

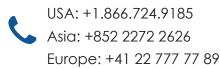


# **Bluetooth Explorer**<sup>™</sup>

## All-in-One Dual-Mode Bluetooth® Protocol Analysis System

Powerful • Advanced • Integrated

Sales Contact:



(*O*) sales@ellisys.com



www.ellisys.com/bex400



## **Powerful Ellisys Features**

- and SPI, Audio I2S, and WCI-2
- insights they need
- discovery/connection traffic and complex topologies
- capture accelerated by Ellisys hardware protocol engine for best-in-class performance
- configuration parameters
- **Emerging Features Support:** Benefit from early implementation of pre-specification feature additions
- **Mesh Support:** Includes full support for Bluetooth Mesh network topologies
- Reprogrammable Bluetooth Digital Radio: Evolvable by software to protect your investment
- Multi-Piconet Support: Visualize all topologies, including multiple piconets and scatternets
- All Protocols and Profiles: Best-of-breed protocol decoding
- Integrated Audio Analysis: Listen to captured over-the-air audio, including audio over HCI and I2S, within the software, in sync with all other traffic
- Raw RF Spectrum Display: Characterize the raw wireless environment and visualize co-ex issues
- Automation: Ellisys provides an automation API, a CLI, and an Injection API to allow for advanced capture control and data insertion/extraction tasks
- Free Maintenance: Hassle-free, no-cost lifetime software updates

"

of use.

Wideband BR/EDR and Low Energy sniffer with concurrent capture of Wi-Fi<sup>®</sup> 2x2 802.11 a/b/g/n, 2.4 GHz spectrum, HCI (USB, UART, SPI), WCI-2, logic signals, generic I2C/ UART/SPI/SWD, and Audio I2S.

## **Innovative Tool for Demanding Users**

Traffic analysis is one of the key day-to-day activities for Bluetooth engineers looking to rapidly test and debug their prototypes and products. Unfortunately, Bluetooth over-the-air sniffing has always been difficult to perfect. Legacy sniffing methods suffered from major technological drawbacks, making them unreliable and even unusable in several circumstances, making Bluetooth engineers' tasks much more difficult.

With its revolutionary wideband Digital Radio, Ellisys lifts protocol capture and analysis to new heights, radically overcoming the drawbacks of those legacy approaches to Bluetooth sniffing. The Ellisys all-in-one whole-band sniffer robustly records any packet, at any time, from any neighboring piconet, with zero-configuration and without being intrusive.

## **Bluetooth Wideband Capture**

Bluetooth wireless technology was originally designed to be robustly impervious to interference on the much-used 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 from 40 (low energy) to 79 (classic) channels pseudo-randomly according to a hopping sequence defined at the piconet's connection time. A hopping sniffer tries to actively synchronize on a specific hopping sequence, and captures the packets only after a successful synchronization. This kind of sniffer has several inherent limitations, making it more difficult to use, less reliable, and usable only in a limited set of scenarios.

Ellisys revolutionized Bluetooth sniffing with the release of the industry's first wideband sniffer. This approach overcomes all of these drawbacks and adds innovative and ground-breaking features, opening 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, and other topologies such as mesh, without any required configuration.

## **Reconfigurable Bluetooth Digital Radio**

With its innovative reconfigurable radio, the Ellisys sniffer can uniquely be updated by software to support changes in the specification, without any change to the hardware, and even without any interaction from the user.

For instance, this flexibility allowed for the addition of next generation Bluetooth baseband features (such as enhanced AES security, Connectionless Broadcast, and more recent features like Bluetooth LE Coded PHY and 2Mbps support) several months before these features were officially released in an updated specification. Additionally, the Bluetooth Explorer comes with free lifetime software updates, so all customers can benefit from these great additions free-of-charge!

## **LC3 Auto-Detect**

The Low Complexity Communications Codec, or LC3, is particularly ideal for Bluetooth Low Energy as it provides a high degree of quality, even at its lowest data rates. This architectural flexibility, which includes a wide selection of bit rates, allows developers to easily manage trade-offs between audio quality and power consumption, enabling extensions to battery life or even smaller battery sizes. Ellisys Bluetooth Analyzers include detailed decoding for LC3 traffic.

An 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 (wirelessly transmitted) 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 is still recognized, understood, captured, and available for further analysis. Even incorrect configuration implementations will not prevent LC3 capture.



All-in-One: Fully hardware-integrated, time-synchronized, and truly one-click concurrent capture of BR/EDR, Bluetooth Low Energy, Wi-Fi, raw RF spectrum, HCI, logic/GPIO, generic I2C, UART, SWD,

• Widely Acclaimed Software: The Ellisys software application provides intuitive understandings of complex protocol and RF behaviors, and flexible configuration and control to give engineers the

Bluetooth Wideband Capture: Easy and rock-solid capture of any traffic on all channels, including

Wi-Fi 802.11 a/b/g/n (2x2) Capture: Extremely accurate and perfectly synchronized Wi-Fi

LC3 Auto-Detect: Proprietary technology to detect and decode LC3 traffic even without capture of

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





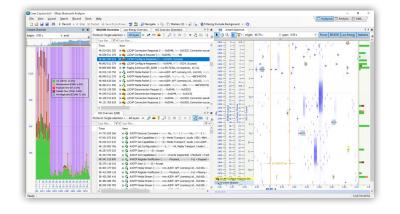
## Ellisys Bluetooth Explorer™

All-in-One Dual-Mode Bluetooth Protocol Analysis System

## **Visualizing Coexistence Issues**

In addition to Bluetooth Classic and Bluetooth Low Energy, Bluetooth Explorer supports capture of Wi-Fi 802.11a/b/g/n 2x2 and raw RF spectrum - **in precise synchronization with each other and all supported wired transmissions.** These technologies are frequently sources of interference and contention with Bluetooth communications, as they share the 2.4 GHz ISM spectrum used by Bluetooth. Increasingly, these technologies are co-resident on the same SoC.

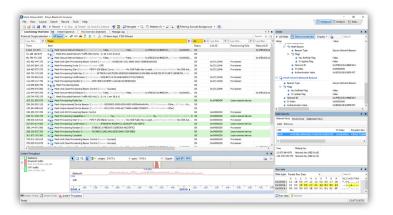
To fully characterize coexistence issues, Explorer delivers a variety of features that make this task easier. The user is provided a precise understanding of RF signatures, sources, and power, various timings, device performance indications, and other related metrics.



## **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.

## **Instant Timing**

Timing is everything as they say, and with Bluetooth, it's always an important focus. Multitudes of timing parameters defined by the Bluetooth specification are system-critical. It is understandably 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.

The Instant Timing view displays various information along a common timestamp, including visualized Bluetooth and Wi-Fi packets, HCI traffic (UART, SPI, and USB), generic communications (SWD, I2C, UART, and SPI), and logic signals. Data throughput and packet transmission statistics are included to complete the approach.

## **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. In-complete payloads, missing or incorrect field values, center frequency violations, timing violations, missing responses, and CRC errors are among the errors indicated.

💈 All fields 🛛 🖶 Show in overv	iew Display 🕶 📄	Search	
Name	Value		
🖃 🔩 Timing			
Start Time	31.687 654	125	
Ouration	80 us		- 1
Delta from Previous	238.50 us (	0.4 slots)	
▲ T_IFS	134.500 u	5	
Packet shall b Connection Interval	e transmitted later than 148 us a 37.500 ms	fter the end of previous packet	
Nominal Connection	Interval 37.500 ms		
Connection Interva	l Violation 0		
Connection Event (	Counter 1'038		

## **Protocol & Profiles Analysis**

Bluetooth 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 in designated Overviews real-time, as the capture progresses.

