
# RF Explorer®

## User Manual

**Updated to Firmware Version 1.16 - BETA SNIFFER EDITION**

# RF Explorer®

RF Explorer is an affordable Handheld Spectrum Analyzer with a growing list of features.

*This little powerful unit is the tool you need*

*to reduce the implementation time and cost*

*of your next wireless project.*

*Updates of the RF Explorer User Manual are available online.*

*Please consider the environment before printing this document.*

# Table of Contents

# Introduction

This document is part of RF Explorer Sniffer project, and includes documentation required to evaluate BETA version of the tool.

This is a work in progress, expect some limitations that will be resolved in upcoming upgrades.

## Features

The current version is available and tested for following models only:

- RF Explorer 433M, 868M, 915M, WSUB1G, ISM Combo, 3G Combo, 6G Combo, WiFi Combo
- Frequency range supported covers 15-2700MHz. It does not cover models defined for 2.4G only.
- Modulation mode currently supported is ASK and OOK RAW, which can easily capture and decode RF remote controls, remote light switches, weather stations, etc.
- RAW sniffer mode is the extremely flexible. It works as a RF digital analyzer, detecting fast digital activity transitions so is virtually capable of decoding any protocol.
- Decoders included:
    - PT2264 and compatible devices (remote controls for lights, door openers, remote door bell, etc – see some examples below)


    - Oregon V2 used by Oregon Scientific Weather Station

- User defined sniffer protocol add-in capabilities: you can now create your own add-in to decode any protocol. Virtually all programming languages are supported, included example in Python 3.5 and .NET, but you can use any other of your choice.

# Firmware

Please upgrade firmware to v1.16 B03 or later included in the zip package.

You can easily go back to v1.15 anytime if you no longer want to use sniffer or if you find any problem.
Please upgrade supported models listed before, we are not testing unsupported models.

# Windows Software

The software to evaluate this BETA feature version is available in below link.

www.rf-explorer.com/downloads

## User Manual

Install and run RF Explorer for Windows normally. You will see a new “Signal Data Sniffer [BETA]” tab available. The software is very capable but works in a very specific defined workflow, so you should read carefully to use the sniffer seamlessly.

To use the sniffer effectively, you first need to find the frequency you need to capture RF activity for. Usual frequencies are 433.920MHz and 315.050MHz, depending on country and product, but may be many others. You should check first close to the gadget you want to work with using standard Spectrum Analyzer mode and see where the peak activity is when the gadget is working.

Once you know the frequency, use a narrow span of 1MHz or less in the spectrum analyzer mode to detect peak with good frequency resolution, otherwise using a large span may display low resolution number and will not be detected by the sniffer later…

As you can see below, RF Explorer detect activity at 433.875MHz which means the gadget is not transmitting signal at expected 433.920MHz but at some offset – this is to be expected in low cost gadgets with low stability internal oscillators.

