Disassembling and Patching Hardware

Recognizing Circuit Board Layout Motifs
and Basic Circuit Mod Techniques

bunnie
bunnie:studios LLC

Agenda

- Hardware Reverser’s Toolkit
- Identifying basic circuit primitives
- Translation to schematics
- Circuit board motifs
- Basic circuit patching techniques
- Circuit patching demo
- Q&A

Hardware Reverser's Toolkit

- Compare to Software Reverser Cycle:
  - Static Analysis: IDA
  - Runtime Analysis: SoftICE, OllyDbg
  - Patch: HexEdit, HackMan, HexWorkshop etc.
- Hardware Cycle:
  - Static Analysis: Eyeballing + continuity tester
  - Runtime Analysis: Oscilloscope, Logic Analyzer
  - Patch: Solder + wire; drop-in “active” hardware patchers (e.g. modchips, man-in-middle attacks)

Specific Sub-topics

- Static Analysis (“IDA” equivalent)
  - How to identify components
  - How to extract connectivity
  - Schematic conventions for recording extracted results
  - High-level motifs (“FLIRT” signatures) / saving time and effort
- Patching (“HexEdit” equivalent)
  - Basic techniques for soldering: theory and practice
  - Basic techniques for desoldering
  - Techniques for tack-soldering to circuit boards

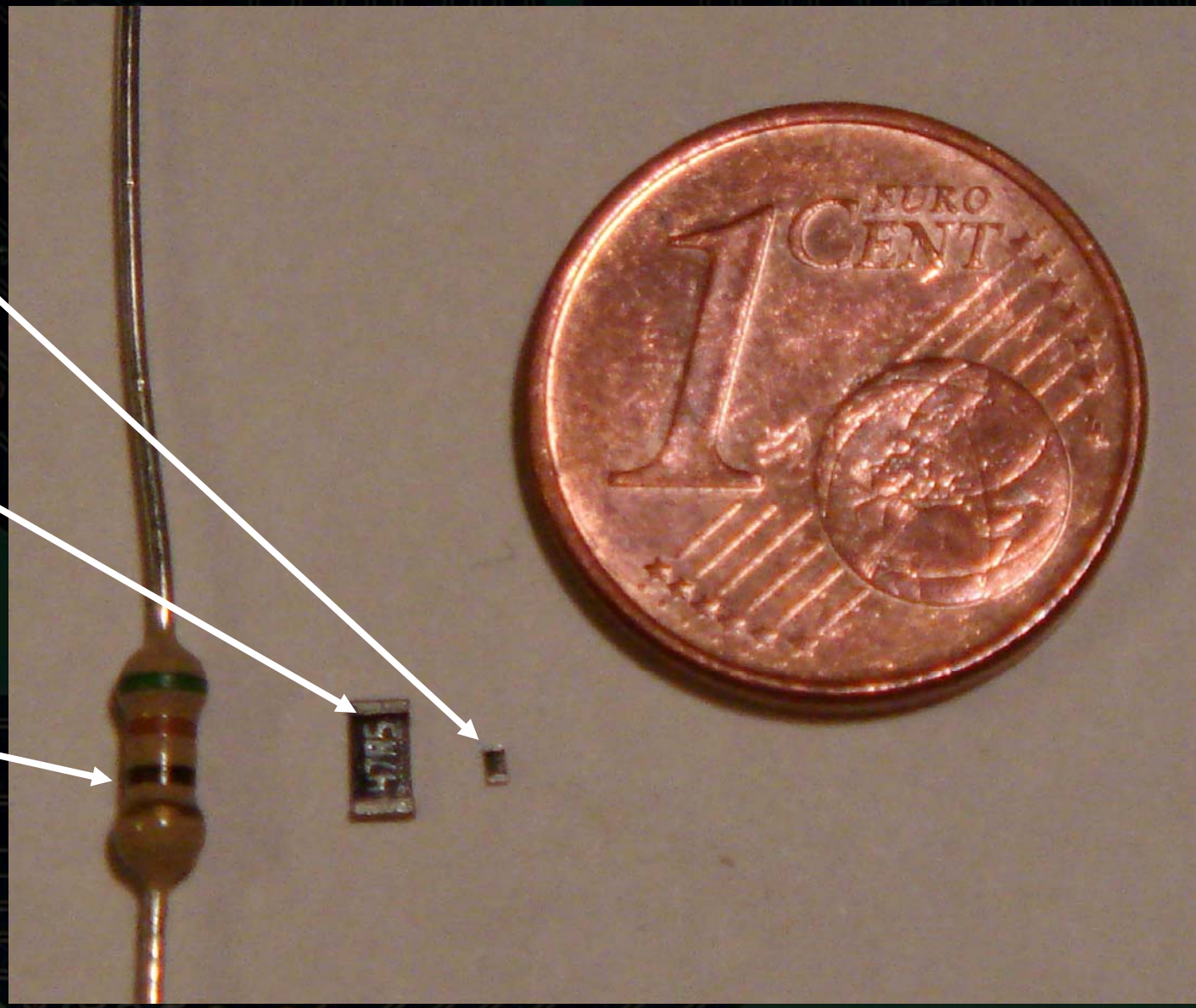
Circuit Primitives

- Passive components
  - Resistors
  - Capacitors
  - Inductors
  - Diodes
- Active components
  - Transistors
  - ICs
    - DIP
    - SOIC / TSSOP / QFP
    - BGA
    - CSP
- Misc common/important components

Resistors

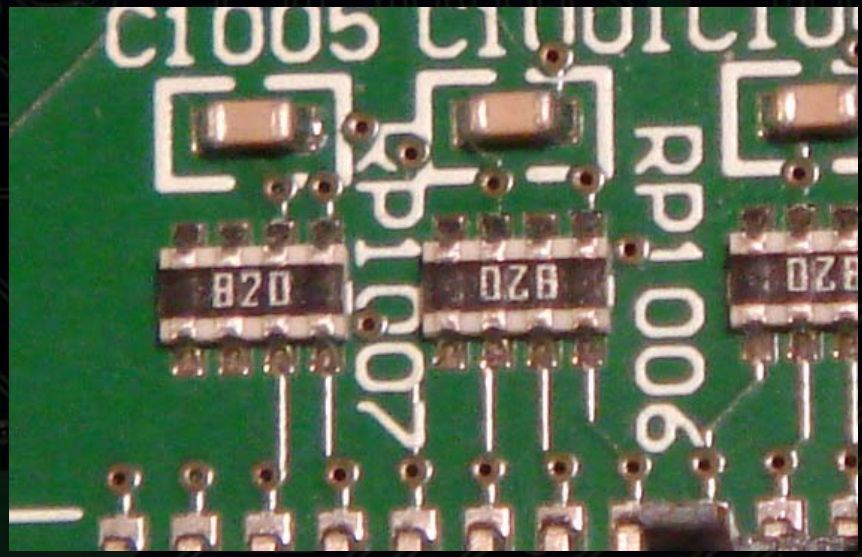
- Used to remove energy from a circuit, or to introduce a controlled amount of energy
  - “Wants to heat up”
- Energy removal rate (e.g., Power) is equal to current through resistor times voltage dropped
  - Simplest Current to Voltage converter
- Common applications:
  - Dissipating excess wavefront energy in high-speed transmission lines
  - Setting voltages on high-impedance nodes (e.g., pullups/pulldowns for strapping options)
  - Pullups on tri-state busses (e.g., I2C, PS2 pullups)
  - Setting gain or dividing voltages in analog circuits
- Relatively few varieties to identify

Resistors


0402 surface-mount
1206 surface-mount
1/4W through-hole
EURO
CENT

Resistors

- Can be in array form



- Or screen-printed

Capacitors

- Used to store energy in the form of *voltage potential* for time-delayed release
  - “Wants to maintain a constant voltage”
- Energy storage capacity is proportional to capacitance times voltage rating
- Common applications:
  - Smoothing out power supply glitches
  - Voltage conversion (boostrapping, charge pumping, switching regulation)
  - Coupling analog signals with different operating points (from Hz to GHz)
  - Participant in complex filter implementation
- Many, many complex varieties to identify

Capacitors

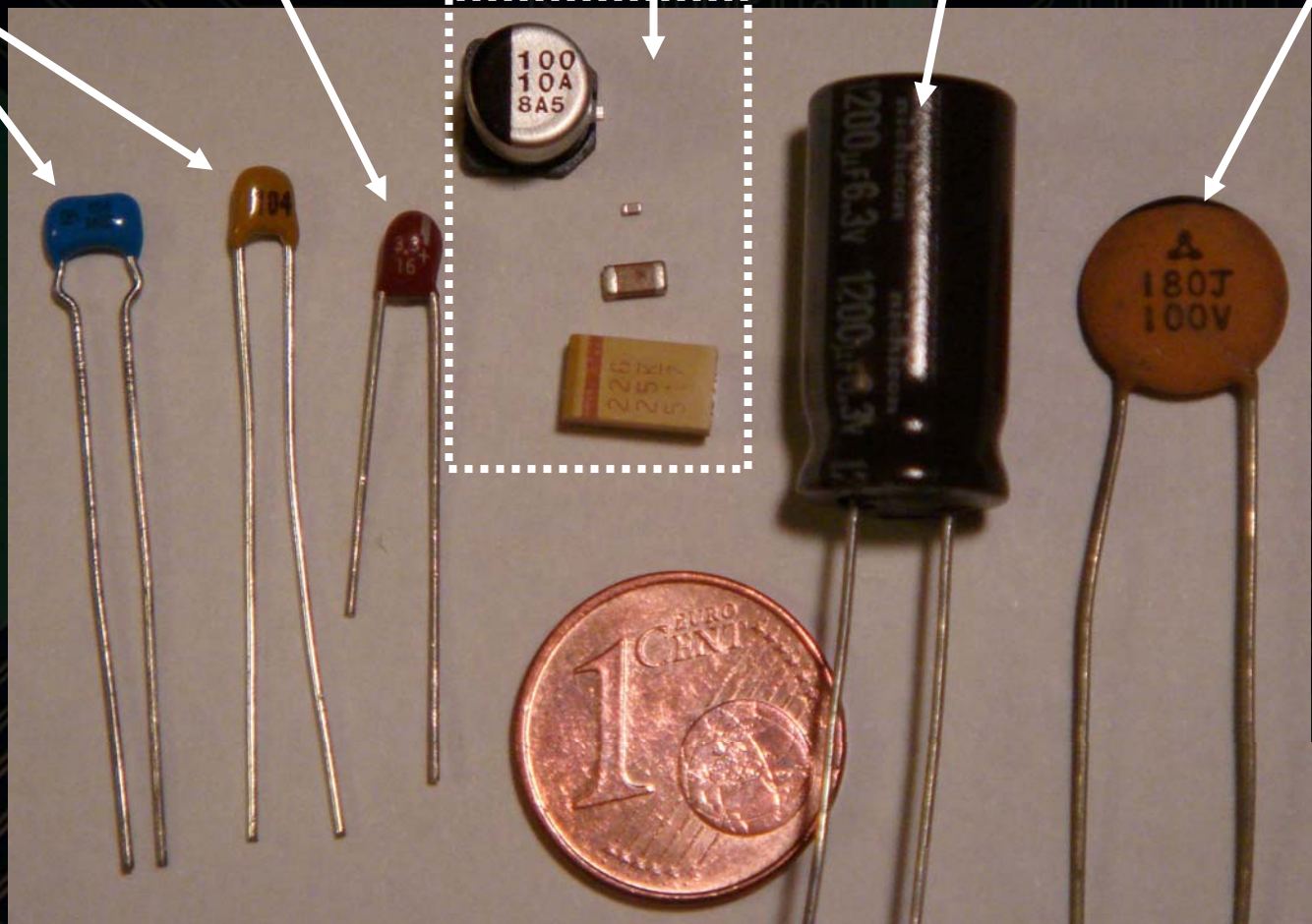
Ceramic radial (0.1 uF)

Tantalum radial (3.3 uF)

SMT (next foil)

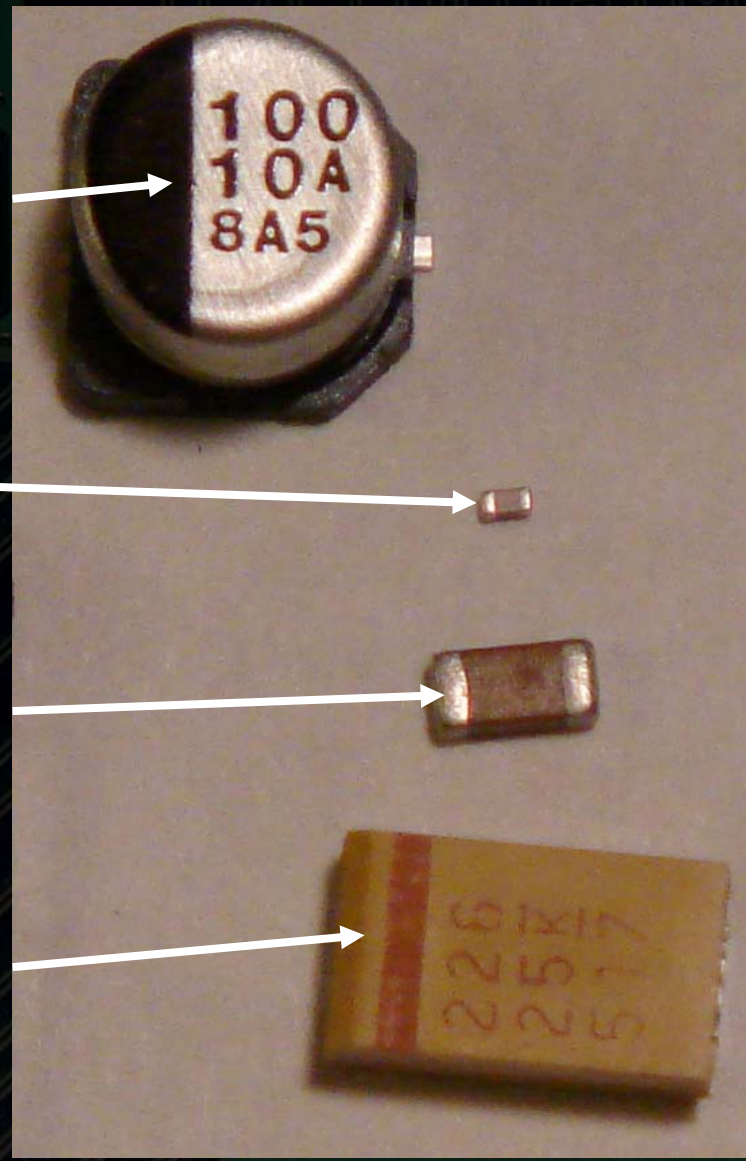
Electrolytic radial (1200 uF)

Ceramic radial (0.000018 uF)



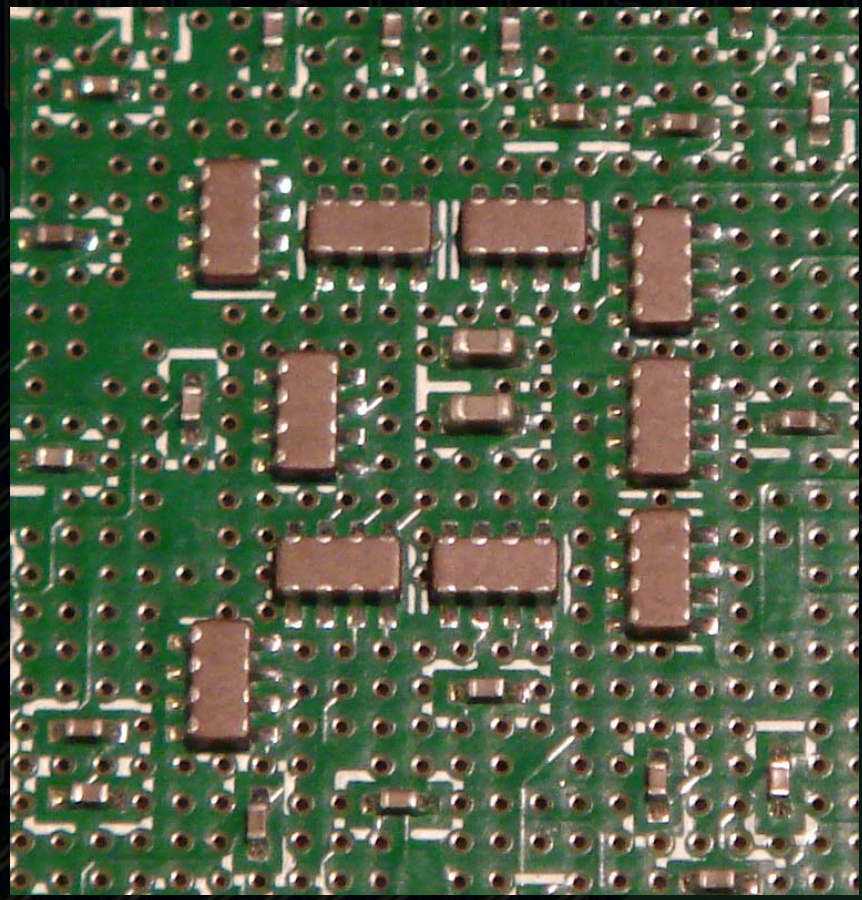
Capacitors

- Material choice relates to application
  - Aluminum electrolytics for bulk, low quality
  - Ceramic for high quality, low capacitance
  - Tantalum for good quality, high capacitance



Capactiors

- Can be in array form
  - Indicative of high performance circuitry nearby



Inductors

- Used to store energy in the form of *magnetic flux* for time-delayed release
  - “Wants to maintain a constant current”
- Energy storage proportional to coil winding density and magnetic core capability
- Coupled flux implementations used to convert AC voltages (e.g. transformers)
- Common applications:
  - Counterbalance to capacitor in power conversion
  - Blocking high frequency noise (EMI filtering)
  - Participant in complex filter implementation

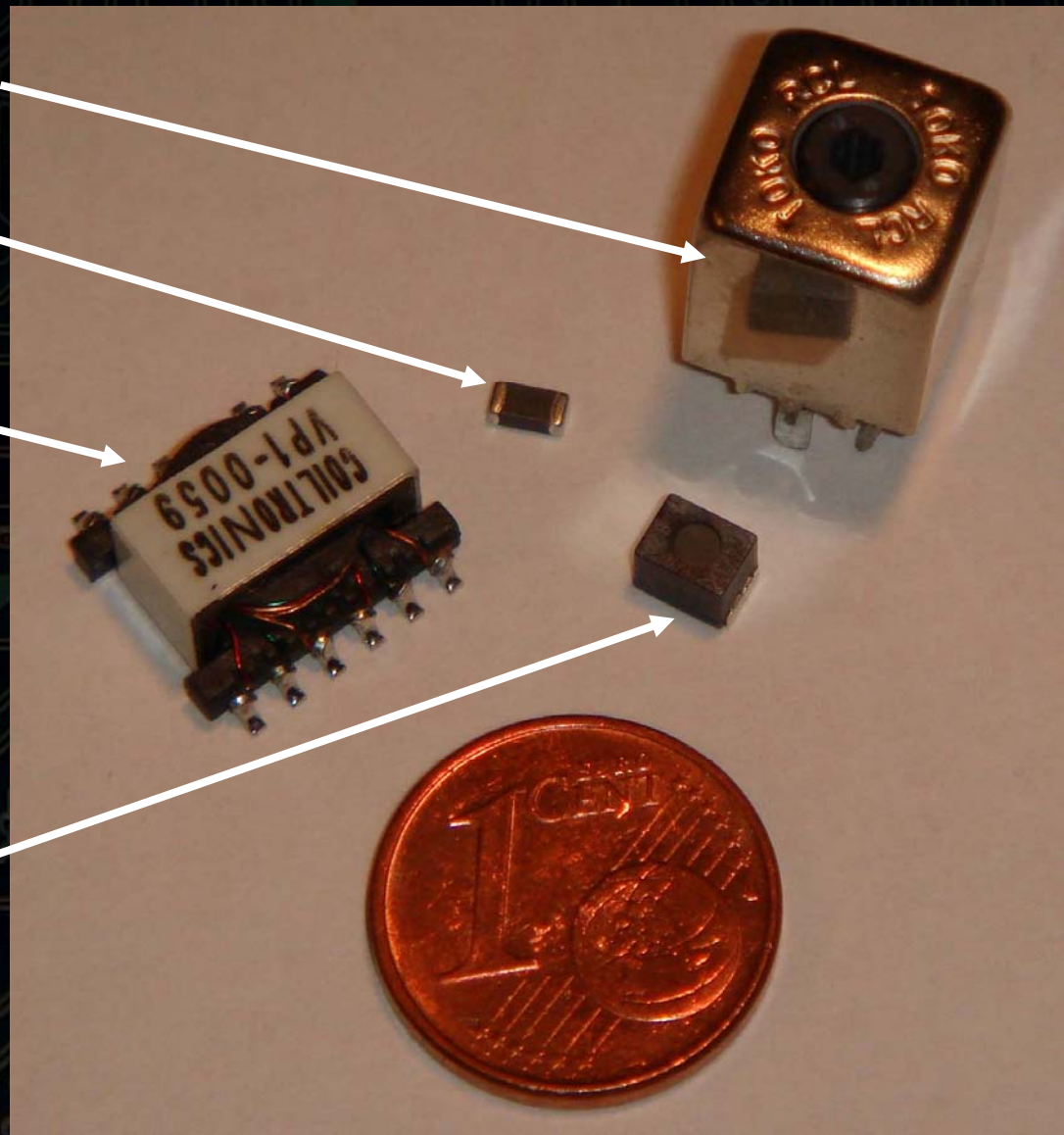
Inductors

Adjustable air-core shielded inductor

Ferrite bead

Unshielded transformer

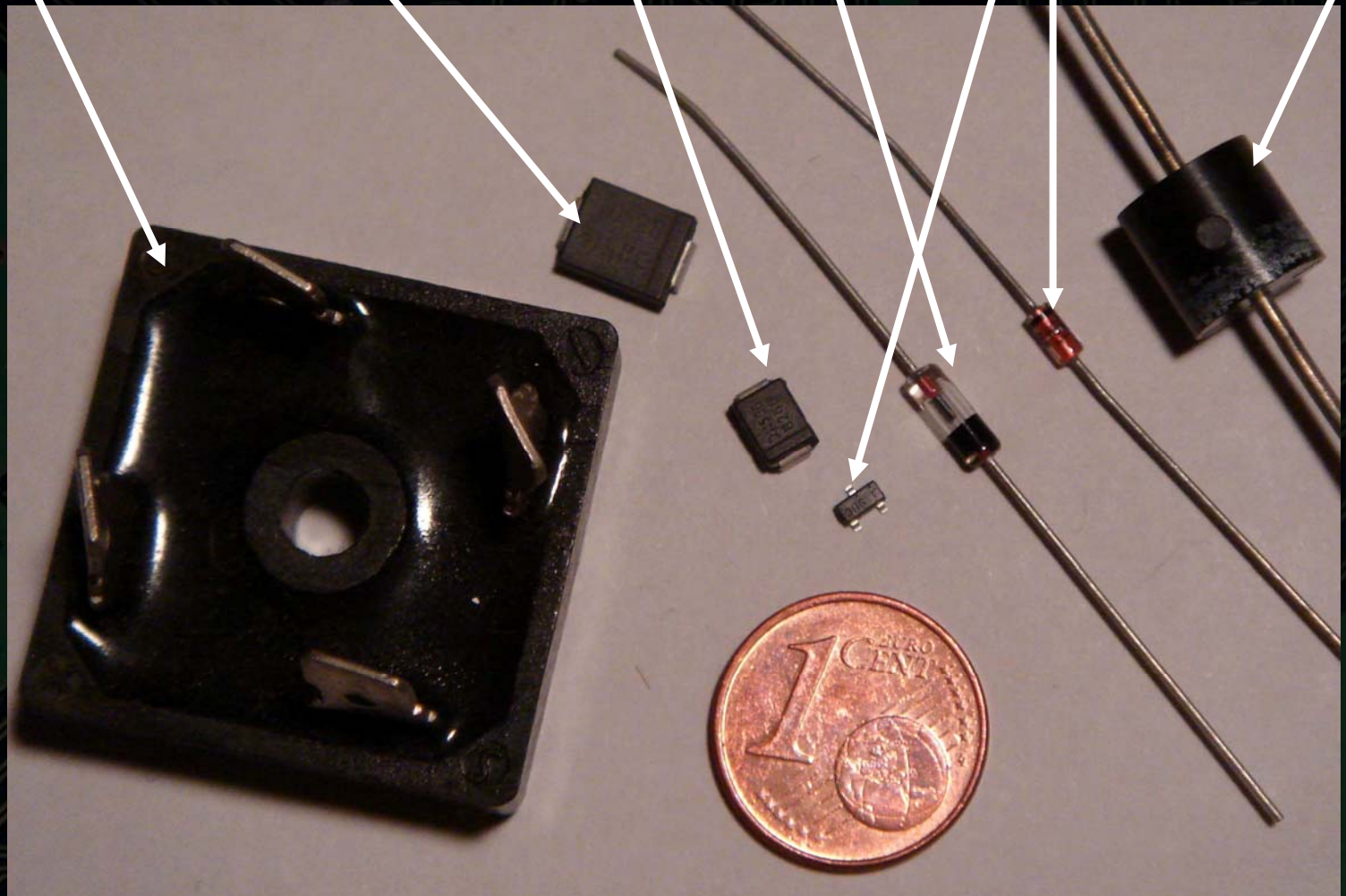
Shielded ferrite core inductor



Diodes

- Used to restrict the flow of current to a single direction (“rectification”)
- “Wants to make current flow in one way”
- Despite being a semiconductor device, it is classified as “passive” because it can provide no gain
- Common applications
  - Rectification of AC to DC
  - An essential component of switching power converters
  - ESD (static electricity) protection
  - Circuit protection against inverted batteries, power supplies
  - (More rare) overshoot/undershoot termination clamp

Diodes


Bridge rectifier
“SMC” schottky
“SMA” schottky
Small signal germanium
Small signal silicon
Power rectifier
1 EURO CENT

3-Terminal Diode??

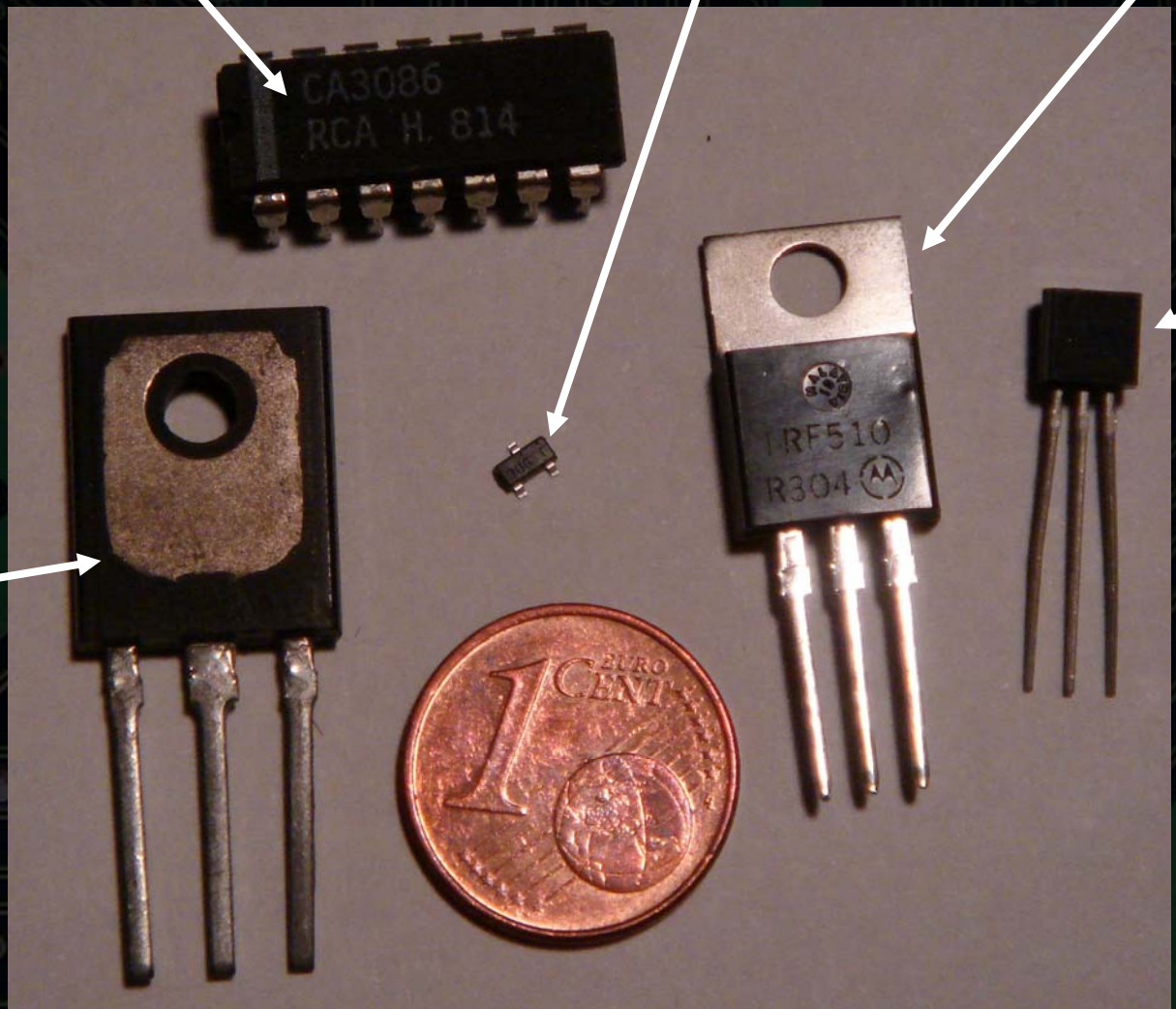
- Note that one diode in previous foil has three terminals
  - Small surface-mount diodes may include a redundant 3rd terminal to assist with assembly
  - Sometimes two diodes are packaged like this, with a common anode or cathode
  - Must rely on circuit board layout cues to determine function!

