Explorer™

Bluetooth® Instant Protocol Analysis

All-Channel, Full-Spectrum, Concurrent Synchronous Capture of *Bluetooth* 2.1 BR/EDR, Low Energy and HCI traffic

ellisys

Better Analysis.

Unique Ellisys Features:

- Robust capture
- Non-intrusive sniffing
- Zero configuration
- Capture an unlimited number of neighboring piconets
- Concurrent capture of BR/EDR and Low Energy traffic
- Concurrent capture of BR/EDR and HCI traffic

Ellisys *Bluetooth*® Explorer 400

Ellisys *Bluetooth*® Explorer 400

Bluetooth® Instant Protocol Analysis System

ellisys

Better Analysis.

All-Channel, Full-Spectrum, Concurrent Synchronous Capture of *Bluetooth* 2.1 BR/EDR, Low Energy and HCI traffic

Bluetooth Days are too short to waste time

Traffic analysis is one of the key day-to-day activities of *Bluetooth* engineers looking to rapidly test and debug their implementations. Unfortunately, *Bluetooth* over-the-air sniffing has always been some difficult task topic. Legacy sniffing methods suffered from major drawbacks, making them unreliable and unusable in some circumstances, therefore making *Bluetooth* engineers' lives difficult.

With its Ellisys *Bluetooth*® Explorer™, Ellisys lifts protocol capture and analysis to new heights, radically overcoming drawbacks of those legacy approaches to *Bluetooth* sniffing. The new Ellisys All-Channel sniffer robustly records any packet, at any time, from any neighboring piconet, with zero-configuration and without being intrusive. With the right tool, your *Bluetooth* Days will not seem too short anymore!

Why were *Bluetooth* systems previously so difficult to sniff?

Bluetooth wireless technology was originally designed to be robustly impervious to interference on the much-used ISM 2.4 GHz band, and was also designed to be non-easily sniffable for security reasons. The two main RF characteristics unique to the *Bluetooth* specification are:

- **Frequency Hopping:** packets are transmitted on one chosen channel amongst 79, every 625us, following a pseudo-random sequence.
- **Data Whitening:** packets are scrambled in order to produce an equal distribution of 1s and 0s, avoiding reception of plain packets from neighboring piconets or sniffers.

A standard *Bluetooth* radio can receive or transmit on only one of the 79 channels at a given time. Legacy *Bluetooth* sniffers used a standard single-channel radio. Because of this inherent limitation, those sniffers had to connect to a piconet's master device using a mandatorily configured 48-bit address, retrieve the master's clock, and eventually follow the hopping sequence based on this information. Main drawbacks of this approach were:

- **Complex configuration was required** – needs expert users and some prior information
- **Was intrusive** – the analyzer must interact with the master
- **Was non-reliable** – loss of sync because of clock drift when master is not active
- **Was limited to a single piconet** – interference issues are out of scope
- **Was not able of recording some connection steps** such as paging and inquiry packets

Ellisys has created a revolutionary sniffer that overcomes all those drawbacks and adds innovative features, opening new horizons to *Bluetooth* debugging and interoperability testing.

Revolutionary Ellisys Rainbow™ All-Channel Capture Technology

This multi-protocol, multi-band and multifaceted protocol analysis system is powered by the revolutionary Ellisys Rainbow™ all-channel capture engine. With this breakthrough technology, Ellisys hardware is capable of capturing concurrently all 79 BR/EDR channels as well as all 40 Low-Energy channels, plus related HCI traffic for cross-analysis.

