RSA Conference 2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: HTA-W04

Tools of the Hardware Hacking Trade

Joe Grand

Principal Engineer
Grand Idea Studio
@joegrand

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

Hardware Hacking

- Information Gathering
  - Obtaining information about the target
- Teardown
  - Product disassembly, component/subsystem ID
- Interfaces
  - Protocol monitoring/analysis/emulation
- Firmware
  - Extract/modify/reprogram code or data
- Chip-Level
  - Silicon die modification/data extraction

Tools of the Hardware Hacking Trade

- Signal Monitoring/Analysis
- Manipulation/Injection
- Imaging

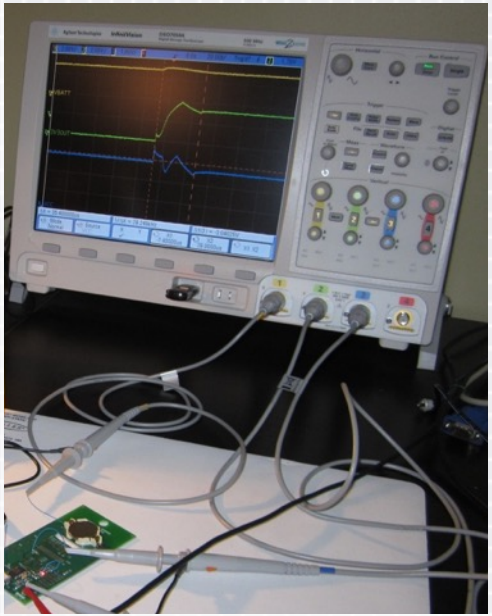
RSAConference2015

San Francisco | April 20-24 | Moscone Center

Signal Monitoring / Analysis

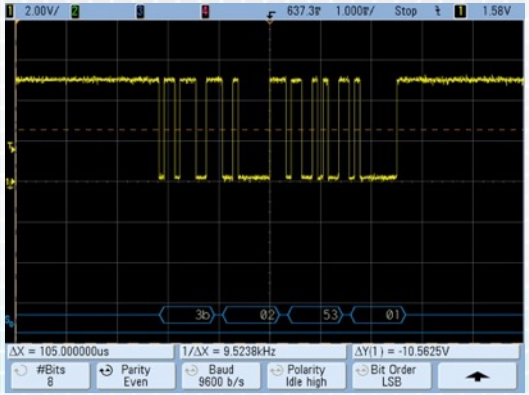
Oscilloscope

- 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, BitScope



Oscilloscope: Example

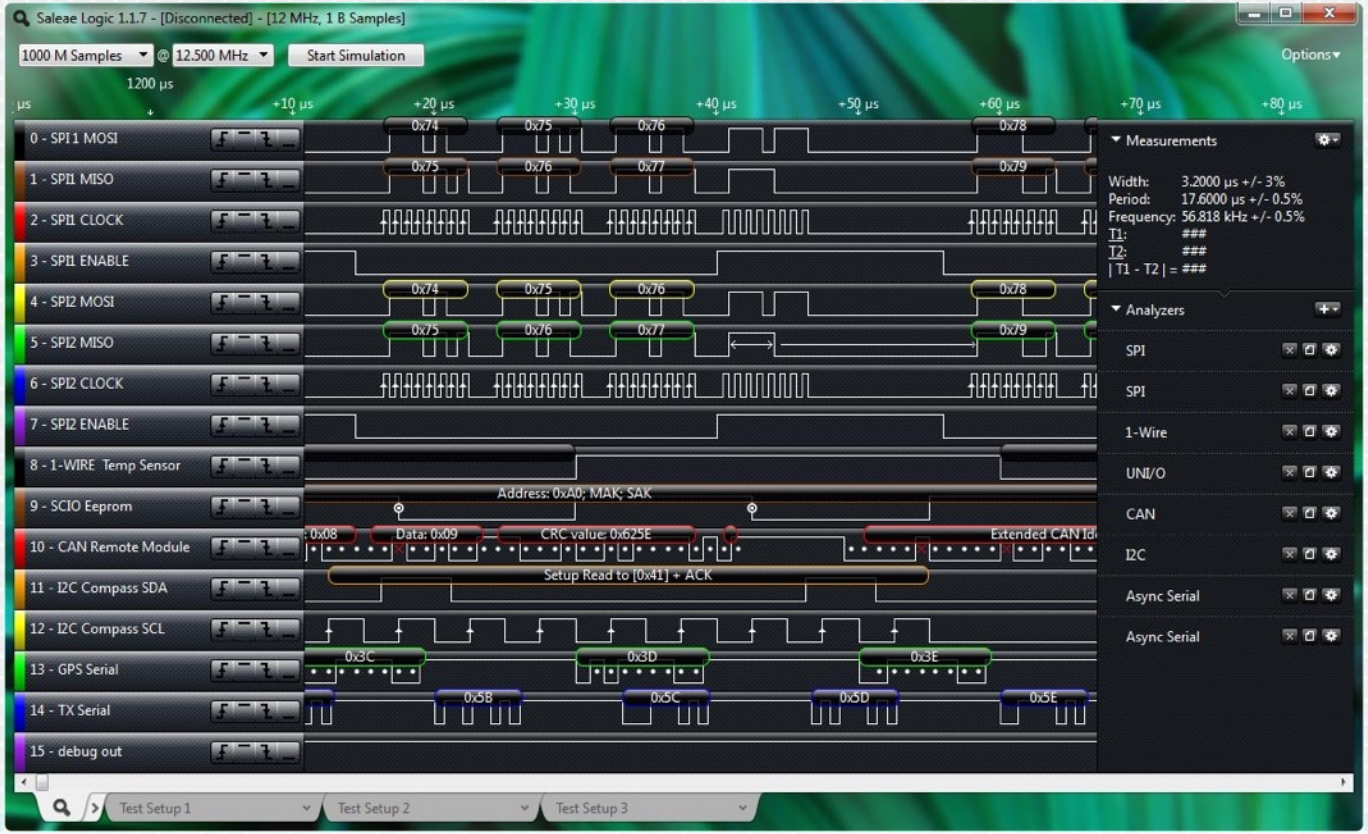
- SFMTA Smart Parking Meter (2009)
  - Joe Grand, Chris Tarnovsky, Jake Appelbaum
  - Monitored meter/card communication w/ oscilloscope
    - Slight variation in signal voltage determined direction of data
  - Created custom Microchip PIC-based smartcard emulator
  - www.grandideastudio.com/portfolio/smart-parking-meters



