


An Introduction to using FTS4BT

Installation of FTS4BT is covered in the Bluetooth Quick-Start Guide which may be found in your FTS4BT desktop folder.


How to setup to capture Bluetooth data:

Open the FTS4BT folder on your desktop.

FTS4BT has different sniffing modes to accommodate various applications. This folder contains shortcuts for the following different modes that will allow you to sniff different situations.

1.  Air Sniffer (Basic)

This is the standard Air Sniffer using the Bluetooth ComProbe (USB dongle) as the hardware interface to Bluetooth air traffic.

2.  Air Sniffer (Mixed Piconet)

Mixed Piconet mode is used to sniff a V1.1 Bluetooth specification device and a V1.2 Bluetooth specification device on the same piconet. A master must use a different Frequency Hopping Pattern when communicating with the V1.2 specification device than with a V1.1 device. FTS4BT will use a second Bluetooth ComProbe to follow the second Frequency Hopping pattern. The data collected by both ComProbes will be shown in the same GUI. There are two I/O Parameter setups for the two different (V1.1 and V1.2) devices. Synchronization setup is the same for both Data Sources.

3.  Air Sniffer (Redundant)


This mode uses two ComProbes to sniff the same Piconet to ensure that no data is being missed.

4.  Air Sniffer (Scatternet)

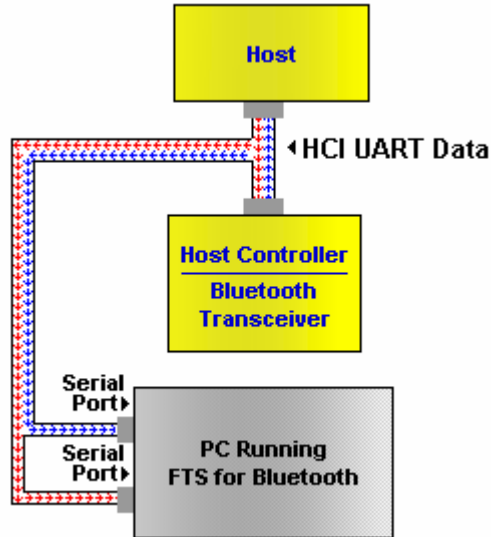
In Bluetooth a device can be a slave in one Piconet and a master in another, this is called Scatternet. Again, as in Mixed Piconet, there is more than one hopping pattern. FTS4BT employs a second Bluetooth ComProbe to follow the second hopping pattern, as it does in Mixed Piconet. If there are more than two Piconets in the Scatternet then additional ComProbes may be added as needed.

5.  Capture File Viewer

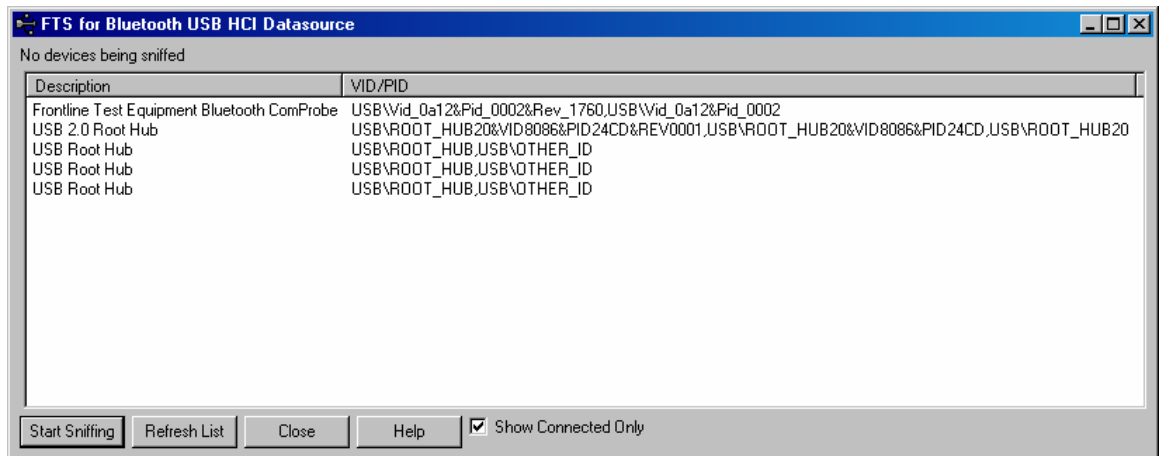
The Capture File Viewer is used for analyzing previously captured data.

