

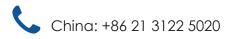


# Bluetooth Explorer

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

Powerful 
Advanced 
Integrated

Sales Contact:



abe@abe-tech.com



www.ellisys.com/bex400



## Wideband BR/EDR and Low Energy sniffer with concurrent capture of Wi-Fi 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 tech**nological 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.

## **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 BLE 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!



## **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.

## Fully Integrated, All-in-One Sniffer

Capturing wireless traffic is a very important aspect of Bluetooth debugging, but other information is equally important for understanding the big picture. This is another aspect where the Ellisys sniffer excels.

The Bluetooth Explorer sniffer supports one-click concurrent and tightly synchronized capture of:

- Classic Bluetooth BR/EDR
- Bluetooth Low Energy (BLE)
- Wi-Fi 2x2 802.11 a/b/g/n [ENT]
- 2.4 GHz Spectrum [PRO]
- USB HCI (1 port), UART HCI (2 ports) and SPI HCI (2 ports) [PRO]
- Logic signals [PRO]
- Audio I2S [PRO]
- Wireless Coexistence Interface 2 (WCI-2) [PRO]
- UART, SPI, I2C and SWD [PRO]

## **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
- 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: Support for new specifications without hardware changes
- Multi-Piconet Support: Visualize all topologies, including multiple piconets and scatternets
- All Protocols and Profiles: Best-of-breed protocol decoding
- I2S, within the software, in sync with all other traffic
- issues
- control and data insertion/extraction tasks.
- Free Maintenance: Free lifetime updates as well as free fully-featured viewer software with unlocked hardware that can be used on any computer

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.



• 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

Integrated Audio Analysis: Listen to captured over-the-air audio, including audio over HCI and

• Raw RF Spectrum Display: Characterize the raw wireless environment and visualize coexistence

• Automation: Ellisys provides an automation API, a CLI, and an Injection API to allow for advanced capture



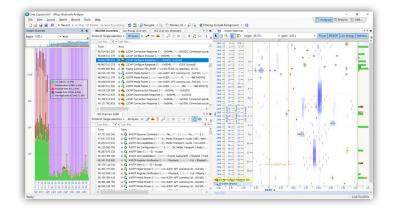


All-in-One Dual-Mode Bluetooth Protocol Analysis System

## **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.

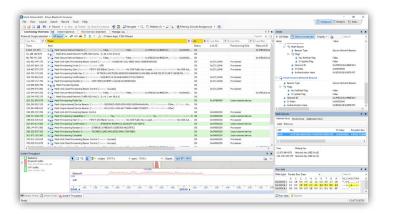
To fully characterize coexistence issues, Explorer delivers a variety of features that make this task easier. The user is provided a precise understanding of RF signatures, sources, and power, various timings, device performance indications, and other related metrics.



