Using Superpowers for Hardware Reverse Engineering

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

Superpowers* Aren't Just for Superheroes!

- Laser
- Acoustic
- X-Ray (2D/3D)

- Subset of work from my DARPA CFT *Research and Analysis of PCB Deconstruction Techniques* project
  - www.grandideastudio.com/portfolio/pcbdt/

* https://en.wikipedia.org/wiki/List_of_superhuman_features_and_abilities_in_fiction

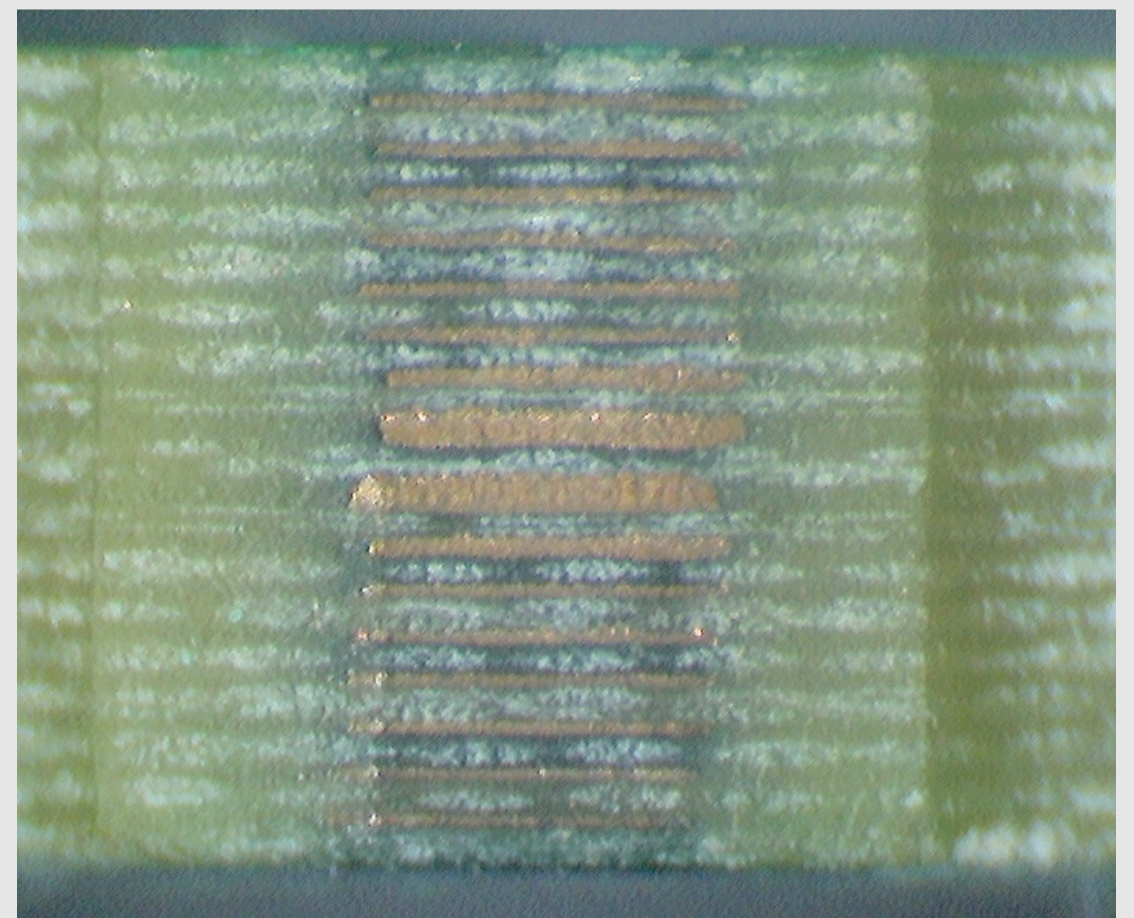
GRAND IDEA STUDIO

HW Reverse Engineering

- The art of "undesigning" an existing system
- Destructive and non-destructive methods
- Why?
  - Determine system or subsystem functionality
  - Forensic analysis/intelligence
  - Security research/verification
  - Identify areas where new features/capabilities can be added
  - Locate specific connectors/interfaces
- How?
  - Access product internals/circuitry
  - Analyze components/interconnections
  - Expose individual PCB layers