6.  Serial HCI Sniffer **(BCSP), (H4), (H5).**

Serial HCI sniffing is used to monitor data going between a Host and Host controller, FTS4BT includes a set of custom cables for Serial RS-232 sniffing. Using HCI sniffing in conjunction with air sniffing, a complete picture of the Bluetooth transmission can be captured. Serial BCSP stands for Blue Core Serial Protocol. This was developed by CSR. Serial H4 is the normal Serial UART. Serial H5 is a new specification 3 wire UART (close in specification to BCSP).



7. USB HCI Sniffer (H2)



The USB HCI Data source dialog allows the user to select which Bluetooth device to sniff and to Start and End the sniffing process. The dialog has a list containing the Bluetooth Devices connected to your system. If the *Show Connected Only* checkbox is unchecked then all USB devices that have ever been connected to your system will be listed. If you have connected or disconnected a device while this dialog is open, click on Refresh List to update the list. To sniff a USB device, just select it with your mouse and click on Start Sniffing.

Note: Start USB HCI sniffer **before** you run an application on the USB port.

8. Virtual Sniffer

The Virtual Sniffer is a live import facility within FTS4BT that makes it possible to access any layer in a stack that the programmer has access to and feed this data into the Virtual Sniffer FTS4BTV. Please refer to the "Show Live Import Information" button on the Virtual Sniffer Datasource window in FTS4BT.

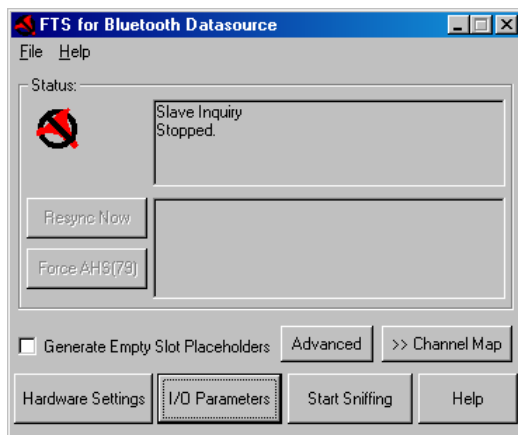
More information is available in the Options Folder in FTS4BT Desktop folder, and a white paper is available at http://www.fte.com/downloads/Datasheets/FTS4BT_Virtual_Sniffing_white_paper.pdf

FTS4BT Setup Folder.

The setup folder contains documentation on program setup and configuration, and the “Bluetooth ComProbe Maintenance Utility” which is used to configure and update firmware in the Bluetooth ComProbe(s).

Setting up FTS4BT to sniff over the air.

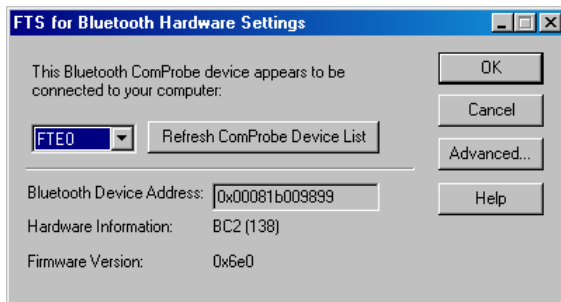
1. Open FTS4BT “Air Sniffer (Basic) in the desktop folder.



This will bring up the FTS4BT Datasource. This is where parameters are set for sniffing, including synchronization mode, and the devices to be sniffed.

Hardware Settings.

Select Hardware settings button.