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 (~>4), sampling rate, buffer memory, trigger capabilities, protocol decoding, probe types, accessories
- Standalone: HP/Agilent, Tektronix
- PC-based: Saleae Logic, LogicPort, USBee, LeCroy LogicStudio, DigiView, sigrok (open source)

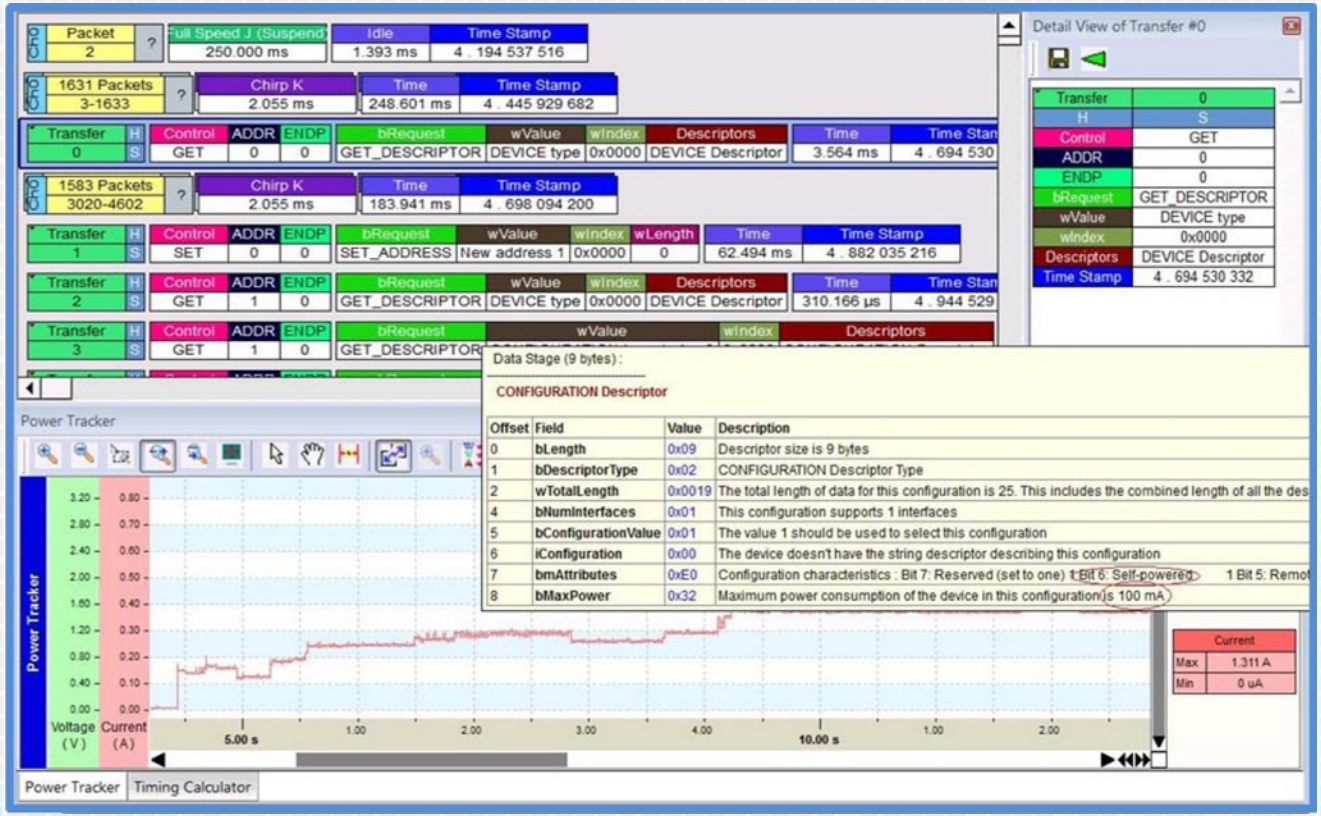
Logic Analyzer: Example



Protocol Analyzer

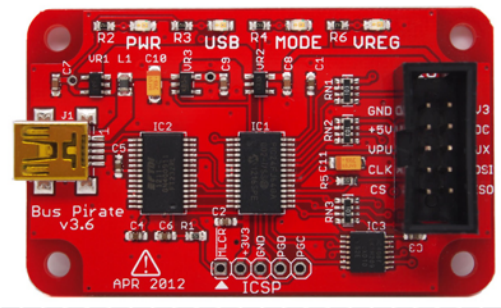
- Real-time, non-intrusive monitoring/capturing/decoding of wired communications
  - HW "man in the middle" to avoid any OS/SW contention/overhead on host
  - Some also support data injection, measurements
- Total Phase Beagle (USB, I2C, SPI) and Komodo (CAN)
- LeCroy Voyager (USB 2.0/3.0)
- International Test Instruments (USB 2.0, PCIe 1.1)
- OpenVizsla (USB), http://openvizsla.org
- Daisho (Ethernet, USB 3.0, HDMI), http://ossmann.blogspot.com/2013/05/introducing-daisho.html

Protocol Analyzer: Example



Bus Pirate

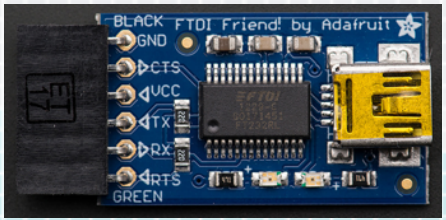
- Open source tool to interface w/ serial devices
  - SPI, I2C, 1-Wire, LCD, MIDI, MCU/FPGA programming, bit bang
- Basic logic analyzer/digital decoding functionality (slow)
- http://dangerousprototypes.com/docs/Bus_Pirate




```
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>
```