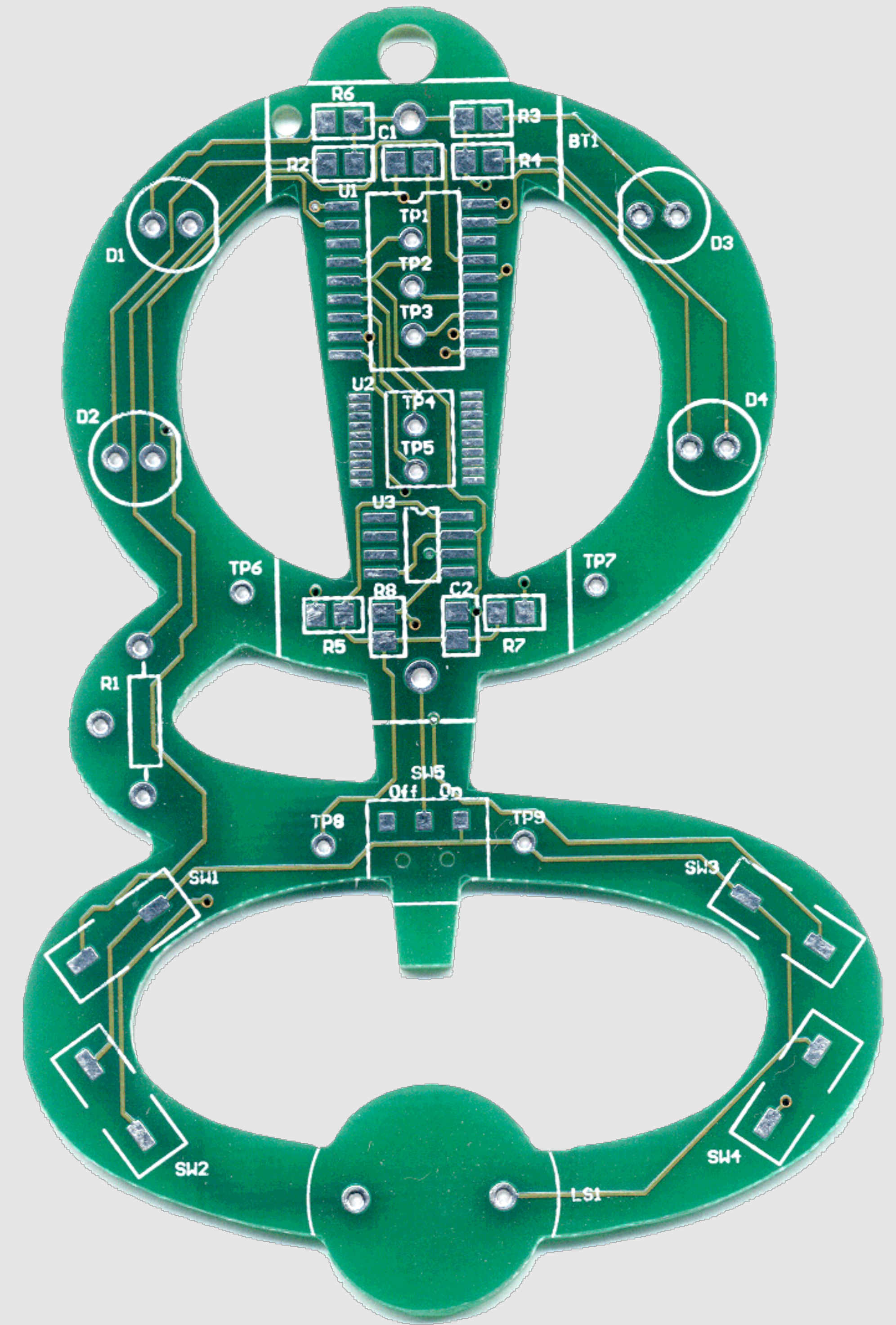
PCB Construction & Layer Stack

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



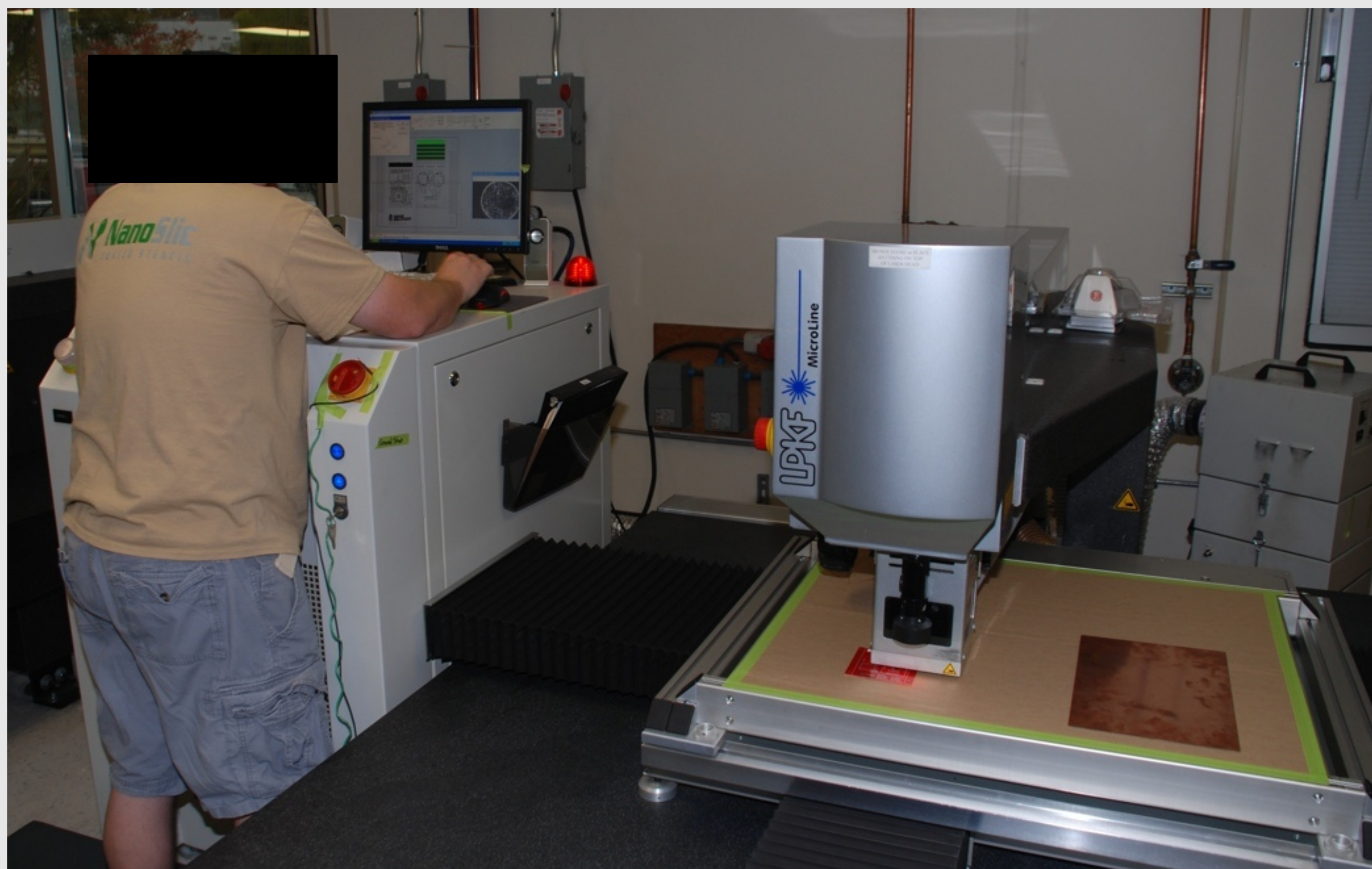
PCB Construction & Layer Stack 2

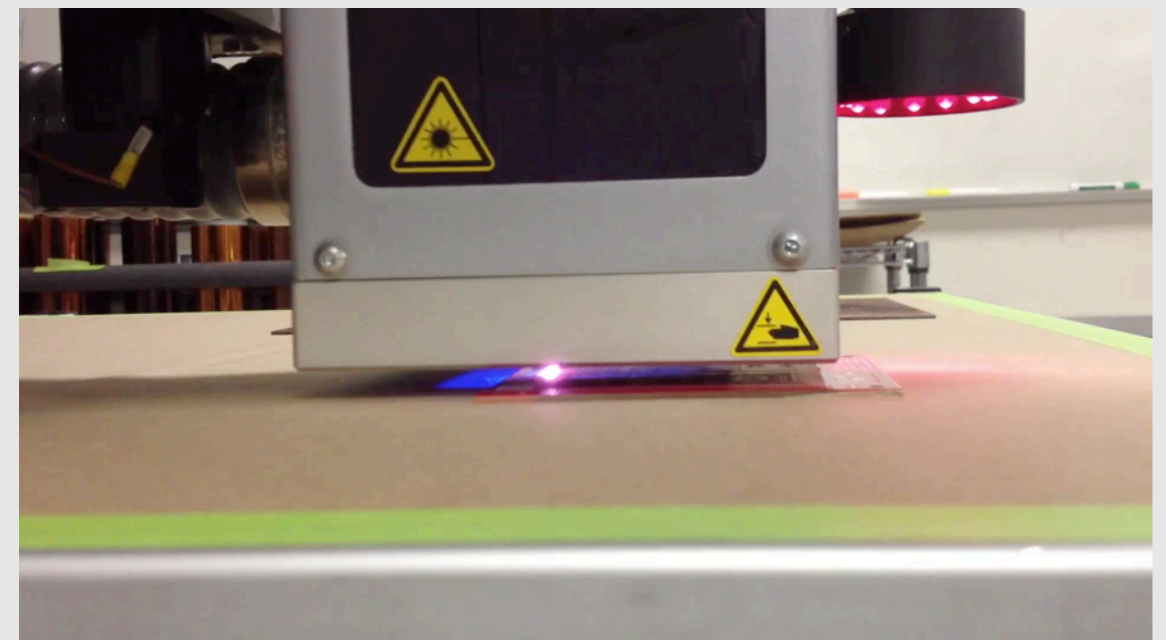
- Silkscreen (Component Legend)
  - Epoxy or printable ink
  - Part designators, symbols/logos, manufacturing/test markings
- Soldermask
  - Protects PCB from dust/moisture
  - Provides access to desired copper areas
- Copper
