

Build Your Own OpticSpy

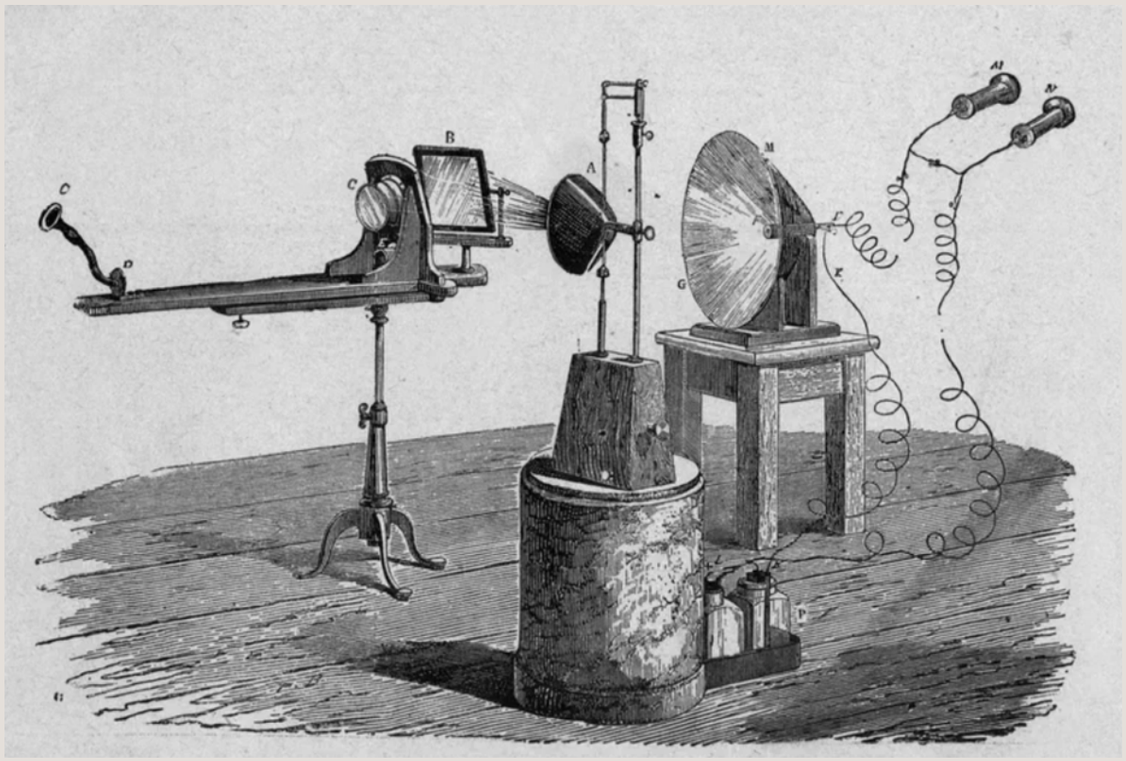
Joe Grand (@joegrand)

OpticSpy (Kit)

- Optical receiver to convert light into voltage
- Wavelength: Visible and near IR light (420-940nm)
- Signal speed: 100Hz-1.5MHz
- Data stream polarity: Select normal v. inverted
- Gain and threshold adjustment via potentiometers
- 6-pin header for connection to USB-to-Serial adapter (FTDI Friend or compatible)

Optical History: An Attempt

- Alexander Graham Bell's Photophone (1880)
- Fiber optic communications (~1963)
- Laser tag (~1979)
- Optical networking systems (VLC, Li-Fi, FSO) (2011)





Covert Channels

- Hidden methods to intentionally exfiltrate/transfer data from a normally functioning system
- Could be achieved with HW and/or FW modification
  - Specifications modified or misdesigned before manufacturing
  - On physical device during manufacturing or in-the-field
  - Hardware implant via interdiction

Exploiting the Environment

- Leakage based on optical, acoustic, thermal, or RF characteristics of a system
  - Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations (Kuhn, Anderson)
  - Emanate Like a Boss: Generalized Covert Data Exfiltration with Funtenna (Cui)
  - Inaudible Sound as a Covert Channel in Mobile Devices (Deshotels)
  - BitWhisper: Covert Signaling Channel between Air-Gapped Computers using Thermal Manipulations (Guri et al.)

Blinkenlights

- Using LEDs to exfiltrate/send data
  - Modulation faster than the human eye can detect
- Optical covert channels
  - Information Leakage from Optical Emanations (Loughry and Umphress, 2002)
  - Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks (Zalewski)
  - Extended Functionality Attacks on IoT Devices: The Case of Smart Lights (Ronen, Shamir)
  - xLED: Covert Data Exfiltration from Air-Gapped Networks via Router LEDs (Guri et al.)

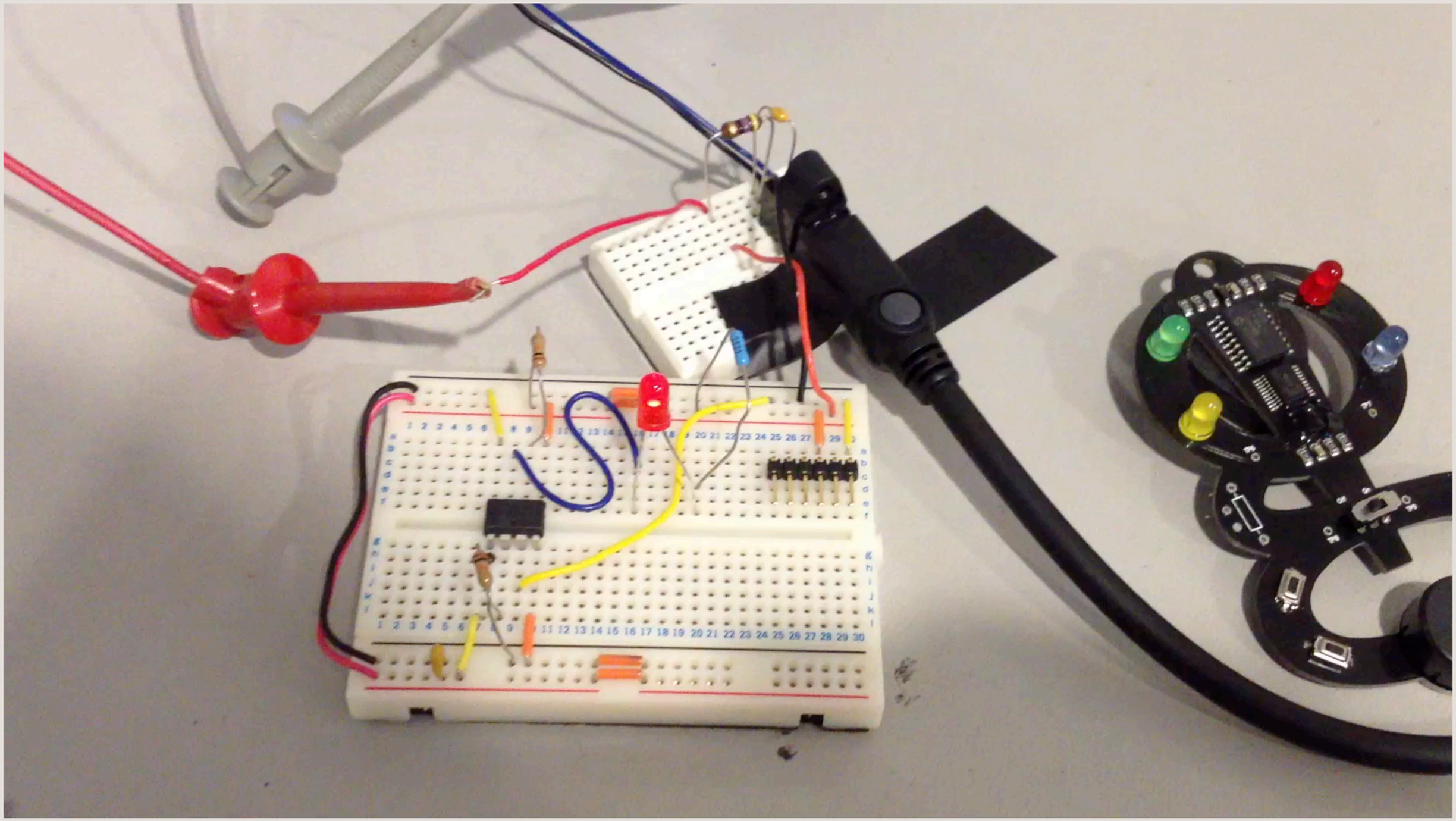
Related Projects

- Heathkit Laser Trainer/Receiver (1985)
- Engineer's Mini Notebook: Optoelectronics Circuits (Forest Mims III, 1985)
- IRis (Craig Heffner, 2016)
- See no evil, hear no evil: Hacking invisibly & silently with light & sound (Matt Wixey, 2017)