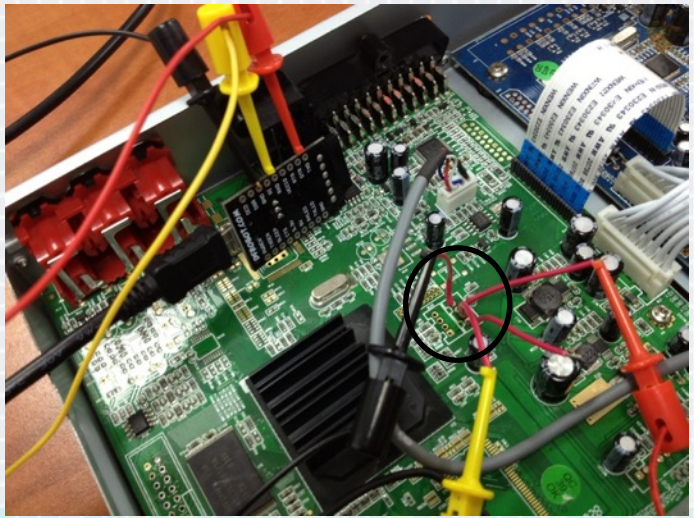
USB-to-Serial Adapter

- Converts logic 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 (often unused)
- 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/root shell
  - Ex.: Exploitee.rs Wiki (formerly GTVHackers), www.exploitee.rs



USB-to-Serial Adapter: Example

- Apex STB236 Set Top Box
  - Visually identify connector
  - Oscilloscope to determine baud rate (115.2kbps)
  - USB-to-Serial adapter
  - Bootloader + U-Boot