The user is provided various controls to easily customize any Overview, including powerful filtering and coloring capabilities designed to quickly isolate specific protocols, profiles, or communications of interest. Traffic can be presented at the highest level of abstraction and the user can drill down to show all intermediate levels, down to the most basic elements, such as packet-only views.



	out Search Becond Jools Help						C mylayout C Analysi	S DT AM
	🖌 🕨 Record + 11 Stop 12 Restart 16 Save & Continue 🚭 📆 💭 Navigate + 15, 🏷 Markes + 20 15, 😻 Ri	tering Only HDS	TL PhoneX + 4	a			and the second	
BEADE Overview					- 113	Details		
acet Single seles	tion + 🛛 All layers 🔶 🐺 📝 1779 items kept, 1002 filtered 👌 WFi Security 📲 WFi Filtering: Only Lovie 2.4gha, mys				Search 2114		Distance Do	iearch
Type fits Y			Colore Dec. 1	Y - Tope Ster		Name .	Take .	
Time	ten	Total Length	Pratocol	Source Address			1858	
	Bern a 🎝 UDP/DPv4 (Drc Addr = 192, 198, 8, 4, Drc Port = 40'537, Cot Addr = 192, 198, 0, 255, Dot Port = 15'500)	67 bytes	HUBBLE	192, MA.O.4	29 bytes (53 45 4) 52 40 48	□ → 2 802.11 frame		
53.804 663 000	a A UDP (DV4 CVC Addr - D4, 358, 8, 4, 570 VOT - 40 335, UDL Addr - 255, 255, 255, 255, 255, 257 VOT - 13500)	336 bytes	LOP	0.0.0.0	308 bytes (01 01 06 00 P9 1	II 🚓 Information		
55.440.658.000	B 20 Conference (Conference), Sector (1990), Contract (25, 25, 25, 25, 25, 25, 25, 25, 25, 25,	330 1998	0.04	0.0.0.0	96 bytes (36 00 02 A1 40 40	Otamel	22	
55.779 256 000	B J Retransited TOP/Pv4 Dir. Adv =54.231.120.186. Src Port=60. Dat Adv = 192.168.0.11. Dat Port=44032. Sec=3724907	40 bytes	1/2	54 231 120 186		Frequency	2'462 MMz	
58.060 802 000	a A LOP SPV4 Circ Add - 4.0.0.0, Src Fort-68, Ont Add - 255, 255, 255, Dat Fort-47	136 butes	IDP	0000	308 bytes (01 01 06 90 F9 1	Prearble Type	Long	
58.475 209 000	a 🔏 2014 Circ Add - 40/e:: 8/5e: ffebre 2/e: 8385, Cot Add - 2ffe 1000	200.64488	0.0	0.0.00	96 bytes (36 00 02 A1 40 40	Data Rate	110/6	
58,980 835 000	B 2 Retransmitted TCP/DPv4 Fire Addres 54 231, 120, 136, for Part-80, Cot Addres 182, 568, 0, 11, Cot Part-40/257, fore-712712701.	at hotes	TOP	54 231 133 186		802.11 Amendment	ь	
58,990 825 000	W M M M M M M M M M M M M M M M M M M M		109	54 231 120 186	2 bytes (20 00)	Channel Width     R552	-20.690	
58,990 826 000	R. +2. Oct Data End-SC/97 (2012) 533. Transfordare 2.4drz. Rev-Cat-ewell				No data	8 de Prane Control	-39 dBn	
58.980 826 000	O. 875 Cind - Transferie 2.4drg. Roy -Ont-myrt0				No data	e Troe	Data	
58,981 192 000	(D) CTS (End + Instrument, IncreColorLarie 2.4(No)				No deta	a Sub Type	Christ Carlie	
58.981 506 000	In Ord Data (Ind-SC IP 2012)33, True Hit-Lone 2 Adv. Revelationed)				50 butes (AA AA 03 00 00 0	Te D5	No	
58, 992 490 000	Adk Cind +Tran-ewet, Roy+Cat-Lone 2.4dpd)				No data	From DS	Yes	
59.025.043.000	10 💑 70P data +adv.0Pv4 Circ Addr = 54,235, 120, 106, Src Port = 80, Oct Addr = 192, 558, 6, 11, Oct Port = 40257, Sec = 71,751,7911, J	40 bytes	TOP	54 231 120 105	2 bytes (00-00)	Power Nanagement	Active mode	
55.207 424 000	🗑 🍌 TOP data +adul9+4 (Inc. Addr 54,235, 120, 186, 5n: Port - 80, Oct. Addr 192, 558,4,11, Oct. Port - 40367, Sec - 71375137311, 1	40 bytes	TOP	54 233 129 186	2 (tytes (20.00)	More Data	Yes	
59.241852000	🗑 💑 TCP data +ads/8Pv4 (inc. Addr - \$4.231, 120, 186, frc. Port - 80, Out. Addr - 192, 168, 8, 11, Out. Port - 467357, Sec 71751, F311, 1	40 bytes	TOP	54.233.329.586	2 bytes (30.00)	¢		
59,379 179 000	🛞 💑 TOP data +ads/8Pv4 (inc Addr - 54.231, 120, 186, Snc Port -80, Ont Addr - 192, 168, 0.11, Ont Port - 47267, Snc - 71375137311, H	40 bytes	TOP	\$4,231,129,186	2 bytes (30-00)	🗊 Detais 🐑 Summary 🕍 Instant O	hannels	
58.983 625 000	🕱 💑 TCP ads/5Pv4 (Src. Addr = 104.65.12.9, Src. Port=443, Oct. Addr = 192, 168.0.11, Cot. Port=37378, Adv. of = 3246/224733)	52 bytes	TOP	104.65.12.9	No data	Instant Descal		
58.983 625 000	# 27 adu D' adu D' 4 (Dr. Adu + 104.65.12.9, Dr. Port + 443, Dr. Adu + 192, 168.6.11, Dr. Port - 37378, Adv. of - 32462247323) # 27 adu D' 2 Adu - 1, Dr. Adu - 275 200 c076 8848)	52 bytes	TOP	104.65.12.9	No data 24 bytes (87 00 85 44 00 00	Instant Piconet		
58.963 625 000 58.965 729 000		52 bytes	TOP	104.65.12.9		Instant Poonet		
58.963 625 000 58.965 729 000 ant Taning	₩ ∰ IP4 € X: A69 -01, DX A69 -26, 2004086868		TOP	104.65.12.9	24 bytes (17 00 85 44 00 00			•
58.563 625 000 58.565 729 000 int Timing			109	104.65.12.9			•	
58.983 625 000 58.985 729 000 ant Timing	₩ ∰ IP4 € X: A69 -01, DX A69 -26, 2004086868		102	124.65.12.9	24 bytes (17 00 85 44 00 00			,
58.983 625 000 58.985 729 000 we Timing (2) Q. (1) 1	* Alge 944 (Fr. Astrin, Dir Astri-29) 200 (Millian) * origen 3,001.31 ms • span 5.14 ms • (Banteelli • Wilf (HC) (KO) (Lega Misc • Digday			104.65.12.9	24 bytes (17 00 85 44 00 00		P	
58.903 625 000 58.905 729 000 ant Timing (2) Q. (0) 2 (0) 2	* Alge 944 (Fr. Astrin, Dir Astri-29) 200 (Millian) * origen 3,001.31 ms • span 5.14 ms • (Banteelli • Wilf (HC) (KO) (Lega Misc • Digday	• Logic inputs		104.65.12.9	24 bytes (17 00 05 44 00 00			
58.903 625 000 58.905 729 000 ant Timing C Q Q 10 1 to sa.as.eed afters	* Alge 944 (Fr. Astrin, Dir Astri-29) 200 (Millian) * origen 3,001.31 ms • span 5.14 ms • (Banteelli • Wilf (HC) (KO) (Lega Misc • Digday	• Logic inputs		10445.12.9	24 bytes (17 00 05 44 00 00		RF1	•
58.563 625 000 58.565 729 000 text Timing (2) Q. (1) (2) (65 (1) (5) (4.45 - 64) (2)	* Alge 944 (Fr. Astrin, Dir Astri-29) 200 (Millian) * origen 3,001.31 ms • span 5.14 ms • (Banteelli • Wilf (HC) (KO) (Lega Misc • Digday	• Logic inputs		19463.12.9	24 bytes (17 00 05 44 00 00	less and		
58.963 625 000 58.965 729 000 int Timing (2 4 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	* Alge 944 (Fr. Astrin, Dir Astri-29) 200 (Millian) * origen 3,001.31 ms • span 5.14 ms • (Banteelli • Wilf (HC) (KO) (Lega Misc • Digday	• Logic inputs		_	24byles (37005544000)	ани ни на солгесство		
58.363 625 000 58.365 729 000 ant Timing 39 Q. 10 11 10 1	* Alge 944 (Fr. Astrin, Dir Astri-29) 200 (Millian) * origen 3,001.31 ms • span 5.14 ms • (Banteelli • Wilf (HC) (KO) (Lega Misc • Digday	• Logic inputs		_	24 bytes (17 00 05 44 00 00	н Этон и и и и и 2047 655 790 Raw deta		
58.983 625 000 58.985 729 000 tant Timing	• A projection of the constraints of the constra	• Logic inputs		_	24byles (37005544000)	Рина Полото Ran dea Cost type: 00211 Frank Dea 7	1	earch -
58.563 625 000 58.565 729 000 ant Taning Co. Co. Co. Co. Co. Co. Co. Co. Co. Co.	• # projection - inter-structure - (Balance) - Mail (RC) (RC) (Sp) Mail - Strategy - Value - Company Mail - Strategy - Mail - Strategy	• Logic inputs		_	24byles (37005544000)	и Бес и и и ин 2007/055700 Ran deta Dris type: 00231 Frame Dria - 1 0 2 2 3 4 40		a earch 1123456789
58.563 625 000 58.565 729 000 ent Timing C2 QL 10 16 17 50 64.66 48.0 g/g-u con tes	• A projection of the constraints of the constra	• Logic inputs		_	24byles (37005544000)	н Вы и и ин ин долгов то Выская О в 2 а 6 а 10 а 4 о 5 а 3 4 1 0 0 3 а 3 4 1	5 6 7 8 9 0 0 05 C0 A5 00	a iearch 123456739 01P
58.563 525 000 58.565 729 000 ant Timing 2 Q. 0 1 10 10 1 10	• A projection of the constraints of the constra	• Logic inputs		_	24byles (37005544000)	Сонструкций и на	5 6 7 8 9 0 0 05 C0 A5 00 0 9 5C 0F K0 K2 \	a earch 1123456789
58.963 625 000 58.965 729 000 ant Timing 2 9 9 10 10 10 10 10 10 10 10 10 10	★ \$ price	• Logic inputs		_	24byles (37005544000)	н Вы и и ин ин долгов то Выская О в 2 а 6 а 10 а 4 о 5 а 3 4 1 0 0 3 а 3 4 1	5 6 7 8 9 0 0 05 C0 A5 00 1 9 5C 0F E0 E2 \ 0 AA A6 03 00 .	a iearch 123454739 b1P
38.960 635 000 38.965 729 000 ant Tining 20 Q. 0 1 1 100 100 100 100 100 100 10		Logic inputs     DC	20	-	24byles (37005544000)	Image: Control of the state of the	5 6 7 8 9 0 0 05 C0 A0 00 1 3 5C 0F E0 E2 1 0 AA AA 03 00 . 0 00 28 A6 89 .	a iarch b1.2454739 b1P 
58.503 625 000 58.505 729 000 or Taning 20 Q. D. Taning 500 500 500 500 500 500 500 50		Logic inputs     DC		_	241ytes (27 005 44 00 00 (2 ) 240y 	Image: Note of the second se	5 6 7 8 9 0 0 03 C0 A5 06 2 3 5C 0F 50 52 \ 0 03 28 A6 89 . 1 36 57 78 3A 9	larch 123456789 1
58.563 625 000 58.565 729 000 ter Timing 0 Q 1 1 1 10 10 1 10 10 1 10 1 10 10 10 1 10 1		Logic inputs     DC	20	-	24byles (37005544000)	The H H H H H Coll 055 705 The H H H H H H Coll 055 705 The H H H H H H Coll 055 705 The H H H H H H Coll 055 705 The H H H H H H Coll 055 705 The H H H H H H Coll 055 705 The H H H H H H Coll 055 705 The H H H H H H H Coll 055 705 The H H H H H H Coll 055 705 The H H H H H H Coll 055 705 The H H H H H H H Coll 055 705 The H H H H H H H Coll 055 705 The H H H H H H Coll 055 705 The H H H H H H H Coll 055 705 The H H H H H H H Coll 055 705 The H H H H H H H Coll 055 705 The H H H H H H H H Coll 055 705 The H H H H H H H H Coll 055 705 The H H H H H H H H Coll 055 705 The H H H H H H H H Coll 055 705 The H H H H H H H H H Coll 055 705 The H H H H H H H H Coll 055 705 The H H H H H H H H Coll 055 705 The H H H H H H H H H Coll 055 705 The H H H H H H H H H Coll 055 705 The H H H H H H H H H H H H H H H H H H H	5 6 7 8 9 0 0 55 0 45 00 1 5 6 7 8 9 0 0 45 0 50 45 0 0 44 44 03 00 - 10 02 26 46 89 - 1 36 27 78 84 9 0 99 45 34 87 - 0 59 11 00 32 2	iarch 121454799 b1
58.963 425 000 38.965 729 000 am Tining 2 Q Q Q Q Q Q 800 800 800 800 800 800 800 80		Logic inputs     DC	20	-	241ytes (27 00 55 44 00 00 (24 ) 5 2400 	Image: Note of the second se	5 6 7 8 9 0 0 55 0 45 00 1 5 6 7 8 9 0 0 45 0 50 45 0 0 44 44 03 00 - 10 02 26 46 89 - 1 36 27 78 84 9 0 99 45 34 87 - 0 59 11 00 32 2	arch 12145(719) 5,0 ,0 ,0
58.963 425 000 38.965 729 000 an Tining 2 Q. Q. T. T 500 700 100 100 800 800 800 800 800 800 800		Logic inputs     DC	20	-	241ytes (27 00 55 44 00 00 (24 ) 5 2400 	The H H H H H Coll 055 705 The H H H H H H Coll 055 705 The H H H H H H Coll 055 705 The H H H H H H Coll 055 705 The H H H H H H Coll 055 705 The H H H H H H Coll 055 705 The H H H H H H Coll 055 705 The H H H H H H H Coll 055 705 The H H H H H H Coll 055 705 The H H H H H H Coll 055 705 The H H H H H H H Coll 055 705 The H H H H H H H Coll 055 705 The H H H H H H Coll 055 705 The H H H H H H H Coll 055 705 The H H H H H H H Coll 055 705 The H H H H H H H Coll 055 705 The H H H H H H H H Coll 055 705 The H H H H H H H H Coll 055 705 The H H H H H H H H Coll 055 705 The H H H H H H H H Coll 055 705 The H H H H H H H H H Coll 055 705 The H H H H H H H H Coll 055 705 The H H H H H H H H Coll 055 705 The H H H H H H H H H Coll 055 705 The H H H H H H H H H Coll 055 705 The H H H H H H H H H H H H H H H H H H H	5 6 7 8 9 0 0 55 0 45 00 1 5 6 7 8 9 0 0 45 0 50 45 0 0 44 44 03 00 - 10 02 26 46 89 - 1 36 27 78 84 9 0 99 45 34 87 - 0 59 11 00 32 2	arch 121454789 1019

