



Bluetooth Sniffer v. 2.0 + EDR

PC based Bluetooth Protocol Analyzer FTS4BT

- ◆ FTS for Bluetooth decodes all Bluetooth protocols and supports most Bluetooth profiles.
- ◆ Captures, decodes, displays, and filters in real time.
- ◆ Data is decoded at the frame, byte, and bit levels, which permits users to rapidly detect and isolate even the most minute and intermittent protocol-related problems.
- ◆ Continuous direct logging to disk with unlimited file size for data and speech (WAV file)
- ◆ Sniffs in the air and serial HCI simultaneously, with synchronized time stamping.
- ◆ Decodes and displays multiple protocol layers of multiple data frames simultaneously.
- ◆ Detects and displays protocol errors (in red) in real time.
- ◆ Supports data decryption, Pairing, Master/Slave Switching, and Park, Hold, and Sniff switches.
- ◆ Channel chart with BER measurement in the header and the pay load



FTS4BT (Frontline Test System for Bluetooth)

The USB dongle was developed in conjunction with CSR (Cambridge Silicon Radio) and was the first protocol analyzer for Bluetooth® version 2.0, complementing the R&S Products like R&S PTW60/70 and R&S CMU200.

In addition to the measurements of the physical RF parameters by R&S CMU200 and the programming capability of protocols by the R&S PTW60/70, Frontline is analysing the application protocols and interoperability of Bluetooth® devices.

The Frontline Bluetooth® protocol analyzer, even though it is also decoding the Baseband, is orientated to the software development of the higher layers. Baseband is of minor importance there, all efforts go to the software application around this chip and that's the field of main application and strength of Frontline's Bluetooth® protocol analyzer.

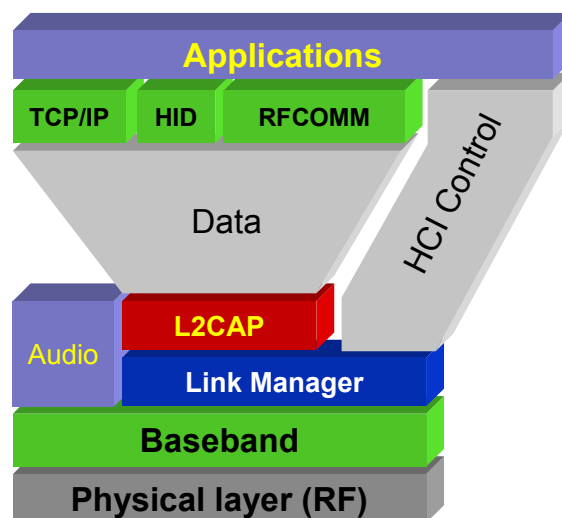
For application debugging, FTS4BT is used as a tool to figure out what is going on with the messaging in real time.

FTS4BT is being used also for verification. In difference to the R&S „Qualification and Compliance“ test, „verification“ is more a functional test of a Bluetooth® device.