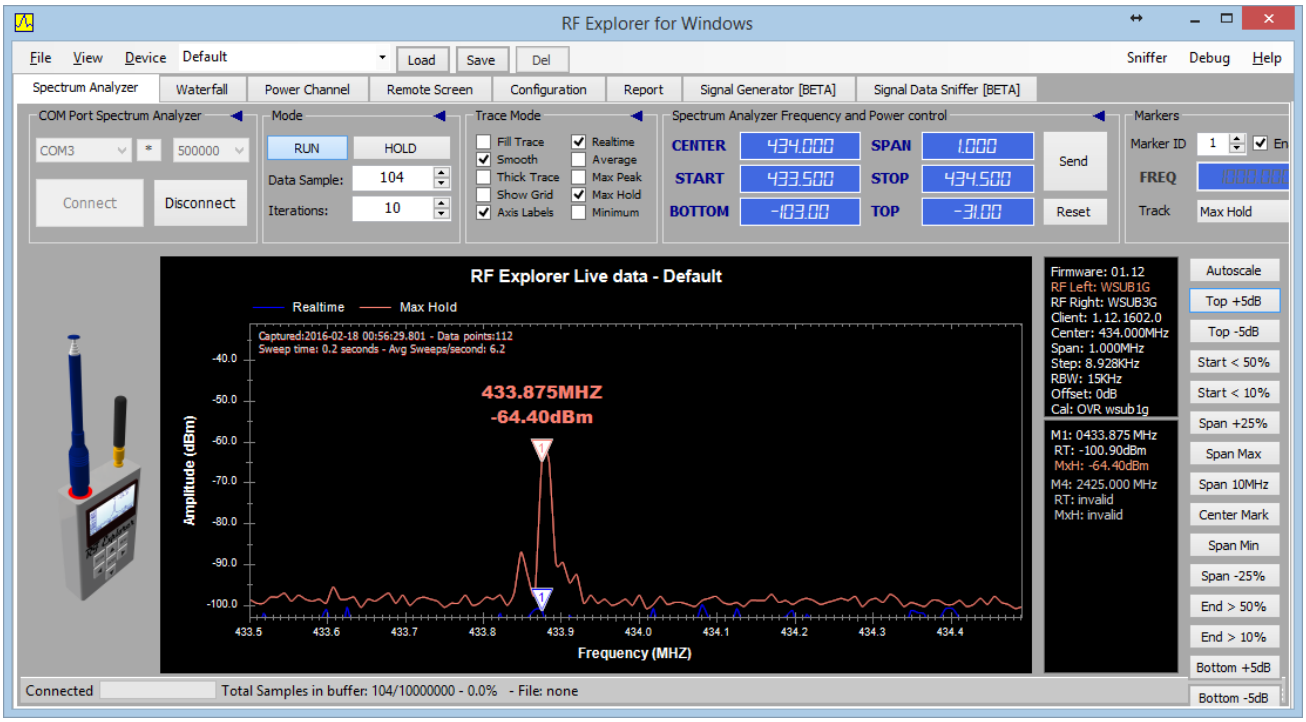
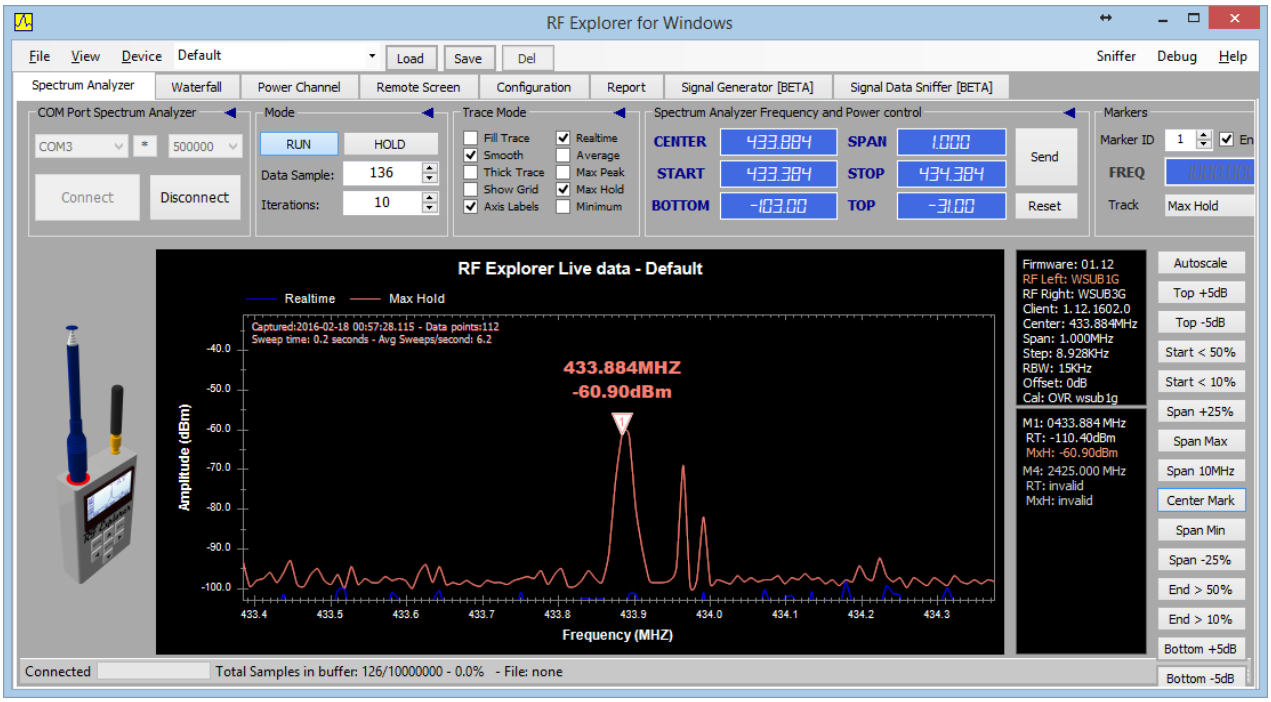
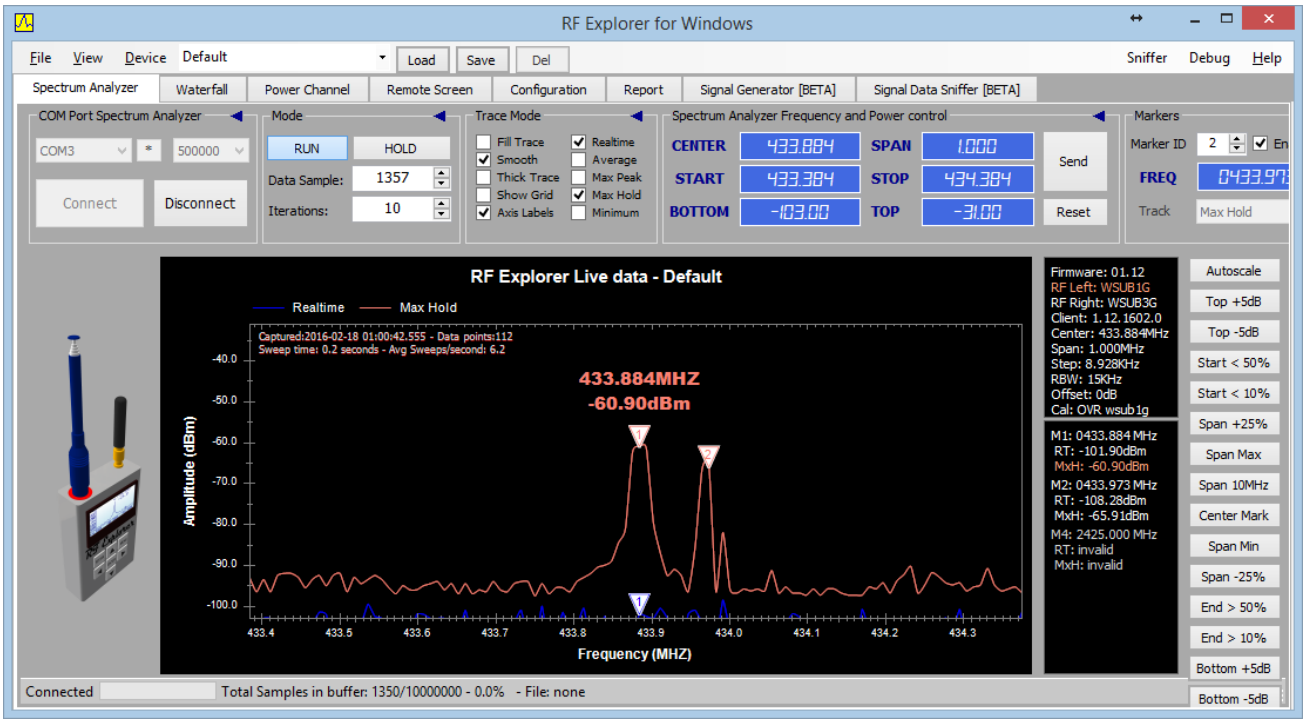



*Figure 1 - note this and some other pictures may come from older versions of the tool, but is functionally identical*

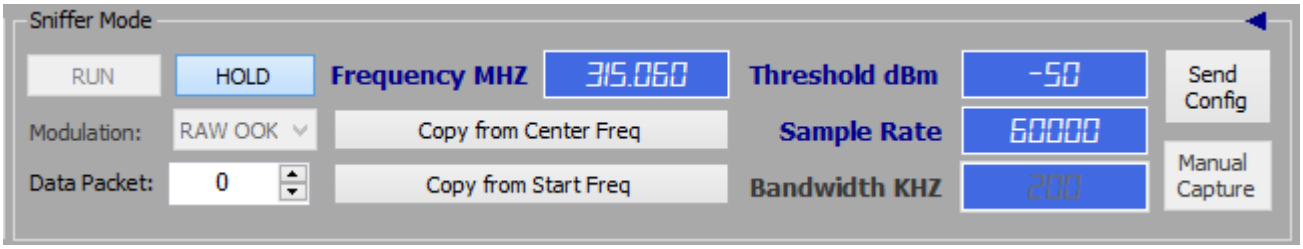
Tip: Select Marker 1 to track MaxHold trace and then use “Center Mark” button to automatically center that frequency on span for easier inspection. See below same activity now centered on span:



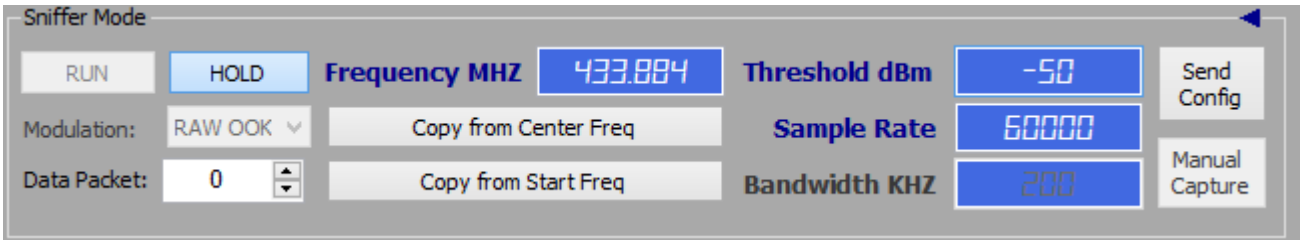

After some accumulative capture you can see multiple transmissions with slightly different frequencies, 433.884 and 433.973MHz:




Once you know the frequency you want to work with, go to the Sniffer tab and either use “Copy from Center Freq” button or type directly in “Frequency MHZ” edit box.




