Separating the Wheat from the Chaff

Introduction

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.

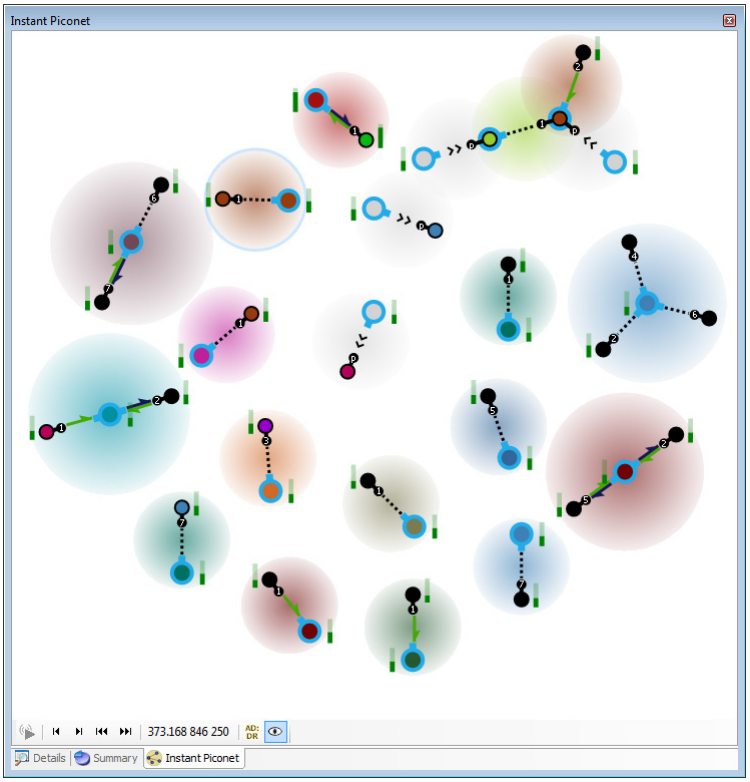
The BEX400 Explorer Instant Protocol Analysis System is uniquely designed to capture all *Bluetooth* traffic in the vicinity, including all piconets and scatternets as well as unsynchronized traffic like pagings and inquiries.

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.

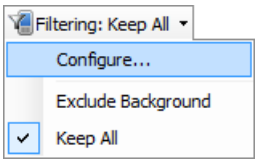
This paper will walk the user through the process of using the powerful *Device Traffic Filter* and associated **Device Database**, and will touch on usage applications for other filter mechanisms.

Creating Specific Criteria Using the Device Traffic Filter

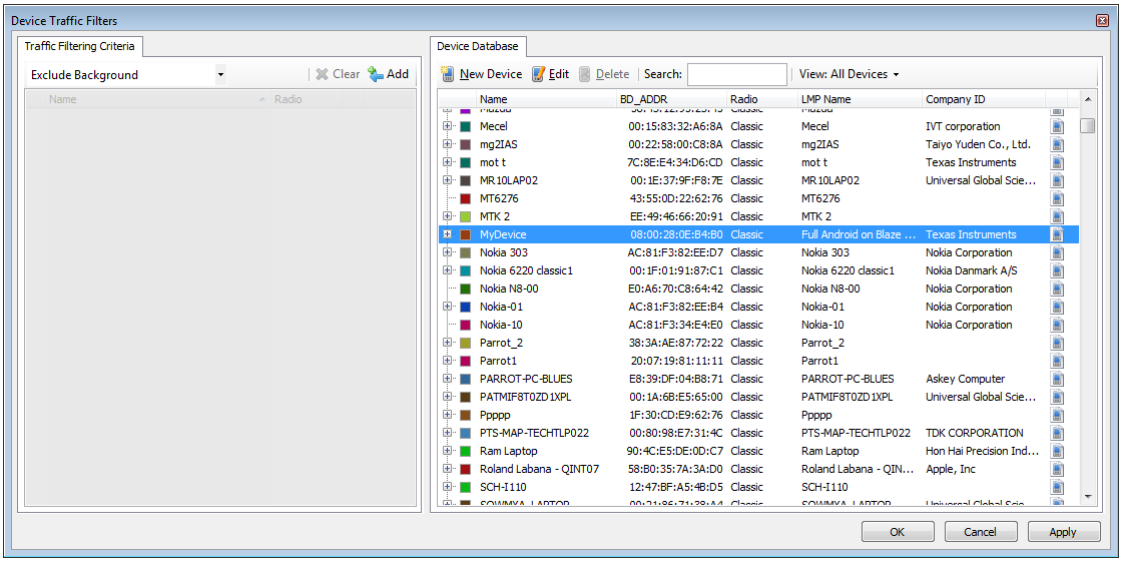
The *Instant Piconet* figure below shows a moderately busy *Bluetooth* environment. At a glance, we can see about 18 piconets, the formation of a scatternet, some data transfers, and paging events. This traffic is also represented in various other panes, such as the *Instant Timing* pane and the *Overview*.



