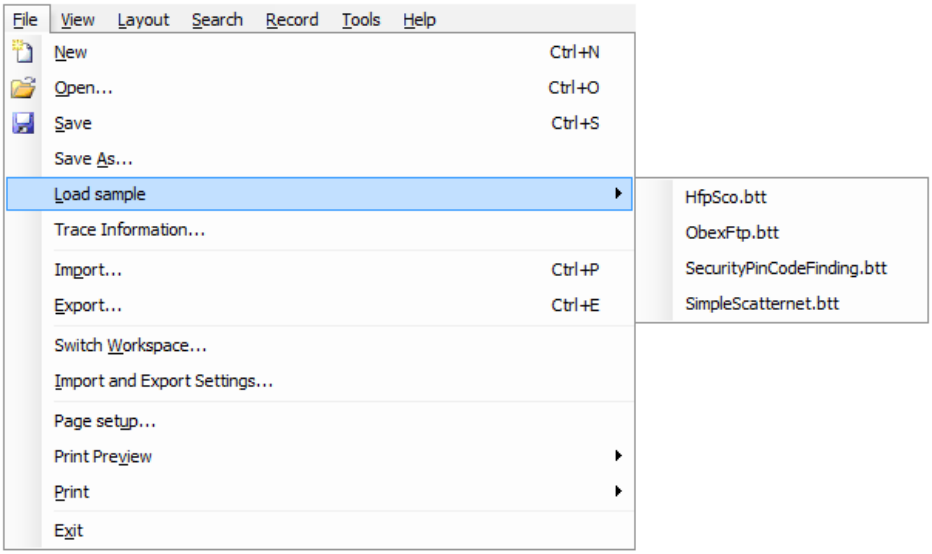
Bluetooth Analysis Tutorial

Introduction

This paper will provide a quick walk-through on the Ellisys *Bluetooth* analysis software.

Sample Captures

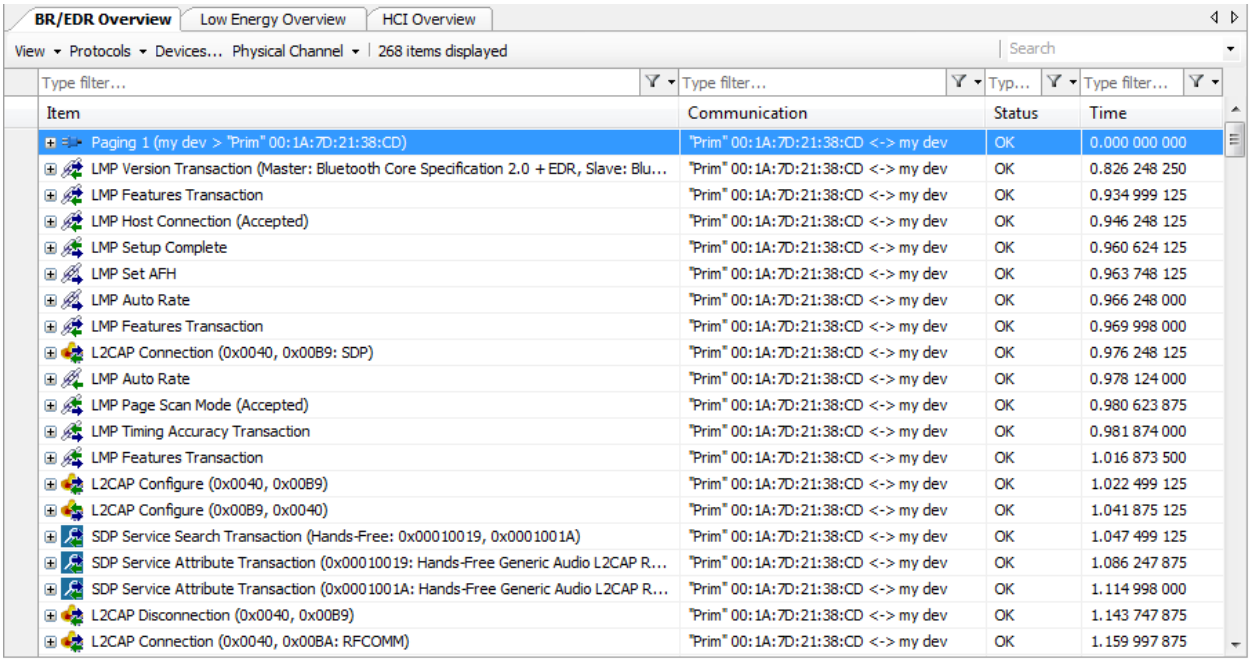
The easiest way to evaluate the Ellisys *Bluetooth* analysis software is by looking at the pre-captured files provided with the installation. These sample captures can be loaded from the File menu > Load sample.