					🖾 mylayout 🔝 Analysis 📑 Add
🔁 🥁 😹 🤮 🕨 🕨 Record • 🗉 Stop 💷 Restart 🗟 Save & Continue 🔮	2 Winesigate - 15	Markers (3) + 🖉 🕒 📲 Filtering: Only HDST	1, Laptop, Phone, Phone2	0	
BR/EDR Overview 4	P X Low Energy Ou	Aeview	41.8	Will Overview	4
Protocol: Single selection + 📶 layers + 🛹 👄 🔶 🝸 🔎 🎼 🎘 🕚 🔶 🤇	2 _ Protocol Single se	selection - All layers + 🛹 👄 🖨 🖗 🕸 🔊	Sc 12 . P	rotocol: Single selection + All la	jers 🔶 👳 🙀 2'761 items displayed 👘 🕴
Tupe file	Type filter	Y Type fiber		Type file	
Time been	A Time	bern	^	Time Item	
4.037 040 750 🐘 🐁 Audo (eSCO, Transparent Data, Codec-er68C, Sunc-H2, x 126)	3,793,633,375	75 Adventment (Phone 2' 50: 34: 95: 30: 8C.#	0. Scener Those 60	57.181.629.000 (# 45. Null (-	tries-3, Snd (Trans-Histopot, Roy (Ost (Ap-Lorie 2.4chz.)
5.027 670 375 R & Audo (e5CO, Transparent Data, Codec-m68C, Sunc-H2, x 134)	38.045 342 12	125 8 1 Advertisement ("Phone 2" 80:34:95:30.8C/F	D. Scamer "Phone" 80	\$7.406 606 000 B 4. Nul C	d+Tram-Hotspot, Ror+Ost+Ao-Lorie 2.4phz, Power-Pow
5.042 043 625 🔗 🐁 Audo (eSCO, Transparent Data, Codec-etSBC, Senc-H2, x 125)	\$7.840 344 37	175 . [1] Advertsement ("Phone2" 80:34:95:30:8C:P	0, Scamer "Phone" 80	57.541 140 000 + Nul (1	d+Tran-Hotspot, Ror+Dat+Ap+Lorie 2.4ghz, Power-Pow
6.032 673 250 🐘 🔹 Audo (eSCO, Transparent Data, Codec-erSBC, Sync-H2, x 134)	152,899 485 7	750 * H Advertsement ("Phone2" 60:34:95:30:8C:#	D, Scamer "Thone" 80	57.805 732 000 🔹 🔩 Nul (**	tries-4, Snd «Tram-Hotspot, Roy «Cat «Ap-Lorie 2.4ghz, I
6.047 046 500 🛛 🙀 🐁 Audio (eSCO, Transparent Data, Codec-ind8C, Sinc-H2, x 126)	258.454 875.8	875 8 3 Advertisement ("Phone2" 80:34:95:30.8C/F	0, Scamer "Phone" 80	57.809 174000 🛞 😘 Nul (+	tries+5, Snd+Trsm-Hotspot, Rov+Dst+Ap+Lorie 2.4ghz, I
7.038 926 250 🛛 👼 🔹 Audio (eSCO, Transparent Data, Codec-#SBC, Sync=H2, x 134)	183.479 111 7				v4 (Sec Add: +0.0.0.0, Sec Part+68, Dat Add: +255.255.25
7.052 049 375 🛛 🙀 🐁 Audio (eSCO, Transparent Data, Codec-#68C, Sync-H2, x 126)	258.055 098 5				rc Addr-80fe::8f5e:ffe0:e2fe:8385, Dit Addr-2ff::100)
8.042 679 250 🙀 🐁 Audio (eSCO, Transparent Data, Codec-#68C, Sinc-H2, x 127)	258.055 098 5				snitted TOP/IPv4 (Src Add -54.231, 120, 186, Src Port-80,
8.057 052 375 R. S. Audio (eSCD, Transparent Data, Codec -mSBC, Sync -H2, x 124)	258.418 860 2	250 L Scan Request Packet (80:C5:59:82:79:8	8 > 80:34:95:30:8C#C*	58.982 857 000 (# 4%, Null () 6	d+Tran -Hotapot, Ror+Dat+Ap+Lorie 2.4ghz, Power+Act
Instant Treing					
		WCI Legic Misc + Display + Legic inputs			De
AV0         2407         2407         2407           Lapler TB3ALABED.         Lapler TB3ALABED.         Lapler TB3ALABED.           Houghest         Lapler TB3ALABED.         Lapler TB3ALABED.	44V2  e	88236; 14163 (n.161946) 		EAG (an 68 byrne) 6 skraj	
Ratetics					
with traffic					
win traffic All Traffic			1	1 1	
			1	1 1	
			1		
		15 mg (13.3 dag)	1	-	• 612/000 vis (1.8 dori)
		125 mi (0.8 fen) Ni 30.338.6 (n.246 bras)	<u> </u>	-	• \$32,000 ut (1.8 den)
* 3003a466000.	BARDA.	91: 20.5 Mill (in 240 byrst)			
<ul> <li>2019pdefa600</li> </ul>	BARDA.	91: 20.5 Mill (in 240 byrst)			