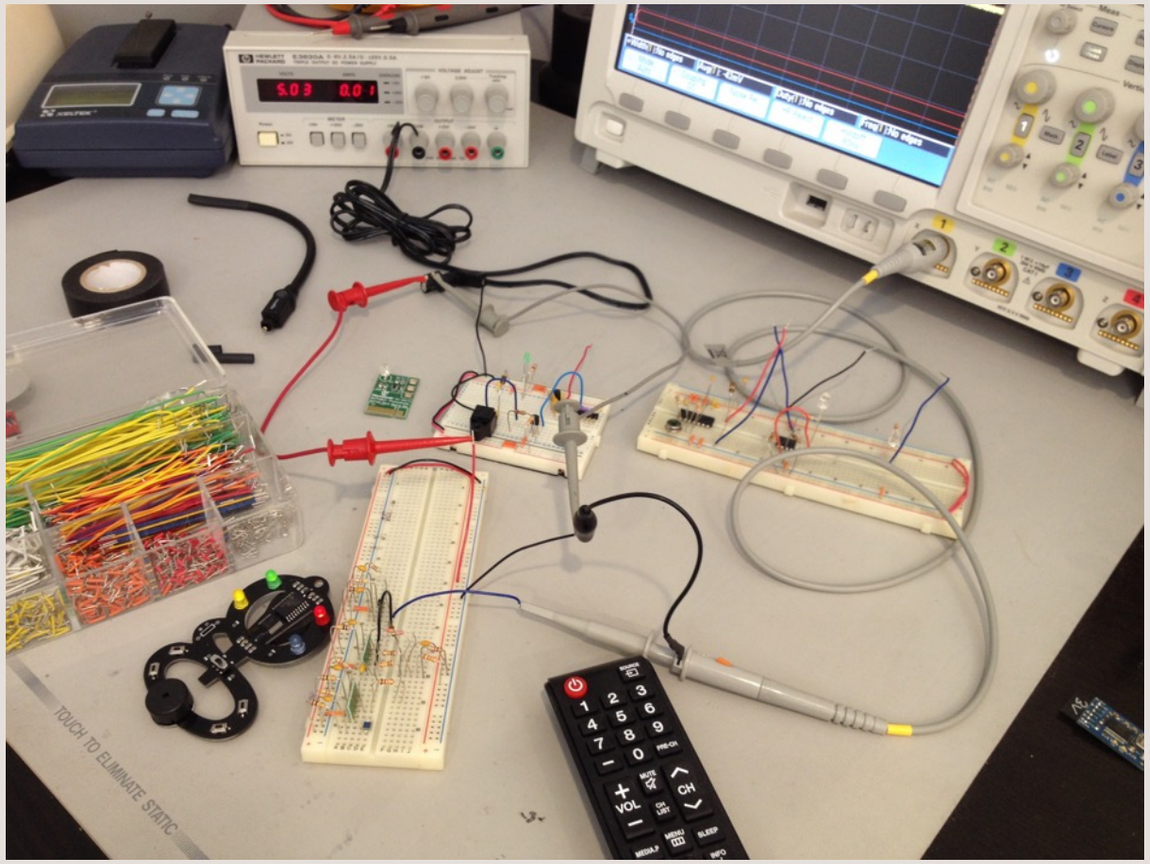
Design Goals

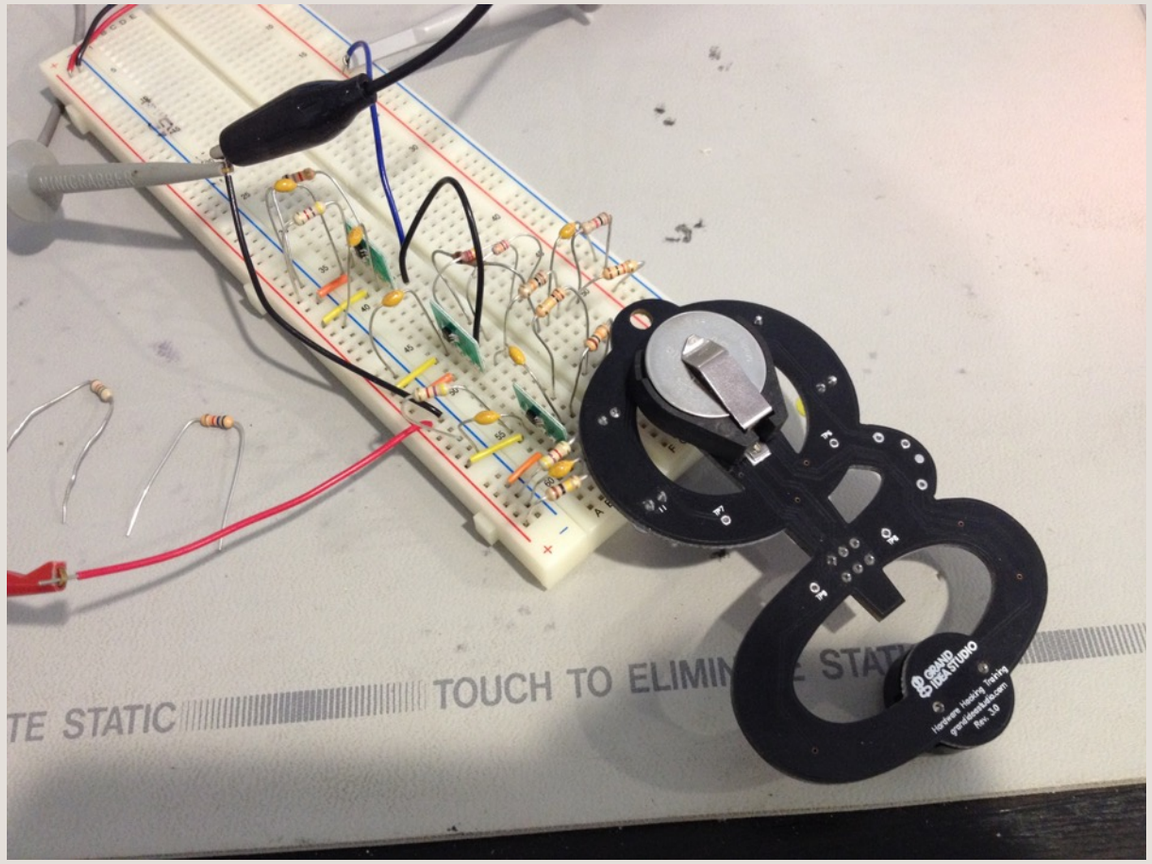
- Open source tool for optoelectronic experimentation
  - Easy to understand theory
  - Off-the-shelf components
  - Hand solderable
- Raise awareness of other interesting communication/ exfiltration methods

Proof of Concept

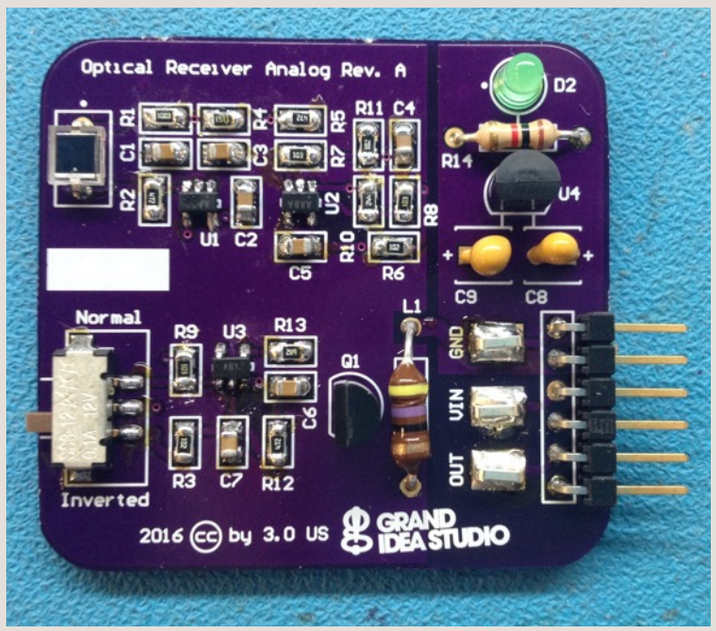


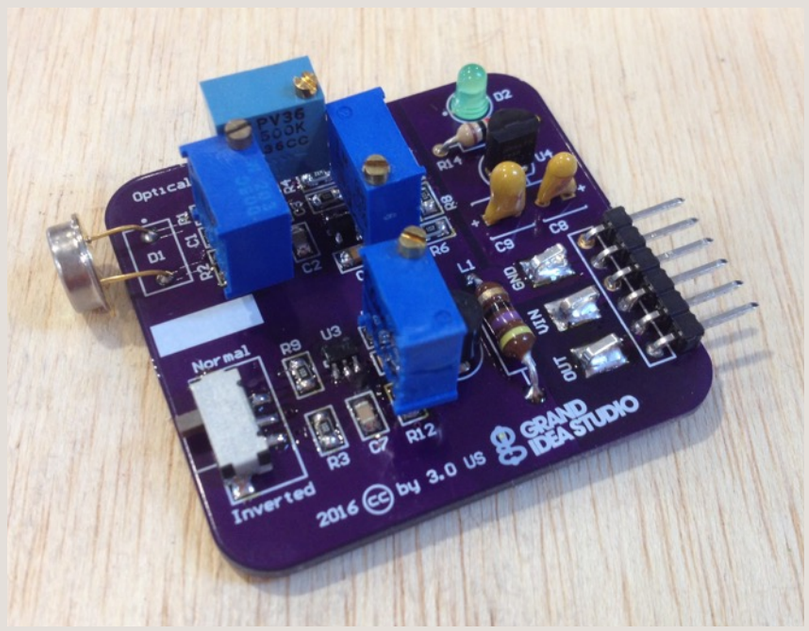
Early Versions



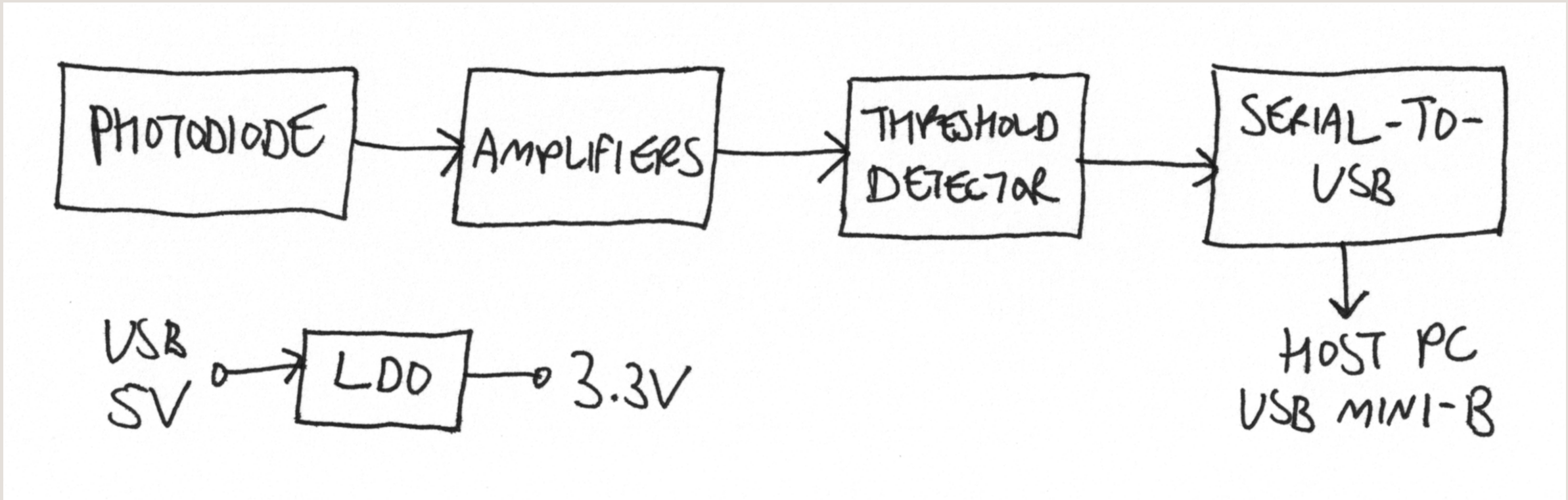




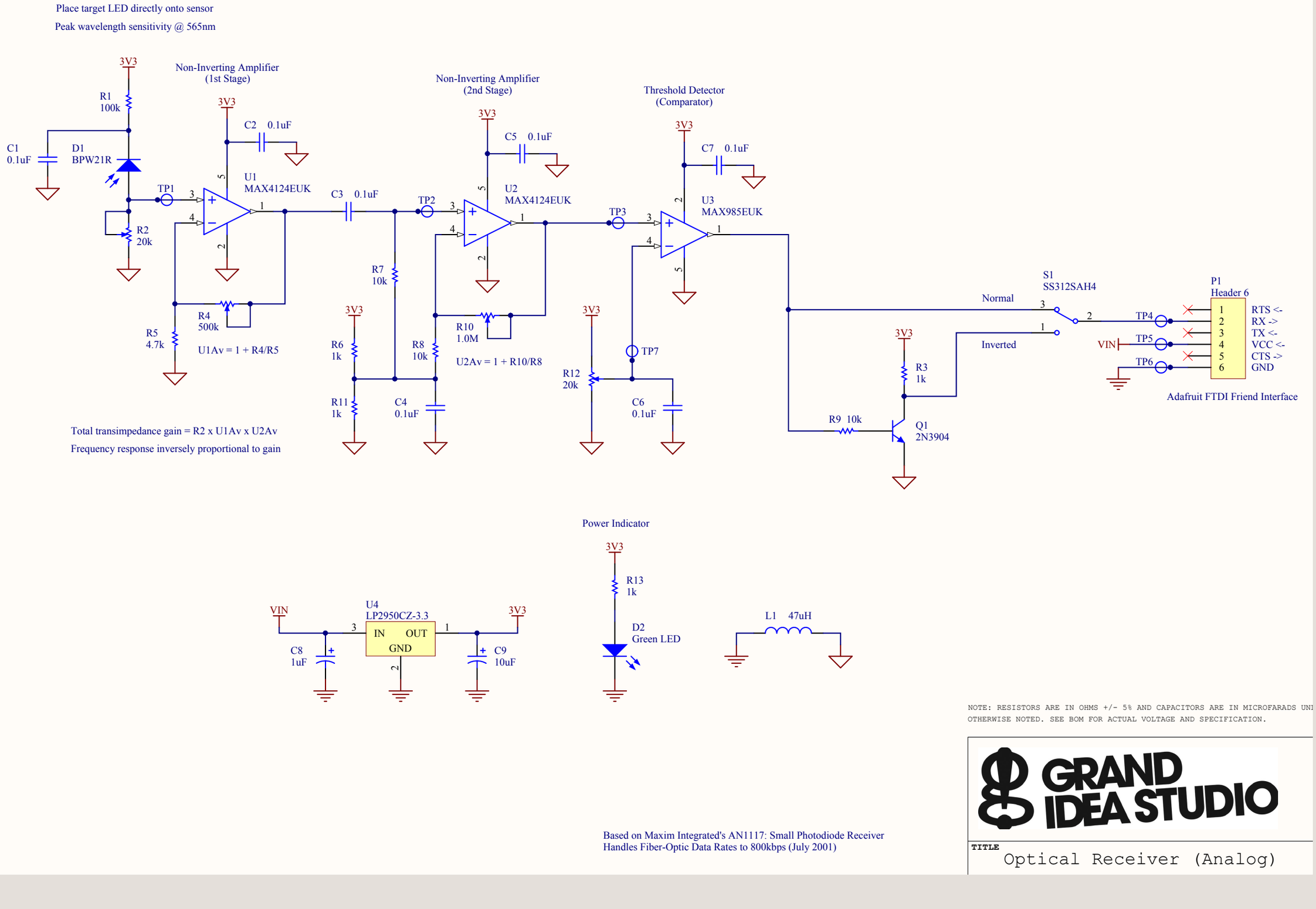




Block Diagram



Schematic (Kit)

