Analyzer Features Tour

Getting Personal with Your Environment

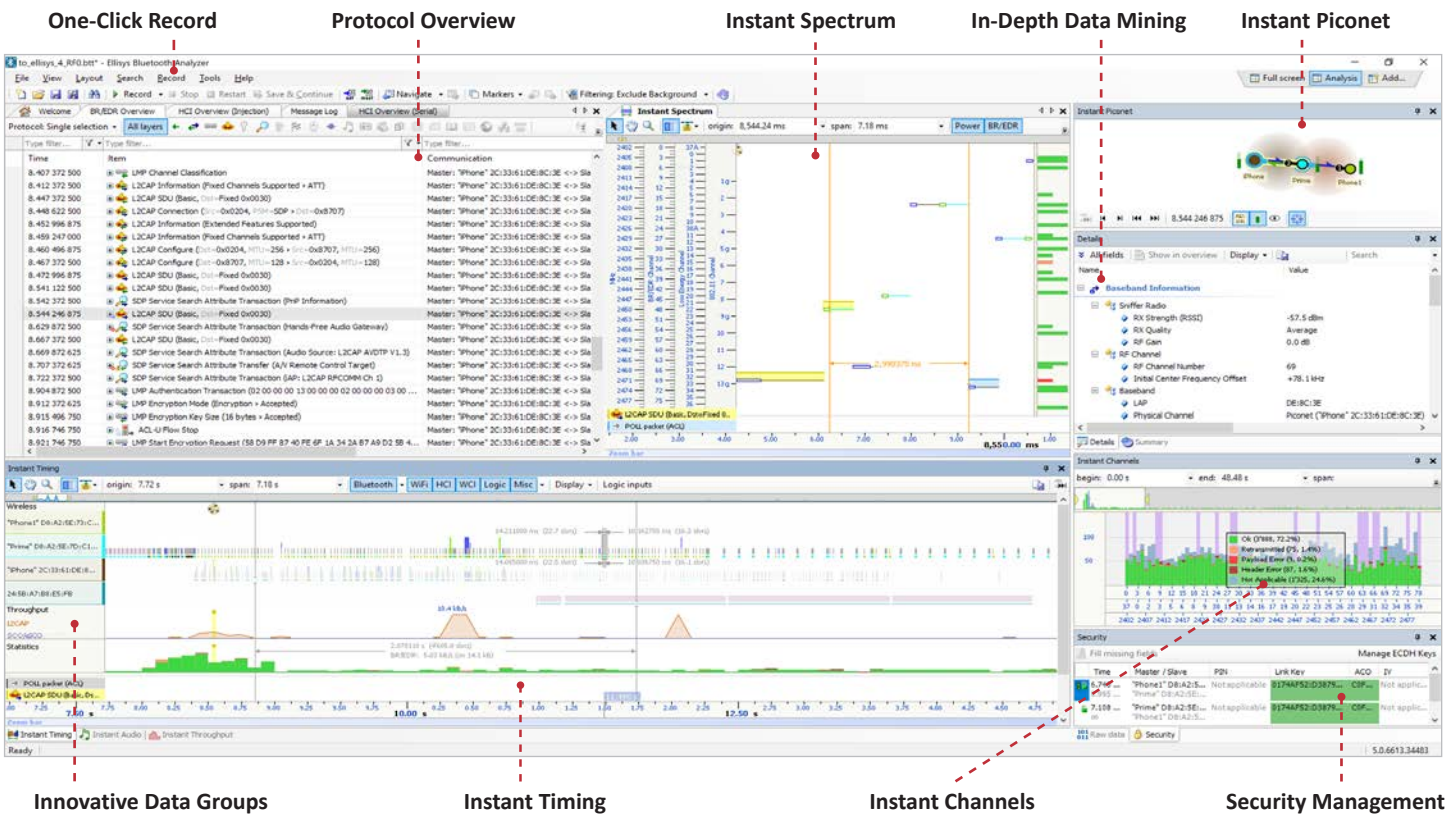
Introduction

Ellisys Bluetooth products are loaded with features and innovations designed to help engineers efficiently understand challenges and optimize performance of their designs and implementations. This Ellisys Expert Note provides a quick walk-through of many of the Ellisys application software capabilities. Refer to the User Guide (located in the **Help** menu) for detailed information on these features.

The Big Picture

Ellisys analyzers are capable of capturing and characterizing BR/EDR, Bluetooth LE, Wi-Fi, raw spectrum information, various HCI interfaces (SPI, UART, USB), WPAN (802.15.4), generic communications interfaces (SPI, UART, I2C, WCI-2, and SWD). All of these can be captured concurrently and with precise central timing.

HELPFUL HINT: The easiest way to become familiar with the Ellisys Bluetooth analysis software is by opening one of the saved captured files provided. These capture samples can be loaded from the **File** menu by selecting Load Sample. Samples are included for both BR/EDR and Bluetooth Low Energy.



Note that the various analyzer models and configurations will have some variability in terms of what is supported (check the user guide for details).

To manage this broad spectrum of capture capabilities, the Ellisys Bluetooth software application provides a variety of features for analyses relating to timing, protocol operations, physical layer behaviors, audio applications, HCI operations, Wi-Fi and WPAN activities, throughput, statistical information, channel quality analyses, topology behaviors, and much more.

As alternatives to operation of the analyzer using the analyzer application software, users can employ an automation API or a command line interface (CLI). See the user guide for download links.

Ellisys Protocol Overviews

The Overviews are the central views of the analysis software. These views will show captured traffic ranging from the most primitive elements to the most complex and hierarchical transactions, and with a great variety of functionality and configurability.

All enabled Overviews (i.e., selected in the **Recording Options** dialog) are populated concurrently, for example when capturing over-the-air (OTA) traffic and Host Controller Interface (HCI) traffic.

There is an Overview for each traffic type captured. Traffic types include BR/EDR, Bluetooth LE, HCI interfaces (SPI, UART, USB, injected), generic communications (I2C, UART, SPI, SWD), Wi-Fi, WPAN (15.4) and others. Note that capture of certain traffic types are model- or configuration-dependent.

An exceptional amount of configurability is provided, including protocol-specific views, powerful textual filtering, searching, colorizing, column add/remove/position, timing measurements, a variety of automated checks and advisories, summary information, and more.

Figure 1 shows traffic in the BR/EDR Overview.

HELPFUL HINT: To see your specific model and configuration, attach your unit to your computer, then check the serial number tab in Help > About.

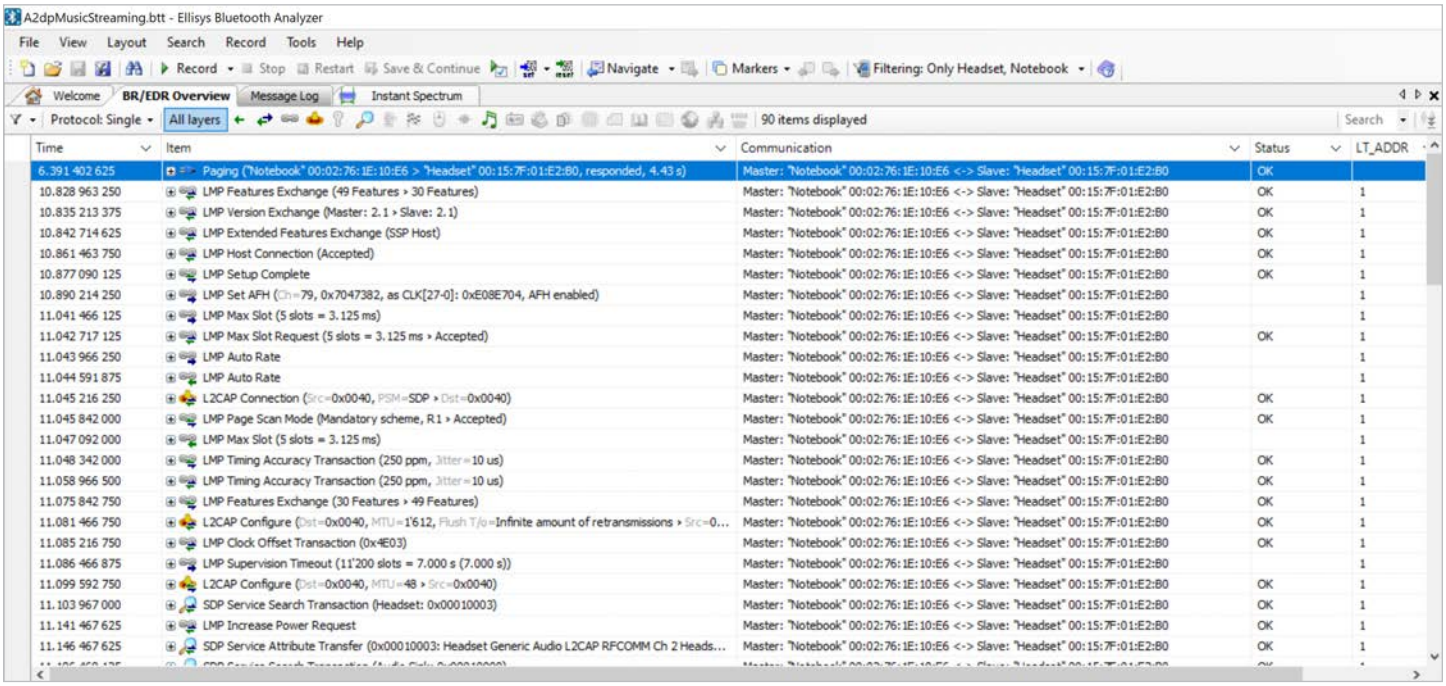


Figure 1 BR/EDR Overview.

HELPFUL HINT: Try a right-click in an Overview and explore the options/selections.

Note the parenthetical summary information provided in the Item column. These can serve as a quick idea as to what sort of information is being exchanged.