After clicking on [Copy from Center Freq] you should get this:




## Enabling the decoder

Next step is to select the Threshold, which is the power level at which you expect valid signals to rise above noise floor. In our pictures before you can see the noise floor is about -100dBm so at -80dBm there should be little to none false positive detections.

Sample rate value should be in range 20,000 – 500,000 for OOK RAW modulation modes usually found in commercial devices, but some experimentation may be needed. This is the sample rate at which the internal decoder will detect activity – the higher this value the better capture resolution but at the cost of a shorter capture time lapse.

The capture buffer works by storing 32,000 bits everytime a power level is detected above Threshold. Think of it as the equivalent of a logic analyzer: once the trigger event is detected (threshold level) the internal decoder will capture all RF activity at that frequency sampling at “sample rate” speed.

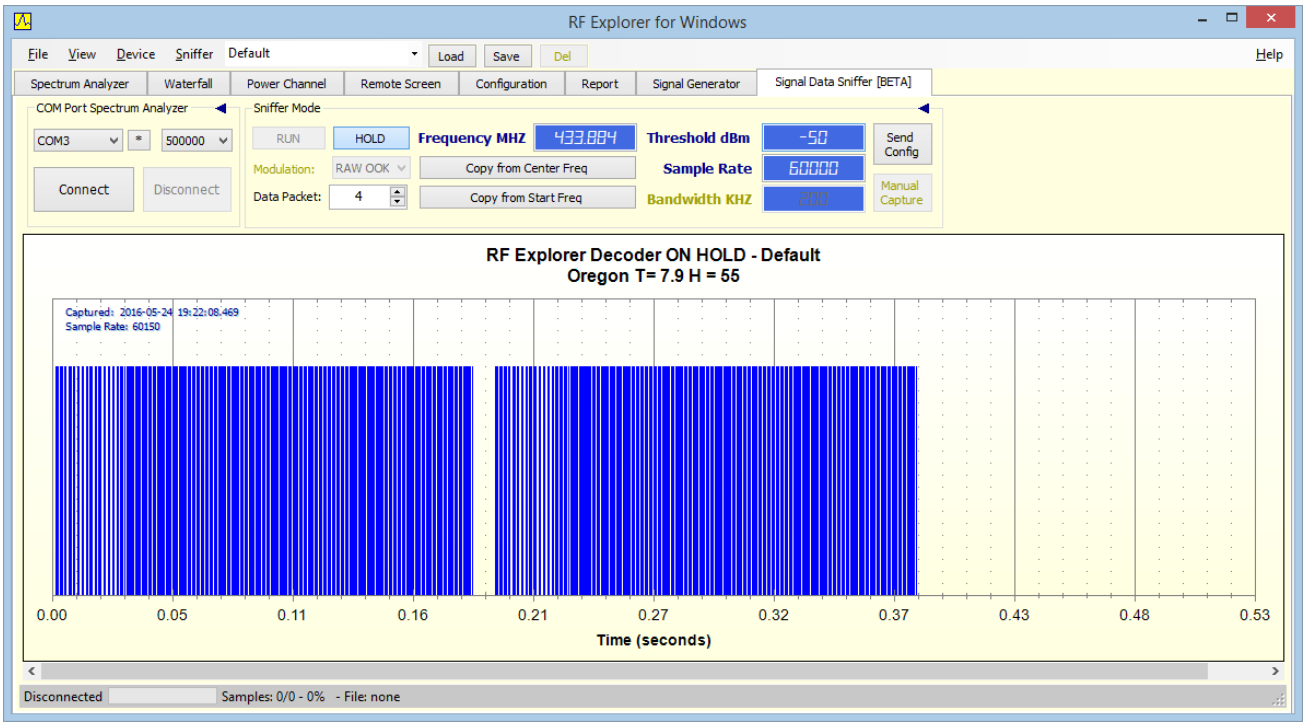
Once you are satisfied with your value selection, click on “Send Config” and that will set your RF Explorer in Sniffer mode – you can confirm that by looking into device screen which will show some parameters including number of packages captured. These values on screen are for debugging purposes only and will be removed in final version, where a simpler “DECODER” message on screen will be displayed.

## Capturing data

Eventually the device will capture activity and will display it on screen. Below is an example of an Oregon Scientific Weather station transmitting at 433.884Mhz.

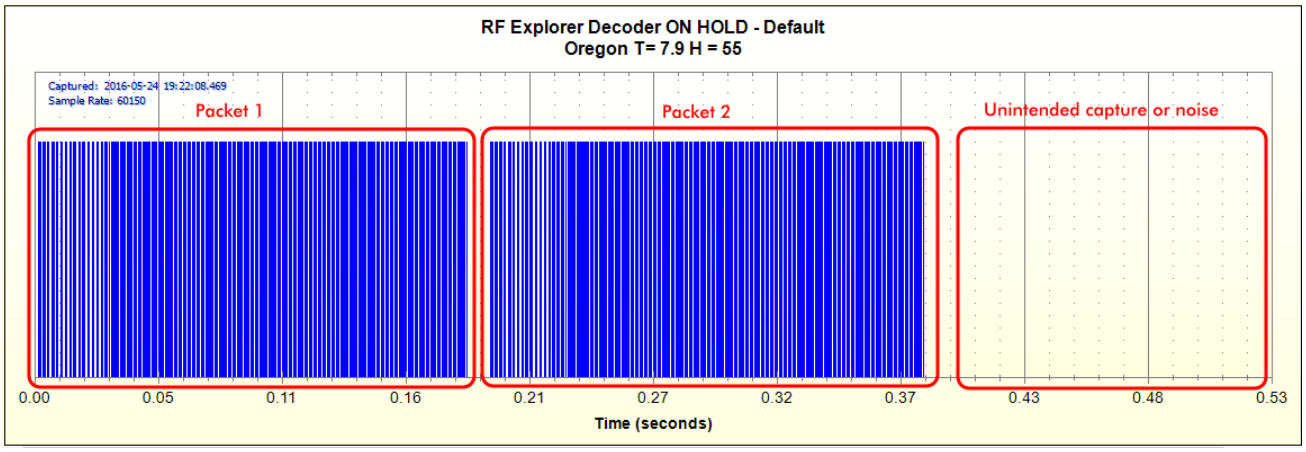
*Figure 2 - Oregon weather station - the white sensor is the transmitter*

You can load a sample file and follow this example by using menu option [Sniffer -> File load RAW from native Sniffer format] then select OregonV2_capture.rfsniffer file.

