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 2.20

Manual Version 1.20

30 September, 2003

Document Disclaimer

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

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

Trademarks and Servicemarks

CATC, BTTracer, BTTrainer, Merlin, Merlin's Wand, Merlin Mobile, and BusEngine are trademarks of Computer Access Technology Corporation.

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

All other trademarks are property of their respective companies.

Copyright

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

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

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

FCC Conference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device and an intentional radiator, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense. The end user of this product should be aware that any changes or modifications made to this equipment without the approval of CATC could result in the product not meeting the Class A limits, in which case the FCC could void the user's authority to operate the equipment.

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

FCC Testing applies to FCC ID: KH7BT004APA-X.

EU Conference Statement

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

Manual Version 1.0 Part number: 730-0037-00

TABLE OF CONTENTS

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

Chapter 2 Installation 9
System Components/Packing List 9
Analyzer LED Descriptions 9
UPAS LEDs (from left to right) 9
UPAS Rear Panel Description 10
Setting Up the Analyzer 11
Installing the Analyzer Software on the PC 11
Recording Bluetooth 1.2 and 1.1 Traffic 14
Determining Which Bluetooth Mode You are In 14
Your First Bluetooth Recording 15
Inquiry Recording 15
Installing the HCI Probe 18
HCI Probe configurations 19
2-port RS232 to USB converter 21
External Interface Breakout Board 22
Pin-Outs for the Data In/Out Connector 22
Prototype Rework Area 23
Configuring the Analyzer for the Breakout Board 24

Chapter 3 Updates 25
Update Files 25
Automatic Updates 25
Software, Firmware, and BusEngine Versions 29
Software Updates 30

License Information 31
Updating the Software License 31

Chapter 4 Software Overview 33

The Main Display Windows. 33
Toolbar 36
Status Bar 42
Recording Progress 42
Status Bar Position Definitions: 42
Recording Status 44
Analyzer Status 44
Search Status 45
Zoom In. 45
Zoom Out 45
Tool Tips. 46
BTTracer Analyzer Keyboard Shortcuts 46

Chapter 5 Recording Wizard 47

Starting Recording Wizard 47
Recording a Traffic on a New Piconet 48
Recording an Existing Piconet 58
Recording in Test Mode 68
Recording in Reduced Hopping Mode 68
Recording in Single Frequency Mode 72

Chapter 6 Recording Options 75

Recording Modes 75
Piconet recording 75
Inquiry recording 75
BTTrainer mode 76
IUT:HCI mode 76
Opening the Recording Options Dialog Box 76
Recording Options - General 77
Recording type 77
Options 78
Buffer Size 78
Trigger Position. 79
Debug 79
Recording Options - Piconet 79
Channel 1 and Channel 2 80
Assignment 80
Frequency Hopping. 81
Sequence 82
Synchronization Method. 82
Loss of Sync Timeout (1-30 secs). 86
Force Re-synchronization 86
Show Paging Traffic 87

Follow Anonymity 87
Advanced 87
Recording Options - Inquiry 89
Recording Options - HCI 91
HCI Trace 91
Recording HCI Traffic 92
Starting the HCI Recording. 95
Editing an HCI Trace Configuration. 96
Recording Options - Events 96
Payload Length Error 103
Recording Options - Actions 104
Action Buttons - Their Functions 105
Blue Dot Menus 107
Saving Recording Options 112
Recording Bluetooth Traffic 112

Chapter 7 Display Options 115

General Display Options 116
Setting Color, Formatting, and Hiding Options 117
Setting Color Display Options 117
Changing Field Formats 118
Hiding Display Options 119
Level Hiding Options. 119
Level Hiding Parameters. 119
Saving Display Options 121

Chapter 8 Reading a CATC Trace 123

Trace View Features. 123
Interpreting the Displayed Information 123
Tooltips. 124
Set Marker 124
Edit or Clear Marker 125
Expanded and Collapsed Data Formats 126
Hide Frequency Hops. 128
Hide Nulls and Polls. 128
Menus in Clicked Fields. 129
Hide Unassociated Traffic 129
Hide Channel 129
Hide Duplicated Traffic 129

Chapter 9 Decoding Protocols. 131

Introduction 131
LMP and L2CAP Messages. 131
Decoding and Viewing Higher Protocol Data 132
Decoding Via the Decoding Toolbar. 132
Decoding Via the Display Options Dialog Box 133
Tooltips. 133

Viewing Packets in LMP and L2CAP Messages 134
Types of LMP and L2CAP Messages 134
Viewing L2CAP Channel Connections 135
Viewing Protocol Messages and Transactions 136
Viewing L2CAP Messages in Protocol Messages 136
How to Decode 136
Expanding Protocol Messages 136
Decoding via the Profiles Toolbar 137
Changing Protocol Assignments 137
Using the Decoding Assignments Dialog Box 138
Removing User-Assigned Protocol Assignments 139
Manually Assigning Protocols 140
Other Assignments: OBEX Client/Server Status 140
Changing an OBEX Client or Server Status 141
Decoding BNEP 141
Decoding HID 141
Other Decoding Options 141

Chapter 10 Exporting Trace Data. 143

Exporting To Text Format 143
Exporting Trace Data to a .CSV Format 144
Exporting Audio Data 145

Chapter 11 Other Features 147

Search 147
Go to Trigger 147
Go to Packet/Message/Protocol 147
Go to Marker 148
Go to 148
Error 152
Soft Bit Error 152
Loss of Sync 152
Find 152
Event Groups 154
Union, Intersection, and Exclusion 157
Using Find 158
Find Next 160
Device List 160
Edit Comment 161
File Information 161
Error Summary 162
Timing Calculations 162
Bus Utilization 163
Traffic Summary 167
Real-Time Statistics 167
Encryption 170
Configuring BTTracer for Encryption 170

Re-applying Encryption Settings 173

Chapter 12 How to Contact CATC 177

Chapter 13 Warranty and License 177

Index 181

1. Overview

The CATC BTTracer™ Protocol Analyzer is the top-of-the-line member of CATC's industry-leading line of high performance, Bluetooth protocol analyzers. Preceded by CATC's Merlin™ and Merlin Mobile Analyzers, BTTracer has been designed using the same modular 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 1.2* 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.

BTTracer can operate in a single or dual channel configuration. Two-channel operation requires a second BTTracer module (i.e., an auxillary module) installed in the right slot.

BTTracer can operate in conjunction with BTTrainer. BTTrainer is a Bluetooth Exerciser used for verification/validation testing or for debugging and analysis.

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 98SE, Windows 2000, 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-25 connector provides a path for externally supplied data or timing data to be recorded along with bus traffic.

This DB-25 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, refer to the *Automation API for CATC Bluetooth Analyzers* reference manual included in the installation CD-ROM. You can also download the document from the CATC website.

1.4 HCI Trace

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

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

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

1.5 Features

General

- Flexible design - reconfigurable hardware for future enhancements.
- User friendly - the Graphical User Interface software of 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.
- Works in combination with the BT*Trainer* Exerciser.
- Supports two BT*Tracer* probe modules - for recording two piconets and mixed piconets made up of 1.1 and 1.2 devices.
- Supports two channel recording.
- Complies with Bluetooth v1.2 specification - but can run in both v1.1 and v1.2 modes.
- Supports point-to-point and point-to-multipoint Bluetooth piconets.
- Supports 79 frequency hop standards, reduced and fixed frequency.
- Automatic tracking of changes in the hopping scheme.
- Automatic tracking of whitened and non-whitened packets and traffic.
- Supports recording of serial HCI traffic from implementation under test (IUT).
- Free non-recording, view-only software available.
- Power-on self-diagnostics.
- Internal 100V to 240 V AC power supply.
- Compliant with FCC class A requirements / meets all CE mark requirements.
- Three year warranty and hot-line customer support.

Physical Components

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

- Trace viewer software support for Microsoft Windows versions 98SE and later.
- Recording memory of 512 MB - enough to record thirty five minutes of high volume traffic and more than two days of low volume traffic.

Display Options

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

Recording Options

- Flexible advanced triggering capabilities including - multiple triggering modes, selective views, timing analysis, search functions, protocol packet errors, transaction errors, packet type and destination device, data patterns, or any of these trigger types in combination.
- User defined trigger position.
- Support for various piconet characteristics by enabling the user to configure the synchronization method and recording parameters.
- Real-time hardware filtering of captured traffic for optimizing analyzer memory usage.

Traffic Generation

Traffic generation capability is provided by 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 configurable building blocks that implement data/state/error detection, triggering, capture filtering, external signal monitoring and event counting & sequencing. And like the flash-memory-based firmware that controls its operation, all BusEngine logic is fully field upgradeable, using configuration files that can be downloaded from the CATC Website.

1.6 Specifications

Package

Dimensions:	UPAS 2500H 12.2 x 12.2 x 3.5 inches (31.1 x 31.1 x 8.9 cm)
Connectors:	AC power connection external clock input (EXT CLK, BNC) host connection (USB, type 'B') data connector (Data In/Out, 25-pin DB)
Weight:	UPAS: 9.5 lbs. (4.3 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

UPAS:	
Power (PWR):	illuminated when the UPAS is powered on.
Status (STATUS)	Illuminated when the analyzer is functioning properly
BTTracer Module:	
Recording (REC):	illuminated when the analyzer is actively recording 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

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

Certification

FCC (Class A), CE Mark

2. 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.

2.1 System Components/Packing List

- One stand-alone BTTracer Analyzer module
- One Antenna
- One External Interface Breakout Board with a 25-pin ribbon cable
- One USB cable
- One SMA Adapter cable (for changing the polarity from reversed to standard. This cable is used for creating wired piconets.)
- HCI Probe
- BTTracer software program installation CD
- User Manual

2.2 Analyzer LED Descriptions

With single probe system, the BT*Tracer* analyzer module occupies the left slot on the CATC Universal Protocol Analyzer System (UPAS). When powered on, the BT*Tracer* activates the user-accessible controls and LEDs on the front and rear panels of the UPAS.

Warning Do not open the UPAS enclosure. There are no operator serviceable parts inside. Refer servicing to CATC.

UPAS LEDs (from left to right)

A Green **PWR** (power) indicator LED for UPAS (lights when the unit power is switched on).

B Red **Status** indicator LED for UPAS (lights during initialization/power up of UPAS base unit. Blinks if a self-test fails).

C Green **REC** (recording) LED (lights when the unit is recording).

D Orange **TRG** (triggered) LED (lights when the unit triggers on an event).

E Green **SYNC** (Synchronize) LED (Flashing indicates that the analyzer is tracking the defined slave or master device. Illuminated indicates that the analyzer is tracking an active piconet.)

F **Manual Trigger** push-button (allows a manual Trace capture).

G Green **REC** (recording) LED (lights when the unit is recording).

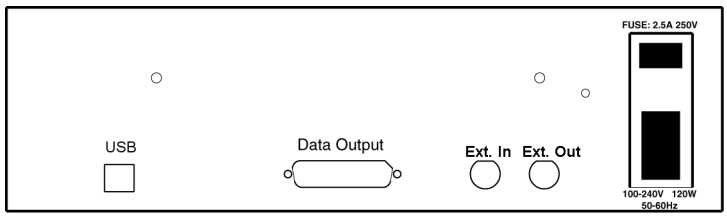
H Orange **TRG** (triggered) LED (lights when the unit triggers on an event).

I Green **SYNC** (Synchronize) LED (Flashing indicates that the analyzer is tracking the defined slave or master device. Illuminated indicates that the analyzer is tracking an active piconet.)

J **Manual Trigger** push-button (allows a manual Trace capture).

2.3 UPAS Rear Panel Description

Figure 1: Rear Panel



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

USB type "B" host computer connector

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

RS-232 25 pin "Data Output" Connector

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

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

These connectors allow BNC cables to be attached to the analyzer for the purpose of triggering on external input signals and for monitoring raw Tx/Rx data.

Wide Range AC Connector Module

The power module is composed of:

- Power on/off switch
- Power socket
- Enclosed 5x20 mm 2.0A 250 V fast acting glass fuse

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

2.4 Setting Up the Analyzer

A UPAS can support up to two BTTracer probes. These modules will come factory-installed in the UPAS. In a single probe system, BTTracer will come installed in the left slot.

To set up a one or two probe system,

Step 1 Attach the Antenna to the ANT connection point for each analyzer probe. The antenna should point up.

Step 2 Connect the provided AC power cord to the rear of the UPAS and to a 100-volt to 240-volt, 50 Hz to 60 Hz, 100 W power outlet.

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

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

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

Step 4 Connect the USB cable between the USB port on the back of the analyzer and a USB port on the analyzing PC.

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

2.5 Installing the Analyzer Software on the PC

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

Step 1 Insert the BTTracer CD into the CD ROM drive of the PC that will be administering the Analyzer.

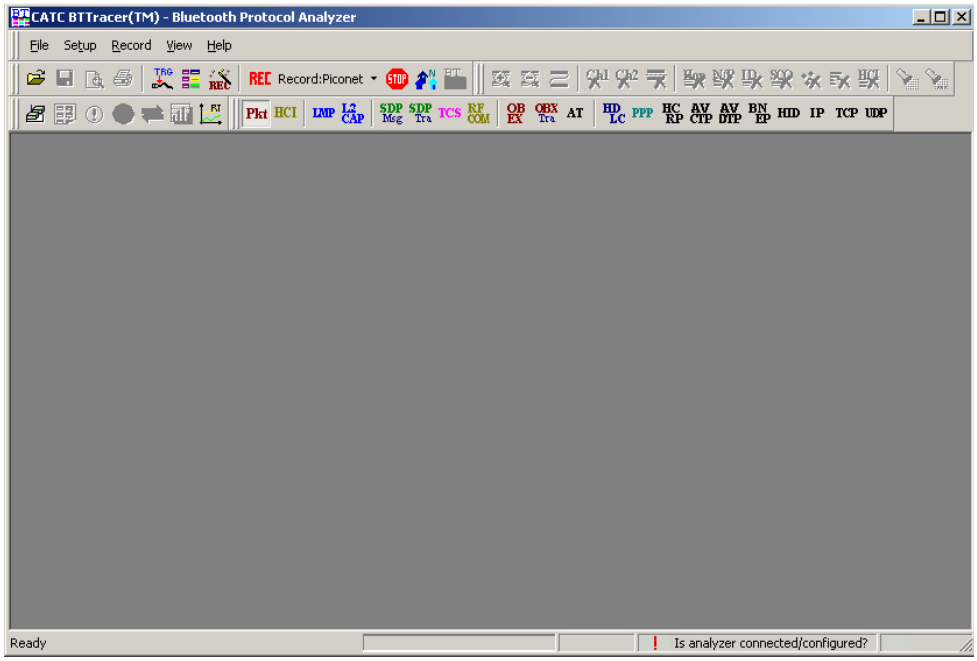
Step 2 Follow Windows on-screen Plug-and-Play instructions for the automatic installation of the BTTracer Analyzer as a USB device on your analyzing PC (the required USB files are included on the BTTracer CD.

Step 3 Select **Install Software** from the installation CD and follow the on-screen installation instructions.

The BT*Tracer* application will install on the PC hard disk.

Step 4 To start the application, launch the **CATC BTTracer** program from the **Start Menu: Start>Programs>CATC>BTTracer**.

The BTTracer program opens.

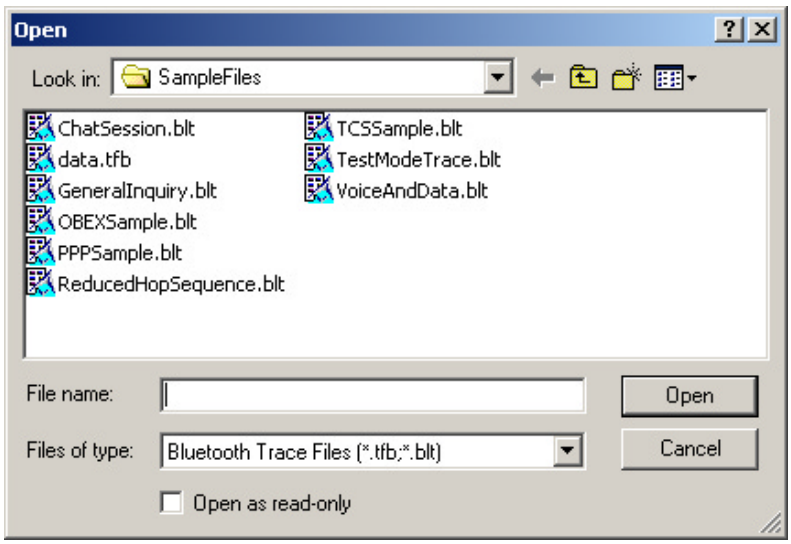


The window shows a menu bar and toolbar at the top, a grey trace viewing area covering most of the window, and a status bar at the bottom.

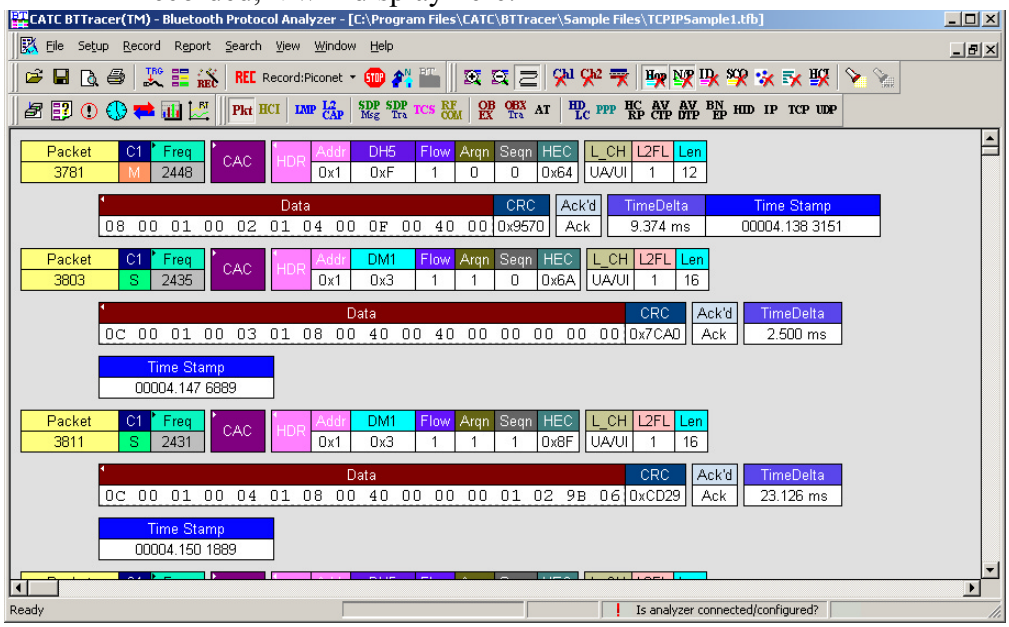
Opening a sample trace will cause most of the buttons on the toolbar to become active.

To open a trace,

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



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



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

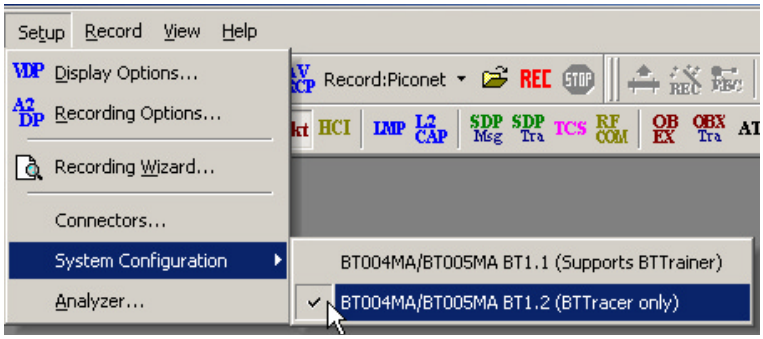
2.6 Recording Bluetooth 1.2 and 1.1 Traffic

By default, BTTracer is configured to record in a mode compliant with the Bluetooth 1.1 specification. This mode is required if you are using BT*Trainer* to generate traffic (BT*Trainer* is compliant only with the Bluetooth 1.1 specification).

To record traffic in a mode compliant with the Bluetooth 1.2 specification, perform the following steps.

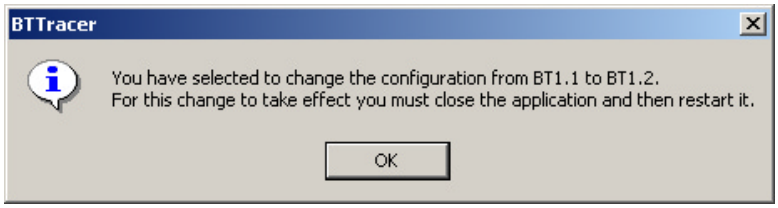
Step 1 From the menu, select **Setup > System Configuration ...**

A dialog box opens.



Step 2 Select **BT1.2 (BTTracer only).**

The following message appears.



Step 3 Click **OK**.

Step 4 Shutdown the BTTracer application by clicking the X in the top right corner of the application.

Step 5 Restart the BTTracer application from the Start menu: **Start>Programs >CATC>BTTracer Suite>BTTracer**.

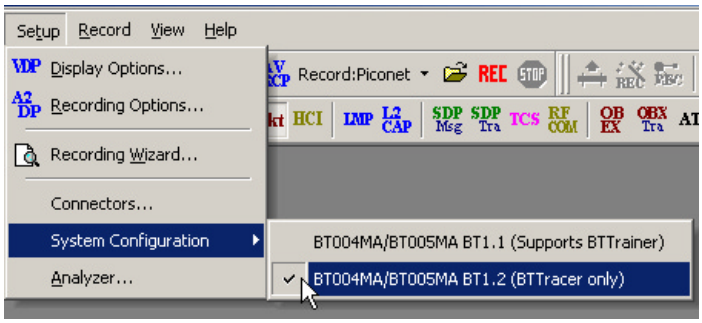
The application starts in the Bluetooth 1.2 mode.

Determining Which Bluetooth Mode You are In

You can quickly determine whether BTTracer is operating in the 1.1 or 1.2 modes from the Setup command described above.

Step 1 From the menu, select **Setup > System Configuration ...**

The menu opens and displays a checkbox next to the current mode.



2.7 Your First Bluetooth Recording

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

Inquiry Recording

To create an inquiry recording, perform the following steps:

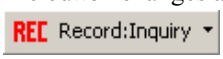
Step 1 Click the down-arrow on the right side of the **Record:Piconet** button on the toolbar

.

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

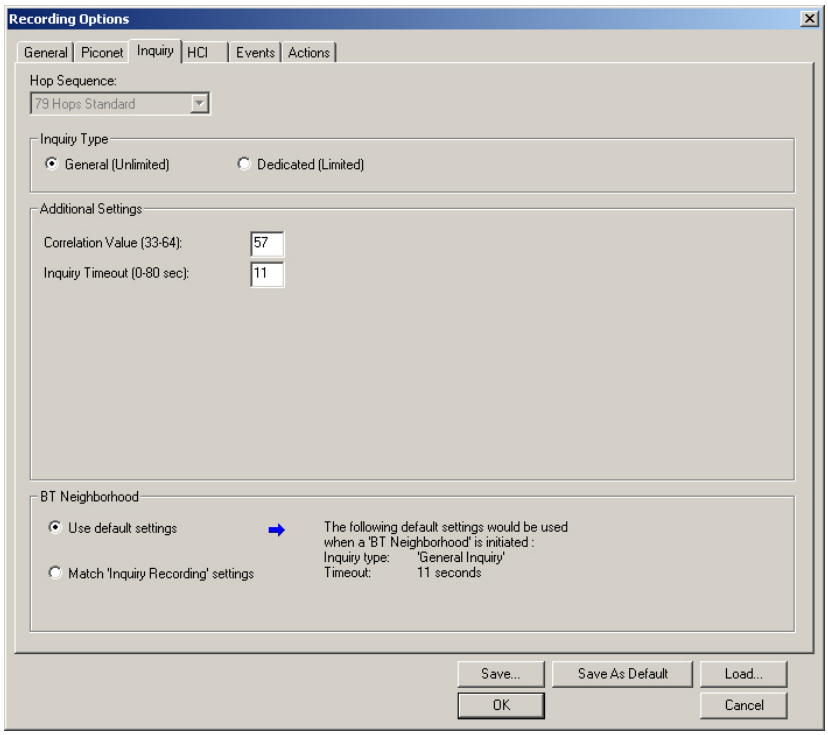
Step 2 Select **Inquiry Recording Mode**.

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



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

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



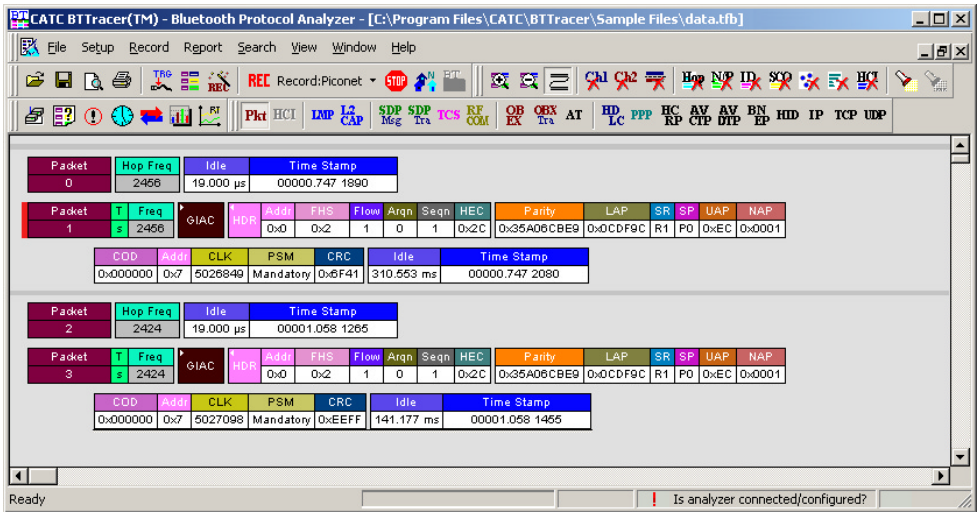
Step 4 If desired, make any changes to the options, then click **OK.**

Step 5 Click the REC Record:Inquiry button (i.e. not the down-arrow.)

BTTracer starts to record the Bluetooth traffic immediately using the settings from the Piconet page in the Recording Options dialog. The Bluetooth Inquiry process will proceed for whatever amount of time is set for creating an Inquiry action (the default is 11 seconds). After the inquiry time has elapsed, the analyzer will upload the data and display the packets. In addition, the Device List window will open and display the updated statuses of the devices.

The screen should look like the sample recording below which shows the FHS packets generated during the Inquiry process.

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



Step 6 To save a current recording for future reference, Select **Save As** under **File** on the Menu Bar.

OR

Click on the Tool Bar.

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

Step 7 Give the recording a unique name and save it to the appropriate directory.

2.8 Installing the HCI Probe

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

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

The probe is composed of the following components:

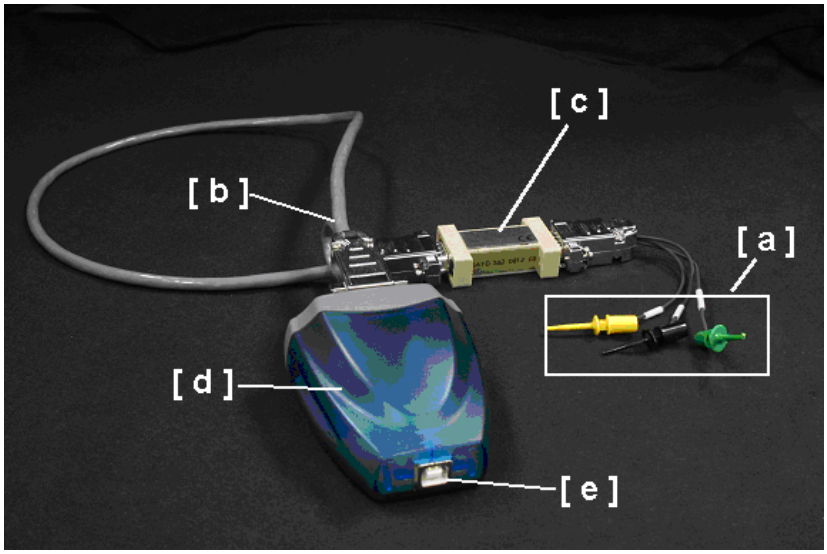
[a] HCITrace Probe Cable

[b] HCITrace RS232 Cable

[c] TTL to RS232 converter

[d] 2-port RS232 to USB converter

[e] Port for USB cable (cable not shown)



HCITrace Probe Cable

The HCITrace Probe Cable has three probes:

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

HCITrace RS232 Cable

Has three DB-9 connectors:

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

TTL to RS232 converter

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

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

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

2-port RS232 to USB converter -

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

USB cable –

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

HCI Probe configurations

The HCI Probe can be used in two configurations:

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

Monitoring UART Level Signals

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

Step 1 Connect the DB-9 connector of the HCITrace Probe Cable [a] to the connector marked with 'TTL' in the TTL to RS-232 converter [c].

Step 2 Connect the DB-9 connector marked with 'RS-232' in the TTL to RS-232 converter [c] to the connector marked with ''RS-232/Probe'' in the HCITrace RS-232 Cable [b].

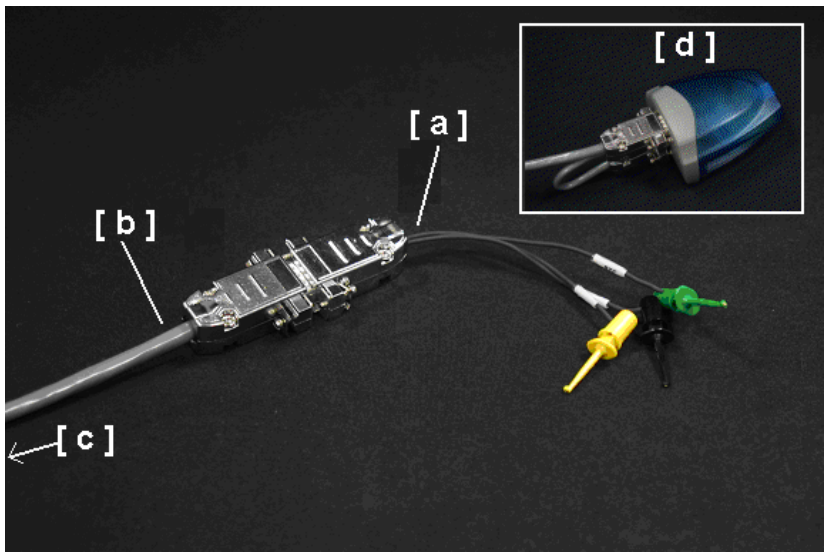
Step 3 Connect the connector marked with 'COM A' in the

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

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

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

Monitoring RS232 level Signals



Legend for photo:

[a] HCI Probe Cable

[b] HCI Trace RS-232 Cable

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

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

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

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

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

RS232 to USB converter [d].

Step 3 Connect the connector marked with 'COM B' in the HCITrace RS-232 Cable [c] to 'Connector B' in the 2-port RS232 to USB converter [d].

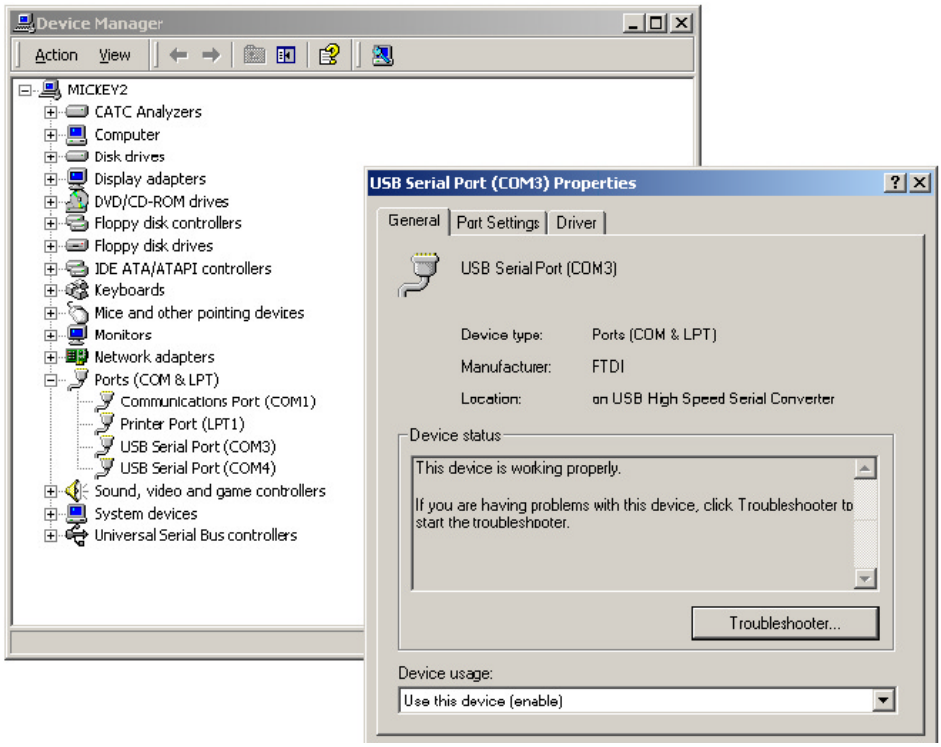
Step 4 Connect the USB cable [not shown] to the USB connector of the 2-port RS232 to USB converter [d].

2-port RS232 to USB converter

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

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

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



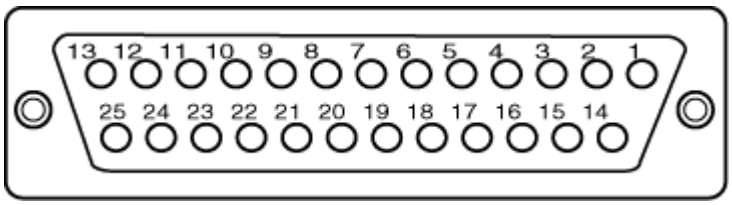
2.9 External Interface Breakout Board

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

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

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

Data In/Out Connector (on cable)



Pin-Outs for the Data In/Out Connector

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

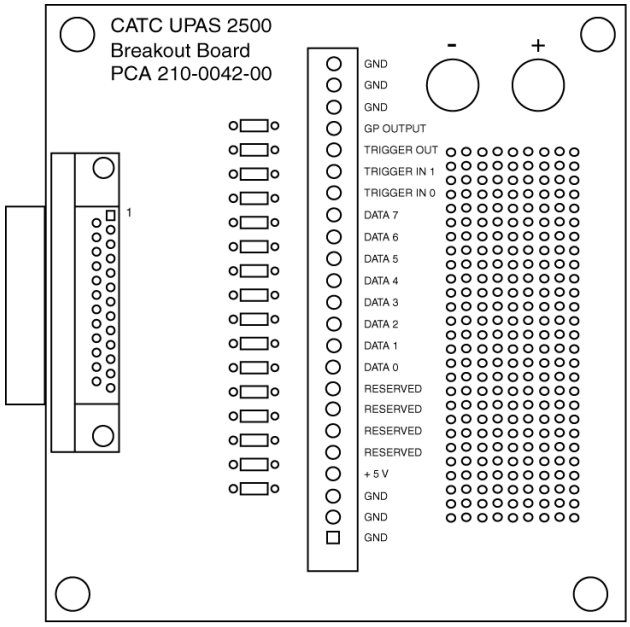
Data In/Out Connector – Pin-Out

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

Pin	Signal Name	Signal Description
16	TRG OUT	Trigger Out
17	TRG IN 0	Trigger In 0
18	DATA 7	Data 7
19	DATA 5	Data 5
20	GND	Ground
21	DATA 2	Data 2
22	DATA 0	Data 0
23	GND	Ground
24	RSV	Reserved
25	RSV	Reserved

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

External Interface Breakout Board



Prototype Rework Area

The Breakout Board contains a prototype rework area for making custom circuits for rapid development. The area consists of plated-through holes, 20 columns wide by 27 rows long. The top row of holes is connected to GND

and the bottom row is connected to +5V. The remaining holes are not connected. Use the rework area to insert custom components and wire-wrap their respective signal, power, and ground pins.

External Recordable Signals

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

External Input Triggers

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

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

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

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

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

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

External Outputs

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

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

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

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

Configuring the Analyzer for the Breakout Board

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

3. Updates

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

3.1 Update Files

Update files are installed with the BTTracer software during the installation procedure and reside in the local directory of the analyzer application. During the update process, the files are taken from this location.

The following update files are provided with each release:

BusEngine - For updating the hardware logic (has an *.rbf extension).

Firmware- For updating the platform firmware (has an *.hex extension).

BT Firmware - For updating the Bluetooth firmware (has an *.esw extension).

3.2 Automatic Updates

When you update the analyzer software, the software may become incompatible with the BusEngine and Firmware. If a recording is attempted, analyzer displays an error message and then automatically begins an update process for the BusEngine and Firmware.

To update the BusEngine and/or Firmware, follow these steps:

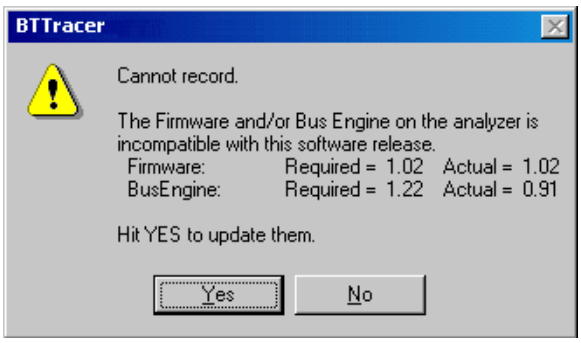
Step 1 If needed, update the analyzer software, following the steps outlined in "Software Updates."

Step 2 Turn on the analyzer.

Step 3 From the **Record** menu, select **Start**.

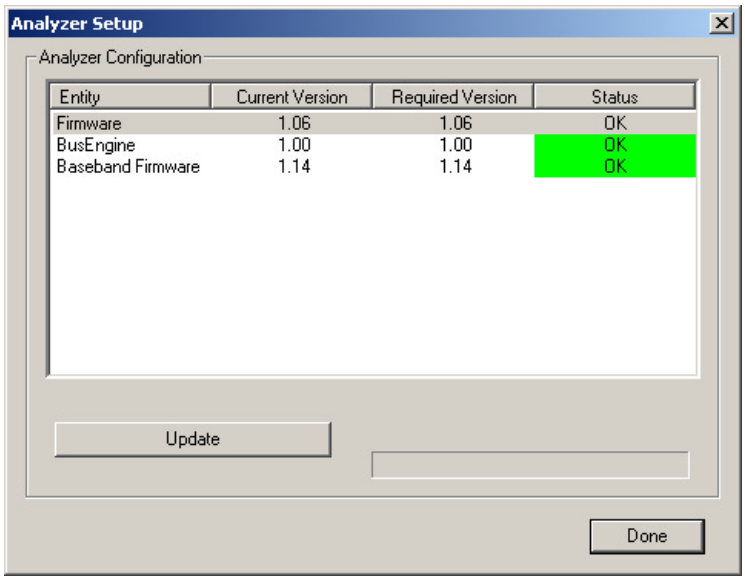
Because the BusEngine and/or the Firmware are incompatible with the current analyzer software version, an error message appears

showing your current versions and indicating what versions you need to install.