“SOT-23” package

Transistors

- THE basic active circuit element
- Generically, a control terminal varies the conductance between two other terminals
  - Think of it as an electronically controlled “switch” or “amplifier”
  - Major varieties are BJT and FET
- Common discrete device applications
  - Element of a switching power supply
  - Power management (e.g. turning off stuff to conserve batteries)
  - Level shifting (typically for power management)
  - Antenna power amplifier (cell phone applications)
  - Use package type and board layout cues to determine function

Transistors



Quad matched transistor array

SOT-23 transistor

TO-220
power FET

TO-92 small
signal BJT

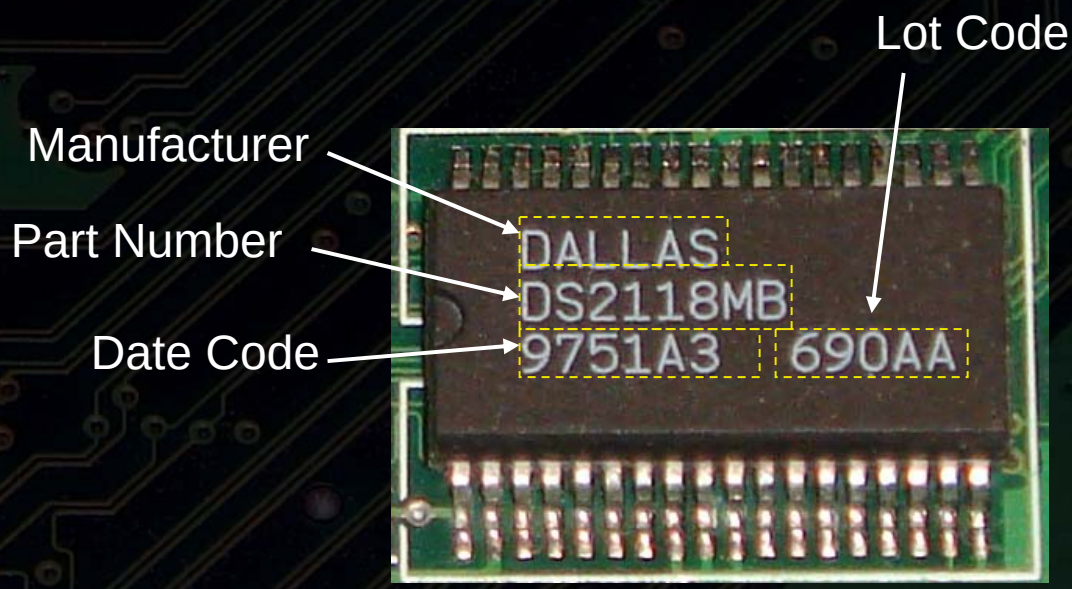
TO-247
Power BJT

Integrated Circuits

- Come in a huge variety of packages and functions
- Deduce part function from part number primarily

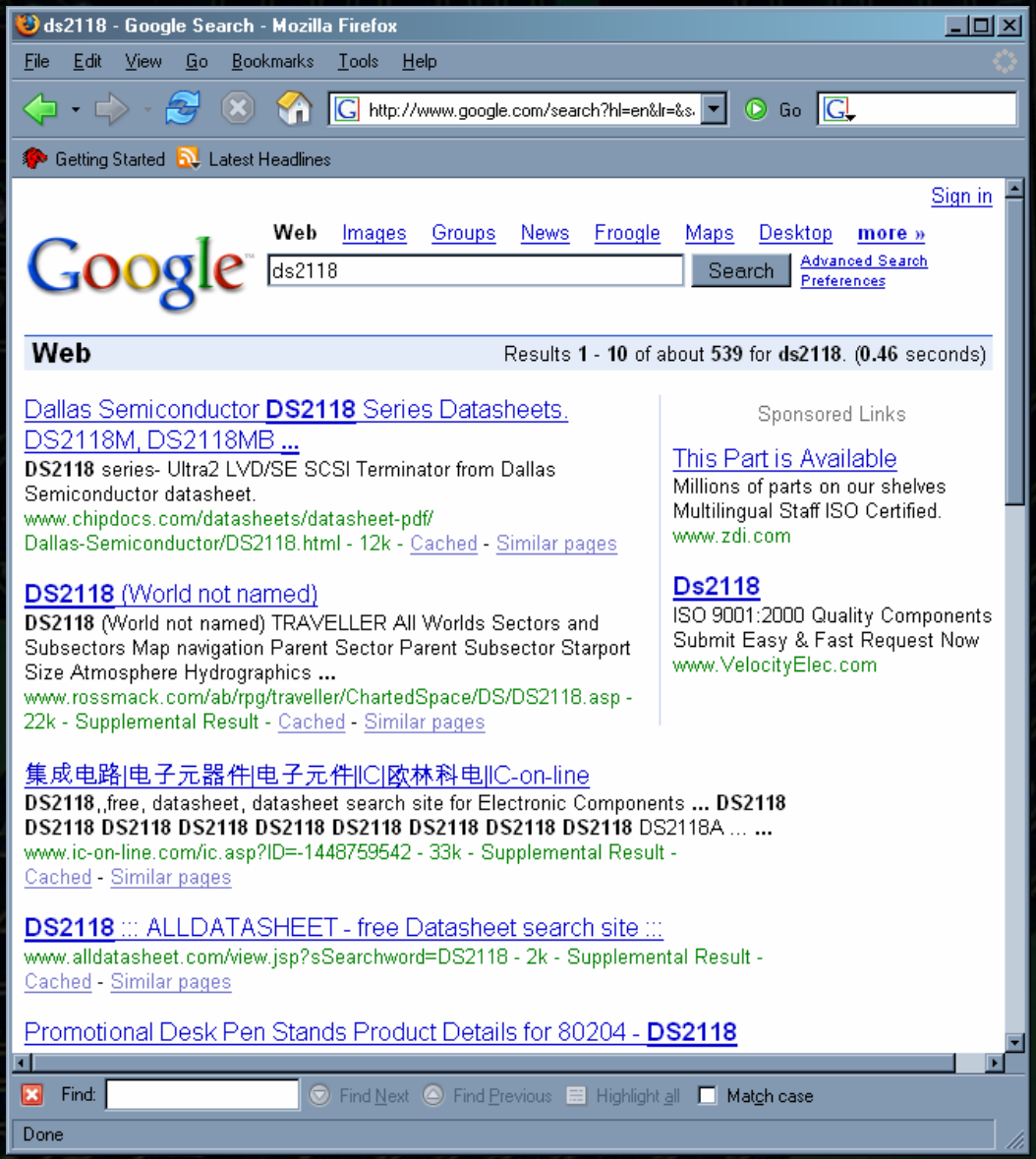
Reading Part Numbers

- Larger chips have full part numbers on them
  - Typically:
    - A manufacturer name or logo
    - A part number
    - A date code and a lot/stepping code



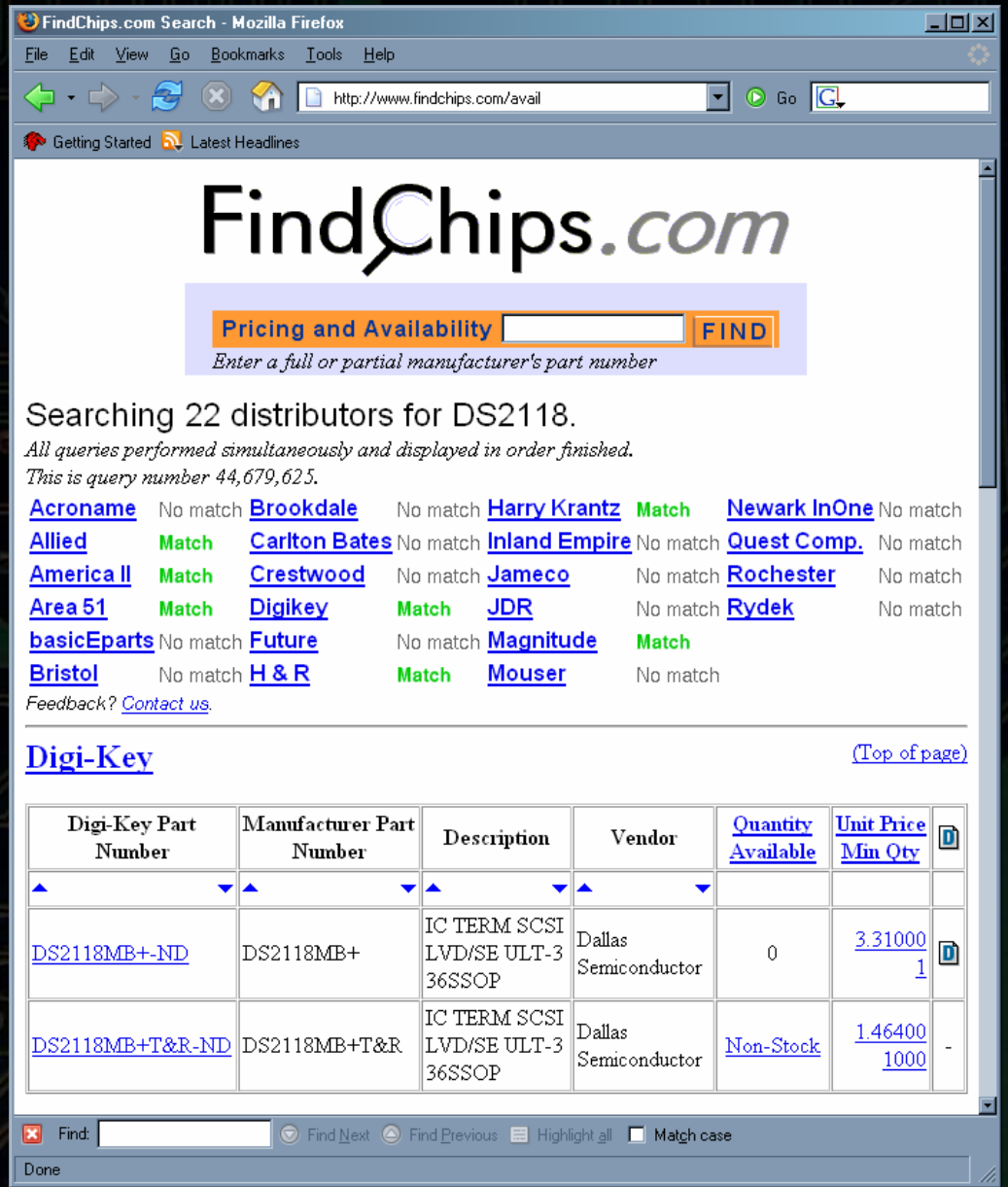
Looking Up Part Numbers

- Google:



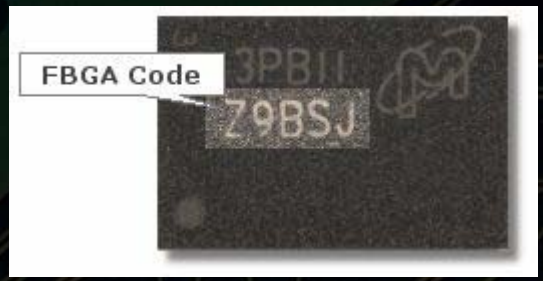
Looking Up Part Numbers

- Findchips.com:

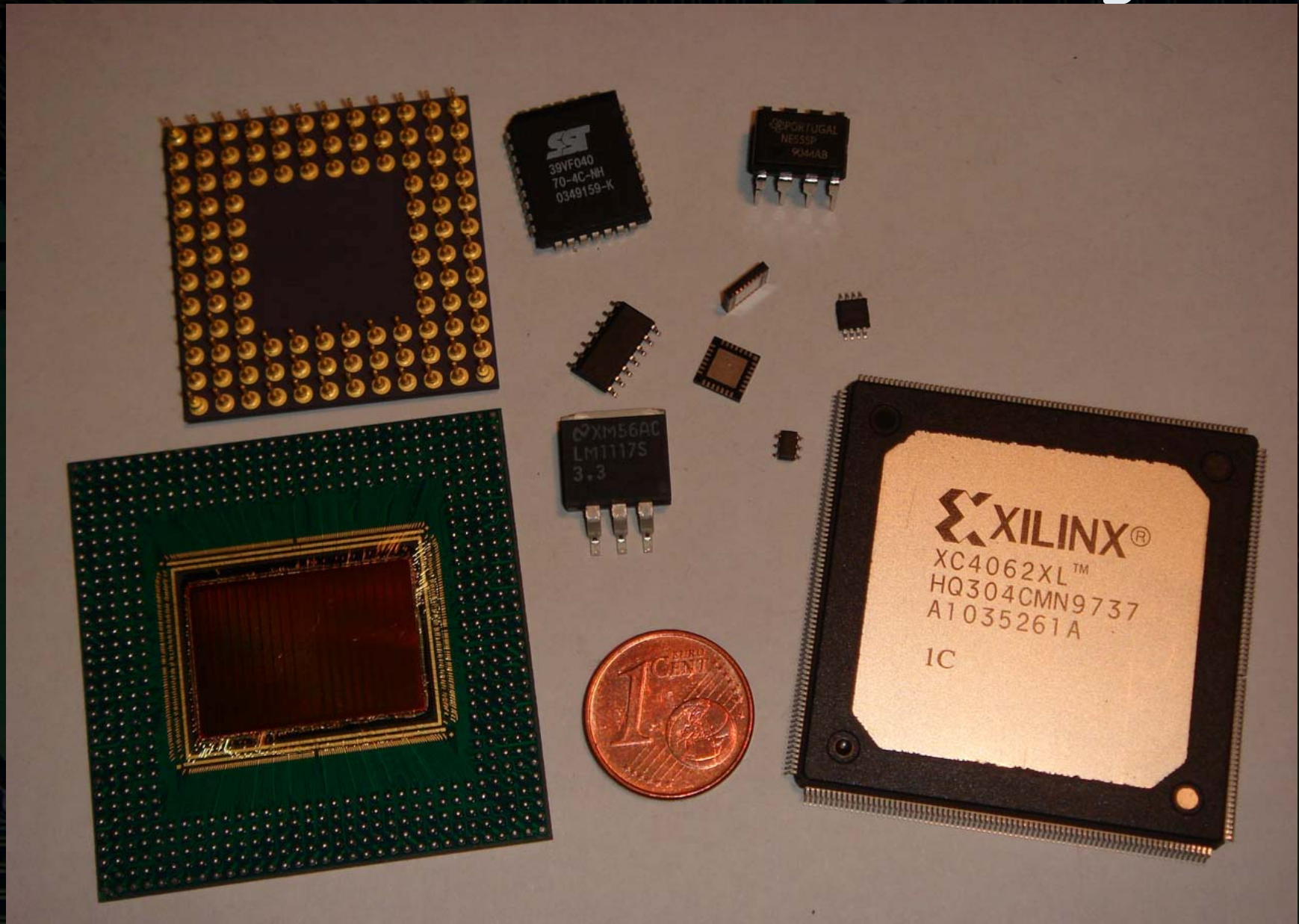


Strange Parts

- Small devices have abbreviated part numbers
  - BGA, SOT-XX parts lack the space to put full part numbers in
  - Abbreviation expanders available via manufacturer websites
  - SOT-XX parts can be very hard to decode (e.g. FDN306P from Fairchild is simply marked “306” and “F”)

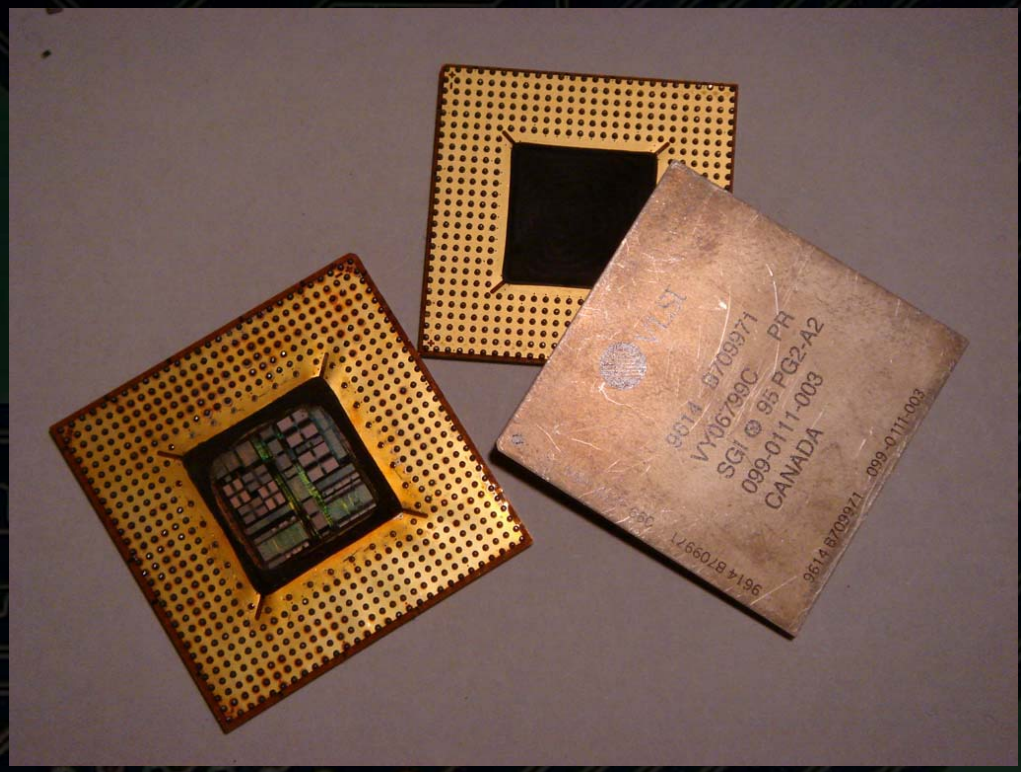


Some Common IC Packages



BGA Packages

- Ball Grid Array packages have fully concealed pin formations that can be very difficult to probe
  - Use connected traces and test points for probing

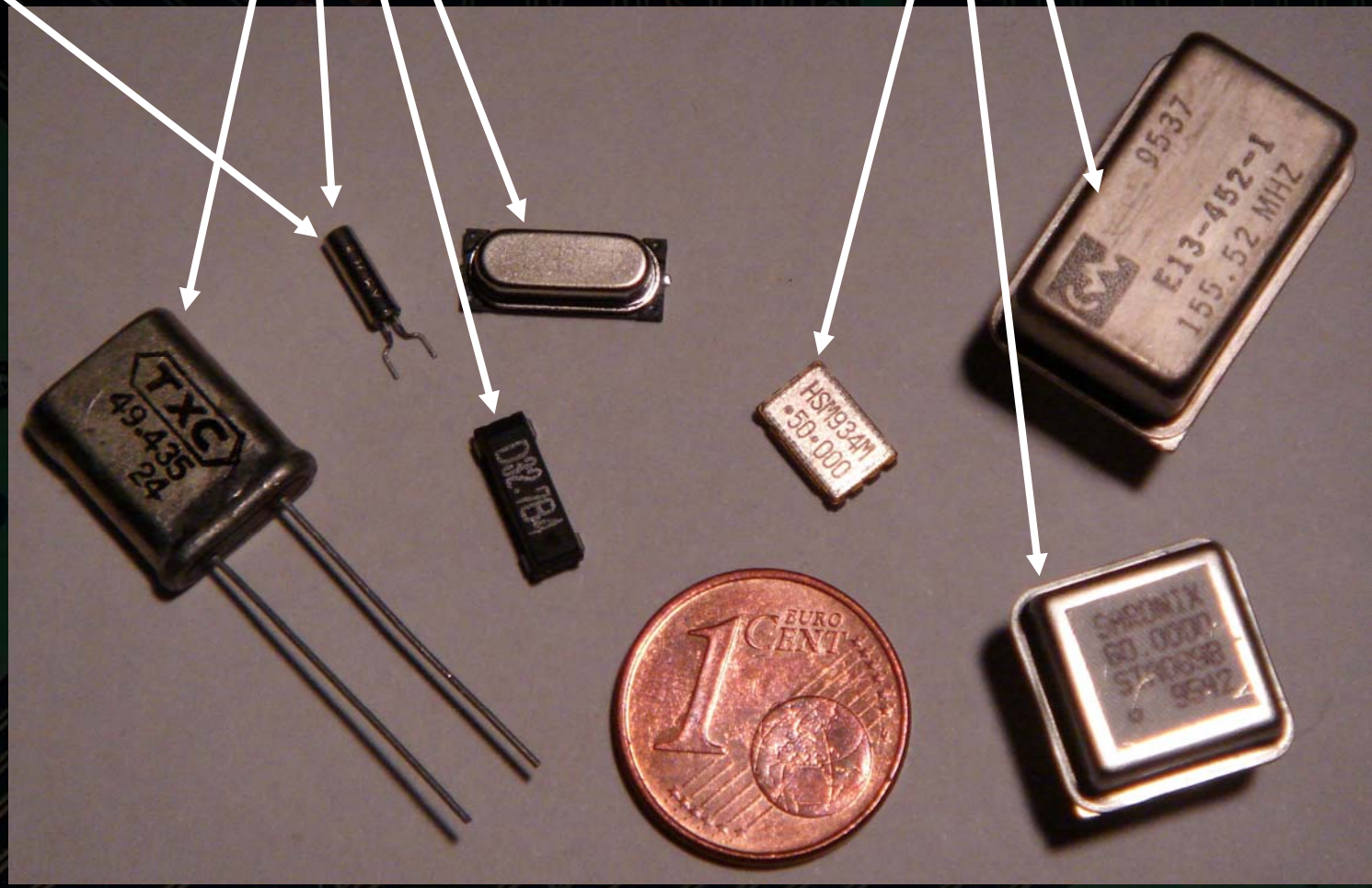


Miscellaneous

32.768 kHz
“watch crystal”

Simple crystals

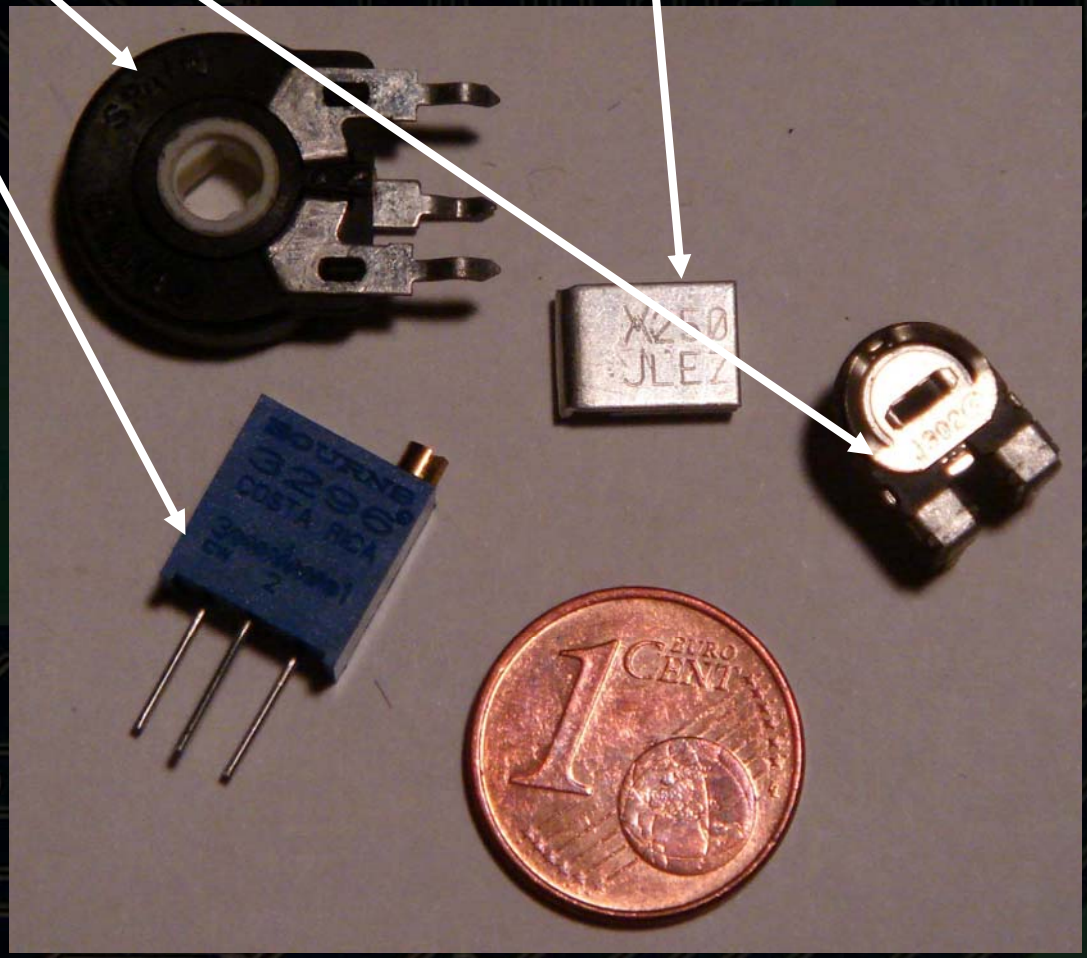
Integrated crystal + oscillators



Miscellaneous

Potentiometers

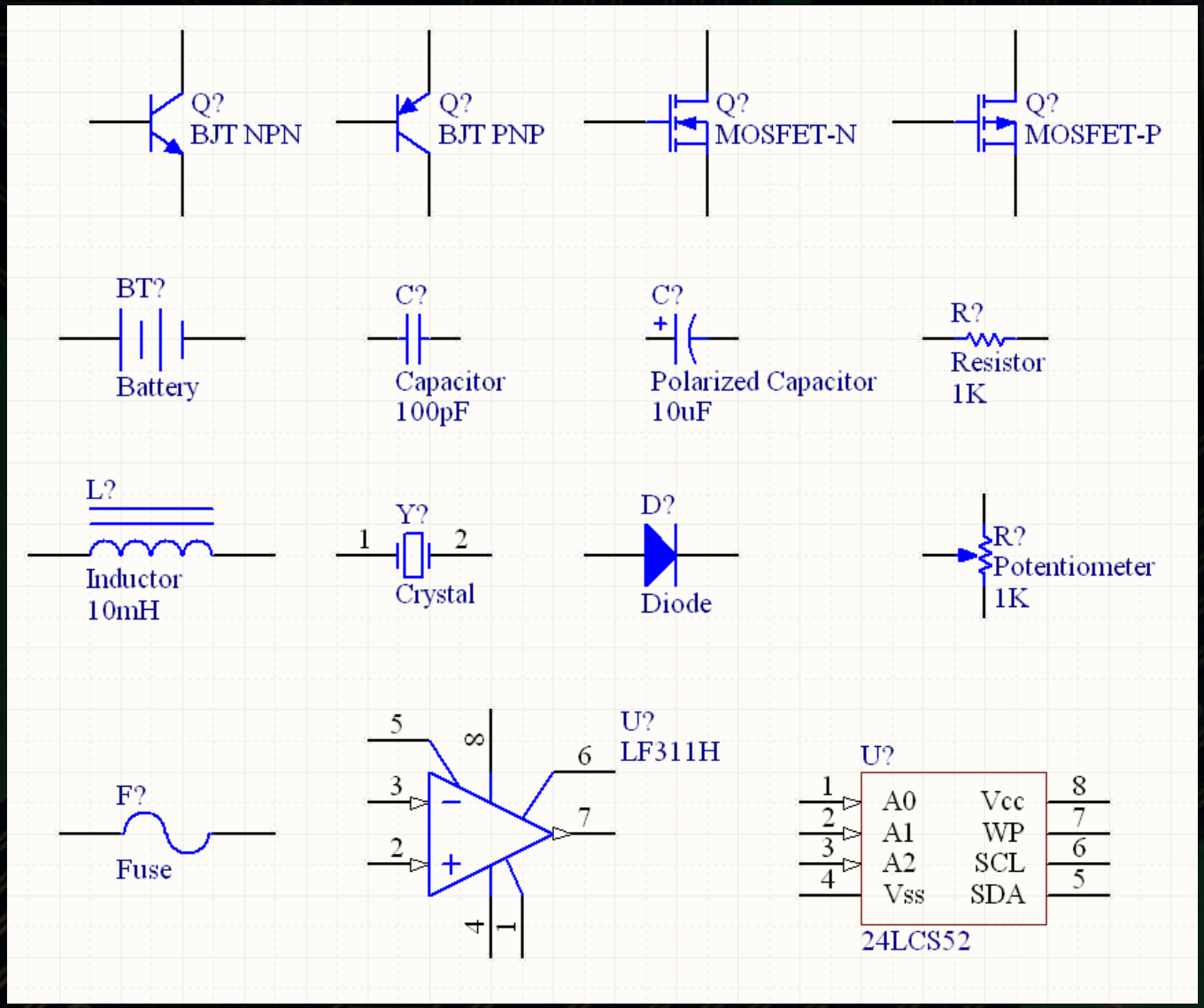
Resettable fuse



Schematics

- Logical representation of physical entities
- Facilitates circuit analysis and meaning extraction
- Common conventions are applied to enable better portability
  - Symbols
  - Reference designators
  - Flow and layout
  - Connect by name

