FTS4BT Air Sniffer Basic Tutorial

Introduction

This tutorial focuses on the procedures necessary to establish a passive connection between the FTS4BT analyzer and the Bluetooth air traffic. Although this tutorial assumes that you chose to run FTS4BT in the Air Sniffer (Basic) mode, the procedures contained in this tutorial apply to setting up the FTS4BT Datasource for all air sniffer modes.

This basic Air Sniffer mode uses the Bluetooth ComProbe (USB dongle) as the hardware interface to Bluetooth air traffic.

Before you begin:

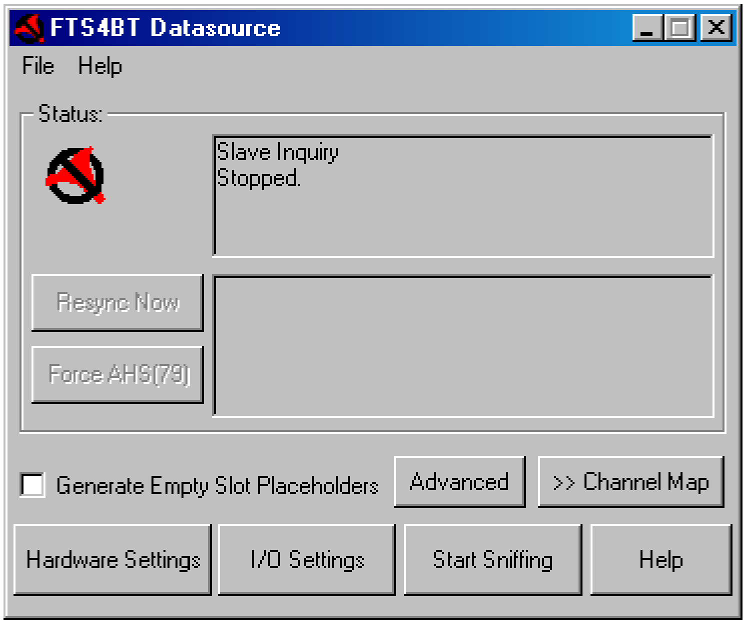
Install your FTS4BT software and Air Sniffer mode hardware (Bluetooth ComProbe) on the computer you intend to use as the analysis computer.

The FTS4BT Quick-Start Guide found in your FTS4BT desktop folder covers FTS4BT installation.

To access the PDF version of the Quick Start Guide from your Windows operating system, click *Start* | *Programs* | *FTS4BT[version #]* | *Bluetooth Quick Start Guide*.

How to setup FTS4BT for Bluetooth data capture:

Open the FTS4BT folder on your desktop and double click the *Air Sniffer (Basic)* shortcut, or from your Windows operating system, click *Start* | *Programs* | *FTS4BT [version #]* | *Air Sniffer (Basic)*. FTS4BT launches and displays the Datasource dialog.



Slave Inquiry
Stopped.

☐ Generate Empty Slot Placeholders

Figure 1 FTS4BT Datasource Dialog

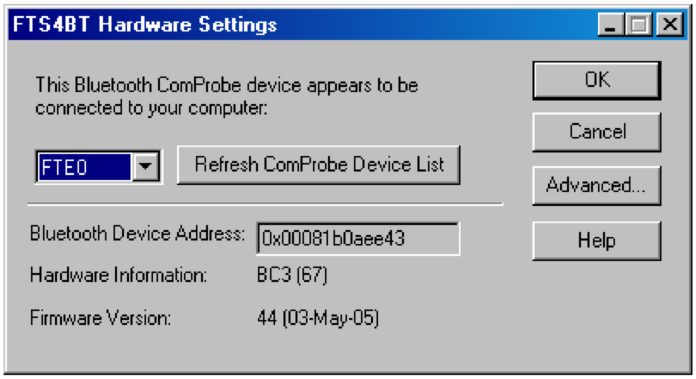
Setting up FTS4BT to sniff the air:

The FTS4BT Datasource is the passive connection between the Bluetooth communications you wish to sniff and the FTS4BT analyzer, and must remain running throughout the capture session.

The FTS4BT Datasource dialog provides you with the means to inform the analyzer about the FTS4BT hardware used as the sniffer, the devices under test, their addresses, which synchronization mode to use, and encryption/decryption parameters.

Hardware Settings

Click the Hardware Settings button on the FTS4BT Datasource dialog to access the Hardware Settings dialog.