## **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 overview   Display 🗸		Search	
Name		Value		-
🖃 🔩 Tir	ning			
4	Start Time	31.687 654 125		
4	Duration	80 us		
4	Delta from Previous	238.50 us (0.4 slots)		
Å	T_IFS	134.500 us		- 1
•	A Packet shall be transmitted late		of previous packet	
9	Connection Interval	37.500 ms		_
9	Nominal Connection Interval	37.500 ms		
4	Connection Interval Violation	0		
4	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 Jook Help						Compleyout C Analysis	ELAN-
	🐘 🕨 Record + 11 Stop 111 Restart 16 Sove & Continue   🔮 💯   🖉 Navigate + 15, 10 Markets + 🕫 15, 1 🦉 R	Itering: Only HDS	TI, PhoneX -	3				
BR,EDR Overview					0.			
	tion + 🛛 All layers 🔶 🤤 🚮 1779 items kept, 1002 filtered 👌 WFi Security 📲 WFi Filtering: Only Lone 2.Aght, mys				Search + 19			ch
Type file V.	Type Bar	Type filter	Type filter	Y * Type filter Y		Name	Yoke	
Tame	ten	Total Length	Pratocol	Source Address	Payload	G +1 802.11 Frame		
53.804 603 000	🕱 💑 LDP/DPv4 (Crc. Addr - 192, 198, 8, 4, Src. Port - 40'537, Det. Addr - 192, 198, 0, 255, Cet. Port - 15'900)	67 bytes	LIDP	192.158.0.4	29 bytm (53 45 41 52 43 48			
54.770 839 000	a 💑 LOP/DPv4 (Src.Add = 6.0.0.0, Src.Part = 68, Crit.Add = 285, 285, 285, 285, 285, Crit.Part = 47)	336 bytes	LOP	0.0.0.0	308 bytes (010106-00 P9 1	Charvel	11	
55.440 658 000	😹 💑 19-v6 (inc. not -40/ex8/5e./fe3.e2fe3385, Cot. not -291x 200)				96 bytes (36 00 02 A1 40 40	frequency	24/2100	
\$5.779 356 000	🗑 💑 Retransmitted TCP/Pv4 (inc Add -54.231.120.186, inc Port-80, but Add - 192.168.0.11, but Port-44032, inc-3734939		TOP	54,231,129,186	2 bytes (30 06)	Prearble Type	Long	
58.060 802 000	🗑 💑 LCP/(Pv4 (Soc Addr = 6.0.0.0, Soc Part= 68, Cat Addr = 255, 255, 255, 255, 255, Cat Part= 47)	336 bytes	LOP	0.0.0.0	308 bytes (01 01 06 00 P9 1	Casta Rater	110.0	
58.475 209 000	8 💑 17-46 Çire Addi -80fest8f8e ffebre2fes8388, Cat Addi +2ffe 300)				96 bytes (86 00 02 A1 40 40	802.11 Amendment	5	
58.980 835 000	18 💑 Retransmilled TCP/DV-4 (in: Add =54.231.120.186, Sri Purt=80, Dol Add = 192.168.0.11, Dol Purt=40'287, Sec=713'512'01		TOP	54.231.130.155	2 livies (20:00)	Channel Width	2014012	
58.990 836 000	🖶 💑 TCP-data+edx(8Pv+{/vc.4dd-54.235.130.386, 5vc.Port=80, Out.4dd-190.268.8.11, Out.Port=40267, Sec=7175137313, A	40 bytes	TOP	54.231.120.196	2 bytes [30-00]	RS52	-29 dBm	
58.900 026 000	🖶 💏 QoS Data (Ind - SCI0F.00.02x85x83, Tran + Ig=Lone 2.4ghz, Rox +Cut-erynt)				No data	El 🍕 frame Control		
58.980 825 000	O, ATS (Indeltame 2.4drs, Receiverynd)				No data	<ul> <li>Type</li> </ul>	Oata	
58.991 192 000	OTS (Ind + Train-week, Rox + Coll-Lorie 2.494)				Ne deta	Sub Type	Quố Deta	
58.981 506 000	<ul> <li>Qui Data (Dist-Scill' Statization, Transico-Lane 2.4(b), Transitionen)</li> </ul>				50 bytex (AA AA 23 00 00 0	To DS	No	
58.992 480 000	<ul> <li>Ack (ind +Tram-myst, Roy +Ean-Lone 2.4ght)</li> </ul>				No data	From DS	Yes Active made	
59.025.043.000	🕷 💑 TOP data+adx/9×4 (/rc. 4xiz = 54.251,120,186, /rc. Port=60, Ont Axiz = 192, 168, 6.11, Ont Port=40.287, Sec = 7153137311, /		TOP	54 231 120 186	2 bytes (30-00)	<ul> <li>Pover Management</li> <li>More Data</li> </ul>	Active mode Yes	
8.207 424 000	🗴 🙀 TCP-deta-reds(Py+4 () = A60 = 54.235,520,386, 51 = 701 = 80, 0 = 1 A00 = 292,388,8,11, 0 = 711 = 47387, 51 = 713 = 1313 = 14, 0		TOP	54 233 120 186	2 bytes (20 00)	<ul> <li>More casa</li> </ul>	165	
58.241852000	8 🛃 TOP data +ads/8Pv4 (inc Add = 54 233, 120, 366, inc Port +80, Ont Add = 392, 588, 8, 11, Ont Port = 47367, Seq = 71373137313, I		TOP	54.231.120.196	2 bytes (30 00)	Detais Summer Meltertert Ch		
	* 🛃 TCP data+ads(Pv4 {rec Addr-54.231.130.386, Src Port-80, Dot Addr-192.388.0.11, Dot Port-40257, Sec-71351331311, J		TOP	54.231.120.106	2 bytes [30:00]	Chargene Campany Bargaron		
58.963 625 000	R 💑 TOP adu/Pv4 (Dr. Antr + 104.65, 12.9, Dr. Port + 443, Det Antr + 192, 168.6, 11, Det Port - 37378, Ad. of - 3246/2247328	52 bytes	TOP	104.65.12.9	No data	Instant Promet		
58.963 625 000								,
58.963 625 000 58.965 729 000	R 💑 TOP adu/Pv4 (Dr. Antr + 104.65, 12.9, Dr. Port + 443, Det Antr + 192, 168.6, 11, Det Port - 37378, Ad. of - 3246/2247328				No data		170	
58.563 625 000 58.565 729 000 not Taning	<ul> <li>         ★ 70% add(\$**4 ((n - 600 + 604 + 65 + 25 , (n - 1 (n + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 +</li></ul>	52 bytes			No data 24 bytes (87 00 85 44 00 00			
58.963 625 000 58.965 729 000 ot Taning	<ul> <li>▲ 10° act/0°+4 (pr. Act 104.45.12, 5, 5° c<sup>3</sup>/2 + 148.5, 112, 101.501 - 102, 108.6, 11, 101.501 - 177.77, Act 72.46724733)</li> <li>★ 4 19°-4 (pr. Act n, 101.Act 271.000.074.0000)</li> </ul>	52 bytes			No data			
58.963 625 000 58.965 729 000 ot Taning	a of To Addref Ellis And Hellis And Hellis A. Strander A. Sindaria A. Santa H. Schröder 2773, And H. Sterzerzer and A. Peterson and the Strander Strander Strander Strander A. Sindaria A. Strander 2773, And H. Sterzerzerzer To Index Schröder A. Sindaria A. Strander A. Strander Strander Strander A. Sindaria A. Strander 2773, And H. Sterzerzerzerzerzerzerzerzerzerzerzerzerze	52 bytes • Logic inputs	P P		No darta 24 bytes (87 00 85 44 00 00 Cial - S			
58.563 625 000 58.565 729 000 or Taning 29 Q. 10 10 50	a 🖌 To Alexandro Marcana Canada Cana	52 bytes	P P		No data 24 bytes (87 00 85 44 00 00			
58,563,625,000 58,565,729,000 not Tanàng C2 Q. 10 11 10 10 11 10,04,06,48,4	a 🖌 To Alexandro Marcana Canada Cana	52 bytes • Logic inputs	P P		No darta 24 bytes (87 00 85 44 00 00 Cial - S		arie.	
58.563 525 000 58.565 729 000 or Taning <b>2 Q. 11 1</b> 50 rr to us.As.enc <b>deve</b>	a 🖌 To Alexandro Marcana Canada Cana	52 bytes • Logic inputs	P P		No darta 24 bytes (87 00 85 44 00 00 Cial - S	Petert Rovet	an a	
8.963 625 000 8.965 729 000 97 Taning 7 9. 10 10 10 10 10 10 10 10 10 10 10 10 10 10 1	a 🖌 To Alexandro Marca and Alexandro Alexandr	52 bytes • Logic inputs	P P		No darta 24 bytes (87 00 85 44 00 00 Cial - S		an a	
8.963 635 000 8.965 729 000 9 9 9 9 10 10 10 10 9 9 9 10 10 10 10 10 9 9 10	a 🖌 To Alexandro Marca and Alexandro Alexandr	52 bytes • Logic inputs	P P	10465.12.9	No darta 24 bytes (87 00 85 44 00 00 Cial - S	Petert Rovet	an a	
58.563 635 000 58.565 729 000 or Taning 79 Q. 10 10 10 17 To (s. M. See) 99 19 A.	a 🖌 To Alexandro Marca and Alexandro Alexandr	52 bytes • Logic inputs	P P	10465.12.9	Ne data 24 bytes (87 00 55 44 00 00 (34 ) 3 24 co	Select Rovel	an a	
58.563 625 000 58.595 729 000 or Taning 29 Q. 10 2 50 77 50 04.46 end drevt 500 505	• A Detailer of the second	52 bytes • Logic inputs	P P	10465.12.9	Ne data 24 bytes (87 00 55 44 00 00 (34 ) 3 24 co	Relatif Romet	E C C	
8.563 635 000 8.563 729 000 9 Taning 9 Q. 8 3 1 Taning 9	a 🖌 To Alexandro Marca and Alexandro Alexandr	52 bytes • Logic inputs	P P	10465.12.9	Ne data 24 bytes (87 00 55 44 00 00 (34 ) 3 24 co	Settion Propert           Image: Million Property Source S	2 1 0 0 1 5em	n 1416789 
8.563 635 000 8.563 729 000 9 Taning 9 Q. 8 3 1 Taning 9	A Description of the second se	52 bytes • Logic inputs	P P	10465.12.9	Ne data 24 bytes (87 00 55 44 00 00 (34 ) 3 24 co	Default Flowert           Image: Second Seco	5000 6 7 8 9 0 05 00 20 0 05 00 20 20 0 50 FD 10 20 2 10 20 0 10 10 0 1	0 14167389 1.P
53.563.523.000 55.563.729.000 or Tanling 2 Q. Q. Q. Q. Q. 50. 50. 50. 50. 50. 50. 50. 50	A Declamation of the second	S2 bytes	10 <sup>9</sup>		Ne data 24 bytes (87 00 55 44 00 00 (34 ) 3 24 co	Bandari         Difference           Image: Image	Image: Control of the contro	0 1456729 
53. 563 523 000 55. 553 729 000 or Tankny <b>2 4 5</b> <b>7</b> <b>7</b> <b>7</b> <b>7</b> <b>7</b> <b>7</b> <b>7</b> <b>7</b>	A Declamation of the second	S2 bytes	10 <sup>9</sup>		Ne data 24 bytes (87 00 55 44 00 00 (34 ) 3 24 co	Better/Hunest           Image: Non-State           Image: Non-S	3         7         8         9         02           4         7         8         9         022           5         5         7         7         9         022           5         5         7 <td>0 1416739 </td>	0 1416739 
58.563 625 000 58.565 727 000 ter Tanko 20 Q. 10 Tanko 20 Z. 10 Tanko 20		S2 bytes	10 <sup>9</sup>		14 das 24 juns (27 005 44 02 00 24 juns (27 005 44 02 00 24 1 2 26 1 2 26 1 26 1	Batter Houset           Image: State of House           Image: State of House	Image: Second	ch (416739) () 
58.963.62.000 38.963.72.000 and Taning 2. Q. 1. 2. 3. 4. 3. 4. 4. 4. 4. 4. 4. 4. 4. 4. 4.		S2 bytes	10 <sup>9</sup>		10 Ges 24 Types (27 00 25 44 00 20 2 2 2 2 2 7 2 2 2 7 2 2 2 7 2 7	Better Houses           Image: State of Houses <td>Image: Second Second</td> <td>9 6) 1436739 14.5, ( 2, 6, x, 2, 6, x, 2, 6, x,</td>	Image: Second	9 6) 1436739 14.5, ( 2, 6, x, 2, 6, x, 2, 6, x,
ero Tritic cause and adjust eco ballic utilic optic automation optic cause optic cause		S2 bytes	10 <sup>9</sup>		14 das 24 juns (27 005 44 02 00 24 juns (27 005 44 02 00 24 1 2 26 1 2 26 1 26 1	Better Houses           Image: State of Houses <td>Image: Second Second</td> <td>1456789 </td>	Image: Second	1456789 

