CSCI 4974 / 6974
Hardware Reverse Engineering

Lecture 16: Printed circuit board RE

Homework 2: PCB RE

- Due last day of class, teams of 2
- Go to one of the tech dumps and find a PCB
- Take photos of both sides, both overview and closeups of interesting areas
- Identify as many ICs as you can
- Draw a block diagram of the board and make a ~10 minute presentation describing its functionality

Today's agenda

- Common structures and what they mean
  - Full circuit extraction leaves nothing to chance
  - But it's sloow!
  - What part of the board is interesting?

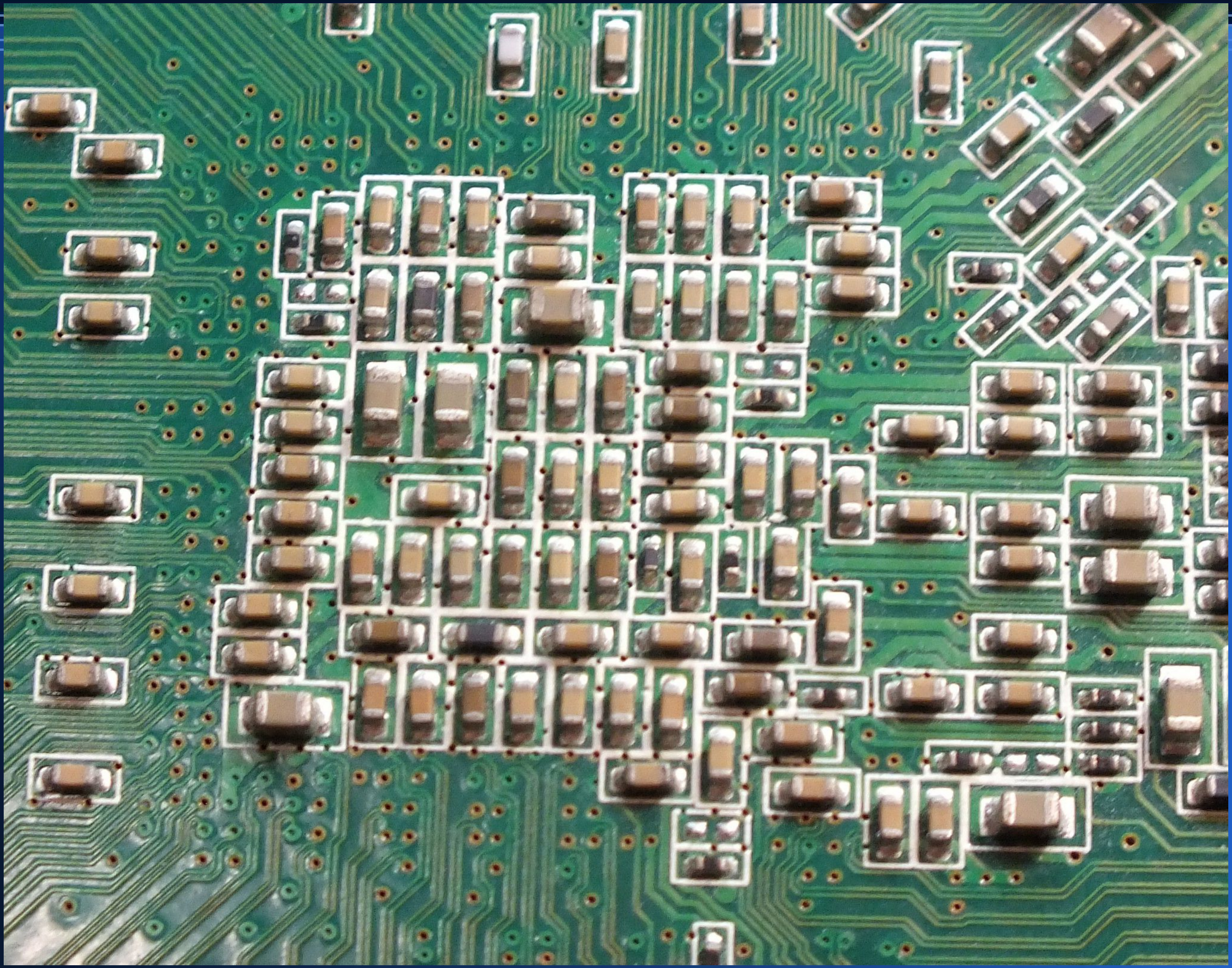
Part datasheets

- Extremely helpful in IDing unknown parts
- Even if you can't get the full datasheet you may find a “product brief” that hints at its function
- alldatasheet.com and family are useful for finding obsolete/rare datasheets

Decoupling capacitors

- Local power filtering for high-speed devices
  - Generally tiny ceramic caps
  - Surrounding device on top side
  - Underneath device on bottom side
- Lots of them indicate a large, complex device
  - This is usually obvious just by looking at it
  - Can be helpful at finding things you can't see
  - Ex: bottom-side board photo in press release

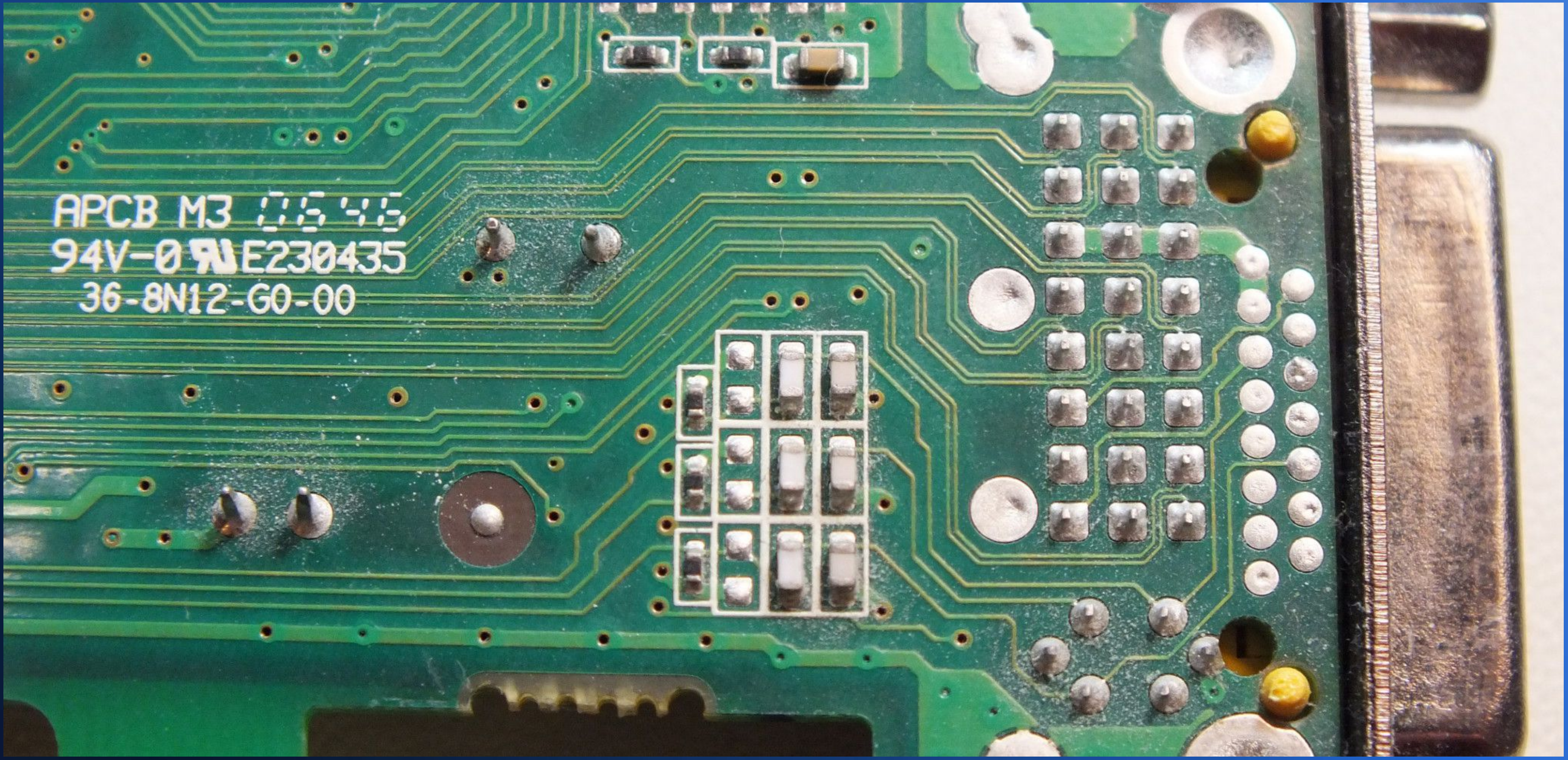
Decoupling capacitors



Differential pairs

- Represent signal as difference of two voltages
  - 1 if X_P > X_N, else 0
- Better noise immunity
  - Noise couples into both sides approx. equally
- Less radiated EMI
  - Smaller loop area = less efficient antenna
- Often an indicator of high-speed serial data
  - DVI, HDMI, SATA, PCIe, Ethernet, DisplayPort

