Deconstructing the Circuit Board Sandwich: Effective Techniques for PCB Reverse Engineering

Joe Grand (@joegrand) aka Kingpin
Grand Idea Studio, Inc.

DEFCON 25

GRAND IDEA STUDIO

PCB Reverse Engineering

- The art of "undesigning" an existing system
- Destructive and non-destructive methods
- Why?
  - Determine system or subsystem functionality
  - Security research/verification
  - Forensic analysis/intelligence
  - Clone a design
  - Inject new (malicious) behavior
- How?
  - Access to copper layers
  - Analyze layout rules/features
  - Trace component interconnections

Deconstruction Techniques

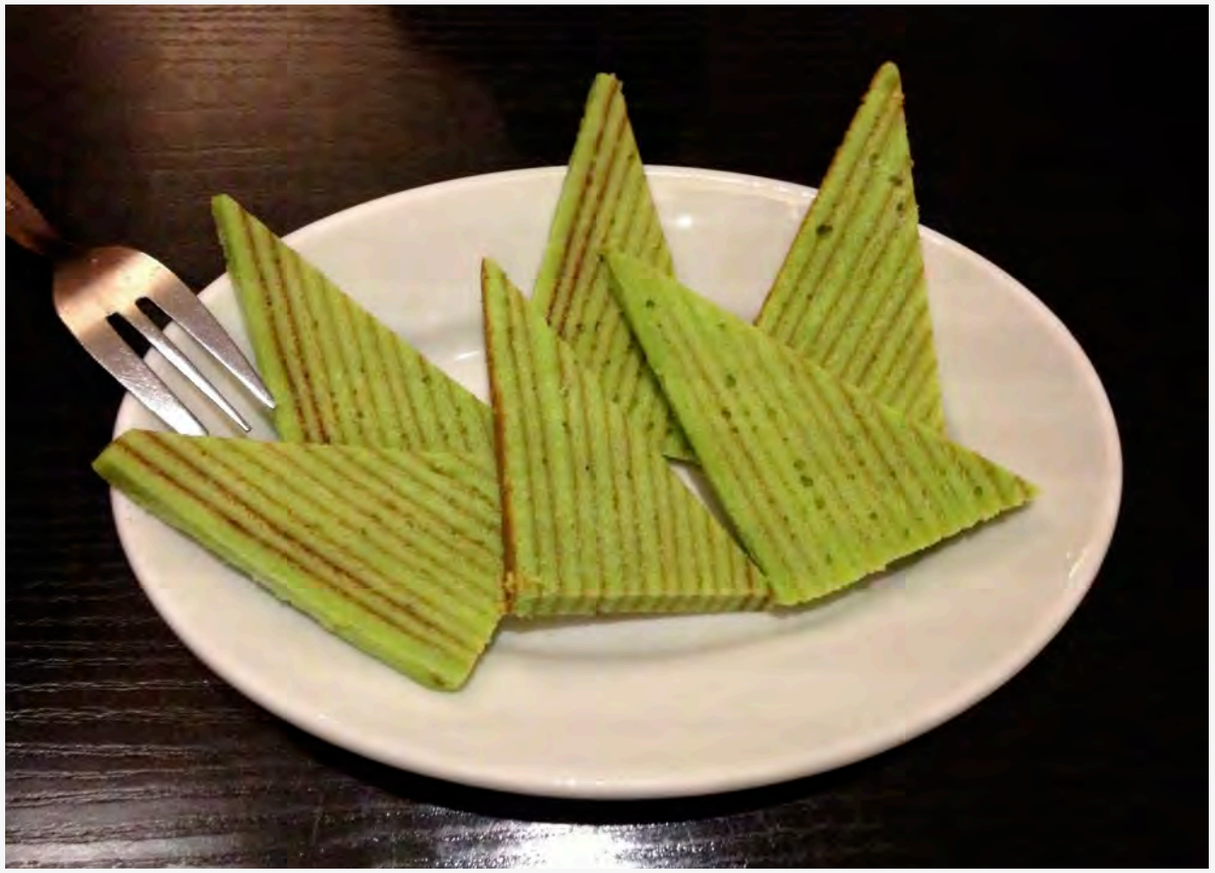
- Solder Mask Removal
- Delayering
- Imaging

* Results of my DARPA CFT *Research and Analysis of PCB Deconstruction Techniques* project

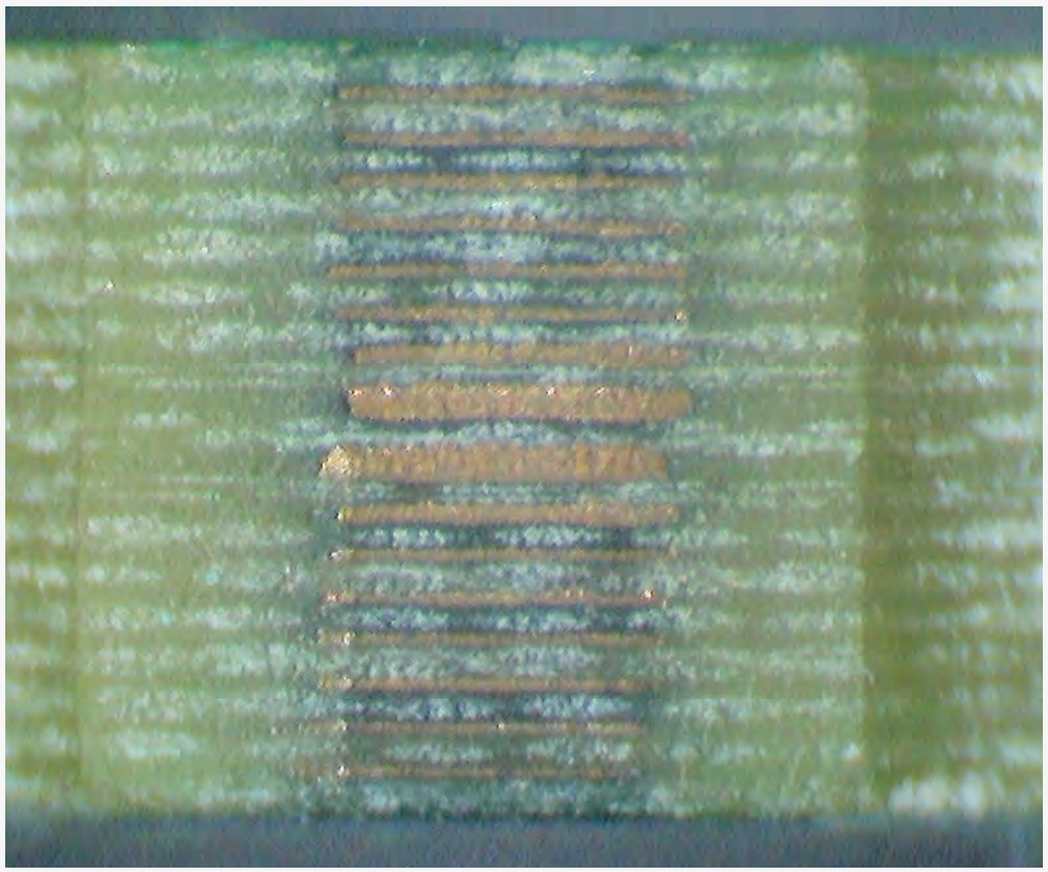
GRAND IDEA STUDIO

PCB Construction & Layer Stack

- Layers of thin copper foil (conductive) laminated to insulating (non-conductive) layers
  - "Circuit board sandwich"
- Form the physical carrier and electrical pathways for components



Spekkoek (not a PCB)

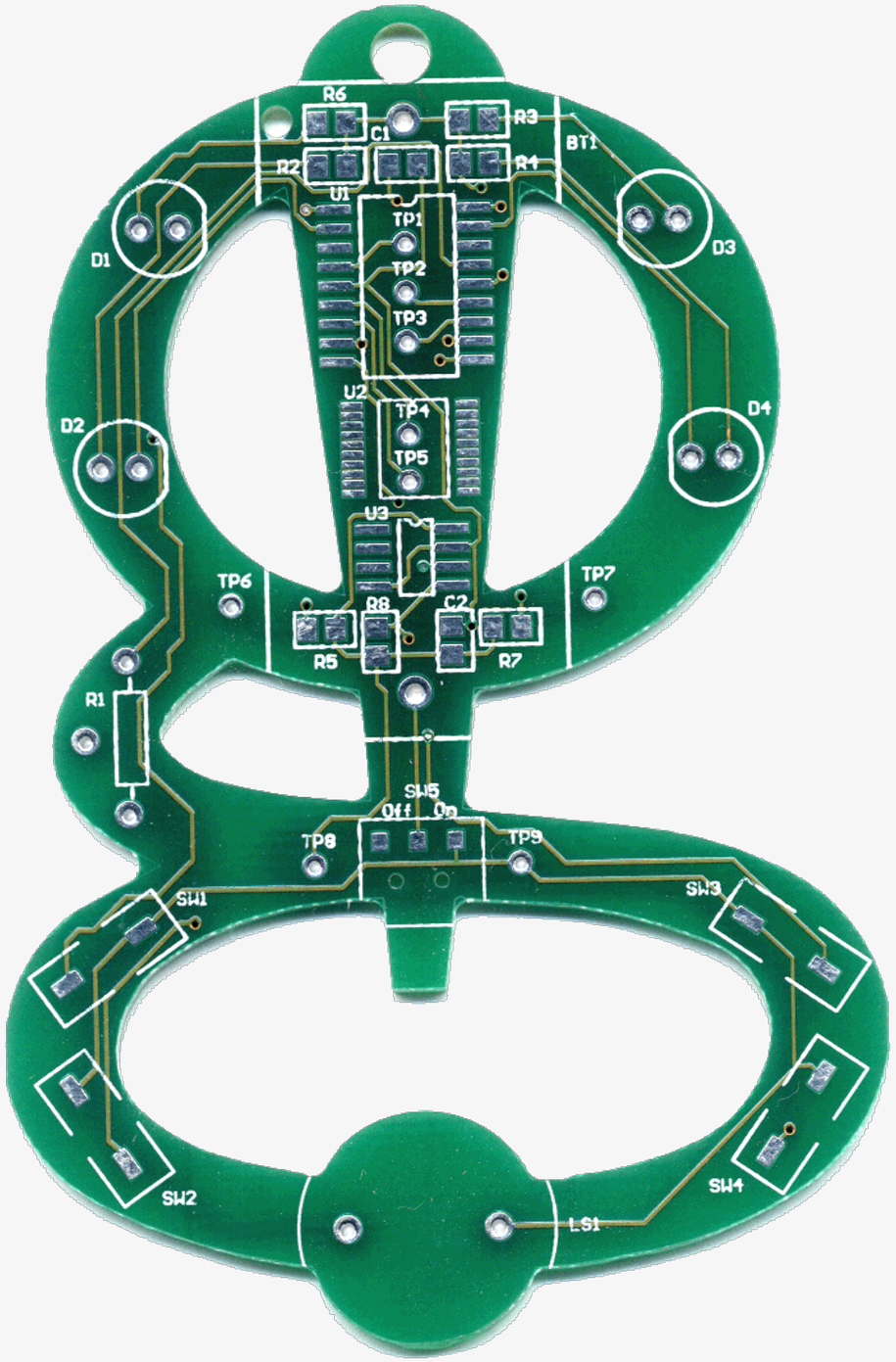


PCB cross-section (16 layer)

GRAND IDEA STUDIO

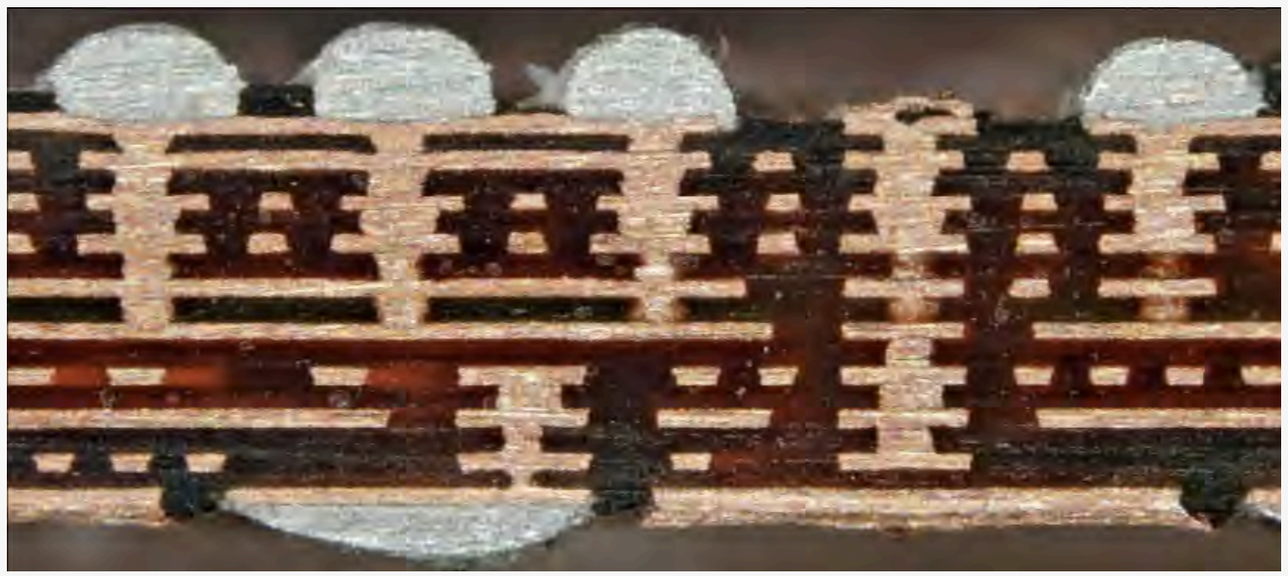
PCB Construction & Layer Stack 2

- Silkscreen (Component Legend)
  - Epoxy or printable ink
  - Part designators, symbols/logos, manufacturing/test markings
- Soldermask
  - Protects PCB from dust/moisture
  - Provides access to desired copper areas
- Copper
  - Thickness = weight of copper/sq. ft.
  - Surface finish provides better solderability
- Substrate
  - Insulating layer
  - Rigid and/or flex, fiberglass/epoxy weave or specialized composite



PCB Construction & Layer Stack 3

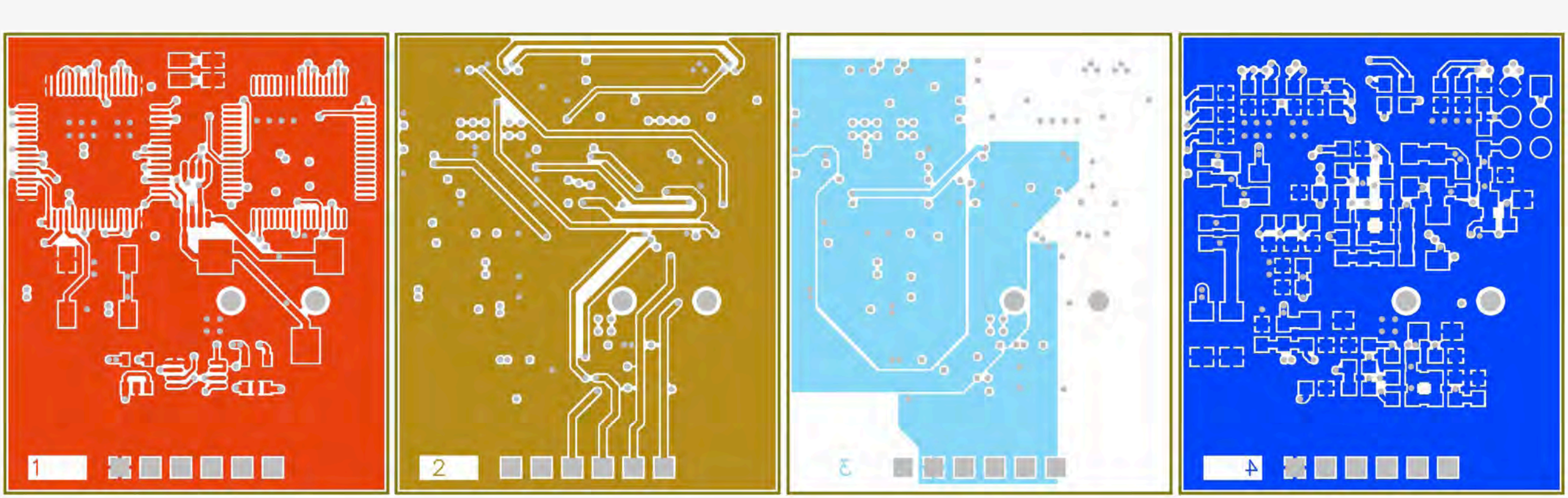
- Traditional capabilities
  - 3 mil trace/space width
  - 8 mil diameter mechanically-drilled vias
  - Buried vias
- State-of-the art capabilities
  - < 1 mil trace/space width
  - 0.4 mil diameter laser-drilled microvia
  - Via-in-pad



D. Carey, *Going Vertical & Staying Small*, www.techinsights.com/uploadedfiles/3d-packaging-trends.pdf

PCB Construction & Layer Stack 4

- Separate layers only tell part (if any) of the story
- Placed together, a complete circuit layout can be identified
- If components are also known, a full electrical design can be reversed



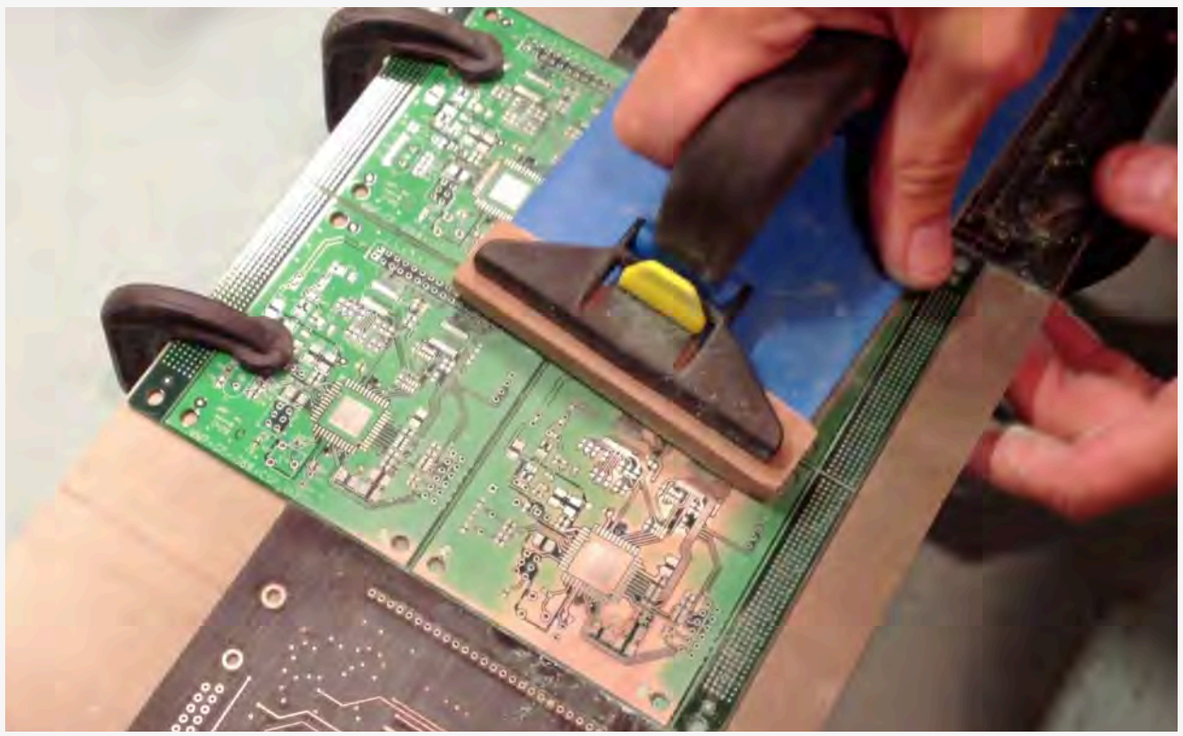
Emic 2 Text-to-Speech Module

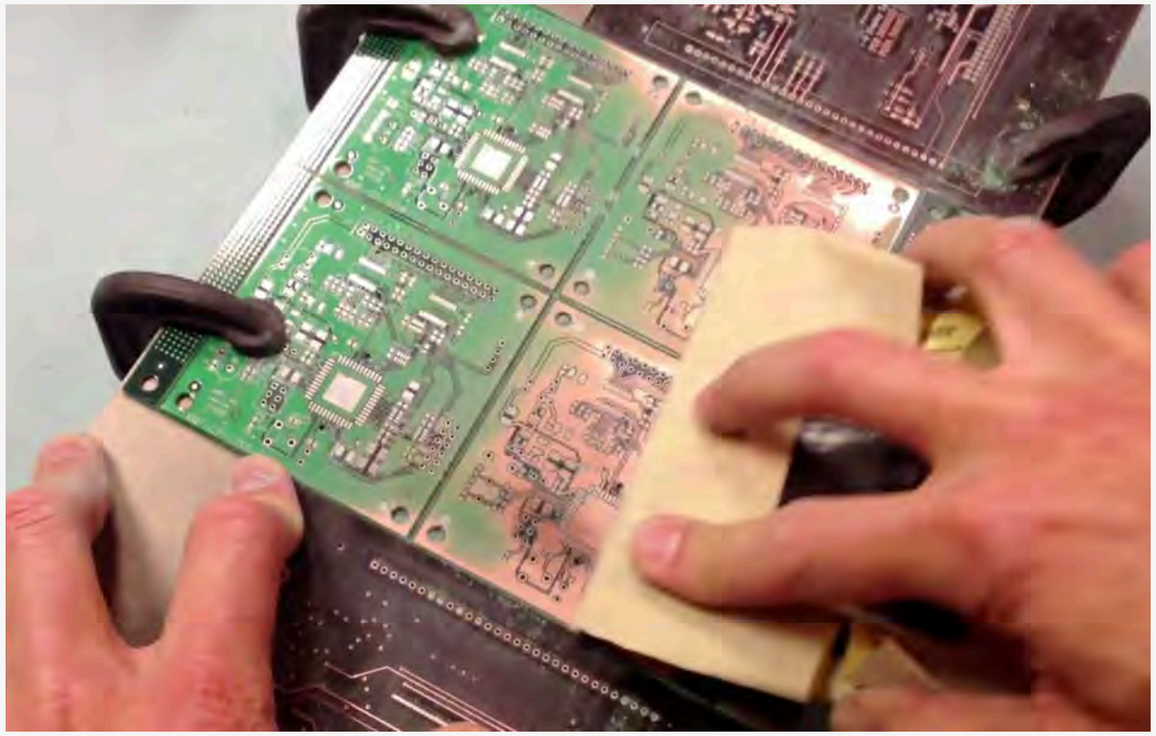
Solder Mask Removal

- Sandpaper/rubbing stone
- Fiberglass scratch brush
- Abrasive sand blasting
- Chemical
- Laser