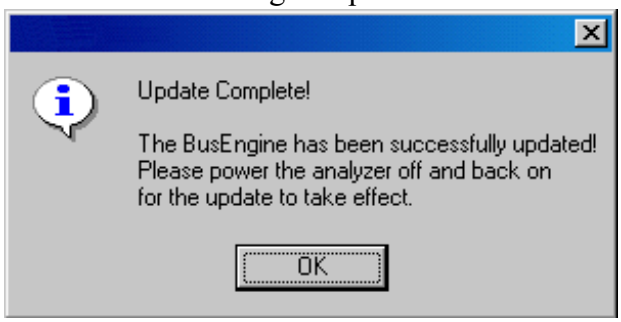
Step 4 Click **Yes**.

The **Analyzer Setup** window appears.



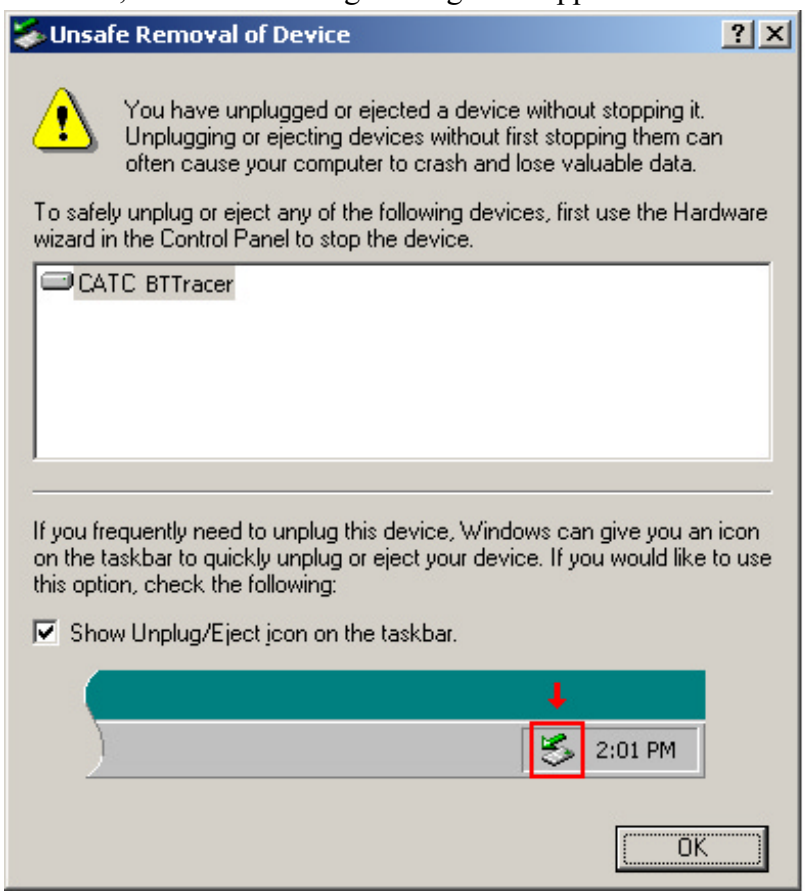
Step 5 Click **Update**.

When the update has finished, a message such as the following appears and tells you that the update is complete. The example below follows a BusEngine update.



Step 6 To complete the update, power cycle the analyzer (turn the unit off then back on).

If you are running Windows 2000, the Analyzer will automatically reboot, and the following message will appear:



Step 7 Click **OK**.

In this instance, you do not need to power cycle the Analyzer (turn off then back on).

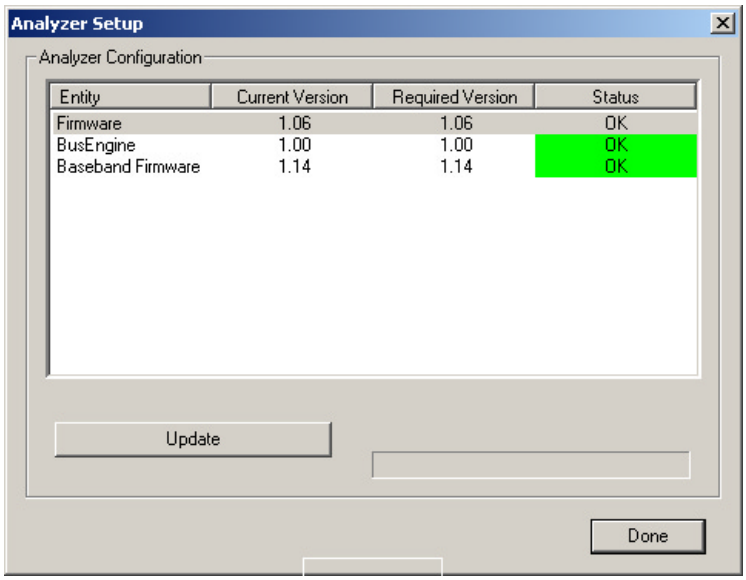
Manual Updates

If you prefer, you can manually update the Firmware, BT firmware and/or BusEngine through the 'Analyzer Setup' dialog. To do this follow these steps:

Step 1 Make sure that the BTTrainer application is not active.

Step 2 Select from the menu: **Setup** > **Analyzer**.

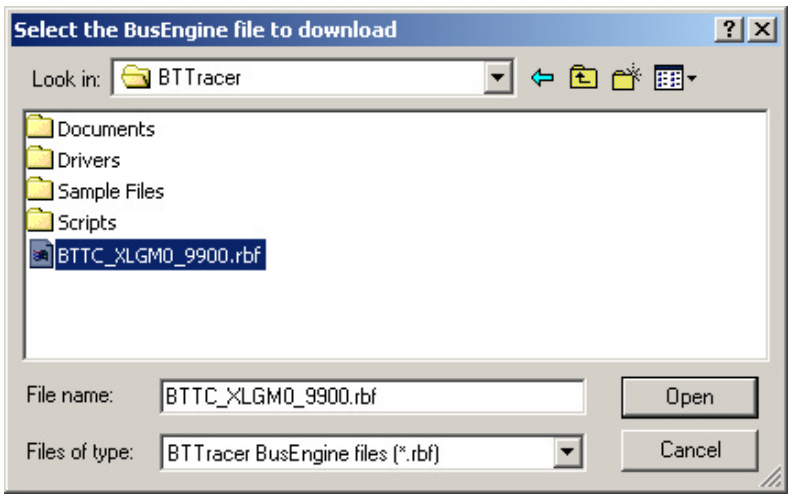
The **Analyzer Setup** dialog box opens.



Step 3 Select the one of the entity that you want to update from the list.

Step 4 Click the **Update** button.

The familiar Open File dialog box will open allowing you to select the proper file, as shown below:



Step 5 Select the file to be updated, and select the Open button.

At this time, the application would start the update process. A progress bar in the dialog would show the progress of the update process.

Please note that in some cases this process would take up to several minutes to complete.

Step 6 When a the application notifies that the update process is done,

you may need to cycle the analyzer's power to cause the program to take effect, or you may need to unplug and then reconnect the USB cable between the analyzer and the computer to cause the new firmware upgrade to take effect.

3.3 Software, Firmware, and BusEngine Versions

The **Readme.html** file on the installation CD and on the installed directory on your hard drive. This file gives last-minute updates about the current release. Included with each release are the most recent downloadable images of the Firmware and the BusEngine.

Once the BT*Tracer* has completed the self diagnostics and is connected to the PC, you can check the latest version of the software and BusEngine.

To check information about the current software, select **About BTTracer…** from the **Help** menu.

The About BTTracer window appears.

About BTTracer details revisions of the following software and hardware:

- Software Version and Build Number
- Product Name
- Firmware Version
- BusEngine Version
- Unit Serial Number
- Slot 1: Model Number
- Slot 2: Model Number (if a second module is present)

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

3.4 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.

The software is also available on CD from CATC.

Updating from CD-ROM

To update the software from CD-ROM, follow these steps:

Step 1 Load the CD-ROM into the CD-ROM drive

Step 2 Open Windows Explorer and double-click on *autorun.exe.* An install screen opens.

Step 3 Click *Install Software* and follow the onscreen instructions.

Updating from the CATC Website

Step 1 Open a web browser and navigate to www.catc.com.

Step 2 Find the latest released software version on the CATC website under **Support** at the link shown at the top of the page.

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

If you are **not** running the latest version.

Step 3 Download the software from the CATC website.

Step 4 If downloading from the web, unzip the files into your choice of directory.

Step 5 Click **Start**, then **Run**, and browse to where you unzipped the files.

Step 6 Select the program named **Setup** and click **Open**.

Step 7 Click **OK** to run the Setup and begin the installation.

Step 8 Follow the on-screen instructions to complete the installation.

Step 9 Read the Readme file for important information on changes in the release.

3.5 License Information

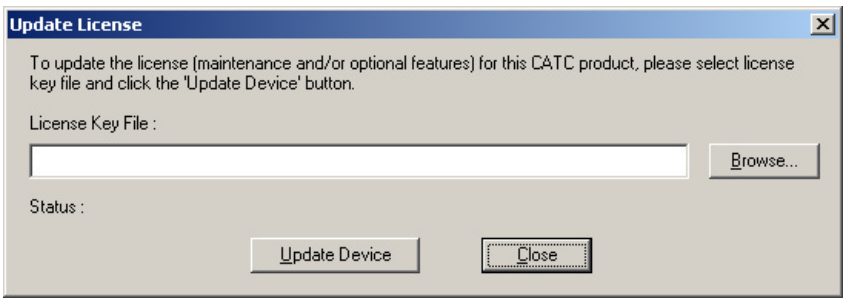
Licensing information for BT*Tracer* can be viewed by selecting **Display Information** from the **Help** menu. The License window provides maintenance expiration and features data for BT*Tracer*.

Updating the Software License

A License key is necessary to enable software maintenance.

A license is granted with the purchase of an analyzer. Thereafter, you must renew your license if you wish to continue receiving support. You obtain a new License Key from CATC. Once the License Key is obtained, follow these steps to install it:

Step 1 From the **Help** menu, select **Update License**. The Update License dialog displays.



Step 2 Enter the path and filename for the License key or use the Browse button to navigate to the directory that contains the License Key.

Step 3 Select the *.lic file, and then click **Update Device**.

4. Software Overview

4.1 The Main Display Windows

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

Table 1: Main Display Pull-Down Windows

Menu	Function
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
Re-apply Encryption Settings ...	If a trace has been recorded with the wrong encryption settings, you can enter the correct ones via the Device List, then run **File> Re-apply Encryption Settings ...** This command will open a Save As dialog box for creating a new trace file using the new settings.
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
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
Export>>Audio Streams	Saves audio data into a file. Presents options for setting the Audio Source format, Output File format, Stream Direction, and Output Sampling
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	Opens a dialog box with checkboxes and drop-down menus for setting up a recording.
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.

Menu	Function
Connectors ...	Opens a dialog box for the output connectors on the back of the UPAS. There are two options: **Default Configuration** - Causes the analyzer to output a low voltage output signal for use by another device such as an oscilloscope. See "External Input Signals" on page 103 for further explanation. **Output Radio Data** - Causes the analyzer to output radio signals through External Output connectors. If you place your mouse pointer over the Output Radio Data option, a tool tip will provide a detailed explanation of this option's function.
System Configuration>> BT004MA/BT005MA BT1.1 (Supports BTTrainer)	Puts BTTracer in Bluetooth 1.1 mode. This modes supports the Bluetooth 1.1 specification. BTTrainer will function in this mode.
BT004MA/BT005MA BT1.2 (BTTracer only)	Puts BTTracer in Bluetooth 1.2 mode - ie in a mode that supports the recording and displaying of traffic that is supported by the Bluetooth 1.2 specification. This mode does not support BTTrainer.
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.
Recording Mode	Presents a drop-down menu with options for setting the analyzer's recording mode: ***Piconet Recording Mode*** -- Causes BTTracer to monitor and record piconet traffic. BTTracer records the traffic data as specified in the Recording Options, then uploads the data as a Trace file when the recording is complete. ***Inquiry Recording Mode*** -- Causes BTTracer to perform an inquiry to detect and record Bluetooth devices within range. After completing the recording, BTTracer uploads the trace to the PC and saves it as a Trace file. ***BTTrainer Recording Mode*** -- Causes BTTrainer Bluetooth Generator application to run. If BTTrainer is not running, this menu item is disabled. ***IUT:HCI Recording Mode*** -- Configures the system to exclusively record HCI traffic from IUTs. This recording mode bypasses the analyzer: HCI traffic from the IUT is recorded directly by the analyzer software without going through the analyzer.
BT Neighborhood Inquiry	Displays Bluetooth Address & clock frequency for devices in range. The expected Bluetooth clock frequency is 3200 Hz +/- 250 ppm.
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 & allows you to go to a specific packet, and save the error file to a uniquely named file.

Menu	Function
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	Presents a sub-menu with options for displaying/hiding the toolbars and an option called Customize which allows the menus and toolbars to be customized or reset to factory default.
Status Bar	Switches display of the Status Bar on or off.
Unhide Cells >	Presents a menu of currently hidden cells. Allows you to unhides any cells that were hidden through the Display Options dialog box (View > Display Options > Color/Format/Hiding)
Zoom In	Increases the size of the displayed elements.
Zoom Out	Decreases the size of the displayed elements.
Wrap	Allows the display to wrap.
Device List	Displays a list of discovered Bluetooth devices and allows you to add and delete devices and security settings by selecting the device, pressing the security button, and modifying the settings.
Real-time Statistics	Opens a dialog box with a graphical summary of the traffic currently being recorded by the Analyzer. Real-time monitoring allows continuous monitoring and displaying of traffic and related statistical dada in a piconet. This processed data is displayed in a set of configurable graphs.
Decoding Assignments	Lists current L2CAP decoding assignments.
L2CAP Connections	Lists current L2CAP connections.
RFCOMM Channel Assignments	Lists current RFCOMM assignments.
Levels	Presents a menu of display levels. This menu replicates the Decode/Display buttons in the toolbar such as Packets, L2CAP, TCS etc.)
Profiles	Presents a menu of profiles. Selecting a profile will cause the analyzer to decode the protocols appropriate for the selected profile.

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

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

4.2 Toolbar

There are five toolbars in the BTTracer user interface toolbar. The Toolbar buttons provide access to frequently-used program functions. Tool tips describe icon functionality as the mouse arrow is moved over an item.

You display or hide toolbars by selecting **View** > **Toolbars** from the menu. The sub-menu lists four toolbar names: **Standard**, **Frequently Used**, **Analysis**, **View Level, and Profiles**.

Standard Toolbar

Open file

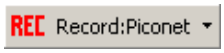
Save As

Print Preview

Print…

Setup Record Options - presents options for setting up a recording.

Setup Display Options - presents options for formatting the display.



Start Recording - starts a recording. The down arrow gives you options for starting different types of recordings: recording piconet, inquiry recording, BTTrainer recording, or IUT:HCI recording.

Stop Recording

Start Recording Wizard - Opens an easy-to-use wizard for setting up and executing a recording.

Bluetooth Neighborhood. Performs an inquiry and then lists the local devices that it discovered

Start BTTrainer - Invokes the BTTrainer application. Enabled only in BTTracer 1.1 configuration. To set BTTracer in the 1.1 configuration, select Setup > System Configuration > BT004MA/BT005MA BT1.1 (Supports BTTrainer).

"Frequently Used" Toolbar

Zoom In

Zoom Out

Wrap

Show/Hide Channel 1 Traffic

Show/Hide Channel 2 Traffic

Show/Hide Duplicated Traffic

Show/Hide Frequency Hops

Show/Hide Nulls & Polls

Show/Hide ID Packets

Show/Hide Voice (SCO) Packets

Show/Hide devices that were specified in the Display Options dialog box

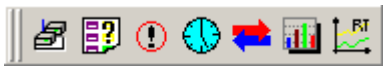
Show/Hide Unassociated Traffic

Show/Hide HCI Traffic

Complex Find

Find Next

Analysis Toolbar



Display device list

File Information Report

Error Summary

Timing Calculations

Traffic Summary

Display Bus Utilization graph

Display Real-Time Statistics

View Level Toolbar

View Packet Level (Baseband)

View HCI Traffic

View/Hide LMP Message Level

View/Hide L2CAP Message Level

View/Hide SDP Message Protocol Level

View/Hide SDP Transaction Protocol Level

View/Hide TCS Protocol Level

View/Hide RFCOMM Protocol Level

View/Hide OBEX Protocol Level

View/Hide OBEX Protocol Transaction Communications Level

View AT Commands Protocol Level

View/Hide HDLC Protocol

View/Hide PPP

View/Hide HCRP

View/Hide AVCTP

View/Hide AVDTP

View/Hide BNEP Protocol

View HID Protocol Layer

View IP Protocol Layer

View TCP Protocol Layer

View UDP Protocol Layer

View Profiles Toolbar

Profile buttons decode the protocols associated with a particular profile. When you press a profile button, the BT*Tracer* software will automatically select for you the protocol buttons associated with that profile such as RFCOMM and OBEX.

Note: This toolbar is hidden on initial activation of the application. To display this toolbar, select **View** > **Toolbars** > **Profiles** from the menu.

Decodes protocols for the GAP profile.

Decodes protocols for the SDAP profile.

Decodes protocols for the CIP profile.

Decodes protocols for the GAVDP profile.

Decodes protocols for the CTP profile.

Decodes protocols for the INT profile.

Decodes protocols for the SPP profile.

Decodes protocols for the HP profile.

Decodes protocols for the DUP profile.

Decodes protocols for the FAX profile.

Decodes protocols for the LAN profile.

Decodes protocols for the SIM profile.

Decodes protocols for the OBEX profile.

Decodes protocols for the OPP profile.

Decodes protocols for the FTP profile.

Decodes protocols for the SYNC profile.

Decodes protocols for the BIP profile.

Decodes protocols for the A2DP profile.

Decodes protocols for the BIP profile.

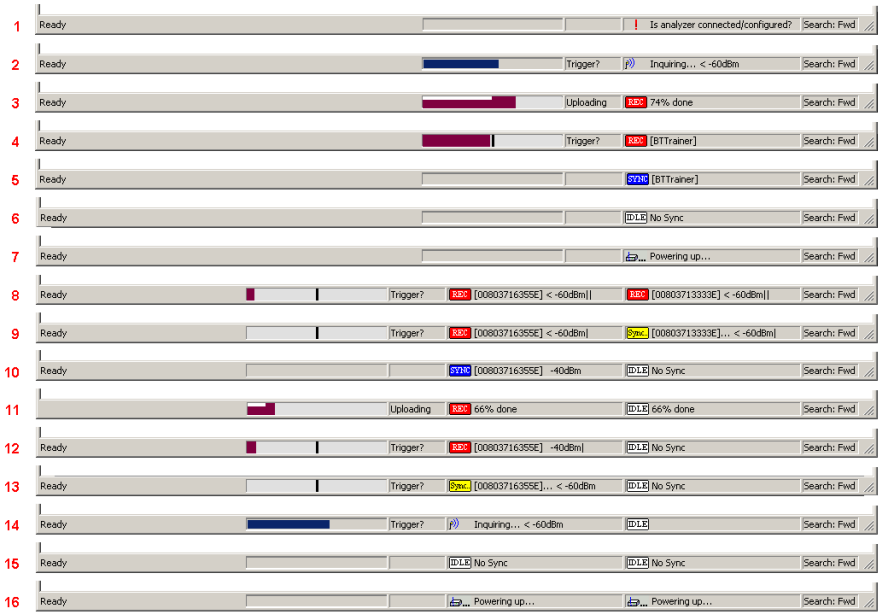
Decodes protocols for the BIP profile.

4.3 Status Bar

The Status Bar is located at the bottom of the main display window. Depending on the current activity, the bar can be divided into as many as four segments. The figure below demonstrates the various displays in the status bar.

Recording Progress

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



Status Bar Position Definitions:

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

1 Analyzer is not connected to the host machine or not configured.

2 Analyzer is performing an inquiry (only channel 1 is present).

3 Analyzer is done recording and is uploading the recorded data.

4 Analyzer is recording (only channel 1 is present).

5 Analyzer is synchronized to a piconet with the master device that has BD_Address 0083716355E.

6 Analyzer is connected to the host machine, but is not performing a thing.

7 Analyzer is connected to the host machine and is powering up.

8 Analyzer is recording on both channel 1 and channel 2. Channel 1 is capturing the traffic of the piconet with master device that has BD_Address 0083716355E while channel 2 capturing the traffic of the piconet with master device that has BD_Address 0083713333E.

9 Analyzer is recording on channel 1 the traffic of the piconet with master device that has BD_Address 0083716355E while channel 2 is trying to sync to the piconet with master device that has BD_Address 0083713333E.

10 Analyzer is synchronized on channel 1 to the piconet with the master device that has BD_Address 0083716355E. Channel 2 is in Idle mode.

11 Analyzer is uploading the recorded traffic from channel 1. Channel 2 is in Idle mode.

12 Analyzer is recording on channel 1 the traffic of the piconet with master device that has BD_Address 0083716355E while channel 2 is in Idle mode.

13 Analyzer is trying to synchronize on channel 1 to the piconet with the master device that has BD_Address 0083716355E while channel 2 is in Idle mode.

14 Analyzer is performing an inquiry. In this case channel 2 is always in idle mode.

15 Analyzer is in idle mode Analyzer is

16 Analyzer is powering up (both channels are present).

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

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

You should be aware of two exceptional conditions:

- If a Trigger Event occurs during the before-Trigger recording, the before-Trigger color changes to the after-Trigger color to indicate that not all the expected data was recorded pre-Trigger.

- When you click **Stop** before or after a Trigger Event, the Progress Bar adjusts accordingly to begin uploading the most recently recorded data.

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

Recording Status

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

— Trigger?

— Triggered!

— Uploading

After recording stops,

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

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

To abort the upload process,

- 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. The status will display one of the following:

No Sync - the system is not synced to any piconet

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

Syncing to [XXX]... -- The system is attempting to synchronize to a piconet where the device with BD_Address XXX is the master.

Synced to [XXX] - The system is synchronized to a piconet where the device with BD_Address XXX is the master.

Monitoring[BTTrainer] - in case the BTTrainer application is active, the system monitors its Bluetooth activities

Recording [XXX] - system is recording the Bluetooth traffic of the piconet where the device with BD_Address XXX is the master. Or, it is recording the traffic of the BTTrainer, in case the BTTrainer is active.

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

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

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

Search Status

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

Zoom In

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

- Click on the Tool Bar.

Zoom Out

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

- Click on the Tool Bar.

4.4 Tool Tips

Throughout the application, tool tips provide useful information.

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

4.5 BTTracer Analyzer Keyboard Shortcuts

Several frequently-used operations are bound to keyboard shortcuts.

Table 2: Keyboard Shortcuts

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

5. Recording Wizard

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

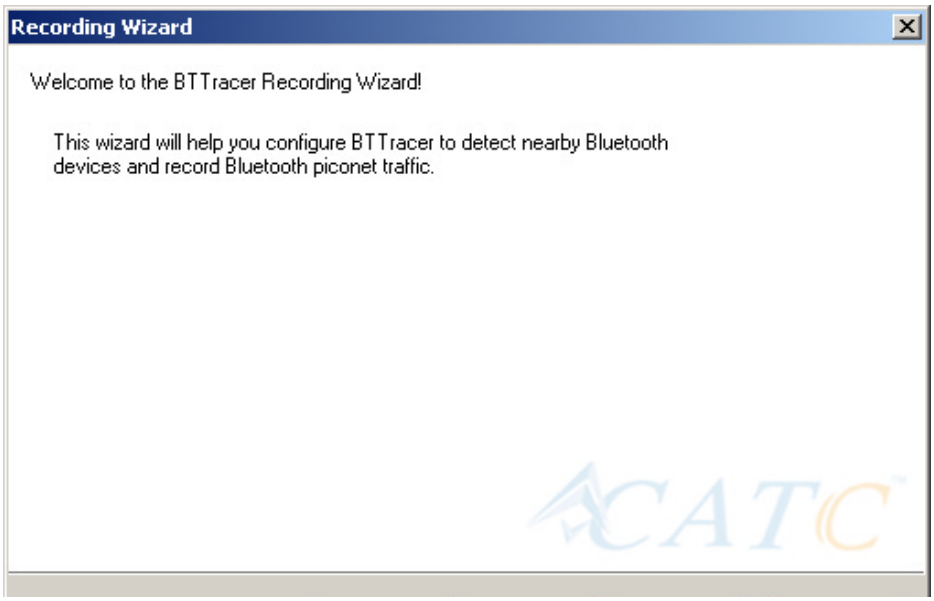
In BTTracer version 2.1, when using two modules, the Recording Wizard can be used to synchronize to a piconet with a basic hopping sequence. The Wizard does not support synchronizing to piconet using Adaptive Frequency Hopping. Also, the Recording Wizard operates only over Channel 1 of the analyzer.

Starting Recording Wizard

To start the **Recording Wizard**,

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

You see the **Recording Options** window:

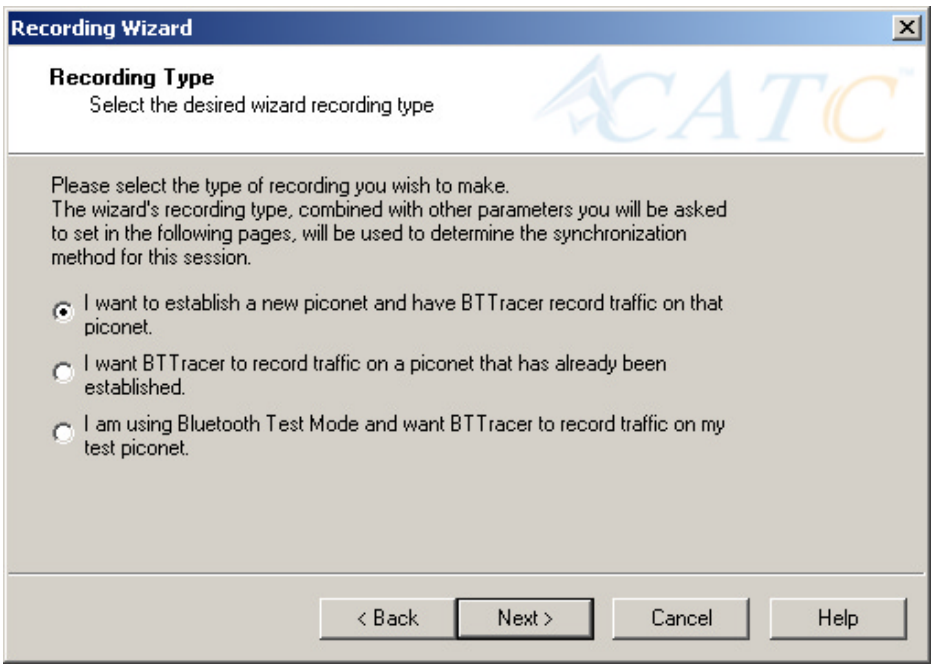


The **Recording Options** window has three buttons marked **Next**, **Back**, and **Cancel** that allow you to move forward or backward through the wizard or to cancel the wizard.

To begin advancing through the wizard,

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

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



- **I want to establish a new piconet and have 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.

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

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

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

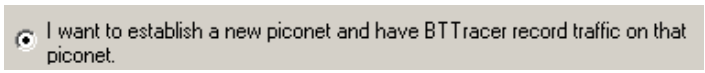
  This option lets BTTracer create either a single frequency range recording of a range that you specify or create a recording of a limited hop frequency range consisting of 5 frequency hops.

5.1 Recording a Traffic on a New Piconet

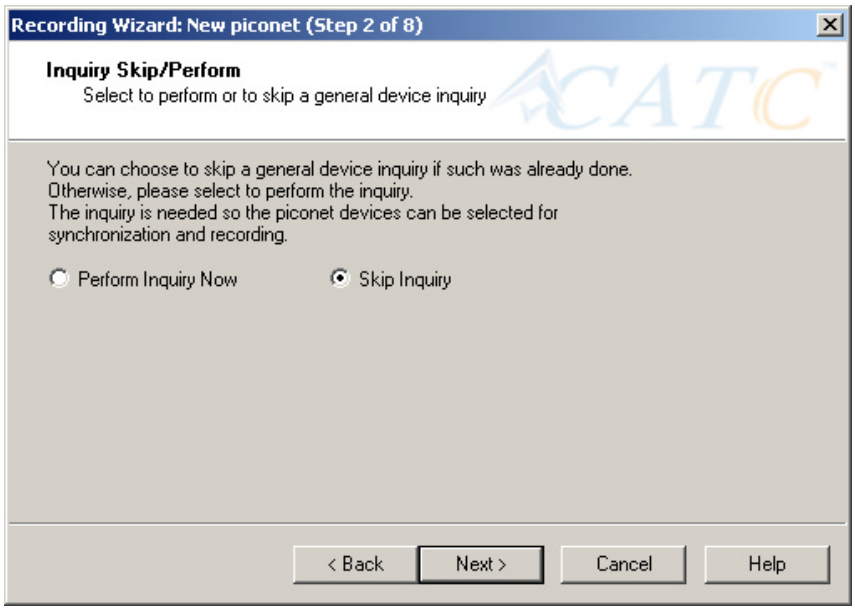
The **New Piconet** option shown in the previous screen presents users with the means of recording the traffic from a new piconet. This option will cause a sequence of screens to prompt you for information such as the piconet Master address.

The following steps 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**.



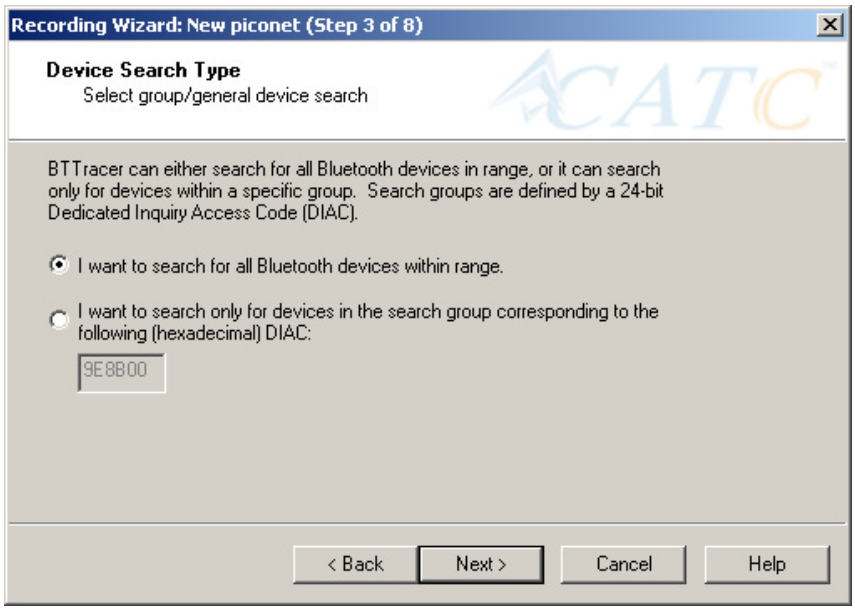
The following screen displays.



Step 2 Select **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**

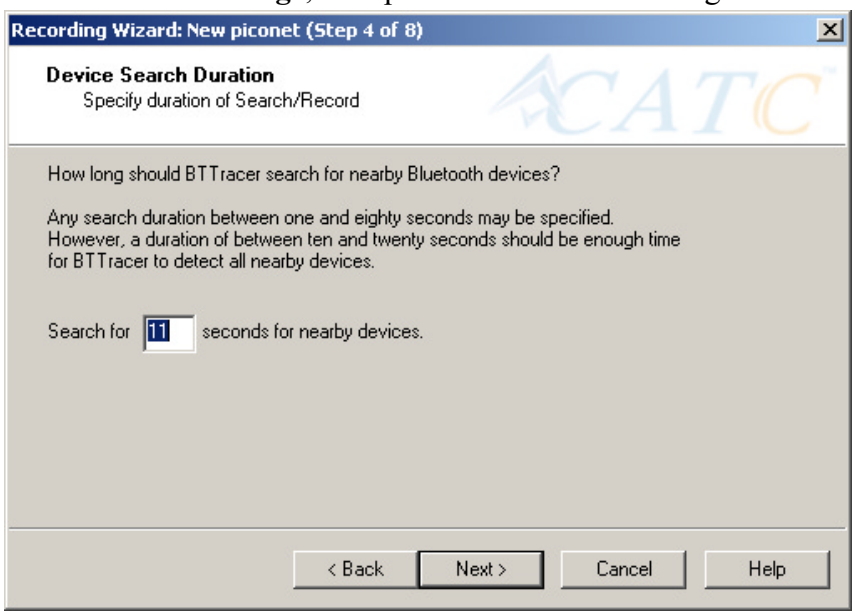
  This option will cause BTTracer to search for all Bluetooth devices that are in range and ready to transmit and receive data (i.e., in *Inquiry Scan Mode*)

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

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



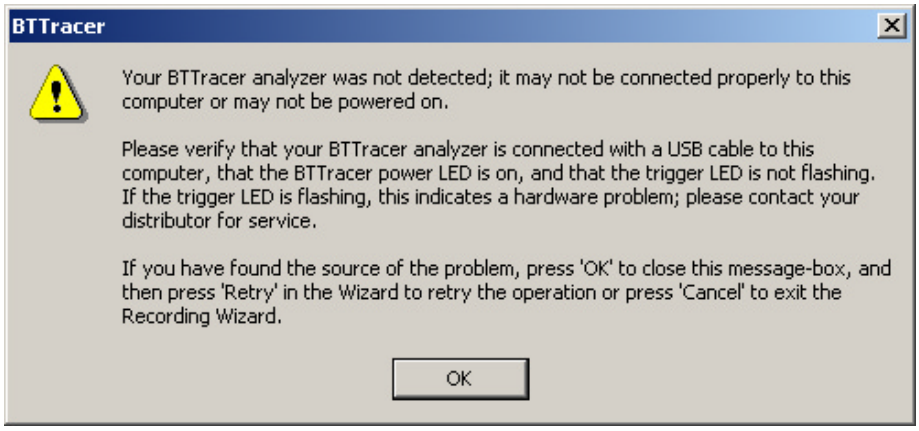
You will see two options:

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

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

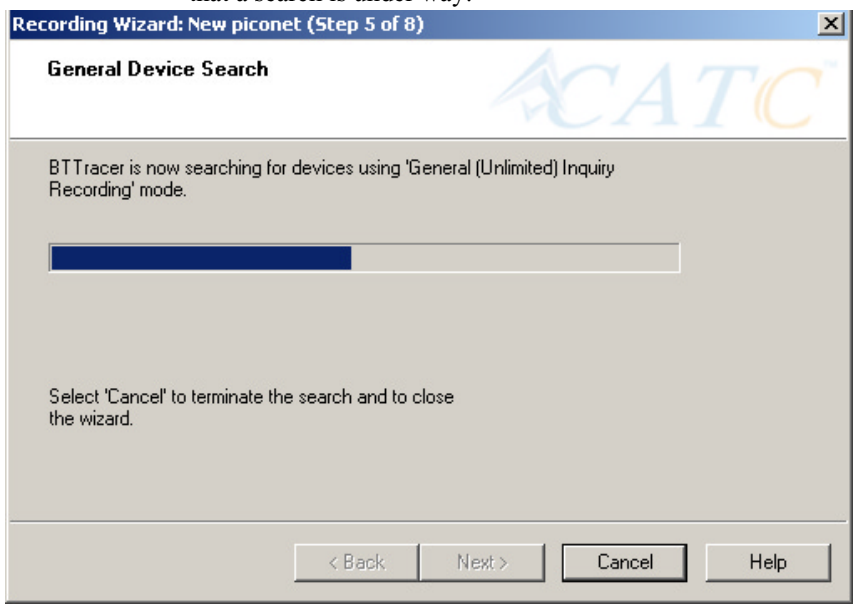
Step 5 Press **Next**.

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

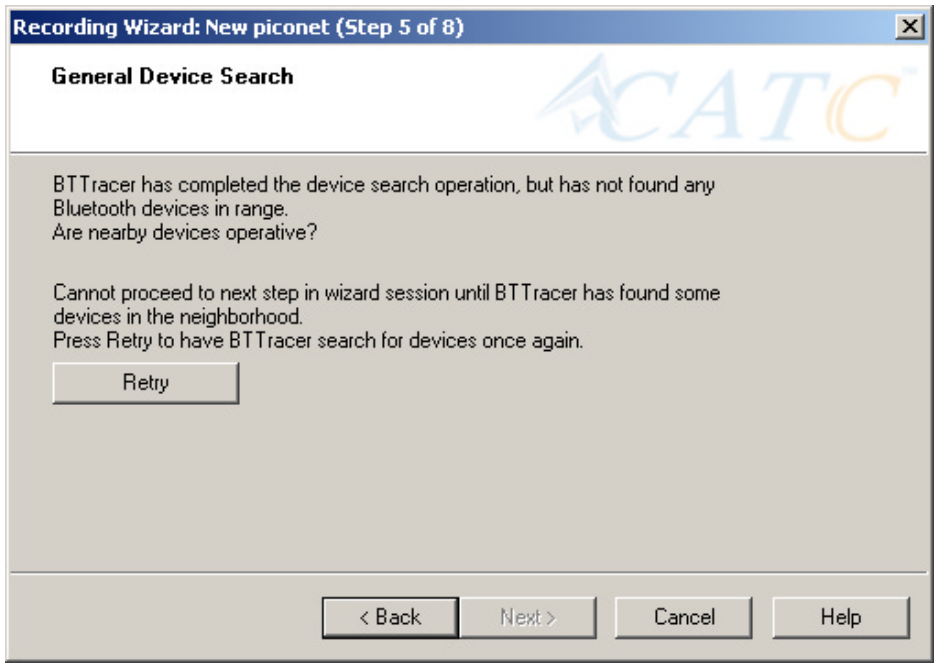


Clicking **OK** will close the message box.