Elle View Layout Search Becord Jools Help								analysis	Add /
🔁 🥁 🙀 🥐 🕨 Record + 🗉 Stop 💷 Restart. 😽 Save & Continue	1 10 13 Nov	gate • 15 0	Markers (3) -	Filtering: Only HDST1, Laptop.	Phone, Phone2			Contraction of the second second	
BREDR Overview	11.8	an Energy Overvie			( ) ×	Willi Overview			4.1
Protocol: Single selection • All layers + 🛹 🚥 🍲 🍸 💭 🐑 🕸 🕘 🔹	12 . Proto	cot Single select	ion + All layers + +	- 48 0 5 A	12.2.4	votocol: Single select	ion • All layers •	🥆 📝 2781 kerns displayed	(4
Tupe file		ice filer	Type Ster			Type file W.*	Type filter	and the second second	
Time been	^	Time	hem		A .	Time	Item		
4.037 040 750 😹 🛳 Audio (#5CO, Transparent Data, Codec -#58C, Sanc -H2, x 13	an 11	3.793 633 375	a 'F' Advertisement (	Phone 2" 80: 34: 95: 30: 8C: FD. Scenne	"Thone" 60	57, 181 629 000	a to had forther-3.	Sed 4Tran - Hotsont, Roy 4Dat 44e-4	orie 2.4chz, P
5.027 670 375 R & Audo (eSCO, Transporent Data, Codec-e68C, Surc-H2, x 13	10	38.045 242 125	a 1 Advertisement (	Phone 2" 80:34:95:30:8C/FD, Scame	"Those" 80	\$7.406 606 000	a 4. NA Cintellion	Hotspot, Row-Date-Lone 2.4ghp	Pontr-Pow
5.042 043 625 🔒 🐁 Audo (eSCO, Transparent Data, Codec -mSBC, Sanc-H2, x 13	15)	57.840 344 375	# 1 Advertoement (	Phone2" 80:34:95:30:8C:FD, Scame	r "Phone" 80	\$7.541 140 000	4 Not God + Tran	Hotspot, Row-Oct+Ap-Lorie 2.4ghp	, Pener -Pour
6.032 673 250 🛛 🙀 🔩 Audio (eSCO, Transparent Data, Codec -et68C, Sync -H2, x 13	49	152.099 485 750	a 📳 Advertsement (	Phone 2" 80:34:95:30:80:PD, Scanne	r "Thone" 80			Stid 4 Trans-Helbpot, Rev +Dat +Ap-4	
6.047 046 500 🙀 🐁 Audio (eSCO, Transparent Data, Codec-mSBC, Sunc-H2, x 13		268.454 875 875		Phone 2' 80:34:95:30.8C/FD, Scame				ShileTran-Hobpot, Revelutedget	
7.038 926 250 😽 🔩 Audio (eSCO, Transparent Data, Codec-e686C, Sync.+H2, x 13		183.479 111 750		Phone 2" 80:34:95:30:8C:FD, Scame				432 +0.0.0.0, Sec Port-68, Cas Addr	
7.052.049 375 🙀 🐐 Audio (eSCO, Transparent Data, Color-InSBC, Sono-H2, x 12		258.055 098 500		Phone2" 80:34:95:30:80:PD, Scanne				-80fe::8f5e:ffe0:e2fe:8385, Ort Add	
8.042 679 250 🙀 🔩 Audio (eSCO, Transparent Data, Codec -mSBC, Sunc -H2, x 12		258.055 098.500		Packet (80/CS/59/E2/79/E8 > 80/34				TOP/09-4 (in: Add -54,231,120,186,	
8.057 052 375 R. S. Audo (eSCO, Transparent Data, Codec -mSBC, Since -H2, x 12		258.418 860 250	"E: Scan Reques	Packet (80:C5:59:82:79:88 > 80:34		58.982 857 000	a 4. Nul Cind+Tree	-Motapot, Roy-Ont +Ao-Lorie 2.4ch	L Power + Act
Instant Timing									
			Legic Misc + Displ						Da
HOST2" SD 14-46-46-02-	2465/2	4	1.35300 m 8.4 slot	2402	4-224,750 vs (6	4 short)			
hroutpd 2000									
Introdytok Goloria Rokko Intelso									
Yaan'a Bakkee Dooloo Do					5				_
Introdytok Goloria Rakko									_
Introdytok Goloria Rakko		(1780) 44	10.4 649		5			2000 m (),1 dag	_
Introdytok Goloria Rakko			(0.4 See) 1946 (so 240 Sync)		5		• •	2000 as (),6 dag	_
Nordez  Solo		MEDRI 34	thich iso 240 bynej						_
	jo , cin ,	MEDRI 34	thich iso 240 bynej	6 '16 '15 '			• •		
Nordez  Solo	fa ' cha	MEDRI 34	thich iso 240 bynej	a ta ta jagan	and the second			de 'sde 'sde sagaestae	54

