Computer Access Technology Corporation

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

CATC BT*Tracer*™

Bluetooth™ Protocol Analyzer

User's Manual

For Software Version 1.0

Manual Version 1.0

8 February, 2002

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

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

All other trademarks are property of their respective companies.

Copyright

Copyright © 2002, Computer Access Technology Corporation (CATC); All Rights Reserved.

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

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.

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).

Manual Version 1.8 Part number: 730-0017-00

TABLE OF CONTENTS

Chapter 1 Overview 1
Bluetooth™ Overview 1
General Description 2
Automation 4
Features 4
General 4
Physical Components 5
Display Options 5
Recording Options 5
Traffic Generation 5
Bluetooth™ BusEngine 6
Specifications 7
Package 7
Power Requirements 7
Environmental Conditions 7
Switches 7
LEDs 7
Recording Memory Size 7
Certification 7

Chapter 2 Quick Installation 9
Setting Up the Analyzer 9
Installing the Software 9
Your First Bluetooth™ Recording 10

Chapter 3 Detailed Installation 13
System Components/Packing List 13
The Installed Merlin Unit 13
Merlin System Setup 14
AC Power Source 14
External Interface Breakout Board 15
Breakout Board External Output Signalling Pins 16
Prototype Rework Area 17
PC Connection 17
Antenna Information 17
Analyzer PC Requirements 17
Merlin Program Installation 18
Loading the Merlin USB Drivers 18
Installing the Merlin Application Program 18
Merlin Program Startup 19
Making a Recording 20

Chapter 4 Updates 21
Software, Firmware, and BusEngine Revisions 21
Software Updates 22

Software License Updates 22
Viewing licensing information 23
BusEngine and Firmware UpdateUpdates 23
Automatic Updates 24
Manual Updates to BusEngine and Firmware 25
Updating the BusEngine 26
Updating the Firmware 27

Chapter 5 Software Overview 29

The Main Display Windows. 29
View Options 31
Tool Bar. 31
Status Bar 33
Recording Progress 33
Recording Status 34
Analyzer Status 34
Search Status 35
Zoom In. 35
Zoom Out 35
Tool Tips. 35
Merlin Analyzer Keyboard Shortcuts 36

Chapter 6 Recording Wizard 37

Starting Recording Wizard 37
Recording a Traffic on a New Piconet 38
Recording an Existing Piconet 49
Recording in Test Mode 58
Recording in Reduced Hopping Mode 58
Recording in Single Frequency Mode 62

Chapter 7 Recording Options 63

Opening the Recording Options Dialog Box 63
Recording Options - General 64
Recording type 64
Options 65
Buffer Size 65
Trigger Position. 65
Recording Options - Modes 66
Recording Mode 67
Inquiry Recording 67
Piconet Recording 68
Hop Sequence 68
Sync Methods 69
Force Re-synchronization 72
Follow Master/Slave Switch 73
Match Clock Rate 73
Show Paging Traffic 73

Piconet Addresses (MSB -> LSB) 73
Other Parameters. 74
Debug/Test 75
Recording Options - Events 75
Events Options 75
Payload Length Error. 81
Recording Options - Actions 82
Actions Window Layout 82
Action Buttons - Their Functions 83
Counting Buttons - Their Functions 83
Blue Dot Menus 85
Saving Recording Options 91
Recording Bluetooth Traffic 92

Chapter 8 Display Options 95

General Display Options 95
Trace Viewing Level. 96
Creating New Display Options Files 96
Color Display Options 97
Formats Display Options 99
Hiding. 100
Saving Display Options 101

Chapter 9 Reading a CATC Trace 103

Trace View Features. 103
Interpreting the Displayed Information 103
Tooltips. 104
Set Marker 104
Edit or Clear Marker 105
Expanded and Collapsed Data Formats 106
Hide Frequency Hops. 107
Hide Nulls and Polls. 108
Menus in Clicked Fields. 108
Hide Unassociated Traffic 108

Chapter 10 Decoding Higher Protocols 109

Introduction 109
LMP and L2CAP Messages. 109
Decoding and Viewing Higher Protocol Data 110
Decoding Via the Decoding Toolbar. 110
Decoding Via the Display Options Dialog Box 111
Tooltips. 112
Viewing Packets in LMP and L2CAP Messages 112
Types of LMP and L2CAP Messages 112
Viewing L2CAP Channel Connections 113
Viewing Protocol Messages and Transactions 114
Viewing L2CAP Messages in Protocol Messages 115

How to Decode 115
Expanding Protocol Messages 115
Changing Protocol Assignments 116
Using the Decoding Assignments Dialog Box 116
Removing User-Assigned Protocol Assignments 117
Manually Assigning Protocols 118
Other Assignments: OBEX Client/Server Status 118
Changing an OBEX Client or Server Status 119
Decoding BNEP 119
Decoding HID 119

Chapter 11 Other Features 121

Search 121
Go to Trigger 121
Go to Packet/Message/Protocol 121
Go to Marker 122
Go to 122
Error 126
Soft Bit Error 126
Loss of Sync 126
Find 126
Event Groups 128
Union, Intersection, and Exclusion 132
Using Find 132
Find Next 134
Edit Comment 135
Reports 135
File Information 135
Error Summary 136
Timing Calculations 136
Traffic Summary 137
BT Neighborhood 139
Encryption 139
Configuring Merlin for Encryption 140

Chapter 12 How to Contact CATC 143

Chapter 13 Warranty and License 143

Index 145

1. Overview

The CATC BTTracer™ Protocol Analyzer is a member in CATC's industry-leading line of high performance, serial bus protocol analyzers. Preceded by CATC's USB Chief™ and IEEE 1394 FireInspector™ Analyzers, BTTracer 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 BTTracer 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. BTTracer 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.

BTTracer 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.

BTTracer 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 BTTracer Protocol Analyzer functions with any personal computer using the Windows 98, 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 BTTracer Protocol Analyzer

BTTracer 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, BTTracer 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 BTTracer to transmit externally two control, timing, or recovered signals for purposes of probing and use by other circuitry.

The BTTracer 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 BTTracer 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 BTTracer 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 BTTracer or remotely over a network connection.

For further details, download the **BTTracer Automation Application Programming Interface User's Manual** from the CATC website:

http://www.catc.com/support.html

1.4 Features

General

- Flexible design - reconfigurable hardware for future enhancements.
- User friendly - the Graphical User Interface software of BTTracer Analyzer is designed to be consistent with the 'CATC Trace' using color and graphics to display Bluetooth™ traffic.
- Radio Level Point of Observation and Capture - traffic capture at the Radio Level for comprehensive analysis.
- Complies with Bluetooth™ v1.1 specification.
- Supports point-to-point and point-to-multipoint Bluetooth™ piconets.
- Supports both 79 frequency hop and 23 frequency hop standards.
- Automatic tracking of changes in the hopping scheme.

- Automatic tracking of whitened and non-whitened packets and traffic.
- 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 all of the above plus Windows 95.
- Recording memory of 128MB - enough to record twenty five minutes of high volume traffic.

Display Options

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

Recording Options

- Flexible advanced triggering capabilities including - multiple triggering modes, selective views, timing analysis, search functions, protocol packet errors, transaction errors, packet type and destination device, data patterns, or any of these trigger types in combination.
- User defined trigger position.
- 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 BTTrainer.

Bluetooth™ BusEngine

CATC's BusEngine™ Technology is at the heart of the new BTTracer 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.

1.5 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. Quick Installation

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

2.1 Setting Up the Analyzer

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

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

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

Step 4 Insert the BTTracer CD into the CD ROM drive of the PC that will be administering the Analyzer. If you prefer to install from diskette, insert the first BTTracer diskette (Disk 1 of 6) into the floppy disk drive.

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

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

2.2 Installing the Software

Step 1 From the setup directory, run **setup**, and follow the on-screen instructions to install the BTTracer application on the analyzing PC hard disk.

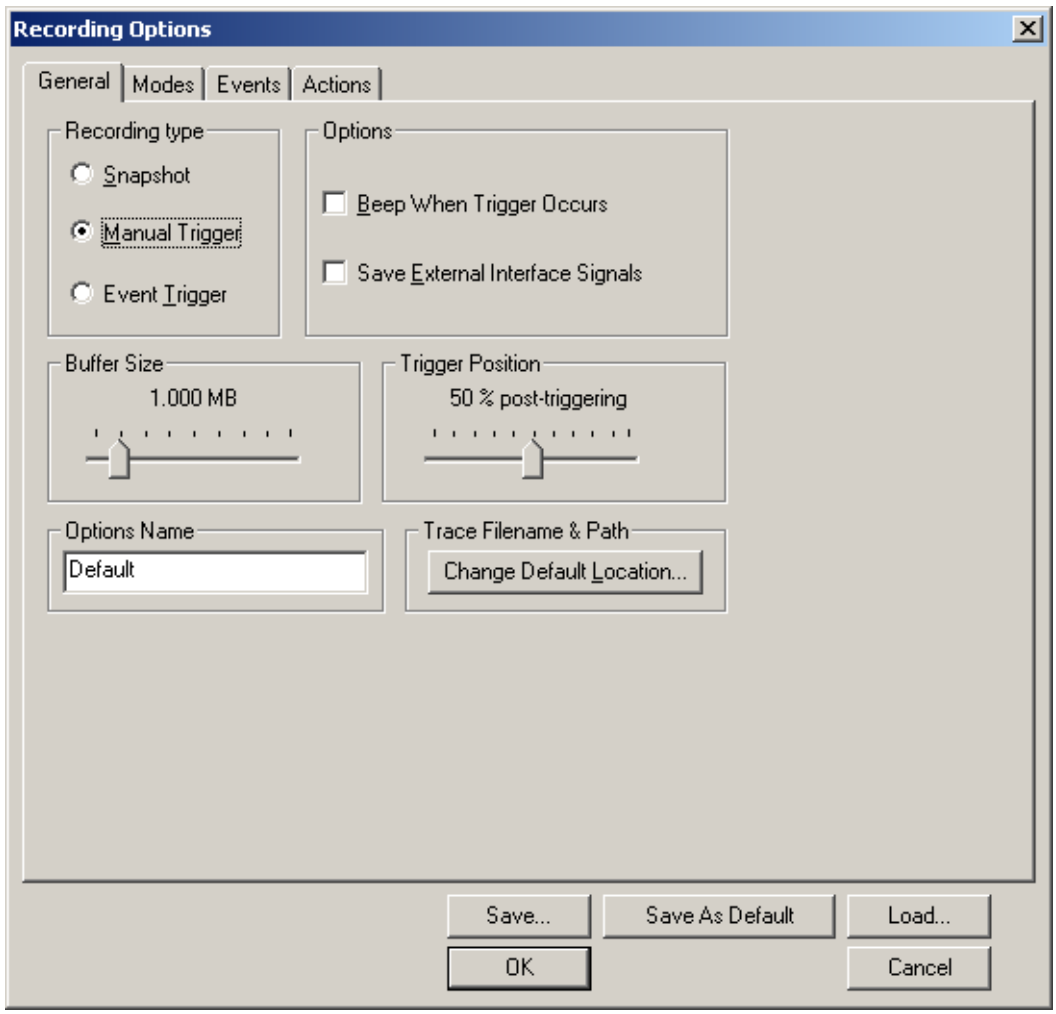
Step 2 To start the application, launch the **CATC BTTracer** program from the **Start Menu: Start>Programs>CATC>BTTracer**.

2.3 Your First Bluetooth™ Recording

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

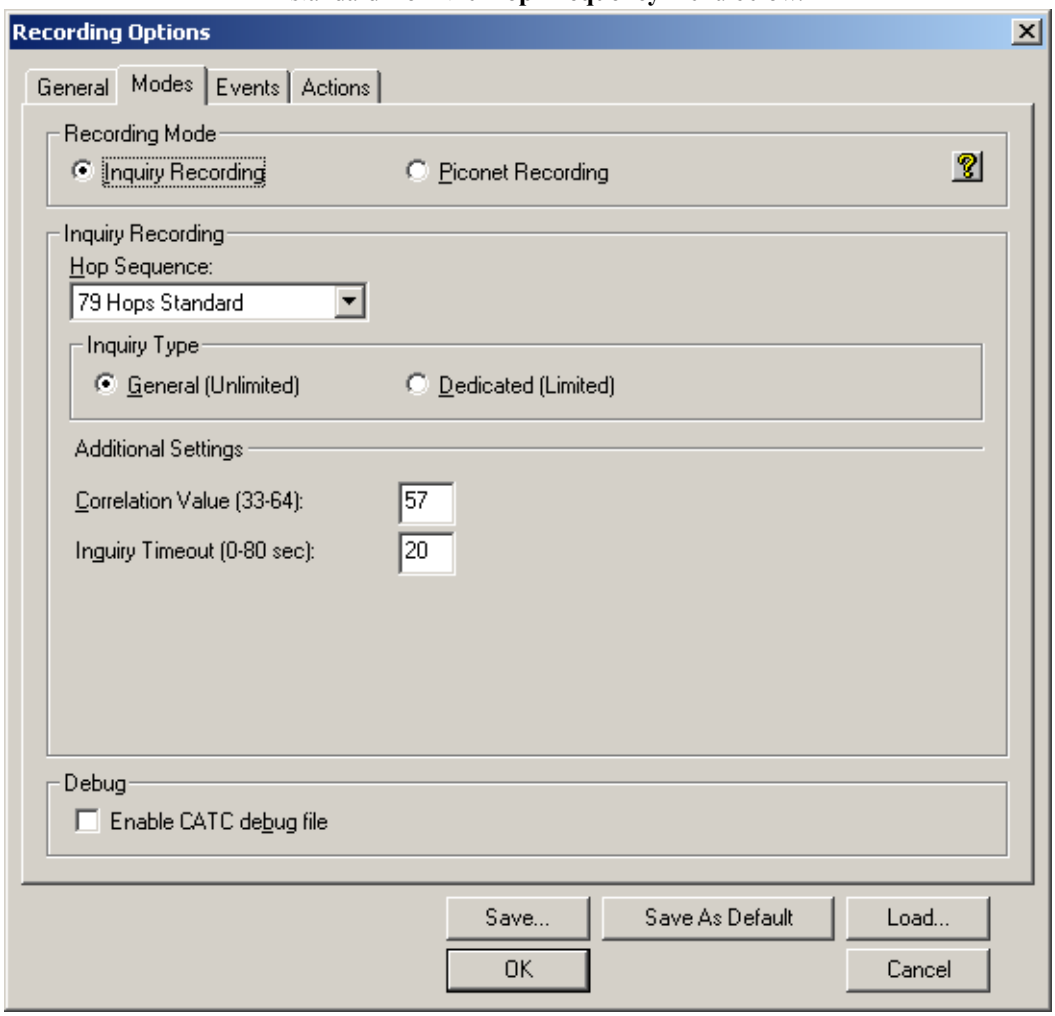
Step 1 Select **Recording Options** under **Setup** on the Menu Bar.

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



Step 2 Select the **Modes** tab.

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



Step 3 Click OK to close the Recording Options window and activate the recording options you selected.

At this point, BTTracer will be ready to record.

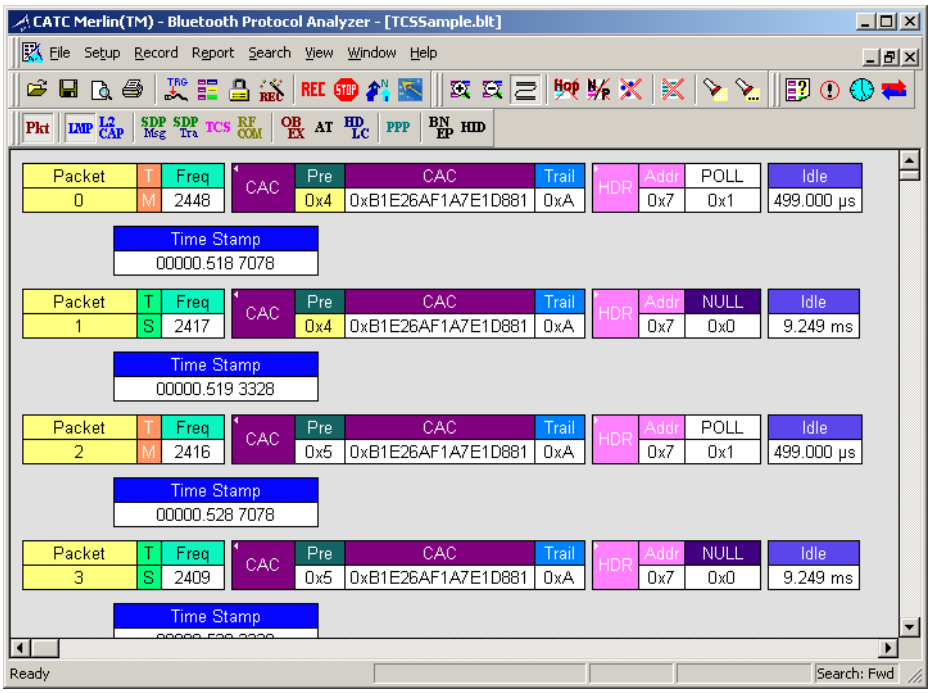
Step 4 Click on the Tool Bar.

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

Step 5 If you wish to terminate the recording before the snapshot

automatically completes, click on the Tool Bar.

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



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

Step 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.

3. Detailed Installation

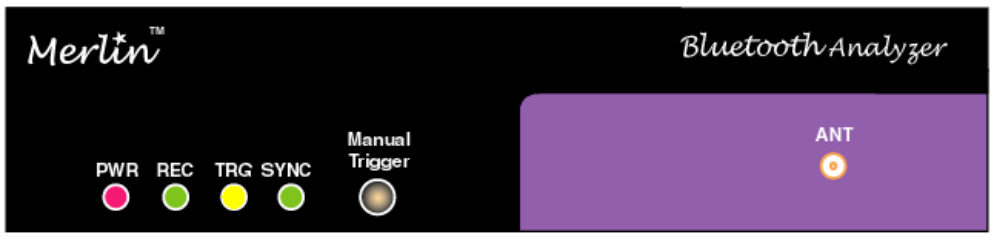
3.1 System Components/Packing List

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

3.2 The Installed BTTracer Unit

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

Figure 1: Front Panel

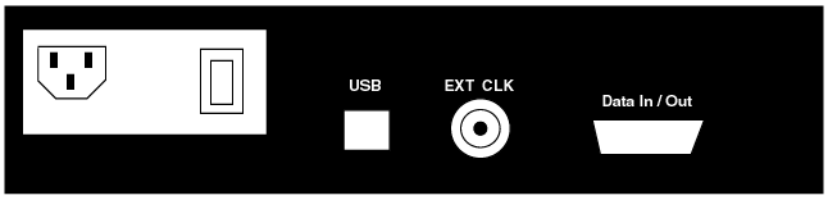


- Red **PWR** (power) indicator LED (lights when the unit power is switched on).
- Green **REC** (recording) LED (lights when the unit is recording).
- Yellow **TRG** (triggered) LED (lights when the unit triggers an event).

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

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

Figure 2: Rear Panel



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

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

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

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

3.3 BTTracer System Setup

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

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

3.4 AC Power Source

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

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

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

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

3.5 External Interface Breakout Board

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

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

Figure 3: Data In/Out Connector

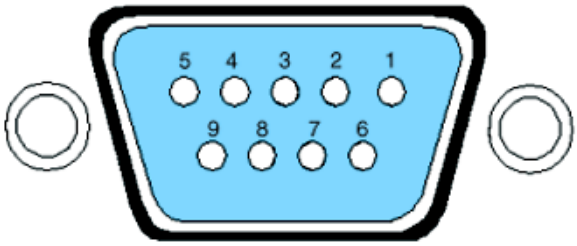


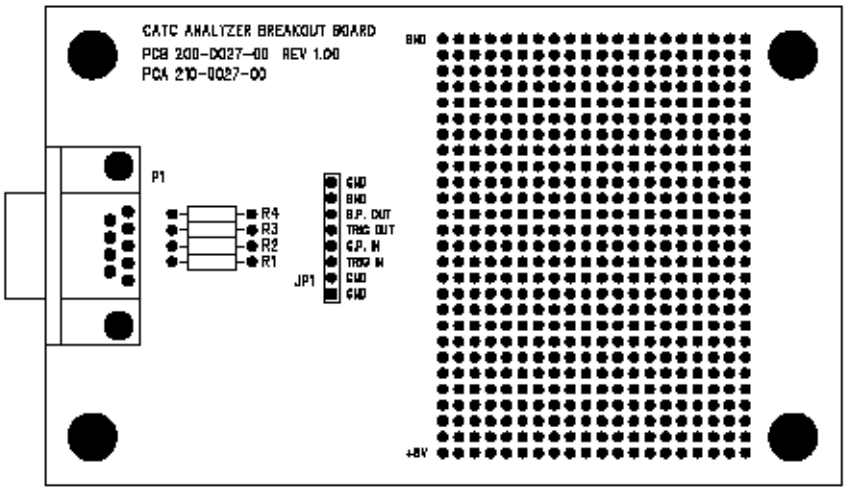
Table 1 lists the pin-out and signal descriptions for the **Data In/Out** connector.

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

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

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

Table 2: External Interface Breakout Board



Breakout Board External Output Signalling Pins

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

TRG OUT

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

G.P. OUT

G.P. OUT needs to be enabled before it will output signalling. See "Blue Dot Menus for the Event Buttons" on page 88 for details on how to enable output signalling.

If enabled, G.P. OUT will provide signalling each time a trigger event is detected by the Analyzer. G.P. OUT's signalling can be set to three different formats - "Pulse High" provides a 16.66 ns (ground to +5V) signal, "Pulse Low" a 16.66 ns (+5 V to ground) signal or "Toggle", a signal with an initial High (+5V) state that alternates with each trigger event between continuous High (+5 V) and continuous Low (Ground). "Pulse High" is the default condition. To change the format, see "Enabling High Pulse, Low Pulse or Pulse Toggle Signal Outputs" on page 88 for details.

Prototype Rework Area

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

3.6 PC Connection

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

3.7 Antenna Information

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

3.8 Analyzer PC Requirements

For an updated description of requirements, please refer to the readme file.

Note If installing BTTracer software on a Windows NT 4.0 system, you will need a separate set of diskettes, which is available from CATC.

3.9 BTTracer Program Installation

The CATC BTTracer software is provided on a CD and also on six 3½ inch diskettes. The software is also available on zip files at the CATC web site:

http://www.catc.com/support.html

If you are downloading the files from the CATC web site, you will be retrieving several zipped files. The first of these has an executable called install.exe. Double-click on this file and follow the on-screen instructions.

Installation of the analyzer software requires a Windows 98, Windows 98SE, Windows 2000, Windows ME, or Windows XP operating system. If you are loading BTTracer onto Windows NT 4.0 you will need to get a separate diskette and instructions from CATC.

Loading the BTTracer USB Drivers

Before you can install the BTTracer Windows application, you will need to install BTTracer as a USB device:

Step 1 Insert the BTTracer program CD into the CD ROM drive of the PC that will be administering the Analyzer. If you prefer to install from floppy diskette, install the floppy for your operating system labeled **Disk 1 of 6** into the **a:** drive.

Step 2 Power-on the BTTracer Analyzer.

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

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

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

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

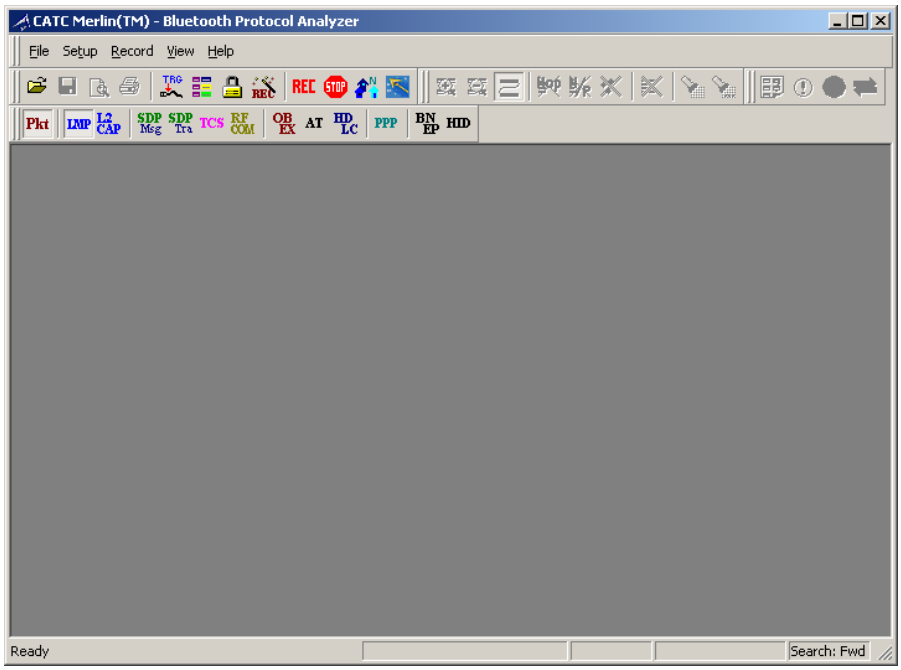
Installing the BTTracer Application Program

Run **Setup.exe** from the BTTracer CD or from the BTTracer floppy disk 1 of 6.

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

3.10 BTTracer Program Startup

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



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

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

3.11 Making a Recording

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

To make your first recording of this traffic,

Step 1 Click REC on the Tool Bar.

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

To terminate the recording before Inquiry timeout occurs,

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

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

To save a current recording for future reference,

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

OR

Click on the Tool Bar.

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

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

4. Updates

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

4.1 Software, Firmware, and BusEngine Revisions

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

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

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

  You see this screen:

About Merlin details revisions of the following software and hardware:

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

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

4.2 Software 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**.

To update the software,

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

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

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

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

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

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

Step 5 Unzip the files into your choice of directory.

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

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

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

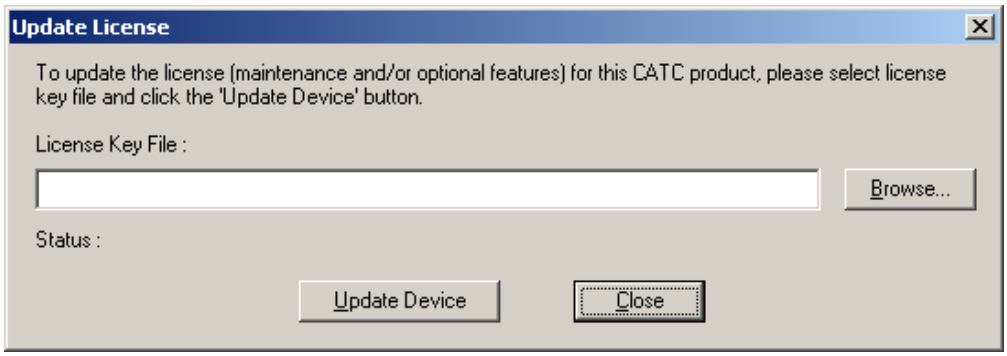
Step 9 Follow the on-screen instructions to complete the installation.

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

4.3 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.

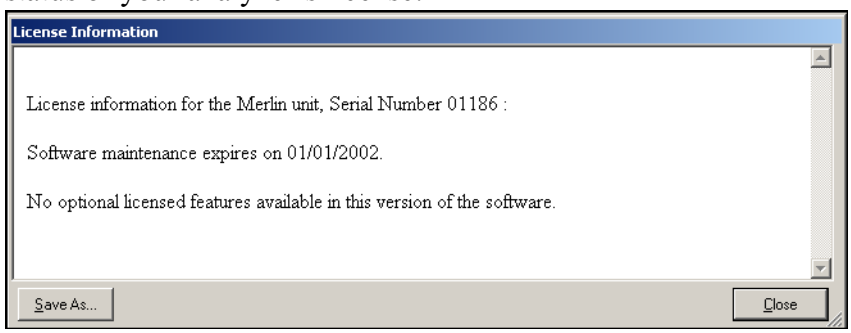
Step 3 Click **Update Device**.

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 Informatio**n.

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



4.4 BusEngine and Firmware UpdateUpdates

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

Automatic Updates

When BTTracer's software is updated, the software may become incompatible with the BusEngine and Firmware. If a recording is attempted, BTTracer will display an error message and then automatically begin an update process for the BusEngine and Firmware. If you prefer, you can abort this update and undertake the steps manually as described later in this chapter.

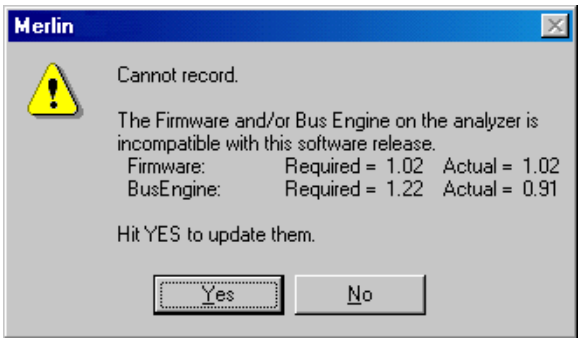
To perform an automatic BusEngine and Firmware update,

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

Step 1 Turn on the Analyzer.

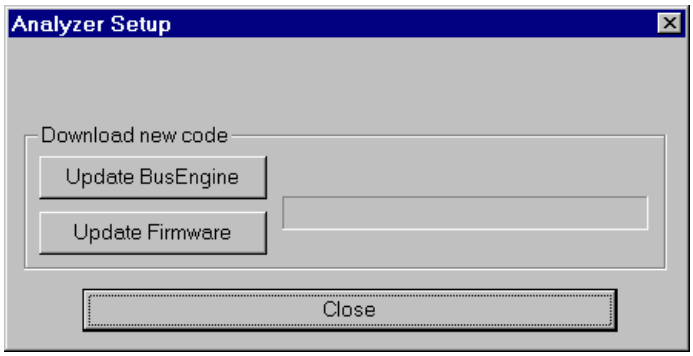
Step 2 On the toolbar, click the REC button.

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



Step 3 Click Yes.

The above window closes and the Analyzer Setup window opens.

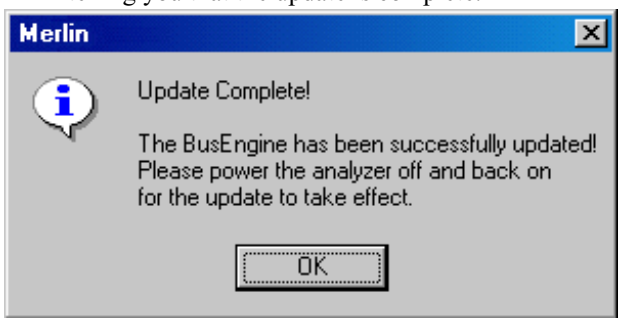


Step 4 Click **Update BusEngine** or **Update Firmware** on the

Analyzer Setup screen.

