Tools of the Hardware Hacking Trade

Black Hat Webcast, April 23, 2014

Joe Grand (@joegrand)

GRAND IDEA STUDIO

Finding the Right Tools for the Job

- Tools can help for design or "undesign"
- Access to tools is no longer a hurdle
- Can outsource to those with capabilities/equipment you don't have
- The key is knowing what tools are available and which one(s) are needed for a particular goal/attack

GRAND IDEA STUDIO

Tools of the Hardware Hacking Trade

- Signal Monitoring/Analysis
- Manipulation/Injection
- Imaging

GRAND IDEA STUDIO

Signal Monitoring / Analysis

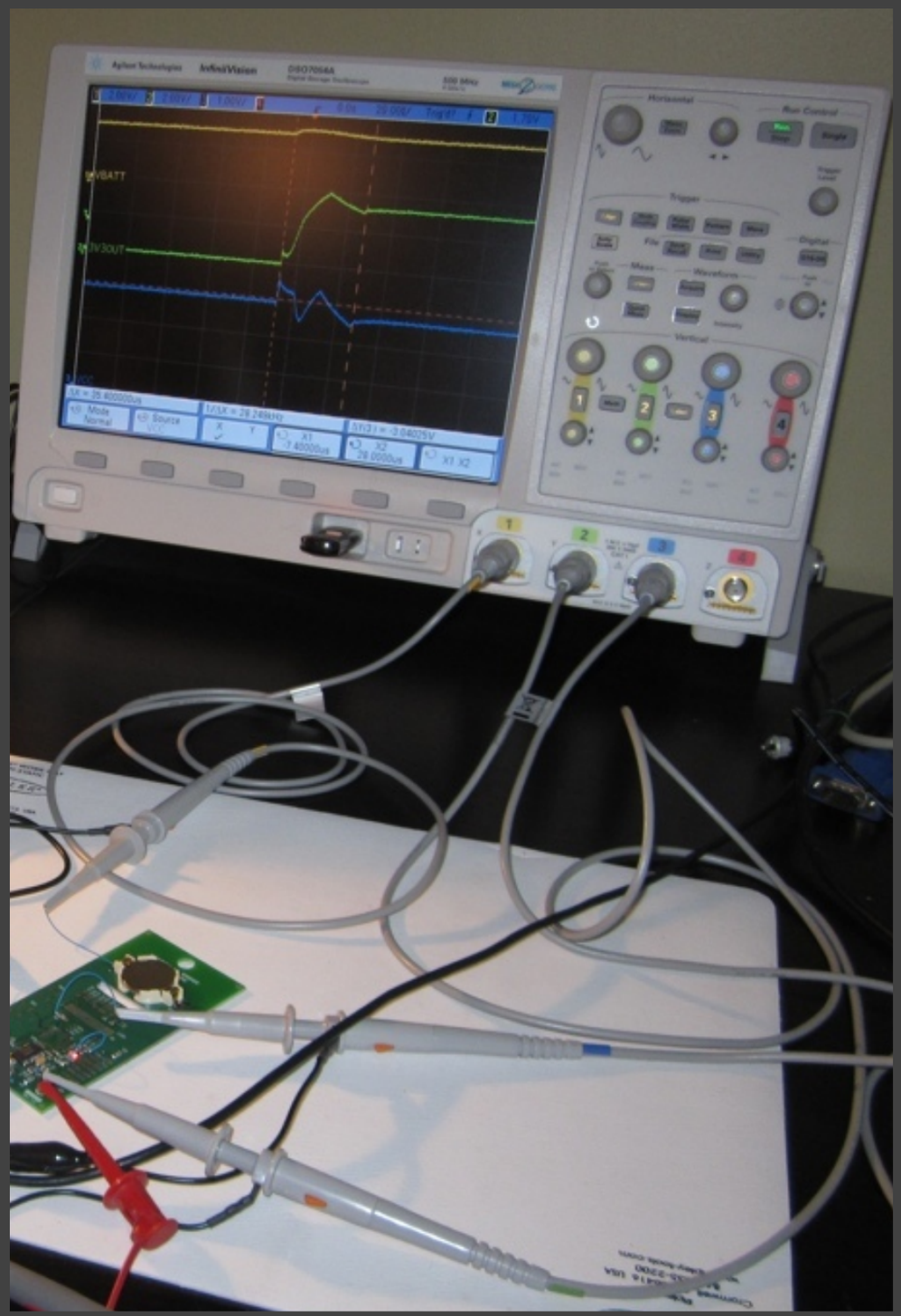
GRAND IDEA STUDIO

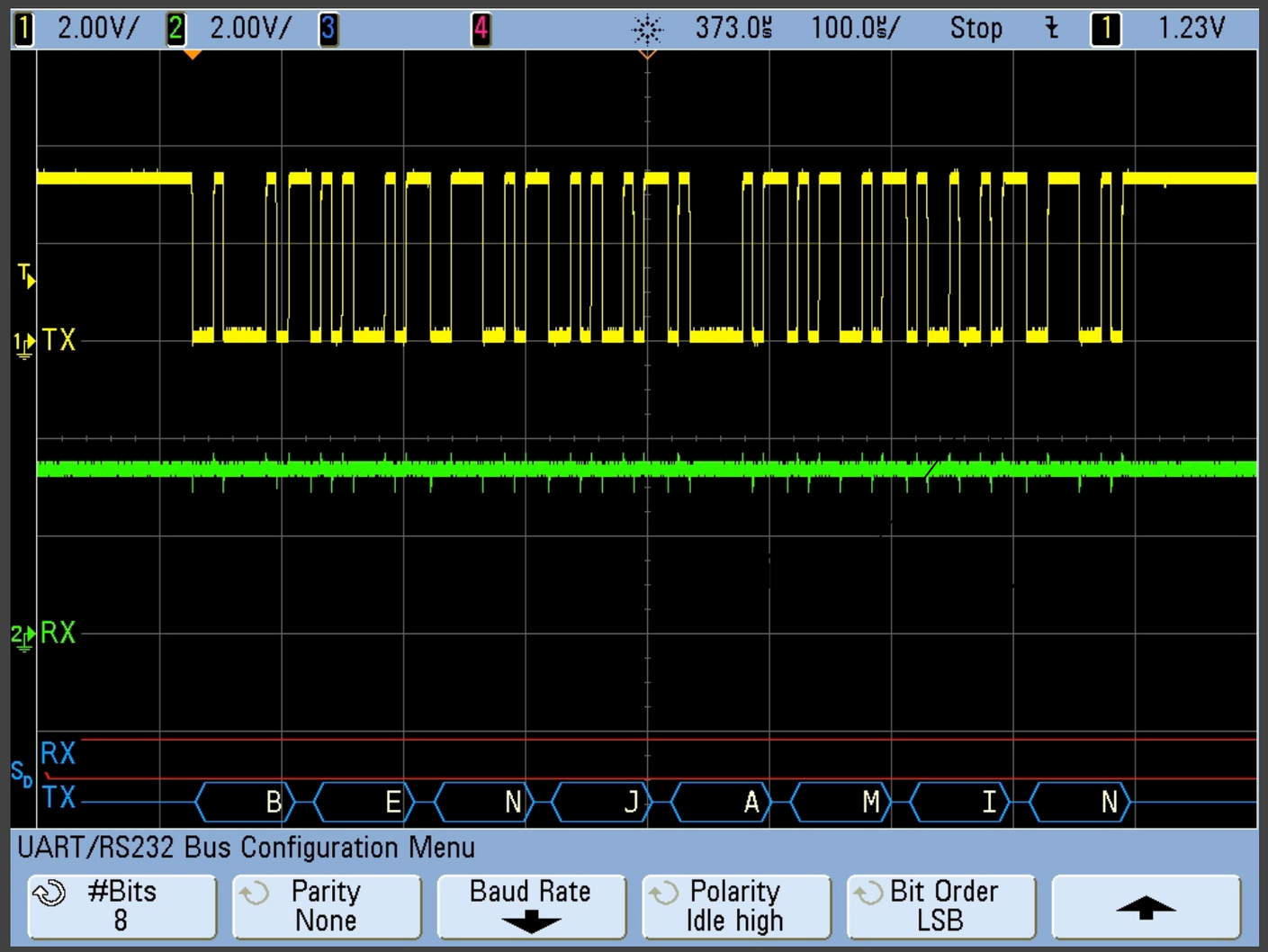
Oscilloscope

- Provides a visual display of electrical signals and how they change over time
- Introductory guides: `www.tek.com/learning/oscilloscope-tutorial`
- Range of hobbyist (low end) and professional (high end) tools
  - Analog/digital/mixed signal, # of channels (~1-4), bandwidth, sampling rate, resolution, buffer memory, trigger capabilities, math functions, protocol decoding, probe types, accessories
- Standalone: HP/Agilent, Tektronix, Rohde & Schwarz, LeCroy, Rigol
- PC-based: PropScope, USBee, PicoScope