Former single-channel capture

	slot 0	slot 1	slot 2	slot 3	slot 4	time →
ch 0	♫ ✓	✖	✖	⇄ ✖	♫ ✓	✖
ch 1	✖	⇄ ✖	♫ ✓	✖	✖	⇄ ✖
...						
ch 77	✖	✖	⇄ ✖	✖	✖	♫ ✓
ch 78	⇄ ✖	♫ ✓	✖	♫ ✓	⇄ ✖	✖

Ellisys Rainbow™ All-Channel capture

	slot 0	slot 1	slot 2	slot 3	slot 4	time →
ch 0	♫ ✓	✓	✓	⇄ ✓	♫ ✓	✓
ch 1	✓	⇄ ✓	♫ ✓	✓	✓	⇄ ✓
...						
ch 77	✓	✓	⇄ ✓	✓	✓	♫ ✓
ch 78	⇄ ✓	♫ ✓	✓	♫ ✓	⇄ ✓	✓

The above illustrations show how legacy sniffers received packets by listening to a single channel at a time, compared to the Ellisys Rainbow All-Channel capture catching all Bluetooth *packets by listening to a 80 MHz wideband frequency range concurrently*

With this method the Ellisys *Bluetooth*® Explorer does not need to follow the hopping sequence of a given piconet; it can receive any packet from any neighboring device! Smart post-capture analysis groups packets into physical channels and determines devices' states, displaying useful high-level information on master and slaves. **Stop Hopping – It Just Works!**

What about security?

Ellisys developed smart security algorithms to further ease engineers' lives. The Ellisys software application will automatically determine PIN codes and Link Keys when pairing are detected. Resulting link keys can be stored, such that any further traffic capture from the same devices will be decrypted automatically.

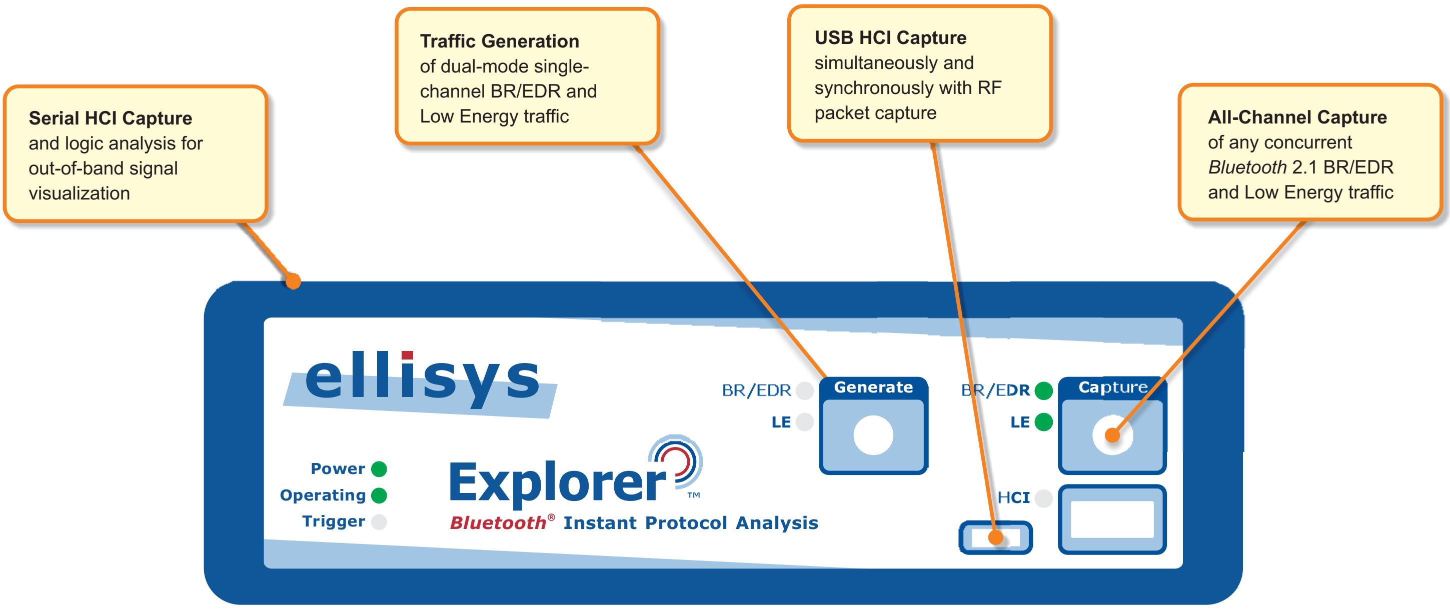
SSP (Simple Secure Pairing) is also supported. SSP uses encryption methods similar to the methods used on the Internet, to secure sensitive information exchanges, such as banking transactions. No algorithm can help automatically determine the keys for decrypting packets. The link key must thus be specified to the analysis software for decryption. Ellisys eases this process by automating link key extraction from HCI traces.