You can select only one item at this point. If both the BusEngine and the Firmware need to be updated, the 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.



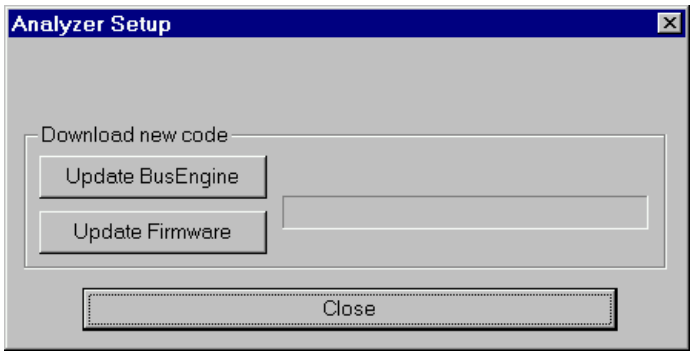
Step 5 Power cycle BTTracer to complete the update.

Manual Updates to BusEngine and Firmware

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

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

You see the **Analyzer Setup** screen:



Step 2 Click **Reset Analyzer**

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

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

Updating the BusEngine

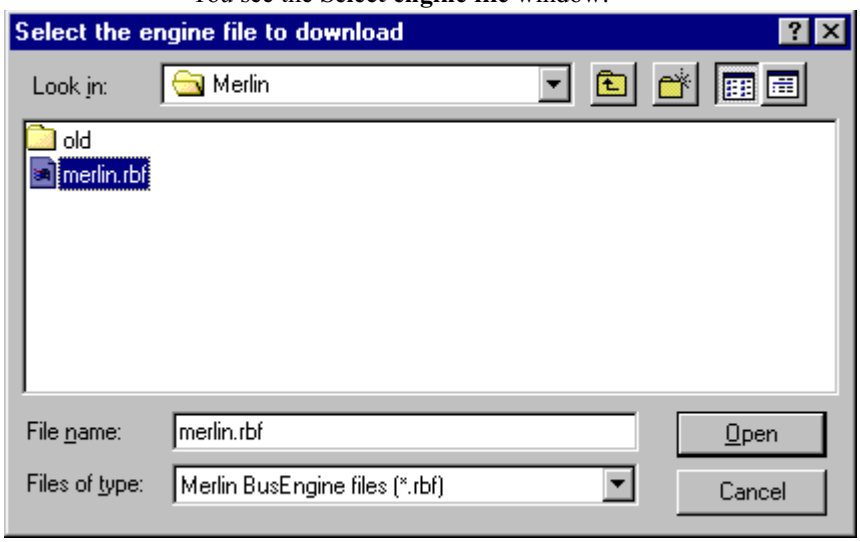
The BusEngine core is the heart of the Merlin Analyzer. Using state-of-the-art PLD technology, it incorporates both the high speed recording engine and the configurable building blocks that implement data/state/error detections, triggering, capture filtering, external signal monitoring, and event counting and sequencing. Both the BusEngine program and the Firmware that manages the internal microcontroller are fully field updateable.

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

To update the BusEngine,

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

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



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

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

Step 2 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.

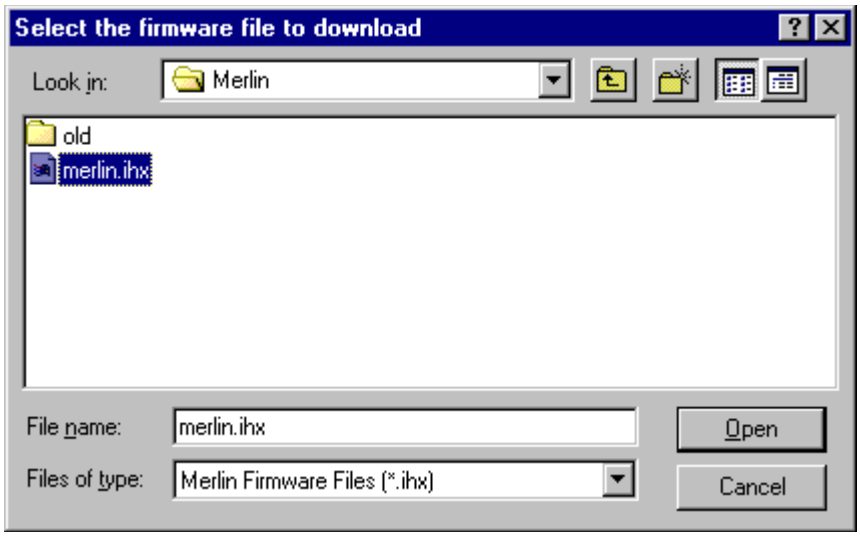
Updating the Firmware

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

To 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.

5. Software Overview

5.1 The Main Display Windows

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

Table 3: Main Display Pull-Down Windows

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

Menu	Function
Report	
File Information	Details such information about the recording as number of packets and triggering setup.
Error Summary	Displays an error summary of the current trace file and allows you to go to a specific packet, and save the error file to a uniquely named file.
Timing Calculation	Starts the calculator dialog for calculating various timing and bandwidth parameters in the recording file.
Traffic Summary	Details the number and type of packets were transferred during the recording, as well as message-level statistics.
Search	
Go to trigger	Positions the display to show the first packet that follows the trigger event.
Go to Packet/Message/ Protocol ...	Positions the display to the indicated packet, LMP/L2CAP message, or Protocol Message (RFCOMM, TCS, or SDP protocols).
Go to Marker »	Positions the display to a previously marked packet.
Go to »	Enables quick searching for specific events using a cascade of pop-up windows.
Find	Allows complex searches.
Find Next	Repeats the previous Find operation. Can also use F3 to find next.
Search Direction	Allows you to specify a forward or backward search of a trace file.
View	
Toolbars	Displays list of available toolbars.
Status Bar	Switches display of the Status Bar on or off.
Unhide cells	Allows you to unhide cells.
Zoom In	Zoom in increases the size of the displayed elements.
Zoom Out	Zoom out decreases the size of the displayed elements.
Wrap	Allows the display to wrap.
BT Neighborhood	Displays Bluetooth™ Address and clock frequency for devices in range. The expected Bluetooth™ clock frequency is 3200 Hz +/- 250 ppm.
Decoding Assignments	Displays current decoding assignments and provides options for changing them.
L2CAP connections	Displays current L2CAP connections and provides options for changing them.
RFCOMM Channel Assignments	Displays current RFCOMM Channel Assignments and provides options for changing them.
Levels	Displays the level you select.

Menu	Function
Window	
New Window	Switches display of the Tool Bar on or off.
Cascade	Displays all open windows in an overlapping arrangement.
Tile	Displays all open windows in a side-by-side arrangement.
Arrange Icons	Arranges minimized windows at the bottom of the display.
Windows	Displays a list of open windows.

Help	
Help Topics...	Displays online help.
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 BTTracer...	Displays version information about BTTracer.

5.2 View Options

The View feature in the Menu Bar allows you to

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

Tool Bar

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

Open file

Save As

Preview

Print…

Setup Record Options

Hide Nulls & Polls

Hide Unassociated Traffic

Complex Find

Find Next

File Information Report

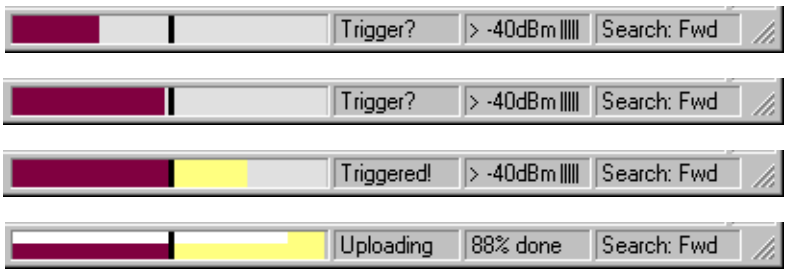
Setup Display Options	Traffic Summary
Start Recording	View Packet Level (Baseband)
Stop Recording	View/Hide LMP Message Level
Bluetooth Neighborhood	View/Hide L2CAP Message Level
Setup Encryption Options	View/Hide SDP Message Protocol Level
Recording Wizard	View/Hide SDP Transaction Protocol Level
Zoom In	View/Hide TCS Protocol Level
Zoom Out	View/Hide RFCOMM Protocol Level
Wrap	View/Hide OBEX Protocol Level
Hide Frequency Hops	View AT Commands Protocol Level
Error Summary	View/Hide PPP
Timing Calculatons	View/Hide HDLC Protocol
Start BTTracer's Wand	View/Hide BNEP Protocol
	View HID Protocol Layer

5.3 Status Bar

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

Recording Progress

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



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

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

You should be aware of two exceptional conditions:

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

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

Recording Status

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

— Trigger?

— Triggered!

— Uploading

After recording stops,

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

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

To abort the upload process,

- Press **Esc** on your keyboard

  OR

  Again click in the Tool Bar.

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

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

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

Analyzer Status

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

Inquiring – BTTracer is conducting a General Inquiry

Syncing – BTTracer is syncing to the Master device

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

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

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

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

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

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

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

Search Status

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

Zoom In

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

- Click on the Tool Bar.

Zoom Out

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

- Click on the Tool Bar.

5.4 Tool Tips

Throughout the application, tool tips provide useful information.

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

5.5 BTTracer Analyzer Keyboard Shortcuts

Several frequently-used operations are bound to keyboard shortcuts.

Table 4: Keyboard Shortcuts

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

6. Recording Wizard

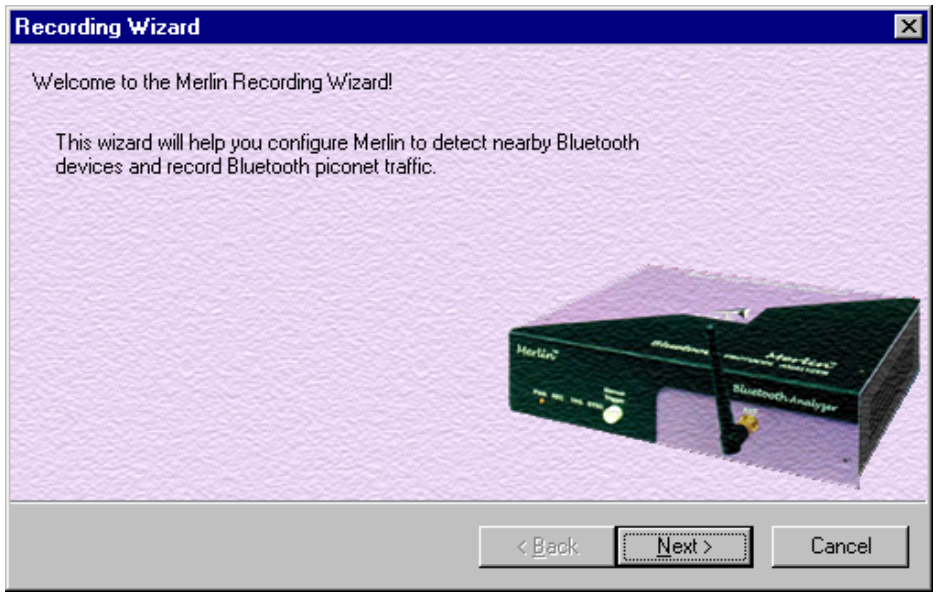
Recording Wizard is an interactive utility that presents a series of user-friendly dialog boxes for setting up a recording session. Recording Wizard serves as an alternative method of configuring the Recording Options dialog box. When you are finished using the Wizard, you can view your settings in the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

Starting Recording Wizard

To start the **Recording Wizard**,

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

You see the **Recording Options** window:

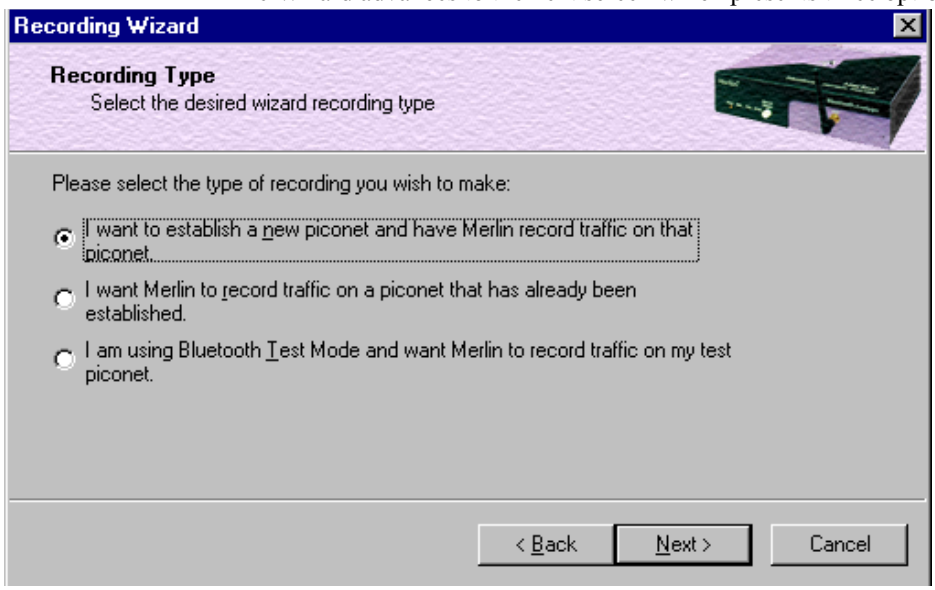


The **Recording Options** window has three buttons marked **Next**, **Back**, and **Cancel** that allow you to move forward or backward through the wizard or to cancel the wizard.

To begin advancing through the wizard,

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

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



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

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

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

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

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

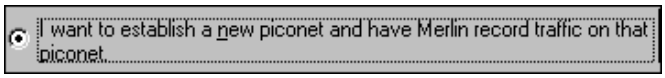
  This option lets BTTracer create either a single frequency range recording of a range that you specify or create a recording of a limited hop frequency range consisting of 5 frequency hops.

6.1 Recording a Traffic on a New Piconet

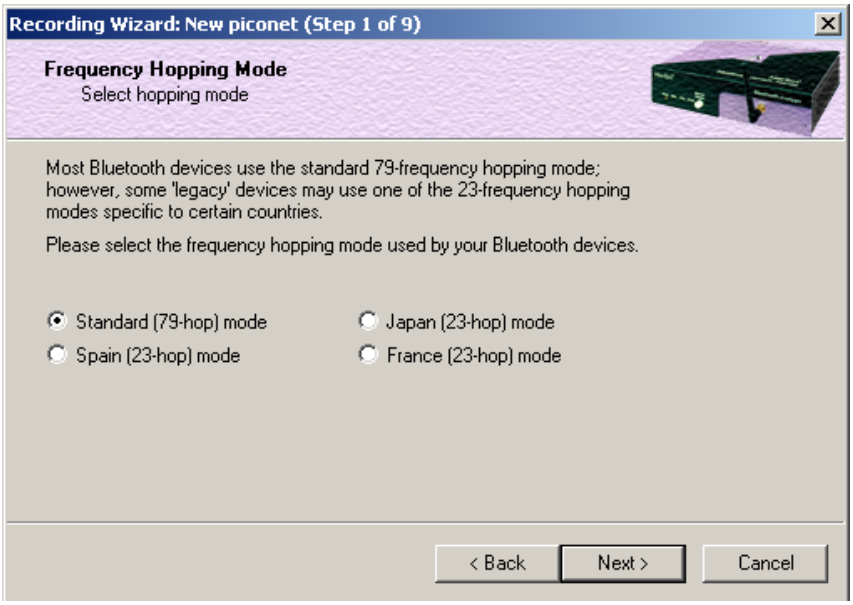
The **New Piconet** option shown in the previous screen presents users with the means of recording the traffic from a new piconet. This option will cause a sequence of screens to prompt you for information such as the piconet Master address.

The following steps shows you how to configure BTTracer 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 BTTracer record traffic on that piconet**, then press **Next**.

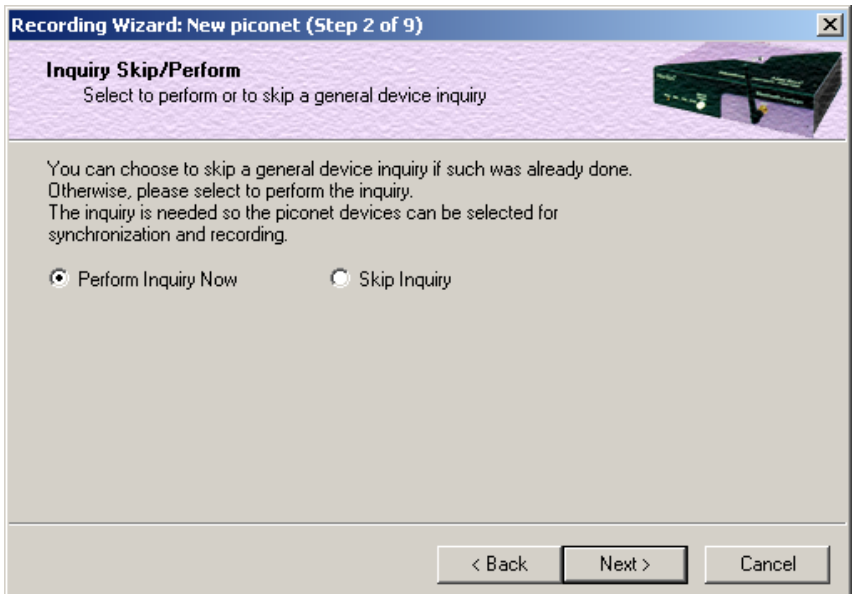


The following screen displays.



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

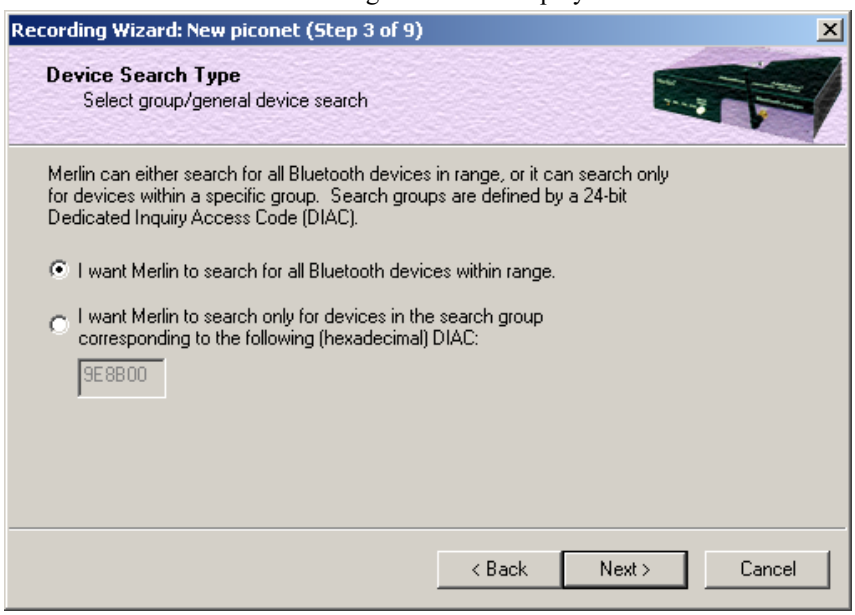
The following screen displays.



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

Selecting **Perform Inquiry Now** will cause BTTracer 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:

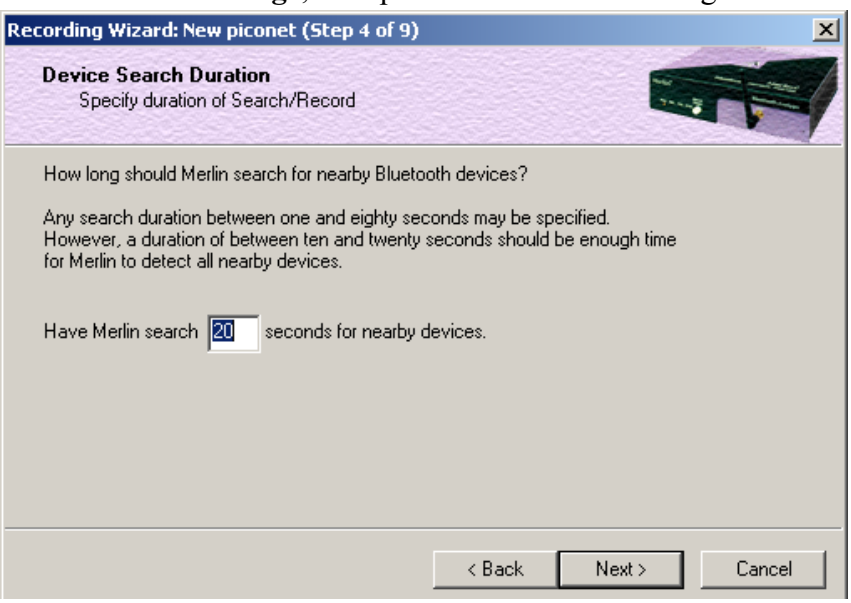
- **I want to search for all Bluetooth devices within range**

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

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



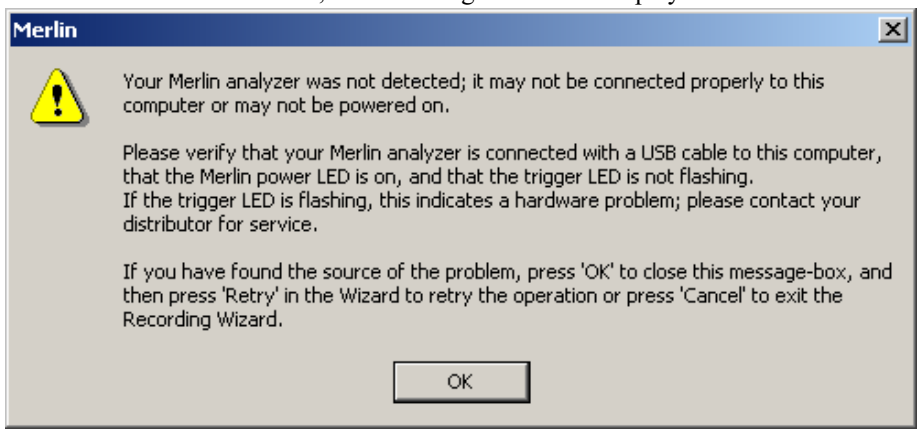
You will see two options:

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

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

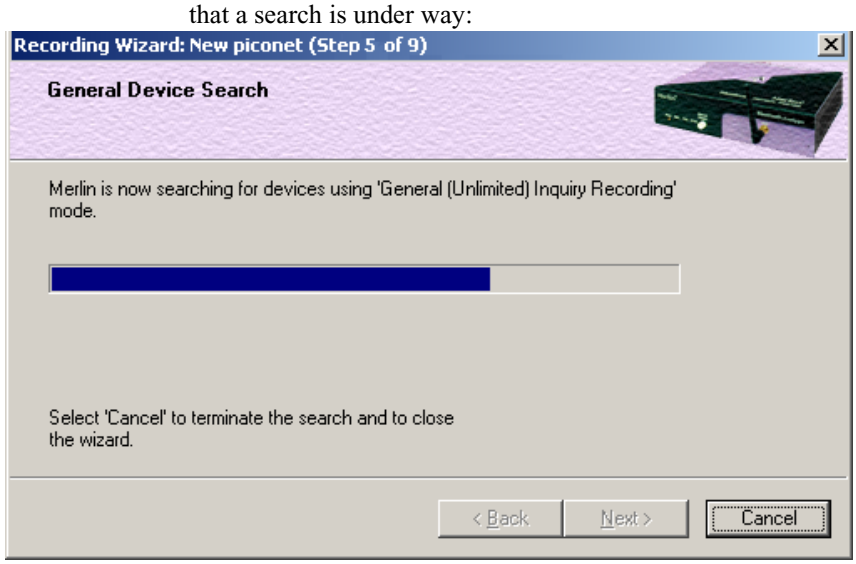
Step 6 Press **Next**.

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

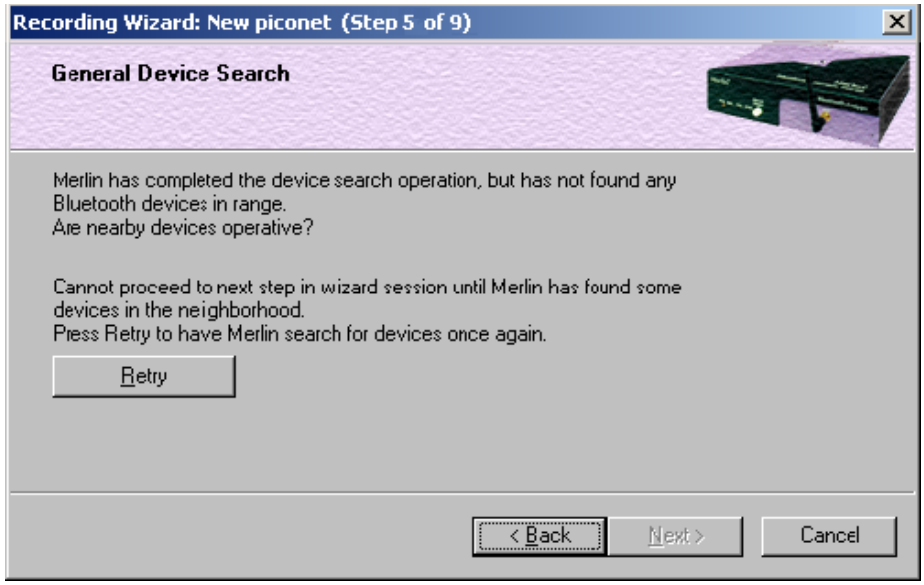


Clicking **OK** will close the message box.

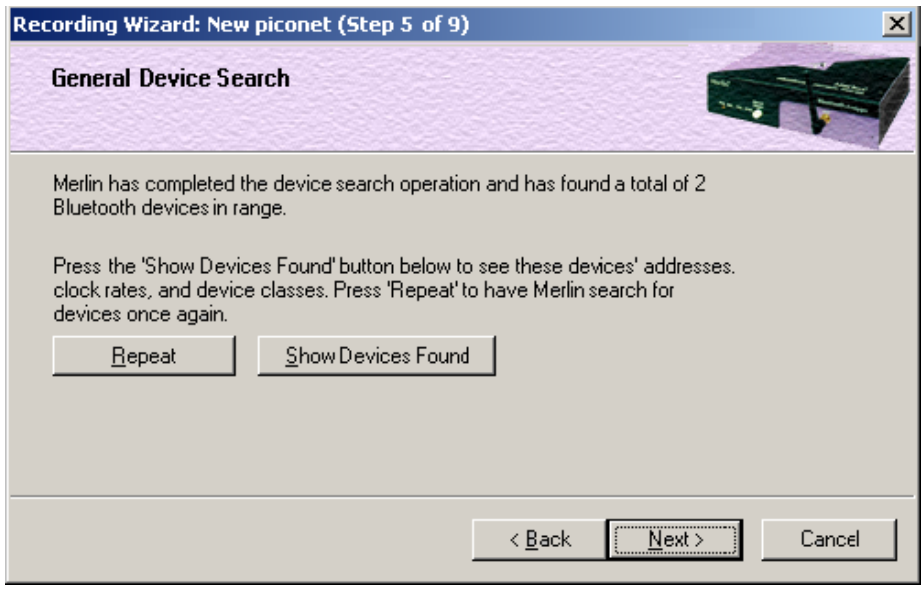
If BTTracer passes the hardware test, it will search for devices. The Recording Wizard will display a progress bar and a message telling you that a search is under way:



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



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

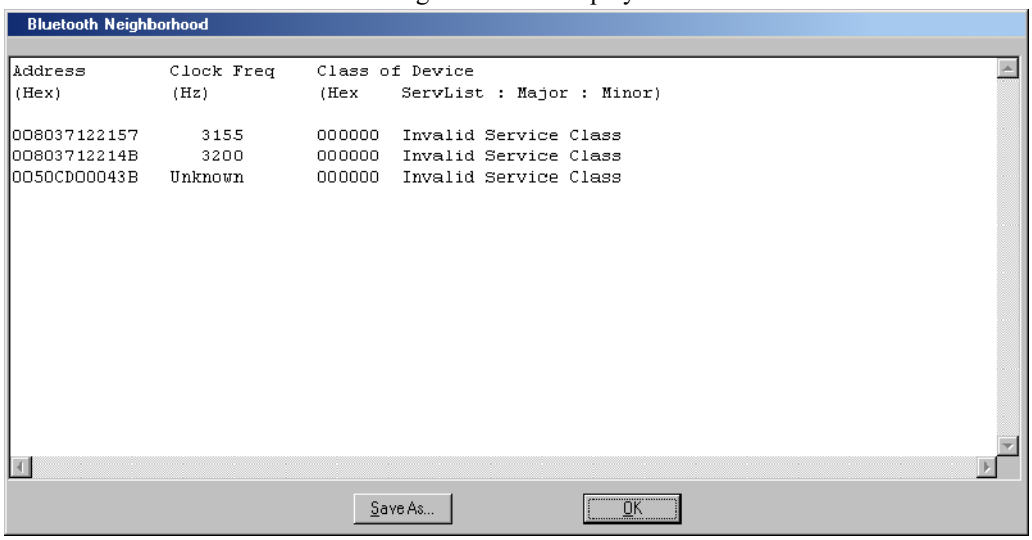


Two buttons will display:

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

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

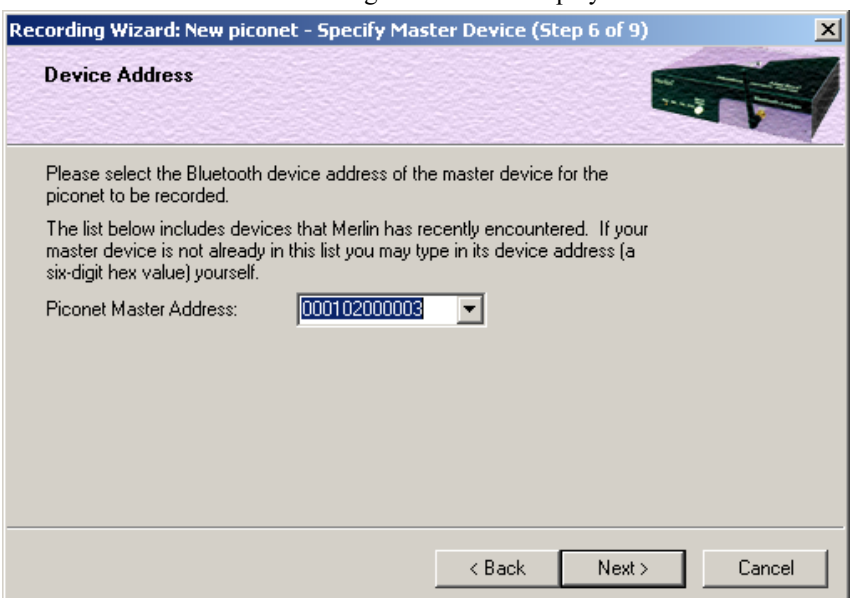
The following screen will display:



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

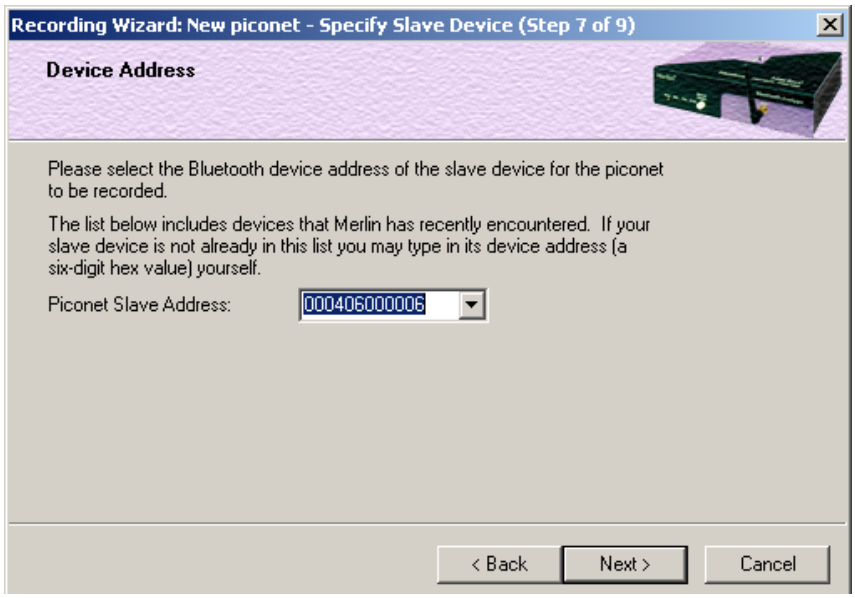
Step 9 Press **Next**.

