WaveConverter User Guide

Overview

WaveConverter extracts digital data from an input signal file based on a set of user-defined signal characteristics collectively referred to as a ***protocol***.

User Interface

Menu Bar

The UI contains a standard menu bar, with File and Help options.

File - Open RF IQ File

File - Quit

About - User Guide

Tool Bar

These controls allow you to save and retrieve protocols to the GUI, as well as other global display options.

Load Protocol – Brings up dialog with a list of stored protocols from which you may select

Save Protocol – If a protocol is currently loaded, this command replaces it with the contents of the GUI. If no protocol is loaded, this button is equivalent to clicking on “Save Protocol As” below.

Save Protocol As – Brings up a dialog asking for a name, a device type and a year. After entering this info and clicking OK, a new protocol is created with this info plus the contents of the GUI.

Demod – Demodulates the current IQ file using the parameters entered on the ***RF Demod Tab***, producing a set of baseband waveforms.

Decode – Decodes the currently loaded baseband waveforms using the parameters entered on the ***Framing*** and ***Payload Decode*** tabs. This baseband waveform may be loaded from a file or the product of a demodulation operation in WaveConverter.

RunStat – Performs a statistical analysis of the decoded data, using the payload properties entered into the ***Payload Stats*** tab.

Hex – This is a toggle switch which is not active by default. When inactive, all payload data is displayed in binary format. When active, all payload data is displayed in hexadecimal format.

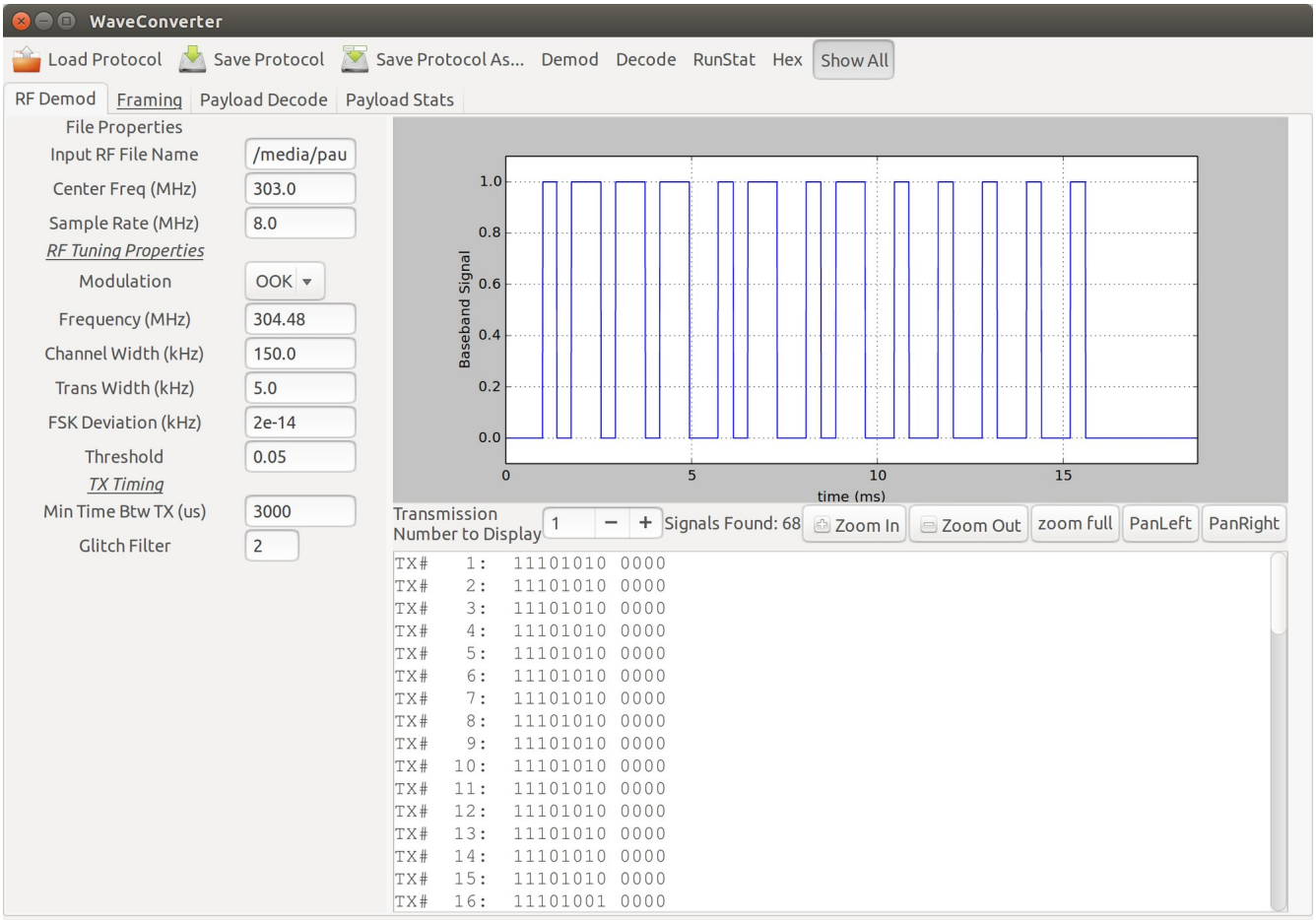
Show All – Toggle switch, inactive by default. When active, all transmissions are displayed and