Unique Ellisys Features

- **Robust capture** without unexpected loss of synchronization, ever
- **Non-intrusive sniffing** – the analyzer does not interact with or disturb piconets under test
- **Zero configuration** – simply click the record button and start sniffing
- **Capture any packet at any time**, including all packets from paging, inquiry, and role switch
- **Capture an unlimited number of neighboring piconets** with a single unit
- **Concurrent and synchronous capture of BR/EDR and Low Energy traffic** with a single unit
- **Concurrent and synchronous capture of BR/EDR and HCI traffic** with a single unit

Product Highlights

- Visualize evolution of piconets and scatternets live in **Ellisys Instant Piconet** view
- Visualize all packets with 1/8th symbol accuracy in **Ellisys Instant Timing** view
- **Decode all protocols** and profiles automatically
- Export *Bluetooth* data to various formats, including **audio waveforms**
- See **relationships between protocol levels** and sequences of different protocols clearly in a single view, or in multiple synchronized views
- **Determine PIN codes automatically** and decrypt data on the fly
- **Free lifetime software updates –** no maintenance fees
- **Free full-featured viewer software** to easily share annotated traces with colleagues and replay captured traffic
- Use Ellisys hardware on **any computer** without the need of additional licenses



Serial HCI Capture
and logic analysis for out-of-band signal visualization

Traffic Generation
of dual-mode single-channel BR/EDR and Low Energy traffic

USB HCI Capture
simultaneously and synchronously with RF packet capture

All-Channel Capture
of any concurrent *Bluetooth* 2.1 BR/EDR and Low Energy traffic

Ellisys *Bluetooth*® Explorer 400

Ellisys *Bluetooth*® Explorer 400
Bluetooth® Instant Protocol Analysis System

ellisys
Better Analysis.