otocols bit - Elloys Bluetooth Analyzer			V I ma		0
i Yew Layout Search Becord Tools Help			El mylayout	🖸 Analysis 📑	Add.
🧉 🗟 🖓 🐴 🕨 Record + 🗉 Stop 💷 Restart 🗟 Save & Continue   🗳 🎇   💭 Navigate + 🕮   🐑 Markers (1) + 💰	🗅 🕒 🧏 Filtering: Exclude Background 🔹 😽				
R/KDR Overview 🗌 Low Energy Overview 🕆 HCI Overview (USB) 🙀 Instant Spectrum 🕆 Hessage Log 🌾 HCI Overvi 🗘 🗙			× Raw data		
scel: Single selection + 🛛 Hayers 🔸 🛹 👄 😓 🖓 🔅 🎋 🗇 🔶 🎝 📾 🚳 🕼 🗇 📖 💷 🕼 🦂 🧌	¥ All fields 🔛 Show in overview Display •	Search Search	· Data type:		
type file V • Type filer	Name	Value	^	0 1 2 3	0123
Time Rem A	1 SDP Service Search Attribute Request (L2CA	P)		36 05 92 35	
100, 518, 162, 500 (# 998, 1MP Twing Acturacy Transaction (250 none, 101er - 32 us)	E + Resident Information	-43.5 dBm (Average) on channel 30		98 09 00 00 0A 00 00 00	
100.519 412 500 R 🐽 L2CAP Information Extended Features Supported + ERTH   FCS)				00 09 00 01	
100.523 162 500 a 19 Extended Features Exchange (SSP Host + SSP Host, LE Host)	🗟 🥐 Retransmission Information			35 03 19 10	
100.525 036 250 R 🝁 L2CAP Information Flowd Channels Supported + Signal   AMP   ATT   SMP	Data Retries	0		00 09 00 04	
100.525.662.375 III in L2CAP Information (Fried Channels Supported - Signal (AMP)	III + Dasebard Packet	LEAddr G, DV / 3-CH1, ACL-U	0x0018:	35 00 35 06	5.5
100.525 602 575 is No. 2009 Promission (Field Channels Supported + Signal (AVP) 100.531 912 375 is No. A2MP Discover Request	🐵 🛶 L2CAP Frame	Dst-0x0046 (SDP)		19 01 00 09	
100.535.036.250 H PG, A2HP Decover Request	🗟 🛶 L2CAP SDU	Basic, 20 bytes		00 01 35 03	
	R 2 SOP POU			19 00 01 09 00 05 35 03	
100.537 536 250 w R A2MP Decaver Response				19 10 02 09	
100.538 162 125 · R A2HP Discover Response	Transaction ID	0x0000		00 06 35 09	
100.543 786 250 🛞 🛖 L2CAP Connection (Fro=0x005D, PSH=5DP + Ort=0x0046)	💷 🔩 Parameters			09 65 65 09	
00.548 162 125 🗉 🎯 LMP Clock Offset Transaction (Dx65F6)	ServiceSearchPattern		0x0038:	00 68 09 01	. 3 .
01.299 339 000 🛞 🚎 LMP Features Exchange (50 Features > 40 Features)	Protocol 1	L2CAP		00 09 01 00	
01.351839.000 🕱 🗣 UMP Extended Features Exchange (SSP Host, LE Host, Smultaneous LE+6R(EDR)	🖶 🔩 AttributetDuiet			25 12 53 65	
131.403.089.000 🛞 Hig LMP Name Transaction ("ABGALLAG-MOBL3")	Attribute ID	All Attributes (Dx0000-CvFTTT)		72 76 69 63	
101.455 838 875 🛞 📲 LMP Detach (Remote User Terminated Connection)	2 SDP Service Search Attribute Response			65 20 44 69 73 63 67 76	
01.554 391 000 🛞 🍁 L2CAP Configure (3st=0x0050, MIU=1024 + Src=0x0046, MIU=1024)	x SUP Service Search Attribute Response			65 72 79 00	
01.556 265 000 (# 🎪 L2CAP Configure (Int - 0x0046, MTU - 1024 + Src - 0x005D)	B 2 50P POU			09 01 01 25	
131.556 890 875 🗉 🗛 LMP Power Control (Increment power one step + GFSK: Max power, DQPSK: Max power, 80PSK: Max power)				25 50 75 62	
101.556 890 875 R HIP Power Control Request (Increment power one step)	😑 🔩 AttributeLists			6C 69 73 68	
01.560 014 875 # 48 LMP Power Control Response (0PSK: Max power, DOPSK: Max power, 80PSK: Max power)	B AtributeLat 1			65 73 20 73	
101, 562 515 000 😑 🧟 SDP Service Search Attribute Transfer (), 2CAPI Service Discovery Server Service Class ID L2CAP SDP Public Browse	Service Record Handle	0x00000000		65 72 76 69	
101,562 515 000 R 2 SDP Service Search Attribute Part Transaction (L2CAP: (1008 bytes)	Service Class ID List	1000 B		63 65 73 20 74 67 20 72	
101,575 014875 8 2 50P Service Search Attribute Part Transaction (L2CAP: 421 bytes)	Service Class 1     Service Class 1     Service Class 1	Service Discovery Server Service Class ID		74 67 20 72 65 60 67 74	
101, 583 764 875 🛞 🥥 SDP Service Search Attribute Transfer (L3CAP) Service Discovery Service Class ID L3CAP SDP Public Browse				65 20 64 65	
101.605 013 750 🖩 🛖 L2CAP Deconnection (Src=0x0030, Ost=0x0046)	E * Protocol 1	124		76 69 63 65	
202,933 112 250 R mg LMP Preferred Rate (IR-No preference, ICR-Use 3 Moss packets, Prof-Use 5-sist packets)		500	0x007C1	73 00 09 01	
104.620 577 125 # 49 LMP Detach Remote Liter Terminated Connection)	Pam     Protocol 2	50P		02 25 0A 4D	
194.620 577 125 is mg. UMP Detach (Remote User Terminated Connection) 194.621 201 125 is mg. UMP Detach (Remote User Terminated Connection)	Protocol 2	576		69 63 72 68	
104.621.201.125 a mg Unit Design (Denote User Terminates Connection)	F State Crown List	4.5		73 67 66 74	
194.621827123 (a) (b) (40.0766 586) 194.873514875 (a) (b) Paging (Bado2' 34:13:58:30:08:17 > "Phone" 94:39:55:CE:4C:82, responded, 1.69 a)	e Group Lat	Public Resurse Group		35 03 09 01	
	Group 1	LYDer bulance munch		00 09 02 01	
105.709 917 000 🗴 🍽 Paging (Unknown BD_ACOR > "MyDevice" 0C:88:FD:04:83:88, responded, 3.72 s)	<ul> <li>Campage base Arroute LD Lat.</li> <li>Clement 1</li> </ul>	25'966		0A 00 00 00	
106.006 835 625 🙀 @ 2nguiry (11 responders, 20 s)	Content 1	23 999		OE 35 90 09	
206.576 012 875 🛞 🎯 UMP Features Exchange (50 Features + 51 Features)	clement 2     clement 3	256		00 00 01 00	
106.579 762 875 💿 👒 LMP Extended Peatures Exchange (SSP Host, LE Host + SSP Host)	Service Name	256 "Service Discovery"		01 00 00 09	
106, 581 512 790 a lia 1MP Host Connection (Across Role Switch, Acrossled)	· pervece hanne	an ner baconny	* 0x00.kB:	00 01 35 03	5