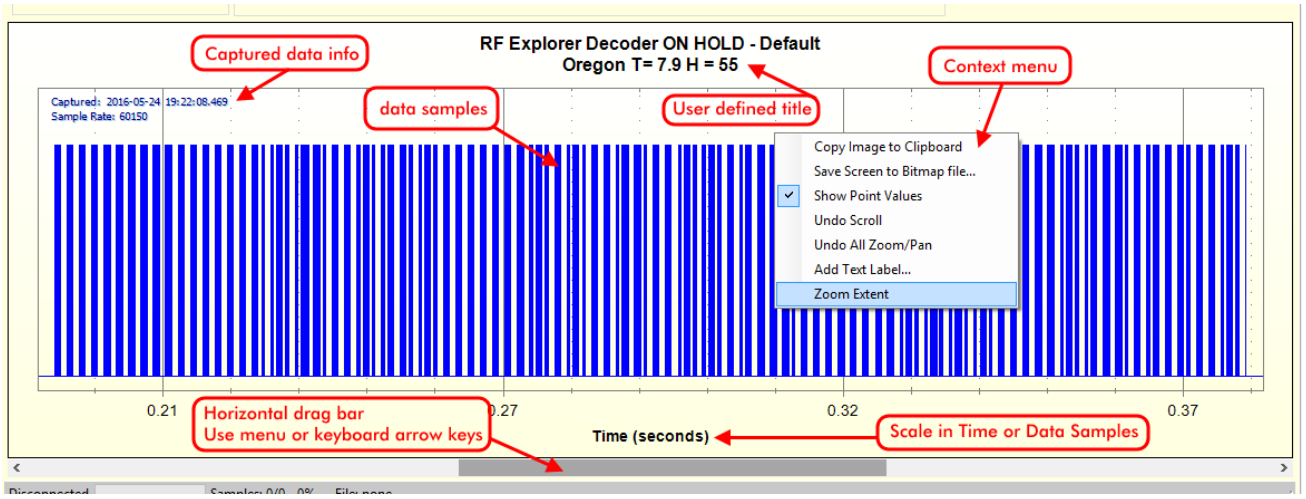



The Y axis is just 0/1 value, and X axis is bit sample ordinal. Same as a digital logic analyzer would display. You can display captured data in seconds or data samples. Use menu [Sniffer -> Display Time] option to define your preference.

In this particular case it is clear the weather station is sending two packets with identical data (repeating is a simple way to maximize change for the receiver station to capture information in the presence of a temporary interference). So we need to discard one data packet as well as any unintended noise received




After selecting with mouse the area delimited with packet 1 or packet 2, you can discard what you do not need.



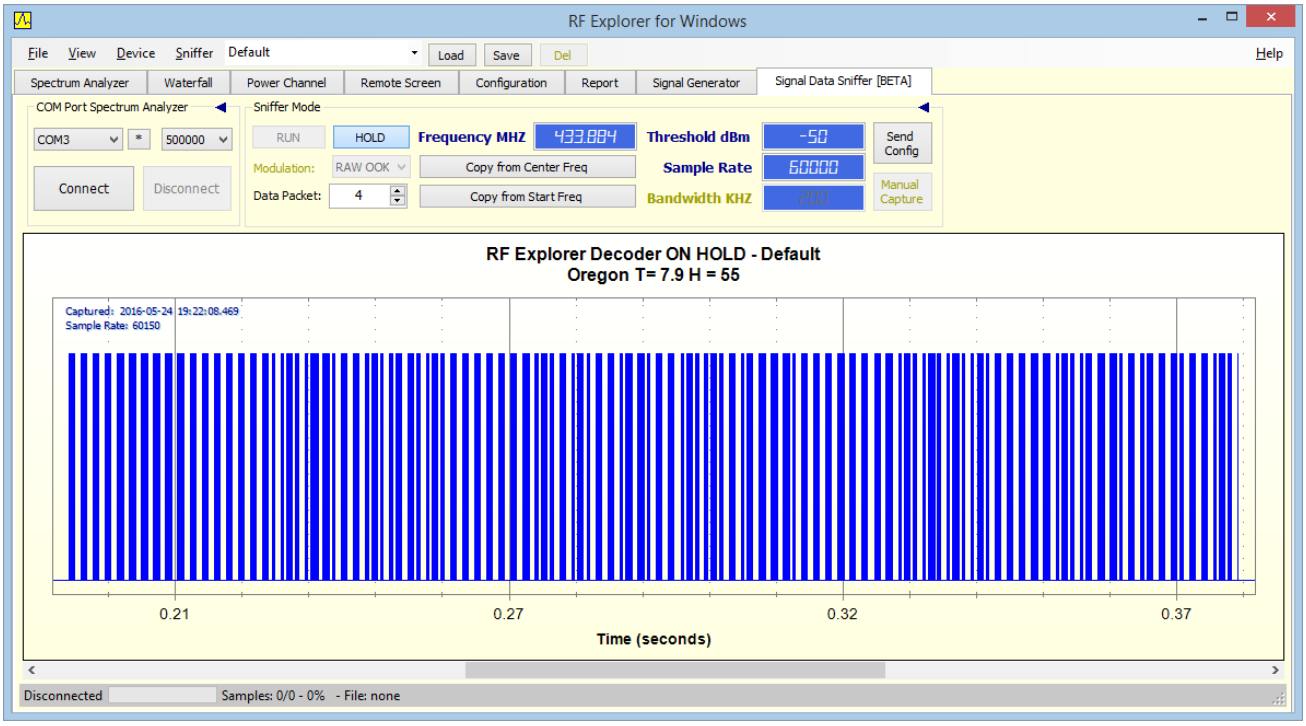

Note how the menu option [View -> User defined Text…] can help you tag the captured data according to the information you have. For instance in above sample screen, we captured RF signal when the Oregon weather station displayed Temp=7.9C and Humidity=55%, in this way you get a better sense of what you are dealing with.

## Processing the captured data

Interpreting the data may not be trivial for some protocols, but the software provides a lot of help.