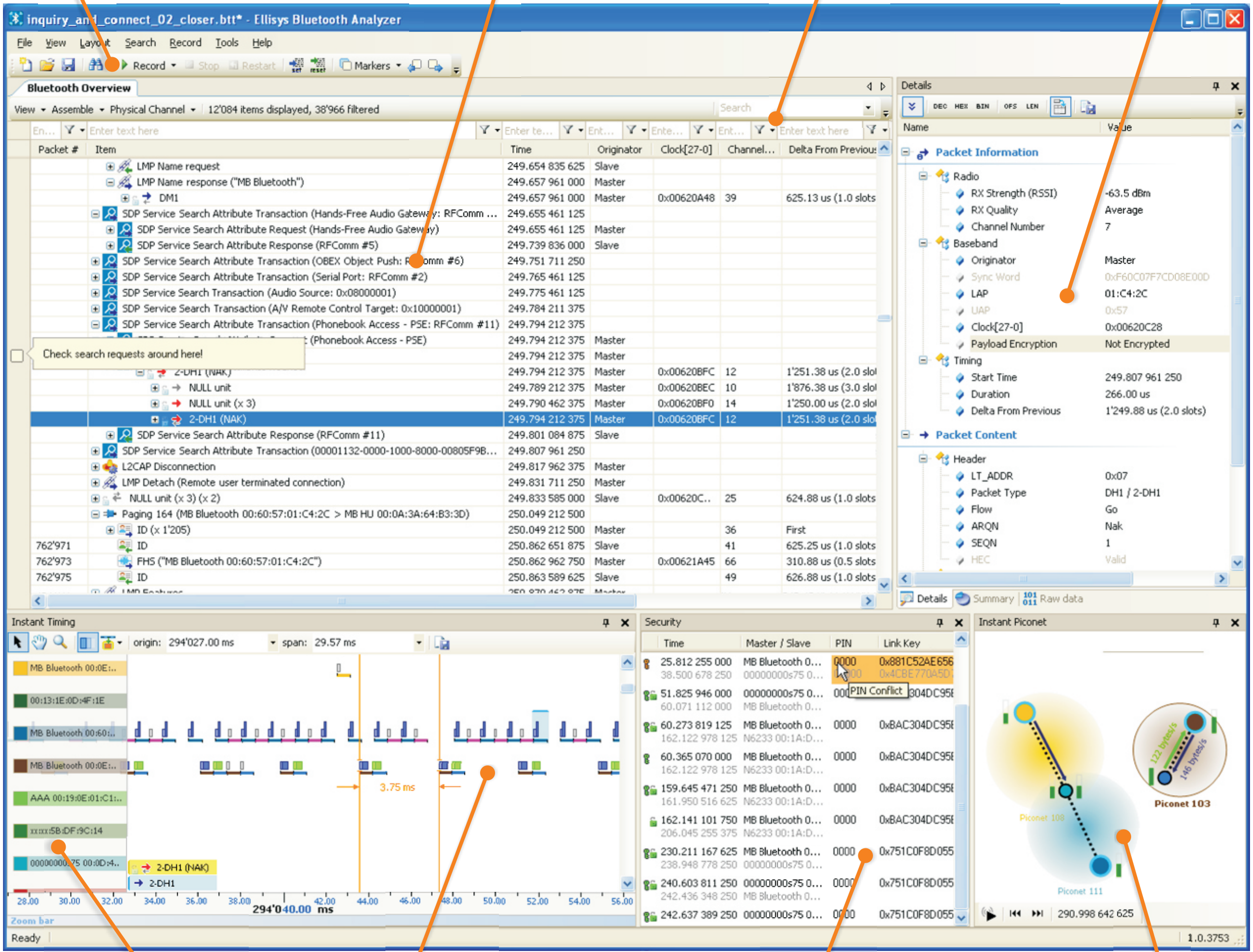
Unique Ellisys Software Features

One-Click Record
Capture starts instantly without any configuration required.
Devices under test are automatically detected.

Protocol Overview
Low-level and stack protocol elements are hierarchically displayed in easily configurable views.

Search and Filtering
Simple or advanced searches and filters enable finding, focusing on, and bookmarking relevant data quickly.

In-Depth Data Mining
Detailed meta-data and protocol fields are clearly displayed, including never-seen-before baseband information.


inquiry_and_connect_02_closer.btt* - Ellisys Bluetooth Analyzer
File View Layout Search Record Tools Help
Record Stop Restart Markers
Bluetooth Overview
View Assemble Physical Channel
Search
Enter text here
Details
DEC HEX BIN OFS LEN
Details Summary Raw data
Instant Timing
Security
Instant Piconet
Ready
1.0.3753