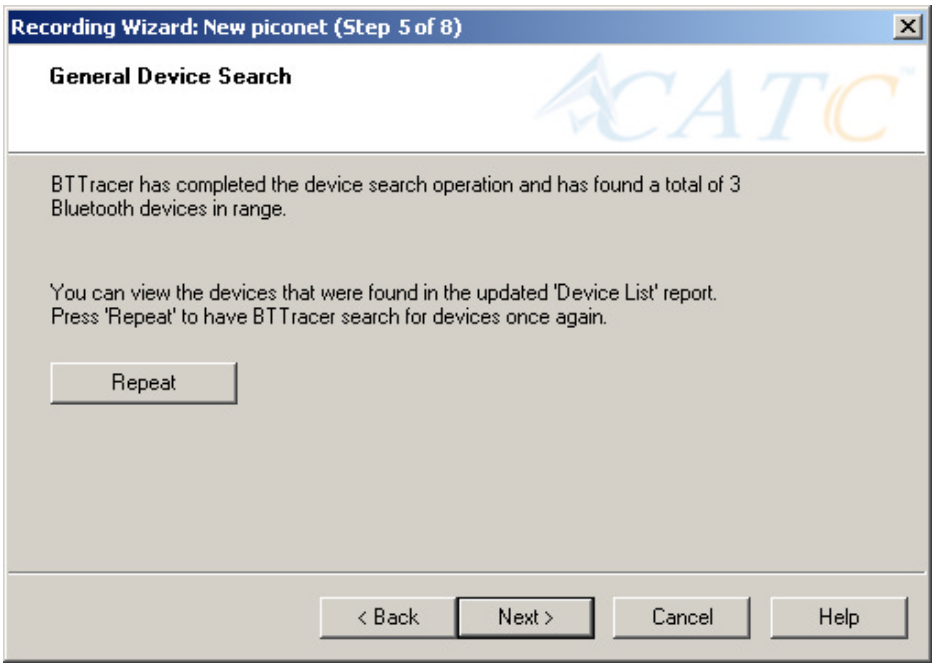
If BTTracer passes the hardware test, it will search for devices. The Recording Wizard will display a progress bar and a message telling you that a search is under way:



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

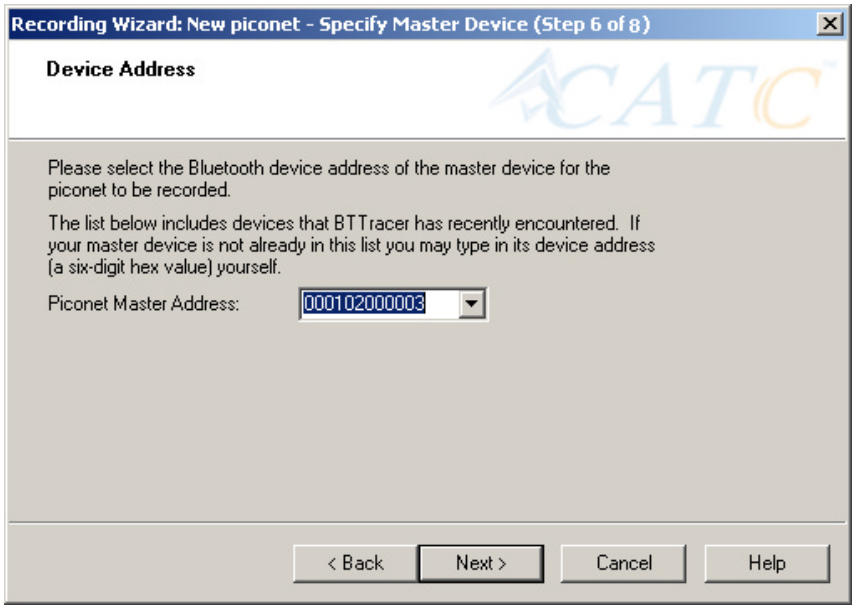


If devices found, the Recording Wizard will display the following screen:



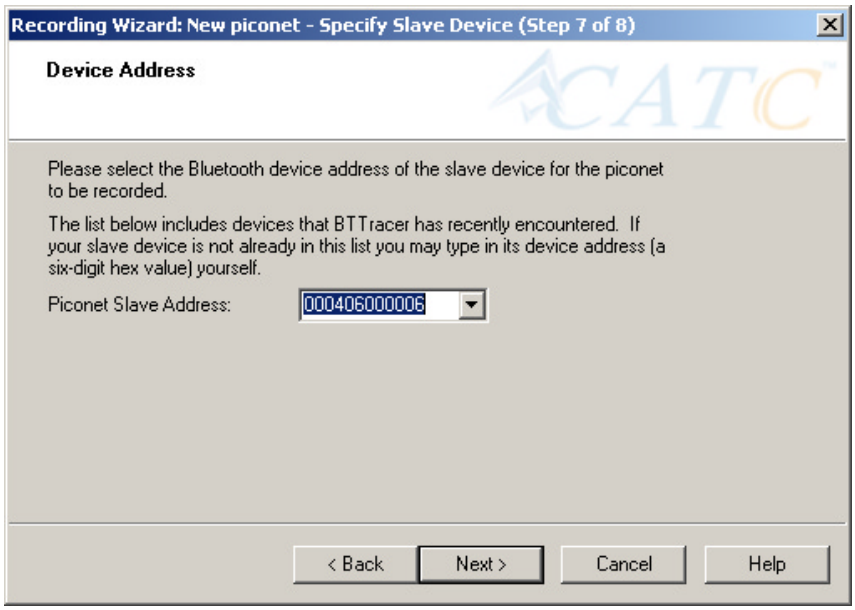
Step 6 Press **Next**.

The following window will display:



Step 7 Select from the drop-down menu the hexadecimal address for your Master device. If you do not see your device's address, you may type it into the text box yourself.

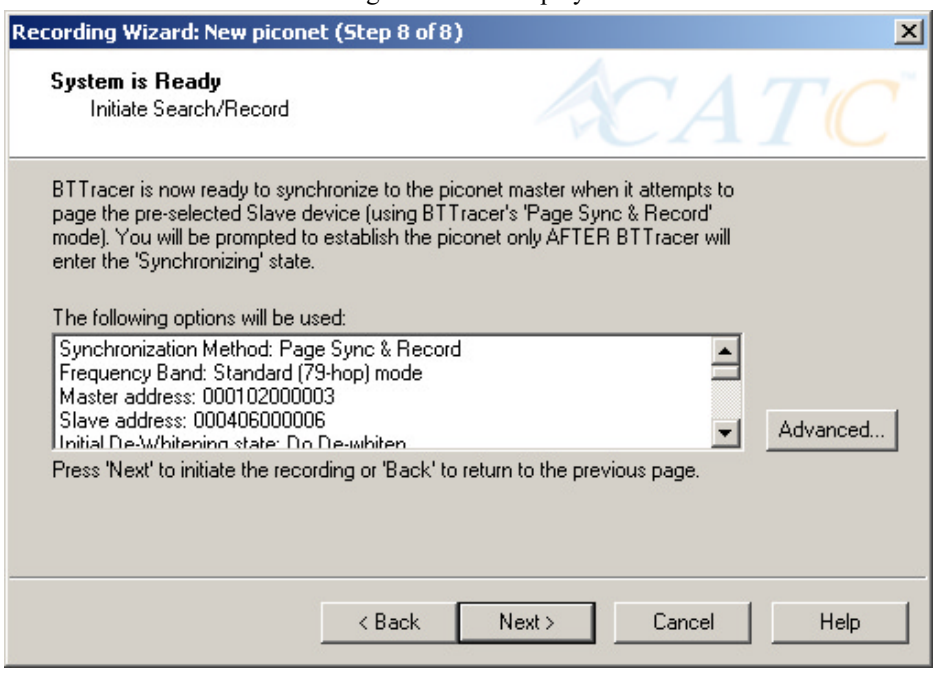
The following window will display:



Step 8 Select from the drop-down menu the hexadecimal address for your slave device into the box labeled **Piconet Slave Address**. If you do not see your slave's address, you can type it into the box.

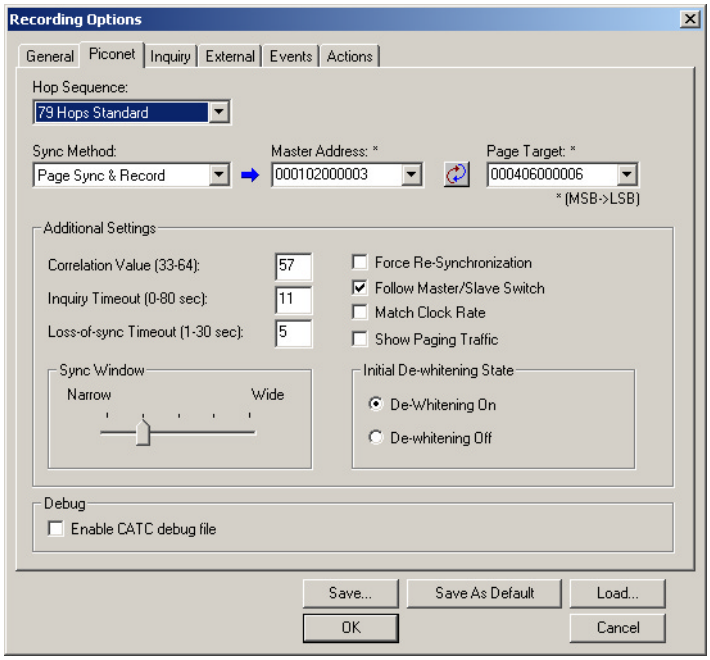
Step 9 Press **Next**.

The following screen will display.



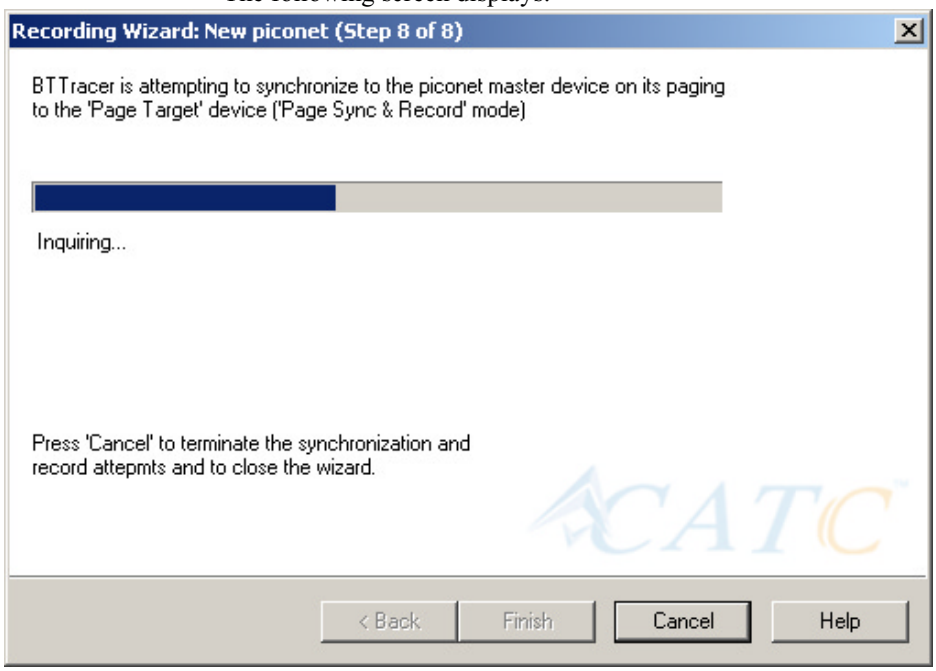
This screen displays the settings you selected.

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



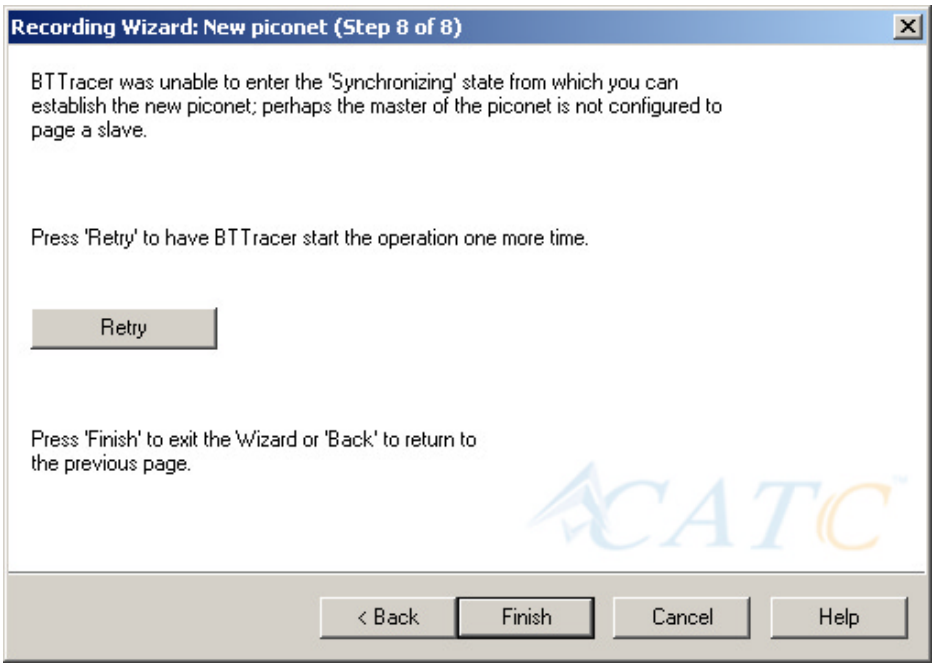
Step 10 Press **Next** to advance the Recording Wizard to the next screen.

The following screen displays:

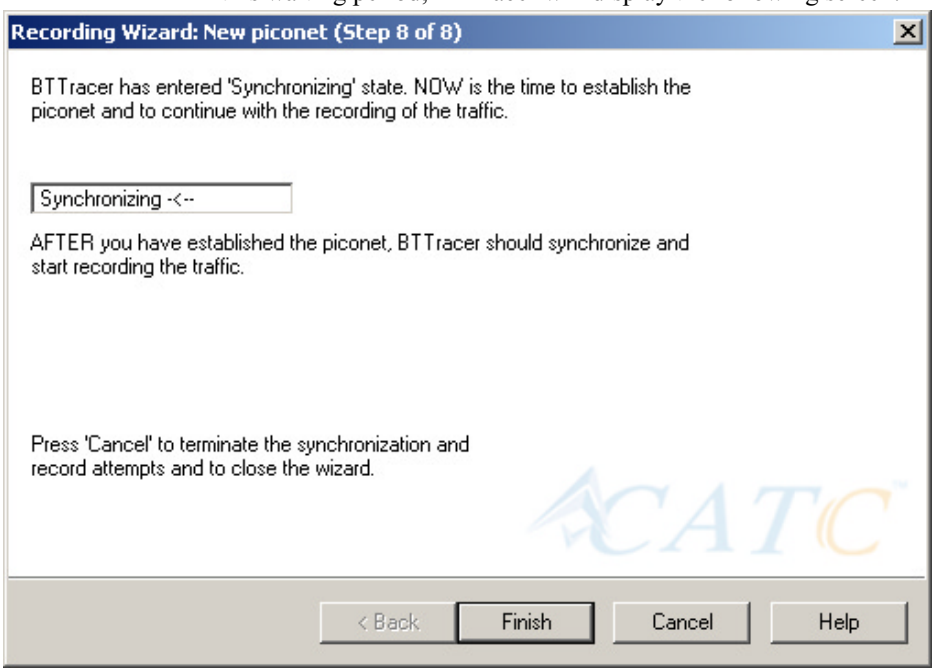


BTTracer pages the Master and if specified in Step 8, the Slave devices.

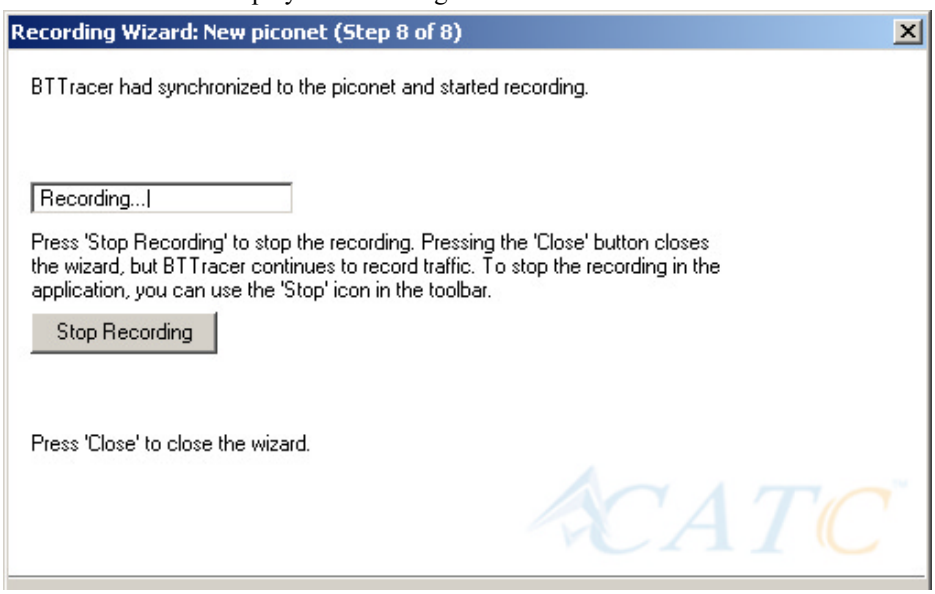
If BTTracer is unable to complete its pages, the following screen will display:



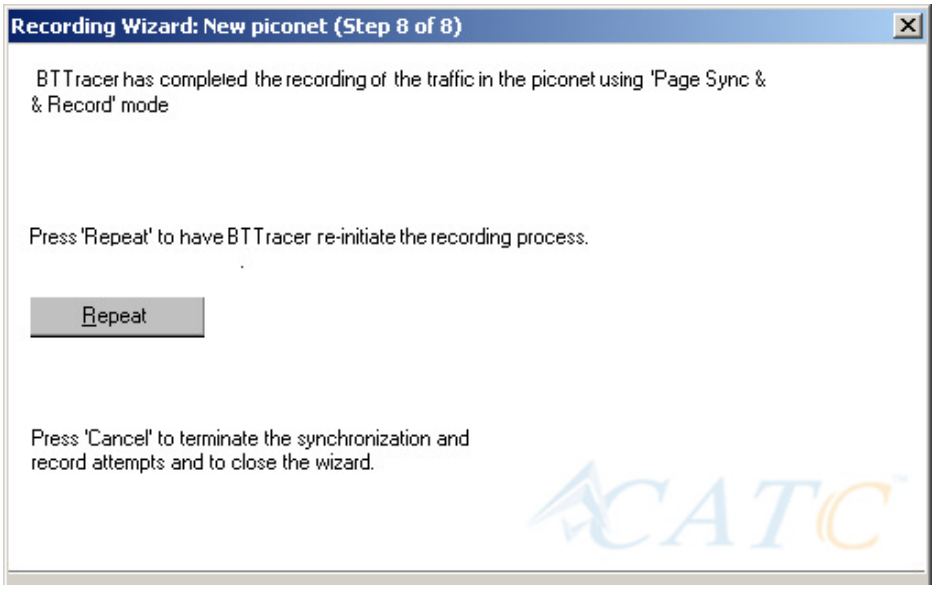
If BTTracer is able to complete its pages, it will enter into a synchronizing state and then wait for you to create the piconet. During this waiting period, BTTracer will display the following screen:



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



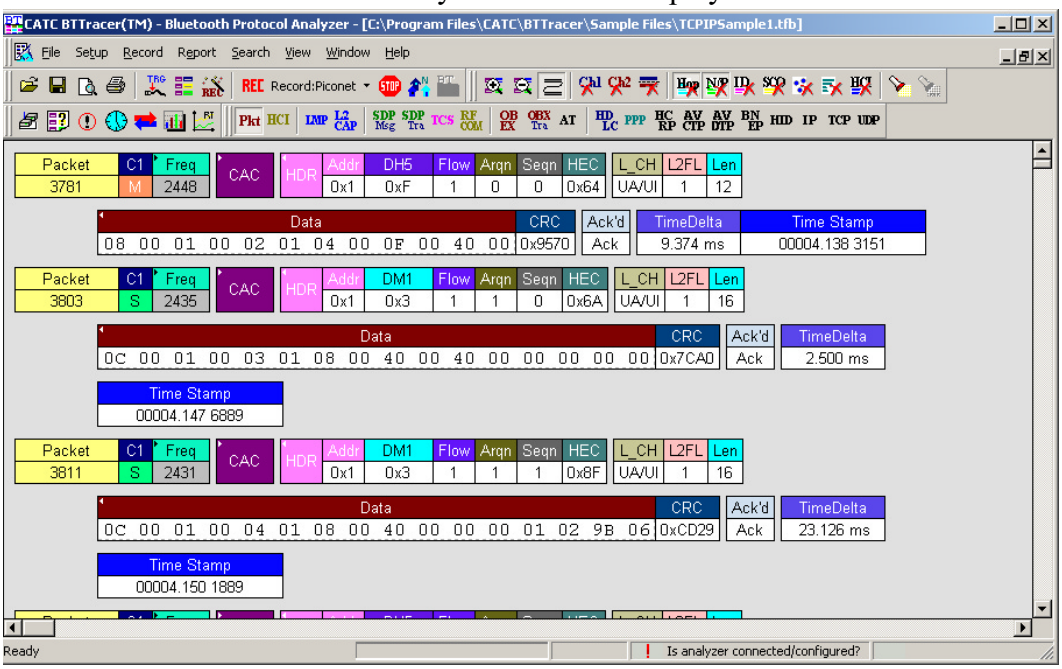
At the completion of the recording, BTTracer will display the following screen:



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

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

The wizard will close and your trace will display.

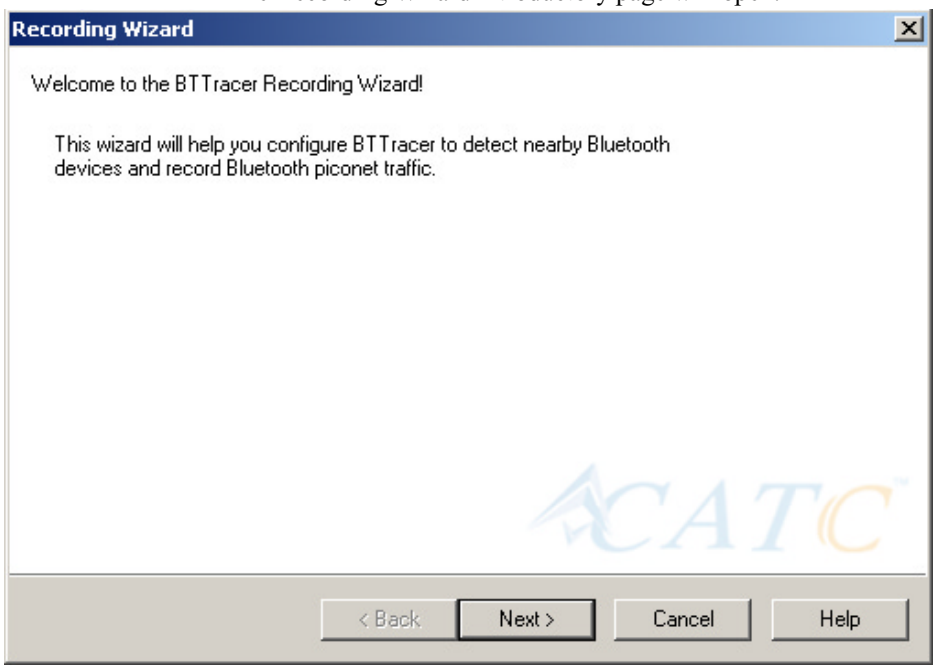


5.2 Recording an Existing Piconet

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

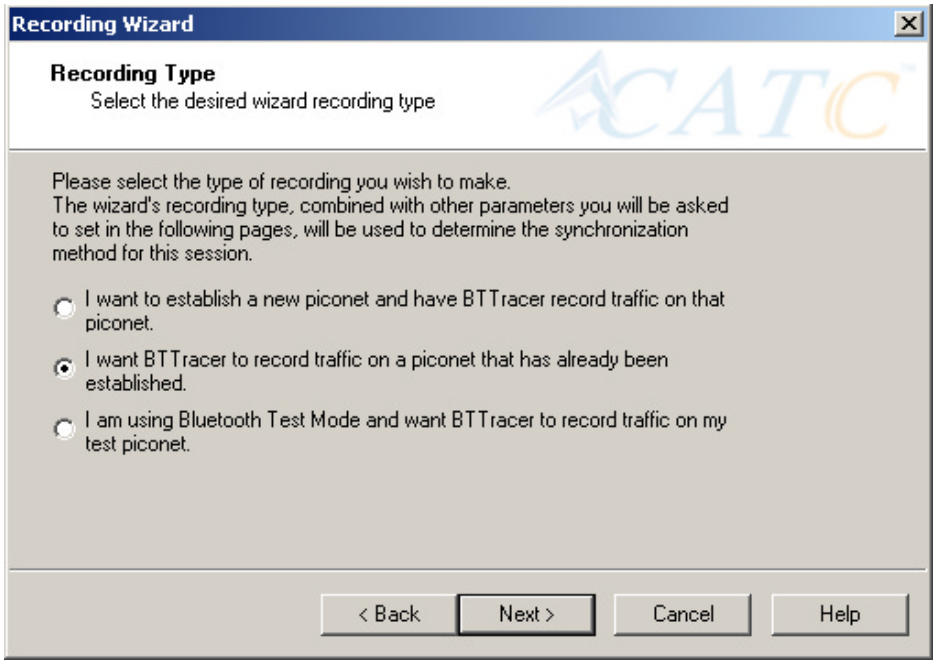
Step 1 To start the Recording Wizard, press or select **Setup > Recording Wizard** from the menu.

The Recording Wizard introductory page will open:



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

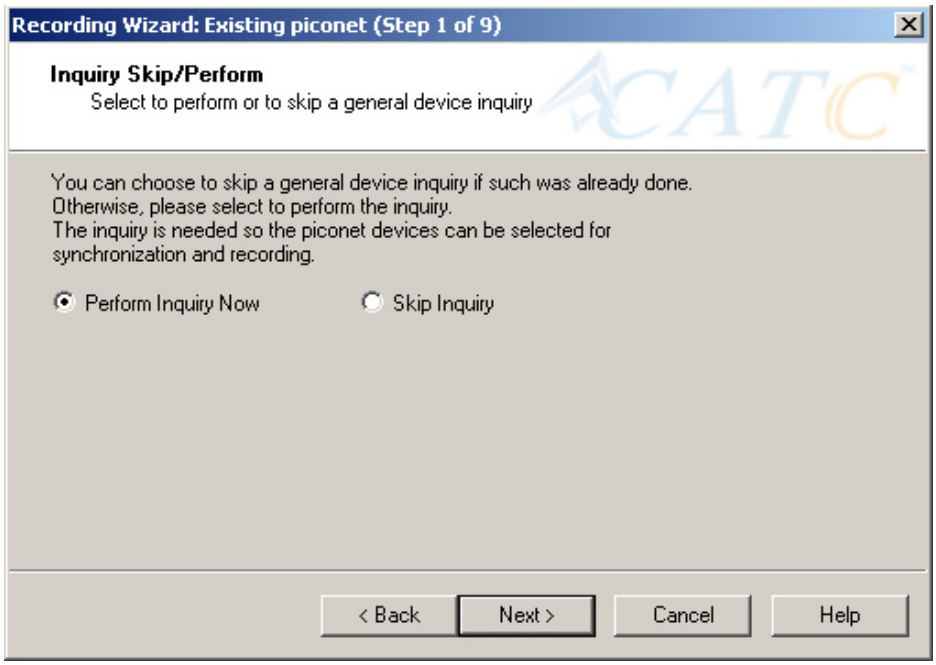
You will see three choices:



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

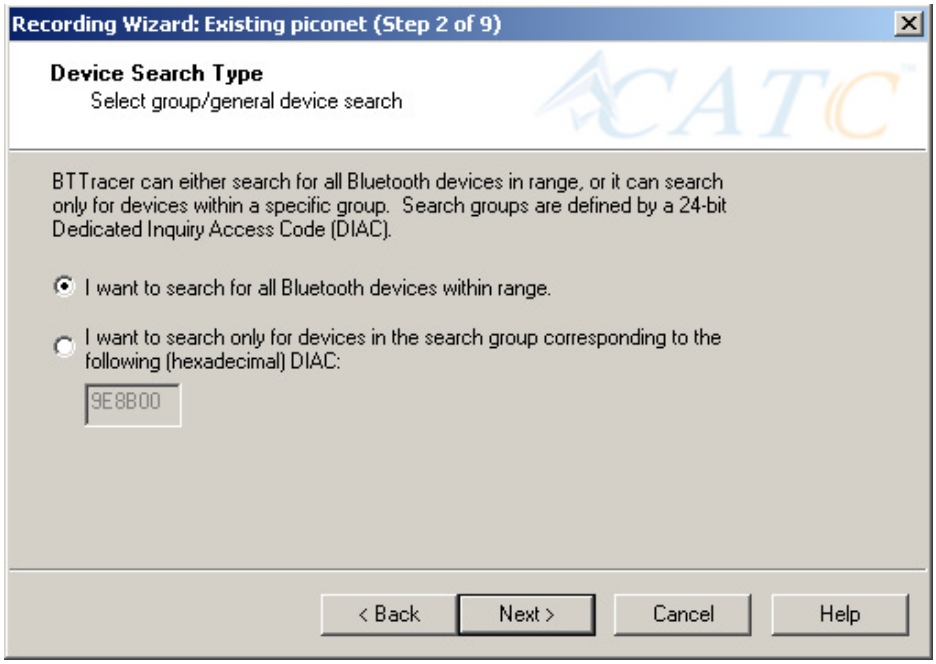
Step 4 Press **Next**.

You will see two choices:



Step 5 Select **Perform Inquiry Now**.

You will see two choices:

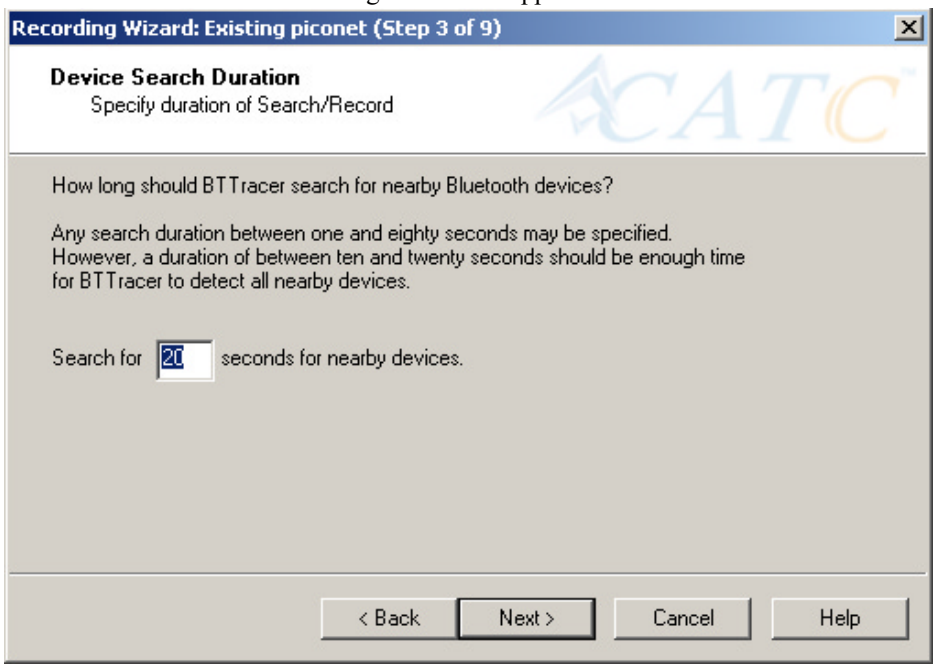


Step 6 Select the first option: **I want BTTracer to search for all Bluetooth devices within range**.

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.

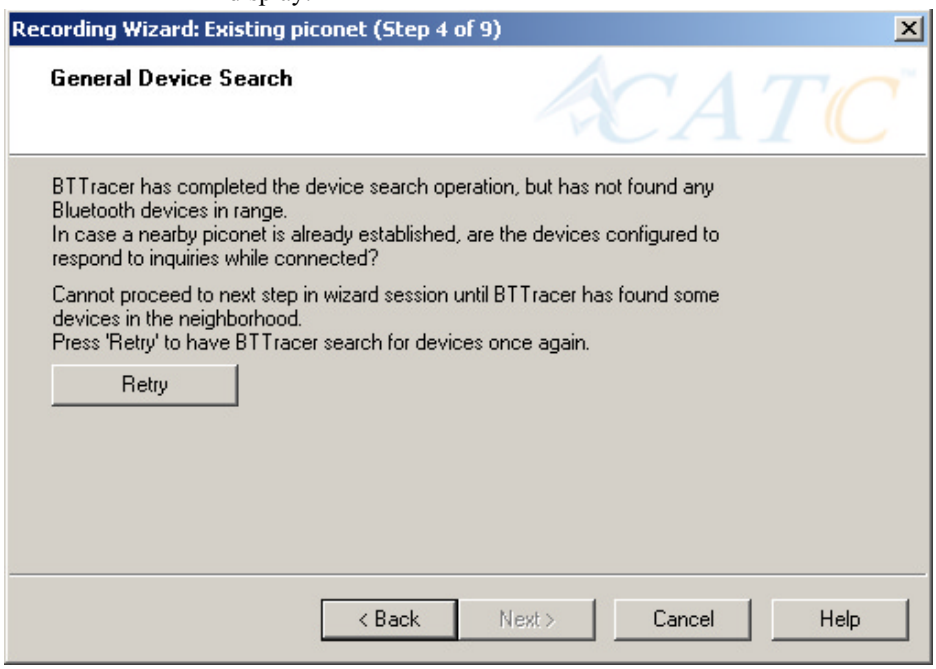
Step 7 Press **Next**.

The following screen will appear:

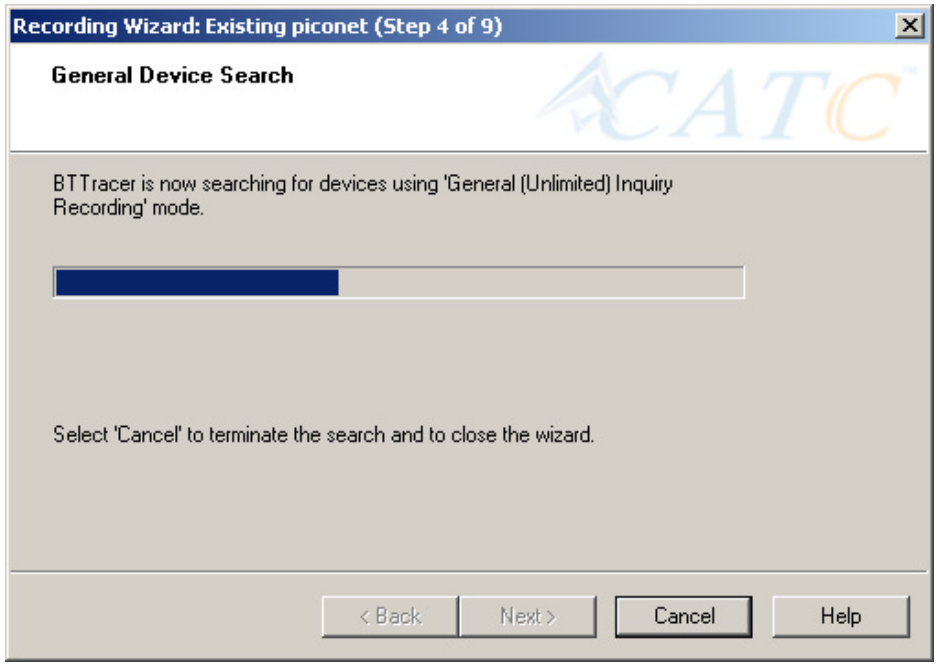


Step 8 If you want to change the search duration, type in a new value into the text box. Otherwise, use the default value (20 seconds), then press **Next**.

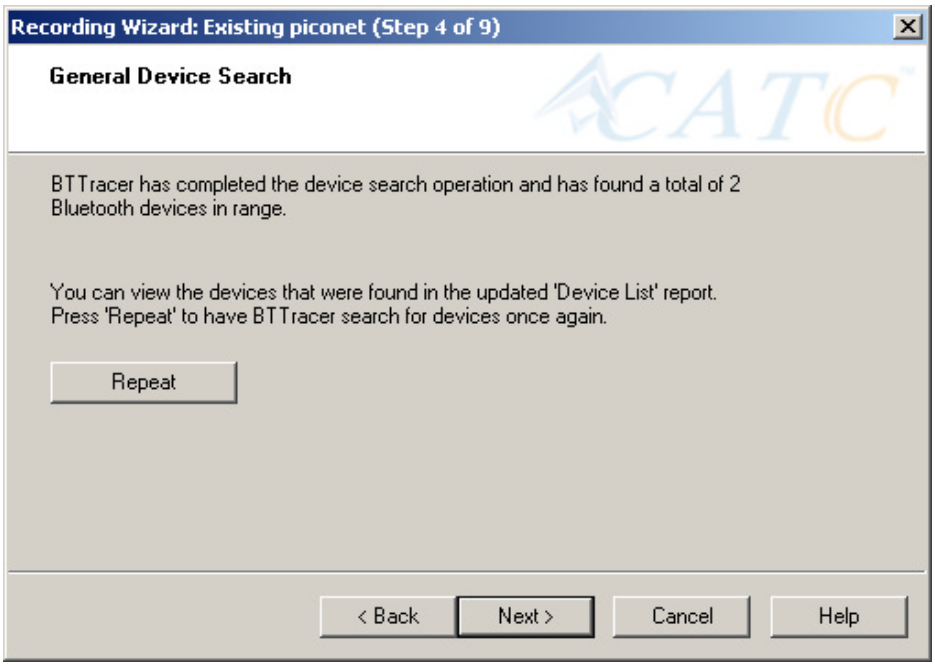
If BTTracer cannot detect other devices, the following message will display:



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



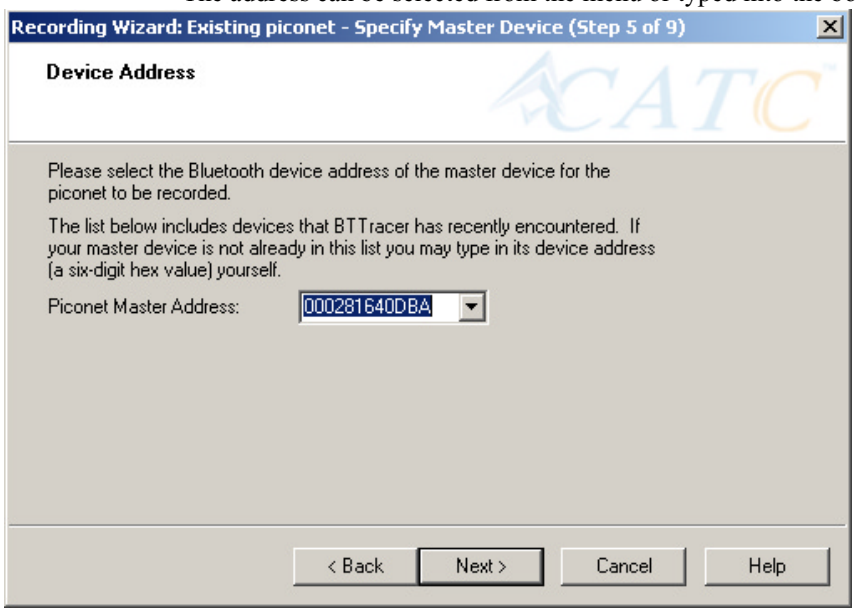
If BTTracer finds Bluetooth devices, it will display the following message:



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

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

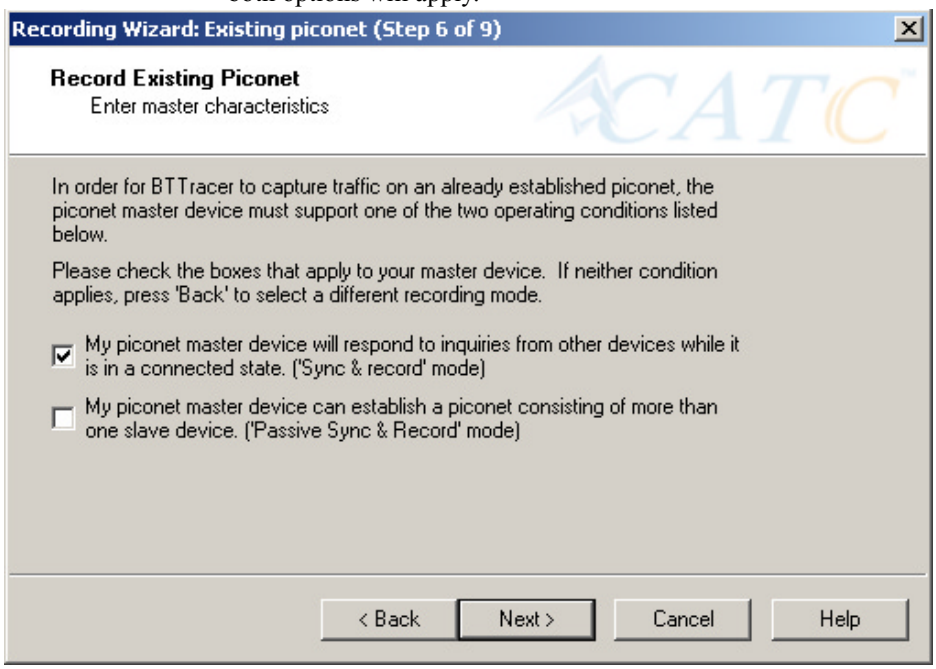
The following screen will prompt you for the Master device's address. The address can be selected from the menu or typed into the box:



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

Step 11 Press **Next**.