GRAND IDEA STUDIO

Oscilloscope 2





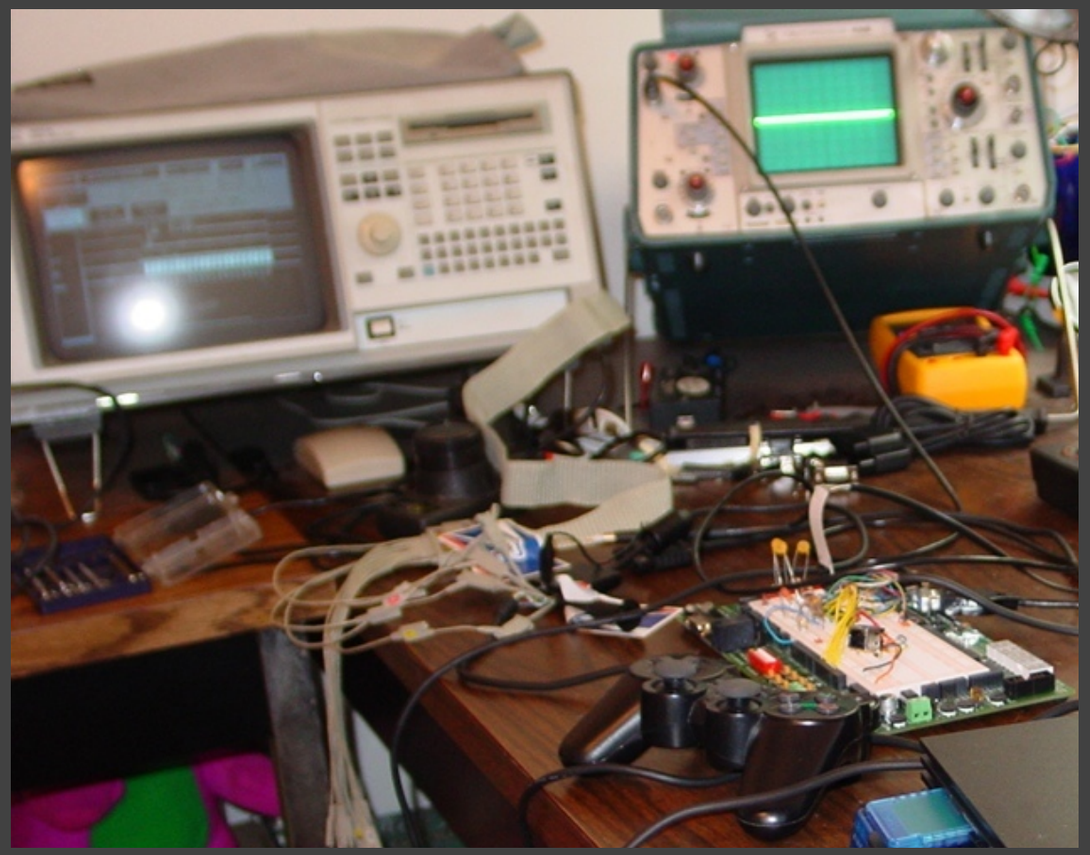
GRAND IDEA STUDIO

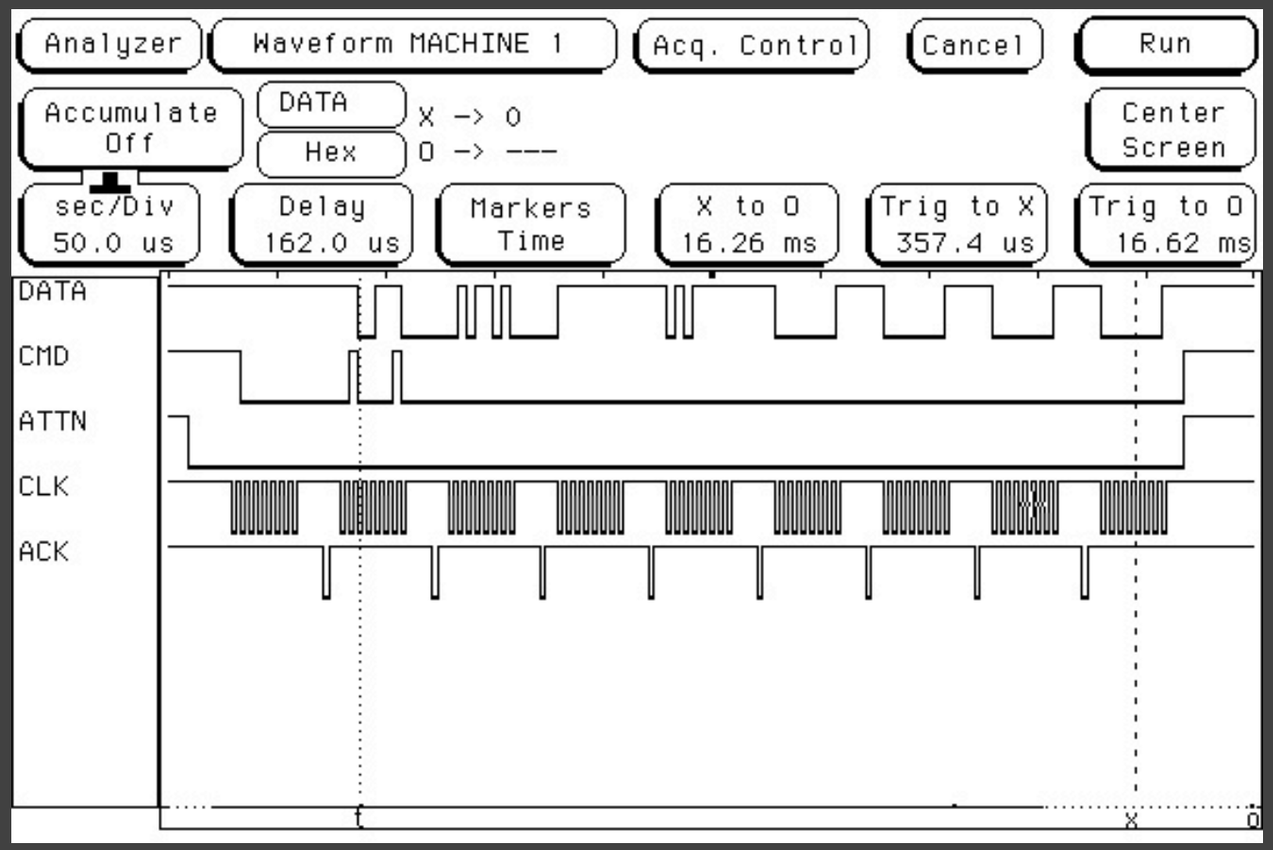
Logic Analyzer

- Used for concurrently capturing, visualizing, and decoding large quantities of digital data
- Introductory guides: `www.tek.com/learning/logic-analyzer-tutorial`
- Range of hobbyist (low end) and professional (high end) tools
  - # of channels (~>8), sampling rate, buffer memory, trigger capabilities, protocol decoding, probe types, accessories
- Standalone: HP/Agilent, Tektronix
- PC-based: LogicPort, Saleae Logic, USBee, LeCroy LogicStudio, DigiView, sigrok (open source analyzer SW)

GRAND IDEA STUDIO

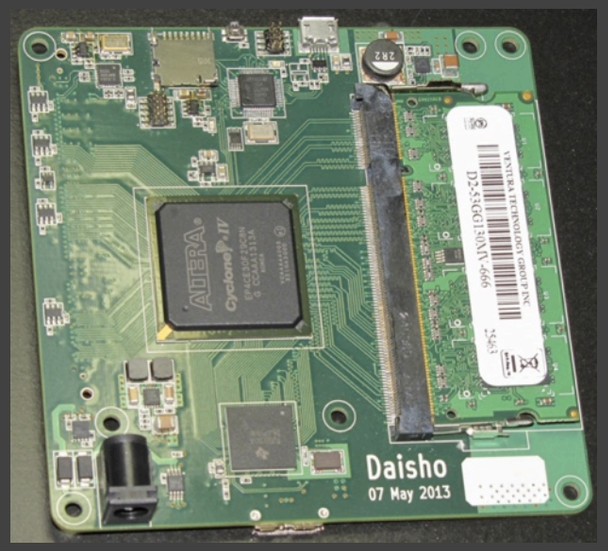
Logic Analyzer 2





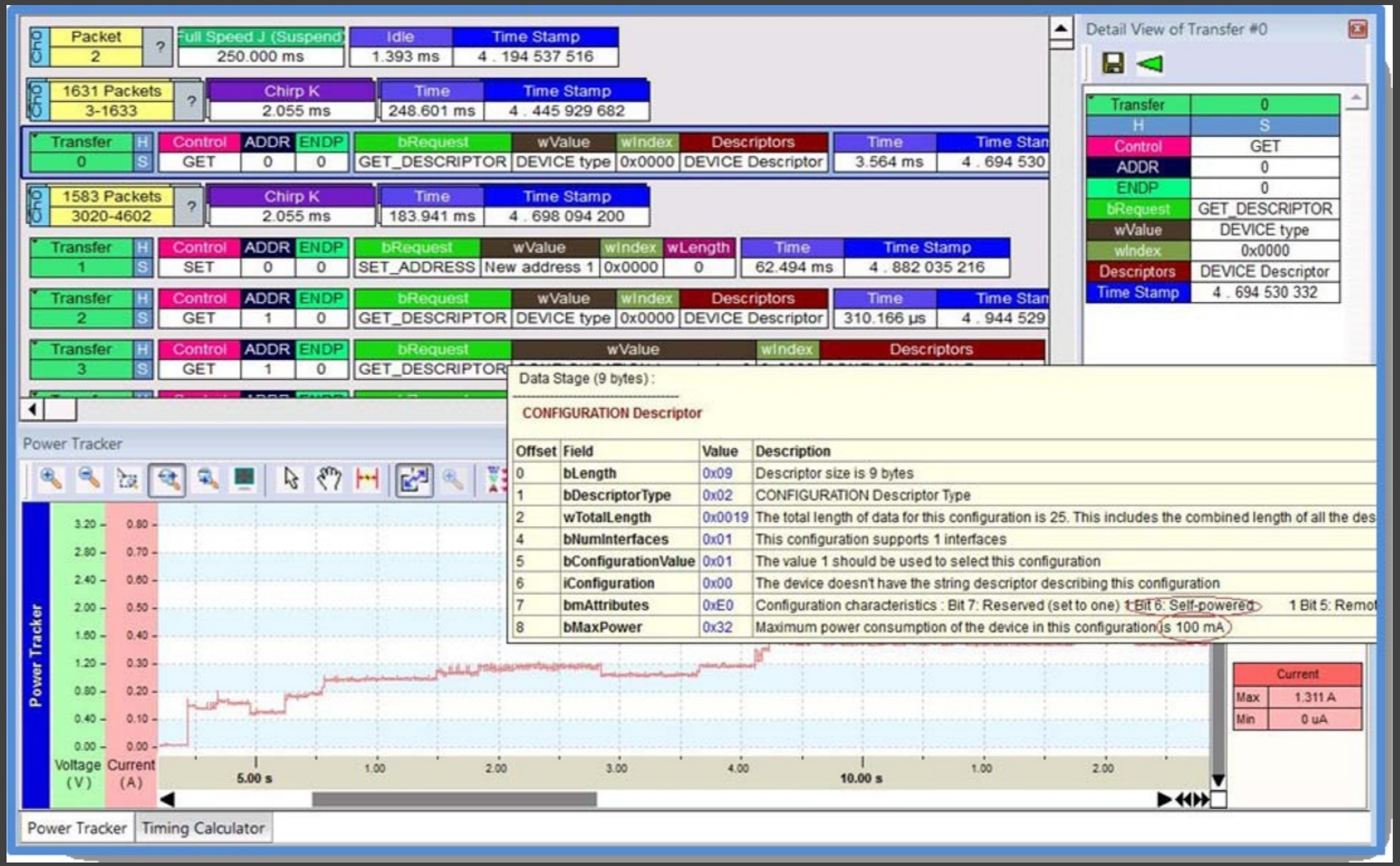
Protocol Analyzer

- Real-time, non-intrusive monitoring/capturing/decoding of wired communications
  - Some also support data injection, current measurements
- HW "man in the middle" to avoid any OS/SW overhead on host
- Total Phase Beagle (USB/I2C/SPI) and Komodo (CAN)
- LeCroy Voyager (USB 2.0/3.0)
- Daisho (Ethernet, USB 3.0, HDMI)
  - `http://ossmann.blogspot.com/2013/05/introducing-daisho.html`