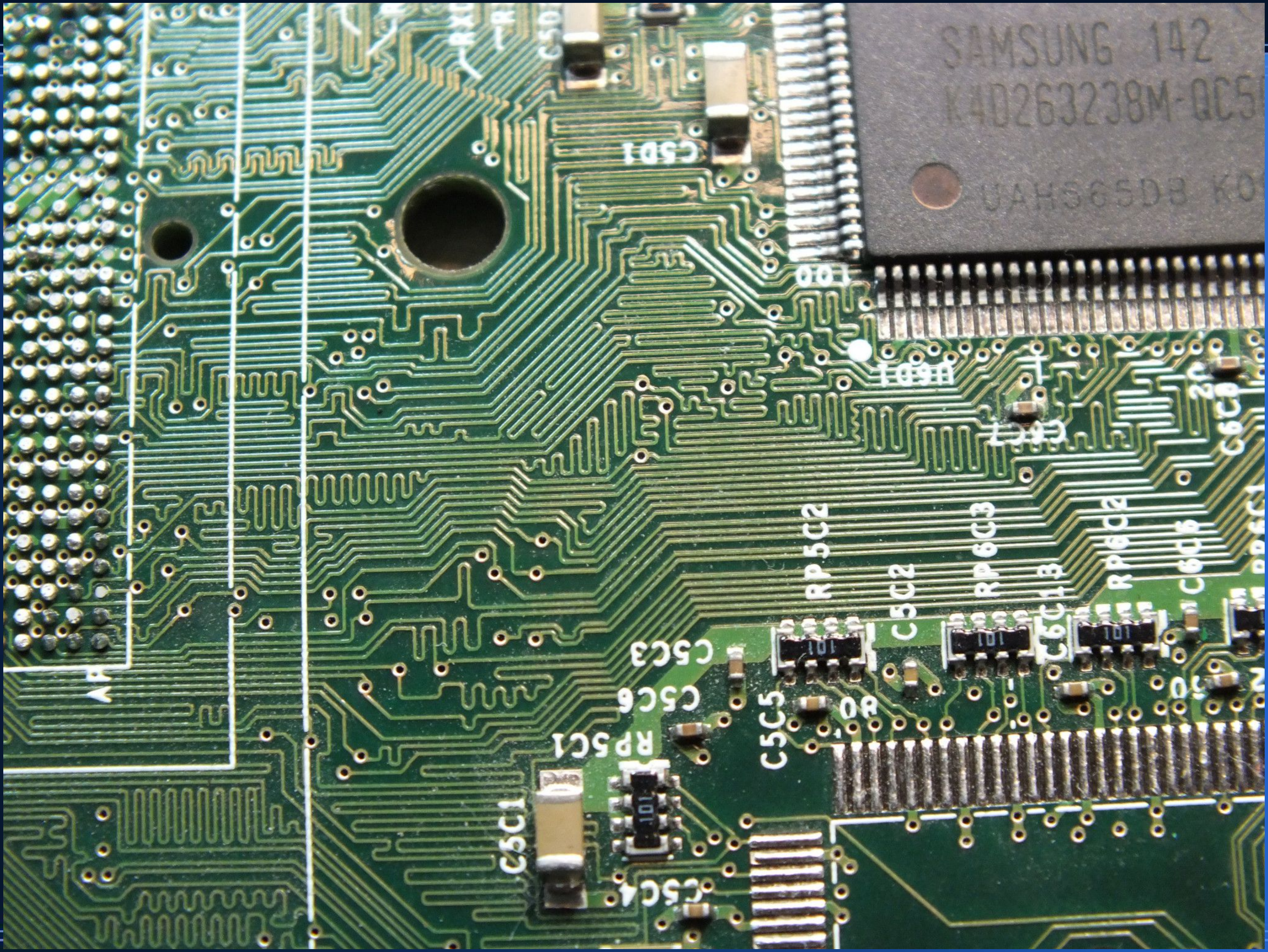
Differential pairs



Length matching

- May be seen on single-ended or differential
- Used for minimizing skew on fast signals
- Typically a sign of a high-speed data bus

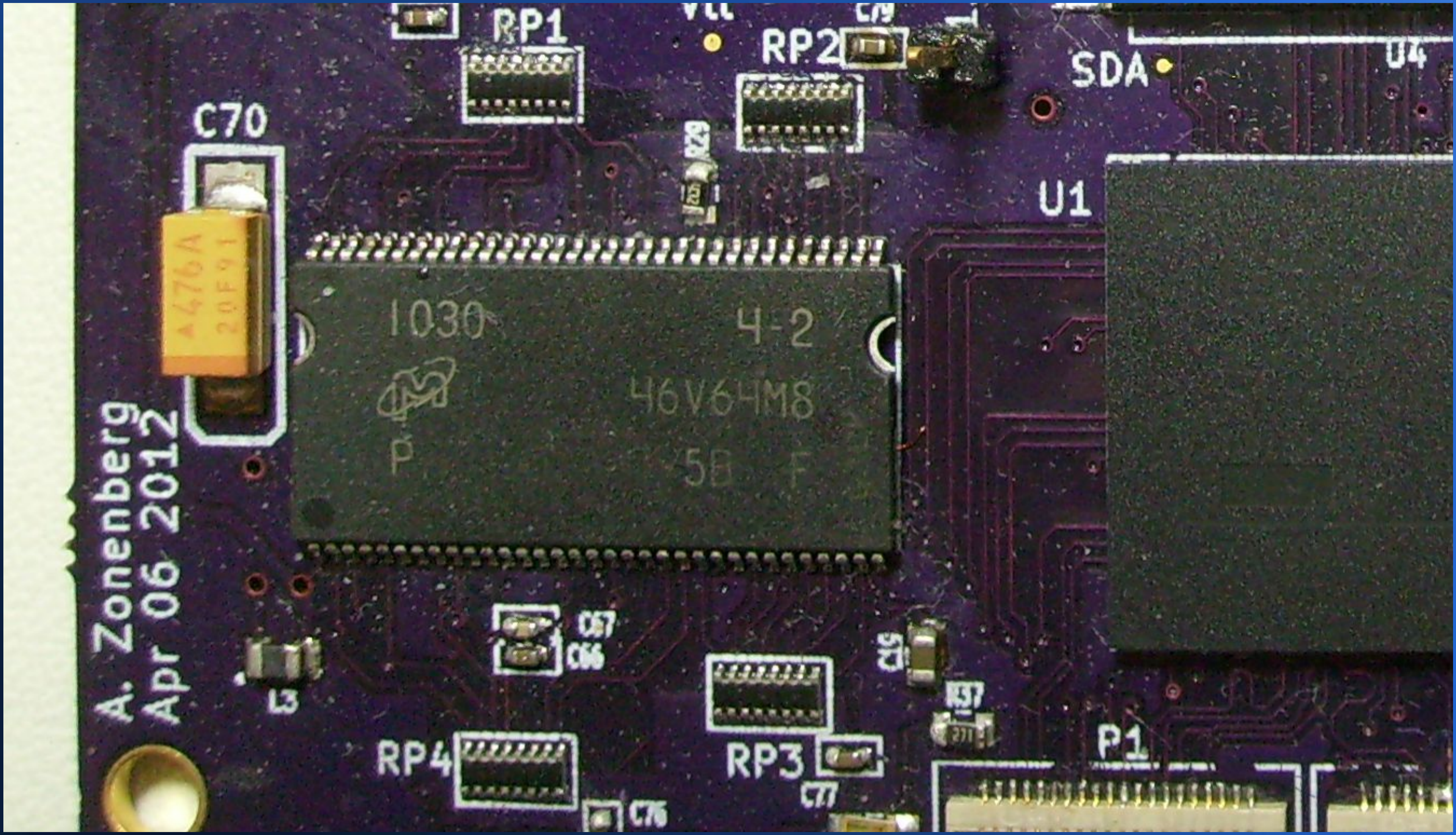
Length matching



DRAM

- DDR and older may be TSOP
- DDR2/3 are BGAs
  - Three rows of balls in each of two columns
  - Several lengths (78, 96 balls) for x4/x8/x16

DDR SDRAM


RP1
Vcc
C79
RP2
SDA
U4
C70
R29
U1
A476A
20F91
1030
4-2
46V64M8
P
5B F
A. Zonenberg
Apr 06 2012
C67
C66
C15
L3
R37
RP4
RP3
C77
P1
C76

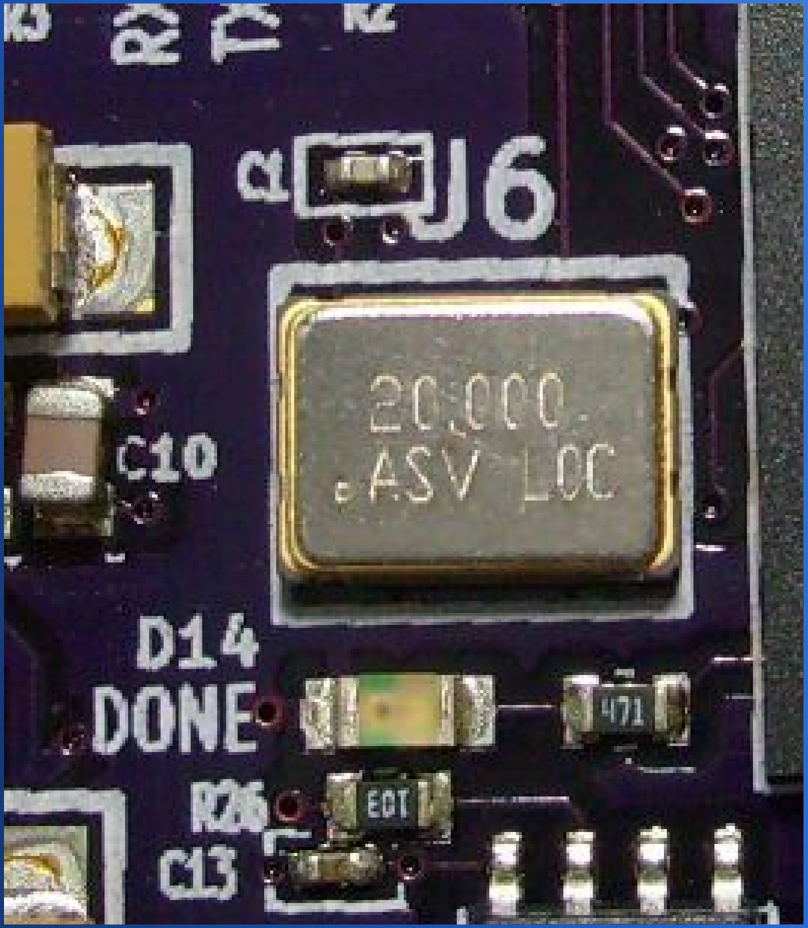
DDR2 SDRAM

DRAM

- Volatile memory
- May be possible to sniff with fast oscilloscope
- Lines are very sensitive to interference
    - Careful setup required to keep system working

Crystals/oscillators

- Small metal cans
  - may be TH or SMD
- Usually labeled with a frequency in MHz



Crystals/oscillators

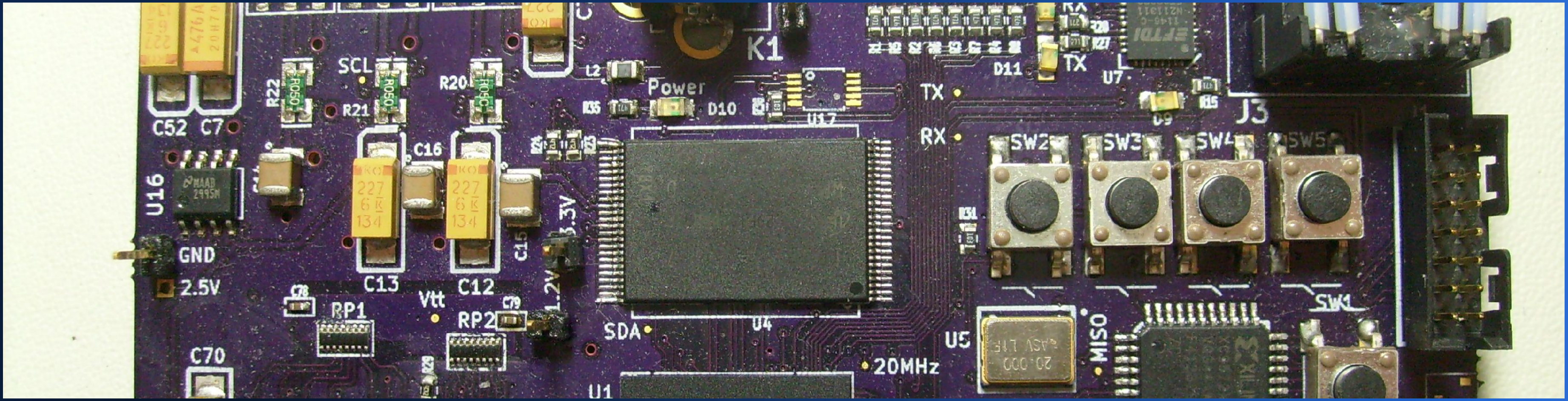
- Frequency markings may hint at circuit function
  - 32768 Hz = realtime clock
  - 3.579545 MHz = NTSC video colorburst
  - 4.43361875 MHz = PAL video colorburst
  - 6/12/24/48 MHz = USB
  - 25 MHz = Ethernet
  - Others
    - http://en.wikipedia.org/wiki/Crystal_oscillator_frequencies