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, throughout all panes in the BEX400 application? 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.

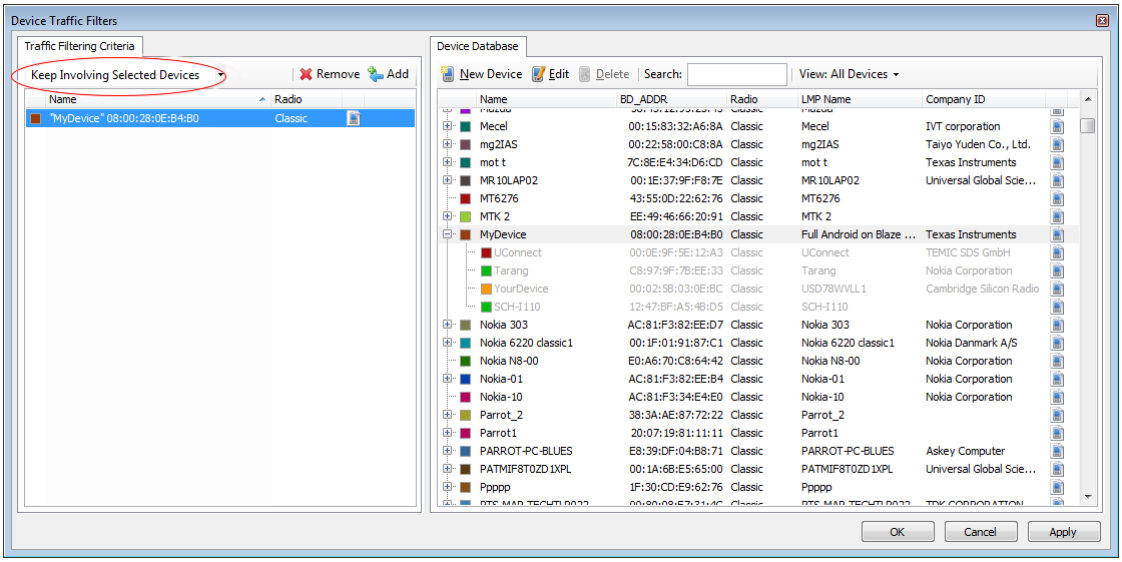


The database will display all devices captured historically and devices captured in the current trace, as well as a list of the communications established between them.

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.