Schematic Symbols



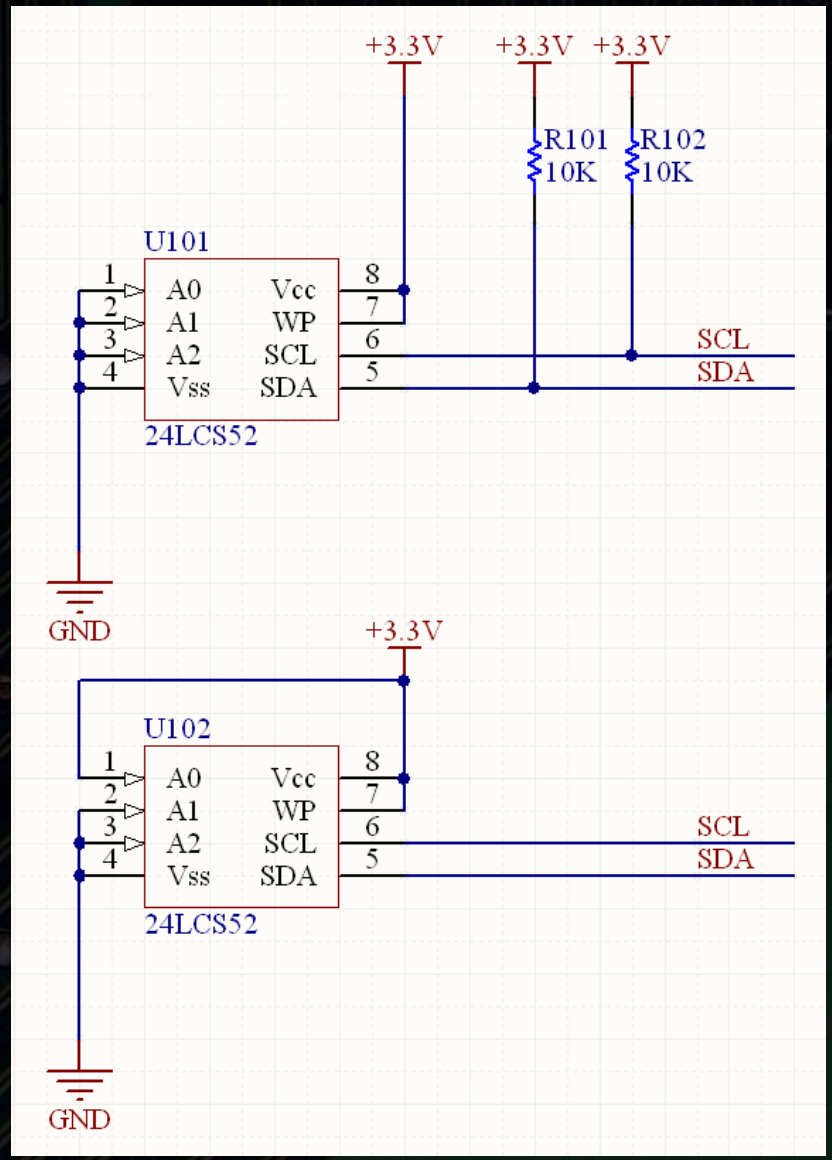
Reference Designators

- Reference designators are used to enumerate components for identification during assembly
- Syntax is typically <component mnemonic> | <unique sequence number>
  - Example: R100, C4, L102

Refdes	Component Type
B or BT	Battery
C	Capacitor
D	Diode
DS	LED or Lamp
E	Antenna
F	Fuse
J, JP, or P	Jumper or Connector
L	Inductor
LS or SP	Speaker
MK or M	Microphone
Q	Transistor
R	Resistor
S or SW	Switch
T	Transformer
U	Integrated circuit
V	Vacuum Tube
W	Wire Jumper
X or Y	Crystal or Resonator

Wire-by-Name

- Explicit wires are often omitted for clarity
  - “Wire by name” convention is applied
  - All nets of a common name are implicitly tied together



Flow and Layout

- Schematics generally follow a top-to-bottom, left-to-right convention
  - Operating node voltages decrease from top to bottom
  - Currents flow from left to right

Anatomy of a PCB

Via (connects to other copper layers, “tented”)

Soldermask (green, coats most of board)

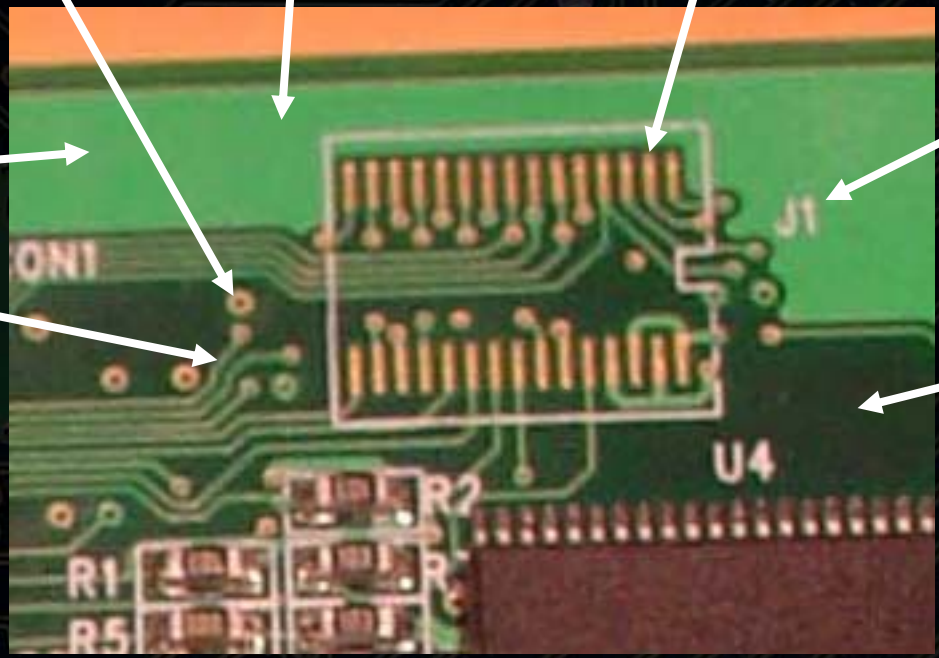
Plated “pad” (gold, opening In soldermask)

Silkscreen (white)

Copper “plane”

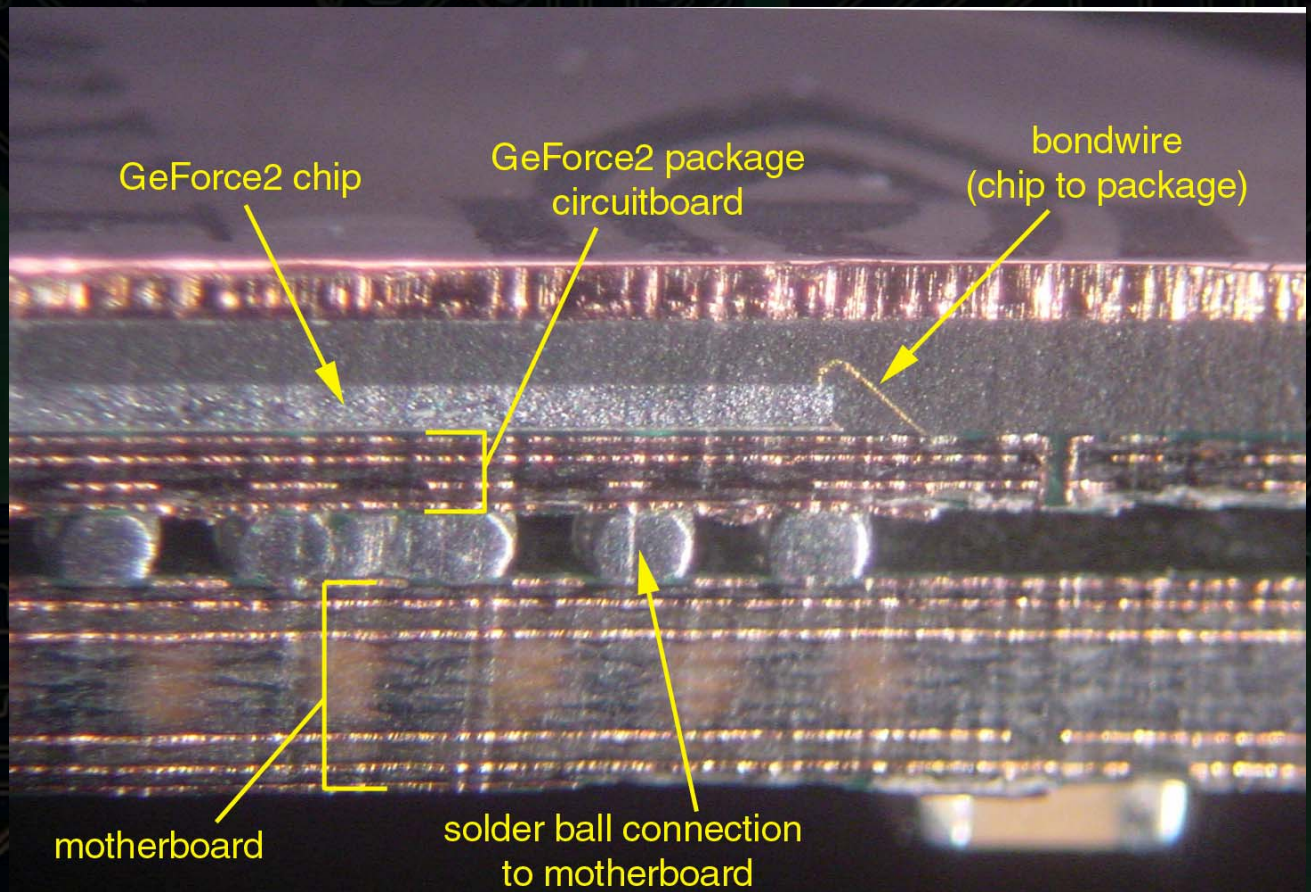
Copper trace

Region with no features



Cross section of a PCB

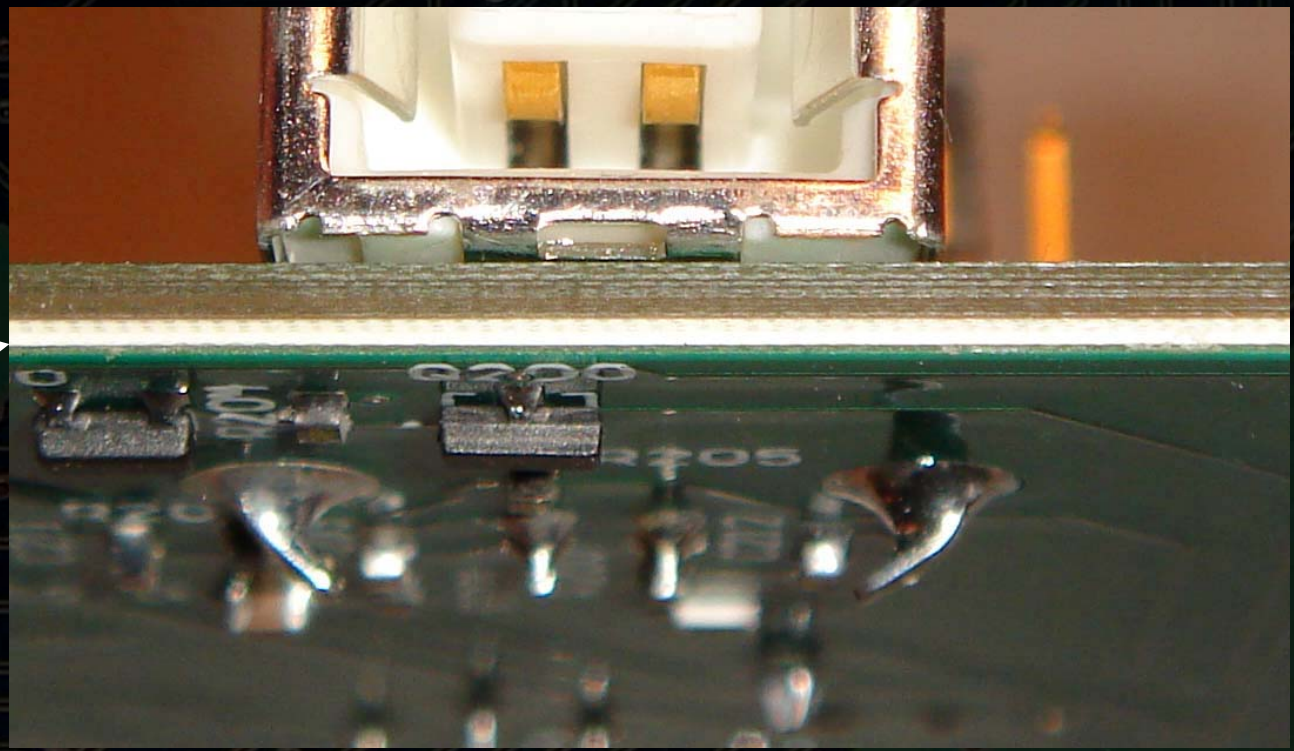
- PCBs often stack multiple buried layers of copper
  - Vias connect between layers
  - Sometimes vias do not go all the way through!



Look Sharp!

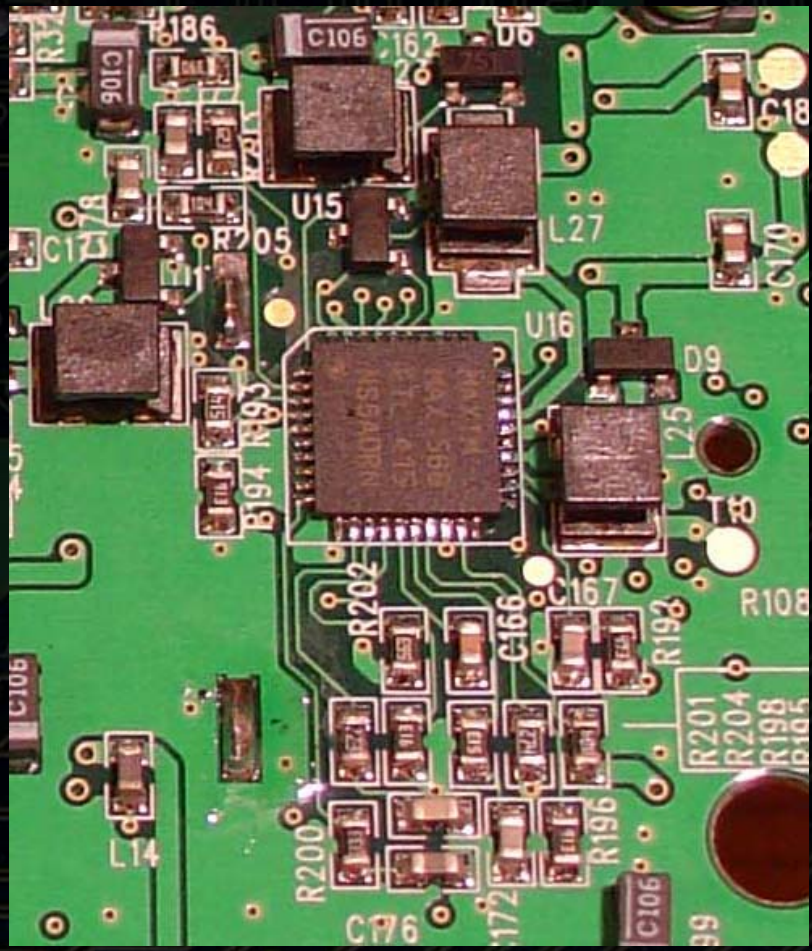
- Buried layers can have different material types
  - White layers indicate high-quality, very-high frequency dielectrics—very interesting stuff is probably going on!

Buried white Layer??



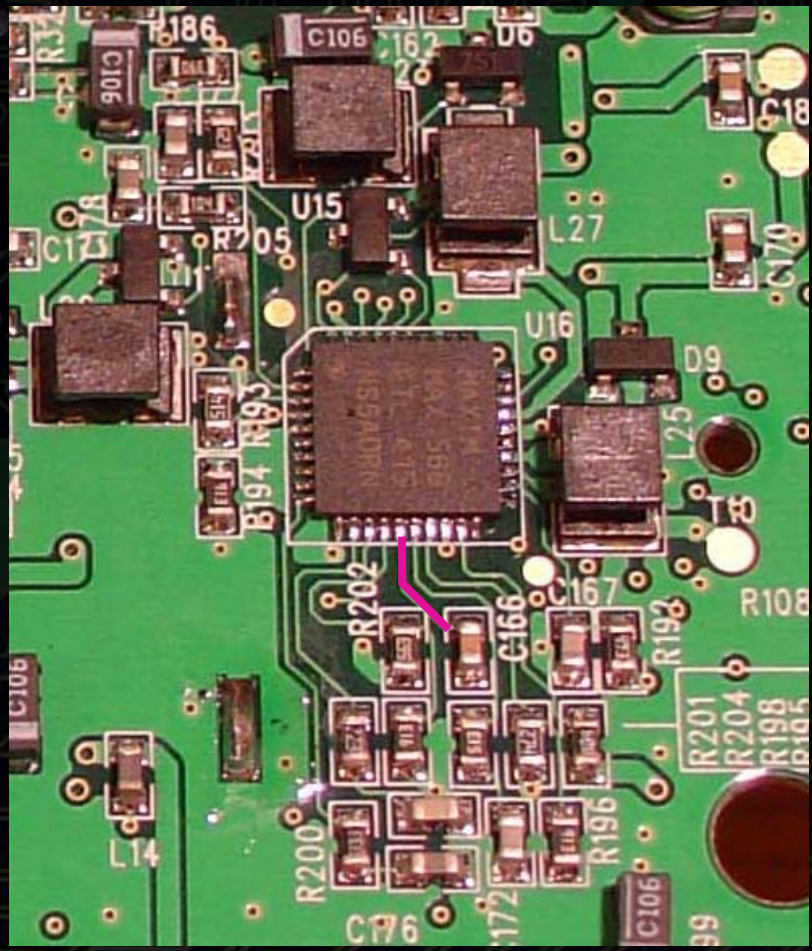
Extracting Connectivity

- Exposed traces: just follow the copper



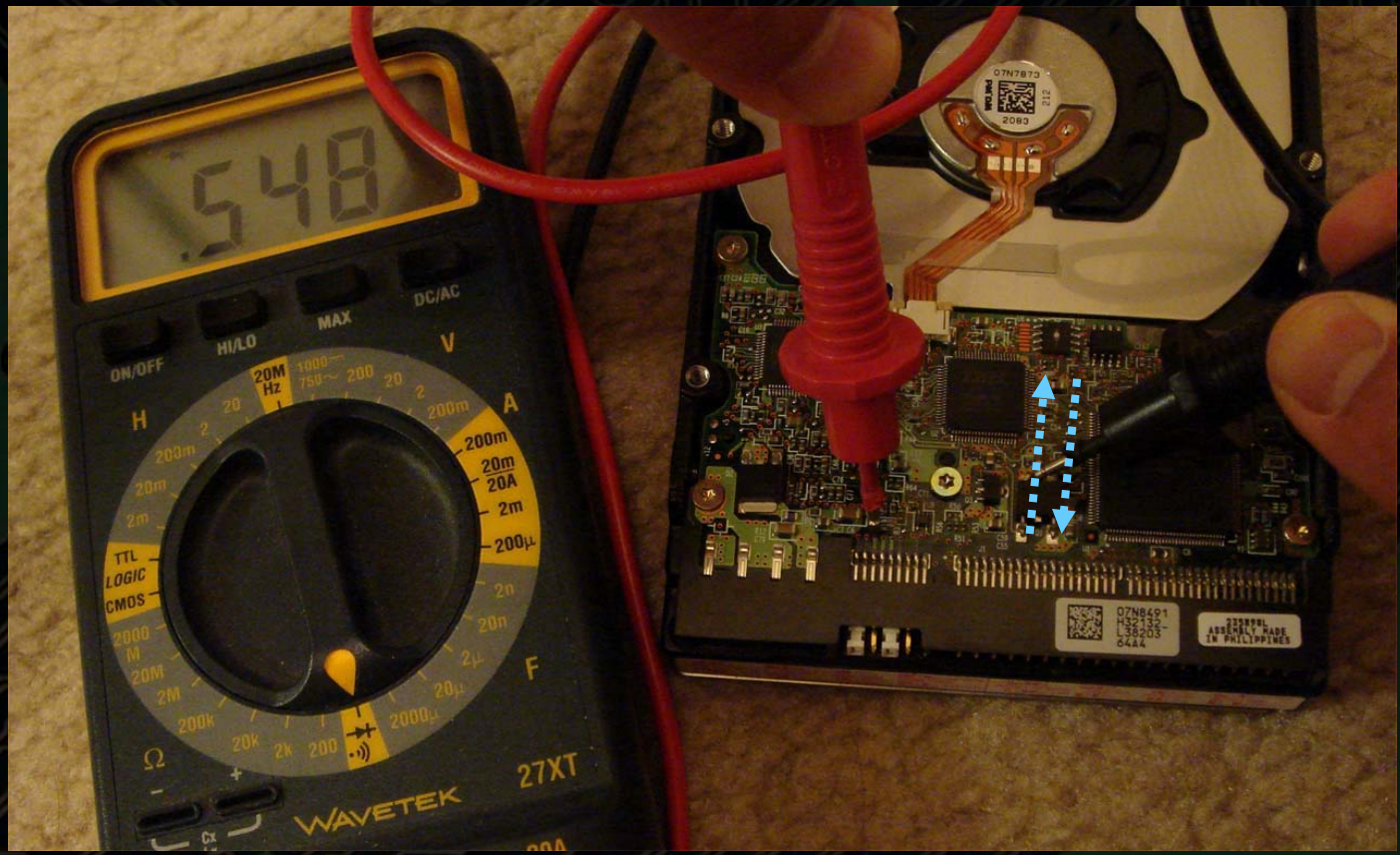
Extracting Connectivity

- Exposed traces: just follow the copper



Buried Traces…

- For traces that are not exposed, use a continuity meter and “sweep” the board to find the connection

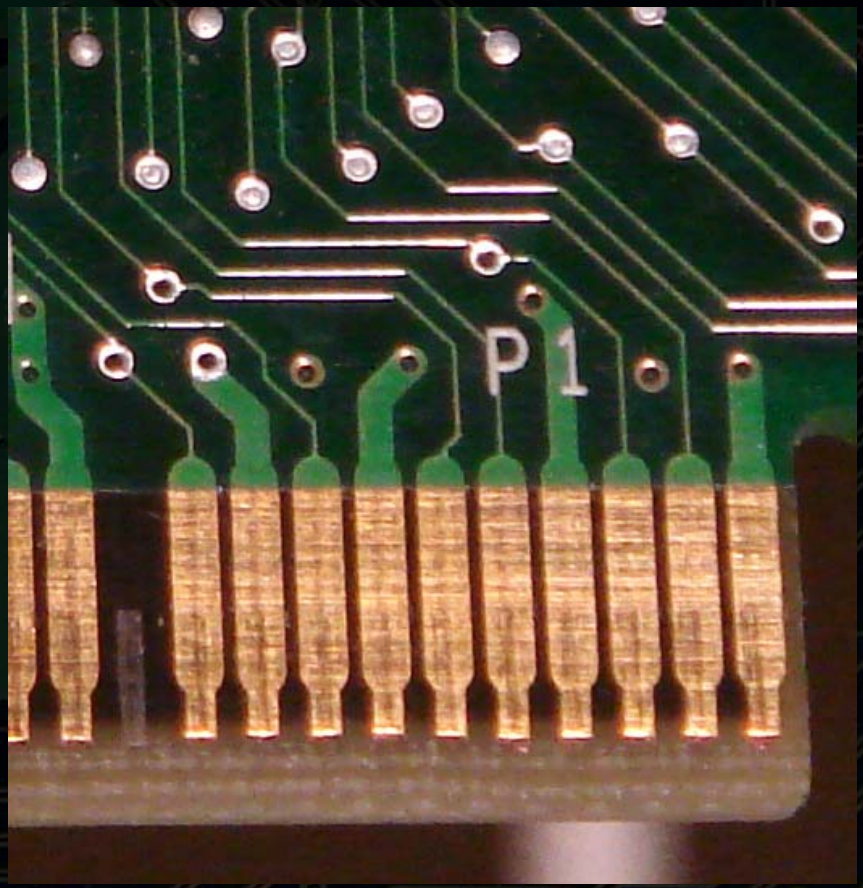


Circuit Board Motifs

- Extracting traces is a time consuming process
- Rely on heuristics to identify trace function without a full connectivity trace
  - Fall back on inviolable physical principles that constrain the flow of electricity to cull the possibility space
  - Also count on lazy designers, e.g. minimal effort for functionality

