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.

raffic Filtering Criteria			Device	Database						
Exclude Background	•	🗮 Clear 🗞 Add	1 N	ew Device 🔣 <u>E</u> dit	Delete	Search:		View: All Devices 👻		
Name		adio		Name		ADDR	Radio	LMP Name	Company ID	
			÷.	Mecel		:15:83:32:A6:8A		Mecel	IVT corporation	
				ma2IAS		:22:58:00:C8:8A		mg2IAS	Taiyo Yuden Co., Ltd.	
				mott		:8E:E4:34:D6:CD		mott	Texas Instruments	
				MR 10LAP02		: 1E: 37:9F:F8:7E		MR 10LAP02	Universal Global Scie	
				MT6276		:55:0D:22:62:76		MT6276		
				MTK 2	EE	:49:46:66:20:91	Classic	MTK 2		
				MyDevice	08	:00:28:0E:B4:B0	Classic	Full Android on Blaze	Texas Instruments	l
				Nokia 303	AC	:81:F3:82:EE:D7	Classic	Nokia 303	Nokia Corporation	1
				Nokia 6220 classic1	00	:1F:01:91:87:C1	Classic	Nokia 6220 classic1	Nokia Danmark A/S	
				Nokia N8-00	E0	:A6:70:C8:64:42	Classic	Nokia N8-00	Nokia Corporation	
				Nokia-01	AC	:81:F3:82:EE:B4	Classic	Nokia-01	Nokia Corporation	
				Nokia-10	AC	:81:F3:34:E4:E0	Classic	Nokia-10	Nokia Corporation	
				Parrot_2	38	:3A:AE:87:72:22	Classic	Parrot_2		
			📄 🖷 🔳	Parrot1	20	:07:19:81:11:11	Classic	Parrot1		
			主 🖿	PARROT-PC-BLUES	E8	:39:DF:04:88:71	Classic	PARROT-PC-BLUES	Askey Computer	
			🗈 · 🔳	PATMIF8T0ZD1XPL	00	:1A:6B:E5:65:00	Classic	PATMIF8T0ZD 1XPL	Universal Global Scie	
				Ppppp	1F	:30:CD:E9:62:76	Classic	Ррррр		
			÷. 🔳	PTS-MAP-TECHTLP0	02 00	:80:98:E7:31:4C	Classic	PTS-MAP-TECHTLP022	TDK CORPORATION	
			.	Ram Laptop	90:	4C:E5:DE:0D:C7	Classic	Ram Laptop	Hon Hai Precision Ind	
			主 🖬	Roland Labana - QI	NT07 58	:B0:35:7A:3A:D0	Classic	Roland Labana - QIN	Apple, Inc	
			📄 🗄 🗉 🔳	SCH-I110	12	:47:BF:A5:4B:D5	Classic	SCH-I110		
			i	COMMVA LADTOD		.01.02.71.00.44	Classic	COMMVA LADTOD	Heimersal Clabel Crie	

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.