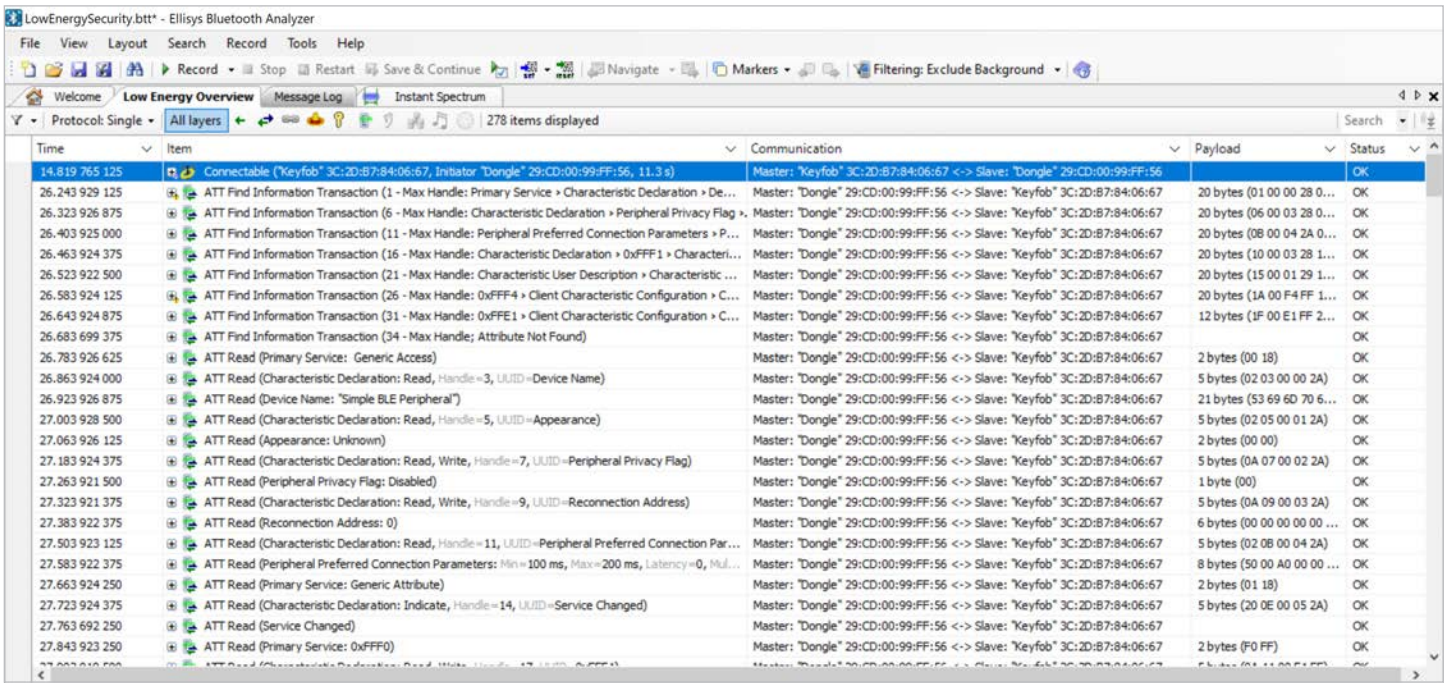


Figure 2 Bluetooth Low Energy.

Figure 2 shows Bluetooth Low Energy Overview.

The Overviews are made to be easily readable. Traffic is grouped hierarchically into protocol layers. The protocol "stack-up" can be easily reviewed by navigating into the tree nodes. Packet-only, Baseband, L2CAP, and Link Layer views are also available.

Let's look at **Figure 3**. We can see a BR/EDR 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.

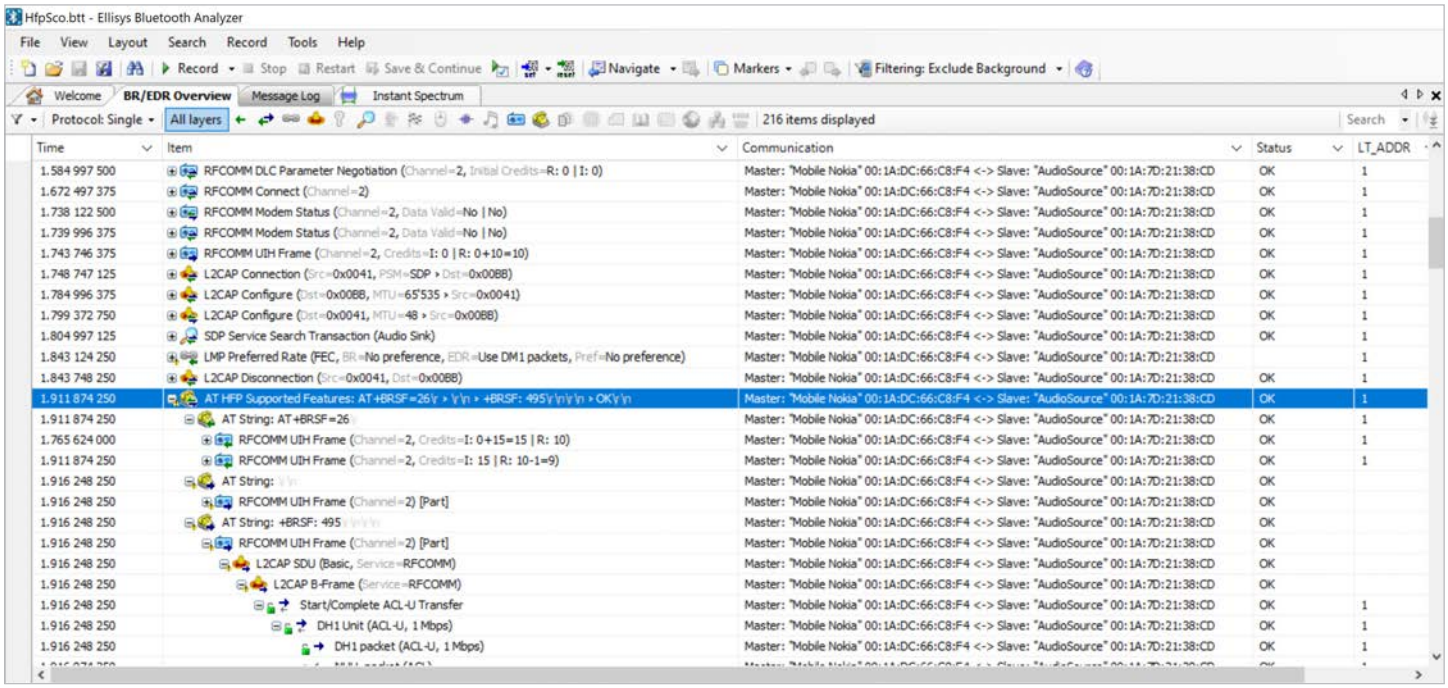


Figure 3 Tree Node Structure of an AT BR/EDR Transaction.

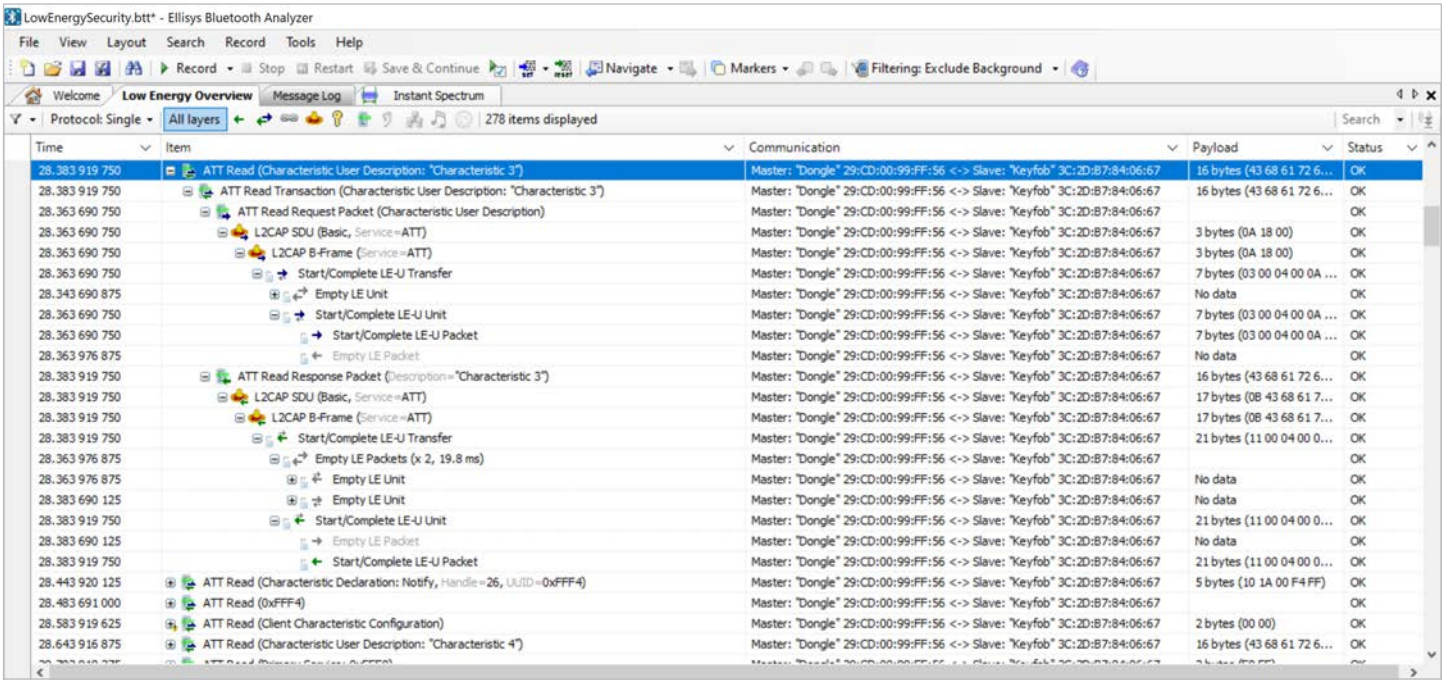


Figure 4 Tree Node Structure of a Low Energy ATT Read Request.

HELPFUL HINT: As you click through the tree, selecting different protocol layers, for example L2CAP or Link Layer, or packets-only, the level of hierarchy in the Details view follows, i.e., if selecting a packet, the Details view (described in the next section) shows the packet elements, and if selecting the ATT transaction, the Details view will show the request and the response (where applicable), and if selecting just the request, the Details view shows just the request. Try this out – the operation will seem intuitive and sensible after a little experimentation.

For the rest of our tour walk-through we will start out with the **LowEnergyWatch.btt** trace sample, which contains ATT traffic between a watch and a mobile phone (see **Figure 4**). Similar to **Figure 3**, notice the tree node structure for Bluetooth Low Energy.

Note that there is a high-level hierarchy that includes (where applicable) a request/response pair on the highest element. The individual parts of the transaction can be seen by opening the tree as shown in **Figure 4**. Note also that this highest-level line includes some parenthetical summary hints as to what is "underneath," potentially saving you some time. This highest level can be removed to show the request/response pair as the highest element. This is done by deselecting Group Transactions in the **Protocol** drop-down menu at top-left of an Overview.