12'084 items displayed, 38'966 filtered

Packet #	Item	Time	Originator	Clock[27-0]	Channel...	Delta From Previous
	LMP Name request	249.654 835 625	Slave			
	LMP Name response ("MB Bluetooth")	249.657 961 000	Master			
	DM1	249.657 961 000	Master	0x00620A48	39	625.13 us (1.0 slots
	SDP Service Search Attribute Transaction (Hands-Free Audio Gateway: RFComm ...	249.655 461 125				
	SDP Service Search Attribute Request (Hands-Free Audio Gateway)	249.655 461 125	Master			
	SDP Service Search Attribute Response (RFComm #5)	249.739 836 000	Slave			
	SDP Service Search Attribute Transaction (OBEX Object Push: RFComm #6)	249.751 711 250				
	SDP Service Search Attribute Transaction (Serial Port: RFComm #2)	249.765 461 125				
	SDP Service Search Transaction (Audio Source: 0x08000001)	249.775 461 125				
	SDP Service Search Transaction (A/V Remote Control Target: 0x10000001)	249.784 211 375				
	SDP Service Search Attribute Transaction (Phonebook Access - PSE: RFComm #11)	249.794 212 375				
	(Phonebook Access - PSE)	249.794 212 375	Master			
		249.794 212 375	Master			
	2-DH1 (NAK)	249.794 212 375	Master	0x00620BFC	12	1'251.38 us (2.0 slot
	NULL unit	249.789 212 375	Master	0x00620BEC	10	1'876.38 us (3.0 slot
	NULL unit (x 3)	249.790 462 375	Master	0x00620BF0	14	1'250.00 us (2.0 slot
	2-DH1 (NAK)	249.794 212 375	Master	0x00620BFC	12	1'251.38 us (2.0 slot
	SDP Service Search Attribute Response (RFComm #11)	249.801 084 875	Slave			
	SDP Service Search Attribute Transaction (00001132-0000-1000-8000-00805F9B...	249.807 961 250				
	L2CAP Disconnection	249.817 962 375	Master			
	LMP Detach (Remote user terminated connection)	249.831 711 250	Master			
	NULL unit (x 3) (x 2)	249.833 585 000	Slave	0x00620C..	25	624.88 us (1.0 slots
	Paging 164 (MB Bluetooth 00:60:57:01:C4:2C > MB HU 00:0A:3A:64:B3:3D)	250.049 212 500				
	ID (x 1'205)	250.049 212 500	Master		36	First
762'971	ID	250.862 651 875	Slave		41	625.25 us (1.0 slots
762'973	FHS ("MB Bluetooth 00:60:57:01:C4:2C")	250.862 962 750	Master	0x00621A45	66	310.88 us (0.5 slots
762'975	ID	250.863 589 625	Slave		49	626.88 us (1.0 slots

Check search requests around here!

Name	Value
Packet Information	
Radio	
RX Strength (RSSI)	-63.5 dBm
RX Quality	Average
Channel Number	7
Baseband	
Originator	Master
Sync Word	0xF60C07F7CD08E00D
LAP	01:C4:2C
UAP	0x57
Clock[27-0]	0x00620C28
Payload Encryption	Not Encrypted
Timing	
Start Time	249.807 961 250
Duration	266.00 us
Delta From Previous	1'249.88 us (2.0 slots)
Packet Content	
Header	
LT_ADDR	0x07
Packet Type	DH1 / 2-DH1
Flow	Go
ARQN	Nak
SEQN	1
HEC	Valid

origin: 294'027.00 ms span: 29.57 ms

Time	Master / Slave	PIN	Link Key
25.812 255 000 38.500 678 250	MB Bluetooth 0... 00000000s75 0...	0000 0000	0x881C52AE656 0x4CBE770A5D
51.825 946 000 60.071 112 000	00000000s75 0... MB Bluetooth 0...	000	304DC95E
60.273 819 125 162.122 978 125	MB Bluetooth 0... N6233 00:1A:D...	0000	0xBAC304DC95E
60.365 070 000 162.122 978 125	MB Bluetooth 0... N6233 00:1A:D...	0000	0xBAC304DC95E
159.645 471 250 161.950 516 625	MB Bluetooth 0... N6233 00:1A:D...	0000	0xBAC304DC95E
162.141 101 750 206.045 255 375	MB Bluetooth 0... N6233 00:1A:D...	0000	0xBAC304DC95E
230.211 167 625 238.948 778 250	MB Bluetooth 0... 00000000s75 0...	0000	0x751C0F8D055
240.603 811 250 242.436 348 250	00000000s75 0... MB Bluetooth 0...	0000	0x751C0F8D055
242.637 389 250	00000000s75 0...	0000	0x751C0F8D055

PIN Conflict

Innovative data groups
Relationships between packets are made clear, by assembling data per piconet's master device, slave, channel and more

Instant Timing
Time ordered, color-coded display of packets, with precise timing measurements, visualization of conflicts, etc.