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



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

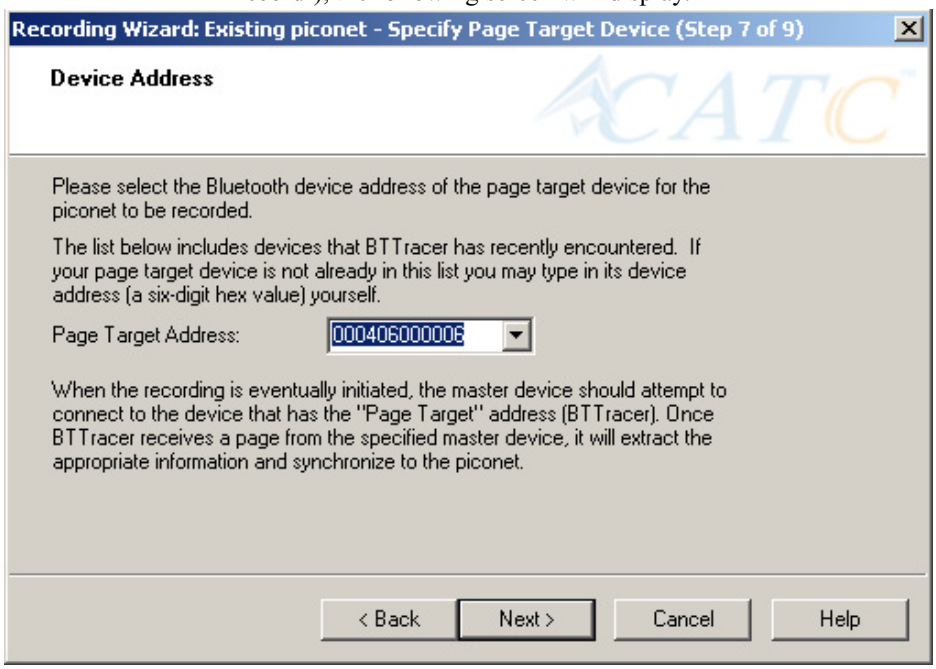
If the Master supports inquiries while in a connected state, select the first option. This will set BTTracer to use the 'Sync & Record' mode in its attempts to synchronize to the Master. This will also cause the wizard to skip to step 8.

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

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



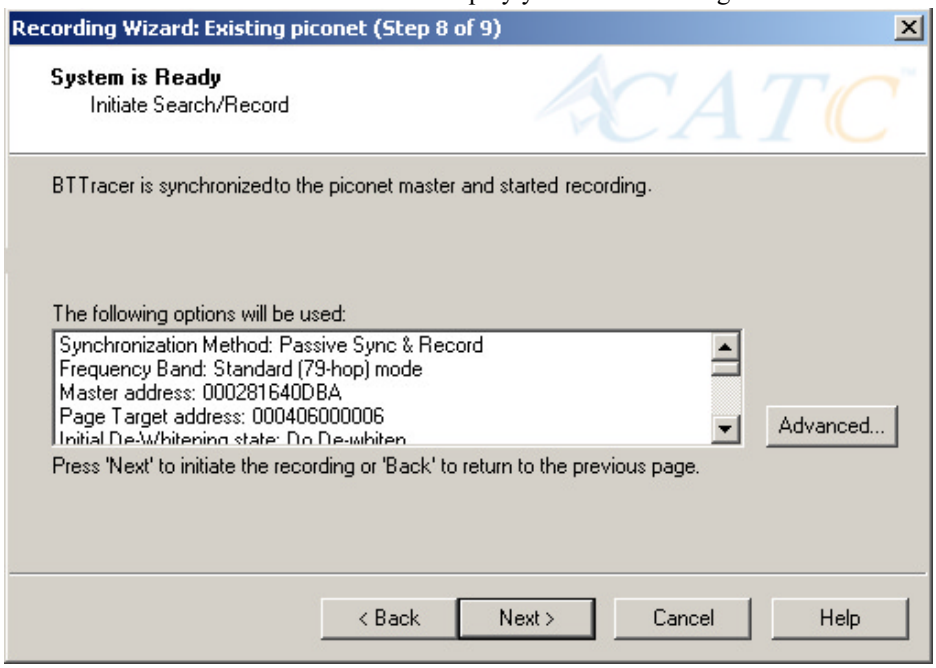
This screen asks you for the address of the Page Target device -- which in this case is BTTracer. Since the devices in your piconet are not able to respond to inquiries, BTTracer will not be able to page the devices and join the piconet. Instead, you will assign BTTracer an address here in this screen, 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 13 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 14 Press **Next**

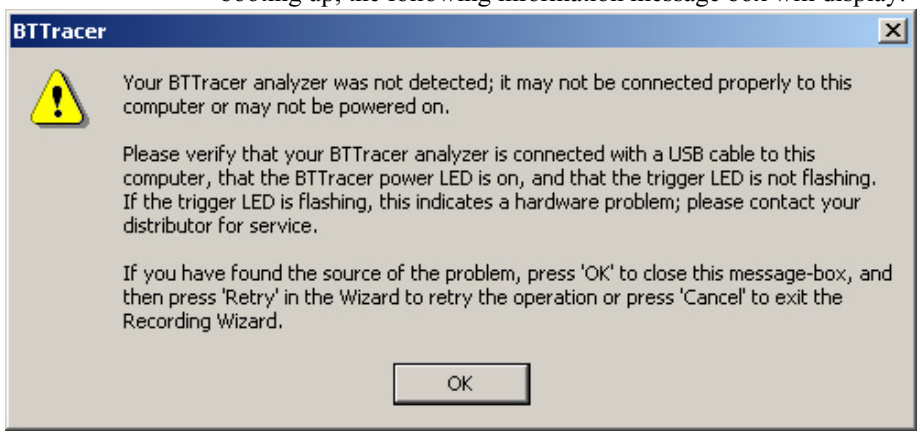
BTTracer will then display your current settings.



The **Advanced** button will open the Recording Options dialog box shown on page 55 and described in detail in Chapter 7.

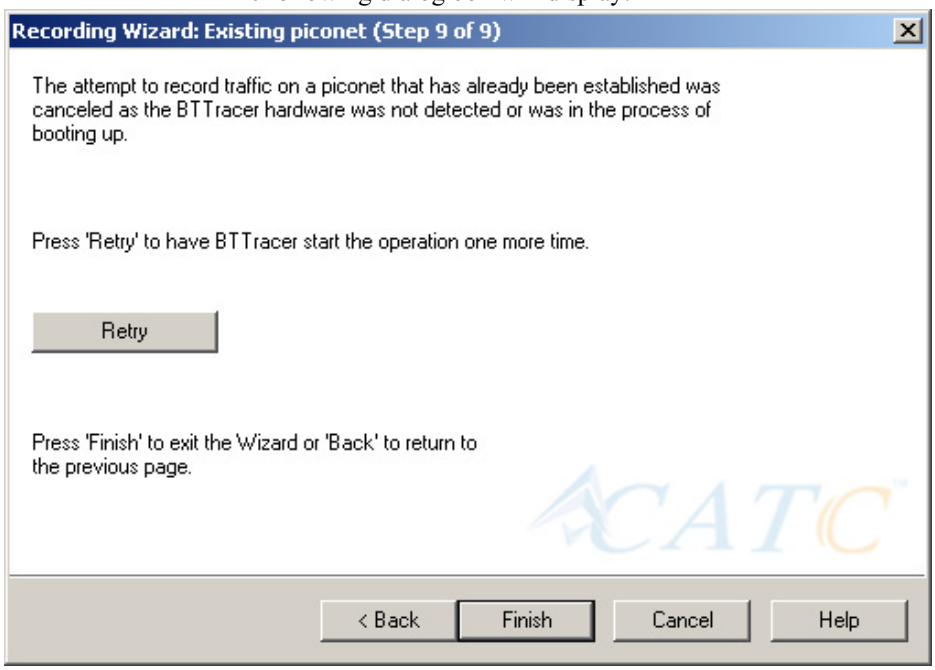
Step 15 Press **Next** to begin the recording.

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



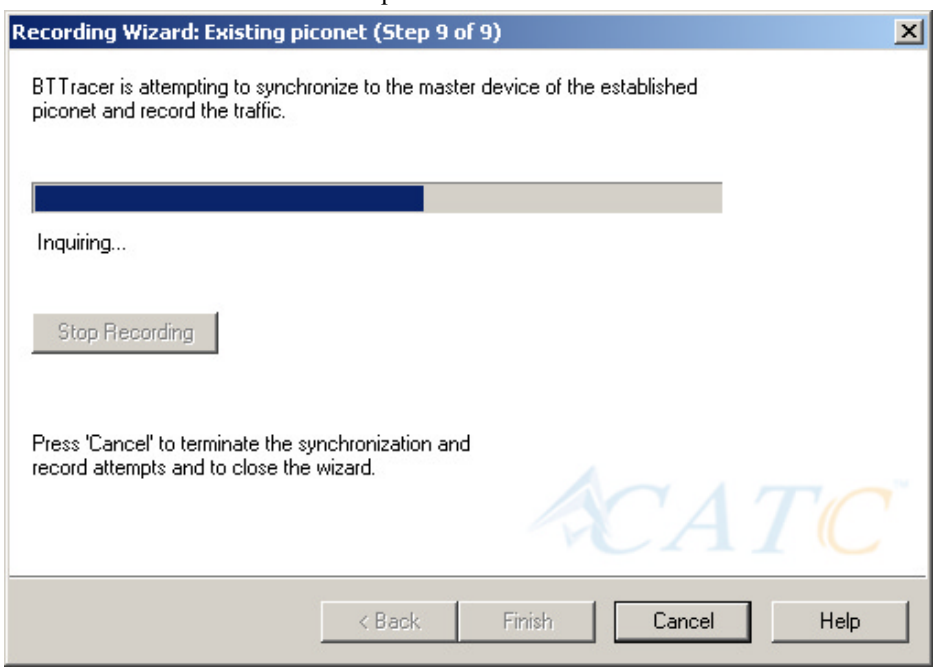
Step 16 If the above information box opened, press **OK** to close it.

The following dialog box will display:



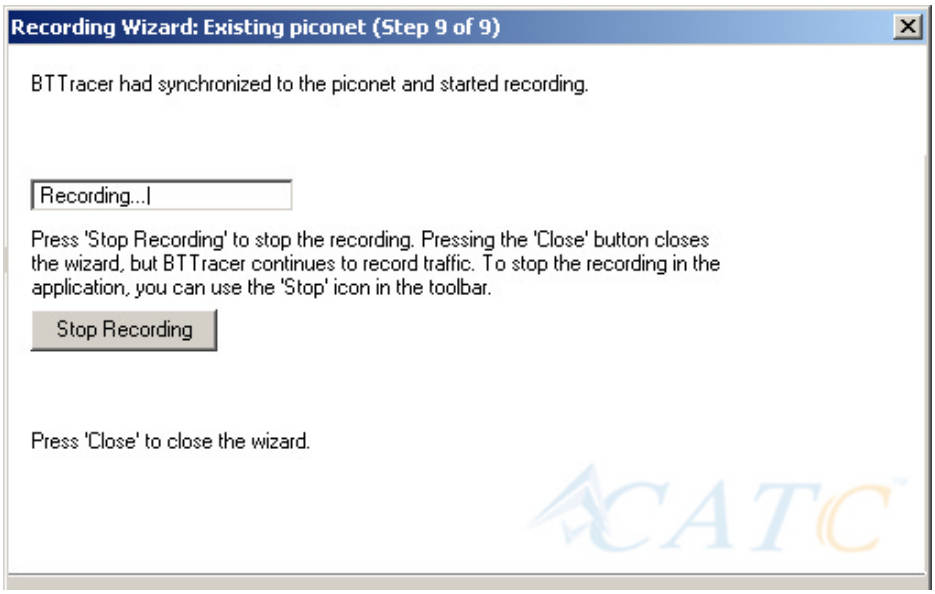
Step 17 Press **Retry** or **Back** to re-attempt the process.

If the hardware failure described above do not occur, 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 18 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 19 When finished, press **Close** to close the Recording Wizard.

5.3 Recording in Test Mode

A Test Mode recording allows you to limit the frequency hopping range that 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

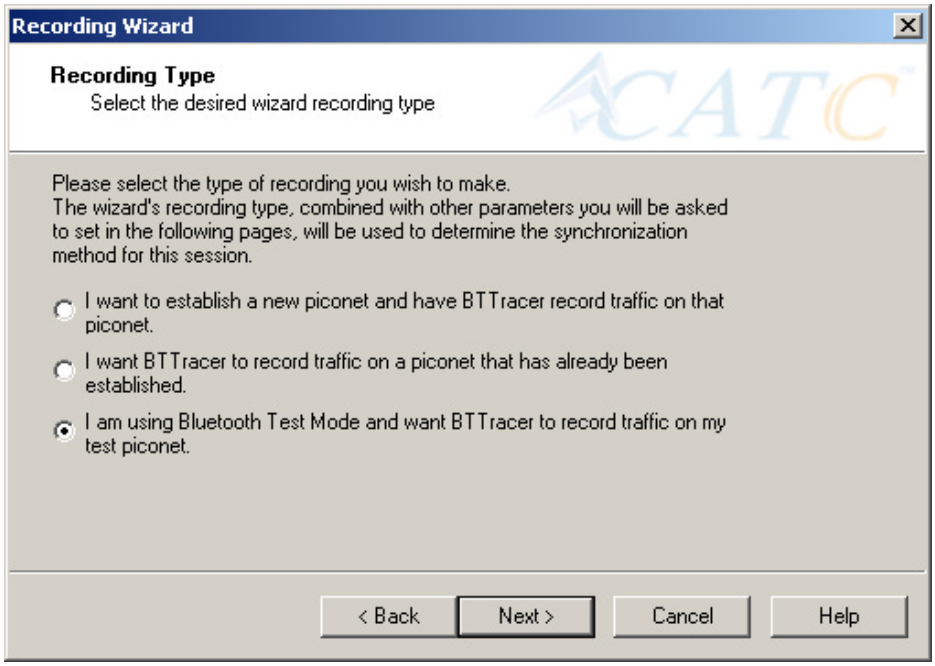
To record in Reduced Hopping Mode, perform the following steps:

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.

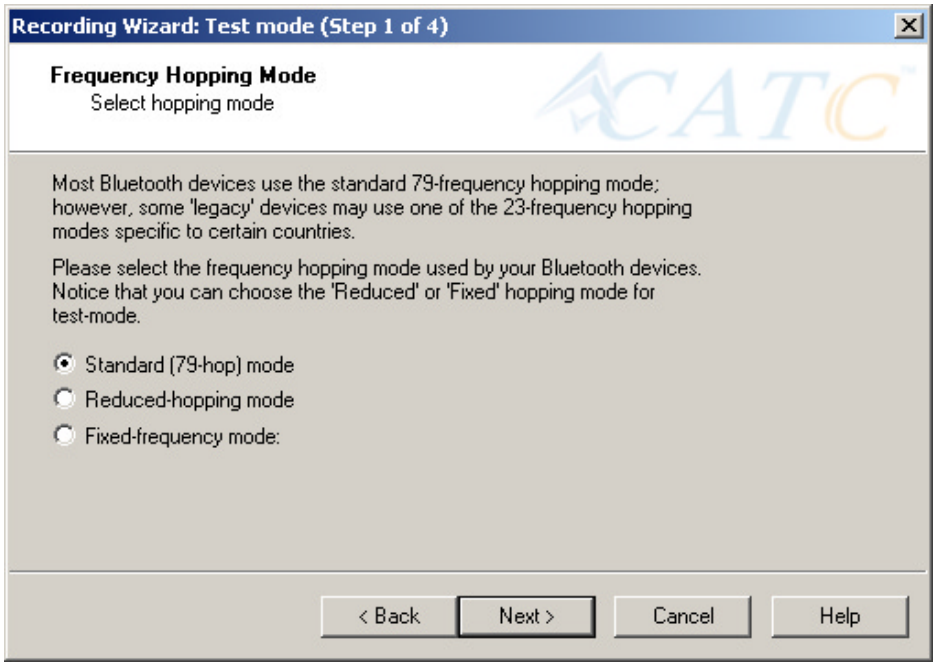
The following screen will display:



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

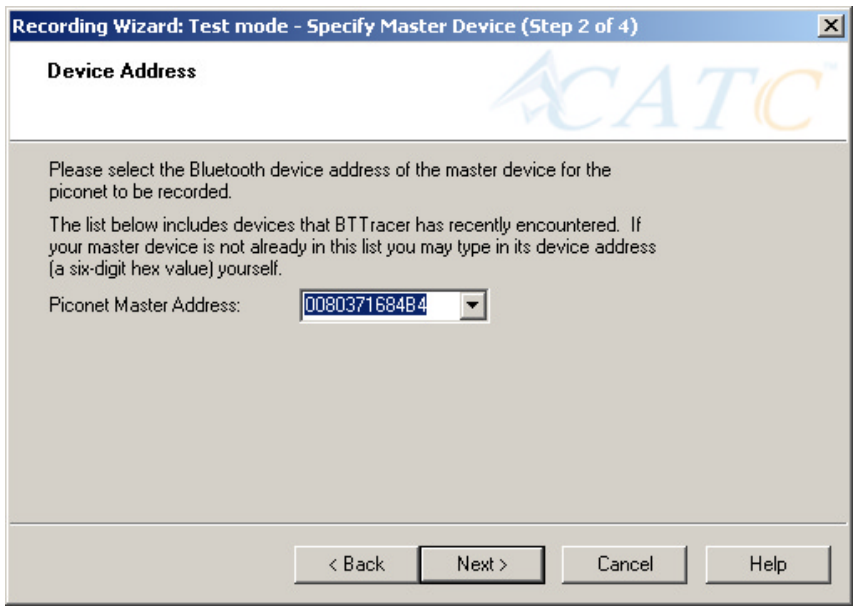
Step 4 Press **Next**.

The following screen will display:



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

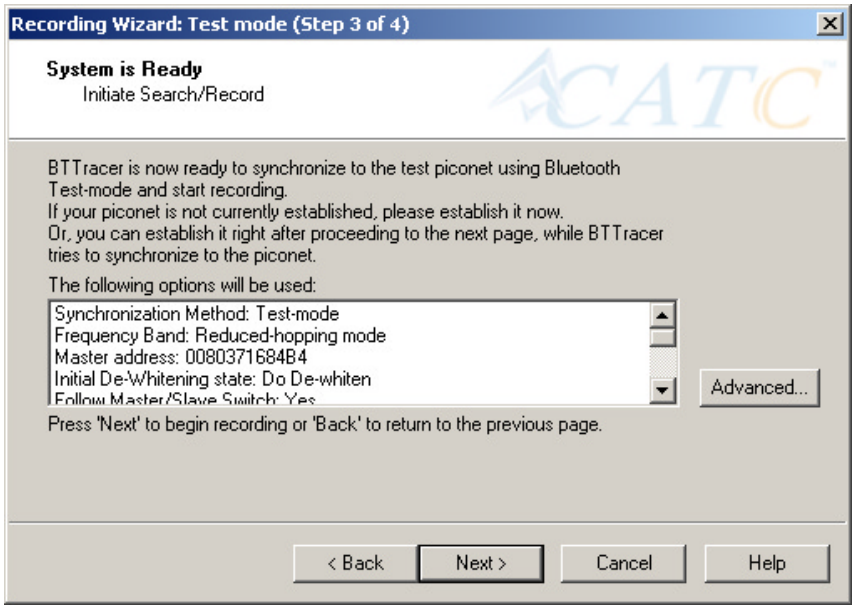
The following screen will display:



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**.

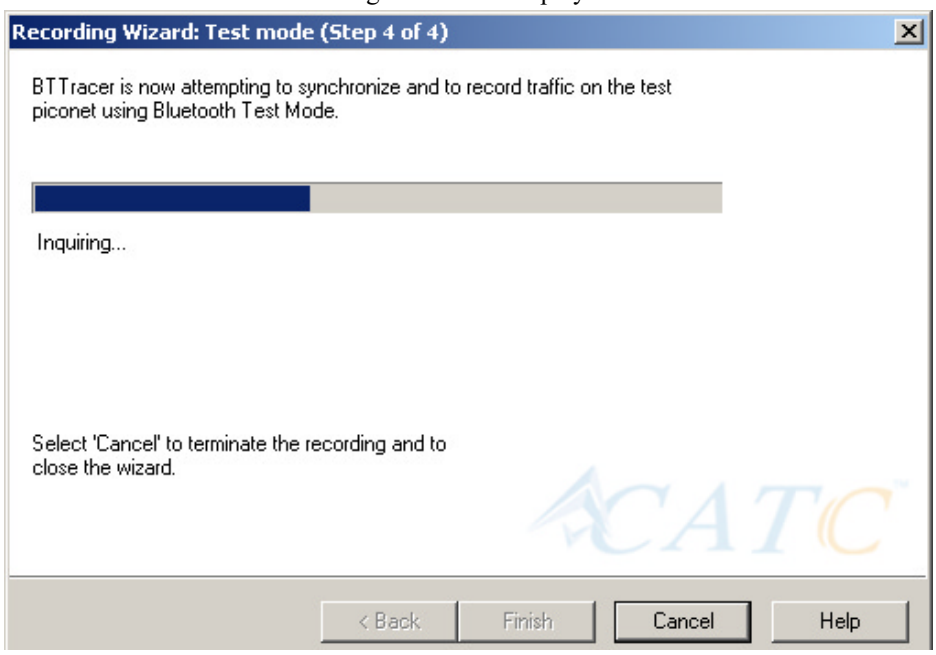
The following screen will display. This screen will show the current settings for the recording:



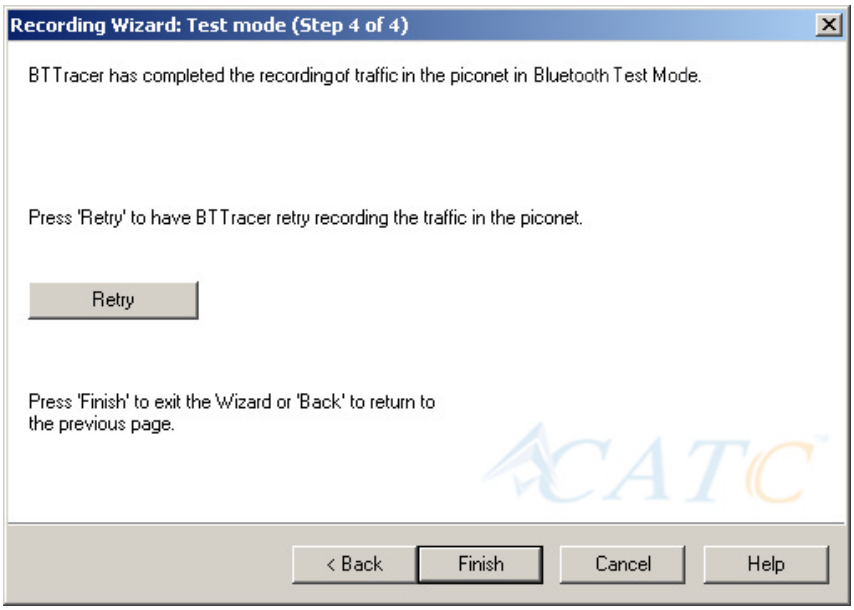
The Advanced button will open the Recording Options dialog box. See Chapter 7 for details on the Recording Options dialog box.

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

The following screen will display:



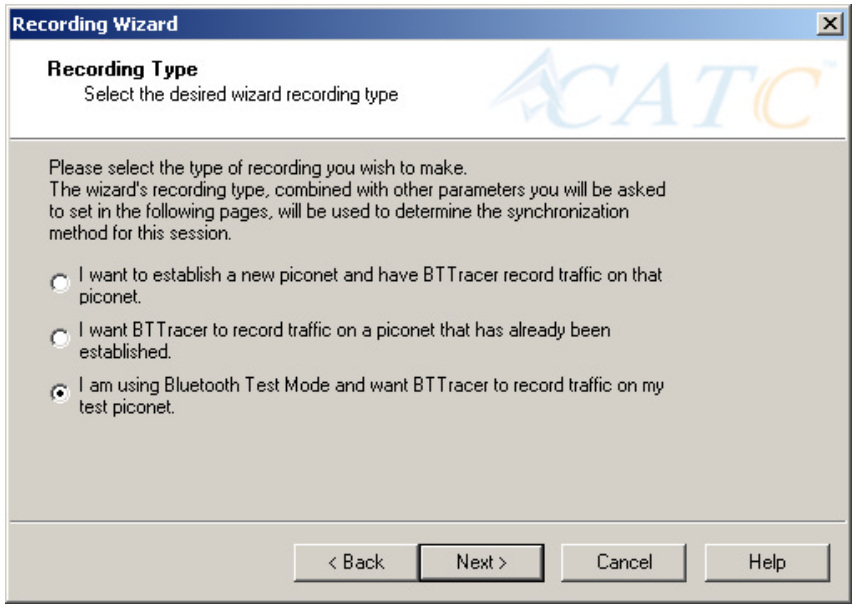
Step 9 When the recording finishes, the following screen will display. You can repeat the recording by pressing the **Repeat** button.



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

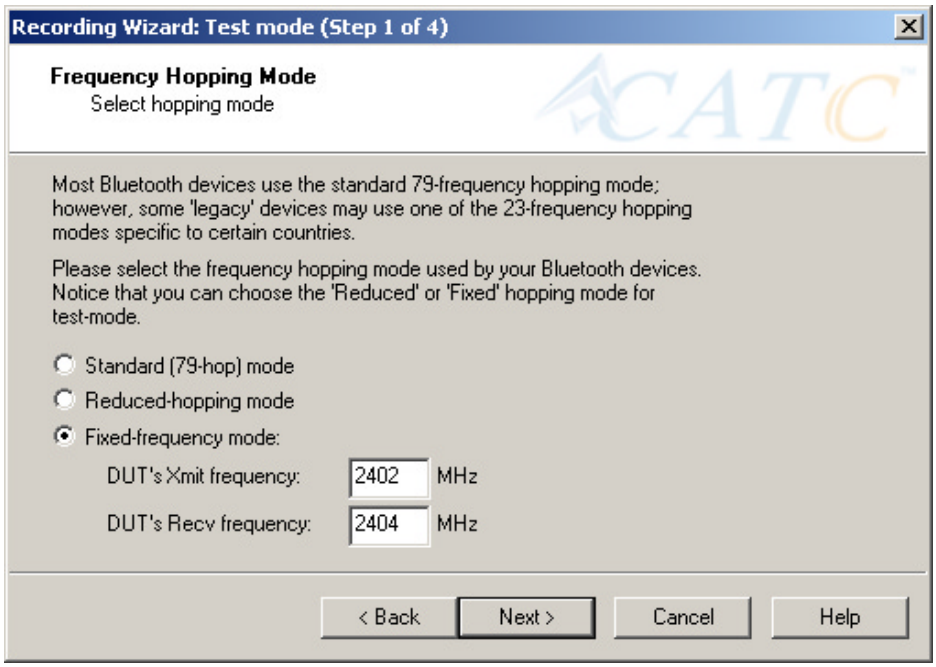
5.4 Recording in Single Frequency Mode

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



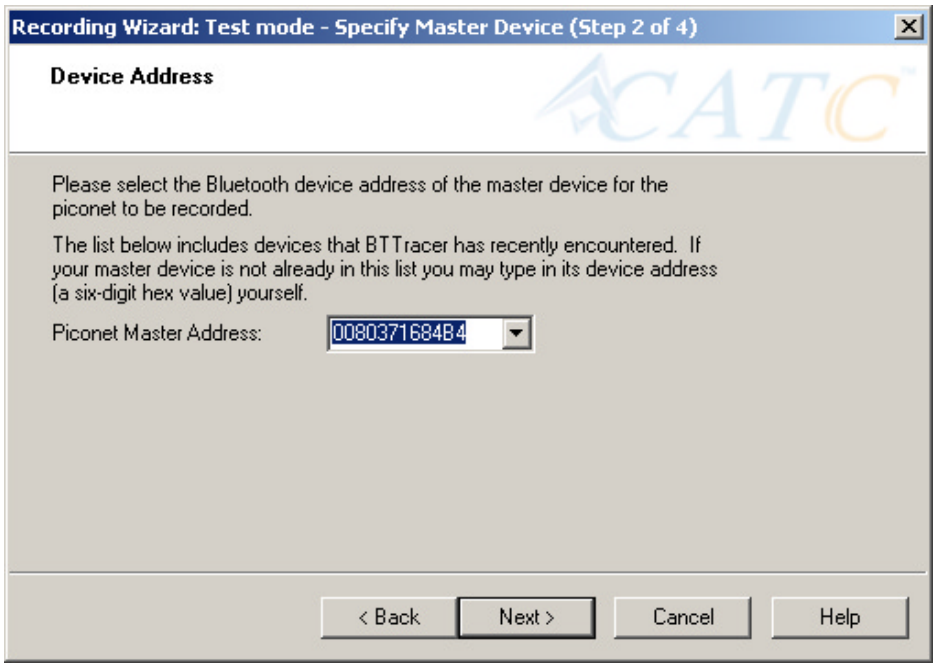
and click **Next**.

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

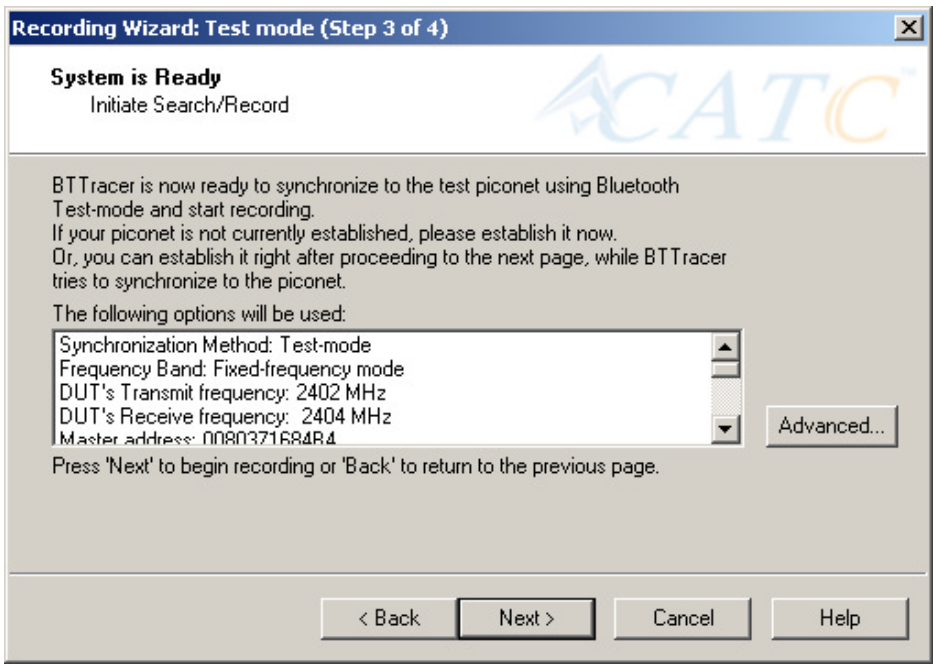


Step 3 In the Master Device address box, enter the BD Address for

your Master Device.

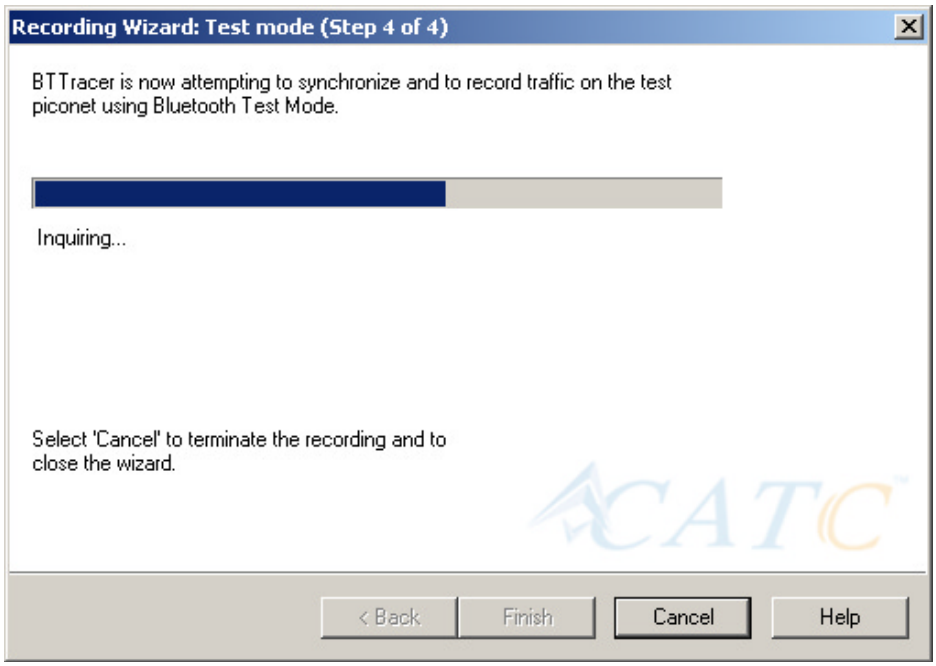


Step 4 Press **Next**.



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

device and begins recording.



6. Recording Options

While the Recording Wizard provides a "walk through" process for setting the recording options, you can get a more detailed view and set more parameters through the "Recording Options" dialog box. The Recording Options dialog box presents all of the settings needed to make a recording. Once you have selected your recording options, you then select the recording mode by clicking the down-arrow on the Record button and selecting from the three mode options: Piconet, Inquiry, and BTTrainer. BTTracer will then use the relevant Recording Options for the selected mode. For example, if you select **Piconet** recording mode, BTTracer will use the options from the **Piconet** page in the Recording Options dialog box.

6.1 Recording Modes

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

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

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

Piconet recording

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

Note: When BTTrainer is active Piconet mode is disabled as the system is monitoring the BTTrainer's activity

Inquiry recording

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

'inquiry' page of the Recording Options. The recorded traffic would consist the transmitted packets as well as the responses received from Bluetooth devices in the area. As in the case of Piconet recording mode, when BTTrainer is active this mode is disabled as the system is monitoring the BTTrainer's activity.

BTTrainer mode

Configures BTTracer to record BTTrainer traffic. BTTracer is "forced" into this mode when the BTTrainer is activated. Here the BTTracer is dedicated to monitor the traffic received and transmitted by BTTrainer. Though BTTracer remains non-intrusive and does not generate any transmitted traffic, the BTTrainer can be an active member of the piconet.

In this mode the BTTracer can also record the HCI traffic (commands and events) flowing between the application and the CATC's Bluetooth baseband. If the HCI traffic is enabled through the Recording options, the BTTracer includes it in the generated trace at the end of the recording session.

Once the BTTrainer application is closed, the BTTracer exits this mode, returning to one of the 'stand-alone' mode.

IUT:HCI mode

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

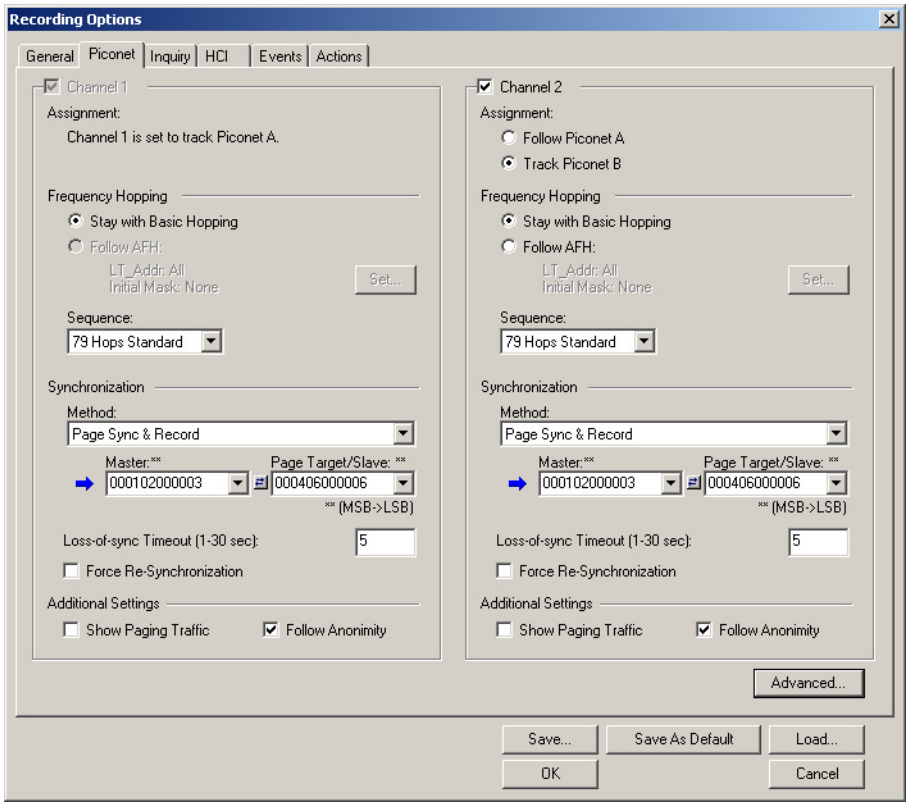
To record HCI traffic, first enable the recording of HCI traffic from IUTs. You do this in the HCI page of the Recording Options dialog. Then set the recording mode to something other than IUT:HCI. If you want to prevent the recording of HCI traffic from IUTs, disable it in the HCI page of the Recording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

6.2 Opening the Recording Options Dialog Box

To open the **Recording Options** menu, click

on the Tool Bar or select **Recording Options** under **Setup** on the Menu Bar.

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

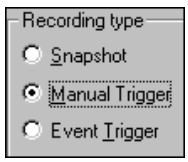


You will need to set options for each of the Recording Options pages. Generally, it is best to begin with the **General** and **Piconet** pages where you can set the type of recording, and then move on to the **Events** and **Actions** pages where you can set triggering events.

6.3 Recording Options - General

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

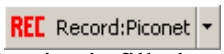
Recording type



The **Recording Type** box presents options that control 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 

on the Tool Bar and ends when either the selected buffer size is filled or you press the Stop button.

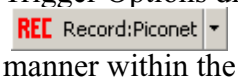
Manual Trigger

A Manual Trigger recording is a one that is manually begun and ended. Recording is begun by pressing

on the Tool Bar. Recording continues in a circular manner within the limits set by the buffer size. Recording ends when

is clicked on the Tool Bar or the Trigger button is pressed on the analyzer's front panel. If you press the Trigger button, recording will continue until the post-trigger memory has been filled.