etocols.btt - Blieys Bluetooth Analyzer					0	2
e Yew Layout Search Becord Tools Help			mylayout	🖸 Analysis 👔	Add.	
😂 🗟 🗿 🐴 🕨 Record + 🗉 Step 🕼 Restert. 🖏 Save & Continue 🔮 🎇 🏭 Navigate + 🖏 🏷 Markers (1) + 🧉	🖓 💪 🦉 Filtering: Exclude Background 🔹 😽					
R/TDR Overview Low Energy Overview HCI Overview (LSB) 🙀 Instant Spectrum 🛛 Hessage Log 🕅 HCI Overv 4 🕨 🗙	Details	8 1	Raw data			
ocol: Single selection + 🗚 layers + 🕫 🚥 📥 🖗 🔎 🐘 🎘 🗇 🔶 🧷 🕸 🖉 💷 🗇 💷 💷 🚳 🖓 🧐 💡	¥ All fields P Show in overview Display •	Search .	Data type:			
Tice fite Y Tros fite	None	Value	•	0 1 2	3 012	23
Time tern ^	# SDP Service Search Attribute Request (L2CA	P)		36 05 92 3		
100, 518 162 500 with LMP Twins Amurany Transaction (250 none. https://doi.org/	E + Reselvend Information	-43.5 dBn (Average) on channel 30		98 09 00 0 0A 00 00 0		
190, 519 412 500 * 🔂 L3CAP Information Extended Features Supported + BRTM LFCS)	R + Retransmission Information			00 09 00 0		
100, 523 (x2, 500 ) 1 He UMP Extended Features Exchange (SSP Host + SSP Host, LE Host)	H 🥐 Retransmission Information			35 03 19 1		
100.525 036 250 + 12CAP Information Found Channels Supported - Siznal   AMP   ATT   SMP	Data Retries	0		00 09 00 0		
100.525.662.375 II 🐽 L2CAP Information (Free Channels Supported - Signal (AMP)	III + Deseband Packet	LtAddr 6, DV / 3-DH1, ACL-U		35 00 35 0		
10.511 912 175 # Pt. A2MP Desiver Request	🗟 🛶 L2CAP Frame	Dist=0x0046 (SDP)		19 01 00 0		
100.531 FL2 275 E Ps. A2MP Decover Request	🗄 🛶 L2CAP SDU	Basic, 20 bytes		00 01 35 0		
	II 2 SOP FOU			19 00 01 0		
100.537 536 250 · R Azre Decaver Response				19 10 02 0		
100.538 162 125 🖷 👰 A2HP Discover Response	Transaction 20	0x0000		00 06 35 0		
100.543 786 250 🛞 🛖 L2CAP Connection (Frontbi0050, FERI-SDP + Ont-Dx0046)	11 🌱 Parameters			09 65 6X 0		
00.548 162 125 🛞 🎯 UMP Cluck Offset Transaction (Dx65F6)	🗟 🔧 ServiceSearchPattern		0x00381	00 6A 09 0	1 .1	
01.299.339.000 🔹 🎬 UMP Features Exchange (S0 Features - 40 Features)	Protocol 1	L2CAP		00 09 01 0		
01.351839.000 🕱 📽 UMP Extended Features Exchange (SSP Host, LE Host, Smultaneous LE+6R(EDR)	😑 🔩 AttributetCust			25 12 53 6		
551-403 089 000 🐨 👾 LMP Name Transaction ("ABGALLAG-MOBL3")	<ul> <li>Attribute ID</li> </ul>	All Attributes (Dv0000-CvFFFF)		72 76 69 6		
131.456 838 875 📱 📲 LMP Detach (Remote User Terminated Connection)	* SDP Service Search Attribute Response			65 20 44 6		
01.554 391 000 🛞 🍫 L2CAP Configure (3xx+0x0050, 200+1024 + 5xx+0x0046, 200) - (024)	x SOF Service Search Attribute Response			65 72 79 0		
01.556 265 000 (# 🍓 L3CAP Configure (Int - 0x0046, MTU - 1024 + Src - 0x005D)	B 2 509 POU			09 01 01 2		
01.556 890 875 👜 📭 LMP Power Control (Increment power one step + OFSI: Max power, DQPSI: Max power, 80PSI: Max power)				25 50 75 6		
131,556 890 875 Reguest Control Request (Increment power one step)	E 😚 AthibuteLists			6C 69 73 6		
01.550 014 875 # 42 LMP Power Control Response (GPSK: Max power, DOPSK: Max power, 8DPSK: Max power)	E AtributeLat 1			65 73 20 7		
01.562 515 000 😑 🥥 SDP Service Search Attribute Transfer (), 3CAPI Service Discovery Server Service Class ID L3CAP SDP Public Browse	Service Record Handle	0x00000000		65 72 76 6		
01.562 515 000 R 2 SCP Service Search Attribute Part Transaction (L2CAP: (1008 bytes)	Service Class ID List			63 65 73 2 74 67 20 7		
01.575 014875 8 2 50P Service Search Attribute Part Transaction (L2CAP: 421 bytes)	Service Class 1     H     Art Protocol Descriptor List	Service Discovery Server Service Class ID		74 67 20 1 65 60 67 3		
01.583 XH 875 🛞 🥥 SDP Service Search Attribute Transfer (LICAP) Service Discovery Service Class ID LICAP SDP Public Browse				65 20 64 6		
01.605 013 750 * 🛶 L2CAP Deconnection (Jrc -0x0050, Det -0x0046)	E *** Protocol 1	Count		76 69 63 6		
92,933 112 250 in Hig LMP Preferred Rate (In No preference, ICH - Use 3 Mors packets, Incl-Use 5-sist packets)		L2CAP 520	0x007C1	73 00 09 0	1 8	
104.620 577 125 • • • UP Peterles Asie ( in the preference, in the process, in the presence)	Pam     Protocol 2	509		02 25 03 4		
04.621 201 125 a mg UMP Detach (Remote User Terminated Connection)	Protocol	576		69 63 72 6		
04.621.201.125 a mg Die Delach (vienoral daer reminante Connection) 04.621.827.125 a mg Die Delach (Vienoral daer	R At Prose Group List	335		73 67 66 7		
	e Grave 1	Public Reavest Group		35 03 09 0		
104.873 514 875 👔 👄 Paging ('Radio2' 34:13:03:00:17 > 'Thone' 94:39:05:02:40:82, responded, 1.69 s)	Group 1	LYDer Businese munch		00 09 02 0		
105.709 917 000 👔 🍽 Paging (Unknown BD_ACOR > "MyDevice" 0C188 (PD104/83)88, responded, 3.72 s)	Generit 1	25'966		0A 00 00 0		
106.006 835 625 🙀 (8) 3nguiry (11 respondens, 20 s)	Comerc 1	23 900		OE 35 90 0		
106.576 012 875 a 🐨 UMP Features Exchange (50 Features + 51 Features)	Dement 2     Dement 3	256		00 00 04 0		
106.579 762.875 🔹 🦏 LMP Extended Features Exchange (SSP Host, LE Host + SSP Host)	Service Name	200 "Service Decovery"		01 00 00 0		
166, 581 512 790 a lia IMD Host Connection (Across Role Switch: Acrossled)	· Person have	Set the Delotty	0x00.kB:	00 01 35 0	05	5