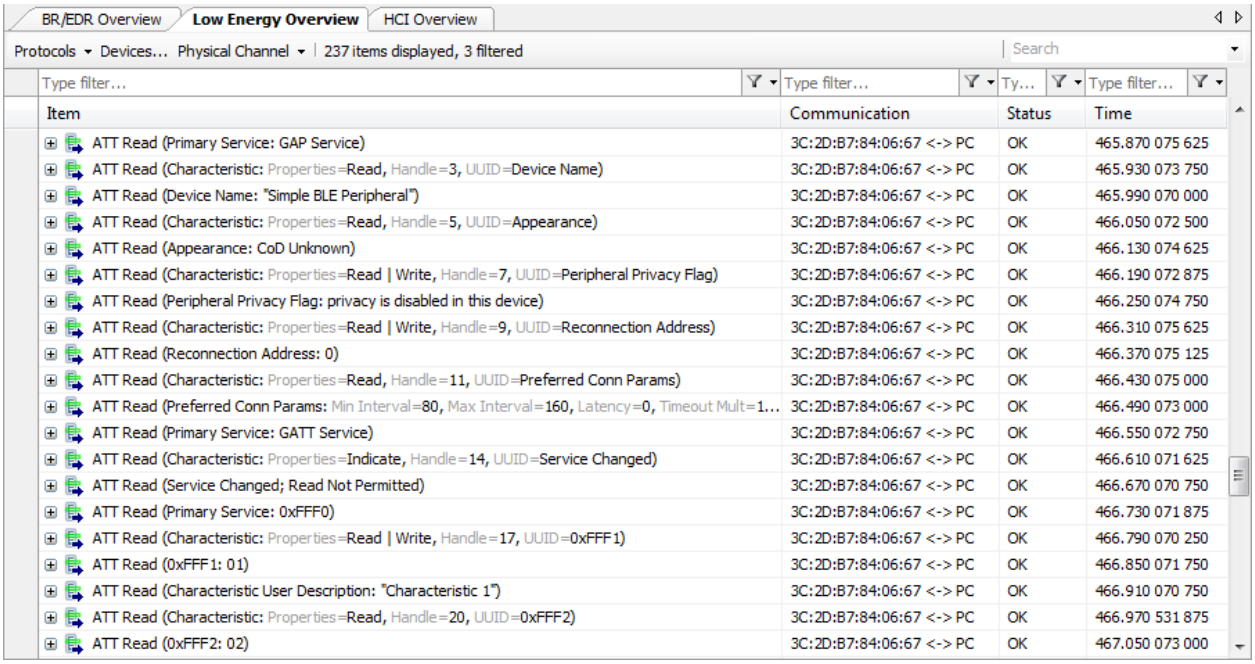
We will start out with the HfpSco.btt sample, which contains traffic between a headset and a mobile phone.

Ellisys Protocol Overview

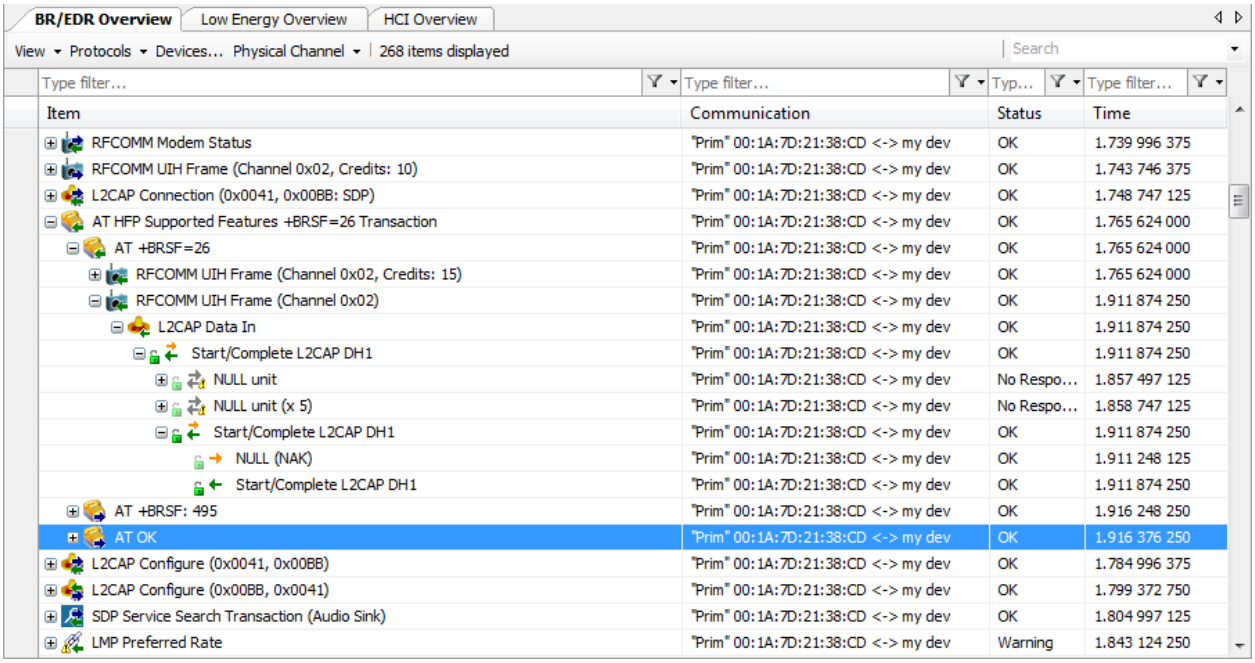
The Ellisys *Overviews* are the central views of the software. These views will show the captured traffic grouped in protocol layers, up to the highest layer. Each medium (Classic *Bluetooth* BR/EDR, Low Energy and HCI) is captured concurrently and is provided with its own *Overview*. Here is some Classic *Bluetooth* traffic:



And here is some Low Energy traffic:

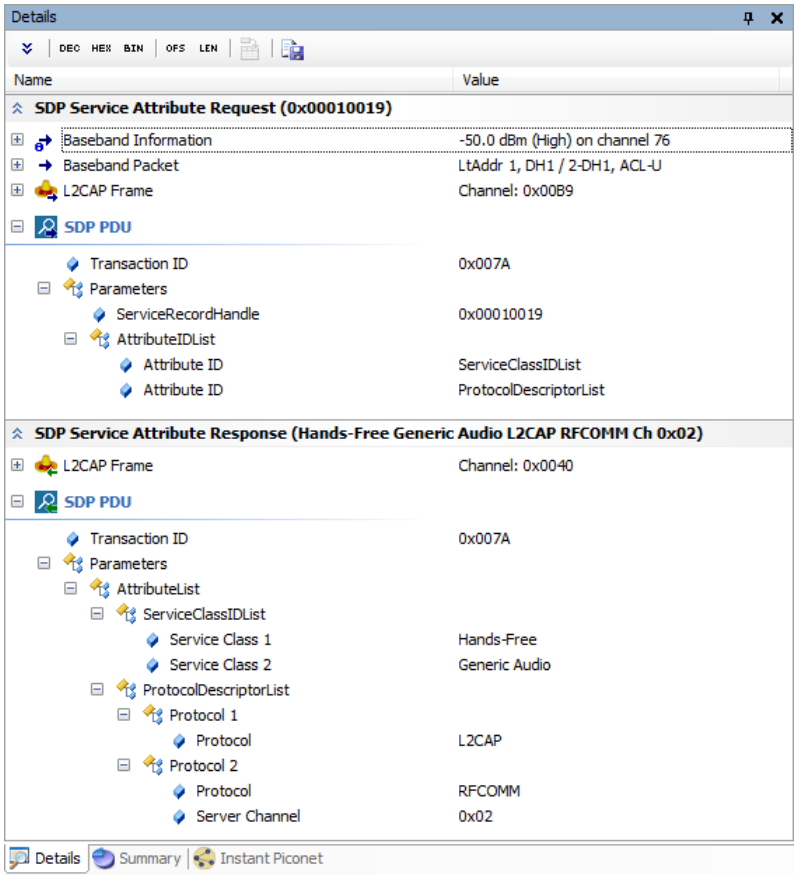


The Ellisys *Overview* is made to be easily readable. Traffic is grouped hierarchically into protocol layers in a tree. The protocol stack-up can be easily reviewed by navigating into the tree nodes. Let's review the following screenshot. We can see an AT HFP transaction consisting of an AT command, an AT response and an AT handshake. Each AT packet is transported with RFCOMM frames, which is on L2CAP, which is on baseband. This stack-up can be seen very easily in the BR/EDR *Overview*.

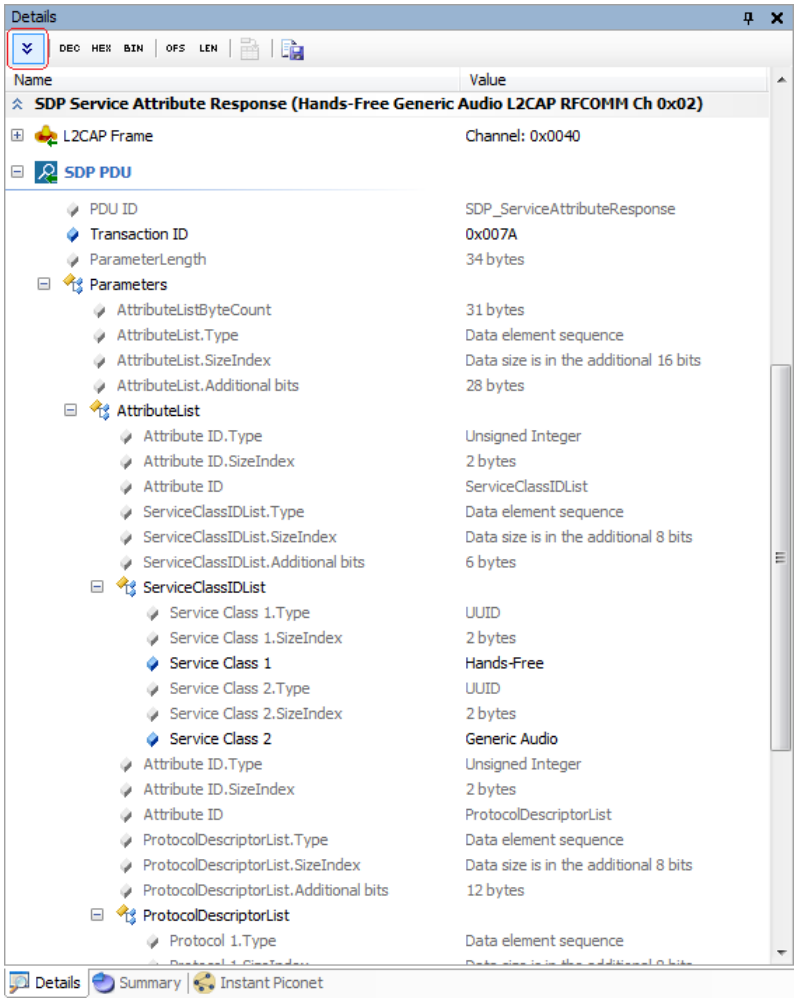


Details View

Each selected line in the *Overview* can be reviewed in detail in the *Details* view. The following screenshot shows the detail of an SDP Service Search transaction. As you can see, not only is the SDP information displayed, but the lower layers (such as L2CAP and baseband) are also displayed. The lower layers are closed and summarized by default, but these lines can be expanded in order to review every detail.