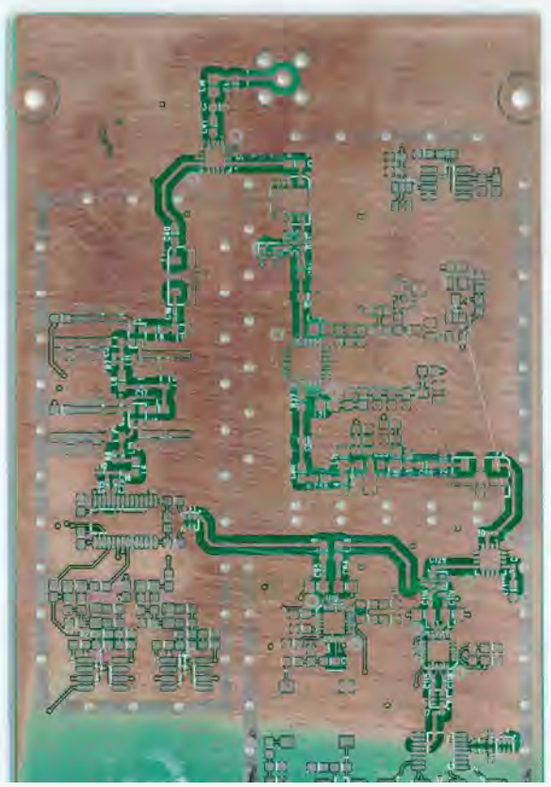
Solder Mask Removal: Sandpaper/Rubbing Stone

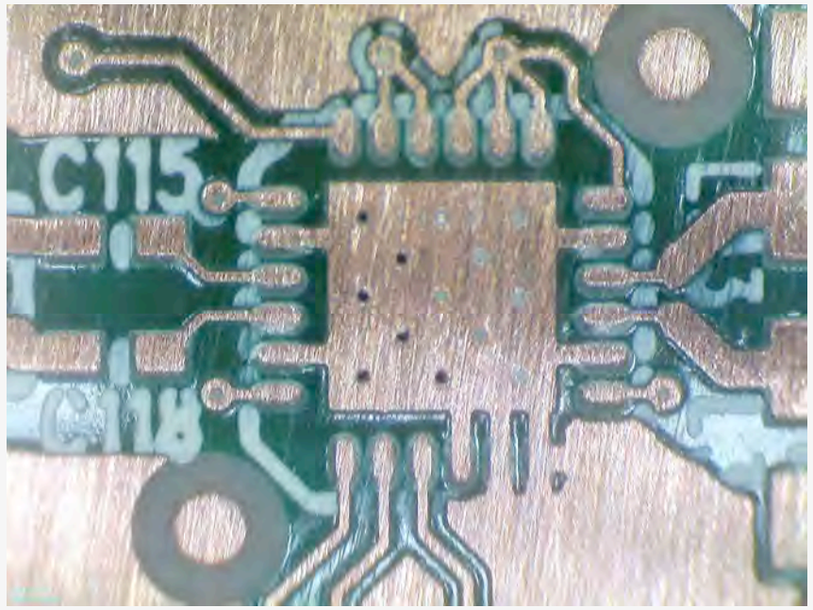
- Effective, lowest cost method
- Even strokes across the entire PCB @ light pressure
- Spare PCBs of same height used on sides to help maintain planar motion
- Different PCB surface finishes require different grit sizes
- Excessive abrasion can cause damage to underlying copper



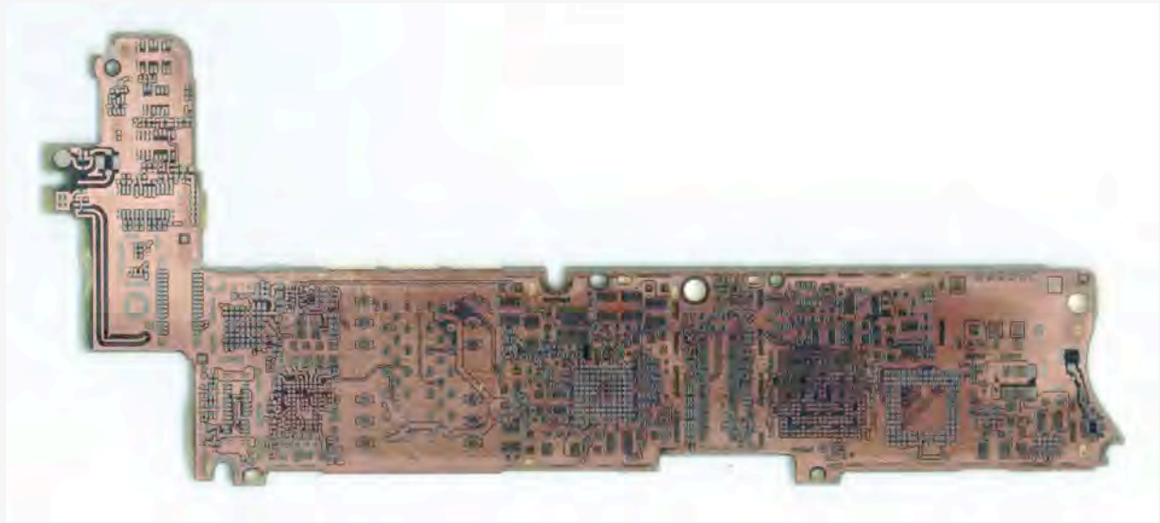


Solder Mask Removal: Sandpaper/Rubbing Stone 2

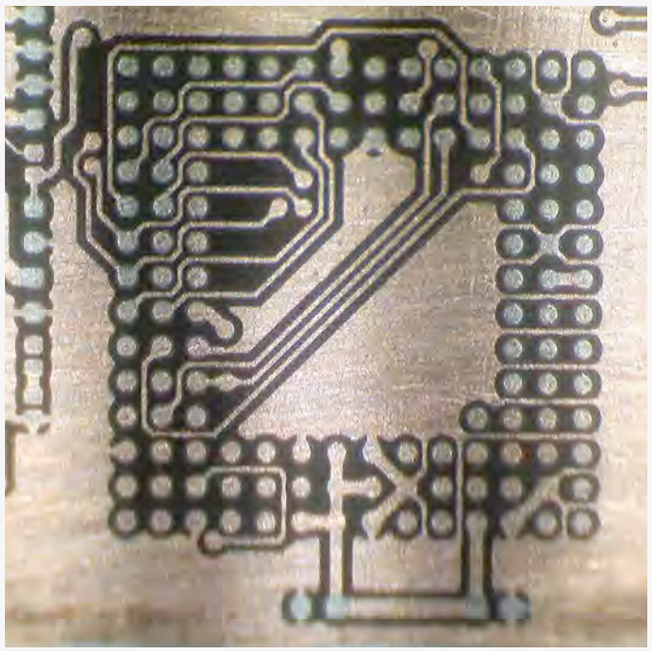




60/80 grit rubbing stone +
220 grit sandpaper

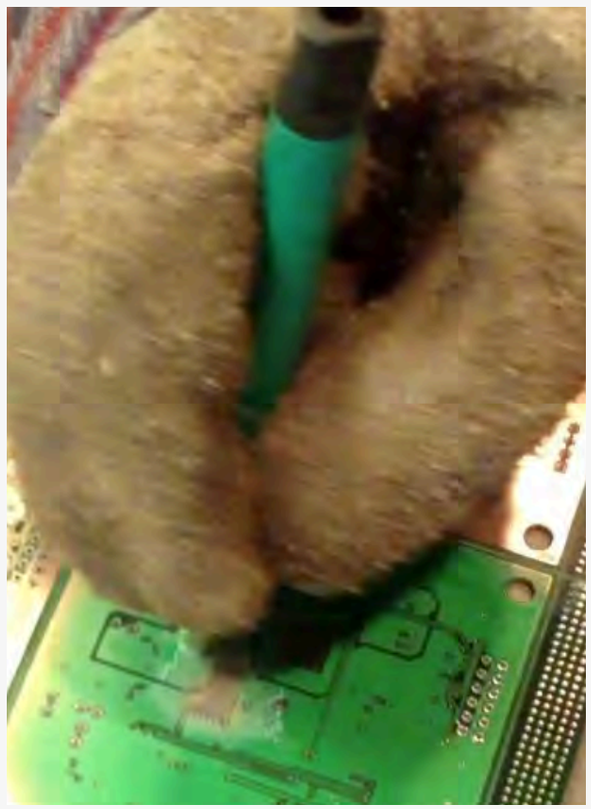


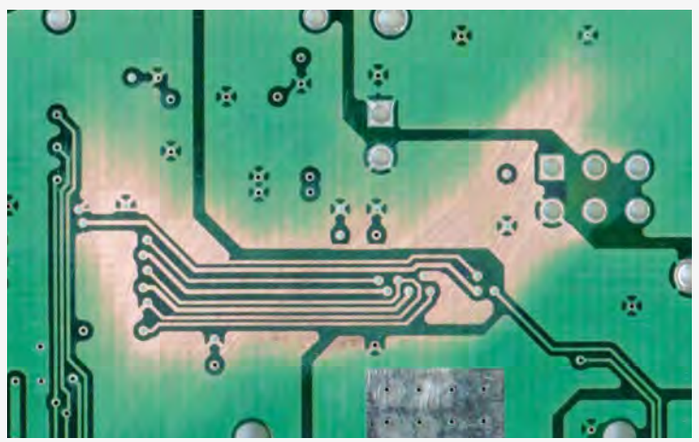
iPhone 4 16GB w/ 400 grit sandpaper

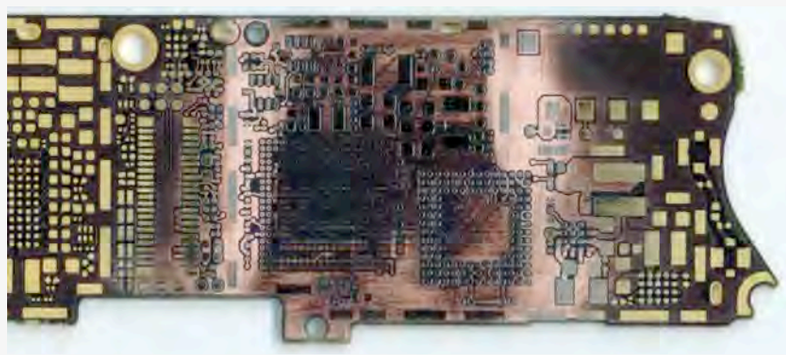


Solder Mask Removal: Fiberglass Scratch Brush

- Handheld, pencil-shaped tool for material cleaning/polishing
- Excelta/Eurotool 267
- Very nice result w/ only light wearing of copper
- Precise control also useful for selective, small area mask removal
- BOLO: Fiberglass shards can/will get stuck in your hands

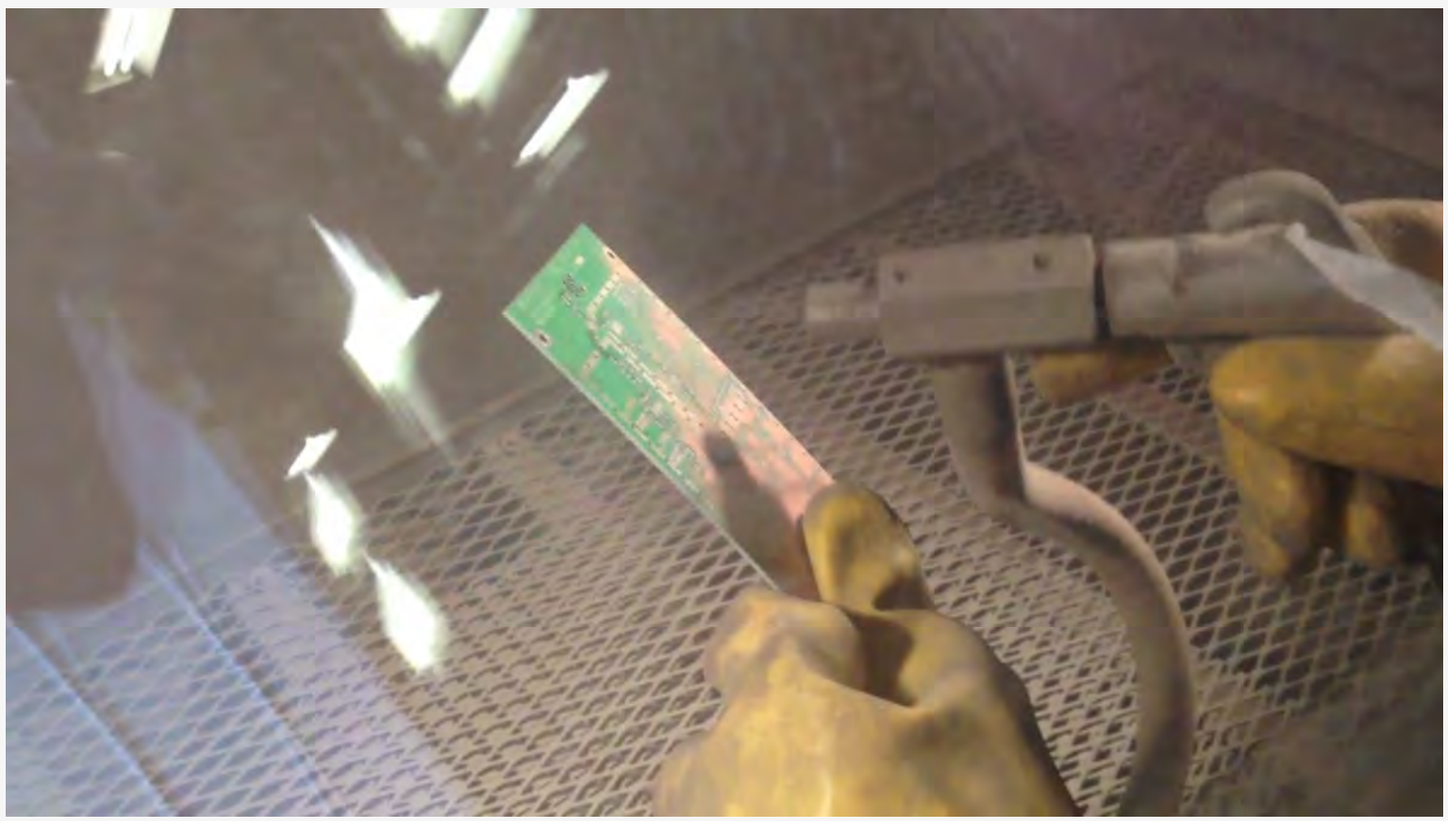






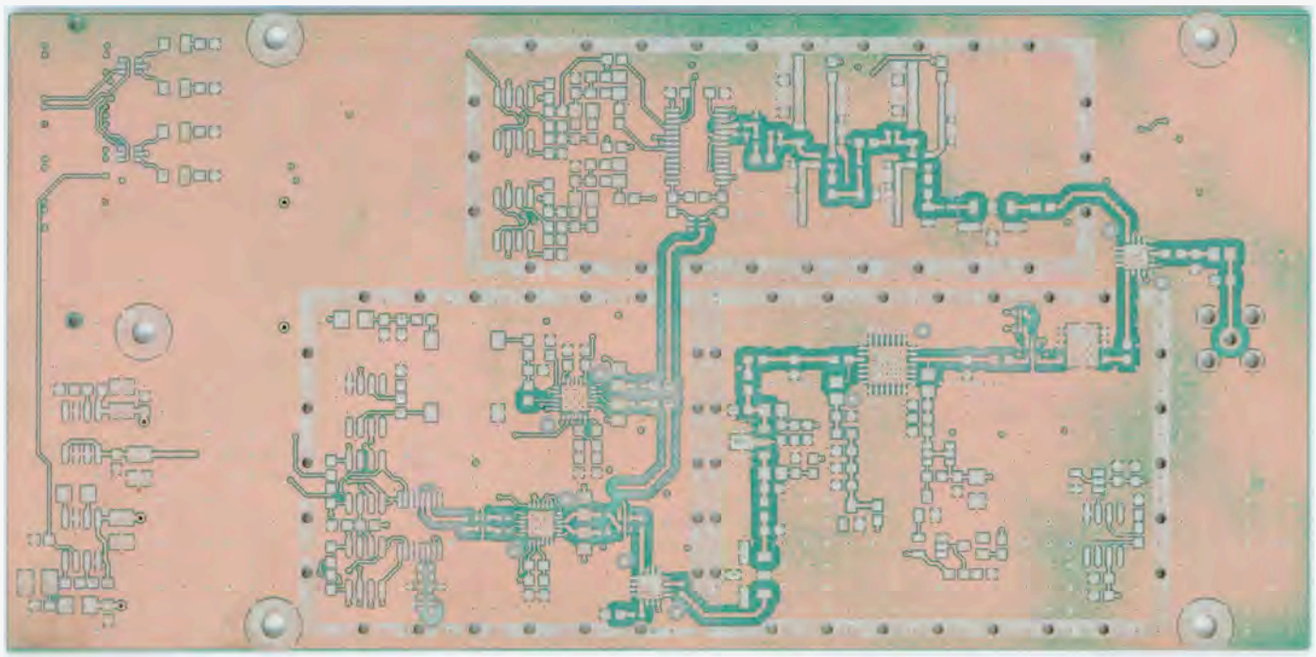
Solder Mask Removal: Abrasive Sand Blasting