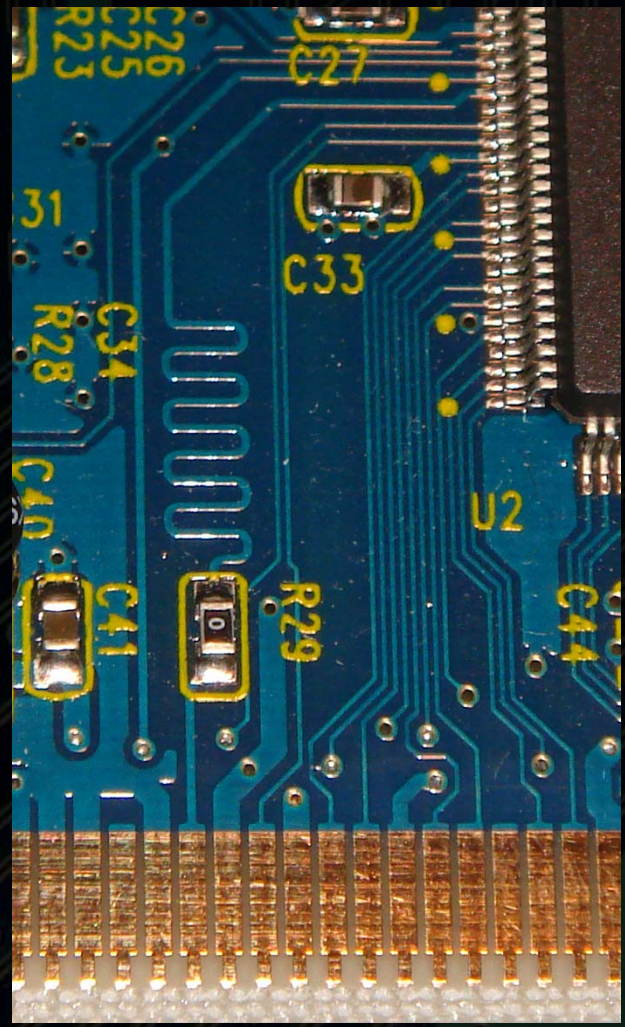
Motif #1

- Power traces are thick and usually short



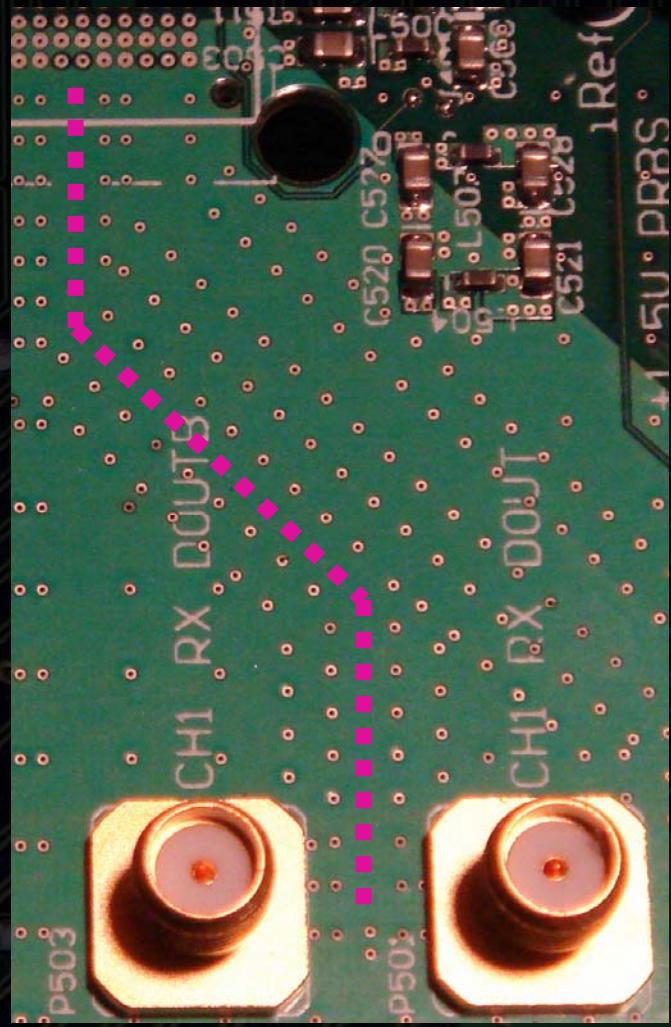
Motif #2

- Impedance controlled signals are thick and usually long
  - Look for in-line resistors as well
- These signals are often:
  - Clocks
  - High-speed data
  - Critical



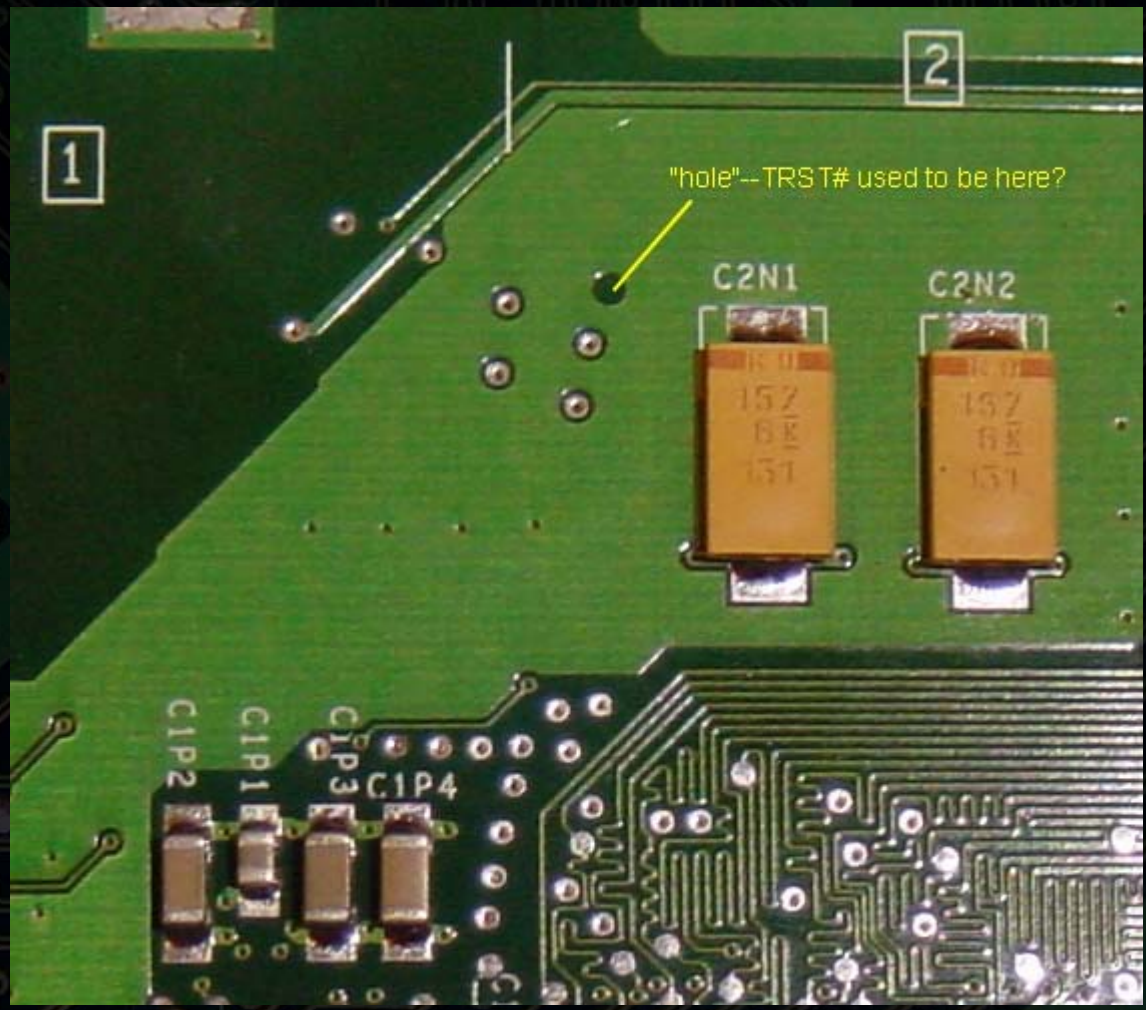
Motif #3

- Look for hints of buried signals
  - Ground stitching is a dead giveaway of buried signals
  - Busses terminating to nowhere indicate buried signals



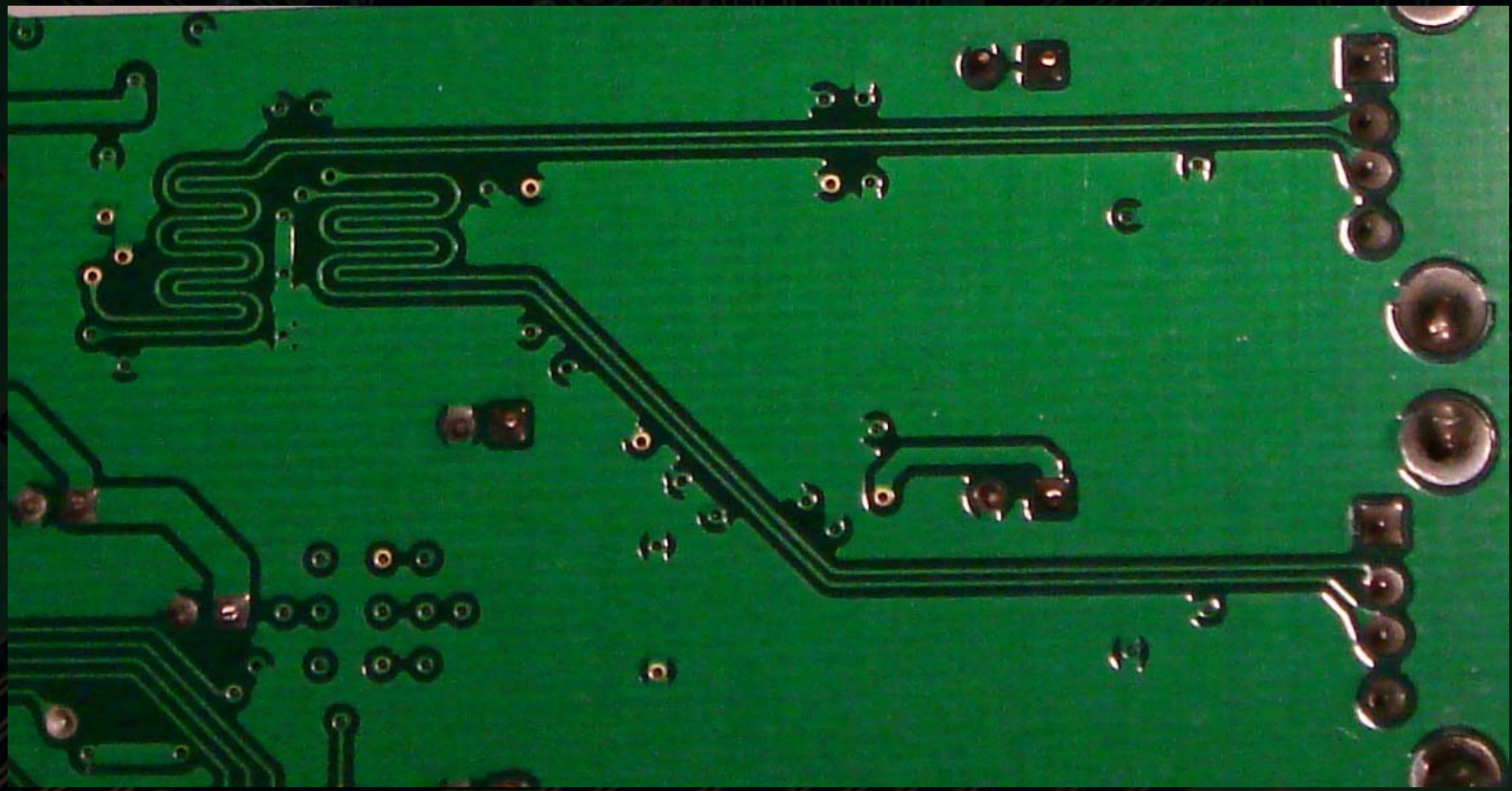
Motif #4

- Look for missing signals



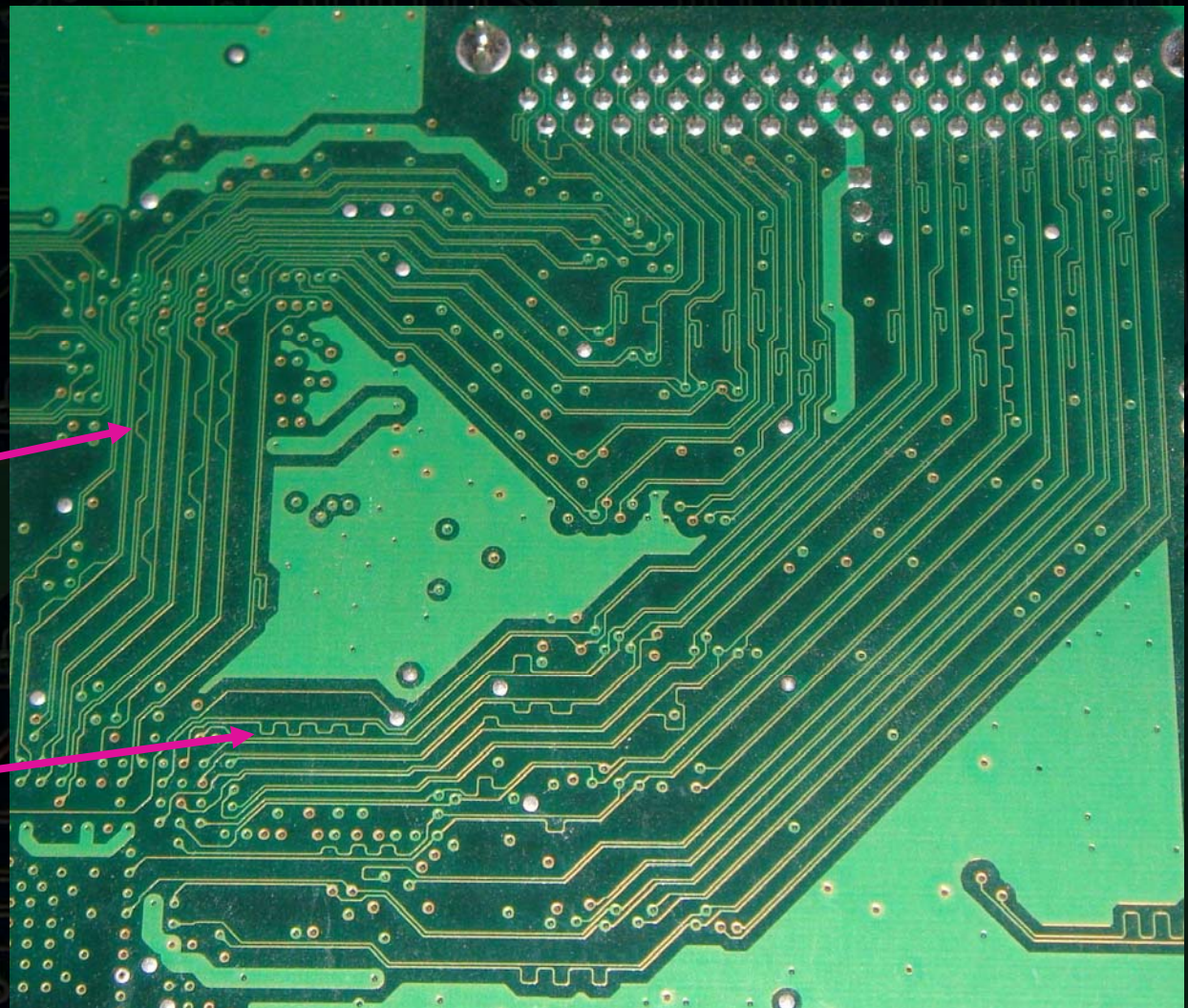
Motif #5

- Pairs of traces indicate differential signaling



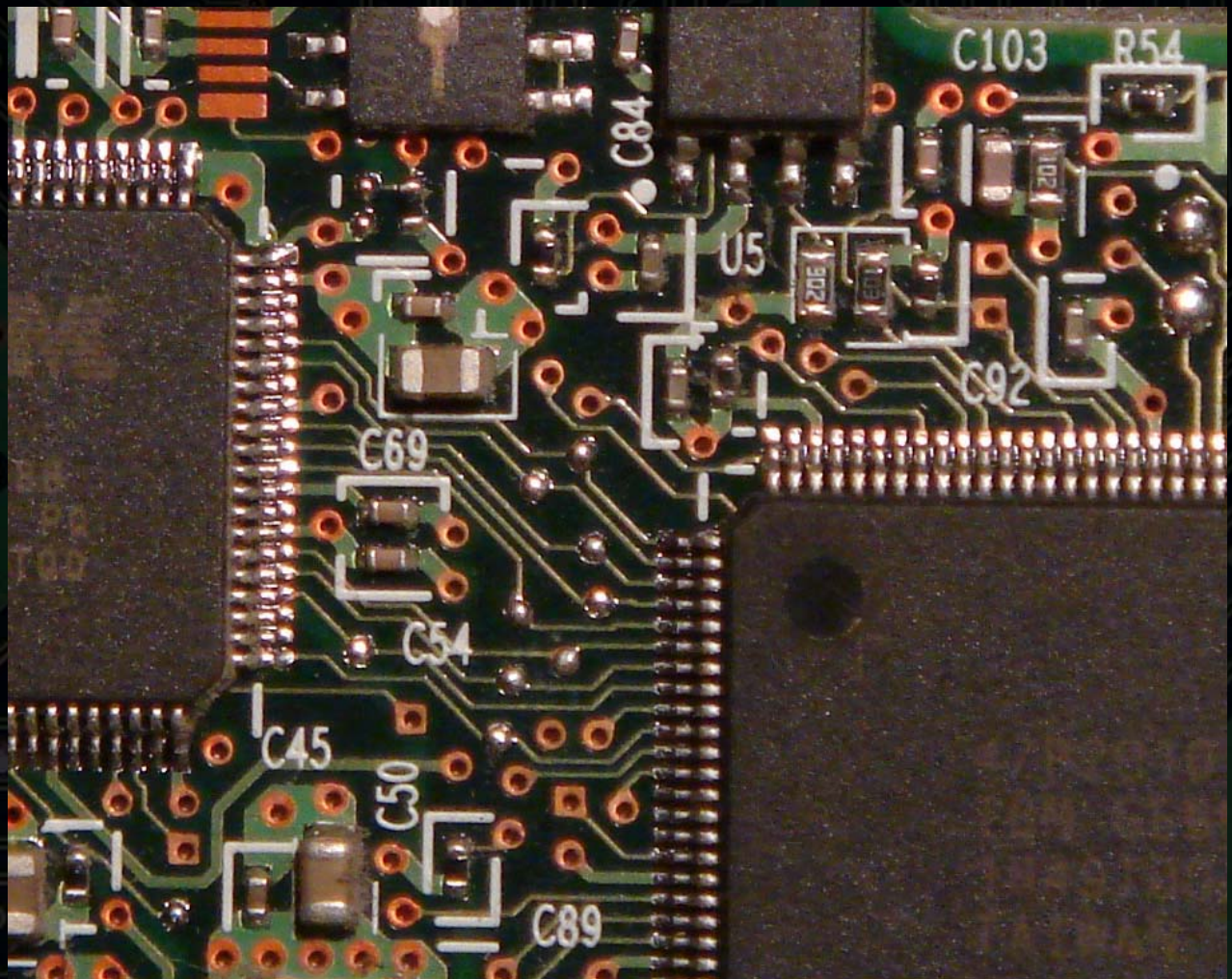
Motif #6

- “Zig-zag” traces indicate length-matched busses



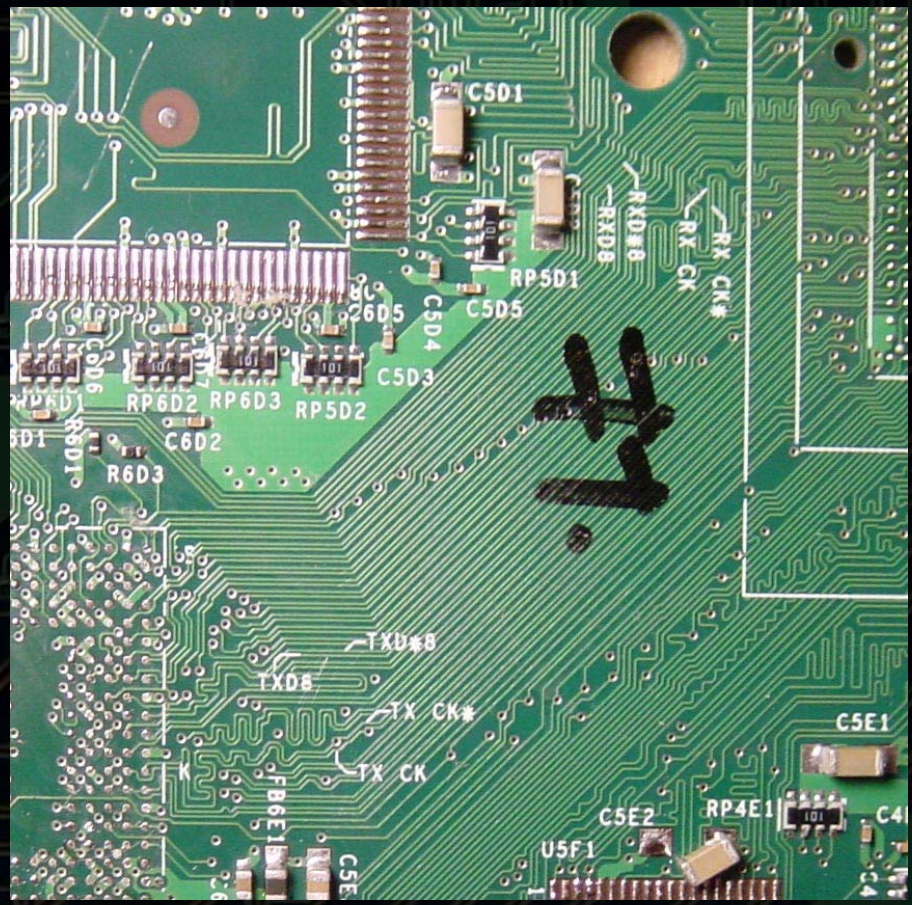
Motif #7

- Look for test points
  - Indication of “interesting” signals…what’s good for the engineer is good for the hacker!



Motif #8

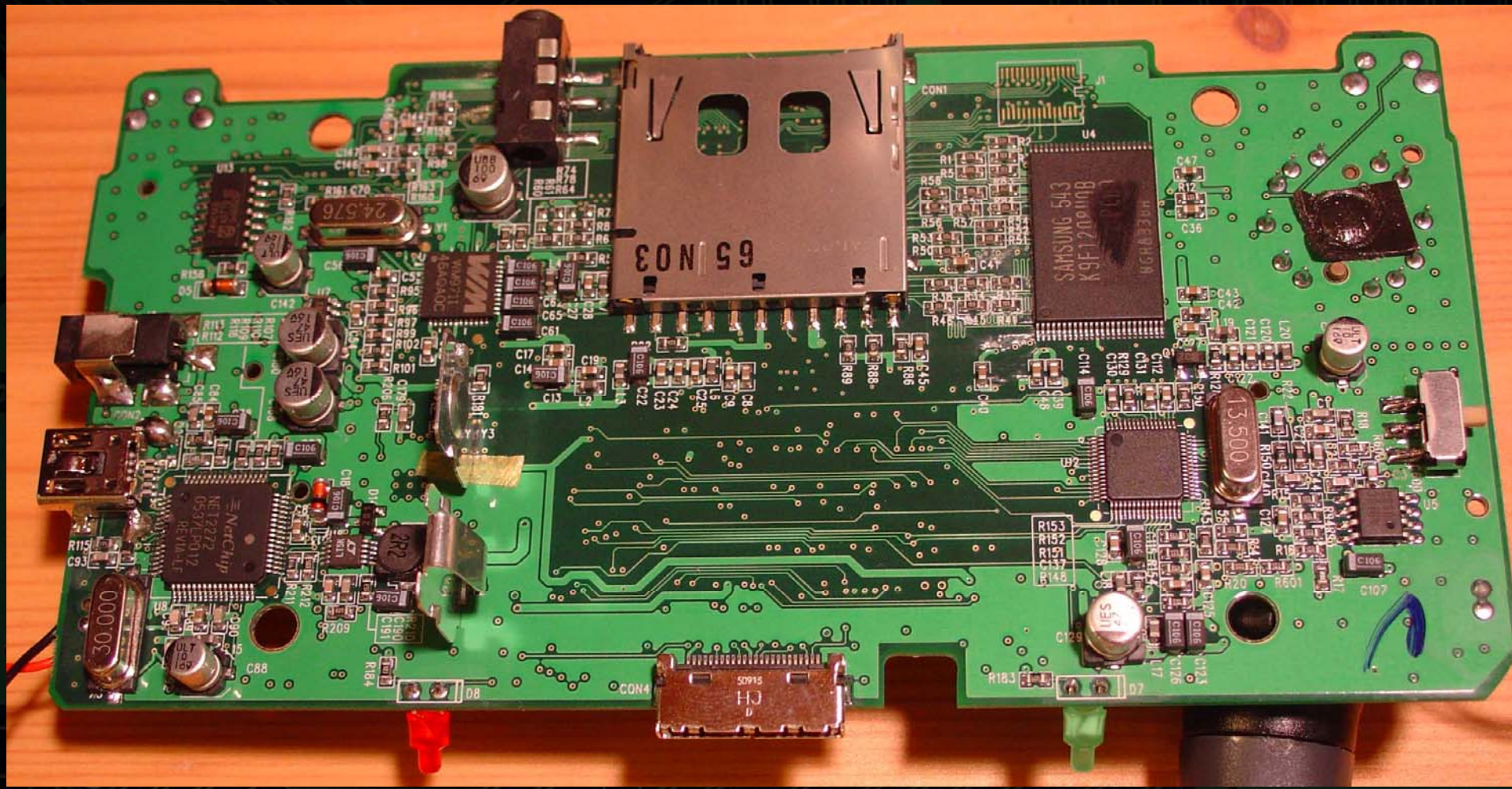
- Traces of similar function are grouped together
  - Count number of traces in group to deduce potential functions



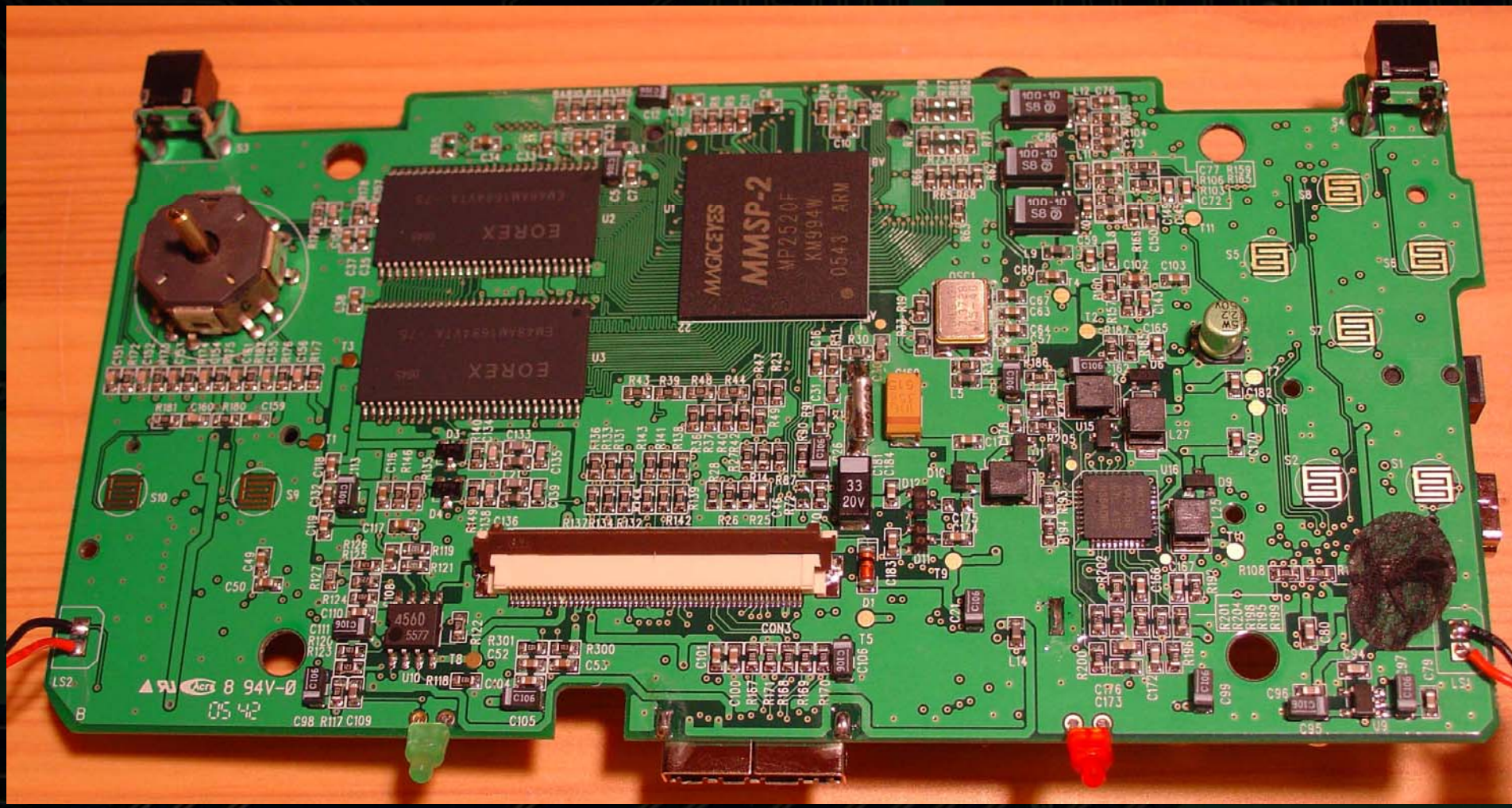
Other Motifs

- With time, one will learn to associate certain logos and package types with general categories of components
  - e.g. SDRAM vs. FLASH memory
  - Power regulators
  - Other support components