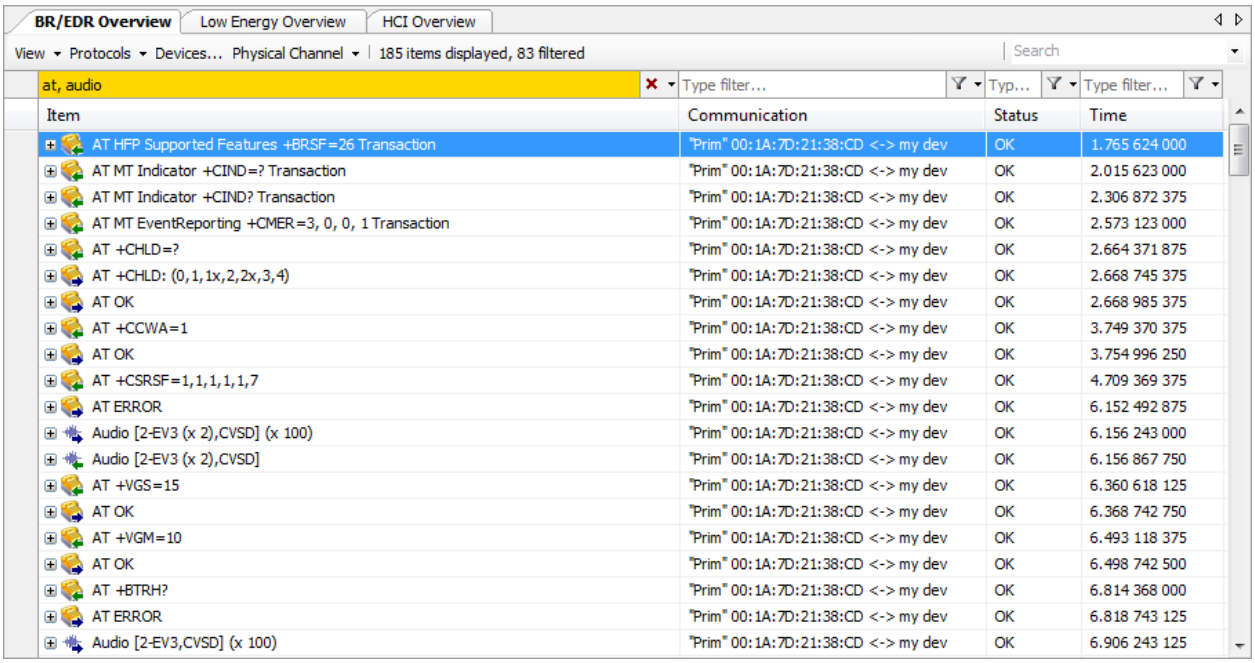
If we take a closer look at the SDP traffic, we see the master issued an SDP Service Search Request in order to discover the available service classes and protocol descriptors. The response clearly shows the returned information in a pretty effective way. But if you know SDP, you also know that it is a quite flexible protocol, requiring many fields for describing this dynamic structure. The screenshot above looks too simple, and actually is. By default, the Ellisys software only displays the most relevant information, and hides all information which is not generally useful for understanding, such as CRCs, lengths, reserved fields, etc. Of course these hidden fields can be shown as needed, and will automatically be displayed if there is anything wrong with them (so an incorrect CRC will not be missed for example). Below, the same SDP event is shown with all fields enabled. The grayed lines are those that are hidden by default.



Ellisys Instant Filters

As seen above, the *Overview* conveniently displays all protocols in a single view. This is very useful in understanding the sequence of events. For example, it's easy to see the paging, L2CAP connection, RFCOMM establishment, and then the AT traffic. But sometimes you need to focus on a given protocol, or some specific traffic. The column-based *Instant Filters* are quite useful in quickly applying display filters to the *Overview*. These filters are based on simple text patterns and also can accept wildcards (*).

Let's walk through an example. We wish to keep only AT and SCO audio traffic. We can simply type "at, audio" in the Item column's *Instant Filter* box. This will keep/show any line beginning with "at" or "audio", as shown below:



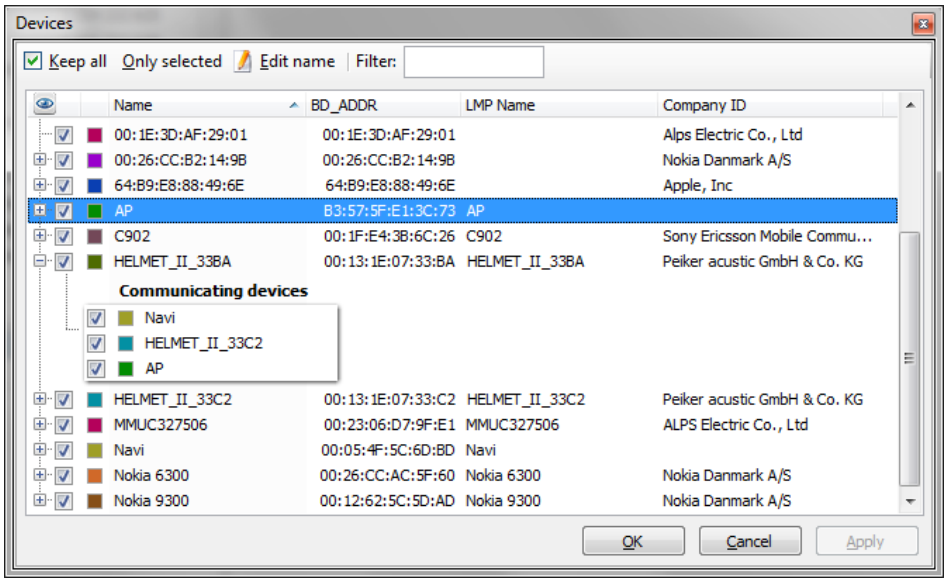
It is also possible to exclude traffic by using the NOT sign (!), for example by typing "!at, audio". This will exclude/hide lines beginning with "at" or "audio", and leave all other traffic displayed.

Wildcards such as '*' (accept any character, zero or more) or '?' (accept any single character) are supported. For example, typing "*ev3" will match any line containing the text "ev3".