The following window will display:



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

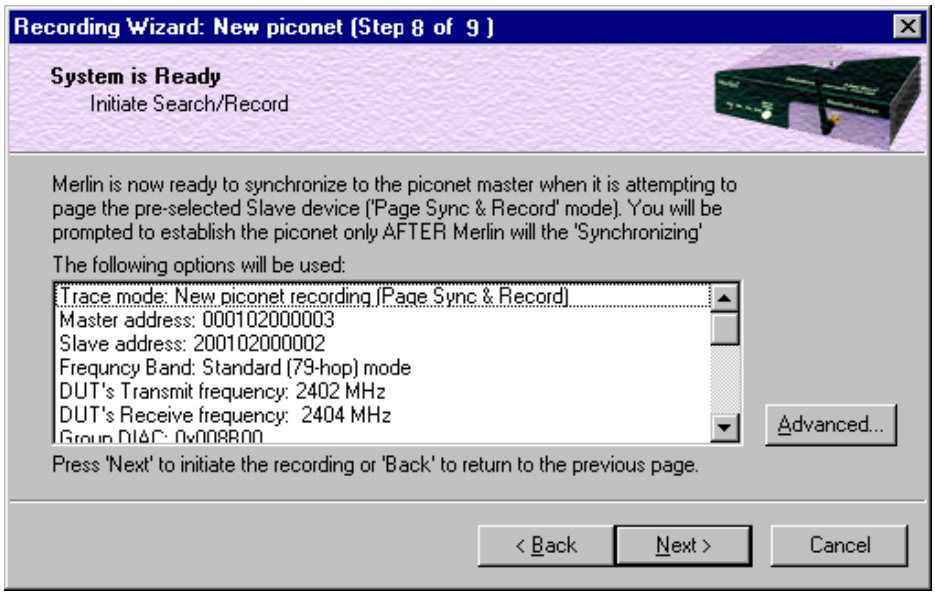
The following window will display:



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

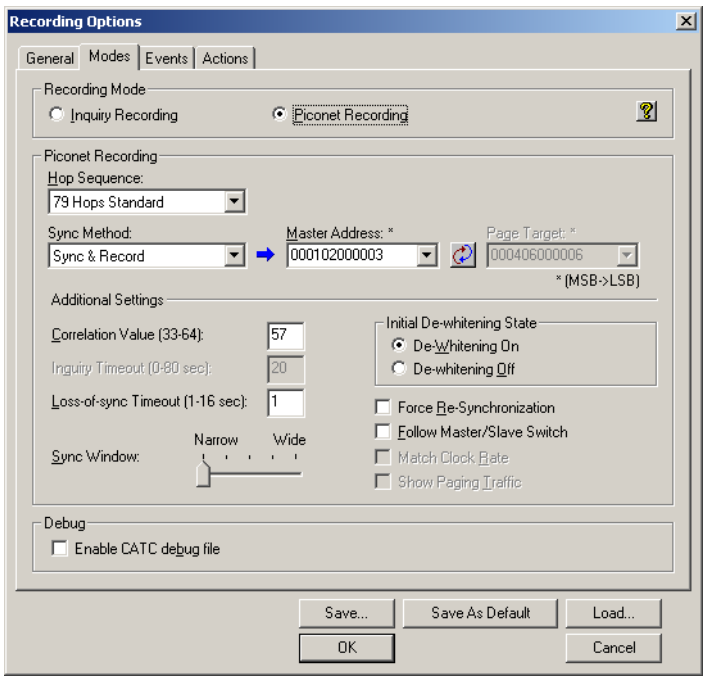
Step 12 Press **Next**.

The following screen 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.

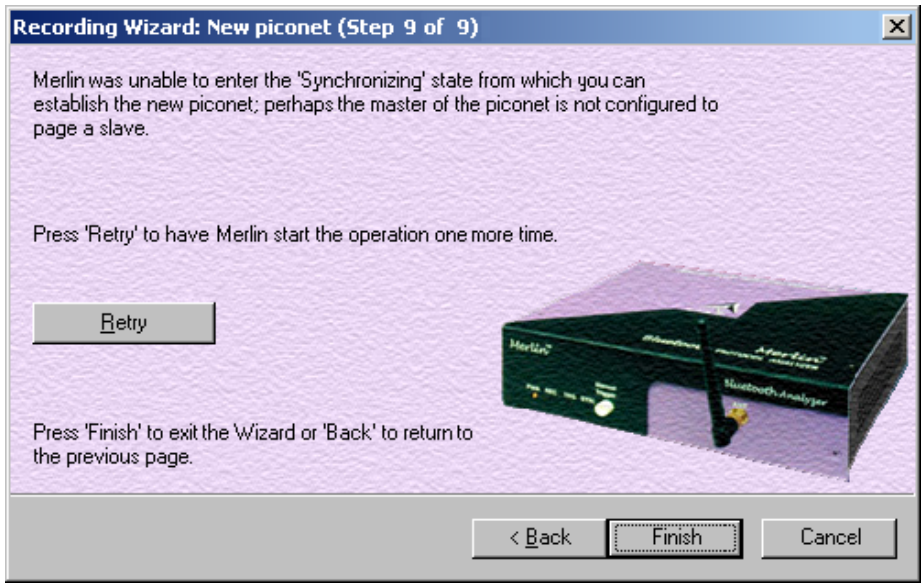


Step 13 Press **Next** to advance the Recording Wizard to the next screen.

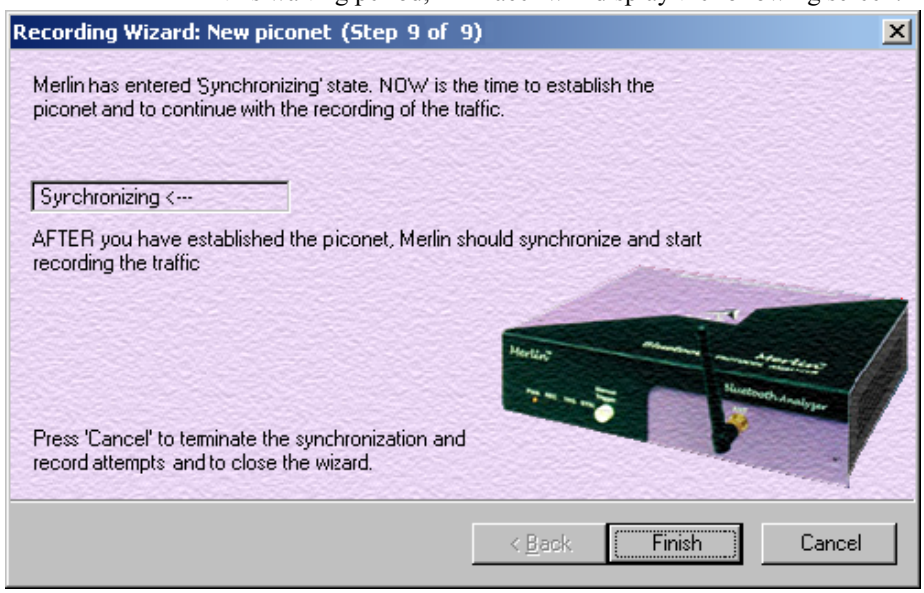
The following screen displays:

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

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

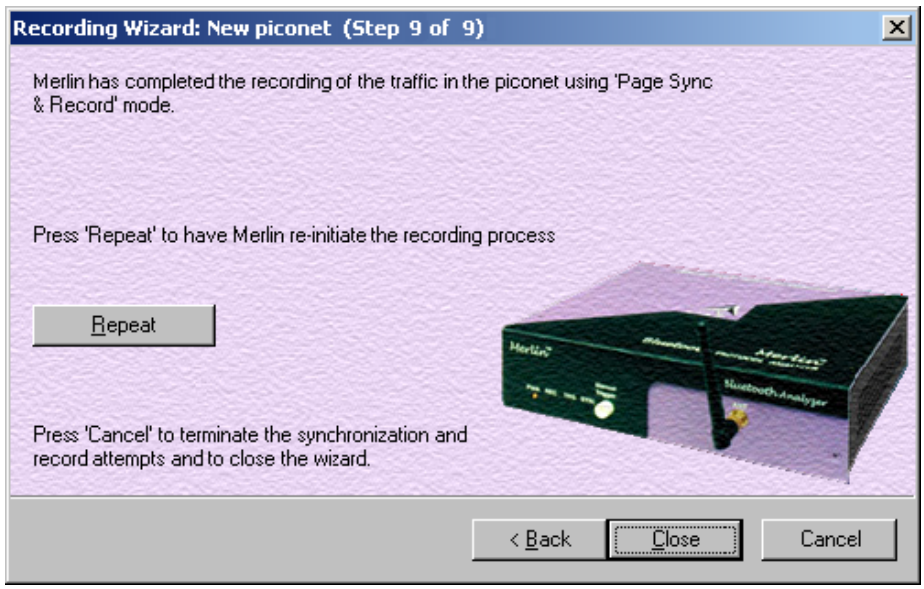


If BTTracer is able to complete its pages, it will enter into a synchronizing state and then wait for you to create the piconet. During this waiting period, BTTracer will display the following screen:



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

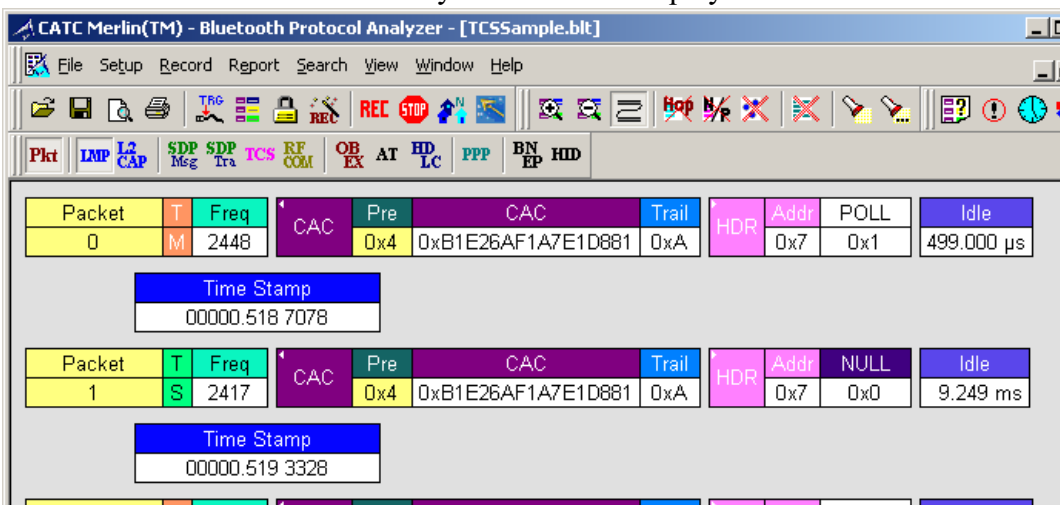
At the completion of the recording, BTTracer will display the following screen:



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

Step 14 To close the wizard, press the **Close** button.

The wizard will close and your trace will display.

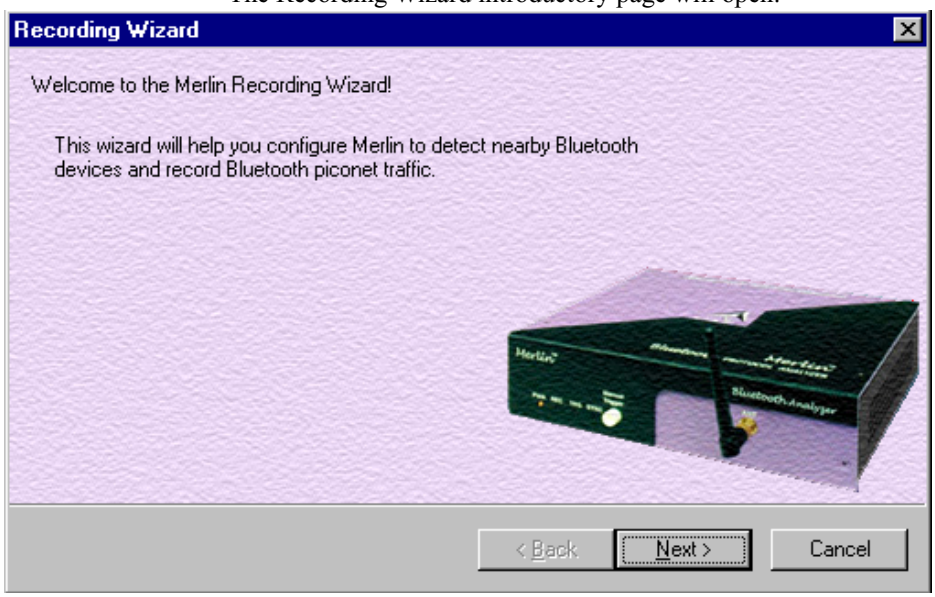


6.2 Recording an Existing Piconet

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.

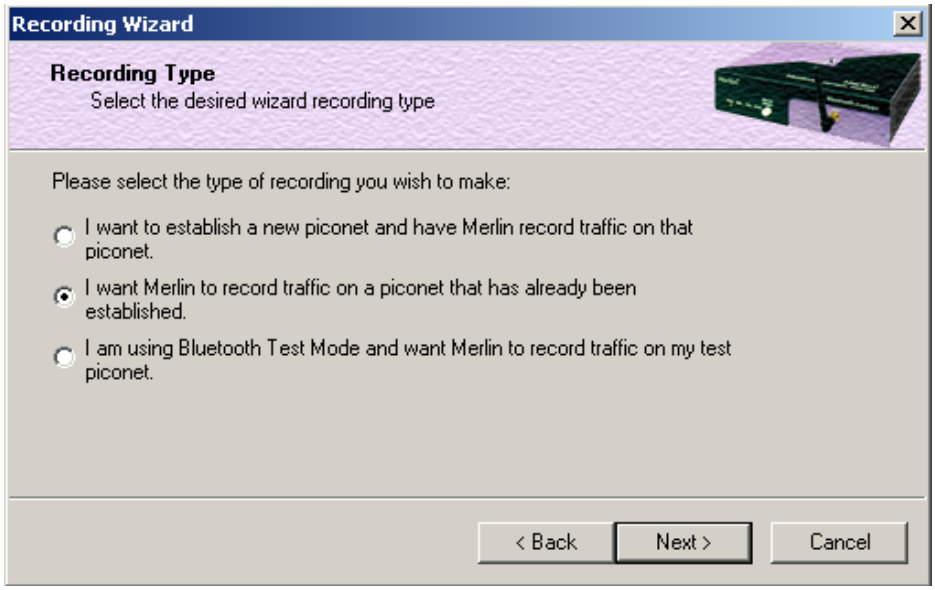
Step 1 To start the Recording Wizard, press REC or select **Setup > Recording Wizard** from the menu.

The Recording Wizard introductory page will open:



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

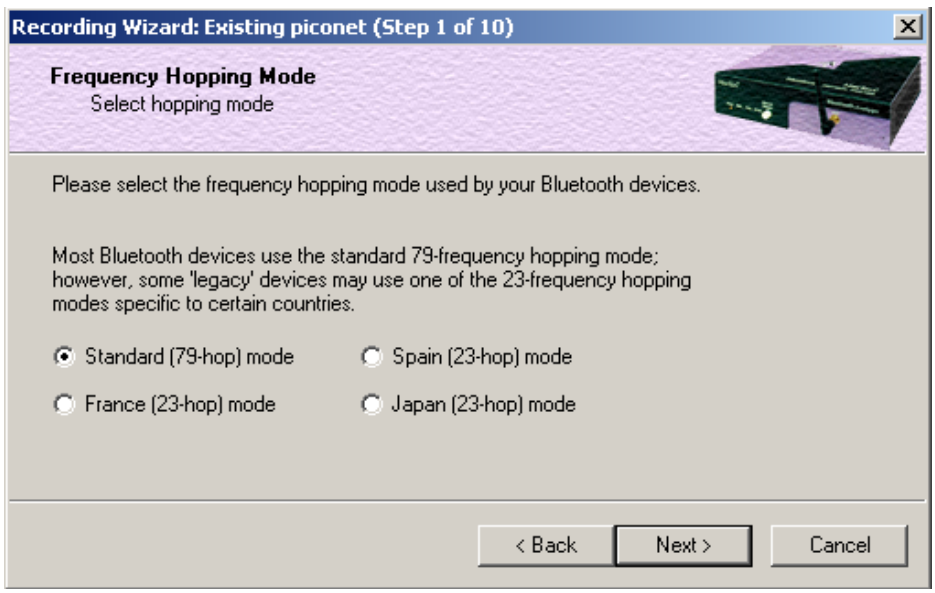
You will see three choices:



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

Step 4 Press **Next**.

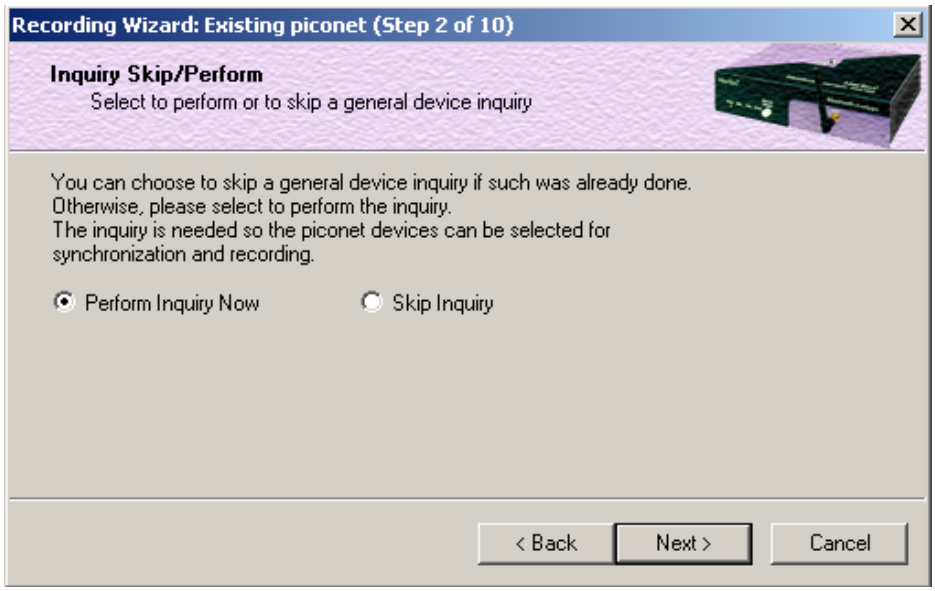
You will see four choices:



Select the hop mode appropriate to your area.

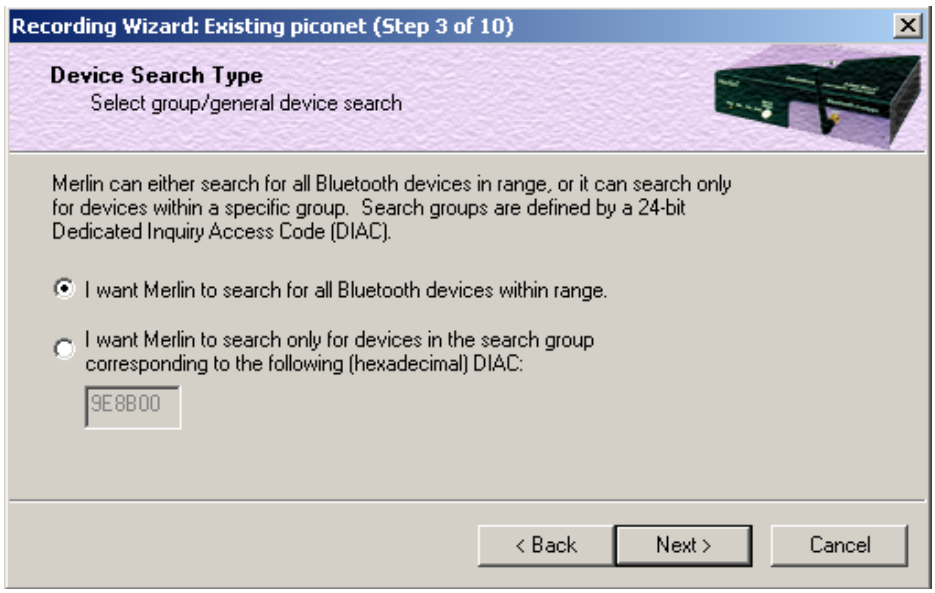
Step 5 Select the hop mode appropriate to your area, then press **Next**.

You will see two choices:



Step 6 Select **Perform Inquiry Now**.

You will see two choices:

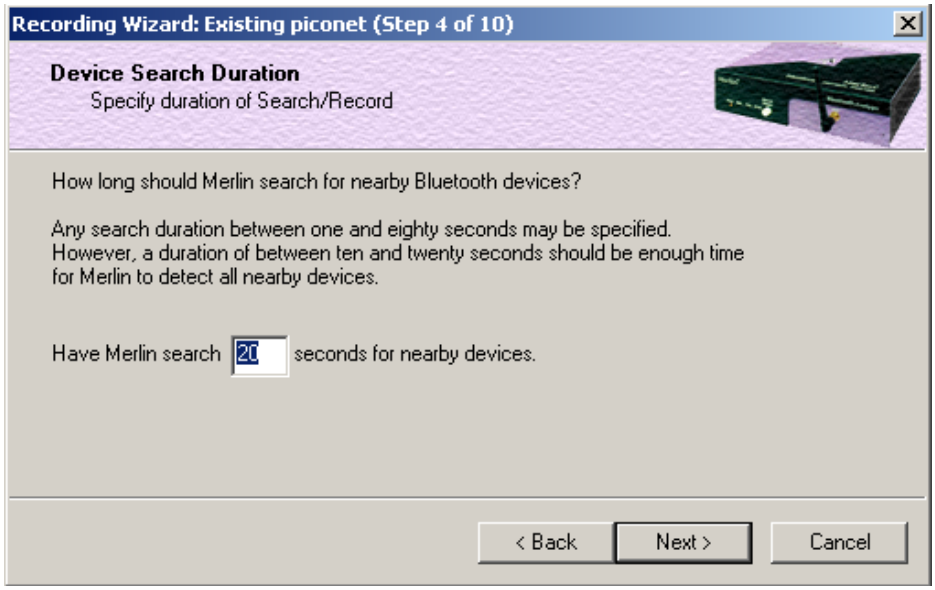


Step 7 Select the first option: **I want BTTracer to search for all Bluetooth devices within range**.

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.

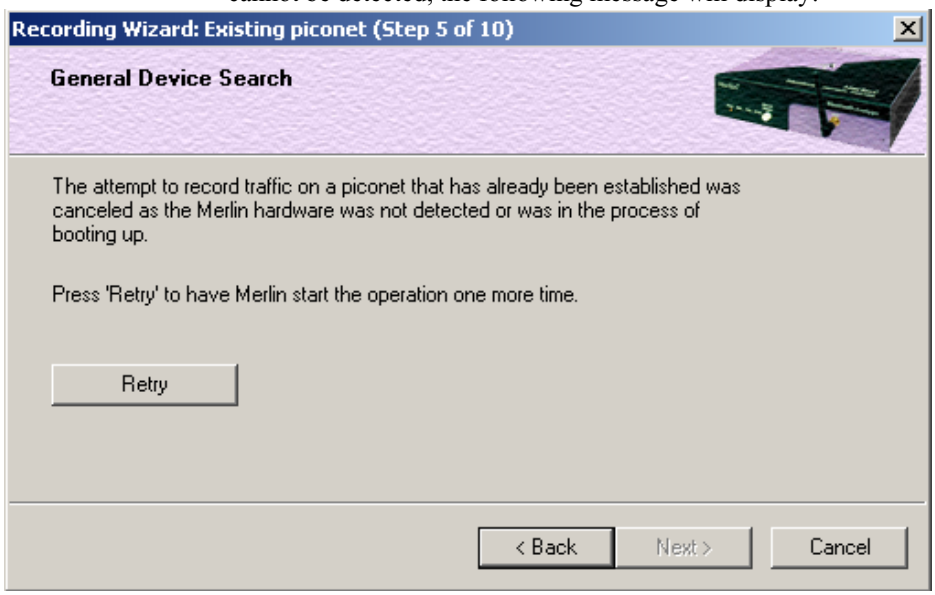
Step 8 Press **Next**.

You will see two choices:

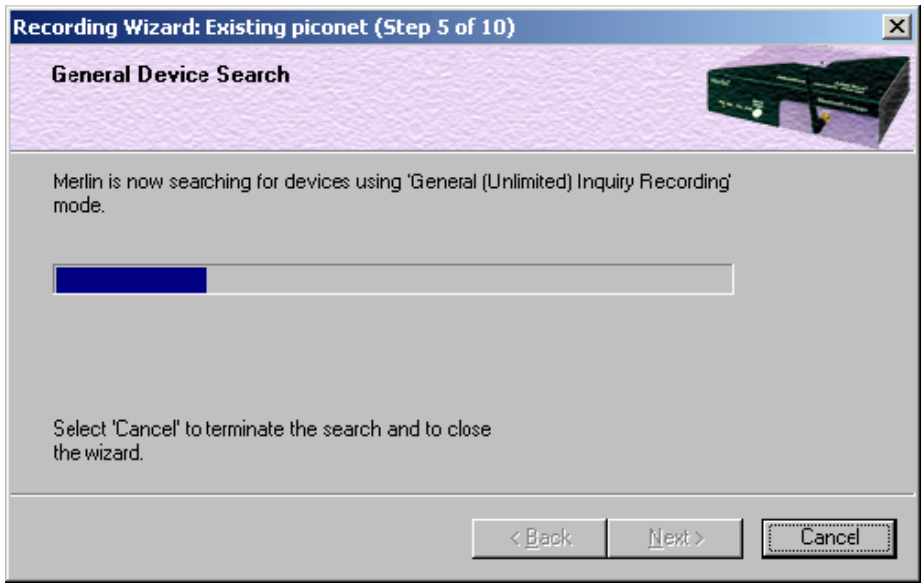


Step 9 If you want to change the search duration, type in a new value into the text box. Otherwise, use the default value (20 seconds), then press **Next**.

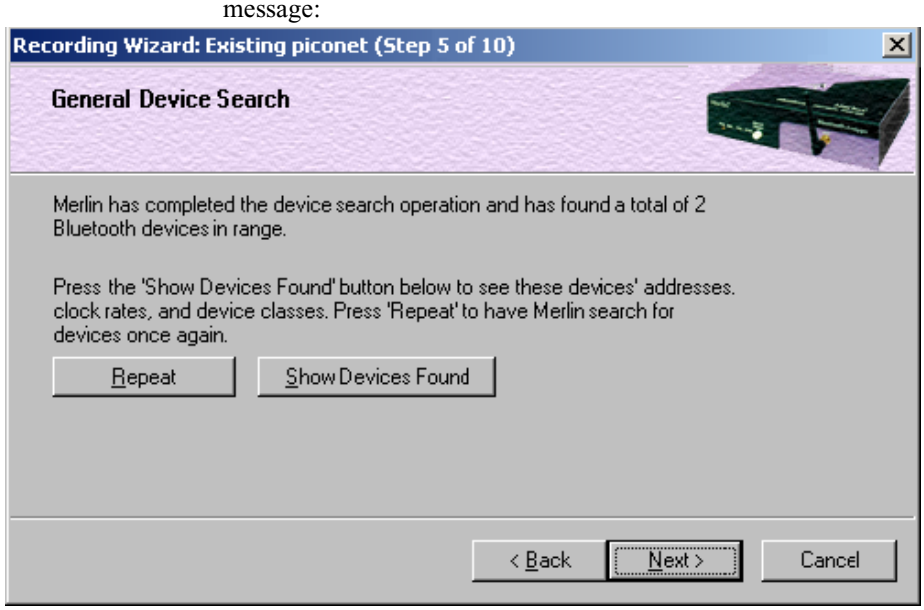
The PC-BTTracer hardware connection will be tested. If BTTracer cannot be detected, the following message will display:



If BTTracer passes the hardware test, it will then goes onto conduct a General Inquiry to locate local Bluetooth devices.