Details View

The line selected in an Overview can be reviewed in extensive detail within the Details view. The following screenshot shows the details of an ATT Write Request (see **Figure 5**), and below that, the associated ATT Response. As you can see, not only is the ATT Write Request displayed, but the lower layers (such as RF, Link Layer and L2CAP) 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 selected ATT Write Request, we see quite a bit of information readily available, starting with lower layer items at the top (RSSI, RF channel, encryption, retransmission statistics, timings, etc.) then a progression through the L2CAP layer, and finally to the protocol (ATT) at the bottom.

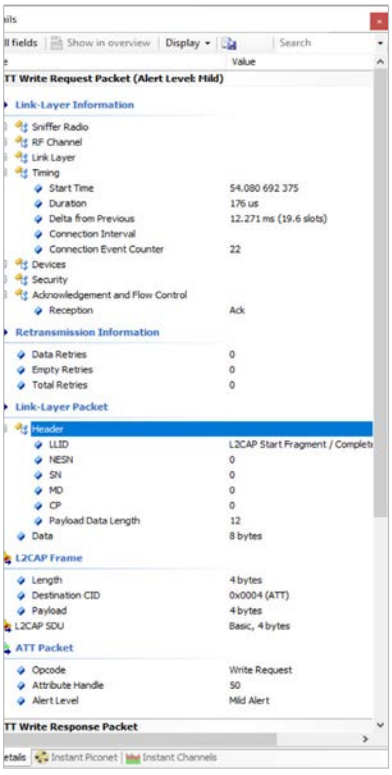


Figure 5 Details View.

The ATT Write Response is detailed similarly to the ATT Write Request. It clearly shows the returned ATT Write Response quite effectively; however, if you know Link Layer, you also know that it is a very flexible protocol, requiring many fields to describe this dynamic protocol.

The Details view in **Figure 5** looks somewhat abbreviated, and it actually is. By default, the Ellisys software only displays the most relevant information, and hides information which is not generally useful for understanding, such as valid CRCs, lengths, reserved fields, etc. Of course these hidden fields can be shown as needed (see the **All Fields** toggle in the **Details** toolbar), and will automatically be displayed if there is anything wrong with them (so an incorrect CRC will not be missed for example).

In **Figure 6**, the same ATT Write Response event is shown with all fields enabled. The grayed lines are those that are hidden by default.

Ellisys Protocol Toolbar

As seen in **Figures 5 and 6**, the Details view conveniently displays all protocols in a single view. This is very useful in understanding the sequence of events and protocol inter-relationships. For example, it's easy to see the ATT request, the L2CAP connection, ATT response and the ATT data. But sometimes you need to focus on a particular protocol, or traffic with specific characteristics. There are two features that are quite useful for this purpose — the Overview's protocol toolbar (described in this section), and the Instant Filters (described in the next section).

A protocol toolbar is located atop all Overviews and is customized to fit the characteristics of the particular Overview. This is very useful for switching between Bluetooth protocols, like Attribute protocol, L2CAP, Security Manager Protocol (SMP), RFCOMM, etc., or between protocol layers, like Link Layer, baseband, packet-only view, etc.

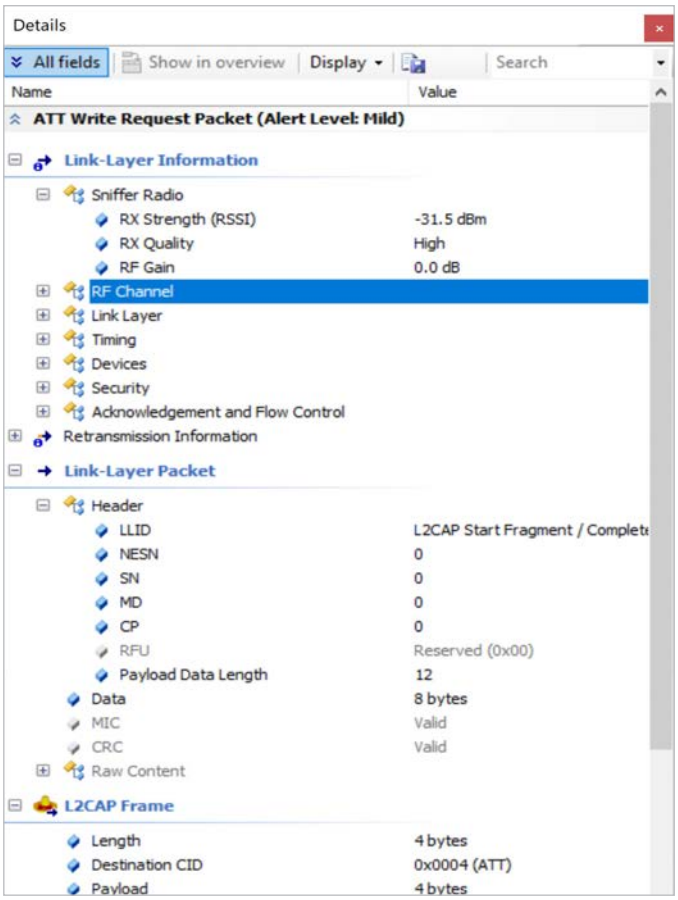


Figure 6 Details View (Expanded).

By default the **All Layers** button is enabled, showing all protocol layers. While this is very useful for understanding the global sequence of events, sometimes it is useful to focus on a single protocol layer.

HELPFUL HINT: Add the "Originator," "Transmitter," and/or "Receiver" fields as an Overview column to see device roles at a glance (you can even colorize these if desired). This can be done by dragging that field from the Details view (the lower protocol layers will show a "Devices" section that includes this field) and dropping it into the Overview, or just right click on the Overviews header and select the desired field(s).

You can also see highlighting of the selected packet or transaction in the Instant Timing view (discussed later), and a flyover there on the packet of interest will produce a pop-up with quite a bit of information.

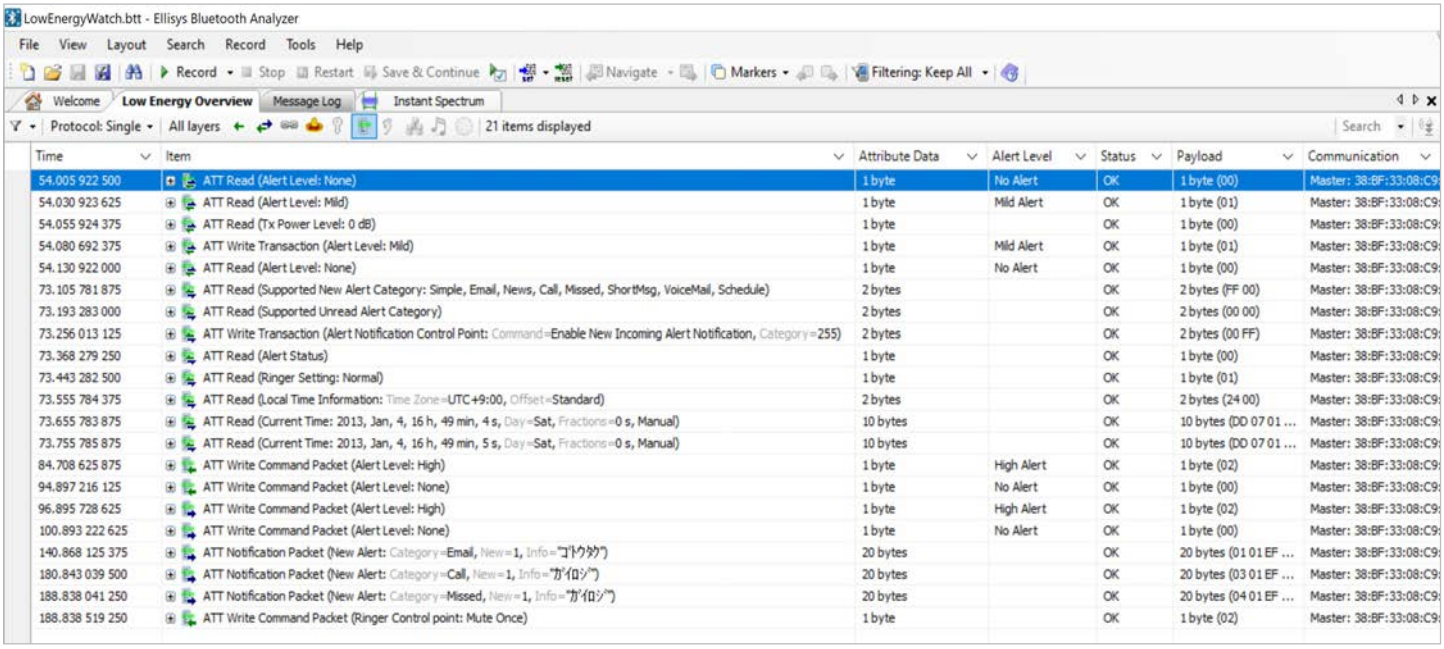


Figure 7 Protocol Toolbar – ATT Only.

For example, if we want see what is going on at the ATT level, we can just click the **ATT button** and we quickly get this view (see **Figure 7**).

Then let's say we wish to look at only L2CAP, so just click the **L2CAP button** and we get the following (see **Figure 8**).

As you may notice, the complement of columns is fully configurable and independent between the different protocol selections, which is quite handy when working extensively with several protocols at the same time.

