Separating the Wheat from the Chaff

Introduction

ellisys

Better Analysis.

Bluetooth topologies are becoming increasingly complex as the technology evolves and new, more sophisticated applications begin to appear. Busy lab environments or public testing events (like UPFs) can involve dozens or even hundreds of devices, all active at the same time.

The BEX400 Explorer Instant Protocol Analysis System is uniquely designed to capture all *Bluetooth* traffic in the vicinity, including all piconets and scatternets as well as unsynchronized traffic like pagings and inquiries.

But how does one isolate this traffic and pinpoint only those communications of interest? To meet this challenge, the BEX400 software includes no less than seven powerful filtering approaches available for real-time capturing and post-capture analysis, as well as a searchable, editable device database.

This paper will walk the user through the process of using the powerful *Device Traffic Filter* and associated **Device Database**, and will touch on usage applications for other filter mechanisms.

Creating Specific Criteria Using the Device Traffic Filter

The *Instant Piconet* figure below shows a moderately busy *Bluetooth* environment. At a glance, we can see about 18 piconets, the formation of a scatternet, some data transfers, and paging events. This traffic is also represented in various other panes, such as the *Instant Timing* pane and the *Overview*.





Now, what if we just want to see the communications between two *Bluetooth* devices or all traffic involving a particular device, and not just in the *Instant Piconet* pane, but globally, <u>throughout all panes in the BEX400 application</u>? There are a few ways to do this actually, such as use of *Instant Filtering* in the *Overview*, but let's use the *Device Traffic Filter* in this case, accessible from the Tool Bar as shown below:



Here's what we see when we open the *Device Traffic Filter* (below). We have a **Device Database** along with a **Traffic Filtering Criteria** tab, where we can define precisely what is displayed throughout the various panes in the application.

Device Traffic Filters							(
Traffic Filtering Criteria		Device Database					
Exclude Background	- 🛛 🗮 Clear 🗞 Add	<u>N</u> ew Device <u> E</u> dit 📗 De	lete Search:	V	iew: All Devices 👻		
Name	 Radio 	Name	BD_ADDR	Radio L	MP Name	Company ID	*
		Mecel	00:15:83:32:A6:8A	Classic M	Aecel	IVT corporation	
		mg2IAS	00:22:58:00:C8:8A	Classic n	ng2TAS	Taivo Yuden Co., Ltd.	
		mot t	7C:8E:E4:34:D6:CD	Classic n	nott	Texas Instruments	
		MR 10LAP02	00:1E:37:9F:F8:7E	Classic N	IR 10LAP02	Universal Global Scie	
		MT6276	43:55:0D:22:62:76	Classic N	116276		
		MTK 2	EE:49:46:66:20:91	Classic N	/TK 2		
		💵 📕 MyDevice	08:00:28:0E:B4:B0	Classic F	ull Android on Blaze	Texas Instruments	
		🐵 🔳 Nokia 303	AC:81:F3:82:EE:D7	Classic N	lokia 303	Nokia Corporation	
		🐵 🔳 Nokia 6220 classic 1	00:1F:01:91:87:C1	Classic N	lokia 6220 classic1	Nokia Danmark A/S	
		🔳 Nokia N8-00	E0:A6:70:C8:64:42	Classic N	lokia N8-00	Nokia Corporation	
		🐵 🔳 Nokia-01	AC:81:F3:82:EE:B4	Classic N	lokia-01	Nokia Corporation	
		···· 📕 Nokia-10	AC:81:F3:34:E4:E0	Classic N	lokia-10	Nokia Corporation	
		🐵 📕 Parrot_2	38:3A:AE:87:72:22	Classic P	arrot_2		
		🖶 📕 Parrot1	20:07:19:81:11:11	Classic P	arrot1		
		PARROT-PC-BLUES	E8:39:DF:04:B8:71	Classic P	ARROT-PC-BLUES	Askey Computer	
		PATMIF8T0ZD 1XPL	00:1A:6B:E5:65:00	Classic P	ATMIF8T0ZD 1XPL	Universal Global Scie	
		🕂 🔳 Ррррр	1F:30:CD:E9:62:76	Classic F	pppp		
		PTS-MAP-TECHTLP022	00:80:98:E7:31:4C	Classic F	TS-MAP-TECHTLP022	TDK CORPORATION	
		🗄 📕 Ram Laptop	90:4C:E5:DE:0D:C7	Classic F	lam Laptop	Hon Hai Precision Ind	
		🖶 📕 Roland Labana - QINT07	58:B0:35:7A:3A:D0	Classic F	toland Labana - QIN	Apple, Inc	
		SCH-I110	12:47:BF:A5:4B:D5	Classic S	CH-I110		
			00.01.02.71.00.44	Changie 6		Universal Clabal Cris	
					OK	Cancel	Apply

The database will display all devices captured historically <u>and</u> devices captured in the current trace, as well as a list of the communications established between them.