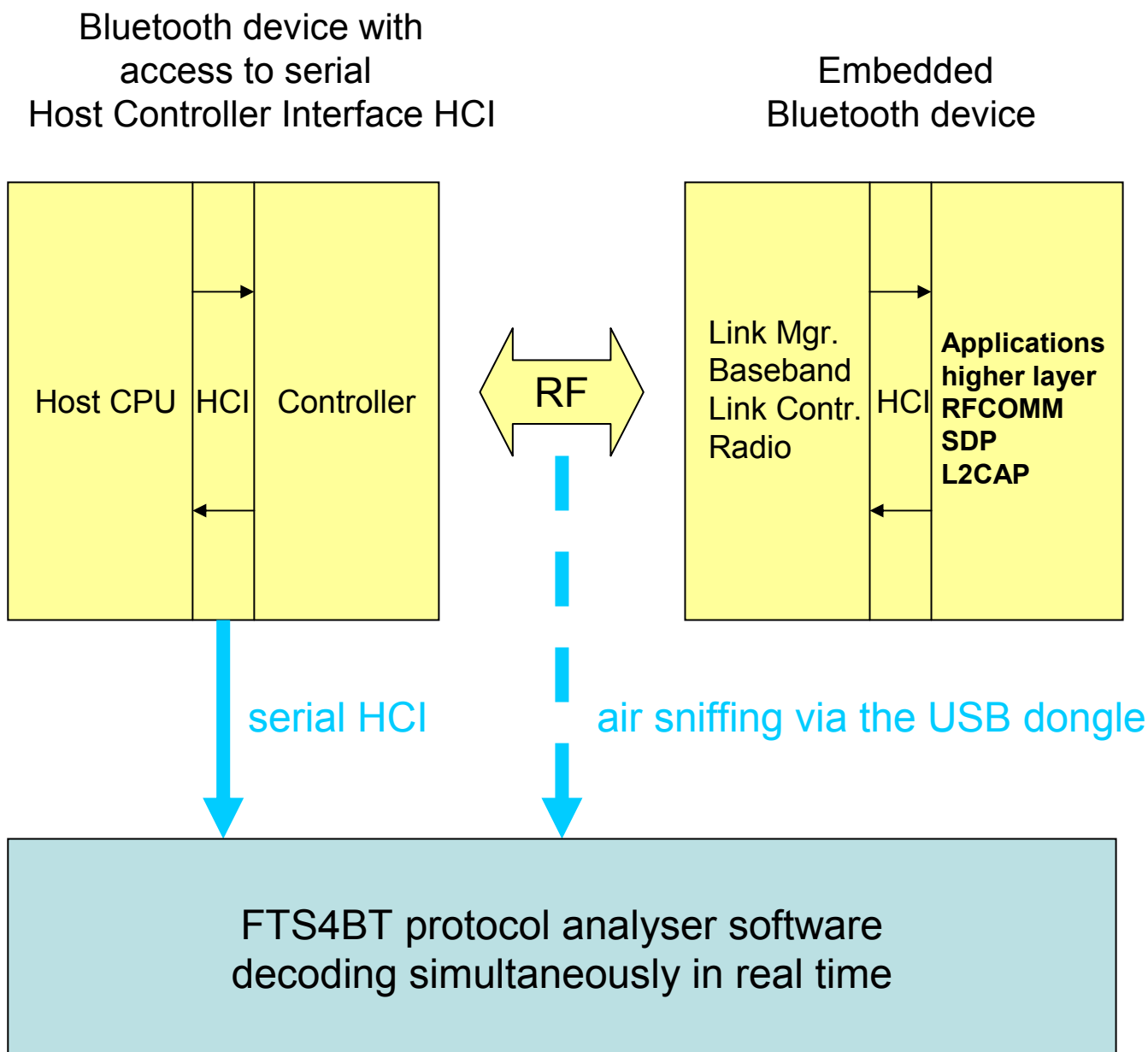
Bluetooth® SIG (Special Interest Group) designates specialized organisations as a BQB (Bluetooth® Qualification Body). In order to qualify a Bluetooth® product (this could be a chip, mobile phone, PDA etc.) the BQB will verify the received documentation (they call this evidence) that shows that the product functions and conforms to the Bluetooth® spec.

FTS4BT is used to produce this documentation by capturing the traffic and then prepare the evidence for the BQB.

FTS4BT's architecture enables quick release of new decoders as protocols are announced by the Bluetooth SIG. The user can rapidly develop and seamlessly integrate Vendor Extension decoders using the built-in FrameDecoder™ feature.



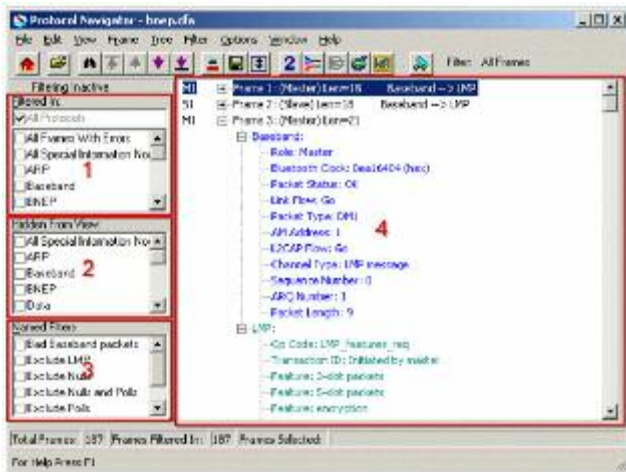
A standard Bluetooth® device consists of a Bluetooth® controller and a CPU with the Bluetooth® application software. These two elements are connected by the HCI (host controller interface). The controller with the LMP (layer3 link manager protocol) incorporates the Baseband and Physical layer (Bluetooth®-radio). Many Bluetooth® devices give physical access to the HCI (three wires) e. g. via a serial interface.