GRAND IDEA STUDIO

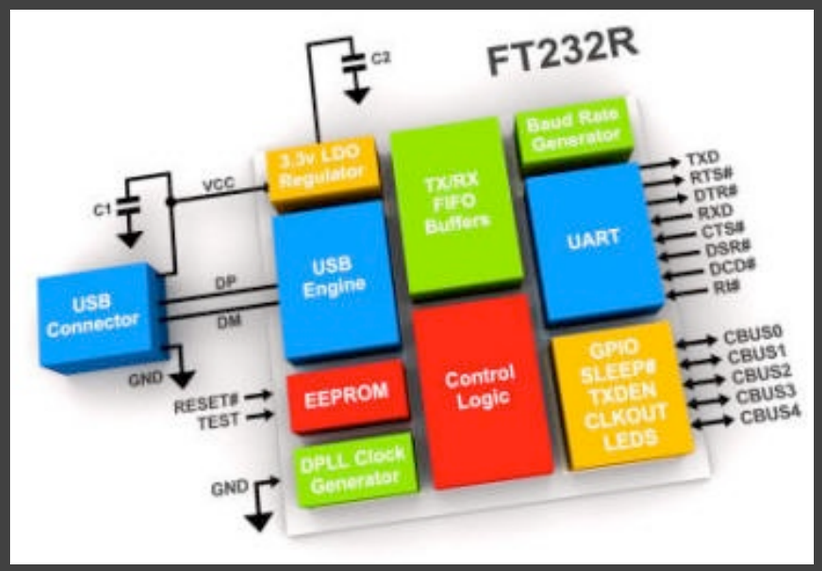
Protocol Analyzer 2

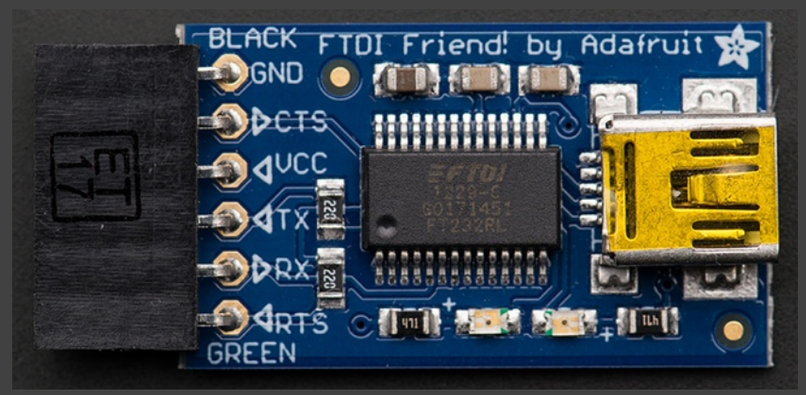


http://teledynelecroy.com/doc/usb-voyager-m3i-power-tracker-usage-case-examples

USB-to-Serial Adapter

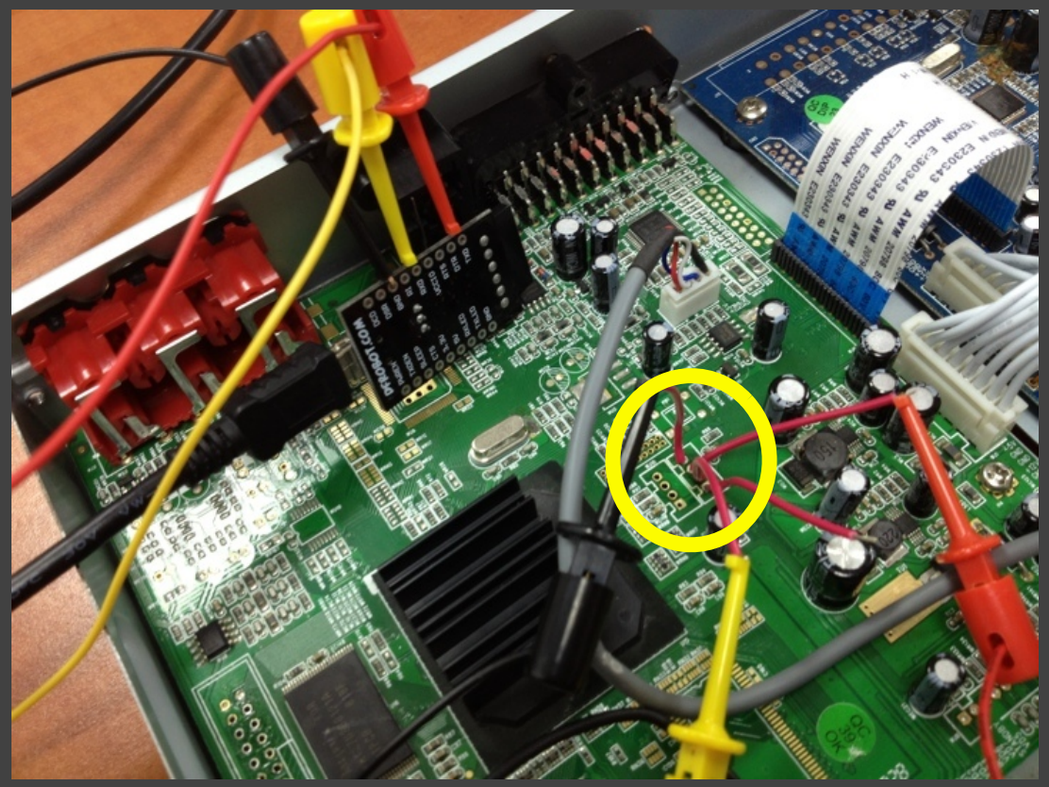
- Converts TTL-level asynchronous serial to USB Virtual COM Port
  - → TXD = Transmit data (to target device)
  - ← RXD = Receive data (from target device)
  - ↔ DTR, DSR, RTS, CTS, RI, DCD = Control signals (uncommon for modern implementations)
- Easily connects to PC, Mac, Linux w/ suitable drivers
- Ex.: FTDI FT232, CP2102, PL2303, Adafruit FTDI Friend
- Many embedded systems use UART as debug output/console/ root shell





GRAND IDEA STUDIO

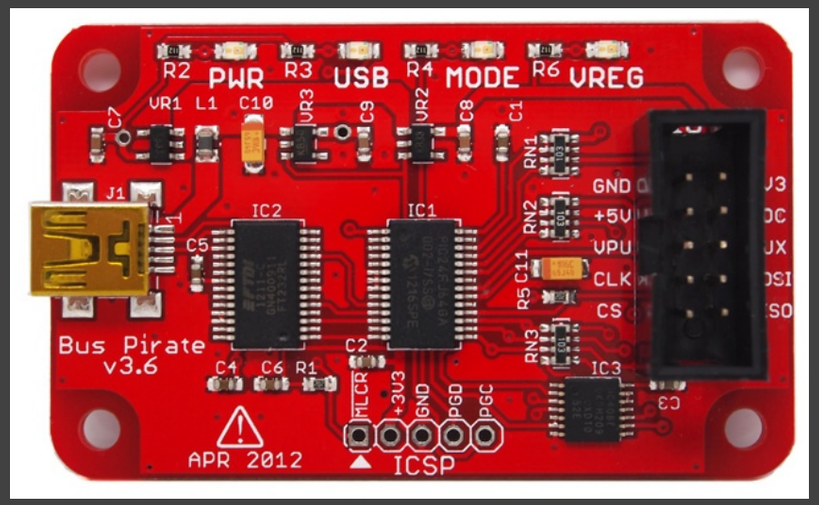
USB-to-Serial Adapter 2



```
-----------------------------------------------------------------
-- STB222 Lite Primary Bootloader 0.1-3847, NI (04:00:34, Feb 17 2009)
-- Andre McCurdy, NXP Semiconductors
-----------------------------------------------------------------
Device: PNX8335 M1
Secure boot: disabled, keysel: 0, vid: 0 (expecting 2)
Poly10: 0x00000000
RNG: enabled
RSA keyhide: enabled
UID: 0000000000000000
AES key: 00000000000000000000000000000000
KC status: 0x00000000
Flash config: 7 (omni: 8bit NAND), timing: 0x0C
CPU clock: 320 MHz
DRAM: 200 MHz, 1 x 1 64MByte 16bit device (SIF0): 64 MBytes
NAND: RDY polling disabled
NAND: (AD76) Hynix SLC, pagesize 512, blocksize 16k, 64 MBytes
NAND 0x00020000: valid header
NAND 0x00020000: valid image
aboot exec time: 179602 uSec


U-Boot 1.2.0.dev (Secondary Bootloader) (Jul 31 2009 - 02:53:01)

CPU: PNX????
Secure boot: disabled
DRAM: 64 MB
NAND: nCS0 (force asserted legacy mode)
NAND: Hynix 64MiB 3,3V 8-bit
NAND 0x02a3c000: bad block
NAND 0x030bc000: bad block
NAND 0x03478000: bad block
NAND 0x0385c000: bad block
Board Opts: SCART PAL
Splash: done
u-boot startup time so far: 1012 msec
Hit any key to stop autoboot:  1 ... 0

STB225v1 nand#
```

Bus Pirate

- Open source tool to interface w/ serial devices
  - SPI, I2C, 1-Wire, LCD, MIDI, MCU/FPGA programming, bit bang
- Basic logic analyzer/digital decoding functionality (slow)
- **`http://dangerousprototypes.com/docs/Bus_Pirate`**

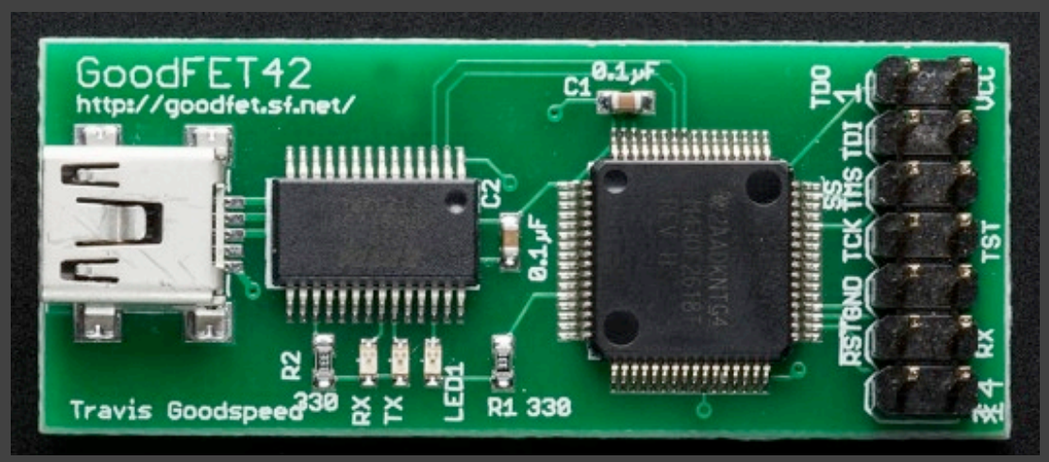



```
HiZ>?
General                                 Protocol interaction
-------------------------------------------------------------------------------
?         This help                     (0)     List current macros
=X/|X     Converts X/reverse X          (x)     Macro x
~         Selftest                      [       Start
#         Reset                         ]       Stop
$         Jump to bootloader            {       Start with read
&/%       Delay 1 us/ms                 }       Stop
a/A/@     AUXPIN (low/HI/READ)          "abc"   Send string
b         Set baudrate                  123
c/C       AUX assignment (aux/CS)       0x123
d/D       Measure ADC (once/CONT.)      0b110   Send value
f         Measure frequency             r       Read
g/S       Generate PWM/Servo            /       CLK hi
h         Commandhistory                \       CLK lo
i         Versioninfo/statusinfo        ^       CLK tick
l/L       Bitorder (msb/LSB)            -       DAT hi
m         Change mode                   _       DAT lo
o         Set output type               .       DAT read
p/P       Pullup resistors (off/ON)     !       Bit read
s         Script engine                 :       Repeat e.g. r:10
v         Show volts/states             .       Bits to read/write e.g. 0x55.2
w/W       PSU (off/ON)          <x>/<x= >/<0>   Usermacro x/assign x/list all
HiZ>
```

```
I2C>(1)
Searching I2C address space. Found devices at:
0xEE(0x77 W) 0xEF(0x77 R)
```