Example



Example


MAGICEYES
MMSP-2
MP2520F
KM9904W
0543 ARM
EOREX
33
20V
4560
5577
CON3

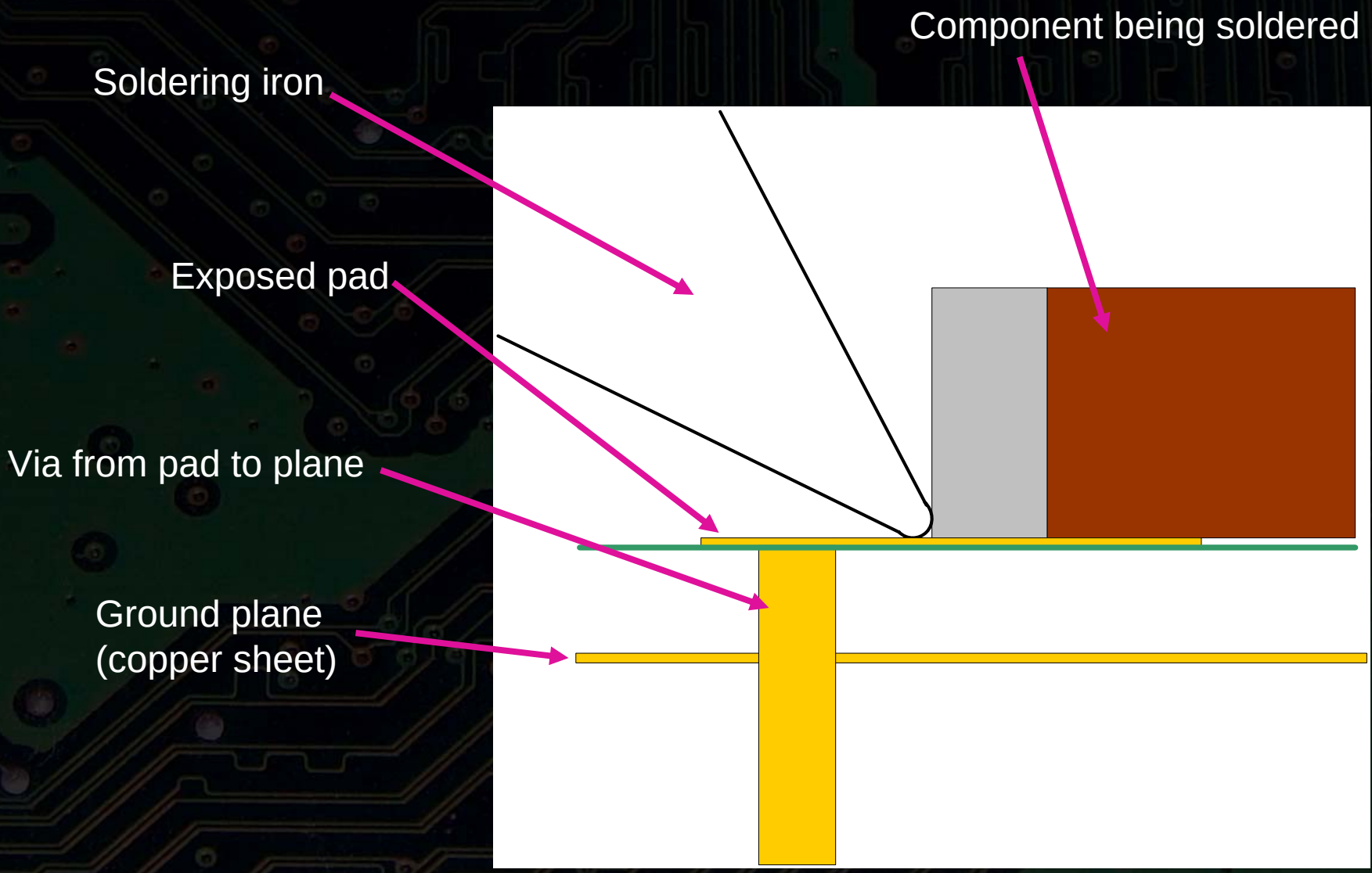
Soldering

- Key principles of making good joints:
  - Everything needs to get hot
    - Circuit board, component, and solder
    - Certain circumstances can make this tricky
    - Solder will “wet” or flow over all clean, hot surfaces
  - Work surfaces need to be oxide-free
    - Use flux to “burn off” contaminants
- Small components are easy to master
  - Mastery of chopsticks to pick up single grains of rice is the equivalent dexterity required for 0603-sized (~millimeter scale) components

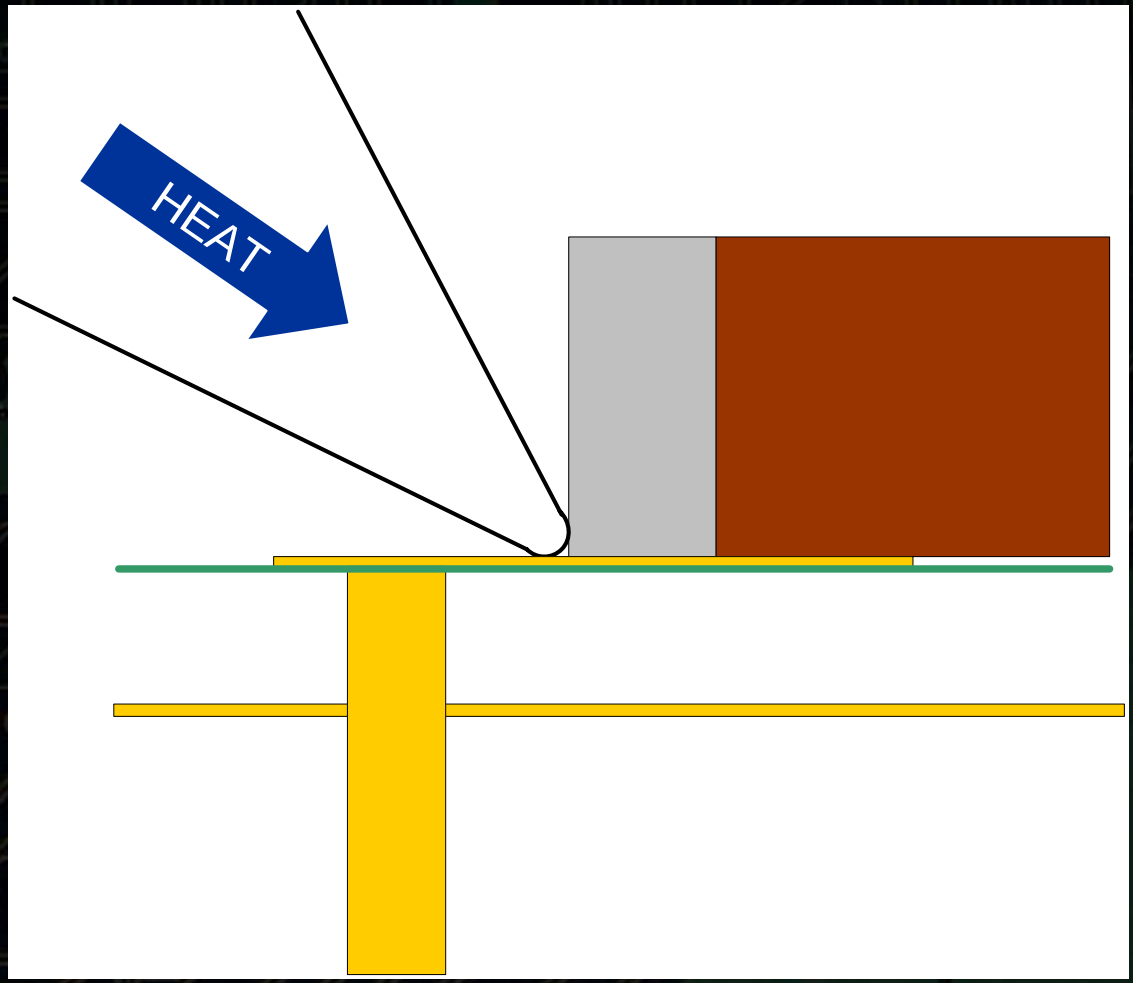
Getting it Hot

- Sometimes it seems like the board or component is not getting hot
  - Two common problems:
    - Connected copper or component has a large thermal mass
      - Solution: wait longer (count to ten or so before applying solder)
    - Insufficient thermal contact of iron to board
      - Soldering iron “tip” has a tiny contact area (<< 1mm^2)
      - Solutions
        - » Adjust iron angle so more contact is made
        - » Add a drop of solder to iron tip to dramatically increase contact area and therefore heat transfer efficiency