Let's create criteria where we show all traffic involving a device we've renamed as "**MyDevice**." All we'll need to do is to locate **MyDevice** in the **Device Database**, and add it to the **Traffic Filtering Criteria**.

Here's a couple of helpful hints - you can use the **Search** box to locate any text string in the various columns in the database. You can also click on the column headers to sort any column.



OK, so we double-click **MyDevice** and it's now added to the *Traffic Filtering Criteria*. Notice that **MyDevice** is added under the label "Keep Involving Selected Devices." This means that we will now see *only* traffic involving **MyDevice**, and everything else will be hidden in every pane in the application.

Device Traffic Filters							E
Traffic Filtering Criteria	Device Datab	base					
Keep Involving Selected Devices	<u>N</u> ew De	evice <u> E</u> dit 📗 <u>D</u> elete	Search:		View: All Devices 👻		
Name ^ Radio	Nam	ne BC	D_ADDR	Radio	LMP Name	Company ID	*
"MyDevice" 08:00:28:0E:B4:B0 Classic	Here Med	el	00:15:83:32:A6:8A	Classic	Mecel	IVT corporation	
		TAS	00:22:58:00:C8:8A	Classic	maZIAS	Taivo Yuden Co., I td.	
	mot	t :	7C:8E:E4:34:D6:CD	Classic	mott	Texas Instruments	
	🕀 🔳 MR1	10LAP02	00:1E:37:9F:F8:7E	Classic	MR 10LAP02	Universal Global Scie	
	— 🔳 МТ6	276	43:55:0D:22:62:76	Classic	MT6276		
	🗼 🗖 МТК	2	EE:49:46:66:20:91	Classic	MTK 2		
	🖃 📕 MyD	Device	08:00:28:0E:B4:B0	Classic	Full Android on Blaze	Texas Instruments	
	··· 🔳 U	JConnect	00:0E:9F:5E:12:A3	Classic	UConnect	TEMIC SDS GmbH	
	🔳 T	arang	C8:97:9F:7B:EE:33	Classic	Tarang	Nokia Corporation	
	📕 Y	ourDevice	00:02:58:03:0E:BC	Classic	USD78WVLL1	Cambridge Silicon Radio	
	🔳 S	CH-I110	12:47:8F:A5:48:D5	Classic	SCH-I110		
	🗷 💼 🔳 Noki	ia 303	AC:81:F3:82:EE:D7	Classic	Nokia 303	Nokia Corporation	
	🗈 🔳 Noki	ia 6220 classic1	00:1F:01:91:87:C1	Classic	Nokia 6220 dassic1	Nokia Danmark A/S	
	🔳 Noki	ia N8-00	E0:A6:70:C8:64:42	Classic	Nokia N8-00	Nokia Corporation	
	😟 🔳 Noki	ia-01	AC:81:F3:82:EE:B4	Classic	Nokia-01	Nokia Corporation	
	📕 Noki	ia-10	AC:81:F3:34:E4:E0	Classic	Nokia-10	Nokia Corporation	
	🗄 📕 Parr	rot_2	38:3A:AE:87:72:22	Classic	Parrot_2		
	🖻 📕 Parr	rot1	20:07:19:81:11:11	Classic	Parrot1		
	🖻 🔳 PAR	ROT-PC-BLUES	E8:39:DF:04:B8:71	Classic	PARROT-PC-BLUES	Askey Computer	
	🕒 🔳 PAT	MIF8T0ZD 1XPL	00:1A:6B:E5:65:00	Classic	PATMIF8T0ZD 1XPL	Universal Global Scie	
	🗄 🔳 Ppp	pp	1F:30:CD:E9:62:76	Classic	Ррррр		<u> </u>
	📖 🔲 пте	MAD TECUTI DOOD	00.00.00.27.21.40	Classic	DTC MAD TECUTI DOOD		
					ОК	Cancel	Apply

So, what began as a fairly large capture with about 40 devices is now reduced throughout the application's panes to **MyDevice** and the corresponding traffic with the four devices it has communicated with in this capture.