FTS4BT can be connected to the **HCI** of the device via a RS232 port, via USB or virtually to analyze commands and events between these Bluetooth® elements. At this point it can be checked if the application profiles and the serial emulation to the L2CAP (logical link control and adaptation protocol) inside of one Bluetooth® device is correct.

In an active Piconet, where at least two Bluetooth® devices (one master, one or more slaves) interact with each other, the USB dongle is **air sniffing** the communication between those. This analysis is required to check interoperability of Bluetooth® devices from different vendors and to troubleshoot problems by detailed protocol decoding.

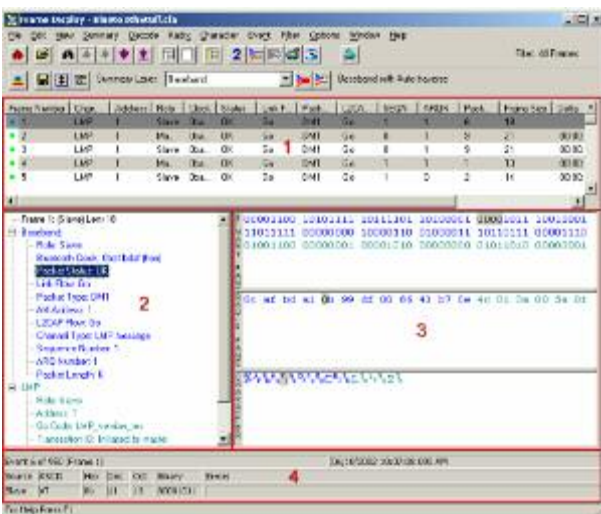
Multiple Protocol Layers within multiple data frames



Protocol Navigator Window: presents decodes of multiple protocol layers within multiple data frames. Simplifies the process of understanding the complex relationships between multiple data frames and the protocol layers that comprise the frames.

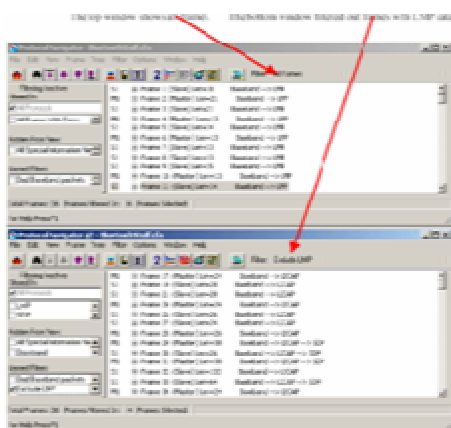
1. Protocol Selection Pane: enables you to view only data frames that contain selected Bluetooth protocols.
2. Protocol Suppression Pane: enables you to suppress selected protocols within the Bluetooth data frames.
3. Frame Filter Pane: enables you to select pre-defined filter conditions that include or exclude specific data frame types.
4. Protocol Decode Pane: displays one or more decoded data frames, with text-based explanations of the various protocol elements.

User Data, from the frame level to the bit level



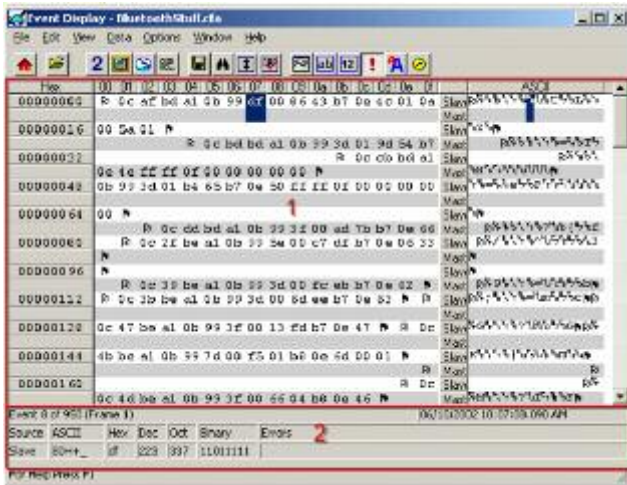
Frame Display Window: presents various views of user data, from the frame level to the bit level, including a detailed decode of a user-selected data frame using a layer-by-layer tree structure. The protocol decode presents text-based descriptions of the protocol-related information resident in each data frame.