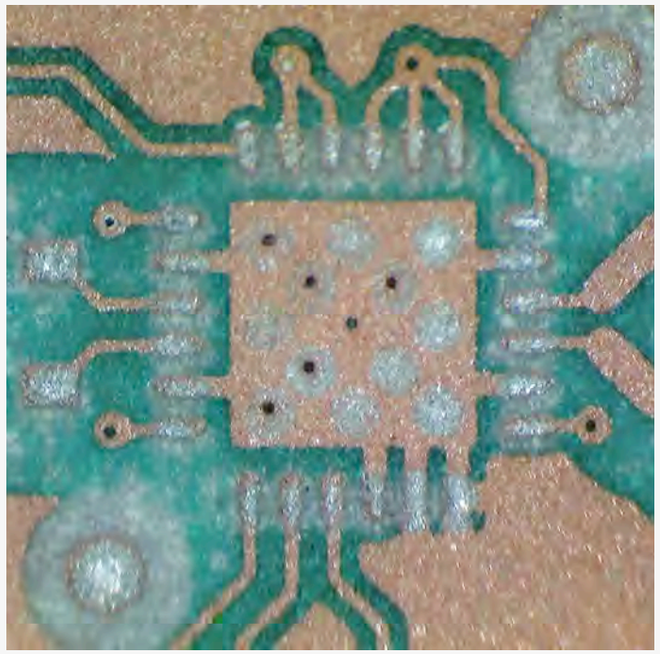
- Typically used to strip material from surfaces (paint, calcium deposits, fungus) or add texture/artificial wear
- TP Tools Skat Blast 1536 Champion Blast Cabinet @ TechShop, San Francisco, CA
- Best results w/ nozzle angled & held 6-8" away from PCB surface



Solder Mask Removal: Abrasive Sand Blasting 2

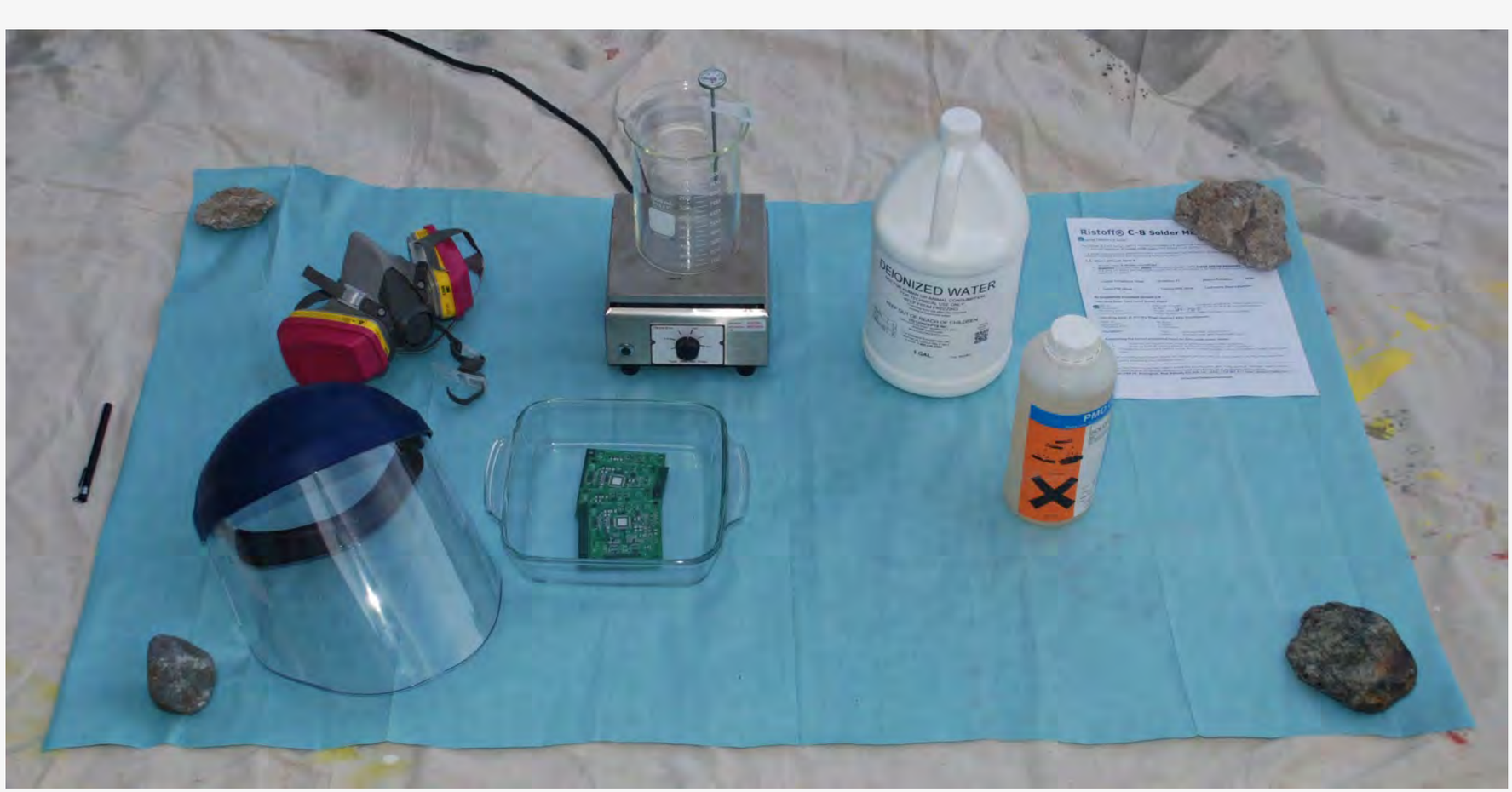
- 60# aluminum oxide @ 80PSI (pounds/sq in), 10-15 CFM (cubic ft/min)
- Noticeable pitting, but copper and substrate remained intact
  - Softer media (crushed walnut shells) may cause less surface wear
  - Risk of damage by focusing on one area of PCB for too long
- Best suited for PCBs w/ trace/space >= 10/10mil & copper weight >= 1oz (1.4mil)





Solder Mask Removal: Chemical

- Typically used by PCB fabricators for failure analysis or to fix a manufacturing error
- BOLO: Requires hazardous chemical handling and disposal procedures



* Not a meth lab.

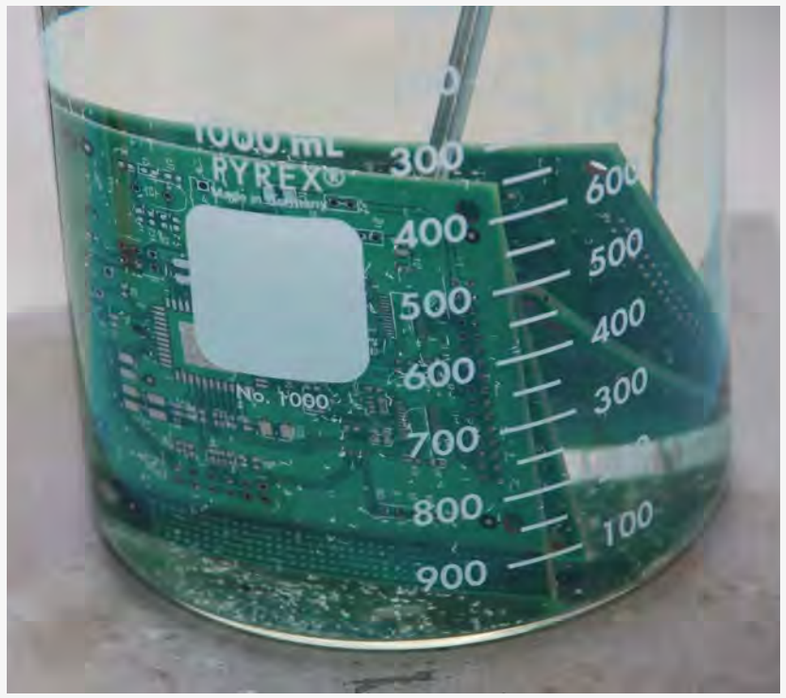
GRAND IDEA STUDIO

Solder Mask Removal: Chemical 2

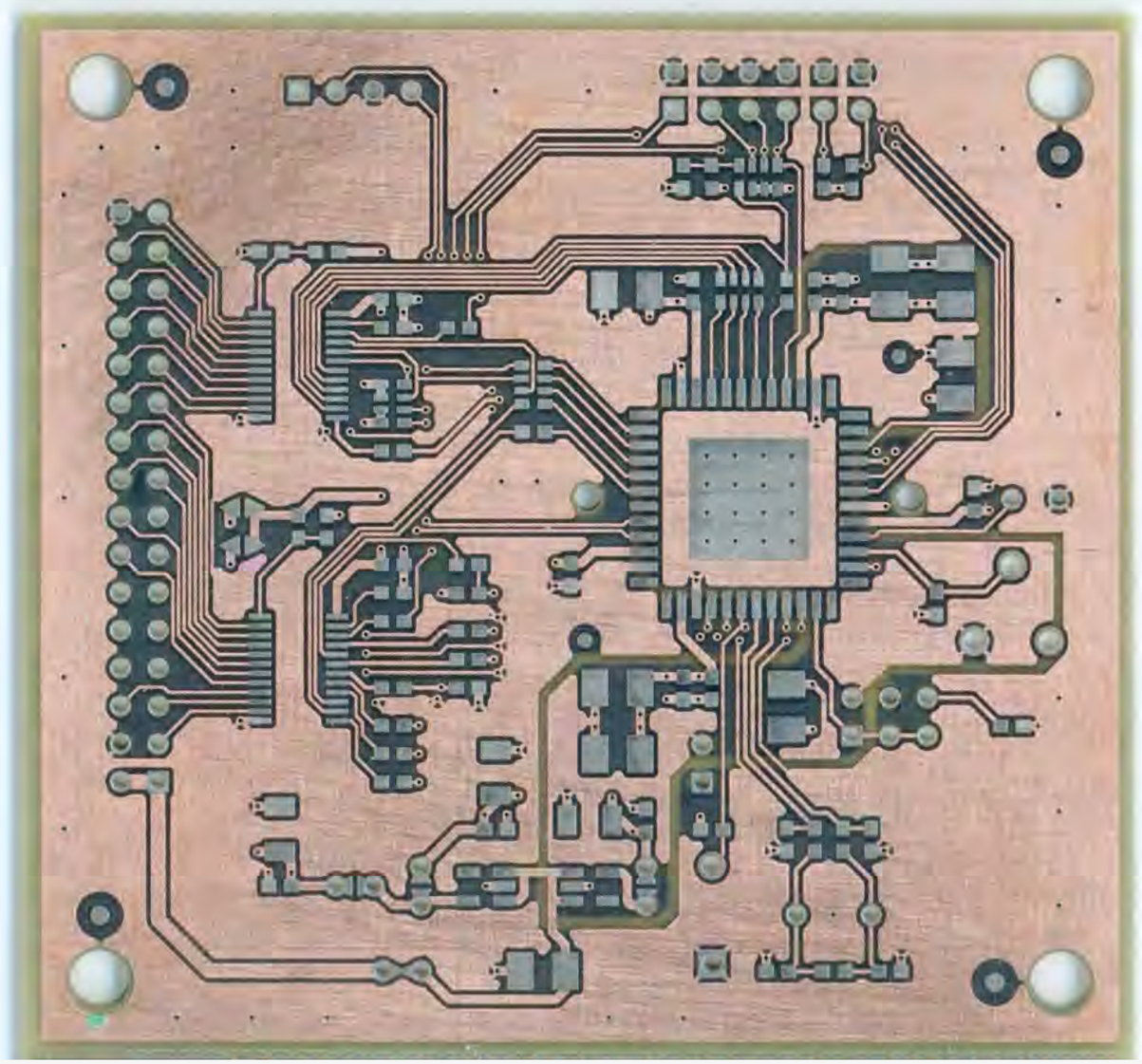
* Not a meth dealer.

Solder Mask Removal: Chemical 3

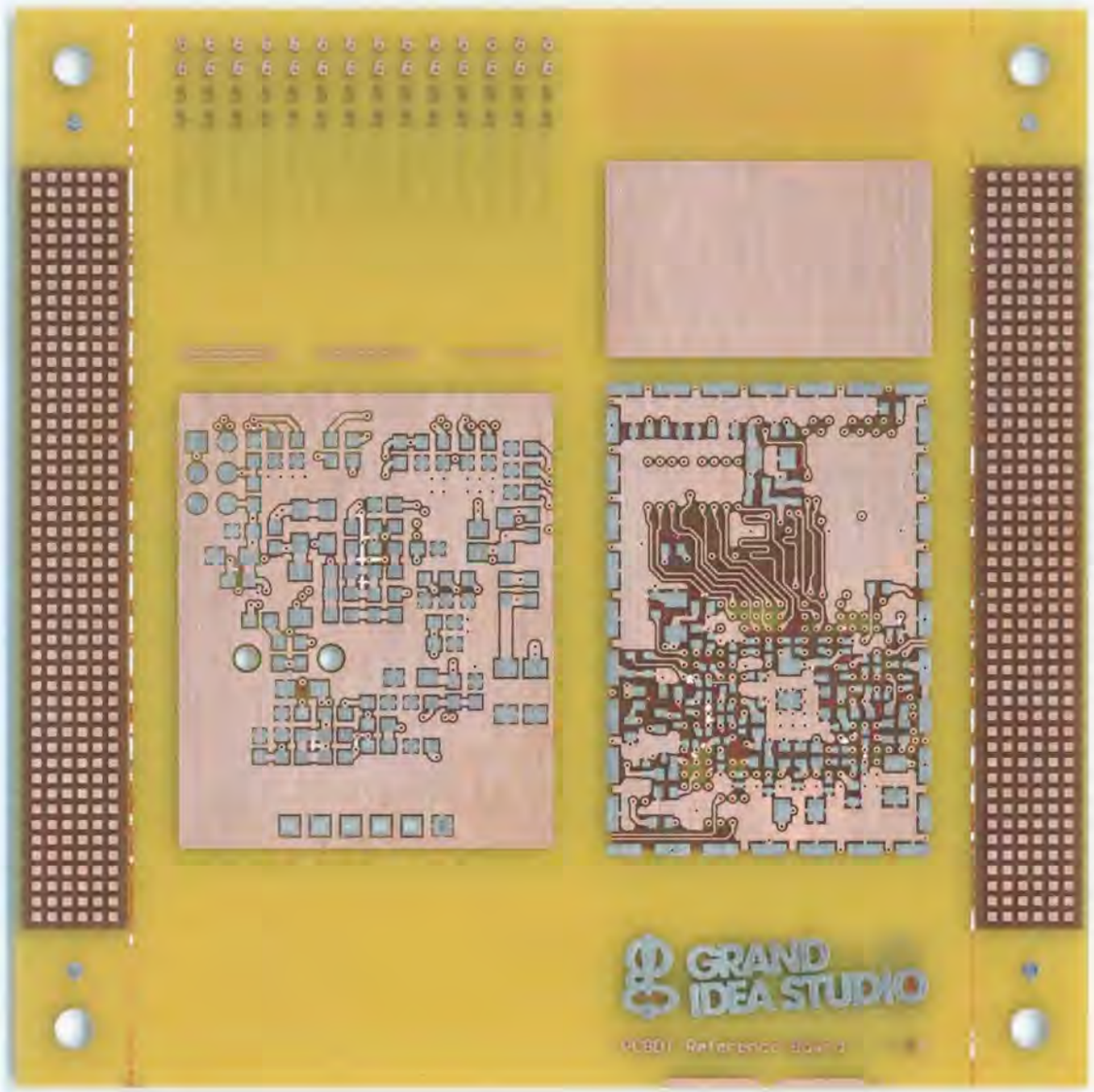
- Ristoff C-8 (NWE Chem Research, UK)
- Magnastrip 500 (RBP Chemical Technology, US)
- Neither chemical will attack the PCB substrate/laminate
- Heat chemical, soak PCB, rinse in water & brush lightly w/ soft metal brush
  - Processing time (~45-120 minutes) varies due to chemical temperature, solder mask composition, and solder mask thickness



Solder Mask Removal: Chemical 4



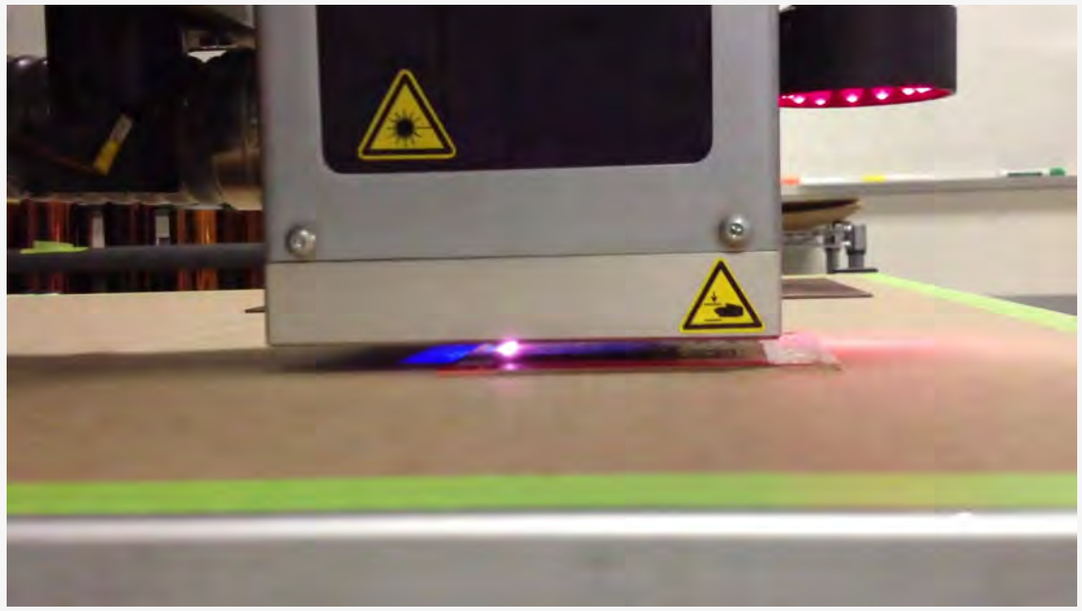
Ristoff C-8 @ 90 minutes, 130°F



Magnastrip 500 @ 75 minutes, 150°F

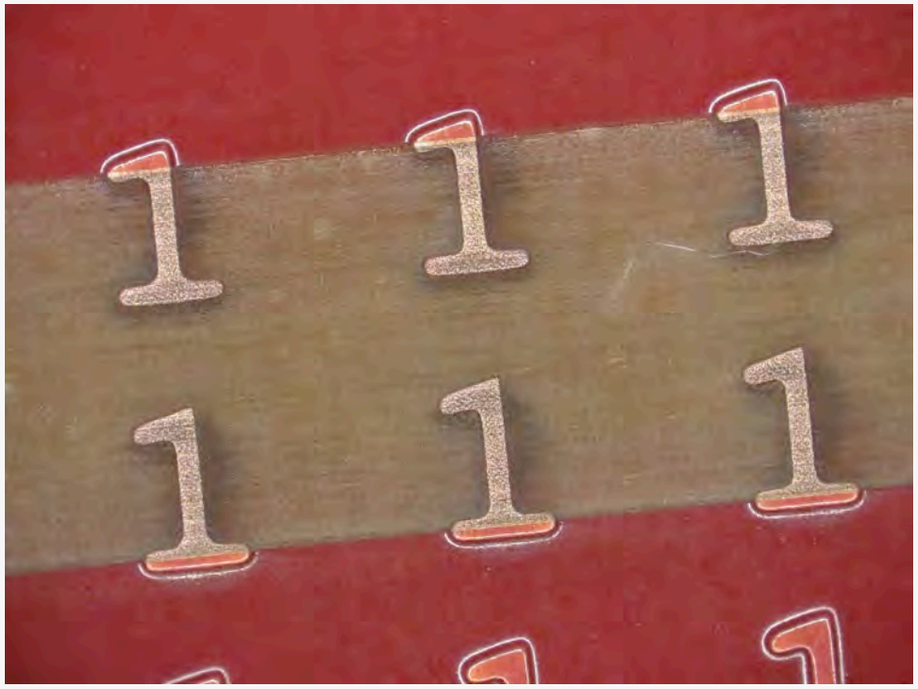
Solder Mask Removal: Laser

- LPKF MicroLine 600D UV Laser System @ A-Laser, Milpitas, CA
- Typically used for cutting of flex circuits and coverlayer material (film, foil, adhesive)
- +/-0.6 mil accuracy, 300mm/sec. (11.8"/sec.) max. travel speed, 20um (0.787mil) beam diameter