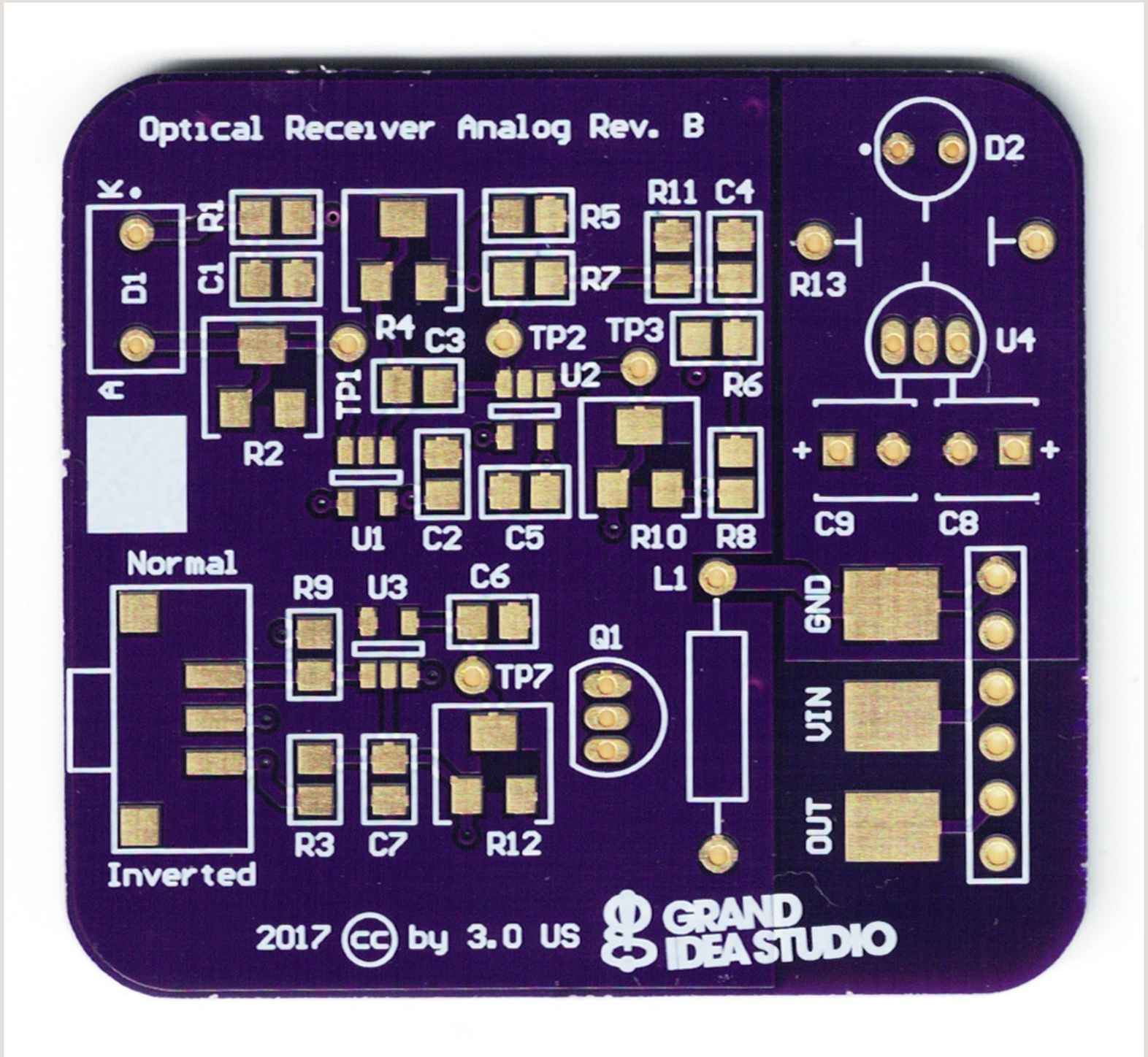


NOTE: RESISTORS ARE IN OHMS +/- 5% AND CAPACITORS ARE IN MICROFARADS UNI
OTHERWISE NOTED. SEE BOM FOR ACTUAL VOLTAGE AND SPECIFICATION.

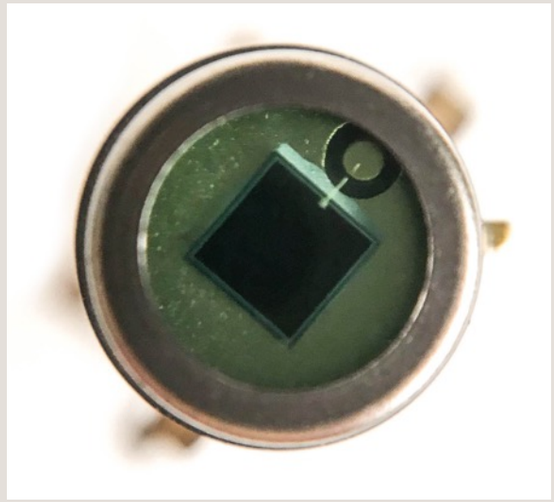
GRAND IDEA STUDIO

TITLE
Optical Receiver (Analog)

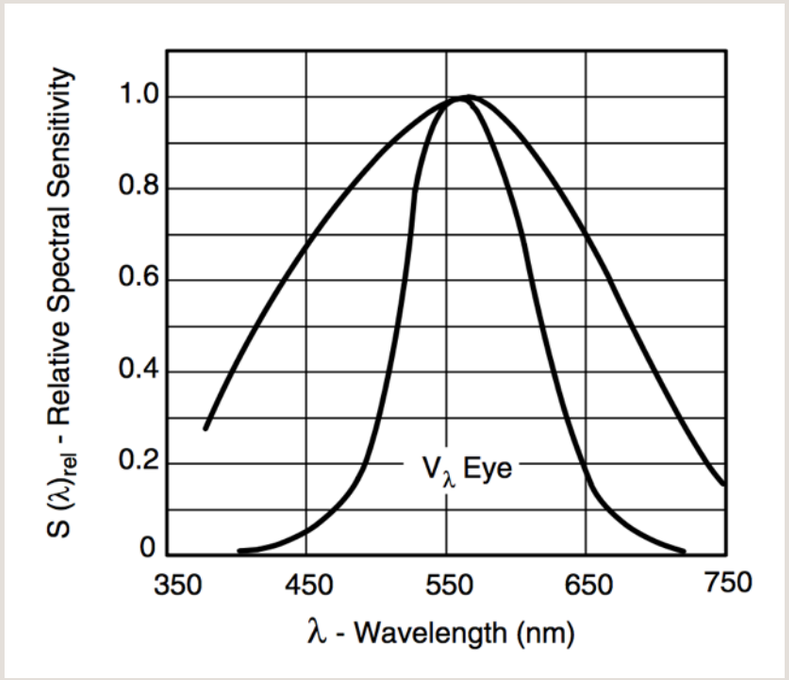
PCB (Kit)

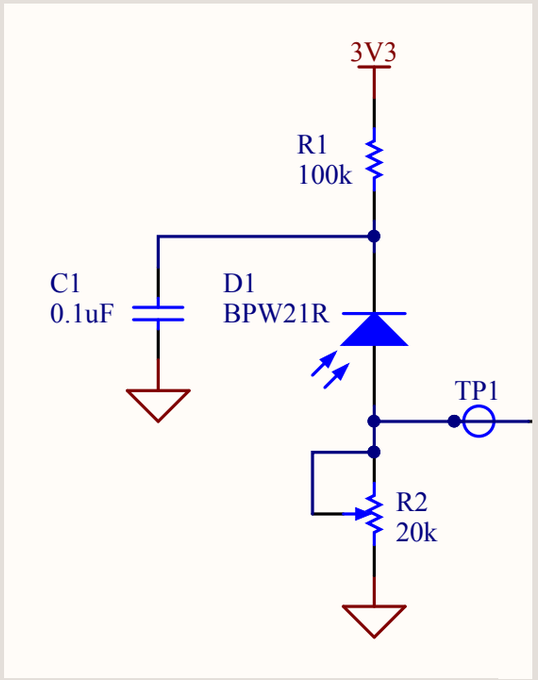

Optical Receiver Analog Rev. B
D1
R1
C1
R2
R4
C3
TP1
TP2
TP3
U2
R5
R7
R11
C4
R6
R10
R8
U1
C2
C5
D2
R13
U4
C9
C8
Normal
Inverted
R9
U3
C6
TP7
Q1
L1
R3
C7
R12
GND
VIN
OUT
2017 cc by 3.0 US
GRAND IDEA STUDIO

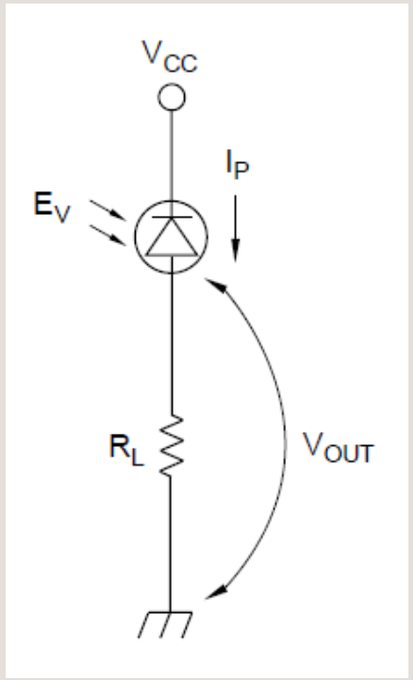
Photodiode



- Vishay Semiconductor BPW21R
- Converts light into current
- Photoconductive mode (reverse bias)
  - Faster response -> higher bandwidth
  - Less sensitivity, increased dark current
- Bias resistor affects response/sensitivity

