



# Bluetooth<sup>®</sup> Explorer<sup>™</sup>

All-in-One Dual-Mode Bluetooth<sup>®</sup>  
Protocol Analysis System

Powerful ■ Advanced ■ Integrated



Sales Contact:



USA: +1 866 724 9185

Asia: +852 2272 2626

Europe: +41 22 777 77 89



sales@ellisys.com



www.ellisys.com/bex400

**Wideband BR/EDR and Bluetooth Low Energy sniffer, with synchronized capture of Wi-Fi®, spectrum, HCI (USB, UART, SPI), Generic UART and SPI, SWD, I2C, SPMI, CAN bus, UCI, WCI-2, logic signals, and Audio I2S.**

### Innovative Tool for Demanding Users

With its revolutionary wideband Digital Radio and integrated All-in-One hardware approach, Ellisys changed the way Bluetooth protocol capture and analysis is done, by radically overcoming the drawbacks of legacy approaches. The Ellisys wideband capture approach robustly records any packet, at any time, from any neighboring piconet, with zero-configuration and without being intrusive.

Bluetooth Explorer's unmatched, deep-featured, and comprehensive software application is an industry-recognized standard that offers excellent flexibility and configurability to tackle even the most complex tasks. A wide range of analyses simplifies debug, interoperability testing, and performance characterizations.

### Reconfigurable Bluetooth Digital Radio

The reconfigurable radio concept for Bluetooth analysis is another major innovation from Ellisys. Reconfigurability means that the analyzer can be updated by software to support new features, without any change to the hardware. This cost-saving flexibility allowed for the addition of many new Bluetooth features, including LE Audio, Coded PHY, 2Mbps Bluetooth LE, and others, many months (years in some cases) before these features were released in an updated specification.

Additionally, Ellisys analyzers come with free lifetime software updates and no restrictions on sharing the application software with co-workers, so our customers can benefit from these great additions hassle-free.

### Industry's First Bluetooth Wideband Capture

Bluetooth wireless technology was originally designed to be robustly impervious to interference on the crowded 2.4 GHz ISM band. It was also designed to be difficult to sniff, for security reasons. To meet these criteria, a Bluetooth radio uses various communications technologies, such as pseudo-random hopping, adaptive frequency hopping, and other schemes.

Ellisys created the industry's first wideband sniffer, adding revolutionary features which opened new horizons for Bluetooth debugging and interoperability testing. The wideband capture approach is as simple as it is powerful — instead of listening to just a few channels, the sniffer captures all channels concurrently. The sniffer thus does not need to synchronize to a piconet; it will listen passively to all nearby Bluetooth piconets, scatternets, broadcasts, and other topologies.

### LC3 Auto-Detect

This innovative feature, based on an Ellisys-designed test equipment-grade LC3 codec, allows for automatic determination of LC3 configuration parameters. Historically, test equipment implementations have required a complete and error-free capture of audio codec configuration parameters to properly capture, characterize, and replay audio.

With this auto-detect innovation, even with otherwise critical configuration packets corrupted by interferences or low signal strength, LC3 audio can be recognized, understood, captured, and available for further analysis.

## Powerful Ellisys Features

- **All-in-One:** Fully hardware-integrated, time-synchronized, and concurrent capture of BR/EDR, Bluetooth LE, Wi-Fi, spectrum, HCI (USB, UART, SPI, Injected), Generic UART and SPI, SWD, I2C, SPMI, CAN bus, UCI, WCI-2, logic signals, and Audio I2S.
- **Widely Acclaimed Software:** Operating on Windows, Mac OS, and Linux, the popular Ellisys software platform provides INTUITIVE rendering of complex protocol and RF behaviors, and flexible configuration and control to give engineers the insights they need.
- **Bluetooth Wideband Capture:** Easy and rock-solid capture of any traffic on all channels, including discovery/connection traffic, complex topologies, mesh, broadcast, and more.
- **Wi-Fi 802.11 Capture:** Fully synchronized Wi-Fi capture for co-existence testing.
- **LC3 Auto-Detect:** Proprietary technology to detect and decode LC3 traffic even without capture of configuration parameters.
- **Emerging Features Support:** Early support for pre-specification features – test early and often to reduce iterations and shorten development.
- **Reprogrammable Bluetooth Digital Radio:** Evolvable by software to protect your investment.
- **All Protocols and Profiles:** Best-of-breed protocol decoding. Includes Ellisys Decode Language (EDL) for custom decodes and scripting for capture of user debug ports (Ellisys Debug Port, EDP).
- **Integrated Audio Analysis:** Comprehensive feature set for audio developers. Listen to captured wireless audio, and audio over HCI and I2S. Audio Grabber accessory for analog audio inputs.
- **RF Spectrum Display:** Characterize the raw wireless environment and visualize co-ex issues
- **Automation and Console Control:** Remote automation capabilities. Command Line Interface (CLI).
- **Free Maintenance:** Hassle-free, no-cost lifetime software updates