considered when computing payload statistics. When inactive, only the transmissions that pass framing and CRC checks are displayed and part of the statistics. Enabling this prevents bad transmissions from distorting your results. It is often useful to disable this during the early part of the reverse engineering process and enable it later on.

Tabbed Interface

The UI is further divided into 4 tabs. Each of the tabs is active at all times, so values entered into a previously opened tab remain unless replaced by a ***Load Protocol*** operation.

RF Demod Tab



This tab is used to define the RF characteristics of the input signal. WaveConverter's demodulator takes an input IQ File, tunes to the target frequency, filters anything but the target signal, decimates to a 100kHz sample rate (10 us samples) and finally demodulates the signal. In this way, WaveConverter takes an IQ file and produces a digital baseband waveform.

The following five parameters are not part of any protocol definition but are user-defined. In other words, signals using the same protocol may have different values for the following five parameters.

Input RF File Name – Name and path of the file containing the RF data on which to operate. This file must contain complex data in an I-Q format, such as the files resulting from the direction of an SDR source to a File Sink in gnuradio.

Center Freq (MHz) – The center frequency of the captured RF data.

Sample Rate (MHz) – The sampling rate at which the I-Q file's data was captured.

Min Time Btw TX (us) – The minimum time in microseconds that separates each transmission. WaveConverter uses this parameter to separate the demodulated signal stream into individual transmissions.

Glitch Filter – The glitch filter ignores any transitions shorter than this value. This value is in units of 10us.

The remaining parameters on this page are part of the signal protocol and will be populated when a protocol is loaded.

Modulation – Directs WaveConverter to use an OOK or FSK demodulation scheme.

Frequency (MHz) – Frequency of the transmissions. It may be helpful to view an FFT or Waterfall plot of your I-Q file to determine the frequency of your signal.

Channel Width (kHz) – The bandwidth occupied by your signal.

Trans Width (kHz) – The transition width (difference between passband and stopband) of the channel filter used before demodulating the signal.

FSK Deviation (kHz) – Difference between space and mark frequencies. Only needed for FSK demodulation.

