```
┬ë╗║uHì #╣╬Q \δ┤≥⌐&╓  )ÄOf╗║¥                                                          "╬Qw«⌠τ1 ¿─╗ïwz┼

σΓε_¢ë┘M─Zñê$──√0≤╣│O»√▌╞5.%Ç▐▐┌+A%}┘┴å╙Σ¼]%üU10╓∞Pçd=:┐F1?éτYÜN└hk║6dXßU╗¶Cì▐ït≈╟ì
¿(▌¢┘Q+iMïoß•┼╥├╙/i╠ï(╬╜╪â;╙+├E4&:Æ▄6hp╟A╕╙«Θp┬┘d'T╢°╞dU╧K¿*,"*}0å╨cï.îHÉxi3Ripº{v
:∩io╚╕uΘá▀hf├o┐iΘ┘Uó╟┘'╤▀Jâ÷Z9┬Ä═╪²î(•f»òî8ƒ╫+æ]ε≈2æ²HëGτn■vr╣▓pGE+╓s╗┬ó⌠óπΘæºï7┘'\
s≈V~è█Θ!░∩r±pGæ£╢║»Φ₧┴┘┤┌e½ñ%≥╤Æñî•IÉyX%╟╪x%▓╓j░¶á≈■nP⌐óE╨>╝⌡ôâτ5mⁿ$éæ┬ƒàâ\─'╧¢╫v┼%
ïw/╝)8╨⌡2r?]ñi╫Æ■╫≥╞ΩdΦ│·i¢─Z┘D*±rä1á£¢┘╧ñ▓εt+=┼9Xj[c·fåδƒn«cnº╒ƒj┘{G╟═¬t9q▌cÅx¢:;ä
«╨═∩viÿ½µ«╓%ú╗i╓ùDrF}à╫─⌐_╫█╕xa▄⌐╨æQ▄P}C┼k╤Vâ¢ñi│≤é╓]3L¼J╝╓∞ñ₧»█JÜσ║<α╒²på▓╚≈Θñüqò№
─7«δtΘá╚q▐mO╕φB┤─e;8┌Éñ╓_+öm/├rx"ú=BΘ╓j3I¼TDì¶Zè┌═%┴▄1V╕4h7Ö∞'π9εf1ª├Γ½n≡•tª¬v:ïI▓║
i⌠g¶╫;~╧1%7öñü'┼•ⁿ╢t╣ëÅA─ⁿ#┘?┼⌠ùHD¢╪Γ═H¬Åτ÷├ErT╧'O─'·NNjφ{∞J╤ù▐√Jqi)═eªÉè≈m⌠ïjÑsU╒

N╓Åì»FJ╗¿∩ë┌eτI½éYΣ/╣╪(╟~╓*fH█╝║h╓å2«àb«≥n6WÑlá+⌐αv╧yú.╨╧╨│╨┼,√┬Cp]w─¶Yªlä£/ⁿ⌠$¥T⌠j
á╕╞░╟»╗÷╨N╓w⌐┘u═┘▓╤r?¬»≈]K*òV03£V■W╤LÖ├U6ßC└'ⁿ⌡¼φ┼ù┘Φwîè}n╜─é╬╗╤]CUñ╜jq[h,ÇâC╨ï╕•äæ
⌐σ╫╨▄÷íÑ▄öô┘µVcb═m┼ⁿ∞⌡Xï╜lè9⌐8Xåⁿ W└·tα!T┬Öè┌Θ«╚N╬Él'HI╗kPh₧Φφ┘εz├H╓╟p;┬*é╪s╜ûnéâèxá
²▐5░UÖJ─y•:äo╫εY║30Xiëθπèg LS─Γ√W!e█╝în╘GpG/Ç₧°íô╪φb?U▄τáH╤√▌{1]"üd▄]¼âδεlb$U[ú╧mc▌
⌡í╥∞v«▀n┘8┴~╣⌡ò°&╓éog¿┌╜¢▄¬₧╧╞╟w°Θæ8bhÆ⌡╫E╫ôê╟▓G║Åⁿ╪·ißα┤╗4<╞6e°(c┌¶,└kµÇô║b{─┤;┐á'
├¶á¿åæφò$ä⌡ù₧P≈É√δLÉ╣!YEîTìmφ┐÷0nô¥²╗¼&/╗▐Ö}│╣∞╝╚ßët£i╧ó8╡÷[τ╧éXÑ│~èªE∞66┘åα}┐¬─½&₧
ⁿ,P┘■yVf╙ßJ╤≡╣Ñ=ÿv╜╗≡╠═âî}δT?αc╧ZRUW₧╗⌐δû0<nS2(&bφiº▐±Dï─KáW╕╨ÿ┘_╬7êuié─î~A{º÷é╙)≡j
G║ri■Å≤3=┐≈å¶╕║•┘l⌐kmÑ│░╕└D)╤▐¿╟(¶î╡£╟¬┘╛/q0ê≡u▄φ¥▓τ╗ErñΩ?φ±εW╫⌐dP6╧¼Φ[j"HS∞╘J╧É÷Kñ

Σ▄¥D╗ò¶╟  %%Hε.─╫ΩY h? ╫Z╧ ¿witc fè#F╙bè⌐¿( ╡ê }╨çöΓeÆÖ╗ñY┐4q÷â█q=5  w¬ï┤₧R╤⌐

╢ p ┬(⌠┴A lÖº ╨ε, d[ i│I²g
```

DATANET PROC RECORD: 2SNKY4U Transnet on/xc-3

```
 .d8888b.  888b    888 8888888888        d8888 888    d8P Y88b   d88P
d88P  Y88b 8888b   888 888              d88888 888   d8P   Y88b d88P
Y88b.      88888b  888 888             d88P888 888  d8P     Y88o88P
 "Y888b.   888Y88b 888 8888888        d88P 888 888d88K       Y888P
    "Y88b. 888 Y88b888 888           d88P  888 8888888b       888
      "888 888  Y88888 888          d88P   888 888  Y88b      888
Y88b  d88P 888   Y8888 888         d8888888888 888   Y88b     888
 "Y8888P"  888    Y888 8888888888 d88P     888 888    Y88b    888

.d8888b. 8888888 8888888b.  .d8888b.  888     888 8888888 8888888888 .d8888b.
d88P  Y88b  888   888   Y88b d88P  Y88b 888     888   888       888   d88P  Y88b
888    888  888   888    888 888    888 888     888   888       888   Y88b.
888         888   888   d88P 888        888     888   888       888    "Y888b.
888         888   8888888P"  888        888     888   888       888       "Y88b.
888    888  888   888 T88b   888    888 888     888   888       888         "888
Y88b  d88P  888   888  T88b  Y88b  d88P Y88b. .d88P   888       888   Y88b  d88P
 "Y8888P" 8888888 888   T88b  "Y8888P"   "Y88888P"  8888888     888    "Y8888P"
```

******** Presented by Joe Grand (@joegrand // grandideastudio.com) ********

[ ] Press Any Key to Begin

Sneaky Circuits

- Not all devices follow the rules
  - Operate in ways unintended by the original designer
  - Provide unexpected/alternate behavior
- Explore fun, annoying, malicious, and/or useful projects

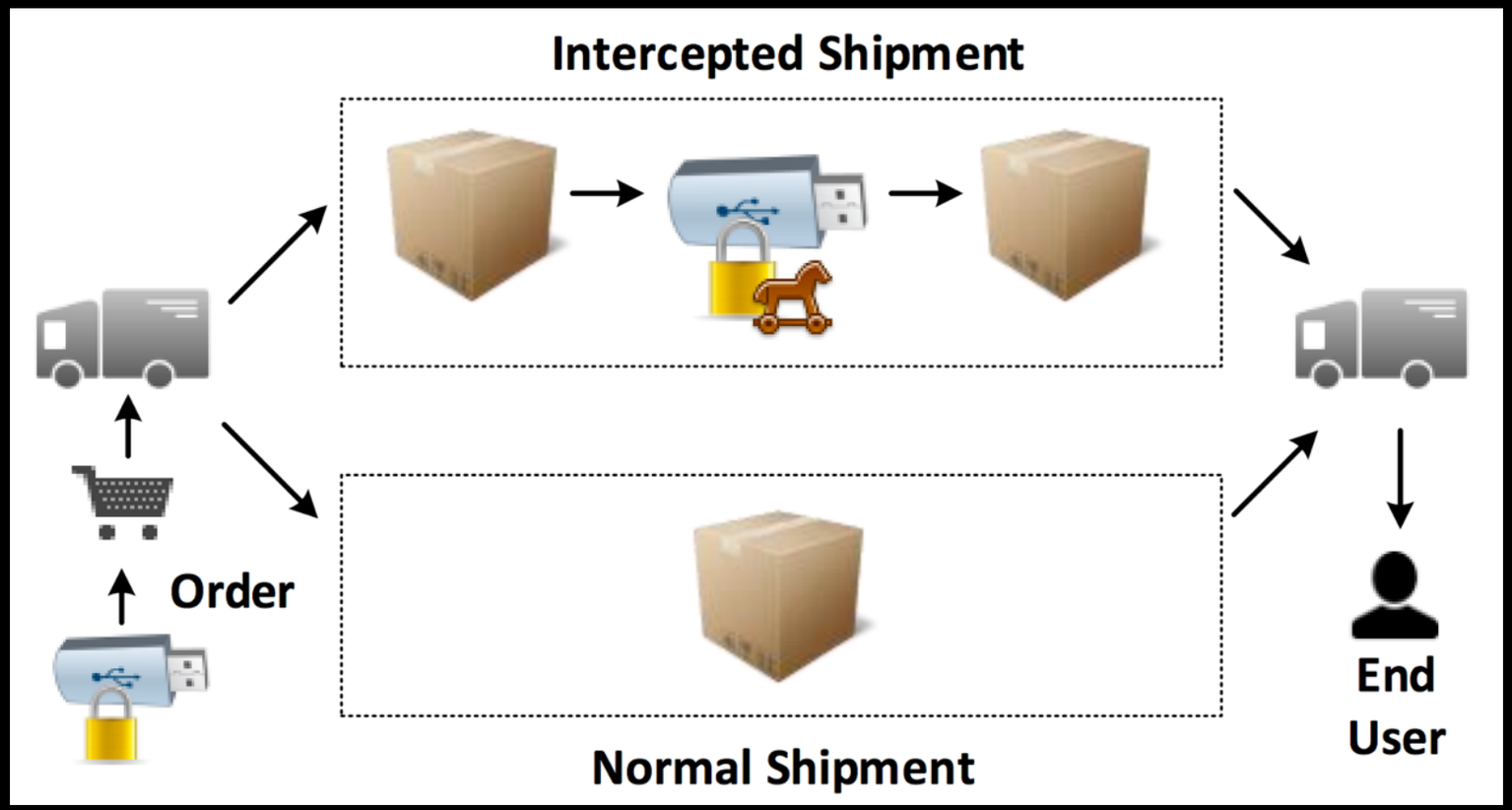
Sneaky Circuits

- Hardware injection
- Audio generation
- Video signal interception
- Covert data exfiltration
- An IC that functions in either orientation