## **Ellisys Bluetooth Explorer**<sup>™</sup>

**R** A

All-in-One Dual-Mode Bluetooth Protocol Analysis System

## **One-Click Record**

<u>File View</u>

i 🛅 💕 🛃

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

Layout Search Record Tools Help

#### **Protocol Overview**

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

| 🕨 Record 🔹 🗉 Stop 🔄 Restart 🐻 Save & Continue | 👾 🎆 🎏 Navigate 👻 💷 👘 Markers 🗸 🚚 🖫 🌾 Filtering: Exclude Background 🔹 🦣

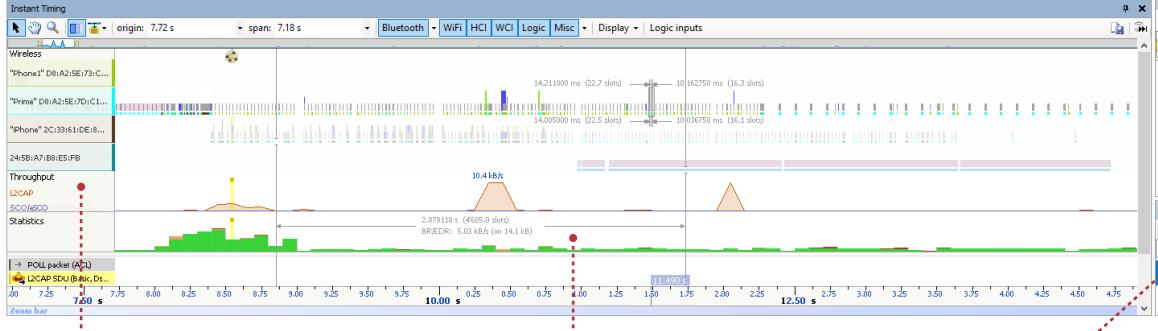
#### Instant Spectrum

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.

Welcome	BR/EDR Overview HCI Overview (Injection) Message Log HCI Overview (S	erial)	📘 Instant Spectrum	
ol: Single selec	ction 🗸 🗚 layers 🗲 🛹 📾 🍛 🖗 🔑 🖶 🎋 🕘 🗰 🎝 📾 🚳 🗊 🌖	4 🛍 🏻 🖓 💑 📟   🛛 😫 🚽	💽 🖑 🔍 🔲 🚡 - 🛛 origin: 8,544.24 ms	✓ span: 7.18 ms ✓ Power BR/EDR
be filter 🛛	Type filter Y	Type filter	2402 0 - 37A -	
ime	ltem	Communication	2405 3 1	•
407 372 500		Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla		
412 372 500	🗉 💩 L2CAP Information (Fixed Channels Supported > ATT)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	2411 - 9 - 4 - 19 - 2414 - 12 - 5 - 19 - 19 - 2414 - 12 - 5 - 19 - 19 - 2414 - 12 - 12 - 19 - 19 - 19 - 19 - 19 - 19	
447 372 500	🗉 🛖 L2CAP SDU (Basic, Dst=Fixed 0x0030)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	2417 15 6 2 -	
448 622 500	🗉 💩 L2CAP Connection (Src=0x0204, PSM=SDP > Dst=0x8707)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla		
452 996 875	🗉 🐟 L2CAP Information (Extended Features Supported)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	2423 - 21 - 30 - 30 - 30 - 30 - 30 - 30 - 30 - 3	
459 247 000	🗉 🖕 L2CAP Information (Fixed Channels Supported > ATT)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	2429 27 11 4	
460 496 875	🗉 🛖 L2CAP Configure (Dst=0x0204, MTU=256 > Src=0x8707, MTU=256)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	2432 - 30 - 13 - 5g -	
467 372 500	🗉 📥 L2CAP Configure (Dst=0x8707, MTU=128 > Src=0x0204, MTU=128)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla		
472 996 875	🗉 🛶 L2CAP SDU (Basic, Dst=Fixed 0x0030)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	$2438 - \frac{1}{2}236 - \frac{1}{2}616 - \frac{1}{2}6 \circ \frac{1}{2}$	
541 122 500	🗉 📥 L2CAP SDU (Basic, Dst=Fixed 0x0030)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	2444 - U 42 - 5 18 - 7 - 7	
542 372 500	🗉 🔎 SDP Service Search Attribute Transaction (PnP Information)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla		
.544 246 875	🖽 🛶 L2CAP SDU (Basic, Dst=Fixed 0x0030)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	2450 - 48 - 22 - 2453 - 51 - 23 - 9g -	
629 872 500	$_{rak H_{ m s}}$ SDP Service Search Attribute Transaction (Hands-Free Audio Gateway)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla		
667 372 500	🗉 秦 L2CAP SDU (Basic, Dst=Fixed 0x0030)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	2450 - 34 - 245 - 40 - 10 - 10 - 10 - 10 - 10 - 10 - 10	
.669 872 625	🗉 💂 SDP Service Search Attribute Transaction (Audio Source: L2CAP AVDTP V1.3)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	2462 - 60 - 28 - 11 - 29 - 11 - 29 - 11 - 29 - 11 - 29 - 11 - 29 - 11 - 29 - 11 - 29 - 11 - 29 - 11 - 29 - 11 - 29 - 11 - 29 - 11 - 29 - 11 - 29 - 11 - 29 - 11 - 29 - 11 - 29 - 11 - 29 - 29	
707 372 625	🖦 🔐 SDP Service Search Attribute Transfer (A/V Remote Control Target)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla		←2,998375 ms
722 372 500	■ → SDP Service Search Attribute Transaction (iAP: L2CAP RFCOMM Ch 1)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	2471 = 69 = 32 -	
.904 872 500	🗉 🚎 LMP Authentication Transaction (02 00 00 00 13 00 00 00 02 00 00 00 03 00	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	2474 72 34 139	<b>p</b>
912 372 625	IMP Encryption Mode (Encryption > Accepted)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla		
.915 496 750	🗉 😋 LMP Encryption Key Size (16 bytes > Accepted)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	E2CAP SDU (Basic, Dst=Fixed 0	
.916 746 750	🕀 😭 🛄 🖕 ACL-U Flow Stop	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	→ POLL packet (ACL)	
8.921 746 750	⊞ 📾 LMP Start Encryption Request (58 D9 FF 87 40 FE 6F 1A 34 2A B7 A9 D2 5B 4	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla <sup>♥</sup>	2.00 3.00 4.00 5.00	6.00 7.00 8.00 9.00 <b>8,550.00 ms</b>
C		>	Zoom bar	