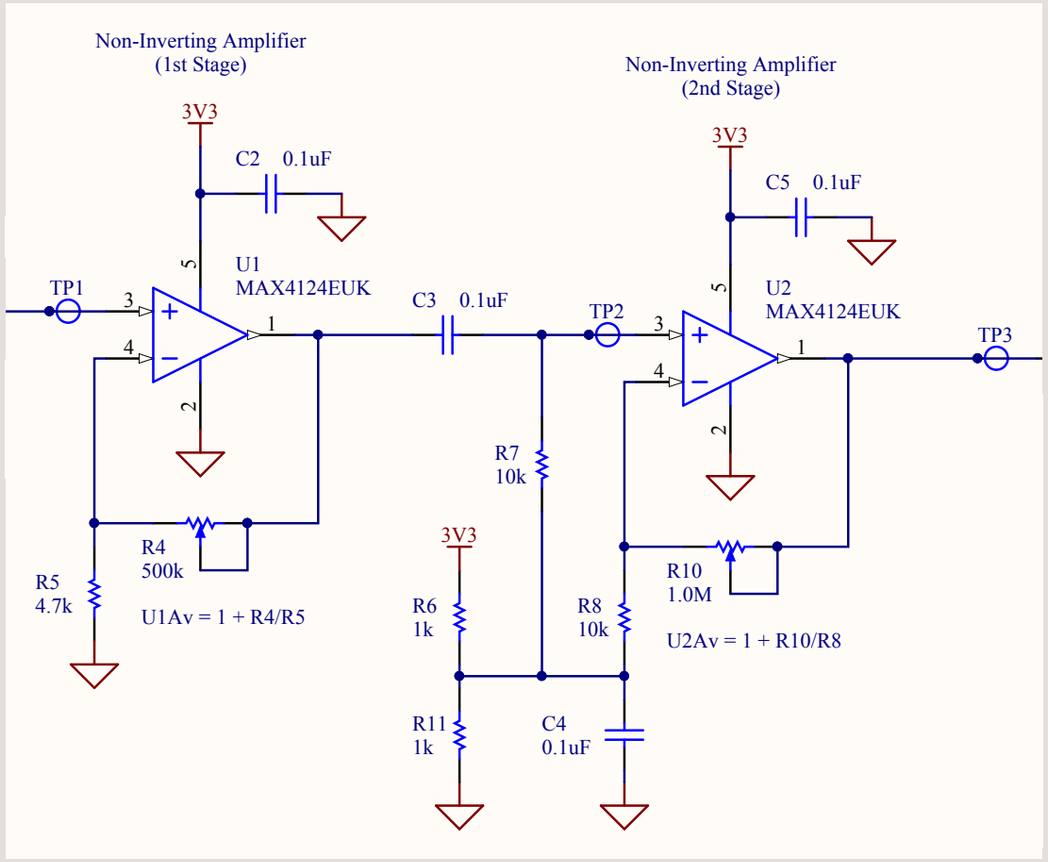






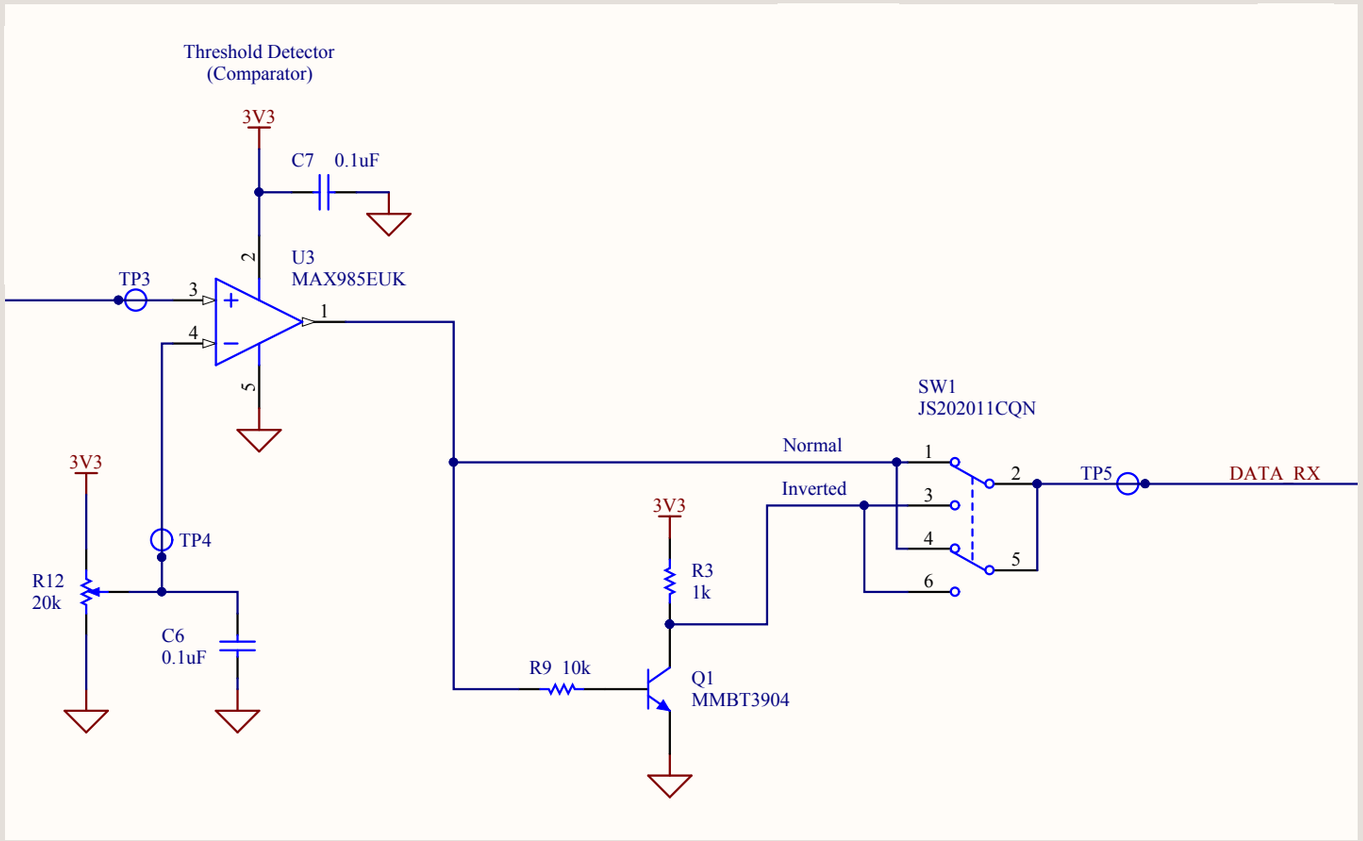
Amplification

- Maxim MAX4124 Wide Bandwidth, Low Power, Rail-to-Rail Operational Amplifier
- Two stages w/ signal massaging in between
  - Lower gain per stage -> less overall noise
- Total transimpedance gain = R2 x U1Av x U2Av



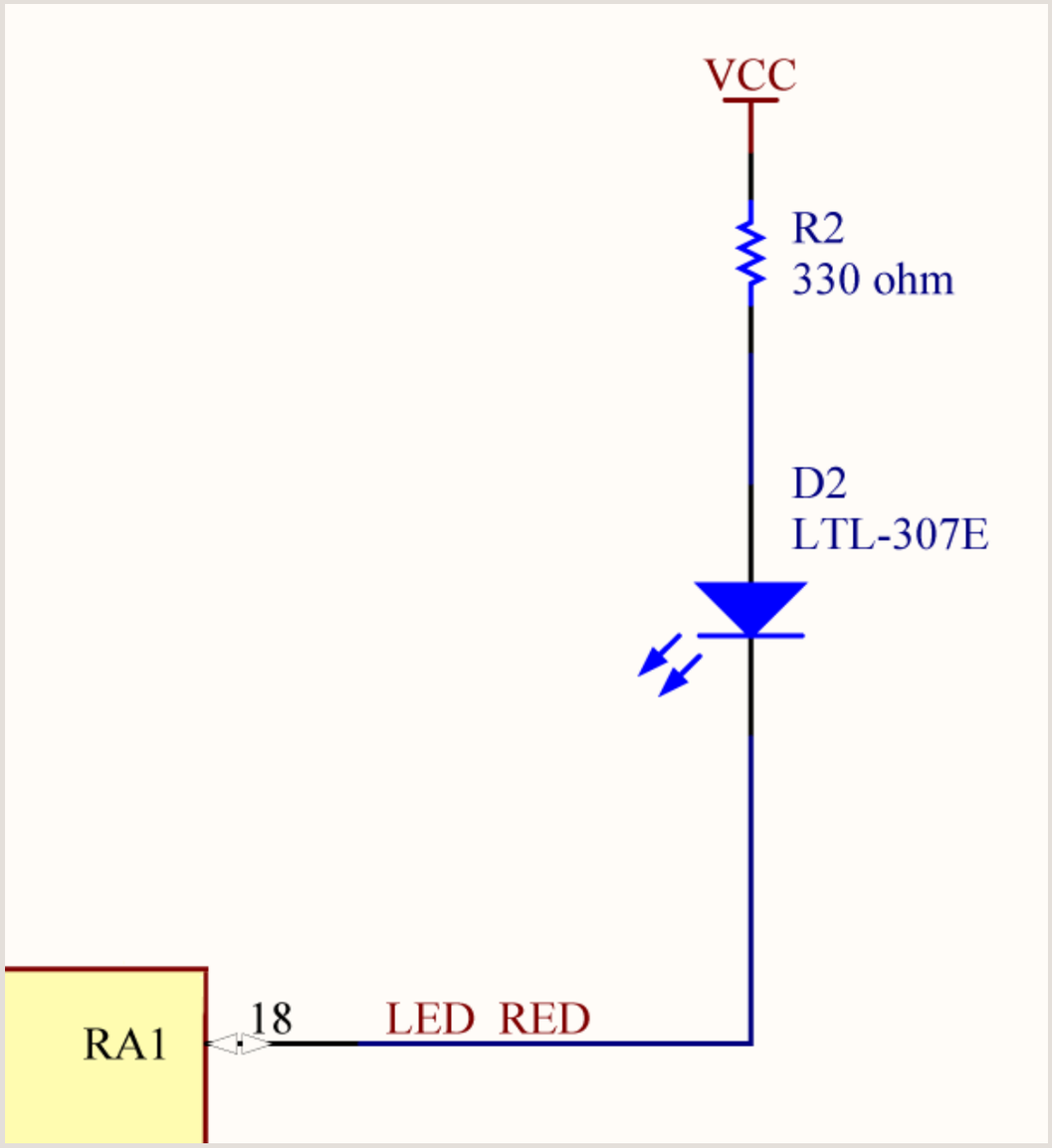
Comparator

- Maxim MAX985 Micropower, Low Voltage, Rail-to-Rail Comparator
- Determine what portion of signal treated as logic level '0' or '1'
- Adjustable threshold voltage w/ potentiometer R12



Target Data Transmission

- Standard LED driver circuit



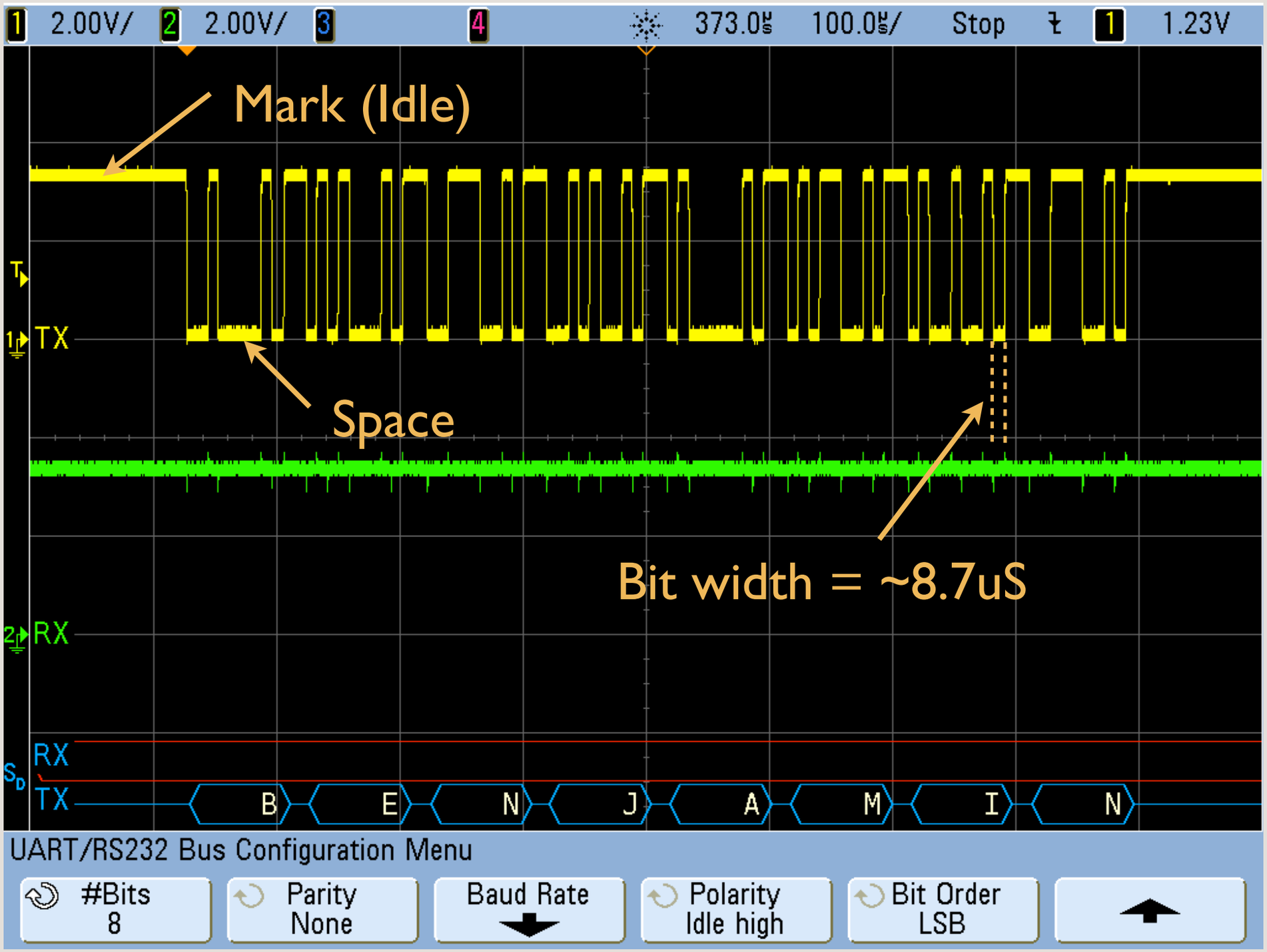
Target Data Transmission

- Asynchronous serial (UART)
  - No external clock needed
  - NRZ (Non-Return-To-Zero) coding
  - Transfer speed (baud rate) selectable
  - Data bits sent LSB first (D0)

1	2	3	4	5	6	7	8	9	10	11
Start bit	**5–8 data bits**								**Stop bit(s)**	
Start	Data 0	Data 1	Data 2	Data 3	Data 4	Data 5	Data 6	Data 7	Stop	