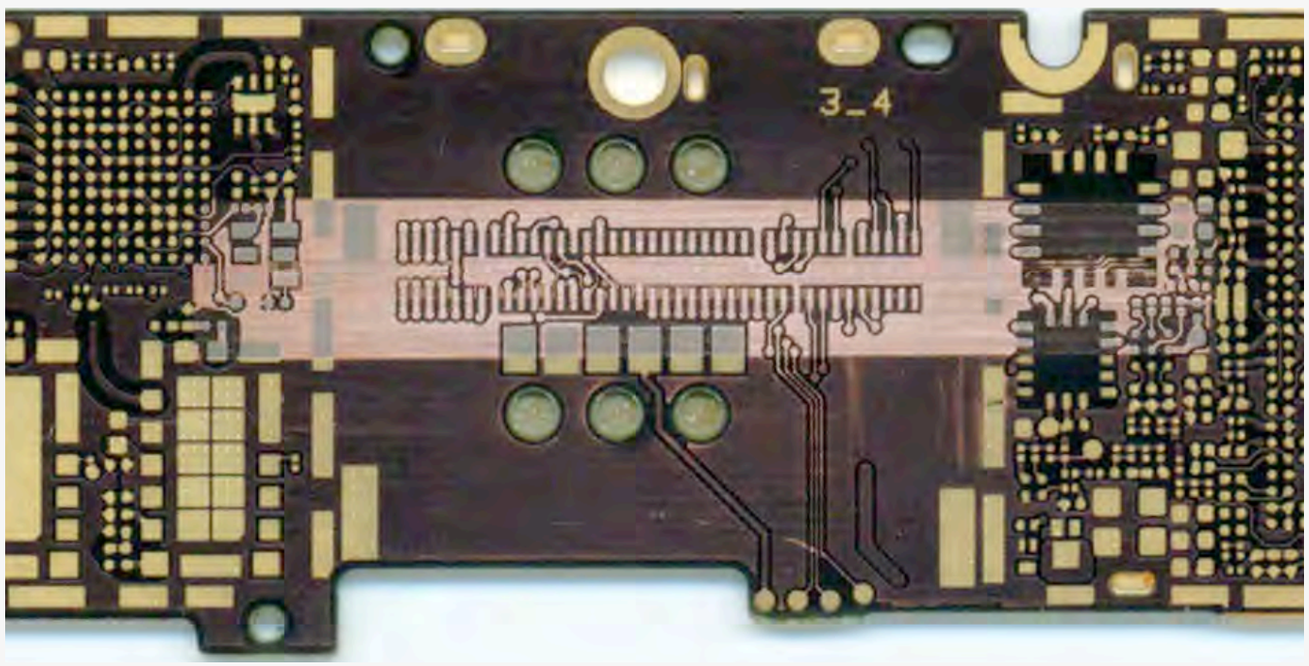


Solder Mask Removal: Laser 2

- Single pass @ medium power
- Copper layer remains fully intact
- Different materials react differently to the laser energy
  - Solder mask and FR4 ablate more quickly than copper
  - Incorrect laser power settings or too many passes can damage underlying copper



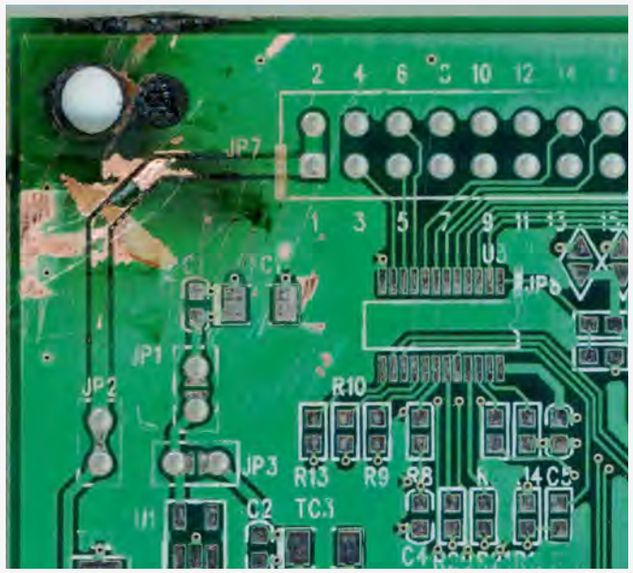
PCBDT Reference Board

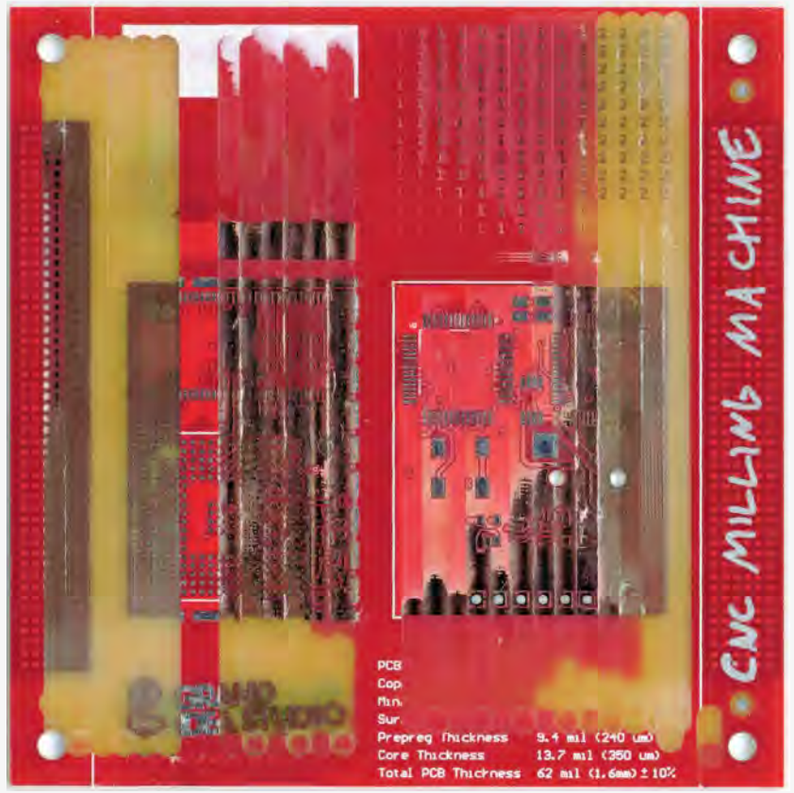


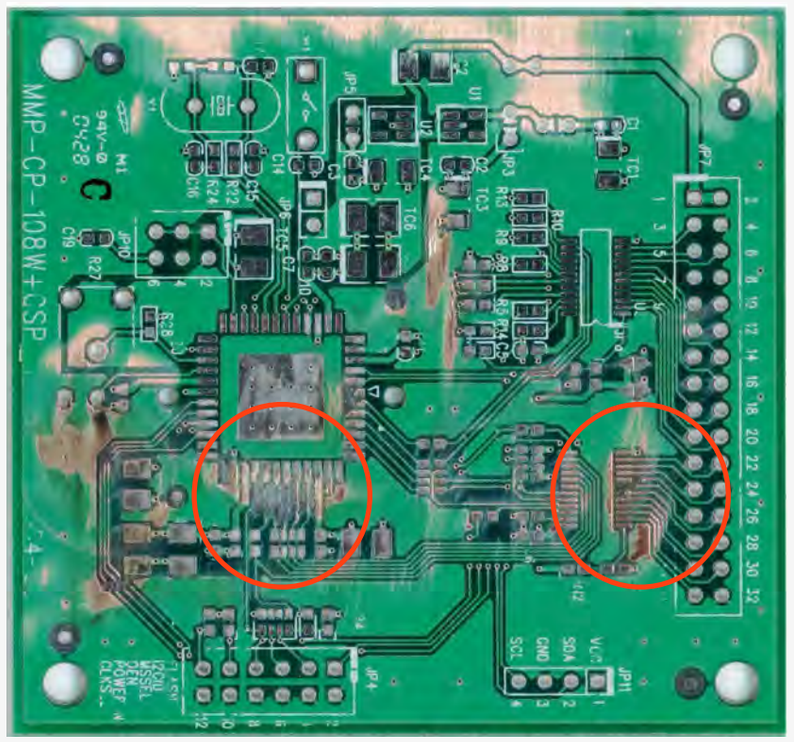
iPhone 4 16GB Logic Board

Solder Mask Removal: Failures

- Hobby knife
- Electric/mechanical eraser
- Dremel tool
- CNC milling
- Chemical
  - Methylene chloride
  - Tetrahydrofuran
  - Acetone
- Heat
  - Heat gun
  - Butane torch







Delayering

- Sandpaper/rubbing stone
- Dremel tool
- CNC milling
- Surface grinding

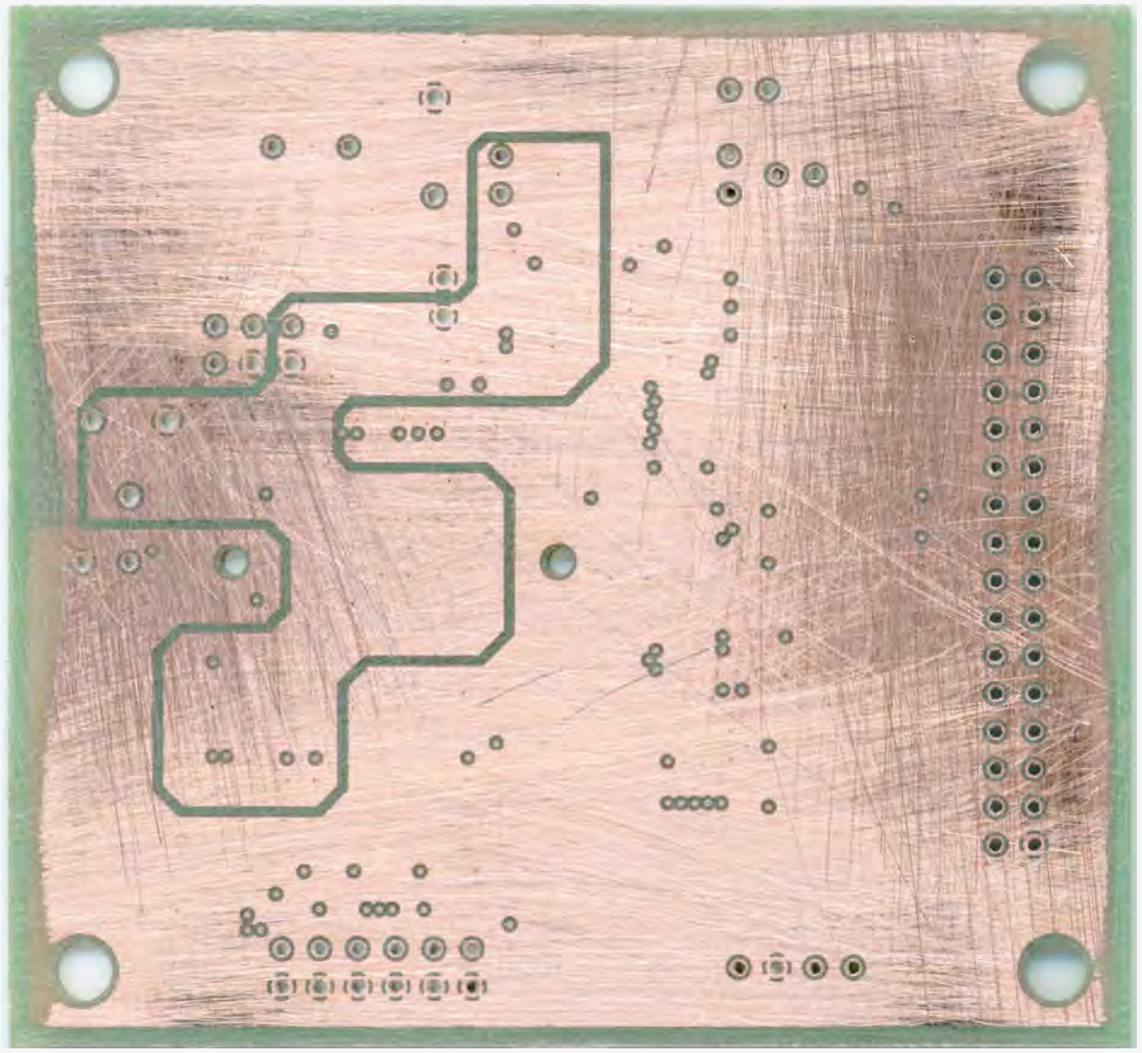
Delayering: Sandpaper/Rubbing Stone

- Effective, lowest cost method
- Affix to work surface w/ double-sided tape
- Full strokes across the entire PCB @ hard pressure
  - One layer at a time
- Physical workout -> operator fatigue

Delayering: Sandpaper/Rubbing Stone 2

Delayering: Sandpaper/Rubbing Stone 3

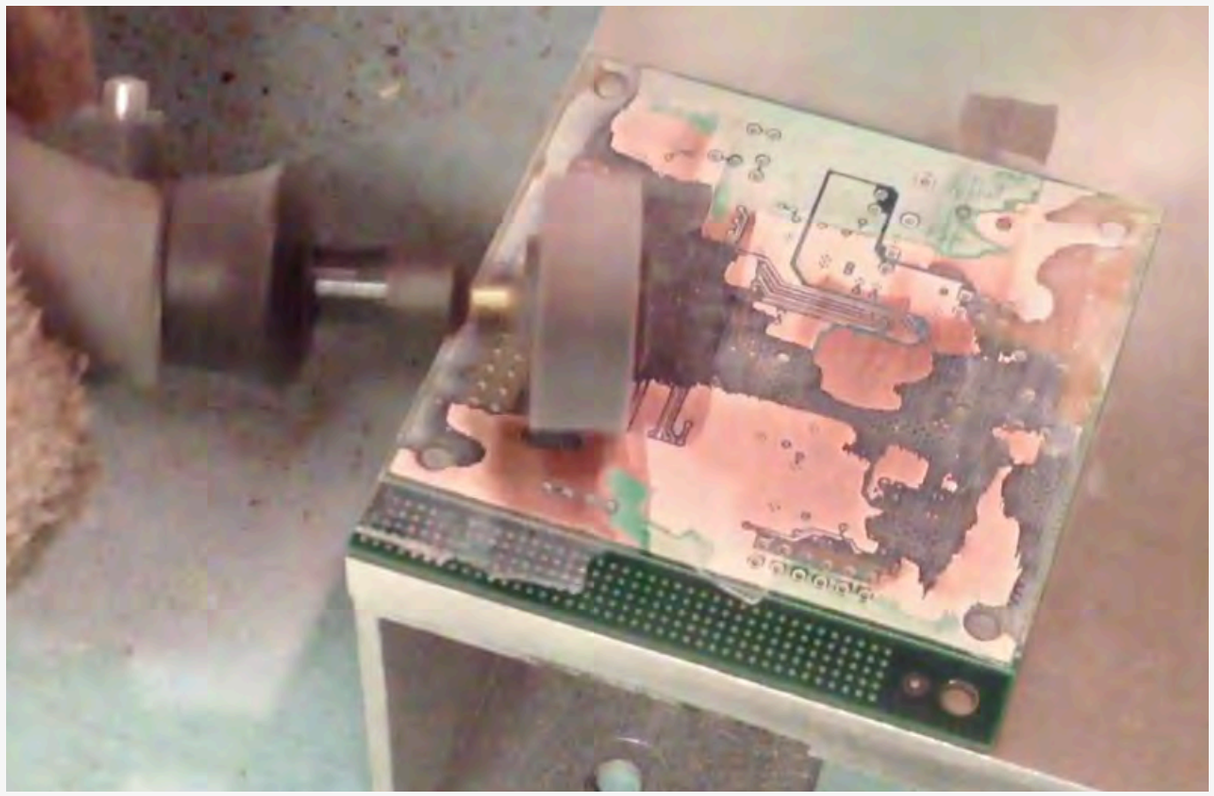
- Minor scratching of inner copper layer
- Noticeable wearing along edges due to uneven sanding

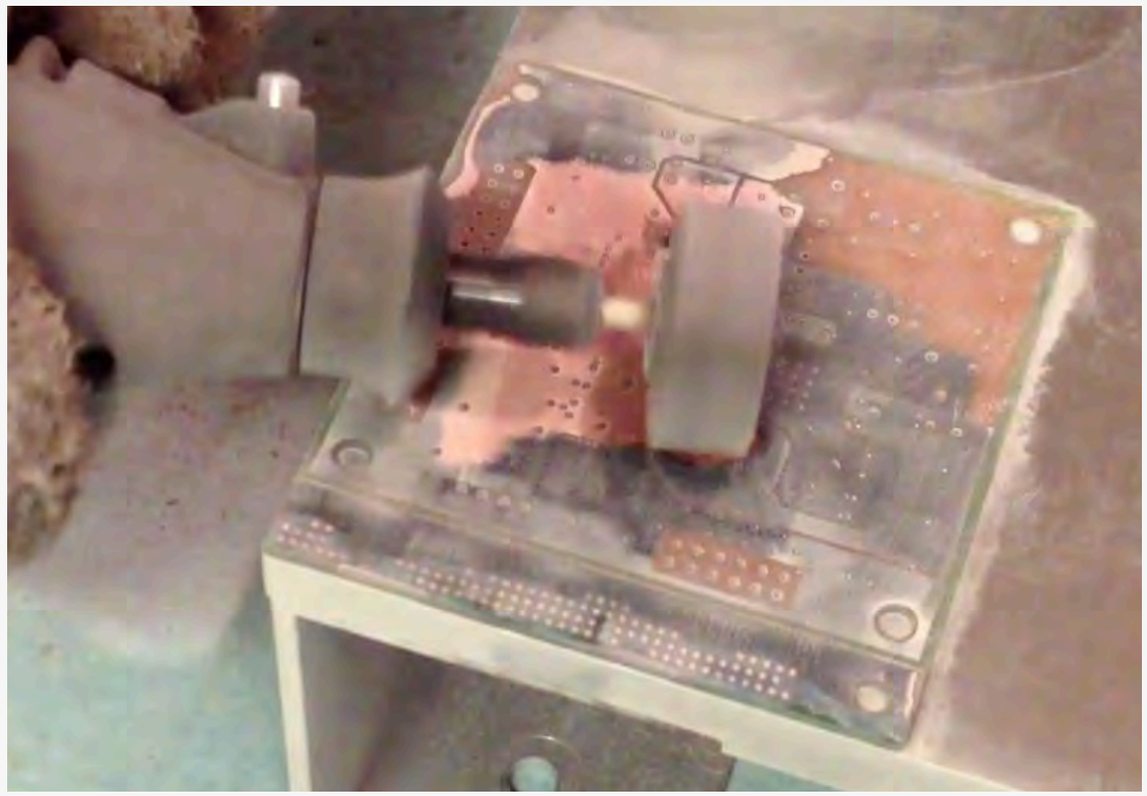


60/80 grit rubbing stone + 220 grit sandpaper

Delayering: Dremel Tool

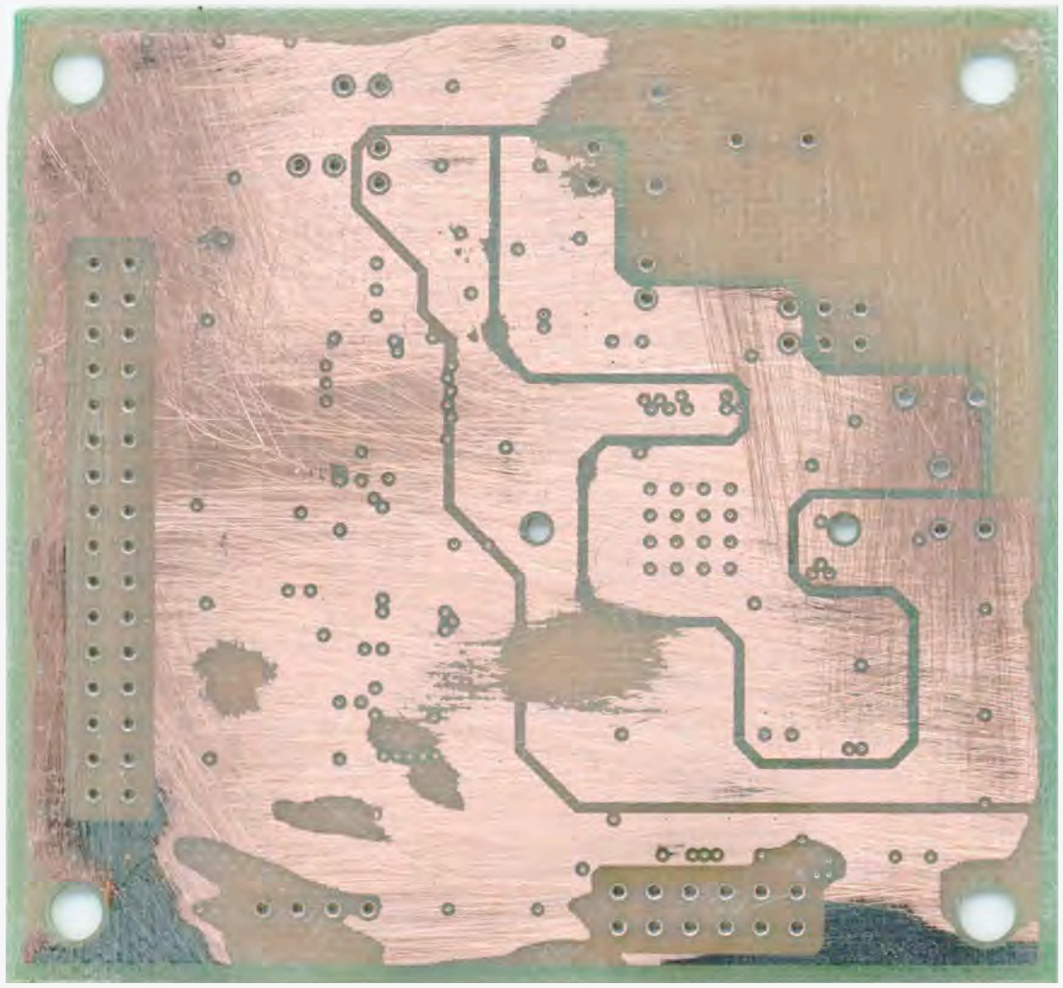
- Off-the-shelf home improvement tool used for cutting, grinding, drilling, routing, polishing, & sanding
- Dremel MultiPro 395 w/ 503 Flapwheel (120 grit, 3/8" wide)
- Back and forth across the PCB @ medium pressure





Delayering: Dremel Tool 2

- Difficult to keep tool flat against the PCB
  - Dremel 225 flexible shaft will help move the tool's body away from the work surface
- Easy to accidentally remove too much material from the target surface
  - More care/practice required!