Here's an added bonus: you can now save this filtered version of the capture to exclude all but the filtering criteria (File menu/Save Filtered Copy), greatly reducing the file size!

Now, what if I want to see traffic between **MyDevice** and **YourDevice**, as opposed to **MyDevice** and all other devices communicating with **MyDevice** as we discussed above?

No problem, except this time, we'll add YourDevice to the *Traffic Filtering Criteria* as shown below.

ffic Filtering Criteria		Device Database					
eep Only Selected Devices 🔹	💢 Remove 놓 Add	<u>N</u> ew Device 📝 <u>E</u> dit	Delete Search: my,you	ur	View: All Devices 👻		
Name	Radio	Name	BD_ADDR	Radio	LMP Name	Company ID	
"MyDevice" 08:00:28:0E:B4:B0 "YourDevice" 00:02:5B:03:0E:BC	Classic 📄	E- Laptop	00:21:86:71:38:A4 00:22:58:41:14:77	Classic	SOWMYA_LAPTOP	Universal Global Scie Taivo Yuden Co Ltd.	
	classic	MyDevice	08:00:28:0E:B4:B0	Classic	Full Android on Blaze	Texas Instruments	
		🕀 📕 MyDeviceY	00:22:58:41:14:77	Classic	IAS	Taiyo Yuden Co., Ltd.	
		🖳 📕 My Android Phone	22:22:BE:D4:E1:8A	Classic	My Android Phone		
		My Android Phone	22:22:FF:FF:7D:DE	Classic	My Android Phone		
		My Blackberry	30:7C:30:EC:17:08	Classic	BlackBerry 9550	RIM	
		My Car	00:09:93:20:00:01	Classic	My Car	Visteon Corporation	
		MyDeviceZ	00:01:60:91:07:8A	Classic	TAS	Taivo Yuden Co., Ltd	
		YourDevice	00:02:5B:03:0E:BC	Classic	USD78WVLL1	Cambridge Silicon Radio	
						,	



Note that even though **MyDevice** and **YourDevice** are communicating to other devices, these other devices are hidden; only communications between **MyDevice** and **YourDevice** are left in the application's panes. Note also that the drop-down in the *Traffic Filtering Criteria* now updates to show "Keep Only Selected Devices."

Another helpful hint: The **Search** box is using a comma to AND devices name beginning with "My" and "Your."

Here's a look at the *Instant Piconet* pane <u>after</u> the filter has been applied:



A global look at the application gives a better perspective on the before and after effects:

Before:

	ooth Analyzer									
Wew Layout Search F	Record Tools Help								myLayout 🔝 Full screen 🗔	Analysis 🛛 🔛 Add /
🧉 🛃 📓 👬 🛛 🕨 Reo	ord - 🗉 Stop 💷 Restart 🔮 🏥 🚚 Navigate	- 🖏 🗋 Markers (2) - 🔎 🔩 🏹 Filtering: Keep Al	- 🎯 📱							
Welcome CRD /FDD Ove	nview C Low Energy Overview C HCI Overview		- 10			d b	Instant Piconet			
nod: Socie selection + All las		🖻 🕅 🦳 🚱 🍰 🖳 🚥 🍈 🛛 7015 itame devlavad				l Search •		🔘 🧑 < 🛑 📘		
Tures filter	V a Viene Blass	V a Van Alan	V - Yours 6	V - Vine River V - V	was films			Parrot_2 SCH-E110	ANDROID BT	0 0
rype inter	• • Type men	• • Type noe	• Type I	Type meet	ype mer					BlackBoury 9270
Time	Item	Communication	Originato	r Status	Payload				Q	charbenty 2010
189.341 295 750	E L2CAP Configure (0x0041, 0x0041)	 Master, "YourDevice" 00:02:58:03:0E: 	3C <-> Slave, "MyDevice" 08:0 Master	OK			0.	•	TONALITE HS	
189.342 545 750	ID packet (ACL, 1 Mbps)	Master, "YourDevice" 00:02:58:03:0E:	3C <-> Slave, Unknown Master	OK				2		
189.343 171 500	L2CAP Configure (0x0041, 0x0041)	 Master, "YourDevice" 00:02:58:03:0E: 	3C <-> Slave, "MyDevice" 08:0 Slave	OK				1	1.	
.89.368 1/1 /50	Recomm Connect (Channel-Signal	aing) Master, Tourbevice 00:02:58:03:06:	3C <-> slave, MyDevice Usio slave	UK			1		mot t*	
89.422939375	Paging (SCH-1110" 12:47/8F:A5:4	HB:D5 > Parrot Master, 'SCH-1110' 12:47:BF:A5:4B:D	5 <-> Slave, "Parrot_2" 38:3A: Master	OK					ŝ	
89.446 295 750	Recommunic Parameter Negotab	on (Initial Credits - R. Master, Tourbevice 00:02:58:03:0E:	3C <-> slave, MyDevice U8:0 slave	No Request Fro				Delphi 1		
89.490 921 375	Recommission (channelling)	Master, TourDevice 00:02:58:03:0E	SC <-> Slave, MyDevice US:0 Slave	OK						20
39.510 045 625	COMM Modelli Status	Master, Tourbevice 00:02:58:03:06:	C < > Slave, Hypevice 08:0 Haster	OK OK						
39, 330 071 300	AT LED Conserved Errors AT 17	master, fourDevice 00:02:58:03:02: PCE=20: + Inter, "YourDevice" 00:02:78:03:02:	PC <-> Slave, hypevide 08:0 Slave	OK OK			Nokis	er.	e	
89 500 471 750	A 1 1 - Supported Peatures: A1 + C A 1 - CAP Connection (0-00-2 - 0-00-2	42: AUDTR) Marter, YourDevice, 00:02:58:03:06:	RC <-> Since "McDexice" 08:0 Plaster	OK.					Debu 5	eel
09,099 121 200 90 601 005 500	(Contraction (Contraction (Contraction))	Condita-Tel 1 Master "YourDevice" 00:02:58:03:061	PC <-> Slave, Hypevide U810 Slave	OK I	No data			0460 TYT HF	SYSTEM	mg21AS
99 641 207 250	AT String: OK Line	Marter "YourDevice" 00:02:55:03:02:	RC <-> Since, hyperide 08:0 Master		4 buter (41 48 00 04)		•	OSHIBA LSI		
30.645.045.500	Al parties on 11 Al parties on 11 Al parties on 1000000 000000	Master, YourDevice 00:02:58:03:06:	RC <-> Slave "MyDevice 00:0 Slave	OK .	To your (T TO OD ON)		2			
99.645.071.750		master, fourDevice 00:02:58:03:0E	PC <-> Slave, hyperide 08:0 Master	OK.			1	14		
99.000 921 230	T C2CAP Comigare (0x0042, 0x0042	 Master, Tourbevice Orio2:58:03:06: Master, Tourbevice Orio2:58:03:06: 	SC CH3 Slave, Hydevice Usio Slave	OK OK			A	Ň.	• •••	
9 200 045 275	AT ME BreakBeaching AT ACMED	=2.0.0 files kills OK Master, "YourDevice" 00:02:50:03:05:	PC <-> Slave, MyDevice 0010111 Master	OK.			Q 1		-	•
9.700 045 375	a CAR Commention (0-0042, 0-004	 Solo, D. 1 - Control Master, Tourbevice 00:02:58:03:06: 42: AVCTO Master, Neuropevice 00:02:58:03:06: 	C < > Slave, Hypevice 08:0 Haster	OK OK			AyDeviceZ			
39.700 071 375	AUDTR Discours Command + Lind-	-No ACR-1 Master, "YourDevice" 00:02:58:03:06:	PC <-> Slave, MyDevice 08:0 Slave	OK OK				00:27:13:9A:BB:E:	HandsFreeUnk	
9 726 295 000	R CAP Parameter Lindate Toronol	lata Master, "YourDevice" 00:02:58:03:08:	BC <-> Slave, MyDevice 00.0 Slave	No Personne Er			•		1.0	iPhone -