*** Start bit + Data bits + Parity (optional) + Stop bit(s)

Target Data Transmission



Target Data Transmission

- Printable ASCII data via standard UART
- printf(message) or equivalent

```
while(1)
{
    #use delay(clock=4000000)
    #use rs232(baud=19200, parity=N, bits=8, xmit=LED_RED, force_sw, stream=LED)
    setup_oscillator(OSC_4MHZ | OSC_INTRC | OSC_PLL_OFF); // increase clock speed
    fprintf(LED, msg_covert); // transmit secret message through the LED
}
```

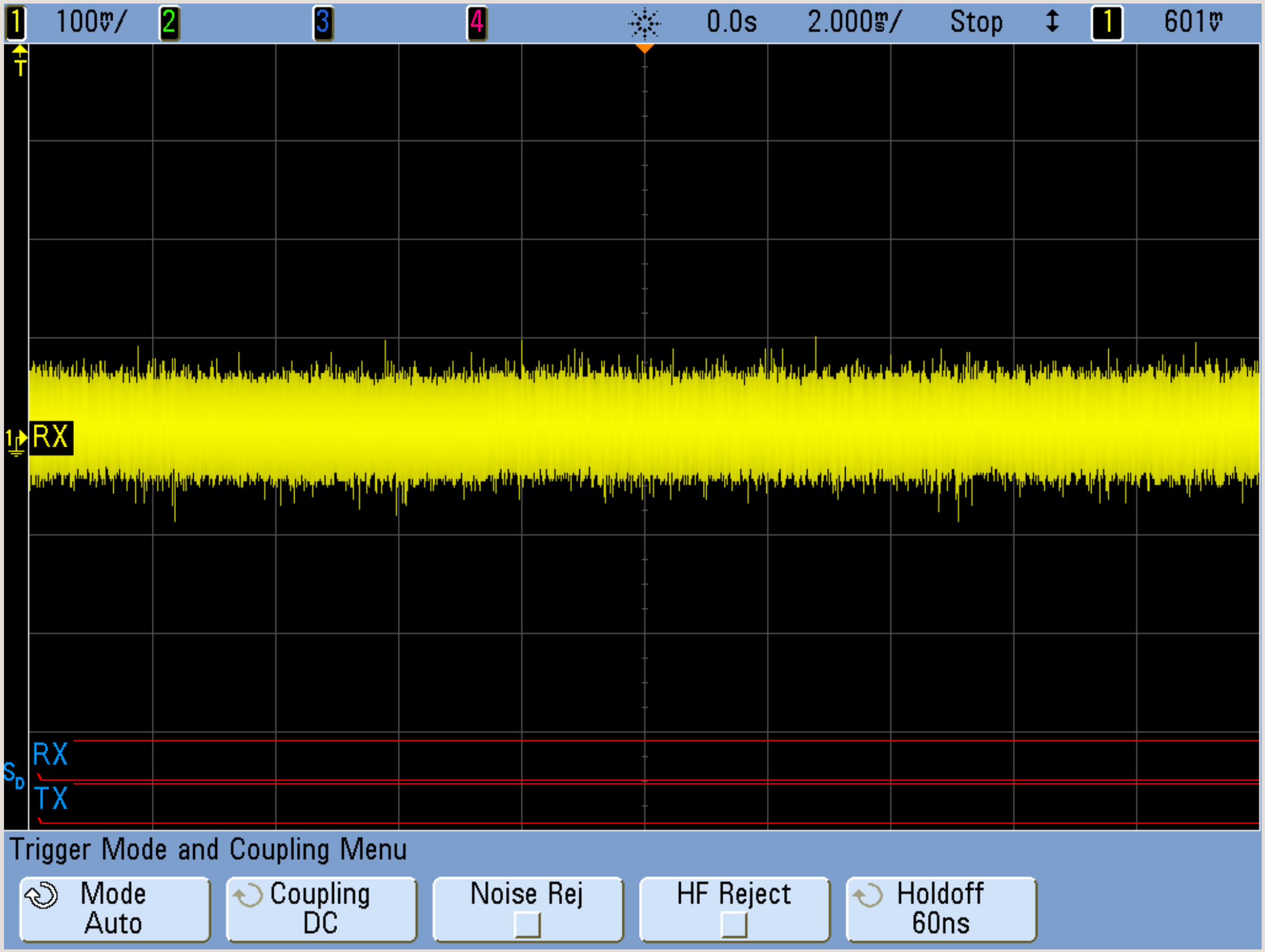
```
// Set up a new serial port
SoftwareSerial opticSerial =  SoftwareSerial(rxPin, txPin);

opticSerial.print(msg_covert); // Transmit secret message through the LED
opticSerial.flush();           // Wait for all bytes to be transmitted
```

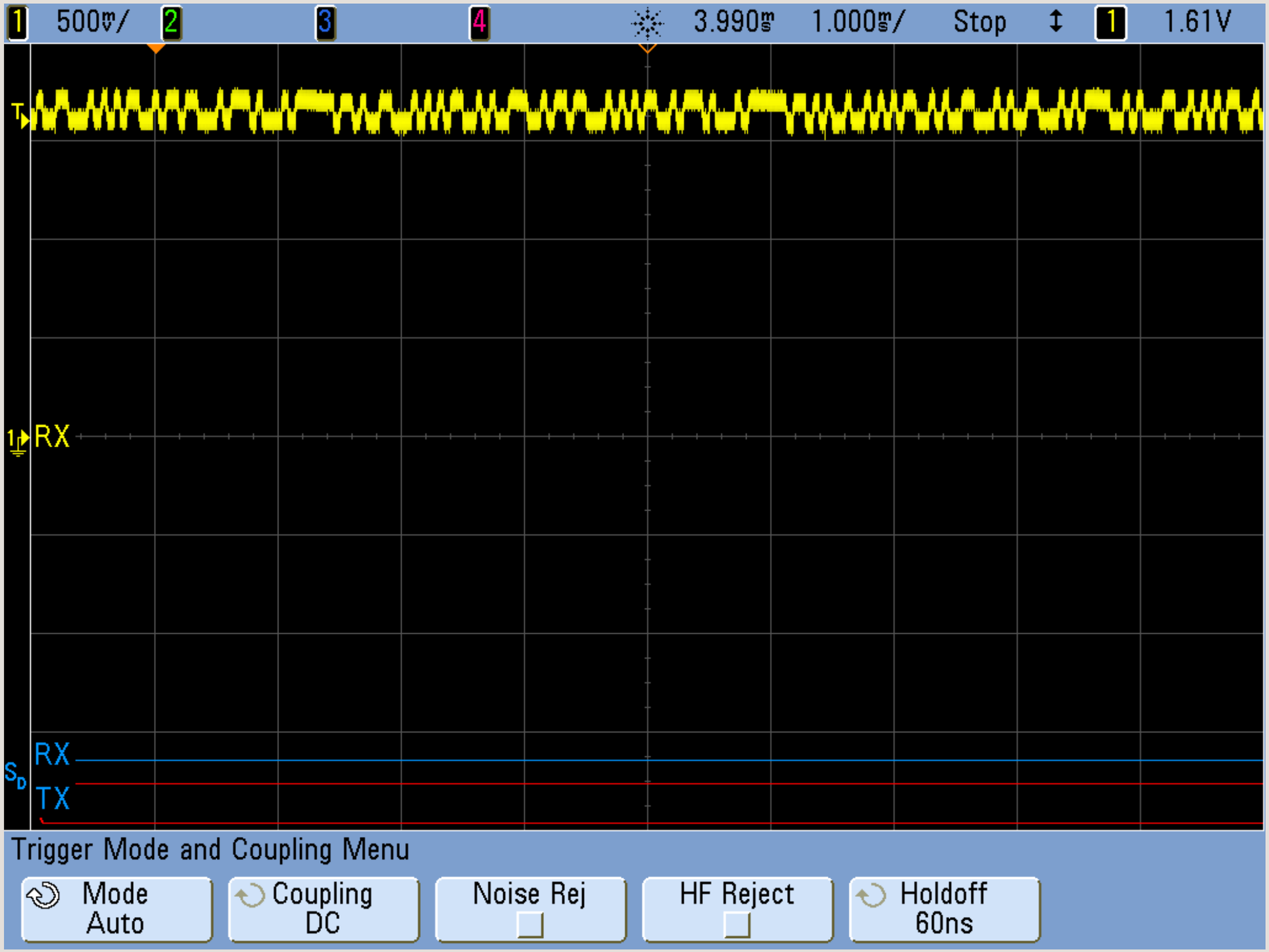
Calibration

- Adjust settings for a particular target system
  - Reduce ambient noise
  - Increase receive distance
  - Change frequency response/bandwidth
  - Dependent on brightness and wavelength of transmitting signal
- Potentiometers
  - Gain adjustment (three stages)
    - Default setting @ mid-range -> 27.6MΩ
  - Threshold voltage adjustment (for comparator)
    - Set to 2.5V during production