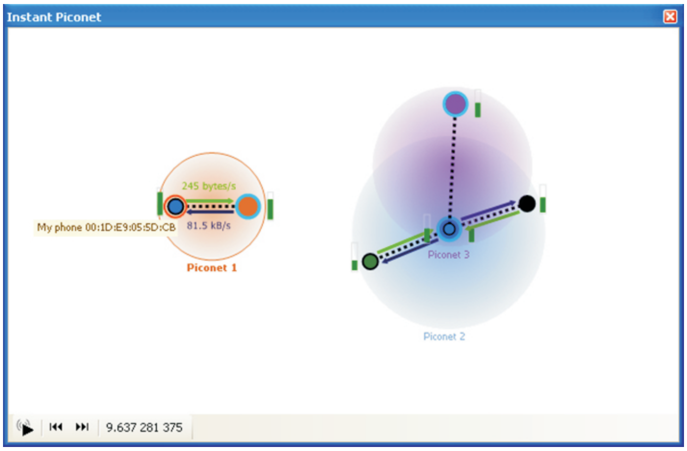
Automatic Decryption
PIN codes are extracted on-the-fly from captured data. Link keys are calculated for seamless encryption handling.

Instant Piconet
Actual piconet and scatternet topology is shown with throughput and other various hints. Works in Live or Replay mode.

Several other features are included with the acclaimed Ellisys protocol analysis software application, such as:

- **Import and Export** – interact with other systems and post-process data easily
- **Cross-platform remote control** – incorporate Ellisys analysis tools in automated test benches or run unattended sessions
- **Multiple screen support and advanced GUI features** – empower your workspace to suit your preferences
- **Free full-featured viewer with unlimited user/computer license** - including Premium Support from Ellisys engineers

Ellisys Instant Piconet

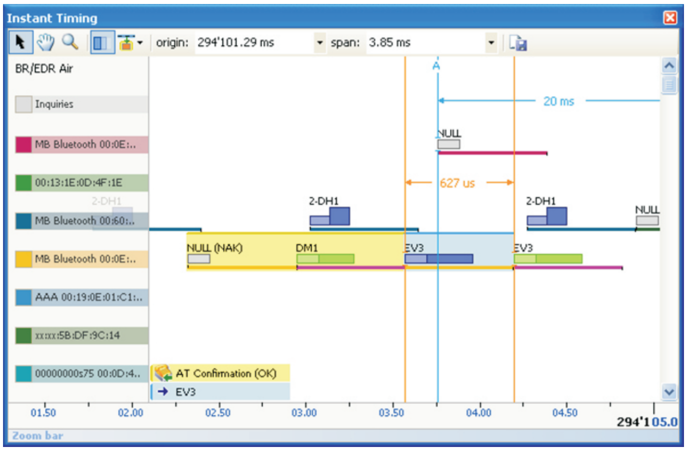


Ellisys Instant Piconet is a unique feature that is only made possible by the use of Ellisys Rainbow™ hardware capture technology. As soon as the analyzer starts recording, the Instant Piconet view displays the current topology of physical channel characteristics created by all neighboring devices. Piconets, scatternets, pagings and inquiries are displayed using symbols inspired by the *Bluetooth* specification and augmented with relevant information: data transfer activity and throughput for both master-slave and slave-master directions, per device RSSI, device names and addresses, etc.

There is **no limit in the topology complexity** that can be represented. Graphs are updated in **real-time** as new devices join or leave piconets, when **role switches** occur, or when any relevant property is modified. Powerful algorithms ensure that important information is always clearly displayed.

