



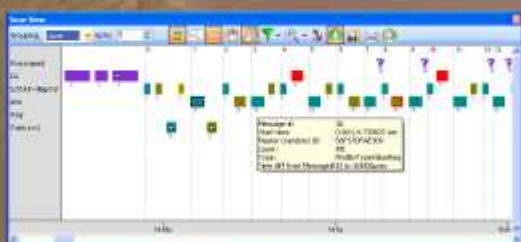
Peryton-Smart - Bluetooth Smart (BLE) Protocol Analyzer

Peryton-Smart is a fully-featured network and protocol analysis tool for Bluetooth Smart traffic.

During actual data capture the tool monitors the advertisement channel or channels and automatically follows the Bluetooth Smart session based on the connecting device relevant address. The Peryton-Smart auto-discovers and displays the connected devices and their connections, easily identifies erroneous or problematic messages, inspects message contents down to the bit level and allows easily sharing of scenarios of interest with colleagues, vendors or customers using integrated built-in options. If pairing process is captured the analyzer extracts the relevant security information in order to decipher the following messages. If the pairing uses an unknown PIN, the analyzer can auto discover this PIN and extract the security key.

Top Level Views

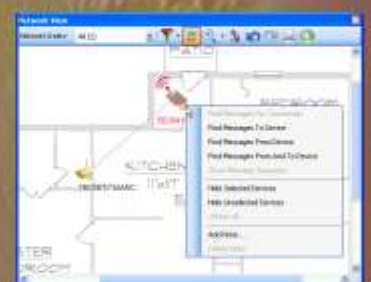
The **Time View window** provides a unique two dimensional view of the received messages using time as the x-y plot horizontal axis. This view provides easy understanding of time related processes. The Time View displays messages' transmission-times relative to the connection start gridline, thus verifying correct message timing. Messages can be sorted along the vertical axis by different parameters like Device, Channel, Protocol Layer, etc.) and user-defined text notes can be attached to messages. When grouped by channel, all the 40 (advertising and data) defined channels are shown, making easier to debug channel and time related potential issues. Specific messages (based on the parameter selected e.g. Protocol Layer, etc.), can be temporarily hidden from view for easy analysis in a heavy-traffic environment.



The **Network View window** auto-discovers participating devices and displays them during real-time data capture. Each device is drawn according to its type (e.g. Master, Slave) with hints showing all known information about it.

Connections between devices are clearly displayed and activity is clearly marked during real-time or simulated captures. Devices can be also drawn over a map or floor plan. Messages sent to/from a device or over a specific connection can be easily found with a single mouse click and user-defined notes can be attached to selected devices.

The **Devices View window** shows the auto-discovered devices in a table format and provides known information about them. The table can be sorted by any of its columns and relevant fields can be edited by the user for convenience of use (e.g. Device Name, etc.). Devices information can be saved to a file for further analysis by external tools (e.g. Excel), or for use as "known data" when analyzing data of the same network in future opportunities.



Down To The Bit Level

The **Message View** window allows diving down to the message fields' bit level. Fields' content is shown numerically and textually, with text and tool-tips showing the field name, description and meaning of the current value. Data is displayed in an intuitive structure allowing expanding or collapsing of sub fields when in graphical mode and the addition of fields of choice to table columns when in tabular mode. Information concluded by the analyzer as well as data deciphered from encrypted fields are clearly marked. These features greatly facilitate quick understanding, and eliminate the need to refer to the protocol or standard off-line documentation.



The **Message Tree View** window shows the message fields in a hierarchical XML-like structure, with field description, value, meaning and user notes, allowing expanding fields and sub fields. It includes hexadecimal and ASCII presentation of the captured data where the bytes carrying the current selected fields are highlighted. For encrypted messages, the clear data is also shown in a relevant section. For binary fields, the bits inside the captured byte/word are highlighted in the "binary" data section.



The **Message Sequence View** window shows the interaction between two devices or more in a single screen.

Like in the other windows, content of the Message Sequence View is synchronized and clicking on any line in it will

also make it recognizable in the Time, Message and Network View sections.



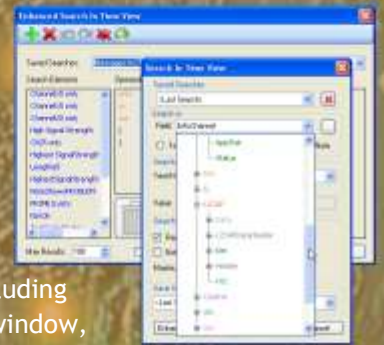
Enhanced Toolbox

The **Featured Toolbox** provides even deeper analysis possibilities of captured data, including **statistics charts**, **message compare** initiating analysis or **traffic-generation** form a **command line** and data exporting options for further analysis with external tools such as Excel and Wireshark.

Basic and Enhanced Search filtering allows searching a value in all or part of the messages properties. Search can be performed over all messages, on a pre-selected messages' group or on the messages resulting from a previous search session (i.e. search 'nesting'). Both basic and enhanced filtering criteria allow searching for a value within a specific field, or group of fields, text, hint, and note or field existence.

Logical combinations of basic defined filter are also possible.

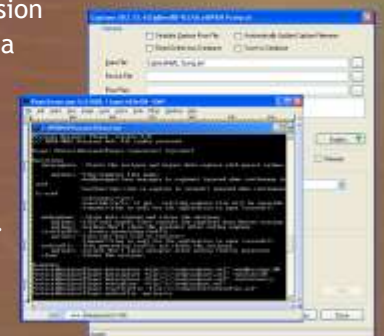
Packing to a Workspace saves the full analyzer state including current view in each window, bookmarks, selected messages with their exact expanded fields, message zoom status and more. Saved workspaces can be easily shared with colleagues for further inspection.



Data Capture

Unlike legacy Bluetooth analyzers that require expensive capture hardware, the Perytons analyzer capture is based on an off-the-shelf low cost receiver that captures the advertisement channel and as soon as it detects a connection message it starts following the network hopping. Only devices that follow the correct frequency hopping channels timing will be captured.

Using the Protocol analyzer Player built-in feature, a capture session can be triggered from a command line (this option is especially useful for scheduling analysis sessions of unattended networks).



Perytons

WWW.PERYTONS.COM