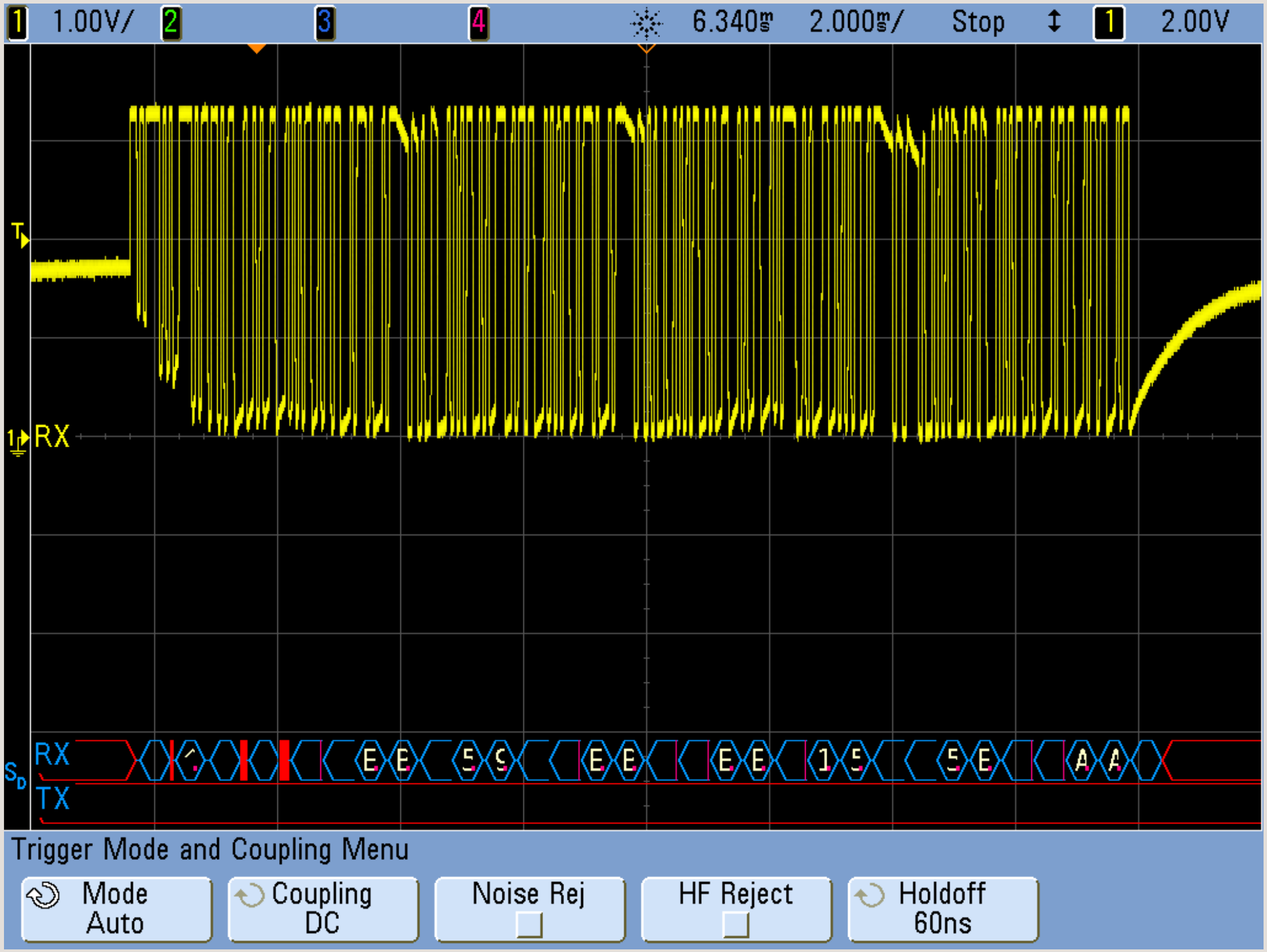
TP1: Photocurrent-to-Voltage



TP2: 1st Stage Amp Output



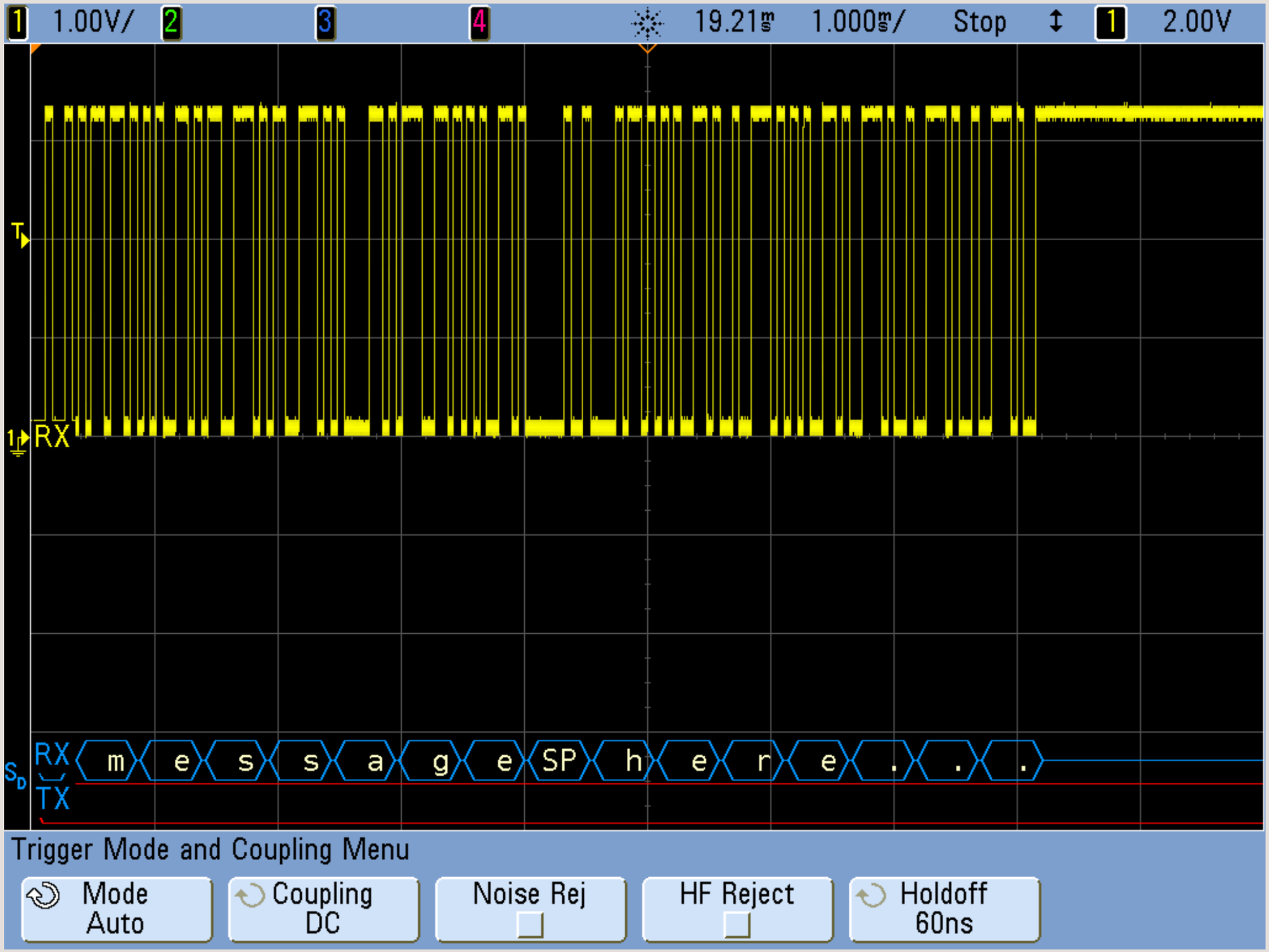
TP3: 2nd Stage Amp Output



TP5: Comparator Output

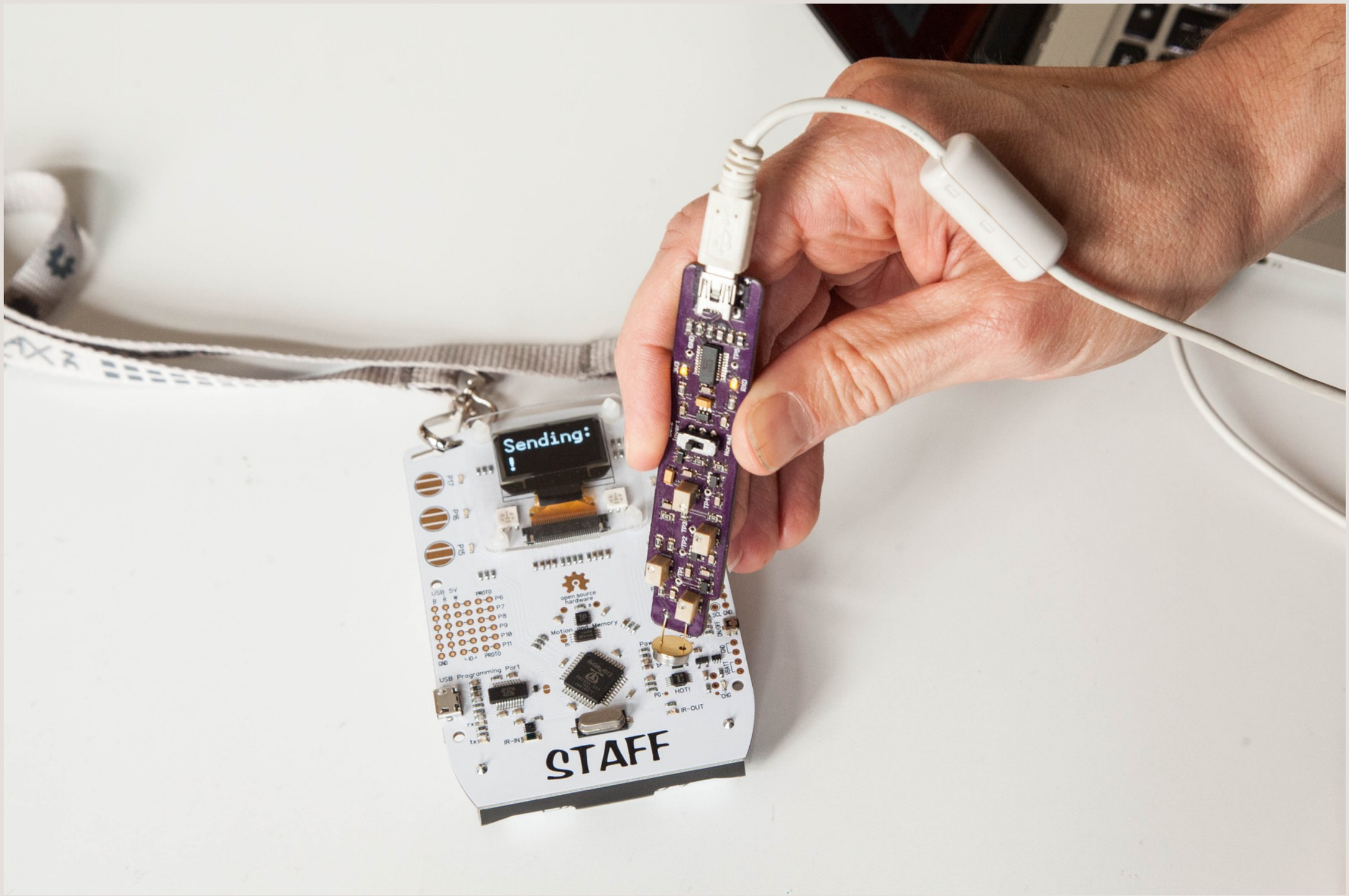


TP5: Comparator Output

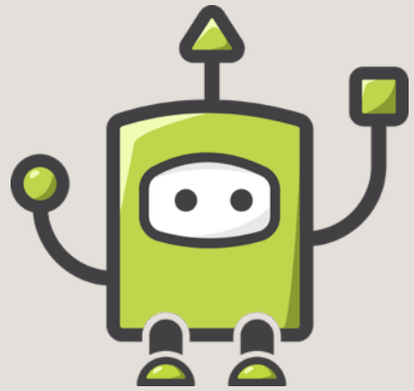


Demonstrations

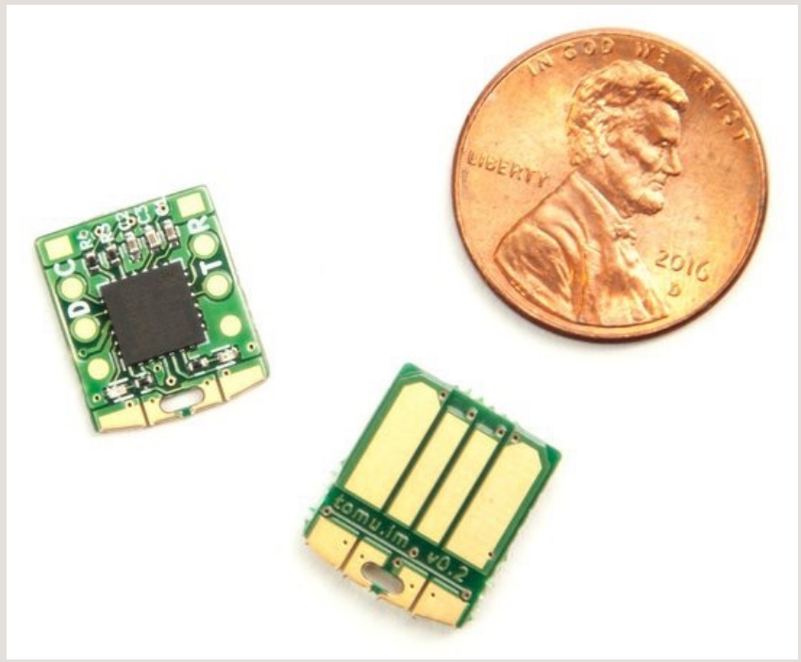
Parallax Electronic Badge

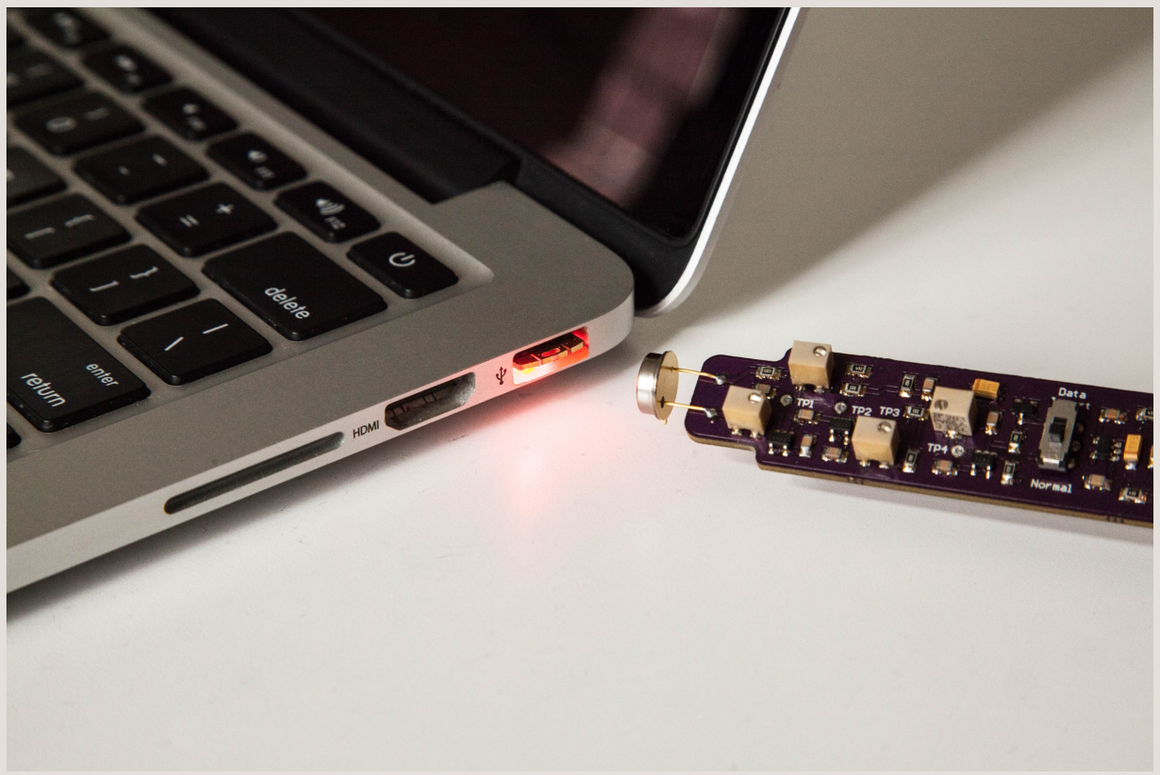


Tomu

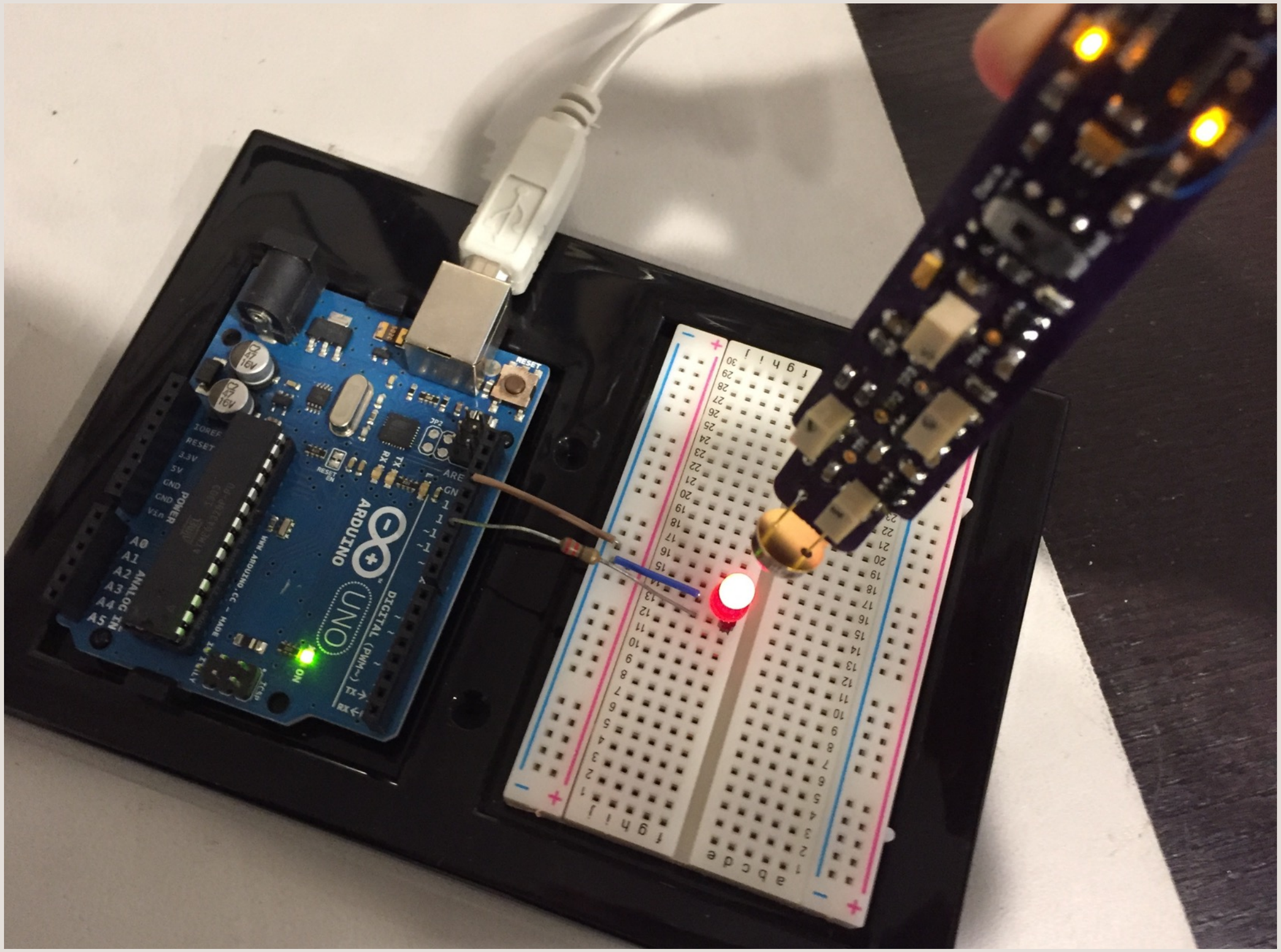


- Silicon Labs Happy Gecko EFM32HG309
- Total 12 components (incl. plastic case)
- 100% Open Source (w/ KiCad)
- http://tomu.im
- https://github.com/im-tomu/tomu-quickstart/tree/master/opticspy





Arduino + External LED

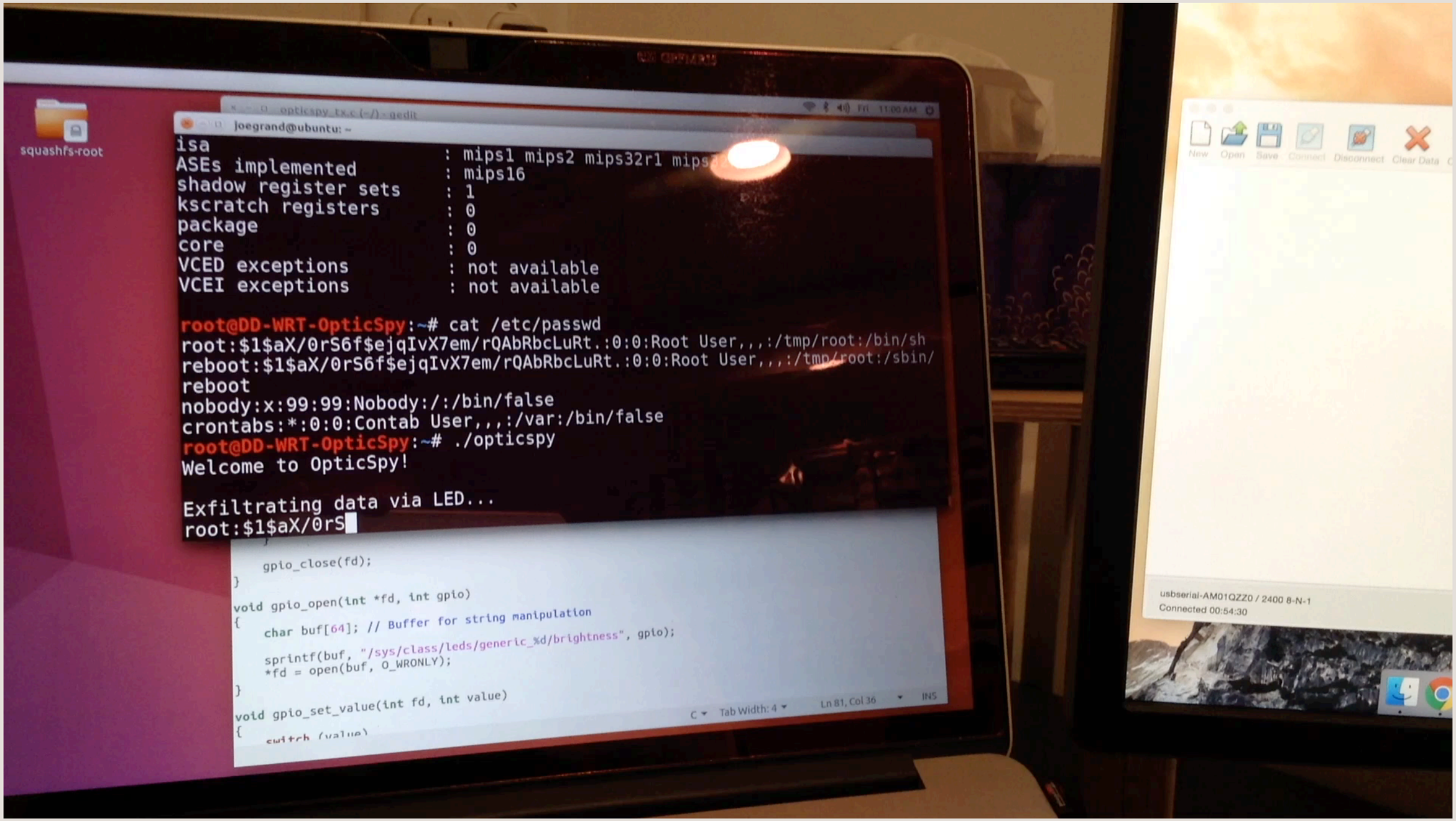


TP-Link TL-WR841N

- Physically unmodified router w/ DD-WRT
- Cross compiled w/ toolchain-mips_24kc_gcc-7.2.0_musl