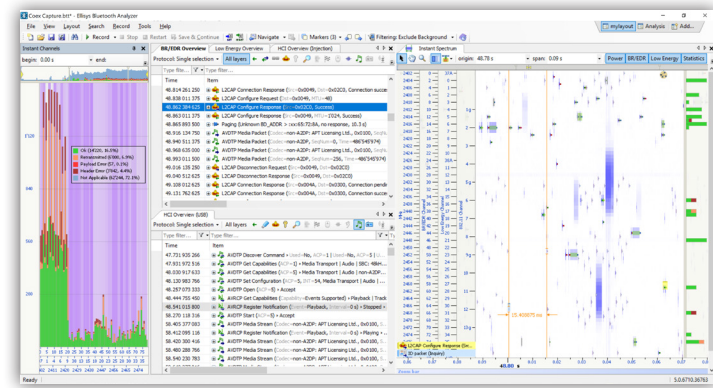
“ Test and characterization of new Bluetooth silicon and end-products is a comprehensive process requiring a diverse set of engineering expertise and an array of specialized, analytical tools, **said Muthu Kumar, Wireless Firmware Engineer, Intel Corporation.** The Ellisys Bluetooth Explorer plays an important role in this process by delivering a clear and complete understanding of the behavior of the ever-evolving Bluetooth technology from both hardware and software perspectives, all while providing exceptional ease of use.

”

## Visualizing Coexistence Issues

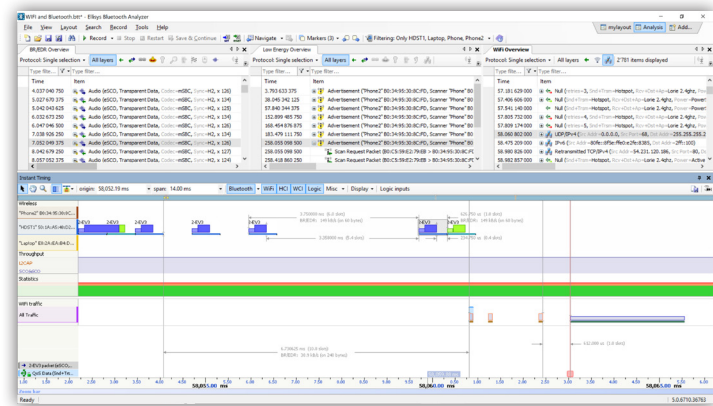
In addition to Bluetooth Classic and Bluetooth Low Energy, Bluetooth Explorer supports capture of Wi-Fi 802.11 and raw RF spectrum - **in precise synchronization with each other and all supported wired transmissions.** Understand and visualize sources of interference and contention with Bluetooth communications, as they share the 2.4 GHz ISM spectrum used by Bluetooth.