USB-to-Serial Adapter: Example 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#
```

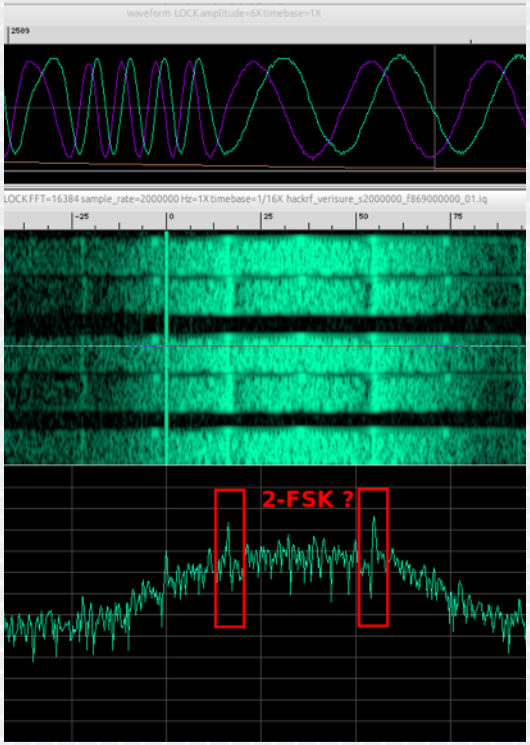
Software Defined Radio

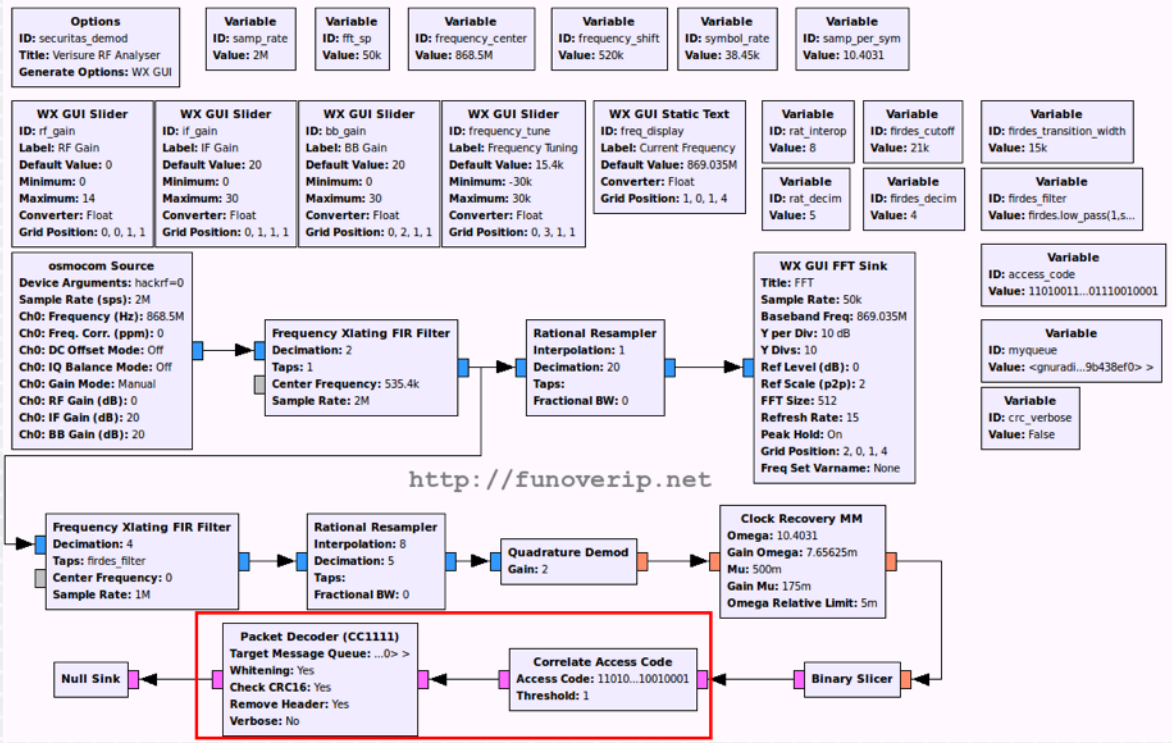
- Communication system where digital signal processing is used to implement radio/RF functions
  - Ex.: Mixers, filters, amplifiers, modulators/demodulators, detectors
  - RF front end + general purpose computer to receive/transmit arbitrary radio signals
- Primary toolset for RF/radio hacking
  - Visualize RF spectrum (spectrum analyzer)
  - Modulate/demodulate/filter raw signal
  - Decode/inject data
- Ex.: RTL-SDR, HackRF One, Blade RF, RFIDler

Software Defined Radio: Example

- Verisure Wireless Home Alarm
  - Discover frequency and modulation scheme using GQRX and HackRF
  - Capture raw signal and import into Baudline for visualization
  - Create custom flowgraph using GNU Radio to capture, filter, demodulate, and slice signal into binary data
  - https://funoverip.net/2014/11/reverse-engineer-a-verisure-wireless-alarm-part-1-radio-communications/

Software Defined Radio: Example 2

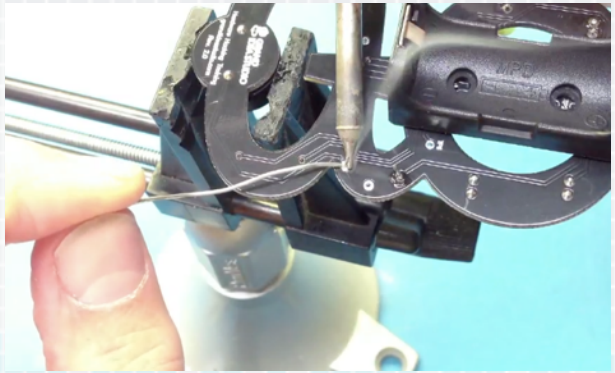




Manipulation / Injection

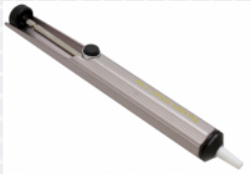
Soldering Iron

- 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

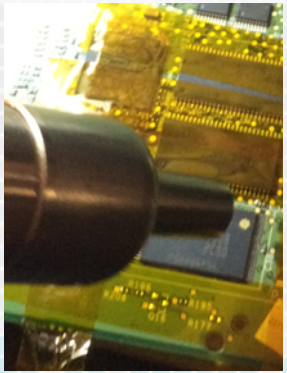




ChipQuik

- Allows the quick and easy removal of surface mount (and some through hole) components
- 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/slide the part easily off of the board
- www.chipquik.com

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



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 > 90k (!) different devices
- Few extraction/read-out/access mechanisms exist
  - Security bit/fuse, password protection
- EE Tools, Xeltek, BP Microsystems, Data I/O

Debug Tools

- Off-the-shelf HW tools designed for interaction w/ target device
  - Can provide chip-level control (single step, access registers)
  - Extract program code or data
  - Modify memory contents
  - Affect device operation on-the-fly
- Either vendor-specific or industry standard (JTAG)
- Many different types available
  - Ensure tool supports your target architecture