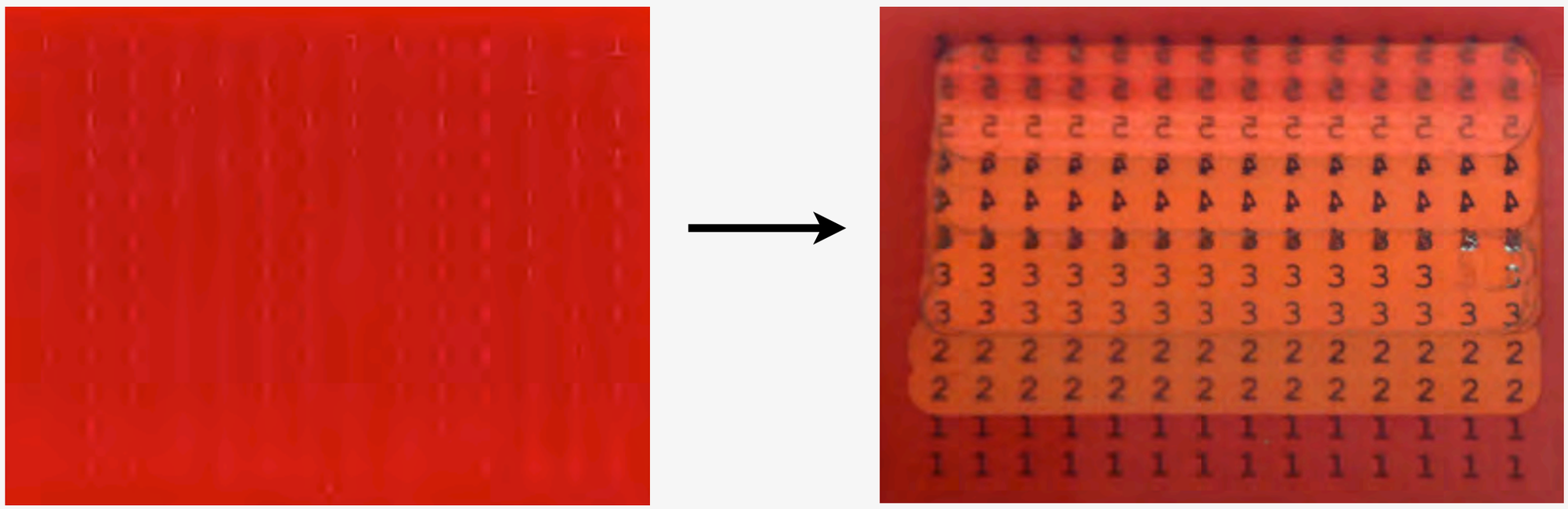


Delayering: CNC Milling

- T-Tech QuickCircuit 5000 PCB Prototyping System
  - Z-axis can be manually adjusted in 10um (0.4mil) increments
- Think & Tinker MN208-1250-019F 1/8” diameter carbide endmill
- IsoPro 2.7 for control and manipulation of milling, drilling, and routing procedures

Delayering: CNC Milling 2

- PCBDT Reference Board
- Z-axis depth incrementally adjusted
- Manual jog to mill away the desired area(s)
- Resulting PCB has a stair-step that can be visually identified and felt with a finger
  - Proved that it was possible to access a specific copper layer using CNC



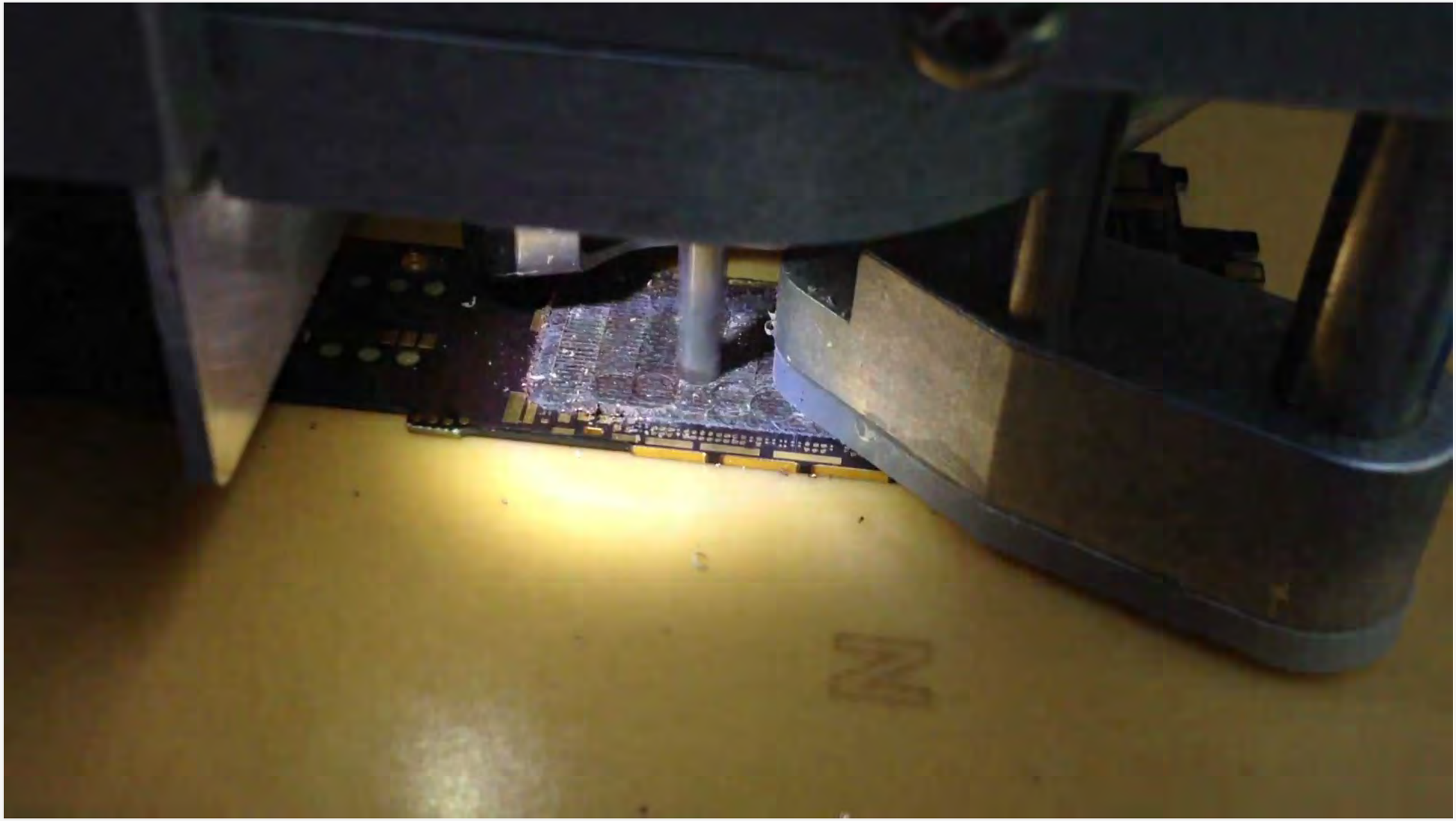
GRAND IDEA STUDIO

Delayering: CNC Milling 3

- iPhone 4 16GB Logic Board
- Mechanical outline of the desired PCB area created in IsoPro
- Configured to rubout all material internal to that area
  - Allows for accurate, repeatable, and automatic positioning of the milling path
- Z-axis depth adjusted in 1mil increments
- When layer of copper was visible beneath the substrate, switched to manual abrasion using fiberglass scratch brush
- Repeat

GRAND IDEA STUDIO

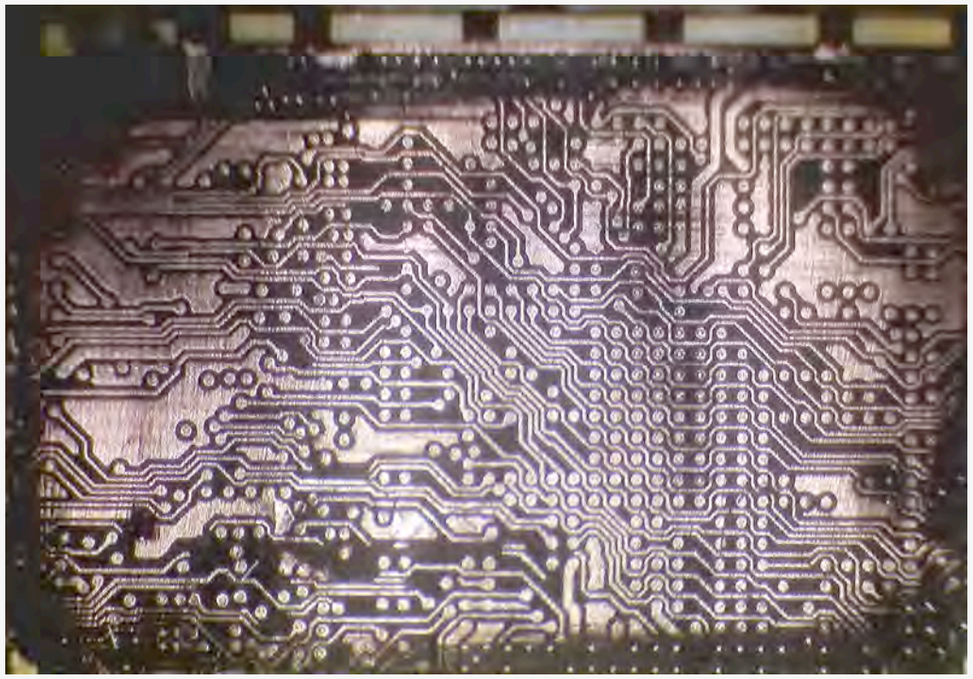
Delayering: CNC Milling 4



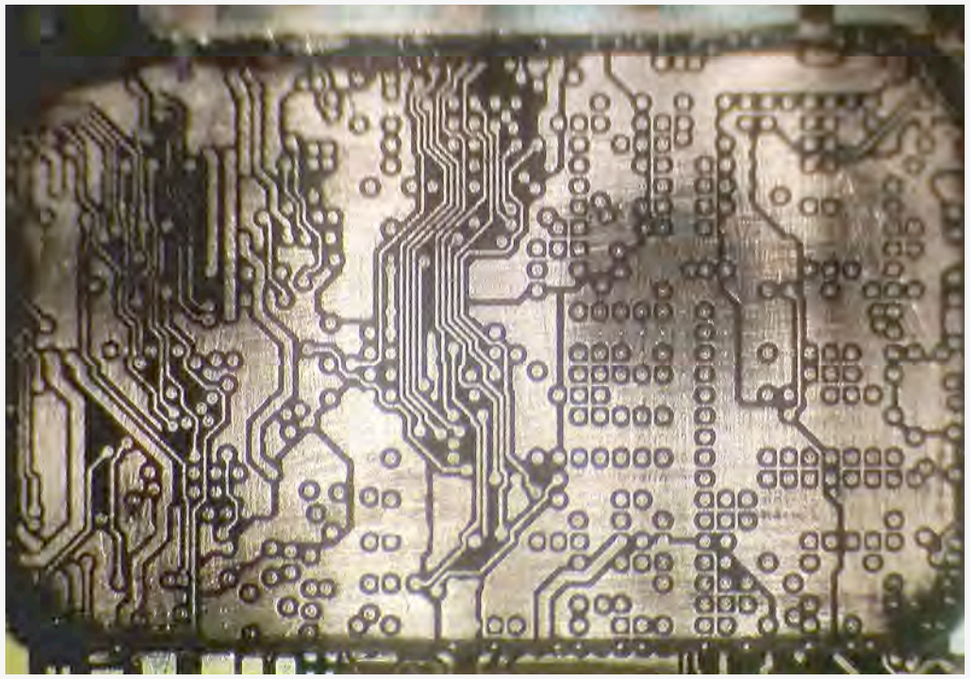
GRAND IDEA STUDIO

Delayering: CNC Milling 5

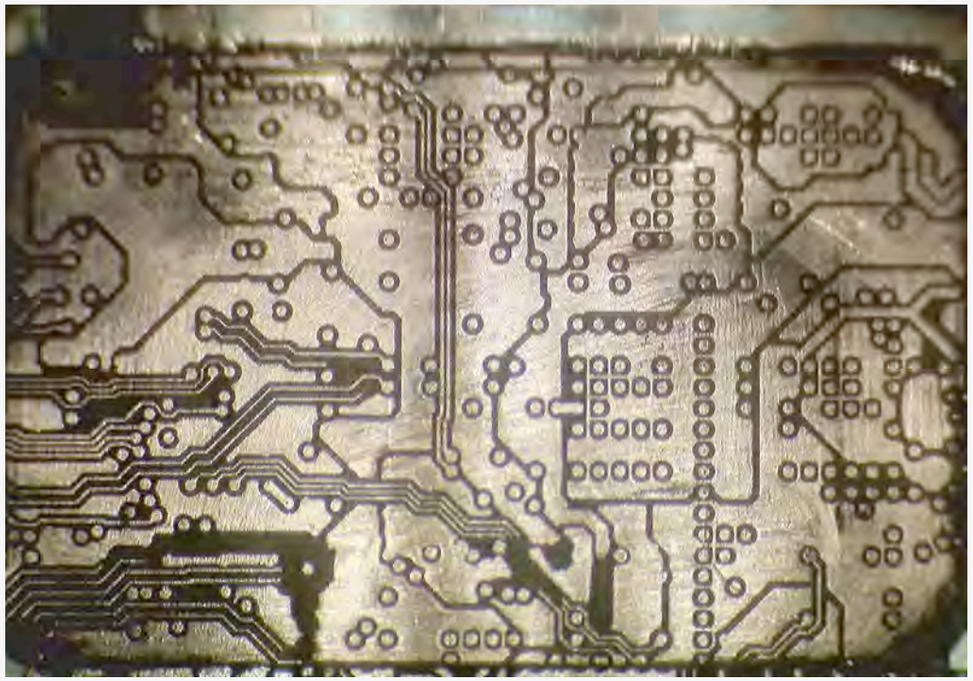
2



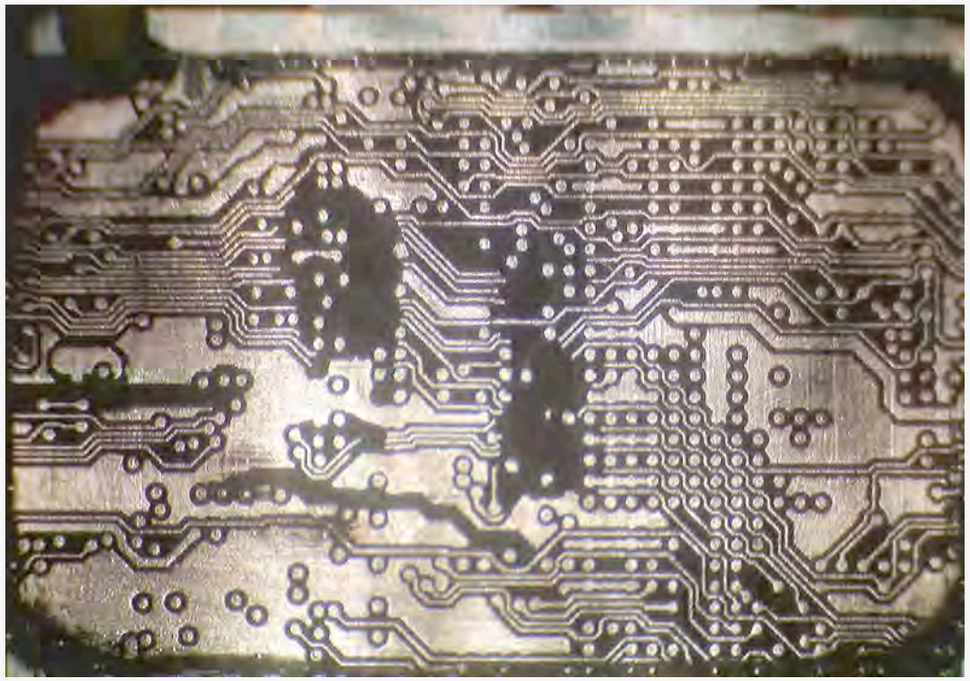
3



4



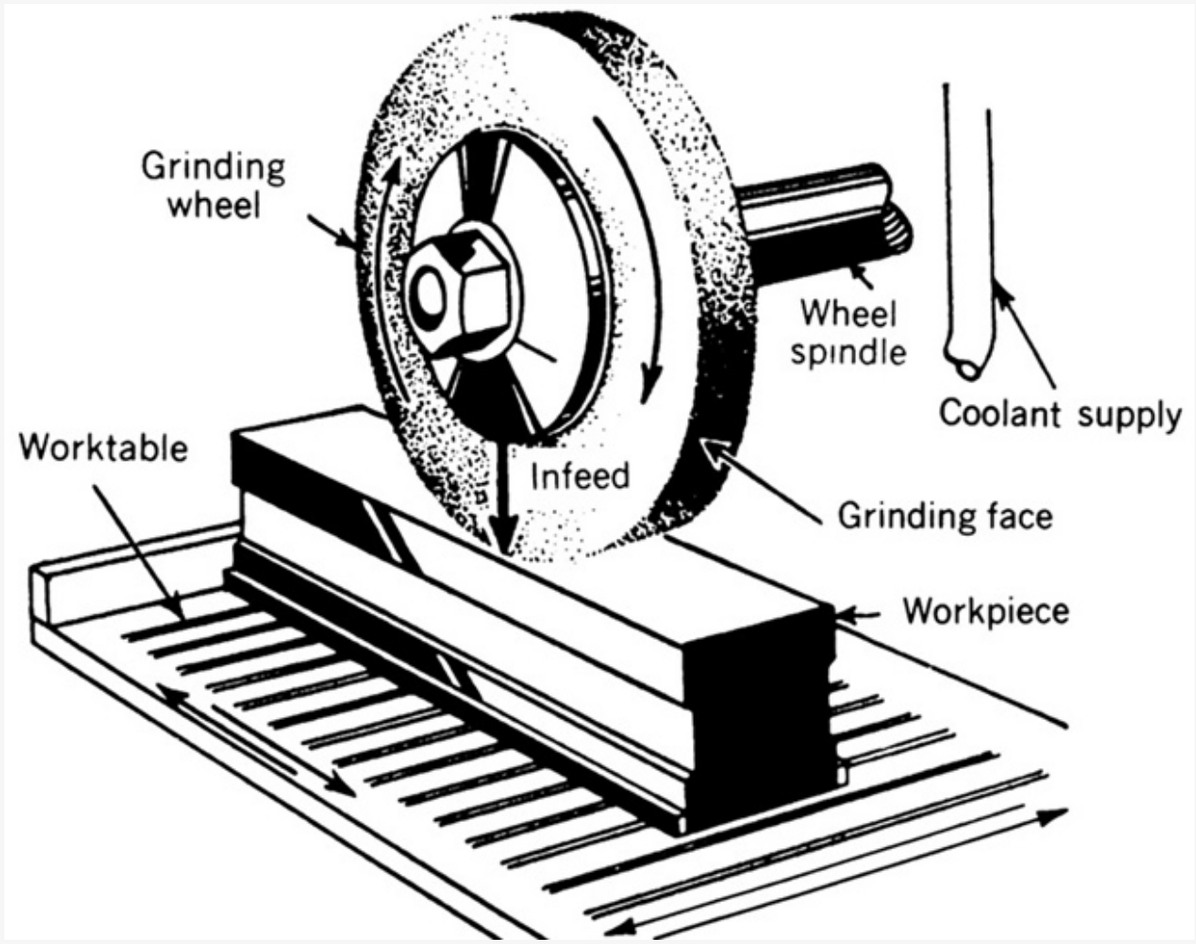
5



iPhone 4 16GB Logic Board (0.92" x 0.58" area)