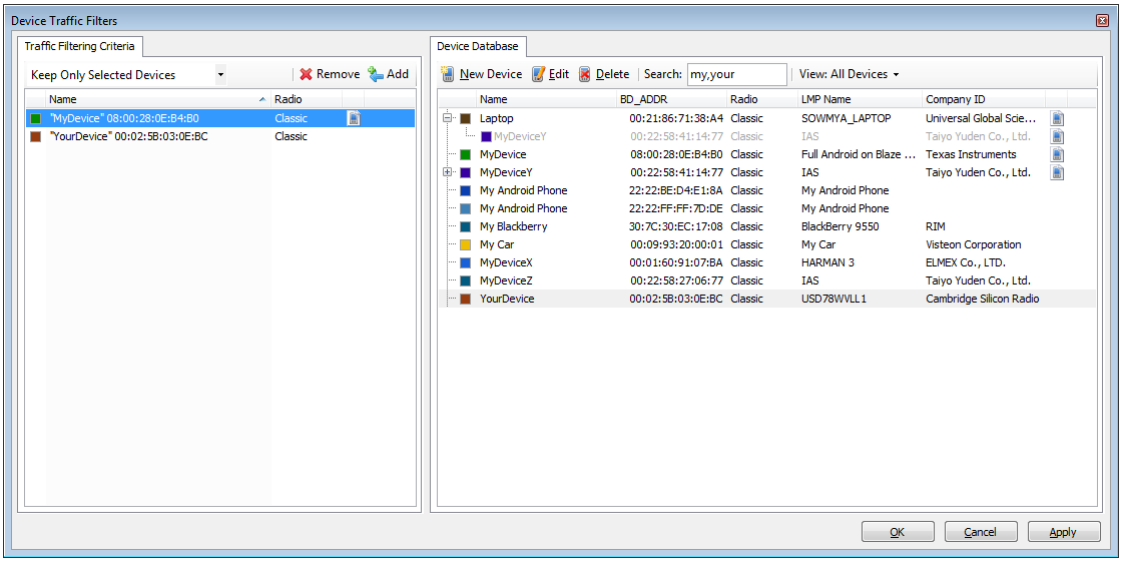


So, what began as a fairly large capture with about 40 devices is now reduced throughout the application's panes to **MyDevice** and the corresponding traffic with the four devices it has communicated with in this capture.

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?

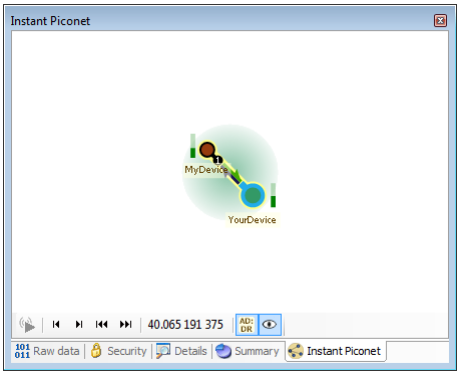
No problem, except this time, we'll add **YourDevice** to the *Traffic Filtering Criteria* as shown below.



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."

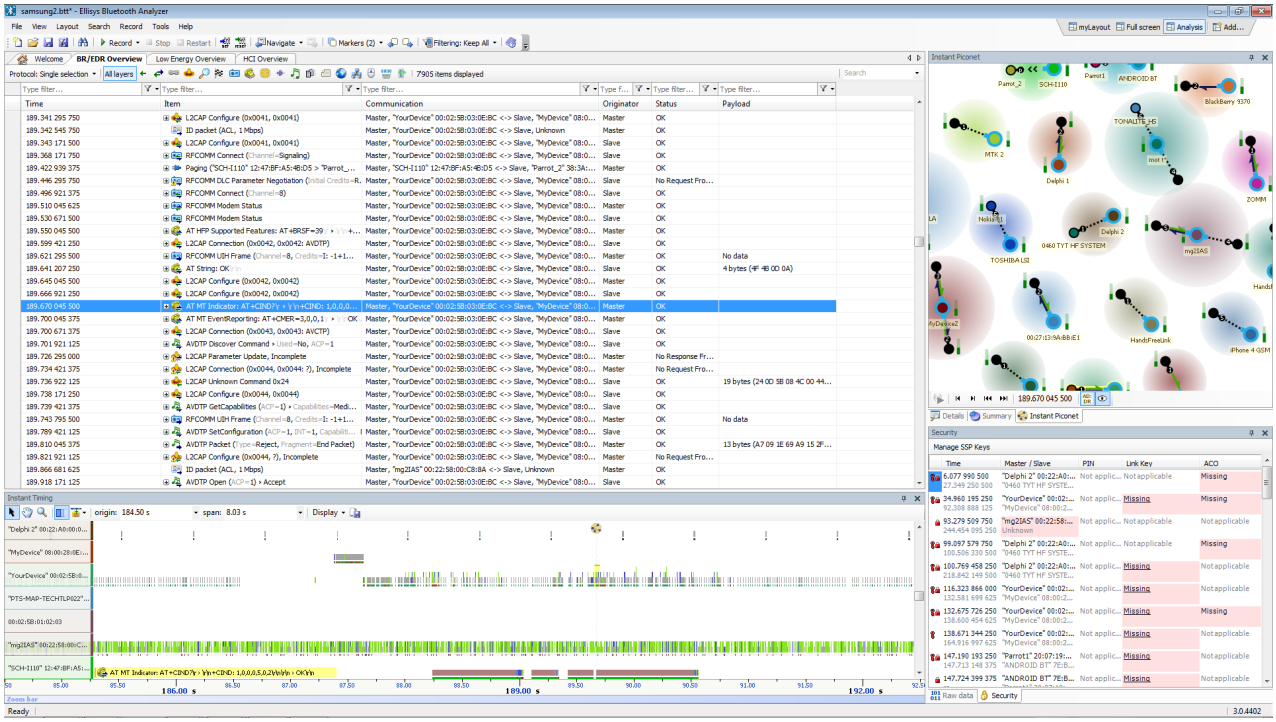
Another helpful hint: The **Search** box is using a comma to AND devices name beginning with "My" and "Your."