### Selecting data to process

First you should select one of the packets only, doing a zoom on screen using left-click mouse drag area. You can then get something like this below, which clearly shows some sort of Manchester encoding in our example:



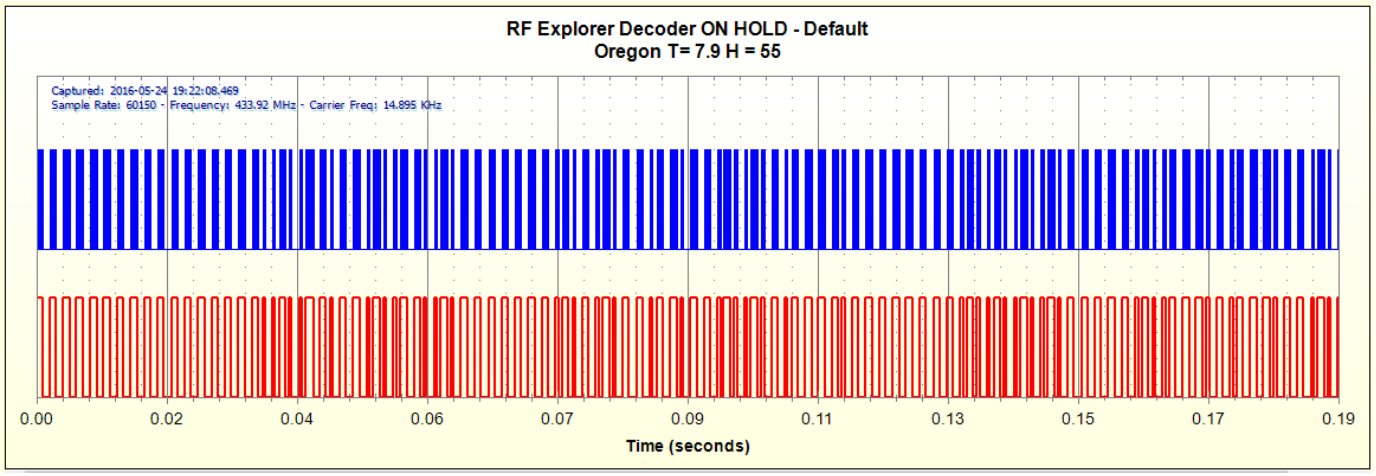

At this point is worth describing all the options you have to move around the screen with the mouse, otherwise navigating through all these data samples may look harder than actually is:

- You can Zoom-In / Zoom-Out easily by using mouse center wheel (make sure to click on graph before)
- You can zoom-in a window defined area by mouse left-clicking and keeping it while you drag it to another corner. Once you defined the window area to zoom-in, release the mouse left button and that will be updated immediately on screen.
- You can easily go back to full screen view using mouse right-click context menu and selecting option “Zoom Extent”
- Last but not least, you can use the horizontal drag bar to easily navigate to data samples on the left or the right.

### Trim data packet

By using the menu [Sniffer -> Trim to Current view], you trim out unwanted signals out of screen, so you get rid of noise and duplicated package data. At the same time, the software will filter the envelope to allow for an easier data manipulation later.

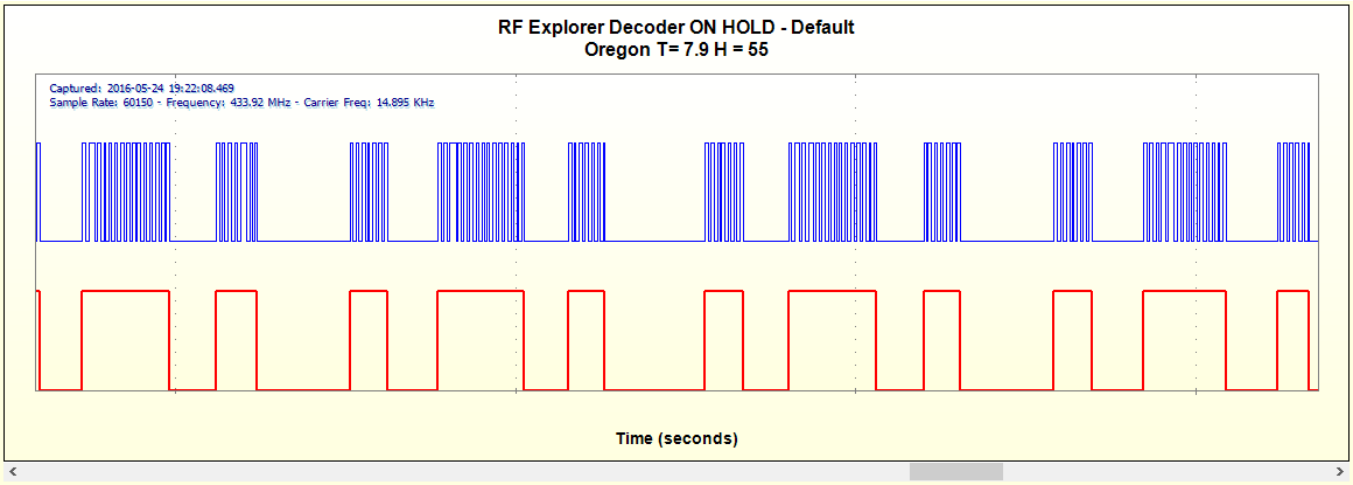
You will get a display view like this below:




Note a few interesting things automatically resolved by the software:

- Data out of view range was automatically removed, the new time scale (or data sample scale) accurately shows the data packet contents only
- The application detects envelope and calculates the averaged carrier frequency used to modulate the signal in origin transmission

If you zoom in a specific area, you can clearly see how software correctly detected envelope; this is extremely helpful step you need to determine how the protocol works.




With this information on screen, you can manually decode using some of the known Manchester variation encoding schemes, or reverse engineer data using some numerical algorithm.

To make that task easier, you can save anytime RAW data into CSV file for external processing or filtering. Use Sniffer menu option for that. The CSV file draft version includes a full dump of 0-1 values, together with some header data. This file will improve in future versions as well.