**A**A

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

#### **One-Click Record**

7

<u>F</u>ile <u>V</u>iew

🛅 💕 🔛

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 🔹 |

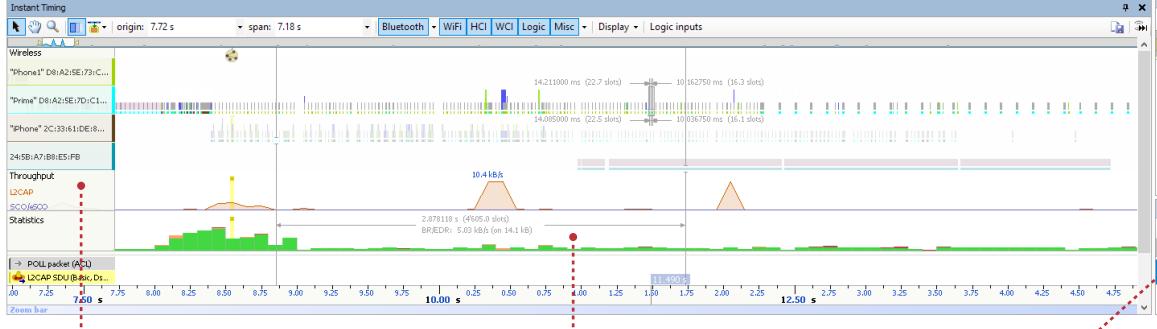
#### Instant Spectrum

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 BF	R/EDR Overview HCI Overview (Injection) Message Log HCI Overview (	[Serial)	Instant Spectrum	· · · · · · · · · · · · · · · · · · ·
ol: Single selecti	ion 🗸 🗚 layers 🖌 🚓 📾 📥 💡 🔎 🕆 🏘 🎒 🏟 🚳 🚳 🇊 (	📴 🗗 🛍 🎬 🌍 🍰 🎬 📔 🧐 😫	🖡 💽 🤍 🔍 🔲 🚡 - 🛛 origin: 8,544.24 ms	→ span: 7.18 ms     → Power BR/EDR
pe filter 🍸	▼ Type filter ▼	Type filter	2402 - 0 - 37A -	
me	ltem	Communication '	2405 3 1	•
407 372 500	🗉 🖙 LMP Channel Classification	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 4 1g - 2414 12 5 - 1g -	
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		Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	2420 - 18 - 8 -	<b>—</b> — <b>—</b> — <b>—</b>
452 996 875	🗉 🛖 L2CAP Information (Extended Features Supported)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	2423 21 3 10 2426 24 38A 4	
459 247 000	🗉 🛖 L2CAP Information (Fixed Channels Supported > ATT)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	2426 24 308 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	2435 - 2 <sup>233</sup> - 2 <sup>14</sup> - 2 <sup>14</sup> - 2 <sup>15</sup>	
472 996 875	🗉 🔶 L2CAP SDU (Basic, Dst=Fixed 0x0030)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	2438 - 236 - 516 - 5 22441 - 239 - 517 - 5	
541 122 500	🗉 🔶 L2CAP SDU (Basic, Dst=Fixed 0x0030)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla		
542 372 500	DP Service Search Attribute Transaction (PnP Information)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	2447 - 2447 - 320 - 8 8 -	
544 246 875	🕀 🛶 L2CAP SDU (Basic, Dst=Fixed 0x0030)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	2450 - 48 - 22 - 2450 - 48 - 22 - 23 - 9g -	
629 872 500	🚓 🔑 SDP Service Search Attribute Transaction (Hands-Free Audio Gateway)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	2453 - 51 - 24 2456 - 54 - 25 - 10	
667 372 500	🗄 🔶 L2CAP SDU (Basic, Dst=Fixed 0x0030)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	2430 - 54 - 25 - 10 - 2459 - 57 - 26 - 27 - 10 - 26 - 10 - 26 - 27 - 27 - 27 - 27 - 27 - 27 - 27	
669 872 625	⊕ 2 SDP Service Search Attribute Transaction (Audio Source: L2CAP AVDTP V1.3)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	2462 - 60 - 28 - 11 -	
707 372 625	🚓 👰 SDP Service Search Attribute Transfer (A/V Remote Control Target)	Master: "Phone" 2C:33:61:DE:8C:3E <-> Sla		←2,998375 ms
722 372 500	⊕ 2 SDP Service Search Attribute Transaction (IAP: L2CAP RFCOMM Ch 1)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	2471 69 31 13g	
904 872 500	🕀 🚎 LMP Authentication Transaction (02 00 00 00 13 00 00 00 02 00 00 03 00	. Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	2474 - 72 - 34 - 1	<b></b>
912 372 625	LMP Encryption Mode (Encryption > Accepted)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	2477 75 75 36 7	
915 496 750	🕀 🚎 LMP Encryption Key Size (16 bytes > Accepted)	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	😂 L2CAP SDU (Basic, Dst=Fixed 0	
916 746 750	🕀 🖀 🗓 🖕 ACL-U Flow Stop	Master: "iPhone" 2C:33:61:DE:8C:3E <-> Sla	→ POLL packet (ACL)	
.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	2,00 3,00 4,00 5,00	6.00 7.00 8.00 9.00 <b>8,550.00 ms</b>



#### **Innovative Data Groups**

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

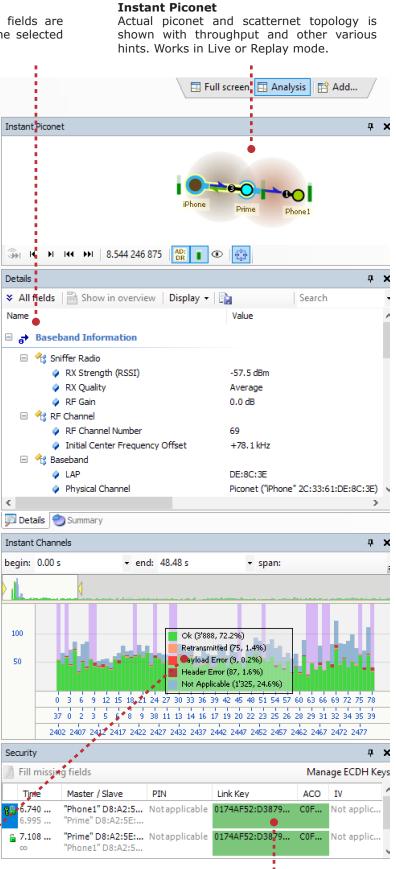
#### Instant Timing

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.



**Logic Analysis** 

is supplied.

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

The logic analysis feature allows for synchronous capture of ex-

ternal 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

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

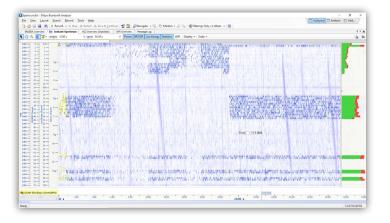
discrete signals. Users can create simple external comparators

and observe thresholds being crossed for various metrics, such a

## **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.



## Integrated Audio Analysis

The Ellisys analysis software includes integrated Audio analysis. **Any captured audio stream can be quickly and easily played back, even live, during capture.** Finding the packet carrying a specific audio portion or seeing event and topology changes at specific audio positions becomes child's play.

Audio captured over HCI or from an Audio I2S input [PRO] can be played back as well. This enables characterization of the complete audio chain, from the uncompressed audio provided to the source radio chip, to the audio transmitted wirelessly, and the decoded audio received by the receiver radio chip. The various audio streams are exportable to WAV format.