FTS4BT Hardware Settings

This Bluetooth ComProbe device appears to be connected to your computer:

FTE0

Bluetooth Device Address: 0x00081b0aee43

Hardware Information: BC3 (67)

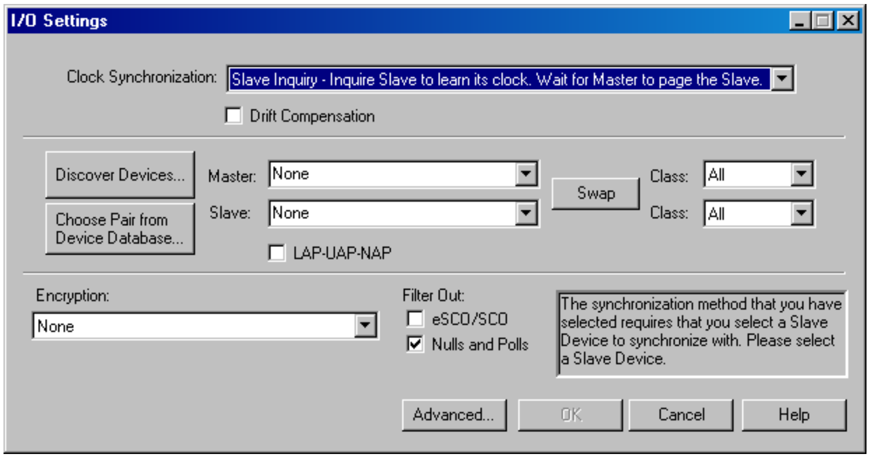
Firmware Version: 44 (03-May-05)

Figure 2 FTS4BT Hardware Settings Dialog

Choose the Bluetooth ComProbe device you wish to use from the drop down list. If the device does not appear in the list, then click Refresh to update (ensure that your Bluetooth ComProbe is installed according to the instructions found in your FTS4BT Quick-Start Guide).

I/O Settings

Click the I/O Settings button on the FTS4BT Datasource dialog to access the I/O Settings dialog.



I/O Settings

Clock Synchronization: Slave Inquiry - Inquire Slave to learn its clock. Wait for Master to page the Slave.

□ Drift Compensation

Master: None Class: All

Slave: None Class: All

□ LAP-UAP-NAP

Encryption: None

Filter Out:
□ eSCO/SCO
☑ Nulls and Polls

The synchronization method that you have selected requires that you select a Slave Device to synchronize with. Please select a Slave Device.

Figure 3 I/O Settings Dialog

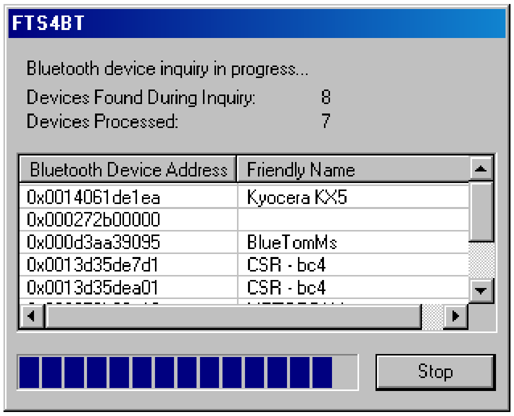
Select Synchronization Mode

Select the synchronization mode that best suits the application from among the following:

- **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 performs an inquiry of the slave and determine its clock. In this mode, the slave must be discoverable.
- **Master Inquiry:** (Inquire the master device to learn its clock). FTS4BT targets the master device, performs a Device Discovery, determines the device 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.
- **Slave Page:** (Page the slave device to learn its clock. Wait for the master to page the slave). Slave Page allows 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 (board address), 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.

Select Bluetooth Devices

Ensure that the Bluetooth device you want to use for synchronization is discoverable (consult the instructions that came with your Bluetooth device for information on making it discoverable). Press the "Discover Devices" button. FTS4BT displays a discovery progress screen and finds any discoverable Bluetooth devices within range of the Bluetooth ComProbe. The discovery screen cycles through once and lists the Bluetooth device addresses of each device it finds, and then cycles through a second time and lists the friendly names (if any).



FTS4BT

Bluetooth device inquiry in progress...