Hardware Injection

Hardware Injection

- Adding custom and/or malicious circuitry in tandem w/ normal functioning system
- Use HW access to give SW control
  - Ex.: Privilege escalation, patch memory, insert backdoor, exfiltrate data

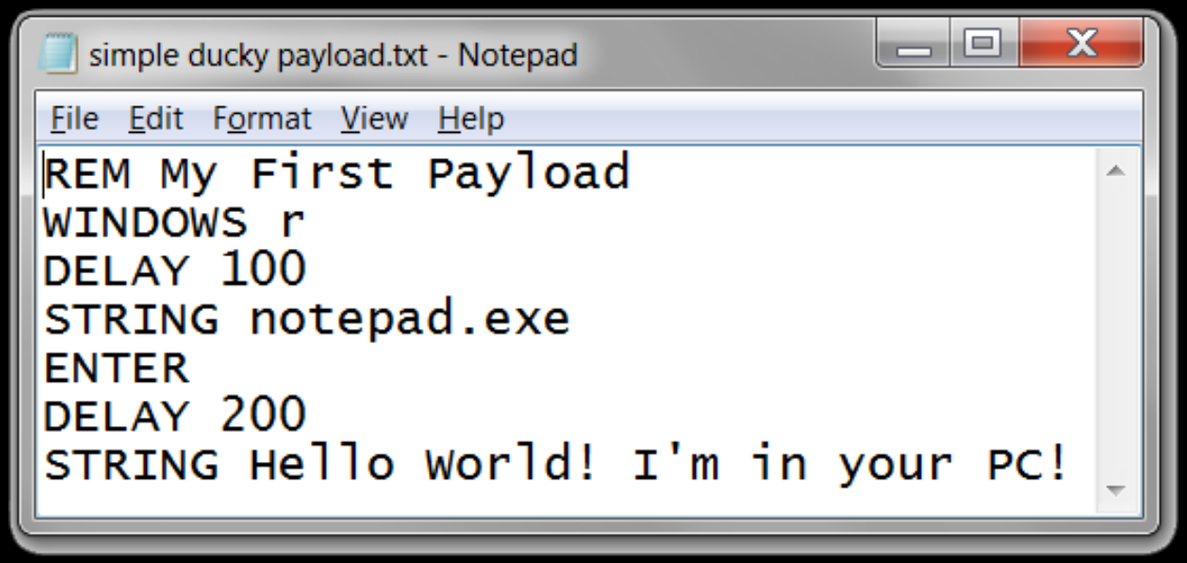


Hardware Injection

- Achieved at any layer of the product
  - Component, silicon/chip, PCB
- Added at any part of the lifecycle
  - Design, fabrication, distribution, integration, in-the-field

USB Rubber Ducky

- Hak5, 2010
- Human Interface Device (HID) keyboard emulation
- Injection/spoofing/scripting
- Payload storage on internal microSD card
- https://hakshop.com/products/usb-rubber-ducky-deluxe

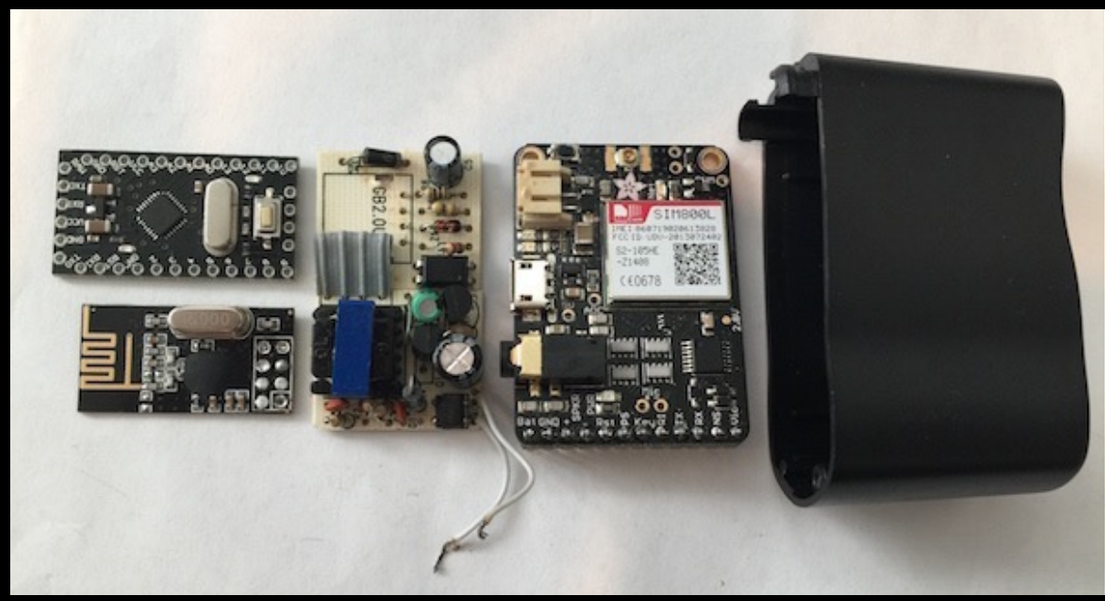


Mr. Self Destruct

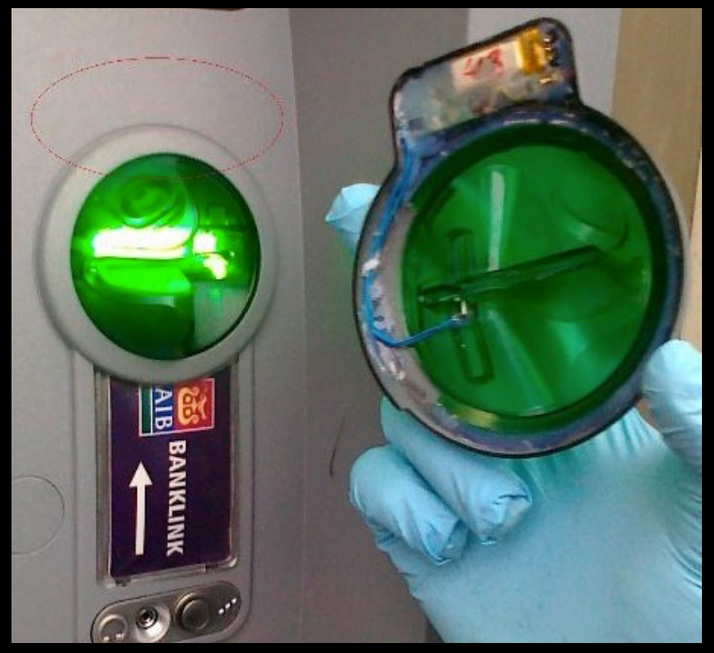
- _MG_, 2017
- USB keystroke injector with software-triggered 5V payloads
- https://mg.lol/blog/mr-self-destruct/

KeySweeper

- Samy Kamkar, 2015
- Arduino-based implant camouflaged as USB wall charger
- Sniffs/decrypts/logs/reports/[injects] keystrokes from certain Microsoft wireless keyboards
- Exploits weakness in proprietary 2.4GHz transmission
- http://samy.pl/keysweeper/