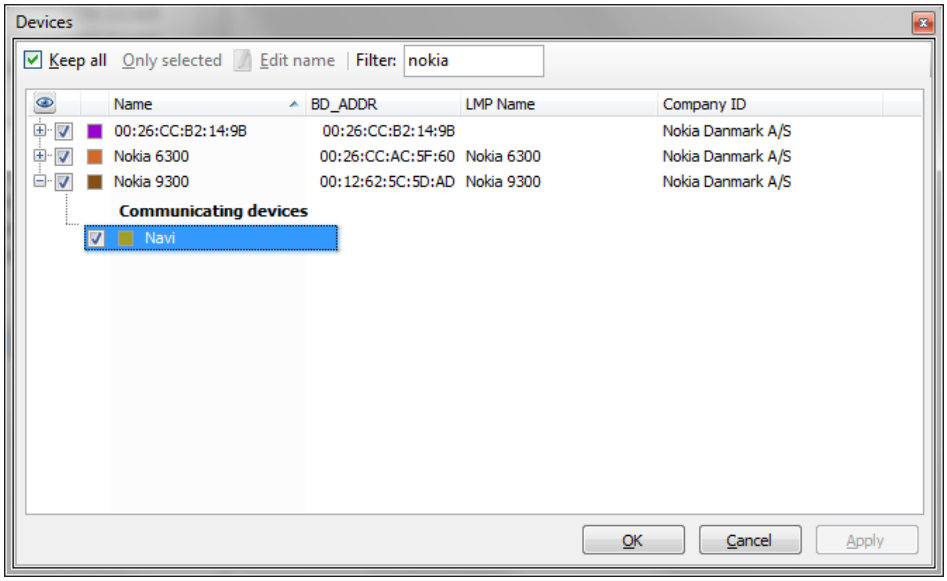
Ranges are supported in numeric columns. A range is specified such as start..stop. For example, to keep items occurring between 0 and 1 second, simply type "0..1" in the Time column's *Instant Filter* box.

Filtering by Devices

When using a whole-band sniffer, all device activity in the area will be captured. Applying a *Devices* filter is quite useful in order to focus only on devices and/or communications of interest. The Ellisys software enables quick and easy filtering in the *Devices* window.



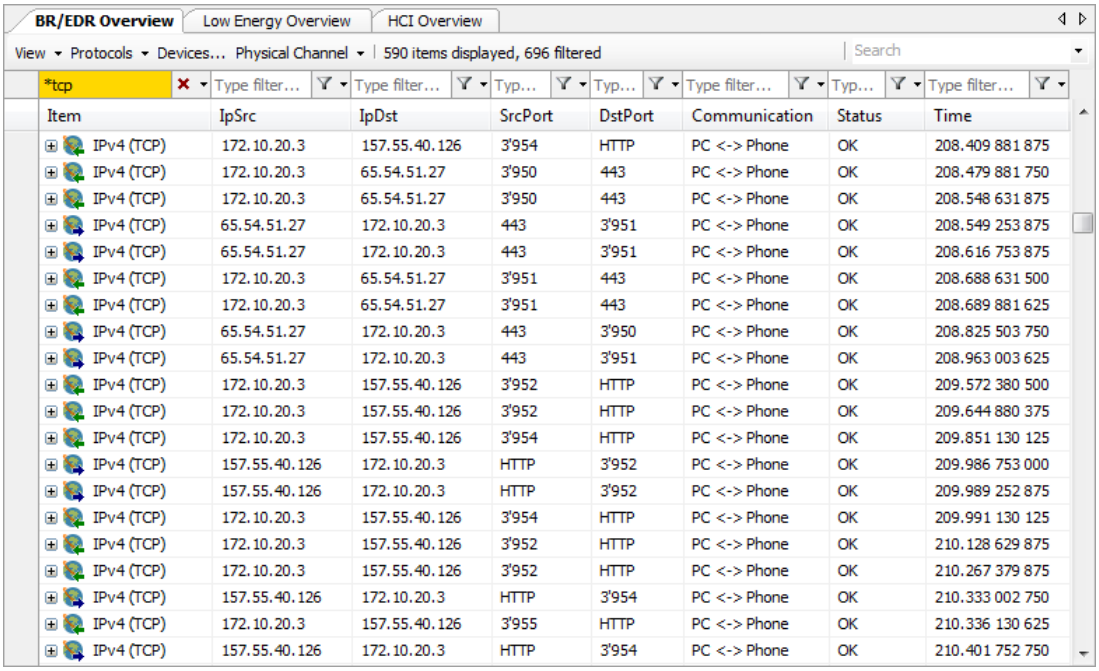
By default, all devices are displayed. The *Devices* window will display all devices captured in the trace, as well as a list of the communications established between them. An easy approach for keeping only the relevant/desired communications is to type the name of the device (or LMP Name), the Company ID, or the BDADDR in the Filter box. Partial text entries work also. This will reduce the list to devices matching what was typed in the box (and reduce what is displayed in the *Overview* to this list).



All devices can be re-enabled/re-displayed by clicking the Keep all button, and then OK.

Customizing the *Overview*

Being able to filter the *Overview* exactly as you wish is nice, but it would not be that useful if it could not be further customized to fit various protocols. Customization is done in a very easy way in the Ellisys software. Just take any field in the *Details* pane, drag-drop it to the *Overview,* and it will appear instantly in a new column. This is especially powerful when combined with *Instant Filters*. The following screenshot shows the *Overview* customized for reviewing TCP traffic. IP addresses and TCP ports have been drag-dropped from the *Details* pane.