GoodFET

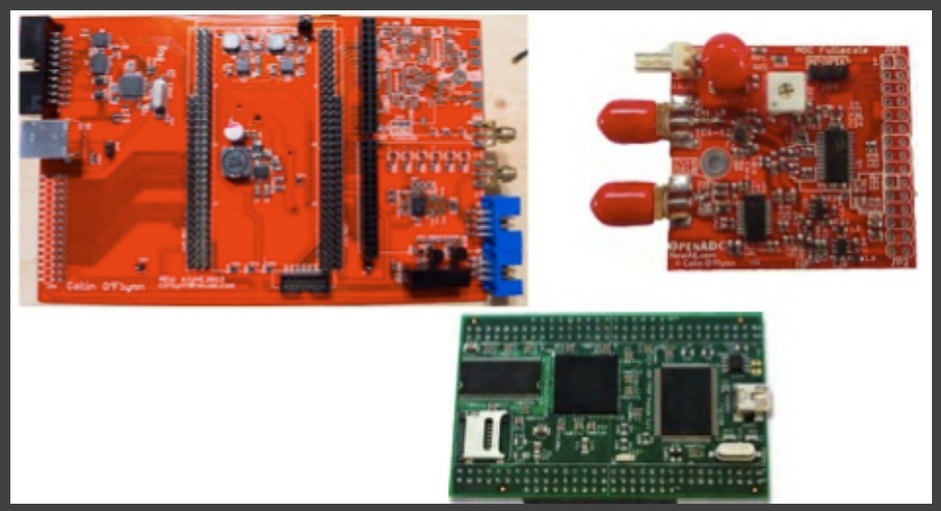
- Travis Goodspeed
- Open source tool for interfacing/hacking chips & target devices
- Different FW and Python scripts for different functionality
  - Ex.: JTAG, SPI, I2C, AVR, PIC, Chipcon/Nordic/Atmel RF
- `http://goodfet.sourceforge.net`

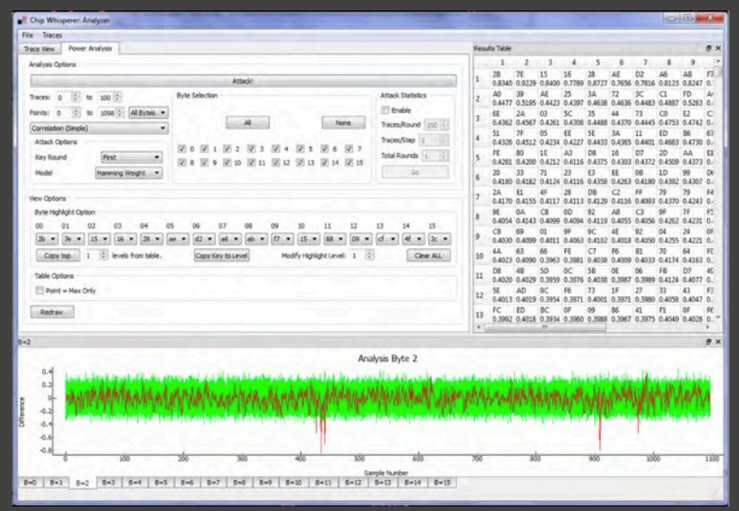


https://jbremnant.wordpress.com/2010/11/23/flashing-ucs-with-goodfet/

ChipWhisperer

- Colin O'Flynn
- Collection of open source HW/SW tools for learning about side channel power analysis
  - Custom board + OpenADC + ZTEX USB-FPGA Module 1.11c (XC6SLX25, SG 3, 64 MB RAM)
- Currently supports AES-128 and -256
- Correlate measured power w/ predicted power to guess byte of key (subkey)
- **`https://www.assembla.com/spaces/chipwhisperer/wiki`**





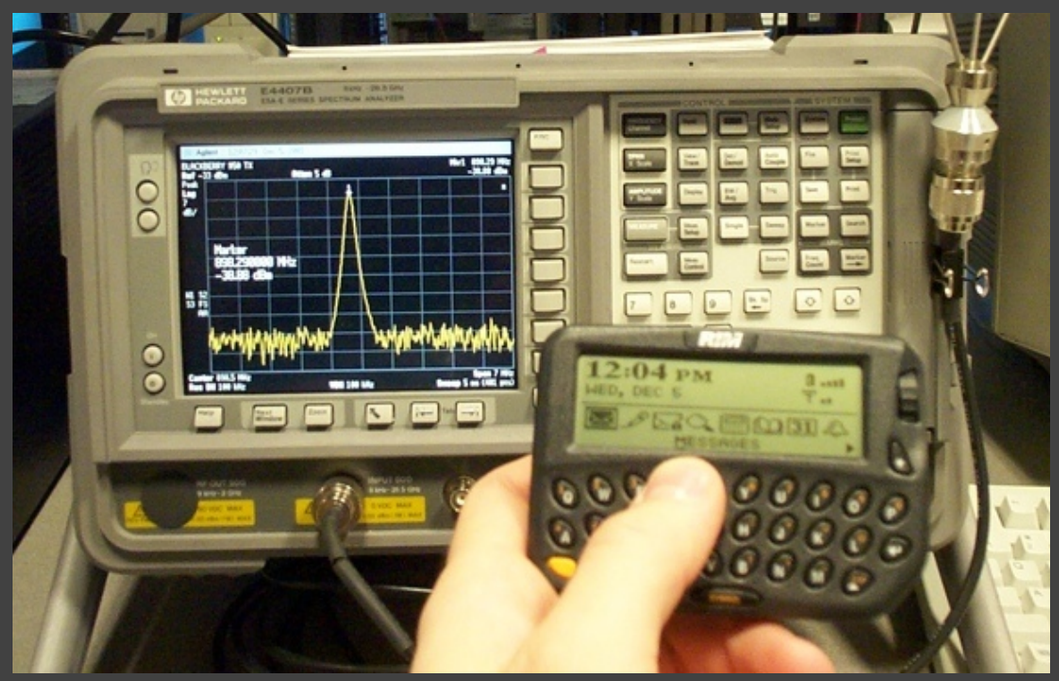
GRAND IDEA STUDIO

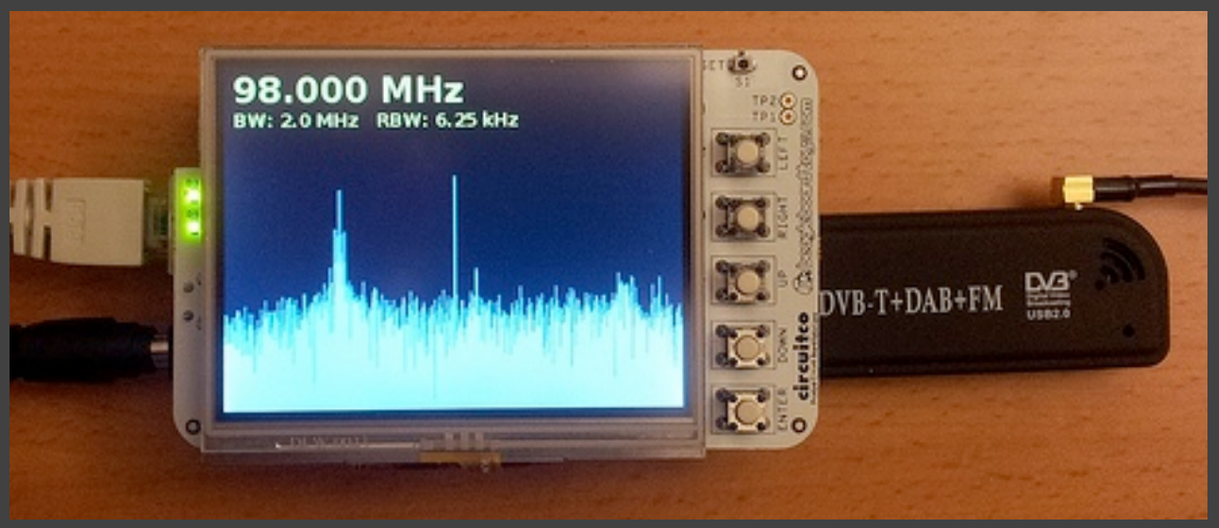
Spectrum Analyzer

- Used for visualizing RF/radio spectrum
  - Measures magnitude of input signal v. frequency
  - Can characterize system operation/emissions by dominant frequency, power, distortion, harmonics
- Introductory guide: `http://cp.literature.agilent.com/litweb/pdf/5965-7920E.pdf`
- Range of hobbyist (low end) and professional (high end) tools
- Ex.: Tektronix, Agilent, Signal Hound, RF Explorer, RTL-SDR (RFL2832U dongle w/ BeagleBone)

GRAND IDEA STUDIO

Spectrum Analyzer 2





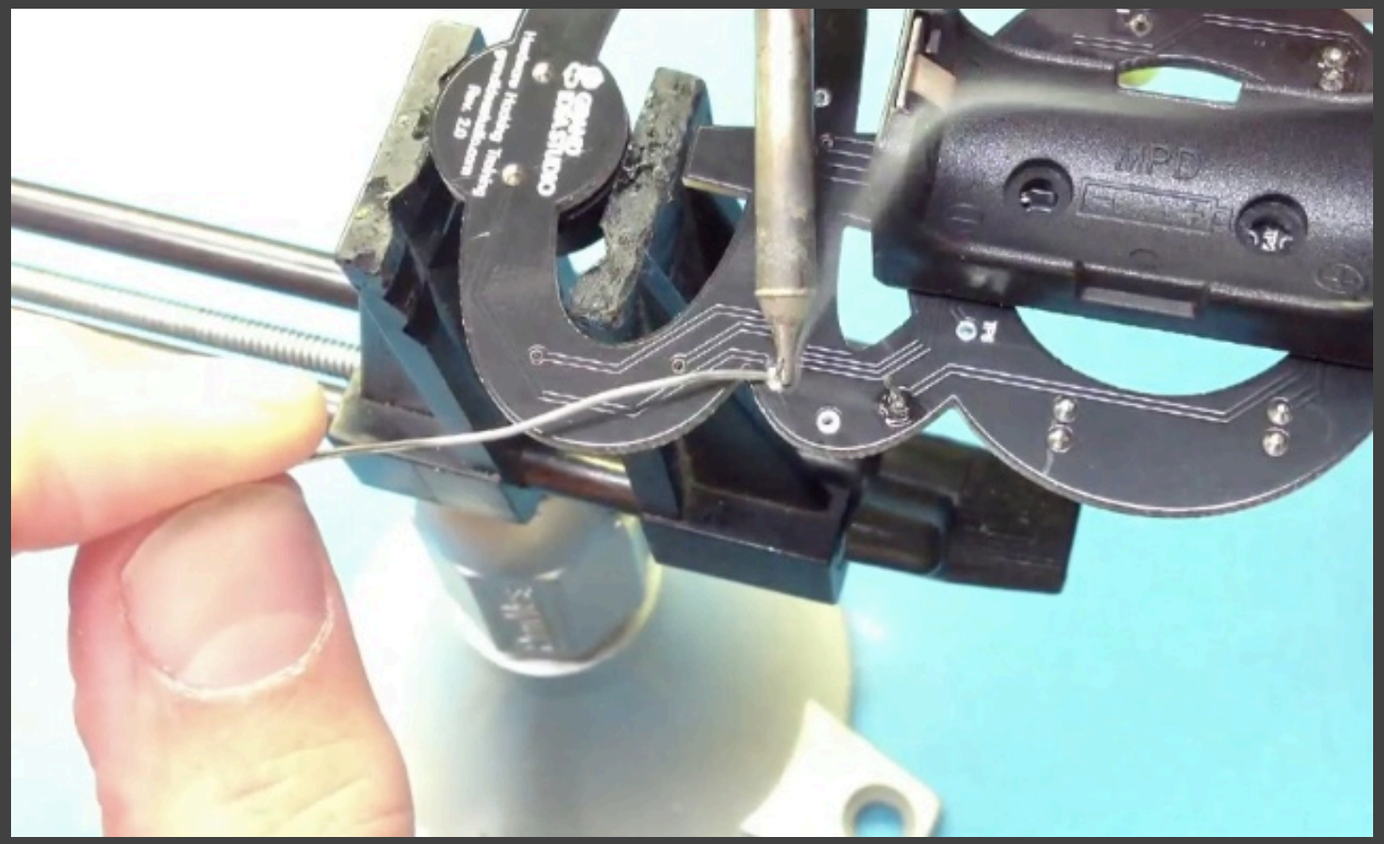
www.oz9aec.net/index.php/beaglebone/480-rtlizer