55.726 255 000	E2CAP Parameter opdate, Incomp (2) 00044, 0x000	Adv 2) Tecomolete Master, "YourDevice 00:02:35:03:05:	PC < > Slave, MyDevice 08:0 Master	No Response Pr				.		
39.734 921 373	R + 12CAP Linknown Command 0x24	Master, "YourDevice" 00:02:58:02:06:	PC <-> Slave, Hypevice 00.0 Hastel	OK OK	19 huter (24 00 58 09 40 00 44					
0 700 171 250	(2) + 12CAD Careforer (0+0044, 0+0044	Naster, YourDevice 00:02:58:02:0E:	PC < > Clause "McDanise" (ReD	OK .	15 07425 (2100 52 00 10 00 11				• • • • • • • • • • • • • • • • • • •	
99 739 431 275	(a) A ANDER CatCoophilities (ACR-1) + C	To abilities Media Master, "YourDevice" 00:02:50:03:05:	PC <-> Slave, Hypevice 00.0 Slave	OK OK			🛸 н н не	₩ 189.670 045 500	AD: DR	
89 743 795 500	REPAIR AND POLICIPAL AND A CONTRACT OF	Cracity-I: +1+1 Marter, "YourDevice" 00:02:58:03:0E:	BC <-> Slave, "MyDevice" 08:0 Marter	OK I	No data		🗊 Details 🕙 Sum	mary 😪 Instant Piconet		
90 700 421 125	AVDTR SetConfiguration (ACR-1)	BIT-1 Canadaliti Master, "YourDevice" 00:02:58:02:05:	PC <-> Share, "MyDevice" 08x0 Sinua	OK I	10 000		Constitu		-	
89 810 045 375	AVDTP Second guided (NOT - 1, 1	mantafied Packet) Master, "YourDevice" 00:02:58:03:08:	BC <-> Slave, "MyDevice" 08:0 Marter	OK 1	13 huter (A7 09 1E 69 A9 15 2E		becomy			
90 921 021 125	(i) c 12CAD Coofe ve (0x0044 2) Terr	melata Master "YourDevice" 00:02:58:02:0E:	PC <-> Share, "MyDerice" 08x0 Master	No Demunst Ere	100740747071200707102		Manage SSP Keys			
99.921 921 123	ID packet (ACL_1 Mbor)	Master mo2165" 00:22:58:00:C8:84	Constant Server Server Server Master	OK OK			Time	Master / Slave	PIN Link Key	ACO
89 918 171 125	AVDTP Onen (ACP-1) > Accent	Master, "YourDesize" 00-02-58-03-0E-	BC <-> Slave "McDevice" 08-0 Slave	OK			6.077 990 500	"Delphi 2" 00:22:A0:	Not applic Not applicable	Missing
19.910 1/1 125	a ve work open (nor - 1) viccept	Mastery Tourberice 00.02.30.03.02.	AC CONSIGNED, HYDEVICE USION, Slave	UN			27.349 250 500	"0460 TYT HF SYSTE		
Timing						4 X	8a 34.960 195 250 92 308 888 125	"YourDevice" 00:02: "MyDevice" 08:00:2	Not applic Missing	Missing
/ 🔍 🔳 🚡 🔹 origin:	184.50 s • span: 8.03 s	• Display •					02 270 500 750	"mo2165" 00:22:59:	Not applic Not applicable	Natapolicable
2* 001221A010010			. 😌 .				244.454 095 250	Unknown	Not applican Not applicable	wocoppricable
					-		PA 99.097 579 750	"Delphi 2" 00:22:A0:	Not applic Not applicable	Missing
ice" 08:00:28:0E:							100.506 330 500	"0460 TYT HF SYSTE		
				i sul a su su			100.769 458 250	"Delphi 2" 00:22:A0:	Not applic Missing	Notapplicable
avice" 00:02:58:0		i i i i i i i i i i i i i i i i i i i	ander and a constants of all tail the should	e o de la site de secondes			218,842 149 500	"0460 TYT HF SYSTE		
							116.323 866 000	"YourDevice" 00:02:	Not applic Missing	Notapplicable
AP-TECHTLP022"							132.581 699 625	MyDevice 08:00:2		
							138,600,454,625	"YourDevice" 00:02: "MyDavica" 08:00:2	Not applic Missing	Missing
0101102105							138 671 344 350	"YourDevice" 00:0012:	Not soplic Missing	Notapplicable
C100-22-58-00-C							164.916 997 625	"MyDevice" 08:00:2	Hor opplication the stand	Nocapplicable
	na dan diana kana dan ang dan ang dalam (ang dalam				in the main function of the second		Re 147.190 193 250	"Parrot1" 20:07:19:	Not applic Missing	Notapplicable
110" 12:47:8F:AS:	17.1. June 17. (D.D.)						147.713 148 375	"ANDROID BT" 7E:B		
AT I	HILLINGCODE WT+CIND/W> WI+CIND: 1,0,0,0,5,0,2W/W/W	CATE					A 147.724 399 375	"ANDROID BT" 7E:B	Not applic Missing	Notapplicable
The second	n	a at the second se		0 00 00	01.00					