Devices Found During Inquiry: 8

Devices Processed: 7

Bluetooth Device Address	Friendly Name
0x0014061de1ea	Kyocera KX5
0x000272b00000	
0x000d3aa39095	BlueTomMs
0x0013d35de7d1	CSR - bc4
0x0013d35dea01	CSR - bc4

Figure 4 Bluetooth Device Discovery Progress Screen

After completing the device discovery, the Bluetooth discovery progress screen disappears, and the system populates the Master and Slave dropdown lists in the I/O Settings dialog with the results.

Select the desired devices from the Master and Slave drop down lists.

Note that it is necessary to select both a master and slave device only if the link you are sniffing is using encryption, or to ensure that you sniff a particular piconet. Otherwise, you need only select the device required by the synchronization method selected earlier (i.e. if you selected Slave Inquiry as your synchronization mode, then you must select a slave device in the slave dropdown list).

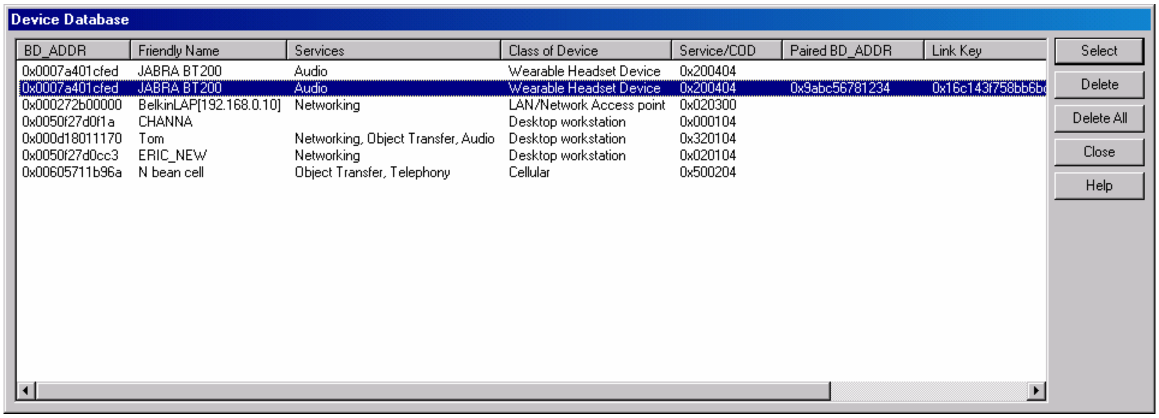
Encryption PIN Code

If you wish to sniff an unencrypted link, then select “None” from the “Encryption” dropdown list.

However, if you wish to sniff an encrypted link, FTS4BT needs the PIN code in order to calculate the link key used by the two Bluetooth devices. Select either “PIN Code (ASCII)” or “PIN Code (Hex)” from the “Encryption” dropdown list and enter the PIN Code in the edit field bellow (the PIN Code should be supplied with you Bluetooth devices).

Device Database

FTS4BT keeps a database of device pairs and their calculated link keys from previous sessions. Access this list by clicking the “Choose Pair from Device Database” button on the I/O Settings dialog.



Device Database

BD_ADDR	Friendly Name	Services	Class of Device	Service/COD	Paired BD_ADDR	Link Key
0x0007a401cfed	JABRA BT200	Audio	Wearable Headset Device	0x200404		
0x0007a401cfed	JABRA BT200	Audio	Wearable Headset Device	0x200404	0x9abc56781234	0x16c143f758bb6b
0x000272b00000	BelkinLAP[192.168.0.10]	Networking	LAN/Network Access point	0x020300		
0x0050f27d0f1a	CHANNA		Desktop workstation	0x000104		
0x000d18011170	Tom	Networking, Object Transfer, Audio	Desktop workstation	0x320104		
0x0050f27d0cc3	ERIC_NEW	Networking	Desktop workstation	0x020104		
0x00605711b96a	N bean cell	Object Transfer, Telephony	Cellular	0x500204		

Figure 5 Bluetooth Device Database Dialog

If you wish to sniff a device pair previously entered into the database, then click on (highlight) the pair in the Device Database list and click the Select button. FTS4BT closes the Device Database dialog, displays the board addresses in the appropriate “Master/Slave” dropdown lists on the I/O Settings dialog, and applies the associated Link Key (if any).

Filter Out

Select the Filter Out (eSCO/SCO, NULL,POLL) set up.

FTS4BT filters out a number of packet types by default. If you wish to include these packet types in the capture, then uncheck the box next to the type of packet. Some of these packet types can be so numerous that they may make it more difficult to locate data packets in the Frame Display and Protocol Navigator windows.