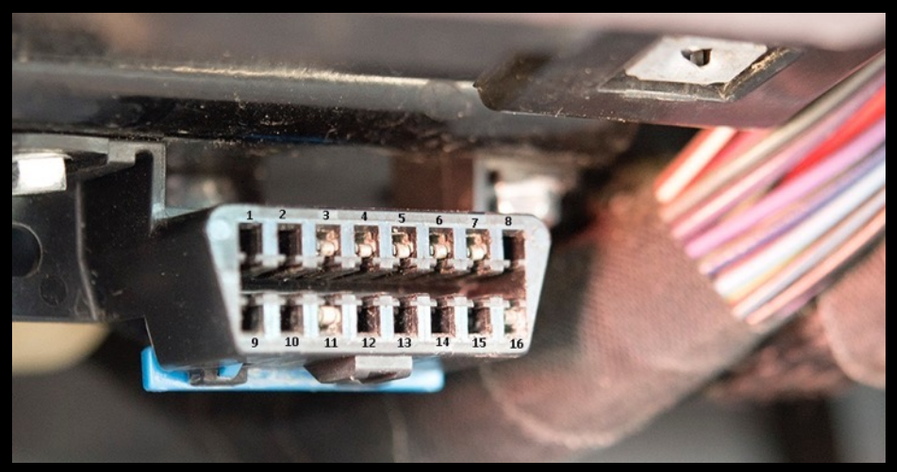
Credit Card Skimmers



http://krebsonsecurity.com/tag/atm-skimmer/

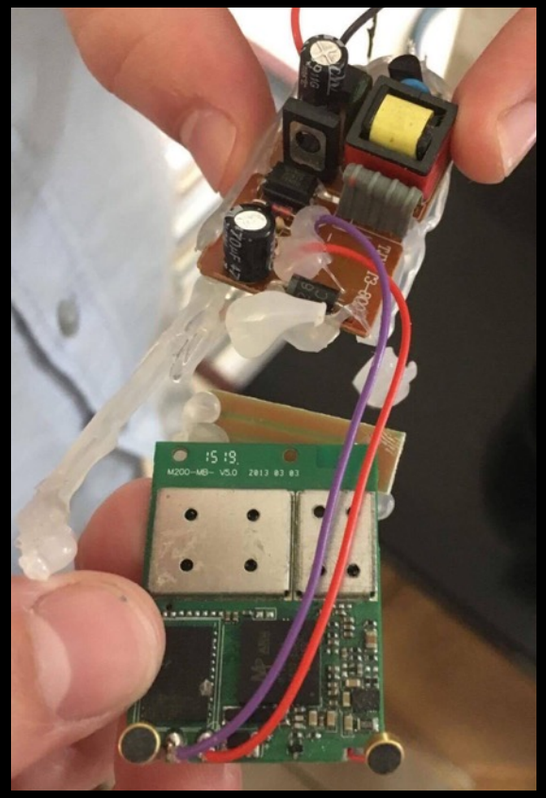
Automotive OBD

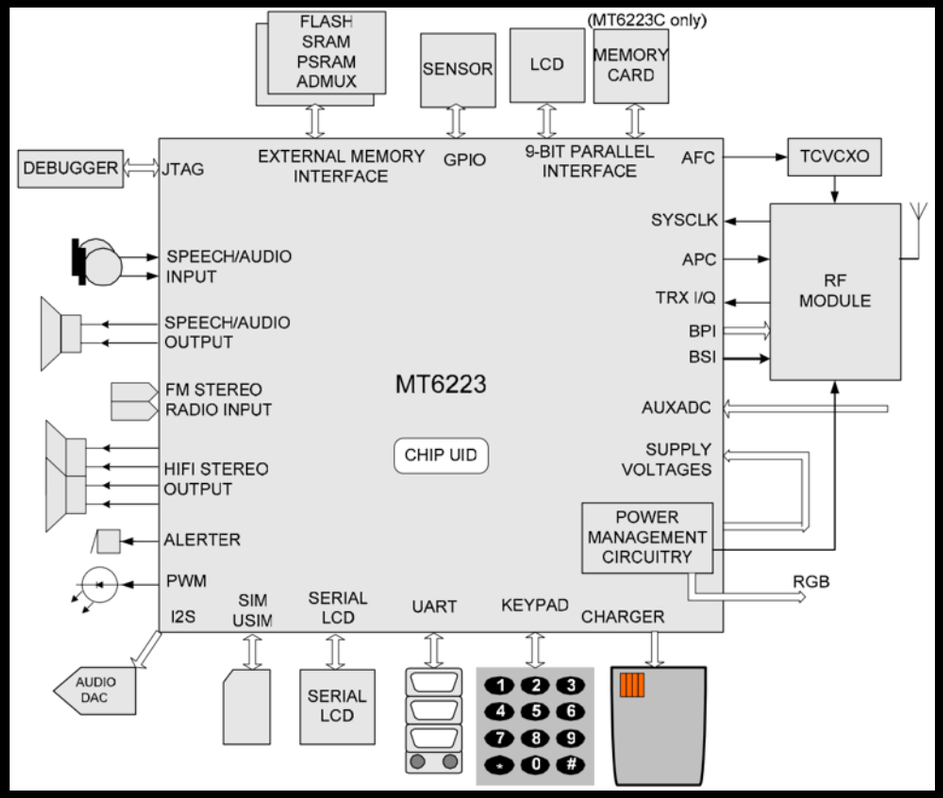
- OBD (On-Board Diagnostic System)
- Available in all cars > January 1, 1996
- Designed to monitor engine and emissions performance
- Provides direct access to ECU communication bus(es)
- Passive monitoring, data injection/manipulation
- www.carhackingvillage.com
- http://illmatics.com/carhacking.html



GSM Audio Surveillance Bugs

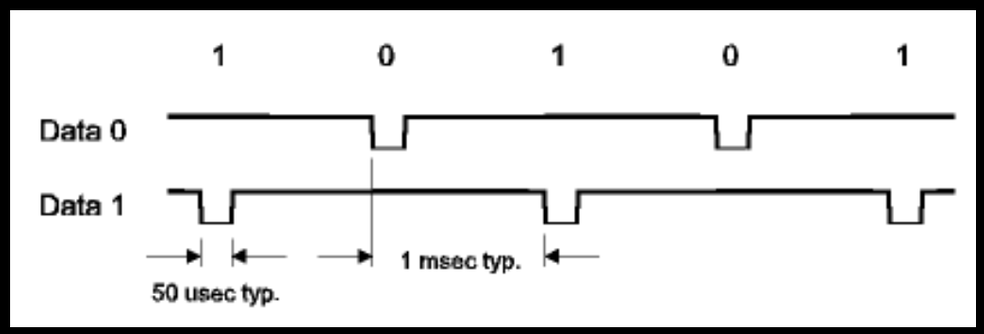
- Detected at a B&B in Wales, UK, buzzing noise coming from the socket, 2017
  - www.reddit.com/r/whatisthisthing/comments/6ktlqn/listening_device_found_behind_power_socket_at/
  - Many units available on eBay/Amazon already built into wall wart, mains plug, mouse, power strip, cables, etc.

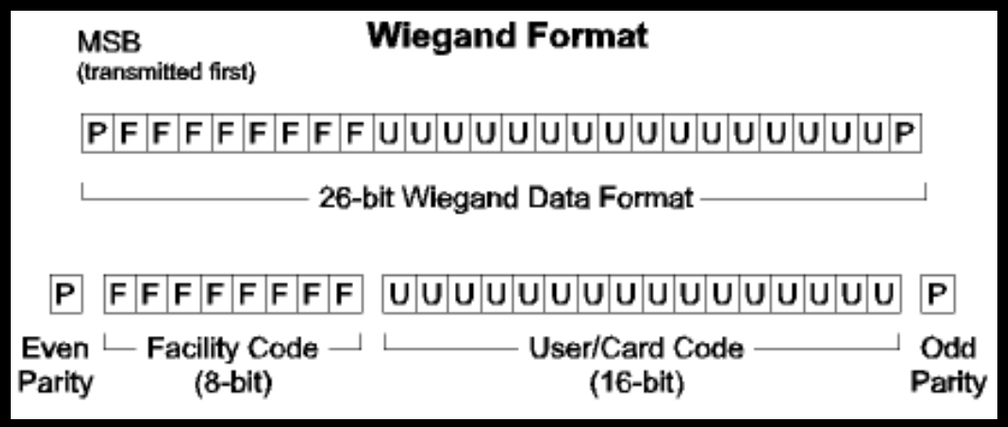




BLEKey

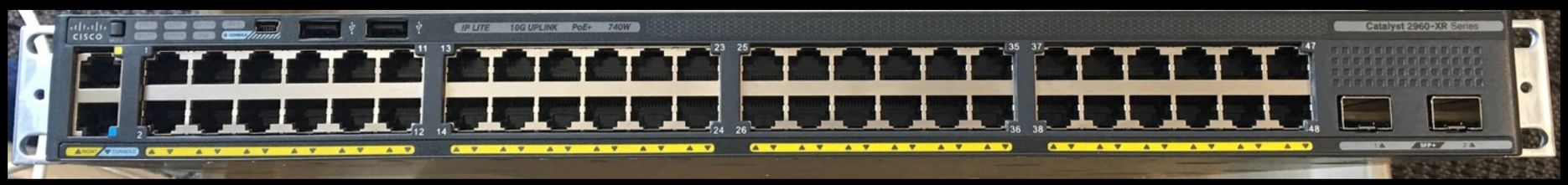
- Eric Evenchick, Mark Baseggio, BH USA 2015
- HW implant into access control systems
- Read/clone/replay Wiegand data
- http://github.com/LinkLayer/BLEKey
- Also, see ESPKey from Kenny McElroy, ShmooCon 2017



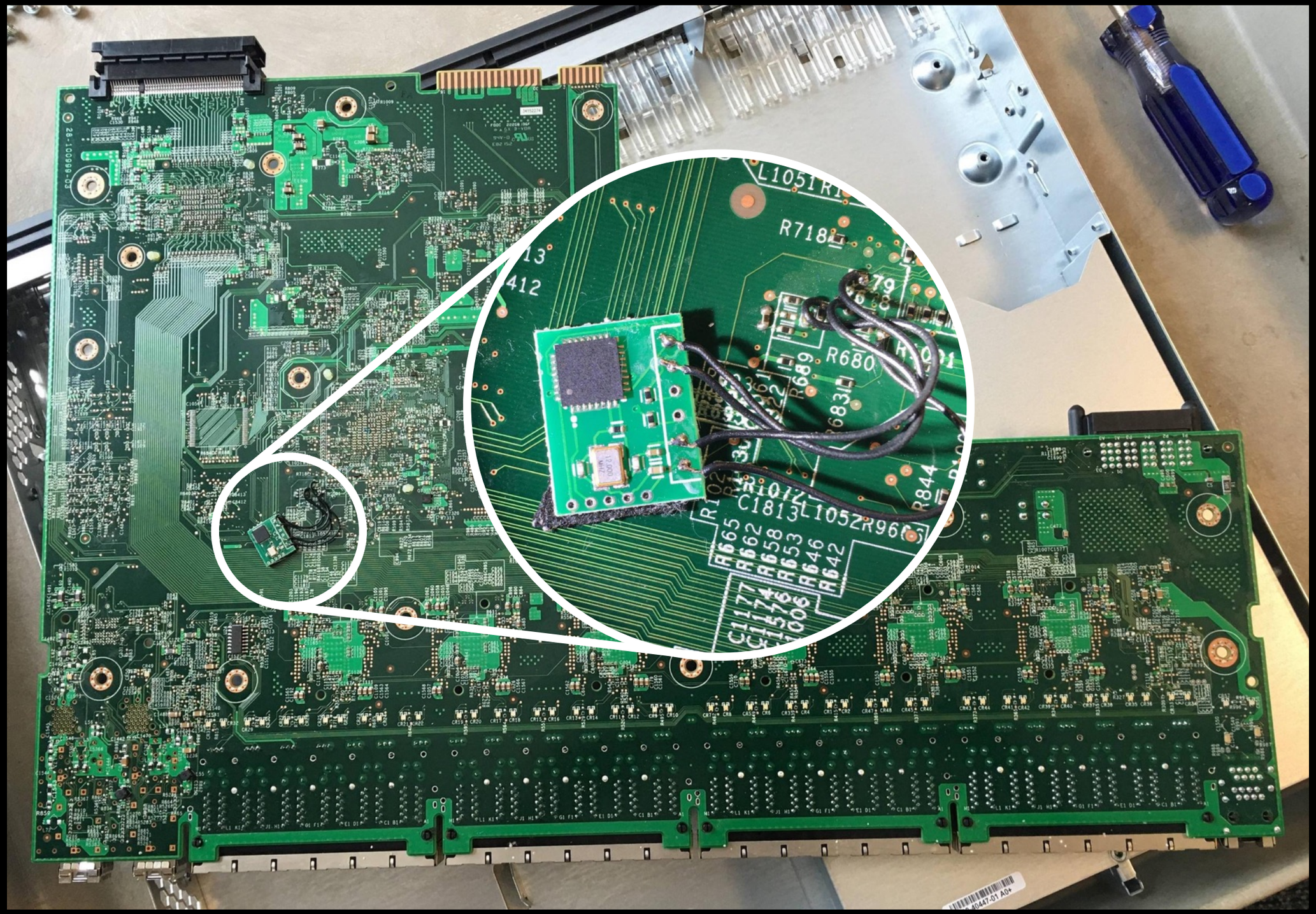


Cisco Catalyst 2960XR Switch

- Purchased on eBay
- Noticed slight physical exterior differences
- Identified small daughterboard on back of PCB
- Possible counterfeit, post-production fix, or malicious implant?
  - Authentication/serial # bypass, reflash BIOS on power-up, software persistence ala FLUXBABBITT
- www.reddit.com/r/networking/comments/4iwa5f/possible_counterfeit_cisco_equipment_wphotos/