©Ellisys 2012. Information contained herein is for illustrative purposes and is not intended in any way to be used as a design reference. Readers should refer to the latest technical specifications for specific design guidance. Ellisys – Chemin Du Grand Puits 38 – CH1217 Meyrin – Geneva +41 22 77 777 89 (USA +1 866-724 -9185) www.ellisys.com.



After:

	ecoon Analyze								
Vew Layout Sea	rch Record Tools Help						🖃 myLayout 📑 Full :	creen 🖪 Analysis	🔛 Add /
🥁 🔛 💹 i 👫 i	🕨 Record 🔹 🗏 Stop 🖾 Restart 🐩 🎇 💭 Navigate 🔹 🖾 🛅 Markers (2) 🔹 🤞	🖓 🗣 🛛 🖓 Filtering: Only YourDevice, MyDevice 🔹 🛛 🧒 👳							
Welcome BR/ED	R Overview Low Energy Overview HCI Overview				4 Þ	Instant Piconet			5
col: Single selection •	Allayers 🗧 🛹 👄 🍐 🔎 🏁 📾 🚳 🥮 🚸 🎝 🗊 🗇 🥸 💑 🖯 👑	🐑 770 items displayed			Search -				
ype filter	V • Type filter	 Type filter 	V • Type f V	Type filter	Y - Type filter				
ime	Item	Communication	Originator	Status	Pavload ^				
32,592,599,625	Big LNP PacketType Table (Accepted)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:84:80	Master	OK					
32.620 100 375	H GR LMP Set AFH	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MvDevice" 08:00:28:0E:84:80	Master	OK					
32,650 100 250	99 LMP Channel Classification Request (AFH Reporting Enabled)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MvDevice" 08:00:28:0E:84:80	Master	ок	E				
32,656 350 250	GR LMP Authentication Transaction	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MvDevice" 08:00:28:0E:84:80	Master	OK					
32.692 601 250	See LMP Engryption Mode (Accepted)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MvDevice" 08:00:28:0E:84:80	Master	OK					
132.715 100 250	Generation Key Size (Accepted)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0	Master	OK					
132.758 850 250	See LMP Start Encryption	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:84:80	Master	No Response From Slave					
132,759 476 125	Ar Encrypted Traffic (x 480)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0	Slave	ок					
137.899 205 250	Paging ("MyDevice" 08:00:28:0E:B4:B0 > "YourDevice" 00:02:58:03:0E:E	IC) Master, "MyDevice" 08:00:28:0E:B4:B0 <-> Slave, "YourDevice" 00:02:58:03:0E:BC	Master	OK			MuDavice		
138.401 705 625		Master, "MyDevice" 08:00:28:0E:B4:B0 <-> Slave, "YourDevice" 00:02:58:03:0E:BC	Master	No Response From Slave			9	1	
138.416 079 875	Wersion Exchange (Master: 4.0, Slave: 2.0)	Master, "MyDevice" 08:00:28:0E:B4:B0 <-> Slave, "YourDevice" 00:02:58:03:0E:BC	Slave	OK					
138.439 829 875	See LMP Role Switch (Accepted)	Master, "MyDevice" 08:00:28:0E:B4:B0 <-> Slave, "YourDevice" 00:02:58:03:0E:BC	Slave	ОК			Touce	sice	
138.599 204 625	FHS (YourDevice) packet (ACL, 1 Mbps)	Master, "MyDevice" 08:00:28:0E:B4:B0 <-> Slave, "YourDevice" 00:02:58:03:0E:BC	Slave	OK	20 bytes (17 D5 3A E4 F				
138.600 454 625	FHS (YourDevice) packet (ACL, 1 Mbps)	Master, "MyDevice" 08:00:28:0E:B4:B0 <-> Slave, "YourDevice" 00:02:5B:03:0E:BC	Slave	OK	20 bytes (17 D5 3A E4 F				
138.601 079 500	ID packet (ACL, 1 Mbps)	Master, "MyDevice" 08:00:28:0E:84:80 <-> Slave, "YourDevice" 00:02:58:03:0E:8C	Master	OK					