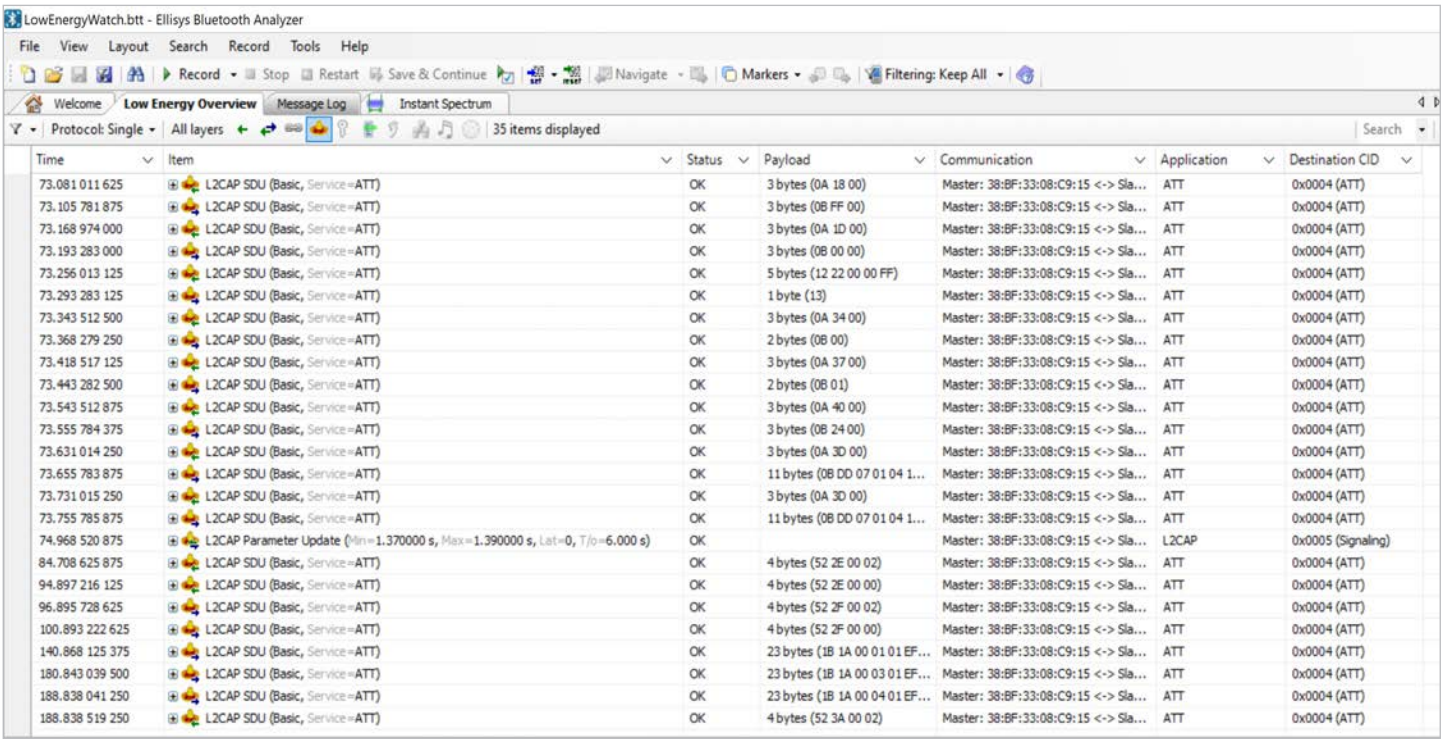


Figure 8 Protocol Toolbar – L2CAP Only.

HELPFUL HINT: Use the Protocol: drop-down menu to specify whether you want to see one protocol selection at a time or any combination of multiple protocols.

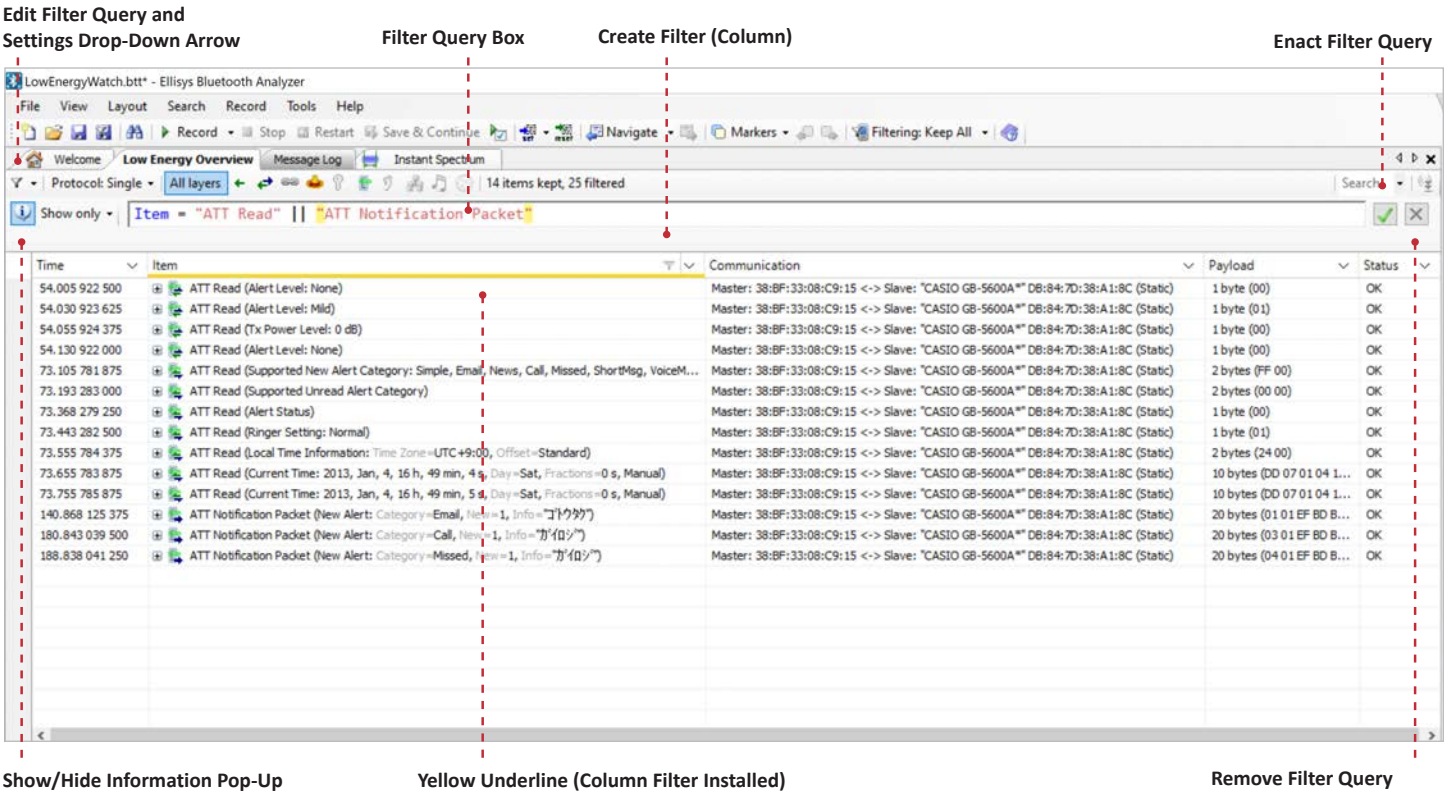


Figure 9 Instant Filters.

Instant Filters

Understanding the various filter approaches throughout the application is key to becoming an expert with the tool. The User Guide (located in **Help** > **User Guide**) describes all filtering approaches in detail.

One of the most common filters customers use is the Instant Filters, which operate on the selected Overview. These filters are enacted as query-based textual entries in the **Filter Query** box located atop the columns in the Overviews. See **Figure 9**.

Instant Filters are quite powerful and can be used to efficiently and precisely locate and display information of interest during capture or on saved captures, using a variety of operators, comparators, and expressions. A helpful pop-up is provided to guide the user in creating these filters. See **Figure 10**.

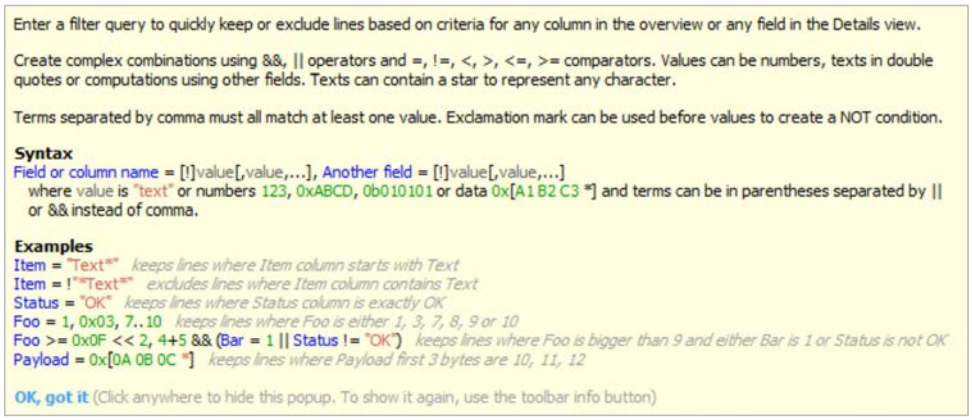


Figure 10 Instant Filters Pop-Up Guide.

Filters can be stored, recalled, and annotated as favorites. Data and information on which these filters operate can be in the active Overview or in the Details view, but it is not required to place fields from the Details view into the Overview to use these fields in a filter query.

Instant Filters are based on simple text patterns and accept a variety of common operators, including wildcards (*). They can be created by typing the desired filter or conveniently, by using a right-click on a column-row intersection in the Overview.

HELPFUL HINT: The auto-complete feature means you'll never have to remember specific packet types, commands, etc. Just start typing in the Filter Query box and the application will suggest options.

Let's walk through a simple example. We want to keep only ATT commands, but we want to filter even further on just the 'ATT Read' traffic.

We can simply type "ATT Read" in the Item column's Instant Filter box.

Item = "ATT Read"

This will keep/show any line beginning with "ATT Read", as shown in **Figure 11** below.

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

Item != "ATT"

Add a comma separator to include another term in the filter, for example:

Item ! = "ATT" "SMP".

Ranges are supported in numeric columns. A range is specified such as start..stop (i.e., separated by two periods). For example, to keep/show items occurring between 0 and 1 second, simply type "0..1" in the Time column's Instant Filter box.

See the User Guide for more examples and additional details.