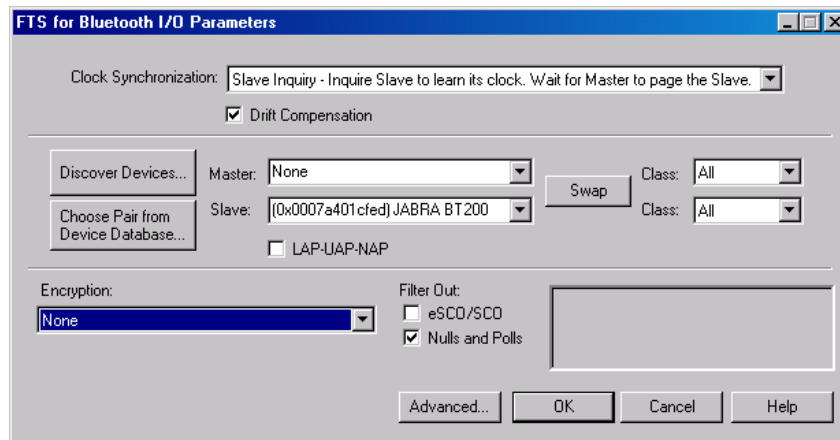


Here the Bluetooth ComProbe may be selected and tested.

- Click Advanced.
- If you have previously captured the pairing of devices, a list of link keys that have been previously calculated by FTS4BT will be displayed here. Two devices that have previously paired will use the same link keys until they are paired again.

2. Open the I/O Parameter window on the FTS4BT Datasource.

How to setup the I/O Parameters.



If you have two Bluetooth devices:

- Make both devices discoverable.
- Press the “Discover Devices” button. FTS4BT will find any discoverable Bluetooth devices in its range. You will then be able to select any of these devices from the master and slave drop down lists.

Select the synchronization mode that best suits your application:

a) **Slave Inquiry** (Inquire the slave device to learn its clock. Wait for the master to page the slave). This is the recommended choice for most situations. FTS4BT will perform an inquiry of the slave and determine its clock. In this mode, the slave must be discoverable.

b) **Master Inquiry** (Inquire the master device to learn its clock). FTS4BT will target the master device, make a Device Discovery and determine its clock and by doing so synchronize to that device clock. It is possible to synchronize to a master’s clock before or after a baseband connection is made in the piconet. The master must be discoverable.

c) **Slave Page**. (Page the slave device to learn its clock. Wait for the master to page the slave). This is how FTS learns the clock of a device that is NOT discoverable. For example, after a phone and a headset have paired, generally the headset will not be discoverable to a general inquiry. If the headset is a slave device and it is not discoverable, then FTS4BT will not be able to synchronize to that device using Slave Inquiry mode. If we know the headset (slave) BD-ADDR then by using Slave Page mode, FTS4BT will be able to page the device, (but will never complete the connection during the page session). After FTS4BT has learned the clock information during the paging process, FTS4BT will discontinue the paging process and will now be synchronized to the undiscoverable slave’s clock.

4. Inform FTS4BT which device is going to be master and which device is going to be slave.
Note that it is necessary to select both a master and slave device only if the link you are

sniffing is using encryption. Otherwise you need only select the device FTS4BT will be synchronizing to.

5. Enter Encryption PIN code if necessary. If the link to be sniffed is encrypted, FTS4BT needs the PIN code in order to calculate the link key the two devices are using. Alternately, you may enter the Link Key if it is known. FTS4BT also keeps a database of the link keys it's previously calculated, which may be accessed by clicking the "Choose Pair from Device Database button:

BD_ADDR	Friendly Name	Services	Class of Device	Service/COD	Paired BD_ADDR	Link Key
0x0007a401cfed	JABRA BT 200	Audio	Wearable Headset Device	0x200404		
0x0007a401cfed	JABRA BT 200	Audio	Wearable Headset Device	0x200404	0x9abc56781234	0x16c143f758bb6b
0x000272b00000	BelkinLAP[192.168.0.10]	Networking	LAN/Network Access point	0x020300		
0x0050f27d0f1a	CHANNA		Desktop work.station	0x000104		
0x000d18011170	Tom	Networking, Object Transfer, Audio	Desktop work.station	0x320104		
0x0050f27d0cc3	ERIC_NEW	Networking	Desktop work.station	0x020104		
0x00605711b96a	N bean cell	Object Transfer, Telephony	Cellular	0x500204		