To fully characterize coexistence issues, Explorer delivers a variety of features that make this task easier. The user is provided a precise understanding of RF signatures, sources, and power, various timings, device performance indications, and other metrics. including tracking on channel avoidance techniques, and a variety of per-channel statistics, including errors, and retransmissions



## Timing View

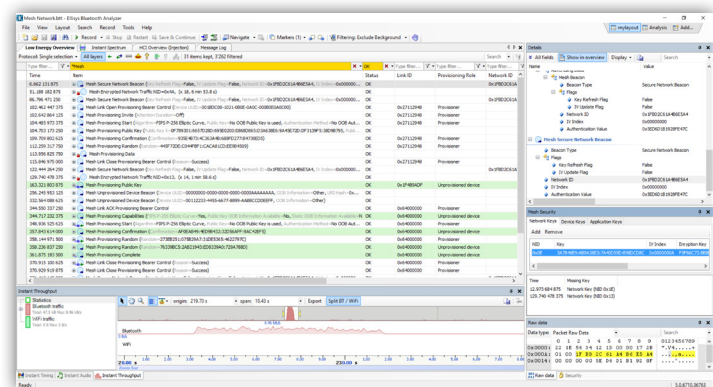
Many timing parameters defined by the Bluetooth specification are system critical. It is important to characterize these timings efficiently and accurately. Hardware and software timing issues are often the source of interoperability and performance issues that can challenge Bluetooth engineers.



All wired and wireless traffic streams captured are presented in the Timing View along a common and precise timestamp. Data throughput, packet transmission statistics, and other information is included to complete the approach.

## Bluetooth Mesh Networking

The Bluetooth Mesh Networking specifications define a broad spectrum of device and system requirements for a large-scale many-to-many network using Bluetooth Low Energy wireless technology. Bluetooth mesh networks can greatly increase the range of Bluetooth communications by using a message relay approach and are inherently uncomplicated and inexpensive to deploy, as there are no requirements for a central router or computer.

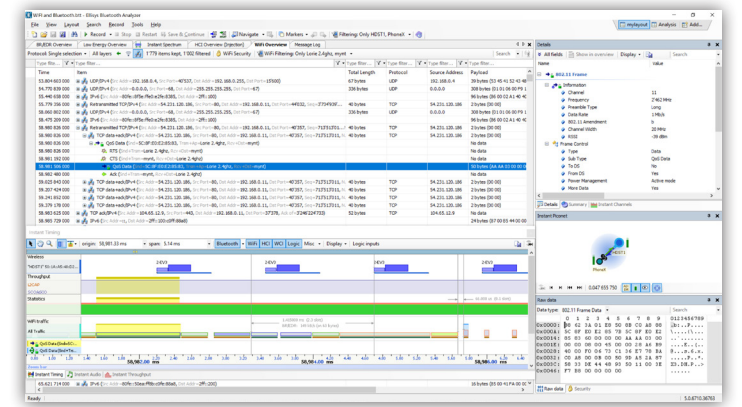


Bluetooth Explorer provides **comprehensive support for capture of mesh network protocol**, related packet and transactional decodes, encryption and key management features, and error detections. Mesh traffic is captured concurrently and in precise synchronization with all other supported traffic streams.

## Wi-Fi Capture

With Explorer, **Wi-Fi traffic is captured using an innovative, Ellisys-designed hardware-accelerated protocol engine.** With lower-performance Wi-Fi capture tools that use a software-based capture approach, the capture process is done with a processor involved. This approach can limit the speed and timing accuracy of the capture – packets can be missed when the processor is outmatched by the incoming streams.

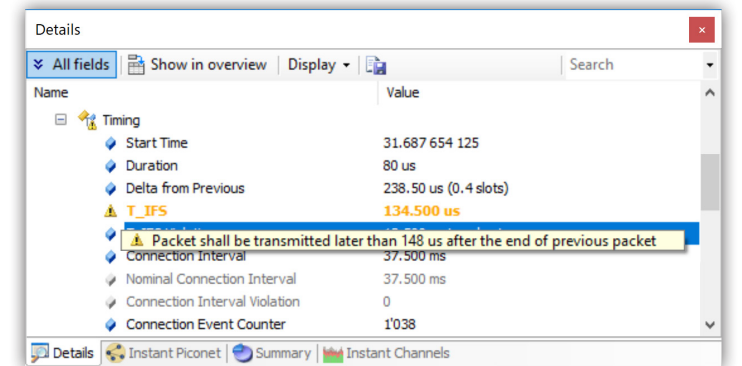
With Explorer's specially designed protocol engine, the Wi-Fi capture is driven directly and without processor dependence to guarantee throughput and minimize latency. Importantly, the Wi-Fi traffic is captured concurrently and in precise synchronization with all other supported wired and wireless capture streams.