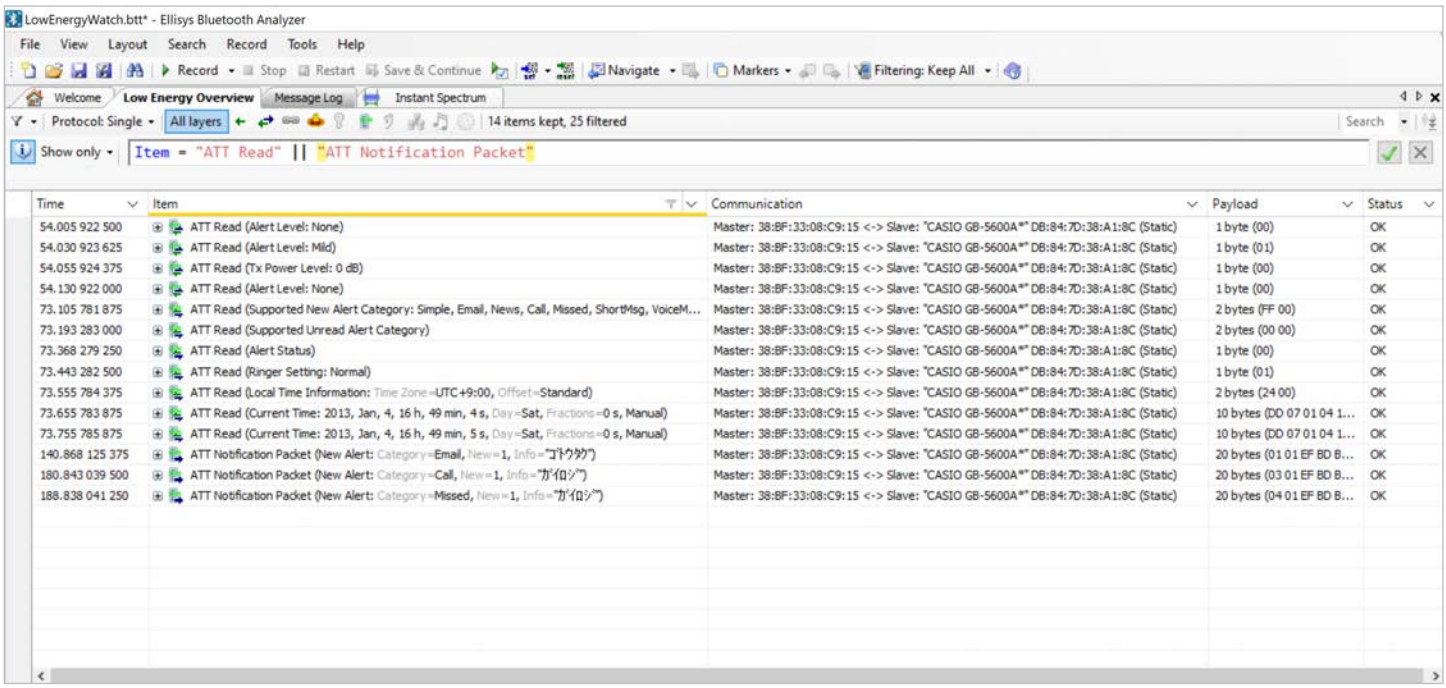


Figure 11 Instant Filters.

HELPFUL HINT: An easy way to specify a filter is by right-clicking on a line at a specific column/row position, and the contextual menu will offer to keep or exclude the traffic type/field selected.

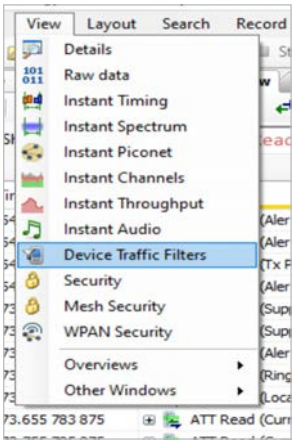


Figure 12 Device Traffic Filters.

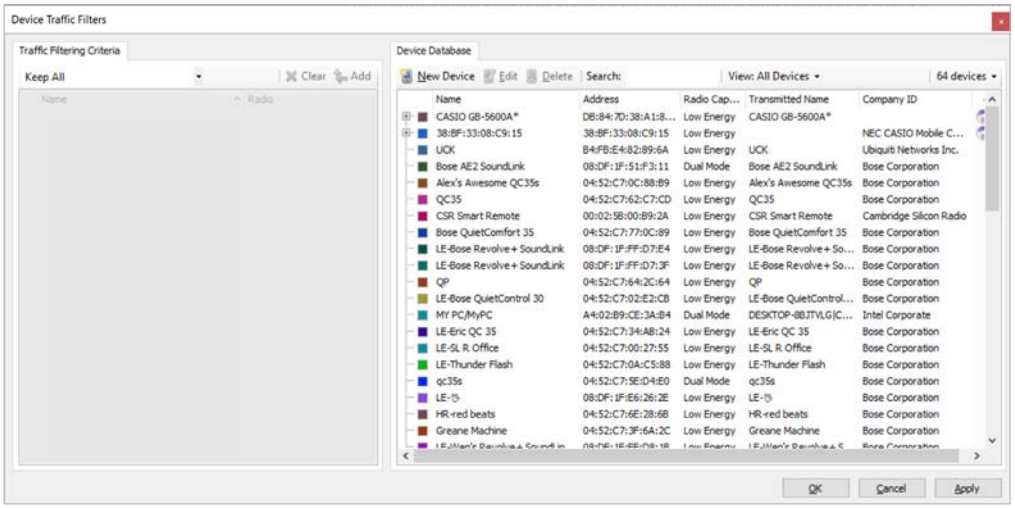


Figure 13 Device Traffic Filter Displaying All Devices.

HELPFUL HINT: In most windows where you see a Bluetooth Device Address (such as an Overview, the Instant Piconet, or the Security window), you can use a right click to install a device-based filter.

Filtering by Devices

When using a wideband sniffer, all device activity in the area will be captured. A device-based (BD_ADDR-based) filter is the "biggest" filter available, and can be useful when you want to focus only on particular devices and/or communications of interest.

In addition, you can get even more creative with device filters by using the **Device Traffic Filter** feature. This is available from the **View menu** (see **Figure 12**) or from the **Filtering**: drop-down selection at the top of the UI.

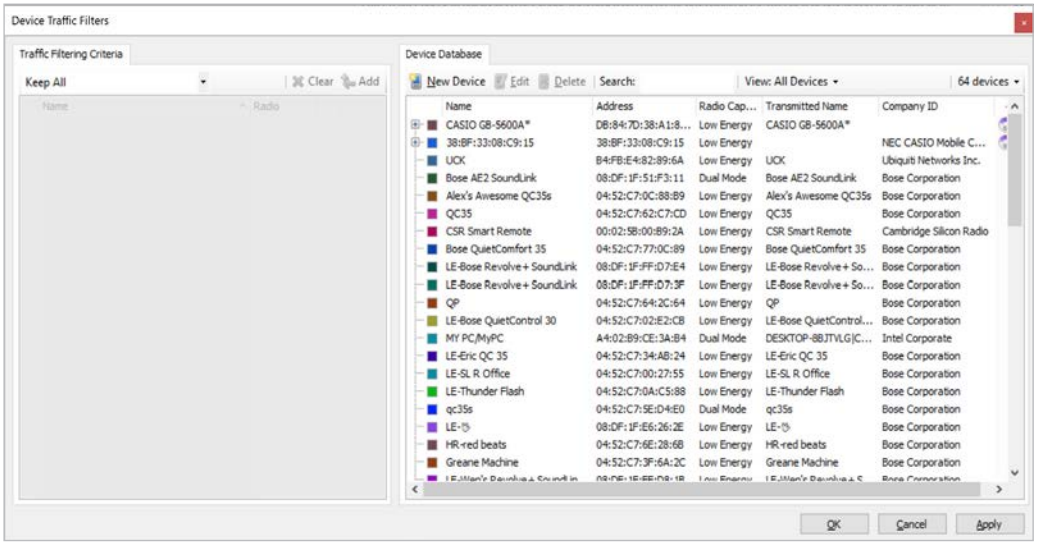


Figure 14 Device Traffic Filter Displaying Name of Device.

HELPFUL HINT: An easy approach to finding the devices desired is to type the Transmitted Name of the device (or Name), the Company ID, or the BD_ADDR in the Filter box. **See Figure 14**. Partial text entries will also work. 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).

By default, all devices are displayed, (See **Figure 13**) which is consistent with the **"Exclude Background"** or **"Keep All"** selections in the **Filter:** drop-down menu at the top of the GUI (and also shown in the Traffic Filtering Criteria section of the Device Traffic Filters window. The Device Traffic Filters window will display all devices captured historically, as well as devices present in the current trace (an icon is provided to designate which devices are in the active/opened trace). A hierarchical list (annotated by a + sign) of the communications established between them is also available to display.

The device can then be added to the left area of the window (Traffic Filtering Criteria) in order to keep only the traffic between or amongst the specified devices, i.e., Keep Only or Keep Involving. If only one device is specified, then all the traffic to and from this device will be displayed. This is known as a Keep Involving filter, which will show all traffic to and from the selected device(s). A Keep Only filter is deterministic, i.e., these show traffic between the selected devices only.

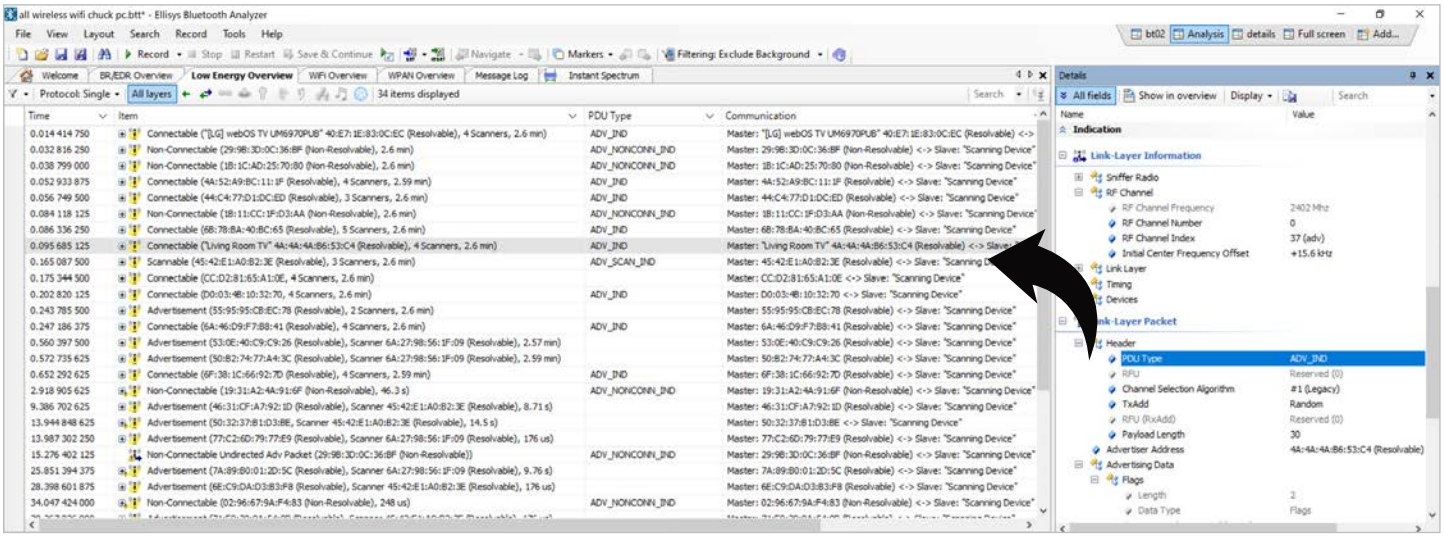


Figure 15 Overview Customized for Reviewing PDU Type Traffic.