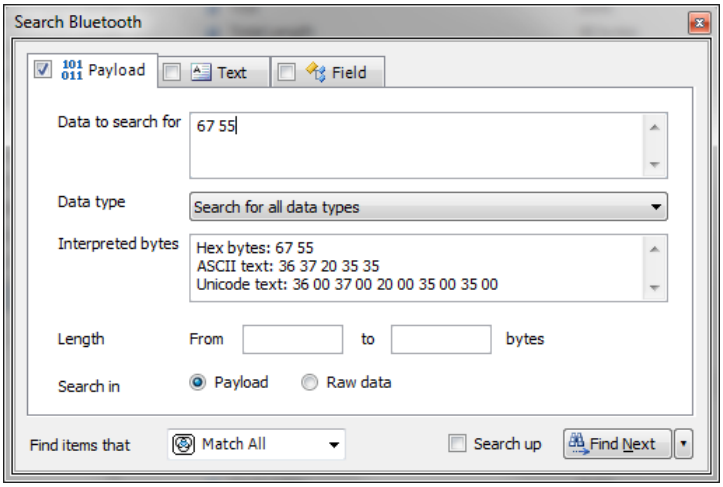


The great thing about this feature is that as soon as a *Details* field has been added to the *Overview* to create a new column, it can then be filtered, searched, used for coloring, exported, etc. This opens a whole world of possibilities. No more frustrations: when something is displayed, it can be used.

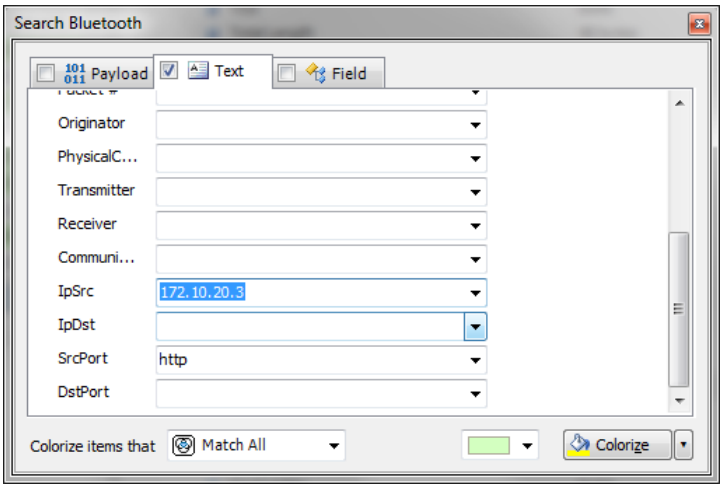
Searching and Coloring

Items can be searched and colored (highlighted). The easiest search feature is the search box located on the top-right of the *Overview*, called *Instant Search*. Text patterns typed in this box will be searched in all *Overview* items and columns.

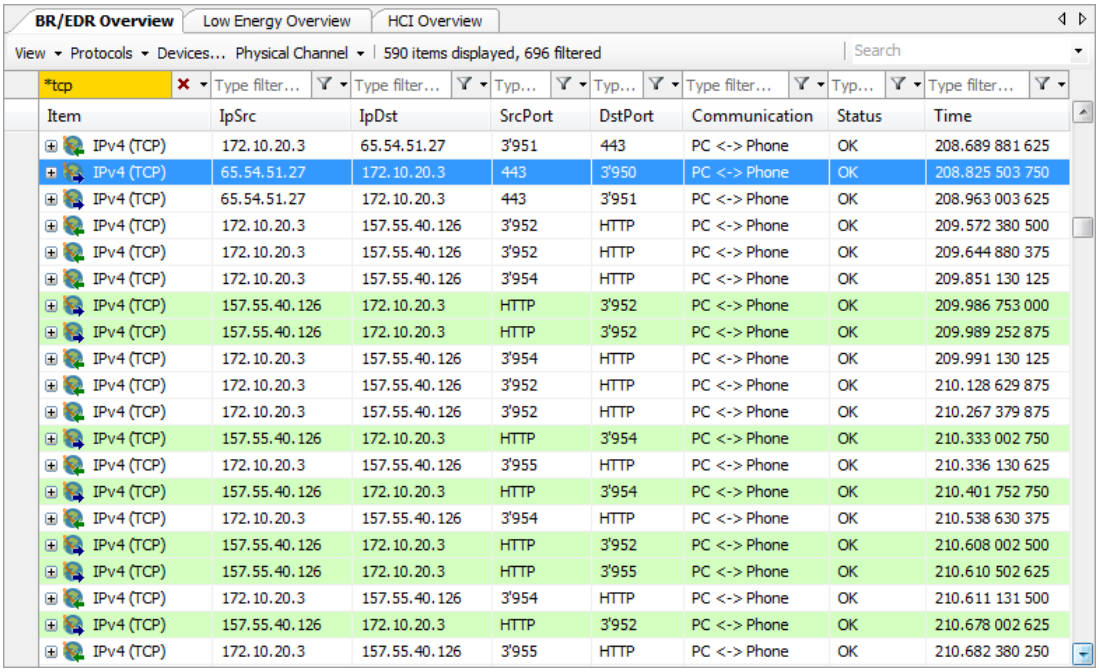
More precise searches can be achieved in the Search dialog, accessible with CTRL+F. Data can be searched, as well as text and fields. Search criteria can be combined to create more advanced searches. Items can be searched, and they can also be colored and counted by using the same criteria.