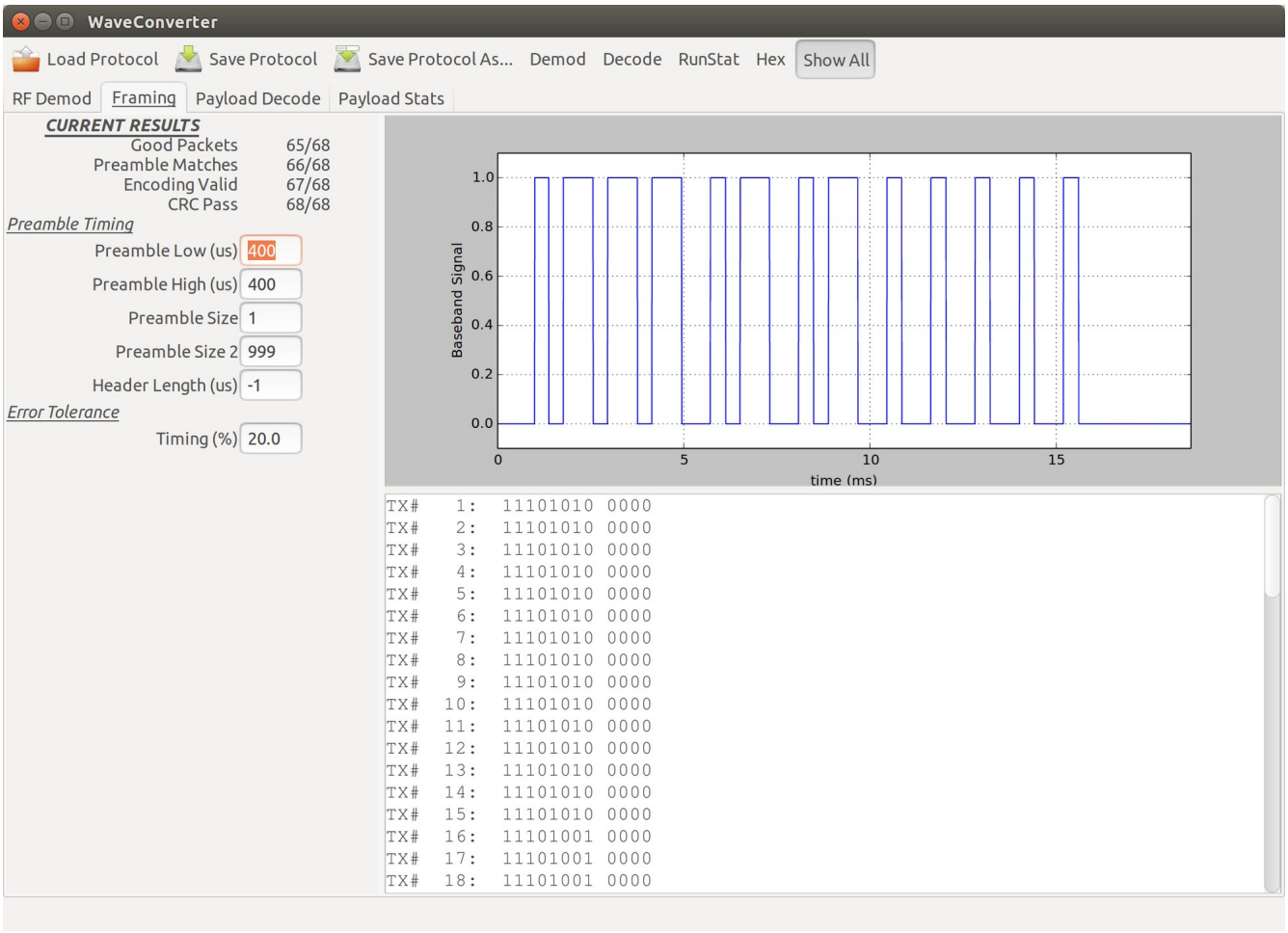
Threshold – Level that defines the difference between a digital zero and a digital one. Dependent on signal strength. Setting this too low may result in noise affecting the demodulator output, especially in OOK signals. Setting it too high may result in a failure to acquire any baseband waveform.

After demodulation, the recovered waveforms are displayed, one at a time, in the waveform display. Immediately after demodulation, the baseband waveform of the first transmission is displayed. To view other transmissions, simply enter the transmission number you'd like to see and press enter. Alternatively, you can click the '+' or '-' buttons to cycle to the next and previous waveform respectively.

You can navigate each waveform by clicking one of the five zoom buttons.

Below the waveform display controls, you can see the decoded transmission output. This will be blank until the decode operation has been executed.

Framing Tab



The framing tab is used to define the preamble and header for the transmissions, which both verifies the integrity of the transmission as well as prepares the transmission for extraction of the payload and CRC.

At the top of the left-hand side you can see the results of the most recent decode operation, including the number of transmissions with valid preambles, valid encodings and valid CRCs.