  - Thickness = weight of copper/sq. ft.
  - Surface finish provides better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



Laser: Soldermask Removal

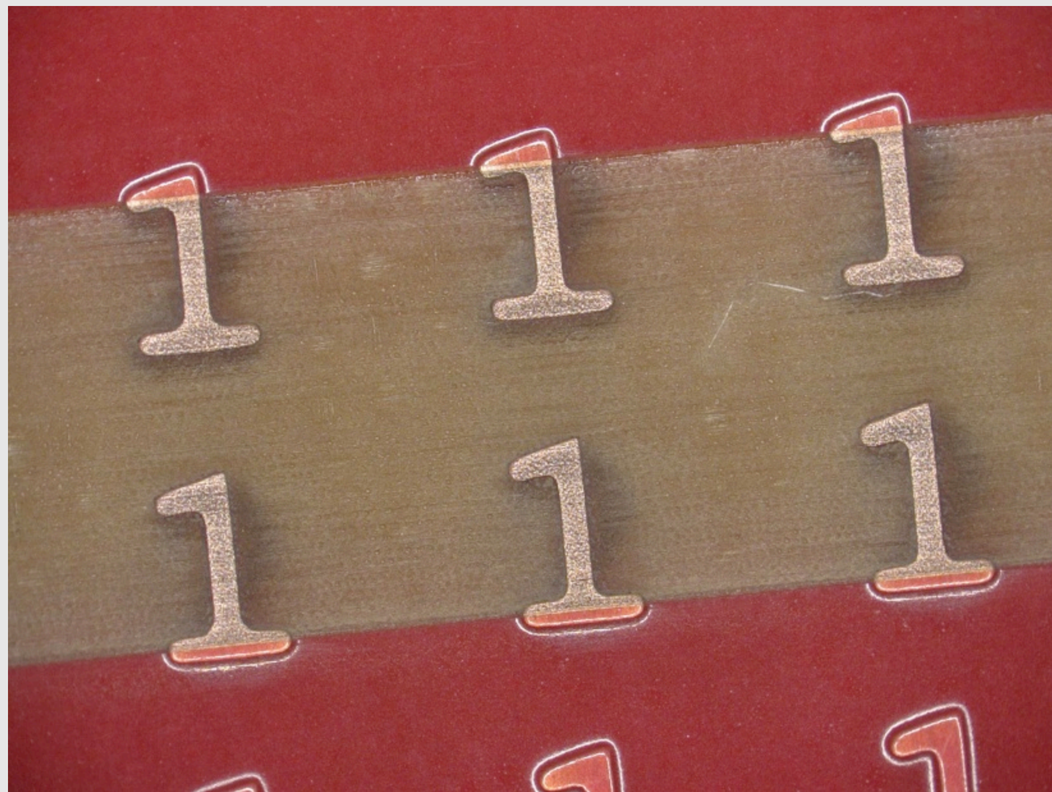
- LPKF MicroLine 600D UV Laser System @ A-Laser, Milpitas, CA
- Typically used for cutting of flex circuits and coverlayer material (film, foil, adhesive), engraving/marking
- +/-0.6 mil accuracy, 300mm/sec. (11.8"/sec.) max. travel speed, 20um (0.787mil) beam diameter