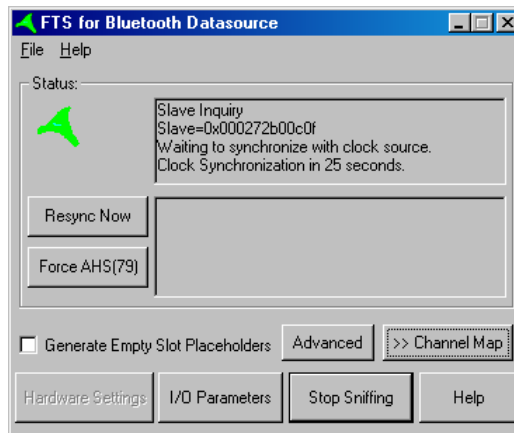
If the link to be sniffed is not encrypted, select None in the drop down list.

6. Select the **Filter Out** (eSCO/SCO, NULL,POLL) set up. These filters are low level hardware filters. There are also Display Filters that you may use later to filter the captured data. Any data filtered out here will not be captured at all.

7. The OK button should now be available. If OK is grayed out, there is something set up incorrectly in the I/O Parameter window. For example, if you select Master Inquiry and do not have a master device selected then OK will be grayed out.

If you're using Slave Inquiry, it's important that you have the ComProbe positioned within six inches or so of the master and to keep the slave at least two feet from the ComProbe. This will give you more consistent synchronization.

Press OK, and then press Start Sniffing. When you Start Sniffing the Status Icon will go red (not yet synchronized). After a short time (less than 30 seconds) the icon should change to green.



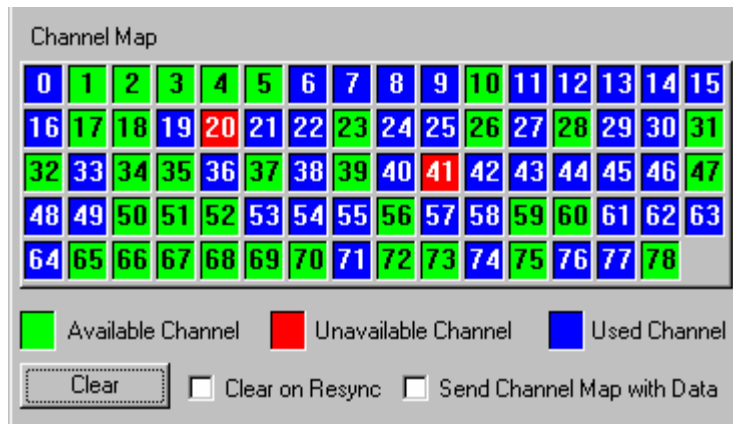
As indicated in the status box, FTS4BT is synchronized to the slave's clock and waiting for the master to connect with a baseband connection.

Every 30 seconds, the sniffer will cycle through the synchronization process again. This is to ensure that there is no clock drift between the ComProbe and the Bluetooth device (slave in this case). With 5 seconds left to re-synchronization the color will change to yellow. When a baseband connection is made the icon color will change to blue. When the icon is blue data will be collected, assuming that either the "Start Capturing to Buffer" or "Start Capturing to Disk" button has been pressed.

The Datasource dialog also has a Channel Map, which is a dynamic visual indication of which channels are used, available or unavailable. This is used for a new feature of Bluetooth spec V1.2 called Adaptive Frequency Hopping, (AFH). AFH is used to assist Bluetooth and WLAN (802.11) in sharing the same ISM band.