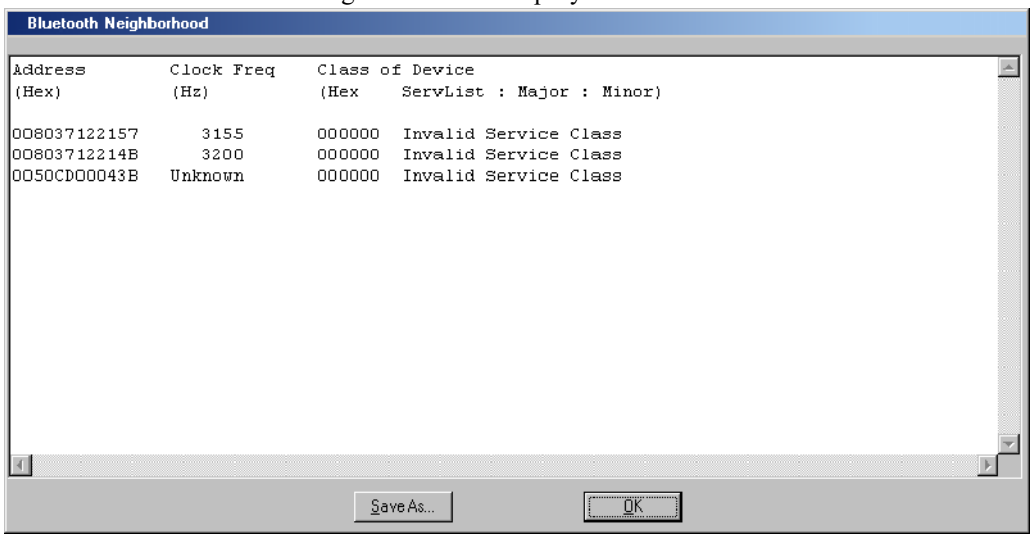
If BTTracer finds Bluetooth devices, it will display the following message:



Step 10 To display a list of the discovered devices, press the button

marked **Show Devices Found**.

A screen will display showing the devices that BTTracer discovered through the General Inquiry:

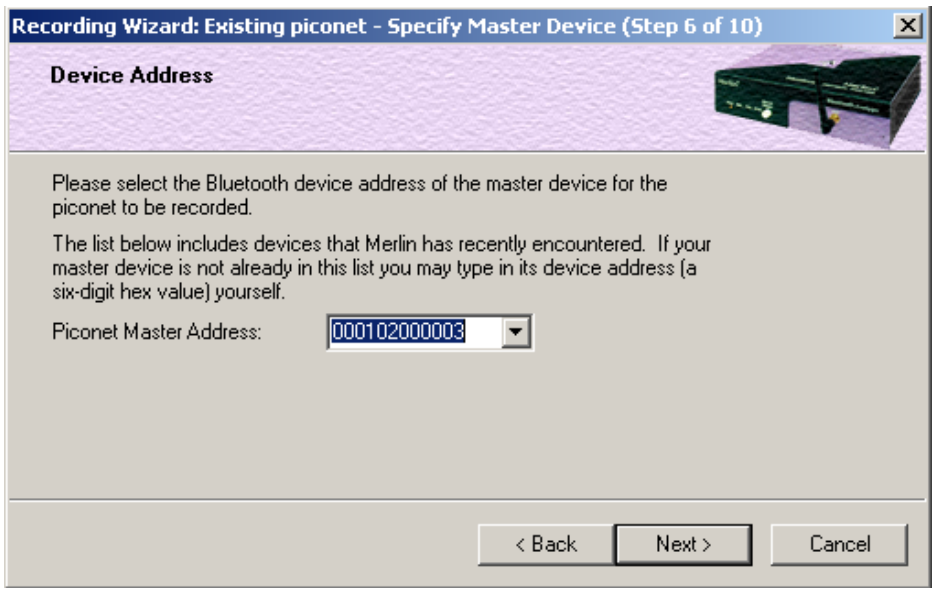


If you feel that the list is incomplete, you can close this window and press the button marked **Repeat**. This will cause BTTracer to repeat the General Inquiry and recollect information on local Bluetooth devices.

Step 11 Press **OK** to close the **Bluetooth Neighborhood** window.

Step 12 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 drop-down menu or typed into the box:

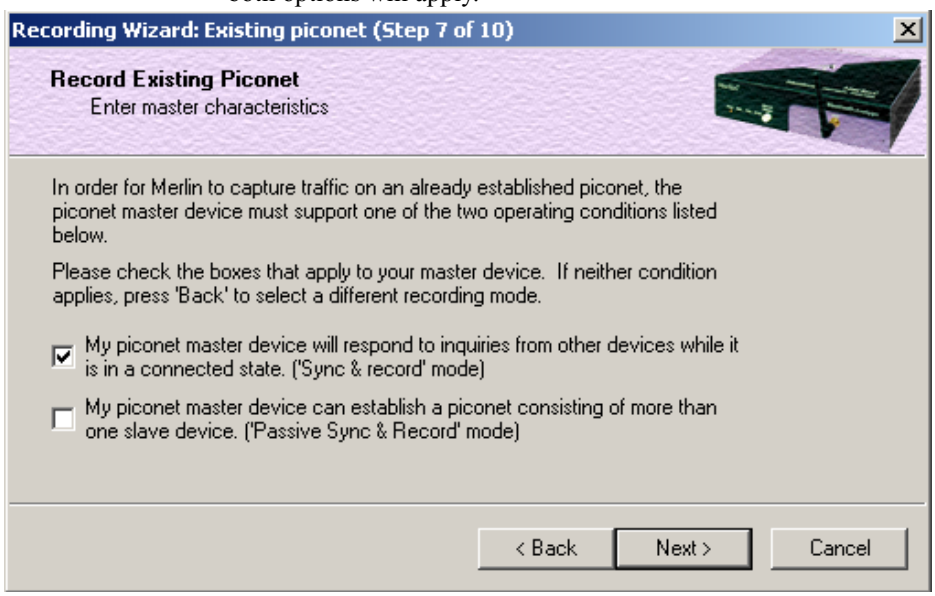


Step 13 Select or type in the Master device's address into the box

next to the label **Piconet Master Address**.

Step 14 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:

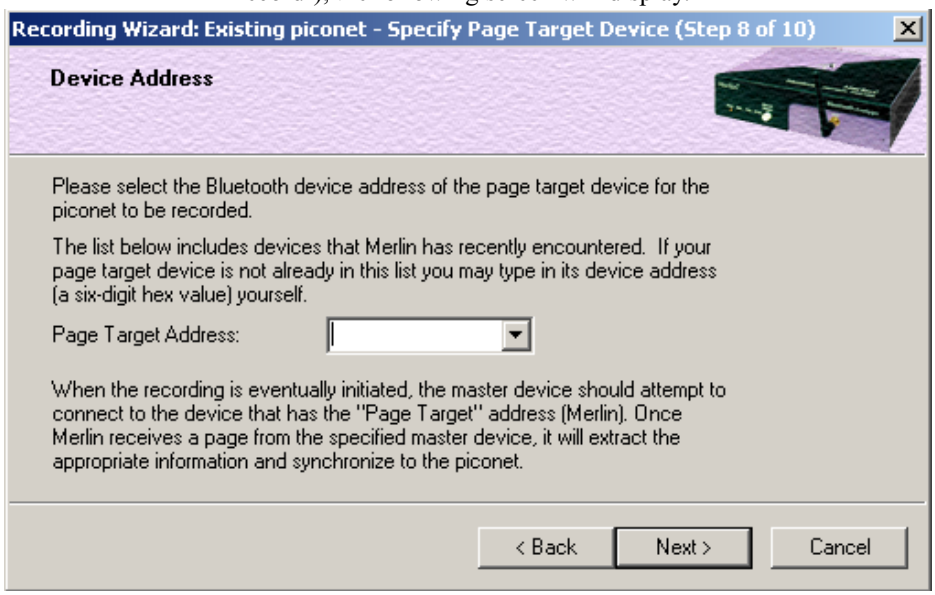
If the Master supports inquiries while in a connected state, select the first option. This will set BTTracer to use the 'Sync & Record' mode in its attempts to synchronize to the Master. This will also cause the wizard to skip to step 8.

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), BTTracer 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, BTTracer will use 'Sync & Record' no matter what was set in the second box.

Step 15 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 15 (='Passive Sync & Record'), the following screen will display.



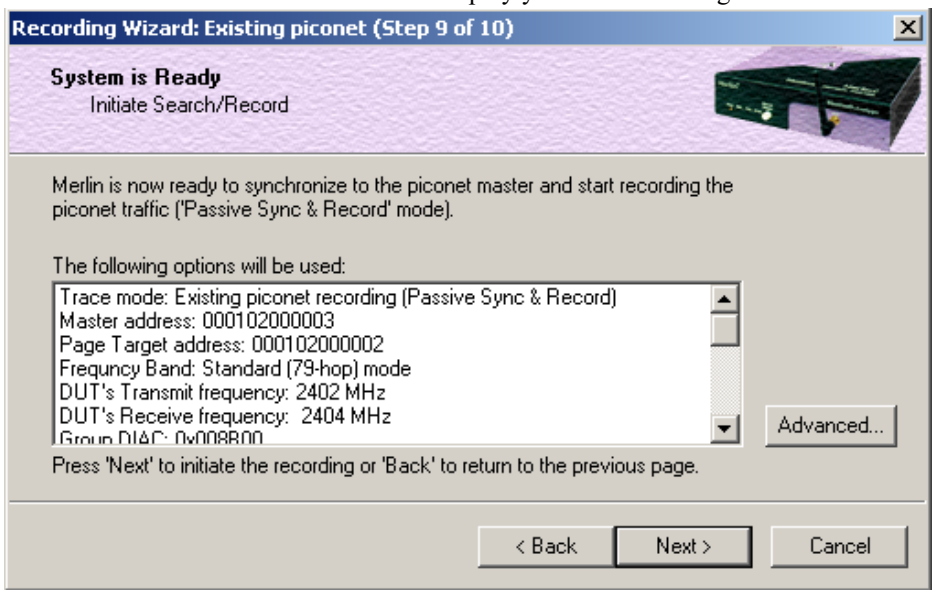
This screen asks you for the address of the Page Target device -- which in this case is BTTracer. Since the devices in your piconet are not able to respond to inquiries, BTTracer will not be able to page the devices and join the piconet. Instead, you will assign BTTracer an address here in this screen,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

Step 16 Type in an address of your choosing for BTTracer (= Page Target).

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

Step 17 Press **Next**

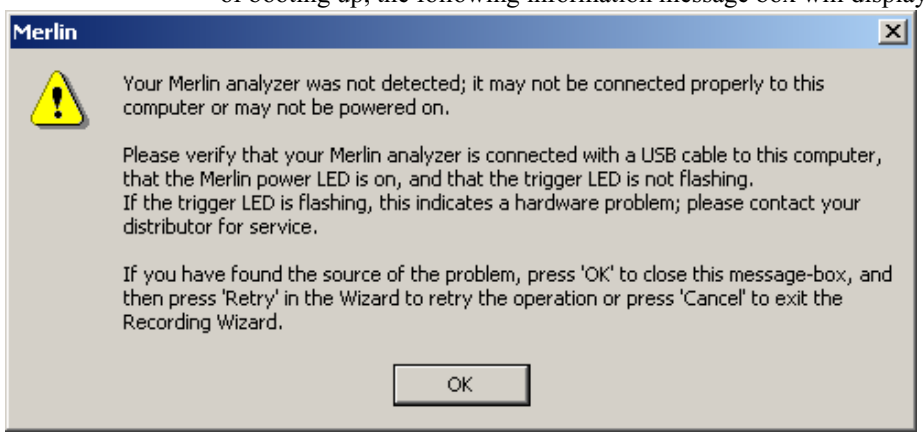
BTTracer will then display your current settings.



The **Advanced** button will open the Recording Options dialog box shown on page 46 and described in detail in Chapter 7.

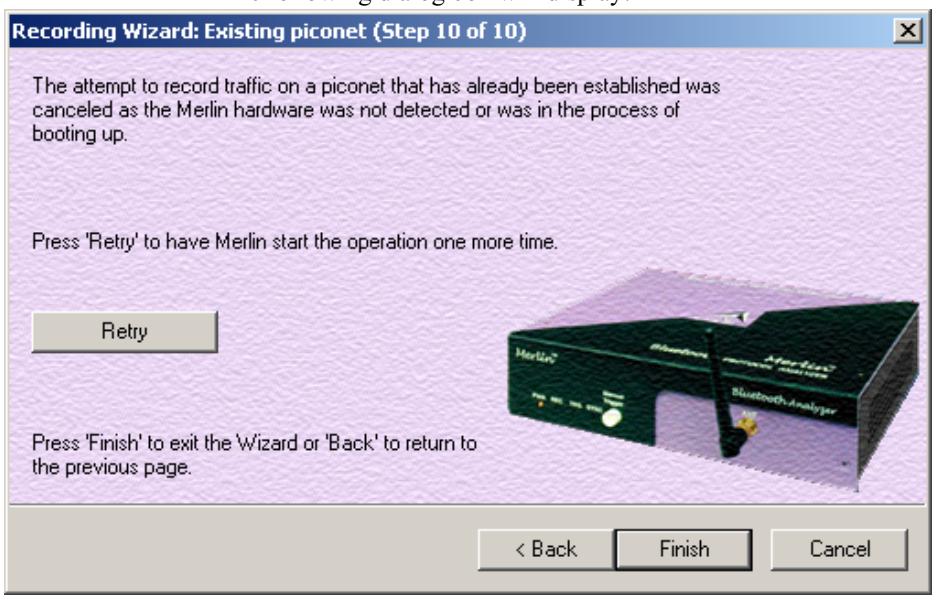
Step 18 Press **Next** to begin the recording.

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



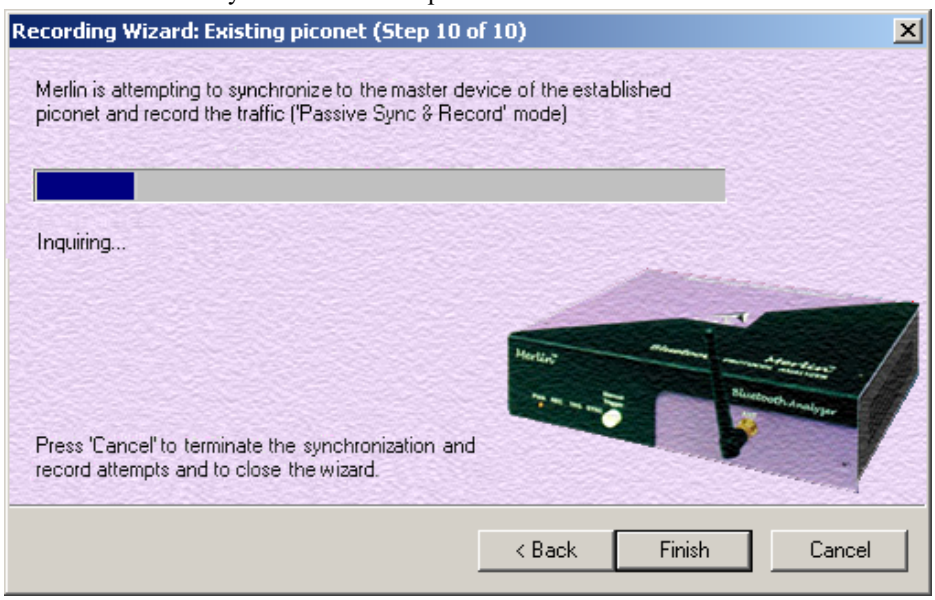
Step 19 If the above information box opened, press **OK** to close it.

The following dialog box will display:



Step 20 Press **Retry** or **Back** to re-attempt the process.

If the hardware failure described in Steps 20 and 21 do not occur, BTTracer will conduct an inquiry. The screen will show that BTTracer 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 21 If you are recording in 'Passive Sync & Record' mode, you will need to direct your Master device to attempt a connection to BTTracer. This will provide BTTracer with the information it needs to record the piconet.

Once BTTracer 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 22 When finished, press **Close** to close the Recording Wizard.

6.3 Recording in Test Mode

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

Recording in Reduced Hopping Mode

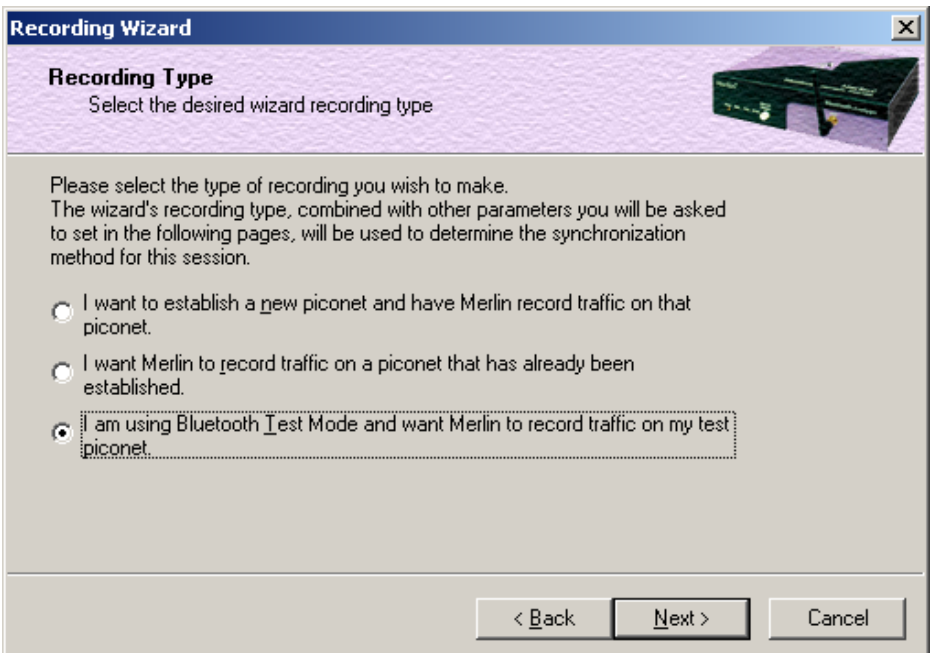
To record in Reduced Hopping Mode, perform the following steps:

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.

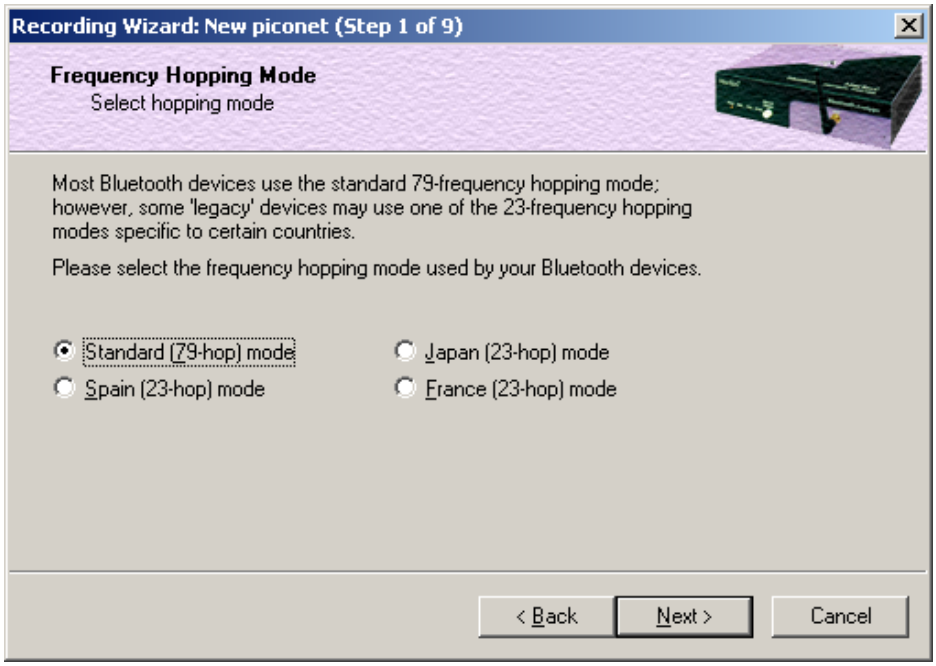
The following screen will display:



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

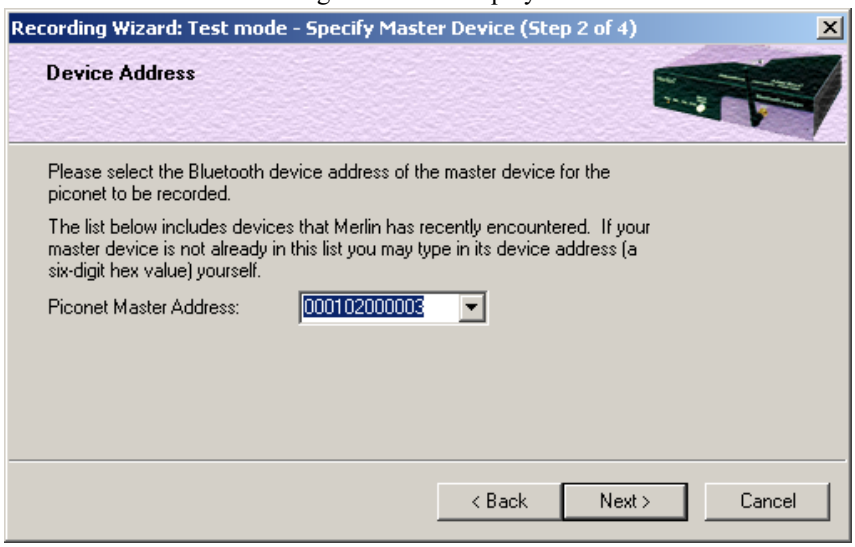
Step 4 Press **Next**.

The following screen will display:



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

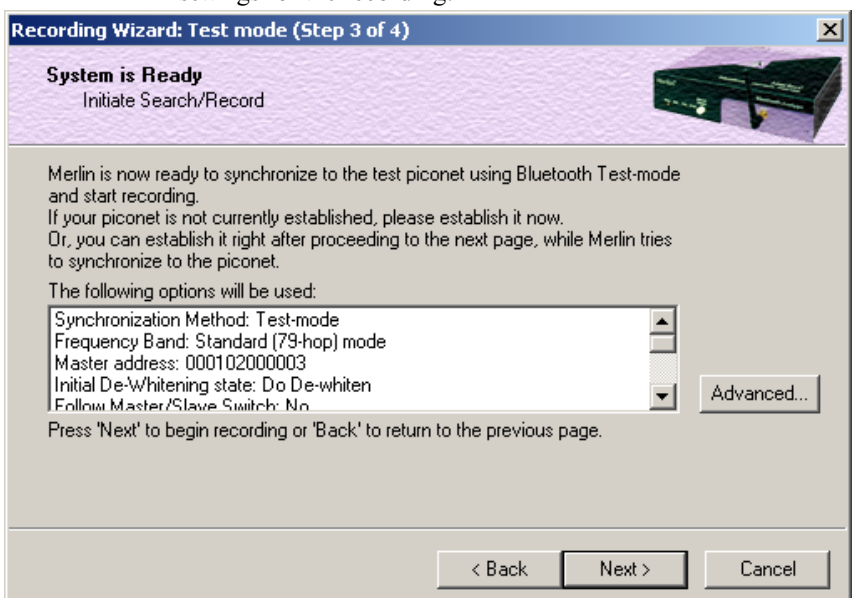
The following screen will display:



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**.

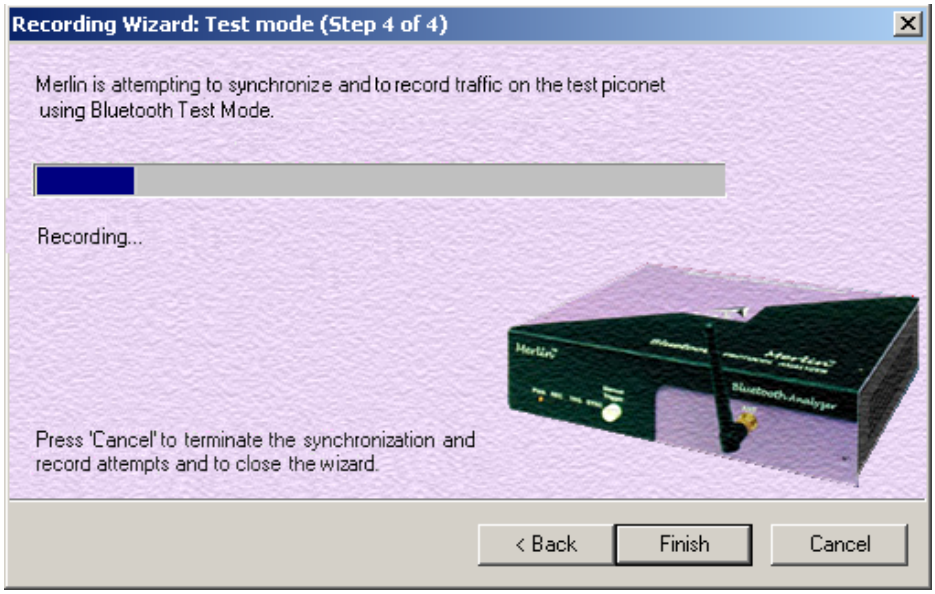
The following screen will display. This screen will show the current settings for the recording:



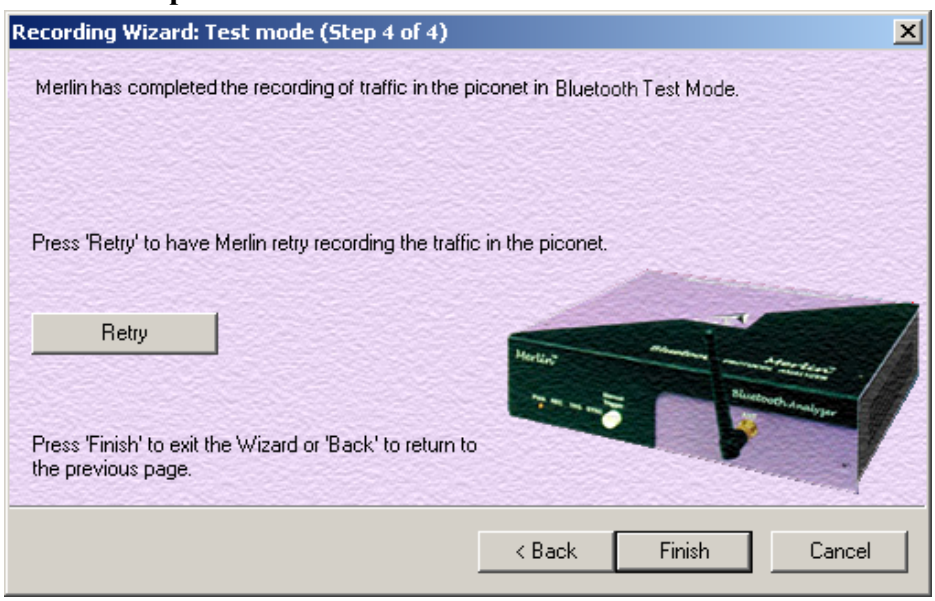
The Advanced button will open the Recording Options dialog box. See Chapter 7 for details on the Recording Options dialog box.

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

The following screen will display:



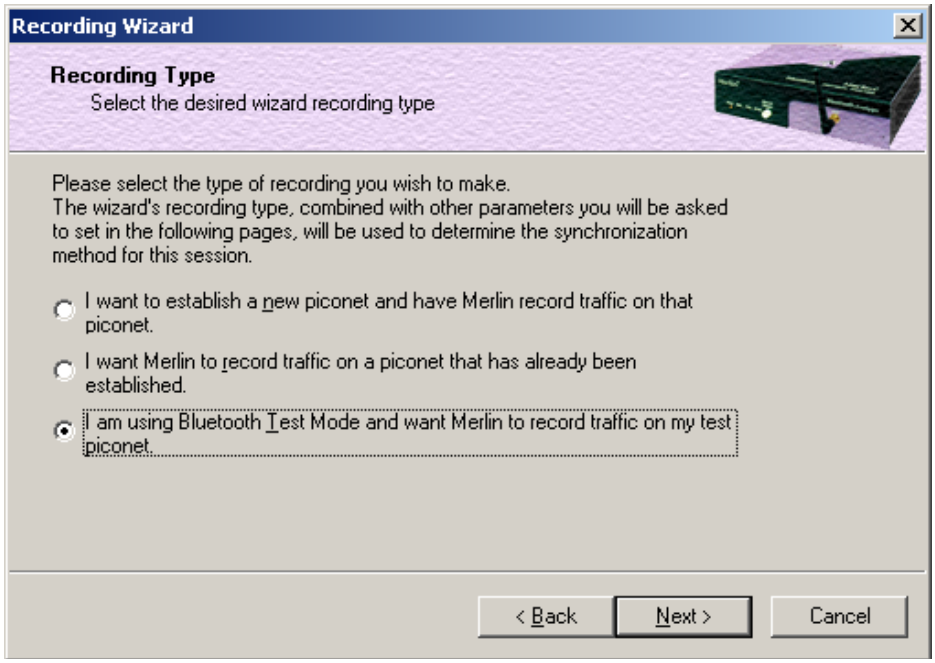
Step 9 When the recording finishes, the following screen will display. You can repeat the recording by pressing the **Repeat** button.



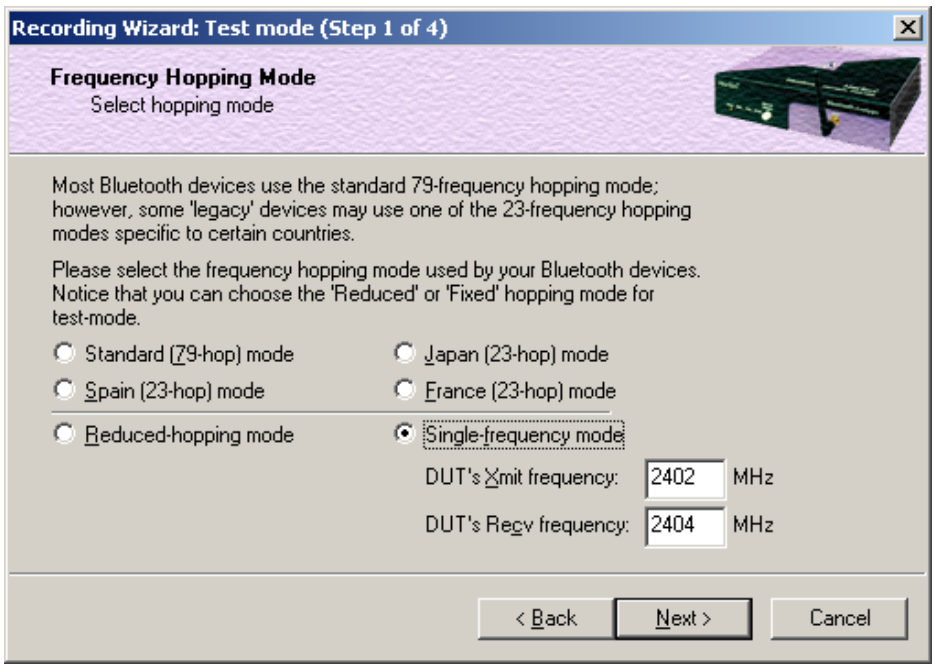
Step 10 To close the wizard, press **Finish**.