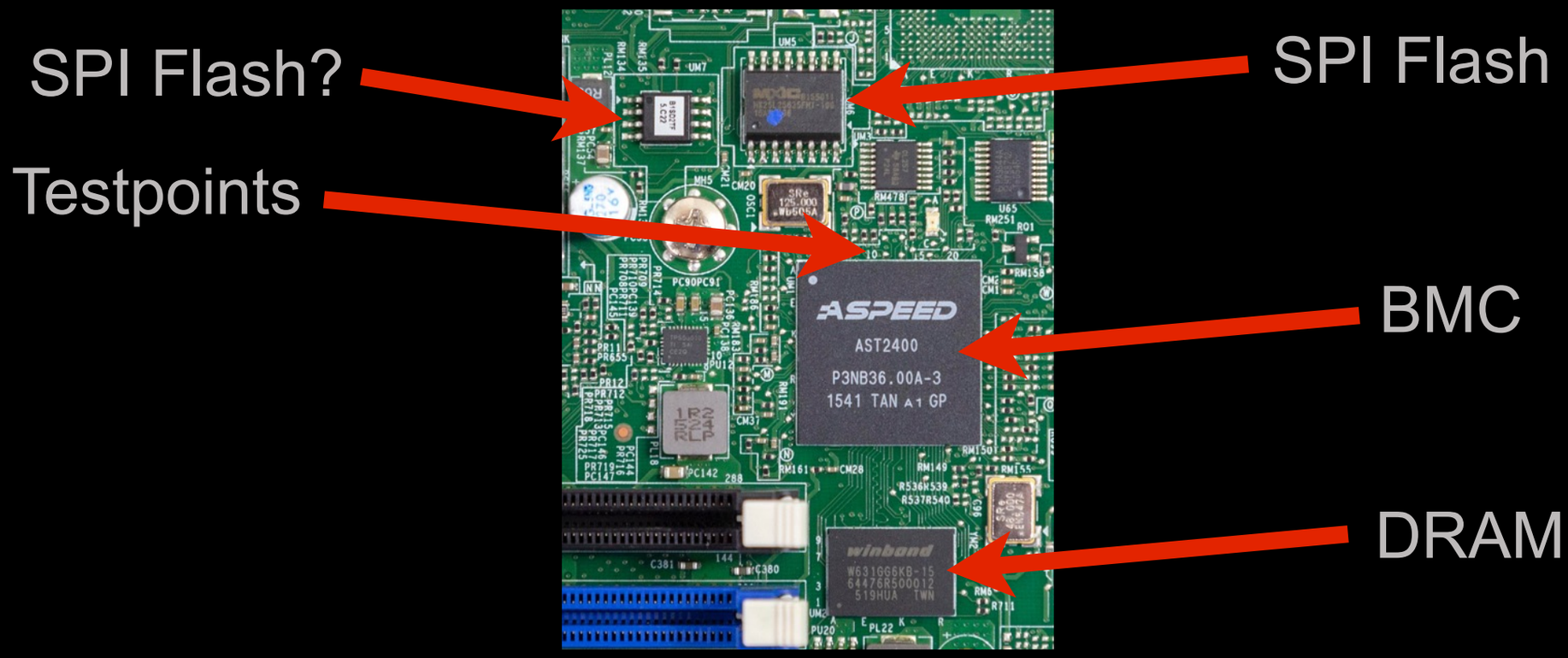


Cisco Catalyst 2960XR Switch



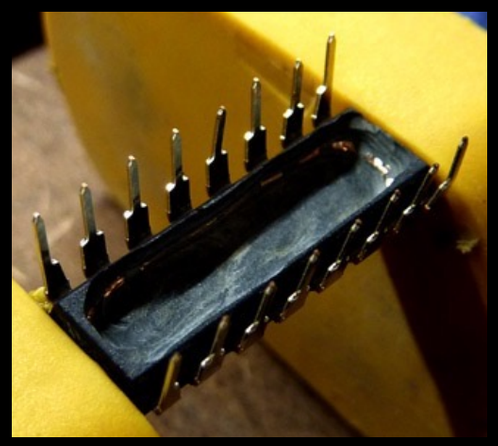
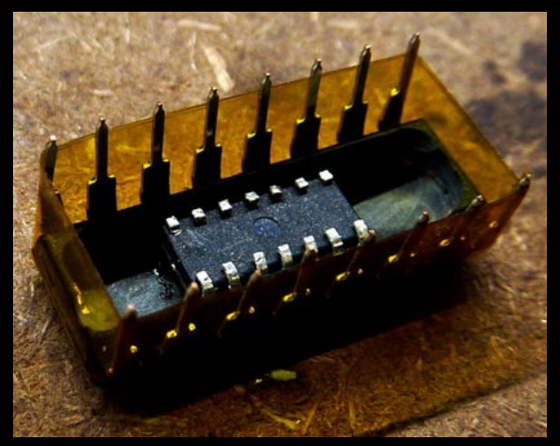
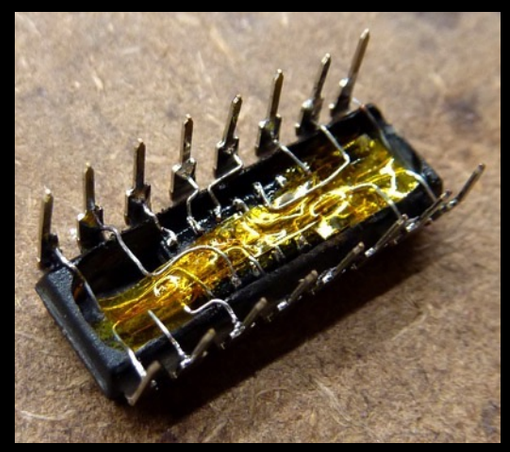
Supermicro (Unconfirmed)

- The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies, Bloomberg 2018
- Man-in-the-middle between external memory and BMC (Baseboard Management Controller)
- Hardware added into actual design at subcontracted manufacturing facilities via bribes/threats



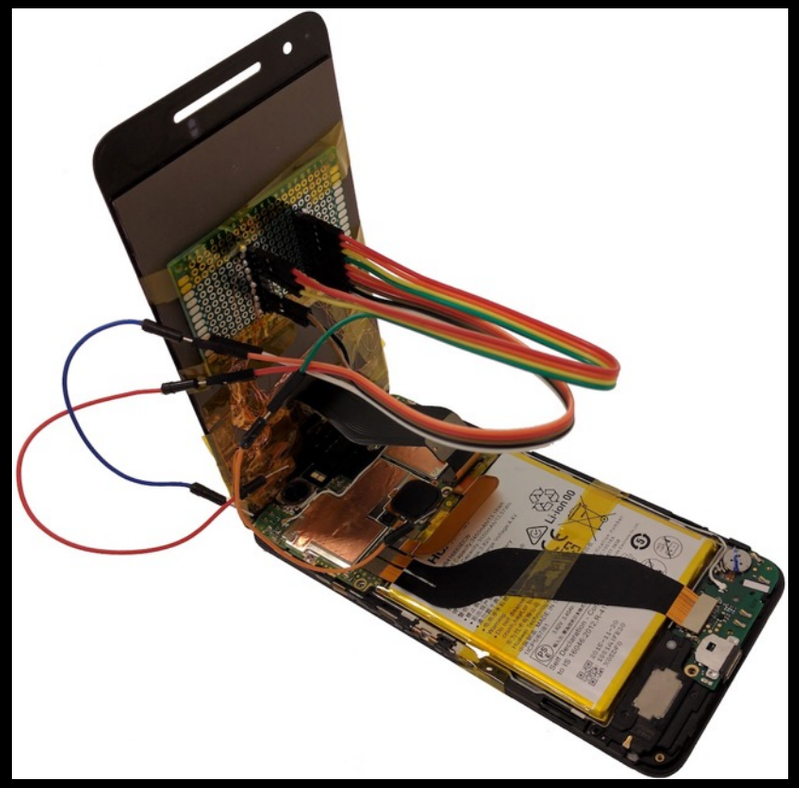
Microcontrollers Not Allowed

- Benign example of component-level injection
- MCU inserted into a modified off-the-shelf logic IC
- Simulates original device, occasionally displays preset messages
- http://ultrakeet.com.au/write-ups/microcontrollers-not-allowed

Third Party/Aftermarket Repairs

- Shattered Trust: When Replacement Smartphone Components Attack
  - Shwartz, Cohen, Shabtai, Oren, USENIX WOOT '17
- Chip-in-the-middle implant between touchscreen & CPU
- Capture/emulate touchscreen actions via I2C bus
- Disable touchscreen while malicious activity is happening
- Ex.: Malicious software installation, taking a picture & sending via e-mail, logging/exfiltration of screen unlock pattern



Audio Generation

Audio Generation

- Built March 1989 (13 years old)
- High-frequency single tone generator
- Simple mischievous device annoys anyone within range

Audio Generation: Inspiration

-[]-

Variable-pitched frequency generator
or
How to annoy your techers!