## Automated Error Detections

The analyzer software alerts the user to a variety of errors detected for both wired and wireless captures. Physical, protocol, and profile layer errors, including packet and transactional errors, are **automatically highlighted without any need to search through the capture.**

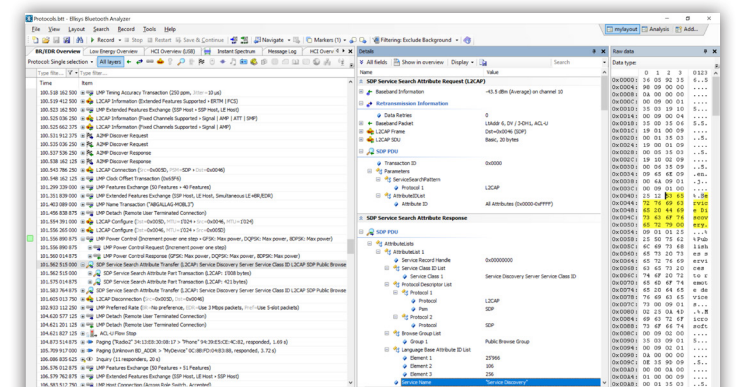
Errors are highlighted on a color-coded system to indicate the relative severity of the errors, summarized in a dedicated status column in each protocol overview, and described in the Details view or with pop-up messages on fly-over in the Overviews. Error indicators include incomplete payloads, missing or incorrect field values, center frequency violations, timing violations, missing responses, and CRC errors, and much more.



## Protocol & Profiles Analysis

Protocols and profiles are displayed in an easy-to-understand, high-level procedures-oriented chronological format in the Overview windows and fully detailed to the lowest bit/byte level in the linked Details view. All supported traffic streams are displayed (and configurable) in designated Overviews real-time, as the capture progresses.

The user is provided many controls to easily customize any Overview, including powerful filter, search, and coloring capabilities designed to quickly isolate items of interest. Traffic can be presented at the highest transactional layers, intermediate layers, and down to the most basic elements, such as packet-only views.



Debug port inputs (Ellisys Debug Port, or EDP) are allowed for UART and SPI. Using Ellisys Decoding Language (EDL), and all traffic streams can be directly edited for custom protocols using a script approach provided in the application.

**One-Click Record**

Capture starts instantly without any configuration. Devices under test are automatically detected.

**Protocol Overview**

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

**Spectrum Analysis**

Visualize hopping sequences, AFH dynamics, statistical per-channel error characteristics, timings, and RF characteristics.

**In-Depth Data Mining**

Detailed meta-data and protocol fields are clearly displayed and linked to the selected item in the overview.

**Piconets View**

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

The screenshot displays the main interface of the Ellisys Bluetooth Explorer. At the top, there is a menu bar (File, View, Layout, Search, Record, Tools, Help) and a toolbar with various icons. Below this is a navigation pane with tabs for 'Welcome', 'BR/EDR Overview', 'HCI Overview (Injection)', 'Message Log', and 'HCI Overview (Serial)'. The main area is divided into several panels:

- Protocol Overview:** A list of captured packets with columns for Time, Item, and Communication. The selected packet is an L2CAP SDU (Basic, Dst=Fixed 0x0030) at 8.544 246 875 ms.
- Spectrum Analysis:** A frequency plot showing power levels across different channels. A specific channel is highlighted with a yellow box, and a time interval of 2.998375 ms is marked.
- Timing View:** A detailed view of the selected packet, showing its structure and timing. It includes sections for Wireless, Throughput, and Statistics. A zoomed-in view of the packet structure is shown at the bottom.
- Channels View:** A bar chart showing the transmission quality of various channels. A legend indicates the status of each channel: Ok (3'888, 72.2%), Retransmitted (75, 1.4%), Payload Error (9, 0.2%), Header Error (87, 1.6%), and Not Applicable (1'325, 24.6%).
- Piconets View:** A diagram showing the topology of the piconet, with nodes labeled 'iPhone', 'Prime', and 'Phone1'.
- Security Management:** A table showing the status of link keys for different devices and PINs.