Crystals/oscillators

- Possible attack point for clock glitching
- Harder to exploit if target has PLL :(

NAND flash

- Wide TSOP, 48 pins
  - Same package is sometimes used for NOR
- Easy to dump, but without FTL may be hard to make sense of image

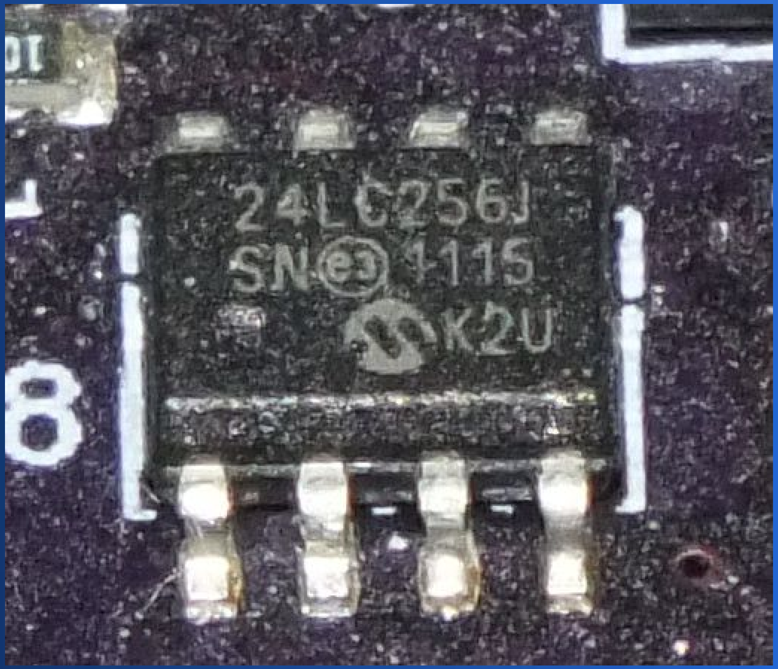


NAND flash

- Sometimes seen in large BGAs
- These are usually only used in SSDs etc

Serial EEPROM

- Usually SOIC8, rarely SSOP or CSBGA
- Part numbers usually have “24” plus a number for capacity
  - 24LC16 = 16 Kb
  - 24C256 = 256 Kb

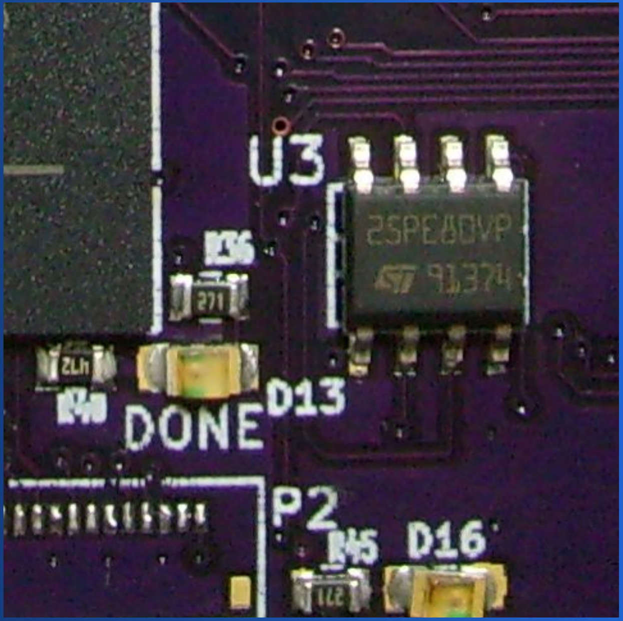


Serial EEPROM

- Compatible parts made by many vendors
- Sizes range from 128 bits to 2 Mb
- Standardized 2-wire I2C serial interface
- Can desolder and dump, or sniff in circuit
  - Big SOIC pins are easy to get probe clips onto

Serial NOR flash

- Usually SOIC8, sometimes socketed DIP8 or larger SOIC with some unused pins
- Part numbers often have “25” plus a number for capacity
  - N25Q128 = 128 mbits
  - M25PE80 = 8 mbits



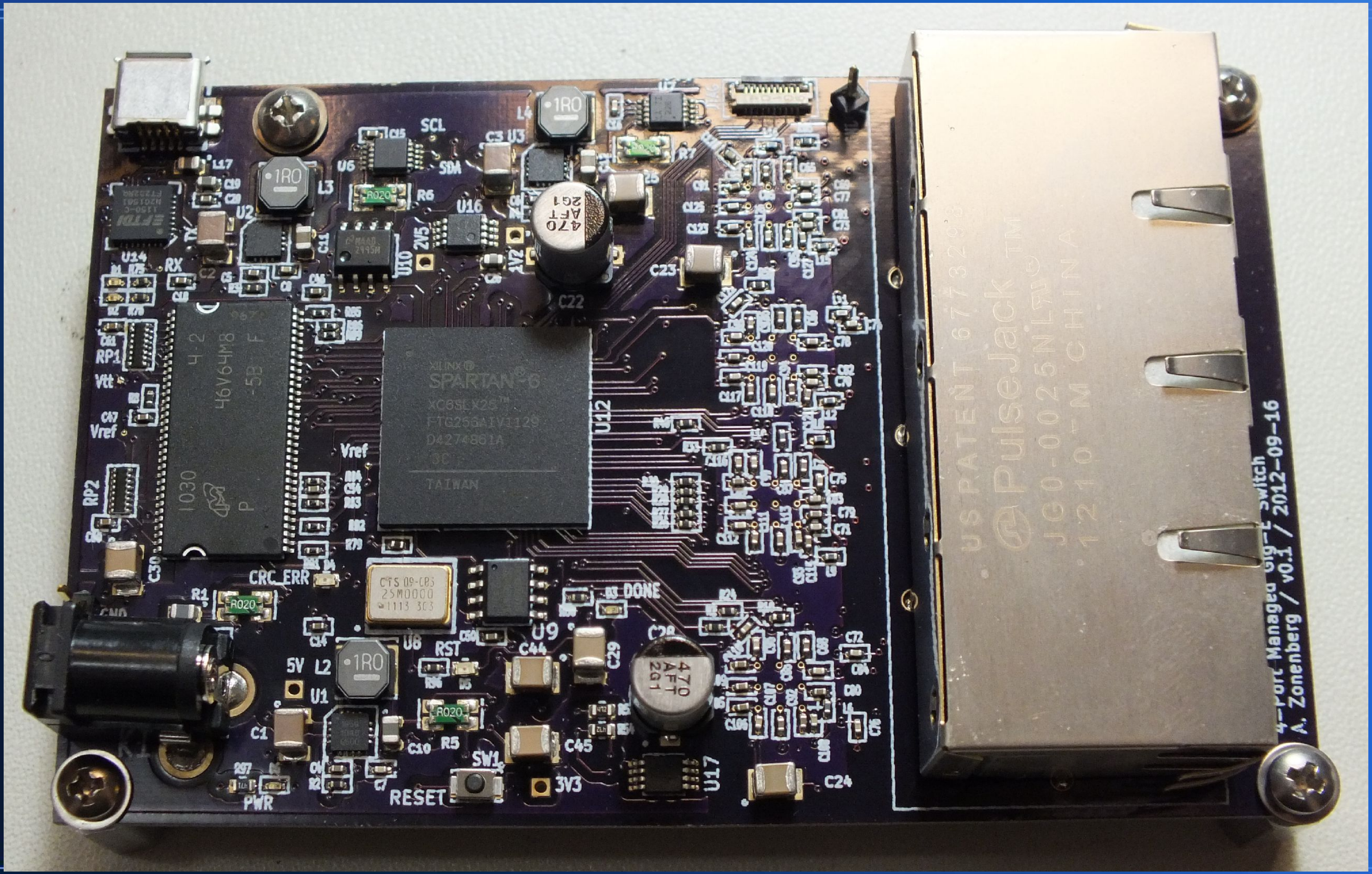
Serial NOR flash

- Compatible parts made by many vendors
- Sizes range from 512Kb to 1Gb
- Standardized 4-wire SPI serial interface
- Can desolder and dump, or sniff in circuit
  - Big SOIC pins are easy to get probe clips onto