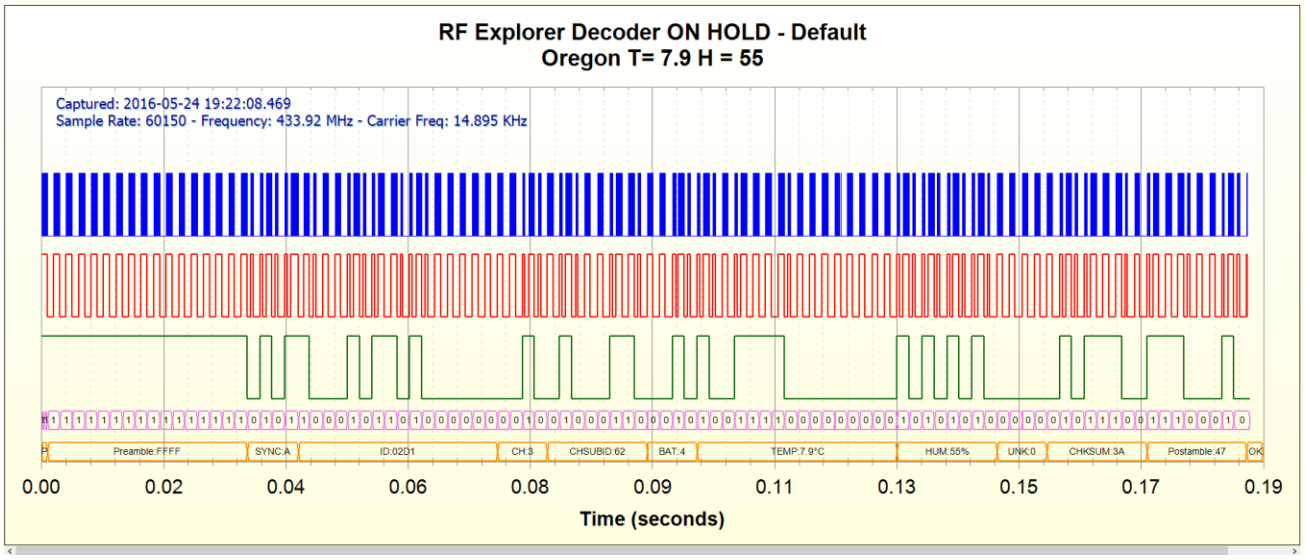
The current limit for captured packages in the same session is 1024. You can go back and forth in the captured data list by changing the “Data Packet” number.

## Automatic protocol decoder

But there is a lot more you can do with RF Explorer Sniffer tool. In this case, we already implemented a full decoder for this protocol, using information available online [ref pending]

To decode Oregon protocol data, use menu [Sniffer -> External Decoder Addin -> Decode Oregon Meteo V2] – you can use the .NET or the Python version, both work the same and are used to show how easily a decoder can be developed and used with RF Explorer.

After decoding, you will get a fully interpreted data dump




Take some time to make yourself familiar with this screen, it shows all the data you need from the captured data packet.

1. The first (blue) signal trace is the original, RAW data packet captured by RF Explorer device
2. The second (red) signal trace is the envelope, automatically resolved signal so you can manually interpret data.
3. The third (green) signal trace is protocol-specific, Oregon V2 decoded data interpreted by the add-in. It correctly interpret 0-1 digital values as defined by the protocol.
4. The fourth (magenta) signal trace are binary interpreted bits according to Oregon V2 protocol.
5. The last (orange) signal trace are meaningful data words with specific interpreted, human readable values according to Oregon V2 protocol. See data for temperature, battery status, humidity, checksum, etc. All data words are correctly interpreted and displayed on screen.

The first two signal traces are universal, RAW captured and demodulated signals. The last three signal traces are protocol specific, and requires a decoder to properly generate them.

Therefore, signal traces 1 and 2 are always available for you to work in any known or unknown captured transmission. The signals 3-5 requires a decoder and we hope we can get help from the community to develop as many as protocols are out there.

This sensible approach display from captured to fully interpreted data, with all intermediate processed signal traces for easy debug and protocol research.

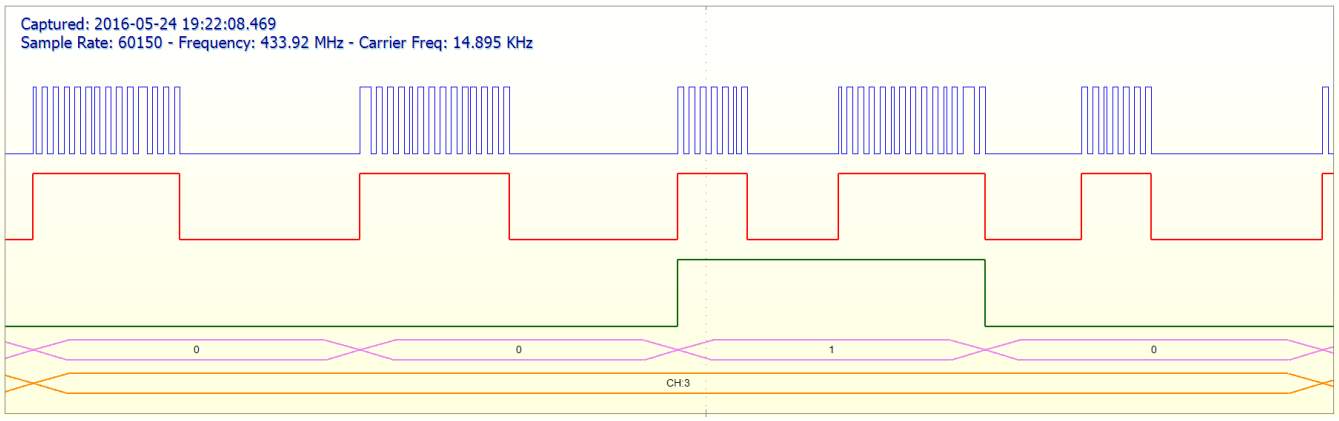



*Figure 3 - fully decoded protocol data word. In this case channel 3 (CH3) is the correctly interpreted value with all intermediate RAW capture, envelope, nibbles, bits and data word taking 4 bits according to Oregon V2 protocol.*

You can move mouse pointer to any data point on screen and will display meaningful information:


*Figure 4 - pointer displays rising edge point digital value = 1 and time position in milliseconds*

You can also right-click mouse on any point of screen, select [Add Text label…] and add custom text to help you define protocol data points or meaningful marks:

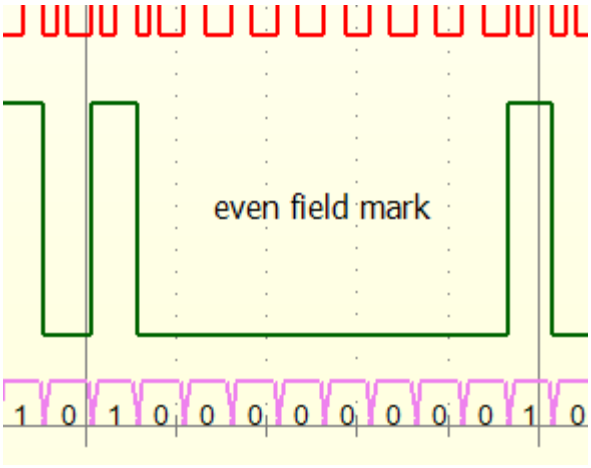



*Figure 5 - custom text defined any point on screen*

## Developing your own decoder add-ins

There are literally unbounded number of RF gadgets out there generating OOK and ASK signals you can now capture and research.