6.4 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 Mod**e, window select the **Single-Frequency Mode** radio button, enter the appropriate values in the text boxes, and click **Next**.



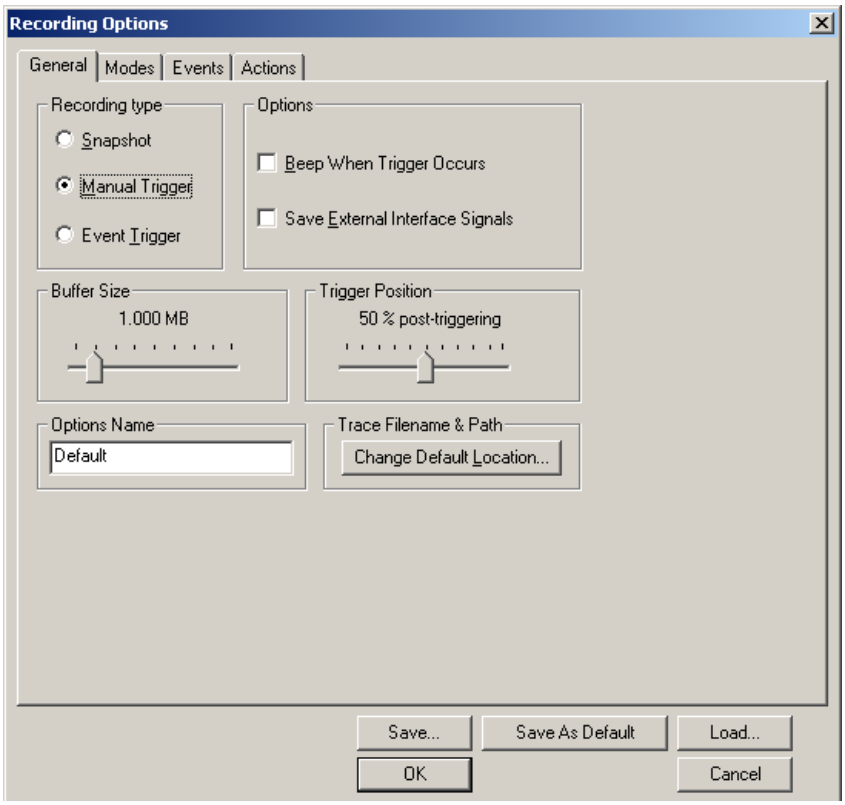
7. Recording Options

The **Recording Options** dialog box lets you configure BTTracer for recording Bluetooth™ data. This dialog box offers an alternative to the Recording Wizard described in the previous chapter. At the top of the Recording Options dialog box are four tabs that provide access to dialog boxes called General, Modes, Events, and Actions. Using these dialog boxes, you can configure BTTracer to create event triggers, increase or decrease memory allocation for recording, and interact with other Bluetooth™ devices in different ways.

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:



The **Recording Options** window has four tabs marked

- **General**
- **Modes**
- **Events**
- **Actions**

7.1 Recording Options - General

The General tab is displayed by default when the Recording Options dialog box is oppened. It is shown in the previous illustration. The General tab display four boxes marked *Recording Type, Buffer Size, Trigger Position,* and *Options*.

Recording type

The **Recording Type** box presents three options that allow you to set how BTTracer 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 REC 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 REC on the Tool Bar. Recording continues in a circular manner within the limits set by the buffer size. Recording ends when STOP 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

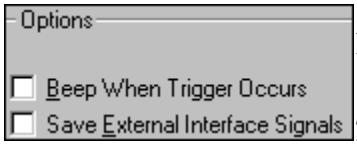
An Event Trigger recording is one that uses an event trigger to end the recording. Before recording begins, you define the event trigger in the Trigger Options dialog box. You begin the recording by clicking REC on the Tool Bar. Recording continues in a circular manner within the limits set by the buffer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

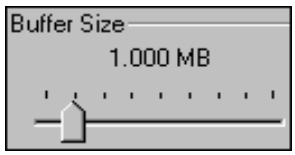


Will cause the PC to beep when a trigger event has occurred.

Save External Interface Signals

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

Buffer Size

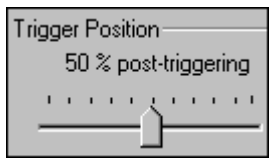


The Buffer Size box has a slide bar for adjusting the recording buffer size from 0.1 megabytes to 128 megabytes.

The Recording Type option determines how this buffer is used. Although there are 128 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 BTTracer 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**.

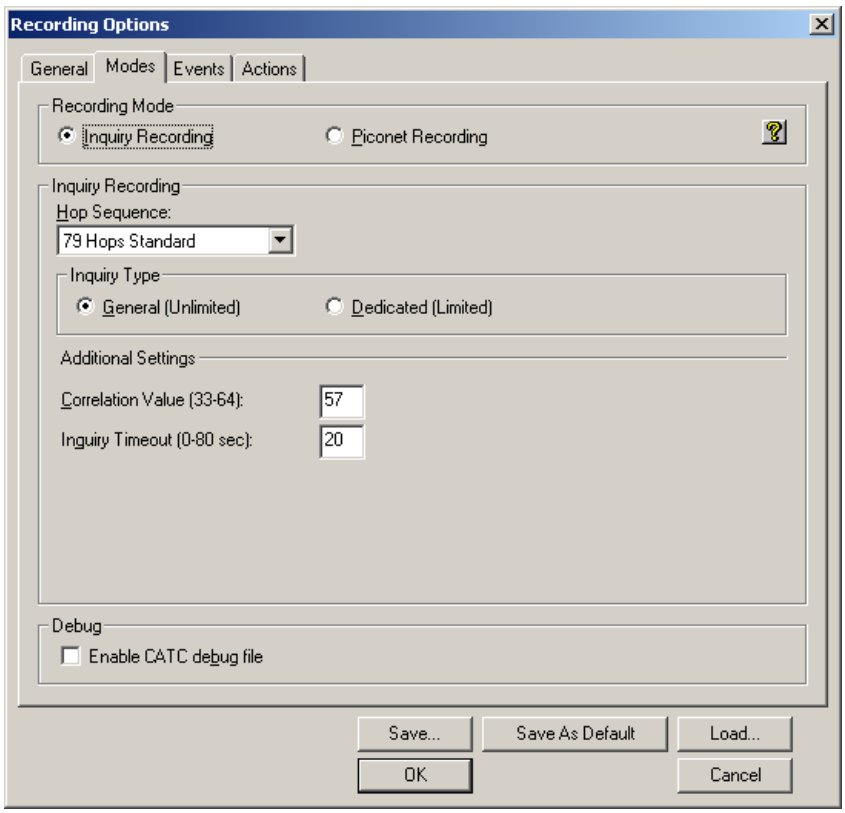
As an example, if the buffer size is set to 16MB, then for the following Trigger Position settings, the amount of pre- and post-Trigger data is

- 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.

7.2 Recording Options - Modes

The tab marked Modes opens a window for setting recording mode options. This window is divided into six boxes marked Recording Mode, Piconet Addresses, Hop Frequency, Other Parameters, and Debug/Test.



Recording Mode

To record Bluetooth™ traffic, the BTTracer analyzer needs to synchronize to the piconet under observation. BTTracer 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.

To synchronize to the piconet under observation, BTTracer can be set up in different recording modes: *Inquiry Recording* and *Piconet Recording*. The option you select affects the types of settings that display in the window.

Inquiry Recording

Selecting the "Inquiry Redcording" button causes the Modes window to display the options shown in the previous screenshot.

The "Inquiry Recording" option presents two choices for recording Inquiries: "General (Unlimited)" and "Dedicated (Limited)."

General (Unlimited)

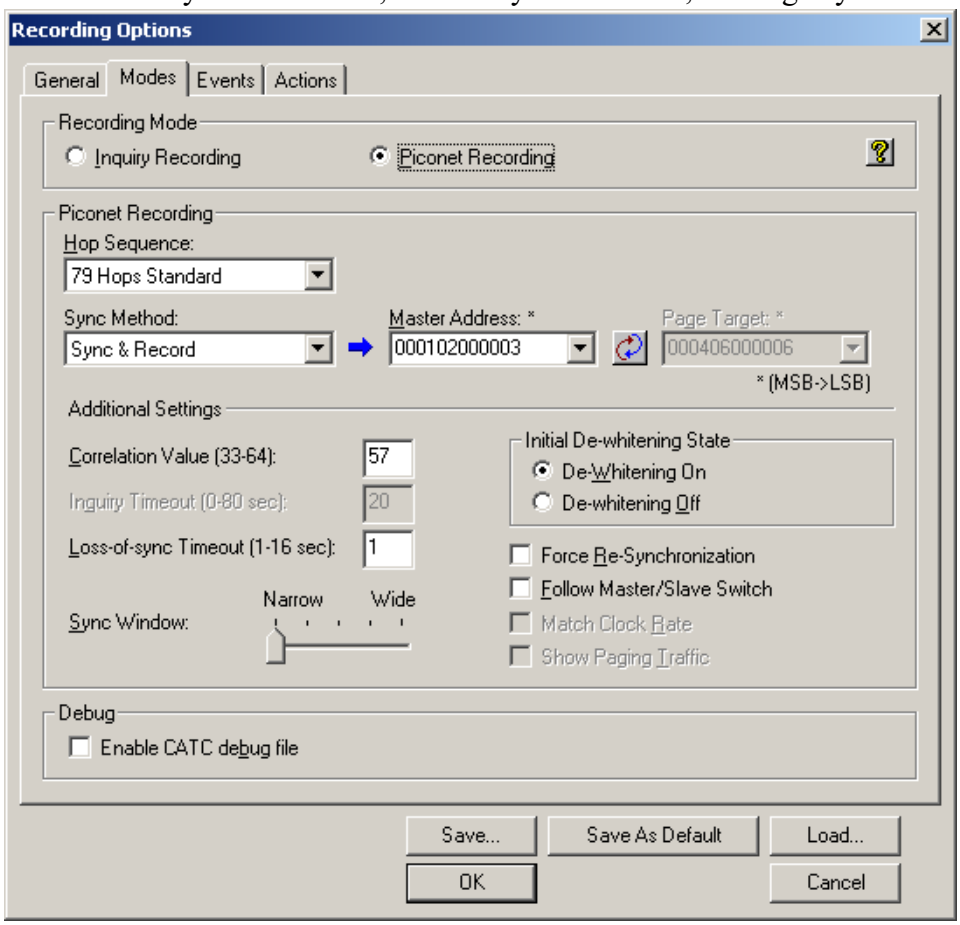
"General" means "General Inquiry" and is used to search for ALL Bluetooth™ devices that are within range, for the amount of time specified in the Inquiry Timeout field. Completion of the inquiry process is indicated by illumination of the "trigger" light on the front of the analyzer. All responding packets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

Piconet Recording

The "Piconet Recording" option presents three choices for recording piconet traffic: Sync and Record, Passive Sync & Record, and Page Sync & Record.



A Help button next to the menu briefly explains these options.

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.

Hop Sequence

Until recently, local regulations in Japan, France, and Spain defined a Bluetooth™ frequency range that was different than the range used by the rest of the world. We have included the selections for organizations for testing of devices developed before all frequencies were made available on a world-wide basis.

To set BTTracer to the correct Hop Frequency, select from the drop-down menu one of the following choices:

- 79 Hops Standard
- 23 Hops Japan
- 23 Hops Spain
- 23 Hops France
- Reduced Hop - Restricts BTTracer 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.
- Single Frequency - Allows the 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 the 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 (+2404) – Allows the setting of the receive signal for the Device Under Test

Sync Methods

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.

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 BTTracer to perform a General Inquiry and collect sync information from the specified slave device when it responds. BTTracer then waits for the Master to begin paging the Slave devices. When paging begins, BTTracer 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 BTTracer perform a General Inquiry. You do this by selecting "General (Unlimited)" from the "Inquiry Recording" drop-down menu on the "Modes" tab in the "Recording Options" window, and then depressing the "REC" button found on BTTracer's toolbar.

Step 3 After the General Inquiry completes, as indicated by the automatic uploading and displaying of a CATC trace (approximately 20 seconds), reselect the "Modes" tab in the "Recording Options". At this point, the addresses of all Bluetooth™ devices that were in range will be listed in the pull-down windows in the "Piconet Addresses" area of this window. Using the pull-down windows select both your "Intended BT Master" as well as your "Intended Slave" address for display in their appropriate windows.

Step 4 After closing this window by pressing the "OK" button at the bottom of the window, once again depress the "REC" button found on BTTracer's toolbar. After approximately 20 seconds, the "SYNC" light on the front of BTTracer will begin to flash, meaning that BTTracer 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.

Step 5 When the piconet is established, the "Sync" light on the front of BTTracer will change from flashing to solid, indicating that BTTracer is fully synchronized to the piconet and is currently recording all traffic within that piconet.

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

Sync & Record

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

Note This mode can only be used to find 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 BTTracer recording by pressing REC icon in the toolbar.

Step 4 When the analyzer is able to Sync up to the Piconet Master Clock, the Green **Sync** LED in the BTTracer front panel will start blinking.

Step 5 Establish connection between the Bluetooth™ devices under analysis.

Step 6 When BTTracer 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, BTTracer enters Inquiry Scan and Page Scan mode and waits for a page from the Master device. When the piconet Master pages BTTracer, BTTracer 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 BTTracer 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 REC button on the toolbar in BTTracer to start a recording session.

Step 6 If necessary, have Master "discover" BTTracer through a General Inquiry.

Step 7 From the Master device, initiate a page to BTTracer's address. This action will enable BTTracer 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, BTTracer 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 BTTracer can take its place in the piconet.

Step 2 Enter the slave's address into BTTracer'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 BTTracer will be able to sync.

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

slave.

Force Re-synchronization

"Force Re-Synchronization" forces BTTracer to re-synchronize at the beginning of each "Page 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 BTTracer 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 BTTracer's data is correct, you can uncheck this checkbox and cause BTTracer to try to use the existing data. If the data is incomplete or incorrect, however, BTTracer will automatically perform a refresh.

To examine BTTracer's Bluetooth™ data, open "BT Neighborhood" under the View menu.

Follow Master/Slave Switch

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

BTTracer is able to follow a role change by listening to the Slave device's Bluetooth clock and hop frequency as soon as it becomes a Master.

Match Clock Rate

Match Clock Rate is a useful option if the Master device's clock is inaccurate. Match Clock Rate causes BTTracer to do a General Inquiry to determine the Page Target's clock rate prior to synchronizing to the piconet. If unchecked, BTTracer 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 BTTracer to capture paging traffic between the Master and Page Target devices. This option is used only with Page Sync and Record Mode.

Piconet Addresses (MSB -> LSB)

- **Master Add**r - Piconet Master Address for device under observation. Used for all Piconet recording modes.
- **Page Target** - User selectable address for the BTTracer Analyzer. Used for Passive Sync & Record and Page Sync &

Record.

- **DIAC LAP**- Device Inquiry Access Code. Used for Device Inquiry.
- **Swap** - The "swap" button swaps the addresses between the Master Addr and Page Target text boxes. This button will allow addresses to be swapped even if the boxes are grayed out.

Note GIAC - General Inquiry Access Code is hard-coded in the analyzer and does not require user selection.

Other Parameters

Correlation Value (33-64)

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

Inquiry Timeout (0-80 secs)

Default value is 20 seconds.

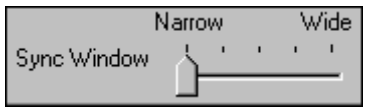
This value specifies how long BTTracer should perform the Inquiry process for the General (unlimited) and Dedicated (limited) recording modes. After the specified time has elapsed, BTTracer will illuminate the trigger light on the front of the analyzer.

Loss of Sync Timeout (1-16 secs)

This value specifies the amount of time that BTTracer 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 BTTracer 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 BTTracer's clock and that of the Master, BTTracer 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, BTTracer will remain in sync as long as there is piconet traffic.

Debug/Test

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.

7.3 Recording Options - Events

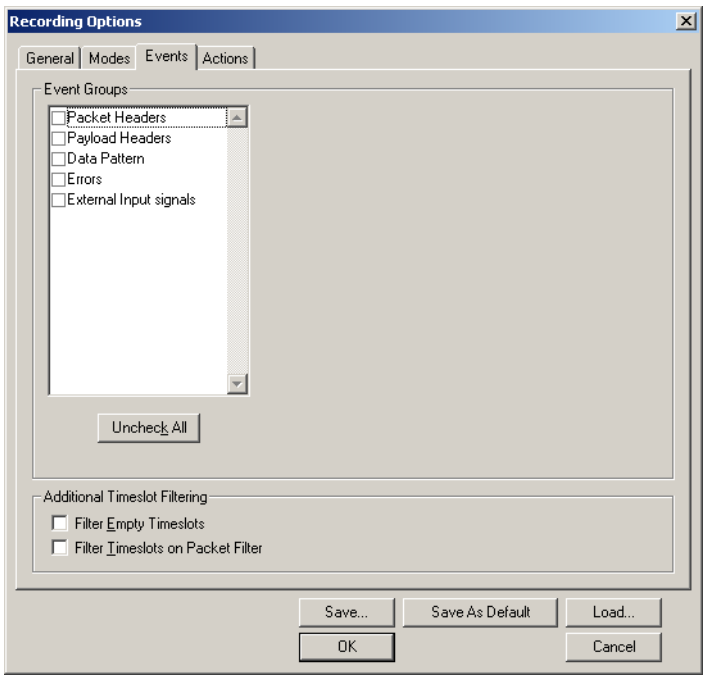
If you have selected **Event Trigger** mode under the **General** tab in the Recording Options screen, you may now select specific Bluetooth™ events using the **Events** tab on the **Recording Option** Screen. You can also use the **Actions** tab to define specific event sequences that will trigger BTTracer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

Events Options

- 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, BTTracer 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, BTTracer 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, BTTracer 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

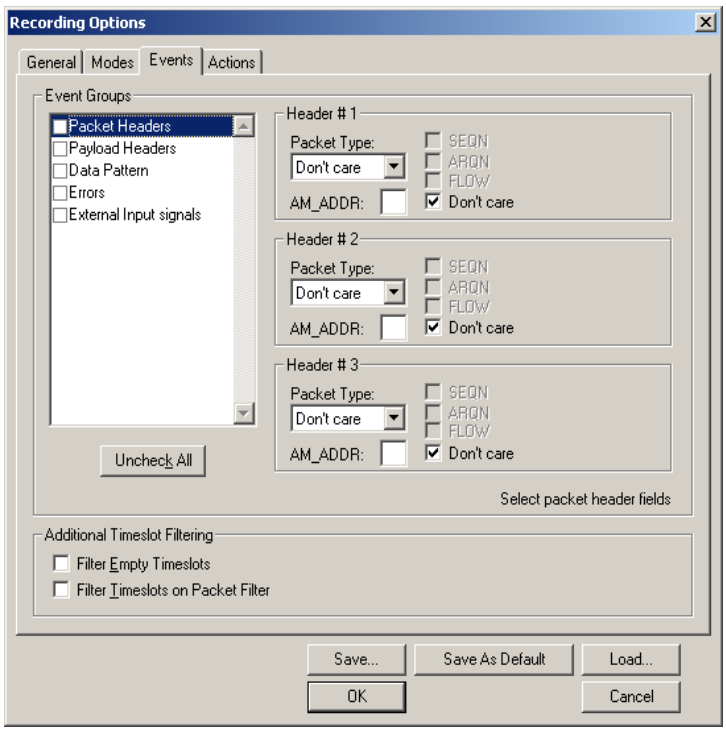
If filters are used to exclude FHS, DM1 or other packets, BTTracer will exclude these packets from a trace and mark their locations with empty packets. The result can be rows and rows of empty packets. The option "Filter Empty Slots" will not exclude these empty slots because they lie immediately in 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 BTTracer 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.

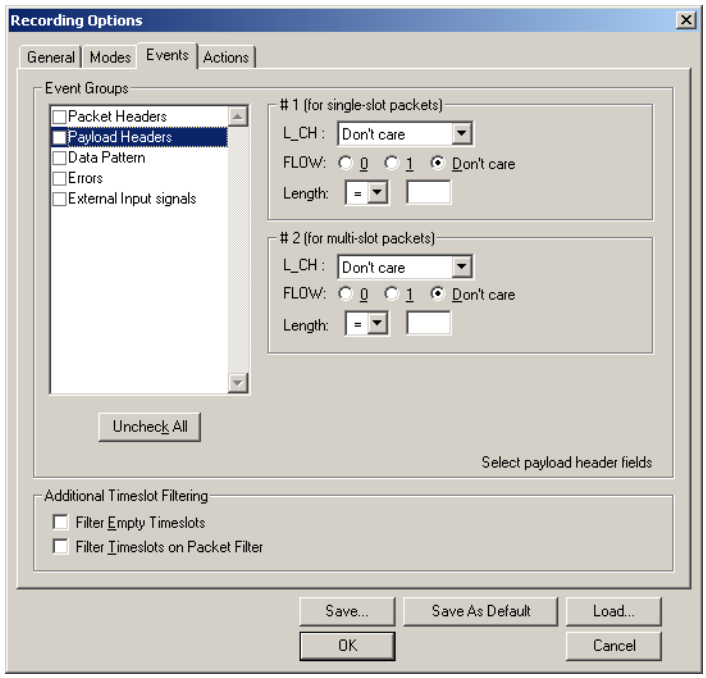
To cause BTTracer to ignore this set of check boxes, choose "don't care."

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."

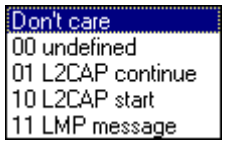
- Select **Payload Headers** under **Event Groups.**

  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:



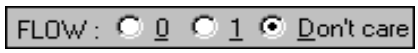
- Don't care
- 00 Undefined

- 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 Flow control:



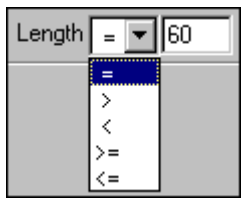
- 0
- 1
- Don't care

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.

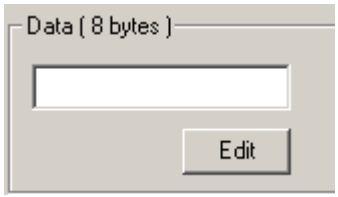


The drop-down menu gives you options for selecting operators such as "greater than" and "equal to." The text box to the right of the drop-down menu lets you enter values.

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 hexidecimal bytes can be entered.

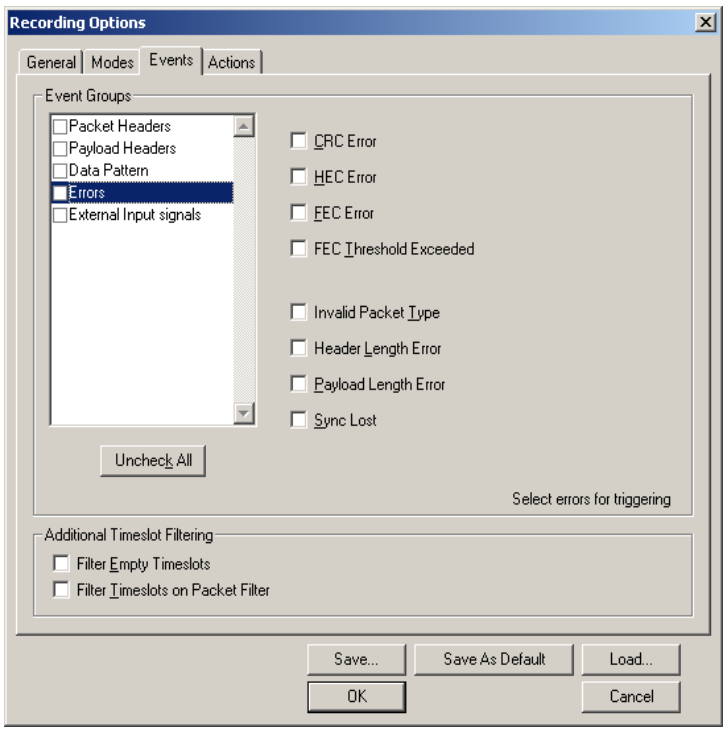


Errors

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.

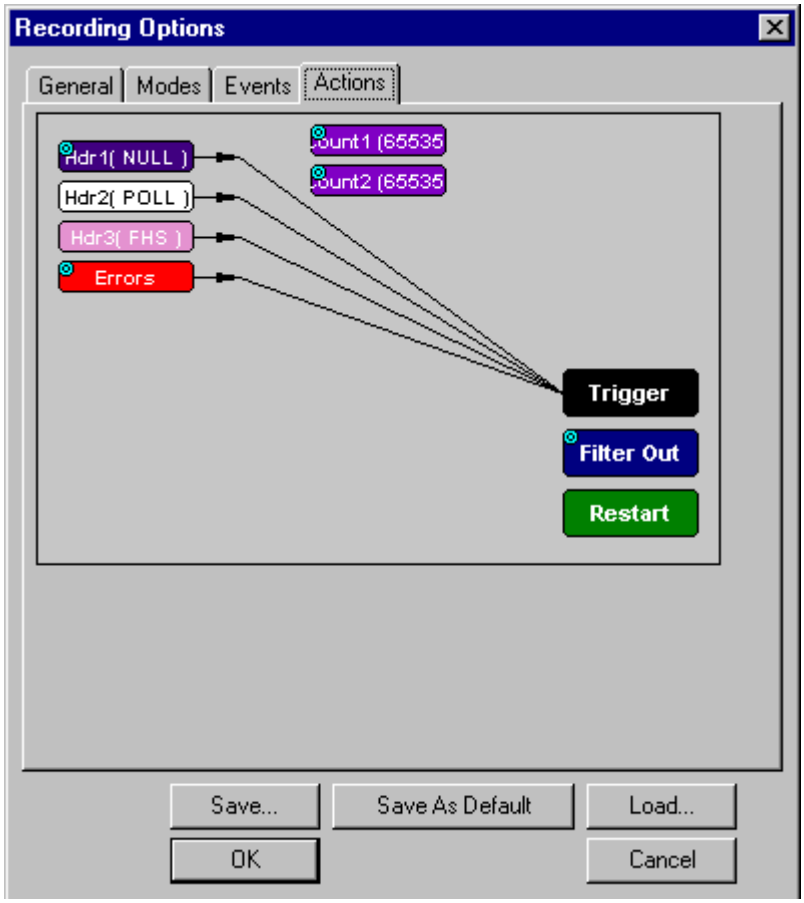
External Input Signals

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:

- Trigger Input [TRIG IN]
- General Purpose Input [G.P. IN]

7.4 Recording Options - Actions

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



Actions Window Layout

The Actions window divides into three sections: a left, a center, and a right section.

The left section displays **Event** buttons such as Header buttons and Error buttons. The number of **Event** buttons displayed depends on the number of Events you selected in the **Events** window. If you selected no Events, no **Event** buttons will display. If all Events were selected, eight **Event** buttons will display.

The center section displays two Counter buttons marked **Count1** and **Count2**. These buttons are used for counting events and are permanent features of this section.

This center section can also hold **Event** buttons such as **Errors** and **Payload Hdr1**. Event buttons in this section are used to create triggers based on a sequence of Events. *Event Sequencing* is explained later in the chapter.

The right section has three permanent buttons for setting actions. These buttons are **Trigger**, **Filter Out/In**, and **Restart**. These buttons allow you to set actions such as triggering or filtering.

Arrows connect **Event, Counting,** and **Action** buttons. Arrows represent the current associations between actions and events. As will be described further on, these associations can be easily changed with the mouse.

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.

Restart

The **Restart** button causes the two counters Count1 and Count2 to be reset to zero.

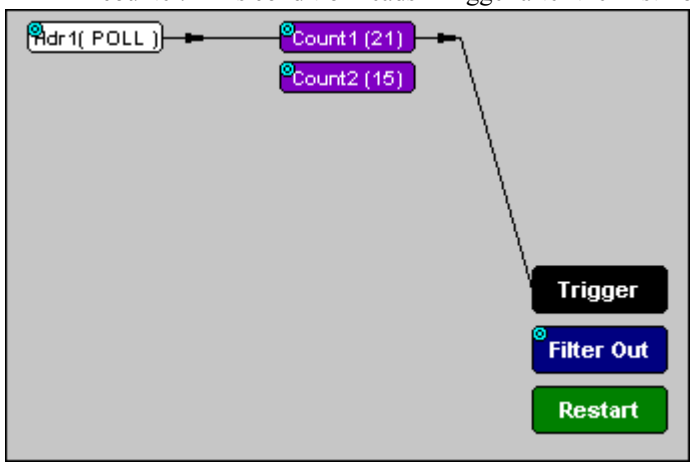
Counting Buttons - Their Functions

The center section of the **Actions** window has two buttons for counting events called **Count1** and **Count2**. Below these buttons, you can add **Event** buttons to create *Event Sequencing*.

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. An arrow will appear that will join the Event to the Counter and then to a trigger.

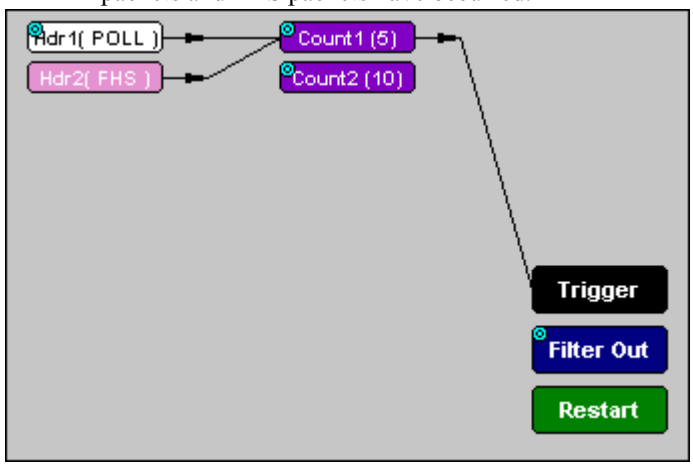
This latter connection between the Counter button and the Trigger button occurs because counters always work in association with triggers. Counters act as assistants to triggers.

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.