#### Innovative Data Groups

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

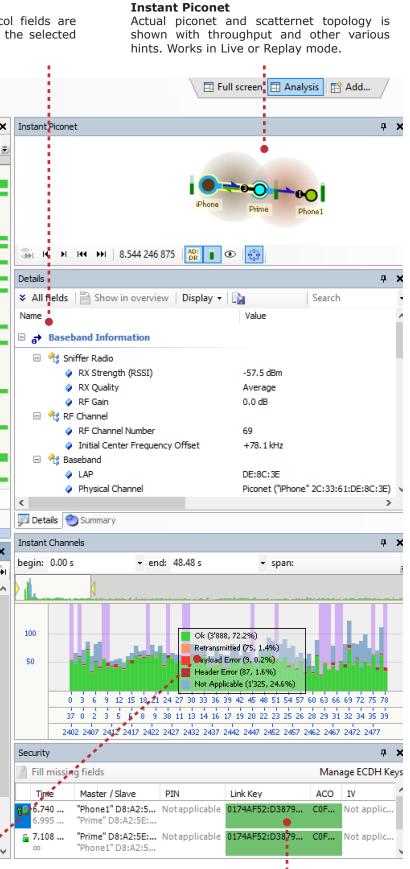
### Instant Timing

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

#### **Instant Channels**

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.





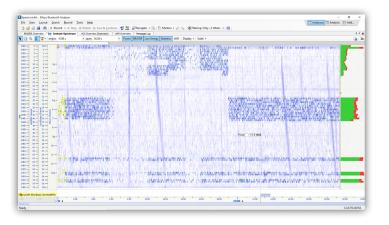
## Ellisys Bluetooth Explorer™

All-in-One Dual-Mode Bluetooth Protocol Analysis System

## **Spectrum Analysis**

The Instant Spectrum feature displays packets by channel, over time and can also synchronously display raw RF spectrum information in the busy and unlicensed 2.4GHz ISM band in which Bluetooth operates. Other users of this band include Wi-Fi, LTE, ZigBee, ANT, microwave ovens, and other products and technologies. 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. Adaptive Frequency Hopping (AFH) behaviors are overlaid, enabling a keen understanding of the complexities of the dynamic RF challenges encountered by any given Bluetooth link.



## 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.

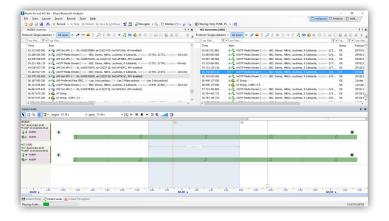
#### These signals are visualized with 5-nanosecond precision

and displayed in the Instant Timing view 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 a power consumption.

## **Integrated Audio Analysis**

Captured audio streams can be easily played back, even during capture. LC3 traffic is **automatically detected** using a test equipment-grade LC3 codec, even without capture of LC3 configuration traffic.

Finding packets carrying specific audio portions or at specific events is easily done. Audio captured over HCI or from an Audio I2S input [PRO] can be played back. This enables characterization of the complete audio chain, including the uncompressed audio provided to the source, the audio transmitted wirelessly, and the decoded audio at the receiver device. Audio streams are exportable to WAV format.



## **HCI Analysis**

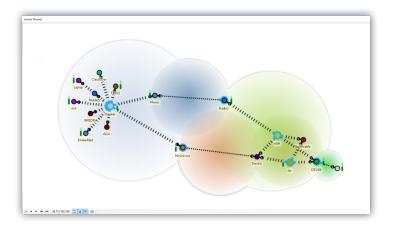
Wireless traffic is the primary element of debug information for Bluetooth engineers, but Host Controller Interface (HCI) traffic can be an equally important complement of information for getting a clear and complete picture of a given situation. Bluetooth Vanguard supports capture of HCI transports 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 and is decoded and displayed in various formats. Conveniently, the Ellisys software **automat**ically extracts any Link Key exchanged over HCI and uses it to decrypt the wireless traffic, all without any user interaction.

## **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 Vanguard is up to the task with its **powerful wideband radio capable of capturing any traffic from any device,** including the most complex topologies. The Instant Piconet view helps developers visualize their topologies live while capturing, and also provides a play-back feature showing step-by-step evolution of topology changes.



## **Channels View**

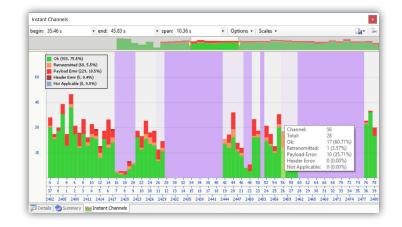
The Channels View feature provides **easy-to-understand visual and statistical analyses on various per-channel transmission characteristics,** including packet retransmissions, header errors, and payload errors. This information can be useful in understanding where in the Bluetooth spectrum all devices, 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 particular 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.