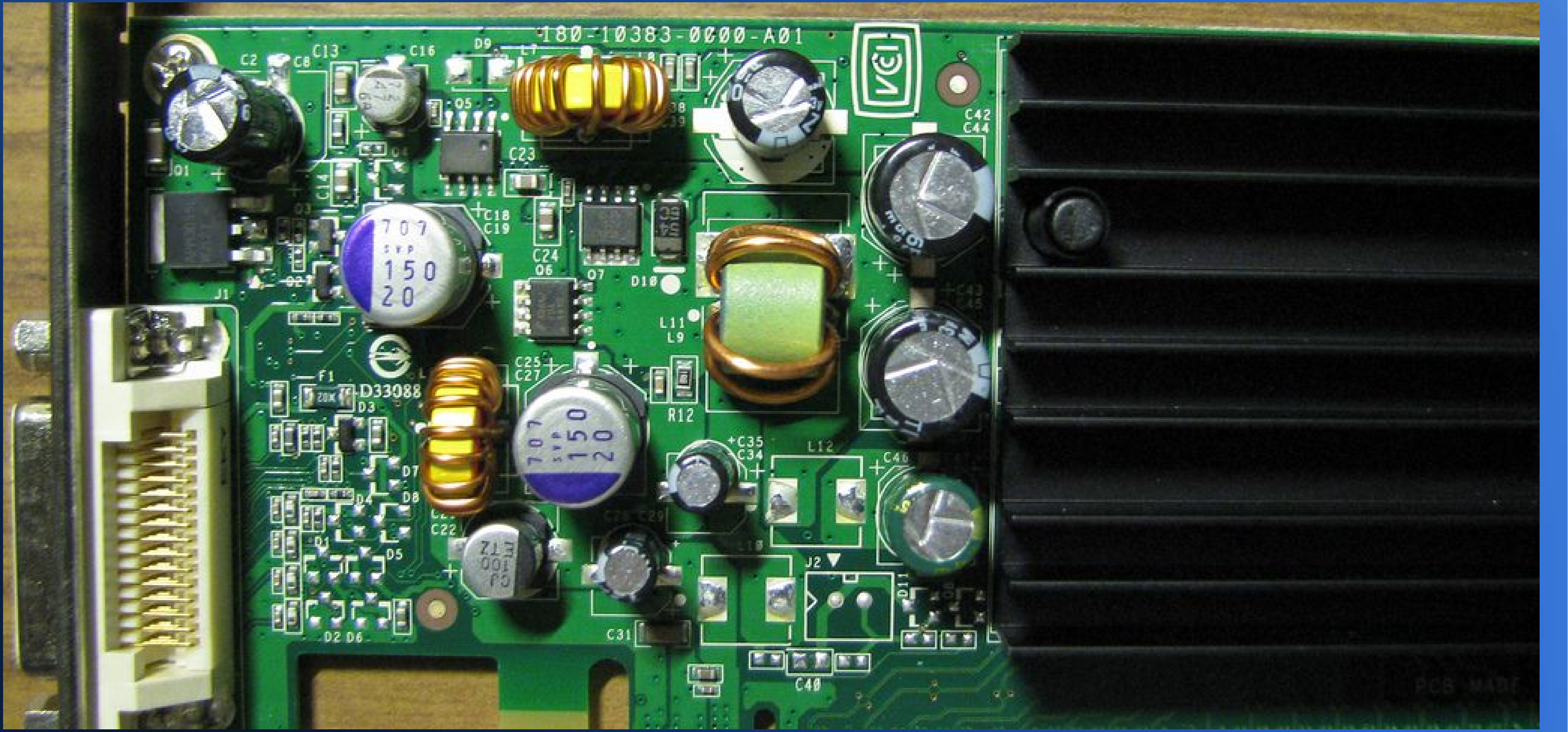
DC-DC switching power supplies

- Single controller chip
  - Usually low-pin-count QFN/BGA/SSOP
- Two or more large capacitors
- One large inductor

Find the SMPS (3 total)

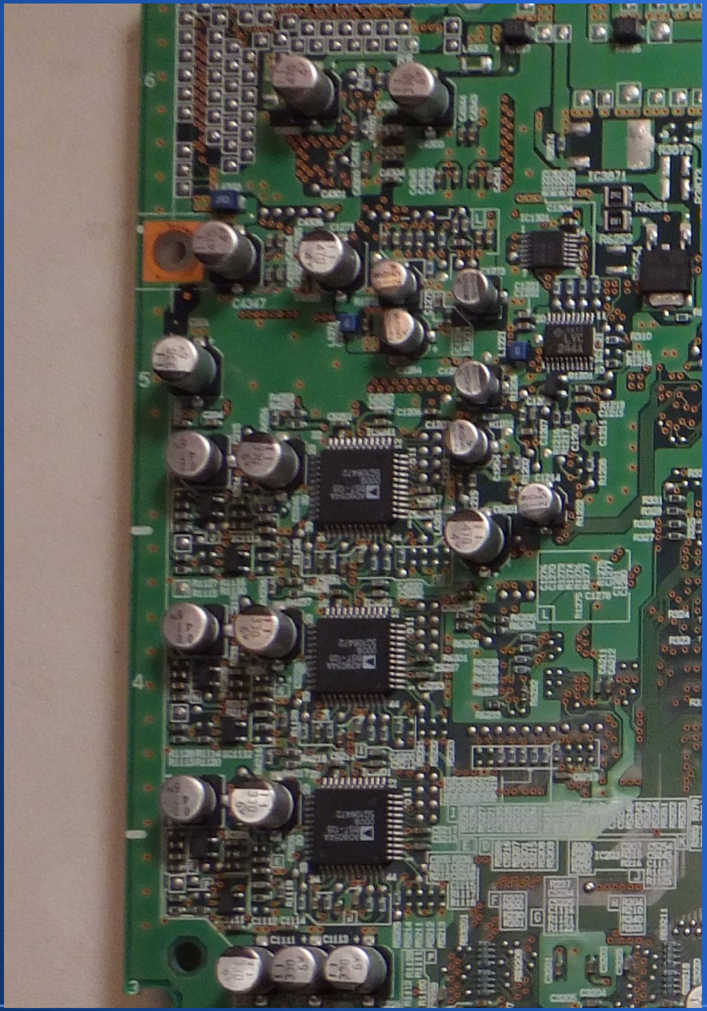


Find the SMPS (3 total)



Video processing

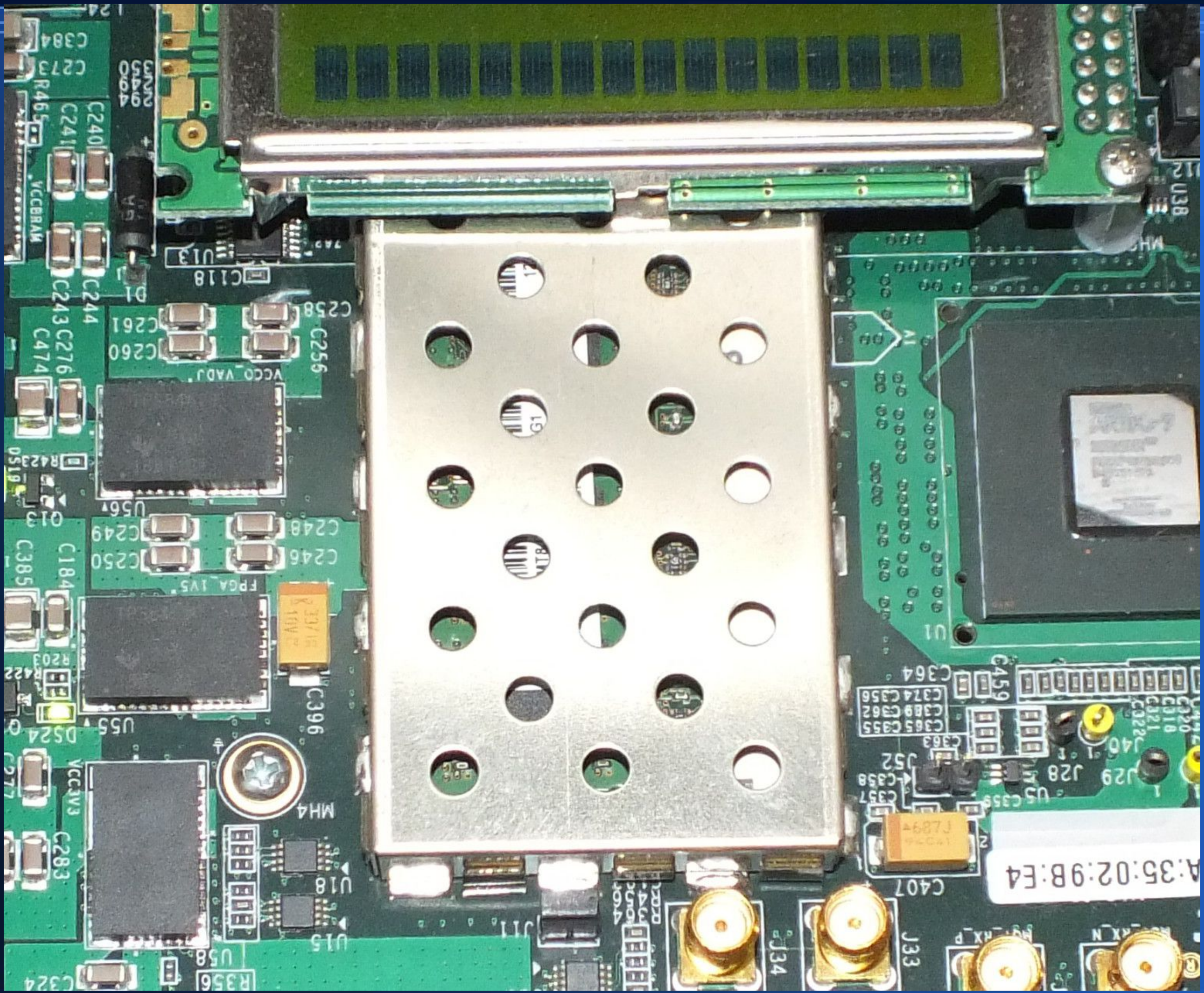
- Anything in threes
  - Fast ADCs
  - Fast DACs
  - RAM



EMI cans

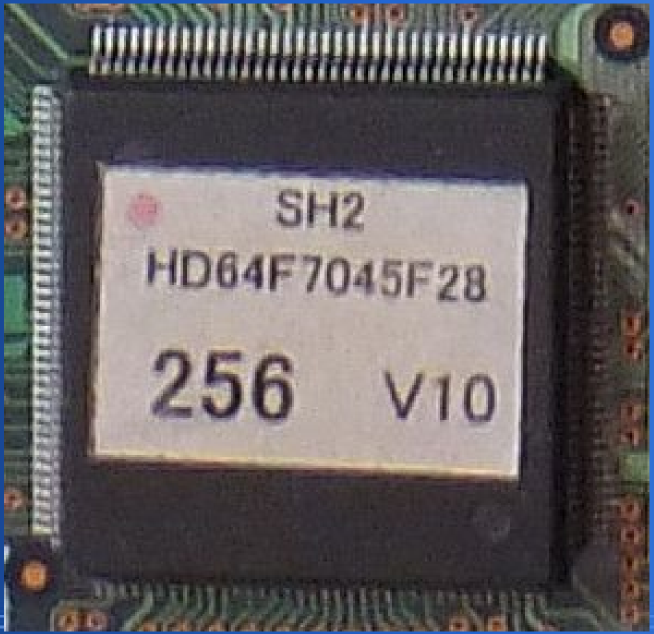
- Metal “can” soldered over part of the board
- Keeps interference from crossing
- Used to shield
  - Noisy stuff (keep radiated emissions down)
  - Sensitive stuff (keep external noise out)
- Usually, not always, a sign of RF communications

EMI cans



Firmware version labels

- Stick-on label with numbers and text
- Also can be a color-coded ink dot
- Denotes something programmable
  - May contain valuable data