affic Filtering Criteria		Device I	Database					
Keep Involving Selected Devices	💢 Remove 놓 Add	<u>1</u> е	ew Device 🔣 <u>E</u> dit 📗 <u>D</u> e	lete Search:		View: All Devices 👻		
Name	 Radio 		Name	BD_ADDR	Radio	LMP Name	Company ID	
"MyDevice" 08:00:28:0E:B4:B0	Classic 📓		Mecel	00:15:83:32:A6:8A		Mecel	IVT corporation	
		÷	mg2IAS	00:22:58:00:C8:8A	Classic	mg2IAS	Taiyo Yuden Co., Ltd.	
			mott	7C:8E:E4:34:D6:CD	Classic	mott	Texas Instruments	
		•	MR 10LAP02	00:1E:37:9F:F8:7E	Classic	MR 10LAP02	Universal Global Scie	
			MT6276	43:55:0D:22:62:76	Classic	MT6276		
		÷	MTK 2	EE:49:46:66:20:91	Classic	MTK 2		
		÷. 🔳	MyDevice	08:00:28:0E:B4:B0	Classic	Full Android on Blaze	Texas Instruments	
			UConnect	00:0E:9F:5E:12:A3	Classic	UConnect	TEMIC SDS GmbH	
			Tarang	C8:97:9F:7B:EE:33	Classic	Tarang	Nokia Corporation	
			YourDevice	00:02:5B:03:0E:BC	Classic	USD78WVLL1	Cambridge Silicon Radio	
		I	SCH-I110	12:47:8F:A5:48:D5	Classic	SCH-I110		
		••• •	Nokia 303	AC:81:F3:82:EE:D7	Classic	Nokia 303	Nokia Corporation	
			Nokia 6220 classic1	00:1F:01:91:87:C1	Classic	Nokia 6220 classic1	Nokia Danmark A/S	
		🔳	Nokia N8-00	E0:A6:70:C8:64:42	Classic	Nokia N8-00	Nokia Corporation	
		🖶 - 📕	Nokia-01	AC:81:F3:82:EE:B4	Classic	Nokia-01	Nokia Corporation	
		🔳	Nokia-10	AC:81:F3:34:E4:E0	Classic	Nokia-10	Nokia Corporation	
		🛨 ·· 📕	Parrot_2	38:3A:AE:87:72:22	Classic	Parrot_2		
		÷. 🔳	Parrot1	20:07:19:81:11:11	Classic	Parrot1		
		÷. 🔳	PARROT-PC-BLUES	E8:39:DF:04:B8:71	Classic	PARROT-PC-BLUES	Askey Computer	
		主 · 🔳	PATMIF8T0ZD1XPL	00:1A:6B:E5:65:00	Classic	PATMIF8T0ZD 1XPL	Universal Global Scie	
		主 · 🔳	Ррррр	1F:30:CD:E9:62:76	Classic	Ррррр		
		<u>.</u>	DTC MAD TECUTI DOOD	00.00.00.07.71.40	Classic	DTC MAD TECUTI DOOD		

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.

affic Filtering Criteria		Device	Database					
Keep Only Selected Devices 🔹	💢 Remove 놓 Add	泪 <u>N</u> e	ew Device 🔣 <u>E</u> dit 😹 <u>D</u> el	ete Search: my,yo	ur	View: All Devices 🔹		
Name A Ra	dio		Name	BD_ADDR	Radio	LMP Name	Company ID	
	sssic		Laptop MyDeviceY MyDeviceY MyDeviceY My Android Phone My Bladberry My Car MyDeviceX MyDeviceZ YourDevice	00:21:86:71:83:44 00:22:58:41:14:77 08:00:28:06:E8:480 00:22:58:41:14:77 22:22:BE:04:E1:48 00:22:58:41:14:77 22:22:BE:04:E1:48 00:09:93:20:001 00:01:66:91:10:78A 00:02:58:03:0E:BC	Classic Classic Classic Classic Classic Classic Classic Classic Classic Classic	SOWMYA_LAPTOP IAS Full Android on Blaze IAS My Android Phone BlackBerry 9550 My Car HARMAN 3 IAS USD78WVLL1	Universal Global Scie Taiyo Yuden Co., Ltd. Texas Instruments Taiyo Yuden Co., Ltd. RIM Visteon Corporation ELMEX Co., LTD. Taiyo Yuden Co., Ltd. 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:

	Record Tools Help							/Layout 📑 Full screen 📑 Ar	nalysis 📑 Add
	tecord • 🗎 Stop 💷 Restart 🐕 🎇 💭 Navigate • 🖏 🖒 Marke	ers (2) 🔹 🤞 🖓 Filtering: Keep All 🔹 😽 👳				41	b Instant Piconet		
	verview Low Energy Overview HCI Overview layers ← ← ∞	A (1) (1) A				Search -			
: Single selection • All			Type f Y		Type filter		Parrot_2 SCH-0110	Paret1 ANDROID BT	
									BlackBerry 9
ne	Item	Communication	Originator	Status	Payload			0	Discriberty
.341 295 750	B 🔹 L2CAP Configure (0x0041, 0x0041)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:		OK				TONALITE HS	
.342 545 750	ID packet (ACL, 1 Mbps)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, Unknown	Master	OK					
.343 171 500	B 🏤 L2CAP Configure (0x0041, 0x0041)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:		OK			1		
.368 171 750	RFCOMM Connect (Channel=Signaling)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:0		OK			MTK 2	mot th	
.422 939 375	Paging ("SCH-I110" 12:47:8F:A5:48:D5 > "Parrot	Master, "SCH-I110" 12:47:8F:A5:48:D5 <-> Slave, "Parrot_2" 38:3A		OK				ė	
.446 295 750		 Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:1 		No Request Fro			Delphi 1	•	1
496 921 375	RECOMM Connect (Channel=8)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:0		OK					
.510 045 625	RECOMM Modem Status	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:		OK			10		
.530 671 500	RFCOMM Modem Status	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:0		OK			LA Noksilt		
.550 045 500		Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:		OK			0 ⁰	Dwiphi 2	
.599 421 250	E L2CAP Connection (0x0042, 0x0042: AVDTP)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:0		OK			- 0460 TYT HF SY	STEM	mellas.
621 295 500	RFCOMM UIH Frame (Channel=8, Credits=I: -1+1	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:	Master	OK	No data		TOSHIBALS		ingenera
.641 207 250	🕀 🏤 AT String: OK 🖓	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:		OK	4 bytes (# 48 00 0A)				
.645 045 500	🕀 💠 L2CAP Configure (0x0042, 0x0042)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:0		OK			1		
.666 921 250	🗉 🐟 L2CAP Configure (0x0042, 0x0042)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:) Slave	OK			1 2		
	AT MT Indicator: AT+CIND?/r > /r/r+CIND: 1,0,0,0	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:						•	
700 045 375		Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:	Master	OK			AvDevice2	1	••••.
700 671 375	E 🏤 L2CAP Connection (0x0043, 0x0043: AVCTP)	Master, "YourDevice" 00:02:SB:03:0E:BC <-> Slave, "MyDevice" 08:) Slave	OK					
701 921 125	AVDTP Discover Command > Used-No, ACP-1	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:) Slave	OK			00.2713:54:68:61	HandsFreeUnk	
726 295 000	🗉 🀅 L2CAP Parameter Update, Incomplete	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:) Master	No Response Fr					
734 421 375	E 2CAP Connection (0x0044, 0x0044: ?), Incomplete	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:	Master	No Request Fro					
736 922 125		Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:) Slave	OK	19 bytes (24 0D 58 08 4C 00 44				