  - Find out what vendor recommends for legitimate engineers

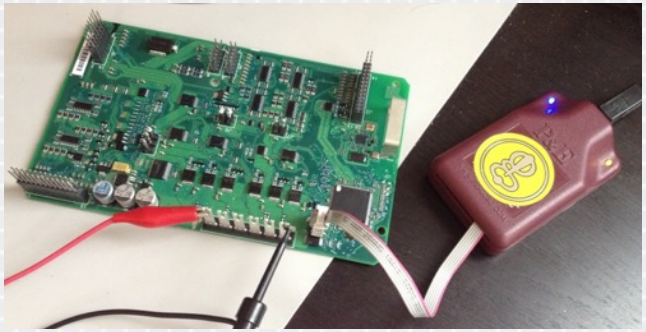
Debug Tools: JTAG

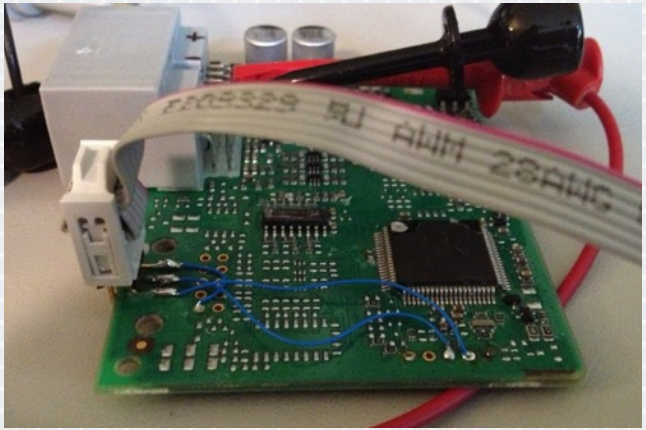
- Bus Blaster (open source)
  - http://dangerousprototypes.com/docs/Bus_Blaster
- SEGGER J-Link
  - www.segger.com/debug-probes.html
- H-JTAG
  - www.hjtag.com/en
- RIFF Box
  - www.jtagbox.com
- Many Others
  - http://openocd.sourceforge.net/doc/html/Debug-Adapter-Hardware.html

Debug Tools: Example

- Ford Electronic Control Units (ECUs) (2013)
  - For Charlie Miller & Chris Valasek
  - Complete firmware extraction to help understand typical CAN traffic/ functionality
  - http://illmatics.com/car_hacking.pdf
  - Used standard, off-the-shelf development tools
    - Freescale CodeWarrior for S12(X) v5.1 + P&E Multilink USB Rev. C

Debug Tools: Example 2





Memory

Auto | Logical

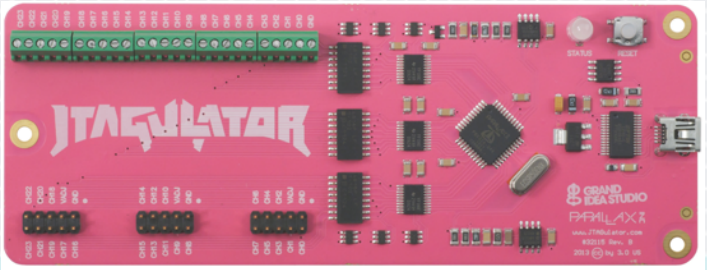
```
000C10'L 41 4C 38 54 2D 31 35 4B  38 36 36 2D 43 46 41 41  AL8T-15K866-CFAA
000C20'L 35 54 2D 31 34 43 32 34  34 2D 43 41 00 00 00 00  5T-14C244-CA....
000C30'L 3F C1 3F 3F 3F 3F 3F 3F  3F 35 3F 3F 3F 3F 3F 3F  ?.???????5??????
000C40'L 3F 3F 3F 3F 3F 3F 3F 3F  3F 3F 3F 3F 3F 3F 3F 3F  ????????????????
000C50'L E7 39 BD EF 7A B4 0E 25  CD EF 7B E7 1F FF FF F8  .9..z..%..{.....
000C60'L CD EF 7B E7 1F FF FF F8  3F 3F 3F 3F 3F 3F 3F 3C  ..{.....???????<
000C70'L EF 7B BC E7 37 9C 1E B8  EF 7B BC E7 37 9C 1E B8  .{..7....{..7...
000C80'L 3F 3F 3F 00 27 3C 00 00  00 00 00 00 00 3F 3F 00  ???.'<.......??.
000C90'L 50 DC 00 3F 1E 3F 3A C0  01 0C 30 33 2D 30 35 2D  P..?.?:...03-05-
000CA0'L 31 38 2D 32 30 30 39 DD  3F 3F 3F 3F 3F 41 4C 38  18-2009.?????AL8
000CB0'L 54 2D 31 34 43 36 34 37  2D 4D 43 01 3F 3F 3F 3F  T-14C647-MC.????
000CC0'L 45 FF FF FF FF FF FF FF  FF DD 23 FF FF C1 55 00  E.........#...U.
000CD0'L FF 9B 52 14 01 9B 54 13  03 FF FF FF 01 FF FF FF  ..R...T.........
000CE0'L 01 FF FF FF 01 FF FF FF  01 FF FF FF 01 FF FF FF  ................
000CF0'L 01 FF FF FF 01 FF FF FF  01 FF FF FF 01 FF FF FF  ................
000D00'L 01 FF FF FF 01 FF FF FF  01 FF FF FF 01 FF FF FF  ................
```

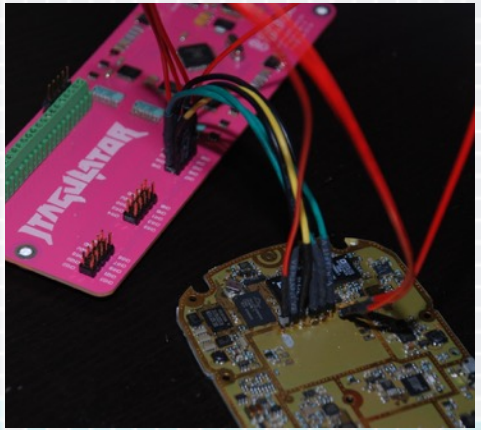
Command