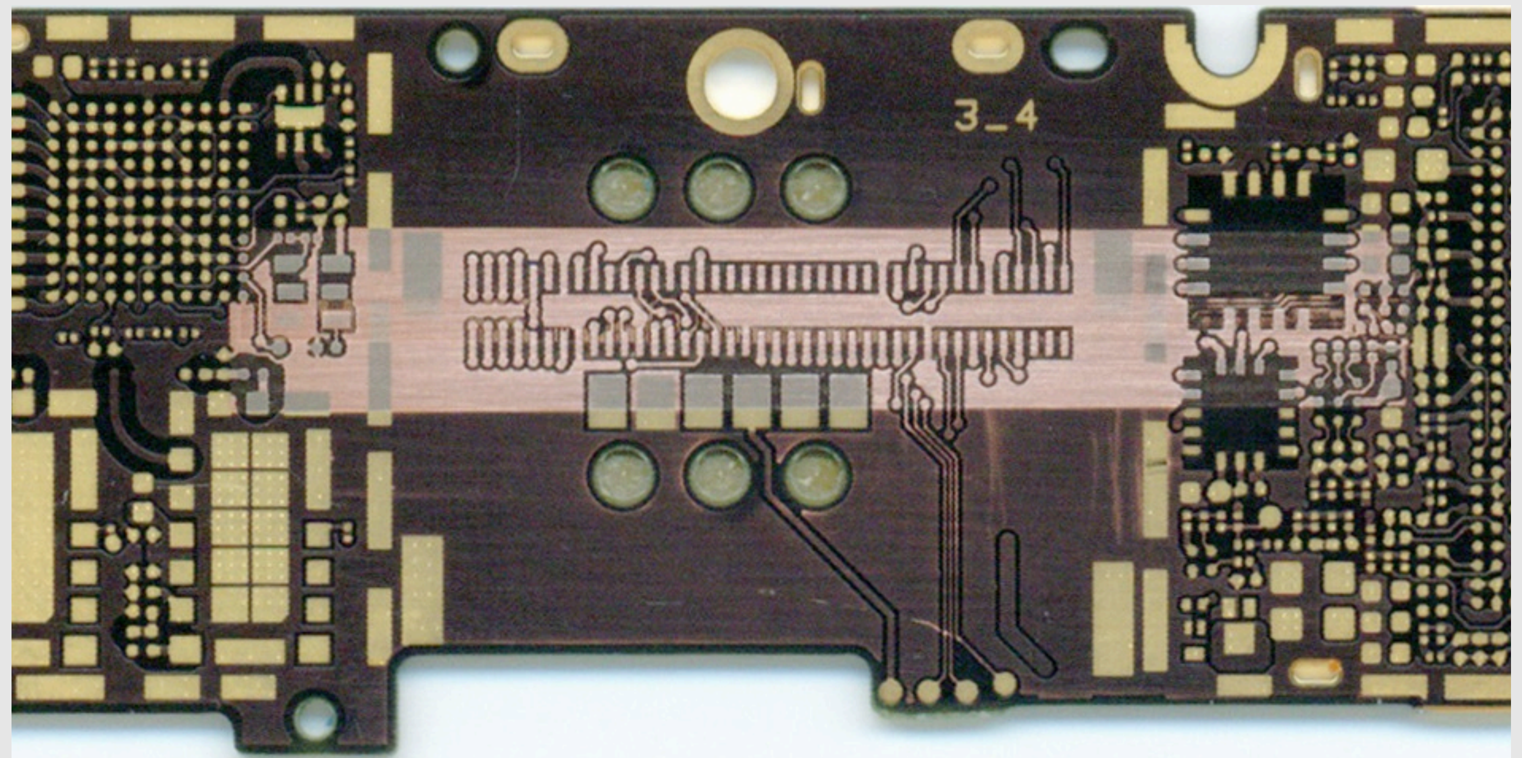


Laser: Soldermask Removal 2

- Single pass @ medium power
- Copper layer remains fully intact



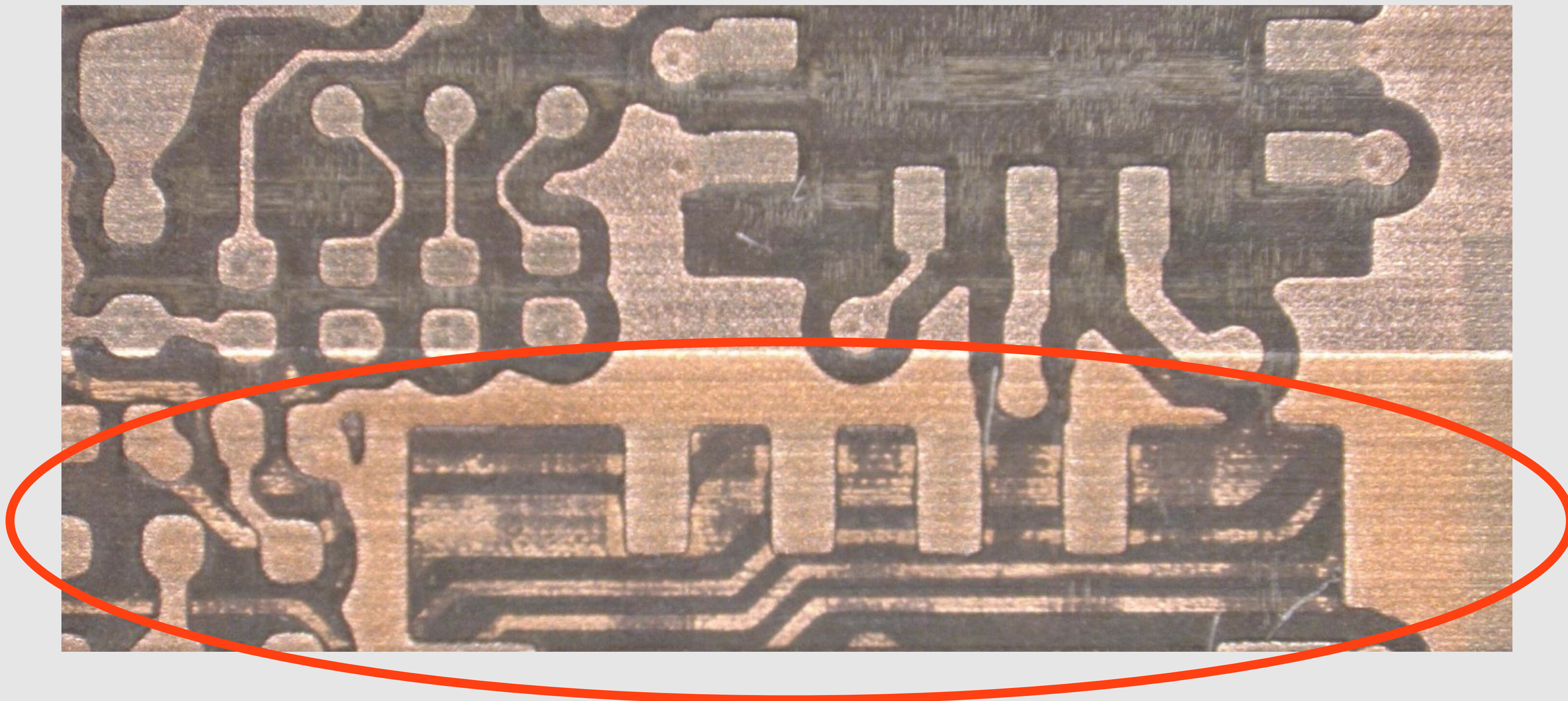
PCBDT Reference Board (Custom)



iPhone 4 16GB Logic Board

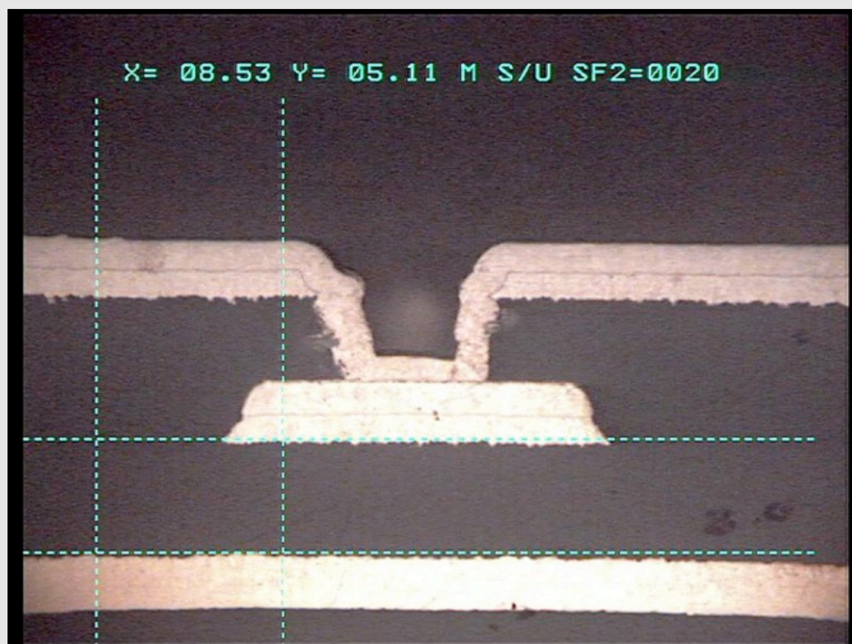