This view can be time-synced with other views and used to focus them on a given piconet or device, with simple mouse clicks.

Ellisys Instant Timing

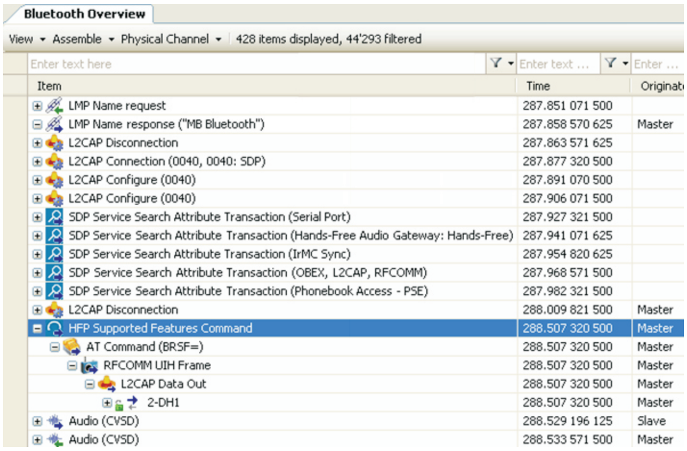


When using Ellisys analysis application, **Ellisys Instant Timing** quickly becomes the central feature that one cannot imagine being deprived of, and that makes one wonder how it was ever possible to work without it. This view displays all captured packets as **time ordered interactive graphical elements**. Length represents duration, while height is proportional to data rate (basic or enhanced). **Packets are color-coded** for type, master/slave direction, error status, device sending or receiving the packet, etc. Slot durations are also represented.

Packets are grouped in lines, using user-selectable criteria such as: master device of the piconet to which they belong, RF channel, sender/ receiver devices, etc. Time scale can be zoomed in to display data with symbol timing precision or zoomed out to display tenth of minutes at a glance. This view can be synchronized with other views.

Instant Measurement cursors are used to quickly get values for clock drifts and other timing-related quantities with one mouse click.

Ellisys Protocol Overview



Item	Time	Originat
⊞ LMP Name request	287.851 071 500	
⊟ LMP Name response ("MB Bluetooth")	287.858 570 625	Master
⊞ L2CAP Disconnection	287.863 571 625	
⊞ L2CAP Connection (0040, 0040: SDP)	287.877 320 500	
⊞ L2CAP Configure (0040)	287.891 070 500	
⊞ L2CAP Configure (0040)	287.906 071 500	
⊞ SDP Service Search Attribute Transaction (Serial Port)	287.927 321 500	
⊞ SDP Service Search Attribute Transaction (Hands-Free Audio Gateway: Hands-Free)	287.941 071 625	
⊞ SDP Service Search Attribute Transaction (IrMC Sync)	287.954 820 625	
⊞ SDP Service Search Attribute Transaction (OBEX, L2CAP, RFCOMM)	287.968 571 500	
⊞ SDP Service Search Attribute Transaction (Phonebook Access - PSE)	287.982 321 500	
⊞ L2CAP Disconnection	288.009 821 500	Master
⊟ HFP Supported Features Command	288.507 320 500	Master
⊟ AT Command (BRSF=)	288.507 320 500	Master
⊟ RFCOMM UIH Frame	288.507 320 500	Master
⊟ L2CAP Data Out	288.507 320 500	Master
⊞ 2-DH1	288.507 320 500	Master
⊞ Audio (CVSD)	288.529 196 125	Slave
⊞ Audio (CVSD)	288.533 571 500	Master

The easiest way to access any layer of the complex *Bluetooth* protocol and profile stack is the **Ellisys Protocol Overview**. This view displays all desired protocol elements in an easy-to-browse **hierarchical tree view.** The exact level of protocol decoding is easily configurable. It is **searchable** at will, and all columns can be used as filtering criteria to drill down data. Any fields displayed in the companion **Detail Pane** can be added and displayed as a whole column, for instant values comparison and custom filtering.