1	1 1	1 1 1	1.1.1	I I						1		
1	1-1	0417487	1 1 1	1.1		1.1	1 1 1	1.1			135.045	
1	1.1	1 1 1	1.1.1	1 1	1.1	1.1	1 1 1	$1 \cdot 1$			1.25145	
-		654.12482.0									1.25 18.5	
-		654.17687 m										
		654.17482 m								-		
-			s ((714.7 slot))									
		- UE: UARTHCEE	404 by such tim 207 by 241 by such tim 207 by									
		_			_							
												271.465460 mg (404.3 slots)
1		1 1 1	1	1	1			1	1 I.			1) 1
										11		
				1.1.1			1 1 1					
				1	1							
111				1.1								
					1							
			1	1					L L			
60	60 60 E0	60 60	60 60 60 0	0 00 00	6.2 6.2	0.2 0.2 0.3	6.0 6.0	60 60	0.3 0.3 0	0		60 60 60 60
0.5	10 10 10	01 01	6x1 0x1 0x1 0	1 01 01	81 85	0.5 0.1 0x	0.1 0.1	NS 015 015	0.1 0.5 0	11		04 04 01 01
	649	0.0 0.0	20 00	0.0	0.0	0.0	80 00	1.00	6.0			64
						81						
		1 1 1	1	1	1	1	1	1	1	1	THE HEAD	
				-			_	-	-	-		
		85 81 81 85	0.5 0.1 0.1 0.5 0.5 0.1									

A2DP and UART HCLbtt - Ellisys Bluetooth Analyzer						- 4	a ×
ile Yiew Layout Search Becord Tools Help				E m	ylayout 🗔 Ar	alysis 📑 A	idd. /
🗅 🤪 🔄 🙀 🔥 🕨 Record 🔹 🗉 Stop 💷 Restart 🗟 Save & Continue   🛃 💆 🚚 Navig	ete - 12, 10	Markers (1) + 🖉 🕒 🕷	Filtering: Exclude Background	- 6			_
BR/EDR Overview Low Energy Overview Message Log 🔚 Instant Spectrum 🖌 HCI Overvi	ew Onlection)	4 P. x	HCI Overview (Serial)				4.9
rtocol: Single selection + 🛛 All layers + 🛹 👄 📤 🖗 🔎 🔅 🕸 🗇 🔶 👘 🖏 🕼 🕼			internet Single selection +	1		6.2 -	
	Dr. Y.		Type fit Y . Type fiter.		Type Y -		
Time Bern	Status	Communication A	Time Pers		Application		Pavloa
37.840 685 000 R 44 L2CAP Canfigure (5x1-0x0044 + 5x1-0x0043)	OK	Masteri Lanton c-> St		Service Search Attribute Transaction (L2CAP) Audio Sink L2CAP AVDTP V1		OK	28 hvts
37.851 936 250 R 4 L2CAP Connection Elec-0x0044, PSH-ANCTP + Dat-0x0045	OK.	Master: Laptop <-> Si		Service Search Attribute Transaction (L2CAP) Adde Shik (L2CAP Write Fig., Service Search Attribute Transaction (PrP Information: PrP Information V		or .	28 byt
37.852 552 250 * 😼 L2CAP Confector (211-0x0044, 1511-48/CIP + 011-08/046) 37.852 552 250 * 🐟 L2CAP Confector (211-0x0044, 1511-1017 + 511-0x0045)	OK OK	Master: Laptop <-> Si Master: Laptop <-> Si		Service search Attribute transaction (HP Information: HP Information V IP Connection (Src=0x0041, FSH=HED Control + Drt=0x0042)	LICAP	OK OK	28 byt
37.863 386 275 R 4 L2CAP Configure Control 00045 - Sec-0x0046	OK .	Master: Laptop <-> Si		P Configure Elist+Ox0041, HTU+1017 + Src=Ox0042, HTU+672)	LICAP	OK .	20 byt
37.964 436 000 R He LMP Unaniff (Accepted)	OK .	Master: Lantas c.o. Sc		Write Link Supervision Timeout (Connection -0x0049, Timeout - 10 s) + Co		OK .	Zhutes
37.964 436 000 a very over (accepted) 37.963 196 875 a A autory Decever Command + Listed -No. ACP+1	OK.	Master: Laptop <-> Si Master: Laptop <-> Si		P Configure (Dst-0x0042, HTU-672 + Src-0x0041, HTU-672)	L2CAP	OK OK	20 hvt
37.983 396 875 (a +2) AVDTP Desiver Command + Use1+Ne, ACP+1 38.032 686 625 (a +2) AVDTP Get Capabilities (ACP+1) + Media Transport   Audo   SBC: 4891z	OK OK	Master: Laptop <-> Si Master: Laptop <-> Si		P Configure ()St-0x0042, MTU-672 + Src-0x0041, MTU-672)     P Connection (Erc-0x0042, PSH-HED Internat + Dct-0x0043)	LICAP	OK OK	20 6yr
		Master: Laptop <-> si Master: Laptop <-> Si			HCL	OK OK	A hute
38.040 687 250 🔹 🧛 AVOTP Set Configuration (1-0*-1, 11/1-52, Media Transport   Audio   SBC: Joint				Link Supervision Timeout Changed (Connection - 0x0049, Timeout - 2 s)			6-by% 44.by%
38.070 688 000 🛞 🦓 AVDTP Open (I/CP-1) + Accept	ok	Master: Laptop <-> Sk		NP Configure (Dst=0x0042, HTU=1017, QoS=Best Effort + Src=0x0043, H.		ok	
38.100 687 750 🔹 🛖 L2CAP Connection (Frc=0x0045, PSH=AX07P + Dit=0x0046)	OK	Master: Laptop <-> Si		4P Configure (Dit+0x0043, HTU+672 + Src=0x0042, HTU+672)	LOCAP	ok	20 byt
38.130.065.000 🔹 🔩 L2CAP Configure (Dst=0x0045, HTU=2000 + Src=0x0046)	ox	Master: Laptop <-> Sk		Sniff Made (Connection=Ox0049, Max=7.5 ms, Min=5 ms, Attempt=3.75		ox	13 by
38.131 938 250 🛞 🚭 L3CAP Configure (3st-0x0046 + Src-0x0045)	ox	Haster: Laptop <-> Sk	37.601 055 580 🛞 🚑 HCI		HCI	ok	3 by b
38.517 557 750 **** UMP Preferred Rate (FEC, IR -No preference, ECR - Use 3 Mbps packets, Pref -N		Master: Laptop <> Sk		Write Scan Enable (Insbin-Page)	HCI	OK	4595
40.003 197 625 🛞 @ Inquiry (no responders, 20 s)	ok	Master: Inquirer <> \$		Read Class of Device + Headset	HCI	OK	30/9
40.099 446 250 🛞 🕸 UMP Preferred Rate (IR -No preference, EDR -Use 3 Mbps packets, Pref-Use 5		Master: Laptop <-> Si		Write Class of Device (Headset)	HCI	OK	6-byte
44.204 464 000 🐵 🎯 LMP Name Transaction ("Xbox Ganepad Controller 281878FA51D9")	ox	Masteri Laptop <-> Si	37.606 204 900 🛞 📜 HID		HID	OK	20 byt
55.142 012 625 🛞 🚖 L2CAP Signaling Reserved (0x00) (15 bytes (EC 86 F0 D8 24/E3 40 5E 0F 22 98 D	Warning	Master: Laptop <-> Si		AP Disconnection (Src=0x0040, Ost=0x0041)	LOCAP	oc	35 by
56.521 396 000 🔹 🕸 UMP Preferred Rate (IR-No preference, EDR-Use 2 Mbps packets, Pref-No pre		Master: Laptop <>> Sk	37.829 949 210 🛞 🛶 L2CA	AP Connection (Src=0x0043, PSH=AV07P + Dst=0x0044)	LICAP	OK	36 by
60.003 294 125 (# 40 Inquiry (2 responders, 20 s)	ox	Master: Inquirer <>> 5		RP Configure (Dist-0x0043, HTU+1017 + Src-0x0044)	LICAP	OK	20 by
64.531 432 875 🛞 🕸 UNP Preferred Rate (PEC, DR -No preference, EDR -Use 3 Mbps packets, Pref -N		Master: Laptop <-> Sk	37.841211920 🗷 😪 L2CA	AP Configure (Dist=0x0044 + Src=0x0043)	LICAP	OK	35 by
78.296 146 125 R Paging (Unknown BD_ADDR > txxtPErCBrCE, no response, 20.6 s)	ox	Master: Unknown 80 /	37.852 450 130 🛞 🛶 L2CA	AP Connection (Src=0x0044, PSM=AVCTP + Dst=0x0045)	LICAP	OK	25 byt
80.003 373 125 🛞 🛞 Inquiry (2 responders, 19.3 s)	ox	Master: Inquirer <-> 5	37,854 682 565 🛛 📦 🗘 1204				
95.477 449 500 (a Deping (Unknown BD_ACOR > coc/FE:CB:CE, no response, 3.44 s)	ox	Master: Unknown 80 /	37,863 712 835 🛞 🛶 L2CA	4P Configure (Dist-Dir0045 + Sirc-Dir0044)	LOCAP	OK .	35 byt
105.838 488 000 🛞 🦓 AVDTP Start (1/2?-1) > Accept	ox	Master: Laptop <-> Sk	37.983 630 080 🛞 🖧 AUD	TP Discover Command + Used-No, ACP+1	A/V	OK	20 byt
195.847 241 500 🛞 🦓 AVDTP Media Stream (Codec - SBC: Joint Stereo, 44. SHz, Loudness, 8 Subbands, 1	OK	Master: Laptop <-> Sk	38.011 138 015 🛞 🖧 AND	TP Get Capabilities (ACP+1) + Media Transport   Audio   SEC: 48kHz	A/V	OK	11 byt
105.828 494 500 🐨 🕰 AVOTP Media Stream (Codec-SBC) Joint Stereo, 44.5Hz, Loudness, 8 Subbands, 1	ox	Masteri Laptop <>> Sk	38.041 114 770 B - AND	TP Set Configuration (10P-1, INT-52, Media Transport   Audio   SBC: Jok	A/V	OK	22.011
107.717 247 625 · AliOTP Media Stream (Codec-SBC: Joint Stereo, 44.5Hz, Loudness, 8 Subbands, 1	ox	Master: Laptop <-> Sk	38.071 140 500 B 4 AIC	TP Open (I/CP = 1) > Accept	AN	OK	11 byt
108.229 748 250 🛞 🐴 AIOTP Media Stream (Codec-58C: Joint Storeo, 44.5Hz, Loudness, 8 Subbands, 5	ox	Master: Laptop <>> Sk	38.101 198 880 · · · · · · · · · · · · · · · · ·	AP Connection (Src-0x0045, PSH-AV07P + Dst-0x0046)	LICAP	ox	35 byt
109.209 753 250 🛞 🐴 AUOTP Media Stream (Codec-SBC: Joint Stereo, 44. SHz, Loudness, 8 Subbands, 1	ox	Master: Laptop <-> Si	38. 102 961 200 B 🐽 L2CA	AP Configure (Dat-Du0045, HTU-1000 + Src-Dx0046)	LICAP	ox	20 byt
110.218 508 000 · A AVOTP Media Stream (Codec-SBC: Joint Stores, 44, Skitz, Loudness, 8 Subbands, 1	ox	Master: Laptop <-> Sk		# Configure (Dat-0x0046 + Sec-0x0045)	LICAP	OK .	35 by
111.238 514 500 @ 🐴 AUOTP Media Stream (Codec-SBC: Joint Stereo, 44.5Hz, Loudness, 8 Subbands, 1	ox	Master: Laotao <> Sk	38.162 299 065 B+4 HCT	Number Of Completed Packets (Connection-0x0049, Packets-1)	HCI	ox	70/10
112, 243 519 375 (# 🐴 AliOTP Media Stream (Codec+SBC: Joint Stereo, 44, Sitts, Loudness, 8 Subbands, 1		Master: Laptop <-> Si		T Sleep Message	Uet	OK .	
113.258 521 125 R A AVOTP Media Stream (Codec-SBC: Joint Steres, 44.3Hz, Loudness, 8 Subbands, 1		Mester: Laptop <> Sk		T Waleup Message	Uet	ox	
114-282 276 125 (# A AUDTP Media Stream (Codec-SBC) Joint Stereo, 44-3Hz, Loudness, 8 Subbands, 1		Master: Lapton <-> St		T Wakeup Message	List	OK .	
115.089 780 750 (a Al AUTTE Media Stream Control SEC: Just Stream, 64 Little, Lowinson, 8 Schlawin, 1		Master: Lanton <-> G *		T Unders Mensage	Liet	OK .	
¢		>	<				