The following screenshot shows the Search box configured to colorize in green if the IpSrc is 172.10.20.3 and the SrcPort is http:



And the result:

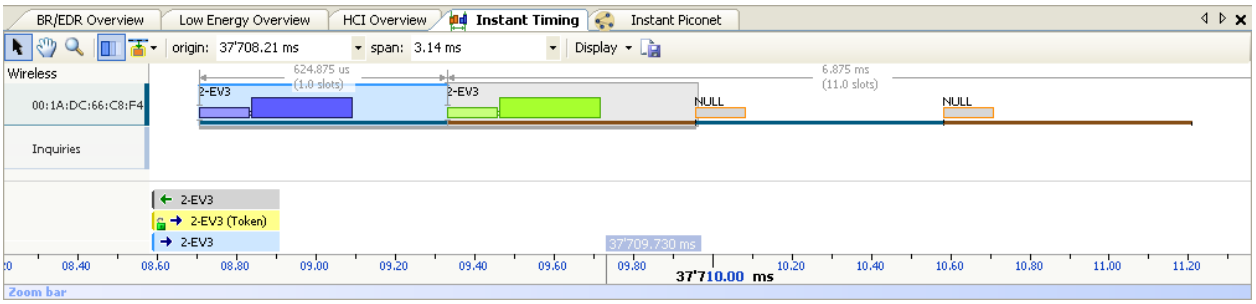


Ellisys Instant Timing

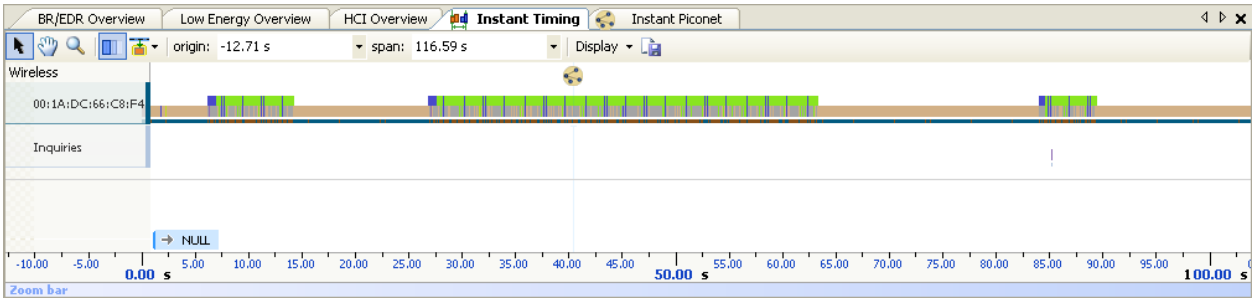
The *Instant Timing* pane displays baseband packets with a precise temporal representation.

The view can be zoomed with the mouse wheel, keyboard UP and DN arrows, or by dragging the zoom bar. The view can be panned by dragging the scale bar, or with the LEFT and RIGHT arrows on the keyboard. Automatic packet detail quotes appear when placing the mouse over packet. A measurement cursor appears when dragging the mouse in the packets area.

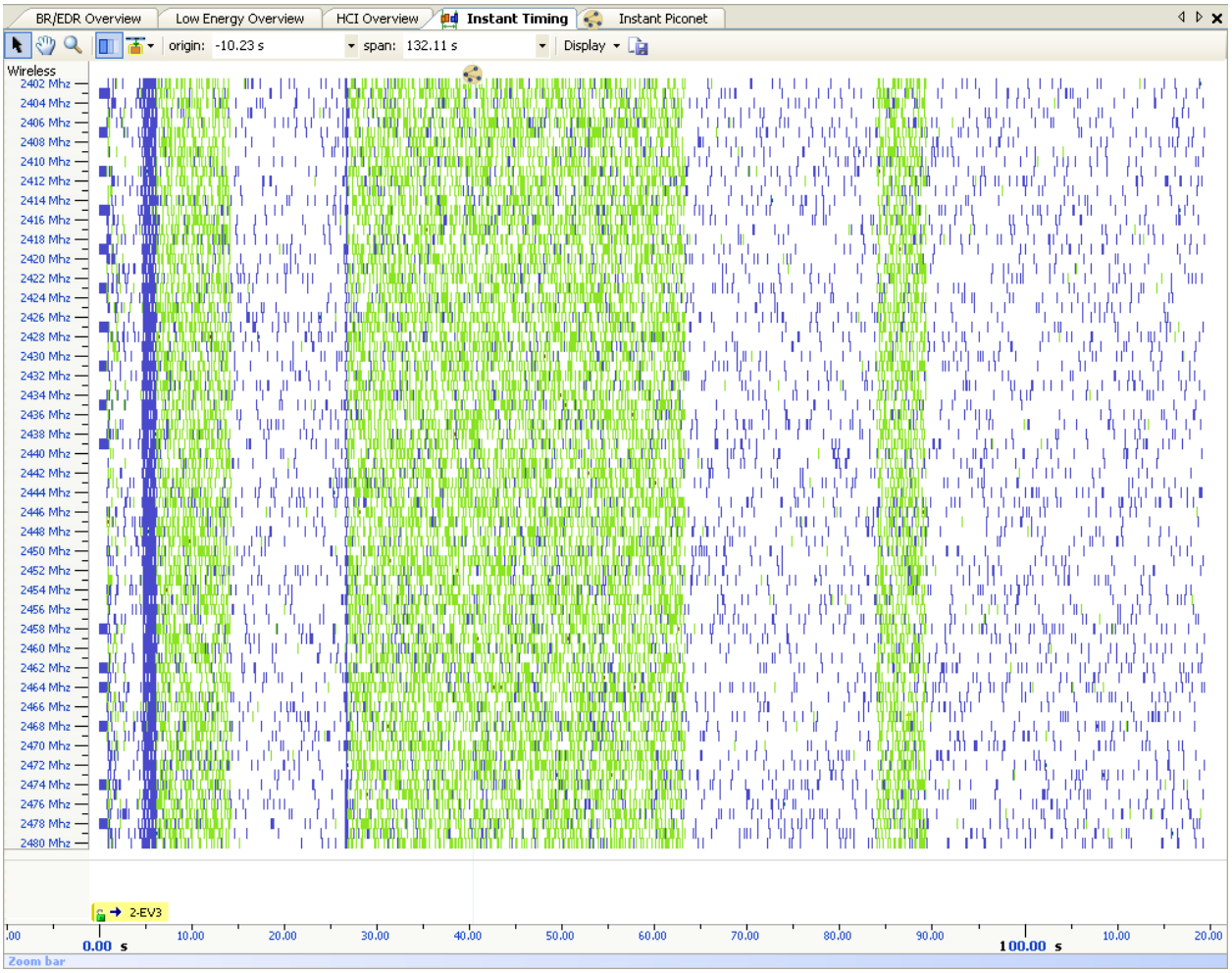
The dynamic range of the *Instant Timing* pane is incredibly high. This view can display details with a hundred nanosecond precision (125ns to be exact, so 1/8th of symbol):