- Loaded onto the device with known administrator credentials (as proof of concept)



TP-Link TL-WR841N



Limitations

- Data must be NRZ encoded in order to pass through USB-to-Serial interface
- Short receive range (up to ~4 inches) w/o additional optics
- Difficult to determine potentiometer settings

Application ideas

- Search for optical covert channels in existing devices
- Discover optical networking/communications systems
- Add data transfer functionality to a project
- Receive/demodulate IR signals
- Measure the world around you

Come into the Light

- grandideastudio.com/portfolio/opticspy
  *** Schematic, BOM, Gerber plots, test procedure, user manual, demonstration code

- oshpark.com/profiles/joegrand
  *** Bare boards

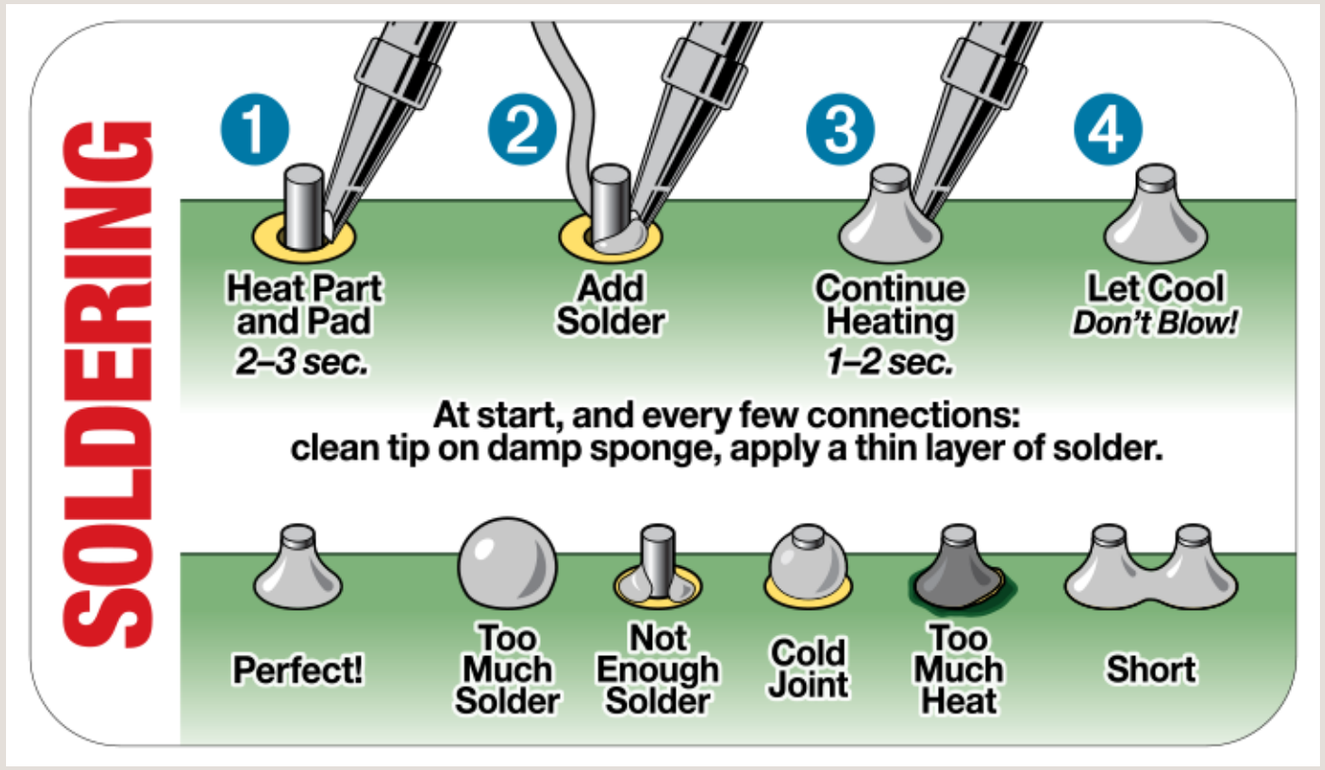
- crowdsupply.com/grand-idea-studio/opticspy
  *** Assembled units