GRAND IDEA STUDIO

Manipulation / Injection

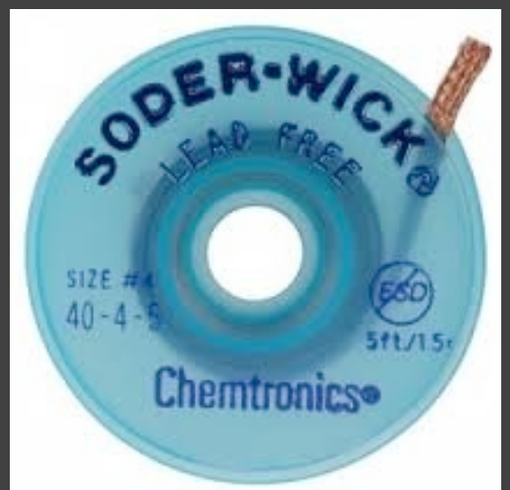
Soldering Iron

- Provides heat to melt solder that physically holds components on a circuit board
- Range from a simple stick iron to a full-fledged rework station
  - Interchangeable tips, adjustable temperature, hot air reflow
- Weller, Metcal, Hakko, Radio Shack (!)



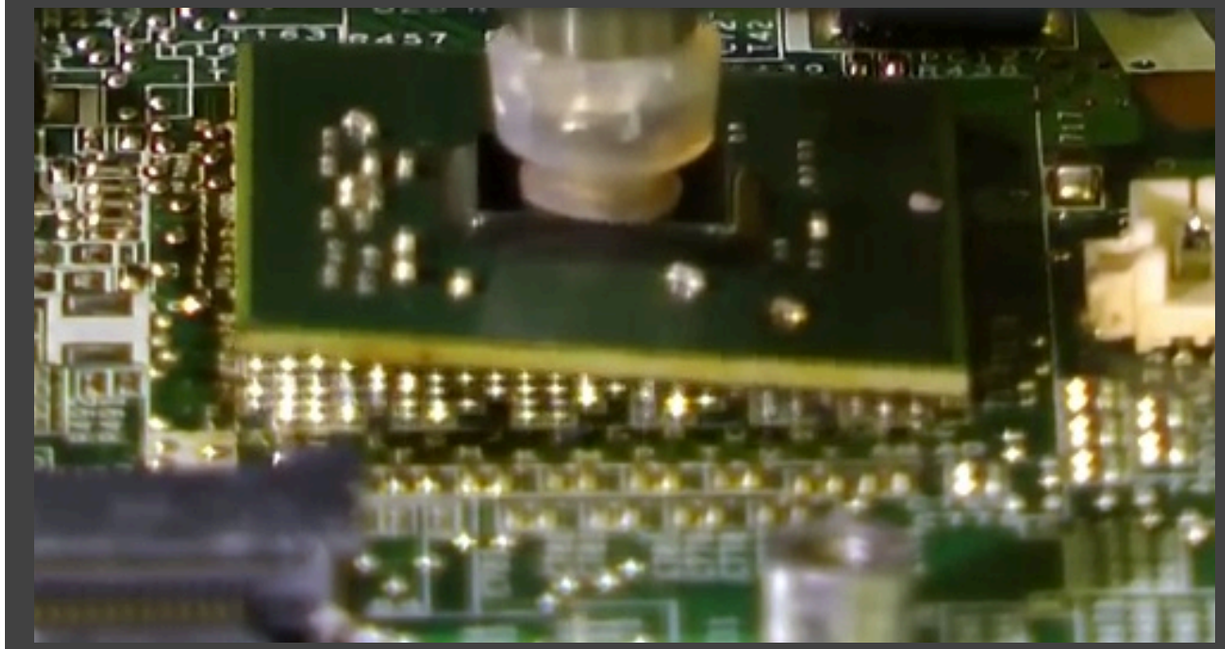
Soldering Accessories

- Solder: Thin gauge (0.032" or 0.025" diameter), ~60/40 Rosin core or lead-free alloy
- Desoldering Tool ("Solder Sucker"): Manual vacuum device that pulls up molten solder into its chamber
- Desoldering Braid: Wicks molten solder up into braid
- Flux: Assists in heat transfer and removal of surface oxides
- Tip cleaner: Helps to keep the solder tip clean for even heat distribution. Ex.: Sponge, tip tinner



Rework station

- Hot air convection, infrared, laser
- Allows easier removal and reflow of individual SMD components
  - Especially BGA (Ball Grid Array) & CSP (Chip Scale Package)
- Nozzles for different package types/mechanical footprints
- Weller, Metcal, Hakko, ZEVAC, Zephyrtronics



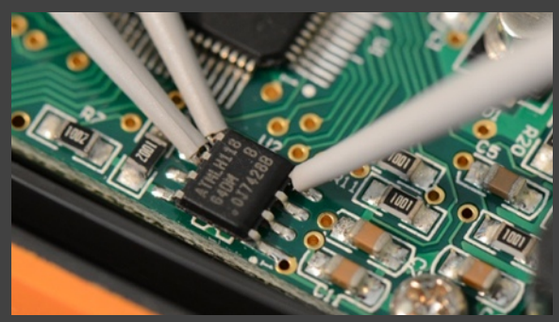
https://www.youtube.com/watch?v=3Vf0nsVBHJE

ChipQuik

- Allows the quick and easy removal of surface mount (and some through hole) components
- **`www.chipquik.com`**
- Primary component is a low-melting temperature alloy (less than 200°F)
  - Reduces the overall melting temperature of the solder
  - Enables you to just lift the part right off of the board

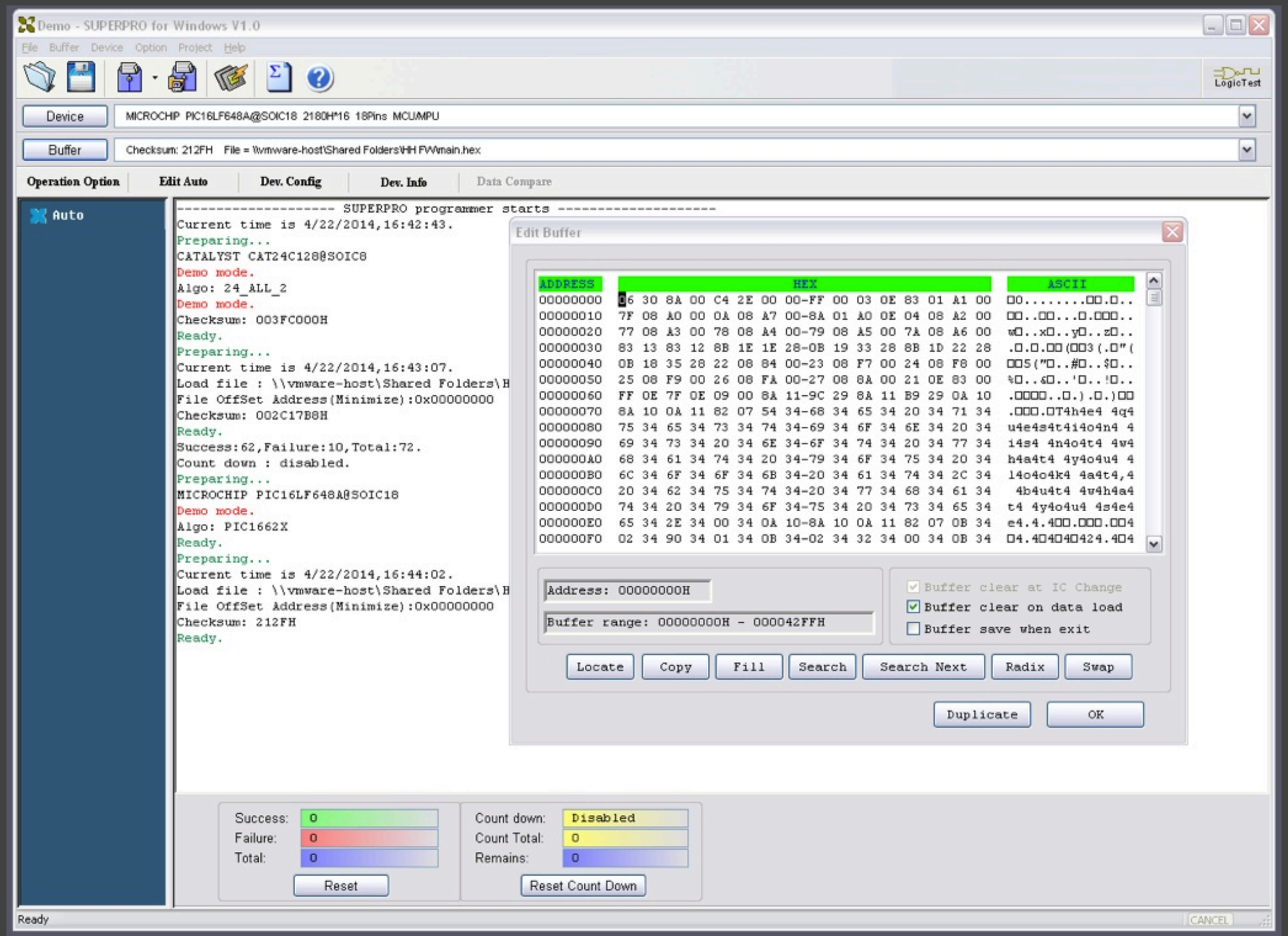
Device Programmer

- Used to read/write most devices that contain memory
  - Standalone or internal to MCU
  - Ex.: Flash, E(E)PROM, ROM, RAM, PLD/CPLD, FPGA
- Some devices can be manipulated in-circuit
- Many support > 35k different devices
- Few extraction/read-out/access mechanisms exist
  - Security bit/fuse, password protection
- EE Tools, Xeltek, BP Microsystems, Data I/O