Program/debug ports

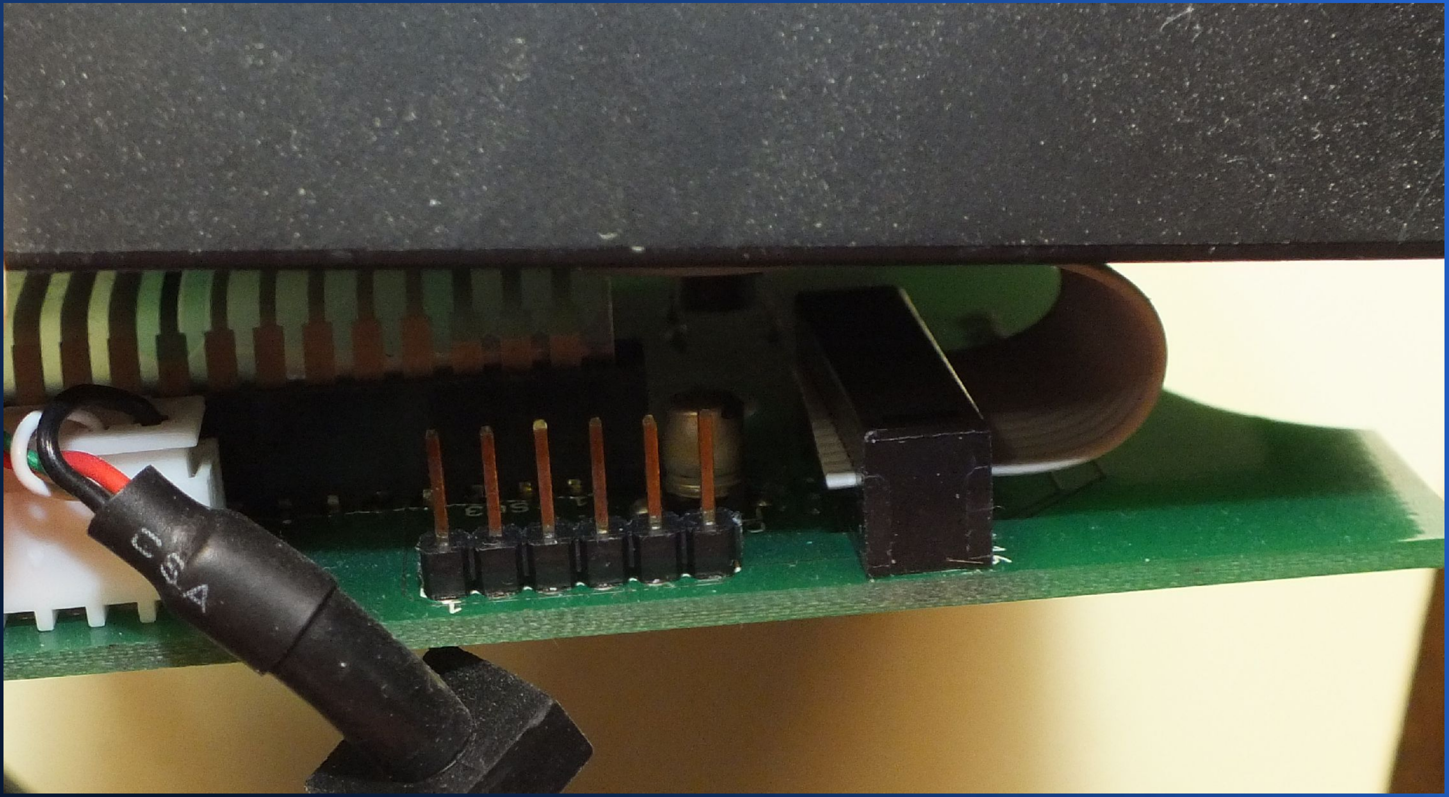
- Extremely useful!
  - May allow full control of target board
  - Even if firmware readout is disabled, JTAG boundary scan may allow some connectivity to be extracted
- Pads may be present even if connector isn't populated
  - You should recognize common pinouts

Microchip ICSP

- Used with PIC microcontrollers
- Five or six pins at 0.1” pitch
  - MCLR (chip reset)
  - Vdd
  - Vss
  - PGD (bidir serial data)
  - PGC (serial clock)
  - PGM/LVP (low-voltage prog mode, optional)