HELPFUL HINT: Errors are highlighted in the Item column using a color-coded icon and fly-over pop-up to indicate the relative severity of the error, summarized in a dedicated status column (such as "warning" in the figure above), and described in the Details view.

Customizing an Overview

Customizations of the Overview are achieved very easily, and there are many of these available. One of the more popular customizations is the drag/drop of a field from the Details view to create a new column in the Overview. 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 useful when combined with Instant Filters, although Instant Filters can operate on any field, whether or not the field is displayed in an Overview column. **Figure 15** shows the Overview customized for reviewing PDU Type traffic.

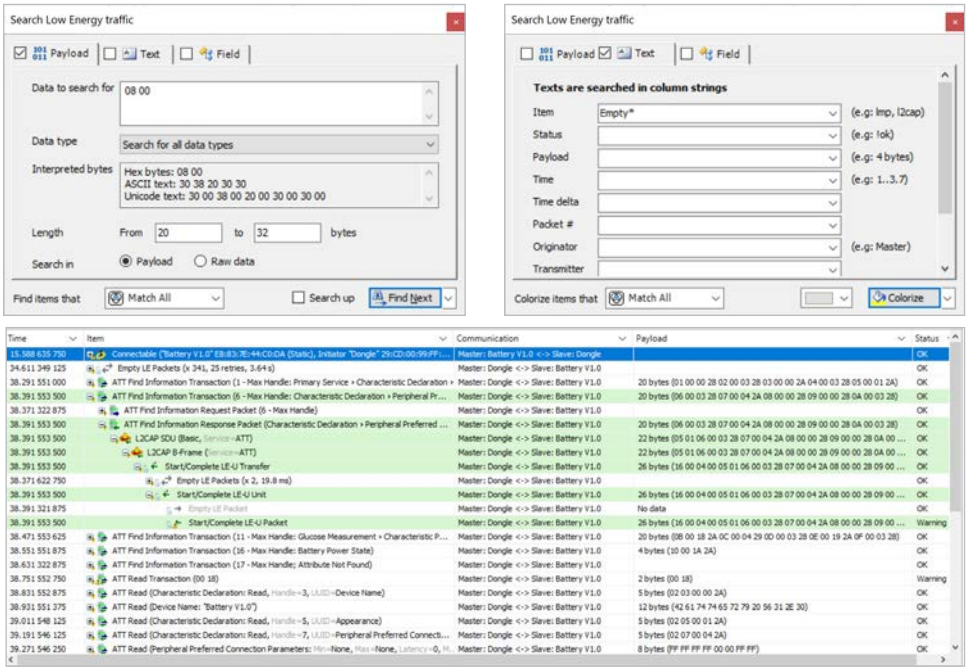


Figure 16 Using 'Colorize'.

Searching and Coloring

Items can be searched and colored (highlighted). The simplest 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 active Overview items and columns.

More precise and advanced searches can be achieved in the Search dialog, accessible with CTRL+F. In **Figure 16**, the user searches for payloads that include 08 00 in payloads having lengths from 20 to 32 bytes.

In addition to data searches, text and fields can be searched. Search criteria can be combined to create more advanced searches.

The Search box changed from Search to Colorize to colorize in any empty packet fields.

HELPFUL HINT: Data can be searched in multiple formats (e.g., hex, ASCII, Unicode). In addition to searching, the Search **dialog's function button** (bottom-right of the window) can be changed to count or colorize according to the criteria specified by the user.

Instant Timing

The Instant Timing pane displays packets with a precise temporal representation. Any packet captured is represented here, as are any logic signals captured. Throughput and statistical information are also presented. A measurement cursor appears when dragging the mouse in the packets area. Very precise measurements can be made between any captured events (e.g., Bluetooth to Bluetooth, Logic to Wi-Fi, HCI packet to Bluetooth Air packet, etc.).

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).

The view is configured by default in the "by master device" mode, so each line represents traffic exchanged between a master device and slave devices in the piconet (via BR/EDR).

Figure 17 is a view of Bluetooth traffic, zoomed out a bit (note the throughput and statistics indications once "Laptop" begins to send data.) Or, **Figure 18** displays that it can drill down (zoom in) on precise traffic.

Figure 17 Bluetooth Traffic.

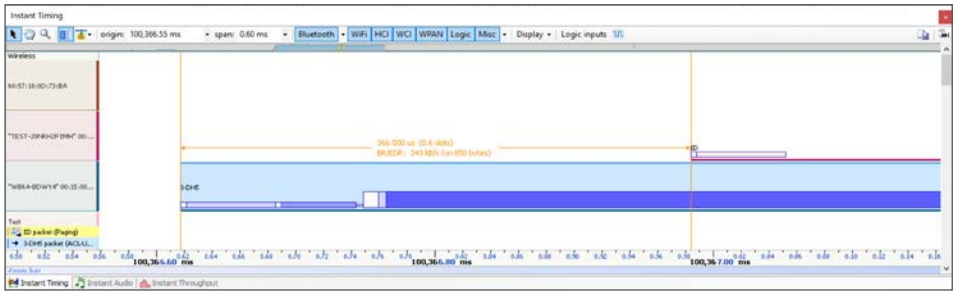


Figure 18 Precise Traffic.

As mentioned, everything captured is represented in **Figure 19**. Here, we see over-the-air traffic at the top, with Serial HCI and several logic signals.

HELPFUL HINT: This view can be zoomed with the mouse wheel, keyboard UP and DN arrows, or by dragging the zoom bar. This view can be also 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.

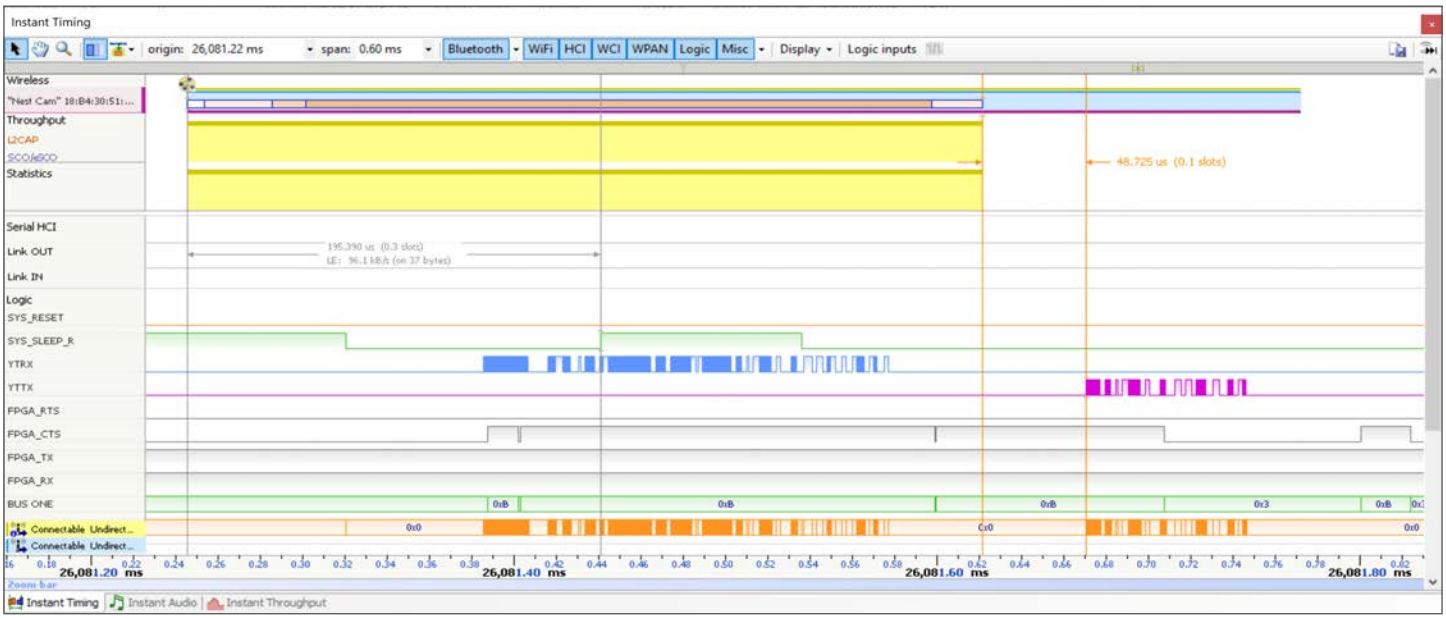


Figure 19 Over-the-air Traffic with HCI and Logic Signals.

HELPFUL HINT: Display filters can be selected from the **Display menu** button on the Instant Timing toolbar 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).

Instant Piconet

The Instant Piconet pane is designed to graphically display the topologies of all captured devices, piconets and scatternets. In addition to topology, the Instant Piconet pane displays inquiries, pagings, advertisements, broadcast events, generalized signal strength, and the data throughput of active 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.

Figure 20 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** on the **Instant Piconet** toolbar will synchronize the Overview.

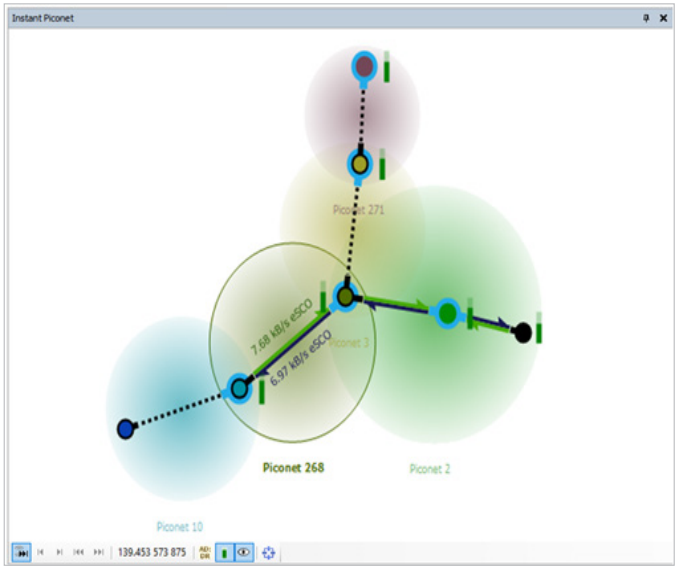
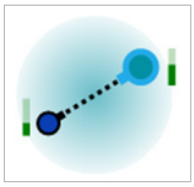


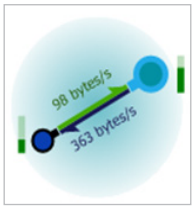
Figure 20 Instant Piconet.