Delayering: Surface Grinding

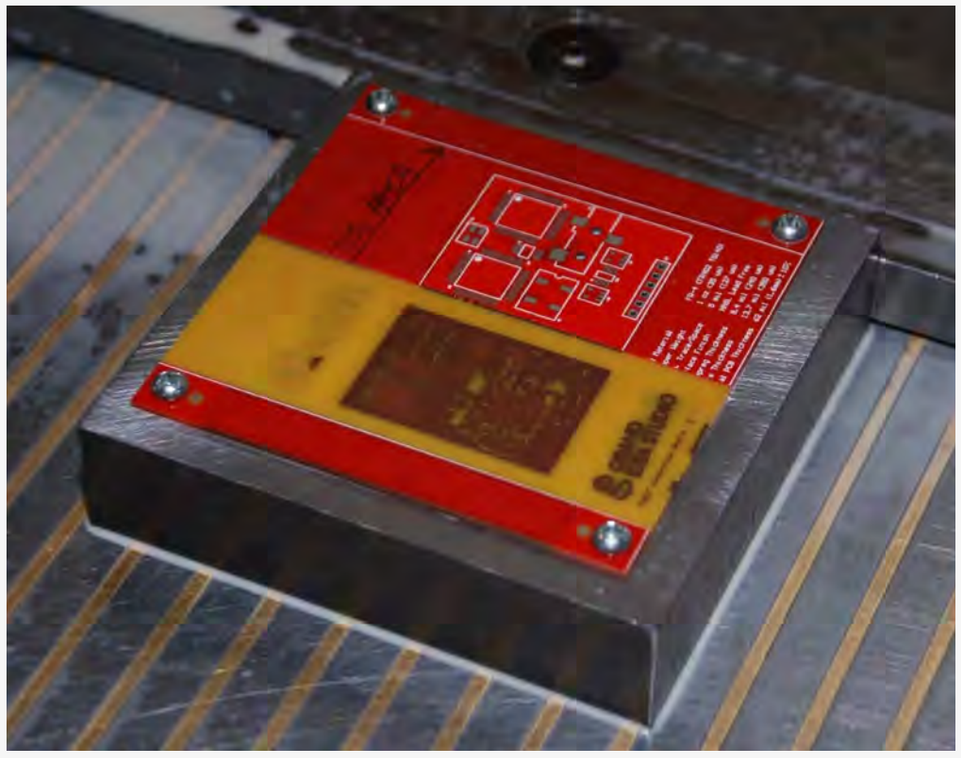
- Typically used for material grinding & surface finishing
- Consists of a rotating abrasive wheel (grinding wheel), work surface, and reciprocating or rotary table (manual or computer control)



http://engineerharry.files.wordpress.com/2012/04/grinder1.png

Delayering: Surface Grinding 2

- Blohm PROFIMAT CNC Creep Feed Surface Grinder w/ Siemens SINUMERIK 810G controller & Radiac 1 3/8”-wide wheel @ General Grinding, Oakland, CA
  - Depth control in 0.1mil increments
- Target PCB mounted to steel block (held in place by magnetic chuck)

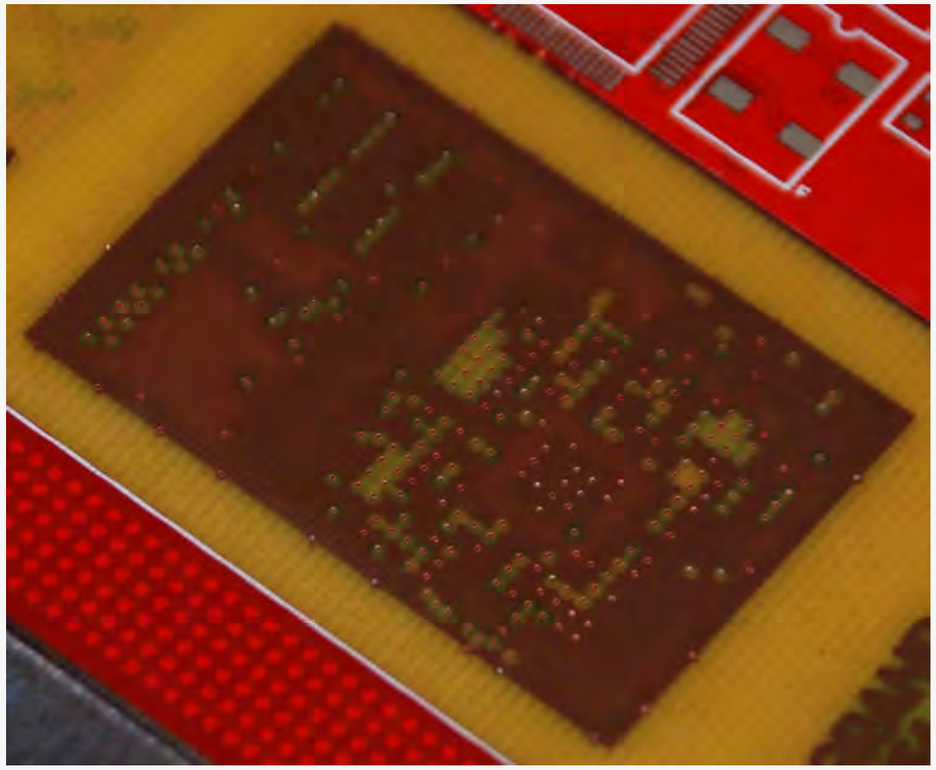


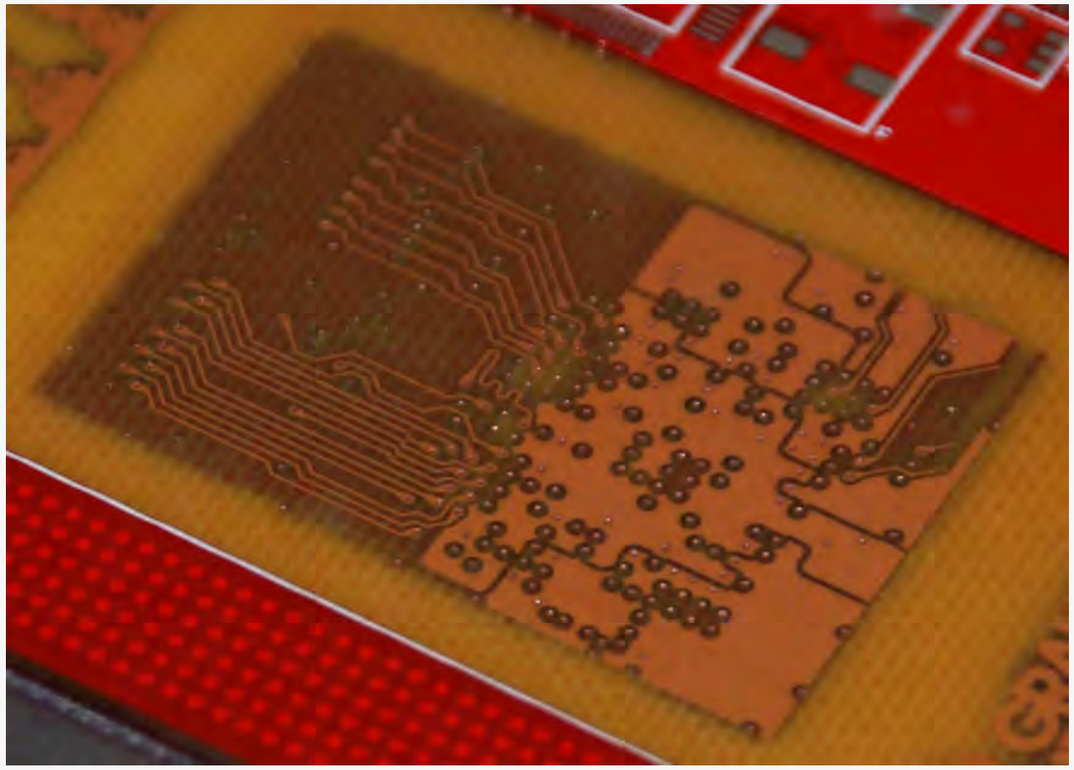
GRAND IDEA STUDIO

Delayering: Surface Grinding 3

Delayering: Surface Grinding 4

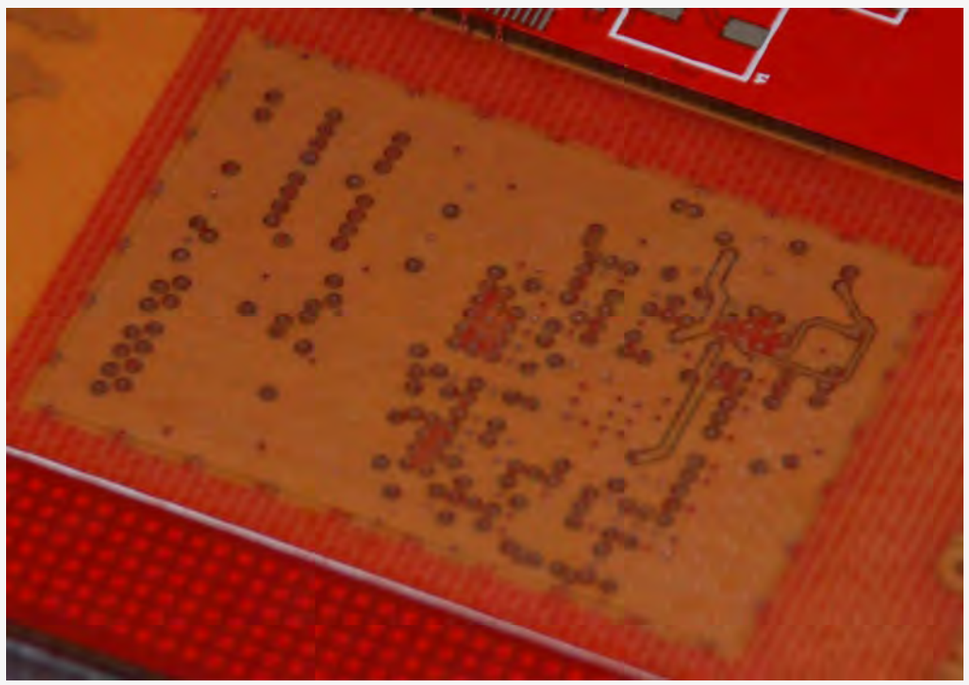
2

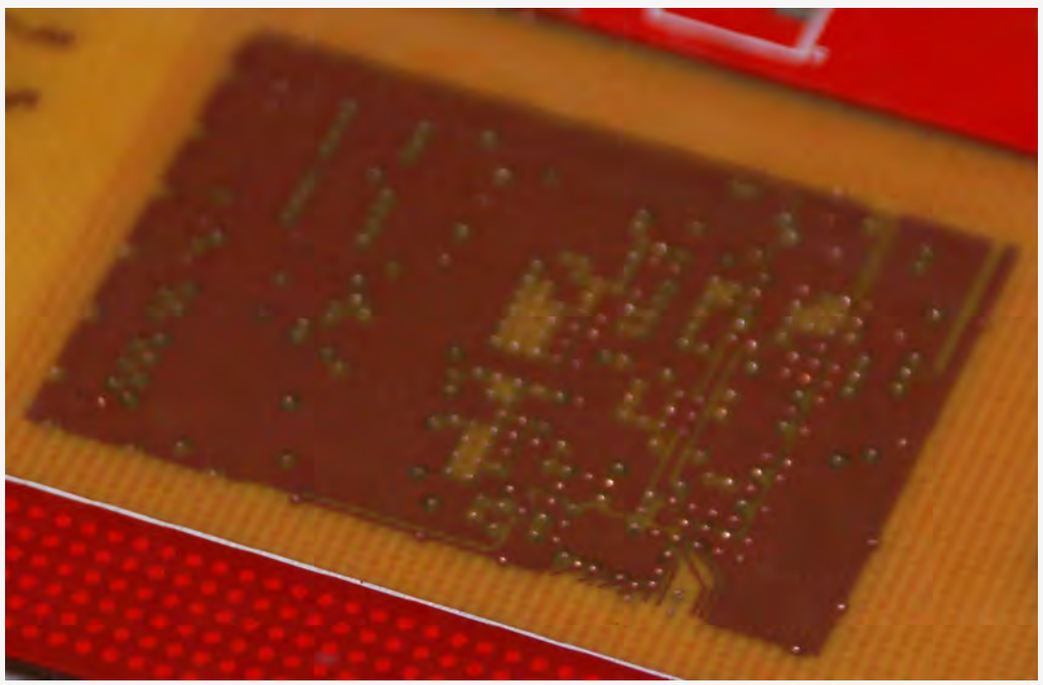




3

4

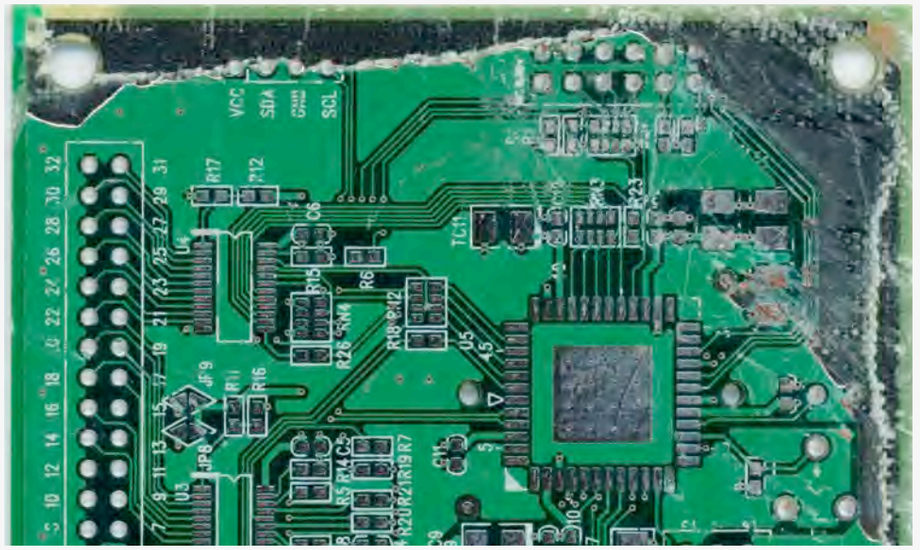


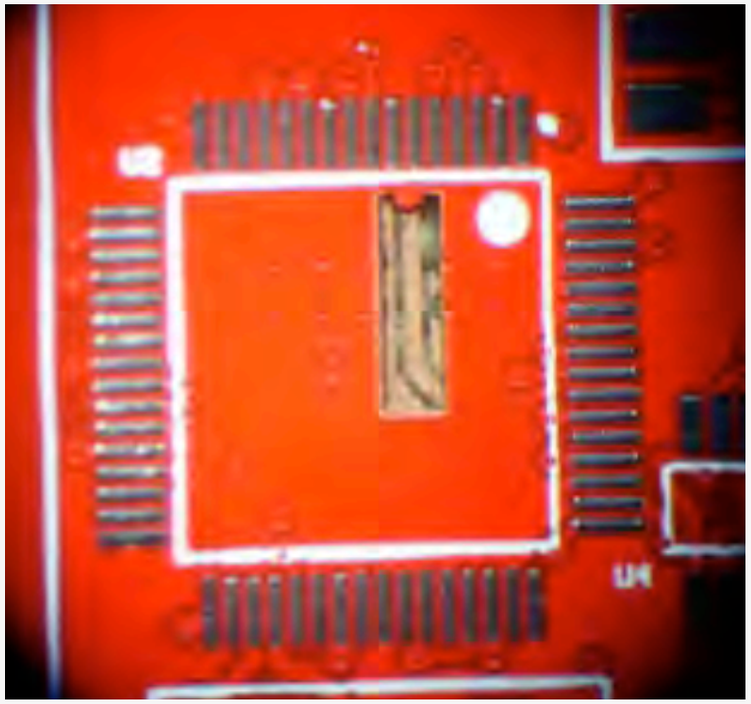


5

Delayering: Failures

- Heat
  - Heat gun
  - Hot knife
- Laser
  - UV/CO2



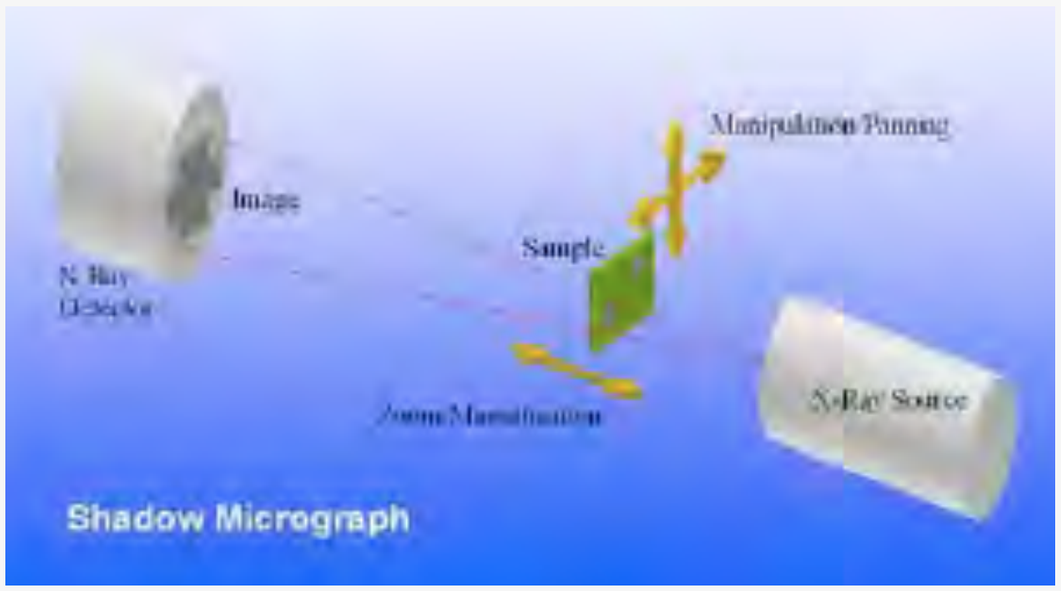


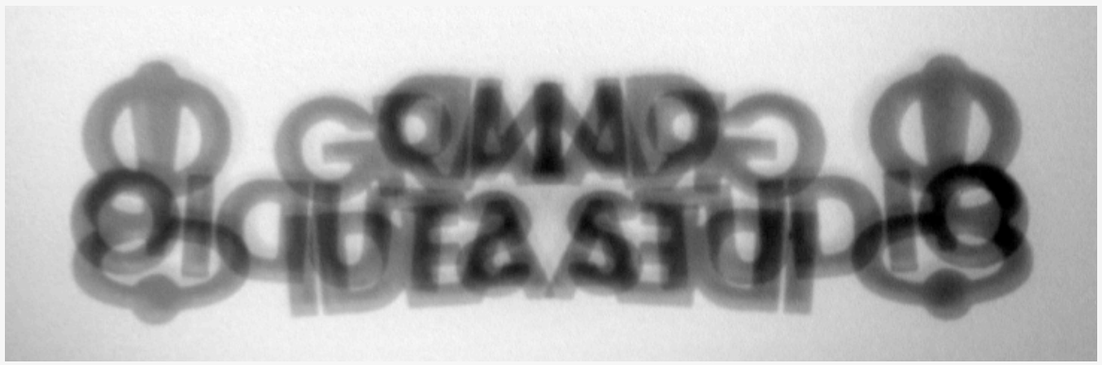
Imaging

- X-ray (2D)
- Computerized Tomography (3D)