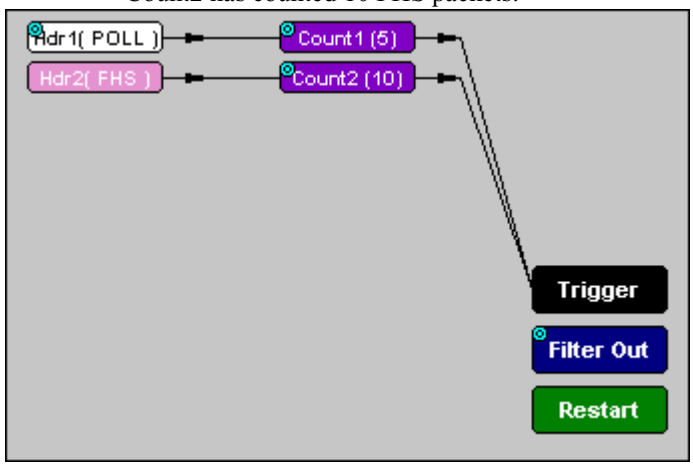
Linking Multiple Events to One Counter - When two or more Events are connected to a counter, it creates a condition that reads "Trigger when the counter value is reached by any combination of the specified events."

The following example reads "Trigger after any combination of 5 Poll packets and FHS packets have occurred."



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 FHS packets."



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.

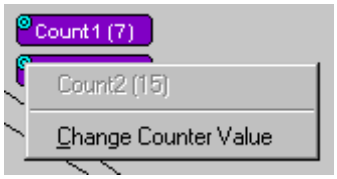
Counters Blue Dot Menu

The **Count1** and **Count2** blue dot menus allow the value of their counters to be changed. The value you specify here tells BTTracer 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,

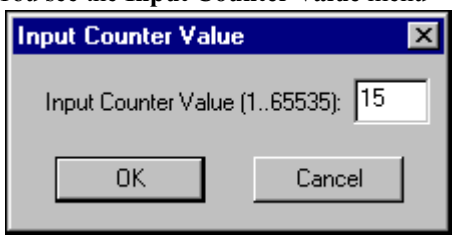
Step 1 Click on the blue dot in the upper left corner of the **Count** button.

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



Step 2 Click **Change Counter Value**

You see the **Input Counter Value** menu

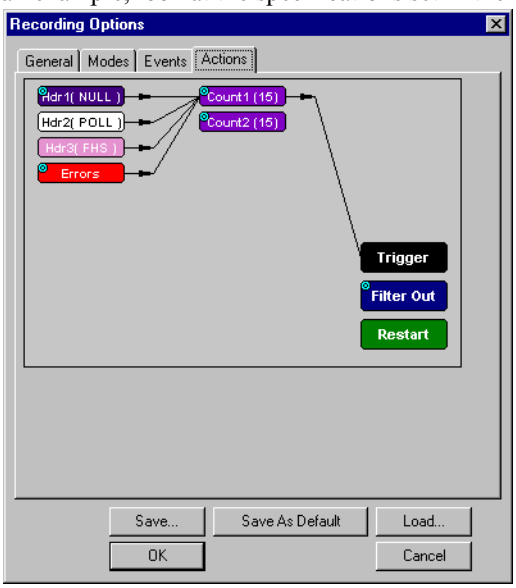


Step 3 Enter an input value to tell the Analyzer how many times this event must occur before triggering the end of a recording

Step 4 Click **OK**.

You may connect as many Event buttons to a counter as you like. However, the Counter does not treat each event as a discrete specification but treats them all as one event.

As an example, look at the specifications set in the following screen:



Counter 1 has been set to trigger four events after 15 occurrences. But the Counter does not count 15 occurrences for EACH event. It counts ALL events as they happen to occur until it reaches a total of 15 and then triggers.

Filter Out/In Blue Dot Menu

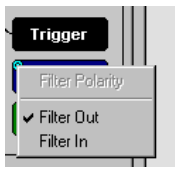
The **Filter Out/In** button toggles between "**Filter Out**" and "**Filter In**".

- **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".

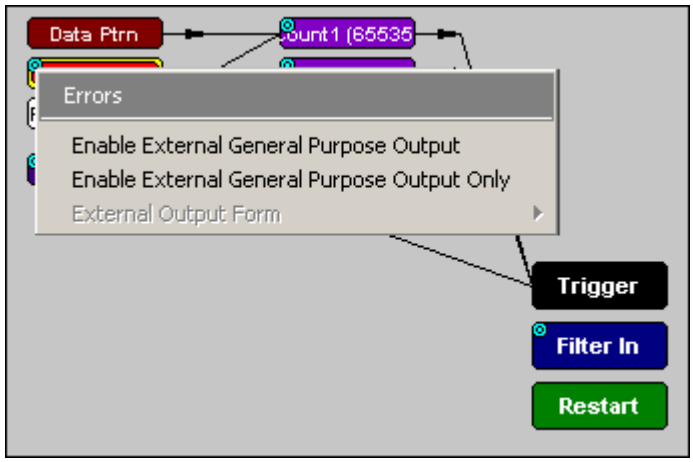
Blue Dot Menus for the Event Buttons

The **Errors** button and the first Headers button (marked "**Hdr1**") have the same Blue Dot menus. These menus allow BTTracer 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.

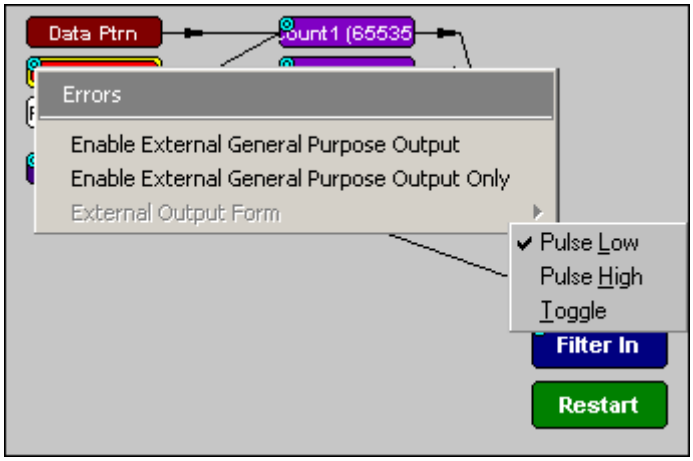
To configure the output signal,

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.

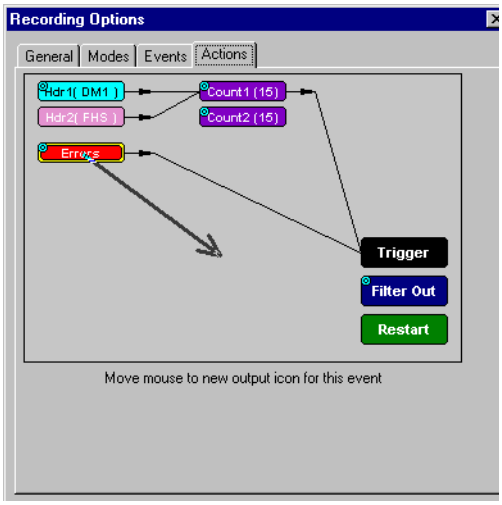
Note that your new selection is now checked.

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.



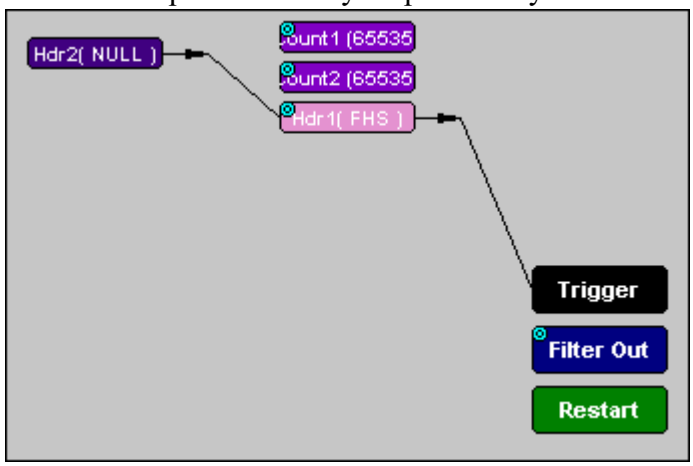
Step 2 Drag the arrow to the desired Action button.

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.



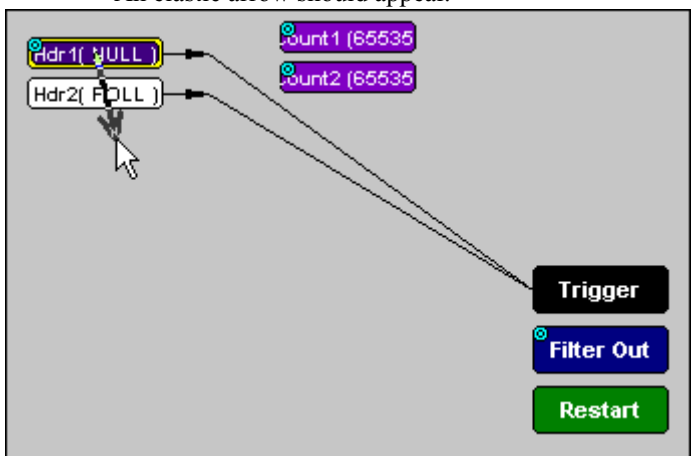
This example means "Trigger when you see a packet with an Null Header followed by a packet with a FHS Header."

To create an event sequence, perform the following steps:

Step 1 Select two events from the Events window

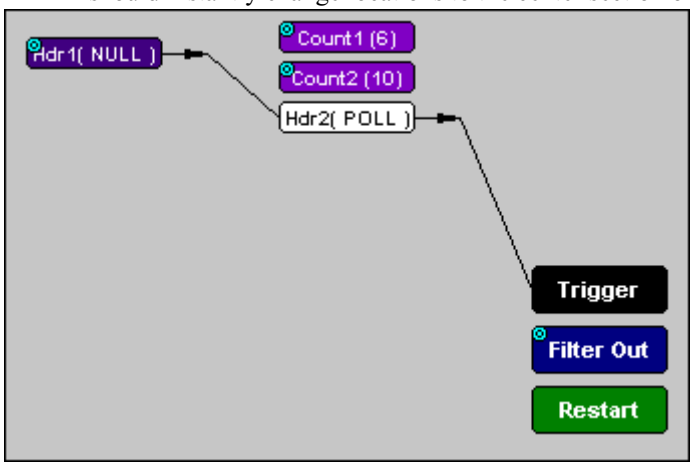
Step 2 Open the Actions window and click on one of the two Event buttons.

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.



7.5 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.

7.6 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.blt** or whatever name you assign as the default filename.

To save a current recording for future reference,

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

OR

Click on the Tool Bar.

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

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

8. Display Options

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

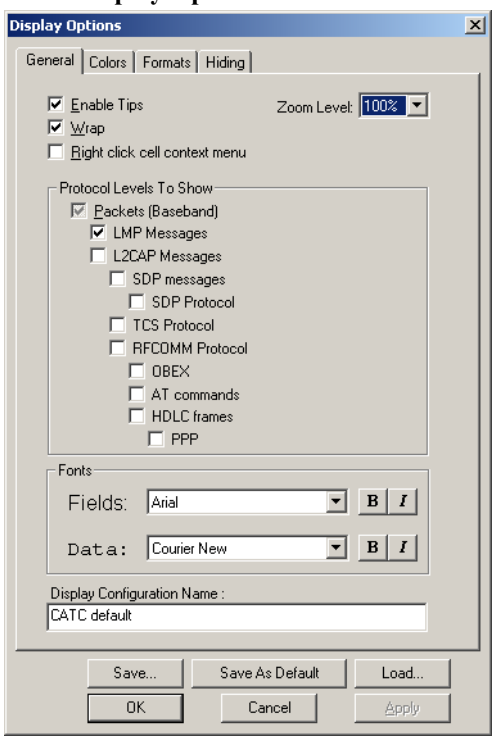
To open the **Display Options** menu,

- Select **Display Options** under **Setup** on the Menu Bar

  OR

- Click on the Tool Bar

  You see the **Display Options** window:



The **Display Options** window always opens with the screen for the **General** tab displayed.

8.1 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 Tool 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**: Inhibits carriage returns in packets when they exceed the width of the window.
- **Trace Viewing Level**: Enables different levels of transaction to be displayed.
- **Display Configuration Name**: A 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.
- **Fonts:** Allows field fonts and data fonts to be changed. The fonts can be italisized and/or bolded by pressing the **I** and/or **B** buttons.

Trace Viewing Level

Trace Viewing Level allows BTTracer to display ten levels of transaction:

- **Packet**
  Packet is the default selection.
- **LMP Messages**
- **L2CAP Messages**
- **STP Messages**
- **STP Protocol**
- **TCS Messages**
- **TCS Protocol**
- **RFCOMM Protocol**
- **OBEX Protocol**
- **AT Commands Protocol**
- **HDLC Frames**
- **PPP**
- **BNEP**

Changing the Trace View Level

To change the Trace Viewing Level, use the decode buttons on the toolbar or select a checkbox in the **Display Options** dialog box.

For further details on these viewing levels, see the Chapter 7: *Decoding Higher Protocols.*

Creating New Display Options Files

To create a new Display Options file,

Step 1 Enter a comment for the new file in the **Display Configuration Name** field.

Step 2 Click **Save**...

You see the **Save As** window.

Step 3 Specify a filename (***.opt**).

Step 4 Click **Save**.

8.2 Color Display Options

- Click the **Colors** tab on the Display Options screen.

You see the **Colors** screen:

Use this menu to customize the colors associated with each field in the Trace View. You can experiment with this option to achieve the color combination best suited to a particular graphic system. A brighter color might be appropriate for a specific field that should stand out in the display (e.g. the Packet Types).

Note The colors of the following packet types cannot be changed: Invalid Data (packet error) field (red) and Softbit Errors (yellow.)

Two color fields are provided for packet number displays to differentiate between pre-Trigger traffic and post-Trigger traffic.

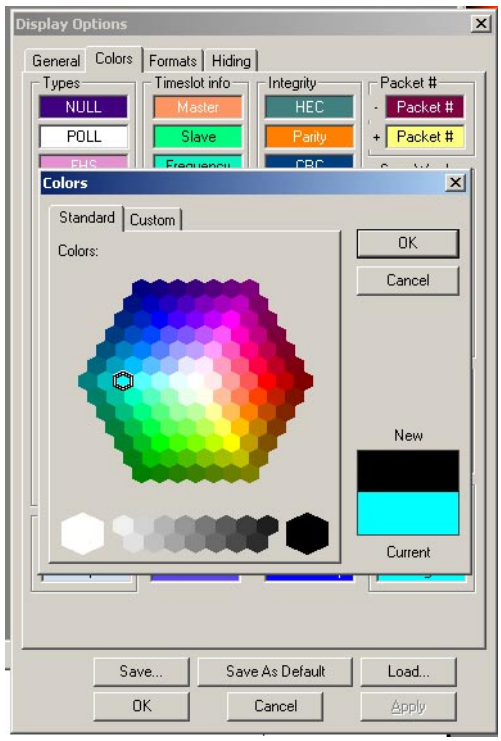
- The packet that causes the Trigger and all the packets before it are colored with the - color.
- The packet that follows a Trigger is colored with the + color.
- All packets are colored with a + color when there is no Trigger.

Use the color buttons labeled + and - under the **Packet #** section of the Colors screen to select a Trigger color.

To select or change a color,

- Click the appropriate color button.

  You see the color palette:

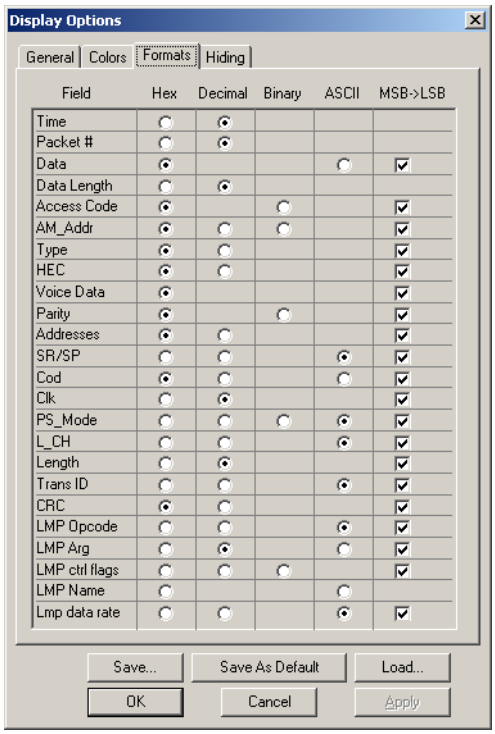


Use this palette to choose the desired color for the Packet Types, Miscellaneous, Integrity, Handshake, Packet #, Access Codes, Data, Idle and Timestamp.

8.3 Formats Display Options

- Click the **Formats** tab on the **Display Options** screen.

  You see the **Formats** window:

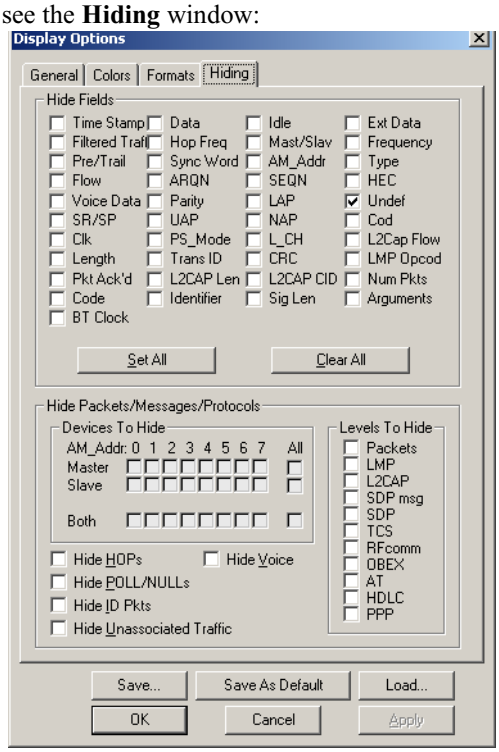


Select a number format corresponding to the column labels along the top of the screen for each number field that labels the rows along the left of the screen. The number format changes in the respective location in the packet view window. You can also select the bit ordering to be displayed. Not every number format is available for every number field.

8.4 Hiding

- Click the **Hiding** tab on the **Display Options** screen.

  You see the **Hiding** window:



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

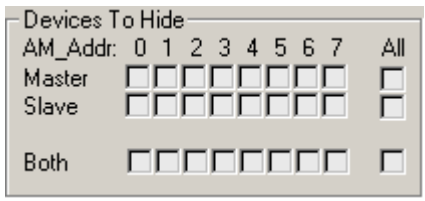
The "Hide Fields" checkboxes allow individual fields to be hidden within a trace. Click the checkbox(es) of your choice to hide one or more fields.

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 devides into columns which represent different devices.



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**.)

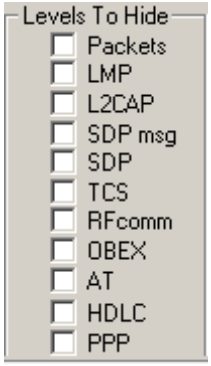
The row in which you place your checkmark determines whether you are hiding traffic going to or from a device.

- 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**.

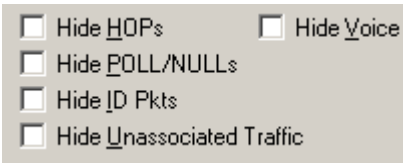
Levels to Hide

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



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.



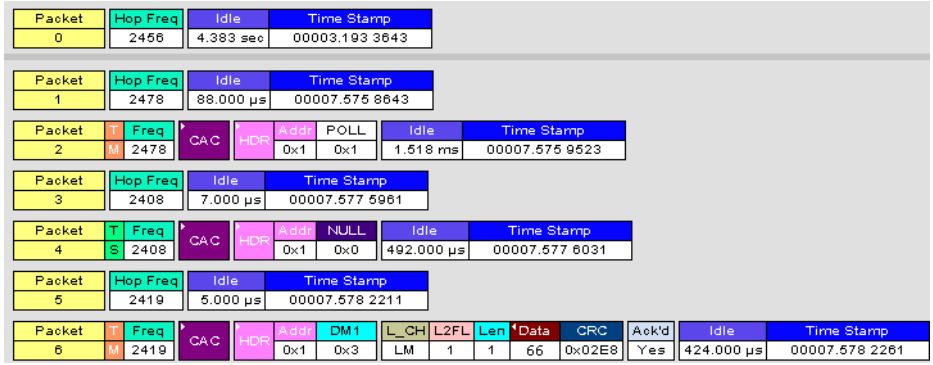
8.5 Saving Display Options

To complete your Display Options settings, use the features at the bottom of the **Display Options** screen. These features remain the same no matter which of the four Display Options screens 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.

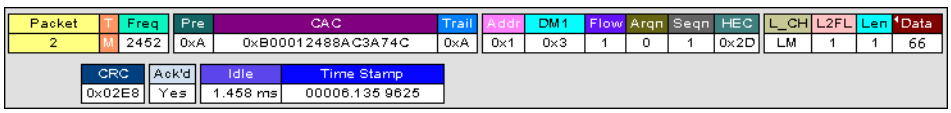
9. Reading a CATC Trace



9.1 Trace View Features

- The BTTracer 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.

9.2 Interpreting the Displayed Information



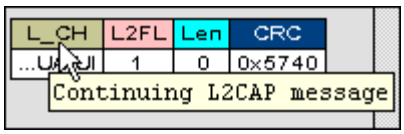
The following table describes the abbreviations used in the Merlin display. Packet #0 is described from left to right:

Packet:#	**Packet/Event Number**
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.

9.3 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.



9.4 Set Marker

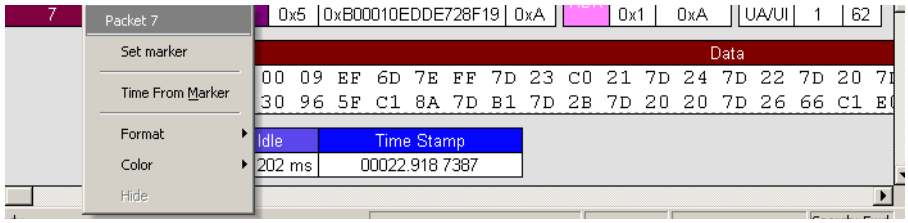
Note The **Set Marker** works in conjunction with the **Go to Marker** feature.

You can define a unique Marker for each packet.

To place a marker on a packet,

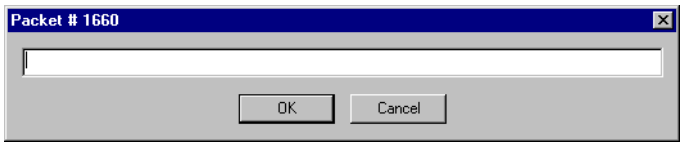
Step 1 Left-click on **Packet #** for the packet you wish to mark.

You see the **Packet** menu:



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**.

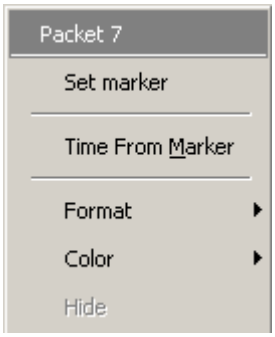
A marked packet is indicated by a vertical red bar along the left edge of the packet # block:

9.5 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.

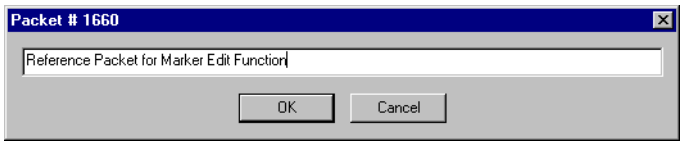
You see the **Packet** menu:



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.

9.6 Expanded and Collapsed Data Formats

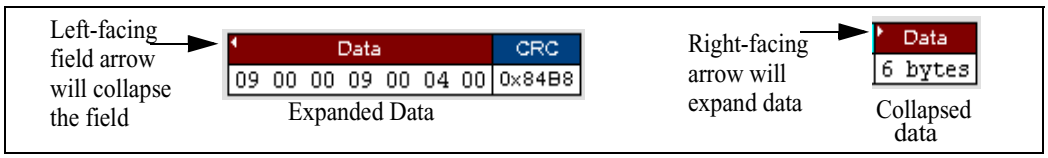
The data field can be expanded to display greater detail or collapsed to a compact view. The Expand/Collapse Data feature operates as a toggle. There are three ways to toggle between the two views.

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.



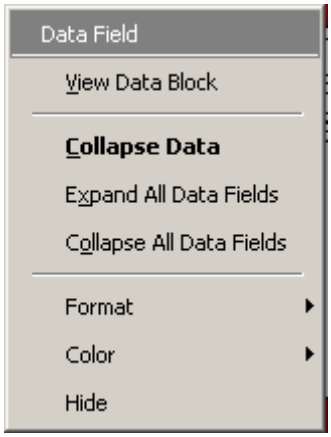
If you click and hold down the left mouse button on one of these arrows, you can collapse or expand the field for *ALL* packets, messages or protocols.

Using the Shortcut Menu

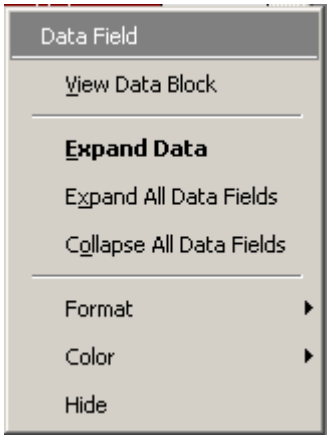
If you left-click on a **Data** field, a menu will open for expanding or collapsing data fields.

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.

9.7 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.

9.8 Hide Nulls and Polls

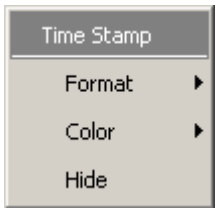
You can hide Nulls and Polls from a trace by pressing the **Hide Nulls and Polls** button on the Tool Bar.

From the Tool Bar

- Click to hide all Nulls and Polls.

9.9 Menus in Clicked Fields

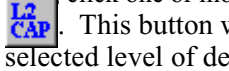
You can display the following menu when you click in a field in a trace.



9.10 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 BTTracer to decode the trace and display selected level of decode.
- Next, click to hide all unassociated traffic.

The **Hide Unassociated Traffic** button will cause BTTracer 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.

10. Decoding Higher Protocols

SDPmsg	T	Addr	PDU ID	Trans ID	ParLength	ServSearchPat	MaxServRecCount	Continuation	Time
0	M	0x1	SrvSearchReq	0xAABB	8	0x1101	8	end	8.314s

SDPmsg	T	Addr	PDU ID	Trans ID	ParLength	TotSrvRecCount	CurSrvRecCount	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	DH1	L_CH	L2FL	Len
1330	S	2429			0x1	0x4	UA/UI	1	18

Data	CRC	Ack'd	Idle
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

Time Stamp
00008.318 8476

10.1 Introduction

BTTracer can decode LMP and L2CAP messages, and RFCOMM, SDP, TCS, HDLC, PPP, and OBEX 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 higher 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, BTTracer can decode these LMP and higher fields and display the data in summary statements called *LMP/L2CAP Messages*, *Protocols Messages, and Protocol Transactions*.

10.2 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 higher protocol data such as RFCOMM, TCS, OBEX or SDP data, the message displays this data in an undecoded format that can be decoded later.

Undecoded higher protocol data

10.3 Decoding and Viewing Higher Protocol Data

Higher 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)
- **LMP** (Display LMP Messages)
- **L2CAP** (Display L2CAP **M**essages)
- **SDP Msg** (Display SDP Protocol Messages)
- **SDP** Tra (Display SDP Transactions)
- **TCS** (Display TCS Protocol messages)
- **RFCOMM** (Display
- **OBEX** (Display OBEX Protocol)
- **AT** (Display AT Commands Protocol)
- **HDLC** (Display HDLC Protocol)
- **PPP** (Display Point to Point Protocol)
- **BNEP** (Display Bluetooth Network Encapsulation Protocol)
- **HID** (Display HID Protocol)

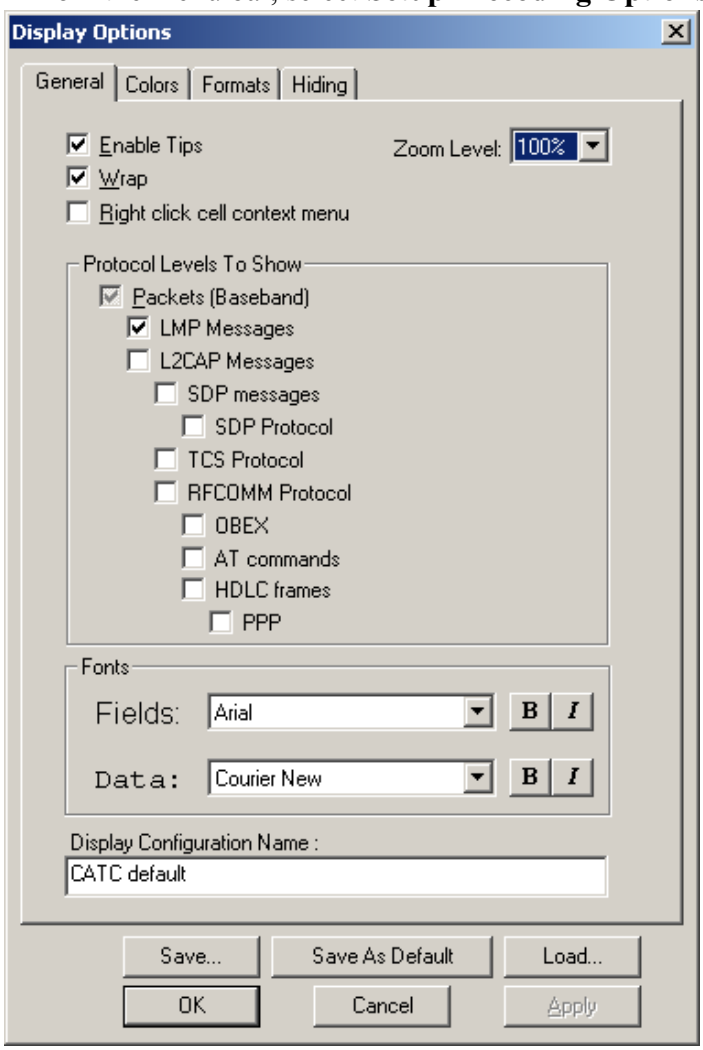
For example, to display LMP messages, click .