These filters are low level hardware filters. They are also Display Filters that you may use later to filter the captured data. Any packets filtered out during a capture session are ignored and cannot be retrieved later.

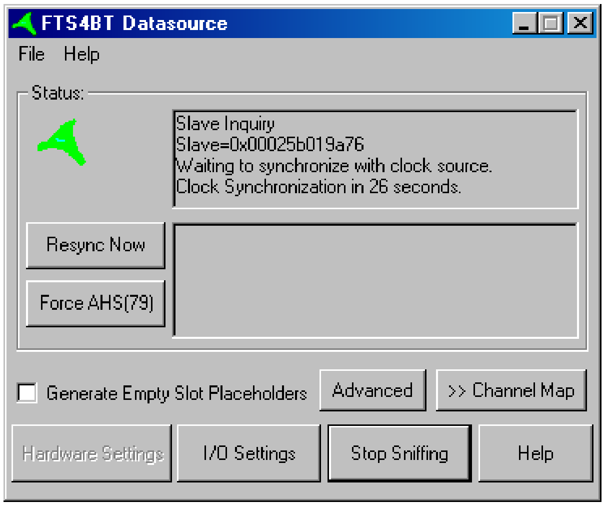
Apply I/O Settings

Once all necessary I/O settings are complete, the OK button is made available. Click OK on the I/O Settings dialog to apply you selections and close the I/O Settings dialog.

If OK is grayed out, there is something incorrect in the I/O Settings dialog. For example, if you select Master Inquiry and do not have a master device selected then OK will be grayed out.

Start Sniffing

Click the Start Sniffing button on the FTS4BT Datasource dialog. When you Start Sniffing the Status Icon will go red (not yet synchronized). After a short time (less than 30 seconds) the icon changes to green.



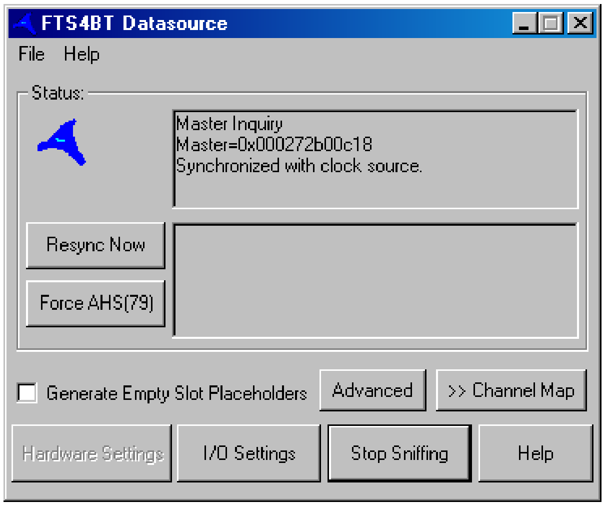
Slave Inquiry
Slave=0x00025b019a76
Waiting to synchronize with clock source.
Clock Synchronization in 26 seconds.

☐ Generate Empty Slot Placeholders

Figure 6 FTS4BT Datasource Synchronization

As indicated in the status box, FTS4BT is synchronized to the slave's clock (in this case as depicted in Figure 6) and waiting for the master to connect with a baseband connection.

Every 30 seconds, the sniffer cycles through the synchronization process again. This eliminates possible clock drift between the ComProbe and the Bluetooth device (slave in this case). With 5 seconds left to re-synchronization, the color changes to yellow. When a baseband connection is made, the icon color changes to blue. When the icon turns blue, the FTS4BT analyzer starts collecting data.



Master Inquiry
Master=0x000272b00c18
Synchronized with clock source.

Figure 7 FTS4BT Datasource Synchronized

DO NOT CLOSE THIS DIALOG. Closing the FTS4BT Datasource dialog stops the sniffing process thereby cutting the communications link between the FTS4BT analyzer and the Bluetooth devices under test. Simply minimize the Datasource dialog to better access the protocol analysis windows.

Refer to the section in the Quick Start Guide titled **Looking At Frames** for information on FTS4BT analysis displays.