Written By

::: Captain Quieg :::

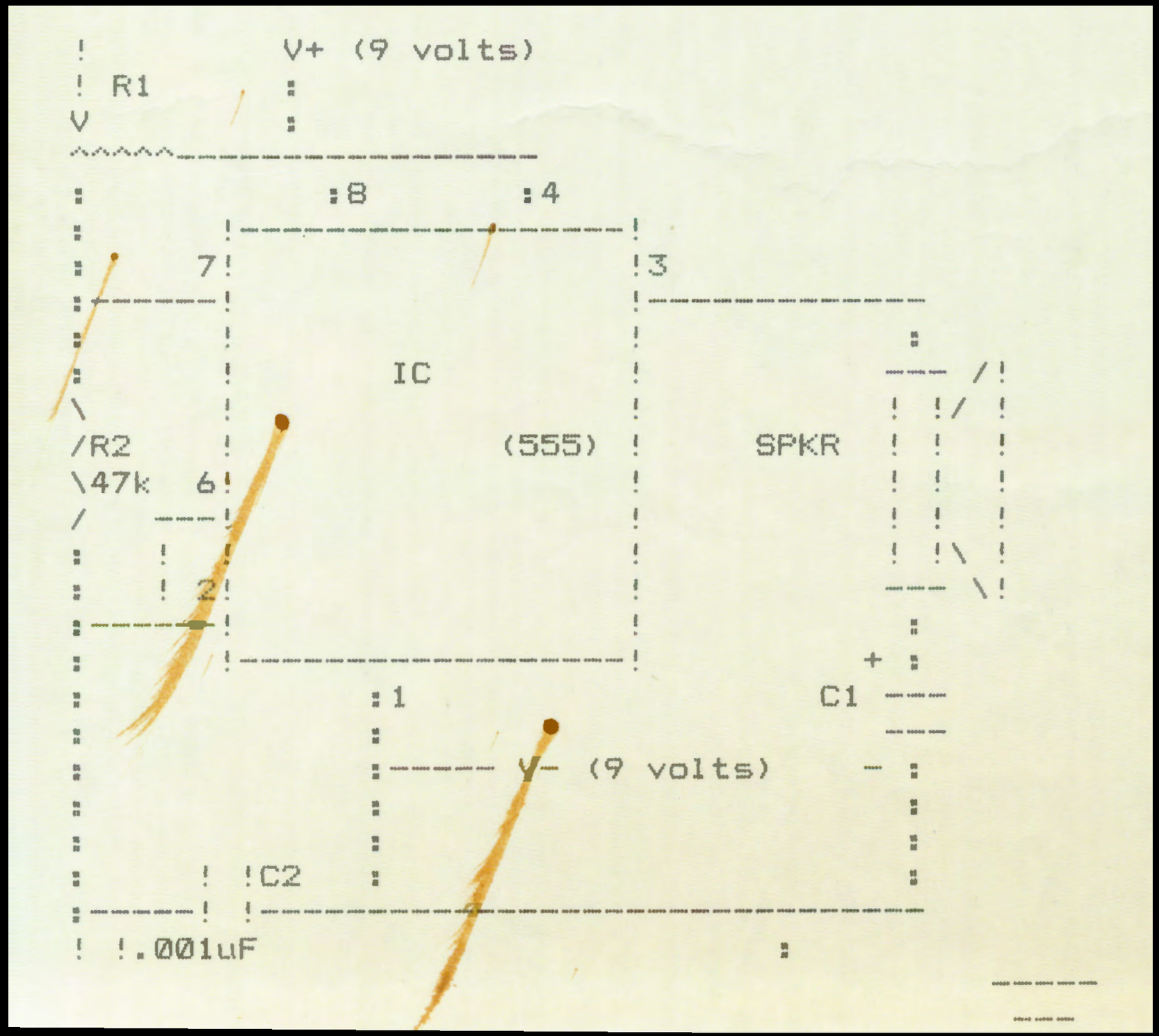
-[]-

In the fast paced world of education one often finds oneself with a burning hatred towards one or more teachers or fellow students. This article will describe how to build a little device that will emit a very high freqency that is -extrememly- annoying to most people and it will wreck concentration and can cause some nasty headaches.