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**

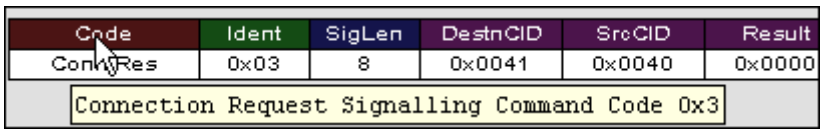


Step 2 Select the option for the desired level of decoding.

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

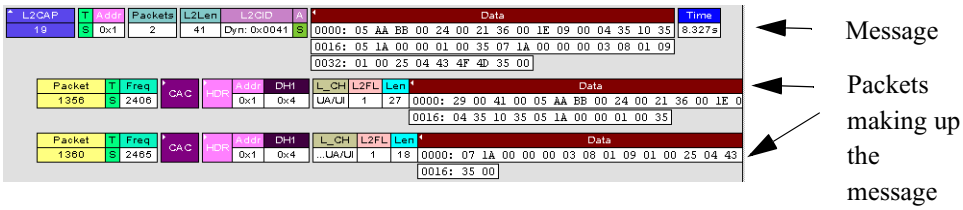
10.4 Tooltips

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.



10.5 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.



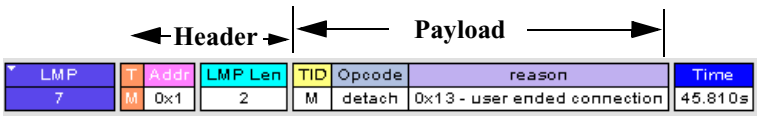
10.6 Types of LMP and L2CAP Messages

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

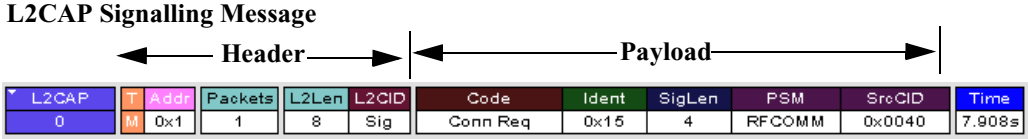
- LMP Signalling Message
- L2CAP signalling Message
- L2CAP Data Transfer Message

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

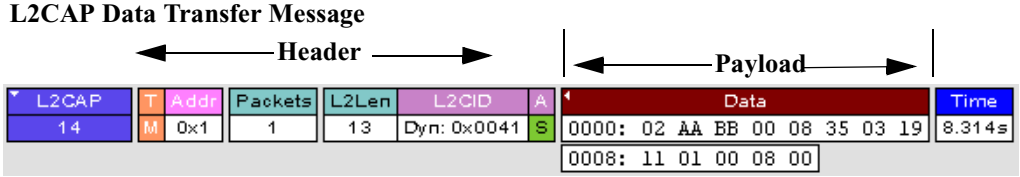
LMP Signalling Message



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 higher 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."

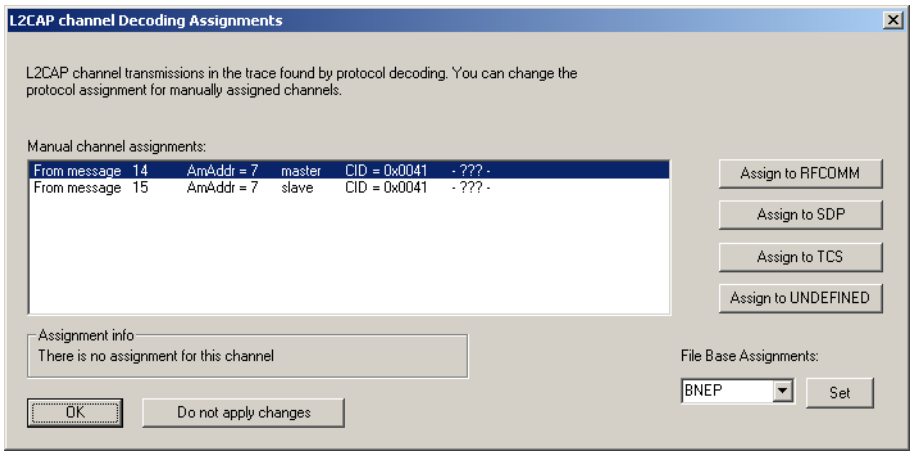
10.7 Viewing L2CAP Channel Connections

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 BTTracer made the channel assignments using data in the trace. You can verify that BTTracer 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 BTTracer performed the channel assignments.

If BTTracer 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.

10.8 Viewing Protocol Messages and Transactions

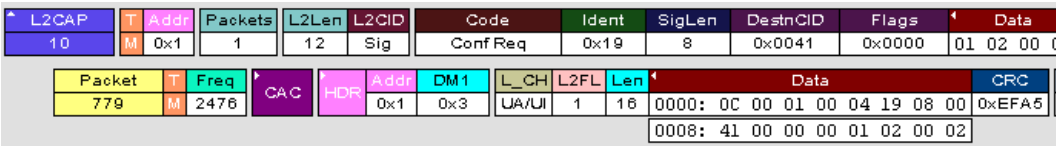
By pressing a button such as SDP Msg or OB EX, you can cause BTTracer to decode the higher level protocol data contained within L2CAP messages and display them as packet-like rows called *Protocol Messages*. Protocol Messages have headers marked "protocol" and fields that vary in appearance and content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

Some Protocol Messages can be grouped into a higher level 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 SDP Tra, BTTracer 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.



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: TCS, PPP, OB EX.

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, BTTracer 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

10.9 Changing Protocol Assignments

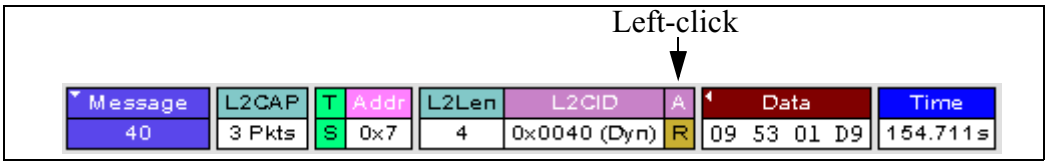
If a sequence of messages is assigned the wrong protocol, errors will display. To change or remove a protocol assignment, you will need to access the **Assignment** menu and issue an Add Assignment command.

Step 1 Click L2 CAP to display L2CAP messages.

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

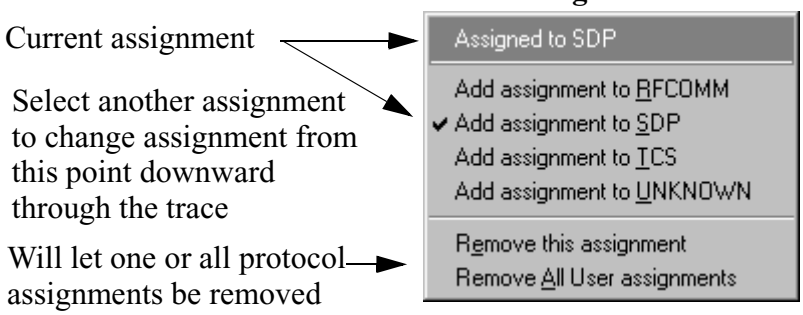
Step 2 Scroll through the trace until you have located an L2CAP message with a field marked "**A**."

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



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.

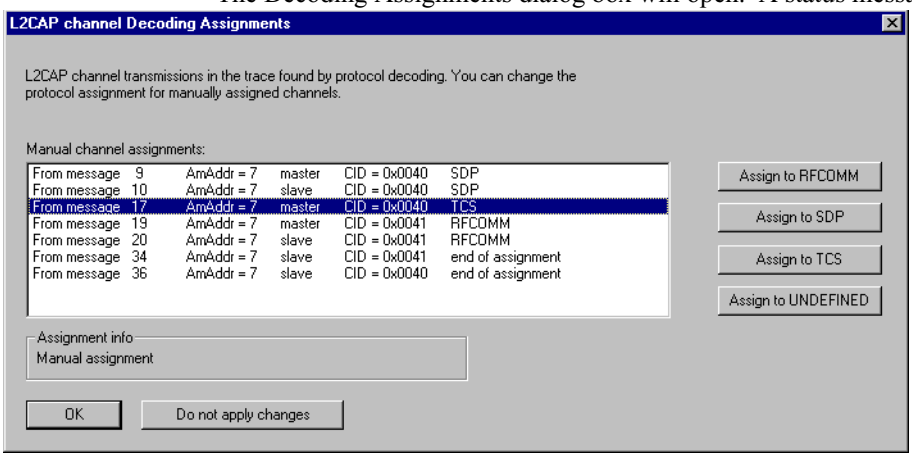
Using the Decoding Assignments Dialog Box

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 BTTracer 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 BTTracer, 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.

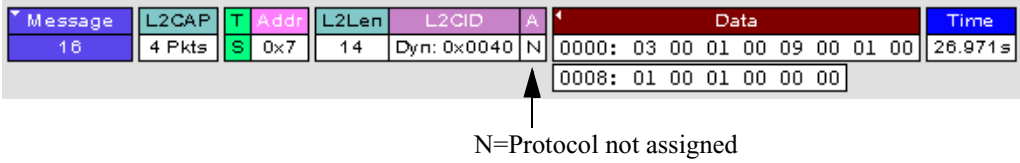
Step 2 Locate a message with a field marked "**A**."

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, BTTracer 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."



N=Protocol not assigned

An L2CAP message without a protocol assignment for the higher protocol data.

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,

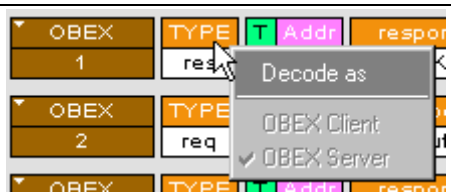
Step 1 Open an OBEX trace file such as the sample file "OBEXsample.blt" in C:\Program files\CATC\BTTracer.

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



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 BTTracer 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 BTTracer 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 BTTracer software. This file tells BTTracer how to decode BNEP fields. Once read, BNEP can be correctly decoded by pressing the BN EP button on the toolbar. If the decode file is not read at initialization, BTTracer 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_BTTracerbluetooth.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 BTTracer what types of HID traffic it will be recording. You do this by editing a script file called *hid.dec*. BTTracer reads this file during the initialization of the BTTracer software. This file tells BTTracer how to decode the HID fields. Once read, HID can be correctly decoded by pressing the HID button. If the decode file is not read at initialization, BTTracer will display the data in an undecoded format.

BTTracer has the capability to decode HID (Human Interface Device profile) based on version 0.90b of the specifications.

11. Other Features

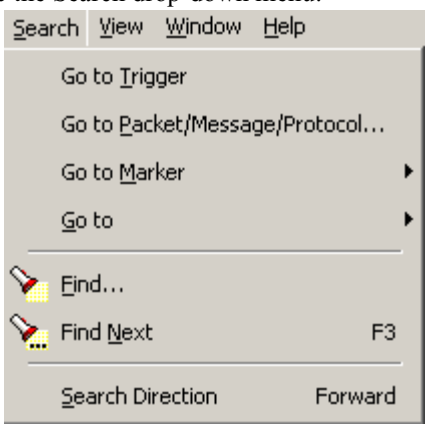
11.1 Search

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

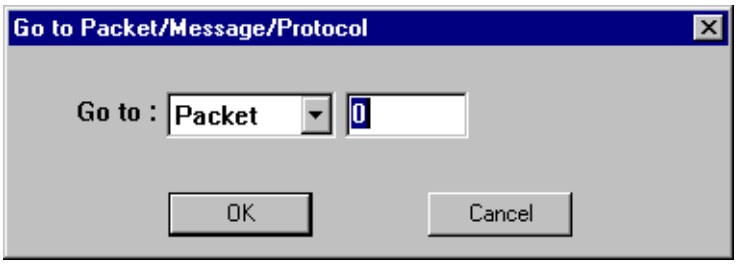
To display a triggering event, select **Go to Trigger** under **Search** on the Menu bar. The **Trace Viewer** display will reposition the trace to show the triggering event at the top of the screen.

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.**

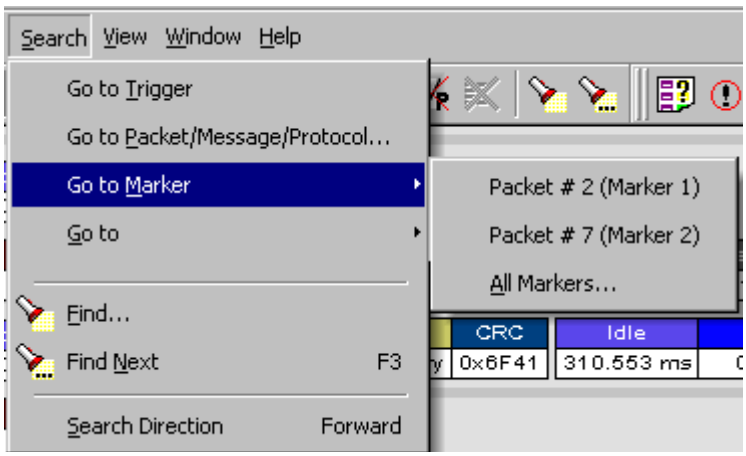
The Trace View repositions to show the packet at the top of your screen.

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.

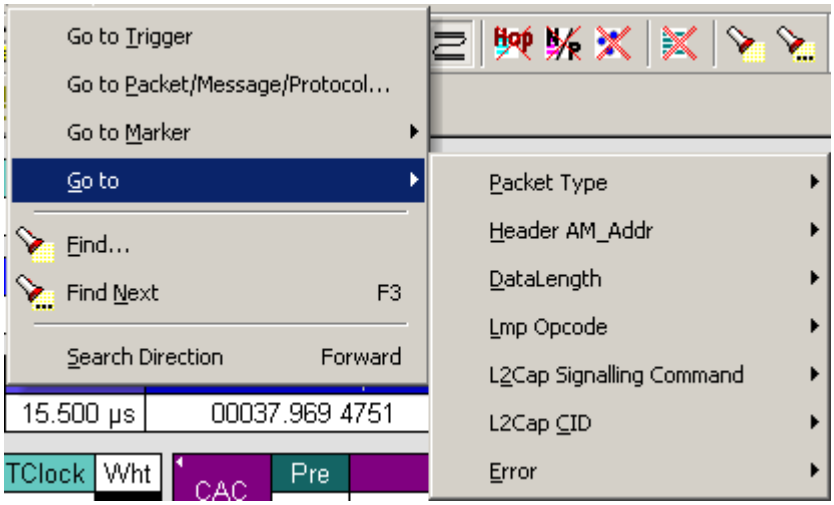
Note The **Go to Marker** feature functions in conjunction with the **Set Marker** feature. The comments within the parentheses following each marked packet are added or edited with the **Set Marker** feature.

Go to

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

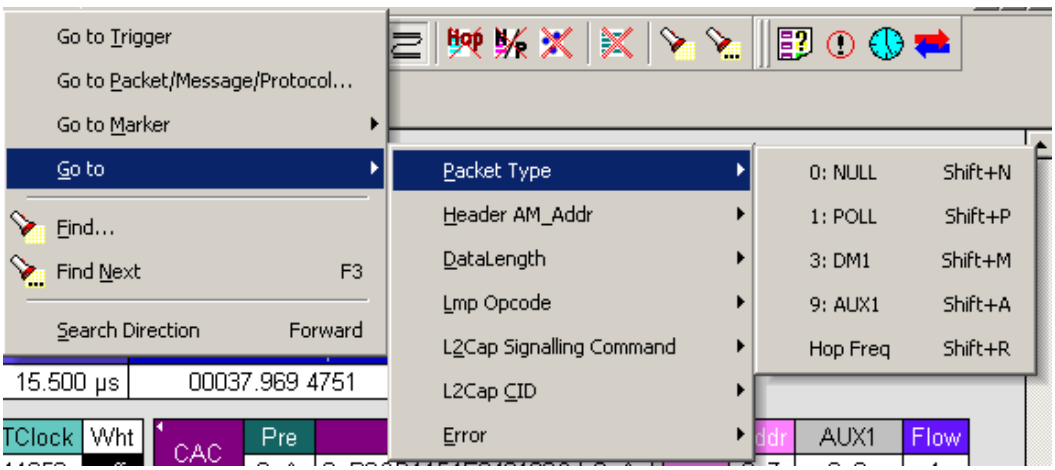
Step 1 Select **Go To** under **Search** on the Menu Bar.

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



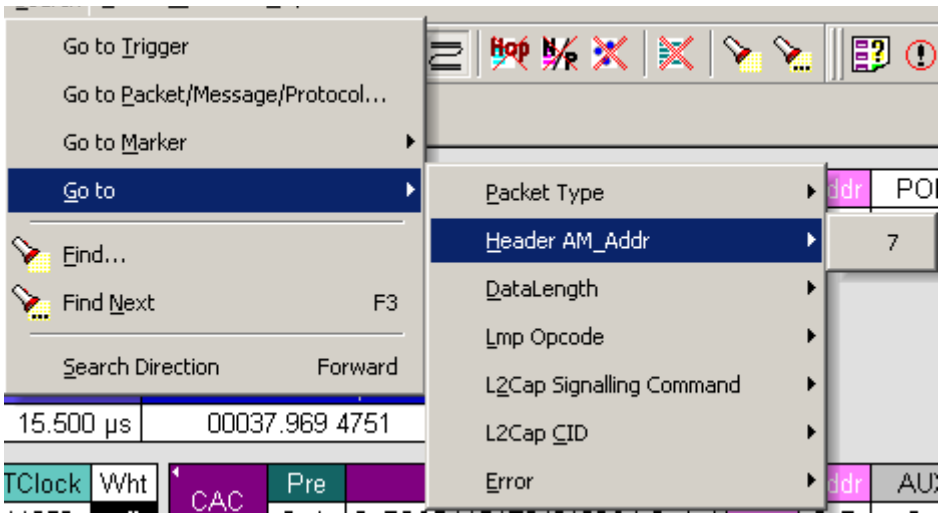
Step 2 Select the event you want to go to and enter the necessary information.

Packet Types



Select the type of packet you want to go to.

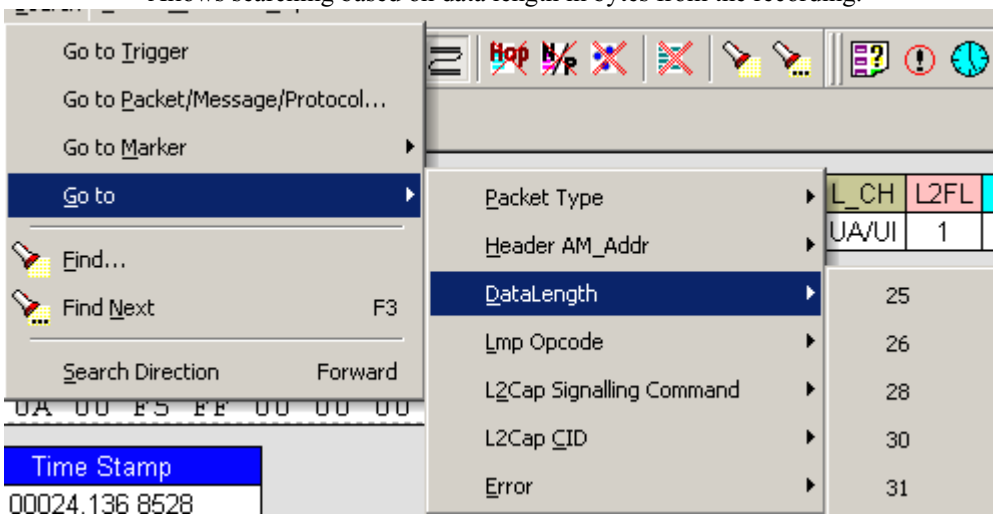
Header AM_Addr



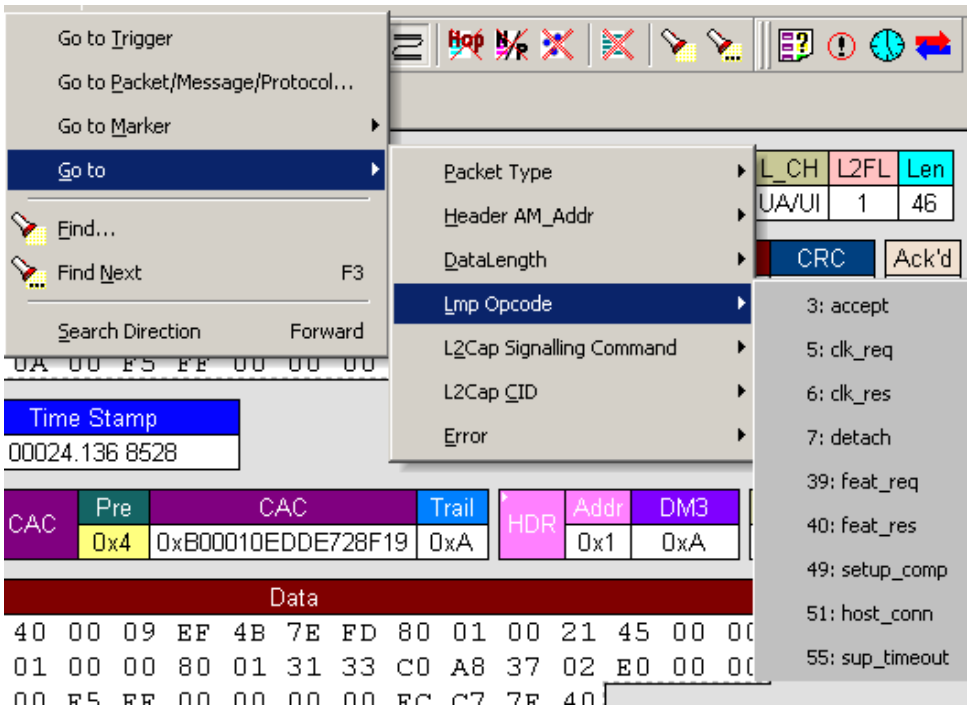
Select an Active Member Address from the list.

DataLength

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

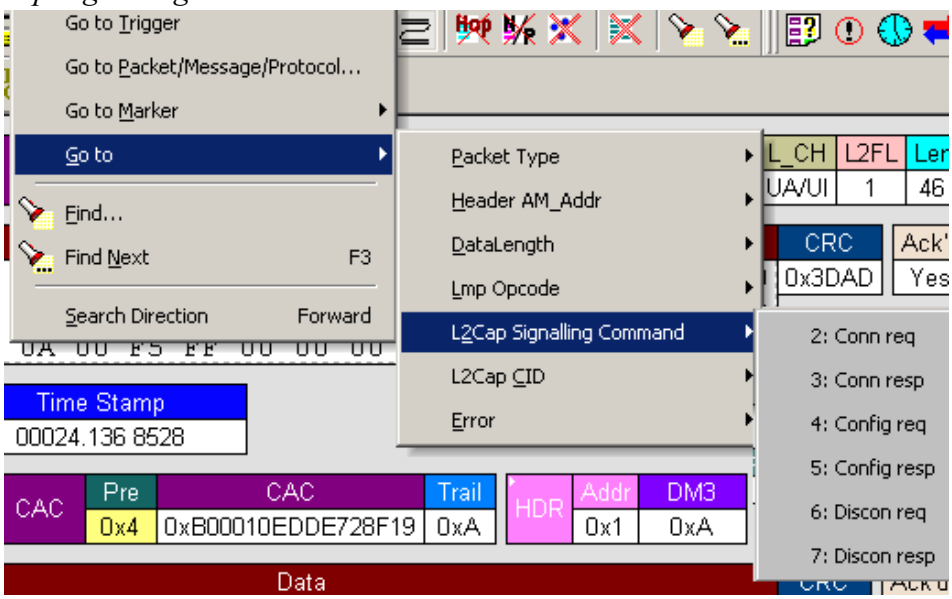


Lmp Opcode



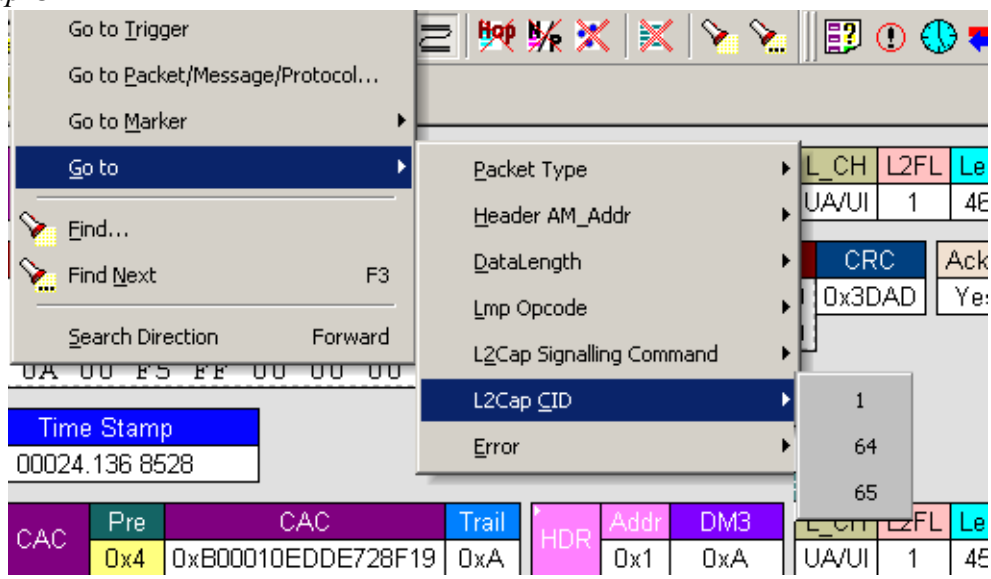
Select the Link Management Protocol Operational Code (Lmp Opcode) that you want to go to.

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 within MBTTracerat 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.

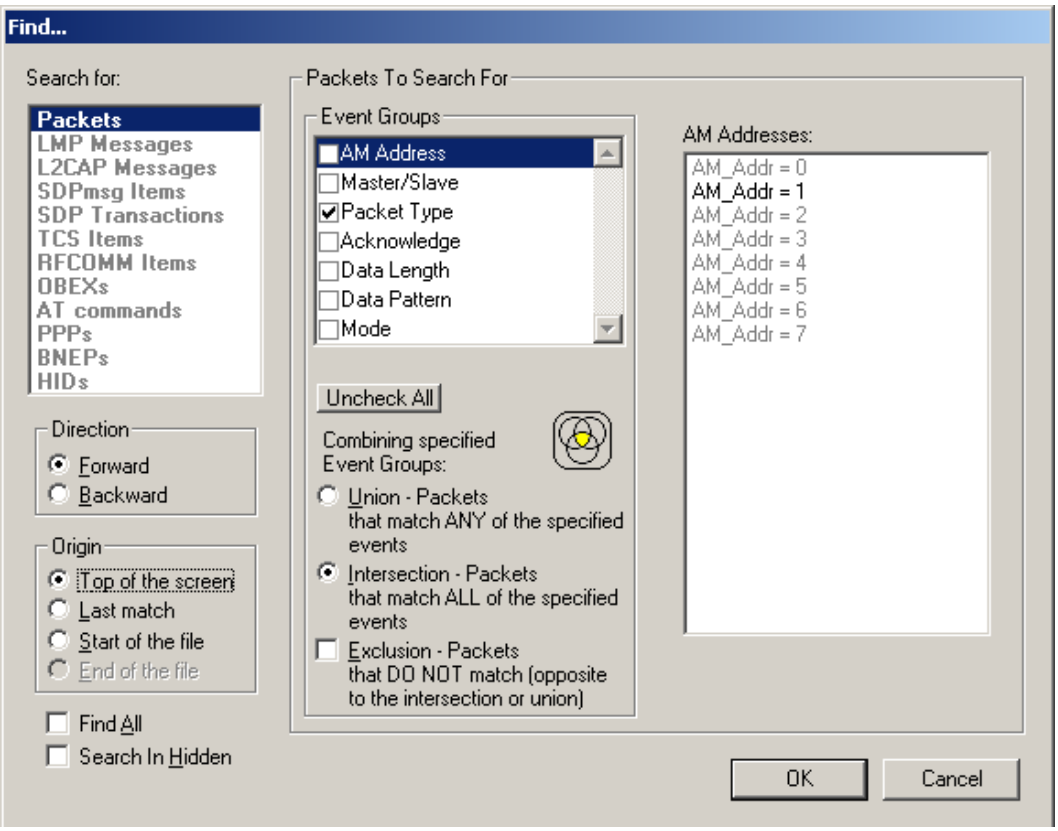
To start find,

- 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 BTTracer 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 NACK**, **Implicit NACK**, 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).

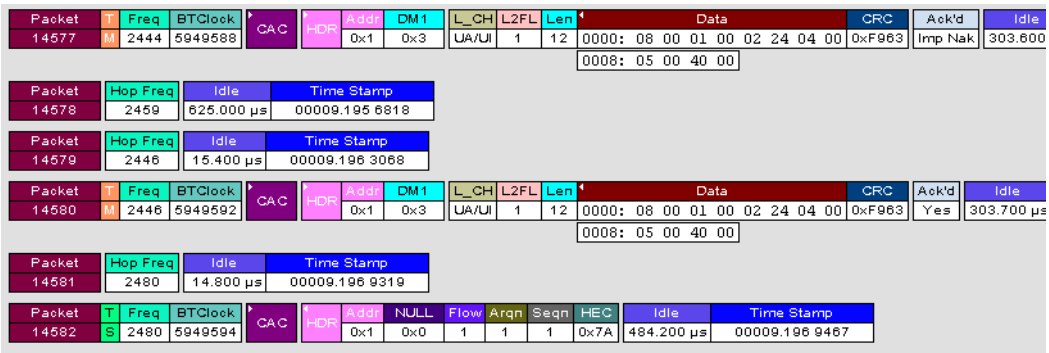
Explicit NACK - Explicitly not acknowledged. An Explicit NACK is an explicit response by a device that it did not receive a data packet. The Explicit NACK is transmitted in the ARQN field (=Acknowledgment Request Negotiation field). ARQN=0 means 'Explicit NACK.'