Bluetooth AFH will:

- Check all 79 Channels and get a status of which channels are busy or have "interference".
- Report those channels to the Bluetooth Baseband.
- Decide which channels it will use.
- Our Dynamic Channel Map represents this graphically, in real time.



Capturing Data:

Press the Start Capture button and the Start Sniffing button.

Synchronizing to the piconet is straightforward if you follow these basic rules.

- Make sure you know which device is master. The device that initiates the connection is the master even though the roles may change later.
- Make sure that you have the correct slave BD_ADDR(s) selected.
- When a baseband connection is established, the icon will turn blue and data should appear in the Frame Display. If you wish to empty the Buffer of data captured from previous activity then you can "Clear the Buffer". "Clear Capture Buffer". "Frame Display" Icon

Decrypting Encrypted Data:

Here is a typical Frame Display of FTS4BT where FTS4BT has successfully captured and decrypted encrypted data. Master initiates a random number. Master and slave initiate Combination Keys and they are authenticated by master and slave.

B...	Fr...	Role	AM_Addr	Opcode	Initiated by	Original Opcode	Frame Size	Delta	Timestamp
3	Master	7	name_req	master			16		08/20/2004 02:25:28.1028 PM
4	Slave	7	name_res	master			25	00:00:00.0118	08/20/2004 02:25:28.1147 PM
5	Master	7	detach	master			16	00:00:00.0056	08/20/2004 02:25:28.1203 PM
8	Master	7	features_req	master			23	00:00:45.2421	08/20/2004 02:26:13.3625 PM
9	Slave	7	features_res	master			17	00:00:00.0118	08/20/2004 02:26:13.3743 PM
10	Master	7	host_connection_req	master			15	00:00:00.0043	08/20/2004 02:26:13.3787 PM
11	Slave	7	accepted	master	host_connection_req		10	00:00:00.1018	08/20/2004 02:26:13.4806 PM
12	Slave	7	setup_complete	slave			9	00:00:00.0025	08/20/2004 02:26:13.4831 PM
21	Slave	7	accepted	master	in_rand		10	00:00:06.1712	08/20/2004 02:26:19.6543 PM
22	Master	7	comb_key	master			31	00:00:00.0131	08/20/2004 02:26:19.6675 PM
23	Slave	7	comb_key	master			25	00:00:00.1431	08/20/2004 02:26:19.8106 PM
24	Master	7	au_rand	master			31	00:00:00.0143	08/20/2004 02:26:19.8250 PM
25	Slave	7	sres	master			13	00:00:00.1418	08/20/2004 02:26:19.9668 PM
26	Slave	7	au_rand	master			25	00:00:00.0025	08/20/2004 02:26:19.9693 PM
28	Slave	7	accepted	master	encrypt_mode_req		10	00:00:00.2425	08/20/2004 02:26:20.2118 PM
29	Master	7	encrypt_key_size_req	master			16	00:00:00.0056	08/20/2004 02:26:20.2175 PM
30	Slave	7	accepted	master	encrypt_key_size_req		10	00:00:00.0043	08/20/2004 02:26:20.2218 PM
34	Master	7	start_encrypt_req	master			31	00:00:00.0268	08/20/2004 02:26:20.2487 PM

Frame 1 of 67 (Master) 08/20/2004 02:25:28.0815 PM

Errors: Baseband:Packet Status

For Help Press F1

This is a full pairing procedure between two devices. FTS4BT must capture this pairing procedure (Between Frame 8 and Frame 34) before it can decrypt the data in the piconet. If FTS4BT misses any of these details then decryption is not possible. FTS4BT MUST also have the correct PIN code that is entered into the two devices.