Baseband packets belonging to the same **retransmission attempt** are grouped into quickly identifiable single elements in order to avoid misleading indications, while increasing the insight given by a single line of text.

Commented **bookmarks** can be attached to any element to mark for future inspection or to share important findings with colleagues. In addition to icons that help to quickly identify protocols, symbols depict the encryption state of packets and show warnings and errors for **auto-detected issues**.

Ellisys *Bluetooth*® Explorer 400

Bluetooth® Instant Protocol Analysis System

ellisys

Better Analysis.

Technical Specifications

Analyzer RF Characteristics

- Ellisys Rainbow™: Synchronous, concurrent capture of all BR/EDR/LE channels
- Frequency band: 2.402-2.480 GHz
- Sensitivity range: From -90 to +15 dBm
- Attenuation: Programmable from 0 to 45 dB
- Modulations: All BR/EDR/LE modulations (GFSK, p/4-DQPSK, 8-DPSK)

Analyzer HCI Characteristics

- USB transport: Low, Full and High Speed
- UART transport: H4/H5/BCSP up to 8 Mbit/s

Generator Characteristics

- Single channel, dual-mode BR/EDR and LE standard radio
- Frequency band: 2.402-2.480 GHz
- Transmit power: Class1

Timing

- Clock: ±1ppm frequency accuracy
- BR/EDR/LE timestamp accuracy: 125ns
- USB HCI timestamp accuracy: 16.7ns

Embedded Memory

- 128 MB of FIFO memory
- Data is stored in highly optimized format
- Analyzed data is uploaded in real time through USB 2.0 connection

Front-Panel Indicators

- Power: unit powered on
- Operating: unit performing requested task
- Trigger: trigger event detected
- Generate: BR/EDR and/or LE packet transmitted
- Capture: BR/EDR and/or LE packet captured
- HCI: HCI packet captured

Front-Panel Connectors

- Capture: Standard SMA female
- Generate: Standard SMA female
- HCI: USB 2.0 Standard-A and Micro-B

Rear-Panel Connectors

- Computer: USB 2.0 Standard-B
- Power: 12-17 VDC, max 18 W
- Trigger: SMA in and out, 50 Ω, max 5 VDC
- IO Probe: supports HCI and logic analysis
- Inter-equipment: in and out, supports interconnection of several units

Power Supply

- Universal 100-240 VAC, 50-60 Hz
- 12 VDC, 18 W

Enclosure

- 174 x 111 x 58 mm (6.9 x 4.4 x 2.3")
- 0.9 kg (2.0 lbs)

Hardware Upgrade

- The Ellisys Rainbow™ engine is automatically updated with each software release (no user intervention required)

Maintenance and Licensing

- Free lifetime software updates – no maintenance fees
- Free full-featured viewer software – easily share annotated traces between computers and colleagues and replay captured traffic
- Use Ellisys hardware on any computer – no additional licenses needed

Warranty

- Two-year limited warranty

Ordering Information

Description	Code
Ellisys *Bluetooth* Explorer 400 (includes a hardware unit with *Bluetooth* 2.1 BR/EDR capture, accessories and carrying bag)	BEX400
Ellisys *Bluetooth* Explorer 400+LE (includes a hardware unit with concurrent BR/EDR and Low Energy capture, accessories and carrying bag)	BEX400LE

Options Chart

	BEX400	BEX400LE
Hardware units	1	1
2.1 BR/EDR capture	yes	yes
Low Energy capture		yes

Contact Information

US Sales Contact

Email: sales.usa@ellisys.com
Phone: +1 (866) 724-9158

International Sales Contact

Email: sales@ellisys.com
Phone: +41 22 777 77 89

More information on: www.ellisys.com/products/bex400