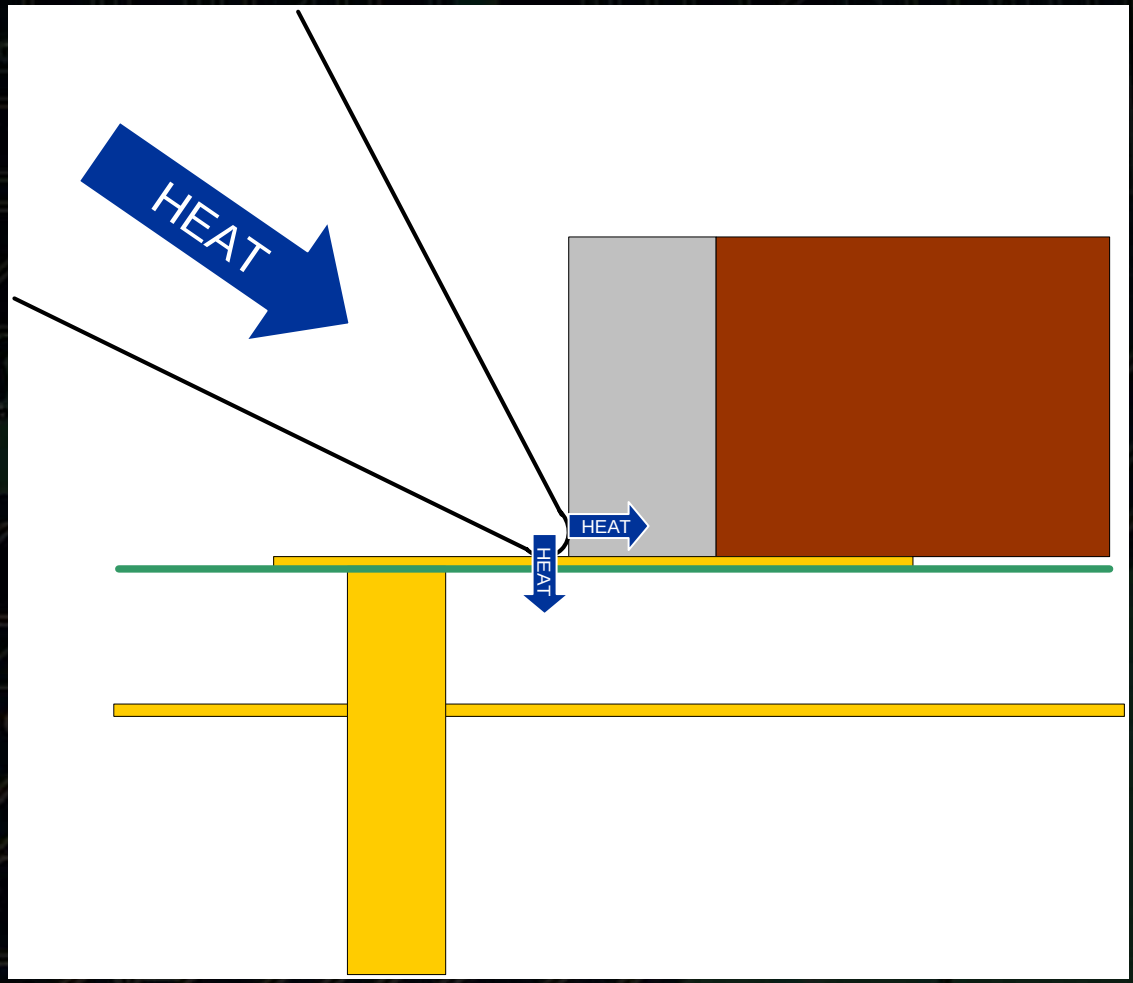
Heat Flow Concepts



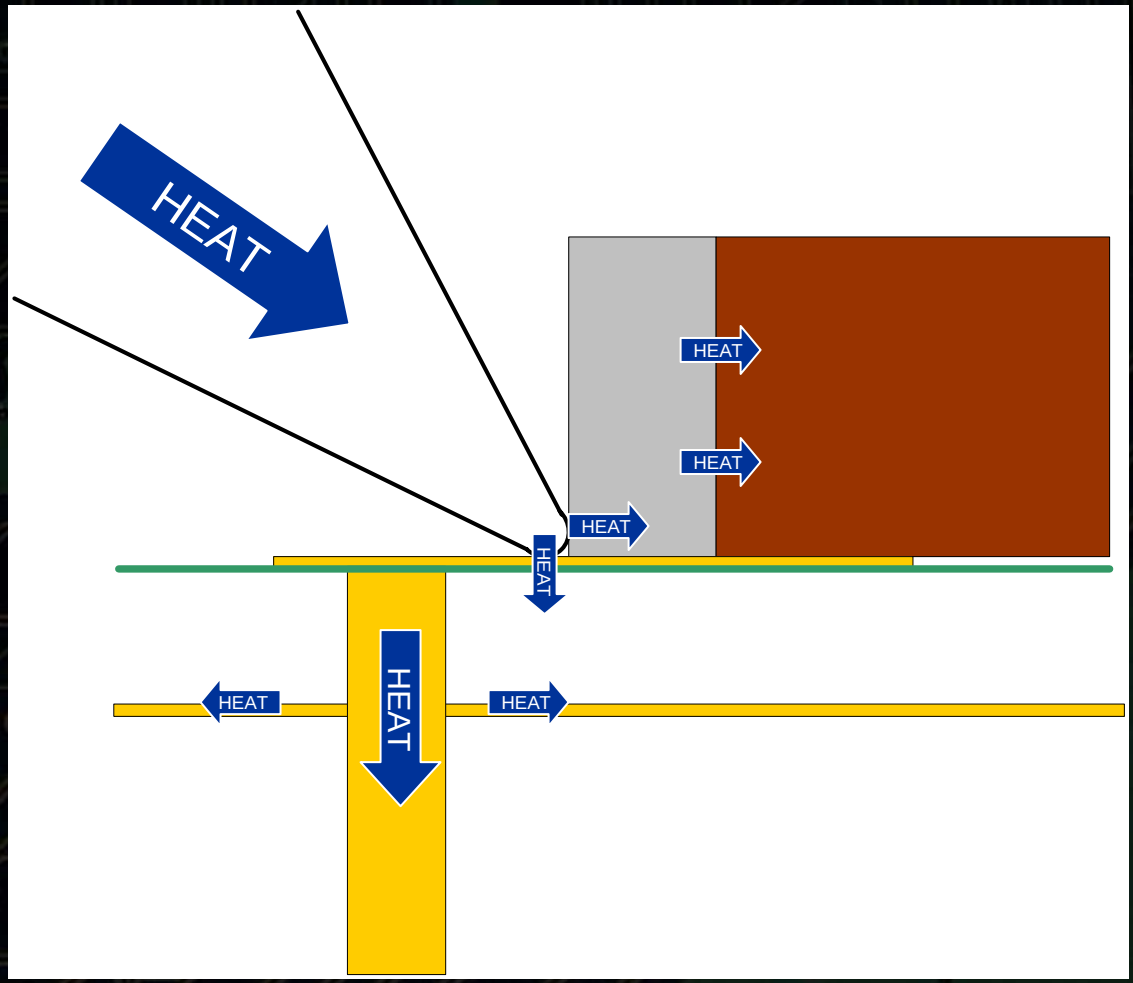
Heat Flow Concepts



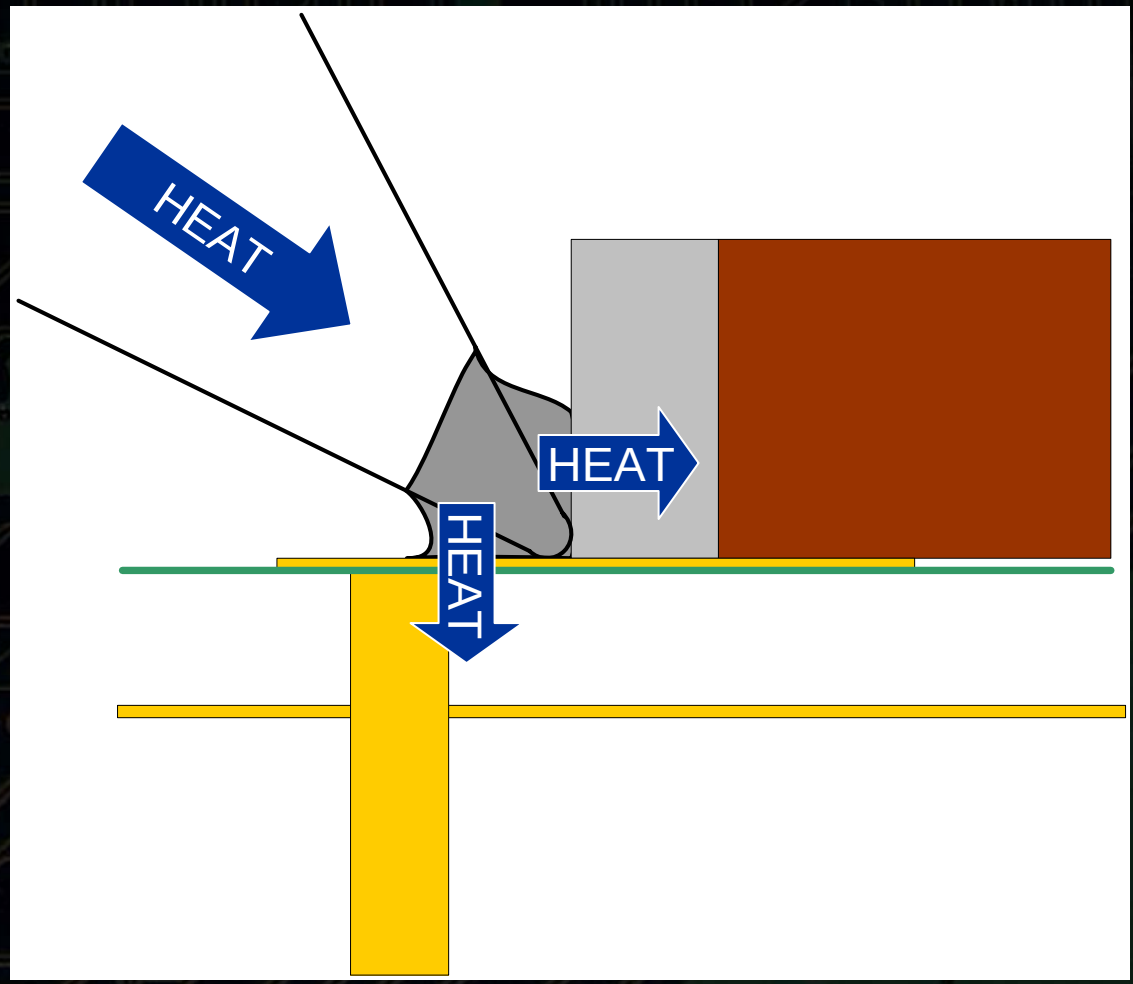
Heat Flow Concepts



Heat Flow Concepts

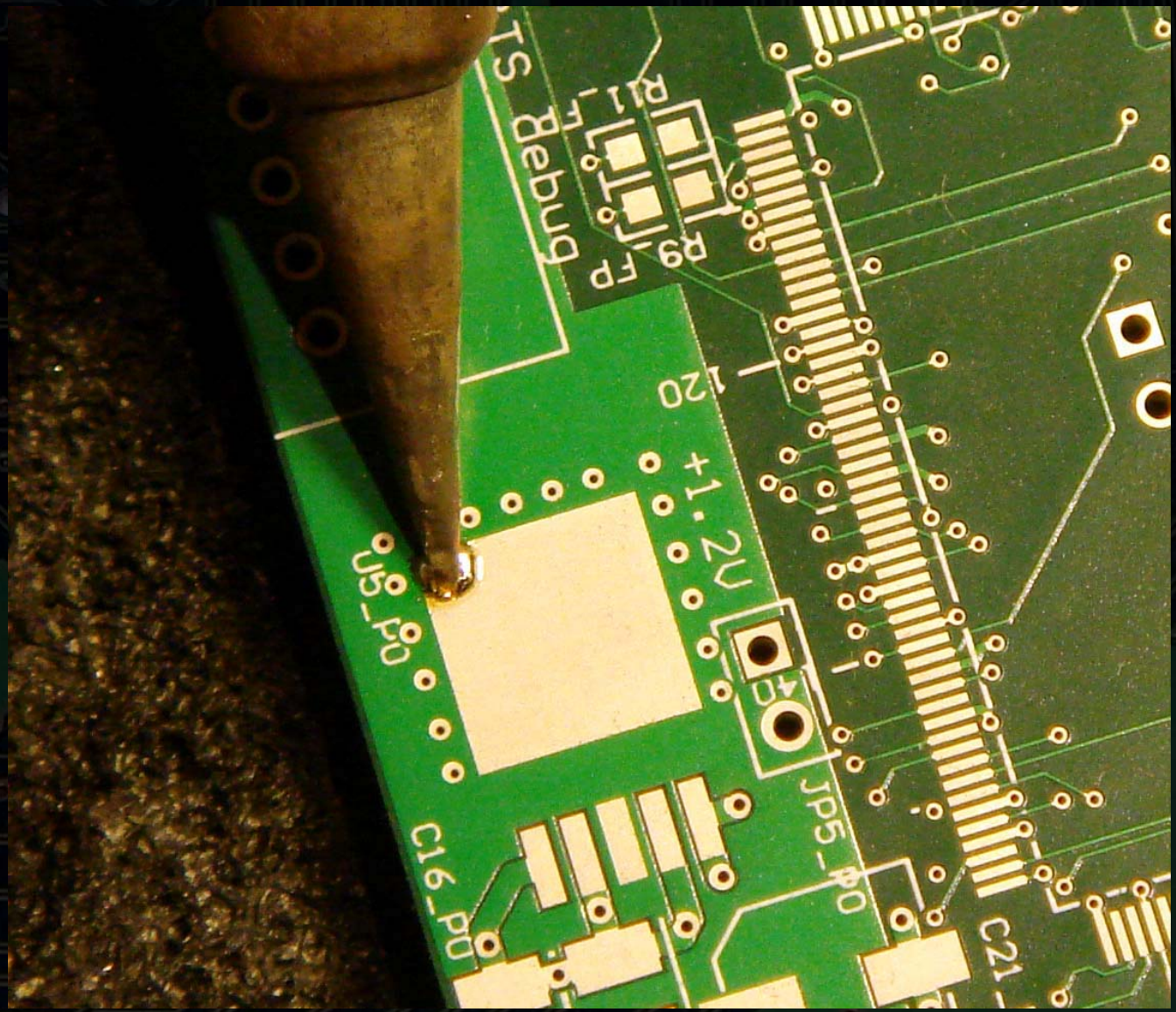


Heat Flow Concepts



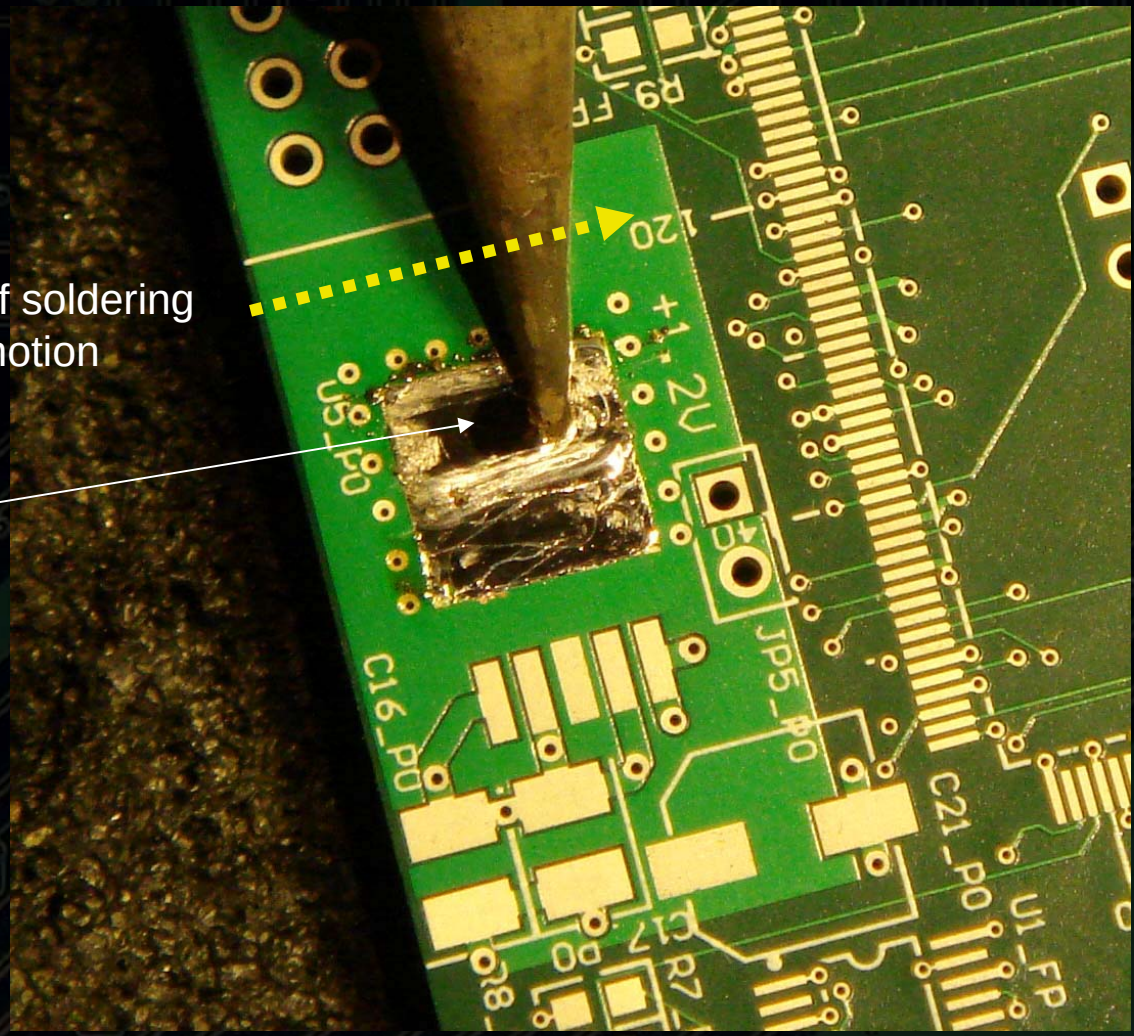
Heat Flow Illustrated

- Insufficient heat flow to heat entire pad



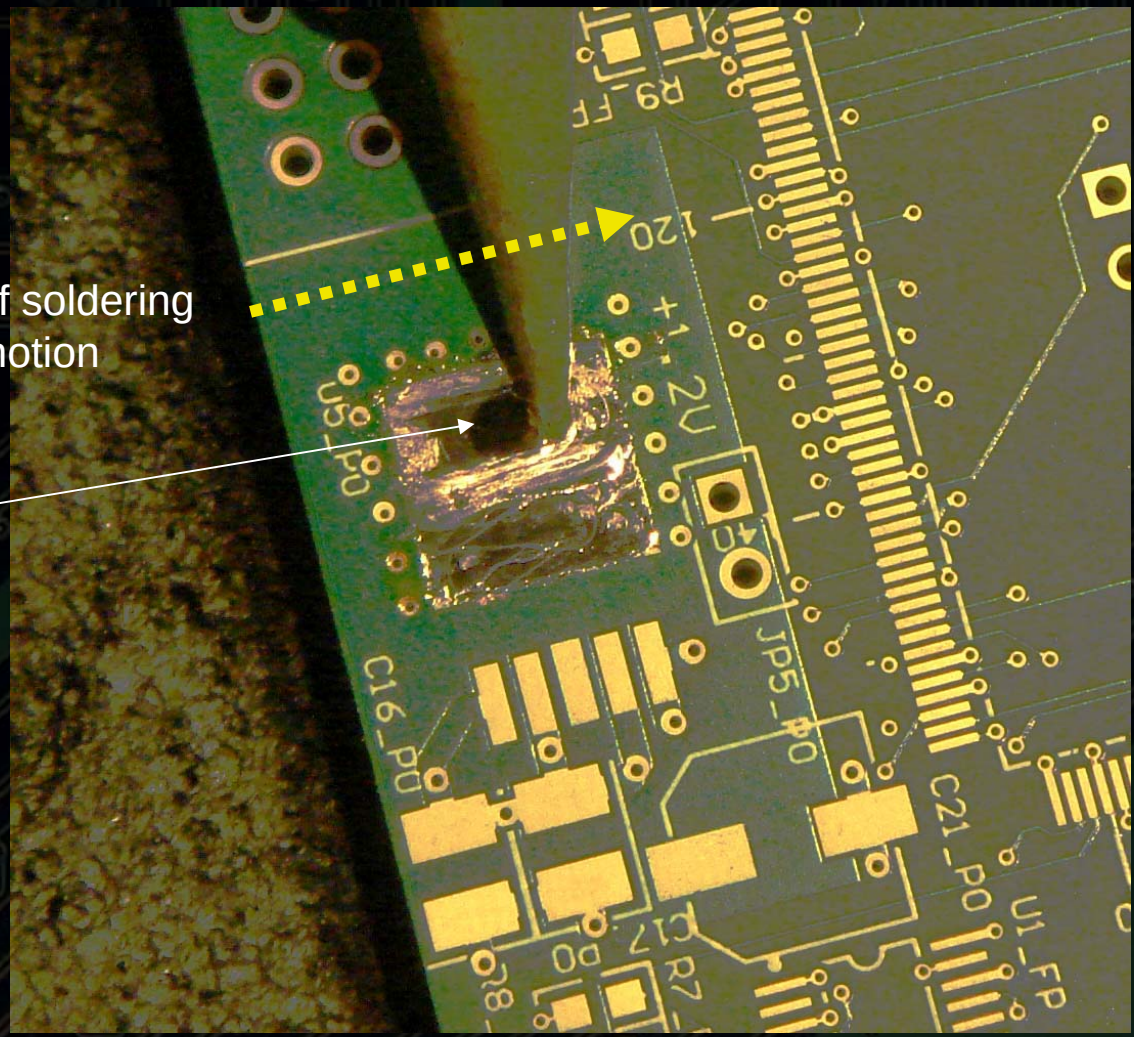
"Melt Pool"

- Look for solid-liquid phase change as a shift in albedo

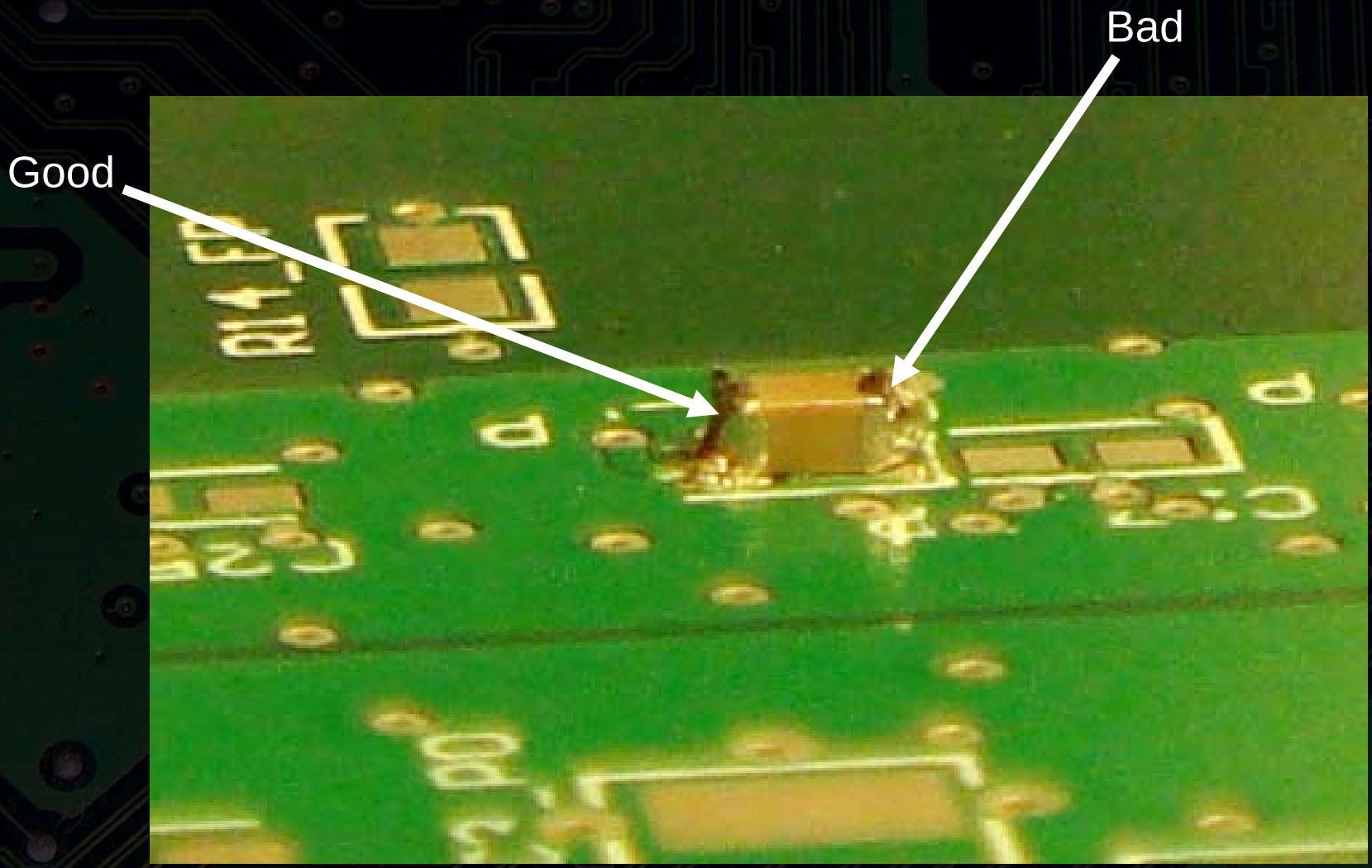


“Melt Pool”

- Look for solid-liquid phase change as a shift in albedo



Good and Bad

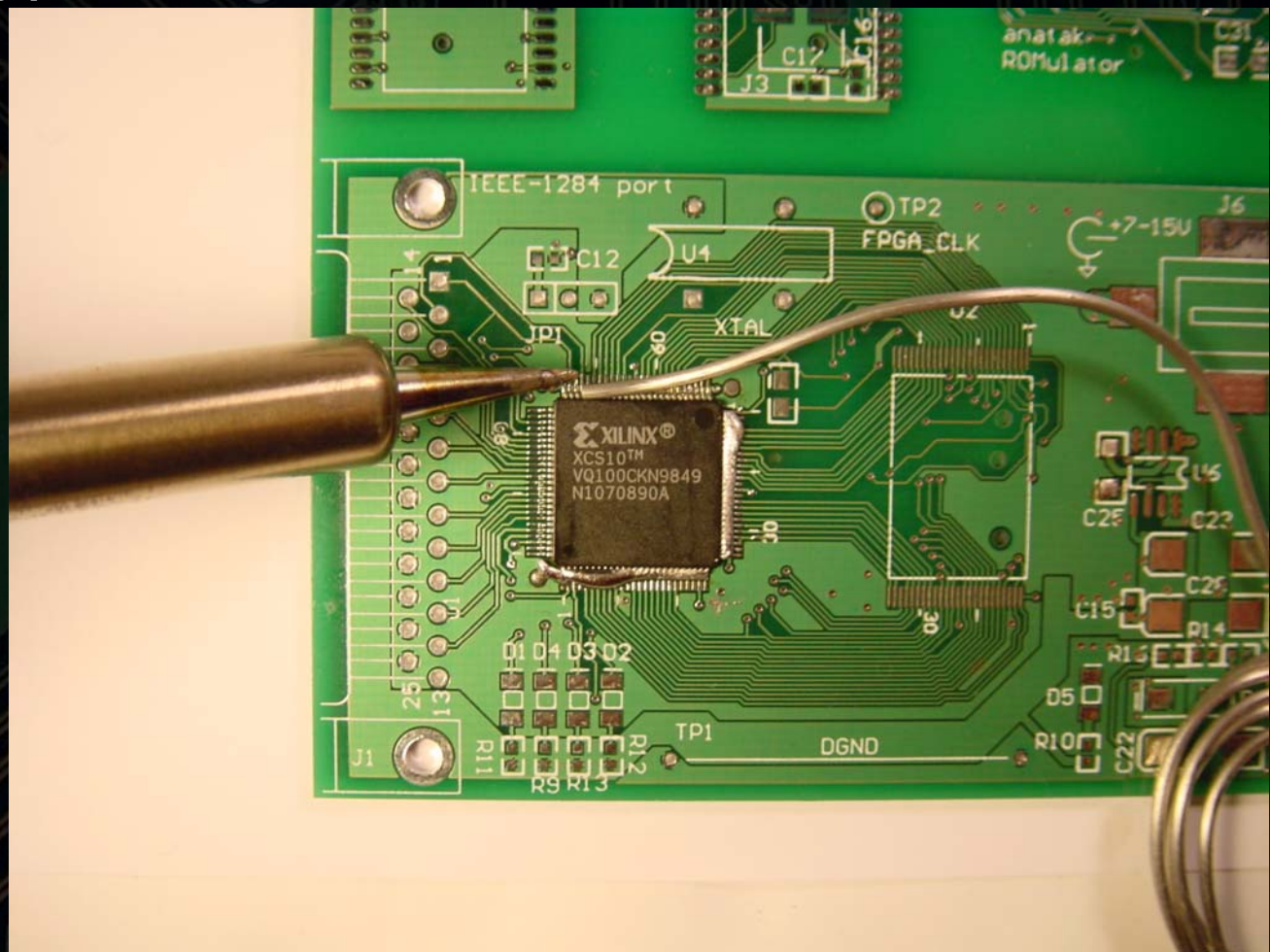


Use Flux

- Flux is a chemical used to clean the work surface
  - Subject metals oxidize normally
  - Oxide cannot be soldered
  - Flux attacks the oxide and enhances solder wetting
  - *MUST* use flux when soldering!

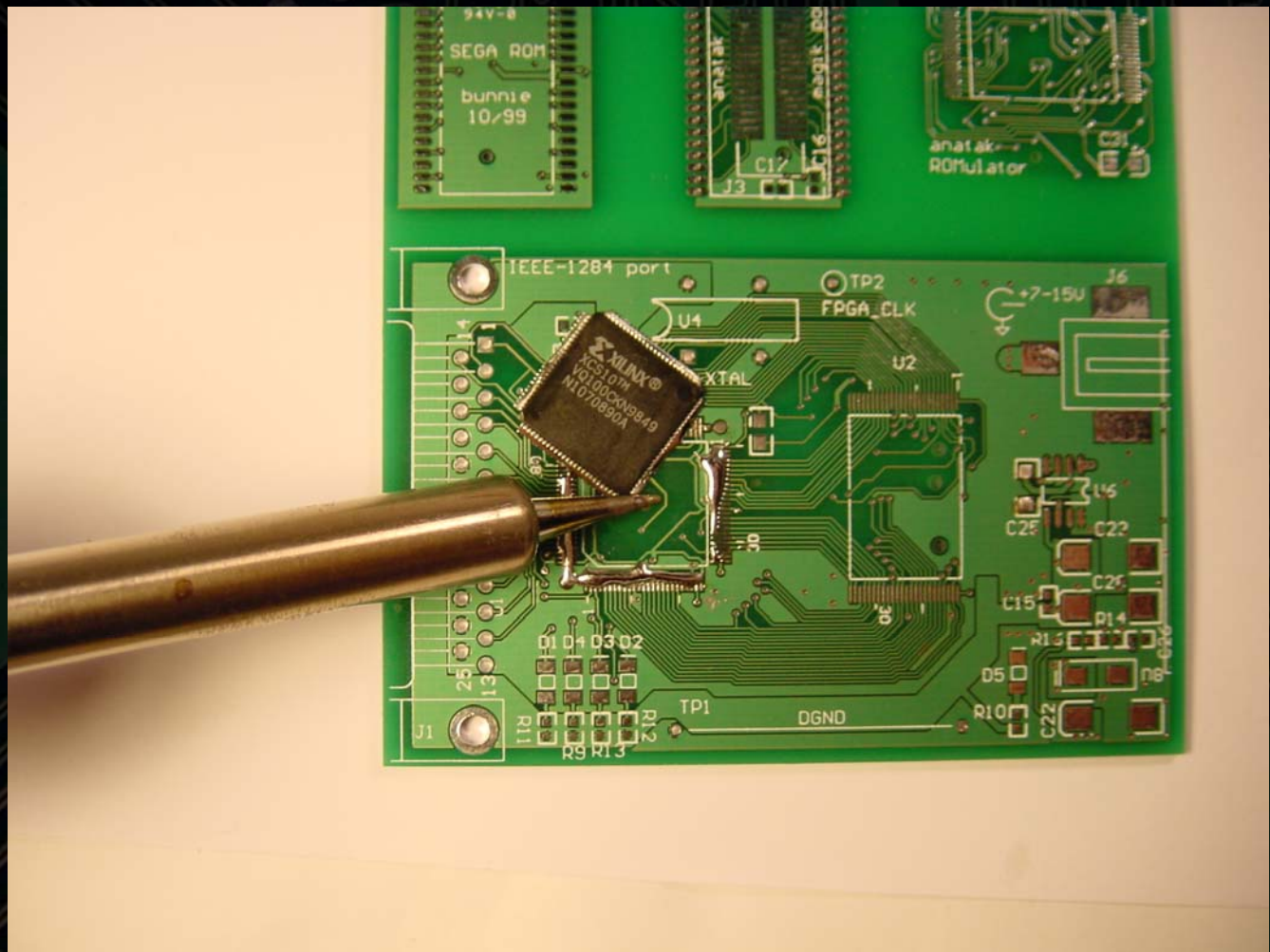
Desoldering

- Simplest method is to use a low-melting point material and alloy them together (e.g., Chipquik alloy)



Desoldering

- Low-melting point alloy enables easy relative thermal selectivity for component to remove

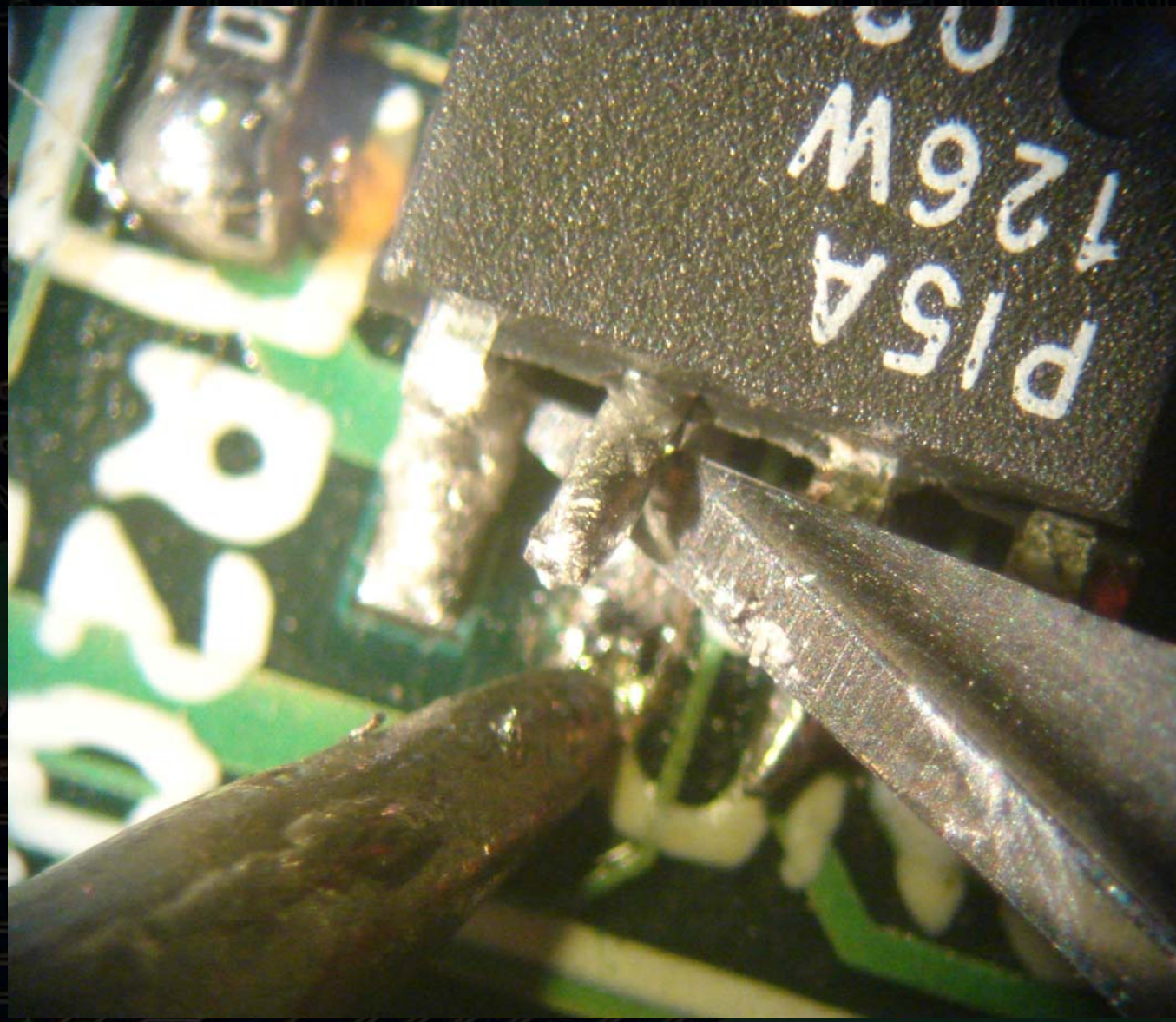


Patching

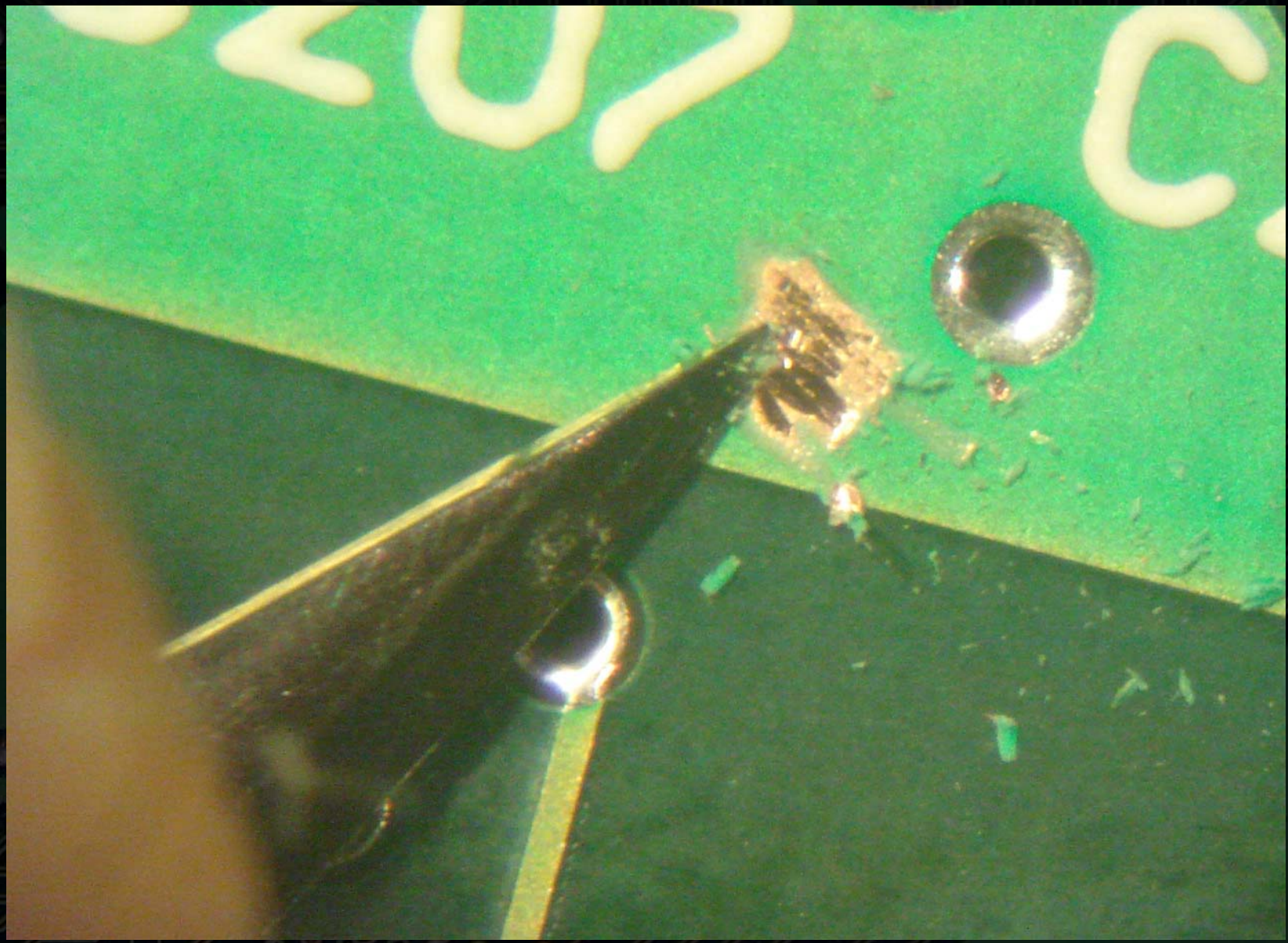
- Essential skill for the hardware hacker
  - Basic techniques:
    - Lifting chip pins
    - Scraping soldermask
    - Cutting traces
    - Adding wires

Lifting Pins

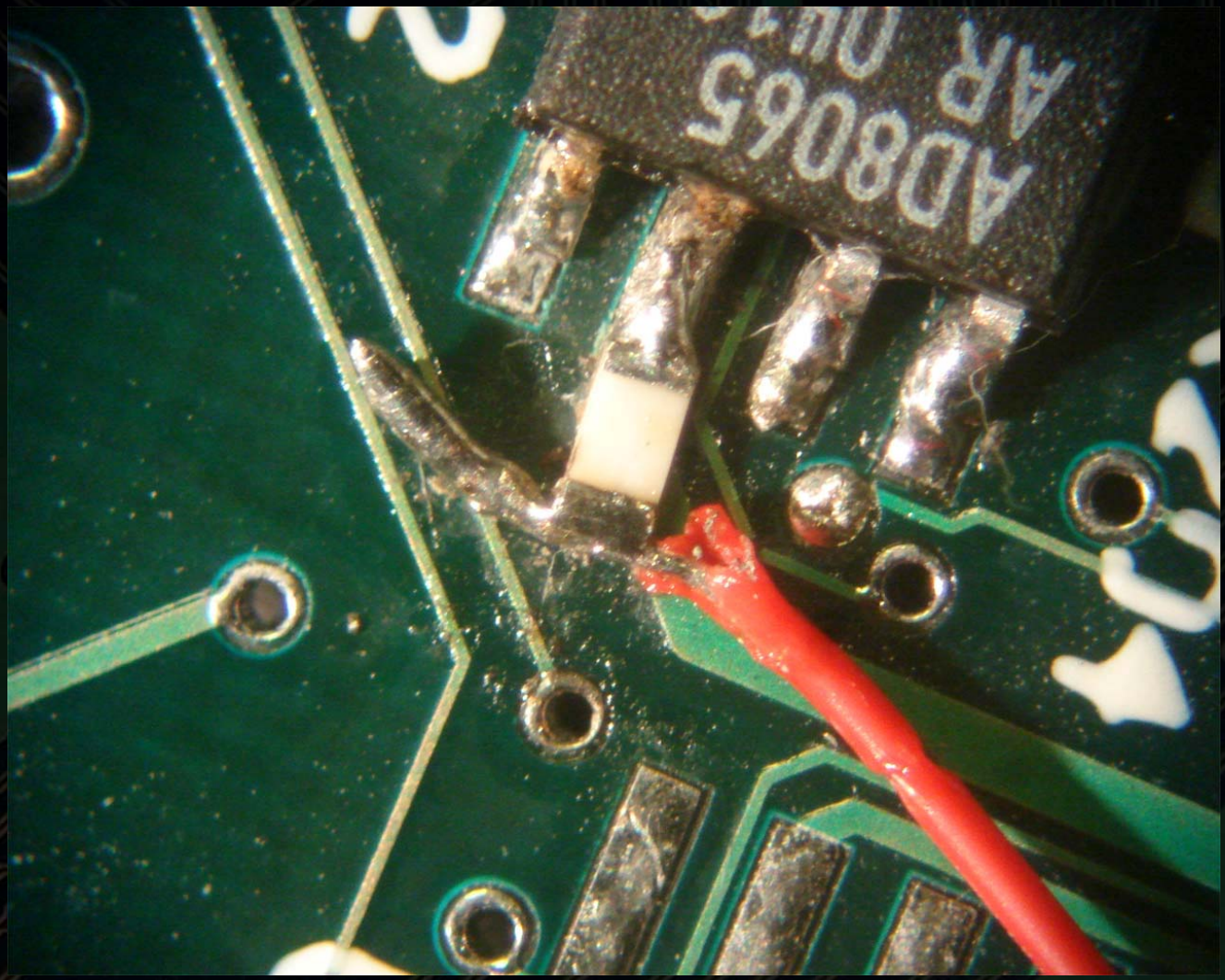
- Apply ample heat to workpiece and use tweezers or knife blade to lift pin from the side