Laser: Soldermask Removal 3

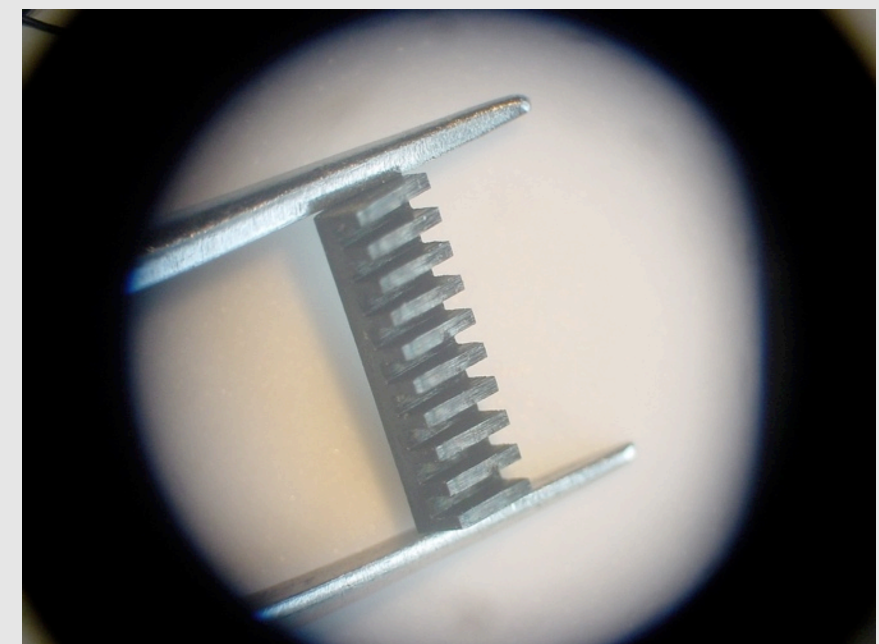
- Different materials react differently to the laser energy
  - Solder mask and FR4 ablate more quickly than copper
  - Incorrect laser power settings or too many passes can expose underlying copper