Currently delivered with RF Explorer are.

- PT2264 and compatible remote controls
- Oregon V2 weather stations

Contact us contact@rf-explorer.com if you want to work in a specific protocol decoder, we can provide you some assistance and help you distribute it openly so the user community can reuse your decoder.

You can read the source code of the Oregon V2 add-in examples and use it as template for your own. Check the addin source code zip file delivered with this BETA.

A specific page in our website will be soon available with detailed information for developing decoder addins, please visit www.rf-explorer.com/sniffer for more details.

## Python configuration

Example released with this version includes a Python 3 decoder. This is optional, RF Explorer for Windows does not require Python installed, except if this particular decoder is used.

In order for it to work, the Windows OS must correctly have associated .py files with the Python 3.x environment, and the python binary must be included in the PATH variable for the decoder to work.

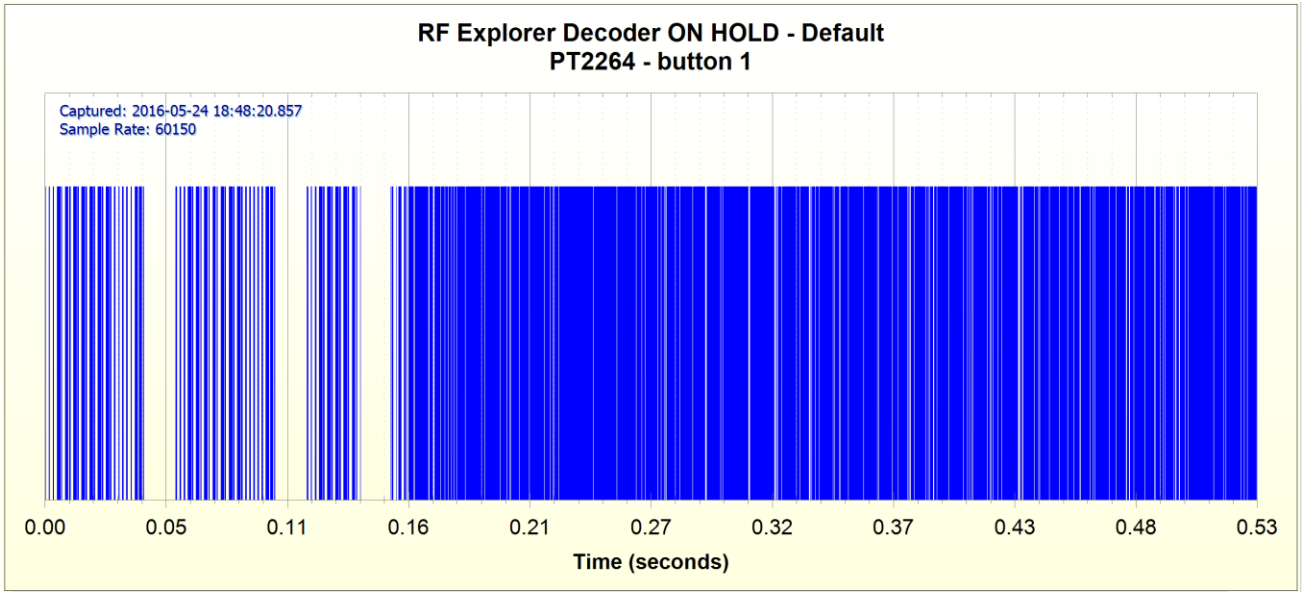
If you need to know current python version installed, run from command line:

- python –V

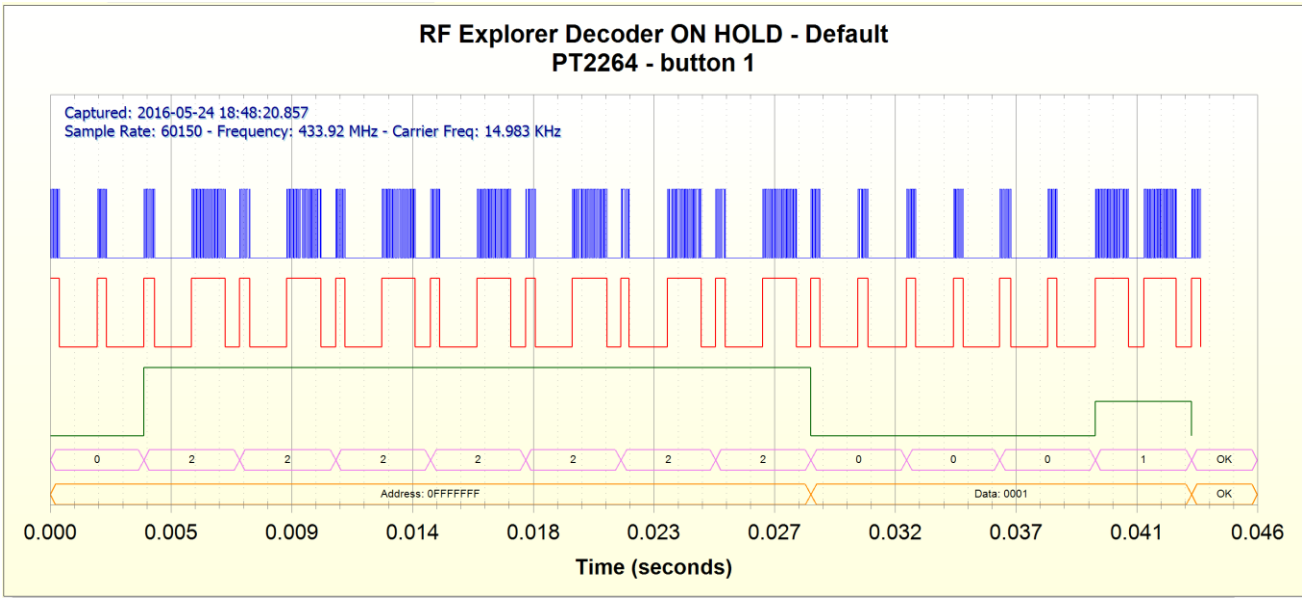
It should get Python 3.5.x, otherwise is recommended to install latest version from www.python.org

## Included examples

File **PT2264_capture.rfsniffer**: data captured from a remote control with 5 buttons, there is one data capture for each button