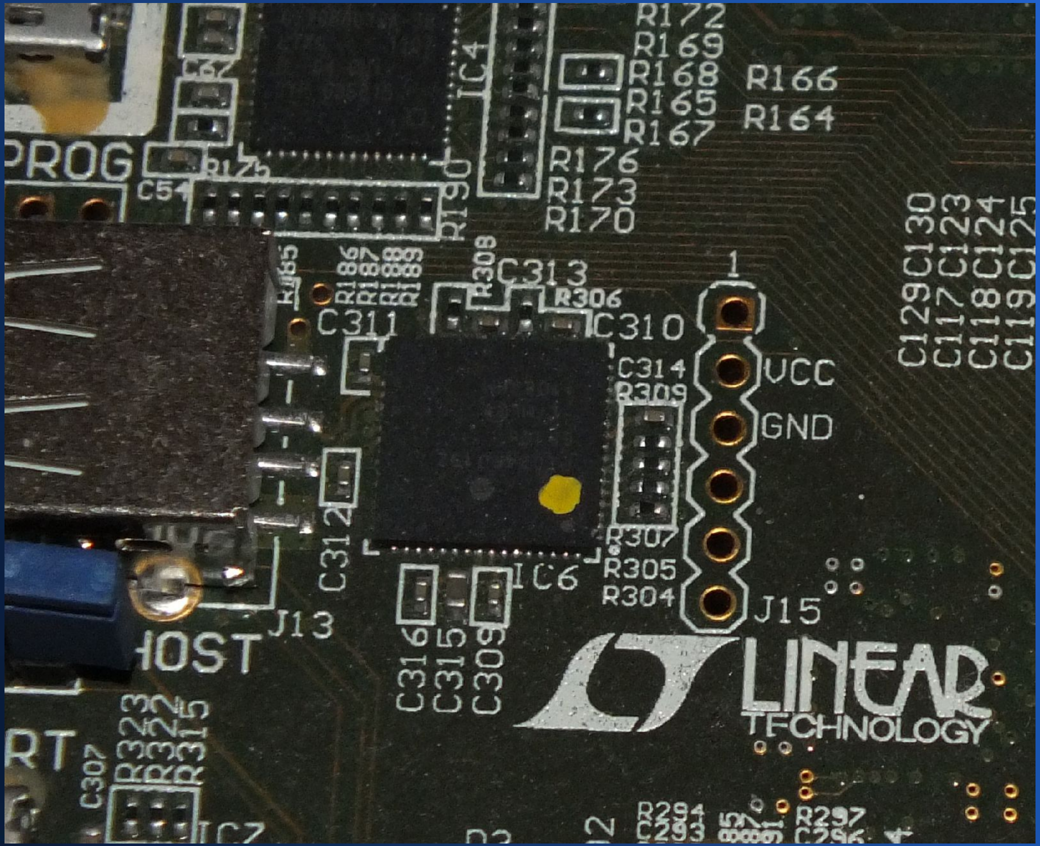
Microchip ICSP

- Male pins on USB keypad



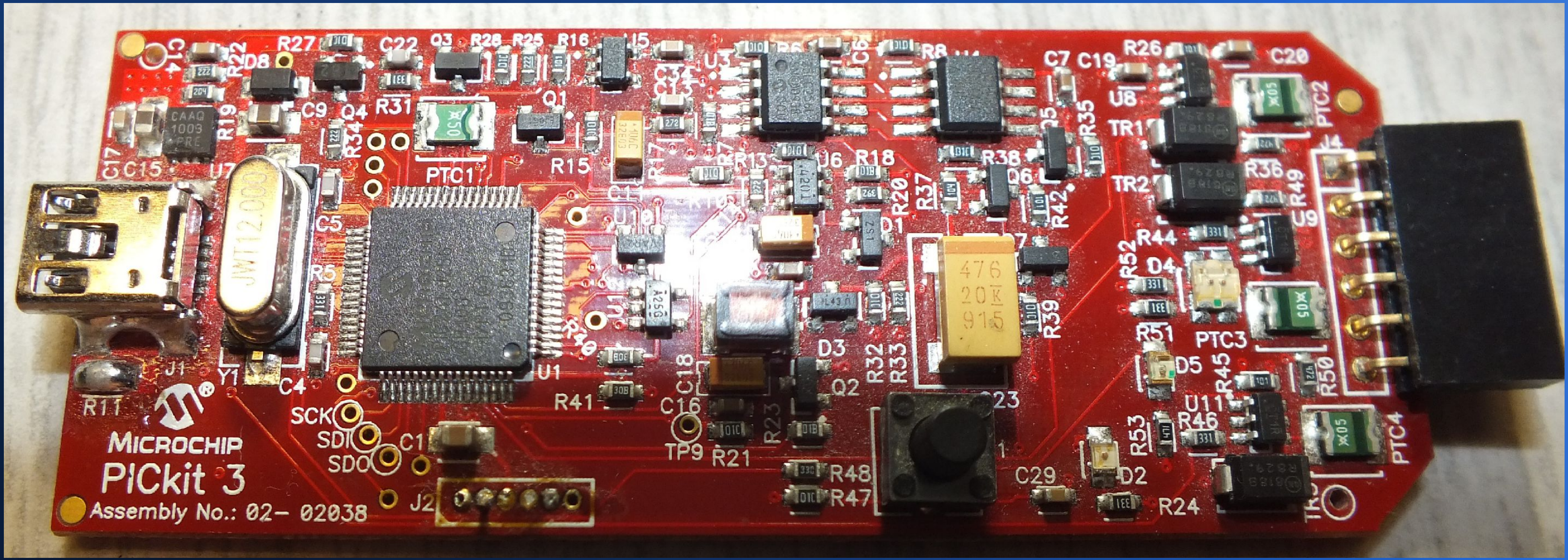
Microchip ICSP

- Unpopulated on Digilent Atlys

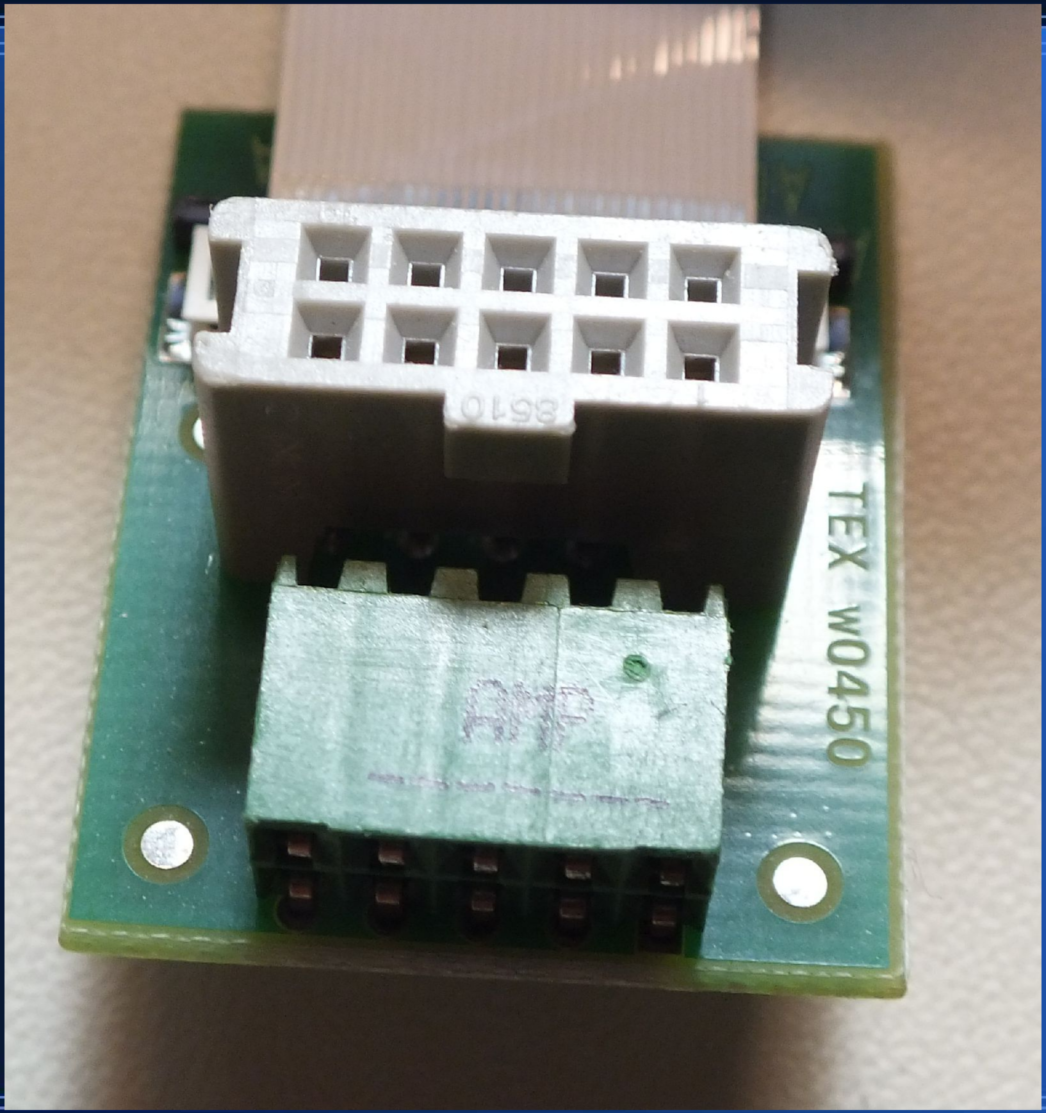


Microchip ICSP

- Fine-pitch (0.05”) unpopulated on PICkit3

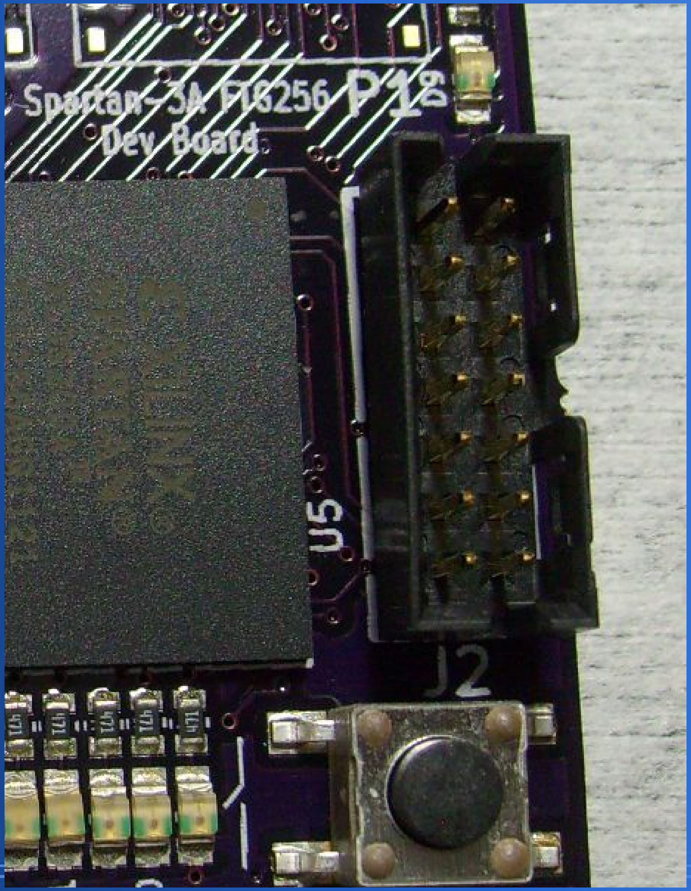


AVR ISP



Xilinx JTAG

- Used with Xilinx FPGA/CPLD devices
- 2x7 pins at 2mm pitch
  - Usually a keyed connector



ARM JTAG/SWD

- ARM makes IP cores, not silicon
- Several common pinouts in use

Traditional ARM JTAG/SWD

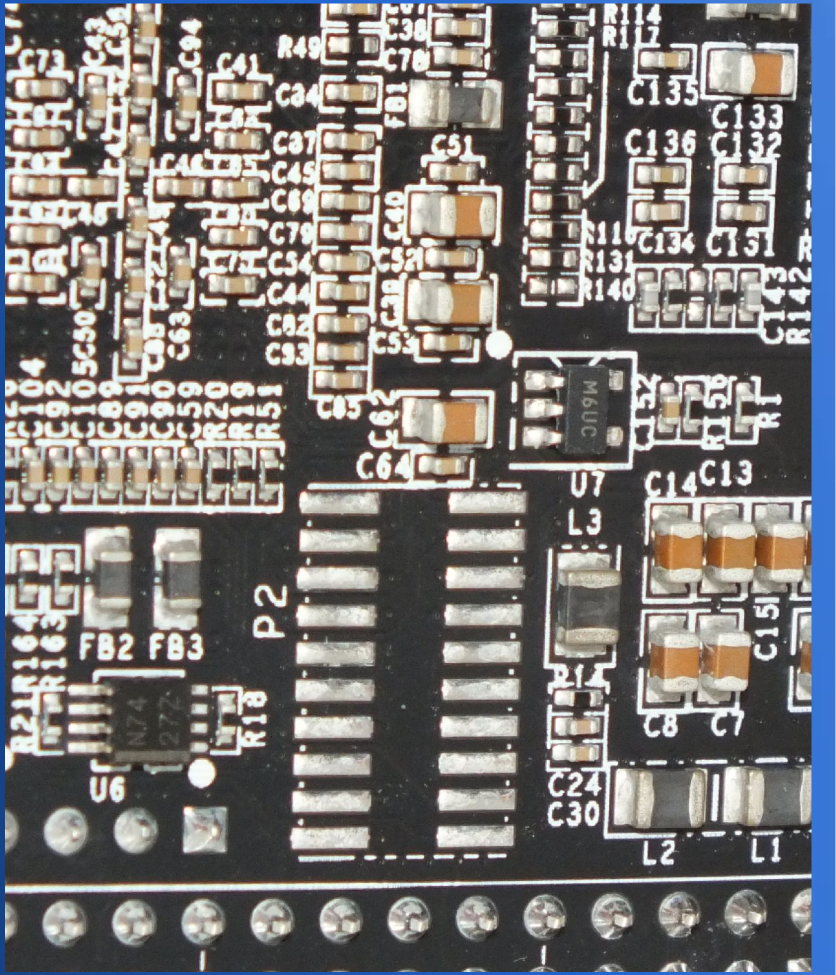
- 20 pin 0.1”
- No examples handy :(

Cortex JTAG/SWD

- 10 pin 0.05”
- No examples handy :(

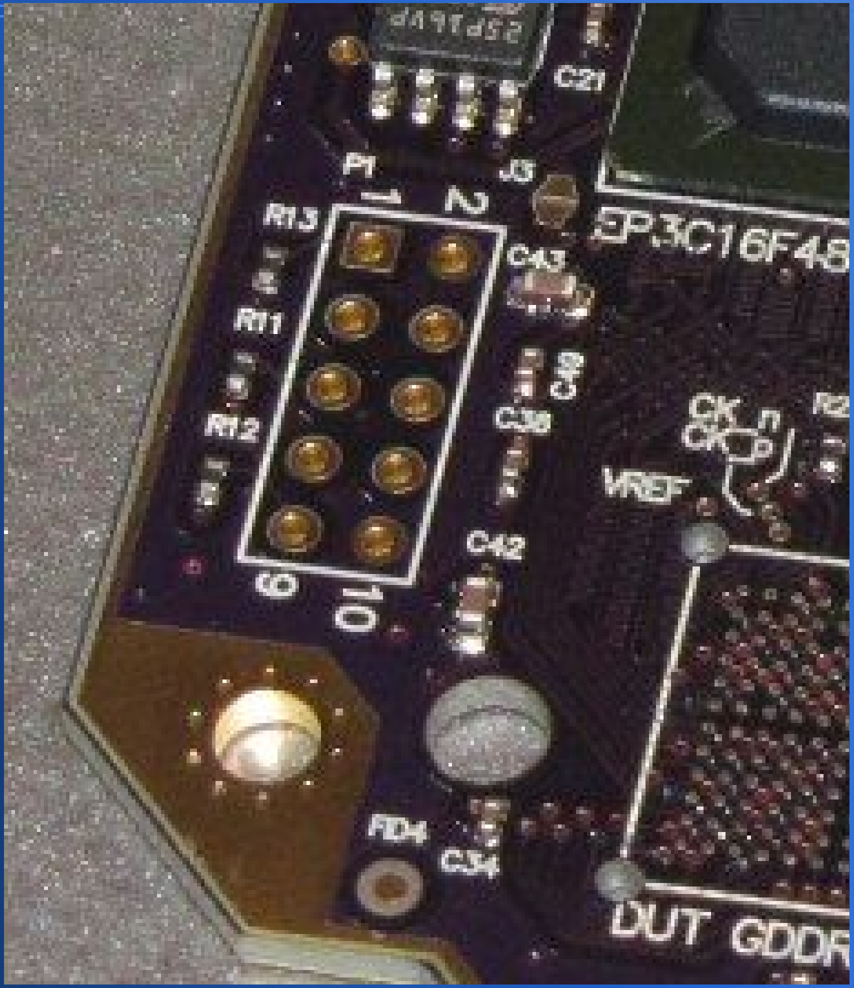
Cortex JTAG/SWD + trace

- 20 pin 0.05” on BeagleBone Black (not populated)