**Innovative Data Groups**

Relationships between packets are made clear, by assembling data per piconet's central device, peripheral, channel and more.

**Timing View**

Time-ordered, color-coded display of air and HCI traffic, statistics, data throughput and logic signals, with precision timing measurements.

**Channels View**

Understand per-channel transmission quality with a variety of statistics, over a user-specified time range.

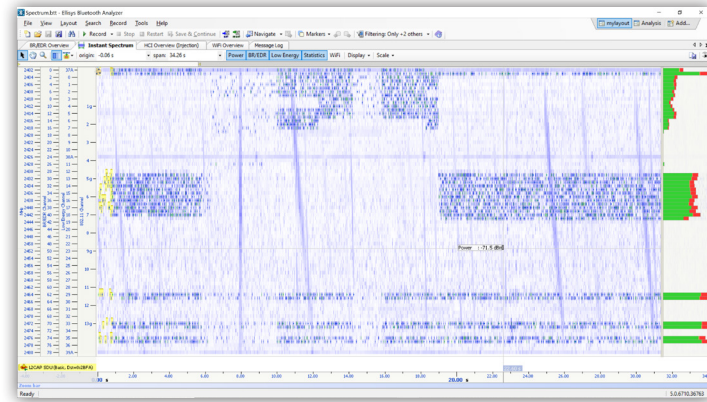
**Security Management**

Manage addition of link keys here. See when a Start Encryption exchange happens and navigate there with a single click.

## Spectrum Analysis

The Spectrum view chronologically displays Bluetooth and packets from other supported technologies packets by channel. Raw **RF spectrum information from any emitter in band(s) used by Bluetooth is provided**, such as Wi-Fi, IEEE 802.15.4, microwave ovens, and much more. These users can and do interfere with each other, and it is often necessary to gain a precise understanding of the wireless environment.

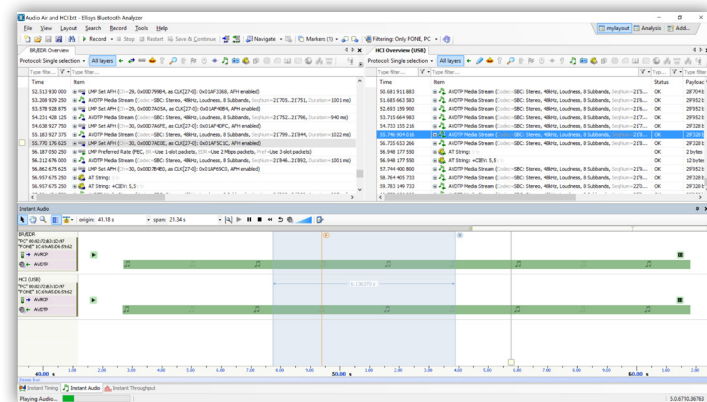
The signal strength of all emitters (RSSI) is displayed at a range of selectable resolutions. Adaptive Frequency Hopping (AFH) and Channel Mapping behaviors are overlaid, enabling a keen understanding of the complexities of coexistence characterization and debug.



## Integrated Audio Analysis

Captured audio streams can be easily played back, even during capture. Audio imperfections and associated protocol sequences can be correlated easily. Audio captured over HCI or from Audio I2S inputs [PRO] can be played back and viewed concurrently.

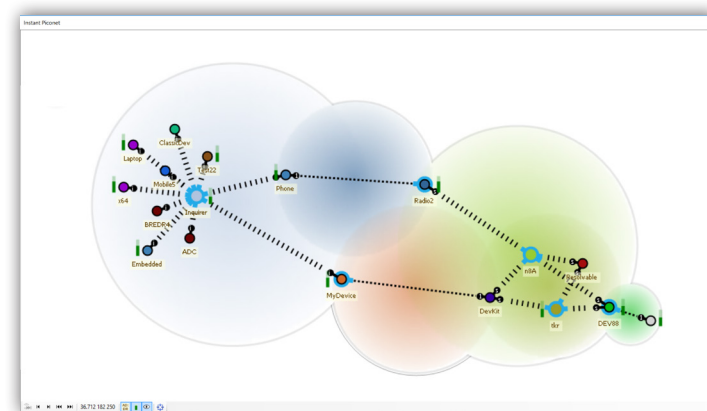
An optional Audio Grabber accessory is available to allow for input of analog audio streams. These features enable characterization of the complete audio chain, including the uncompressed audio provided to the source, DAC and ADC outputs, and audio transmitted wirelessly. Audio streams are exportable to WAV format.