1. Summary Pane: displays a high level overview of each Bluetooth data frame, including all significant fields associated with the selected protocol layer.
2. Frame Display Decode Pane: displays a single decoded data frame at levels of detail ranging from the frame level to the bit level.
3. Data Panes: display Bluetooth data in various formats, including binary, hexadecimal, and characters.
4. Selected Data Detail Section: provides protocol-related information pertaining to user-selected portions of the data frame.



Window Duplication: the Duplicate Button creates a second window that is identical to the first. Duplication enables you to view two segments of the data stream simultaneously, or to compare identical data streams with different filter conditions applied.

Data at the byte level

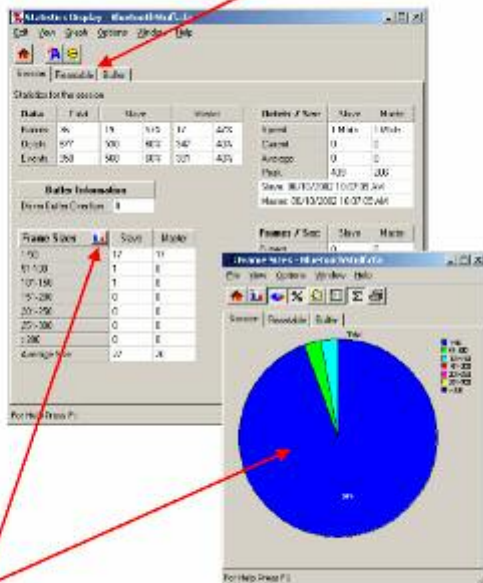


Event Display Window: used to monitor and analyze data at the byte level, and to conduct searches for data patterns.

1. Byte Display Panes: display data flows among Bluetooth devices, in various formats, at the byte level.
2. Selected Data Detail Section: provides protocol-related information pertaining to user-selected, multi-frame portions of the data stream.

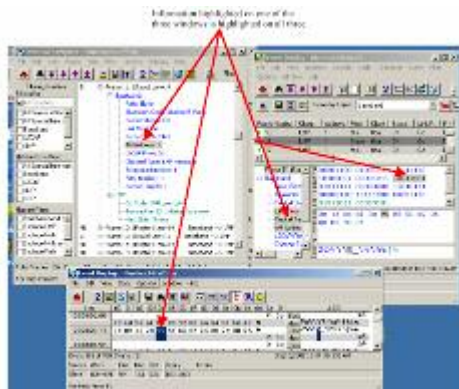
Statistical data flow parameters

Analyze traffic statistics in three different modes: for the entire session, from a user-specified point in the session, and for data in a capture buffer.



Statistics Window: provides statistical information on Bluetooth data flow parameters such as number of characters, frames and errors.

Click on the graphics icon to obtain a graphical view of the data.



Window Synchronization: the Protocol Navigator, Frame display, and Event Display Windows are synchronized. Selecting information in any of these windows highlights the same information in the other two windows

Technical Description

Data Capture Features

Data Capture Modes

Sniffs data in three modes simultaneously, with synchronized timestamping:

- ♦ Through the air via an attached device called the Bluetooth ComProbe, which connects to the USB port on the host PC.
- ♦ From the serial HCI interface between a Bluetooth Host CPU and a Bluetooth Host Controller (Bluetooth Device).
- ♦ By "virtual sniffing" via the product's Live Import feature, which permits any application to feed data into FTS for Bluetooth via Microsoft's COM interface for interprocess communication.

Piconet Synchronization Methods

- ♦ Master Inquiry.
- ♦ Slave Inquiry.
- ♦ Passive Slave Page.

Data Capture

- ♦ Captures, decodes, displays, and filters in realtime.
- ♦ Supports full piconet data capture.
- ♦ Captures, decrypts, and analyzes encrypted data.
- ♦ Supports Pairing, Master/Slave Switching, Park, Hold, and Sniff switches, and Null and Poll capture.
- ♦ Captured data includes data bytes and error conditions.
- ♦ Data can be captured to RAM or directly to disk.
- ♦ Capture buffer sizes are limited only by available memory or disk space.

Data Analysis Features

Data Displays

- ♦ Data can be analyzed in realtime using the Event Display, Frame Display, Signal Display, Protocol Navigator, and Statistics Windows.
- ♦ Decodes and displays multiple protocol layers of multiple data frames simultaneously.
- ♦ Data can be analyzed simultaneously in each of the product's three operating modes: air, serial HCI, and Live Import.
- ♦ Multiple synchronized windows can be viewed simultaneously.
- ♦ Byte level information is displayed in either a split-line format, or in a mixed format.
- ♦ Characters can be displayed in ASCII, EBCDIC, or Baudot.
- ♦ Nonprintable characters are displayed using hex and mnemonics.