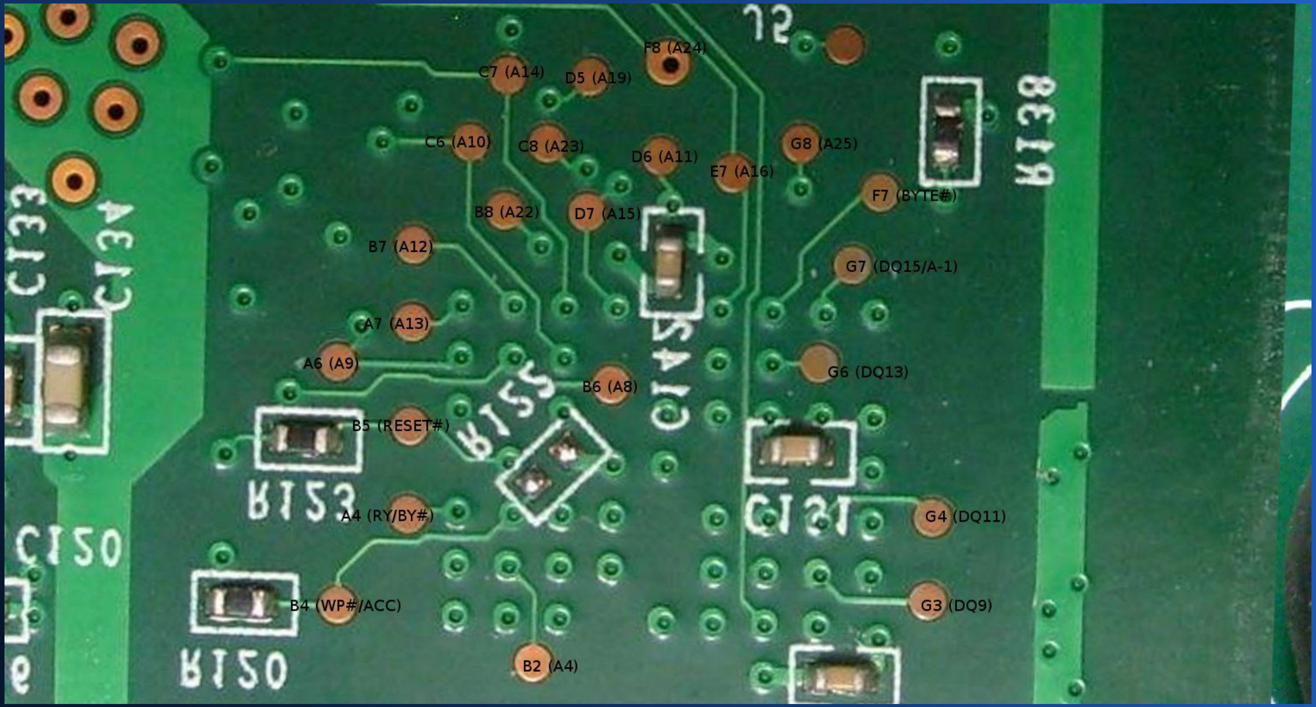
Altera JTAG

- 2x5 pin unpopulated



Test points

- Unmasked vias or bare copper pads
- Sometimes labeled “TPx” in silkscreen



Test points

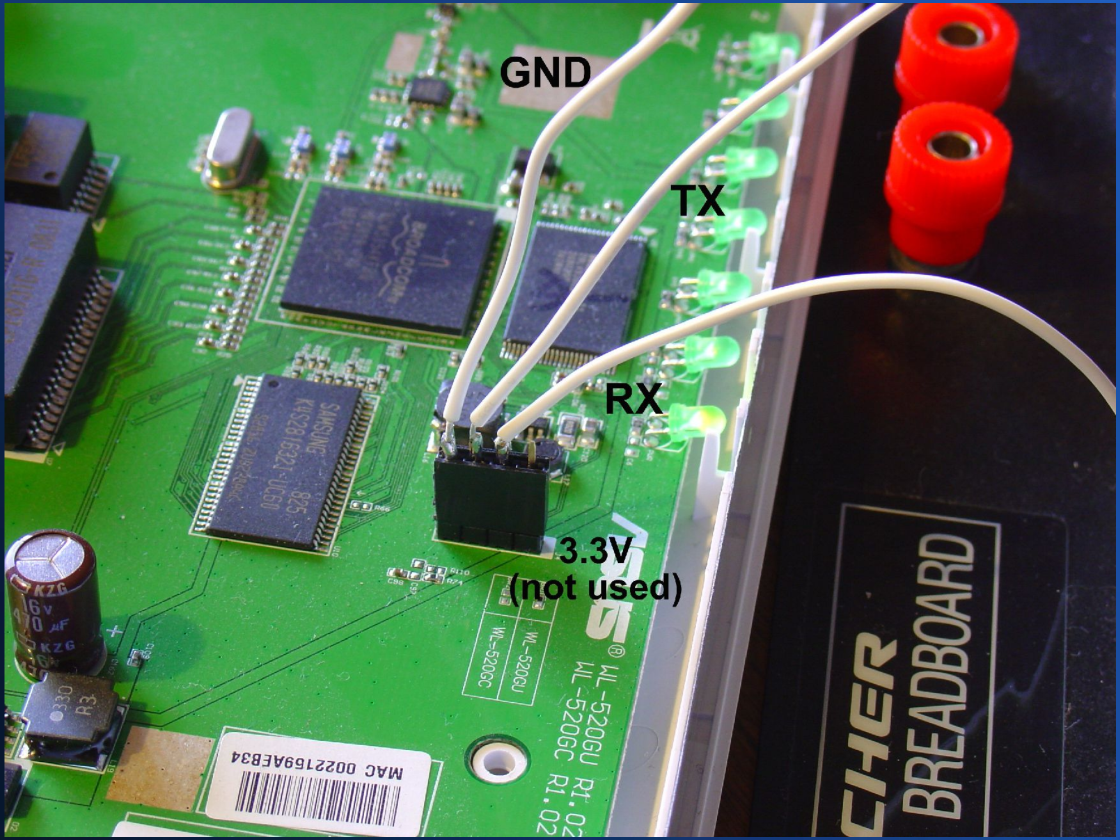
- Often give access to extremely useful signals!
- Anything that was interesting for board bring-up/test is probably going to be helpful for RE

Serial ports

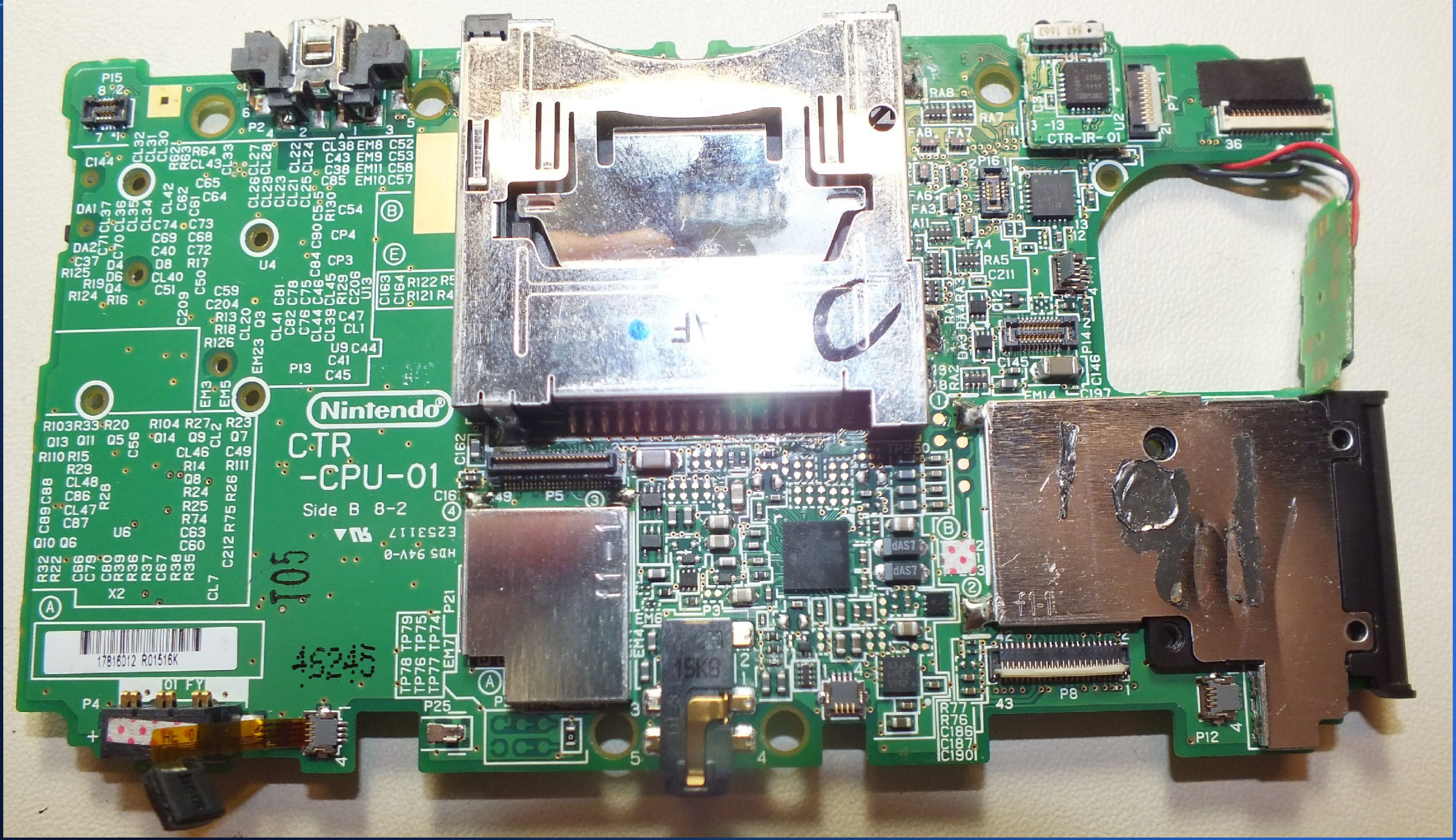
- Usually 3 or 4 pins at 0.1”
  - [Vdd], TXD, RXD, GND
  - May also have CTS/RTS lines
- Check with oscilloscope during boot
- May provide console access or debug logs
  - Boot loaders sometimes allow memory dumps