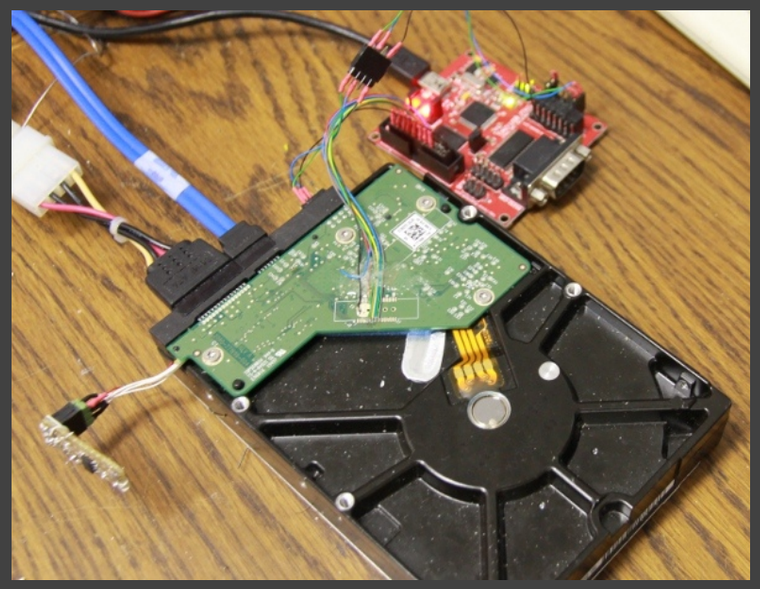
GRAND IDEA STUDIO

Device Programmer 2

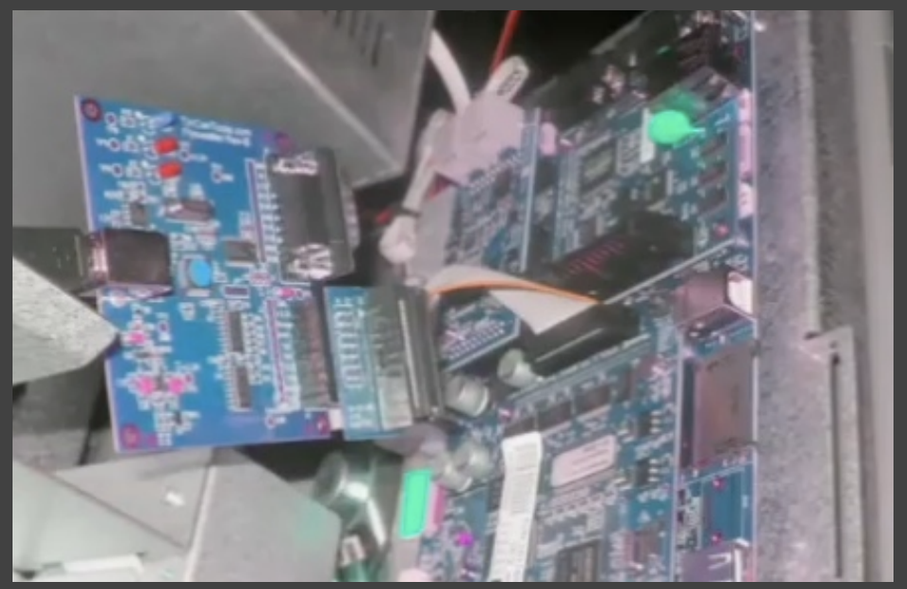


JTAG Tools

- Off-the-shelf HW tools designed for JTAG-based interaction w/ target device
- JTAG = Industry-standard test/program/debug I/F, could be useful for attack or stepping stone against embedded device
- Many different types available
  - Ensure tool supports your target architecture
  - Find out what the IC vendor recommends for legitimate engineers



http://spritesmods.com/?art=hddhack



www.blackhat.com/html/bh-us-10/bh-us-10-archives.html#Jack

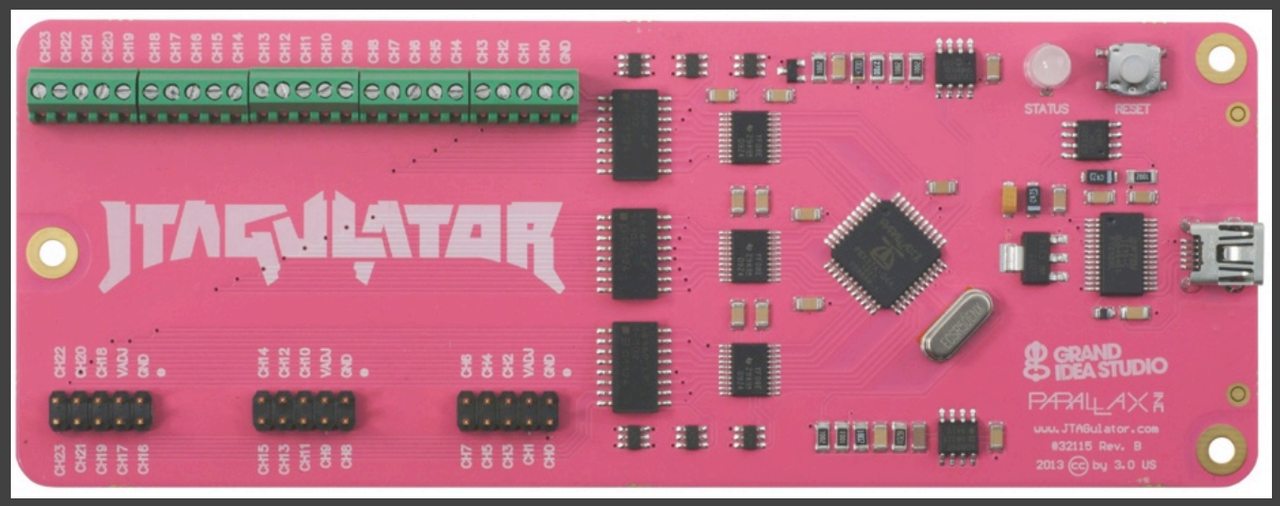
GRAND IDEA STUDIO

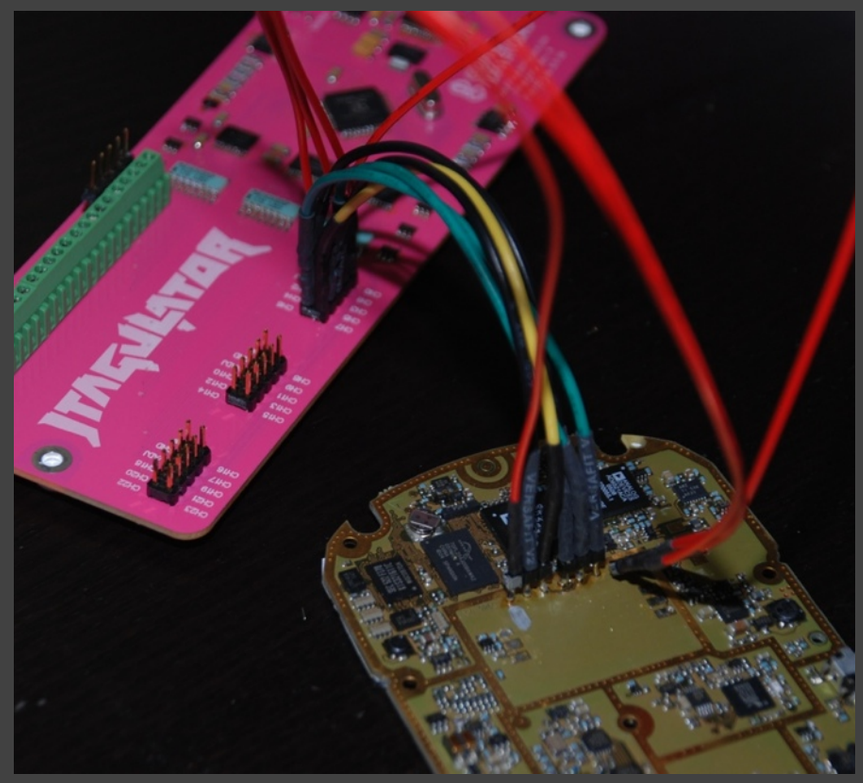
JTAG Tools 2

- RIFF Box
  - Mainly used for unbricking/data extraction from mobile phones
  - **www.jtagbox.com**
- H-JTAG
  - Standalone software & works w/ existing target IDEs
  - **www.hjtag.com/en/**
- SEGGER J-Link
  - Works w/ existing target IDEs
  - **www.segger.com/debug-probes.html**
- Bus Blaster (open source)
  - **http://dangerousprototypes.com/docs/Bus_Blaster**
- Wiggler or compatible (parallel port)
  - **ftp://www.keith-koep.com/pub/arm-tools/jtag/jtag05_sch.pdf**

JTAGulator

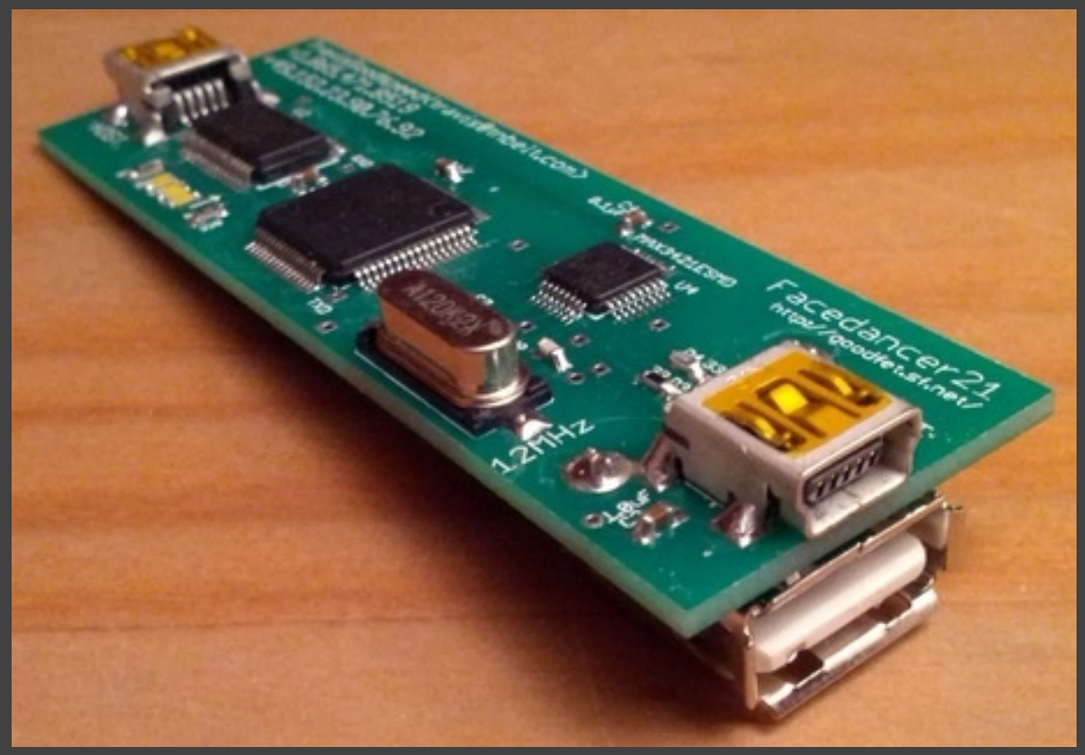
- Joe Grand
- Open source tool to assist with discovery of on-chip program/ debug interfaces
- Currently detects JTAG & UART/asynchronous serial
- Supports up to 24 connections to unknown points on target circuit board, adjustable target voltage (1.2V-3.3V), input protection, firmware upgradable
- **`www.jtagulator.com`**





Facedancer

- Travis Goodspeed
- Emulate USB devices for host-based testing/fuzzing/analysis
  - `http://travisgoodspeed.blogspot.com/2012/07/emulating-usb-devices-with-python.html`
  - `http://goodfet.sourceforge.net/hardware/facedancer21/`