Or, it can show the big picture, by displaying hundreds of seconds of traffic:



The view is configured by default in the "by master device" mode, so each line represents traffic transmitted by a master device and its slaves. The view can alternatively be configured in the "by RF channel" mode, using the Display menu button on the *Instant Timing* toolbar. In this case, packets will be arranged by frequency/RFchannel, as shown below:

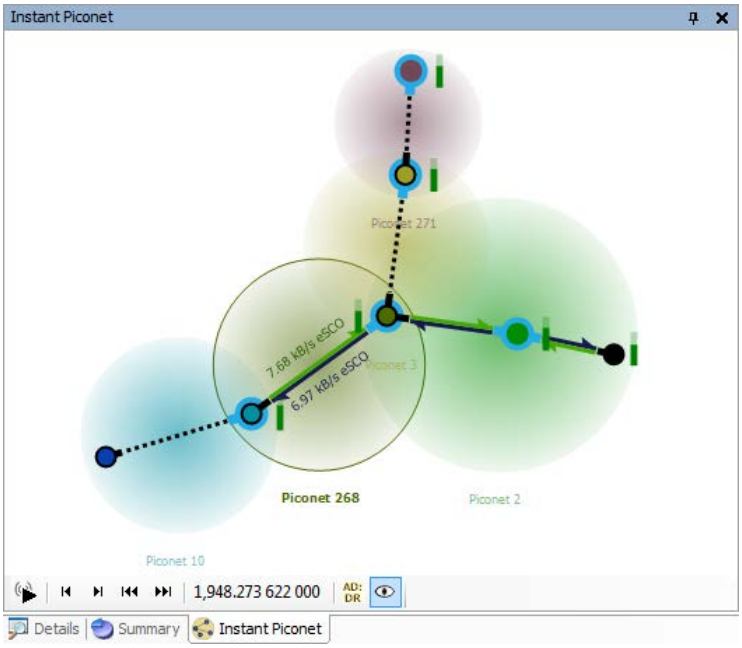


Display filters can be selected from the Display menu button as well, in order to hide establishment traffic (such as inquiries, pagings, and advertisements) and idle traffic (such as poll / null packets and empty packets).

Ellisys Instant Piconet

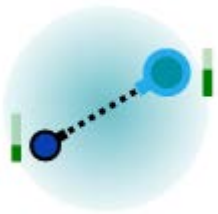
The *Instant Piconet* pane is designed to graphically display the topologies of all captured piconets and scatternets. In addition to topology, the *Instant Piconet* pane displays inquiries and paging events, and the data throughput of active ACL and SCO connections. This view works live (during capture) as is the case with all views in the Ellisys software, and can also be used in playback mode to replay captured traffic.

The following screenshot shows a rather complex scatternet in the *Instant Piconet*:

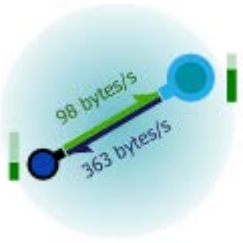


All views/panes are linked together, so changing the selected event in the *Overview* will update the *Instant Piconet* to this position. Clicking on the timestamp in the *Instant Piconet* will synchronize the *Overview*. The *Instant Timing* has a special cursor showing the exact time of the *Instant Piconet* (moving this cursor will update the *Instant Piconet*).

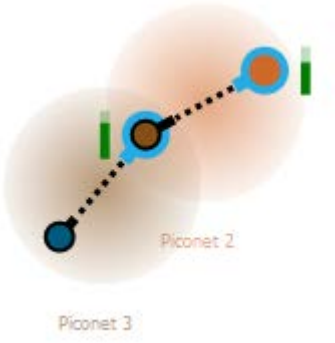
Here is a quick summary of the various representations you can find in the *Instant Piconet*:



Represents a **idle connection** between a master and a slave. Master devices always have a blue outline. Slave devices always have black outline. The gauge on the side represents the RSSI of the device.



Represents an **active data connection**. Throughputs are indicated.



Represents a **scatternet** composed of two simple piconets. The device in the center is the slave of the device on the right, and the master of the device on the left.

Represents an **inquiry**. The inquirer device is represented with blue outline, like masters, while responding devices are represented with black outline.

Represents a **paging**. The pager device is represented with blue outline, like masters, while the paged device is represented with black outline.

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.

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_BT03 - Your First Wide-Band Capture
- EEN_BT04 - Optimal Placement of Your Analyzer
- EEN_BT05 - Understanding Antenna's Radiation Pattern
- EEN_BT06 - Bluetooth Security - Truths and Fictions
- EEN_BT07 - Secure Simple Pairing Explained
- More Ellisys Expert Notes available at: http://www.ellisys.com/technology/expert_notes.php

Rev. A. Updated 2011-05-16