Event Trigger

An Event Trigger recording is one that uses an event trigger to end the recording. Before recording begins, you define the event trigger in the Trigger Options dialog box. You begin the recording by clicking 

on the Tool Bar. Recording continues in a circular manner within the limits set by the buffer size. Once the trigger event occurs, some post-trigger recording occurs, then the recording ends.

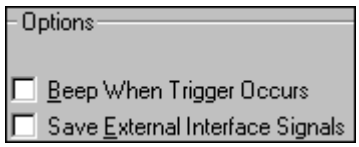
Note In this mode, the recording can be stopped manually in the same way as for "manual trigger" mode.

Options

The Options box contains two options:

Beep When Trigger Occurs

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

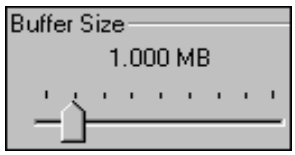


Save External Interface Signals

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

Buffer Size

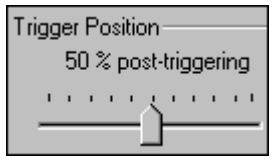
The Buffer Size box has a slide bar for adjusting the recording buffer size from 0.4 megabytes to 512 megabytes.



The Recording Type option determines how this buffer is used. Although there are 512 megabytes of physical memory in the analyzer, the efficiency of the recording ranges from 2:1 to 4:1 ratios of physical memory to actual Bluetooth traffic. Shorter Bluetooth packets yield a less efficient recording. The non-traffic portion of physical memory is utilized for control and timing information.

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

Trigger Position



The Trigger Position slide bar sets the amount of post-trigger recording that 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.

Debug

Enable CATC debug file

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

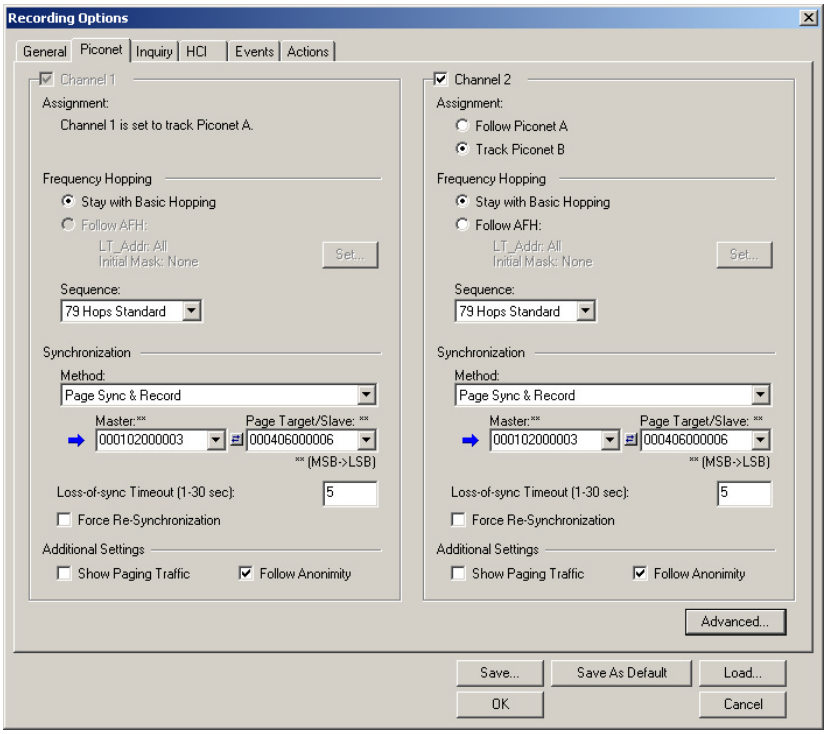
6.4 Recording Options - Piconet

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

For recording in Piconet mode, the **Piconet** page lets you specify the type of piconet you will be recording and how BTTracer should synchronize and record the piconet.

The **Piconet** page divides into a right and left half. Each half displays a set of options for configuring a BT*Tracer* probe. The right-hand set of options

will be greyed out unless you have a second BT*Tracer* probe installed in the right UPAS slot and the system is set to BT1.1 mode.



Channel 1 and **Channel 2**

Each Channel represents a BT*Tracer* probe. The checkboxes enable/disable the piconet options listed below them. For UPASs with only the left side BT*Tracer* probe, the Channel 2 options will be greyed out and the checkbox for Channel 1 should be checked.

If you have two probes, the second channel is going to be available for selection.

When using BT 1.2 configuration with two probes present, Channel 1 is set to follow the AFH while Channel 2 is set to track the basic hopping. To set the analyzer to BT 1.2 configuration, select **Setup** > **System Configuration** > **BT004MA/BT005MA BT1.2 (BTTracer Only)**.

Assignment

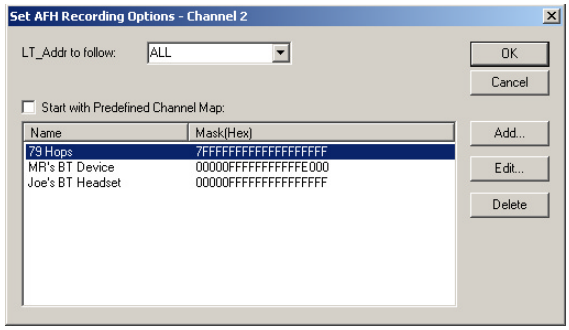
This setting tells the analyzer which piconet to record. With a two probe system, you can record traffic from two different piconets (Piconet "A" and Piconet "B") or traffic from a single piconet (Piconet "A") with different hopping sequences.

Frequency Hopping

Stay with Basic Hopping - Configures the probe to use the Basic Hopping sequence as defined by the Bluetooth 1.1 specification.

Follow AFH - Configures the probe to use the Adaptive Frequency Hopping sequence as defined by the Bluetooth 1.2 specification.

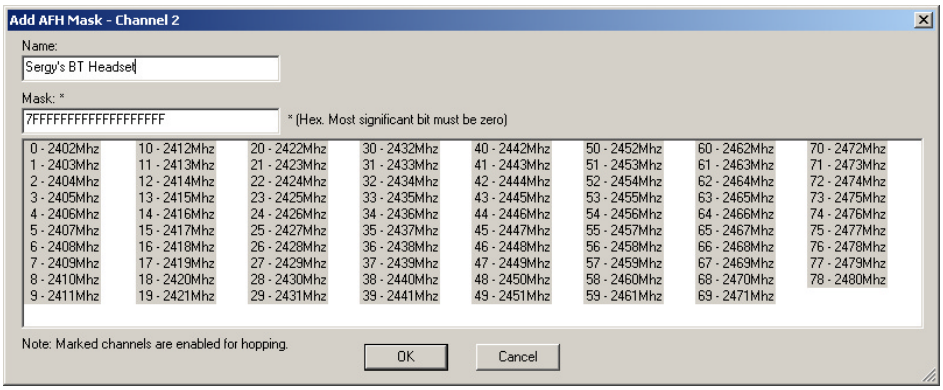
Set... - Opens a dialog box for selecting the channels you would like BT*Tracer* to use.



LT_ADDr to Follow: Select devices to be followed.

Start with Predefined Channel Map: Tells BT*Tracer* whether to use the selected channel map from the table. Select an AFH sequence from the list, check **Start with Predefined Channel Map**, then click **OK**.

Add ...: Opens a dialog box for selecting multiple channels. You can shift-click or control-click to select or deselect multiple channels. Add a name to the box marked **Name** and then click **OK** to close the dialog box and keep your selection.

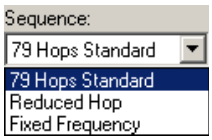


Edit ...: Opens the dialog box shown above and lets you change the current settings.

Delete: Deletes the selected AFH sequence.

Sequence

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

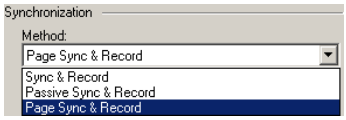


- **79 Hops Standard** - This is the option used for most recordings.
- **Reduced Hop** - Restricts BTTracer to five hop frequencies defined in the test mode specification of the Bluetooth Specification. When Reduced Hop or Single Frequency is selected, the Sync method is set to Test Mode and cannot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

  Enter values into the two text boxes to 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

Synchronization Method



To record Bluetooth traffic, BTTracer 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.

Synchronization Method options let you configure how BTTracer synchronizes to the piconet under observation. There are three options:

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

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

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

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

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

Between the two text boxes is the following button:

- Swaps the Master and Page Target addresses.

When to Use the Different Piconet Recording Modes

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

Sync & Record

Sync and Record works just like "Page Sync and Record" except that 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", "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 the Record button on the toolbar.

Step 4 When the analyzer is able to Sync up to the Piconet Master Clock, the Green **Sync** LED in the 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:

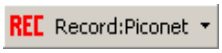
Step 1 Establish a connection between two or more Bluetooth devices.

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 record 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 is 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.

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 pressing the BT Neighborhood button

Step 3 After the General Inquiry completes, the addresses will populate the menus marked **Master Device** and **Page Target**. Select or enter the

addresses for both your Master Device and Page Target.

Step 4 Click **OK** at the bottom of the window to close the Recording Options dialog box.

Step 5 Press the

button found on 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.

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

Step 6 When the piconet is established, the "Sync" light on the front of 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.

Loss of Sync Timeout (1-30 secs)

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

Force Re-synchronization

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

Unchecking the "Force Re-Synchronization" checkbox tells 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 the Device List (**View > Device List**).

Show Paging Traffic

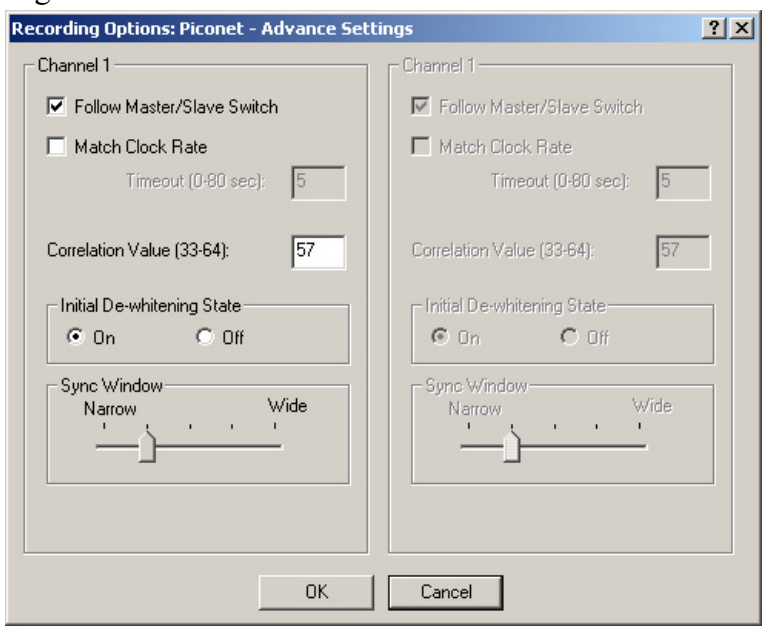
Show Paging Traffic causes BTTracer to capture paging traffic between the Master and Page Target devices. This option is used only with Page Sync and Record Mode.

Follow Anonymity

Allows BT*Tracer* to follow devices that are using anonymity mode. Anonymity mode is an addressing mode in which devices are assigned Bluetooth addresses based on a pseudo-random value. Anonymity mode is defined in the Bluetooth 1.2 specification.

Advanced ...

The Advanced button opens a dialog box with additional piconet settings:



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.

Timeout (0-80 secs)

Default value for Inquiry Timeout is 20 seconds.

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.

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.

Initial De-whitening State

De-Whiten On -- Turns on De-Whitening

De-Whiten Off -- Turns off De-Whitening

This setting controls the initial de-whitening state.

If " De-Whitening Off" is selected, BTTracer will try to synchronize without de-whitening the received packets, and assume that they were transmitted un-whitened.

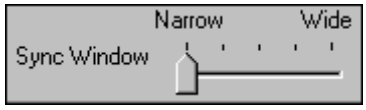
If " De-Whitening On" is selected, BTTracer will use received packets to try to synchronize while it is performing a de-whitening process that complies with Bluetooth specifications.

This setting controls the initial state for the synchronization. After BTTracer has synchronized to the piconet, it will try to follow changes in the whitening scheme and dynamically track whitened and non-whitened traffic.

In case a recording was stopped and you want to restart a recording session of the same piconet, you should remember that BTTracer might still be synchronized to the same piconet. As BTTracer dynamically follows whitening scheme changes, it will not use the initial de-whitening state. However, if you want to force an initial de-whitening state, check the "Force Re-Synchronization" flag.

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.

6.5 Recording Options - Inquiry

The **Inquiry** page configures how BTTracer records Inquiry traffic. Two main options are presented in the **Sync Method** drop-down menu: General (Unlimited) Inquiry and Dedicated (Limited) Inquiry. These options tell BTTracer what kind of Inquiry traffic it should expect to record.

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

General (Unlimited)

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

Dedicated (Limited)

"Dedicated" means a specific class or group of Bluetooth devices (designated by the DIAC field of the Recording Options dialog). Selecting "Dedicated" causes 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.

Timeout (0-80 secs)

Default value for Inquiry Timeout is 20 seconds.

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.

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.

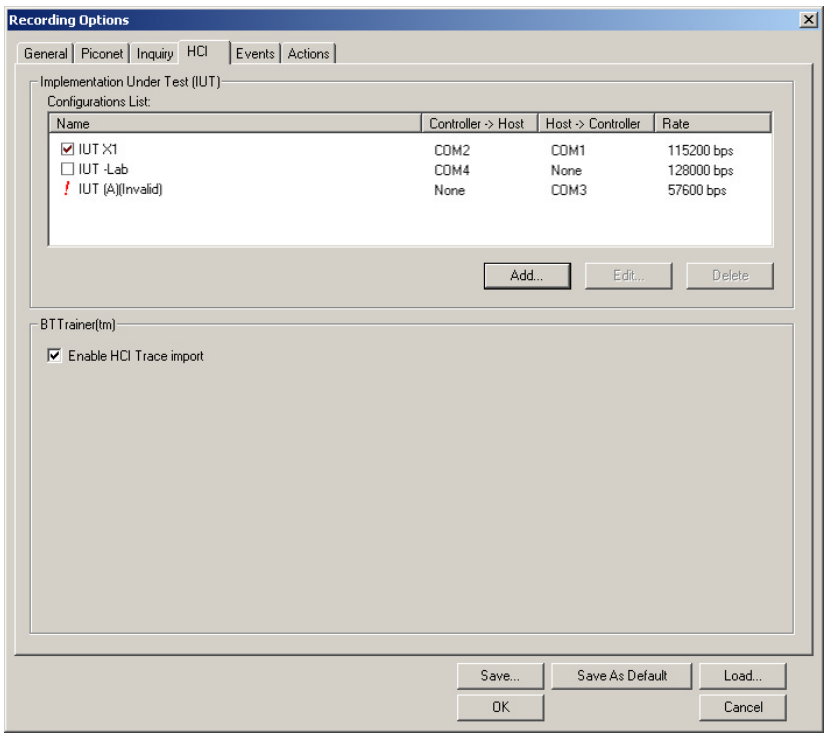
BT Neighborhood

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

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

6.6 Recording Options - HCI

The HCI property page lets you include/exclude HCI traffic from the BTTrainer or Implementations Under Test (IUTs) into the trace. HCI traffic consists of commands and data that are sent from the host to the controller and events and data sent from the host to the controller. By default, this option is disabled - meaning that HCI traffic is not shown in the trace.



These settings are relevant only for BTTrainer mode, where the BTTracer is monitoring the BTTrainer. The Internal HCI traffic of BTTrainer can also be recorded.

HCI Trace

Using the analyzer's hardware and radio module, the BTTracer can record serial Bluetooth HCI traffic from Bluetooth devices, or "IUTs" (Implementations under test).

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

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

Probe setup is described in Section 2.8, "Installing the HCI Probe" on page 18.

Recording HCI Traffic

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

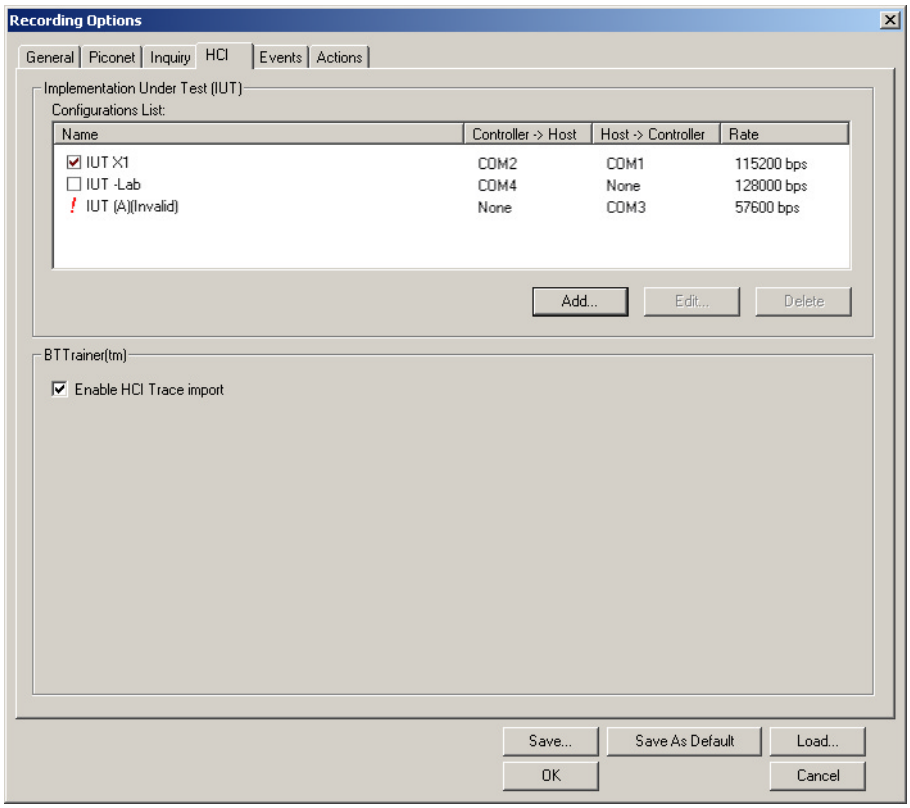
Step 1 Connect the IUT to the PC that is running BT*Tracer* following the steps outlined in the previous section.

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

This is the only recording mode supported by BTTracer. This mode configures BTTracer to exclusively record HCI traffic from IUTs.

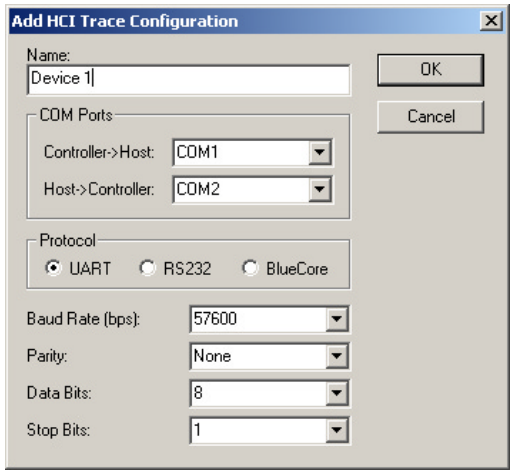
Step 2 From the menu, select **Record > Recording Options**.

The Recording Options dialog box opens showing the HCI page.



Step 3 Click **Add ...**.

The following dialog box will open:



Step 4 Enter the information appropriate to your setup for each of the IUTs:

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

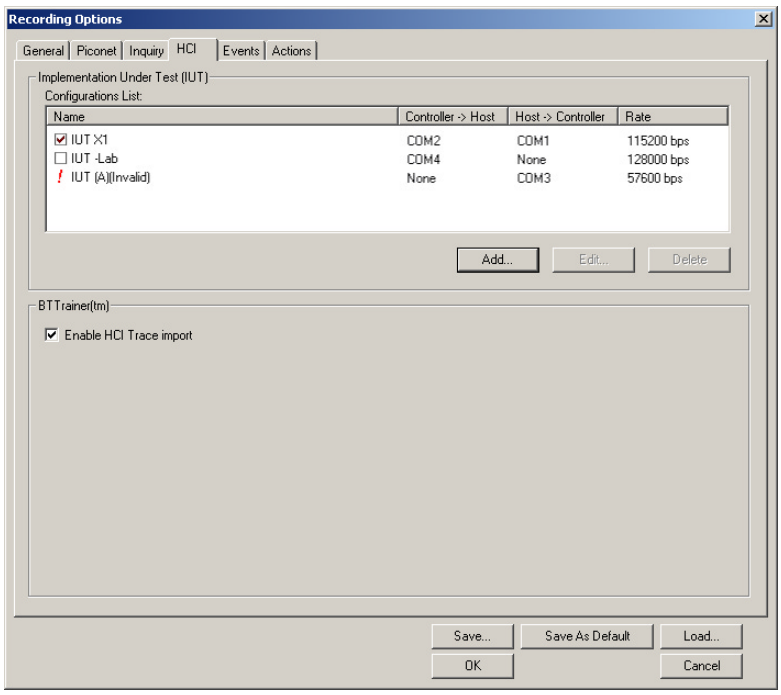
The list displays three possible states for each one of the entries:

- **Enabled** - The HCI traffic from the IUT is going to be recorded.
- **Disabled** - The HCI traffic from the IUT is not going to be recorded.

  Invalid - The analyzer failed in opening the COM port for accessing the IUT, with the listed parameters. In this case, you should refer to Windows configuration of the COM ports or check whether the same COM port(s) is (are) used by other applications in the host machine or that the parameters are set correctly.

Step 5 Click **OK** to close the **Add HCI Trace Configuration** dialog box.

The information you entered will appear in the HCI Page.



The following description explains the fields in the HCI Trace Configuration dialog box:

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

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

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

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

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

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

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

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

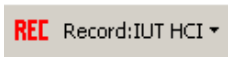
Step 6 Click **OK** to close the Recording Options window and activate the recording options you selected.

At this point, BTTracer will be ready to record.

Starting the HCI Recording

Once the HCI probe has been connected and the Recording Options have been configured, you can begin recording HCI traffic. To start a recording,

Step 1 Be sure that **IUT Recording Mode** is selected on the Record button .



Step 2 Click the Record button (i.e. the button itself, and not the down-arrow.)

BTTracer starts to record the Bluetooth traffic immediately using the settings from the HCI page in the Recording Options dialog.

Step 3 Click to end the recording.

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

Step 4 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 5 Give the recording a unique name and save it to the appropriate directory.

Editing an HCI Trace Configuration

To edit the HCI trace configuration,

Step 1 In the HCI page of Recording Options, click **Edit**.The Edit HCI Trace Configuration dialog appears.

Step 2 Change the data in the data fields according to your desired changes, and click **OK**. The changes are reflected in the Extern page of Recording Options.

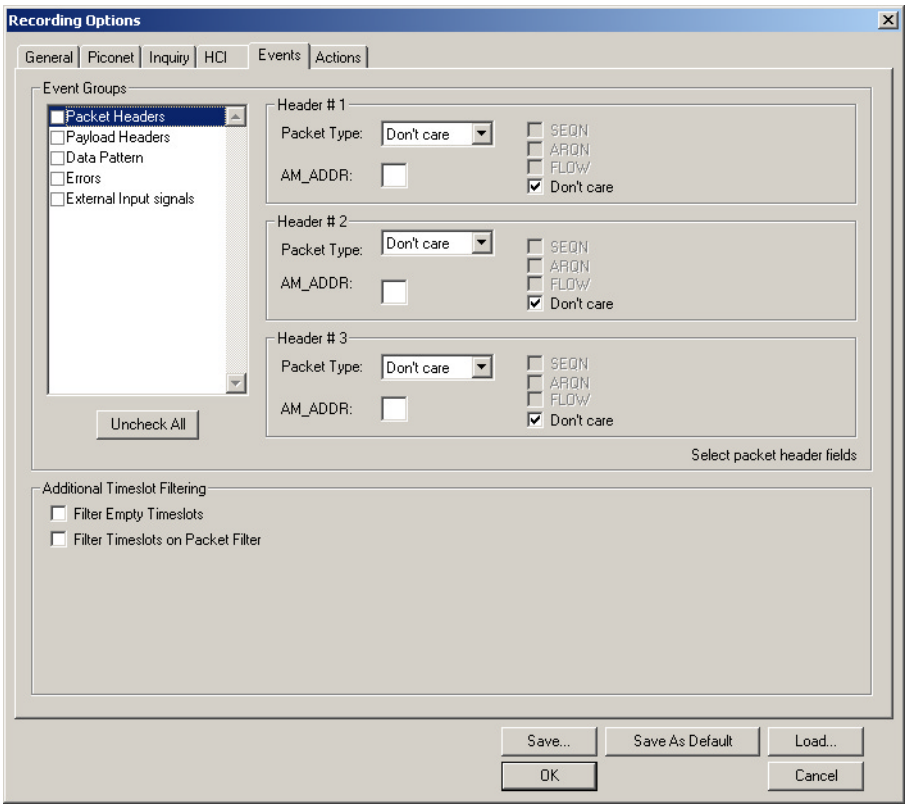
6.7 Recording Options - Events

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.

- 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

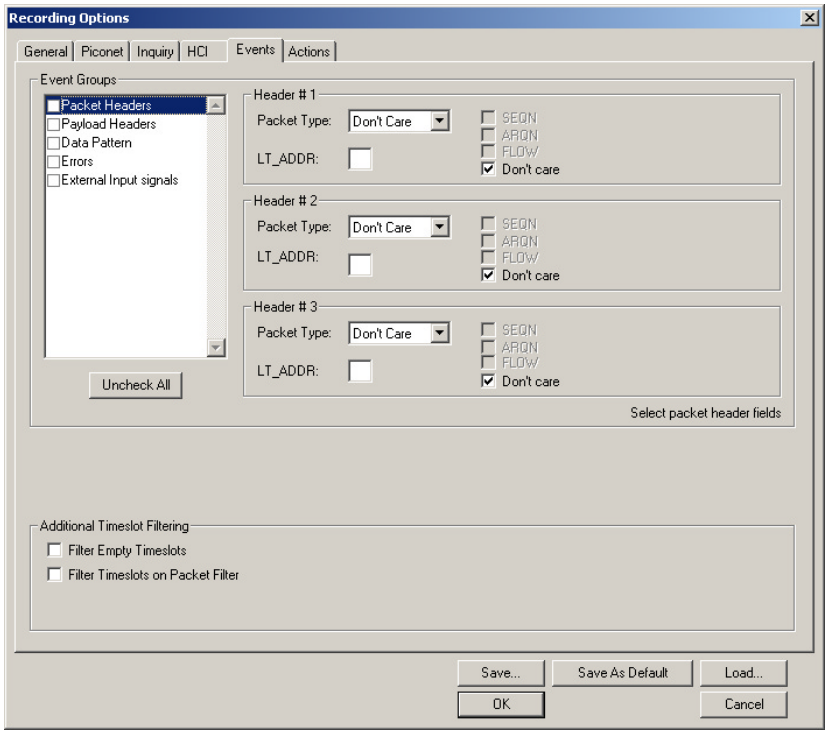
If filters are used to exclude FHS, DM1 or other packets, BTTracer will exclude these packets from a trace and mark their locations with empty packets. The result can be rows and rows of empty packets. The option "Filter Empty Slots" will not exclude these empty slots because they lie immediately in 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/EV3, DV, AUX1/PS, DM3, DH3, EV4, EV5, DM5, or DH5.

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

LT_ADDR

(Logical Transport Address) The LT_ADDR is a three bit slave address. To select packets from a particular slave device for filtering or triggering, enter an address into the LT_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.

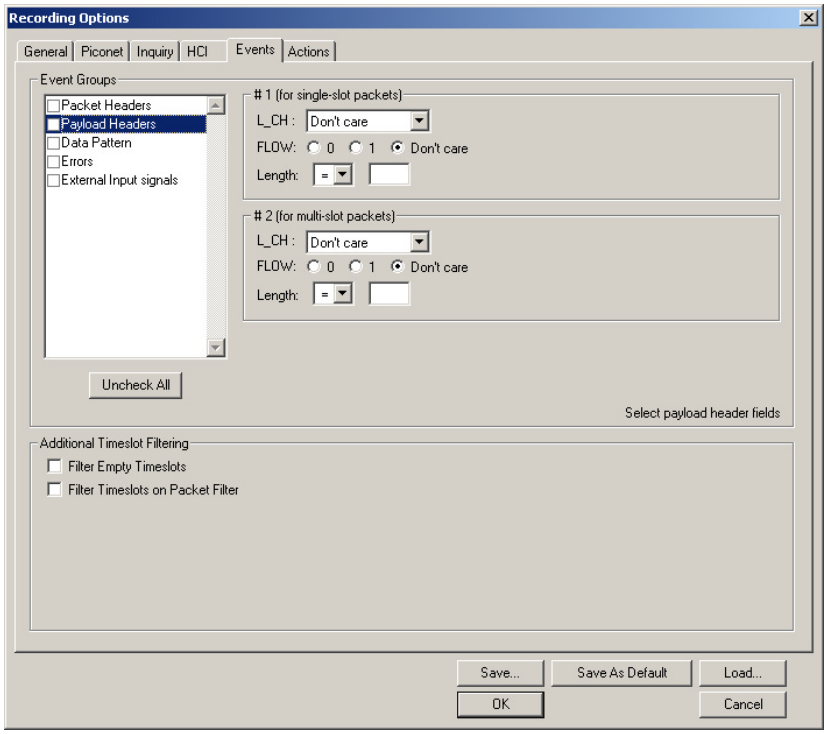
To cause BTTracer to ignore this set of check boxes, choose "don't care."

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."

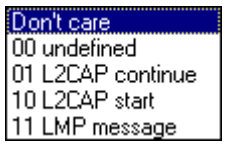
- Select **Payload Headers** under **Event Groups.**

  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:

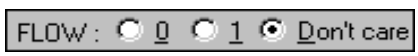


- Don't care
- 00 Undefined
- 01 L2CAP continue
- 10 L2CAP start
- 11 LMP message

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:

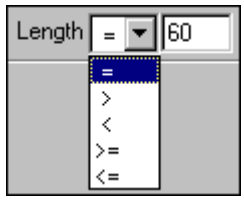


- 0
- 1
- Don't care

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)

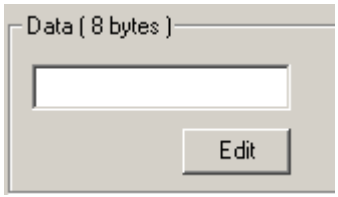


Using both the drop down menu and the text box, you can set conditions based on data field length. The maximum length for a single slot packet is 29 bytes. The maximum length for multi-slot packets is 339 bytes.

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



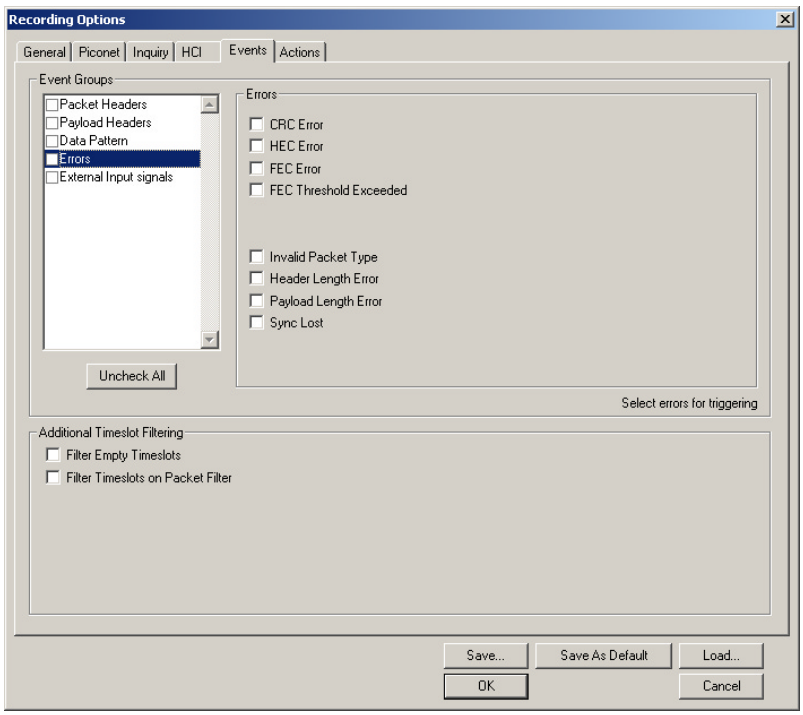
Clicking "Data Patterns" causes a text box to appear for entering patterns to be matched in the raw payload data. Patterns of up to eight hexidecimal bytes can be entered.

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 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

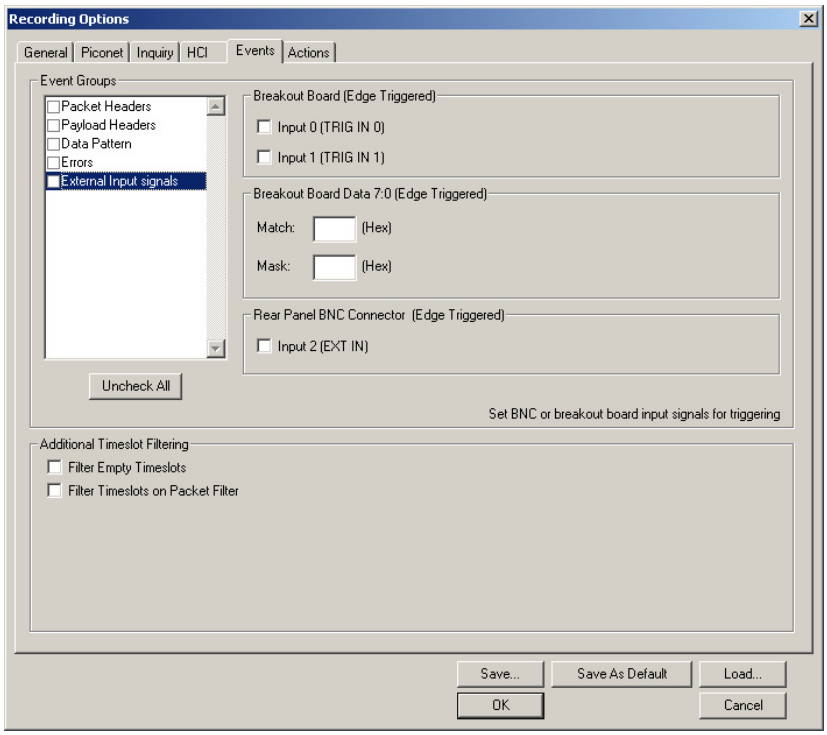
Indicates that the payload of a received Bluetooth data packet was either longer than expected, or that a Bluetooth data packet terminated before the expected end of the payload data.

Sync Loss

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

External Input Signals

Selecting "External Input Signals" causes the analyzer to trigger an external signal is received through one of the ports on the back of the analyzer (Data In/Out or Ext. In). If you are using the 25 pin Data In/Out port, connect a cable from that port to a Break-out Board. Then connect pins on the breakout board to a signal source.



Breakout Board (Edge Triggered)

The following names are derived from pins on the CATC-provided breakout board.

- *Input 0 (TRIG IN 0)* - Selectable Edge triggered inputs. Will trigger on any edge it detects. Note that only Data1 - Data0 can be recorded into the trace.

- *Input 1 (TRIG IN 1)* - Selectable Edge triggered inputs. Will trigger on any edge it detects. Note that only Data1 - Data0 can be recorded into the trace.

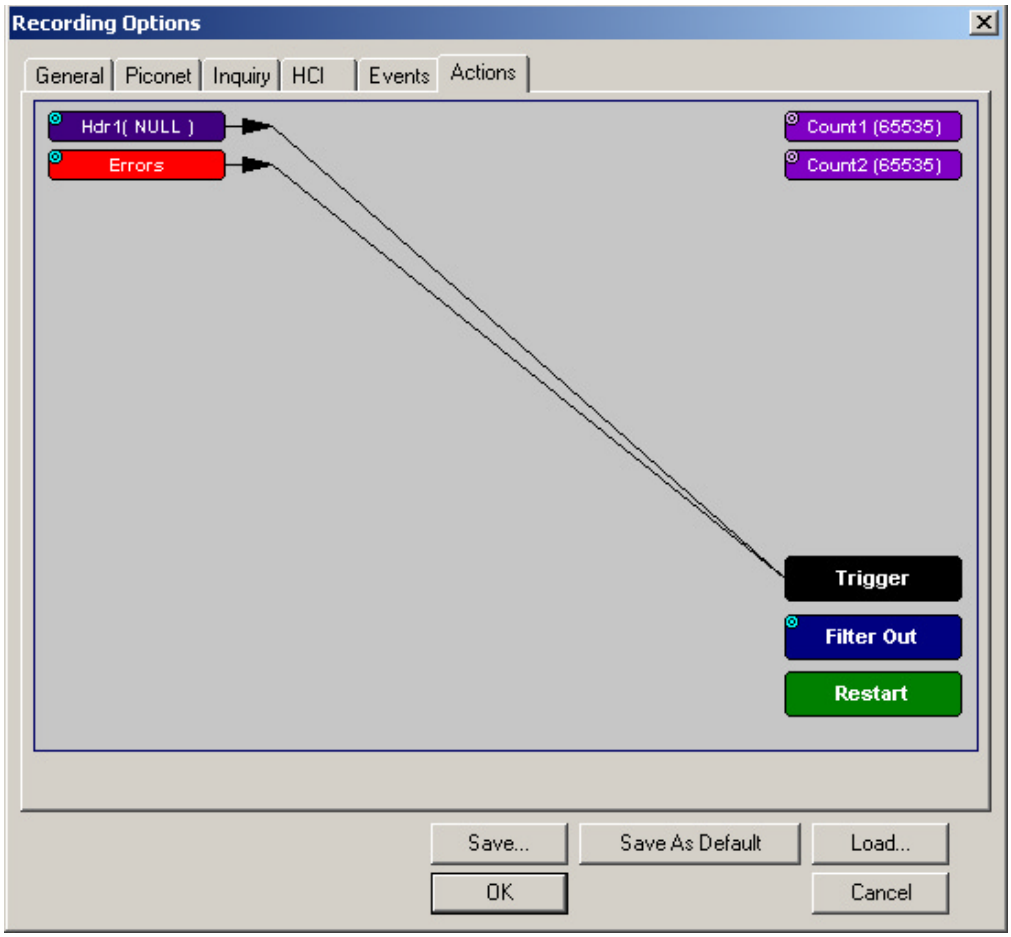
Breakout Board Data 7:0 (Edge Triggered) - Triggers on an 8-bit input pattern on any of the breakout board pins marked Data 0 through 7.

Rear Panel BNC Connector (Edge Triggered)

- ***Input 2 (EXT IN):*** Selectable Edge triggered inputs. Will trigger on any edge it detects.

6.8 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.



Action Buttons - Their Functions

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

Trigger

The **Trigger** button enables event triggering.