	M   D Record - II Stop (I Restart 16 Save & Con	Harris 1 22 - 22 ( Secondate + 15   C) Ma						
BR/EDR Overview			4 9 8	HCI Overview (USB				4 9 8
		) • /] 📾 👶 🕸 🗐 🗇 💷 🖓 • (	401 4.			🔑 한 분 한 속 한 🮝 📾 🔕 10 🗇 🗇 💷		11所住。
Tape filte V •					<ul> <li>Type filter</li> </ul>	3	r • Typ N	
53.208 929 250 53.578 928 875	Rem # <sup>10</sup> LMP Set APH (01 - 29, 0x000 79984, as CLX[27:0]: 0x # <sup>2</sup> AUDTP Meda Stream (100cc - SBC: Stream, 48Hz, Lo # <sup>10</sup> LMP Set APH (01 - 29, 0x000 74054, as CLX[27:0]: 0x	udness, 8 Subbands, Section – 21705.–21751, Do d1AP4004, APH enabled)		Time 50.681 911 883 51.685 663 583 52.693 159 900	응 시 AUDTP Meda Stream (Cot 응 시 AUDTP Meda Stream (Cot	<ul> <li>SBC: Stares, 48Hz, Loudness, 8 Subbands, Schum – 215</li> <li>SBC: Stares, 48Hz, Loudness, 8 Subbands, Schum – 215</li> <li>SBC: Stares, 48Hz, Loudness, 8 Subbands, Schum – 216</li> </ul>	OK	Payloac * 287041 299521 299521
	■ ALDTP Hedia Stream (Color:-SBC) Steres, 48Hz, Lo ■ ■ LMP Set AFH (Ch-30, 0x0007AGFE, as CLX227-C): 0x		/aton-940 ms)	53.715.664.983 54.733 155 236		c:-SBC: Steres, 48kHz, Loudness, 8 Subbands, Schum-217. c:-SBC: Steres, 48kHz, Loudness, 8 Subbands, Schum-217.		299521 293281
53.770 176 625 56.187 050 250 56.212 676 000 56.862 675 625 56.957 675 250	a         A. (2017) Hedda Steam (Color) - dSC (2 brees, 4 blec), to           a         DA (2 blec) AH (-1, -30, 0 block) 7400, to         SC (2 blec), and (2 blec) AH (-1, -30, 0 block) 7400, to           a         DA (2 blec) AH (-1, -30, 0 block) 7400, to         SC (2 blec), AH (-1, -30, 0 block) 7400, to         SC (2 blec), AH (-1, -30, 0 block) 7400, to           a         DA (2 blec) AH (-1, -30, 0 block) 7400, as CL (2 2 - 0), to         SC (2 blec), AH (-1, -30, 0 block) 7400, as CL (2 2 - 0), to           a         DA (2 blec) AH (-1, -30, 0 block) 7400, as CL (2 2 - 0), to         SC (2 blec), AH (-1, -30, 0 block) 7400, as CL (2 - 0), to           a         DA (2 blec) AH (-1, -30, 0 block) 7400, as CL (2 - 0), to         SC (2 blec), AH (-1, -30, 0 block) 7400, as CL (2 - 0), to	(01AFSC3C, AFH enabled) R-Use 2 Mbps packets, Prof-Use 3-slot packets) udress, 8 Subbands, Scripton-2184621892, Do		51.746.904.016 56.735.653.266 56.948.177.550 56.948.177.550 57.744.400.800 58.764.405.733 59.783.149.733	ALOTP Media Stream (Con     AL AT String:	200. Stores, SNI12, Loudress, S.S.Boards, 2010.         2010.           SIC: Stores, 494rz, Loudress, S.S.Boards, Scillan - 21%         2010.           SIC: Stores, 494rz, Loudress, S.S.Boards, Scillan - 21%         2020.           SIC: Stores, 494rz, Loudress, S.S.Boards, Scillan - 21%         2020.           SIC: Stores, 494rz, Loudress, S.S.Boards, Scillan - 21%         2020.           SIC: Stores, 494rz, Loudress, S.S.Boards, Scillan - 21%         2020.           SIC: Stores, 494rz, Loudress, S.S.Boards, Scillan - 21%         2020.           SIC: Stores, 494rz, Loudress, S.S.Boards, Scillan - 21%         2020.	0K 0K 0K	297328 t 2 bytes 12 bytes 29752 t 29752 t 297328 t
	2	• µ ⊨ ∎ ≪ 5@	<b>B</b>		*	· · · · ·		
TC" 60.82.72.63-82-67 "FORE" 10.89.45.04.59.62		- © C +  ■  =	<b>B</b>	ي فل	8	л <i>г</i>	ņ	
	2		(*)	Д 07	8	у. "д.	л	
A 20 2. ■ ■     BildER     BildER     BildER     Alson     Constant Data     Torem Located Data     Alson			Ð	д ол	8	а 2	л л	•
Control = 1     Control	* # <u>1</u>	4	Ð	a.	sh ak th	2 2 3 4 - 1/2 - 1/2 - 1/2	Д Д	. 2 de

## **HCI Analysis**

power consumption.

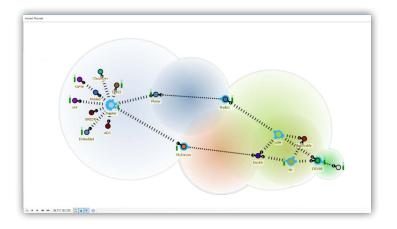
Wireless traffic is the primary element of debug information for Bluetooth engineers, but Host Controller Interface (HCI) traffic can be an equally important complement of information for getting a clear and complete picture of a given situation. Bluetooth Vanguard supports capture of HCI transports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



## **Instant Channels**

The Instant Channels 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.



Vedeos Tel Device" EtraCidSc-	1					_	_		_		_	_	9	-				_	-	_	_	-		1		_A			T					
enciencia.ex-eco	1		1	1	1			1			1	1			1	1			1							25.68.5								
CAP																																		
00600			-		_									-						-		-	_						-					
tatistics			-	_										•											÷.						_			
NeHCI													-																	271,45540	1 M.S. (404	a shore		
sk out			1			1.1	0.1		1		1	1		1	1		1	1					+					ш						
nk IN			1			1 1	1 1		1		1	1		1	1		1	1		1		1		111	11	L1	111	11	1		1			
9K																																		
IS , NESET																																		
S,SARP,I				-				4		-					-	-			-		_		μ.											
ex.												-										<u> </u>												
TK			Ψ.	_	-			_	-	-		-			-		-	-	_	-	-	-	-	1.0					ų				_	-
NAJATS												-		1.1	-		-			+														
NA_CTS									_			_			_		_			_														
NGA_TX NGA KX			-						-		-	-		-	-			_						1			11		-					
IS ONE	602	8.2	1.1.	2 60	1 0.7	100	10	00 0		2 0.2	6.7	10	02 02	62	02 0	010	0 100	60	63 0	0.1.01	1.64	1.00		1								60 60		-
JS TWO	21	81		1 01				61 0					81 85		61 0		-	91	01 0		0.5	1 444		1								0.5 0.5		
STHEE	-	-		6.0	1.44		0.0	0.0		84	0		0.0	0		8.0		10	0.0		64									121110111	151111			-
IS FOUR						1.00								61			-						- 1.9	1					-					
4			1			1.1	1		1		1	1		1	1		1			1			1	10	111		TT.	L L L						
						-	-				-	-			-		-	_					-		-									
3																																		

