OpticSpy (DEFCON Workshop)

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 Joe Grand of Grand Idea Studio.

This version is provided in kit form for use at DEFCON 26. A fully assembled, more integrated version is available via 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

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 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. Test points are accessible on the module for observing each stage of signal processing.

The 6-pin header allows direct connection to an Adafruit FTDI Friend or compatible USB-to-Serial Interface. The FTDI Friend will power the module and decode asynchronous serial data streams that use NRZ (Non-Return-to-Zero) encoding, such as those generated from a microcontroller's UART interface, for display using a standard terminal program (such as PuTTY, CoolTerm, minicom, or screen). If the target data stream uses an unknown encoding scheme, you can preempt the FTDI Friend interface by connecting a logic analyzer, Arduino, or any other tool capable of displaying/processing raw digital signals to OpticSpy's OUT (Comparator Output) pad. You would then need to demodulate and/or decode the signal manually.

To use OpticSpy, provide 5VDC to the module via the VIN pad or by connecting the FTDI Friend. The green LED will illuminate indicating that the module is properly powered. Then, hold the face of OpticSpy's photodiode towards the target's light source. The signal, if one exists, will be received, processed, and output to the OUT pad and FTDI Friend connector. 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. If the received message appears garbled, toggle SW1 (Data Invert v. Normal) to invert the polarity of the signal.

Calibration

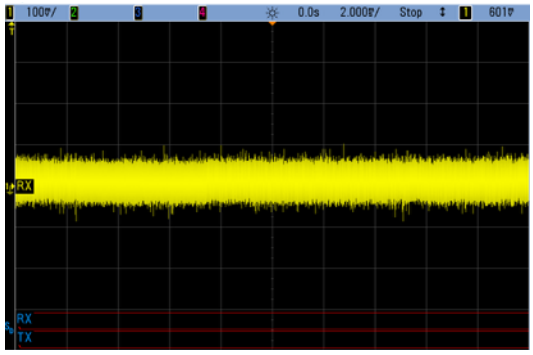
If the default OpticSpy settings aren't working with your particular target or you want to try to reduce ambient noise, increase receive distance, or change the frequency response/bandwidth, the potentiometers will let you adjust the gains of the amplification stages and set the comparator voltage threshold,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

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.

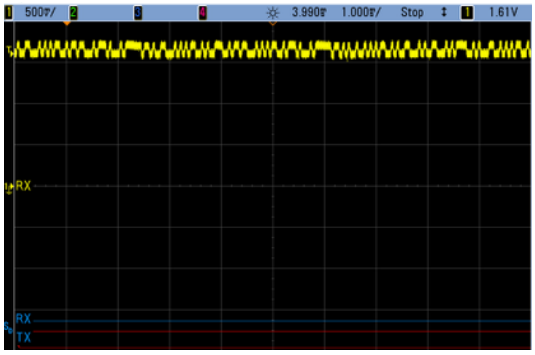
Next, view TP3, the output from the 2nd stage non-inverting amplifier. Adjust R10, the 2nd stage gain, until the received signal is visible without distortion or saturation. It should resemble a digital signal, but may show relaxation effects at the '0' and '1' levels. The minimum and maximum voltage 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 TP7 with an oscilloscope or multimeter and adjust R12 until the desired voltage level is achieved. The final processed signal can be viewed at the OUT pad and should appear as a rail-to-rail digital signal with minimal noise.

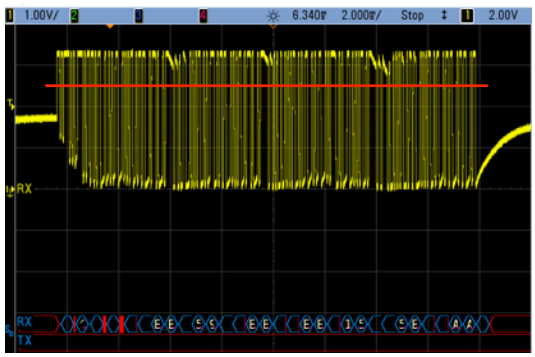
The following oscilloscope screenshots show the progression of signal reception, amplification, and thresholding. Your results may vary depending on OpticSpy's settings and transmitter characteristics.



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 (TP7).

OUT: 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.

Detailed Description

OpticSpy is based on Maxim Integrated's AN1117: Small Photodiode Receiver Handles Fiber-Optic Data Rates to 800kbps application note. This section details OpticSpy's amplification and comparator stages.

The photodiode D1 generates a current when light is shined onto its surface. It is configured in photoconductive mode and is biased with series load potentiometer R2. The resulting voltage has a transimpedance (current-to-voltage) gain equal to R2 and is fed to the input of U1, the 1st stage non-inverting amplifier. R1 and C1 provide filtering for the photodiode's voltage supply.

The capacitive coupling by C3 between U1 and U2, the 2nd stage non-inverting amplifier, negates the amplification of U1's offset voltage. However, capacitive coupling cannot maintain a DC signal and any DC portion will "relax" towards U2's reference voltage (set to 1.65V, one-half of the 3.3V system voltage, by the R6/R11 divider). This effect, particularly noticeable for signals that contain long periods without transitions, is directly affected by the RC time constant of R7 x C3. R7 and C3 are set to minimize this relaxation effect while matching U2's inverting-input source resistance to minimize the offset voltage of the 2nd stage amplifier. The minimum signal frequency before the relaxation effect becomes too large to overcome is approximately 100 Hz (corresponding to a pulse width of 5 ms).

The circuit's overall transimpedance gain depends on the settings of potentiometers R2, R4, and R10. With the default potentiometer positions at mid-range, the overall transimpedance gain is:

$$R2 \times U1Av \times U2Av = 10000\Omega \times (1 + 250/4.7) \times (1 + 500/10) = 27.6M\Omega$$

U1 and U2 both have a gain-bandwidth product of 25 MHz. With OpticSpy's default settings, the maximum signal frequency will be approximately 460 kHz (25 MHz / U1Av). Reducing the amplifier gains will increase the frequency response/bandwidth to a maximum signal frequency upwards of 1.5 MHz. In order to ensure stability of U1 and U2, the gain of each amplifier must be > 10.

Comparator U3 serves as a threshold detector for the received signal and determines the point at which it is treated as a logic level '0' or logic level '1'. Potentiometer R12, which forms a resistor divider, is used to set the threshold voltage. The comparator output goes low when the signal is below the threshold and goes high when the signal is above the threshold. The default setting of R12 results in a voltage threshold of 1.65V. The threshold may need to be adjusted to avoid erroneous transitions. It should be set to a point where the logic levels of '0' and '1' are easily distinguished. The output of U3 should appear as a rail-to-rail digital signal with minimal noise.