Scraping Soldermask

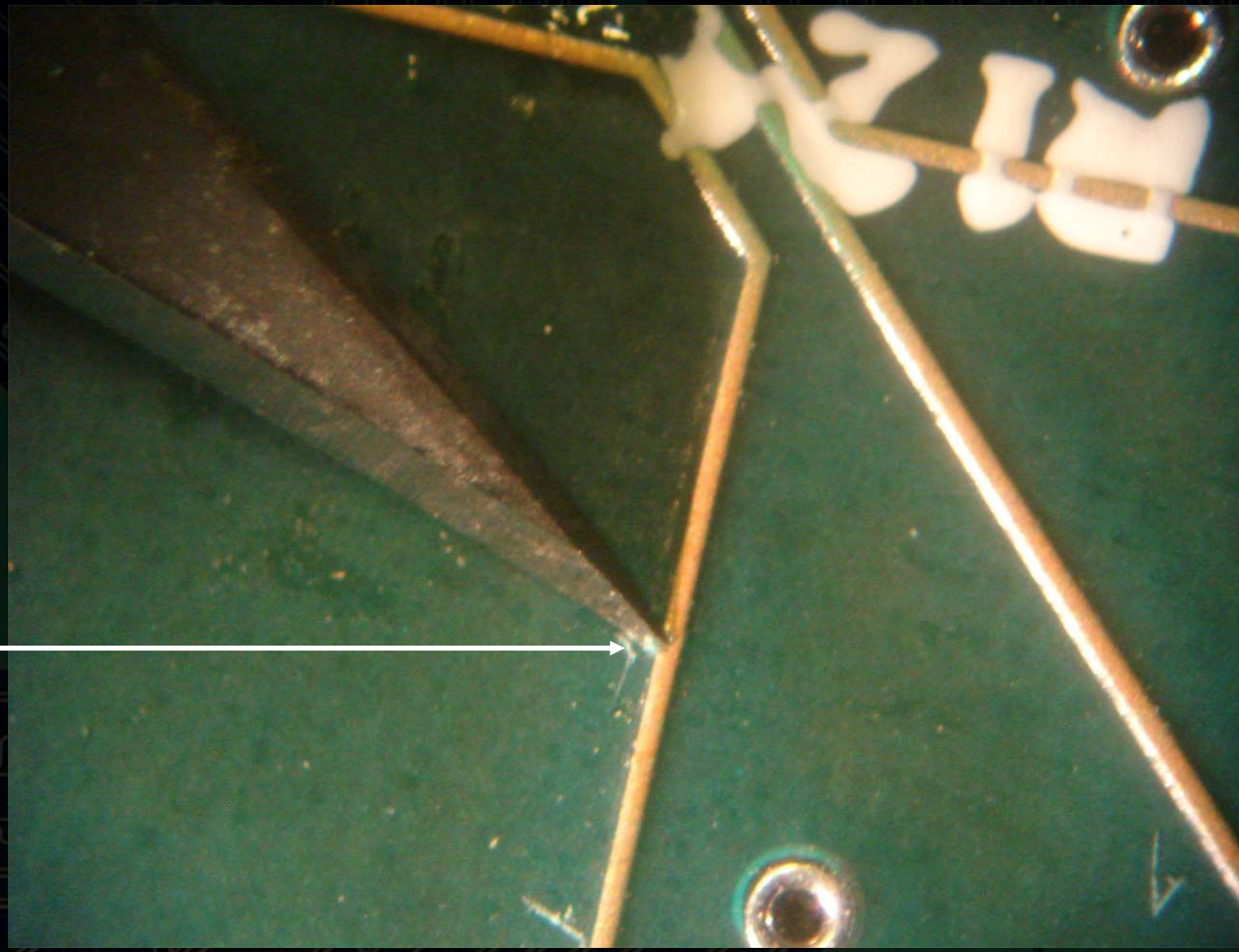


Tack Soldering (1)

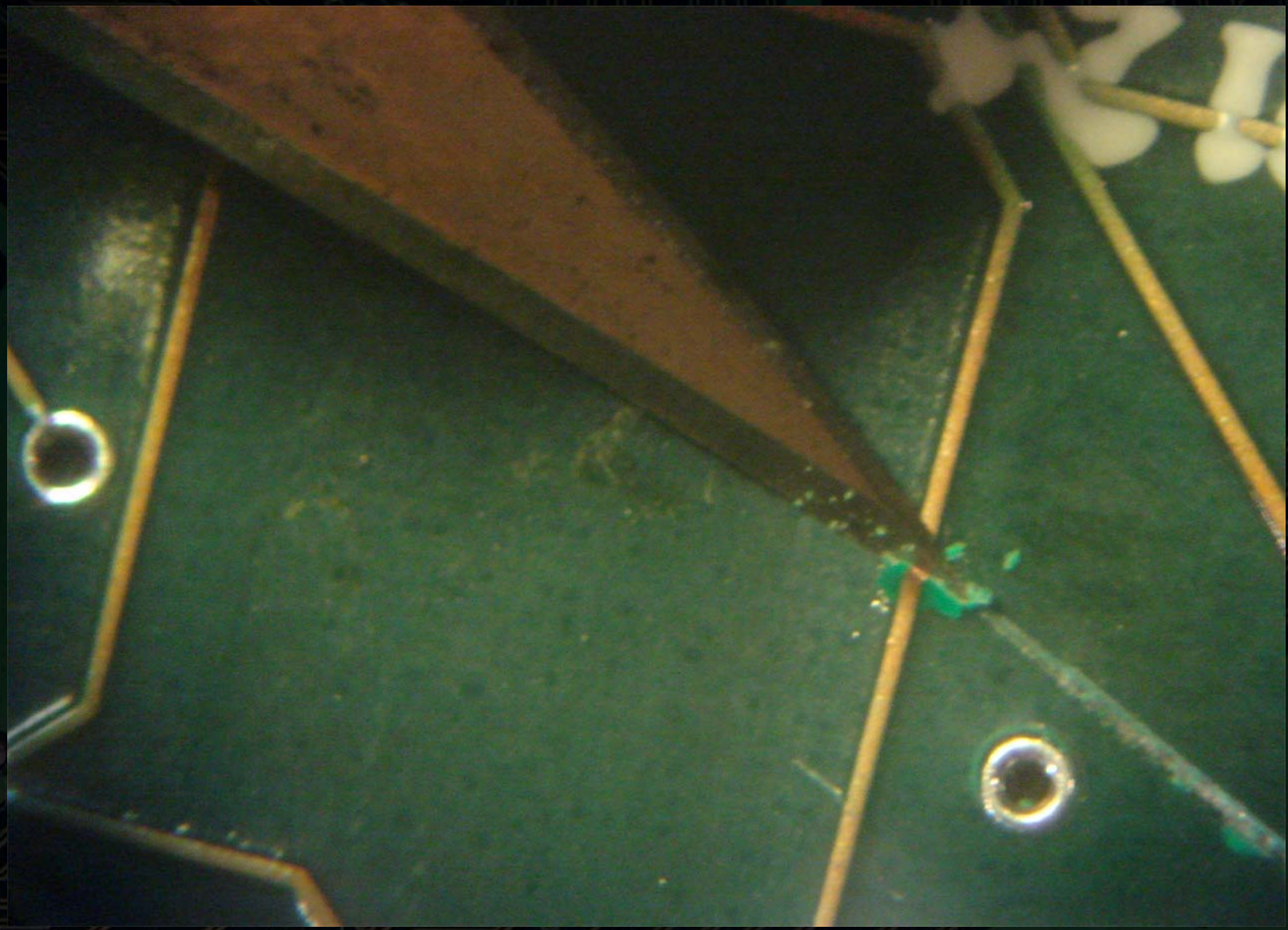


Tack Soldering (2)

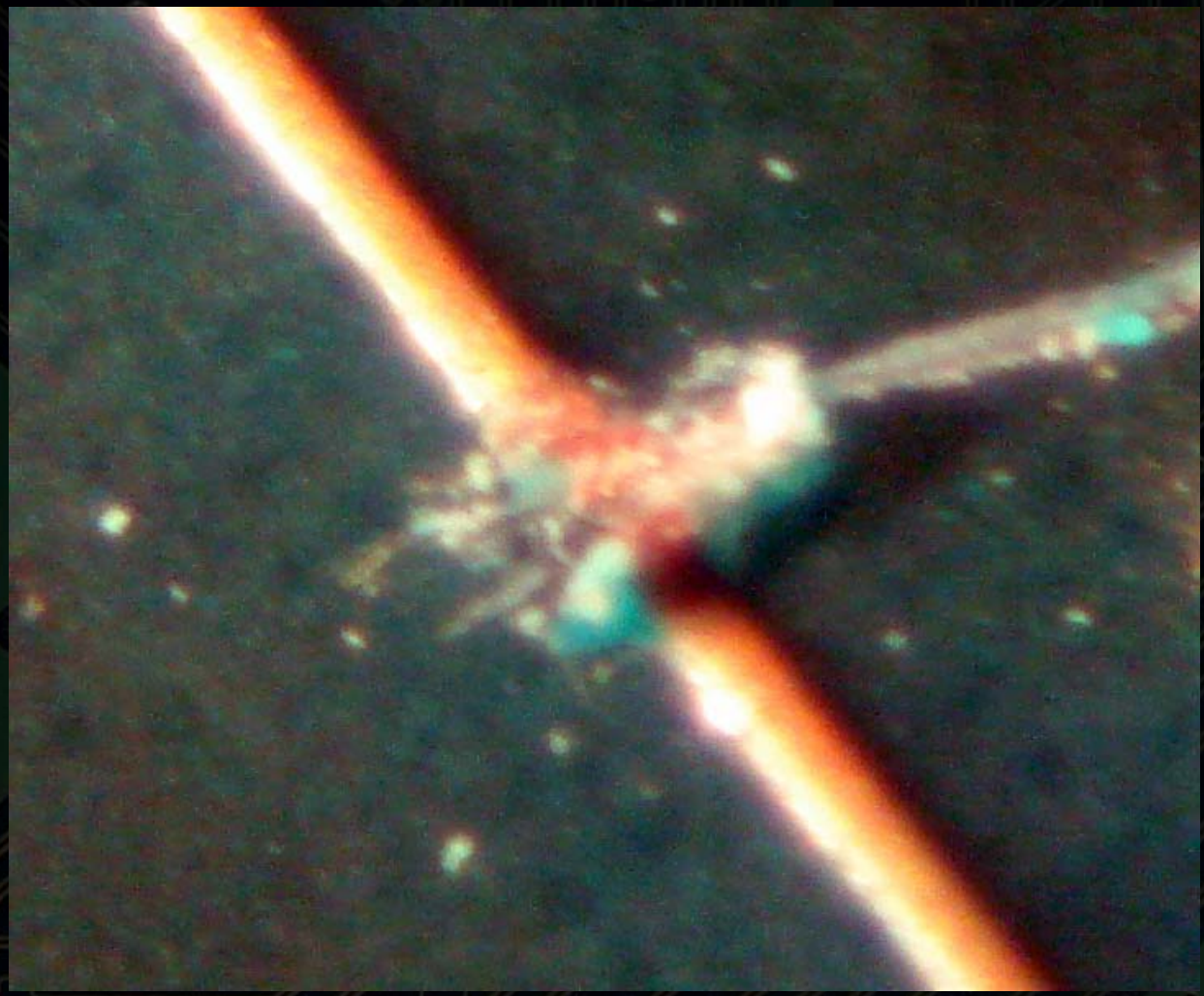
Trace Cutting (1)



Trace Cutting (2)



Trace Cutting (3)



Applied Knowledge

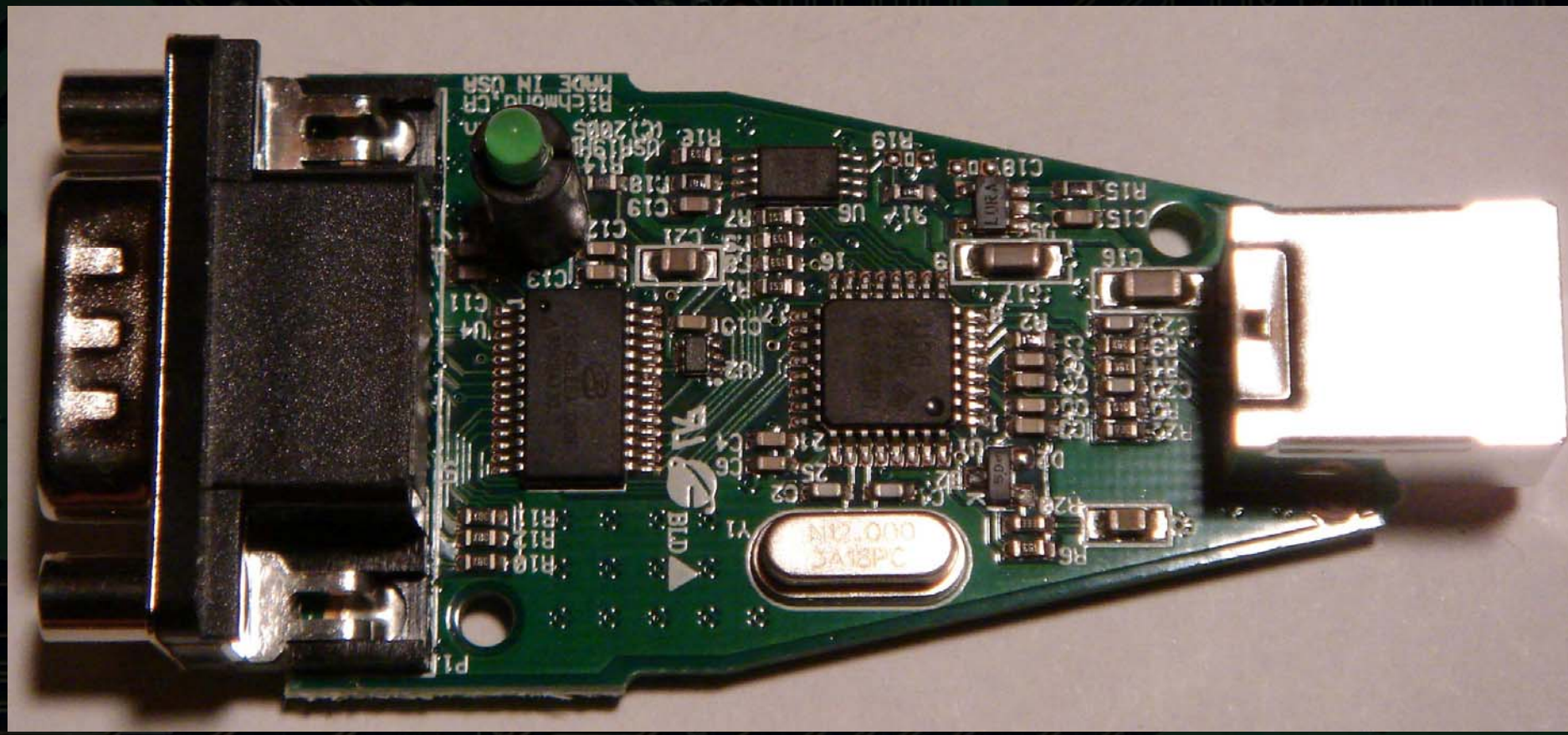
- Now starts the practical demo part…
  - Wish me luck!

Problem Statement

- Embedded devices often have an internal serial debug port
  - Connects directly to processor
  - Typical processors today can barely tolerate 3.3V, often times less
  - This is incompatible with plugging into your PC RS-232 port
    - RS-232 is an [ancient] high-voltage standard, requires signal swing of > +/- 7V to indicate 1's and 0's
  - Many computers don't even have an RS-232 port anymore
- Want a "quick and dirty" low voltage serial to USB converter—but you can't just buy one because it is non-standard

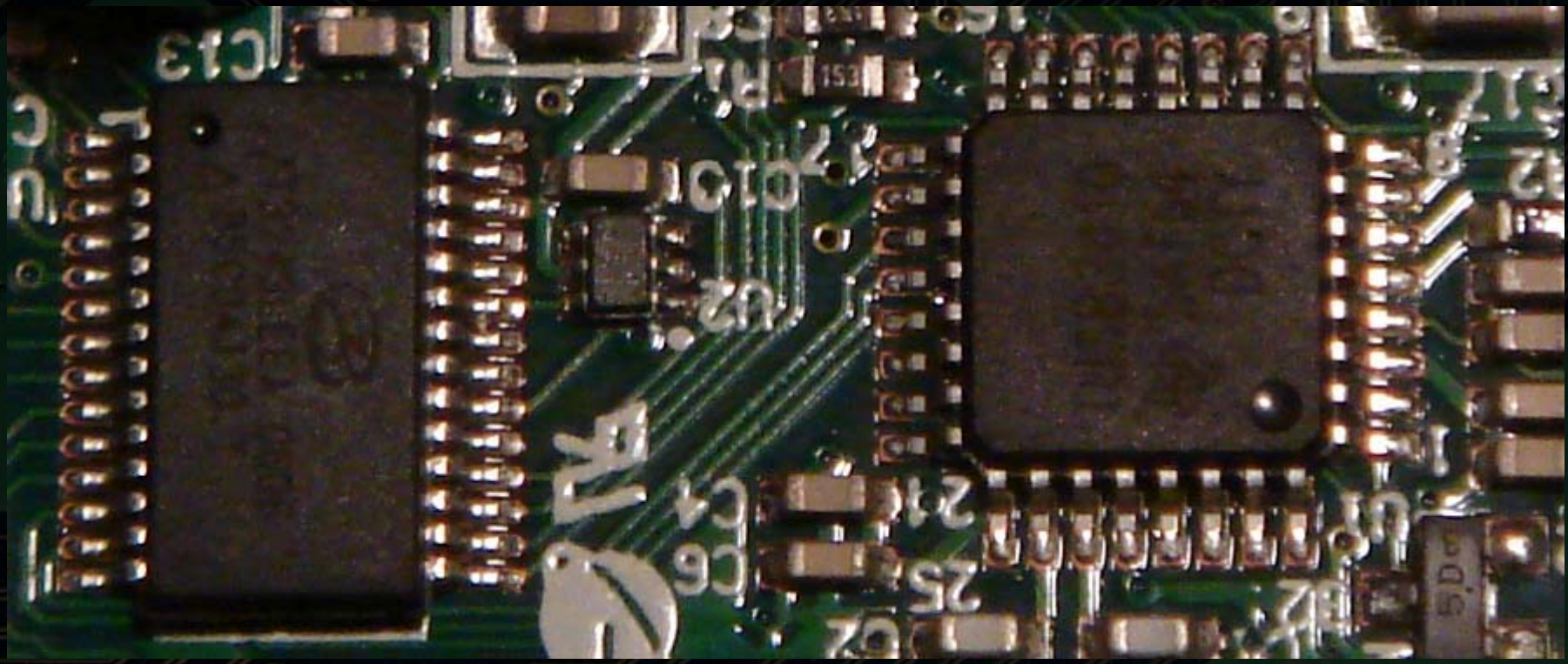
Solution

- Modify a stock RS-232 to USB dongle by pre-empting the internal low-voltage signals

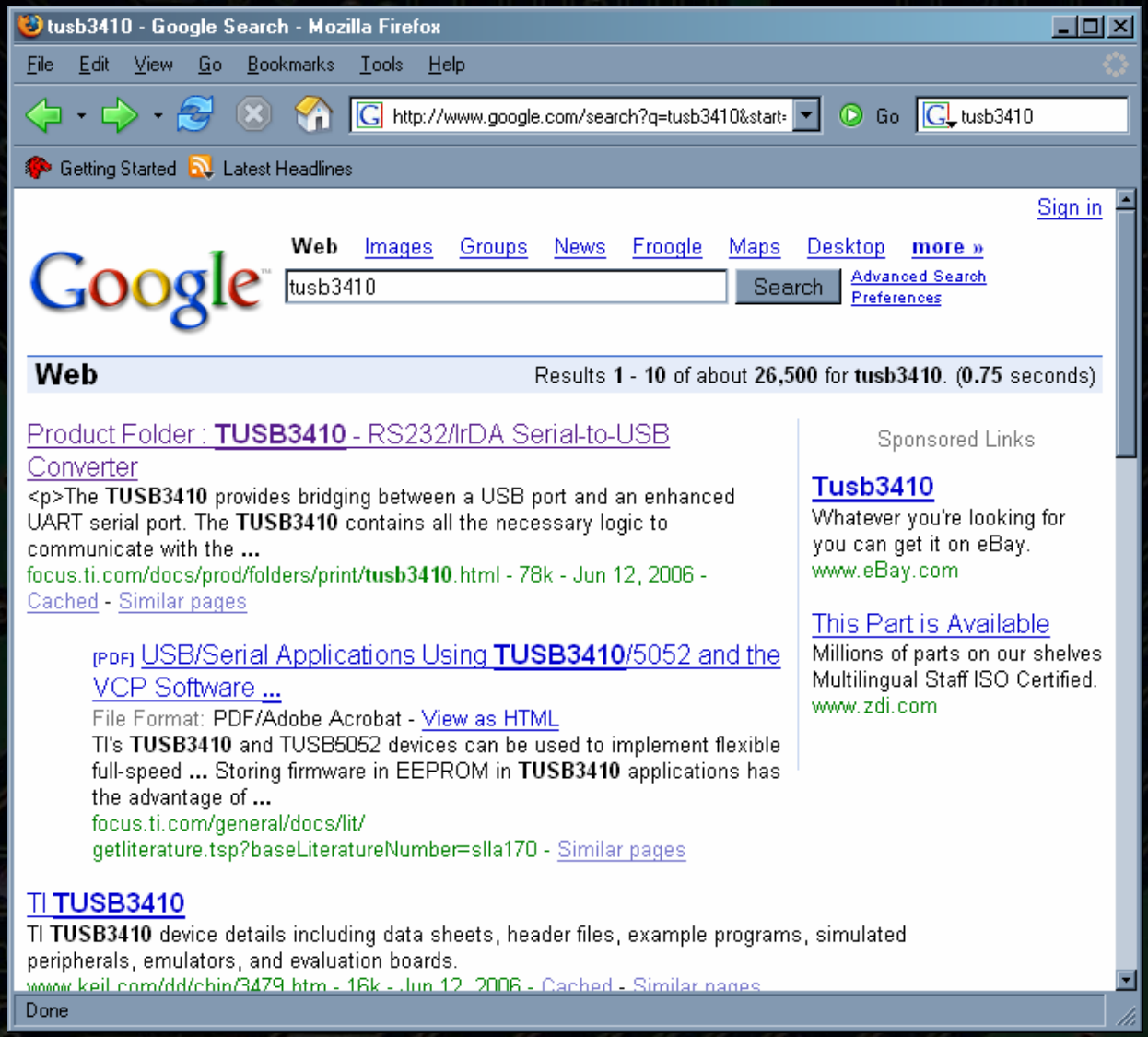


Key Parts

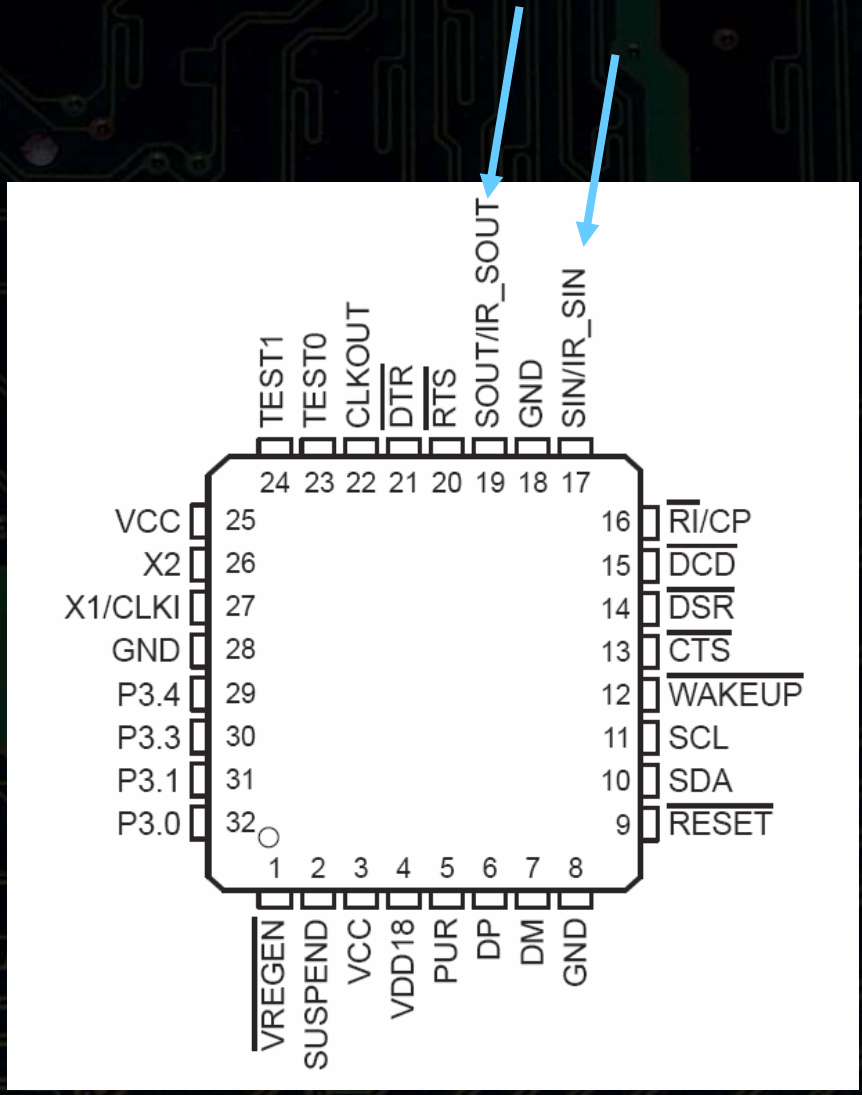
- TUSB3410 and ZT3243



Google!


tusb3410 - Google Search - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.google.com/search?q=tusb3410&start=
Go
tusb3410
Getting Started
Latest Headlines
Sign in
Google
Web Images Groups News Froogle Maps Desktop more »
tusb3410
Search
Advanced Search
Preferences
Web
Results 1 - 10 of about 26,500 for tusb3410. (0.75 seconds)
Product Folder : TUSB3410 - RS232/IrDA Serial-to-USB Converter
<p>The TUSB3410 provides bridging between a USB port and an enhanced UART serial port. The TUSB3410 contains all the necessary logic to communicate with the ...
focus.ti.com/docs/prod/folders/print/tusb3410.html - 78k - Jun 12, 2006 - Cached - Similar pages
[PDF] USB/Serial Applications Using TUSB3410/5052 and the VCP Software ...
File Format: PDF/Adobe Acrobat - View as HTML
TI's TUSB3410 and TUSB5052 devices can be used to implement flexible full-speed ... Storing firmware in EEPROM in TUSB3410 applications has the advantage of ...
focus.ti.com/general/docs/lit/getliterature.tsp?baseLiteratureNumber=slla170 - Similar pages
TI TUSB3410
TI TUSB3410 device details including data sheets, header files, example programs, simulated peripherals, emulators, and evaluation boards.
www.keil.com/dd/chip/3479.htm - 16k - Jun 12, 2006 - Cached - Similar pages
Sponsored Links
Tusb3410
Whatever you're looking for you can get it on eBay.
www.eBay.com
This Part is Available
Millions of parts on our shelves Multilingual Staff ISO Certified.
www.zdi.com
Done