```
RUNNING

in>s
STOPPING
HALTED

in>save 0x800..0xffff dump3.s19
RUNNING

in>
```

JTAGulator

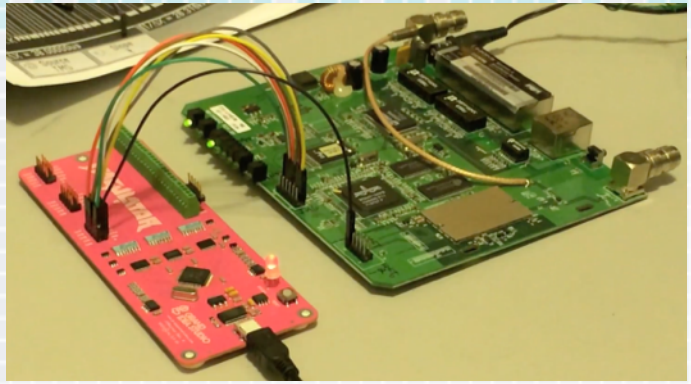
- Joe Grand
- Assisted discovery of on-chip debug interfaces (JTAG & UART)
- Supports up to 24 connections to unknown points on target circuit board, adjustable target voltage (1.2V-3.3V), input protection, firmware upgradable
- www.jtagulator.com





JTAGulator: Example

- Linksys WRT54G v2
  - Broadcom BCM4712
  - IDCODE = 0x1471217F

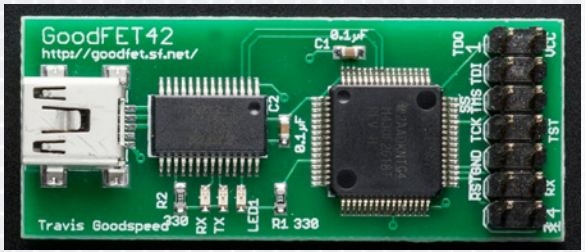


```
U   Identify UART pinout
P   UART passthrough

General Commands:
V   Set target system voltage (1.2V to 3.3V)
R   Read all channels (input)
W   Write all channels (output)
J   Display version information
H   Display available commands
:b
Enter number of channels to use (4 - 24): 6
Ensure connections are on CH5..CH0.
Possible permutations: 360
Press spacebar to begin (any other key to abort)...
JTAGulating! Press any key to abort.....................
TDI: 3
TDO: 4
TCK: 1
TMS: 5
TRST#: 2
Number of devices detected: 1
.............
BYPASS scan complete!
:_
```

```
U   Identify UART pinout
P   UART passthrough

General Commands:
V   Set target system voltage (1.2V to 3.3V)
R   Read all channels (input)
W   Write all channels (output)
J   Display version information
H   Display available commands
:d
IDI not needed to retrieve Device ID.
Enter new TDO pin [0]: 4
Enter new TCK pin [0]: 1
Enter new TMS pin [0]: 5
Enter number of devices in JTAG chain [0]: 1
All other channels set to output HIGH.

Device ID: 0001 0100011100010010 00010111111 1 (0x1471217F)
-> Manufacturer ID: 0x0BF
-> Part Number: 0x4712
-> Version: 0x1

IDCODE listing complete!
:_
```

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



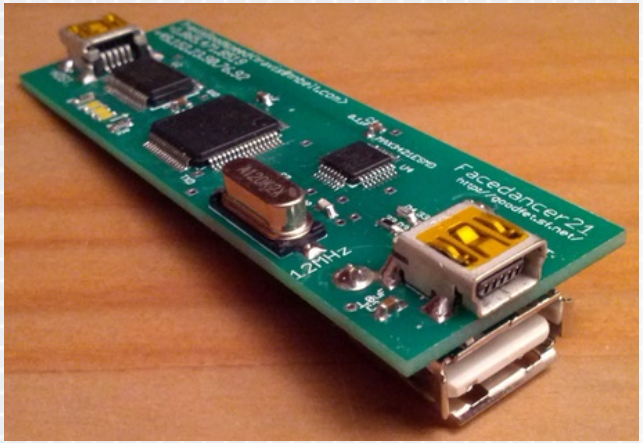
GoodFET: Example

- Travis Goodspeed & Michael Ossmann
- Reprogram firmware in Chipcon C1110 MCU (8051)
- Change IM-Me from $16 toy to a pocket spectrum analyzer
- https://jbremnant.wordpress.com/2010/11/23/flashing-ucs-with-goodfet/