738 171 250	E 🛖 L2CAP Configure (0x0044, 0x0044)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:) Slave	OK			🛸 н н н нн 189,670 045 500 🍊		_
739 421 375	AVDTP GetCapabilities (ACP - 1) + Capabilities - Medi	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:) Slave	OK					
743 795 500	RFCOMM UBH Frame (Channel=8, Credits=1: -1+1	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:) Master	OK	No data		🗊 Details 🕙 Summary 😪 Instant Piconet		
789 421 125	AVDTP SetConfiguration (ACP-1, INT-1, Capabilit	I Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:) Slave	OK			Security		
810 045 375	AVDTP Packet (Type = Reject, Fragment = End Packet)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:0) Master	OK	13 bytes (A7 09 1E 69 A9 15 2F		Manage SSP Keys		
.821 921 125	Avenue of the second seco	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:0	Master	No Request Fro					
.866 681 625	ID packet (ACL, 1 Mbps)	Master, "mg2IAS" 00:22:58:00:C8:8A <-> Slave, Unknown	Master	OK				IN Link Key	ACO
918 171 125	AVDTP Open (ACP=1) > Accept	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:0	Slave	OK			 6.077 990 500 "Delphi 2" 00:22:A0: No 27.349 250 500 "0460 TYT HF SYSTE 	it applic Notapplicable	Missing
ming								ot applic Missing	Missing
🔍 🔲 🚡 - 🛛 origir	n: 184.50 s • span: 8.03 s • Display • 💽						92.308 888 125 "MyDevice" 08:00:2	Copplican <u>Plaaning</u>	ring
		a					93.279 509 750 "mg2IAS" 00:22:58: No	st applic Notapplicable	Notapplic
001221A010010	1 1 1 1	1 1 1	🤗 I -	1	1	1 1	244.454 095 250 Unknown		
" 0810012810E1			} .	•		· ·	😭 99.097 579 750 "Delphi 2" 00:22:A0: No	ut applic Not applicable	Missing
" 08:00:28:0E1							100.506 330 500 "0460 TYT HF SYSTE		
os" 00:02:58:0			. <mark>.</mark>	and an arrest			100.769 458 250 "Delphi 2" 00:22:A0: No 218.842 149 500 "0460 TYT HF SYSTE	it applic Missing	Notapplic
Ce 0000215000		recent childraithe is discharged a second day	ta di secondo di second	r of a life of the state of a			218.842 149 500 0400 111 HF STSTE 2016.323 866 000 "YourDevice" 00:02: No	the second s	Notapplic
TECHTI DI22"							116.323 866 000 "YourDevice" 00:02: No 132.581 699 625 "MyDevice" 08:00:2	ic applic Missing	Notapplic
							132.675 726 250 "YourDevice" 00:02: No	ot applic Missing	Missing
01:02:03							138.600 454 625 "MyDevice" 08:00:2	s opprion <u>ringbilly</u>	
							138.671 344 250 "YourDevice" 00:02: No	at applic Missing	Notapplic
00:22:58:00:C	NAME AN AND AND A TAXANG AT A REPORT OF AN ANALY MADE AND A REPORT OF A DATABASE AND A REPORT OF AN AND A REPORT	NATIONAL TO AN TO AN TO AN TO AN THE AREA TO AN THE AREA AND AND AND AND AND AND AND AND AND AN	a da mangana a			TRACTOR AND A DECEMPTION OF	164.916 997 625 "MyDevice" 08:00:2		
							147.190 193 250 "Parrot1" 20:07:19: No	ot applic Missing	Notapplic
1 12:47:8F:AS:	AT MT Indicator: AT+CIND7k > Wn+CIND: 1,0,0,0,5,0,2Wn/m > OKWn		1				147.713 148 375 "ANDROID BT" 7E:B		
							A 147.724 399 375 "ANDROID BT" 7E:B No	at applic Missing	Notapplica
	5.50 86.50 87.00 87.50	88,00 89,50 89,50	00.00	20.50	91.00 91.50	192.00 5			