HELPFUL HINT: The Instant Timing has a special cursor showing the exact time of the Instant Piconet (moving this cursor will update the Instant Piconet).

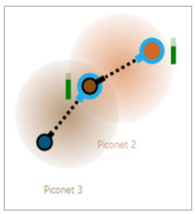
Below is a quick summary of the various representations you can find in the Instant Piconet. See the User Guide for more details.



Represents an **idle connection** between a master and a slave. Master (or Central) devices always have a blue outline. Slave (or Peripheral) 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** or **scanning**. 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.

HELPFUL HINT: With today's typically high prevalence of Bluetooth LE devices and broadcast events and generally busy lab environments, the Instant Piconet view can get very busy with broadcast events. To add clarity, you can deselect the **Broadcast icon** (the eye on the Instant Piconet toolbar) to hide representations of broadcast devices and show only formed connections. Any device filter applied will also affect this view (and other views) by removing devices not included by the filter. Once Broadcast packets are hidden, and your device filter installed, re-enable broadcast events to see such events should they occur with devices selected in your filter.

Instant Channels

The Instant Channels feature provides visual cues and statistical analyses on various per-channel transmission characteristics, including packet retransmissions, header errors, AFH indications, and payload errors. A summary of the selected span shows a count and percentage of categorized packets.

The Instant Channels view provides immediate indications of the channels on which devices are communicating, which channels are being avoided, and important statistics like retransmissions, payload errors, and header errors.

In **Figure 21**, it is clear that the communications between the devices are avoiding three areas, which are typically occupied by Wi-Fi channels 1, 6, and 11 (see the scale at the bottom of the view). Note that the retransmission rate is fairly low, indicating that in this case, the devices are doing a good job of communicating in spite of Wi-Fi interferences.

In **Figure 22** the value of the Ellisys software really becomes apparent. We see AVDTP communications (audio) between a computer and a set of headphones, and characterizations of per-channel performance (Instant Channels), spectrum (Instant Spectrum), and we can actually hear the audio (Instant Audio) as it is recorded (or afterwards).

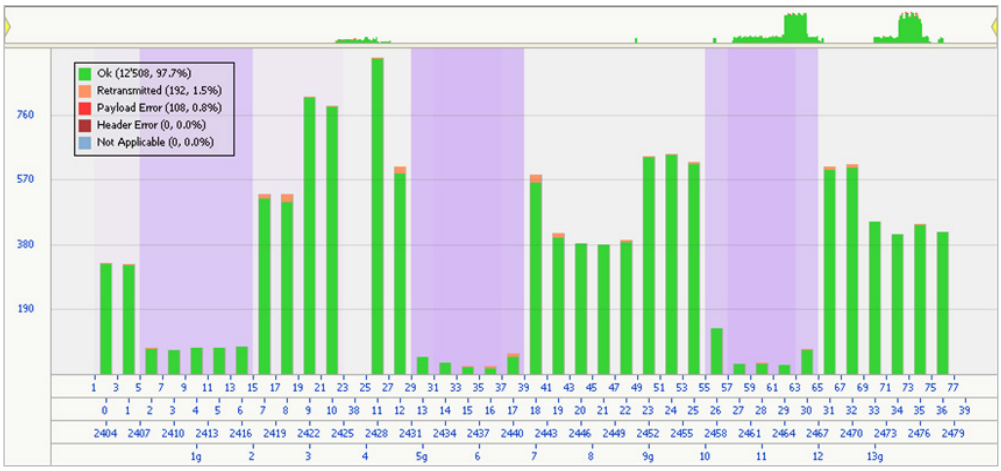


Figure 21 Instant Channels View Showing Wi-Fi Channels 1, 6, and 11 Being Avoided.

HELPFUL HINT: The Instant Channel view, like most views, is sensitive to any device filters established. If no filters are established, then this view shows an aggregate performance characterization (i.e., all devices). When a device filter is established/active, all characterizations are particular to the devices included in the filter.

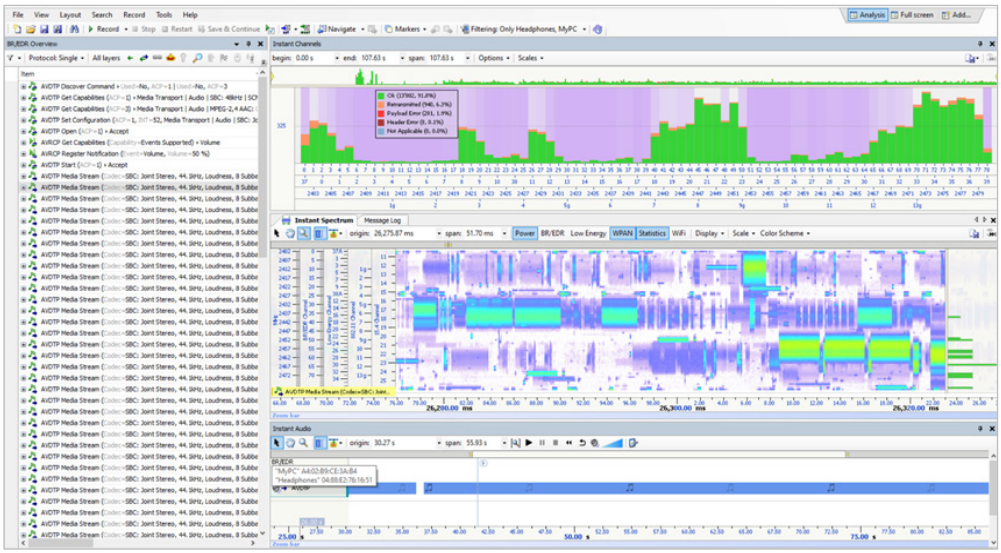


Figure 22 Feature Coherency.

HELPFUL HINT: The position of the analyzer relative to the devices being analyzer can affect payload and header error numbers. Retransmissions however are generally considered an excellent indicator of spectral-related performance. See Expert Note, EEN_BT04 "Optimal Placement of Your Analyzer" for more information.

Note the color scheme in the Instant Spectrum view, as it indicates very strong (Wi-Fi) signals at the top, middle, and lower portions of the Bluetooth spectrum (Wi-Fi channels 1, 6, and 11). Two things are worth noting here: one, the performance indicated in Instant Channels is very good, especially considering the very busy spectrum (a fairly low percentage of retransmissions are indicated), and two, the audio (Instant Audio) plays back very well (no pops or noticeable quality issues). The value of multiple characterizations and friendly software that is easily configured is also apparent.

HELPFUL HINT: The various shades of magenta in the Instant Channels view are intended to indicate a relative frequency of channel avoidance over the time period selected (the entire trace in this case, about 107 seconds.) Use the Nav Bar at the top of the Instant Channels view to select a portion of the trace to characterize.

Instant Spectrum

As we saw in the prior section, the Instant Spectrum feature can be used to understand the physical environment and how it may be affecting your device's performance. This feature, another Ellisys innovation, provides a unique and intuitive way to understand the spectral behaviors of Bluetooth, Wi-Fi, and WPAN traffic, as well as all other RF events within the ISM spectrum that is used by Bluetooth (e.g., a microwave oven).

Bluetooth, Wi-Fi, and WPAN packets are presented chronologically left to right on the channel they are transmitted and are uniquely color-coded per the packet's sender. On the right, graphical per-channel statistics on Bluetooth packet errors and retransmissions are presented in a graphical format. A variety of color-scheme options are available to represent signal strength.

In **Figure 23**, note that there is heavy Wi-Fi traffic centered on channels 1, 6, and 10 (there is Wi-Fi on other channels as well). Note the Statistics at the right side as well, and the color-coded indications of retransmissions (orange) and payload errors (red).

In **Figure 24**, let's see which channels a given link is avoiding. This is done with a fly-over on a Bluetooth packet. Note that the Bluetooth packets displayed are generally in the regions (channels) where the Wi-Fi is present (such as Wi-Fi channel 1).

In **Figure 25**, let's take a look at Instant Channels side-by-side with Instant Spectrum. (Learning to re-position the windows like this is quite useful — the User Guide discusses this feature). Note the legend at top-right of the Instant Channels, and the percentages shown there. In this case, over a span of about 31 seconds, nearly 90% of the packets are "OK," and there is a retransmission rate of around 7.4%. Given the extremely busy physical spectrum (there are hundreds of devices nearby), this seems a reasonably good result, although the user might wish to consider other factors, such as application-level performance. In this case, the application is audio, and we may wish to listen to the audio or export it to WAV for further analysis.

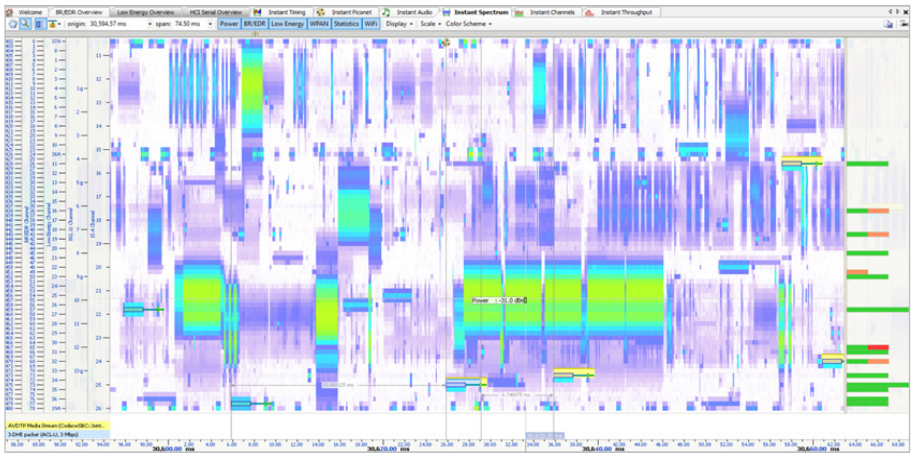


Figure 23 Heavy Wi-Fi on Channels on 1, 6, and 10.

