OpticSpy

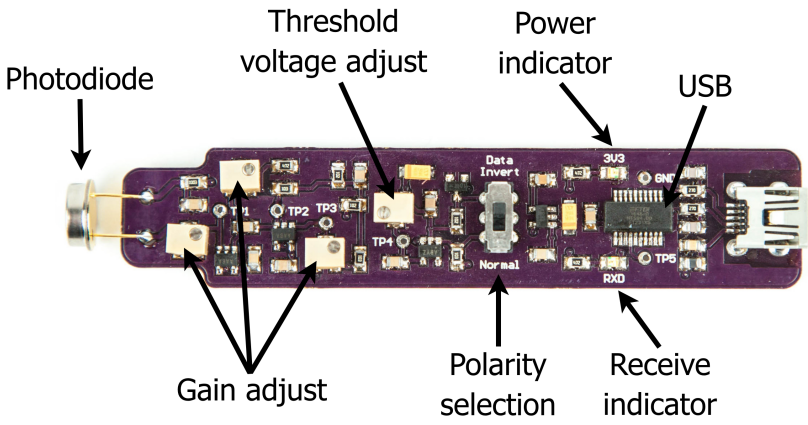
OpticSpy is an open source hardware module for exploring and experimenting with optical data transmissions. It captures, amplifies, and converts an optical signal into a digital form that can be analyzed or decoded with a computer. OpticSpy was designed by Grand Idea Studio and is distributed by Crowd Supply.

Features

- Easy-to-use light-to-digital converter
- Supports both visible and near infrared (IR) light emissions (420 to 940 nm)
- Works with signal frequencies from 100 Hz to 1.5 MHz
- Gain and threshold adjustment via potentiometers for fine-tuning of a particular target signal
- On-board switch to select normal or inverted polarity data streams
- USB interface for direct connection to a host computer (PC, Macintosh, or *nix)

Application Ideas

- Search for optical covert channels that may exist within devices
- Add data exfiltration functionality into a project
- Receive/demodulate IR signals from remote controls and other consumer electronics
- Discover Li-Fi networks or Visible Light Communication (VLC) systems



Usage

OpticSpy is an optical receiver module consisting of analog and digital subsystems. The analog section consists of a photodiode, two stages of amplification, and a comparator, which receives the optical transmission, amplifies it, and converts it into a digital signal, respectively. The output from this section feeds into an FTDI FT231X USB-to-Serial IC for connection to a host computer (drivers available directly from FTDI). Test points are accessible on the module for observing each stage of signal processing.

OpticSpy is powered from the host computer's USB port. When connected, it will appear as a Virtual COM port and will have a COM port number automatically assigned to it. OpticSpy's 3V3 LED will illuminate indicating that the module is properly powered.

OpticSpy is primarily designed to receive and decode asynchronous serial data streams that use NRZ (Non-Return-to-Zero) encoding, such as those generated from a microcontroller's UART interface and which are supported by standard terminal programs (such as PuTTY, CoolTerm, minicom, or screen). The module supports signal frequencies from 100 Hz to 1.5 MHz, corresponding to UART data rates of 300 bps to 3 Mbps, depending on OpticSpy's gain settings and the brightness and wavelength of the transmitting signal.

To use, simply hold the face of OpticSpy's photodiode towards the target's light source and adjust the terminal program's communication settings to the correct baud rate of the transmitting signal. The signal will be received, processed, and sent through the FT231X directly to the terminal program. This will let you see any printable characters or other data sent by the target. Depending on the speed of the transmitting signal, the target's light source may be blinking faster than the human eye can detect, so it will appear to be steadily illuminated. When a signal is being received, regardless of data type, OpticSpy's RXD LED will illuminate or blink. If the received message appears garbled, toggle SW1 (Data Invert v. Normal) to invert the polarity of the signal.

If the target data stream uses an unknown encoding scheme or one not supported by a terminal program, you can preempt the FT231X interface by connecting a logic analyzer, Arduino, or any other tool capable of displaying/processing raw digital signals to OpticSpy's TP5 (Comparator Output) test point. You would then need to demodulate and/or decode the signal manually.

If the target data stream is modulated with a fixed carrier frequency, such as with IR-based remote controls that range from 30 to 60 kHz, increasing OpticSpy's gain will reduce the frequency response/ bandwidth and could result in OpticSpy stripping the carrier from the signal. This convenient trick will leave you with the actual data stream and avoids the need for subsequent demodulation.

Receive range between OpticSpy and the target is also affected by OpticSpy gain settings and the brightness and wavelength of the transmitting signal. The photodiode used in OpticSpy's front end approximates the spectral response of the human eye and has an ideal range from 420 to 675 nm. This means that it can detect visible light better than typical photodiodes, which have a peak response for near IR. The photodiode is still quite sensitive to IR, which allows OpticSpy to support a wide range of wavelengths. OpticSpy has been tested successfully up to 940 nm. For visible light transmissions, typical distance from the transmitting LED to OpticSpy is up to 2 inches (tested with a variety of MCU platforms containing different colored, diffused T-1 3/4 LEDs). For near IR signals, typical distance is up to 4 inches (tested with a variety of television remote controls).