©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:

	luetooth Analyzer						El myLayout El Ful so	En autori	- @
	earch Record Iools Help ▶ Record • ⊟ Stop ⊒ Restart 📽 🎇 J⊒Navigate • 🖏 🖱 Markers (2) • J⊐	- Vieltering: Only YourDevice, MyDevice -					🛛 🖽 myLayout 🖽 Full sc	reen 🗄 Analysis	Add
	DR Overview Low Energy Overview HCI Overview				4 Þ	Instant Piconet			
ol: Single selection •	- Allayers + 🛹 🚥 📥 🔎 🏁 📾 🍪 🥮 🚸 🎝 🗊 🗇 🥸 💑 🖰 👑 🖠	770 items displayed			Search 🔹				
ype filter	V - Type filter V -	Type filter	▼ • Type f ▼	Type filter Y	Type filter				
ime	Item	Communication	Originator	Status	Payload ^				
32, 592 599 625	See LMP PacketType Table (Accepted)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0	Master	ок					
32,620,100,375	⊕ G = Hole High Hole (Headpledy) ⊕ G = LMP Set APH	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0	Master	OK					
32.650 100 250	LMP Channel Classification Request (AFH Reporting Enabled)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MvDevice" 08:00:28:0E:B4:B0	Master	OK	E				
132.656 350 250	Green Construction Transaction	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0	Master	OK					
32.692 601 250	Weight LMP Encryption Mode (Accepted)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0	Master	OK					
132.715 100 250		Master, "YourDevice" 00:02:38:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0 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:B4:B0 Master, YourDevice 00:02:58:03:0E:BC <-> Slave, MyDevice 08:00:28:0E:B4:B0	Master	No Response From Slave					
132.759 476 125	grad Lee Start Encryption B g 4 ² Encrypted Traffic (x 490)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:84:80 Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:84:80	Slave	OK					
132.759 476 125		Master, "MyDevice" 08:00:28:0E:84:80 <-> Slave, "YourDevice" 08:00:28:0E:8C	Master	OK					
							MyDevice		
138.401 705 625	See LMP Features Exchange	Master, "MyDevice" 08:00:28:0E:B4:B0 <-> Slave, "YourDevice" 00:02:58:03:0E:BC	Master	No Response From Slave			0	7	
138.416 079 875	George LMP Version Exchange (Master: 4.0, Slave: 2.0)	Master, "MyDevice" 08:00:28:0E:B4:B0 <-> Slave, "YourDevice" 00:02:5B:03:0E:BC	Slave				YouDev	ice	
138.439 829 875	Grad LMP Role Switch (Accepted)	Master, "MyDevice" 08:00:28:0E:B4:B0 <-> Slave, "YourDevice" 00:02:58:03:0E:BC	Slave	ок					
38.599 204 625	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				
38.600 454 625	RHS (YourDevice) packet (ACL, 1 Mbps)	Master, "MyDevice" 08:00:28:0E:B4:B0 <-> Slave, "YourDevice" 00:02:58:03:0E:BC	Slave	ОК	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	ок					
38.610 093 500		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	Implement BacketType Table (Accepted)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0	Master	ок					
38.611 969 625		Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0	Slave	No Response From Master					
138.638 844 375	GO UNP Set APH	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:84:80	Master	ок					
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	ок					
138.671 344 250	EMP Authentication Transaction	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:84:80	Master	OK					
38.715 094 250	Image: Bigg: Bi	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0	Master	OK		🛸 н н не	₩ 138.596 705 125 AD: OR		
38.725 094 250	EMP Encryption Key Size (Accepted)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0	Master	OK		Detaile I 🔿 Curr	mary 😪 Instant Piconet		
138.776 344 375	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					
38.783 220 750	🕀 🚰 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			
38.788 844 250	🕀 😋 Unknown LMP Message	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:84:80	Master	OK		Manage SSP Keys			
38.791 344 250	🔣 🥧 L2CAP SDU (Basic, Dest=0x8F36)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0	Master	ОК		Time	Master / Slave PIN	Link Key	ACO
38.791 970 375	🛞 🖼 Unknown LMP Message	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0	Slave	ок		34.960 195 250		Missing	Missing
38.793 844 250	B de L2CAP SDU (Basic, Dest=0x14D7)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0	Master	ок		92.308 888 125	"MyDevice" 08:	- mpping	rissing
38.794 469 625	🛞 🛖 L2CAP C-Frame (ACL-U Flow Events)	Master, "YourDevice" 00:02:58:03:0E:BC <-> Slave, "MyDevice" 08:00:28:0E:B4:B0	Slave	ок	-	8a 116.323 866 000	"YourDevice" 00 Not applic. "MyDevice" 08:	Missing	Not app
t Timing					. ×		"YourDevice" 00 Not applic.	Missing	Missing
	origin: 138,590.91 ms 🔹 span: 20.01 ms 🔹 Display 🔹 🍙					138.600 454 625	"MyDevice" 08:		
s	Congrine 130,300 SErris - Spane 20,02 His - Display - M	- 4					"YourDevice" 00 Not applic. "MyDevice" 08:	Missing	Not app
vice" 08:00:28:0E:	<u>, , , , , , , , , , , , , , , , , , , </u>					164.991 319 500 187.633 229 625	"YourDevice" 00 0000 "MyDevice" 08:	22D28102:223F.	. 3DD826
vevice" 00:02:58:0				<u> </u>			"YourDevice" 00 0000 "MyDevice" 08:	22D28102:223F.	. 3CD8474
						86 187.713 797 375 204.888 780 000	"YourDevice" 00 0000 "MyDevice" 08:	22D28102:223F.	. 63CBC5
						189.289 421 750	"YourDevice" 00 Missing "MyDevice" 08:	Missing	Not app
						213.558 772 500	"YourDevice" 00 0000 "MyDevice" 08:	22D28102:223F.	A05D4Fr
	Bit packer (ACL, 1 Mbps) (B) ID packer (ACL, 1 Mbps)					219.205 017 500	"YourDevice" 00 0000 "MyDevice" 08:	22D28102:223F.	m 6002758
	93,00 94,00 95,00 95,00 97,00 98,00 99,00	138.600.00 ms 01.00 02.00 03.00 04.00 05.00	66,00	07.00 03.00	138,610.00 ms		"YourDevice" 00 0000	22D28102:223E	E1EC990

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	ltering: 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.

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		ок
	BD_ADDR	::FD:90:3C:09	
	Name	xcxx:FD:90:3C:09	<u>C</u> ancel
	Color	•	
	Radio	Classic	

As edited:

Edit Device		
Parameters BD_ADDR Name	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		Create
BD_ADDR	11:22:33:44:55:66	
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