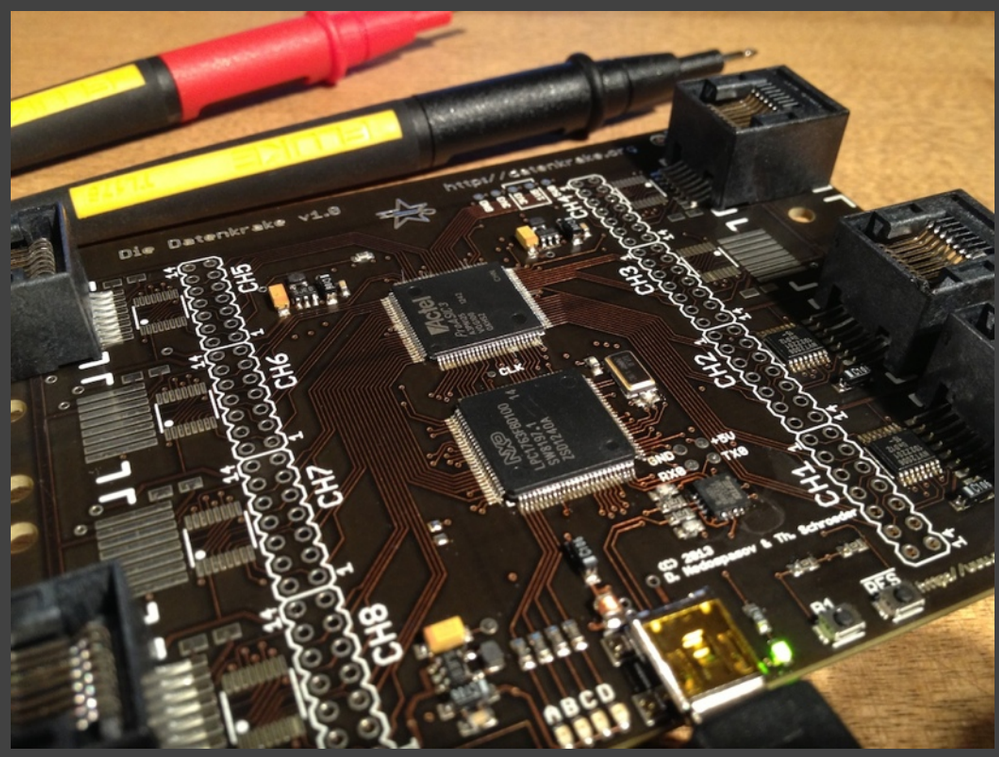



```
# Finds devices supported by the OS
$ python3 umap.py -P /dev/ttyUSB3 -i
# Fuzz a HID device class
$ python3 umap.py -P /dev/ttyUSB3 -f 03:00:00:C
# Try to identify the operating system
$ python3 umap.py -P /dev/ttyUSB3 -O
# Run a single fuzz test case
$ python3 umap.py -P /dev/ttyUSB3 -s 03:00:00:C:16
```

http://blog.j-michel.org/post/67652808280/a-journey-in-script-kiddie-land-and-kernel-land

Die Datenkrake

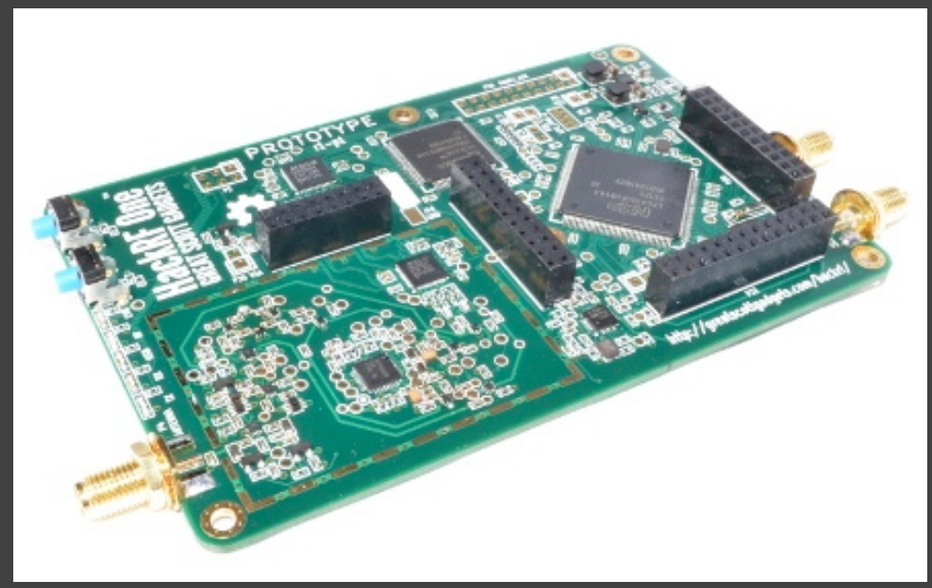
- Dmitry Nedospasov & Thorsten Schroeder
- Low cost, open source development & attack platform
  - ARM Cortex-M3 + FPGA
- Fuzzing, glitching, protocol analysis
- Requires off-the-shelf IDEs for FW & FPGA development
- Creation of tools/examples on-going
- **`www.datenkrake.org`**
- **`https://github.com/ddk/`**



GRAND IDEA STUDIO

RF Tools (Software Defined Radio)

- Hack RF
  - Michael Ossmann
  - **http://greatscottgadgets.com/hackrf/**
- Blade RF
  - **http://nuand.com**
- Ubertooth One (2.4GHz/Bluetooth)
  - Michael Ossmann
  - **http://greatscottgadgets.com/ubertoothone/**
- RFIDler (RFID Reader/Writer/Emulator)
  - Adam Laurie aka Major Malfunction
  - **http://adamsblog.aperturelabs.com/2013/08/rfidler-open-source-software-defined.html**

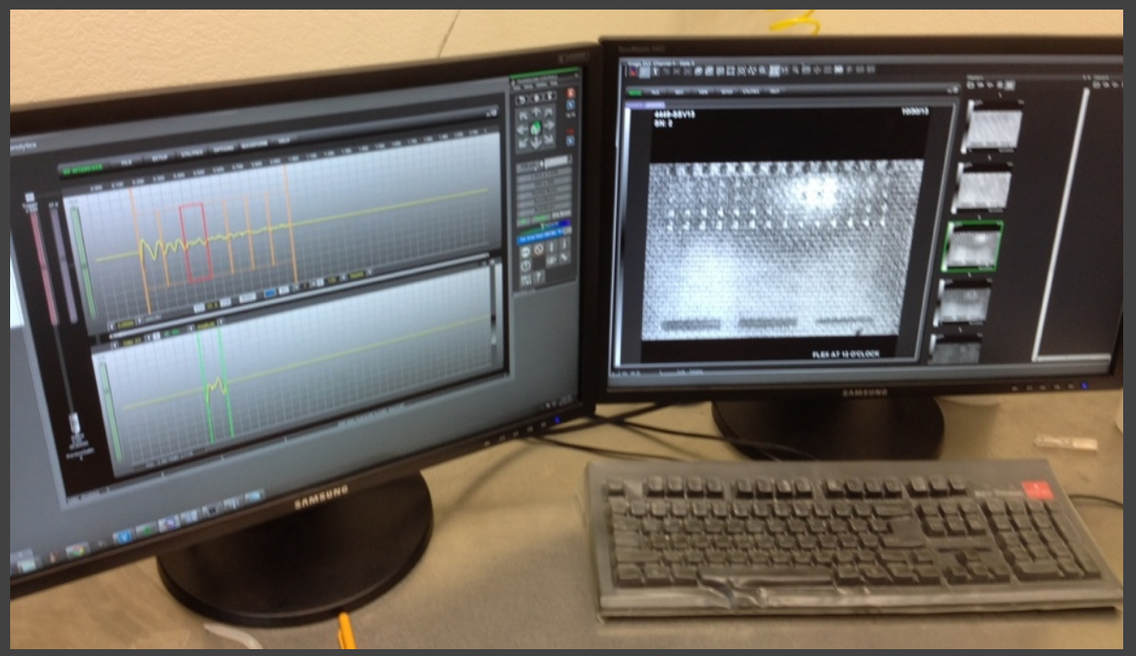


GRAND IDEA STUDIO

Imaging

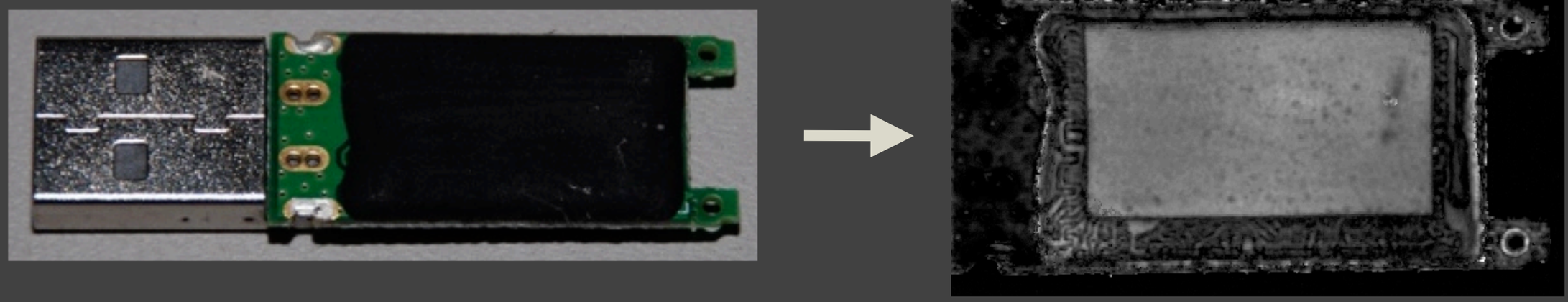
Acoustic Microscopy

- Target placed into bath of DI water or alcohol
  - Serves as liquid coupling medium to transfer sound waves to target
- Ultrasound emitted into target (15-300MHz)
- Return echoes are captured (reflection)
- Transmission through the target is measured (thru scan)



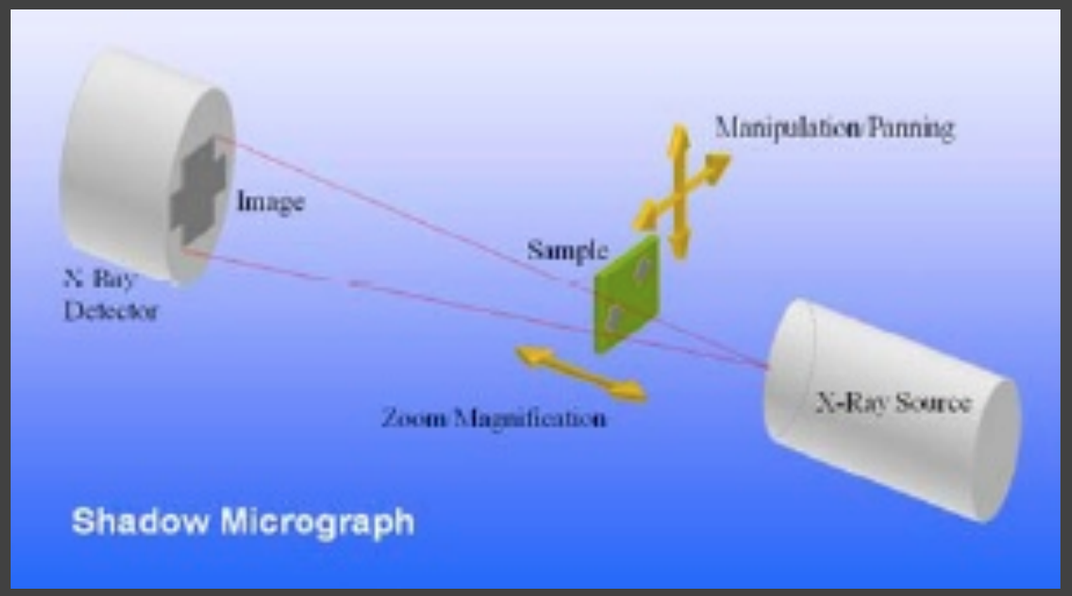
Acoustic Microscopy 2

- Typically used for non-destructive failure analysis & reliability testing/verification of ICs, components, packaging, wafers
  - Can identify air gaps/voids, delamination, cracks/mechanical stress, counterfeits
- We can use it for examining through epoxy encapsulation
  - Identify key components, connections, or locations