2DP and UART HCLbtt - Ellisys Blaetooth Analyzer						- 1	•
le Yew Layout Search Becord Tools Help				📰 mytay	out 🖸 An	elysis 📑 A	dd_ /
🗅 🤪 🔄 🙀 🔥 🕨 Record - 🗉 Stop 🔅 Restart 🗟 Save & Continue 🔮 💥 💭 Naviga	ete - 15 ( C	Markers (1) + 💭 🗛 📢	ing: Exclude Background 🔹 🐴				
BR/EDR Overview Low Energy Overview Message Log 😸 Instant Spectrum HCI Overvi	ew (Injection)	41.8	Overview (Serial)				4
tocol Single selection + 🛛 All layers 🔸 🕫 🚥 🥧 🍸 🔎 🐘 🕸 🗇 + 🎝 📾 🖏 🗇 💷	60 92 10	0.201 4.11	at Single selection + All levers + 🖉 📥 🍸 💭 🕛 🕫 🗇 🔶	A = 6 + =	0.00	03=	1. 14
	Trou V.		e fit V • Tuge fiter			Type V	
Time tem	Status	Communication ^	me bern	A	pplication	Status	Paylos
37.840 685 000 * 🐽 (3CAP Configure Chit-Ox0044 + Src-Ox0040)	ox	Hester: Lanton <-> Sk	1458 634 870 R. & SDP Service Search Attribute Transaction 0.2CAP: Audio Sir	ALICAP AVOTE VILLE S	90	OK .	28.0+5
37,851 936 250 * 4 L2CAP Connection Elec-0x0044, PER-AVCTP + Det-0x00451	OK .	Hester: Laptop <-> St	1509 886 320 R 🔍 SDP Service Search Attribute Transaction (PriP Information)			OK .	28 byt
37.862 562 250 ** 4 L3CAP Cenfoure Chit-0x0044, HTU-1017 + Src-0x0045)	ox	Master: Laptop <-> Sk	1572 447 400 🖉 🛶 L3CAP Connection (Src0x0041, PDF-HED Control + Drf-C	v0042) L3	5.43	ox	25 byt
37.663 186 375 R 🙀 L2CAP Configure (Trut-Ox0045 + Cru-Ox0044)	OK.	Haster: Lastas <-> Sk	1574 120 410 (R 🏟 L2CAP Configure (Data-0x0041, MILL+ 1017 + Sat-0x0042,		XAP	OK .	20 byt
37,964 436 000 ****** UMP Unaniff (Accepted)	OK.	Master Lantas dia Sk	. 574 800 620 🛞 🧟 HCI Write Link Supervision Timeout (Connection-Ox9049, 1	menuta 10 sl x Co. H	CT	OK .	Thute
37.983 186 875 a Au0TP Discover Command + Used-Ne, ACP+1	ox	Master: Lantan <-> Sk	1580 015 035 🗉 🛖 L2CAP Configure (011-0x0042, HTU-672 + (111-0x0041, H		XAP	OK .	20 hvf
38.032 696 625 AUDTP Get Capabilities (///P+1) + Media Transport   Audo   SBC: 48kHz	OK.	Hester: Laptop <-> St	1588 698 750 R 🐽 L2CAP Connection Elici - 0x0042, PSH-HED Internupt + Det-		CAP.	OK.	35 by
38.040 687 250 🔹 🐴 AV0TP Set Configuration (HCP = 1, TH = 52, Media Transport   Audio   58C; Joint		Master Lanton c.o.Sk	1990 143 295 . HCI Link Supervision Timeout Changed (Connection-Dx004			OK .	6.040
38.070 488 000 R A AUDTP Open (UCP - 1) + Accept	OK.	Master: Lapton <-> Si	1990 530 920 R 🏟 L2CAP Configure (Dat-0x0042, MTU - 7017, Coll-Rest 875		20.02	OK .	44 by
38, 100 687 750 (# 🐽 L2CAP Connection (Src=0x0045, PSH=AV07P + Dit=0x0046)	ox	Haster: Laptop <-> Sk	1996 266 385 R 🙀 L2CAP Configure (2011-0x0043, MRU-672 + Src-0x0042, M			ox	20 by
38, 130 065 000 + 44 12CaP Configure (Data-0x0045, 1111-11000 + (cr-dx0046)	CK.	Hester: Lastes c-2 Sk	1999 302 585 (ii) 2 HCI Soff Made (Connections OxOM), https://2.5.866.101.15		e1.	OK .	13 by
38, 131 938 250 * 4 L3CAP Configure (1)::-0x0046 + (n:-0x0045)	OK .	Haster: Laptop <-> Sk	.601 055 580 R 2 HCI Read Scan Enable + Both			OK .	3242
38.517 567 750 a Pg. UMP Preferred Rate (PEC, CH -No preference, CCH -Use 3 Mbps packets, Pref -N		Master Lantas d.h.S.	1602 468 620 a 🖉 HCI Write Scan Brable (Instin-Page)	H		ox	the
40.001 197 625 * (0) Inquiry (na regionders, 20 s)	ox	Master: Inquirer <-> 5	404 066 975 R R HCI Read Class of Device + Headket			ox.	3219
40.099 446 250 a Hig UNP Preferred Rate (TR -No preference, 1278 - Use 3 Moos packets, Pref-Use 5		Master Lantes dub Si	1505 495 900 R CI Write Class of Device (Headset)			OK .	6340
44.204 464 000 a Hig LMP Name Transaction ("Xbox Gamepad Controller 281878FA5109")	OK.	Master Lantan c-> 5	406 204 900 · () · HD Set Me (Late-Infinite)		80	OK .	23 hvt
55, 142 012 625		Master: Laptop <-> Sc	204 949 380 8 4 L2CAP Disconnection (Sco-Ox0040, Cat-Ox0041)			ox.	35 by
56.521 396 000 R Pg UMP Preferred Rate (11 -No preference, 1011 -Use 2 Mors packets, Prof-No pre		Master Lantas c.h St	1829 949 210 R 🛖 L2CAP Connection (1+c=0x0043, 1511-AV079 + 0x1-0x004			ox	16.00
60.001 204 125 · · · · · · · · · · · · · · · · · · ·	OK.	Master: Inquirer <-> 5	1832 338 255 * 4 L2CAP Configure (1+1-0x0043, 1+1++1017 + (++-0x0044)			0K	20 by
64.531 432 875 W PB UMP Preferred Rate (PDC, DR -No preference, CDR -Use 3 Mbps packets, Pref -N.,		Master: Laptop <-> Sk	1841 211 920 * 🐽 L2CAP Configure (2011-0x0044 + 201-0x0043)			OK .	35 by
78.296 146 125 B Pasino Bairnown RD ACCR > courFE CECE, no response, 20.4 c)	œ	Hester: Linknown FD /	US2 450 130 R CLCAP Connection First-du0044. Pint-du079 > Int-du004			ox.	16 by
80.001 273 125 + (0) Inquiry (2 responders, 19,3 s)	OK.	Nester: Inquirer <-> 5	154 662 565 In 🖬 L2CAP Configure ( Dx0044, 1017 + 0x0045)			00	2154
95.477 449 500 a Paging (Jirknown ED, ACCR > coc/FE-CB-CE, no response, 3.44 s)	OK .	Naster: Unknown 80.7	1863 712 835 8 4 (JCAP Configure Ent-0x0045 + Src-0x0046)			OK .	25 byt
105.818 488.000 + 2 AVDTP Start (1/2+1) + Accest	ox.	Master: Lastas <-> Si	1983 630 080 H 2 AUDTP Despire Command + Line 1-No. ACT-1			ox.	20 byt
195.847 241 500 🖷 🐴 AVOTP Media Stream (Codec-SBC: Joint Stereo, 44. Setz, Loudness, 8 Subbands, 1		Master: Laptop <-> Sk	(011 138 015 · A ANDTP Get Capabilities (ACT-1) • Media Transport   Audo			ox	11 by
105.838 494 500 m Ja AUOTP Media Stream (Codece-SBC) Joint Stereo, 44, 5442, Loudress, 8 Subbands, 1		Master Lastas <-> Sk	1041 114 720 and autory bet Conferration (102+1, 201+52, Media Transport			ox.	22 hv
107.717 247 625 · A AVOTP Heda Stream (Coder - SBC: Joint Stereo, 44, SHz, Loudness, 8 Subbands, 1		Master: Laptop <-> Si	(071 140 500 # 4 AVDTP Open (1/2P - 1) + Accept			OK.	11 by
108.229 749 250 a 21 AVOTP Hedia Stream (Coder - 58C; Joint Stereo, 44, Urb, Loudress, 8 Subbands, 1		Mester: Laplag <> Si	1001 198 880 (III 4 L2CAP Connection Circ-0x0045, PSH - AV07P + Dot-0x004			ox.	15 by
199, 229 749 250 III A AVOTP Hedia Stream (Linter - SBC) Joint Starteo, 44, 1947, Loudress, 8 Subbands, 1 199, 209 753 250 III A AVOTP Hedia Stream (Linter - SBC) Joint Starteo, 44, 1947, Loudress, 8 Subbands, 1		Haster: Laptop <-> Si	L302 961 200 H 🙀 L2CAP Confector (211-0x0045, 151-140047, 151-0x0046)		X.AP X.AP	OK.	20 by
130.235 508 000 a 🖓 AllOTP Meda Stream (Color-SBC: John Stereo, 44, Druchess, 6 Subbards, 1		Master: Laptop <-> Sk	L132 448 805 H 🛶 L2CAP Configure (Ditt-De0046 + Drc-De0045)			OK .	25 by
111.238 514 500 a A AVOTP Heda Stream (Liner-SBC) John Steres, 44, SHD, Loudness, 8 Subbands, 1 111.238 514 500 a A AVOTP Heda Stream (Liner-SBC) John Steres, 44, SHD, Loudness, 8 Subbands, 1		Matter: Laptop <-> Si Matter: Laptop <-> Si	L32 We dos a we L2CAP Configure (111-0x00H6 + 31C-0x00H5) L352 299 065 a + HCI Number Of Completed Packets (Connection-Ox00H9, II			OK OK	25 OY
112.243 519 375 H AL AVOTP Media Stream (Concer SBC: John Stereo, 44, 5Hz, Loudress, 6 Subbands, 1		Master: Laptop <-> Si	Los 297 510 V UART Seeo Hessage			ox.	
112.240 Stir 3/5 a V1 AVOTP Heda Stream (Licori - SSC: Joint Stereo, 44, Shta, Loudress, 8 Subbands, 1 113.258 S21 125 a V1 AVOTP Heda Stream (Licori - SSC: Joint Stereo, 44, Shta, Loudress, 8 Subbands, 1		Master: Laptop <-> Si Master: Laptop <-> Si	5.819-099 VART Welcup Message		art let	OK.	
113.230 521 125 III 24 AVOIP Hedia Stream (Local Soci Jord Stereo, 44, DHz, Loudress, 8 Subbards, 114.282 276 125 III 47 AVOIP Hedia Stream (Local - SBC) Joint Stereo, 44, SHz, Loudress, 8 Subbards, 1		Master: Laptop <> St Master: Laptop <> St	5.819 368 X LIART Weinup Message			OK	
115 080 200 120 PT AUDIT Netla Grean (Colors OF) bord Green, dd Litter ( outress, 8 Schlavds,		Mester: Lantan <-> Si. Y	K A15 540 V LIAST Linker Message		ar.	ox.	
C		3					