Filter In/Out

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

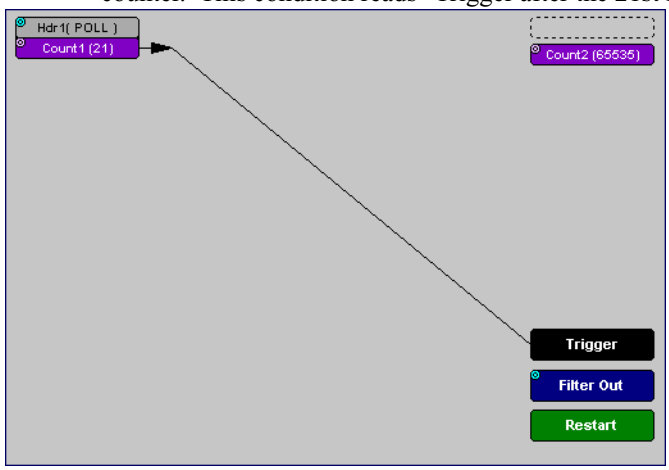
Restart

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

Count1, Count2

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

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



Connecting Events to Counters

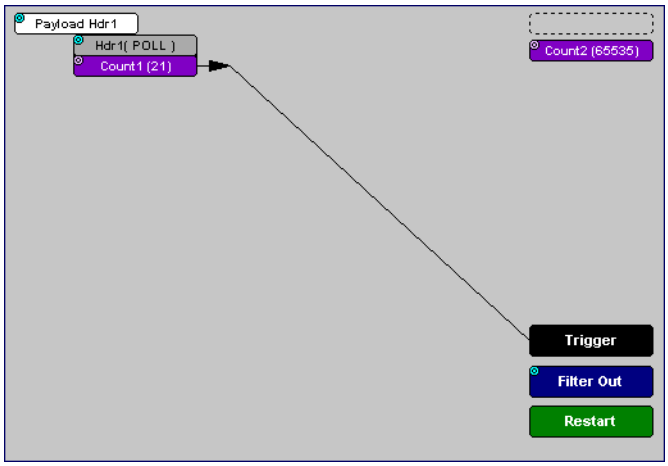
To connect an event to a counter, click an Event button, then click one of the two counter buttons. The Counter will reposition itself immediately below the event. A line will the connect the counter to the Trigger button.

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

Setting Multiple Conditions with Counters

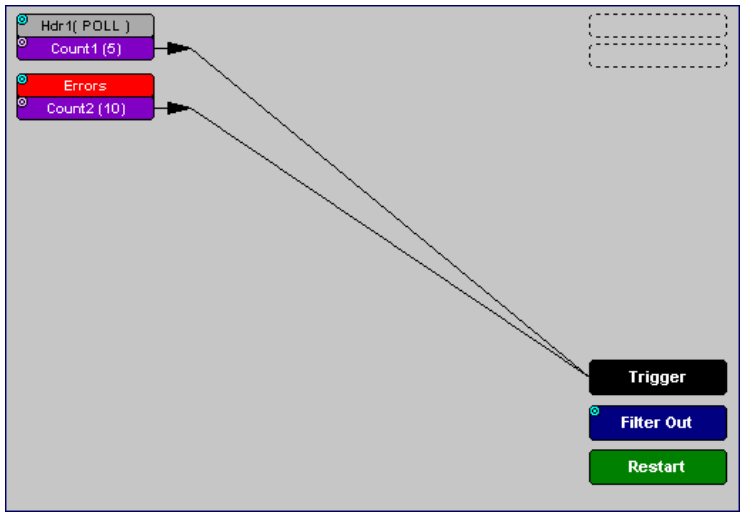
You can create multiple event conditions by linking a counter to multiple events or by linking two counters to two or more events.

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



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

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



Blue Dot Menus

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

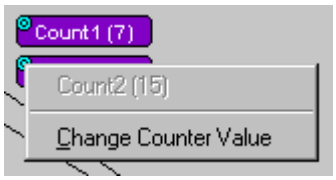
Counters Blue Dot Menu

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

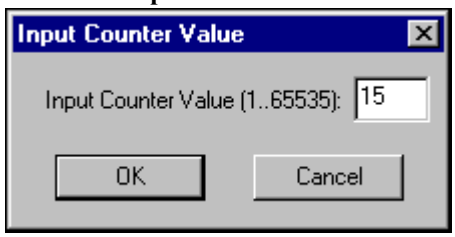
Step 1 Click on the blue dot in the upper left corner of the **Count** button.

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**.

Filter Out/In Blue Dot Menu

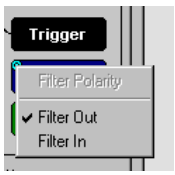
The **Filter Out/In** button toggles between "**Filter Out**" and "**Filter In**".

- **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".

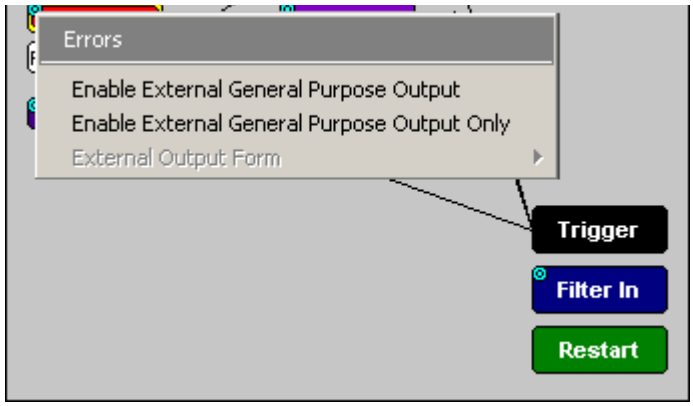
Blue Dot Menus for the Event Buttons

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.

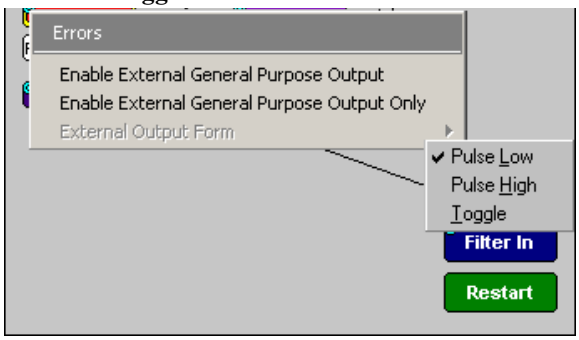
To configure the output signal,

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.

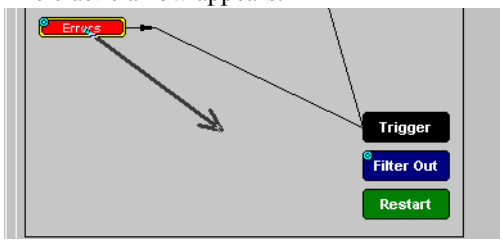
Note that your new selection is now checked.

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.



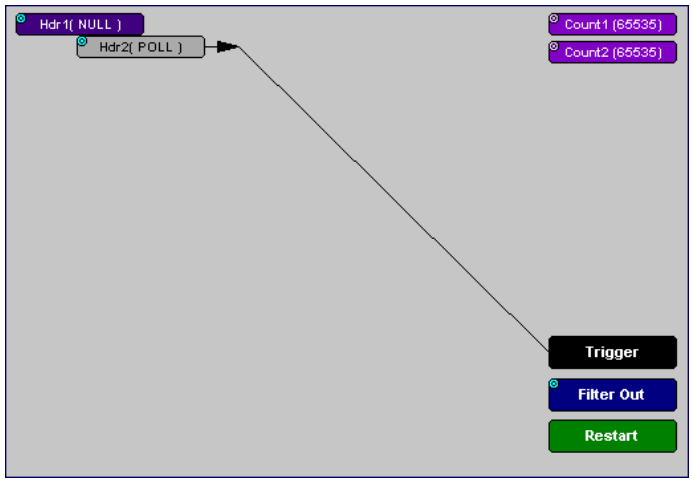
Step 2 Drag the arrow to the desired Action button.

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.



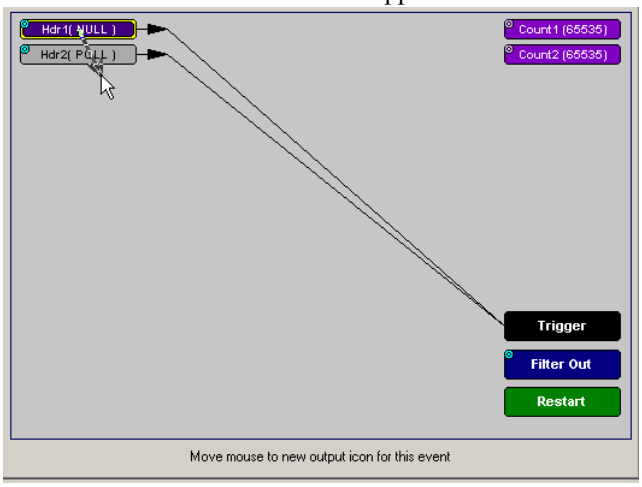
This example means "Trigger when you see a packet with an Null Header followed by a packet with a Poll Header."

To create an event sequence, perform the following steps:

Step 1 Select two events from the Events window

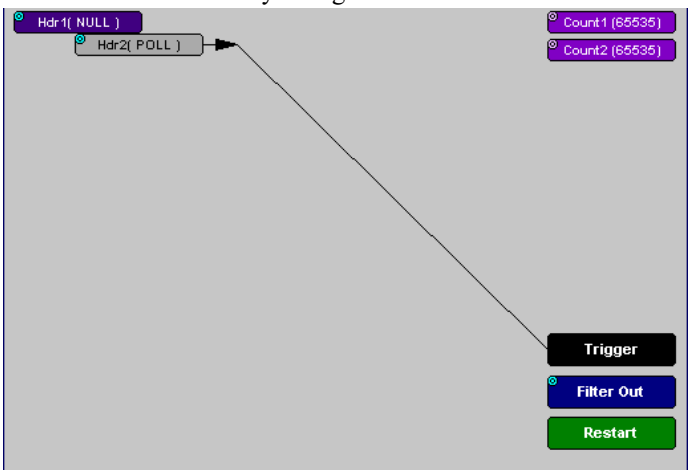
Step 2 Open the Actions window and click on one of the two Event buttons.

An elastic arrow should appear.



Step 3 Click on the other event.

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



6.9 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.

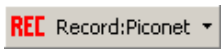
- Click **Save** to save the currently specified Recording Options for use in future recording sessions. Any file name can be specified, though use of the **.rec** is recommended; if no extension is specified, **.rec** is added by default.
- Click **Load** to load a previously saved ***.rec** file, thus restoring a previous set of Recording Options. You can also load the recording options from trace files.
- The **Save as Default** function is equivalent to the **Save** function, specifying the file name **default.rec.** Whenever you start up the Analyzer, it automatically loads the **default.rec** file if one exists.
- Click **OK** to apply any changes and close this dialog box.
- Click **Cancel** to cancel any immediate changes you have made and exit the Recording Options menu.

6.10 Recording Bluetooth Traffic

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

If you have enabled the recording is serial HCI traffic from IUT, then a second trace file is created called data_hci.tfb.

To save a current recording for future reference,

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

OR

Click on the Tool Bar.

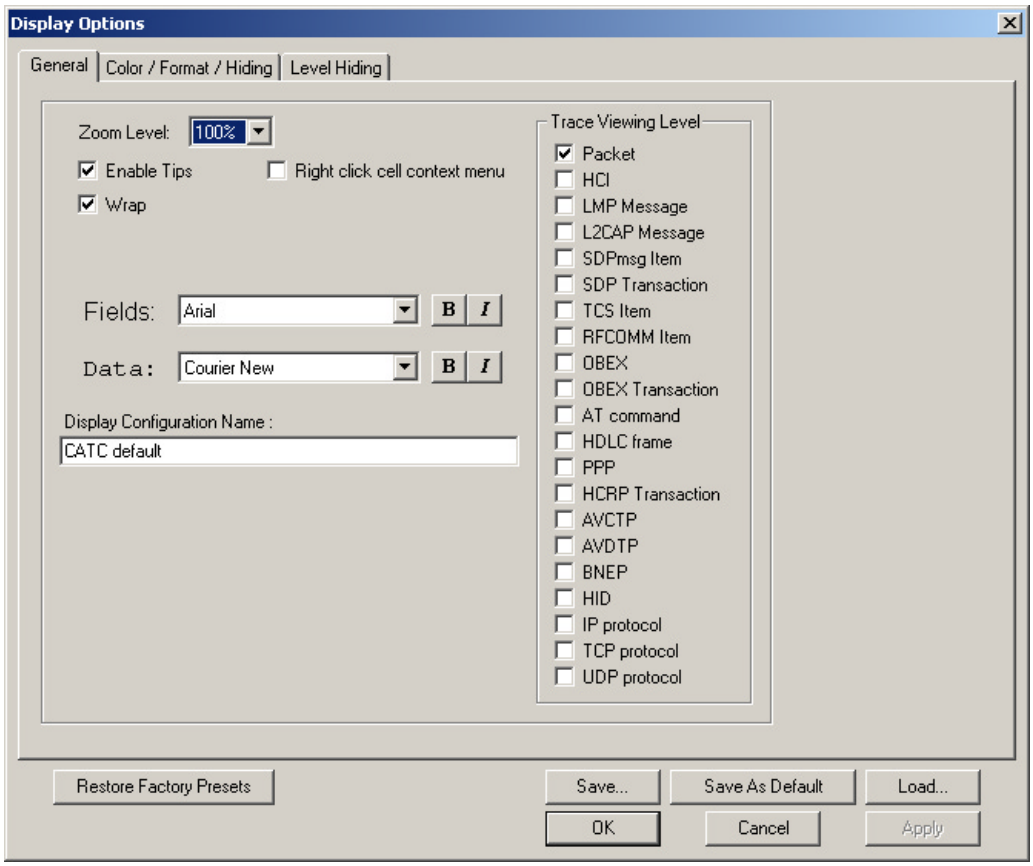
You see the standard **Save As** screen.

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

7. Display Options

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

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



7.1 General Display Options

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

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

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

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

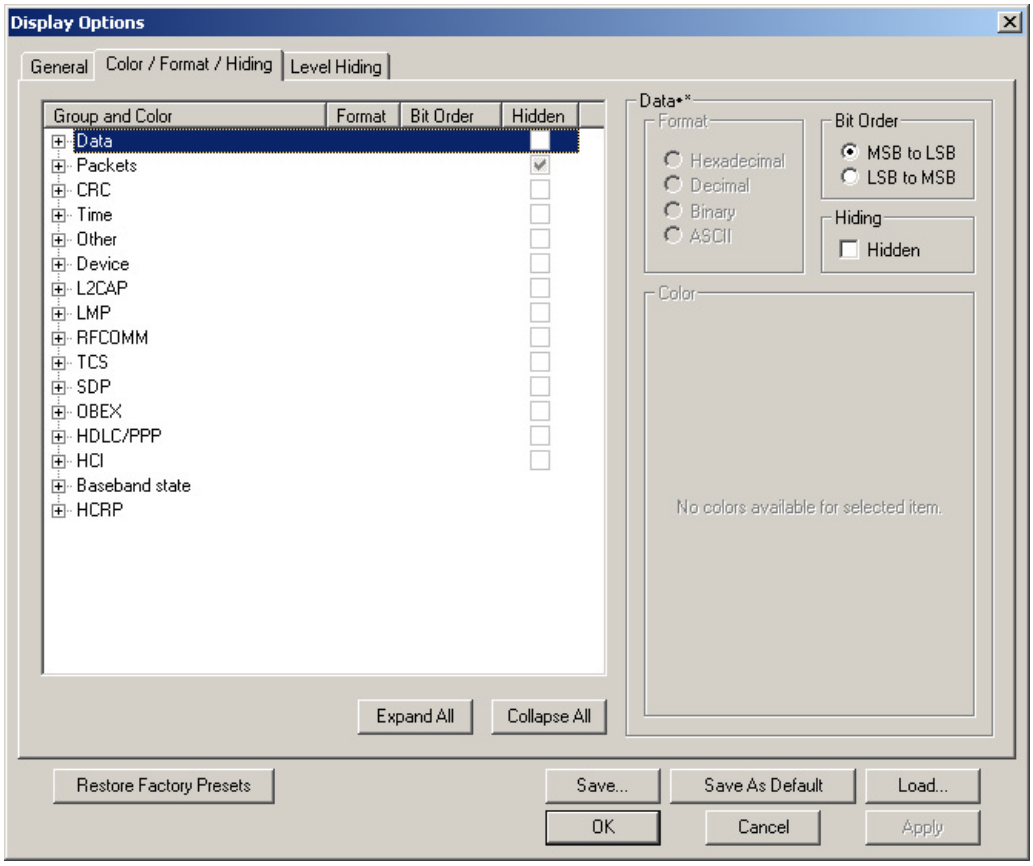
Step 2 Click **Save**...

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

Step 4 Click **Save**.

7.2 Setting Color, Formatting, and Hiding Options

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



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

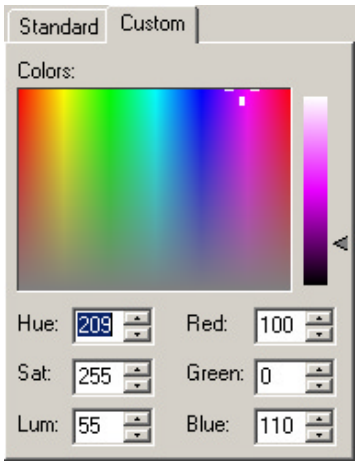
Setting Color Display Options

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

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

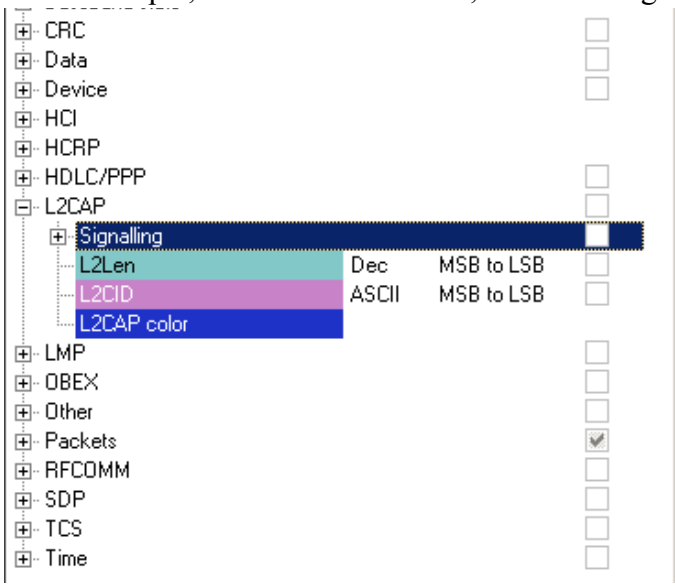
Use this window to customize the colors associated with each field in the trace. You can experiment with these options to achieve the color combination best suited to a particular graphic system.

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

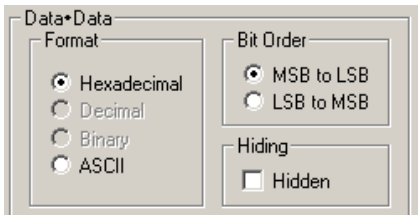


Changing Field Formats

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



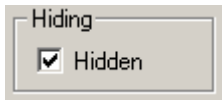
The following formats are available:



Note Not every format is available for every item.

Hiding Display Options

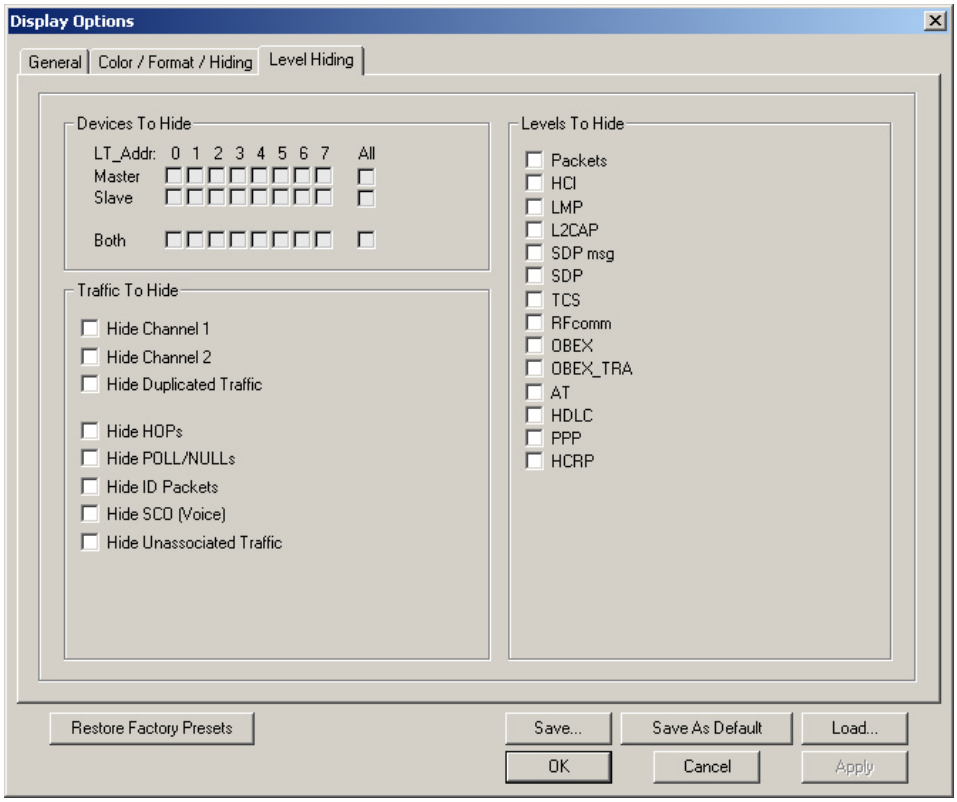
To hide one or more fields in the trace, select the appropriate item from the Group and color column, click the checkbox marked **Hidden**, and click the **Save** button.



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

7.3 Level Hiding Options

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



Level Hiding Parameters

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

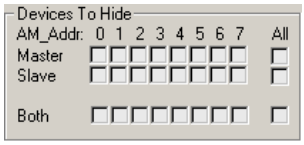
Hiding Fields

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

Hiding Packets, Messages, and Protocols

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

Devices to Hide



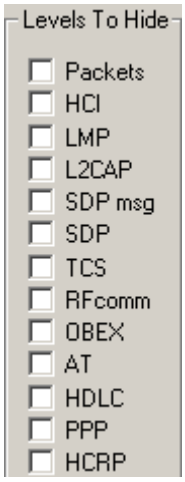
The "Devices to Hide" grid lets you hide traffic according to device address. The grid divides into columns which represent different devices.

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**.

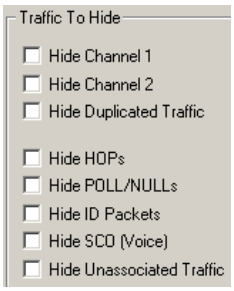


Levels to Hide

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.

Traffic To Hide

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

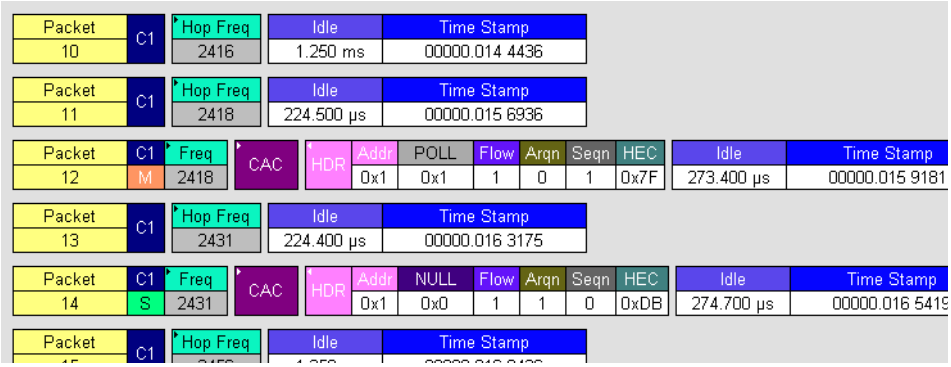


7.4 Saving Display Options

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

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

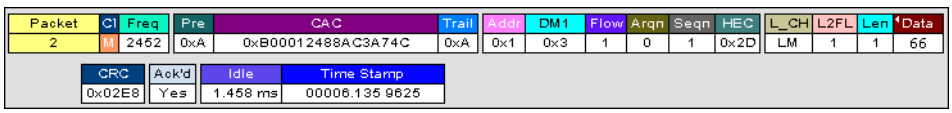
8. Reading a CATC Trace



8.1 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.

8.2 Interpreting the Displayed Information



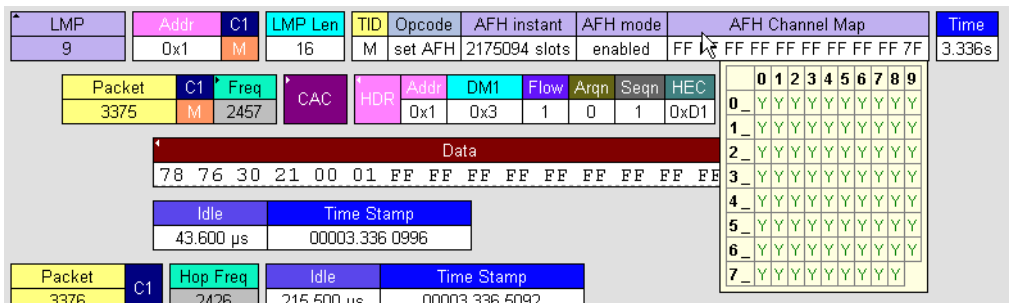
The following table describes some of the abbreviations used in the BTTracer display. Packet #0 is described from left to right:

Packet:#	**Packet/Event Number**
C1/M, C2/S	M =Master Device Transmitting; S = Slave Device Transmitting C1 = Channel 1; C2 = Channel 2
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 LT_ADDR
Idle	Idle Time in nanoseconds
Time Stamp	Decimal in Seconds.Milliseconds.Microseconds*10 This is the analyzer internal clock as a reference with resolution of 100 ns.

8.3 Tooltips

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



8.4 Set Marker

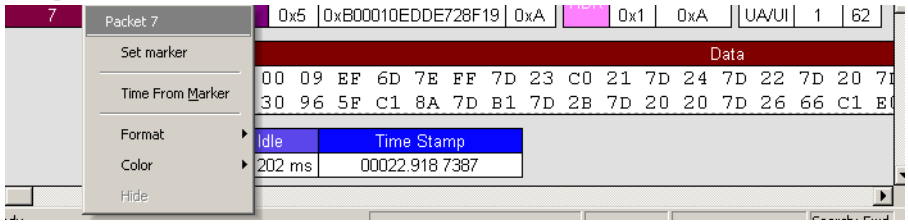
Note **Set Marker** works in conjunction with the **Go to Marker** feature.

You can define a unique Marker for each packet.

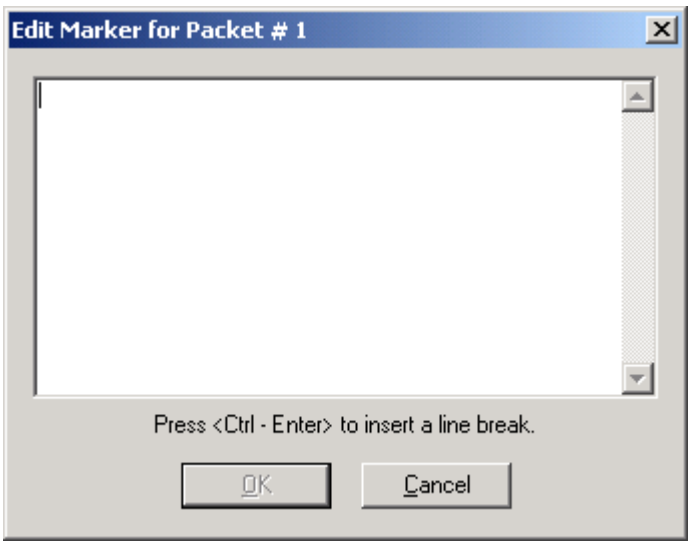
To place a marker on a packet,

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

Step 2 Select **Set Marker**.



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



Step 3 Enter your comment.

Step 4 Click **OK**.

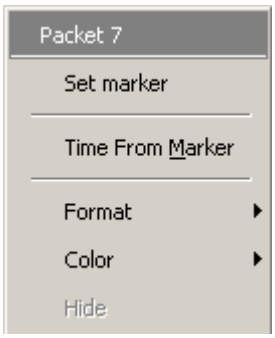
A marked packet is indicated by a vertical red bar along the left edge of the packet # block:

8.5 Edit or Clear Marker

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

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

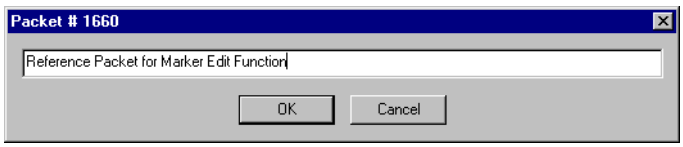
You see the **Packet** menu:



To edit the Marker Comment,

Step 2 Select **Edit marker**.

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



Step 3 Edit the comment as desired.

Step 4 Click **OK**.

To clear a Marker,

Step 5 Click **Clear marker**.

The vertical red Marker bar disappears.

8.6 Expanded and Collapsed Data Formats

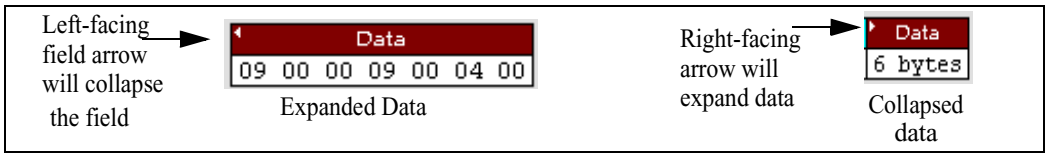
The data field can be expanded to display greater detail or collapsed to a compact view. The Expand/Collapse Data feature operates as a toggle. There are three ways to toggle between the two views.

Double-Clicking

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

Left-clicking a Field Arrow

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



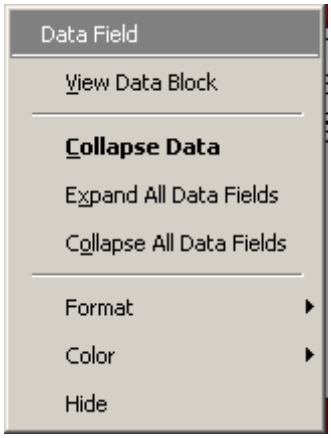
If you click and hold down the left mouse button on one of these arrows, you can collapse or expand the field for *ALL* packets, messages or protocols.

Using the Shortcut Menu

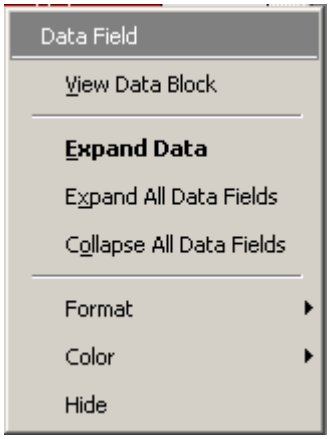
If you left-click on a **Data** field, a menu will open for expanding or collapsing data fields.

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

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



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



Note that you can choose to expand or collapse

- **Only** the Data in the selected Data packet

  OR

- **All** Data Fields in the Trace View.

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

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

8.7 Hide Frequency Hops

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

From the Tool Bar

- Click to hide all Hop packets.

8.8 Hide Nulls and Polls

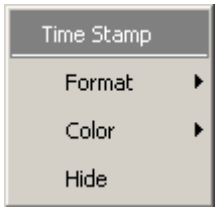
You can hide Nulls and Polls from a trace by pressing the **Hide Nulls and Polls** button on the Tool Bar.

From the Tool Bar

- Click to hide all Nulls and Polls.

8.9 Menus in Clicked Fields

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



8.10 Hide Unassociated Traffic

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

From the Tool Bar

- First, click one or more decode buttons such as the **View L2CAP Messages** . This button will cause 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.

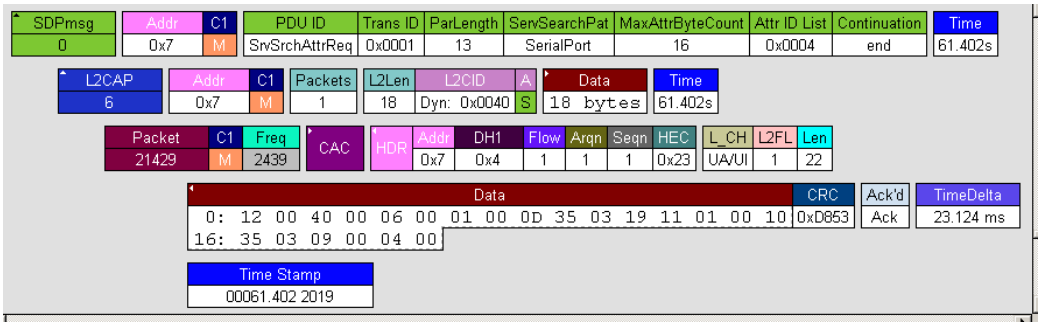
8.11 Hide Channel

You can hide all traffic recorded by the channel by pressing . on the toolbar.

8.12 Hide Duplicated Traffic

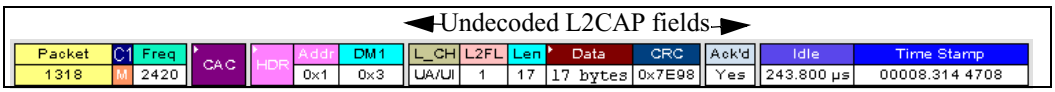
On two-channel recordings some packets may be recorded by both channels. You can hide duplicated packets by pressing on the toolbar.

9. Decoding Protocols



9.1 Introduction

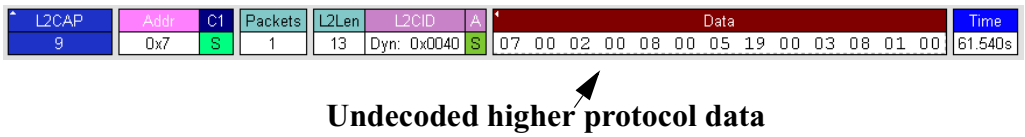
BTTracer can decode HCI, LMP and L2CAP messages, and RFCOMM, SDP, TCS, HDLC, PPP, OBEX, HCRP, BNEP, HID, IP, TCP, and UDP protocols. The default is *packet level* decoding, which means that baseband packets will be displayed when you first view a trace. If these packets are carrying LMP, L2CAP or other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



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*.

9.2 LMP and L2CAP Messages

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



9.3 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)
- **HCI** (Display HCI Protocol)
- **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 RFCOMM Protocol)
- **OBEX** (Display OBEX Protocol)
- **OBEX Tra** (Display OBEX Protocol Transactions)
- **AT** (Display AT Commands Protocol)
- **HDLC** (Display HDLC Protocol)
- **PPP** (Display PPP)
- **HCRP** (Display HCRP)
- **AVCTP** (Display AVCTP)
- **AVDTP** (Display AVDTP)
- **BNEP** (Display Bluetooth Network Encapsulation Protocol)
- **HID** (Display HID Protocol)
- **IP** (Display IP)
- **TCP** (Display TCP)
- **UDP** (Display UDP)

For example, to display LMP messages, click

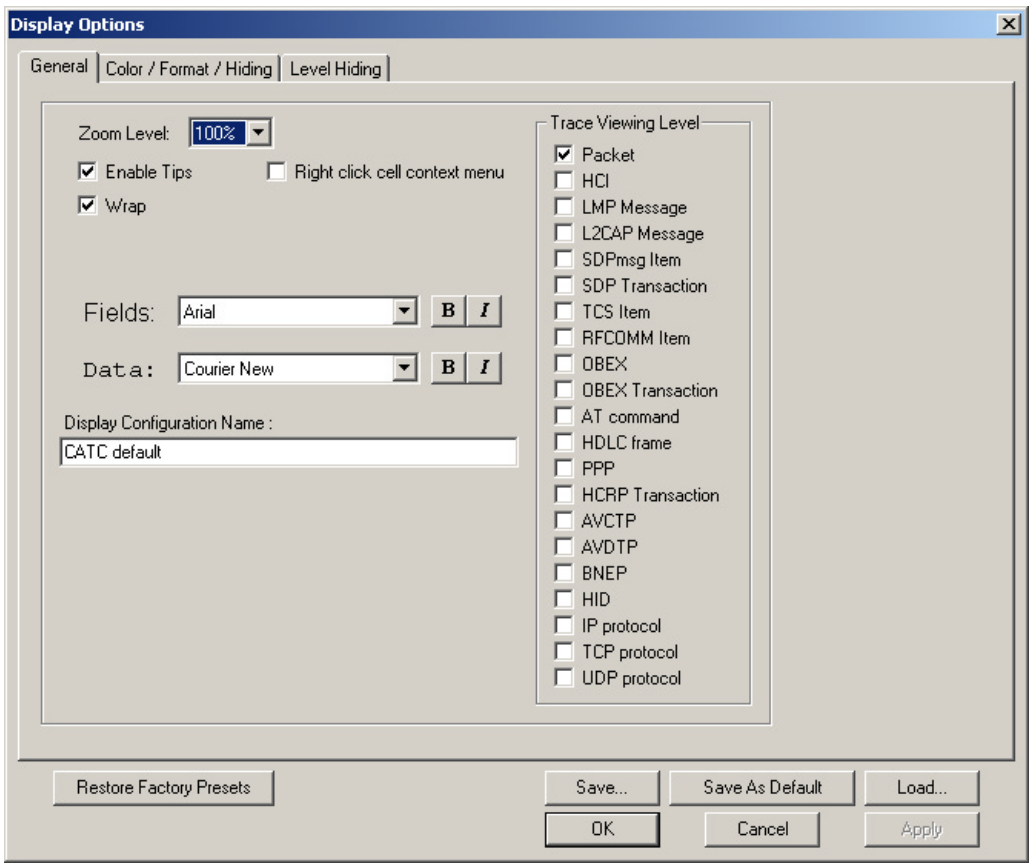
.

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

Decoding Via the Display Options Dialog Box

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

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

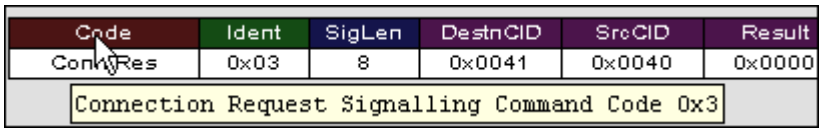


Step 2 Select the option for the desired level of decoding.