Good Packets - The number of transmissions with no framing, encoding or CRC errors. Good packets also have payloads of the specified length (this length is given on the next tab)

Preamble Matches – The number of transmissions for which the preamble matches that entered into this tab.

Encoding Valid – The number of transmissions for which the payload is encoded in a valid manner. The encoding type is specified on the next tab.

CRC Pass – The number of transmissions for which the payload and the specified CRC are valid. For protocols with no specified CRC, transmissions are always considered to have passed. The CRC parameters are entered into the next tab.

The next group of parameters define the timing at the start of each transmission.

Preamble Low (us) – For each cycle of the preamble, this is the time in microseconds during which it is low.

Preamble High (us) - For each cycle of the preamble, this is the time in microseconds during which it is high.

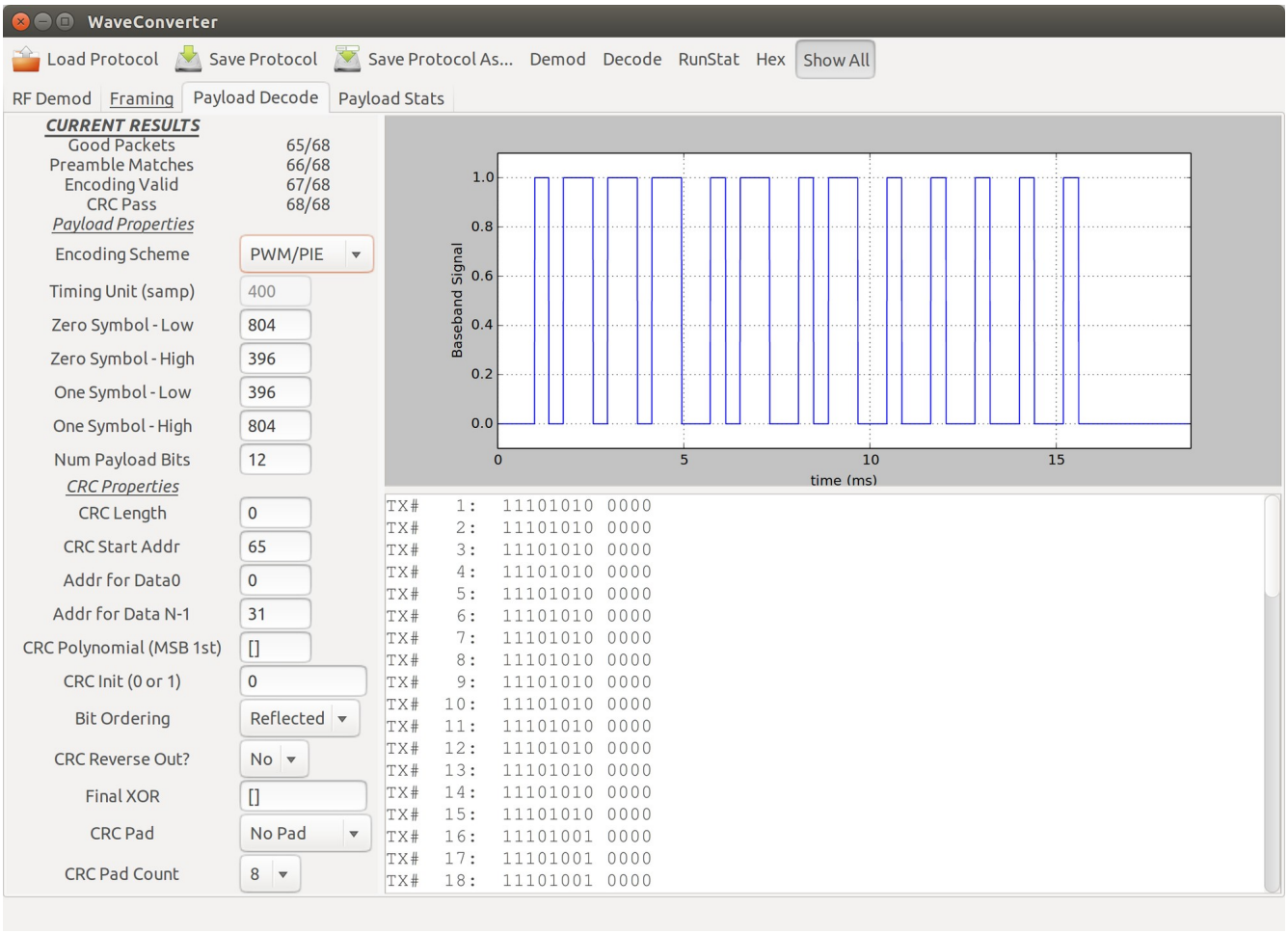
Preamble Size – This is the number of full cycles that constitute a complete preamble.