138.610 093 500	KIMP Host Connection	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0	Slave	No Request From Slave					
38.611 344 625	Begg LMP PacketType Table (Accepted)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0	Master	OK					
38.611 969 625	geometry LMP Setup Complete	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0	Slave	No Response From Master	r i i i i i i i i i i i i i i i i i i i				
38.638 844 375	Set APH	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:84:80	Master	OK					
138.668 844 375	IMP Channel Classification Request (AFH Reporting Enabled)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0	Master	OK					
38.671 344 250	George LMP Authentication Transaction	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:84:80	Master	OK					
38.715 094 250	Mege LMP Encryption Mode (Accepted)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:84:B0	Master	ОК		🛸 н н не т	H 138.596 705 125 AD: 0	Ð	
138.725 094 250	General Content of the state of the sta	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0	Master	OK		Datale Cum	ary 🙆 Instant Biospat		
138.776 344 375	Spectral EMP Start Encryption	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0	Master	No Response From Slave			ary was a source to the		
138.783 220 750	🕀 👷 Unknown LMP Message	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0	Slave	No Request From Slave		Security			
138.788 844 250		Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:84:80	Master	OK		Manage SSP Keys			
138.791 344 250	🙉 🛶 L2CAP SDU (Basic, Dest=0x8F36)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0	Master	OK		Time	Master / Slave PIN	Link Key	ACO
138.791 970 375	Geg Unknown LMP Message	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0	Slave	OK		34.960 195 250	"YourDevice" 00 Not applie	Missing	Missing
138.793 844 250	🗉 🛶 L2CAP SDU (Basic, Dest=0x14D7)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0	Master	OK		92,308 888 125	"MyDevice" 08:		
138.794 469 625	B 🎃 L2CAP C-Frame (ACL-U Flow Events)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0	Slave	OK		8 116.323 866 000	"YourDevice" 00 Not applie	Missing	Not applic
•						132.581 699 625	"MyDevice" 08:		
t Timing					0 X	132.675 726 250 138.600 454 625	"YourDevice" 00 Not applie "MyDevice" 08:	Missing	Missing
🎾 🔍 🔳 🚡 🖓	igin: 138,590.91 ms • span: 20.01 ms • Display • 📓					138,671 344 250	"YourDevice" 00 Not applie	Missing	Not applic
55	6					164.916 997 625	"MyDevice" 08:		
wice" 08:00:28:0E:						8 164.991 319 500	"YourDevice" 00 0000	22D28102:223F	3DD826D0
						187.633 229 625	"MyDevice" 08:		
Device" 00:02:58:0						8 170.225 690 750	YourDevice 00 0000	22D28102:223F	3CD847C7
						187.633 229 625	MyDevice us:		
						204 888 780 000	"YourDevice" 00 0000 "MyDevice" 08:	22D28102:223F	63CBC5D8
						 189 289 421 750 	YourDevice 00 Missing	Missing	Not apply
						204.888 780 000	"MyDevice" 08:	Phasing	ivor appin
						g 213.558 772 500	"YourDevice" 00 0000	22D28102:223F	. A05D4FF6
						217.045 330 375	"MyDevice" 08:		
[]	ID packet (ACL, 1 Mbps)					8 219.205 017 500	"YourDevice" 00 0000	22D28102:223F	600275E3:
6	ID packet (ACL, 1 Mbps)					221.628 764 500	"MyDevice" 08:		