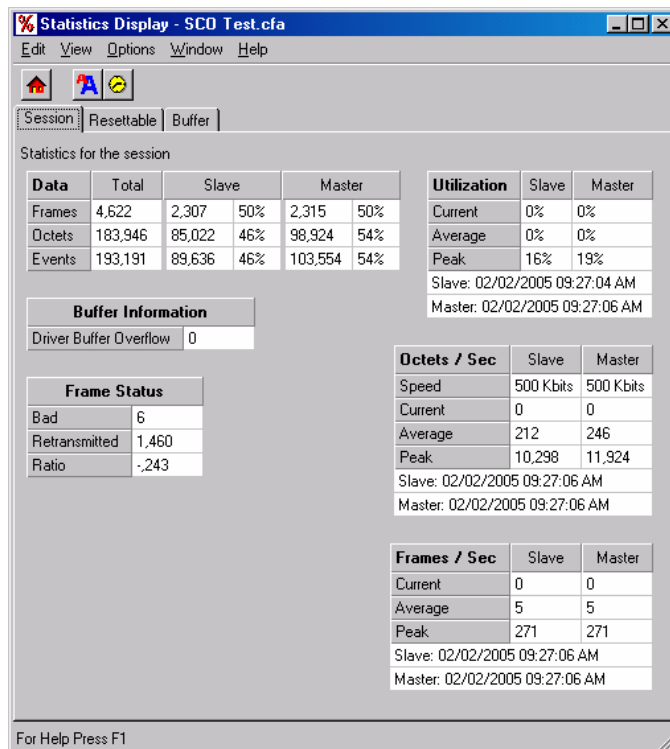
Failure to Decrypt:

If FTS4BT doesn't have all the information it needs, it won't be able to calculate the link key correctly. The link key is made up from the combination keys and the BD_ADDRs and the PIN code. If FTS4BT gets any of these parameters wrong it will generate an incorrect link key. Note, after the "Start Encryption Request" (frame 24, highlighted). All the frames following are shown as bad packets. This is a good indication that the sniffer is unable to decrypt any payload data in the baseband packets after encryption is enabled within the piconet. The most common cause of this is an incorrect PIN code entered in the I/O Configuration window, or FTS4BT synchronizing too late and consequently not calculating the correct Link Key.

All Protocols																	
Baseband																	
LMP																	
B...	Frame#	CLK	Chan	Role	BD...	AM...	Status	TYPE	LLID	FLOW	L2CAP Fl...	SEQN	ARQN	Len	LMP Opcode	Tran ID	Original Opcode
●	19	0x0000b8b4	59	M	7	OK	OK	DM1	LMP	Go	N/A [1]	0	1	2	encrypt_mo...	M	
●	20	0x0000b93a	43	S	7	OK	OK	DM1	LMP	Go	N/A [1]	0	0	2	accepted	M	encrypt_mode...
●	21	0x0000b93e	11	S	7	OK	OK	DM1	LMP	Go	N/A [1]	1	0	1	setup_com...	S	
●	22	0x0000b94c	16	M	7	OK	OK	DM1	LMP	Go	N/A [1]	1	1	2	encrypt_ke...	M	
●	23	0x0000b96a	23	S	7	OK	OK	DM1	LMP	Go	N/A [1]	0	0	2	accepted	M	encrypt_key_s...
●	24	0x0000b9b4	52	M	7	OK	OK	DM1	LMP	Go	N/A [1]	0	1	17	start_encry...	M	
●	25	0x0000ba3e	67	S	7	CRC...	CRC...	DM1	LMP	Go	N/A [0]	1	0	15			
●	26	0x0000bad8	73	M	7	Leng...	Leng...	DM1	L2...	Go	Stop	1	1	25			
●	27	0x0000badc	69	M	7	Leng...	Leng...	DM1	LMP	Go	N/A [0]	0	1	29			
●	28	0x0000bae0	57	M	7	Leng...	Leng...	DM1	LMP	Go	N/A [1]	1	1	31			
●	29	0x0000bb3c	30	M	7	Leng...	Leng...	DM1	Co...	Go	Stop	0	1	19			
●	30	0x0000bb48	0	M	7	Leng...	Leng...	DM1	L2...	Go	Stop	1	1	20			