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

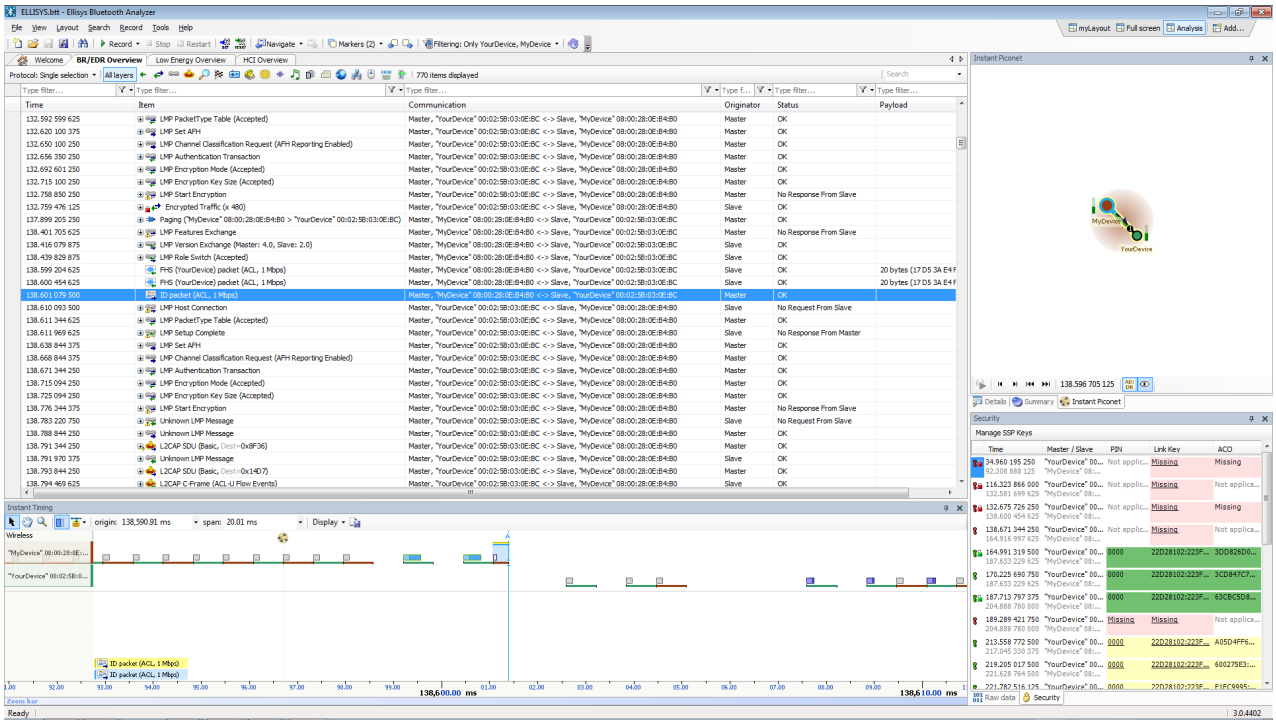


A global look at the application gives a better perspective on the before and after effects:

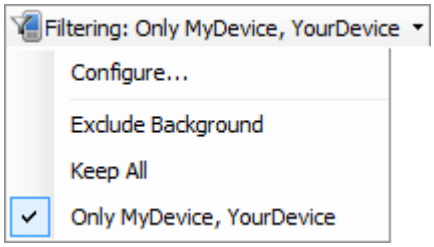
Before:



After:

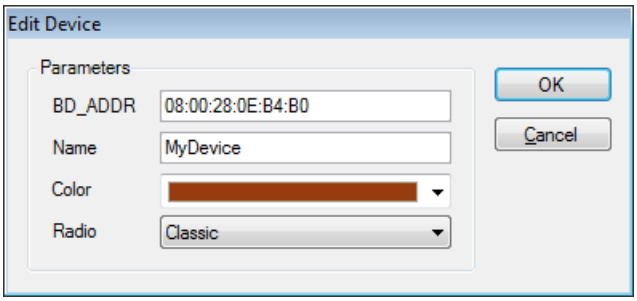


This new filter (**Only MyDevice, YourDevice**) is now saved and is quickly accessible in the **Filtering** drop-down menu located on the tool bar, and can easily be enabled and disabled:



Benefits of Editing a Device's Properties

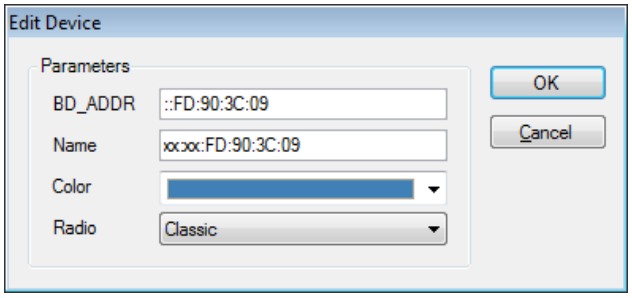
The **Device Traffic Filter** provides the user with the ability to edit various device properties (**Edit** icon), including the BD_ADDR, name, color, and radio type. These edits are used throughout the various panes to identify the device, and can help greatly with visual recognition, for example by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



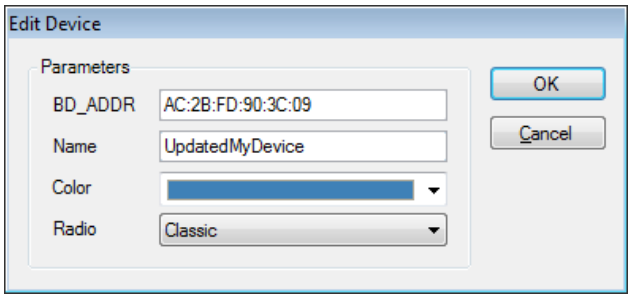
But why make the BD_ADDR editable? Well, as we know, the BD_ADDR of a device is not always transmitted over the air and in fact in most cases it is only partially present over the air. This can lead to difficulties in decrypting the device's traffic, as the full BD_ADDR is one of the components required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

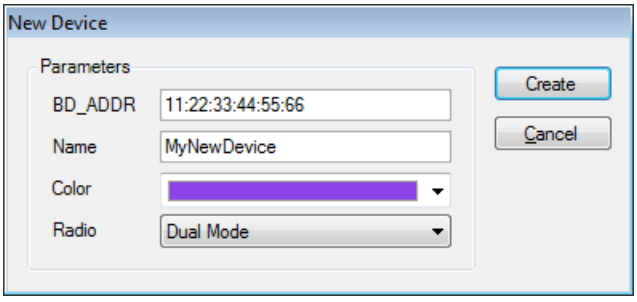


As edited:



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:



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	*Right-click on Instant Piconet* pane	Filters all panes to show only Piconet(s) or LE Connection(s) of interest.
Devices Filter	Atop header bar on *Overview*	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 *Instant Timing* toolbar	Shows/hides Establishment traffic and Idle traffic in the *Instant Timing* pane.
Instant Timing Keep-Only Filter	Right-click on packet in *Instant Timing* 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 expert@ellisys.com.

Other interesting readings

- EEN_BT01 - Capturing Bluetooth Traffic, the Right Way
- EEN_BT02 - Bluetooth Analysis Tutorial
- EEN_BT03 - Your First Wide-Band Capture
- More Ellisys Expert Notes available at: http://www.ellisys.com/technology/expert_notes.php

Rev. A. Updated 2012-01-25