136
  - packet types 137
  - packet/Message/Protocol 135
- Graphs

- areas menu 155
- bus utilization 153
- buttons 155
- Grid
  - lines 154
  - on Top 154
- Groups, events 88
- H
- HDLC 124
- Headers
  - AM\_Addr 138
  - length error 95
  - packets 90
  - payload 91
- HEC 116
- HEC Error 94
- Help menu 35
- Hexadecimal patterns, searching 145
- HID 124
- Hiding 120, 121
- Higher protocols, decoding 123
- High-pulse output 102
- Hops
  - hiding 120
  - reduced mode 64
  - sequence 19
- Hot keys 41
- Humidity 7
- HV1, 2, 3 packet 90
- I
- Idle 116
- Implicit NACK 142
- Information, interpreting 115
- Input signals 88, 95
- Inquiry
  - dedicated 19
  - general 83
  - perform/skip 45
  - recording 19
  - timeout 19, 82
- Installation
  - basic 9
- Interpreting a trace 115

- Intersection search 146
- Introduction 1
- Invalid packet type error 94
- K
- Keyboard shortcuts 41
- L
- L\_CH (Logical Channel) 92, 116
- L2CAP
  - channel connections 127
  - CID, searching 140
  - described 124
  - messages 121, 123, 126
- L2FL 116
- Len 116
- Length of data 93
- License 163
- Limited inquiry 19
- Linking events 98
- LMP
  - described 124
  - messages 123, 126
  - Opcode 139
- Logical Channel 92
- Long pattern, searching 145
- Loss of sync
  - searching for 140
  - timeout 82
- Low-pulse output 102
- M
- Manual trigger 7, 18, 74
- Markers
  - editing and clearing 117
  - searching 136
  - setting 116
- Master
  - and slave 142
  - switch 81
- Master/address 60
- Match clock rate 81
- Memory, Recording 7
- Menus
  - blue dots in events 100
  - clicked fields 121

- pulldown 33
  - view settings 154
- Merlin
  - configure encryption 159
  - description of 2
- Message
  - searching 135
- Messages
  - LMP, L2CAP 123, 126
  - transfer 126
- Modes
  - test, recording in 64
- N
- NULL packet 90
- Nulls, hiding 120
- O
- OBEX 124
- Opcode 116
- Operating temperature 7
- Options
  - general recording 71
  - name 18
  - search 62
- Orient horizontally 154
- Output signals, enabling 102
- Overview 1, 33
- P
- Package dimensions 7
- Packets
  - 1100, 1101 90
  - AUX1 90
  - DM1, 2, 3 90
  - DV 90
  - FHS 90
  - headers 88, 90
  - headers in 90
  - hiding 112
  - HV1, 2, 3 90
  - invalid type error 94
  - NULL 90
  - POLL 90
  - searching 135, 137
  - types 90, 142

- viewing 126
- Page
  - sync and record 88
- Paging traffic 82
- Passive sync and record 78
- Patterns, data 93
- Payload
  - headers 88, 91
  - length error 95
- Percentage of triggering 75
- Phone numbers, Technical Support 163
- Physical Components 5
- Piconet
  - established devices 79
  - master address 60
  - private device 79
  - recording 19, 50, 54
  - recording traffic on 44
  - sample 3
  - search options 62
  - slave address 50
  - sync and record 79
  - synchronizing 50
  - target address 61
  - Wizard 51
- PIN 159
- Pkt 124
- Polls
  - hiding 120
  - POLL packet 90
- Position of trigger 75
- Post triggering, percentage 75
- Power
  - LED 7
  - Switch 7
- PPP 124
- Pre-triggering 75
- Private Device Piconets 79
- Program
  - installation 11
- Progress indicator, recording 38
- Protocol
  - Analyzer 2



- Architecture 3
  - decoding 124
  - searching 135
- Pull-down menus 33
- Pulse low signal 102
- Pulse toggle signal 102
- R
- Reading a trace 115
- Record inquiry 83
- Record menu 33
- Recording
  - Bluetooth traffic 18, 105
  - existing Piconet 54
  - LED 7
  - memory 7
  - mode 19
  - Piconet 50
  - progress indicator 38
  - reduced hop mode 64
  - session 21
  - type 73
- Recording Options
  - events 88
  - general 18, 71, 73
  - in Wizard 51
  - saving 104
- Recording type 54
- Recv, DUT freq 77
- Reduced hops 64
- Reports
  - menu 33
- Restart button 98
- Resynchronization, forced 81
- RFCOMM 124
- S
- Sample
  - Piconet 3
  - recording 21
- Saving
  - recording options 104
- SDP Msg 124
- Search 48
  - duration of 56

- general 58
- Search menu 33
- Search options 62
- Search type 46, 56
- Searching
  - by data pattern 145
  - complex 140
  - data length 138
  - for bit pattern 145
  - for bit patterns 145
  - for errors 140
  - Header AM\_Addr 138
  - L2Cap CID 140
  - Lmp Opcode 139
  - packet types 137
  - recorded traffic 135
- Security 159
- SEQN condition 91
- Sequence
  - event 103
- Set marker 116
- Setup
  - menu 33
- Shortcuts, keyboard 41
- Show markers 154
- Show plumb Line 154
- Signalling
  - message 126
- Signals
  - input 88, 95
  - outputs, enabling 102
- Size of buffer 74
- Slave device, address 50
- Slave switch 81
- Snapshot 18, 74
- Soft Bit Error, searching 140
- Software
  - installation 11
  - overview 33
- Special Interest Groups (SIGs) 1
- Specifications 7
- Status
  - status bar 154

- Status bar 38
- Status of Analyzer 40
- Storage temperature 7
- Summary
  - error 151
  - traffic 156
- Support, technical 163
- Switches 7, 81
- Sync
  - and record 78
  - loss error 95
  - loss of, searching 140
  - timeout, loss of 82
  - window 82
- Synchronization, forced 81
- Synchronize Piconet 50
- Synchronized LED 7
- T
- Tabs
  - recording events 88
  - recording, general 18, 72
  - recording, modes 19
  - recording, options 71
- Technical Support 163
- Temperature tolerances 7
- Test debug 83
- Test mode, recording in 64
- Threshold Exceeded error 94
- TID 116
- Tile vertically 154
- Time Stamp 116
- Timeout
  - inquiry 82
  - loss of sync 82
- Timeslot filtering 89
- Timing calculations 151
- Tips, tool 41
- Toggle signal 102
- Toolbar 36
- Tooltips 41, 116, 126
- Trace
  - filename 18
  - reading 115

- sample 21
- Traffic
  - Bluetooth 105
  - generation 6
  - hiding 121
  - on Piconet 54
  - paging 82
  - recording 62
  - recording on piconet 44
  - searching 135
  - summary 156
- Trail 116
- Transfer message, data 126
- Trigger
  - event 74
  - external form 102
  - LED 7
  - position 18, 75
  - post triggering 75
  - recording, manual 74
- Type of recording 73
- U
- Unassociated traffic, hide 121
- Union search 146
- V
- Values, changing counters 100
- View
  - menu 33
  - options 36
  - packets 126
  - settings menu 154
- W
- Warranty 163
- Weight 7
- Window menu 35
- Wizard
  - Piconet 51
- X
- Xmit, IUT freq 77
- Z
- Zoom 41