Imaging: X-Ray (2D)

- Typically used during PCB assembly (component placement/ solder quality) or failure analysis (troubleshooting defective features)
- 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

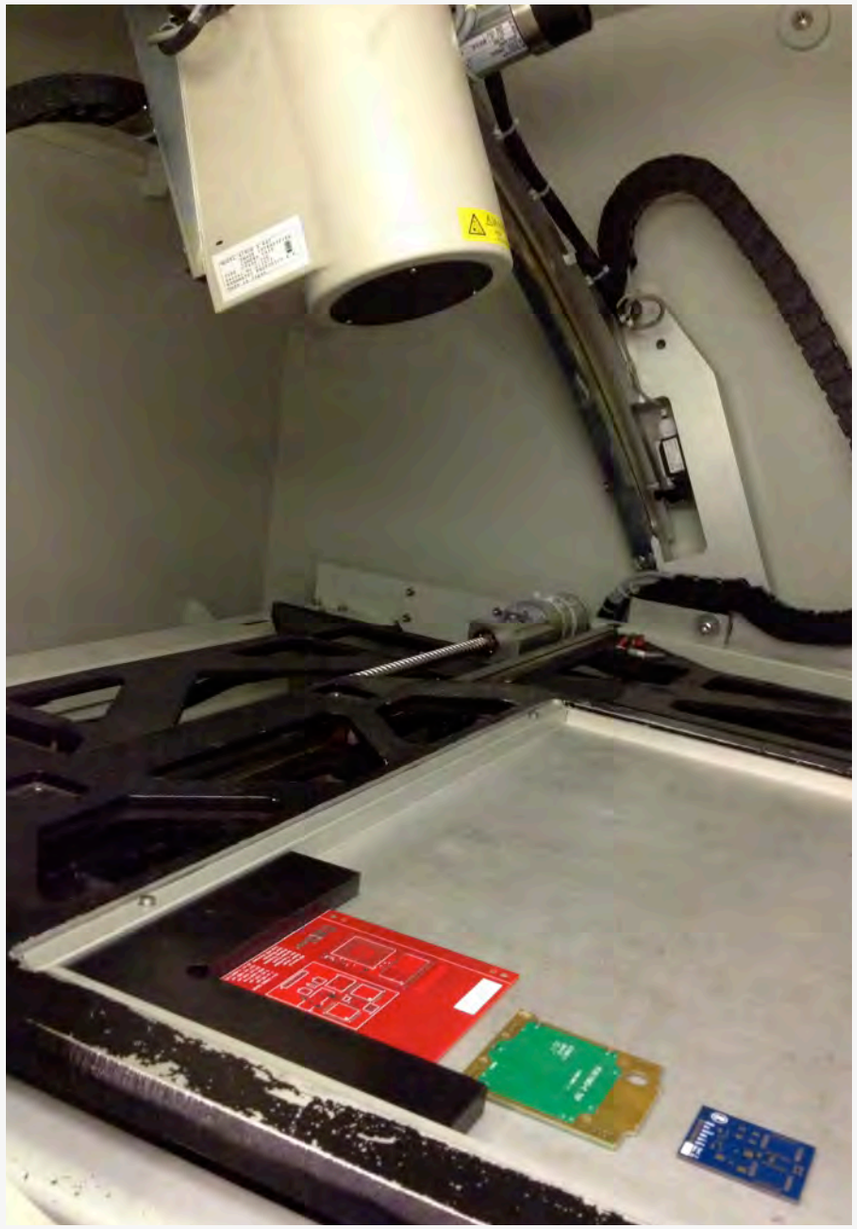




http://datest.com/resources-boardtestmeth-primer2d3d.php

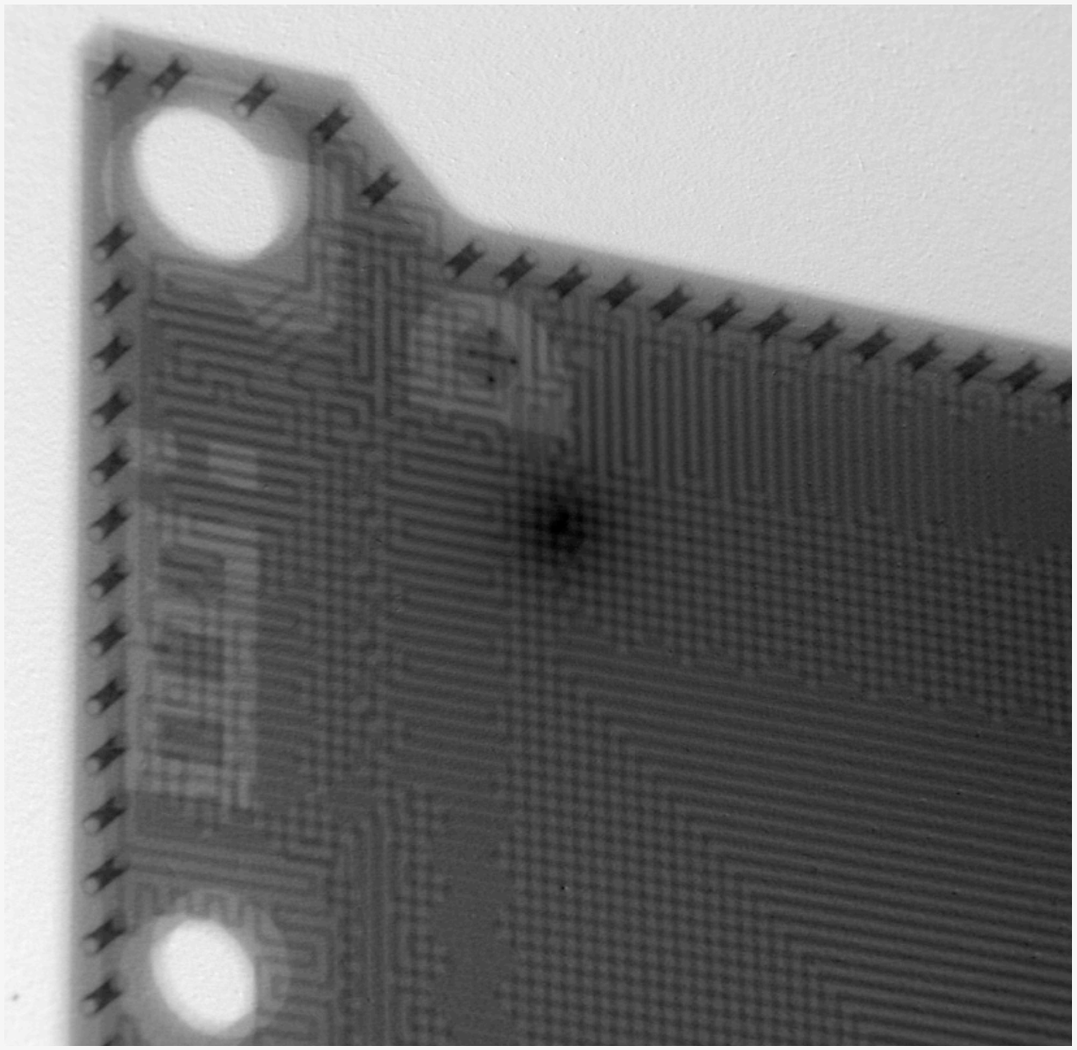
Imaging: X-Ray (2D) 2

- Nordson DAGE XD7500VR X-ray Inspection System @ Sonic Manufacturing, Fremont, CA



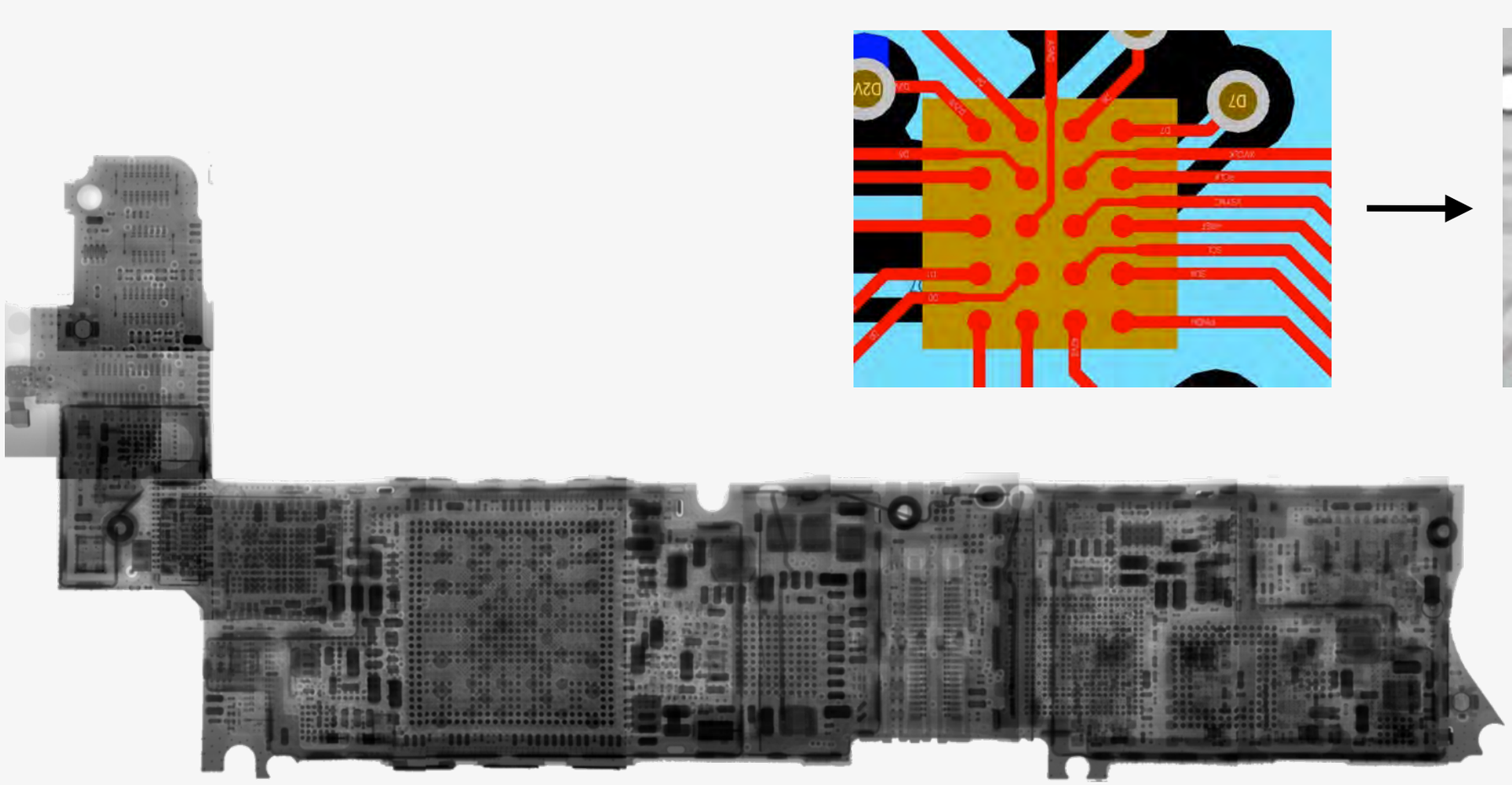
Imaging: X-Ray (2D) 3

- Can get clues about PCB construction/layout, component location, layer count, hidden/embedded features
- VeriFone PINpad 1000SE active security envelope

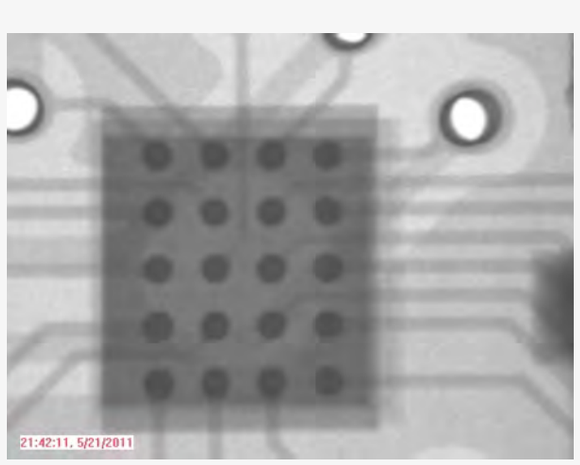


Imaging: X-Ray (2D) 4

- For simple boards, can visually follow traces/interconnections
  - Composite image makes it difficult to determine on which layer a particular trace is located
  - Manipulating the X-ray angle and field-of-view in real time will help

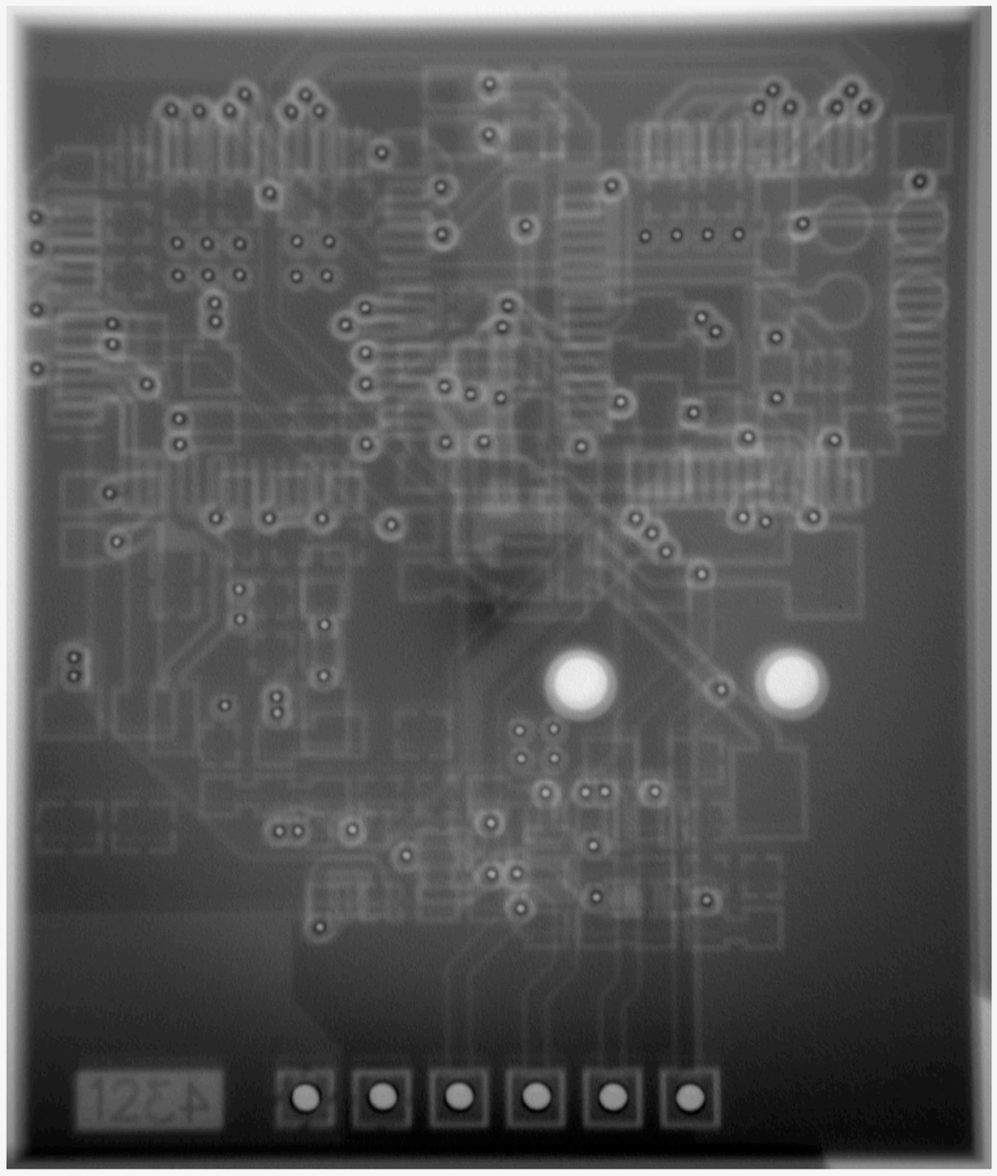


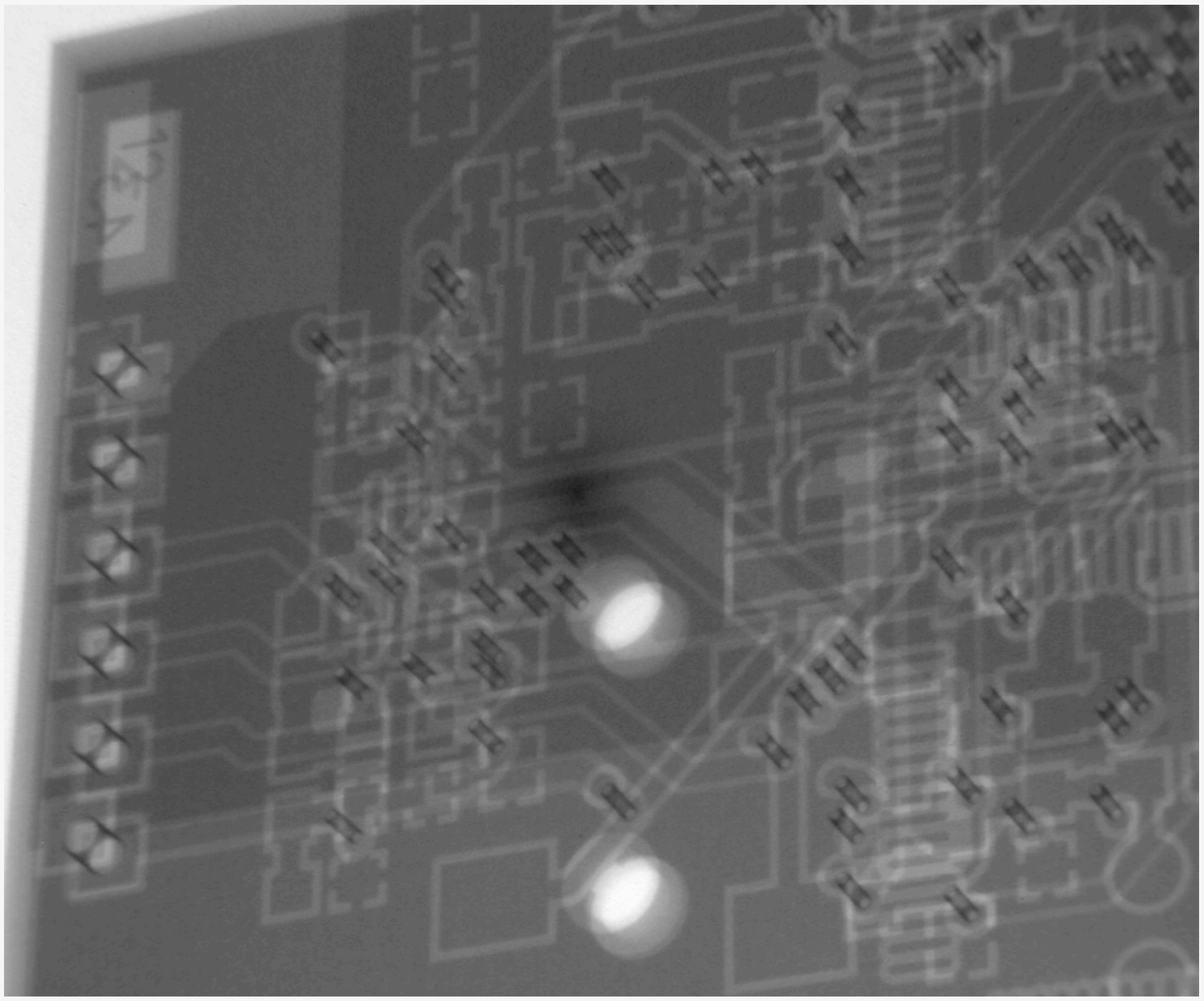
iPhone 4 16GB Assembled



20-pin uBGA (CSP3)