Serial port

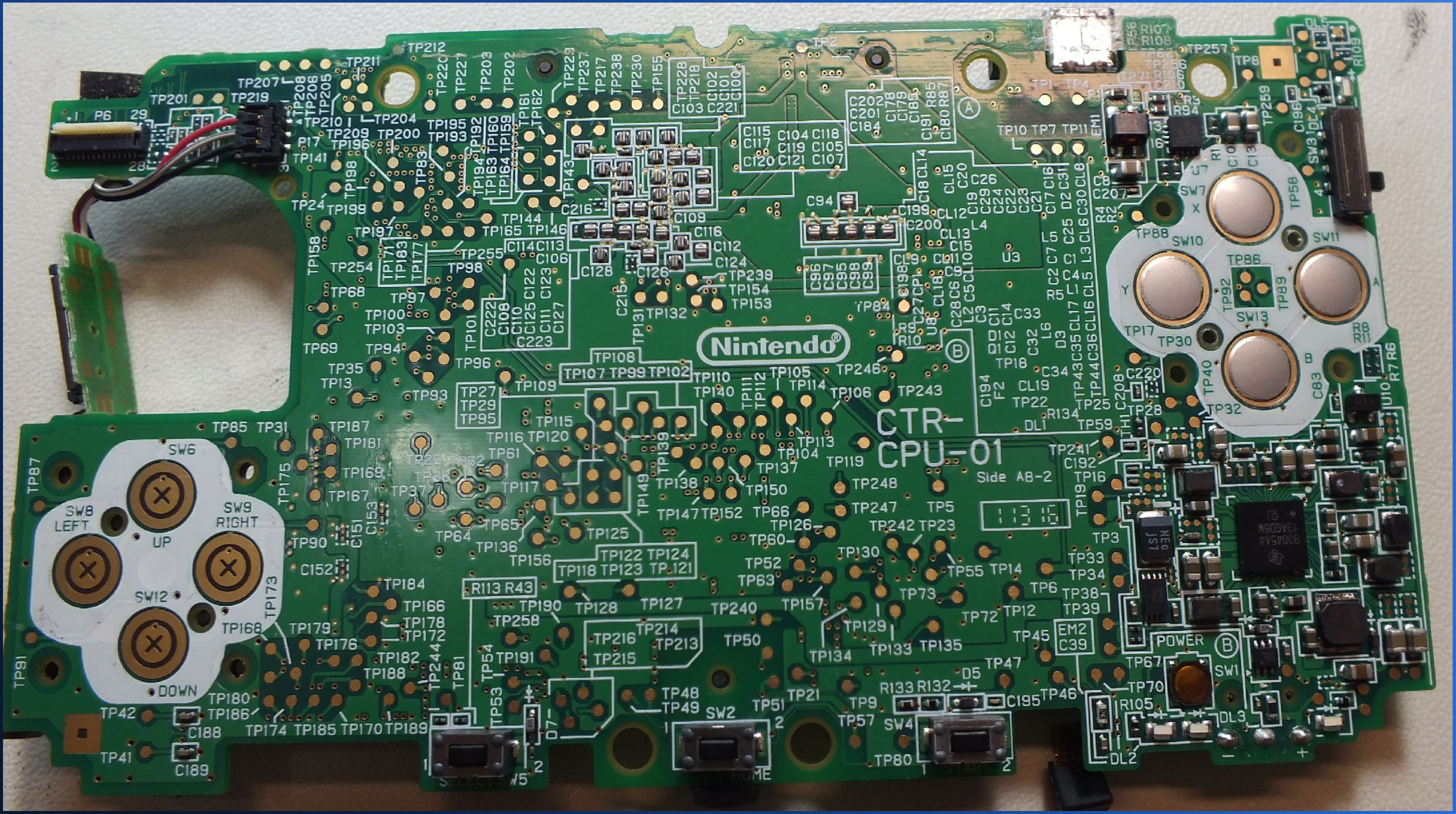
- Serial port on unknown wireless router



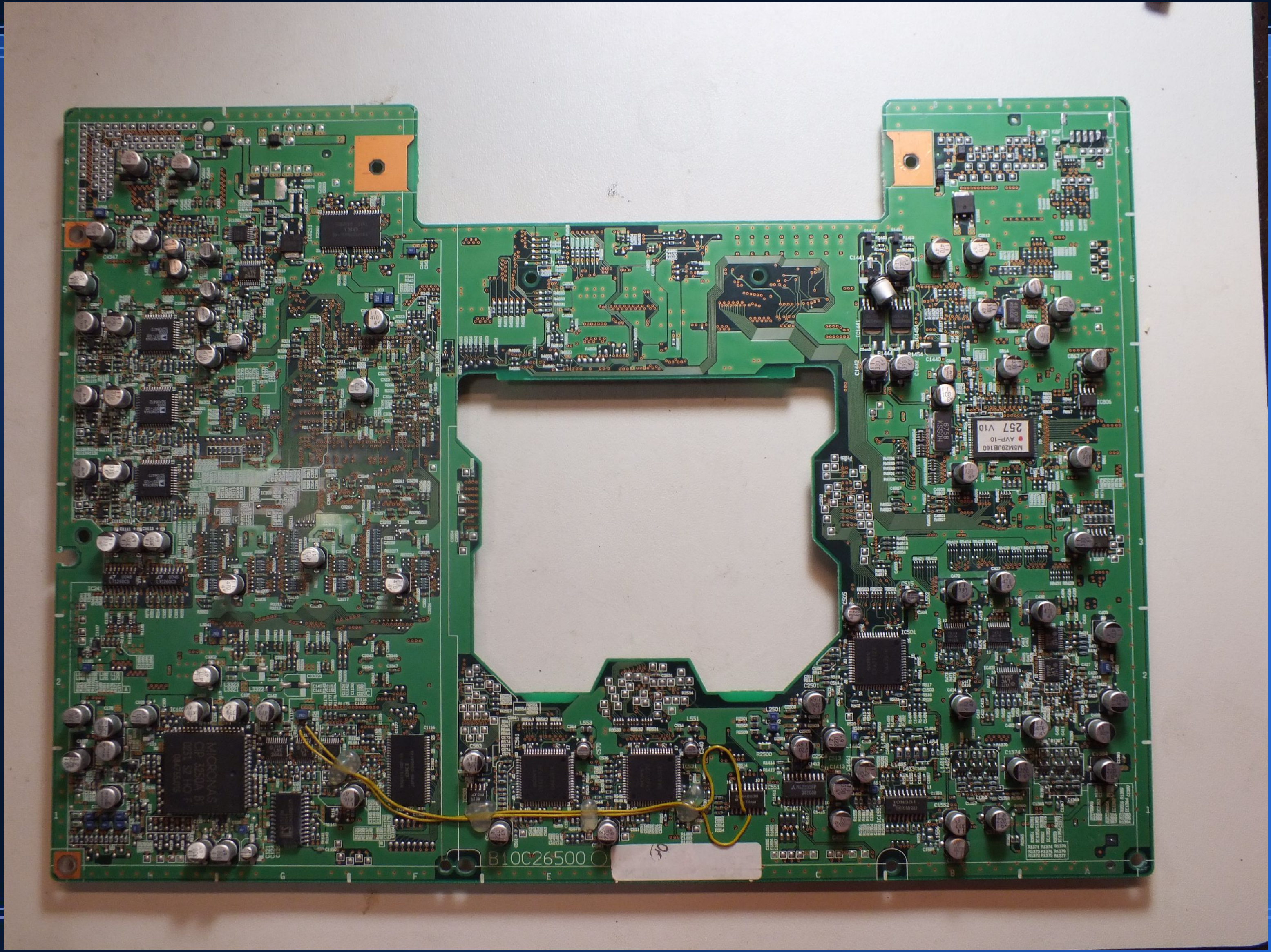
In-class exercise



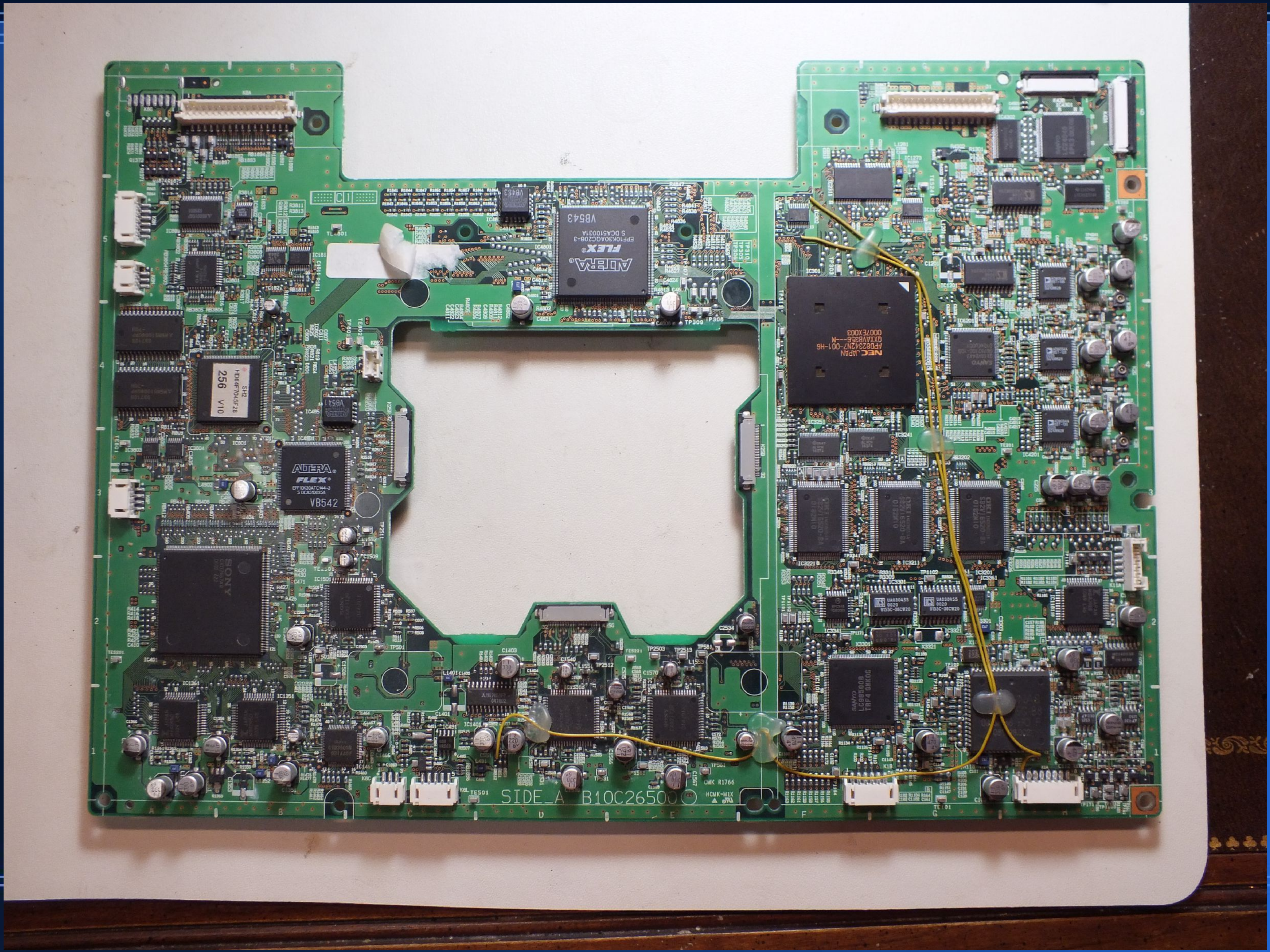
In-class exercise



In-class exercise



In-class exercise



Questions?

- TA: Andrew Zonenberg <azonenberg@drawersteak.com>
- Image credit: Some images CC-BY from:
  - John McMaster <JohnDMcMaster@gmail.com>
  - Edmund Tse http://www.flickr.com/photos/tseedmund/
  - Jeff Keyzer on flickr
  - marshallh

cc BY