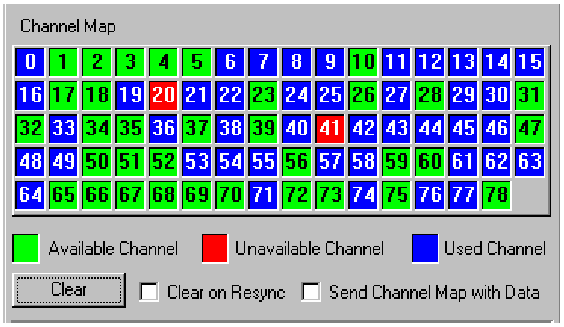
Additional Features and Information

The Channel Map Display

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.



Channel Map

🟦 0	🟩 1	🟩 2	🟩 3	🟩 4	🟩 5	🟦 6	🟦 7	🟦 8	🟦 9	🟩 10	🟦 11	🟦 12	🟦 13	🟦 14	🟦 15
🟦 16	🟩 17	🟩 18	🟦 19	🟥 20	🟦 21	🟦 22	🟩 23	🟦 24	🟦 25	🟩 26	🟦 27	🟩 28	🟦 29	🟦 30	🟩 31
🟩 32	🟦 33	🟩 34	🟩 35	🟦 36	🟩 37	🟦 38	🟩 39	🟦 40	🟥 41	🟦 42	🟦 43	🟦 44	🟦 45	🟦 46	🟩 47
🟦 48	🟦 49	🟩 50	🟩 51	🟩 52	🟦 53	🟦 54	🟦 55	🟩 56	🟦 57	🟦 58	🟩 59	🟩 60	🟦 61	🟦 62	🟦 63
🟦 64	🟩 65	🟩 66	🟩 67	🟩 68	🟩 69	🟩 70	🟦 71	🟩 72	🟩 73	🟦 74	🟩 75	🟦 76	🟦 77	🟩 78	

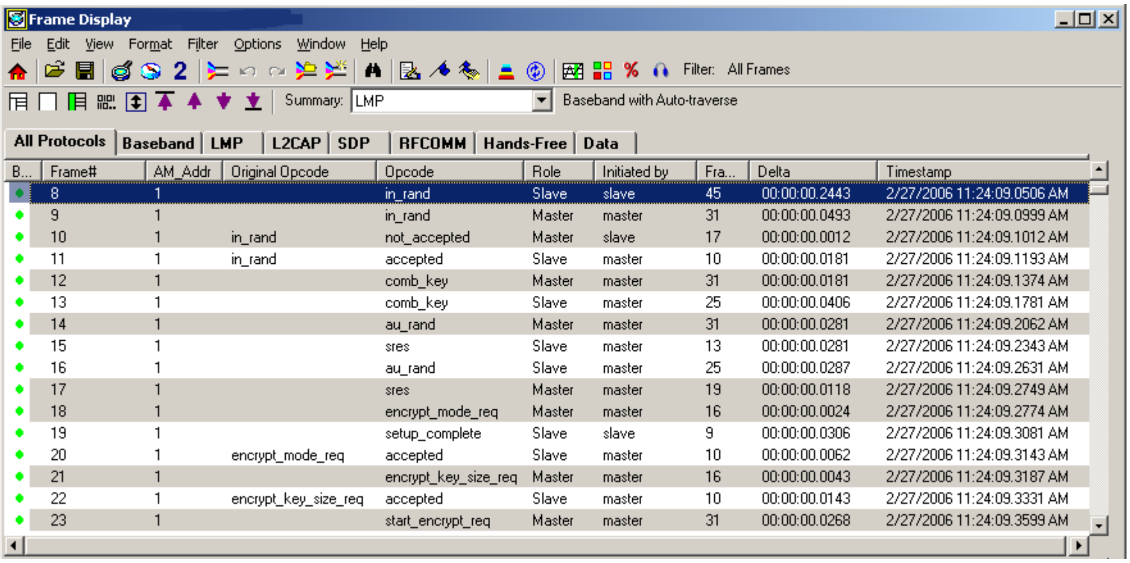
🟩 Available Channel 🟥 Unavailable Channel 🟦 Used Channel

□ Clear on Resync □ Send Channel Map with Data

Figure 8 Channel Map Display

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.