Build Your Own OpticSpy

- Soldering Primer
- Kit Distribution
- Assembly and Testing

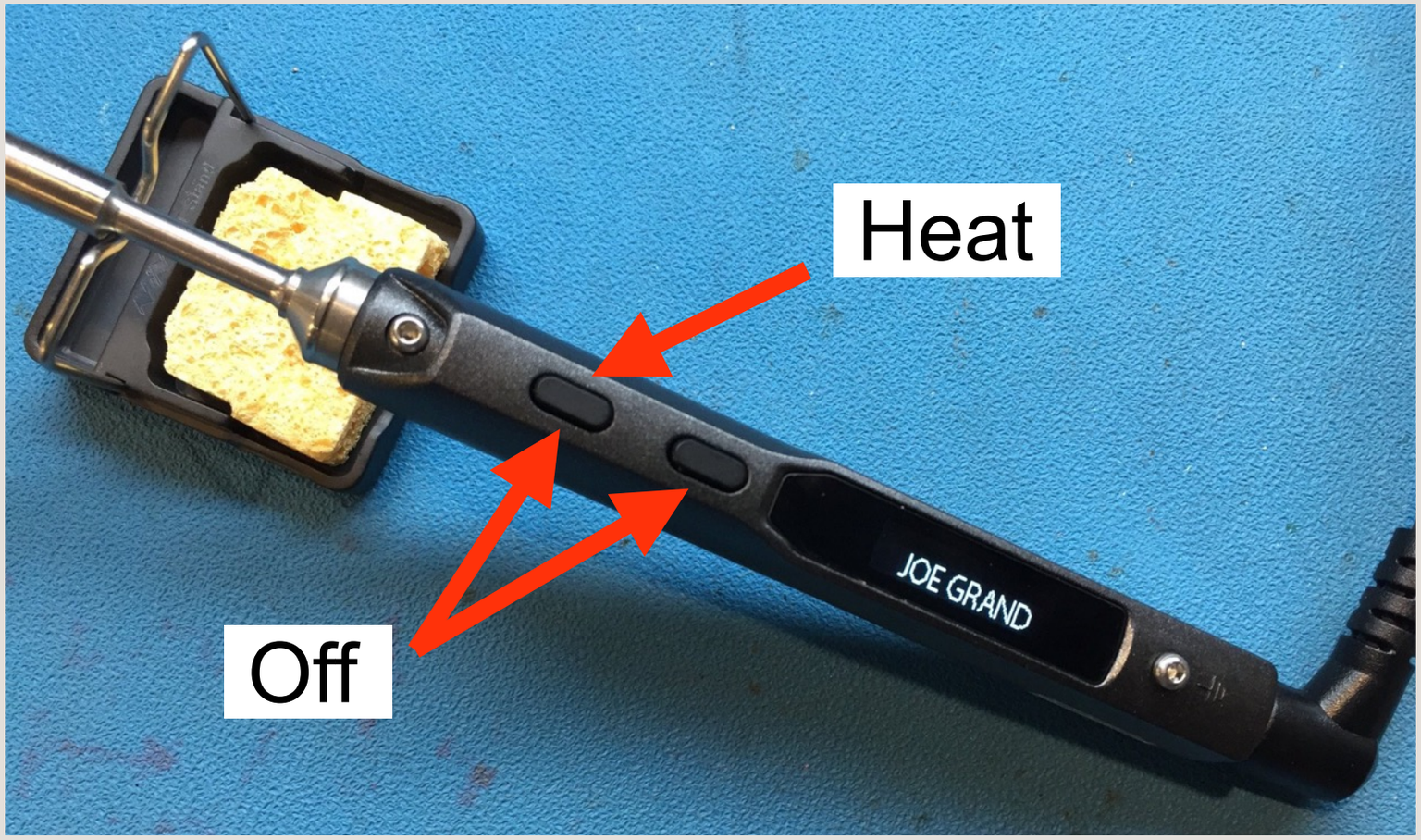
Soldering

- Process to hold components together and/or mount them to a surface
- Melting and putting a filler alloy (solder) between the target surfaces
- Requires sufficient heat distribution

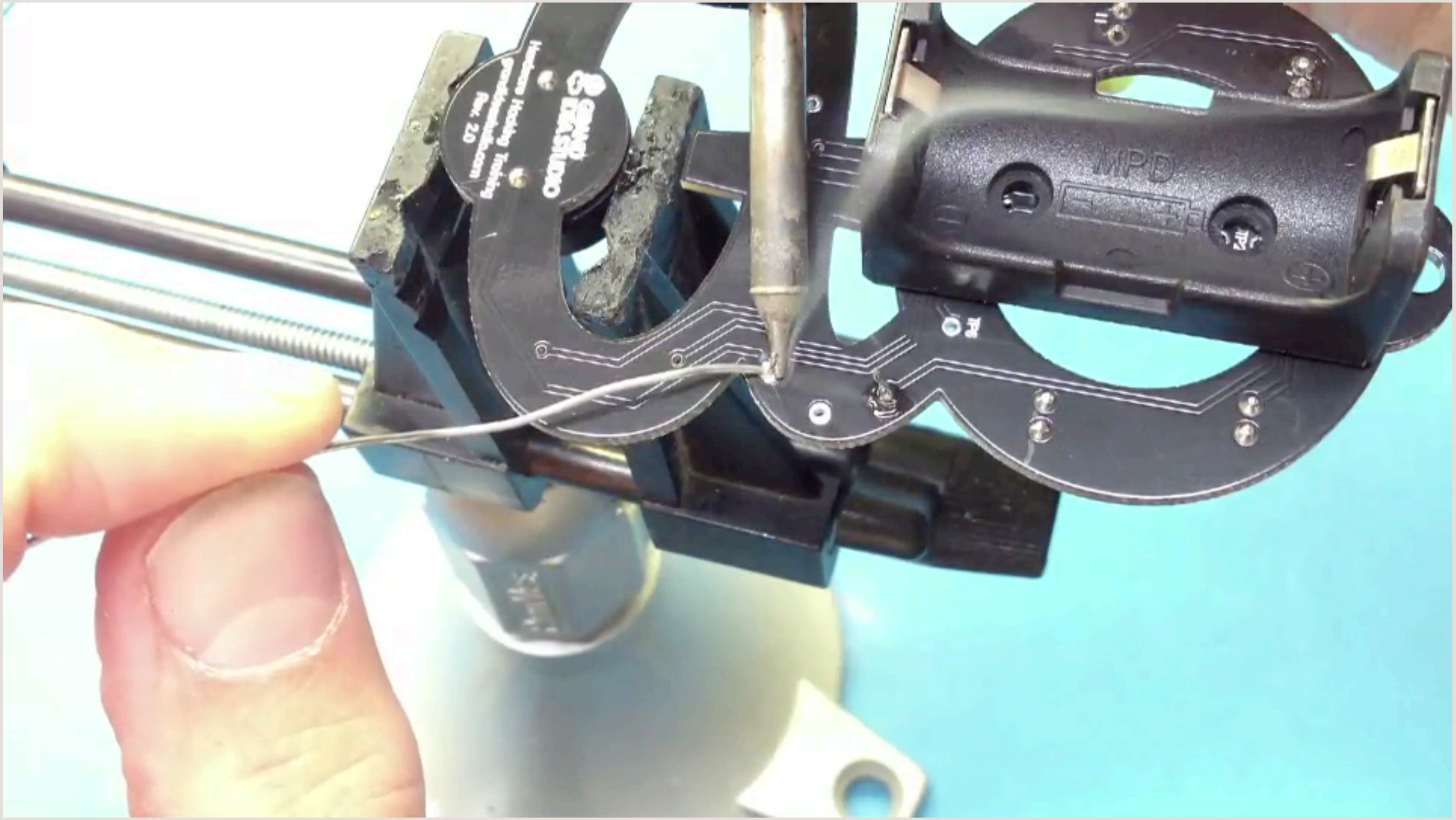


Sainsmart Pro32 (TS100)

- Fast heating: 315°C / 600°F @ ~10 sec.
- Auto-sleep: Cool down @ 2 min., turn off @ 5 min.
- Powered by barrel jack, not USB



Soldering Video



Kit Distribution

- Organize parts in a way that works for you
- Double-check placement before soldering
- Try not to lose anything :)

Item	Quantity	Reference	Manufacturer	Manuf. Part #	Distributor	Distrib. Part #	Description
1	7	C1, C2, C3, C4, C5, C6, C7	Kemet	C0805C104K5RACTU	Digi-Key	399-1170-1-ND	Capacitor, 0.1uF, 50V, Ceramic, 10%, X7R, 0805
2	1	C8	AVX	TAP105K020SCS	Digi-Key	478-1833-ND	Capacitor, 1uF, 20V, Tantalum, Radial
3	1	C9	AVX	TAP106K016SCS	Digi-Key	478-1839-ND	Capacitor, 10uF, 16V, Tantalum, Radial
4	1	D1	Vishay Semiconductor	BPW21R	Digi-Key	751-1013-ND	Photodiode, Silicon PN, 420-675nm, TO-5
5	1	D2	Lite-On	LTL-1CHG	Digi-Key	160-1710-ND	LED, Green diffused, 2.1V, 569nm, 3mm
6	1	L1	EPCOS (TDK)	B78108S1473J	Digi-Key	495-5568-1-ND	Inductor, 47uH, 1.1R, 450mA, Axial
7	1	P1	Molex	22-28-8062	Digi-Key	WM50015-06-ND	Header, Single row, R/A, 6-pin, 0.244" L, 0.1” P
8	1	Q1	Fairchild Semiconductor	2N3904BU	Digi-Key	2N3904FS-ND	Transistor, NPN, 40V, 0.2A, TO-92
9	1	R1	Any	Any	Digi-Key	P100KACT-ND	Resistor, 100k, 5%, 1/8W, 0805
10	2	R2, R12	Bourns	PVG5A203C03R00	Digi-Key	490-2667-1-ND	Resistor, Variable Trimmer, 20k, 1/8W, SMD
11	3	R3, R6, R11	Any	Any	Digi-Key	P1.0KACT-ND	Resistor, 1k, 5%, 1/8W, 0805
12	1	R4	Bourns	PVG5A504C03R00	Digi-Key	490-2674-1-ND	Resistor, Variable Trimmer, 500k, 1/8W, SMD
13	1	R5	Any	Any	Digi-Key	P4.7KACT-ND	Resistor, 4.7k, 5%, 1/8W, 0805
14	3	R7, R8, R9	Any	Any	Digi-Key	P10KACT-ND	Resistor, 10k, 5%, 1/8W, 0805
15	1	R10	Bourns	PVG5A105C03R00	Digi-Key	490-2663-1-ND	Resistor, Variable Trimmer, 1.0M, 1/8W, SMD
16	1	R13	Any	Any	Digi-Key	1.0KQBK-ND	Resistor, 1k, 5%, 1/4W, Axial
17	1	S1	NKK Switches	SS312SAH4	Digi-Key	360-3250-ND	Switch, Slide, SPDT, R/A, 0.4VA @ 24V
18	3	TP4, TP5, TP6	Keystone	5016	Digi-Key	5016KCT-ND	Testpoint, SMT
19	2	U1, U2	Maxim Integrated	MAX4124EUK+T	Digi-Key	MAX4124EUK+TCT-ND	IC, Operational Amplifier, Rail-to-Rail, SOT23-5
20	1	U3	Maxim Integrated	MAX985EUK+T	Digi-Key	MAX985EUK+TCT-ND	IC, Comparator, Push-Pull, Rail-to-Rail, SOT23-5
21	1	U4	Texas Instruments	LP2950CZ-3.3/NOPB	Digi-Key	LP2950CZ-3.3/NOPB-ND	Linear Regulator, LDO, 3.3V @ 100mA, TO-92
22	1	PCB	OSH Park	OPTICSPY ANALOG	N/A	N/A	PCB, Fabrication

Assembly and Testing

- Surface mount
  - SOT23-3 (U1, U2, U3)
  - Potentiometers (R2, R10, R12)
  - Discretes
  - Switch
- Through hole
  - TO-92 (Q1, U4)
  - Note polarity of D1, D2, C8, C9
- Attach FTDI Friend
- Set TP7 to 2.5V via R12





The End.