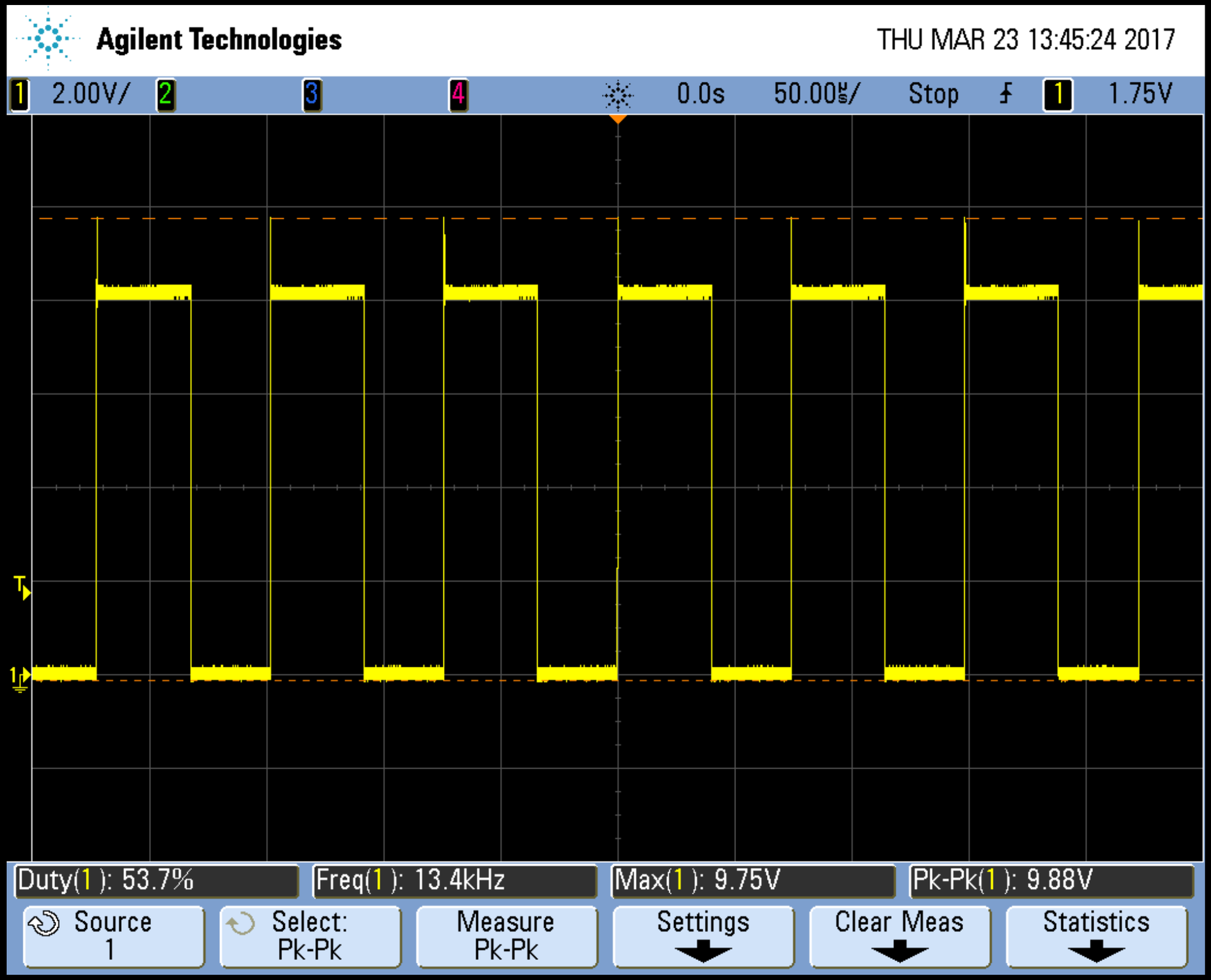
-[]-

www.textfiles.com/anarchy/MISCHIEF/noise.ana

Audio Generation: Schematic



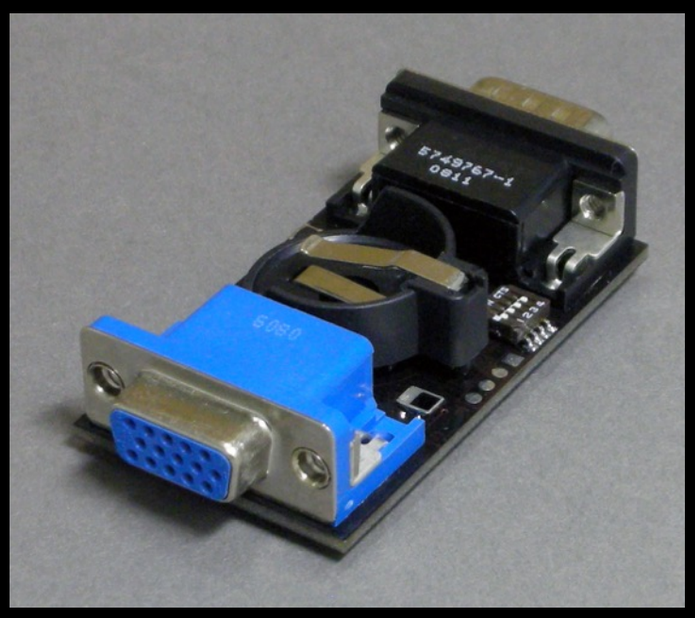
Audio Generation: Output

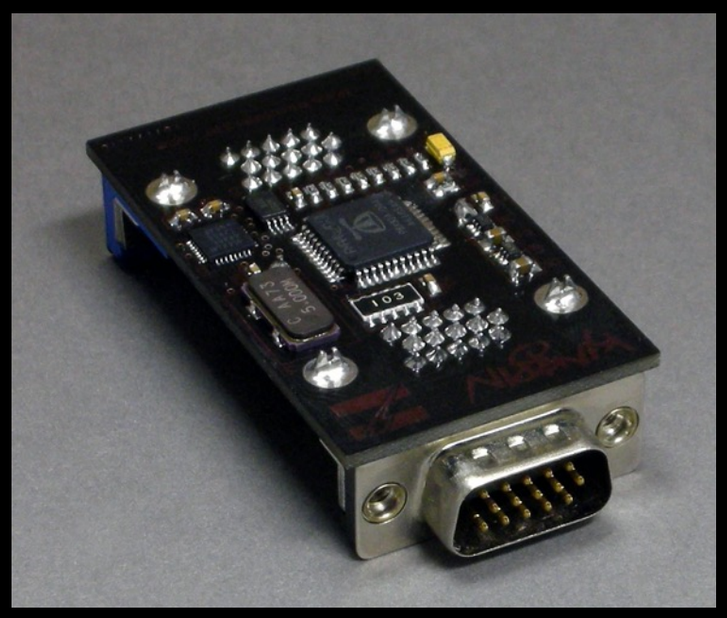


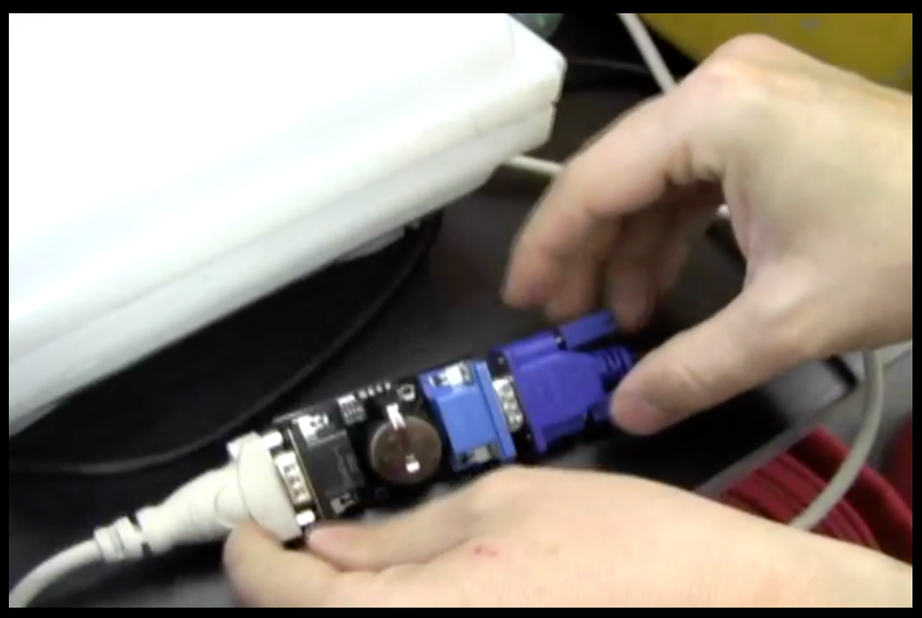
Video Signal Interception

BSODomizer

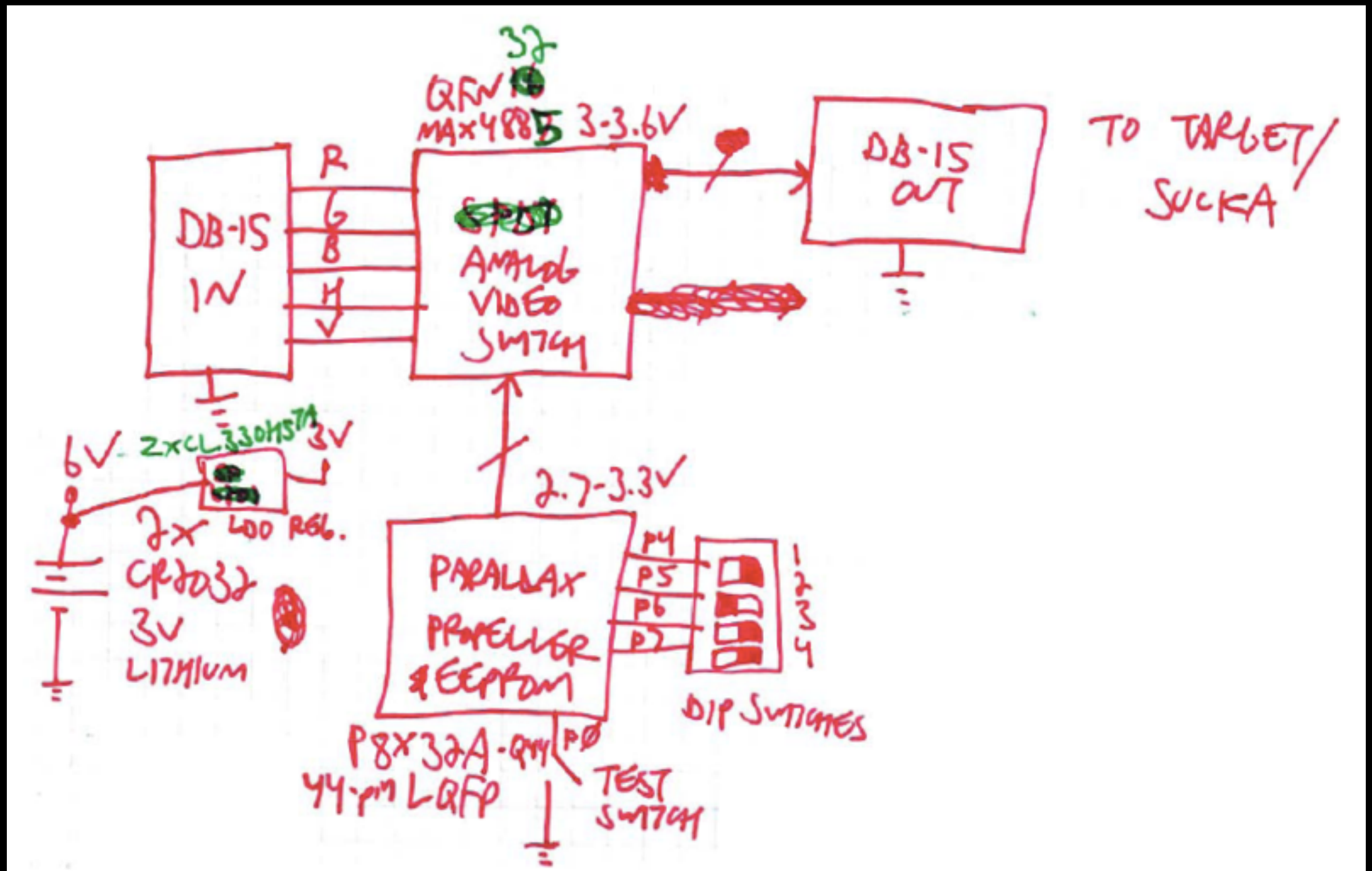
- Released at DEFCON 16 (2008)
- Video pass-through w/ interception/injection
- XGA (1024 x 768) w/ text only
- Parallax Propeller, reprogrammable w/ PropClip
- www.grandideastudio.com/portfolio/bsodomizer







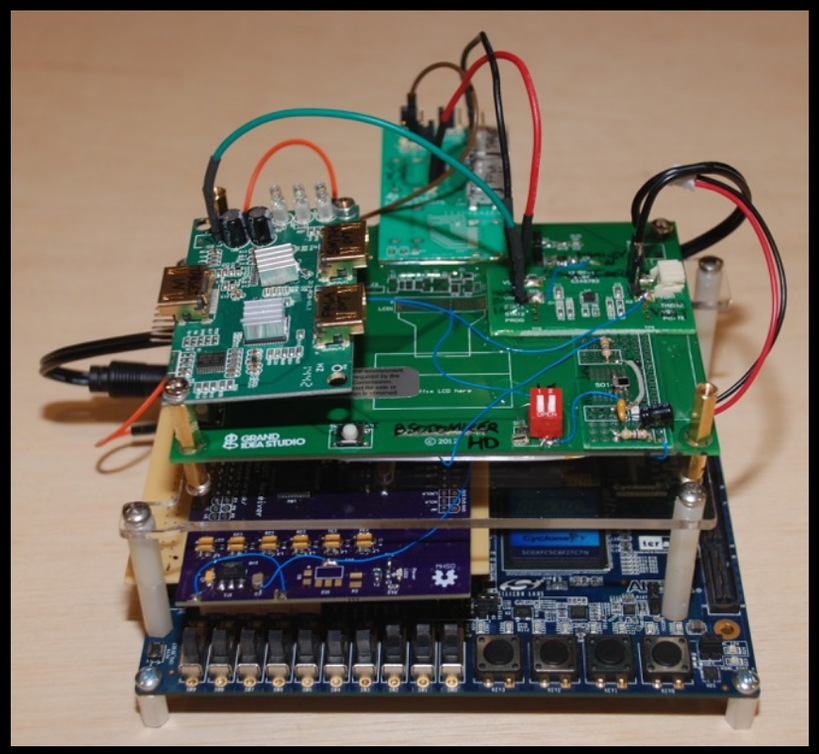
BSODomizer: Block Diagram



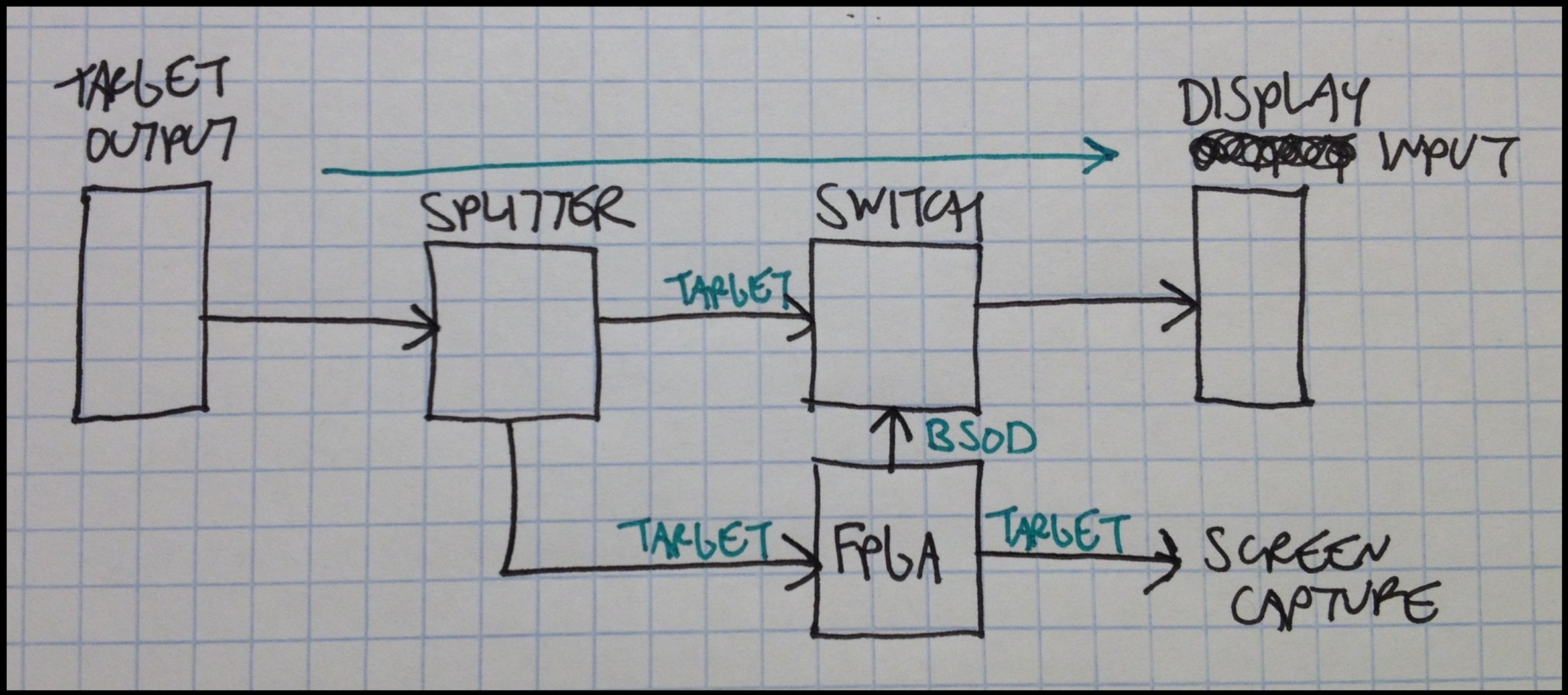
BSODomizer: Action Shot

BSODomizer HD

- Released at DEFCON 24 (2016)
- Video pass-through w/ interception/injection @ 1080p
- Internally generated display modes, user-loadable images from microSD card, frame capture
- Open source FPGA reference design (Cyclone 5CGXFC5C6F27C7N)