## Topology Analysis

Bluetooth technology has become very popular among consumers and continues to evolve into new applications and markets, leading to more complex use cases. The only way to support these new use cases is to create more complex topologies, for example, Mesh Networking.

Debugging complex topologies has always been a difficult task, but Bluetooth Explorer is up to the task with its powerful wideband radio capable of capturing any traffic from any device, including the most complex topologies. The Piconet view helps developers visualize topologies live while capturing, and provides a play-back feature showing step-by-step evolution of topology changes. Several filters, such as show/hide broadcast, allow for distillation of the many devices typically present in development environments.



## Logic Analysis

The logic analysis feature allows for synchronous capture of external logic signals. Any digital signal is supported, including general-purpose inputs/outputs (GPIOs) or dedicated pins such as TX/RX Active, CTS, RTS, etc. A convenient color-coded probe is supplied.

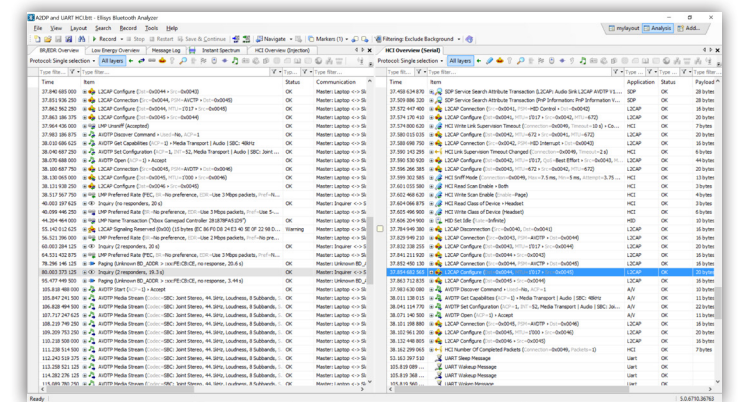
These **signals are visualized with 5-nanosecond precision** and displayed in the Timing view synchronized with all over-the-air and wired traffic streams. Signals can be assigned custom names and colors for easy identification. Custom signal groups can be created and displayed as buses, in addition to the display of discrete signals. Users can create simple external comparators and observe thresholds being crossed for various metrics, such as power consumption.



## HCI Analysis

Wireless traffic is the primary element of debug information for Bluetooth engineers, but Host Controller Interface (HCI) traffic can be an equally important complement of information for getting a clear and complete picture of a given situation. Bluetooth Explorer supports capture of HCI transports over USB, UART, and SPI.

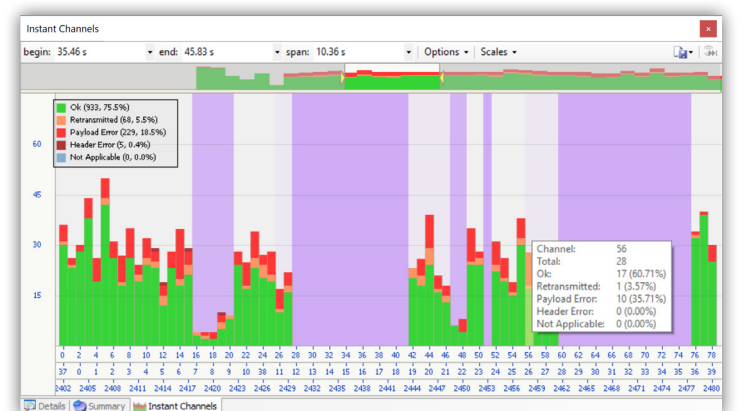
HCI traffic is captured concurrently with the wireless traffic and other wired streams using the same precision clock for perfect synchronization and timing analysis. This traffic is fully decoded and displayed in various formats. Conveniently, the Ellisys software automatically extracts any Link Key exchanged over HCI and uses it to decrypt the wireless traffic, all without any user interaction. Injected HCI traffic is also available.