Laser: Controlled-Depth Skiving

- Typically used for selective, highly controlled material removal or rework
  - Stencils, marking, microvia drilling, cavity formation, flex/polyimide ablation, soldermask removal, micro machining
  - Could be used to defeat epoxy encapsulation?
- +/-0.5 mil beam position accuracy, 25um (1mil) min. hole diameter, 1.25mm (50mil) min. skiving depth

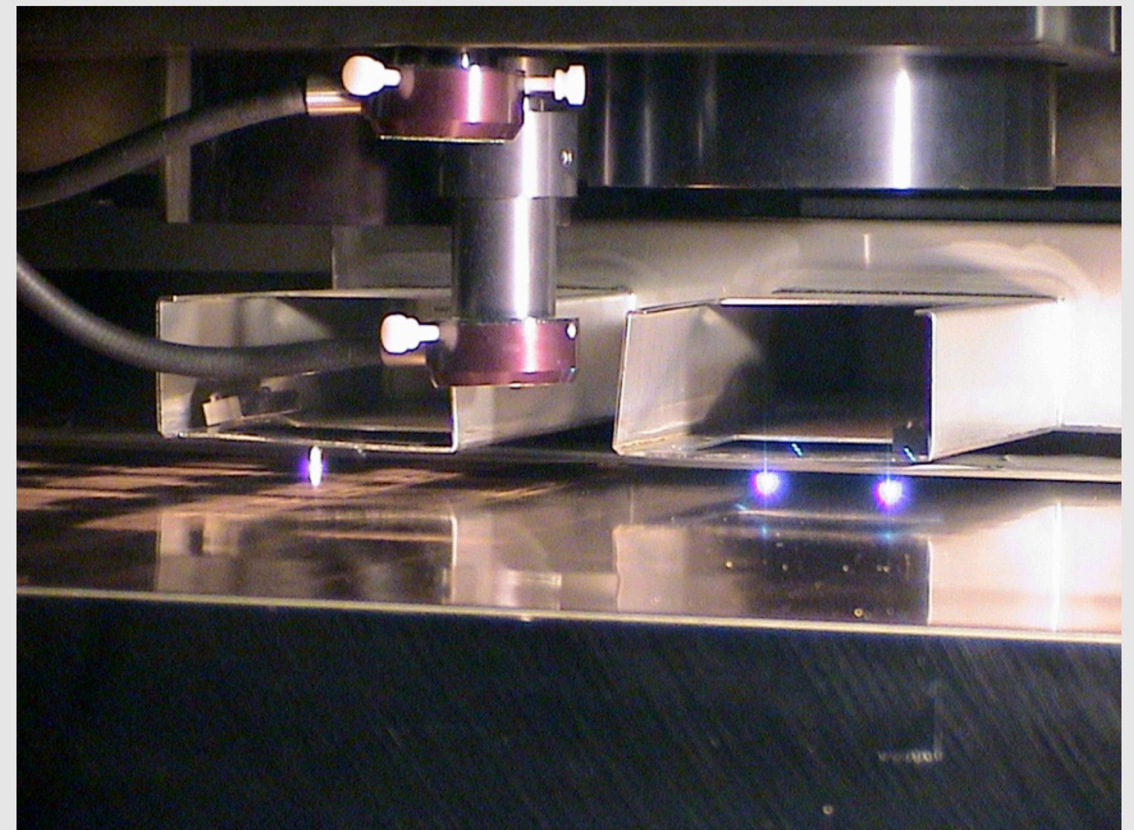




www.micronlaser.com/gallery.php

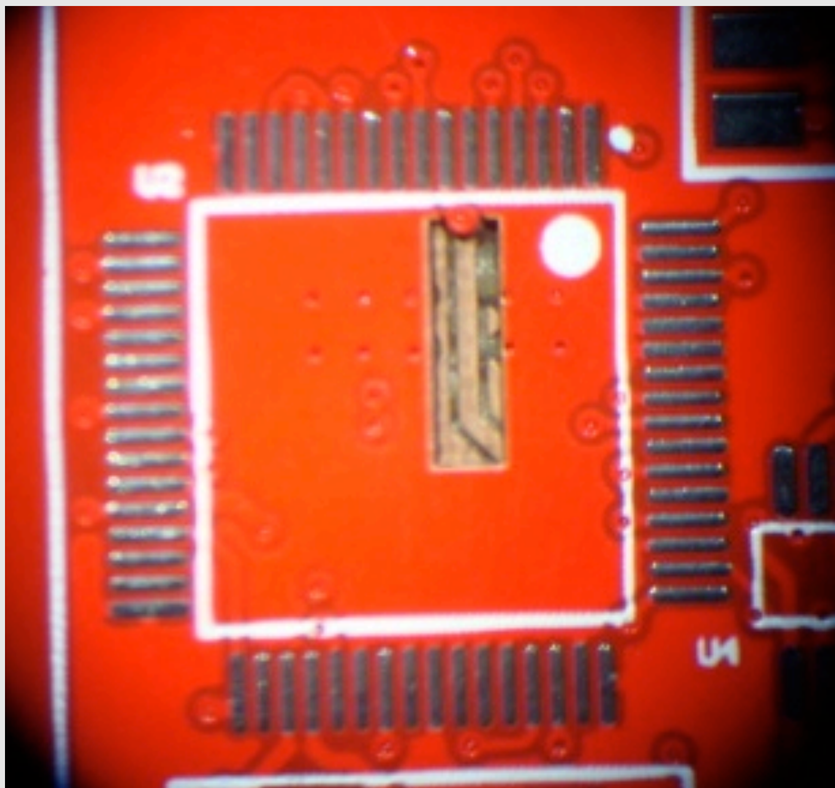
Laser: Controlled-Depth Skiving 2

- GSI Lumonics DrillStar GS-600 Laser Drilling System @ Micron Laser Technology, Portland, OR
  - Heavily modified to support different laser types (UV, CO_2), processes, and materials