X-Ray (2D)

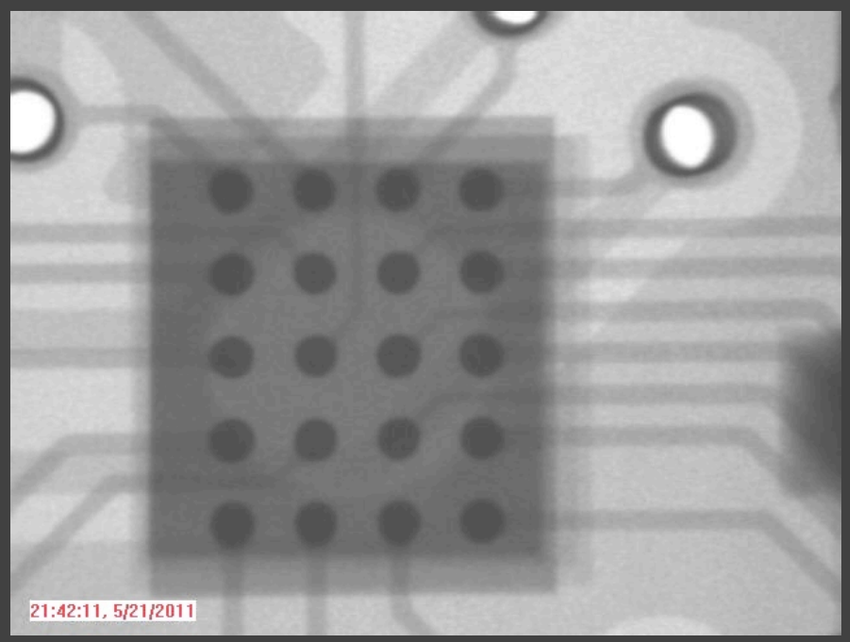
- X-rays passed through target and received on detector
  - All materials absorb radiation differently depending on density, atomic number, and thickness
- Provides a composite image of all layers in target



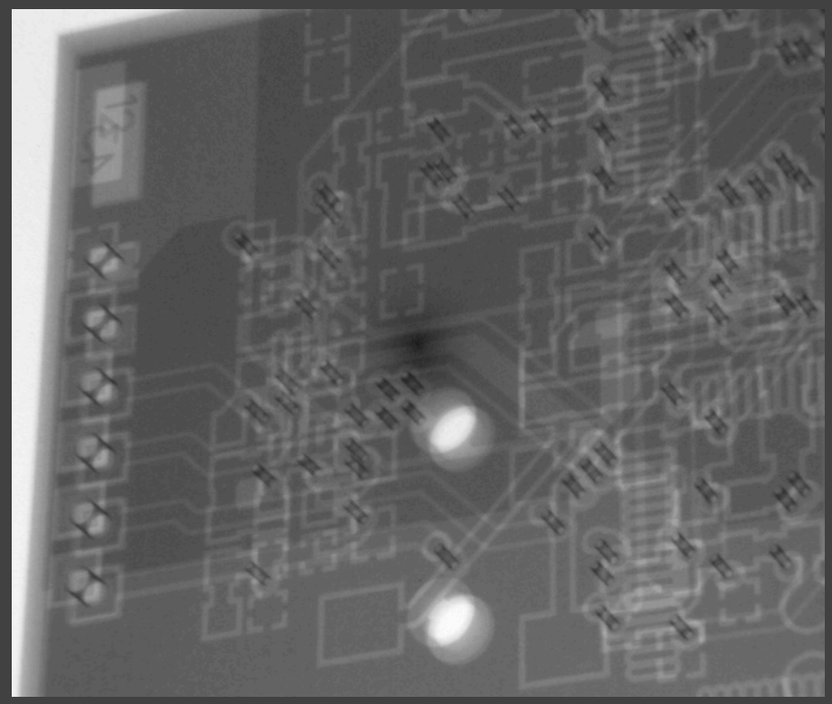
http://datest.com/resources-boardtestmeth-primer2d3d.php

X-Ray (2D) 2

- Typically used during PCB assembly (component placement/ solder quality) or failure analysis (troubleshooting defective features)
- We can use it for general PCB inspection and examining through epoxy encapsulation
  - Can get clues of PCB fabrication techniques, component location, layer count, hidden/embedded features

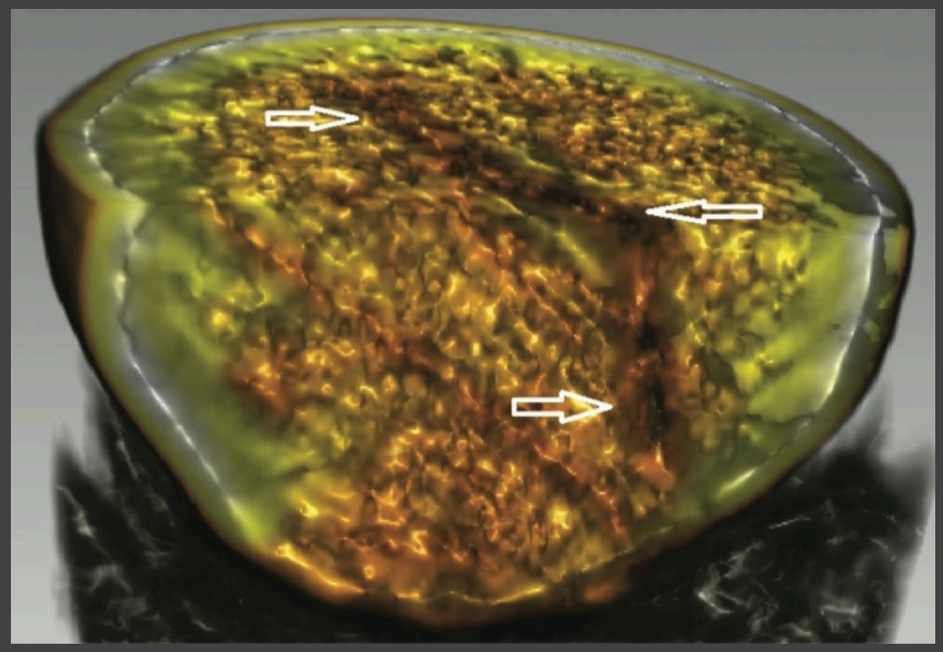


20-pin uBGA (CSP3)



X-Ray (3D/CT)

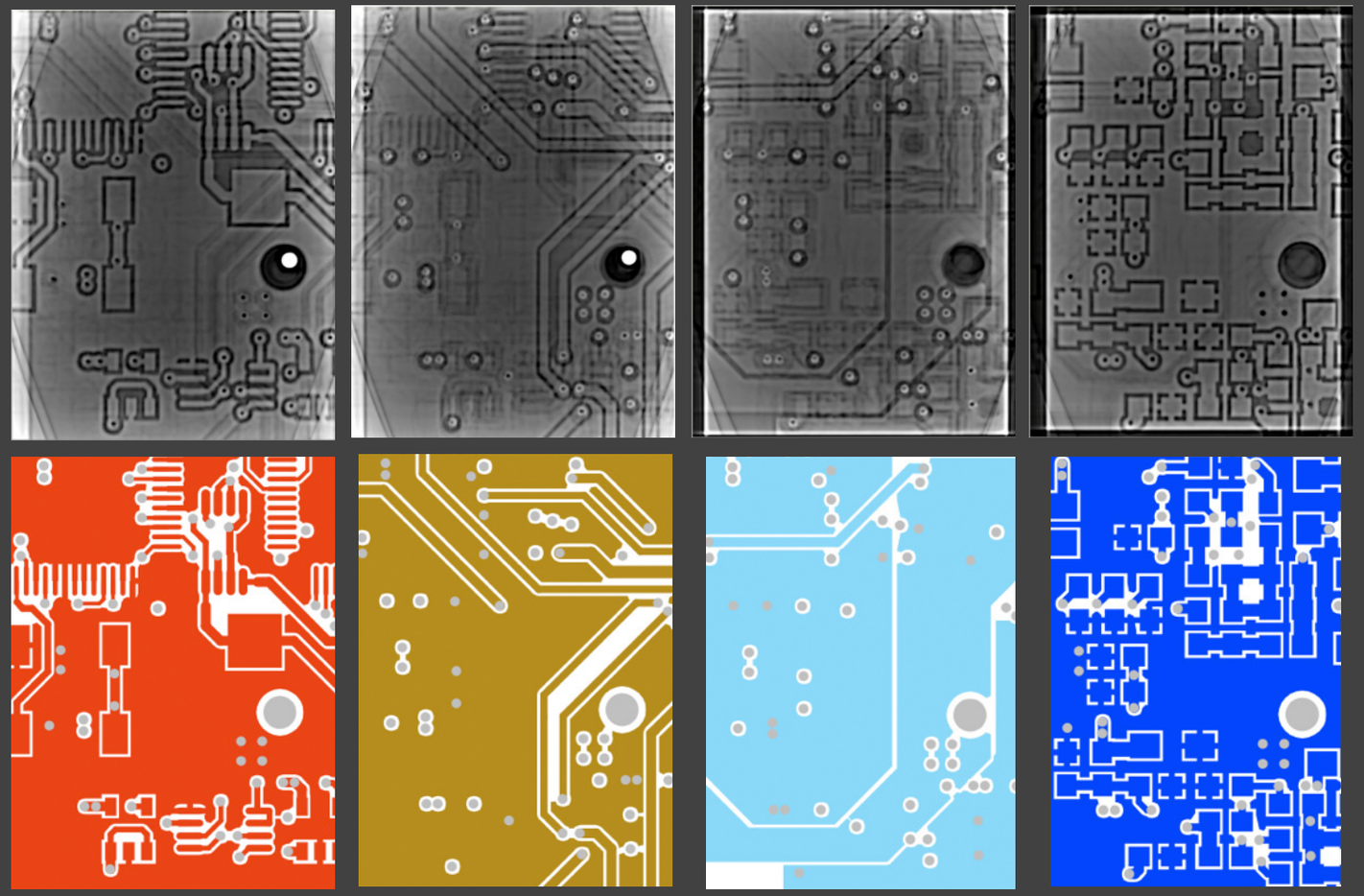
- Computed Tomography (CT)
  - A series of 2D X-ray images post-processed to create cross-sectional slices of the target
  - X-ray beam rotated 360° in a single axis around the target
- Acquisition
  - Capture a series of 2D X-ray images (60-720 depending on desired resolution)
- Reconstruction
  - Post-processing results in 2D slices that can be viewed in any plane (X, Y, Z)
  - Can be manipulated with 3D modeling software



http://datest.com/resources-brochures.php

X-Ray (3D/CT) 2

- Typically used for complex inspection and failure analysis of PCBs, component packaging, solder ball/joint quality
- We can use it to extract individual layers of a PCB
  - Results may vary based on layer count, inter-layer thickness, copper weight, substrate composition



GRAND IDEA STUDIO

The End.