Preamble Size 2 – For some transmissions, there may be two possible lengths for the preamble. For example, the first transmissions in a series may have 50 cycles of the preamble, while any successive transmissions will only have 10 cycles. If your preamble only has one length (which is most common), simply enter ***999*** for this.

Header Size (us)– Some transmissions include a dead time (low logic level) after the preamble and before the payload. Enter the duration of this dead time here. If your transmission type contains no dead air, enter -***1***.

Error Tolerance (%) - For WaveConverter to recognize any timings as valid, they must fall within this percentage of the specified timing.

Payload Decode Tab



Encoding Scheme – There are currently two options available for the encoding scheme:

Manchester – This scheme requires you to provide a ***Timing Unit*** in microseconds. This is the smallest unit timing observed in the payload. The Symbol high and low times are not required for this mode.

Manchester Inverted – NOT YET IMPLEMENTED

PWM/PIE – Both of these modes encode data via distinct timing width. Pulse Width Modulation has a uniform symbol duration and encodes ones and zero by using different duty cycles. Pulse Interval Encoding also uses different pulse widths to encode the data, but the duty cycle is not uniform. Both of these schemes are defined by Symbol high and low times. No ***Timing Unit*** is required.

Timing Unit (us) – All signal timings in Manchester-encoded payloads are either one or two unit lengths. For this parameter, you will need to observe the baseband waveform and determine the shortest timing in the payload portion.

For PWM and PIE modes, there are distinct timings for the symbol representing a digital zero and for the symbol representing a digital one. To determine these values, simply observe the payload portion of the baseband waveform, you should see pulses of two different widths. Typically, the longer pulse represents a one and the shorter pulse a zero.

Each symbol is defined first by a low signal level, then by a high signal level. (NEED IMAGE HERE)

Zero Symbol Low - For the shorter of the two pulse lengths, enter the low time duration preceding it into this parameter.

Zero Symbol High - For the shorter of the two pulse lengths, enter the duration of the pulse.

One Symbol Low - For the longer of the two pulse lengths, enter the low time duration preceding it into this parameter.