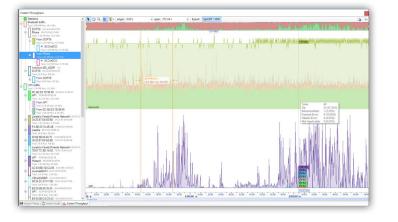


**Ellisys Bluetooth Explorer**<sup>™</sup> All-in-One Dual-Mode Bluetooth Protocol Analysis System

## **Instant Throughput**

Understanding device data throughout performance is a common task for wireless engineers. These metrics are the domain of the Instant Throughput view, which **provides throughput by device and by L2CAP or SCO/eSCO channel and Wi-Fi communications.** A convenient statistical overlay provides information on how various transmission inefficiencies may be affecting throughput, such as packet retransmissions.

Each device and channel is color-coded and can be shown or not shown as the user may prefer. A navigation bar is provided to allow the user to select a time range to pan through the entire capture to see trends, as well as high and low peaks on data throughput.



## **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.

## **Configurations and Purchase Information**

Radio Configuration	EDR	LE	DUAL
BR/EDR Capture	x		x
Low Energy Capture		x	x
Editions	Standard	Pro	Enterprise
Wideband Bluetooth Capture	x	x	x
HCI Capture		x	x
Logic Capture		x	x
I2C, UART, SPI, SWD Capture		x	x
Spectrum Capture		x	x
Audio I2S Capture		x	x
WCI-2 Capture		x	x
Wi-Fi 802.11 a/b/g/n Capture			x
Warranty	2 years	2 years	3 years

## Description

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 Enterprise Dual Mode Ellisys Bluetooth Explorer 400 Enterprise Dual Mode Ellisys Bluetooth Explorer 400 Enterprise Dual Mode Ellisys Bluetooth Explorer 400 Enterprise Dual Mode



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

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



## **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
- Channel width 5GHz: 20MHz or 40MHz
- I1n MCS 2.4GHz 20MHz channel: 0 to 15
- I1n 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

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

Copyright© 2020 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 SIG, Inc. and any use of such marks by Ellisys is under license. Wi-Fl® and the Wi-Fl Alliance. Other trademarks and words of the trademarks are those of their respective owners. All other trademarks are owned 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 warrenty of any kind, either express or implical. Pettures in this publication are for illustration only: actual products may differ.

#### 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

## **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



#### 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

## 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® 7 or higher .net framework 4.6.1