BSODomizer HD: Signal Path



Covert Data Exfiltration

Covert Data Exfiltration

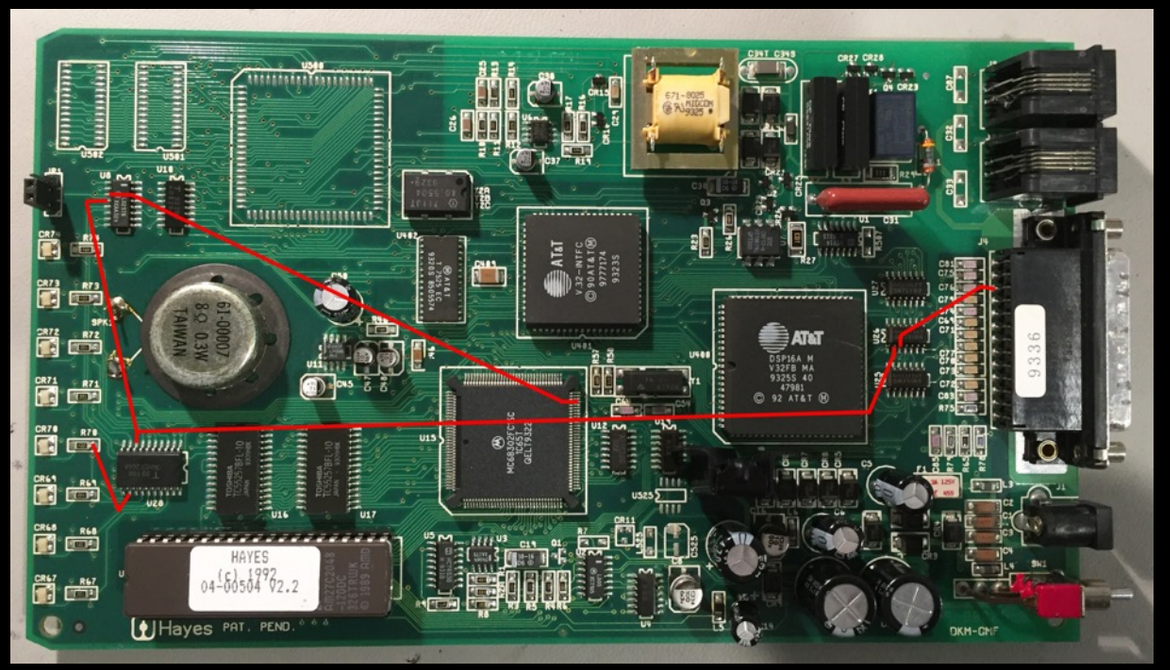
- Hidden methods to intentionally exfiltrate/transfer data from a normally functioning system
  - Typically non-conventional, out-of-band methods
- Requires collusion between transmitter & receiver
  - Software pre-loaded onto target
  - Hardware modification of target not usually needed
  - Knowledge of compromised target & expected results
- Leakage based on electromagnetic/RF, electric, magnetic, acoustic, thermal, or optical

Optical Covert Channel

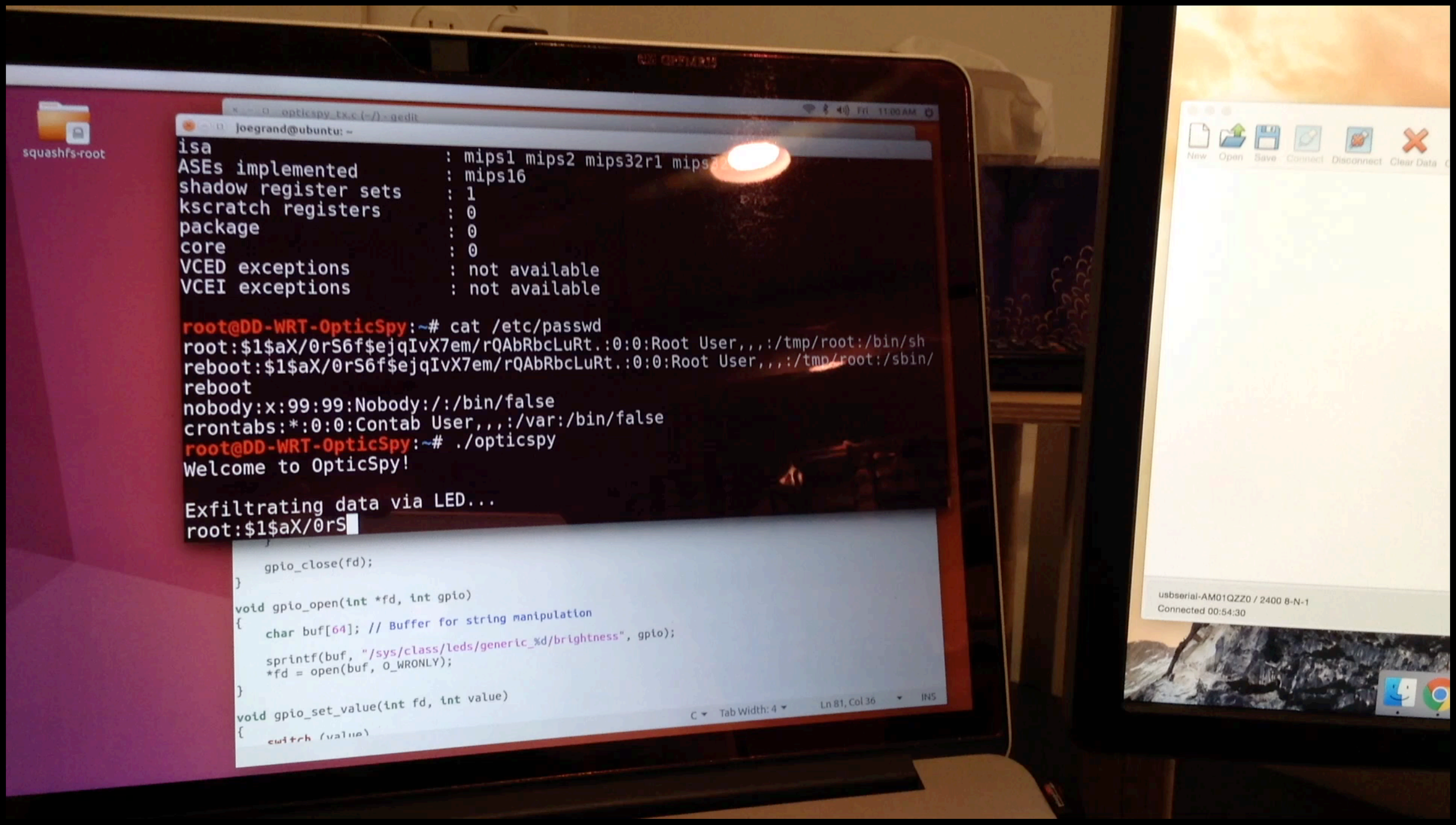
- Using LEDs to exfiltrate/send data
  - Mis-design leading to unintentional leakage
  - Modification of HW/FW to redirect data output to LED
  - Modulation faster than the human eye can detect
- Requires optical receiver to convert light into voltage
  - www.grandideastudio.com/portfolio/opticspy

Hayes Smartmodem Optima

- Indicator LEDs tied to serial port data lines
  - Data leakage through SD (Send Data) and RD (Receive Data) LEDs
- Information Leakage from Optical Emanations (Loughry and Umphress, 2002)
- www.applied-math.org/optical_tempest.pdf