If the default OpticSpy settings aren't working with your particular target or you want to try to reduce ambient noise, increase receive distance, or change the frequency response/bandwidth, the potentiometers will let you adjust the gains of the amplification stages and set the comparator voltage threshold, which is used to determine the point at which the received signal is treated as a logic level '0' or a logic level '1'. See the Calibration section for more information.

Calibration

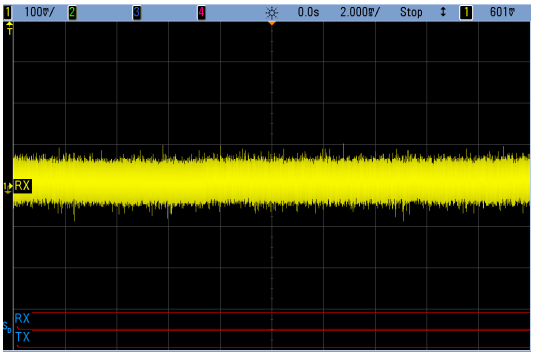
This section describes OpticSpy's calibration process. The oscilloscope screenshots below show the progression of signal reception, amplification, and thresholding. Your particular images may vary depending on OpticSpy's settings and the transmitting signal's characteristics. OpticSpy's schematic and assembly drawing show the part designators. The default potentiometer positions are set to mid-range, except for R12, which has been adjusted to set the comparator voltage threshold (TP4) to 2.5V.

With the desired target signal facing OpticSpy's photodiode, use an oscilloscope to view TP2, the output from the 1st stage non-inverting amplifier. Adjust R4, the 1st stage gain, until the received signal is visible without distortion or saturation. It will have a positive offset and may have noise at the '0' and '1' levels. If additional gain is needed at this stage, adjust R2, the photodiode's bias resistor.

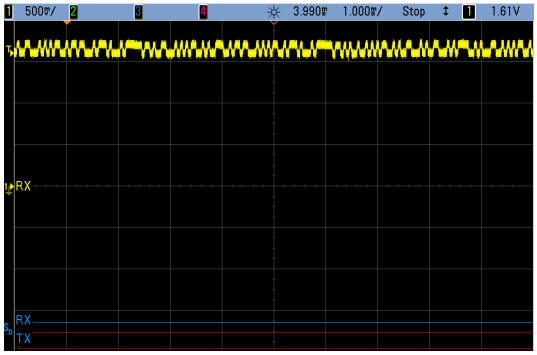
Next, view TP3, the output from the 2nd stage non-inverting amplifier. Adjust R10, the 2nd stage gain, until the received signal is visible without distortion or saturation. It should resemble a digital signal, but may show relaxation effects at the '0' and '1' levels. The minimum and maximum voltage levels will vary depending on the target and its distance to D1.

At this point, you must manually determine a suitable voltage level that will serve as the threshold to reliably discern a logic level '0' from a logic level '1'. The level should be as high as possible without encroaching on any "drooping" portion of the signal. View or measure TP4 with an oscilloscope or multimeter and adjust R12 until the desired voltage level is achieved.

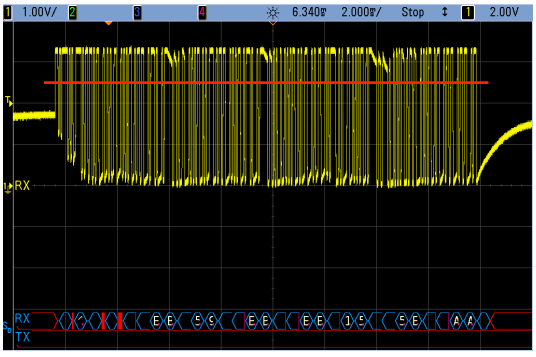
The final processed signal can be viewed at TP5 and should appear as a rail-to-rail digital signal with minimal noise.



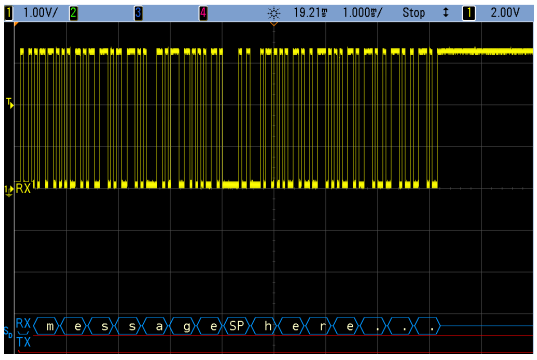
TP1: Photodiode signal before the 1st stage amplifier. The signal is too small to detect through the surrounding noise.



TP2: Signal after the 1st stage amplifier. The received digital signal is visible, though offset by ~1.6V and noisy at the '0' and '1' levels.



TP3: Signal after the 2nd stage amplifier. "Drooping" is visible at the '0' and '1' levels. The red line indicates the comparator voltage threshold (TP4).



TP5: Partial view of the fully decoded, rail-to-rail digital signal showing a printable ASCII message received from the target's LED at 19.2 kbps.