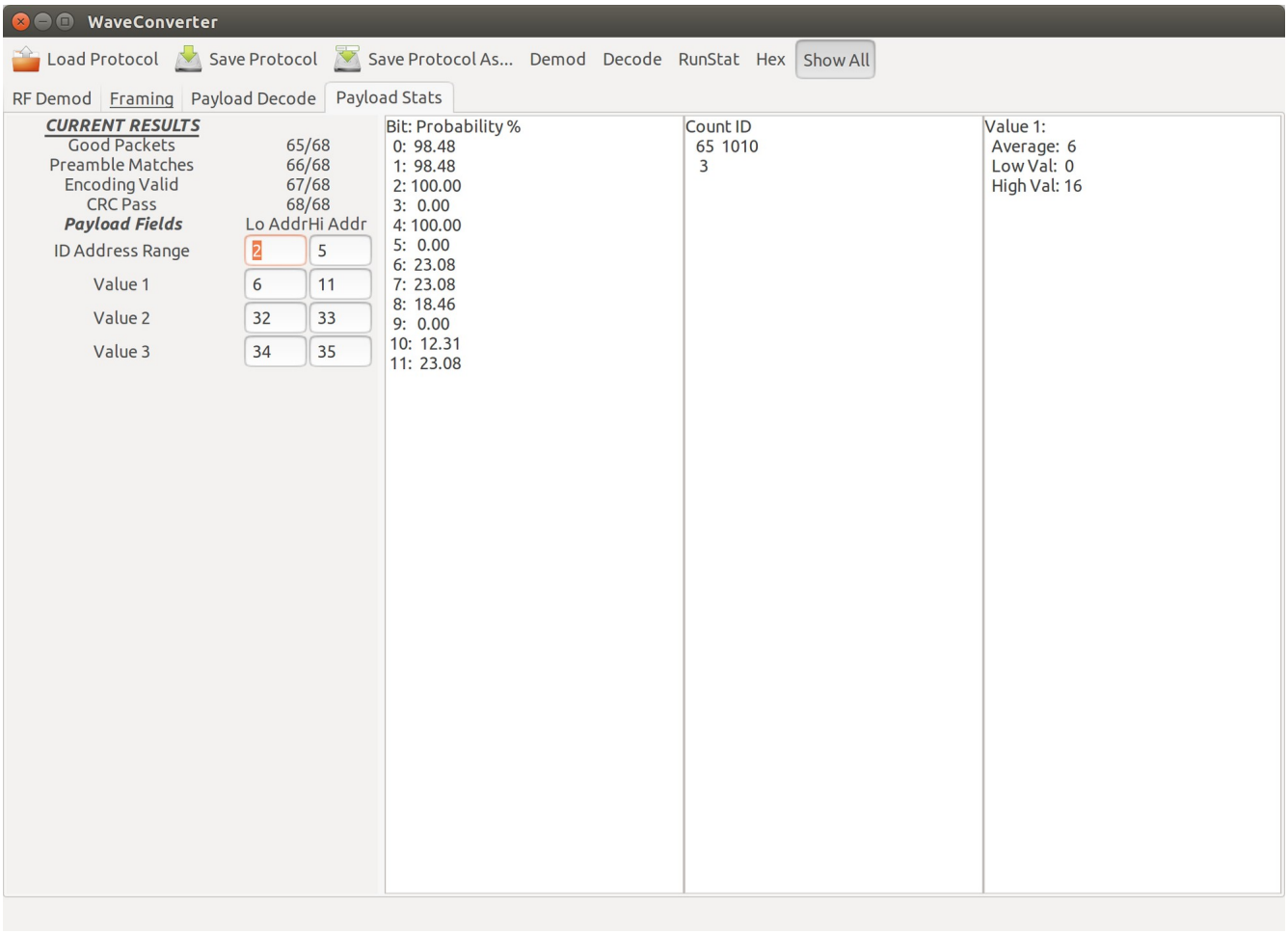
One Symbol High - For the longer of the two pulse lengths, enter the duration of the pulse.

Num Payload Bits – Enter the number of symbols in your payload

WaveConverter contains a CRC calculator that verifies the integrity of each received transmission. To make use of this, you must first identify the portion of the payload occupied by the CRC. You will then need to determine the CRC algorithm used by the transmitter.

NEED TO FILL IN THIS SECTION

Payload Stats Tab



This tab provides statistical information about the transmissions you have decoded. To make full use of it, you must first define the bit boundaries of any fields.

Even if you don't enter these, however, you'll still be able to view the bit probabilities in the left-most pane of the display. These bit probabilities will help you determine the general function of the different parts of the payload. To derive useful information from this data, however, you will need to have a substantial number of transmissions or the statistical analysis will be invalid.

If you see a probability near 0 or 100%, these bits are likely used for some kind of identification field. If you suspect only one transmitter is sending data, then this could be the ID of the single transmitter. If you have multiple transmitters, you may see a number of consecutive bit probabilities with similar, or even identical values.

If you see several consecutive probabilities with a value nearly 50%, you are likely looking at a CRC or a set of encrypted payload data.

A string of bits with similar, but not identical probabilities often represents a measurement of some kind.

The following parameters will allow deeper analysis:

ID Address Range – Enter the bit addresses of the low and high extents of the payload that you think represent an ID value. After clicking the RunStat button on the tool bar, the center pane will display the ID values residing at the specified address range along with how many times they occurred.

Value 1-3 Address Range – Enter the bit addresses of the low and high extents of the payload that you think represent measured values. After clicking RunStat, the right-most pane will display the range of values contained in those addresses, after first converting from binary to integer.