Filter: All Frames

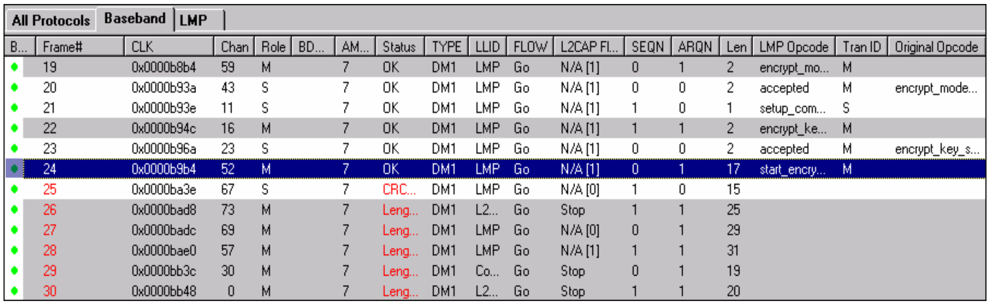
Summary: LMP Baseband with Auto-traverse

B...	Frame#	AM_Addr	Original Opcode	Opcode	Role	Initiated by	Fra...	Delta	Timestamp
●	8	1		in_rand	Slave	slave	45	00:00:00.2443	2/27/2006 11:24:09.0506 AM
●	9	1		in_rand	Master	master	31	00:00:00.0493	2/27/2006 11:24:09.0999 AM
●	10	1	in_rand	not_accepted	Master	slave	17	00:00:00.0012	2/27/2006 11:24:09.1012 AM
●	11	1	in_rand	accepted	Slave	master	10	00:00:00.0181	2/27/2006 11:24:09.1193 AM
●	12	1		comb_key	Master	master	31	00:00:00.0181	2/27/2006 11:24:09.1374 AM
●	13	1		comb_key	Slave	master	25	00:00:00.0406	2/27/2006 11:24:09.1781 AM
●	14	1		au_rand	Master	master	31	00:00:00.0281	2/27/2006 11:24:09.2062 AM
●	15	1		sres	Slave	master	13	00:00:00.0281	2/27/2006 11:24:09.2343 AM
●	16	1		au_rand	Slave	master	25	00:00:00.0287	2/27/2006 11:24:09.2631 AM
●	17	1		sres	Master	master	19	00:00:00.0118	2/27/2006 11:24:09.2749 AM
●	18	1		encrypt_mode_req	Master	master	16	00:00:00.0024	2/27/2006 11:24:09.2774 AM
●	19	1		setup_complete	Slave	slave	9	00:00:00.0306	2/27/2006 11:24:09.3081 AM
●	20	1	encrypt_mode_req	accepted	Slave	master	10	00:00:00.0062	2/27/2006 11:24:09.3143 AM
●	21	1		encrypt_key_size_req	Master	master	16	00:00:00.0043	2/27/2006 11:24:09.3187 AM
●	22	1	encrypt_key_size_req	accepted	Slave	master	10	00:00:00.0143	2/27/2006 11:24:09.3331 AM
●	23	1		start_encrypt_req	Master	master	31	00:00:00.0268	2/27/2006 11:24:09.3599 AM

This is a full pairing procedure between two devices. FTS4BT must capture this pairing procedure (Between Frame 8 and Frame 23) 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 does not have all the information it needs, it will not 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.



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	DM1	LMP	Go	N/A [1]	0	1	2	encrypt_mo...	M	
●	20	0x0000b93a	43	S		7	OK	DM1	LMP	Go	N/A [1]	0	0	2	accepted	M	encrypt_mode...
●	21	0x0000b93e	11	S		7	OK	DM1	LMP	Go	N/A [1]	1	0	1	setup_com...	S	
●	22	0x0000b94c	16	M		7	OK	DM1	LMP	Go	N/A [1]	1	1	2	encrypt_ke...	M	
●	23	0x0000b96a	23	S		7	OK	DM1	LMP	Go	N/A [1]	0	0	2	accepted	M	encrypt_key_s...
●	24	0x0000b9b4	52	M		7	OK	DM1	LMP	Go	N/A [1]	0	1	17	start_encry...	M	
●	25	0x0000ba3e	67	S		7	CRC...	DM1	LMP	Go	N/A [0]	1	0	15			
●	26	0x0000bad8	73	M		7	Leng...	DM1	L2...	Go	Stop	1	1	25			
●	27	0x0000badc	69	M		7	Leng...	DM1	LMP	Go	N/A [0]	0	1	29			
●	28	0x0000bae0	57	M		7	Leng...	DM1	LMP	Go	N/A [1]	1	1	31			
●	29	0x0000bb3c	30	M		7	Leng...	DM1	Co...	Go	Stop	0	1	19			
●	30	0x0000bb48	0	M		7	Leng...	DM1	L2...	Go	Stop	1	1	20			

End