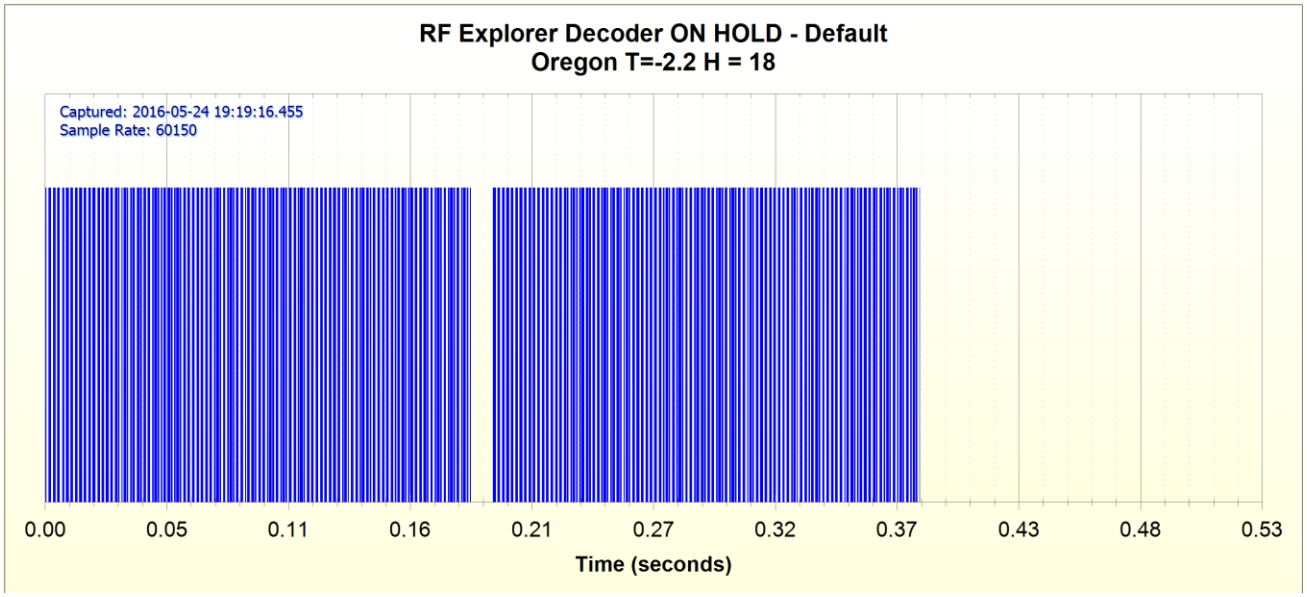



File **PT2264_decoded.rfsniffer**: decoded captured data using the included PT2264 decoder. You can decode the File PT2264_capture.rfsniffer file yourself or load this PT2264_decoded.rfsniffer file already processed.

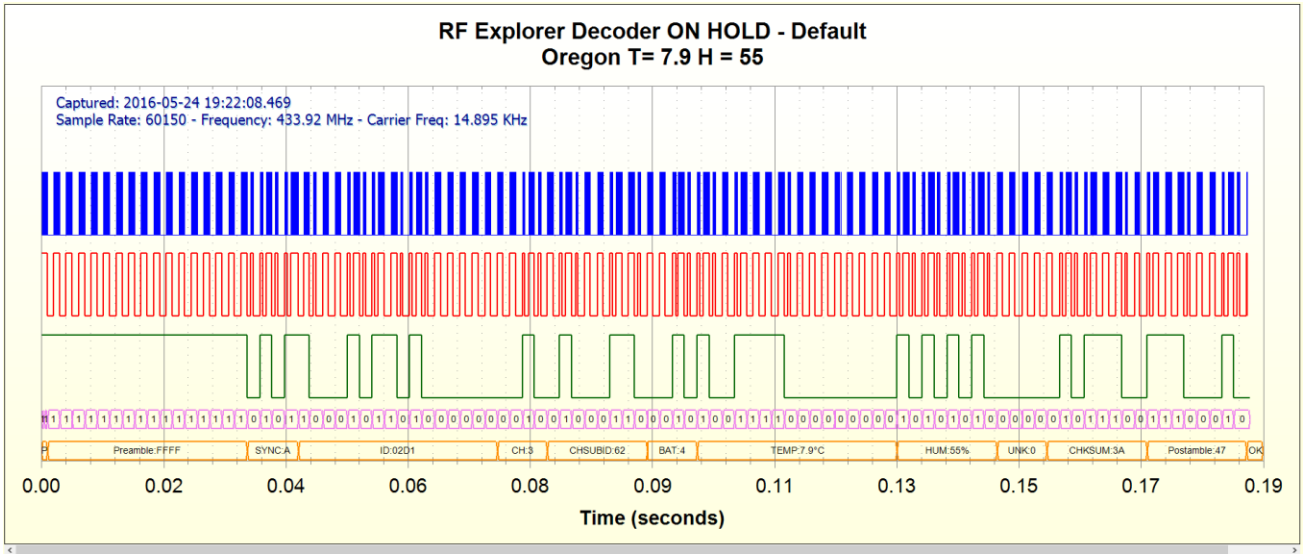



You can see PT2264 decoded data is typically defined by an address of 8 bits, and then 4 bits of data. Interestingly enough, each bit is 3 stage (not binary bit 0-1 but 0-1-2 being 2 a high impedance state)

File **OregonV2_capture.rfsniffer**: data captured from an Oregon Weather Station, at 5 different temperatures.




File **OregonV2_decoded.rfsniffer**: decoded captured data using the included Oregon V2 external add-in.




You can decode the File OregonV2_capture.rfsniffer yourself or use this decoded file OregonV2_decoded.rfsniffer already.

In this file, you can see what happens when a data packet is received corrupt or incomplete, the software shows a FAIL message on decoded info which cannot be processed. Information of reasons why the data packet was incorrect is in the Report tab, message like this may be visible:

```
-------------------------
Error decoding the protocol
-----------------------------------------------
Data saved in the CSV file:
Header: RF Explorer RAW sniffer file: RFExplorer PC Client - Format v001
Decoded protocol (true = 0/false = 1): False
Decoded Bits:
```

```
----------------
0      255

Interpreted bits:
----------------
0      FAIL
```

## Stopping Sniffer mode

You can click on Run/Hold buttons to temporarily put the capture activity on hold. This is useful when you are trimming data or inspecting a captured signal, otherwise if the device keeps capturing additional packages will automatically go to the last captured signal.

To completely shut down the sniffer mode, go to the Spectrum Analyzer tab and the device will automatically get back into analyzer mode. If you unplug the device from USB it will also get back to analyzer mode if it was still in sniffer mode.

## Specifications

For a complete list of features and RF Explorer models, expansion boards available, and accessories please check the RF Explorer Model Map online.

**www.rf-explorer.com/models**

## Acknowledgments

This product could not be possible without the SeeedStudio Team who manufacture, test and distribute RF Explorer worldwide.

RF Explorer is a reality thanks to the great community behind, always suggesting features and providing useful feedback.

## FCC and CE regulations

RF Explorer is a Test and Measurement device, and therefore compatible with US FCC regulation 47 CFR Part 15.103(c).

RF Explorer is certified for CE compliance under regulations EN/IEC61236 and EN/IEC61000.

## License