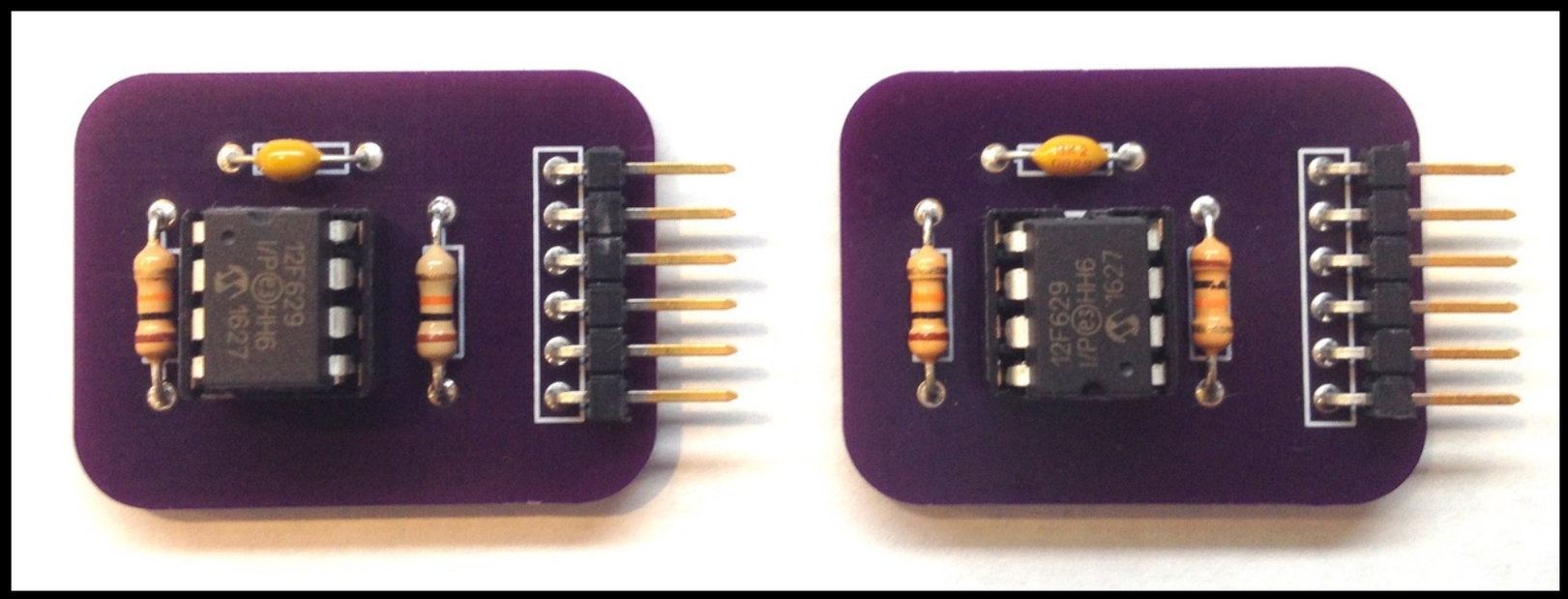
TP-Link TL-WR841N



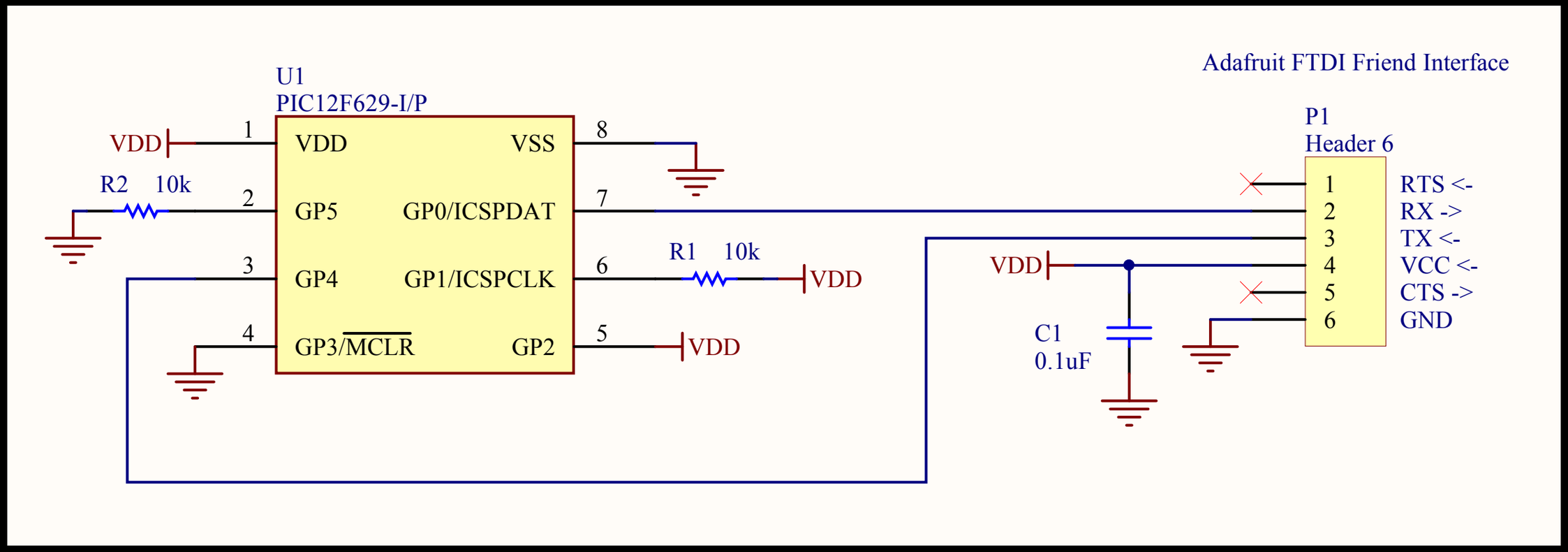
DIP Flip Whixr Trick

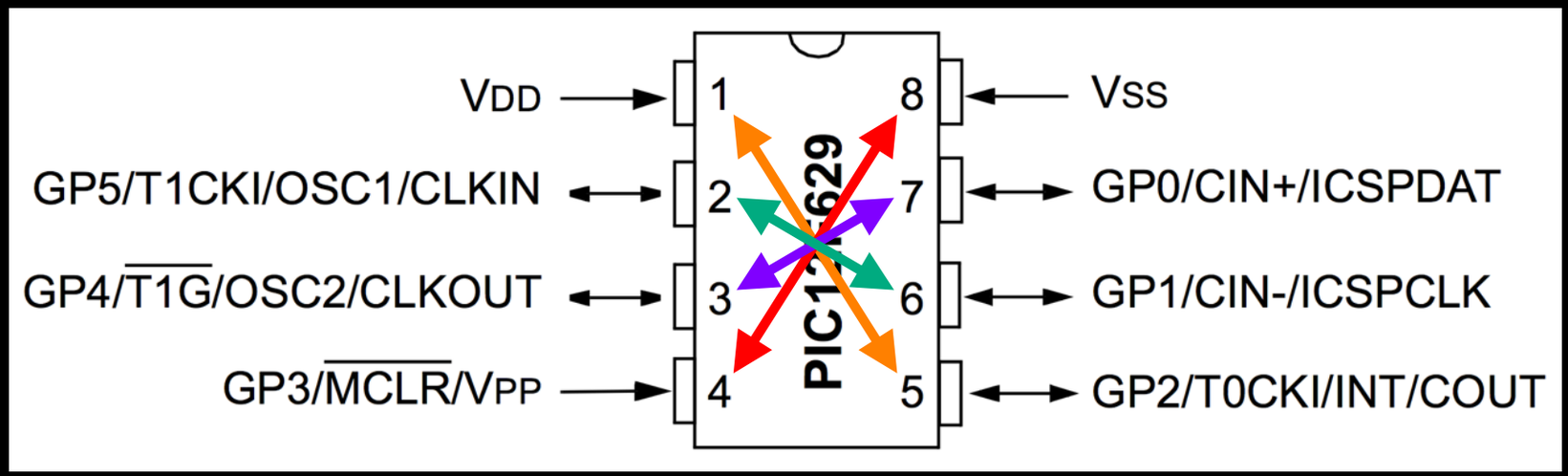
DIP Flip Whixr Trick

- Sneaky circuit that defies common convention
- MCU can operate in either orientation
  - Normal v. alternate functionality
- Example of intentional corruption during chip fabrication/assembly/manufacturing process
- www.grandideastudio.com/portfolio/sneaky-circuits

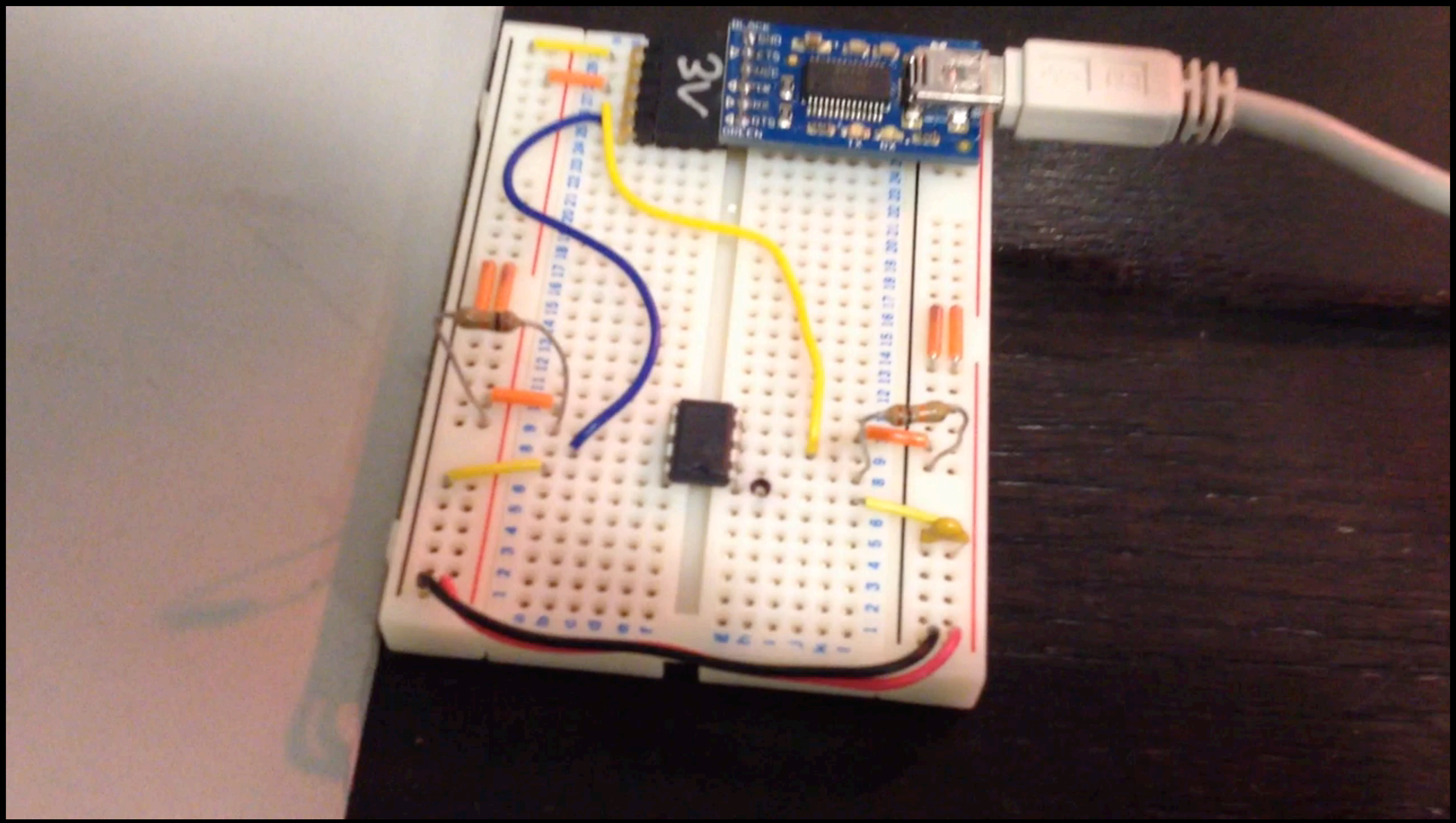


DIP Flip Whixr Trick: Schematic





DIP Flip Whixr Trick: Action Shot



Setec Astronomy

- HW should not be inherently trusted
  - Defined functionality is not guaranteed
  - Lots of trickery, lots of ways to go undetected
- Electronic circuits are a new canvas for many
  - Don't delay! Create your own sneaky circuit today!