Implicit NACK - Implicitly not acknowledged. An Implicit NACK is a NACK that is implied rather than explicitly stated. If a device responds to a data packet by sending an empty packet, the NACK 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 BTTracer traces because BTTracer 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	CAC	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 0008: 05 00 40 00	0xF963	Imp Nak	303.600

Packet	Hop Freq	Idle	Time Stamp
14578	2459	625.000 µs	00009.195 6818

Packet	Hop Freq	Idle	Time Stamp
14579	2446	15.400 µs	00009.196 3068

Packet	T	Freq	BTClock	CAC	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 0008: 05 00 40 00	0xF963	Yes	303.700 µs

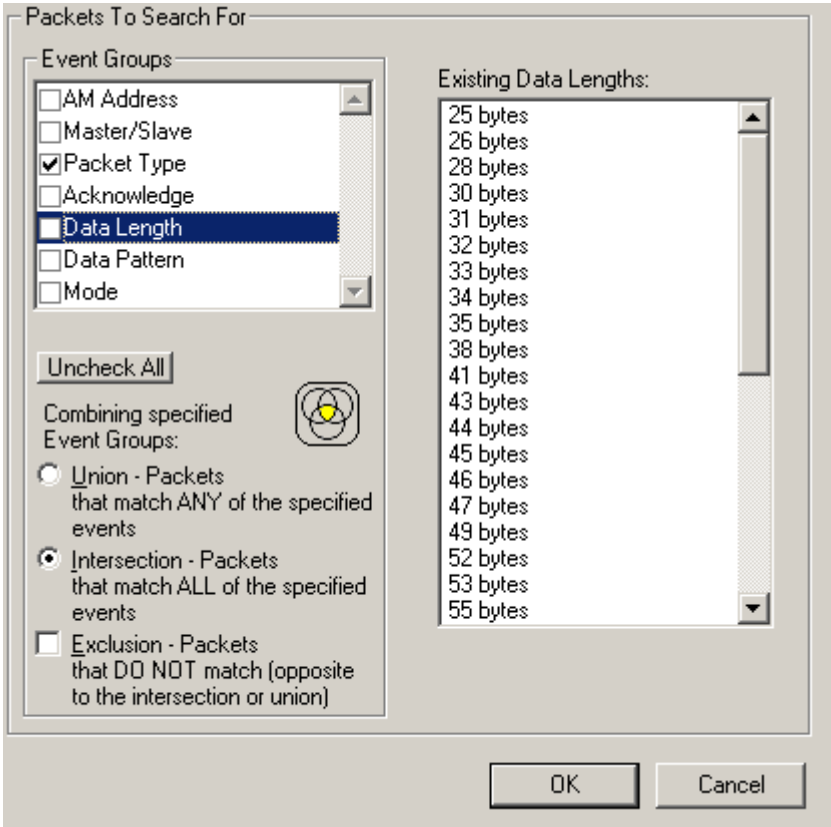
Packet	Hop Freq	Idle	Time Stamp
14581	2480	14.800 µs	00009.196 9319

Packet	T	Freq	BTClock	CAC	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 NACK - 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 NACK** (i.e., implicitly not acknowledged). BTTracer 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**.

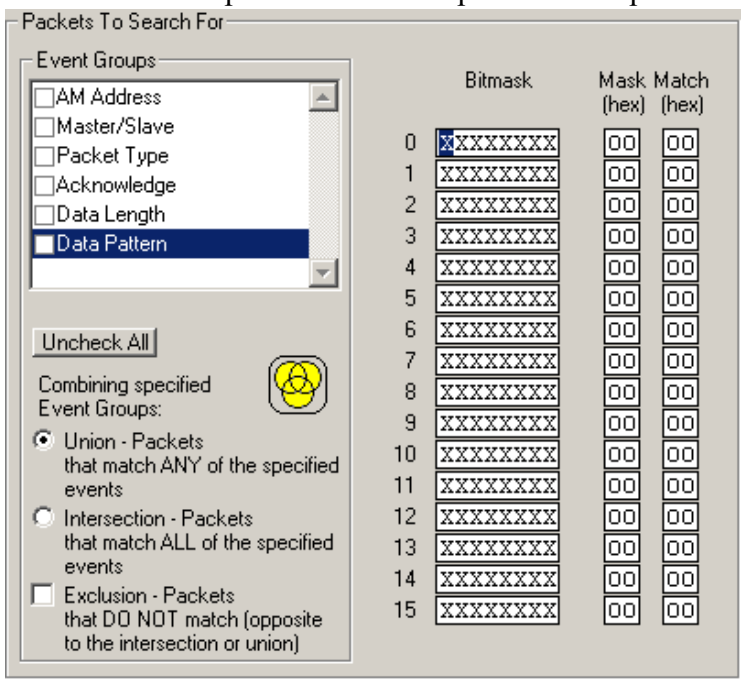
ACK - Packet 14580 is the Master's retransmission of the data sent in packet 14577. Packet 14582 is the reply by the Slave device. This reply contains an ARQN field with a value of (= Acknowledge). BTTracer summarizes this packet exchange by setting the **Ack'd** field on packet 14580 to **Ack**.

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.



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 BTTracer 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	11XXXXXX	C0	C0

Searching for Hexadecimal Patterns

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

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.

Example - A Match of 03 and a Mask of '0F' tells BTTracer 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 BTTracer to exclude packets with any of the specified events.
- **Exclusion + Intersection** -- tells BTTracer 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.

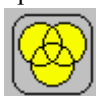
Step 2 Select a search direction and origin.

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.

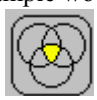
Step 4 If you have selected two or more criteria, then select either :

- **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 cunjunction 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 BTTracer 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

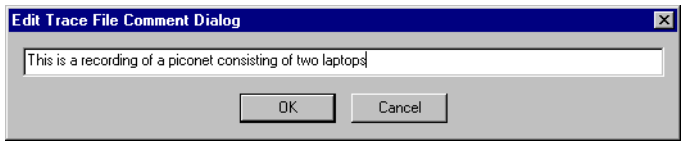
  Click on the Tool Bar.

11.2 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**.

11.3 Reports

The Report menu provides several reports to assist you in analyzing Bluetooth™ traffic recorded by the analyzer.

File Information

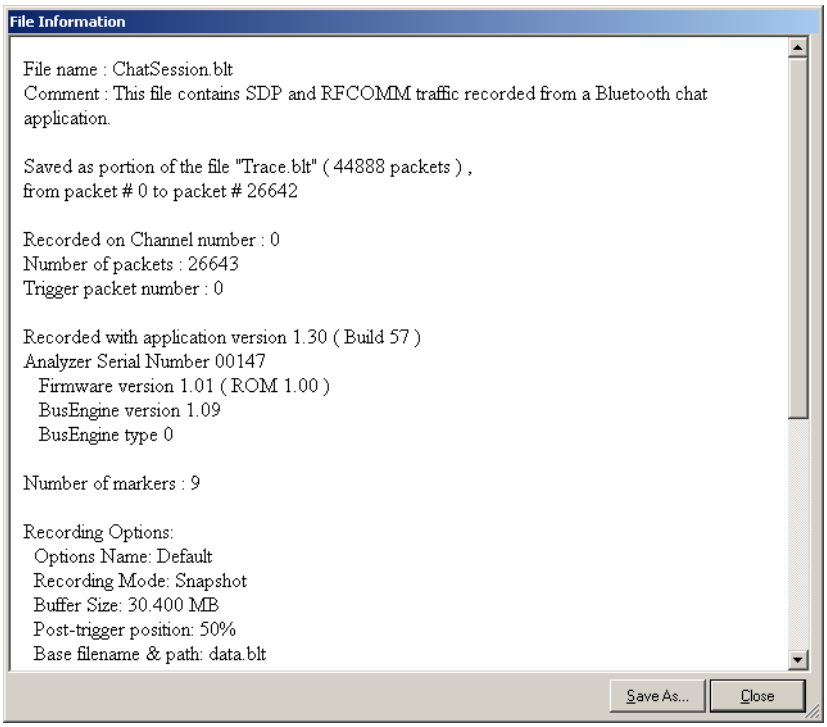
To display a File Information report,

- 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.

Error Summary

The Error Summary command 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 Calculations

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

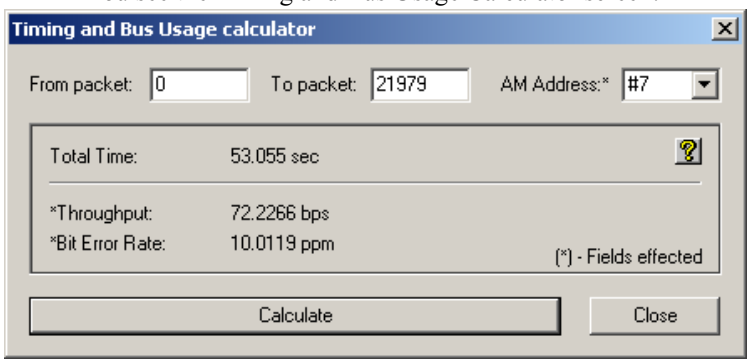
To display a File Information report,

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

  OR

  Click in the Tool Bar.

You see the Timing and Bus Usage Calculator screen:



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."

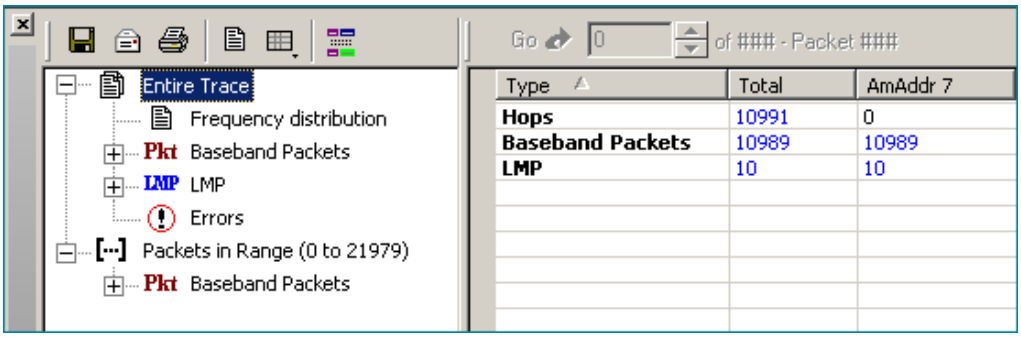
Step 2 If you wish to limit your calculations to a single device, select the device's address from the AM Address drop-down menu.

Step 3 Click the "Calculate" button.

At this point, bus usage will be calculated.

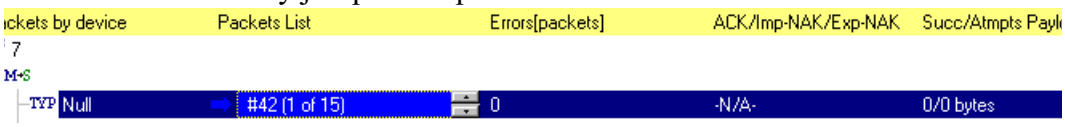
Traffic Summary

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

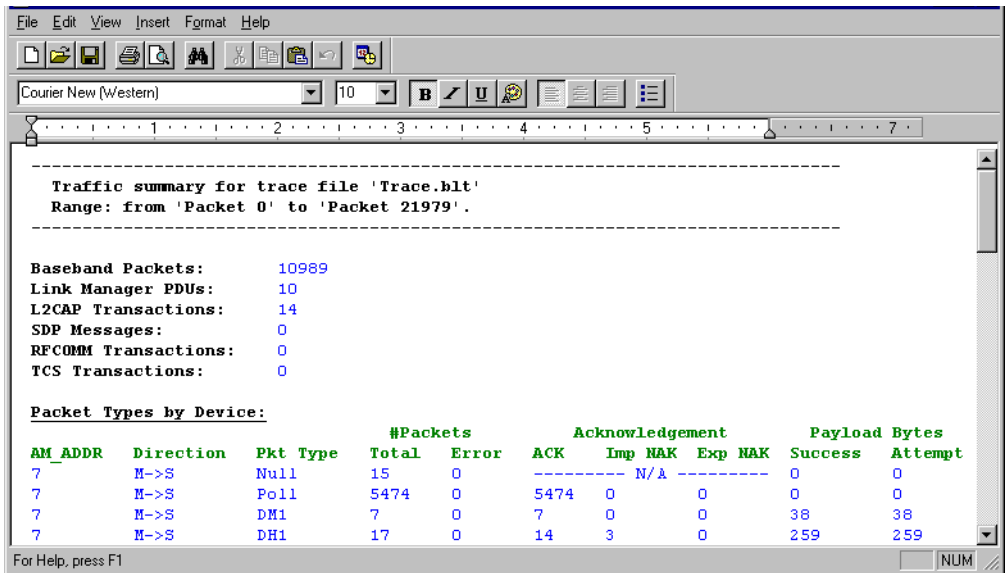


The Traffic Summary window divides into two main sections: a short top section (shown above in the top left corner of the window) that summarizes traffic for each protocol level, and a long section below describing the traffic details for each protocol level.

The second section is scrollable: click on an item below one of the headings to display scroll arrows. The arrows will allow you to scroll through the packets or transactions within that section. As you scroll, the trace will simultaneously jump to the packet or transaction that is listed.

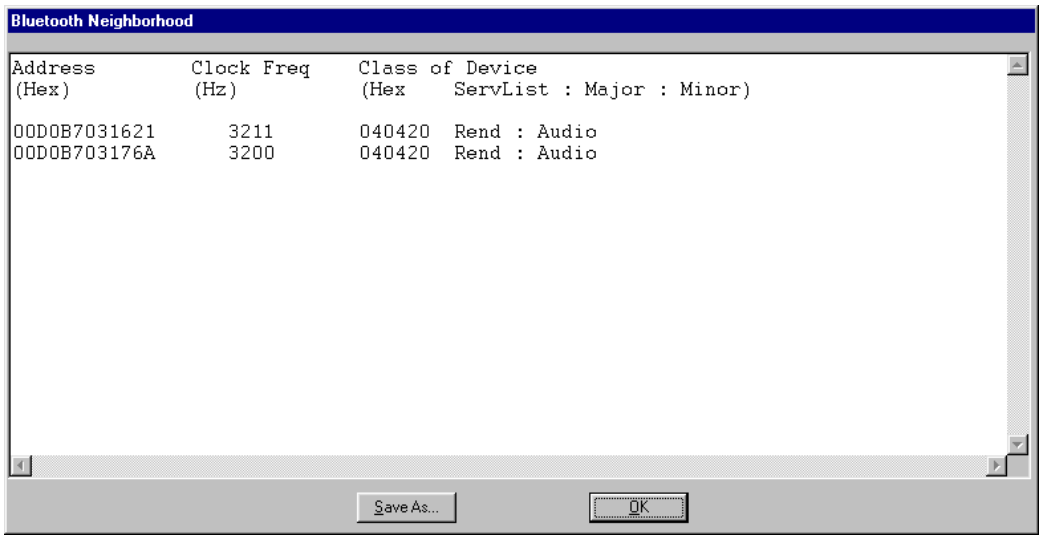


At the bottom of the Traffic Summary window is a button marked "Textual Summary." Clicking this button will cause WordPad to open and display the current Traffic Summary, as shown below. This data can then be printed or saved.



11.4 BT Neighborhood

The BT Neighborhood status box displays information about known Bluetooth™ devices. This command is accessible through the View menu in the menu bar. Three types of data are displayed: Device Address, Class of Device (COD), and the Bluetooth™ Clock Frequency for each discovered device. The expected Bluetooth™ clock frequency is 3200 Hz +/- 250 PPM.



11.5 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 BTTracer 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 BTTracer the PIN for a device

and allow BTTracer to discover the Link Key on its own. Once BTTracer 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 BTTracer for Encryption

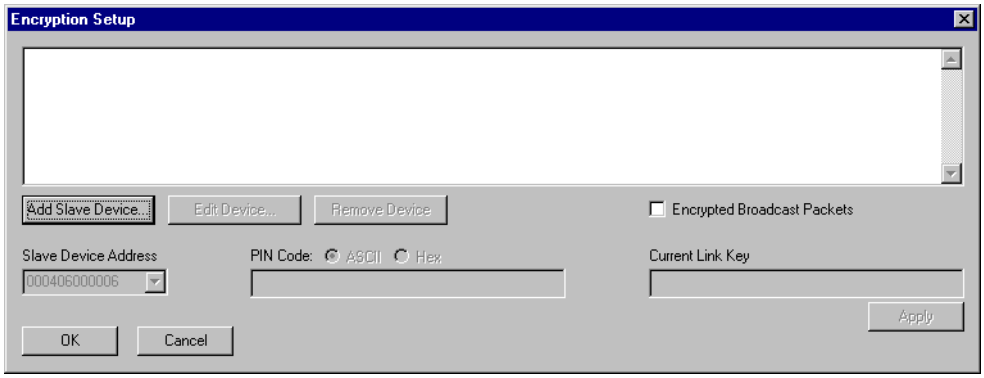
For BTTracer to successfully decrypt traffic, two steps need to be performed: 1) BTTracer needs to be given the PIN or Link Key for each Master-Slave connection; and 2) Recording needs to be begun *before* the Slave connects to the Master. If recording is begun prior to the creating the Master-Slave connection, BTTracer will be able to obtain the encryption key and decode encrypted traffic.

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

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

Step 1 Select **Setup >Encryption Options ...**

The following dialog box opens.



Step 2 Click the button marked **Add Slave Device**.

When you click this button, a list of devices will appear in the **Slave Device Address** drop-down menu.

Step 3 Select an address from the drop-down menu marked **Slave Device Address** or enter the Device Address manually if it is not in the list.

Step 4 Enter the appropriate Personal Identification Number (PIN) for the selected device to the box marked **PIN Code**. This PIN allows BTTracer 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 5 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 BTTracer with the Link Key and not simply the PIN.

Step 6 Click **Apply**

The changes you have made are applied and the information is displayed in the dialog box as shown below. Four fields will display: Device Address, PIN, the Link Key, and Link Key status.

Link Key status may read:

Mstr (=Master unit's Link Key)

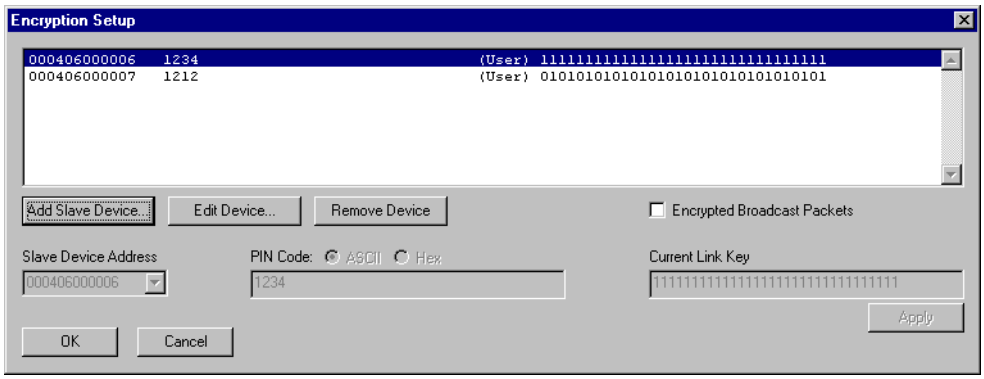
Slve (=Slave unit's Link Key)

Comb (=Combination Key)

Init (=Initialization Key)

Temp (=Temporary Key)

User (=User-defined Key)



Step 7 Click **OK**.

The dialog box closes.

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…	http://www.CATC.com/

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

Numerics

1100 packet 77
1101 packet 77

A

Abort upload 34
About Merlin 21
Acknowledge 128
Action buttons 31, 83
Actions tab 82
Addr 104
Addresses
    AM_ADDR 77
    Bluetooth 54
    piconet 73
    slave device 44
    swap 74
    target 55
AM Address 128
Analyzer
    describing Bluetooth 2
    requirements 17
    set up 9
    status 34
    updates 24
API 4
Application installation 9, 18
Architecture of Piconet 3
Arqn 104
ARQN condition 77
AT 110
AT commands protocol 96
Authentication 139
Automatic updates 24
Automation Feature 4
AUX1 packet 77

B

Basic installation 9
Bit pattern, searching 131
Blue dot menus 85
Bluetooth
    antenna 13
    BusEngine 6
    described 1
    device address 54
    first recording 10
    limited search 67
    neighborhood 139
    recording traffic 92
    search for device 51
    searching for devices 40
    target address 55
BNEP 96, 110
Breakout board 15
BT neighorhood 139
Bubble help 35
Buffer size 10, 65
BusEngine
    automatic updates 24
    Bluetooth 6
    general updates 21, 23
    manual updates 25
Buttons
    counting 83
    toolbar 31

C

CAC 104
Calculations, timing 136
Capturing a trace 20
CATC Technical Support 143
Certification 7
Changing trace view 96
Channel connections, L2CAP 113
Circuits, custom 17
Clicked fields, menus in 108
Clock rate, match 73
Collapse data 106
Colors 97
Comments, editing 135
Components, physical 5
Configuring encryption 140
Connecting events 84
Connectors

data 7, 15
physical 7, 15
Correlation Value 74
Counters
connecting events 84
value 85, 86
Counting buttons 83
CRC 104
CRC error 80
Creating Display Option Files 96
Custom circuits 17

D

Data
connector 15
decoding 110
expand, collapse 106
filename 10
length 79
pattern 75, 79
searching by length 124
searching by pattern 131
transfer message 112
DB-9 15
Debug file 11, 75
Decoding 110
Dedicated inquiry 11
Description of Merlin 2
Detailed installation 13
Device
address 139
Bluetooth address 54
general search 42
hiding 100
inquiry 74
search 40
search for Bluetooth 51
search results 53
slave address 44
DH1, 2, 3 packet 77
DIAC LAP 74
Display configuration name 96
Display options
colors 97
creating files 96
formats 99
general 95
hiding 100
saving 101
Displaying information 103, 135
DM1 104
DM1, 2, 3 packet 77
Drivers, loading USB 18
Duration of search 51
DUT Recv/Xmit Freq 69
DV packet 77

E

Editing comments 135
Enable
debug file 75
tooltips 95
Encryption 139, 140
Environmental Conditions 7
Error summary 136
Errors
CRC 80
FEC 80
header length 81
HEC 80
invalid packet 80
payload length 81
Searching for 126
setting conditions for 80
sync loss 81
threshold exceeded 80
types of 75
Established Piconets 71
Events
conditions 77
connecting 84
options 75
sequencing 90
tab 75
trigger 10, 64
Exclusion search 132
Existing Piconet, recording 49
Expand data 106

Explicit NACK 128
External
    input signals 75, 81
    interface 15
    trigger form 89

F

Features 4
FEC Error 80
FHS packet 77
File information, displaying 135
File menu 29
Filename and data 10
Filter In/Out button 83
Filter Out/In 87
Filtering 76, 77
Find feature, using 132
Finding 126
Finding devices 40
Firmware updates 21, 23, 24, 25, 27
Flow 104
Fonts 96
Force resynchronization 73
Formats tab 99
Found devices 43, 53
France hops 69
Frequencies, DUT 69
Frequency hops, hiding 107
frequency mode 50

G

G.P. OUT 17
General description 2
General features 4
General inquiry 11, 67, 70
General options
    display 95
    recording 63
General purpose output 89
Generating reports 135
Go to
    DataLength 124
    error 126
    Header AM_Addr 124
    L2Cap CID 126
    Lmp Opcode 125
    marker 122
    packet types 123
    packet/Message/Protocol 121
Groups, events 75

H

HDLC 110
HDLC frames 96
Headers
    AM_Addr 124
    length error 81
    packets 76
    payload 78
HEC 104
HEC Error 80
Help menu 31
Hexadecimal patterns, searching 131
HID 110
Hiding 100, 107, 108
Higher protocols, decoding 109
High-pulse output 88
Hop 50
Hops
    hiding 107
    reduced mode 58
    sequence 11, 68
Hot keys 36
Humidity 7
HV1, 2, 3 packet 77

I

Idle 104
Implicit NACK 128
In/Out connector 15
Information, interpreting 103
Input signals 75, 81
Inquiry
    dedicated 11
    general 67
    perform/skip 39
    recording 11, 67
    timeout 11, 74

Installation
basic 9
detailed 13
Merlin 18
Interpreting a trace 103
Intersection search 132
Introduction 1
Invalid packet type error 80

J

Japan hops 69

K

Keyboard shortcuts 36

L

L_CH (Logical Channel) 78, 104
L2CAP
channel connections 113
CID, searching 126
described 110
messages 96, 108, 109, 112
L2FL 104
Len 104
Length of data 79
License 143
information 23
update software 22
Limited inquiry 11
Linking events 84
LMP
described 110
messages 96, 109, 112
Opcode 125
Logical Channel 78
Long pattern, searching 131
Loss of sync
searching for 126
timeout 74
Low-pulse output 88

M

Manual trigger 7, 10, 64
Manual updates 25
Markers
editing and clearing 105
searching 122
setting 104
Master
address 73
and slave 128
device, syncing to 34
switch 73
Master/address 54
Match clock rate 73
Memory, Recording 7
Menus
blue dots in events 85
clicked fields 108
pulldown 29
Merlin
configure encryption 140
description of 2
installation 18
installing software 18
program startup 19
rear panel 14
setup 14
Message
searching 121
Messages
hiding 100
LMP, L2CAP 109, 112
transfer 112
Mode, recording 67
Modes
test, recording in 58
Modes tab 66

N

Neighborhood, BT 139
Nine-pin connector 15
NULL packet 77
Nulls, hiding 108

O

OBEX 110
OBEX protocol 96
Opcode 104

Operating temperature 7
Options
  general display 95
  general recording 63
  name 10
  Piconet recording 68
  search 56
Output signaling pins 16
Output signals, enabling 88
Overview 1, 29

P

Package dimensions 7
Packets
  1100, 1101 77
  AUX1 77
  DM1, 2, 3 77
  DV 77
  FHS 77
  headers 75, 76
  headers in 76
  hiding 100, 101
  HV1, 2, 3 77
  invalid type error 80
  NULL 77
  POLL 77
  searching 121, 123
  types 77, 128
  viewing 112
Page
  sync and record 68, 69
  target 73
Paging traffic 73
Passive sync and record 71
Patterns, data 79
Payload
  headers 75, 78
  length error 81
PC requirements 17
Percentage of triggering 66
Perform inquiry 50
Phone numbers, Technical Support 143
Physical Components 5
Piconet
  addresses 73
  established devices 71
  master address 54
  private device 72
  recordiing 68
  recording 11, 45, 49
  recording traffic on 38
  sample 3
  search options 56
  slave address 44
  sync and record 71
  synchronizing 45
  target address 55
  Wizard 46
PIN 139
Pin-out description 15
Pins, output signaling 16
Pkt 110
Polls
  hiding 108
  POLL packet 77
Position of trigger 65
Post triggering, percentage 66
Power
  LED 7
  Switch 7
PPP 96, 110
Pre-triggering 66
Private Device Piconets 72
Program
  installation 9, 18
  starting Merlin 19
Progress indicator, recording 33
Protocol
  Analyzer 2
  Architecture 3
  decoding 110
  hiding 100
  searching 121
Prototype rework area 17
Pull-down menus 29
Pulse low signal 88
Pulse toggle signal 88

R

Radio strength 35
Reading a trace 103
Record inquiry 67
Record menu 29
Recording
    a trace 20
    Bluetooth traffic 10, 92
    existing Piconet 49
    LED 7
    memory 7
    mode 11
    mode, inquiry 67
    Piconet 45
    piconet 68
    progress indicator 33
    reduced hop mode 58
    session 12
    type 64
Recording Options
    events 75
    general 10, 63, 64
    in Wizard 45
    Piconet 68
    saving 91
    synchronization methods 66
Recording type 49
Recv, DUT freq 69
Reduced hops 58, 69
Reports
    generating 135
    menu 29
Requirements, Analyzer and PC 17
Restart button 83
Results of search 53
Resynchronization, forced 73
Revisions 21
Rework area, for prototype 17
RFCOMM 110
RFCOMM protocol 96

S

Sample
    Piconet 3
    recording 12
Saving
    display options 101
    recording options 91
SDP Msg 110
Search 42
    duration of 51
    general 52
Search menu 29
Search options 56
Search results 53
Search type 40, 51
Searching
    by data pattern 131
    complex 126
    data length 124
    for bit pattern 131
    for bit patterns 131
    for errors 126
    Header AM_Addr 124
    L2Cap CID 126
    Lmp Opcode 125
    packet types 123
    recorded traffic 121
Security 139
SEQN condition 77
Sequence
    event 90
    hop 68
Set marker 104
Setup
    menu 29
    Merlin 14
Shortcuts, keyboard 36
Signalling
    message 112
    output pins 16
Signals
    input 75, 81
    outputs, enabling 88
    strength, radio 35
Single frequency hops 69

Size of buffer 65
Skip inquiry 50
Slave device, address 44
Slave switch 73
Snapshot 10, 64
Soft Bit Error, searching 126
Software
  automatic updates 24
  installation 9, 18
  license updates 22
  overview 29
  regular updates 21
  starting Merlin 19
Spain hops 69
Special Interest Groups (SIGs) 1
Specifications 7
Standard hops 69
Starting Merlin 19
Status bar 33
Status of Analyzer 34
Storage temperature 7
STP messages, protocol 96
Strength of signal 35
Summary
  error 136
  traffic 137
Support, technical 143
Swapping addresses 74
Switches 7, 73
Sync
  and record 70, 71
  loss error 81
  loss of, searching 126
  methods 68, 69
  timeout, loss of 74
  to a master device 34
  window 74
Synchronization, forced 73
Synchronize Piconet 45
Synchronized LED 7
System setup, Merlin 14

T

Tabs
  display colors 97
  display formats 99
  general display 95
  hiding display 100
  recording events 75
  recording, general 10, 63
  recording, modes 11, 66
  recording, options 63
Target, page 73
TCS messages, protocol 96
Technical Support 143
Temperature tolerances 7
Test debug 75
Test mode, recording in 58
Threshold Exceeded error 80
TID 104
Time Stamp 104
Timeout
  inquiry 74
  loss of sync 74
Timeslot filtering 76
Timing calculations 136
Tips, tool 35, 95
Toggle signal 88
Toolbar 31
Tooltips 35, 95, 104, 112
Trace
  addresses 74
  filename 10
  reading 103
  recording 20
  sample 12
  view level, changing 96
Traffic
  Bluetooth 92
  generation 5
  hiding 108
  on Piconet 49
  paging 73
  recording 20, 56
  recording on piconet 38
  searching 121
  summary 137

Trail 104
Transfer message, data 112
TRG OUT 16
Trigger
    event 64
    external form 89
    LED 7
    position 10, 65
    post triggering 66
    recording, manual 64
Type of recording 64

U

Unassociated traffic, hide 108
Union search 132
Updates
    automatic 24
    firmware, BusEngine 23
    software license 22
    software, firmware, BusEngine 21
USB drivers, loading 18

V

Values, changing counters 85
View
    menu 29
    options 31
    packets 112

W

Warranty 143
Weight 7
Window menu 31
Wizard
    Piconet 46
Wrap 96

X

Xmit, DUT freq 69

Z

Zoom 35, 95