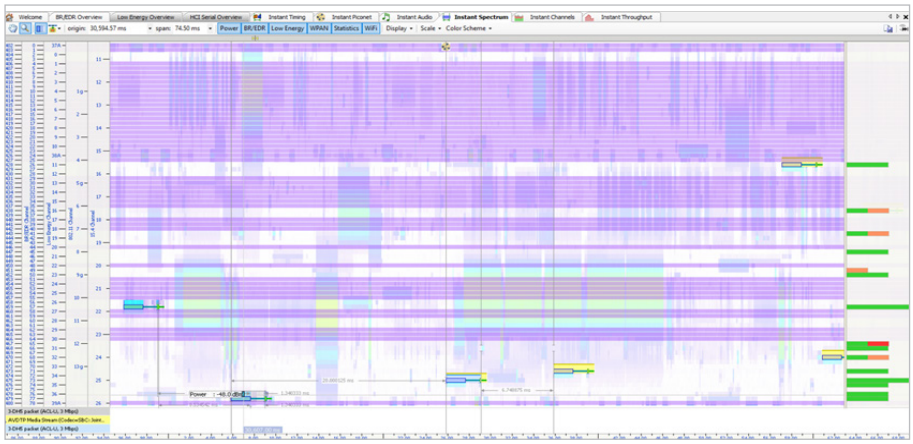


Figure 24 Bluetooth Packets Avoiding Interferences.

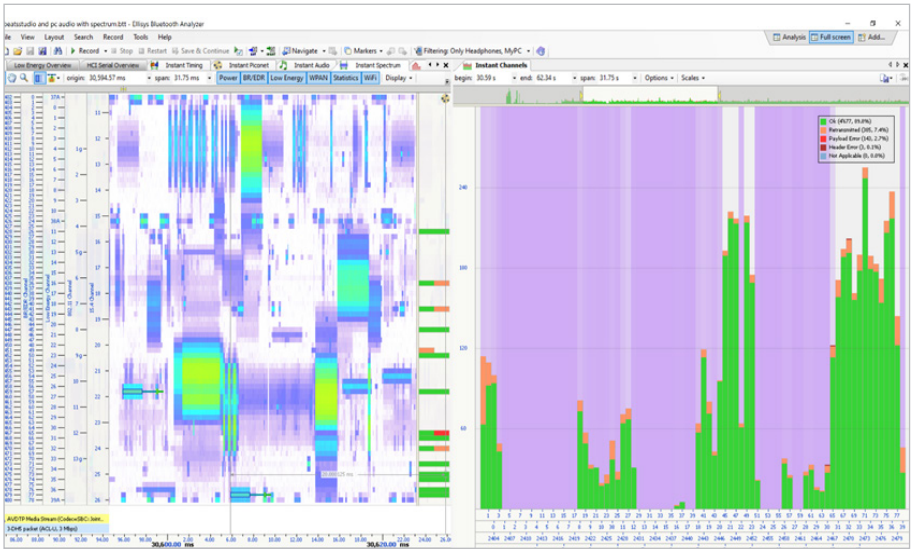


Figure 25 Instant Channels Side-by-side with Instant Piconet.

The Instant Audio feature, discussed next, can be used to monitor audio live or post-capture. Audio can be exported from the **Export dialog**, located in the **File menu**. The end result here is that Bluetooth is really doing a great job avoiding problematic areas (channels) that are being utilized by other emitters, in this case a Wi-Fi emitter.

Instant Audio

The Instant Audio feature provides a visual representation of captured audio traffic (over-the air, HCI, or I2S) that can be played real-time (during recording) or post-capture, looped, or configured to play selected user-defined ranges. As audio is played, a vertical cursor tracks the present position of the audio being played.

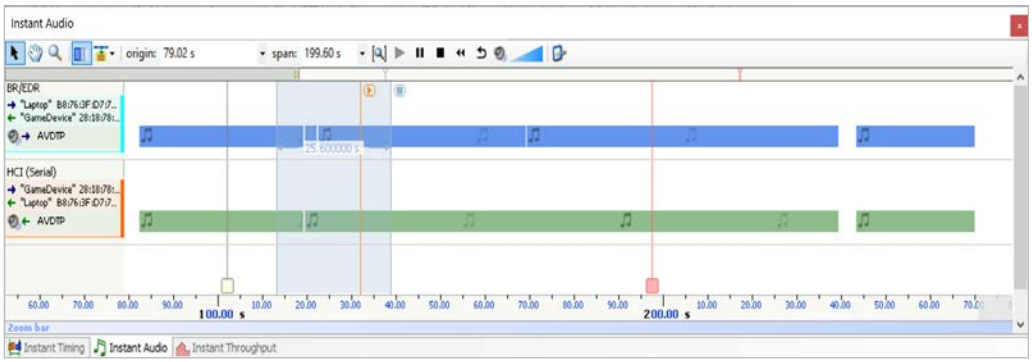


Figure 26 Instant Audio Showing Over-the-air Audio and HCI Audio Streams.

Various control features are provided, including rewind, looping, pausing, enable and disable of selected streams, and other controls. Export is available from **File>Export**.

Any available sound devices installed on the controlling PC are can be selected for use by this feature. Bookmarks are available to add to this view, and bookmarks added in other views will appear here (there are two seen in the **Figure 26**).

In **Figures 26 and 27**, there are two audio streams represented, one over-the-air and the other via HCI (UART).

This is an ideal capture approach that can be quite useful in pinpointing audio issues to host or controller areas very quickly, as the two streams can be compared audibly, or via WAV analysis on export.

Conclusion

With its precision into a window of time and its visual cues provided, the Ellisys wideband sniffer provides the user a thorough understanding of the propensity of a given device, or an aggregate of devices, to debug and troubleshoot issues throughout the duration of an entire capture and with all of its views, can be configured to characterize all devices in the vicinity or specific devices.

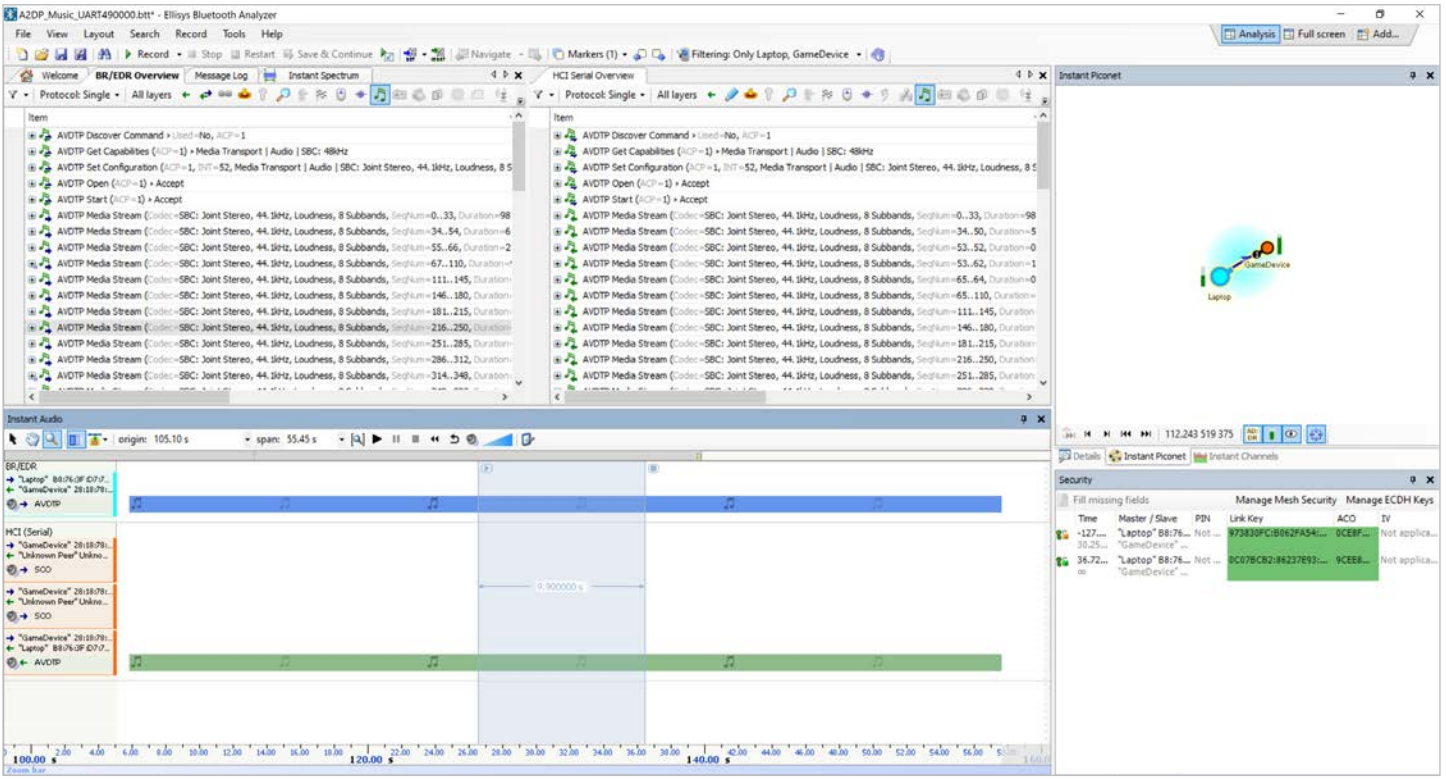


Figure 27 Instant Audio, BR/EDR and HCI Overviews Filtered for Audio Protocols.

HELPFUL HINT: Click the speaker icon at left of the Instant Audio window to enable/disable the audio.

Capturing Traffic

Please consult our Expert Note, EEN_BT03 “Your First Wideband Capture” to learn how to properly configure and operate your analyzer to achieve a clean capture.

Getting the Software

The analyzer software is available upon request via Ellisys: http://www.ellisys.com/products/bex400/download.php. The download is subject to approval, but approval will likely be granted to any company that is part of the Bluetooth SIG or seriously involved in Bluetooth development.

Visit ellisys.com or email support@ellisys.com for more information.

Other Interesting Reading

- EEN_BT03 - Your First Wideband Capture
- EEN_BT04 - Optimal Placement of Your Analyzer
- EEN_BT05 - Understanding Antenna Radiation Patterns
- EEN_BT06 - Bluetooth Security - Truths and Fictions
- EEN_BT07 - Secure Simple Pairing Explained

More Ellisys Expert Notes available at:
www.ellisys.com/technology/expert_notes.php

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

Sales Contact:

USA: +1.866.724.9185
Asia: +852 2272 2626
Europe: +41 22 777 77 89

sales@ellisys.com

www.ellisys.com

Connect with us.