Error Detection

- ♦ Detects and displays protocol errors (in red) in realtime.

Search

Search criteria include:

- ♦ Byte Level: timestamp, errors, and patterns (patterns include wildcard characters at the bit level, nibble level, and byte level);
- ♦ Frame Level: frame decodes can be searched on the text of the decode, with or without wildcards.

Display Filters

- ♦ Display Filter parameters include protocol, data pattern, and an advanced mode for complex filters.

Statistics Display

- ♦ Provides session totals for characters, frames, events, errors, characters per second, and percentage utilization.

Data Transmission (serial HCI only)

- ♦ Data strings and files can be transmitted one time, multiple times, or continuously.
- ♦ Data transmission delays can be inserted in millisecond, second, or minute increments.

Timestamping

- ♦ Sniffs data in three modes simultaneously, with synchronized timestamping.
- ♦ Provides both absolute and relative displays of event timing.
- ♦ Calculates time intervals between events (delta time) and data rate.
- ♦ Microsecond resolution.

Configuration Management

- ♦ I/O configurations, protocol stacks, and filters can be saved for future use.
- ♦ Supports user-definable protocol stacks.

Help

- ♦ Comprehensive online help provides complete operating instructions.
- ♦ Quick Start Guide enables rapid product set-up and operation.

FrameDecoder

- ♦ Quickly create custom decoders for proprietary protocols and Vendor Extensions.

Air Sniffing

- ♦ Air interface is a small lightweight USB dongle.
- ♦ Any Windows PC with a USB port and 64 MB RAM. (Air sniffing is not supported under Windows 95 and NT. Captured data may be viewed under 95 and NT.)

Virtual Sniffing

- ♦ Any Windows PC with 64 MB RAM.

Serial HCI Sniffing

- ♦ Supports HCI UART (H4) and BCSP.
- ♦ Up to 115.2 Kbps using any Windows PC with two serial ports and 64 MB RAM.
- ♦ FTS monitoring cables included.
- ♦ Up to 921 Kbps with optional high-speed serial card(s).
- ♦ Supports board-level (TTL) voltages with optional TTL to RS-232 converters.

Protocols Supported: Bluetooth® stack

Baseband, LMP, L2CAP, HCI, UART (H4), HCI, OBEX, TCS Binary, CMTP, HDLC, SDP, RFCOMM, TCS, AVDTP, BNEP, HCRP, HID, AVCTP, AVDTP, OBEX

TCP/IP stack

IPv4, HTTP, NBNS, UDP, IPv6 DHCPDNS, NBSS, TCP, ICMP, SMB, ARP, NBDS, SMTP

Common LAN Protocols

802.2, SNAP, IPX, NCP, IBM_NETBIOS, AT commands

Common WAN Protocols

AsyncPPP, PPP

Profiles Supported:

Generic Access Profile, Cordless Telephony Profile, Serial Port Profile, Headset Profile, Hardcopy cable Replacement Profile, Generic Audio Video Distribution Profile, Audio/Video Remote control Profile, Video Conferencing Profile, Dial-up Networking Profile, LAN Access Profile, Phone Access Profile, Service Discovery Application Profile, Intercom Profile, Generic Object Exchange Profile, Hands-Free Profile, Human Interface Device Profile, Advanced Audio Distribution Profile, Video Distribution Profile, SIM Access Profile, SIM Access Profile, Fax Profile, Personal Area Networking Profile, Basic Imaging Profile, Basic Printing Profile, Common ISDN Access Profile etc.

Bit Order: LSB (normal) or MSB (reversed) first
Character Sets: ASCII, 7-bit ASCII, EBCDIC, Baudot
Parity: None, Even, Odd, Mark, Space
Word Length: 5, 6, 7 or 8 bits
Stop Bits: 1, 1.5 or 2 bits
Timestamping: Absolute and relative timestamping: microsecond resolution.
Timestamps are synchronized over all three operation modes.

Order number:

FTS for Bluetooth with two years warranty and software care:	FTS4BT
One year additional software care:	FTSBLUE-PS1
Three years of additional software care:	FTSBLUE-PS3
Additional USB-dongle:	COM-Probe