```
$ goodfet.cc flash specan.hex
Flashing specan.hex
Buffering 0000 toward 000000
Buffering 0100 toward 000000
Buffering 0200 toward 000000
Buffering 0300 toward 000000
Flashing buffer to 0x000000
Flashed page at 000000
...
```

Facedancer

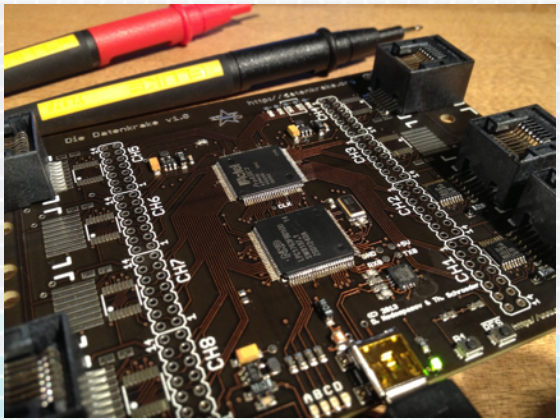
- Travis Goodspeed
- Emulate USB devices for host-based testing/fuzzing/analysis
  - http://goodfet.sourceforge.net/hardware/facedancer21/




```
# 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
```

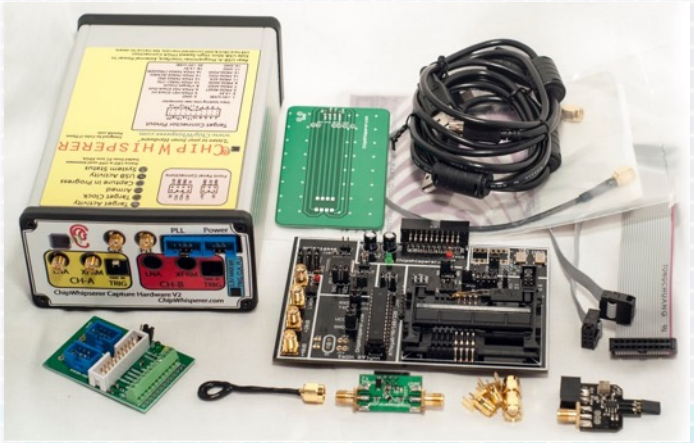
Die Datenkrake

- 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
- www.datenkrake.org



ChipWhisperer

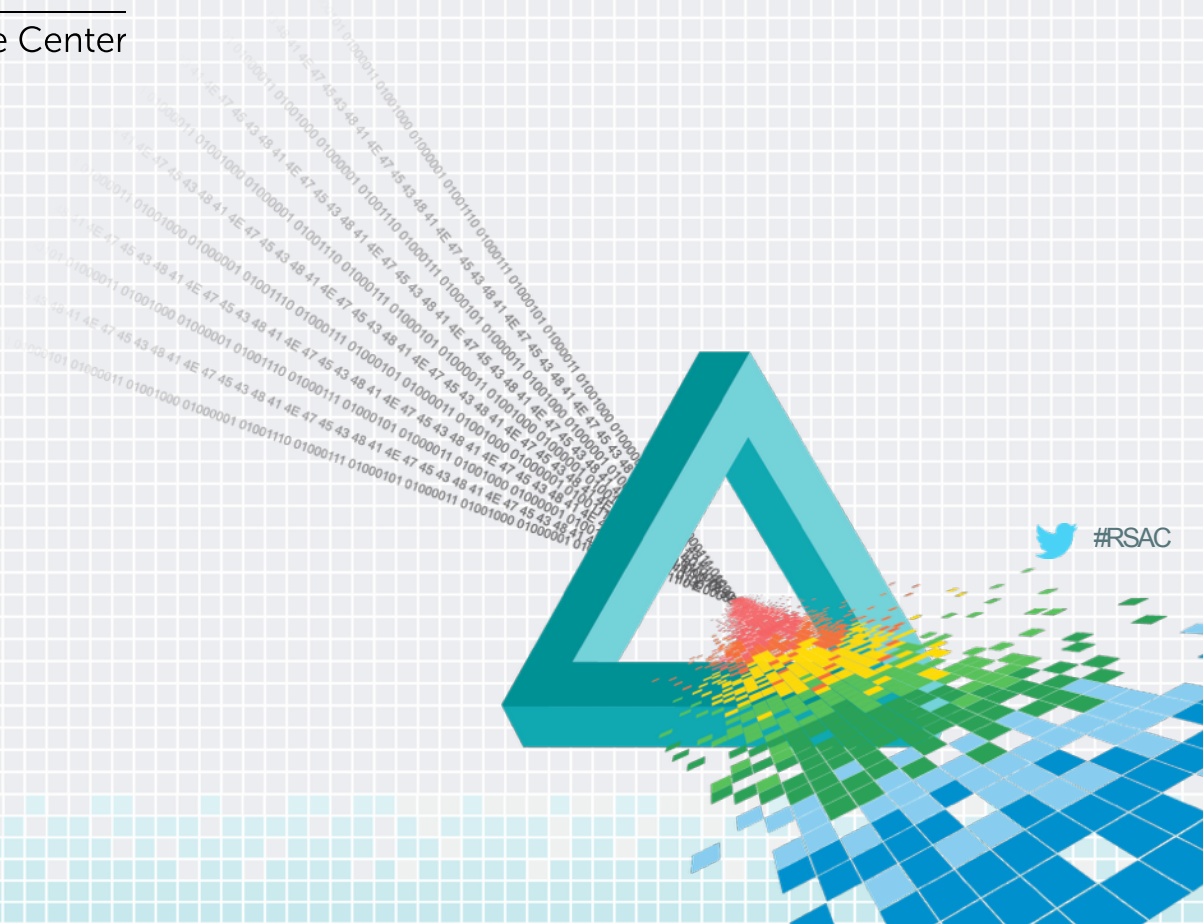
- Colin O'Flynn
- Collection of open source HW/SW tools for side channel, timing, and glitching attacks
- Supports AES-128/256 key extraction via EM/power analysis
- www.chipwhisperer.com



RSAConference2015

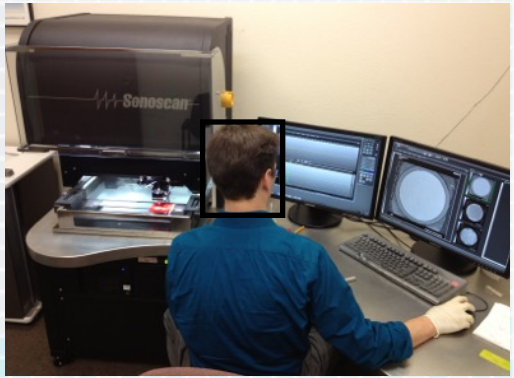
San Francisco | April 20-24 | Moscone Center

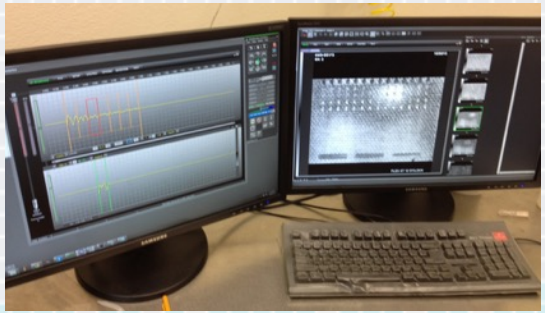
Imaging



Acoustic Microscopy

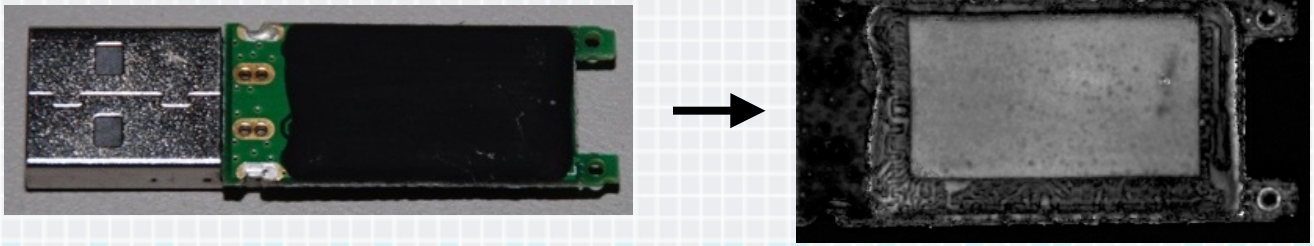
- Target placed into bath of DI water or alcohol
  - Serves as liquid coupling medium to transfer sound waves to target
- Ultrasound emitted into target (15-300MHz)
- Return echoes are captured (reflection)
- Transmission through the target is measured (thru scan)





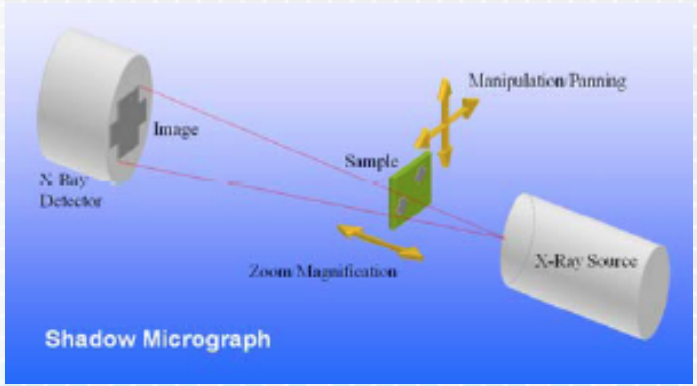
Acoustic Microscopy 2

- 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)

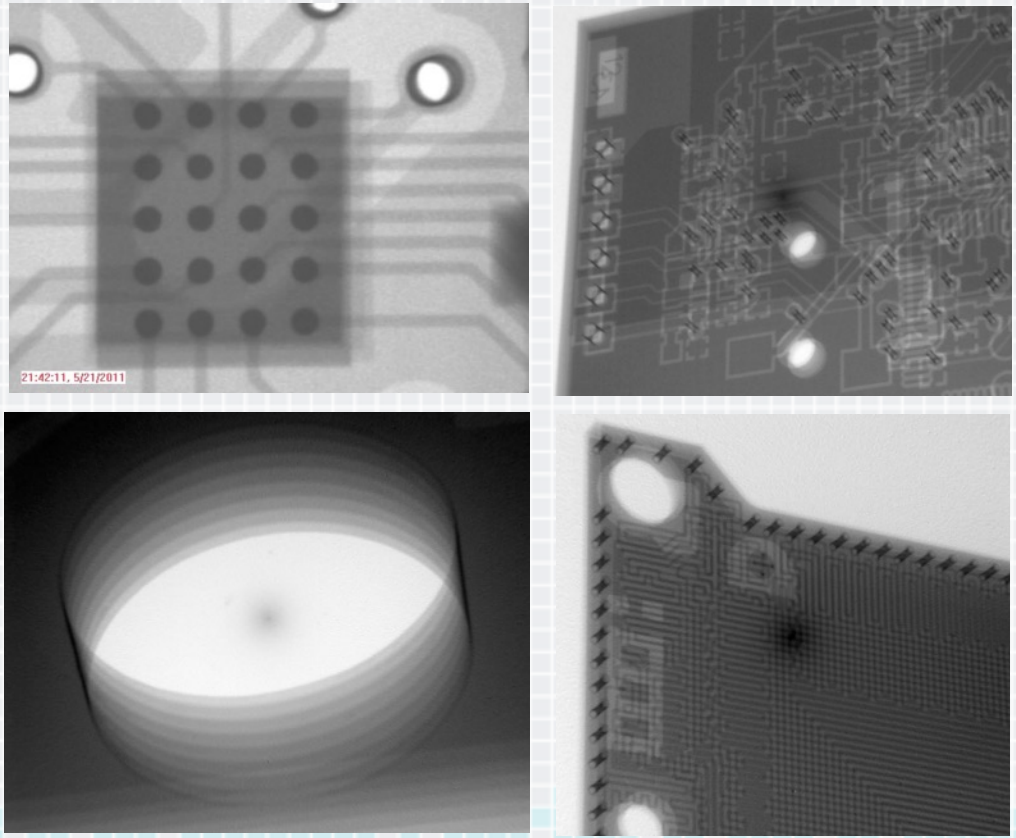
- X-rays passed through target and received on detector
  - All materials absorb radiation differently depending on density, atomic number, and thickness
- Provides a composite image of all layers in target



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

X-Ray (2D): Examples

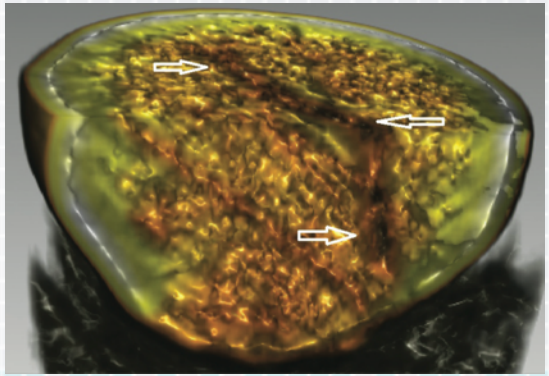