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

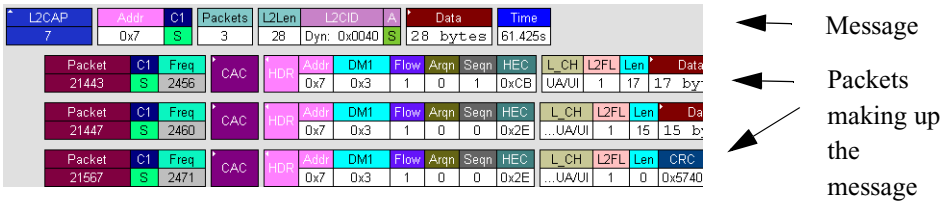
9.4 Tooltips

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



9.5 Viewing Packets in LMP and L2CAP Messages

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



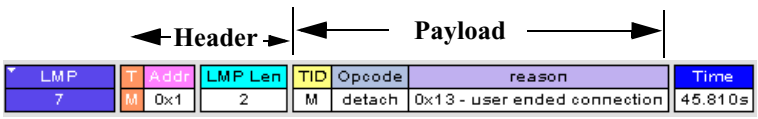
9.6 Types of LMP and L2CAP Messages

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

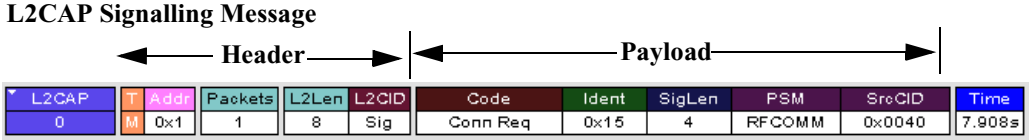
- LMP Signalling Message
- L2CAP signalling Message
- L2CAP Data Transfer Message

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

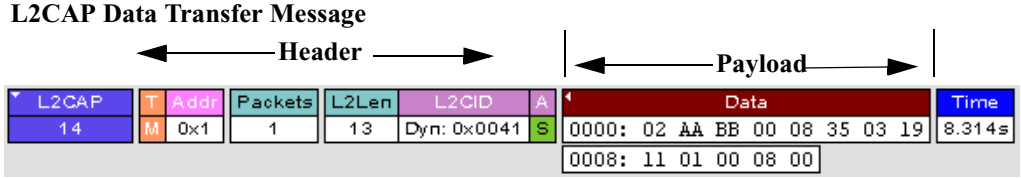
LMP Signalling Message



L2CAP Signalling Message



L2CAP Data Transfer Message



LMP and L2CAP Signalling messages have payloads of commands for establishing LMP and L2CAP channels. L2CAP Data-Transfer messages have a payload that may include RFCOMM, SDP, or TCS data. In order to

view 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."

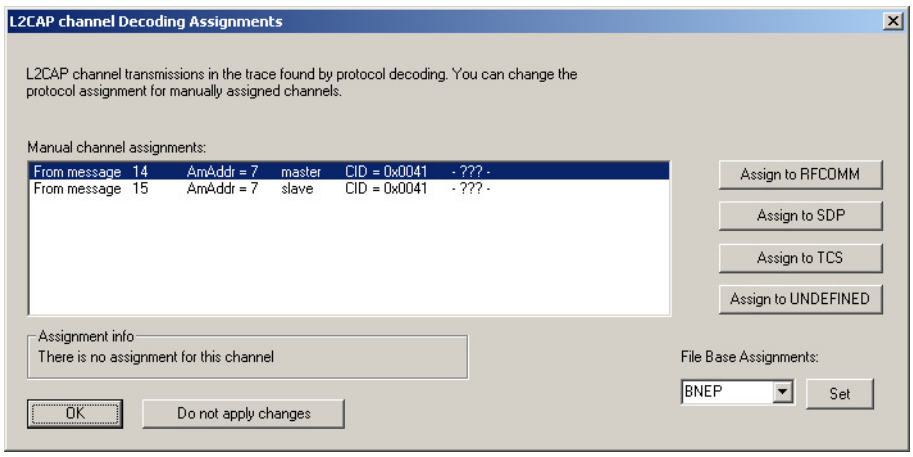
9.7 Viewing L2CAP Channel Connections

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

To view or change an L2CAP channel connection,

Step 1 Select from the menu bar
View>Decoding Assignments

The following dialog box will open.



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

If the Connect and Disconnect buttons are grayed-out, it means that 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 LT_Addr (Active Member Address). If possible, select an address other than the currently displayed address.

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

9.8 Viewing Protocol Messages and Transactions

By pressing a button such as

or

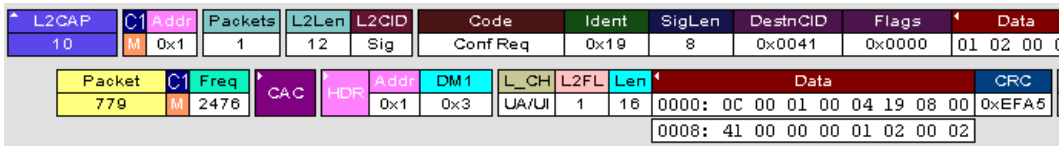
, you can cause BTTracer to decode the higher level protocol data contained within L2CAP messages and display them as packet-like rows called *Protocol Messages*. Protocol Messages have headers marked "protocol" and fields that vary in appearance and content depending on the type of protocol.

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

, 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:

.

.

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

9.9 Decoding via the Profiles Toolbar

The Profiles toolbar presents buttons that represent profiles. The Profiles buttons do not represent an additional set of decodes; rather, they represent shortcuts for the existing decodes. By clicking a Profiles button, the analyzer software will automatically depress the protocol buttons needed to decode all of the protocols associated with the selected Profile - for example, RFCOMM, PPP, or IP.

To display the Profiles toolbar, select **View** > **Toolbars** > **Profiles**.

9.10 Changing Protocol Assignments

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

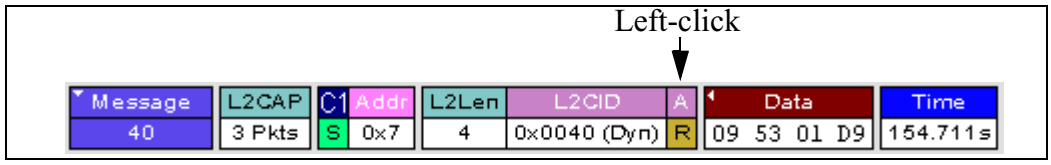
Step 1 Click

to display L2CAP messages.

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

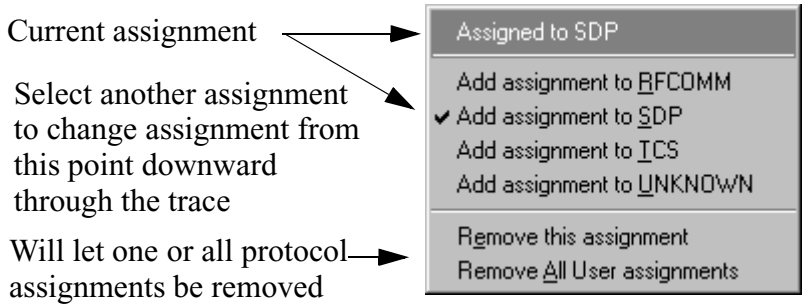
Step 2 Scroll through the trace until you have located an L2CAP message with a field marked "**A**."

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



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.

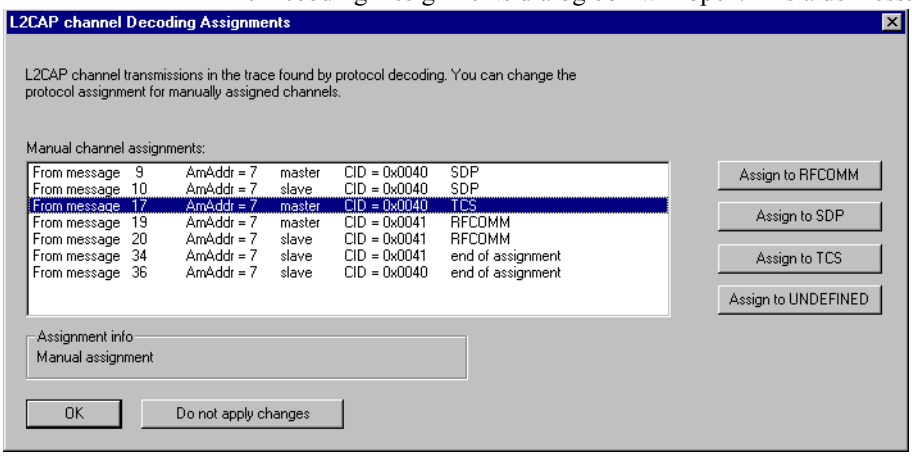
Using the Decoding Assignments Dialog Box

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.

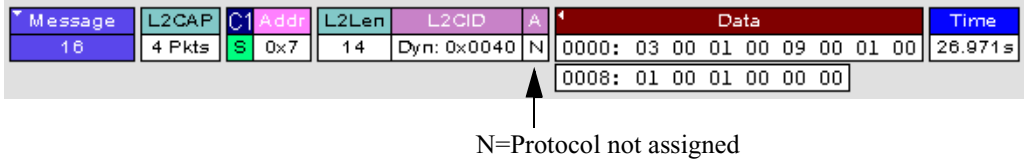
Step 2 Locate a message with a field marked "**A**."

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."



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.tfb" 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

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

button. If the decode file is not read at initialization, BTTracer will display the data in an undecoded format.

Other Decoding Options

Other decoding options include the following:

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

10. Exporting Trace Data

BT*Tracer* has export commands that enable you to extract trace data to CSV, text and other file formats. This chapter describes the export process.

Export commands are accessible through the menu: **File** > **Export**. The Export menu has five options:

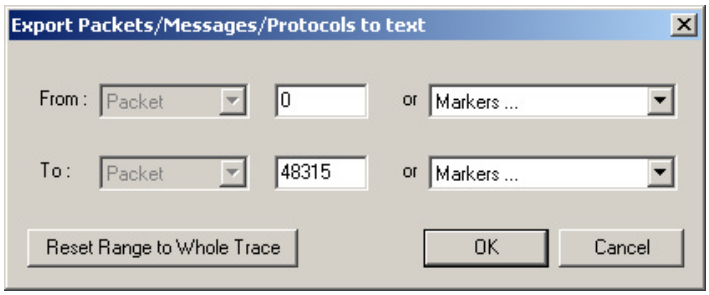
- Packets to Text (Packets View Format) ...
- Packets to CSV Text ...
- Audio Streams ...

10.1 Exporting To Text Format

To export trace data to a text file,

Step 1 Select **File** > **Export** > **Packets to Text (Packet View Format) ...**

The following dialog box opens.



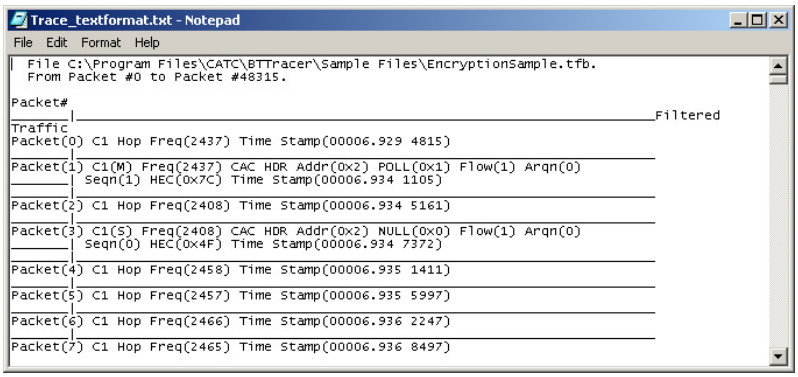
Step 2 Select the type and range of traffic to be searched from the From and To menus

Step 3 Click OK.

A **Save As** dialog box opens.

Step 4 Enter a name for the file and click **OK**.

The file is then saved. Exported text files look like this:



10.2 Exporting Trace Data to a .CSV Format

CATC's BT*Tracer* generates over a dozen performance metrics automatically for every trace and measures them in the Traffic Summary, Bus Utilization, and Timing Calculations dialogs. BT*Tracer* also has the ability, however, to extract a far wider range of performance data to a Comma Separated Value **(.csv)** format where it can be analyzed and measured with a spreadsheet, database or other application.

The command that extracts performance data to .csv format is called **Export to CSV Text** and is found under the File menu. This section describes the export process.

Step 1 In BT*Tracer*, open a trace.

Step 2 From the SATracer menu, select F**ile > Export > CSV Text**. The CSV Export dialog box opens.

Step 3 Select a range using the **From** and **To** boxes.

Step 4 Select a folder where you want to export the file, and click **OK.** A **.csv** file will then be created. Below is an example

of a .csv file opened in Microsoft Excel.

Microsoft Excel - csvtext_example.csv

File Edit View Insert Format Tools Data Window Help

Arial 10 E11

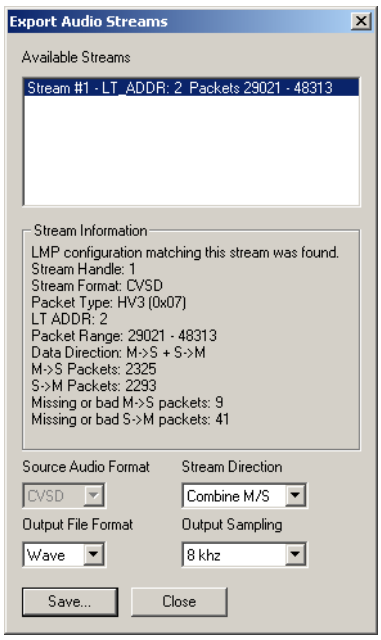
	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Packet	M/S	Freq	BTClock	Preamble	SyncWord	Trailer	LT_ADDR	TYPE	FLOW	ARQN	SEQN	HEC
2	0												
3	1	M	2437					0x2	POLL	1	0	1	0x7C
4	2												
5	3	S	2408					0x2	NULL	1	0	0	0x4F
6	4												
7	5												
8	6												
9	7												
10	8												
11	9	M	2462					0x2	DM1	1	0	1	0x1B
12	10												
13	11	S	2410					0x2	NULL	1	1	0	0xD8
14	12												
15	13	M	2470					0x2	POLL	1	0	1	0x7C
16	14												
17	15	S	2418					0x2	NULL	1	1	0	0xD8

10.3 Exporting Audio Data

BT*Tracer* has an **Export Audio Streams** command that allows you to extract audio data from a trace and export it into a file. The command lets you narrow your selection to a particular stream direction (master to slave or slave to master), and to set the output file format and output sampling.

Step 1 Select **File** > **Export** > **Audio Streams** from the menu.

The dialog box shown right opens.



Source Audio Format - Select the Source format.

Output File Format - Select an output format: WAVE or raw.

Stream Direction - Select stream direction that you wish to capture: Master to Slave, Slave to Master, or both ("Combine M/S").

Output Sampling - Select a sampling rate for the exported audio.

Step 2 Set the parameters, then click **Save**.

A Save As dialog opens.

Step 3 Select the name of the file to be created and its location, then click **OK**.

11. Other Features

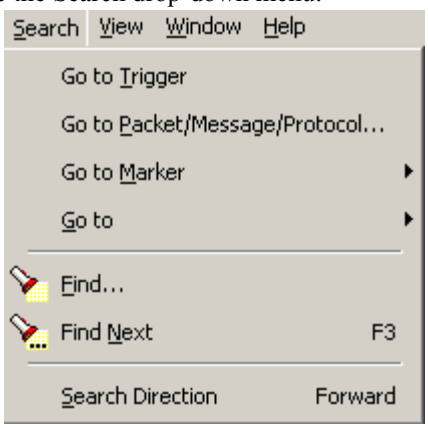
11.1 Search

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

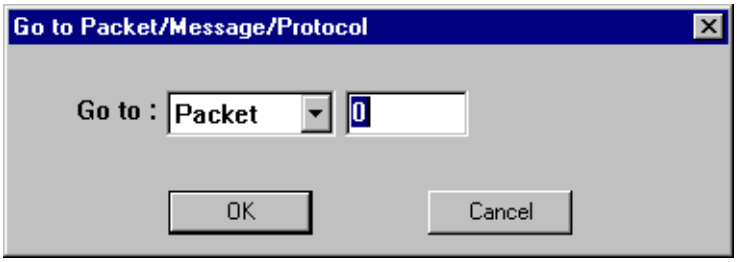
To display a triggering event, select **Go to Trigger** under **Search** on the Menu bar. The **Trace Viewer** display will reposition the trace to show the triggering event at the top of the screen.

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.**

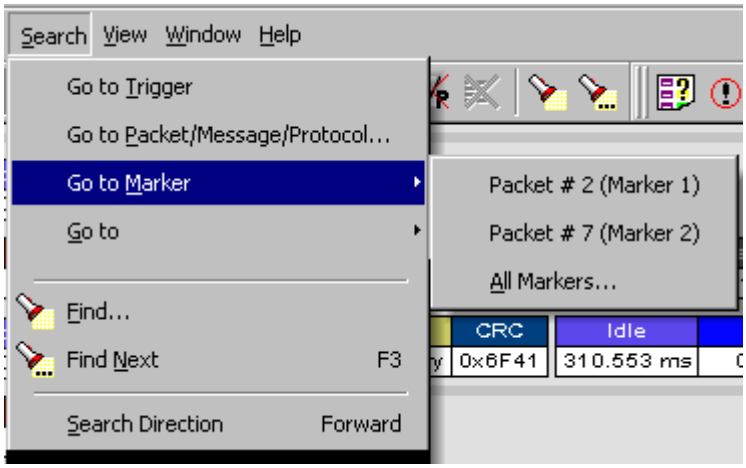
The Trace View repositions to show the packet at the top of your screen.

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.

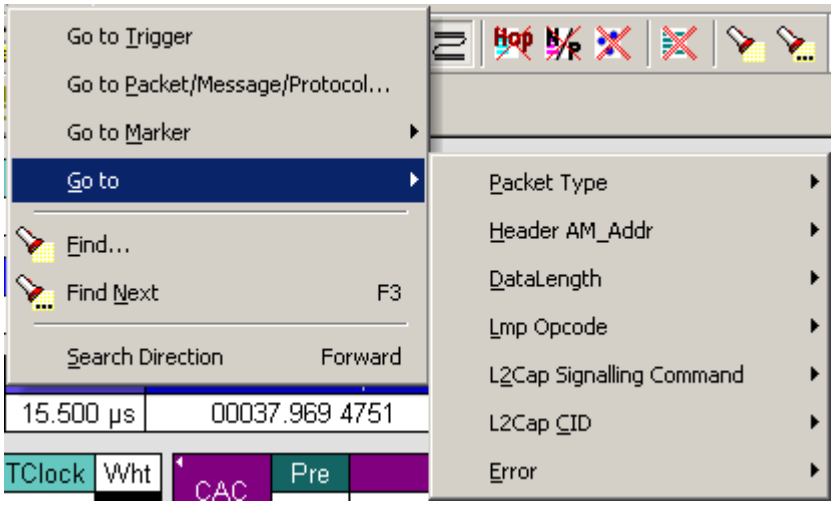
Note The **Go to Marker** feature functions in conjunction with the **Set Marker** feature. The comments within the parentheses following each marked packet are added or edited with the **Set Marker** feature.

Go to

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

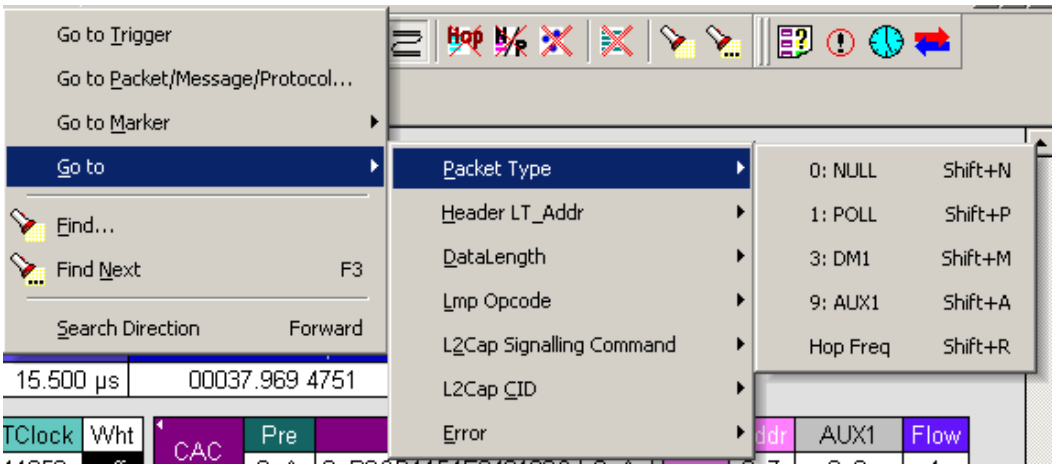
Step 1 Select **Go To** under **Search** on the Menu Bar.

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



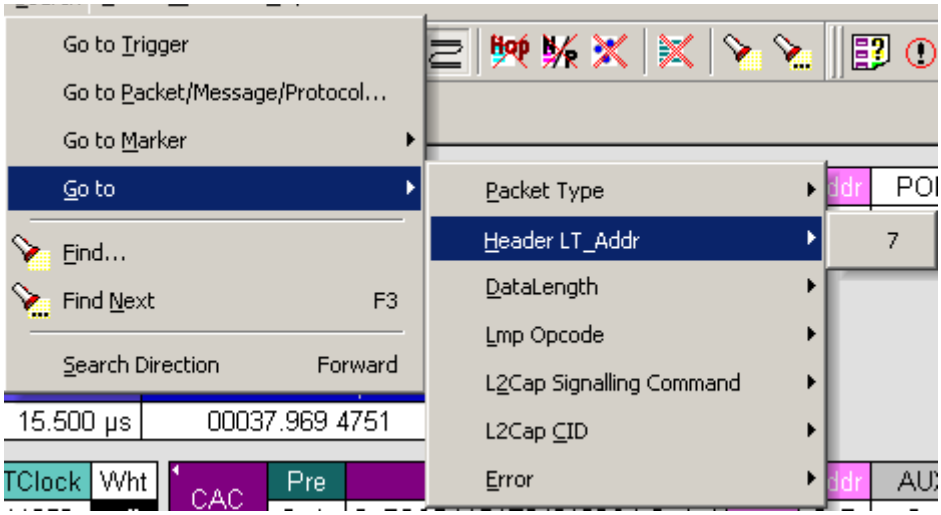
Step 2 Select the event you want to go to and enter the necessary information.

Packet Types



Select the type of packet you want to go to.

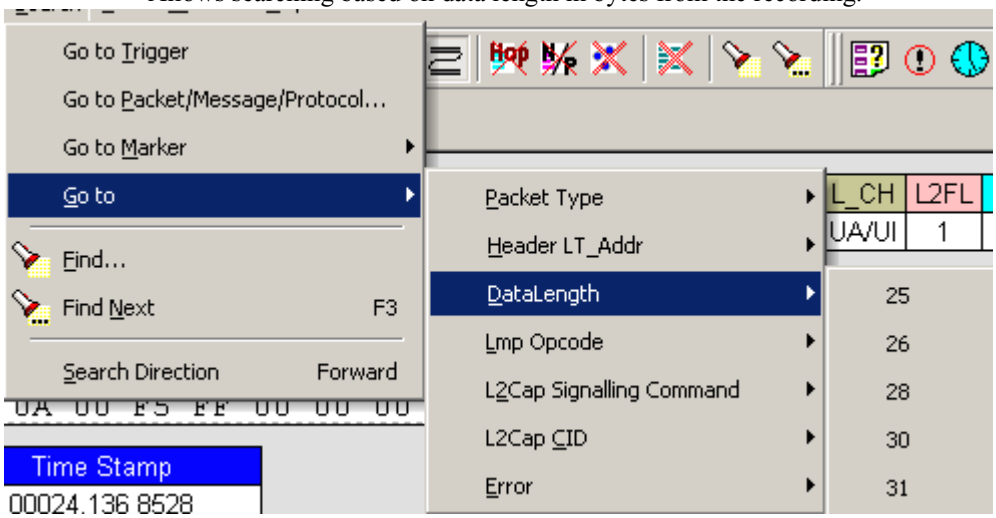
Header LT_Addr



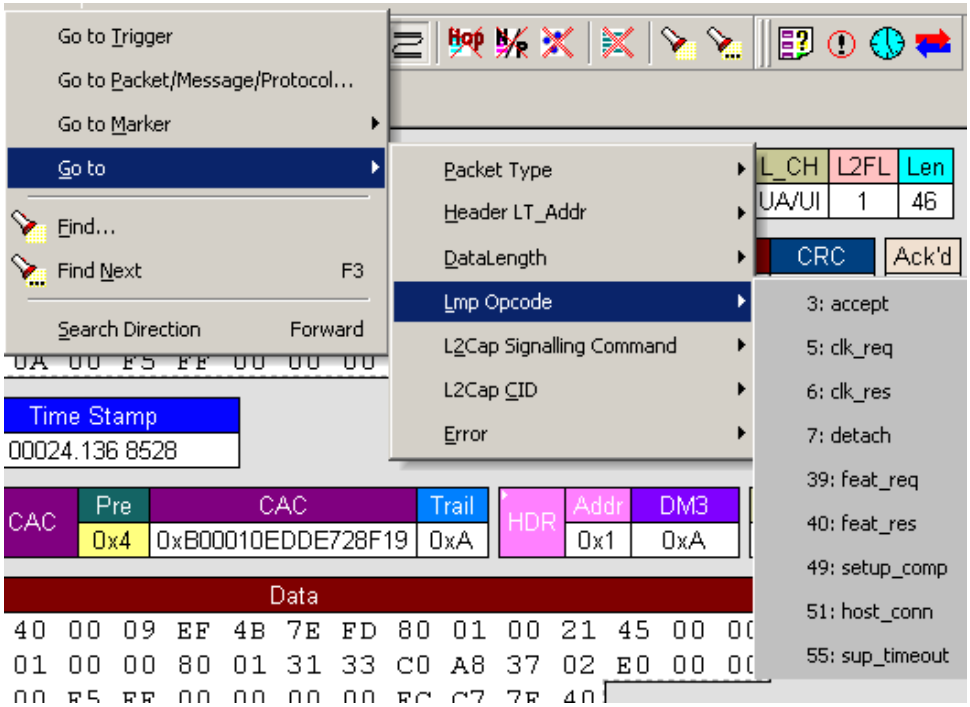
Select an Logical Transport Address from the list.

DataLength

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

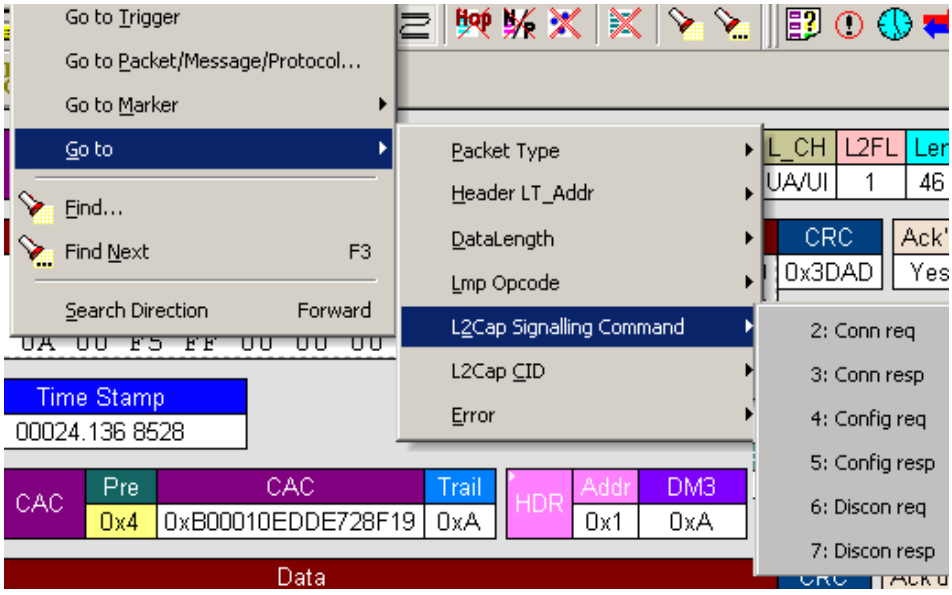


Lmp Opcode



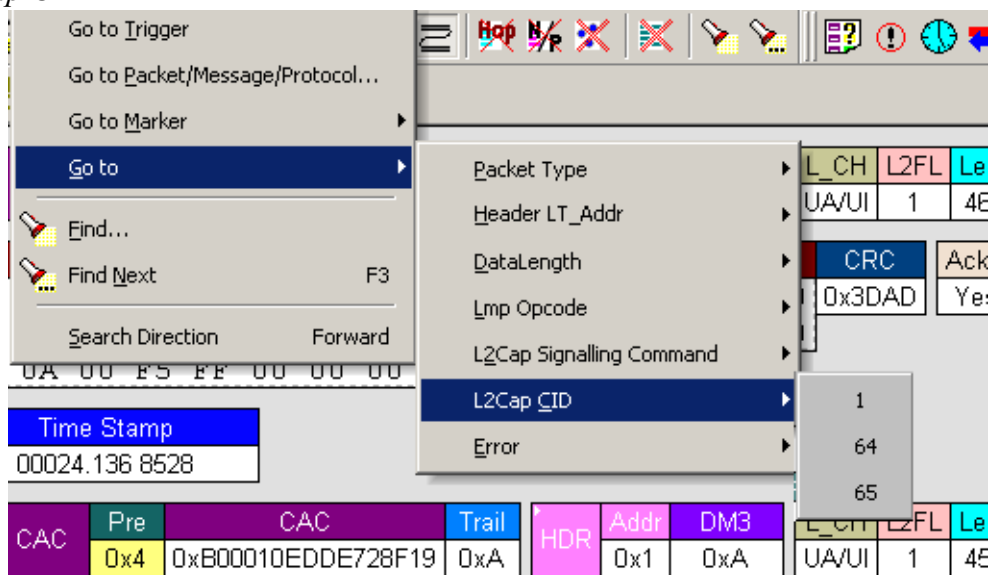
Select the Link Management Protocol Operational Code (Lmp Opcode) that you want to go to.

L2Cap Signalling Command



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

L2Cap CID



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

Error

Moves trace view to next uncorrected error.

Soft Bit Error

Moves trace view to next soft (corrected) error.

Loss of Sync

Moves trace viewer to the next loss of sync.

Find

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

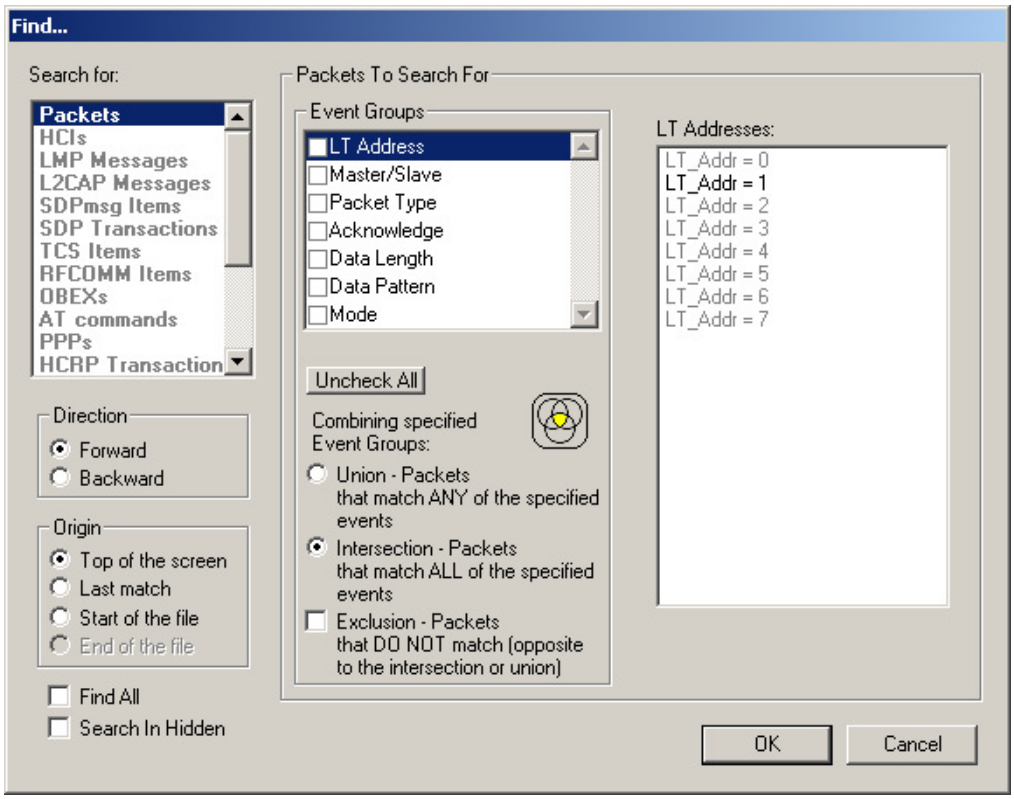
To start find,

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

OR

Click in the Tool Bar.

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



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

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

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

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

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

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

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

In the screenshot shown above, for example, LT 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.

LT Address

Contains a list of seven Logical Transport 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).

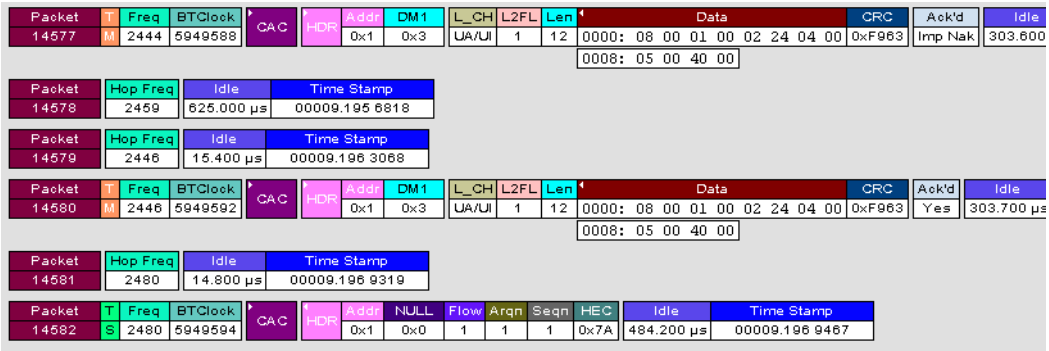
Explicit NACK - Explicitly not acknowledged. An Explicit NACK is an explicit response by a device that it did not receive a data packet. The Explicit NACK is transmitted in the ARQN field (=Acknowledgment Request Negotiation field). ARQN=0 means 'Explicit NACK.'

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.

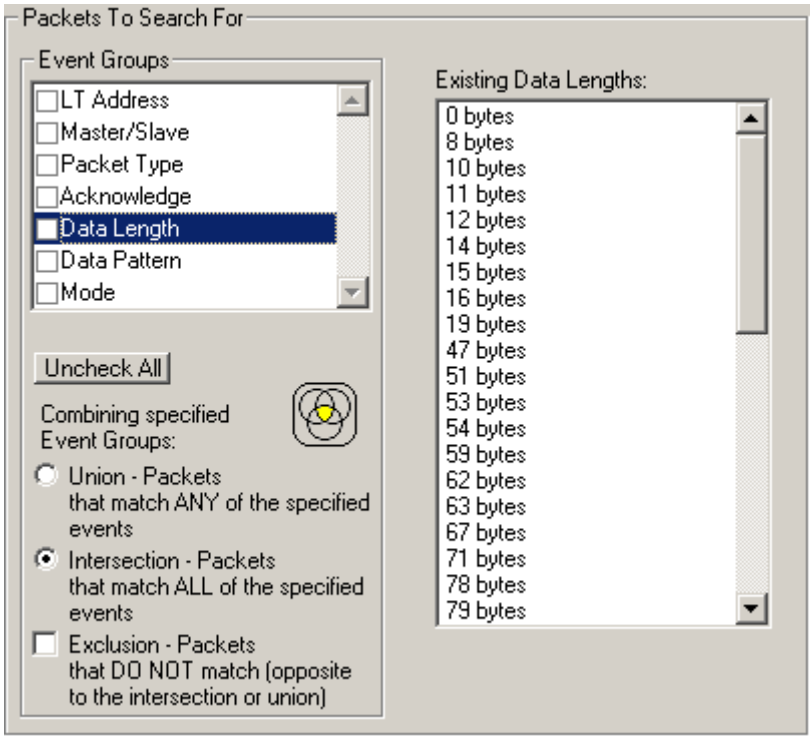


Implicit NACK - Packet 14577 is a data packet sent by the piconet Master device. Packet 14579 should have been a data packet with an acknowledgment. Instead, it is an empty packet. This Master interprets this empty packet as an **Implicit NACK** (i.e., implicitly not acknowledged). BTTracer summarizes 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**.

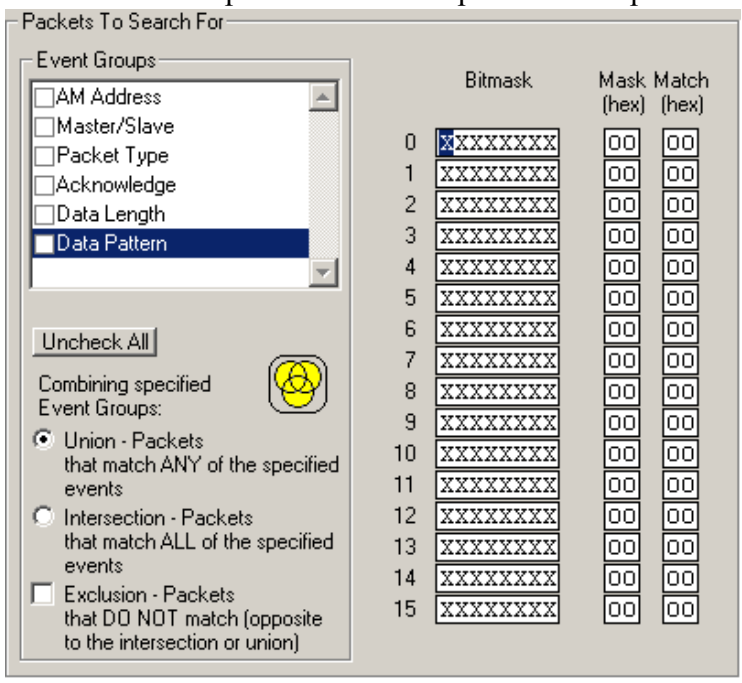
Data Length

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.'

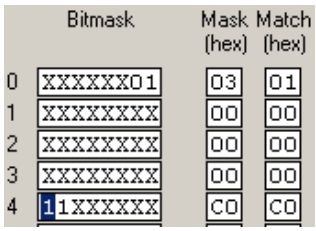
Example -- xxxxxx01 means 'Look for a data pattern where the first 6 bits can be any value but the last two bits must be 01.'

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.'



Searching for Hexadecimal Patterns

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

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.

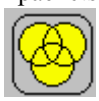
Step 2 Select a search direction and origin.

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.

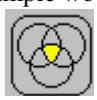
Step 4 If you have selected two or more criteria, then select either :

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

Step 5 Click **OK**.

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

Some Find Examples

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

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

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

Step 3 From the Event Group, select **Header LT_Addr**.

Step 4 From the box on the right, select **LT_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 Logical Transport 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 LT_Addr** from the Event Group.

Step 4 Select **LT_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 LT_Addr=7* and *Poll packets with LT_Addr=7*.

Exclude all packets with ANY of the following attributes: DM1, Poll, or LT_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 LT_Addr** from Event Group.

Step 4 Select **LT_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 LT_Addr=7*.

Find Next

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

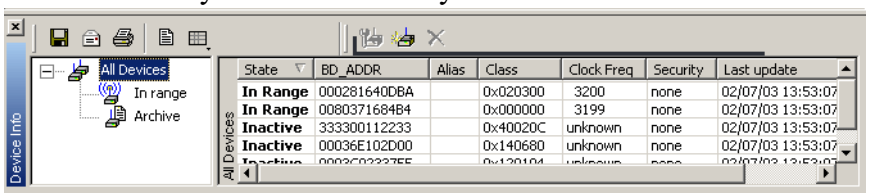
- Select **Find Next** under **Search** on the Menu Bar

  OR

  Click on the Tool Bar.