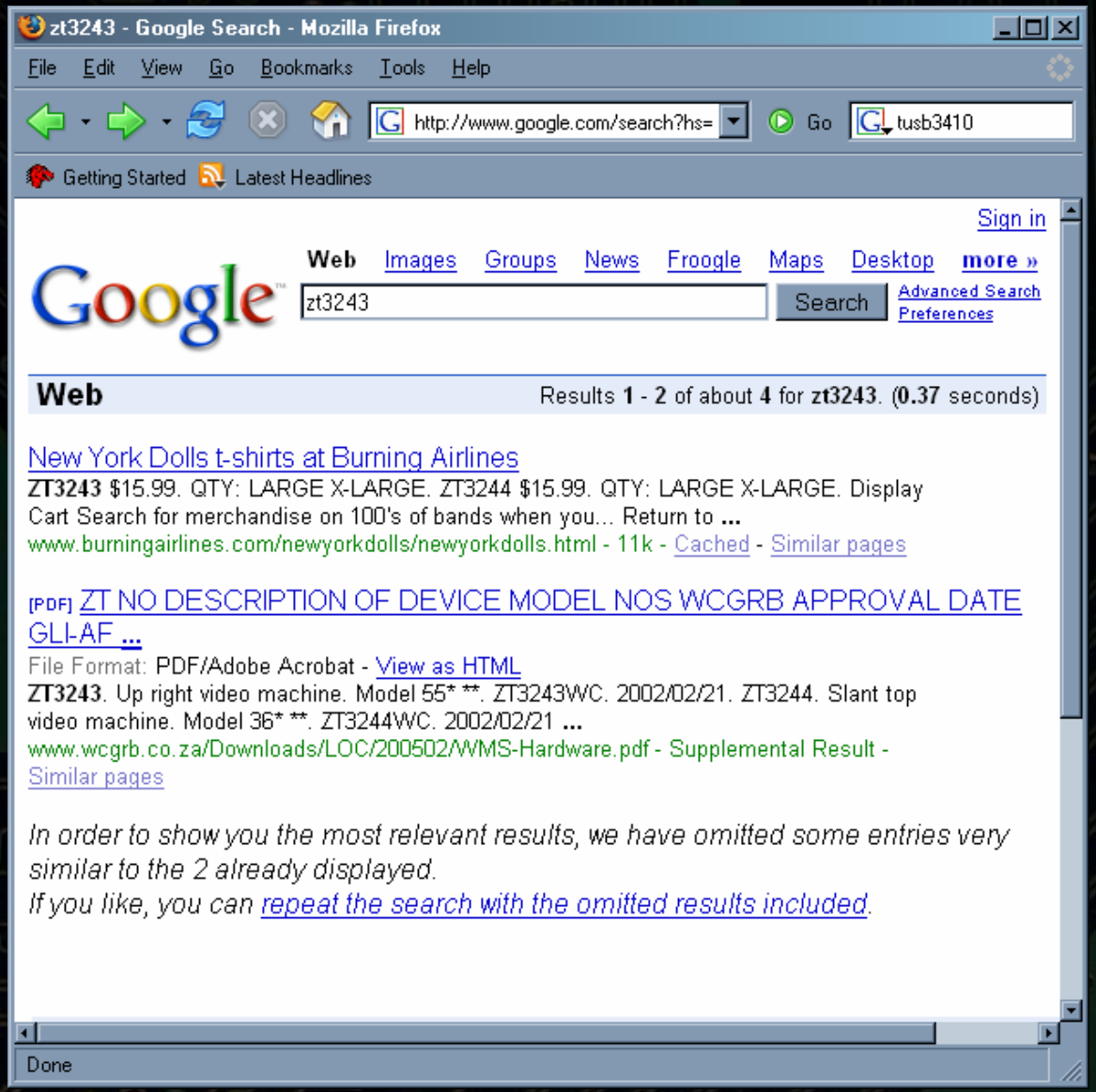
Pinout


TEST1
TEST0
CLKOUT
DTR
RTS
SOUT/IR_SOUT
GND
SIN/IR_SIN
24 23 22 21 20 19 18 17
VCC 25
X2 26
X1/CLKI 27
GND 28
P3.4 29
P3.3 30
P3.1 31
P3.0 32
16 RI/CP
15 DCD
14 DSR
13 CTS
12 WAKEUP
11 SCL
10 SDA
9 RESET
1 2 3 4 5 6 7 8
VREGEN
SUSPEND
VCC
VDD18
PUR
DP
DM
GND

Key Pins Described

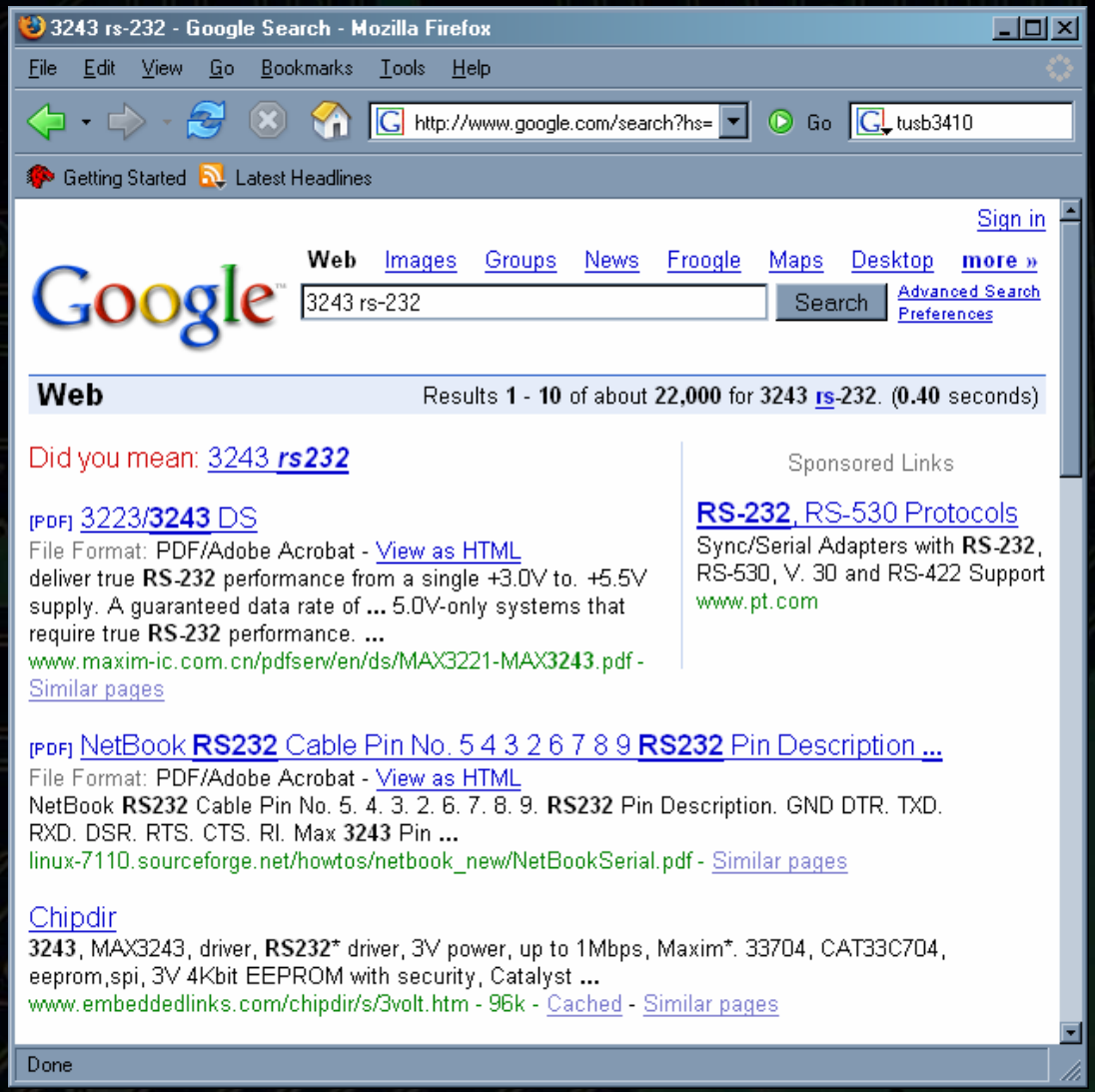
TERMINAL NAME	TERMINAL NO.	I/O	DESCRIPTION
SIN/IR_SIN	17	I	UART: Serial input data / IR Serial data input (see Note 6)
SOUT/IR_SOUT	19	O	UART: Serial output data / IR Serial data output (see Note 7)

Uh-oh…


zt3243 - Google Search - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.google.com/search?hs=
Go
tusb3410
Getting Started
Latest Headlines
Sign in
Web Images Groups News Froogle Maps Desktop more »
Google
zt3243
Search
Advanced Search
Preferences
Web
Results 1 - 2 of about 4 for zt3243. (0.37 seconds)
New York Dolls t-shirts at Burning Airlines
ZT3243 $15.99. QTY: LARGE X-LARGE. ZT3244 $15.99. QTY: LARGE X-LARGE. Display Cart Search for merchandise on 100's of bands when you... Return to ...
www.burningairlines.com/newyorkdolls/newyorkdolls.html - 11k - Cached - Similar pages
[PDF] ZT NO DESCRIPTION OF DEVICE MODEL NOS WCGRB APPROVAL DATE GLI-AF ...
File Format: PDF/Adobe Acrobat - View as HTML
ZT3243. Up right video machine. Model 55* **. ZT3243WC. 2002/02/21. ZT3244. Slant top video machine. Model 36* **. ZT3244WC. 2002/02/21 ...
www.wcgrb.co.za/Downloads/LOC/200502/WMS-Hardware.pdf - Supplemental Result - Similar pages
In order to show you the most relevant results, we have omitted some entries very similar to the 2 already displayed.
If you like, you can repeat the search with the omitted results included.
Done

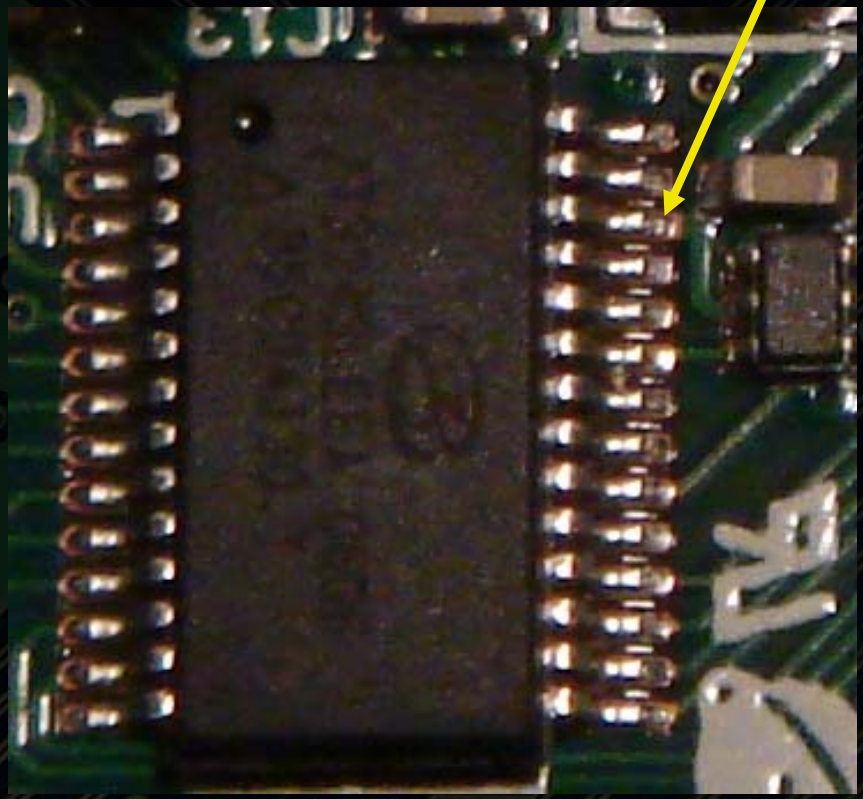
Guesswork

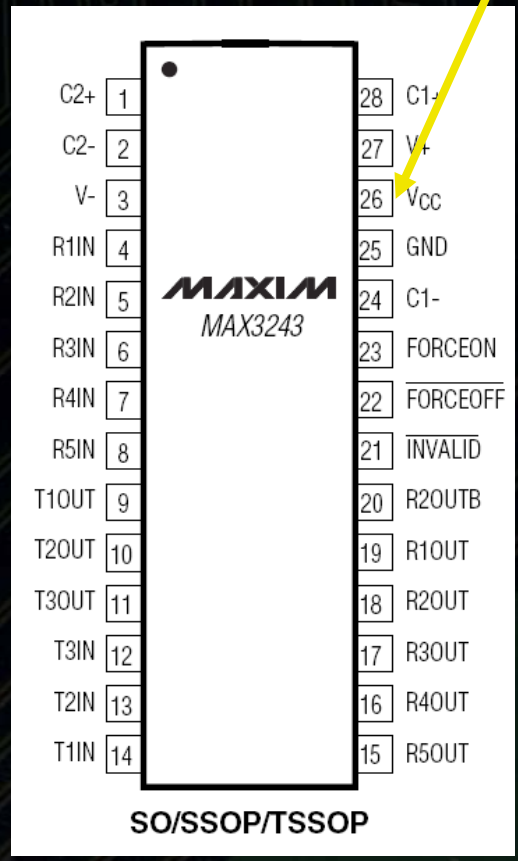
- Ah-hah!
  - ZT (whoever they are) are cheap Asian knock-offs of American chips
  - Cross-reference base part number to American version and pray



Looks like a match

- Right number of pins
- Thicker power connections line up…

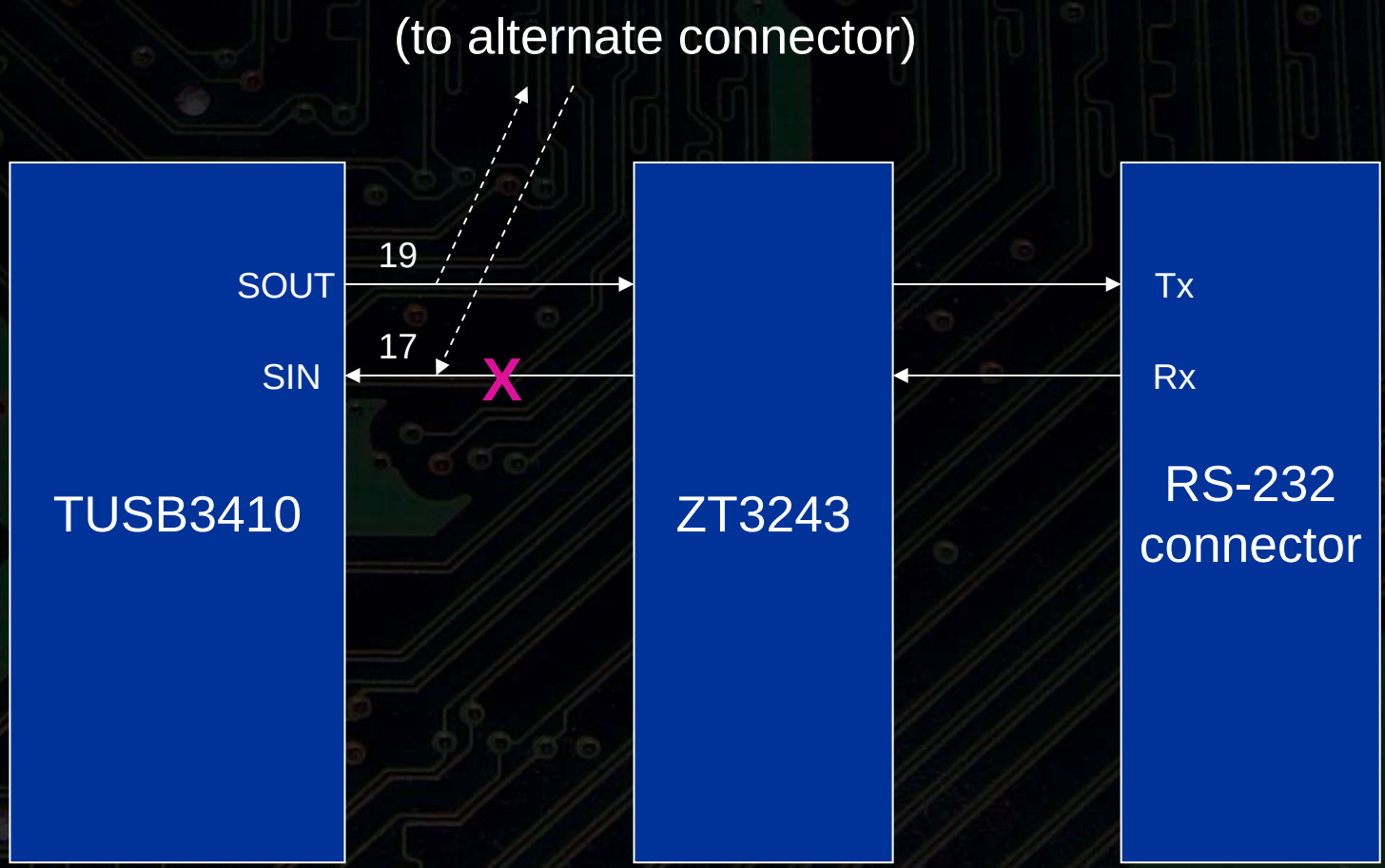




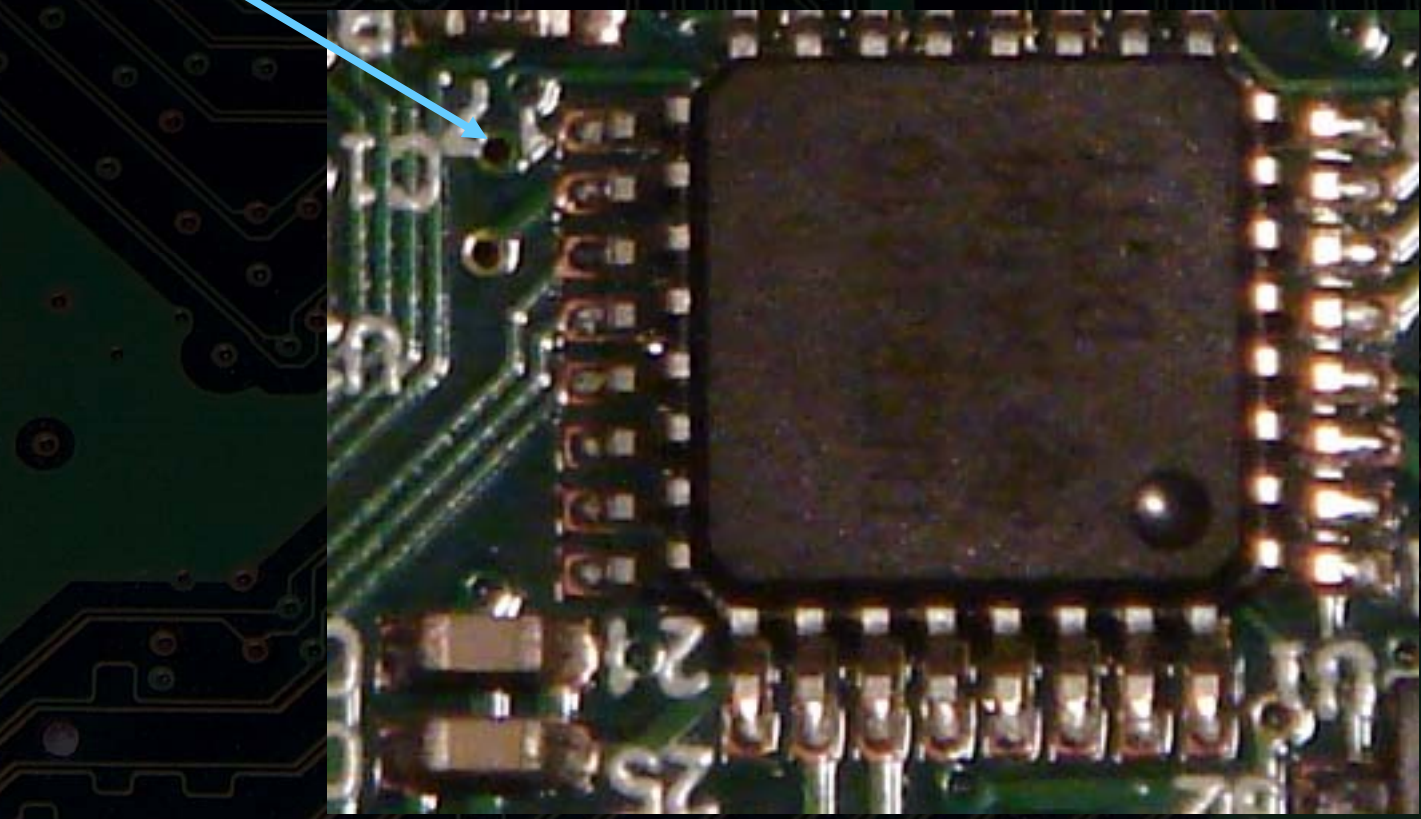
Datasheets

- Datasheets typically contain:
  - Product overview
  - Pinout and pin function
  - Electrical parameters and functional limits for engineering
  - Application data
  - Package drawings
  - For processors, additional data is provided
    - Programming model, etc.

Basic Idea


(to alternate connector)
19
17
SOUT
SIN
X
TUSB3410
ZT3243
Tx
Rx
RS-232
connector

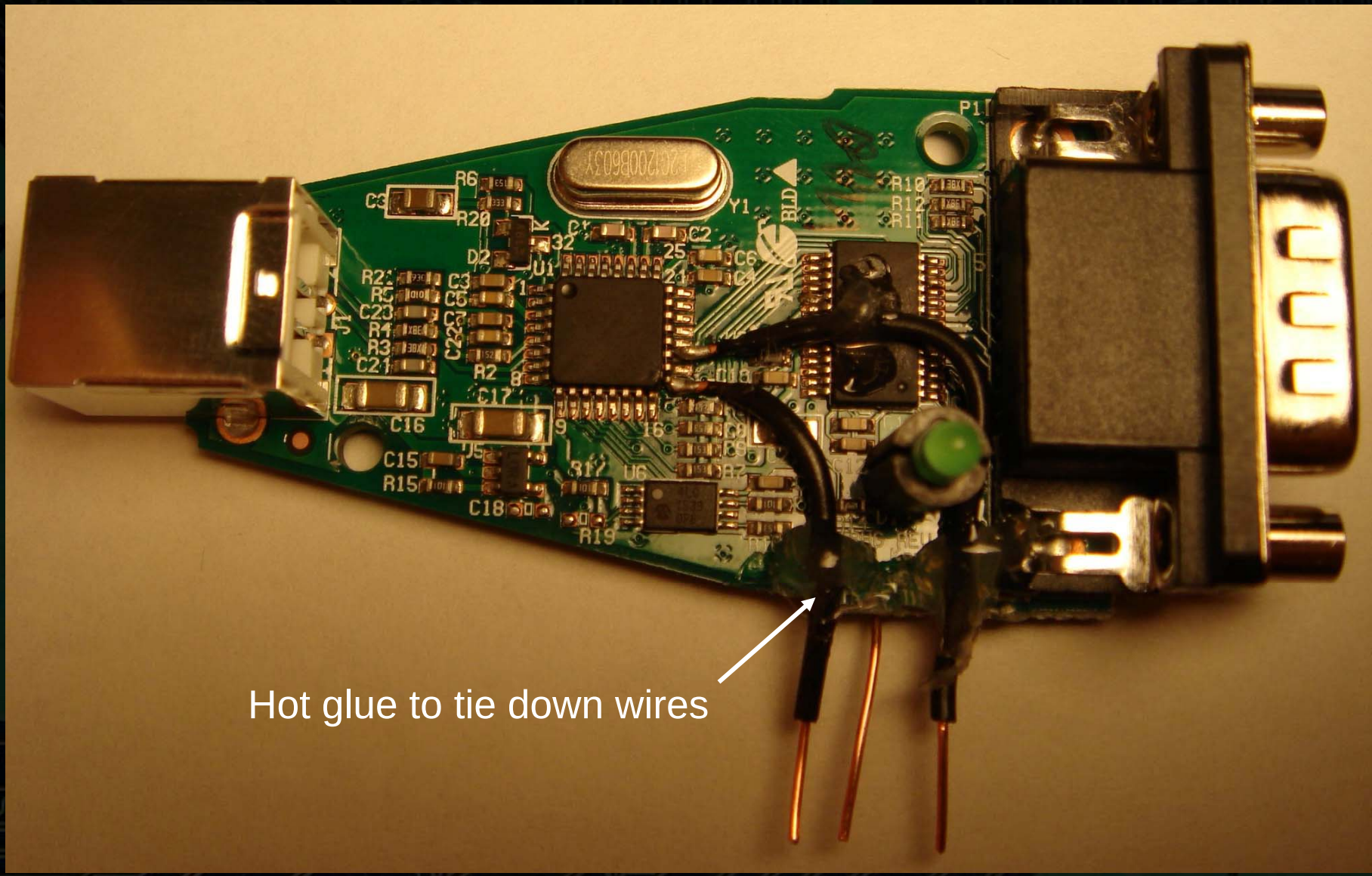
Tracing The SIN



Cut to Live Demo

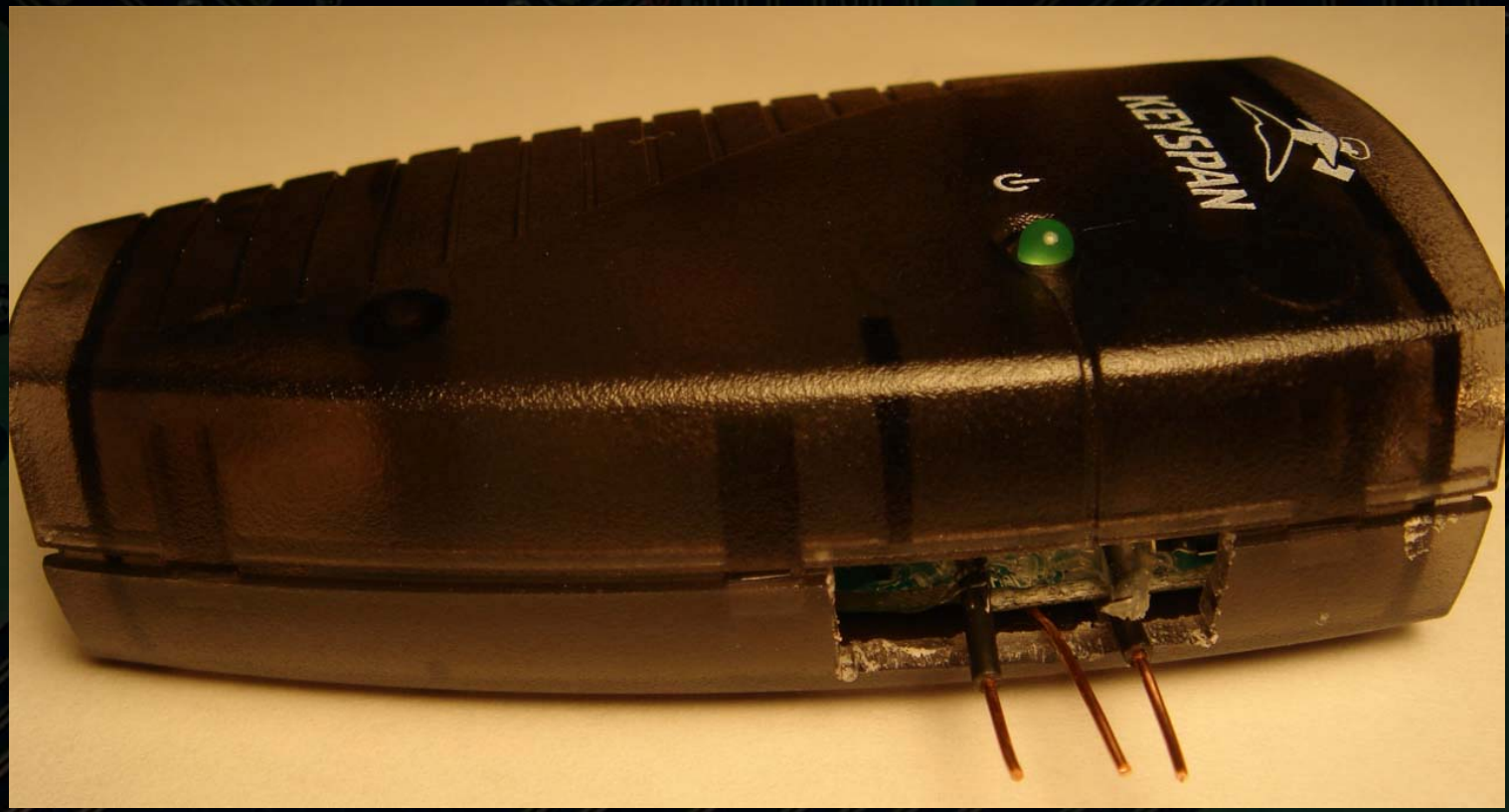
- Cut SIN
- Solder 2x wires
- Clear soldermask
- Add ground wire
- Glue to tack it all down

Finished Patch



Finished Patch

- Dremel out hole to make it look nice (thanks hb!)



Q&A

- Thanks for your attention!