Ellisys Bluetooth Explorer<sup>™</sup> All-in-One Dual-Mode Bluetooth Protocol Analysis System

## **Configurations and Purchase Information**

Radio Configuration	
BR/EDR Capture	
Low Energy Capture	
Editions	
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	

## Description

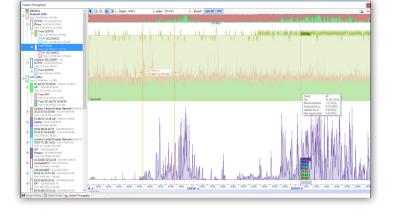
Warranty

Ellisys Bluetooth Explorer 400 Standard BR/EDR Ellisys Bluetooth Explorer 400 Low Energy Ellisys Bluetooth Explorer 400 Dual Mode Ellisys Bluetooth Explorer 400 Pro BR/EDR Ellisys Bluetooth Explorer 400 Pro Low Energy Ellisys Bluetooth Explorer 400 Pro Dual Mode Ellisys Bluetooth Explorer 400 Enterprise BR/EDR Ellisys Bluetooth Explorer 400 Enterprise Low Energy Ellisys Bluetooth Explorer 400 Pro Upgrade Ellisys Bluetooth Explorer 400 Enterprise Upgrade Ellisys Bluetooth Explorer 400 Enterprise Upgrade

# Throughput and Airtime

Understanding device data throughout 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 data 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 – another Ellisys innovation. Ellisys maintains close relationships with radio developers worldwide and with various technical groups involved in outlining new Bluetooth specifications.

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



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.

"



EDR	LE	DUAL
x		x
	x	x

Standard	Pro	Enterprise
x	x	x
	x	x
	x	x
	x	x
	x	x
	x	x
	x	x
		x
2 years	2 years	3 years

Code
BEX400-STD-EDR
BEX400-STD-LE
BEX400-STD-DUAL
BEX400-PRO-EDR
BEX400-PRO-LE
BEX400-PRO-DUAL
BEX400-ENT-EDR
BEX400-ENT-LE
BEX400-ENT-DUAL
BEX400-PRO/UPG
BEX400-ENT/UPG
BEX400-DUAL/UPG

## Ellisys Bluetooth Explorer™

All-in-One Dual-Mode Bluetooth Protocol Analysis System

## ellisys Better Anglysis

## **Technical Specifications**

## Bluetooth Capture Characteristics

- Ellisys Rainbow<sup>™</sup>: 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
- Channel width 5GHz: 20MHz or 40MHz
- 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

- UART: Up to 8 Mbit/s automatic detection of all parameters
- SPI: Up to 8 Mbit/s, automatic detection of all parameters
- I2C: Up to 1 Mb/s
- SWD: Up to 8 Mb/s

#### Timing

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

#### 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<sup>™</sup> 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

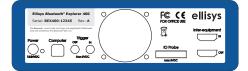


## **Front-Panel Indicators**

- 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 Ω, max 5VDC
- IO Probe: supports UART/SPI HCI, WCI-2 and logic analysis
- Inter-equipment: in and out, supports connection of several units

#### Warranty

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

#### **Minimum Requirements**

- Intel Core, 2 GHz or compatible processor
- 4 GBytes of RAM
- 1280 x 1024 display resolution with at least 65,536 colors
- USB 2.0 EHCI host controller
- Windows<sup>®</sup> 7 or higher .net framework 4.6.1

## More information at: www.ellisys.com/bex400

Copyright© 2021 Ellisys. All rights reserved. Ellisys, the Ellisys logo, Better Analysis, Ellisys Bluetooth Explorer and Rainbow are trademarks of Ellisys, which may be registered in some jurisdictions. The Bluetooth® word mark and logos are registered trademarks owned by the Bluetooth BIG, Inc. and any use of such marks by Ellisys is under license. Wi-Fl® and the Wi-FA illiance logo are trademarks or Wi-Fl® and trade names are those of their respective owners. All other trademarks are wonded by their respective owners. All other trademarks are wonded by their respective owners. Information in this publication supersedes all earlier versions. Ellisys reserves the right to change the specifications without notice. Information in this publication is provided "as is" without warranty of any kind, either express or implical. Pictures in this publication are for illustration only: actual products may differ.