11.2 Device List

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



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

Fields in the Device List

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

Buttons

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

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

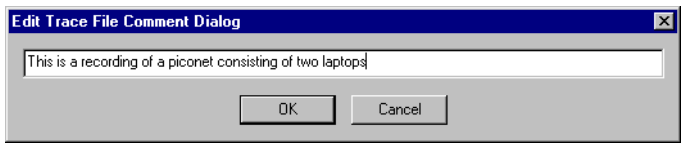
Remove Device -- Removes the selected device from the Device List.

11.3 Edit Comment

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

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

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



Step 2 Create, view, or edit the comment.

Step 3 Click **OK**.

11.4 File Information

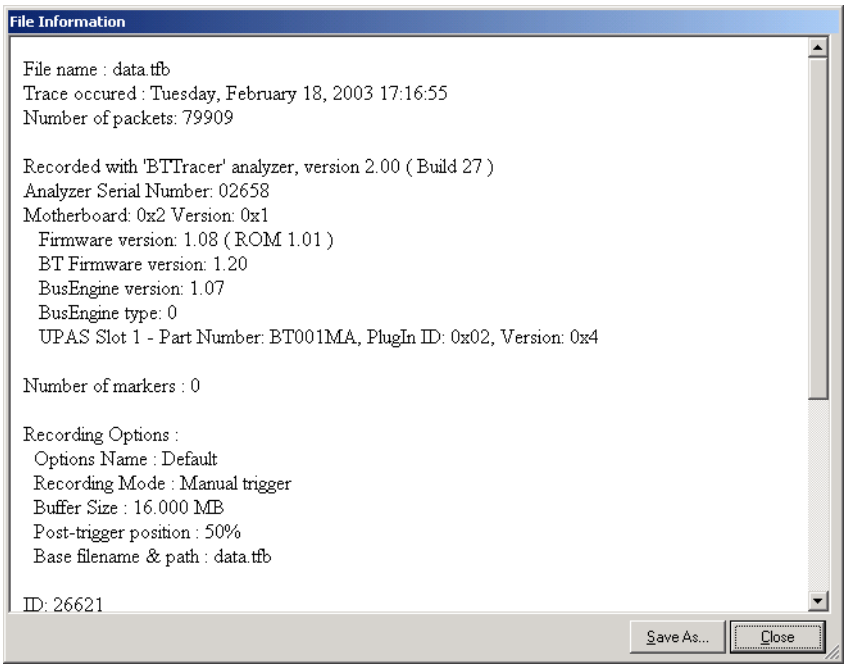
To display a File Information report,

- 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.

11.5 Error Summary

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

11.6 Timing Calculations

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

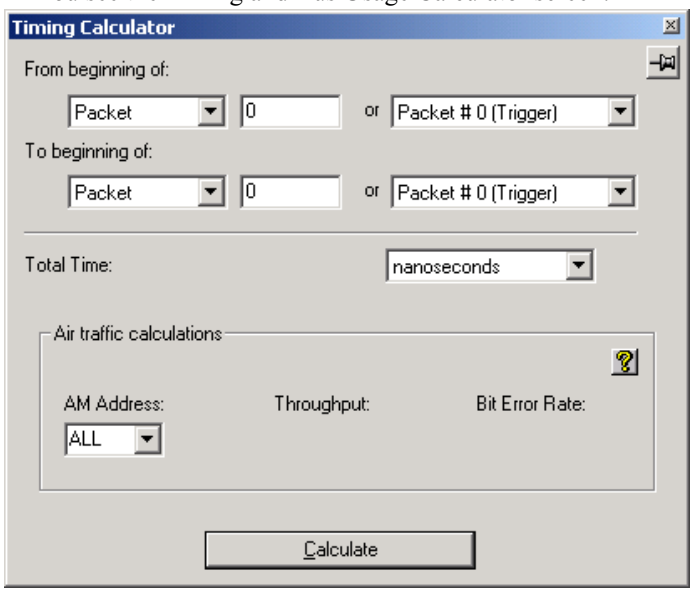
To display a File Information report,

- 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 LT Address drop-down menu.

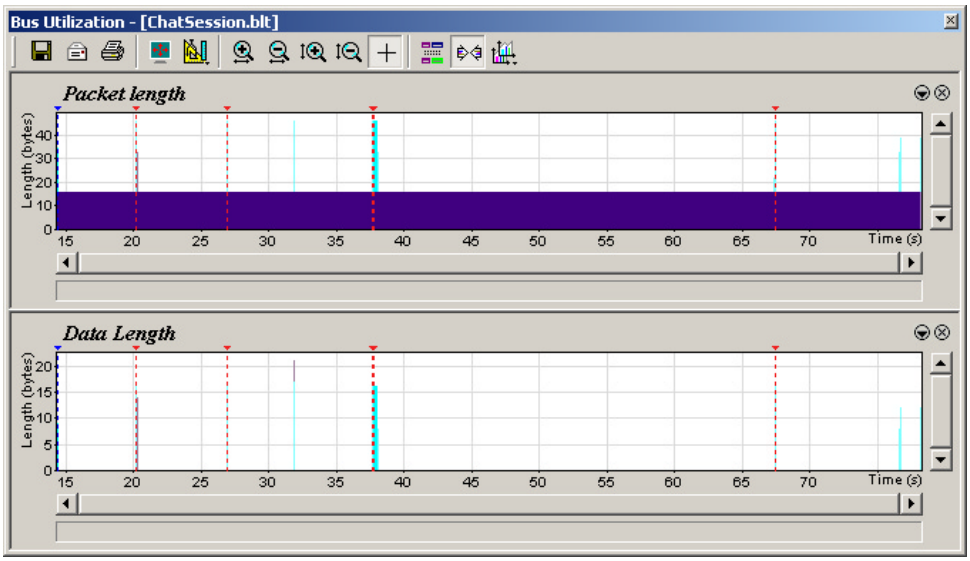
Step 3 Click the "Calculate" button.

At this point, bus usage will be calculated.

11.7 Bus Utilization

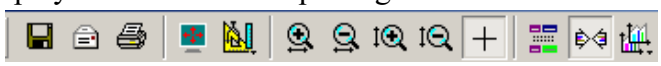
The **Bus Utilization** window displays a graph of bandwidth use within a displayed trace.

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



Bus Utilization Buttons

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



The buttons have the following functions:

Save As - Saves the graphs as a bitmap file (*.bmp)

Email - Creates an email with a *.bmp file attachment of the graphs

Print

Full Screen

View Settings - opens a sub-menu with options for formatting the display. See "View Settings Menu" below.

Vertical zoom in

Vertical zoom out

Click and Drag zoom - Click diagonally to select and zoom in on part of the graph

Select Range

Sync and Graph areas - If two or more graphs are displayed, this button will synchronize the graphs to one another. Once synchronized, the positioning slider of one graph will move the other graphs

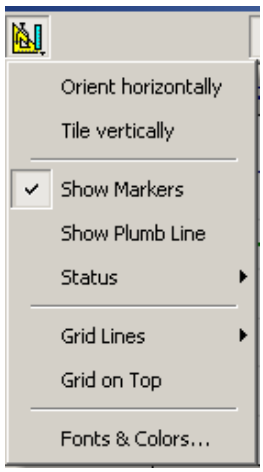
Horizontal zoom in

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

Horizontal zoom out

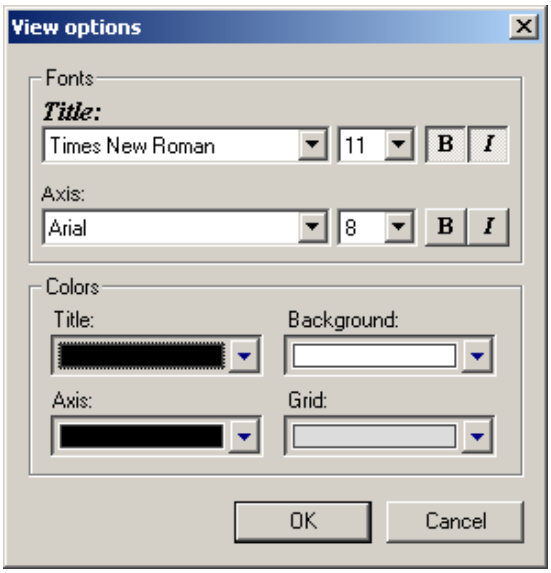
View Settings Menu

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



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

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

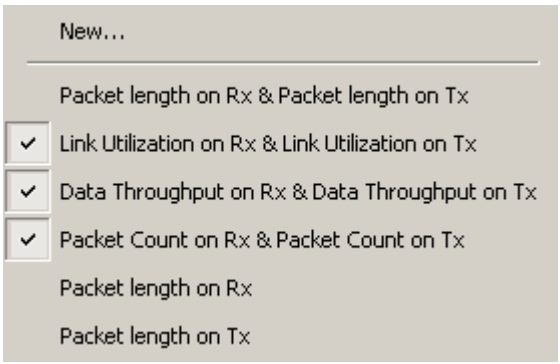


Graph Areas Menu

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

Step 1 Click the button.

The Graph Areas menu opens.



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

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

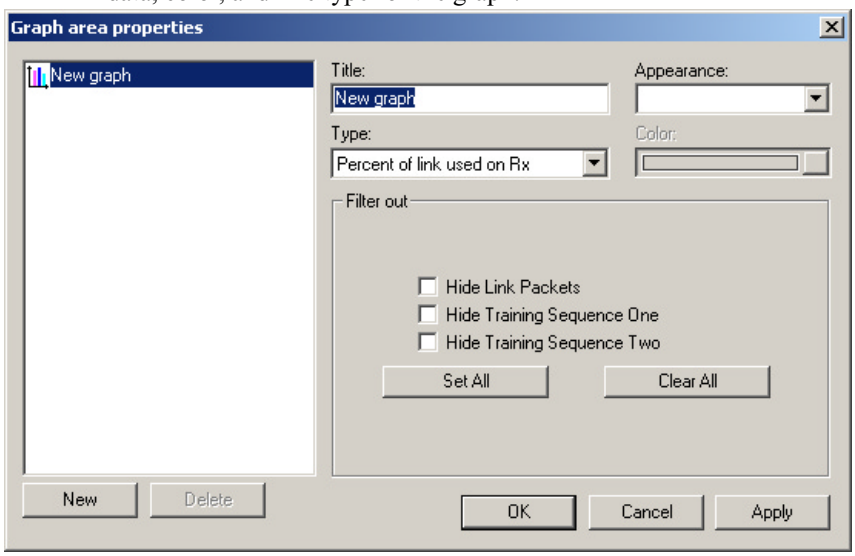
Step 1 In the **Graph Area**s menu, select the type of data to be displayed.

Step 2 Click **OK**.

Or

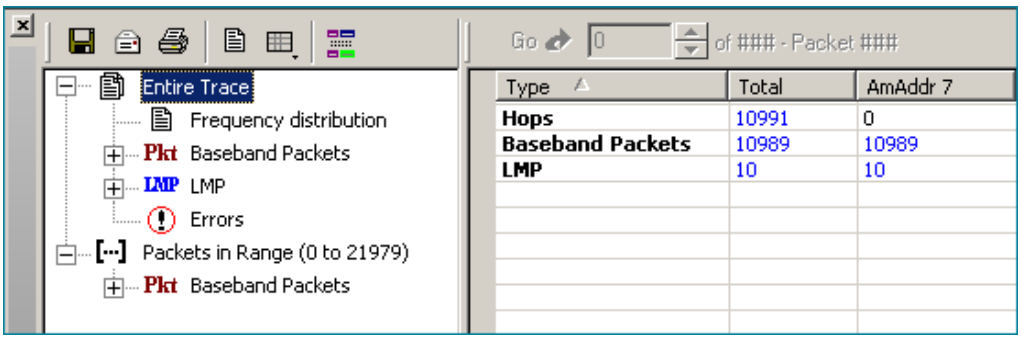
To make a new graph, click **New**.

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



11.8 Traffic Summary

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



To open the Traffic Summary window, press .

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

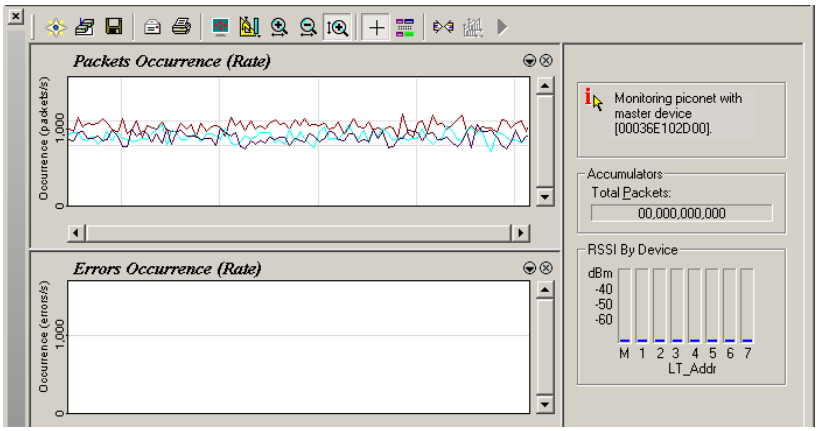
11.9 Real-Time Statistics

The Real-Time Statistics window displays a graph of real-time link activity.

Real Time Statistics displays a summary of the traffic currently being recorded by the analyzer.

To display the Real-Time Statistics window, click in the Tool Bar.

The Real Time Statistics window opens:



In order to see a graph of traffic, you will need to start recording. After starting piconet activity, press to start the Real-Time statistics monitor. BT*Tracer* will then synchronize to the piconet and stream data in real time to this window and presented in a format of your choice.

To stop the monitor, press .

Real-Time Statistics Buttons

The Real-Time Statistics toolbar has buttons for changing the format of the displayed data and for exporting data:

The buttons have the following functions:

Save As - Saves Real-Time graphs as bitmap files (*.bmp)

Email - Creates an email with a *.bmp file attachment of the graphs

Print

Full Screen

View Settings - opens a sub-menu with options for formatting the display.

Vertical zoom in

Vertical zoom out

Click and Drag zoom - Click diagonally to select and zoom in on part of the graph

Select Range

Sync and Graph areas - If two or more graphs are displayed, this button will synchronize the graphs to one another. Once synchronized, the positioning slider of one graph will move the other graphs

Horizontal zoom in

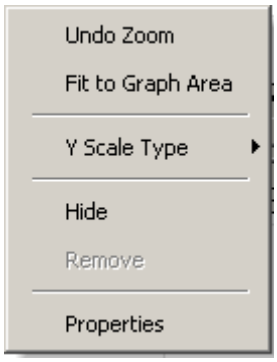
Horizontal zoom out

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

Start. Starts the Real-Time Monitor.

Stop Real-Time Monitoring.

Reset. Resets the graphs.



Real-Time Statistical Monitor Pop-up Menu

If you right-click a graph in the Real-Time window, a pop-up menu will appear with options for changing the format of the display.

Undo Zoom - If you have zoomed in, this command will undo the zoom.

Fit to Graph Area - Redisplays graph so that the entire trace fits inside graph area.

Y Scale Type -·

Linear - Converts display to linear format.

Logarithmic - Converts display to logarithmic format.

Hide - Hides the selected graph.

Properties - Opens a dialog box with options for changing the colors, titles and other features of the graphs.

Displaying Multiple Graphs

The Real Time Statistics window gives you the ability to create up to three separate graphing windows so that you can create separate graphs of traffic and tile them vertically. Within these windows, you can format the graphs in a number of ways.

- To view two or three graphs simultaneously, click the **Graph Areas** button.

A menu opens with the following graph options:

- **General Statistics**
- **Packet Occurrence (rate)**
- **Errors Occurrence (rate)**

- **Retransmissions -** This graph shows the rate of retransmitted packets. In the Real-Time Statistics, a packet is evaluated as 'retransmitted' if at least one non-FHS seqn bit has already been received and if the previous sequence bit is the same as the current sequence bit. As the sequence bit toggles on data payloads carrying CRC, the Real-Time Statistics tracks the seqn bits in DM, DV, DH payload, and checks for correctness only if the payload was correctly decoded without errors.

11.10 Encryption

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

In order for 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.

Note - The encryption settings here are for the BTTracer only. The BTTrainer has its own encryption settings.

Note - There is no need to configure Encryption settings if BT*Tracer* is used to record BT*Trainer* traffic.

Configuring BTTracer for Encryption

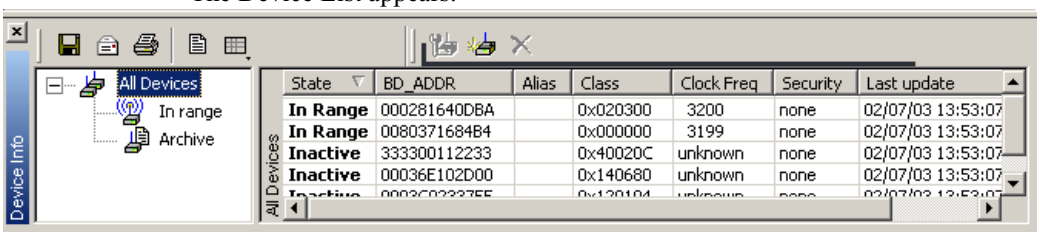
For BTTracer to successfully decrypt traffic, two steps need to be performed: 1) BTTracer needs to be given the PIN or Link Key for each Master-Slave connection; and 2) Recording needs to be begun *before* the Slave connects to the Master. If recording is begun prior to the creating the Master-Slave 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 **View >Device List**

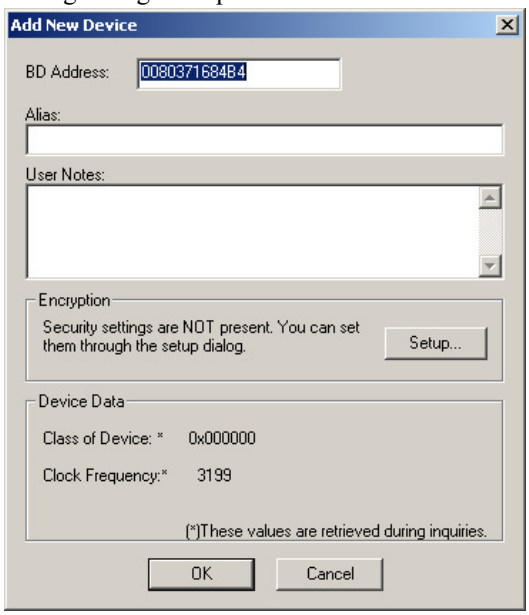
The Device List appears.



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

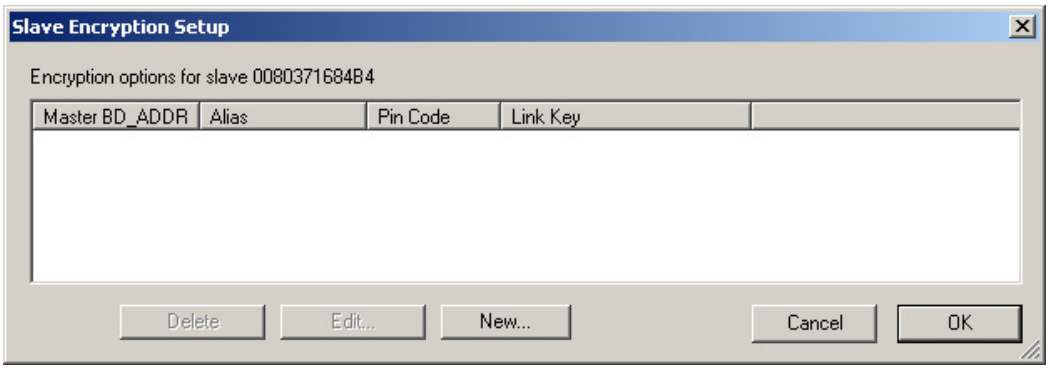
Step 3 Click the Edit Devices button

The following dialog box opens.



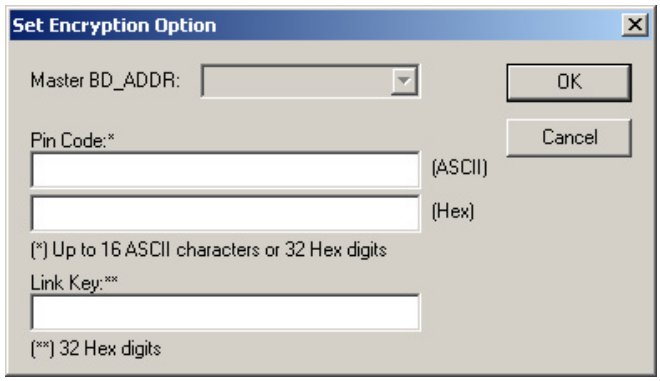
Step 4 Click the **Setup ...** button.

The following dialog box opens:



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

The following dialog box appears.



Step 6 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 7 If you do not have the PIN, or if the Master and Slave have already agreed upon the Link Key, manually enter a Link Key as a 128 bit (sixteen byte) hex value into the box marked **Current Link Key**. If you have the PIN, you can skip this step.

Step 1 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 2 Click **OK**

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

Step 3 Click **OK**.

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

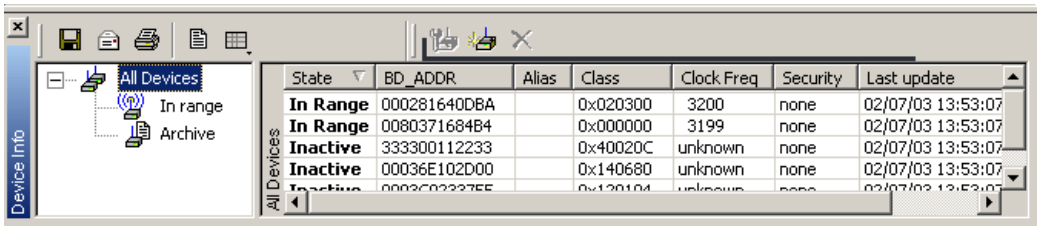
11.11 Re-applying Encryption Settings

If you record a trace with the wrong encryption settings, the trace will not decrypt properly. BT*Tracer* lets you correct the problem by re-applying encryption settings after a recording is finished.

To correct an improperly decrypted trace file, perform the following steps.

Step 1 With the trace open, open the Device List by selecting **View > Device List** from the menu.

The Device List opens.

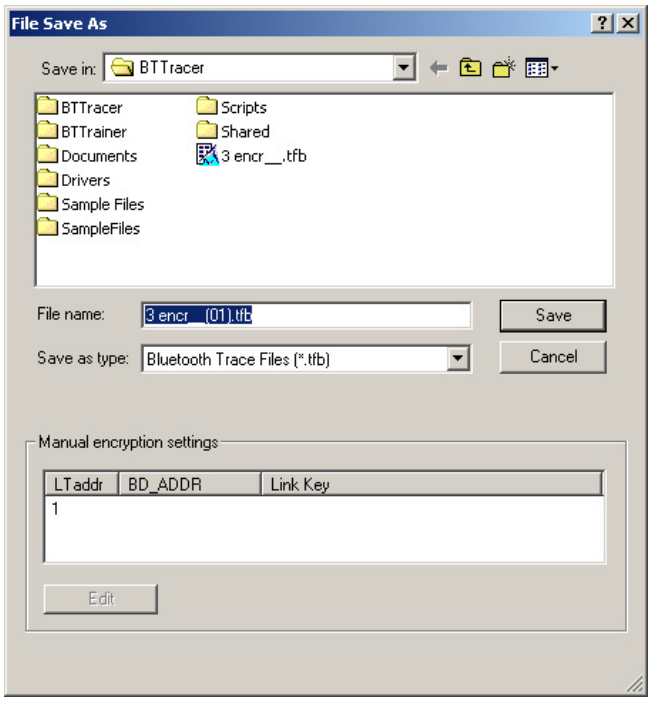


Step 2 Follow the directions outlined above in Section 11.10, "Encryption" on page 170 for adding/editing encryption settings.

Step 3 Once the new encryption settings have been applied, run the

command **File > Re-apply Encryption Settings ...**

A Save As dialog box opens.



Step 4 Enter a file name (or use the default) and click **OK**.

The file is saved and the new settings are automatically applied. The new file opens automatically.

The file should now be decrypted properly.

Re-applying Encryption On Incomplete Traces

If your trace does not capture the authentication procedure, there will be no way for the analyzer to determine the BD Address of the Slave device. Accordingly, the software will not be able to decrypt the trace file.

If you are using a development kit and already know the BD Address of the Slave device and the Link Key, you can enter it manually in the Save As dialog box shown above.

Note LMP_start_encryption_req still has to be present in the trace in order to manually correct the settings.

Step 1 Select **File** > **Re-apply Encryption Settings**.

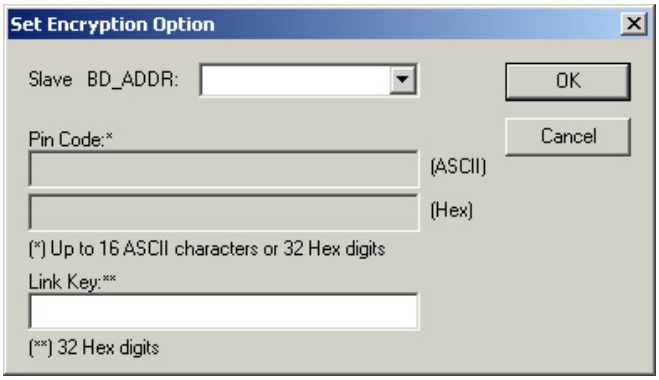
The Save As dialog opens (shown on preceding page.)

Step 2 Select the LT Address for the device whose traffic you are

trying to decrypt.

Step 3 Click the **Edit** button.

Step 4 The **Set Encryption Options** dialog box opens.



Step 5 Enter the BD Address and Link Key.

Step 6 Click **OK**.

The dialog box closes.

Step 7 Click **Save**.

The dialog box closes and the traffic is decrypted according to your settings.

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

Limited Hardware Warranty

So long as you or your authorized representative ("you" or "your"), fully complete and return the registration card provided with the applicable hardware product or peripheral hardware products (each a "Product") within fifteen days of the date of receipt from Computer Access Technology Corporation ("CATC") or one of its authorized representatives, CATC warrants that the Product will be free from defects in materials and workmanship for a period of three years (the "Warranty Period"). You may also complete your registration form via the internet by visiting http://www.catc.com/support/register/. The Warranty Period commences on the earlier of the date of delivery by CATC of a Product to a common carrier for shipment to you or to CATC's authorized representative from whom you purchase the Product.

What this Warranty Does Not Cover

This warranty does not cover damage due to external causes including accident, damage during shipment after delivery to a common carrier by CATC, abuse, misuse, problems with electrical power, including power surges and outages, servicing not authorized by CATC, usage or operation not in accordance with Product instructions, failure to perform required preventive maintenance, software related problems (whether or not provided by CATC), problems caused by use of accessories, parts or components not supplied by CATC, Products that have been modified or

altered by someone other than CATC, Products with missing or altered service tags or serial numbers, and Products for which CATC has not received payment in full.

Coverage During Warranty Period

During the Warranty Period, CATC or its authorized representatives will repair or replace Products, at CATC's sole discretion, covered under this limited warranty that are returned directly to CATC's facility or through CATC's authorized representatives.

How to Obtain Warranty Service

To request warranty service, you must complete and return the registration card or register via the internet within the fifteen day period described above and report your covered warranty claim by contacting CATC Technical Support or its authorized representative. CATC Technical Support can be reached at 800-909-7112 or via email at support@catc.com. You may also refer to CATC's website at http://www.catc.com for more information on how to contact an authorized representative in your region. If warranty service is required, CATC or its authorized representative will issue a Return Material Authorization Number. You must ship the Product back to CATC or its authorized representative, in its original or equivalent packaging, prepay shipping charges, and insure the shipment or accept the risk of loss or damage during shipment. CATC must receive the Product prior to expiration of the Warranty Period for the repair(s) to be covered. CATC or its authorized representative will thereafter ship the repaired or replacement Product to you freight prepaid by CATC if you are located in the continental United States. Shipments made outside the continental United States will be sent freight collect.

Please remove any peripheral accessories or parts before you ship the Product. CATC does not accept liability for lost or damaged peripheral accessories, data or software.

CATC owns all parts removed from Products it repairs. CATC may use new and/or reconditioned parts, at its sole discretion, made by various manufacturers in performing warranty repairs. If CATC repairs or replaces a Product, the Warranty Period for the Product is not extended.

If CATC evaluates and determines there is "no trouble found" in any Product returned or that the returned Product is not eligible for warranty coverage, CATC will inform you of its determination. If you thereafter request CATC to repair the Product, such labor and service shall be performed under the terms and conditions of CATC's then current repair

policy. If you chose not to have the Product repaired by CATC, you agree to pay CATC for the cost to return the Product to you and that CATC may require payment in advance of shipment.

General Provisions

THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE ADDITIONAL RIGHTS THAT VARY BY JURISDICTION. CATC'S RESPONSIBILITY FOR DEFECTS IN MATERIALS AND WORKMANSHIP IS LIMITED TO REPAIR AND REPLACEMENT AS SET FORTH IN THIS LIMITED WARRANTY STATEMENT. EXCEPT AS EXPRESSLY STATED IN THIS WARRANTY STATEMENT, CATC DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES FOR ANY PRODUCT INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF AND CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES THAT MAY ARISE FROM ANY COURSE OF DEALING, COURSE OF PERFORMANCE OR TRADE USAGE. SOME JURISDICTIONS MAY NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, SO THE PRECEDING LIMITATION MAY NOT APPLY TO YOU.

CATC DOES NOT ACCEPT LIABILITY BEYOND THE REMEDIES SET FORTH IN THIS LIMITED WARRANTY STATEMENT OR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES INCLUDING, WITHOUT LIMITATION, ANY LIABILITY FOR THIRD PARTY CLAIMS AGAINST YOU FOR DAMAGES, PRODUCTS NOT BEING AVAILABLE FOR USE, OR FOR LOST DATA OR SOFTWARE. CATC'S LIABILITY TO YOU MAY NOT EXCEED THE AMOUNT YOU PAID FOR THE PRODUCT THAT IS THE SUBJECT OF A CLAIM. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE PRECEDING EXCLUSION OR LIMITATION MAY NOT APPLY TO YOU.

The limited warranty on a Product may be transferred for the remaining term if the then current owner transfers ownership of the Product and notifies CATC of the transfer. You may notify CATC of the transfer by writing to:

Technical Support
Computer Access Technology Corporation
2403 Walsh Avenue
Santa Clara, CA 95051-1302 USA

or by email at: support@catc.com.

Please include the transferring owner's name and address, the name and address of the new owner, the date of transfer, and the Product serial number.

INDEX

Symbols

!IXGEN_DONT_EDIT_THIS! 47

Numerics

1100 packet 99
1101 packet 99

A

Abort upload 44
Acknowledge 154
Action buttons 36, 105
Actions tab 104
Addr 124
Addresses
  AM_ADDR 99
  Bluetooth 64
  slave device 54
  target 65
Analyzer
  describing Bluetooth 2
  set up 9
  status 44
API 4
Application installation 11
Architecture of Piconet 3
Arqn 124
ARQN condition 99
AT 132
Authentication 170
Automation Feature 4
AUX1 packet 99

B

Basic installation 9
Bit pattern, searching 157
Blue dot menus 107
Bluetooth
  BusEngine 6
  described 1
  device address 64
  first recording 15
  limited search 89
  recording traffic 112
  search for device 60
  searching for devices 50
  target address 65
BNEP 132
Bubble help 46
Buffer size 15, 78
Bus utilization 163
BusEngine
  Bluetooth 6
Buttons
  bus utilization 164
  graph area 166
  toolbar 36

C

CAC 124
Calculations, timing 162
CATC Technical Support 177
Certification 7
Channel connections, L2CAP 135
Clicked fields, menus in 129
Clock rate, match 88
Collapse data 126
Comments, editing 161
Components, physical 5
Configuring encryption 170
Connecting events 106
Connectors
  data 7
  physical 7
Correlation Value 87
Counters
  connecting events 106
  value 107
CRC 124
CRC error 102

D

Data
  decoding 132
  expand, collapse 126
  filename 15
  length 101

pattern 96, 101
searching by length 150
searching by pattern 156
transfer message 134
Debug file 79
Decoding 132
Description of Merlin 2
Device
Bluetooth address 64
general search 52
search 50
search for Bluetooth 60
slave address 54
DH1, 2, 3 packet 99
Displaying information 123, 161
DM1 124
DM1, 2, 3 packet 99
Duration of search 60
DUT Recv/Xmit Freq 82
DV packet 99

E

Editing comments 161
Enable
debug file 79
Encryption 170
Environmental Conditions 7
Error summary 162
Errors
CRC 102
FEC 102
header length 102
HEC 102
invalid packet 102
payload length 103
Searching for 152
setting conditions for 102
sync loss 103
threshold exceeded 102
types of 96
Established Piconets 84
Events
conditions 99
connecting 106
sequencing 111
tab 96
trigger 15, 78
Exclusion search 157
Existing Piconet, recording 58
Expand data 126
Explicit NACK 154
External
input signals 96, 103
trigger form 110

F

Features 5
FEC Error 102
FHS packet 99
File information, displaying 161
File menu 33
Filename and data 15
Filter In/Out button 105
Filter Out/In 108
Filtering 97, 99
Find feature, using 157
Finding 152
Finding devices 50
Flow 124
Fonts 166
Force resynchronization 86
Frequencies, DUT 82
Frequency hops, hiding 128

G

General description 2
General features 5
General inquiry 85, 89
General options
recording 75
General purpose output 110
Go to
DataLength 150
error 152
Header AM_Addr 150
L2Cap CID 152
Lmp Opcode 151
marker 148

packet types 149
packet/Message/Protocol 147
Graphs
areas menu 166
bus utilization 164
buttons 166
Grid
lines 165
on Top 165
Groups, events 96

H

HDLC 132
Headers
AM_Addr 150
length error 102
packets 98
payload 99
HEC 124
HEC Error 102
Help menu 36
Hexadecimal patterns, searching 157
HID 132
Hiding 128, 129
Higher protocols, decoding 131
High-pulse output 109
Hops
hiding 128
reduced mode 68
Hot keys 46
Humidity 7
HV1, 2, 3 packet 99

I

Idle 124
Implicit NACK 154
Information, interpreting 123
Input signals 96, 103
Inquiry
general 89
perform/skip 49
Installation
basic 9
Interpreting a trace 123
Intersection search 157
Introduction 1
Invalid packet type error 102

K

Keyboard shortcuts 46

L

L_CH (Logical Channel) 100, 124
L2CAP
channel connections 135
CID, searching 152
described 132
messages 129, 131, 134
L2FL 124
Len 124
Length of data 101
License 177
Linking events 106
LMP
described 132
messages 131, 134
Opcode 151
Logical Channel 100
Long pattern, searching 157
Loss of sync
searching for 152
timeout 86
Low-pulse output 109

M

Manual trigger 7, 15, 78
Markers
editing and clearing 125
searching 148
setting 124
Master
and slave 154
switch 87
Master/address 64
Match clock rate 88
Memory, Recording 7
Menus
blue dots in events 107
clicked fields 129

pulldown 33
veiw settings 165
Merlin
configure encryption 170
description of 2
Message
searching 147
Messages
LMP, L2CAP 131, 134
transfer 134
Modes
test, recording in 68

N

NULL packet 99
Nulls, hiding 128

O

OBEX 132
Opcode 124
Operating temperature 7
Options
general recording 75
name 15
search 66
Orient horizontally 165
Output signals, enabling 109
Overview 1, 33

P

Package dimensions 7
Packets
1100, 1101 99
AUX1 99
DM1, 2, 3 99
DV 99
FHS 99
headers 96, 98
headers in 98
hiding 120
HV1, 2, 3 99
invalid type error 102
NULL 99
POLL 99
searching 147, 149
types 99, 154
viewing 134
Page
sync and record 96
Paging traffic 87
Passive sync and record 84
Patterns, data 101
Payload
headers 96, 99
length error 103
Percentage of triggering 79
Phone numbers, Technical Support 177
Physical Components 5
Piconet
established devices 84
master address 64
private device 85
recording 54, 58
recording traffic on 48
sample 3
search options 66
slave address 54
sync and record 84
synchronizing 54
target address 65
Wizard 55
PIN 170
Pkt 132
Polls
hiding 128
POLL packet 99
Position of trigger 79
Post triggering, percentage 79
Power
LED 7
Switch 7
PPP 132
Pre-triggering 79
Private Device Piconets 85
Program
installation 11
Progress indicator, recording 42
Protocol

Analyzer 2
Architecture 3
decoding 132
searching 147
Pull-down menus 33
Pulse low signal 109
Pulse toggle signal 109

R

Reading a trace 123
Real time statistics 167
Record inquiry 89
Record menu 33
Recording
Bluetooth traffic 15, 112
existing Piconet 58
LED 7
memory 7
Piconet 54
progress indicator 42
reduced hop mode 68
session 16
type 77
Recording Options
events 96
general 15, 75, 77
in Wizard 55
saving 112
Recording type 58
Recv, DUT freq 82
Reduced hops 68
Reports
menu 33
Restart button 105
Resynchronization, forced 86
RFCOMM 132

S

Sample
Piconet 3
recording 16
Saving
recording options 112
SDP Msg 132
Search 52
duration of 60
general 62
Search menu 33
Search options 66
Search type 50, 60
Searching
by data pattern 156
complex 152
data length 150
for bit pattern 157
for bit patterns 157
for errors 152
Header AM_Addr 150
L2Cap CID 152
Lmp Opcode 151
packet types 149
recorded traffic 147
Security 170
SEQN condition 99
Sequence
event 111
Set marker 124
Setup
menu 33
Shortcuts, keyboard 46
Show markers 165
Show plumb Line 165
Signalling
message 134
Signals
input 96, 103
outputs, enabling 109
Size of buffer 78
Slave device, address 54
Slave switch 87
Snapshot 15, 77
Soft Bit Error, searching 152
Software
installation 11
overview 33
Special Interest Groups (SIGs) 1
Specifications 7

Statistics
real-time 167
Status
status bar 165
Status of Analyzer 44
Storage temperature 7
Summary
error 162
traffic 167
Support, technical 177
Switches 7, 87
Sync
and record 83, 84
loss error 103
loss of, searching 152
timeout, loss of 86
window 89
Synchronization, forced 86
Synchronize Piconet 54
Synchronized LED 7

T

Tabs
recording events 96
recording, general 15, 76
recording, options 75
Technical Support 177
Temperature tolerances 7
Test debug 79
Test mode, recording in 68
Threshold Exceeded error 102
TID 124
Tile vertically 165
Time Stamp 124
Timeout
loss of sync 86
Timeslot filtering 97
Timing calculations 162
Tips, tool 46
Toggle signal 109
Toolbar 36
Tooltips 46, 124, 133
Trace
filename 15
reading 123
sample 16
Traffic
Bluetooth 112
generation 6
hiding 129
on Piconet 58
paging 87
recording 66
recording on piconet 48
searching 147
summary 167
Trail 124
Transfer message, data 134
Trigger
event 78
external form 110
LED 7
position 15, 79
post triggering 79
recording, manual 78
Type of recording 77

U

Unassociated traffic, hide 129
Union search 157

V

Values, changing counters 107
View
menu 33
options 36
packets 134
settings menu 165

W

Warranty 177
Weight 7
Window menu 36
Wizard
Piconet 55

X

Xmit, DUT freq 82

Z

Zoom 45