## Channels View

The Channels view provides easy-to-understand visual and statistical analyses on various per-channel transmission characteristics, including packet retransmissions, header errors, and payload errors. This information can be useful in understanding where in the Bluetooth spectrum all devices, or specific devices, are communicating and the spectral areas (channels) they are avoiding, generally due to external interferences.

Visual cues are provided to give the user an understanding of the propensity of a given device, or aggregate devices, to avoid channels. This information is provided for the duration of an entire capture and can be configured to characterize all devices in the vicinity or specific devices.



## Throughput and Airtime

Understanding device throughput and airtime utilization are common tasks for wireless engineers. **These characterizations are managed by the Throughput and Airtime views.** A statistical analysis overlays graphics in both views to provide information on how various transmission inefficiencies relate to performance.

A navigation bar is provided to allow the user to select a time range to pan through the entire capture to see trends, including high and low peaks on throughput or airtime utilization. **Various controls are available to drill down to device connections,** individual transmitters, L2CAP channels, and audio channels. A synchronization feature allows for precise tracking with other views.



## Emerging Features Support

All Ellisys Bluetooth analyzer systems are reconfigurable with software updates. Ellisys is engaged with technical working groups and early adopters to provide support for upcoming Bluetooth extensions and specifications.

This approach allows new features and technologies to be added and tested, even in the conceptual stages, long before they become standardized in a public release of the Bluetooth specification. This is a significant advantage to Bluetooth radio and IP developers, and to the Bluetooth developer ecosystem in general, as new features can be refined and validated well before they are committed to silicon, greatly reducing chances of re-spins or post-spin discoveries of issues in the marketplace.



“ *The new advanced features provided by Ellisys provide our teams with tools that substantially increase visibility into the workings of Bluetooth technology, said Miles Louis Smith, Senior R&D Engineer, Test Group, Nordic Semiconductor. We use the sniffer to diagnose complex timing issues that other sniffers might not be able to capture. Due to the unique radio architecture of the Ellisys sniffer we can capture all packets regardless of the timing. The reconfigurable hardware is very flexible, and the Ellisys team provides great support to help us get products to market sooner.* ”

## Configurations and Purchase Information

Radio Configuration	EDR	LE	DUAL
Bluetooth Classic Capture	✓		✓
Bluetooth LE Capture		✓	✓ <sup>(1)</sup>

(1) Bluetooth LE 2M capture disables BR/EDR capture

Editions	Standard	Pro	Enterprise
Wideband Bluetooth capture	✓	✓	✓
HCI Capture		✓	✓
Logic capture		✓	✓
I2C, UART, SPI, SWD capture		✓	✓
Spectrum capture		✓	✓
Audio I2S capture		✓	✓
WCI-2 capture		✓	✓
Wi-Fi 802.11 a/b/g/n capture			✓
Warranty	2 years	2 years	3 years

Description	Code
Ellisys Bluetooth Explorer 400 Standard BR/EDR	BEX400-STD-EDR
Ellisys Bluetooth Explorer 400 Standard LE	BEX400-STD-LE
Ellisys Bluetooth Explorer 400 Standard Dual Mode	BEX400-STD-DUAL
Ellisys Bluetooth Explorer 400 Pro BR/EDR	BEX400-PRO-EDR
Ellisys Bluetooth Explorer 400 Pro Low Energy	BEX400-PRO-LE
Ellisys Bluetooth Explorer 400 Pro Dual Mode	BEX400-PRO-DUAL
Ellisys Bluetooth Explorer 400 Enterprise BR/EDR	BEX400-ENT-EDR
Ellisys Bluetooth Explorer 400 Enterprise Low Energy	BEX400-ENT-LE
Ellisys Bluetooth Explorer 400 Enterprise Dual Mode	BEX400-ENT-DUAL
Ellisys Bluetooth Explorer 400 Pro Upgrade	BEX400-PRO-UPG
Ellisys Bluetooth Explorer 400 Enterprise Upgrade	BEX400-ENT-UPG
Ellisys Bluetooth Explorer 400 Dual Mode Upgrade	BEX400-DUAL-UPG

## Technical Specifications

### Bluetooth Capture Characteristics

- Ellisys Rainbow™: Industry's first wideband concurrent capture of all Bluetooth channels
- Frequency band: 2.402-2.480 GHz
- Sensitivity range: From -90 to +15 dBm
- Gain: Programmable from -30 to +15 dB
- Modulations: All BR/EDR/LE modulations(GFSK 1/2Mbps, p/4-DQPSK, 8-DPSK)
- Baseband: Support of Bluetooth 5.x, upgradeable by software.