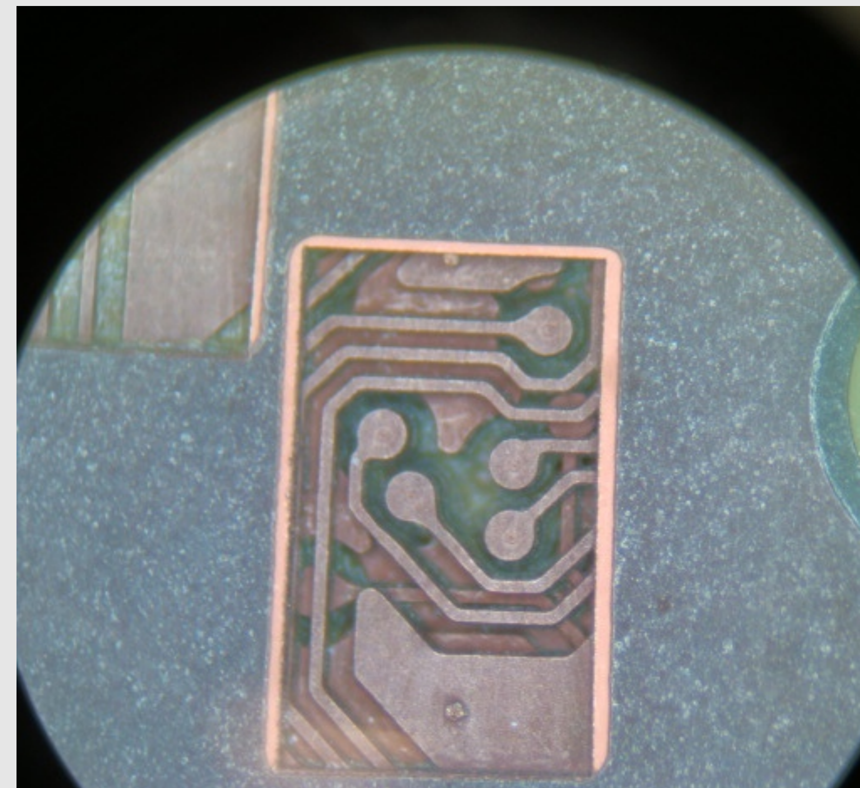


Laser: Exposing Inner Layers

- PCBDT Reference Board & iPhone 4 Logic Board
- Top copper plane removed w/ UV laser
- Series of low energy passes w/ CO_2 laser removed any substrate not blocked by copper
- No data provided to operator in advance



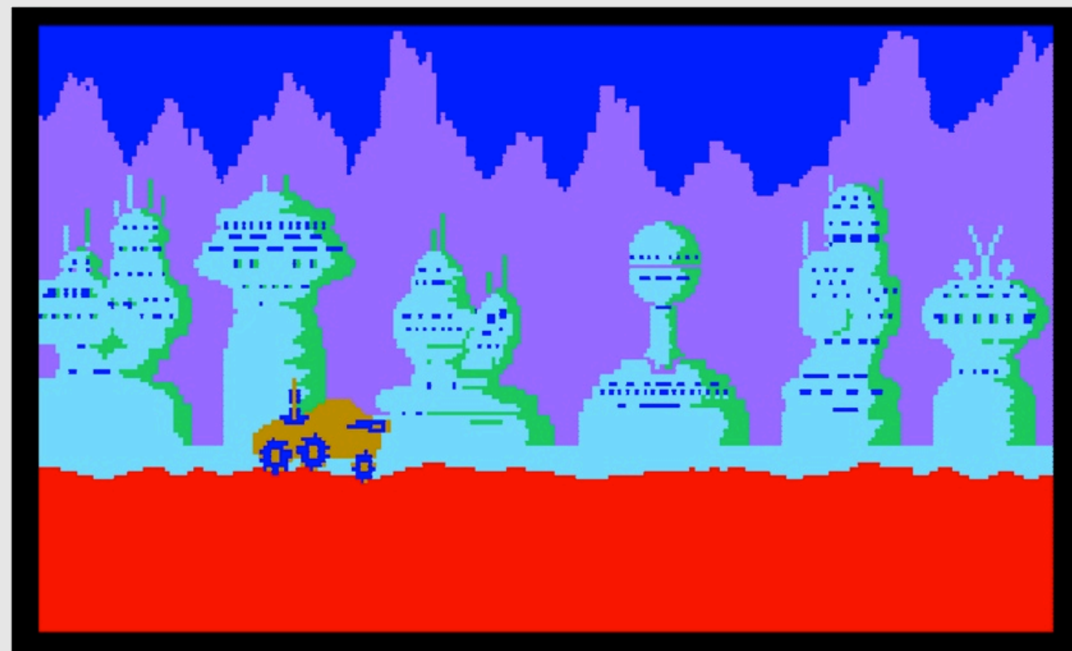
TQFP-64, Working area 0.06" x 0.2"



Working area 0.07" x 0.1"