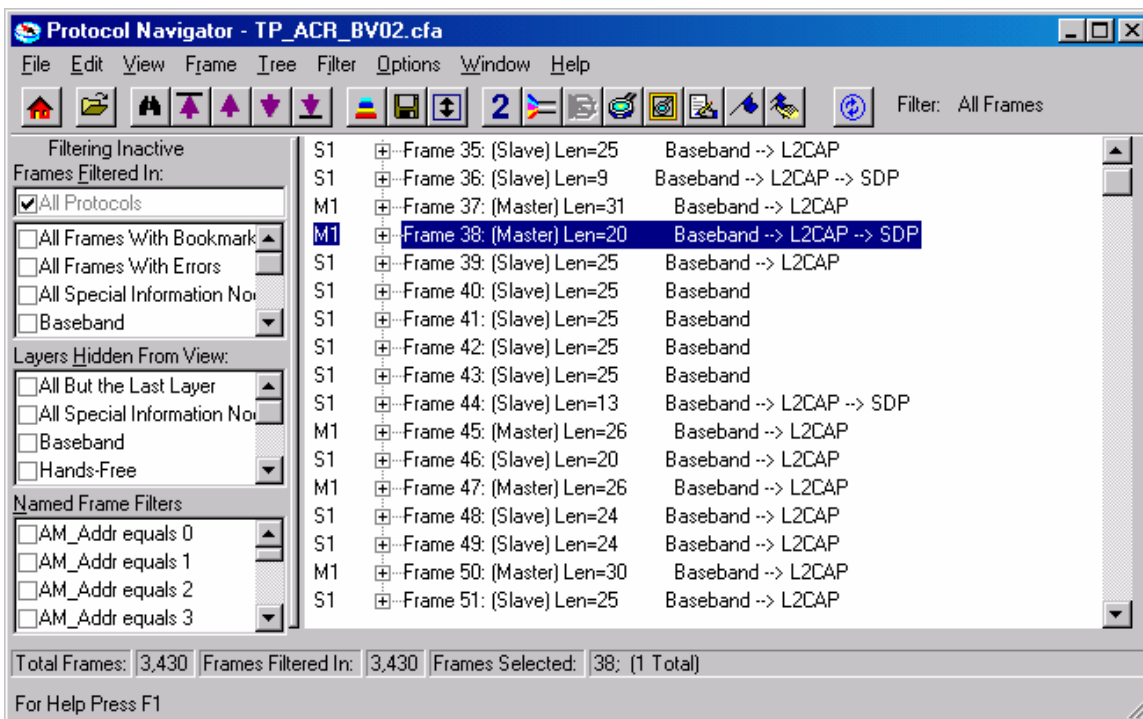
Features and Benefits of the GUI Statistics Viewer:

Check Live Data rate speed.
Bad Packets/Retransmitted Packets Ratio.