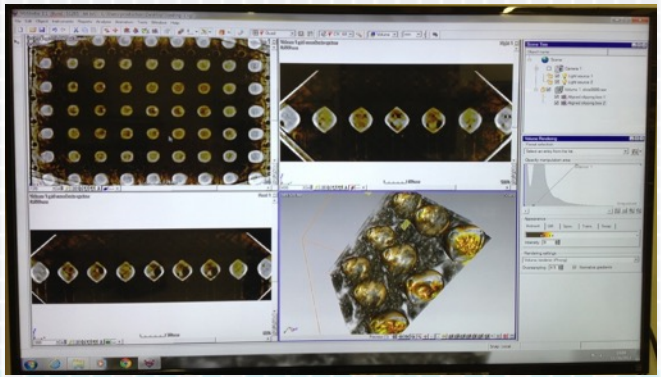
X-Ray (3D/CT)

- 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
  - Post-processing results in 2D slices that can be viewed in any plane (X, Y, Z)
  - Can be manipulated with 3D modeling software

X-Ray (3D/CT) 2

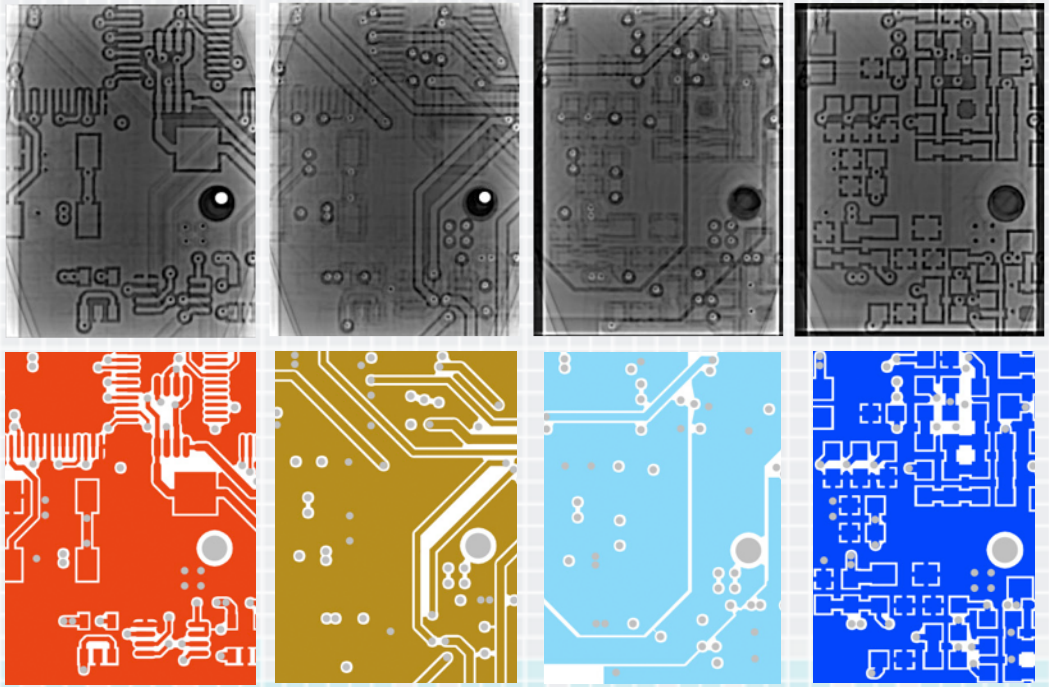
- Typically used for complex inspection and failure analysis of PCBs, component packaging, solder ball/joint quality
- We can use it to extract individual layers of a PCB
  - Results may vary based on layer count, inter-layer thickness, copper weight, substrate composition





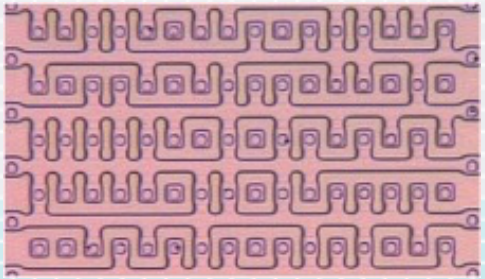
X-Ray (3D/CT): Example

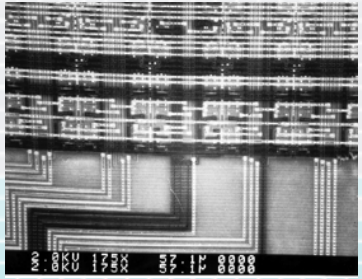
- PCB layer extraction, www.grandideastudio.com/portfolio/pcbdt/



Scanning Electron Microscope

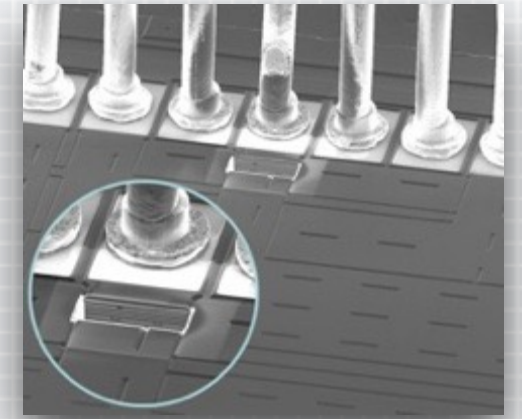
- Uses electrons instead of light to form an image
  - Wide range of magnifications, better quality than optical microscope
- Provides an entire chip-level and gate-level view of the device
  - May need to remove other layers before access to gate structures
- Voltage contrast microscopy
  - Gate charges and voltage levels shown as brightness variations
  - Useful for failure analysis/comparisons and signal/bus monitoring





FIB (Focused Ion Beam)

- Send a focused stream of ions onto the surface of the chip
- Beam current/velocity and optional use of gas/vapor changes the function:
  - Imaging
  - Cutting
  - Deposition



Now What?

Now What?

- Create a hardware hacking lab (if you haven't already)
- Keep an eye out for new tools by hackers and industry
- Collaborate with others who may have complementary skills/tools
- Use these tools to validate your product's security or to better understand attack techniques

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Questions?