This new filter (**Only MyDevice, YourDevice**) is now saved and is quickly accessible in the **Filtering** drop-down menu located on the tool bar, and can easily be enabled and disabled:

V	iltering: Only MyDevice, YourDevice	e •
	Configure	
	Exclude Background	
	Keep All	
~	Only MyDevice, YourDevice	

Benefits of Editing a Device's Properties

The **Device Traffic Filter** provides the user with the ability to edit various device properties (**Edit** icon), including the BD_ADDR, name, color, and radio type. These edits are used throughout the various panes to identify the device, and can help greatly with visual recognition, for example by providing an easy name, such as **MyDevice**, or changing the color associated with the device as used in other panes.

Name MyDevice Color Image: Color Radio Classic	Edit Device Parameters BD_ADDR Name Color Radio	08:00:28:0E:B4:B0 MyDevice	OK <u>C</u> ancel
--	--	-------------------------------	----------------------

©Ellisys 2012. Information contained herein is for illustrative purposes and is not intended in any way to be used as a design reference. Readers should refer to the latest technical specifications for specific design guidance. Ellisys – Chemin Du Grand Puits 38 – CH1217 Meyrin – Geneva +41 22 77 777 89 (USA +1 866-724 -9185) www.ellisys.com.



But why make the BD_ADDR editable? Well, as we know, the BD_ADDR of a device is not always transmitted over the air and in fact in most cases it is only partially present over the air. This can lead to difficulties in decrypting the device's traffic, as the full BD_ADDR is one of the components required for decryption. See <u>EEN_BT07 – Secure Simple Pairing</u> <u>Explained</u> for more details.

There are ways to make a device to send its full BDADDR (such as doing an Inquiry to force a discoverable device to send its FHS packet), but it may be simpler to just add the full BD_ADDR into the Device Database. This new information is stored by the BEX400 application and can now be used by the application's Security features to decrypt traffic.

As captured:

Ed	lit Device		
	Parameters		
	BD_ADDR	::FD:90:3C:09	
	Name	xcxx:FD:90:3C:09	<u>C</u> ancel
	Color	•	
	Radio	Classic	

As edited:

Edit Device		
Paramete BD_ADI	DR AC:2B:FD:90:3C:09	OK Cancel
Color Radio	Classic •	

Adding a New Device

As mentioned above, we can edit a partial BD_ADDR on a given device in the *Device Database*. Interestingly, we can also add a *new* device, without ever having captured this new device. Simply click on the **New Device** button in the *Device Traffic Filter*, and edit the properties as needed:

New Device		
Parameters		Croate
BD_ADDR	11:22:33:44:55:66	Create
Name	MyNewDevice	<u>C</u> ancel
Color	·	
Radio	Dual Mode 🔹	

The advantage of this approach is that the devices are known right away by the BEX400 software, without any need of auto-detection, which can eliminate potential issues in special cases.



Summary of All Filters Available

The table below summarizes the various filters and their purposes. More details on all filters are accessible in Chapter 8 of the User Manual, which installs along with the BEX400 application.

Filter Type	Filter Location	Purpose of Filter
Instant Filters	Atop each Overview column	Highly flexible text string filter used to include or exclude items displayed in any column. Includes wildcards.
Protocol/Profile Filters	Filter Bar atop Overview	Single, Multiple, and Custom Grouping Selections. Allows for display in all panes of only selected protocol(s), profile(s).
Instant Piconet Keep Only Filter	<i>Right-click on Instant Piconet</i> pane	Filters all panes to show only Piconet(s) or LE Connection(s) of interest.
Devices Filter	Atop header bar on <i>Overview</i>	Provides a list of all devices in the current capture and a database of previously captured devices, and allows for show/hide of specified device communications. Allows for exclusion of background traffic. Affects all panes.
Instant Timing Display Filter	Display button on <i>Instant</i> <i>Timing</i> toolbar	Shows/hides Establishment traffic and Idle traffic in the <i>Instant Timing</i> pane.
Instant Timing Keep- Only Filter	Right-click on packet in <i>Instant</i> <i>Timing</i> pane.	Allows user to keep only the selected piconet. Affects all panes.
Overview Keep/Exclude Filter	Right-click menu on Overview	Line/Column (cell) context-sensitive filter to Keep or Exclude selected item.

Capturing Traffic

Please consult our Expert Note, "Your First Wide-band Capture" to learn how to properly configure and operate your analyzer to take clean captures. A link is provided below.

Getting the Software

The software is available upon request on the Ellisys website at: http://www.ellisys.com/products/bex400/download.php

The download is subject to approval, but approval will likely granted to any company that is part of the *Bluetooth* SIG or seriously involved in *Bluetooth* development.

Feedback

Feedback on our Expert Notes is always appreciated. To provide comments or critiques of any kind on this paper, please feel free to contact us at <u>expert@ellisys.com</u>.



Other interesting readings

- <u>EEN BT01 Capturing Bluetooth Traffic, the Right Way</u>
- <u>EEN BT02 Bluetooth Analysis Tutorial</u>
- <u>EEN BT03 Your First Wide-Band Capture</u>
- More Ellisys Expert Notes available at: <u>http://www.ellisys.com/technology/expert_notes.php</u>

Rev. A. Updated 2012-01-25