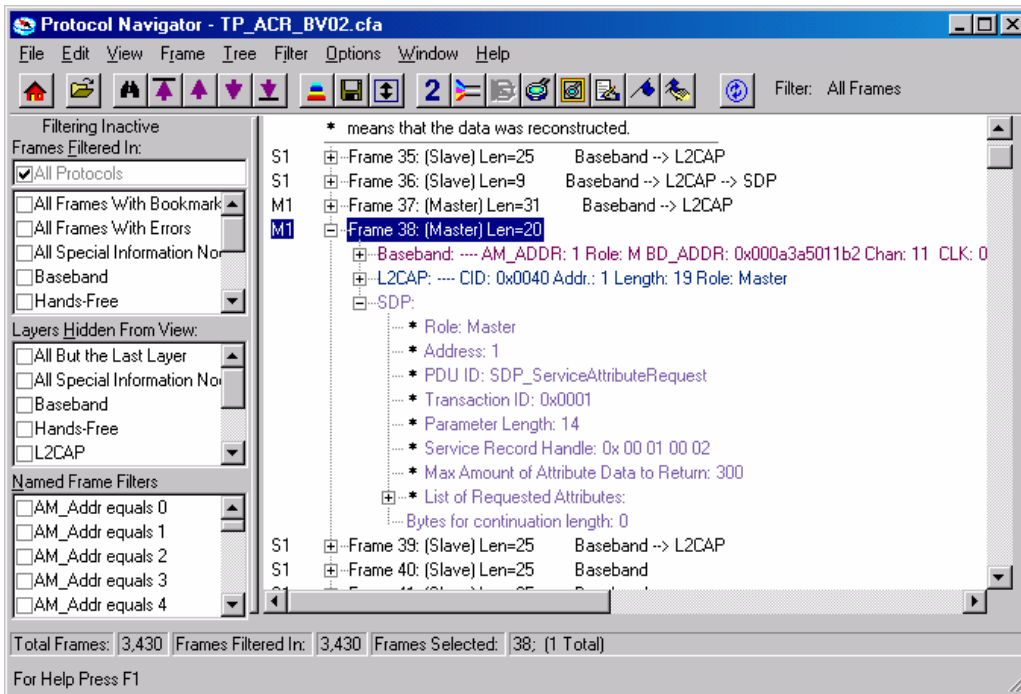


Protocol Navigator:

The Protocol Navigator (PN) can give a good overall view of protocols decoded in a log file. Data may be shown at a high level:



. The branches of the tree may be expanded in order to drill down into the details of the decode:

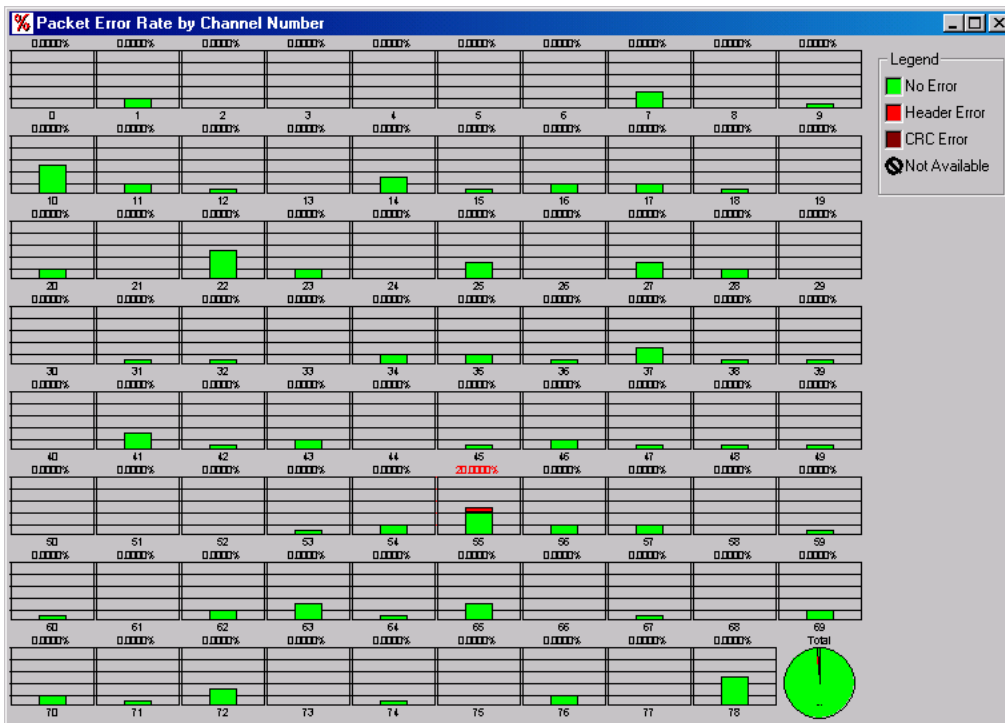


Plugins

At the moment there are three different types of Plugins.

FTS4BT intend to add more Plugins in the near future.

- OBEX extraction Application Data
- Show Packet Error rate (PER) Status.
 - Error rates are displayed graphically, by individual channel number:



- Audio extraction of eSCO/SCO to .wav file format. With this feature, you may convert captured audio data to a .wav file that may be played back with the Windows Media Player, or other audio playback software.