Imaging: X-Ray (2D) 5

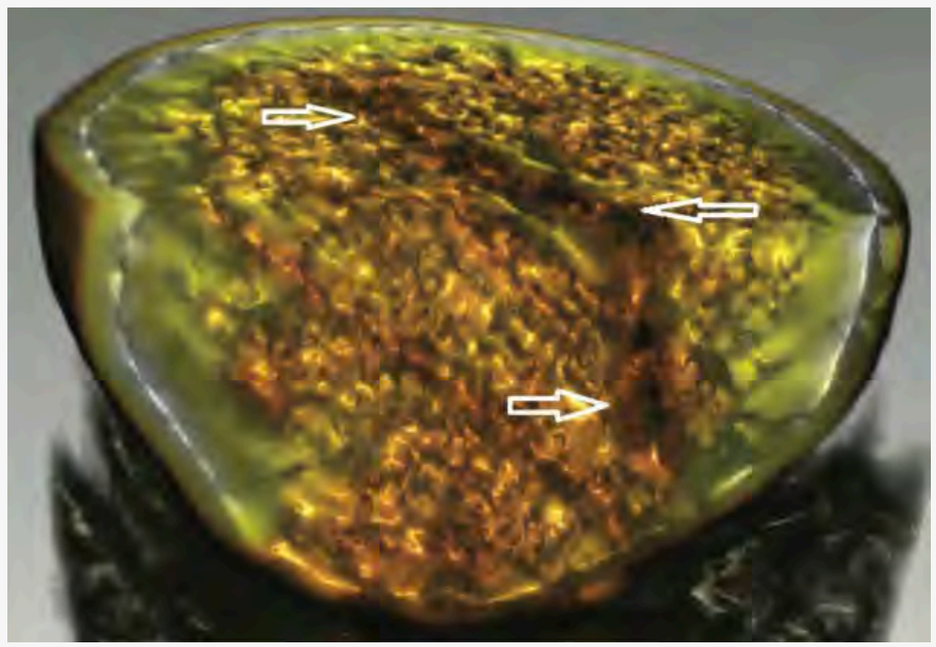




Emic 2 Text-to-Speech Module

Imaging: 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
- Typically used for complex inspection and failure analysis of PCBs, component packaging, solder ball/joint quality
- 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

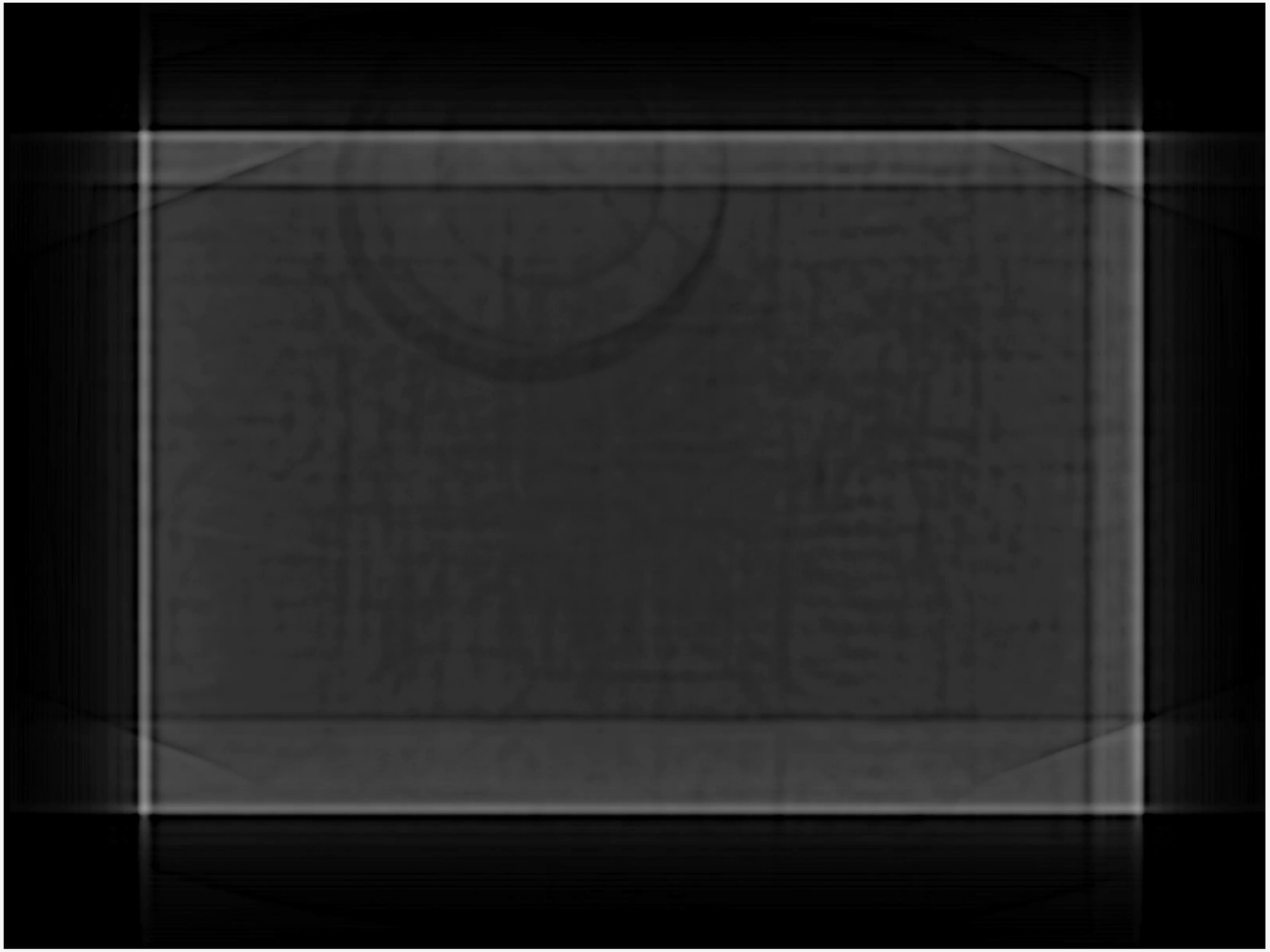
Imaging: X-Ray (3D/CT) 2

- Nordson DAGE XD7600NT Ruby X-ray Inspection System w/ X-Plane option @ Datest, Fremont, CA

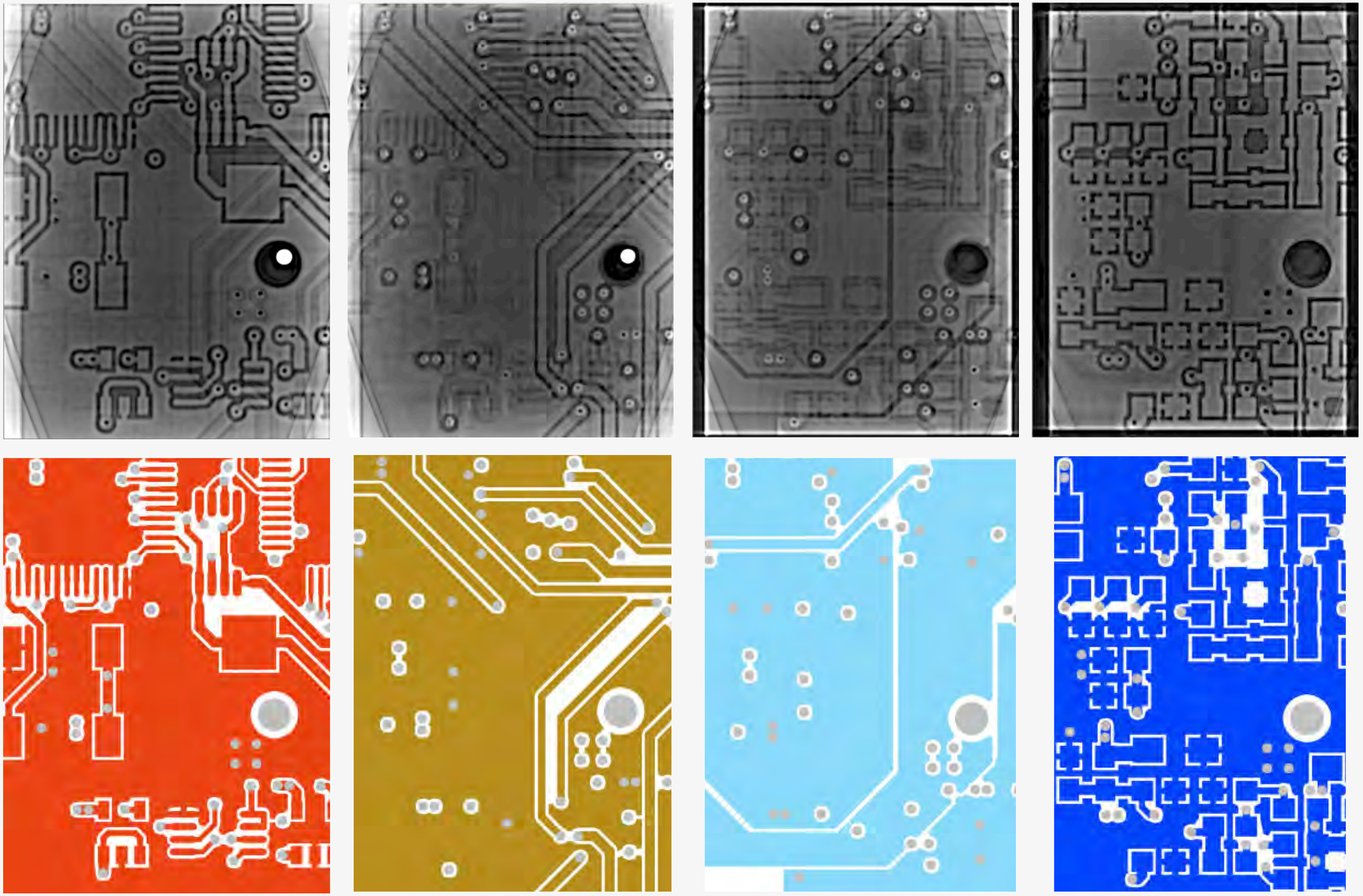
Imaging: X-Ray (3D/CT) 3

- Emic 2 Text-to-Speech Module
- 360 2D images taken at a 50° inclination angle
  - One image every 6 seconds
- Imported into VGStudio 2.1 for 3D model manipulation
- Manually moved through Z plane (top to bottom) to identify each layer
  - Could also measure substrate thickness between layers
  - Limited field-of-view will require multiple "segments" to be stitched together if working on a full PCB
- Results may vary based on layer count, inter-layer thickness, copper weight, substrate composition

Imaging: X-Ray (3D/CT) 4



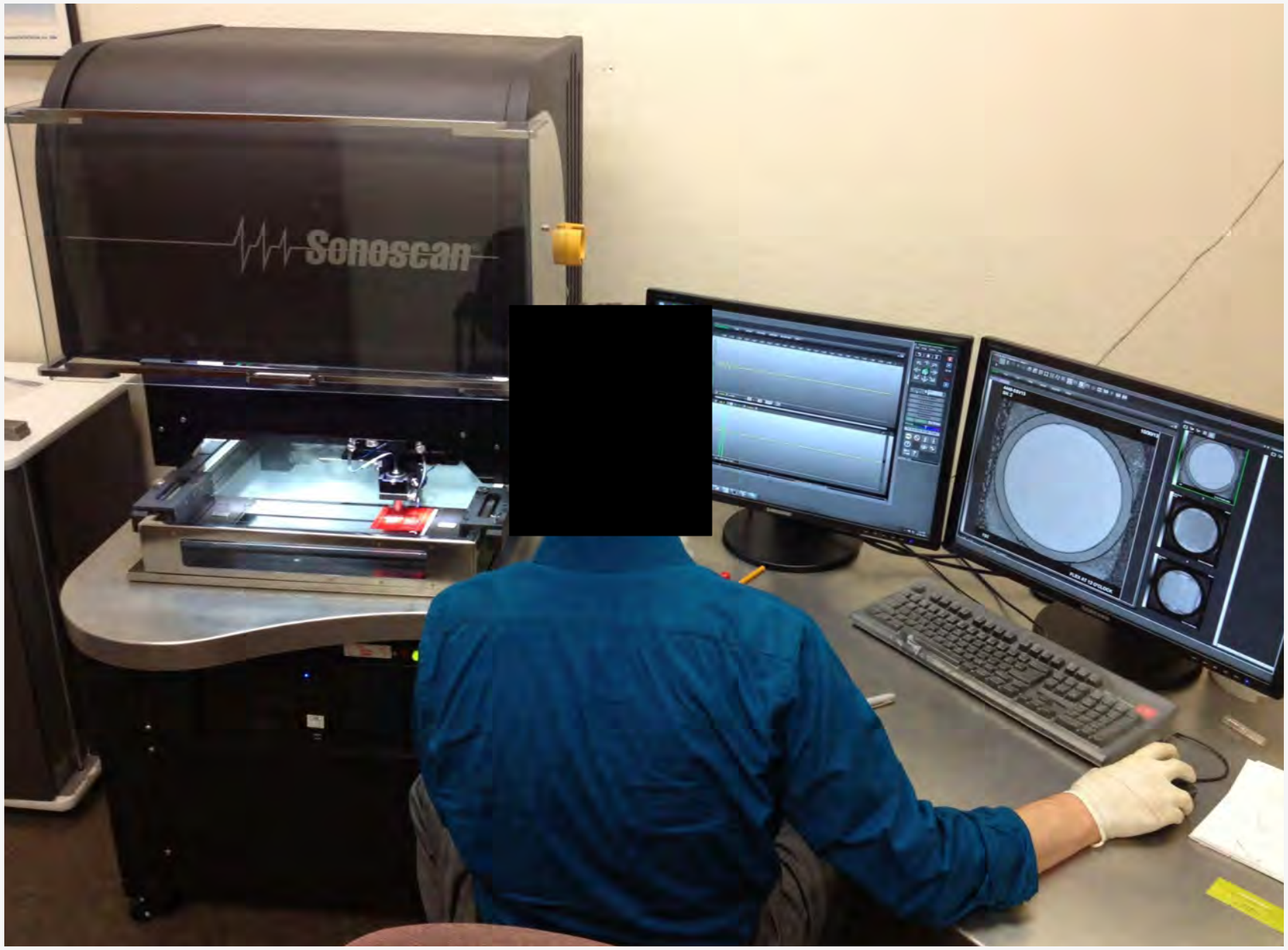
Imaging: X-Ray (3D/CT) 5

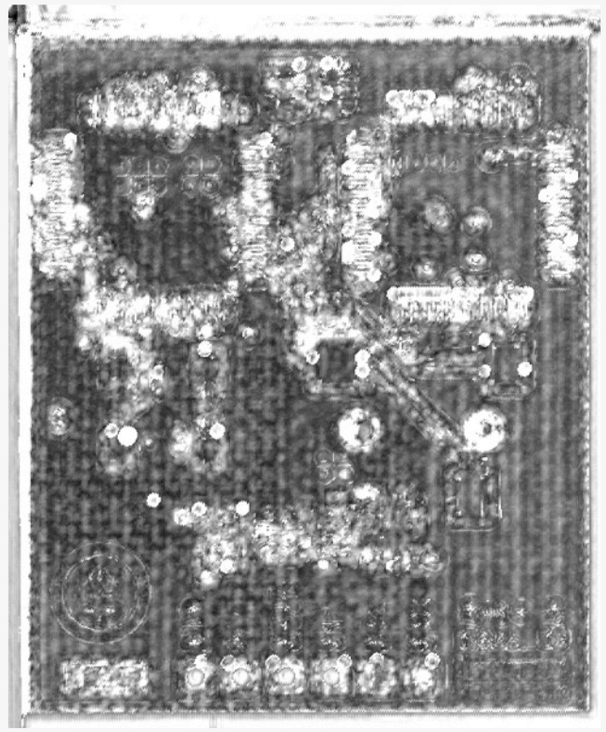


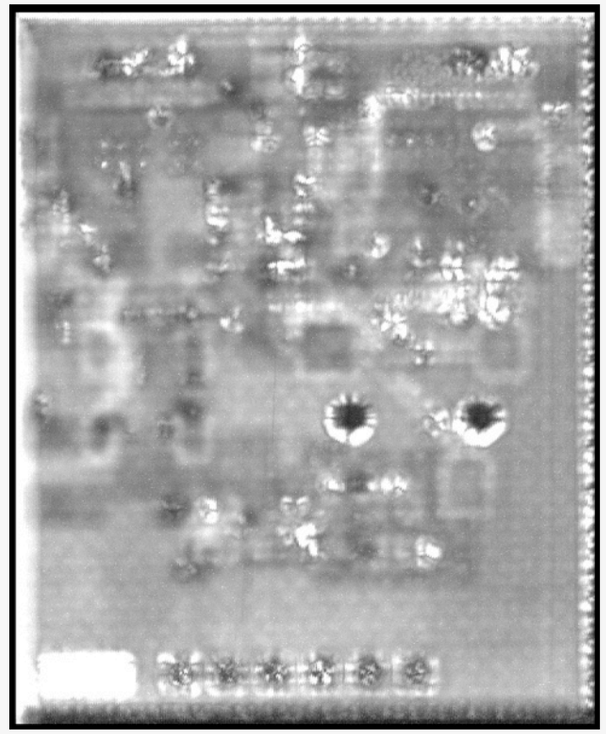
Emic 2 Text-to-Speech Module (5/8" x 7/8" area)

Imaging: Failures

- Acoustic Microscopy







GRAND IDEA STUDIO

Characterization Matrix

Technique	Time Required	Cost	Access to Equipment	Ease of Use	Likelihood of Success	Quality of Result
Solder Mask Removal						
Sandpaper	< 1 hour	$	Easy	Easy	Fair	Good
Fiberglass scratch brush	< 1 hour	$	Easy	Easy	Excellent	Excellent
Abrasive sand blasting	< 1 hour	$$	Moderate	Medium	Fair	Good
Ristoff C-8	3-4 hours	$$	Difficult	Hard	Excellent	Excellent
Magnastrip 500	3-4 hours	$	Difficult	Hard	Excellent	Excellent
Laser	2-3 hours	$$$	Moderate	Hard	Varies	Excellent
Delayering						
Sandpaper	2-3 hours	$	Easy	Easy	Fair	Excellent
Dremel tool	< 1 hour	$	Easy	Medium	Poor	Varies
CNC milling	3-4 hours	$$	Moderate	Hard	Excellent	Excellent
Surface grinding	3-4 hours	$$$	Moderate	Hard	Excellent	Excellent
Imaging						
X-ray (2D)	Many	$$$	Moderate	Medium	Poor	Varies
Computerized Tomography	1-2 hours	$$$	Moderate	Medium	Fair	Excellent

GRAND IDEA STUDIO

Next Steps

- Test additional delayering techniques
  - Methyl Ethyl Ketone, drum sander
- Development of software toolkit (in progress)
  - Automated/assisted creation of schematic based on PCB layer images
  - Computer vision/image processing routines
  - Open source, cross platform (Python + OpenCV)
  - Ala *degate* or *rompar*, but for PCBs

* All documentation, videos, and research available at **`www.grandideastudio.com/pcbdt/`**

The End.