### Wi-Fi Capture Characteristics

- 802.11 2x2 a/b/g/n (2 streams)
- Channel width 2.4GHz: 20MHz or 40MHz, configurable
- 11n MCS 2.4GHz 20MHz channel: 0 to 15
- 11n MCS 2.4GHz 40MHz channel: 0 to 7
- 11n MCS 5GHz 20MHz channel: 0 to 7
- Guard Interval: 800ns and 400ns GI
- Frame encoding: BCC (LDPC not supported)
- Max AMPDU size: 16,384 bytes

### Logic Capture Characteristics

- Maximum bandwidth: 20 MHz
- Sampling precision: 5 ns
- Supported input voltage: 1.8 to 7V

### HCI Capture Characteristics

- USB HCI transport: Low, Full, and High Speed, with automatic detection
- UART HCI transport: Up to 8 Mbit/s, automatic detection of all parameters
- SPI HCI transport: Up to 8 Mbit/s, automatic detection of all parameters

### Embedded Memory

- 512 MB of FIFO memory
- Data is stored in highly optimized format
- Analyzed data is uploaded in real time

### Low-Speed Serial Capture Characteristics

- Generic Maximum Capture Rate 8Mbps
- Technologies supported include: UART/SPI HCI, generic SPI and UART, I2C, SWD, SPMI, WCI-2, Audio I2S, UCI, Ellisys Debug Port (UART and SPI), CAN bus, and logic signals.

### Timing

- Clock:  $\pm 10$ ppm frequency accuracy over -10 to +60 degrees Celsius range
- BR/EDR/LE timestamp accuracy:  $\pm 125$ ns
- Wi-Fi timestamp accuracy:  $\pm 1$ us
- USB HCI timestamp accuracy:  $\pm 16.7$ ns
- Logic timestamp accuracy:  $\pm 5$ ns

### Enclosure

- 180 x 170 x 58 mm (7.1 x 6.7 x 2.3")
- 1.0 kg (2.0 lbs)

### Power Input

- DC input (12-24 V)

### Power Adapter

- Input: 100-240 VAC
- Output: 24 VDC
- Power: 40 W
- Plug: 5.5 x 2.1 x 12 mm barrel straight
- Safety: CB, TUV, UL, CCC, PSE
- EMI: CE, FCC, VCCI, RCM

### 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
- Use Ellisys hardware on any computer – no additional licenses needed

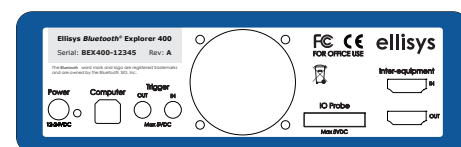


### Front-Panel Indicators

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

### Front-Panel Connectors

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



### Rear-Panel Connectors

- Computer: USB 2.0 Standard-B
- Power: 12-24 VDC, max 18 W
- Trigger: SMA in and out, 50  $\Omega$ , max 5VDC (RFU)
- IO Probe: supports logic analysis, UART/SPI HCI, generic SPI and UART, I2C, SWD, SPMI, WCI-2, Audio I2S, UCI, Ellisys Debug Port (UART and SPI), CAN bus
- Inter-equipment: in and out, supports connection of several units (RFU)

### Warranty

- Two-year limited warranty [STD, PRO]
- Three-year limited warranty [ENT]

### Minimum Requirements

- Windows® 10 (minimum recommended) & .NET framework 4.6.1
- macOS and Linux supported via Ellisys Runtime
- 8 GBytes of RAM
- USB 2.0 EHCI host controller

More information at: [www.ellisys.com/bex400](http://www.ellisys.com/bex400)