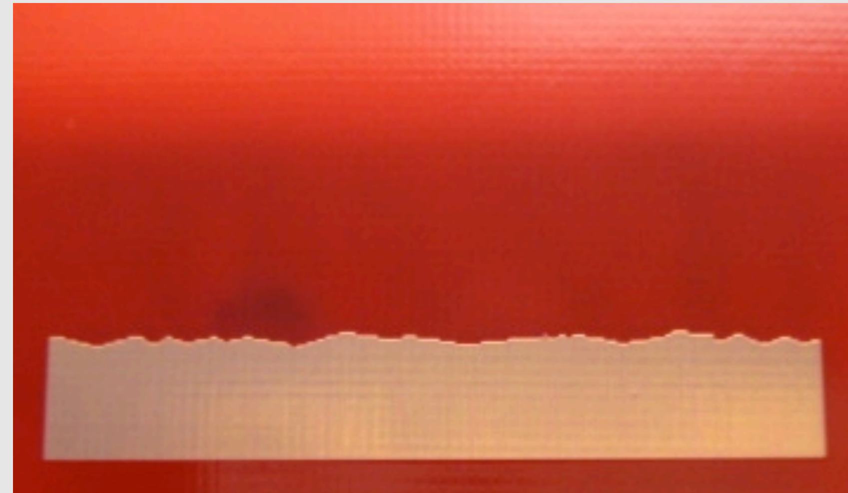
Laser: Full PCB Layer Ablation

- Moon Patrol image on PCBDT Reference Board
- Substrate removed w/ CO2 laser, leaving only copper features of each layer
- PCB layout data provided to operator in advance
  - Difficult to expose full layers of a "black box" PCB (unknown layout and/or composition)
- Small copper features delaminated due to heat from the rushed ablation process



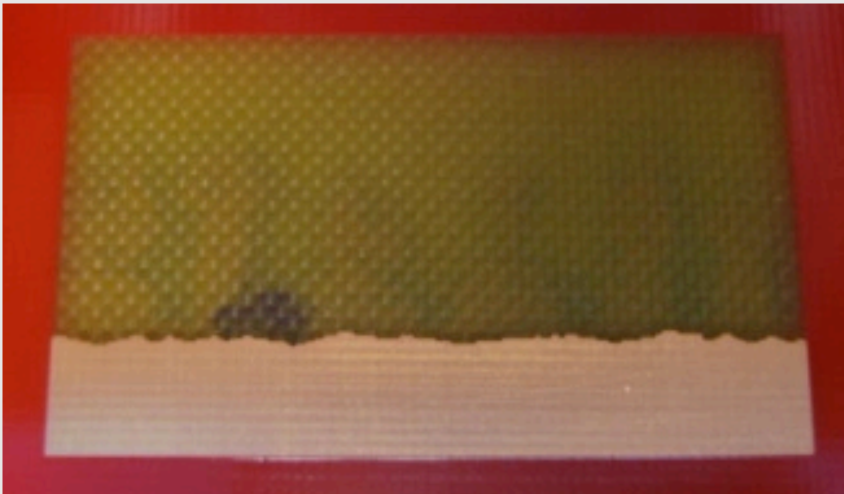
Laser: Full PCB Layer Ablation 2

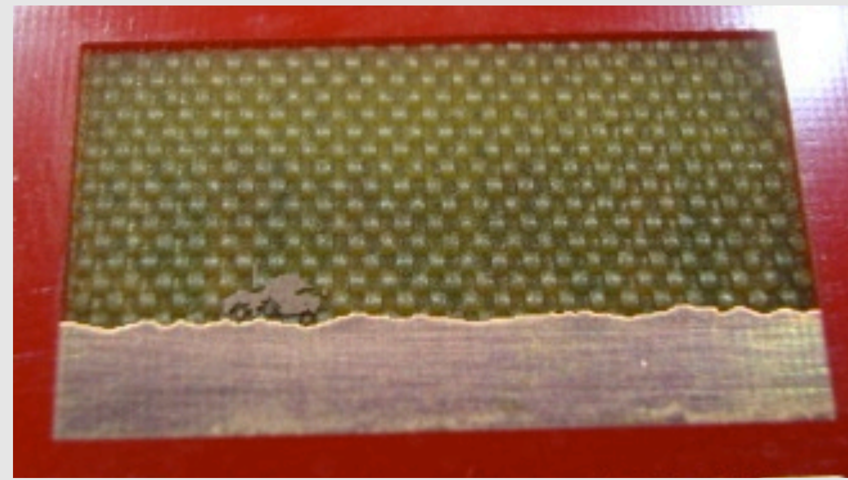
1



2

3





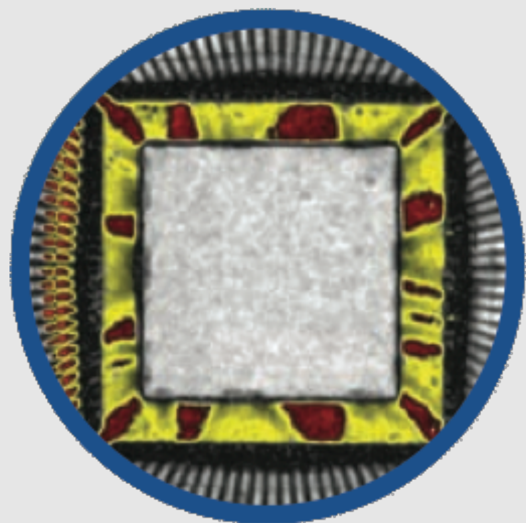
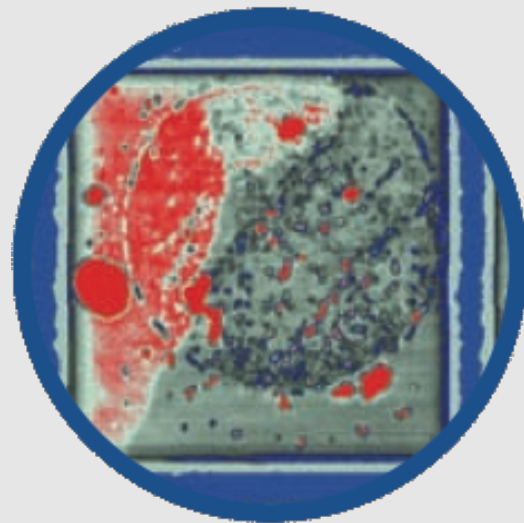
4

5

6

Acoustic Microscopy

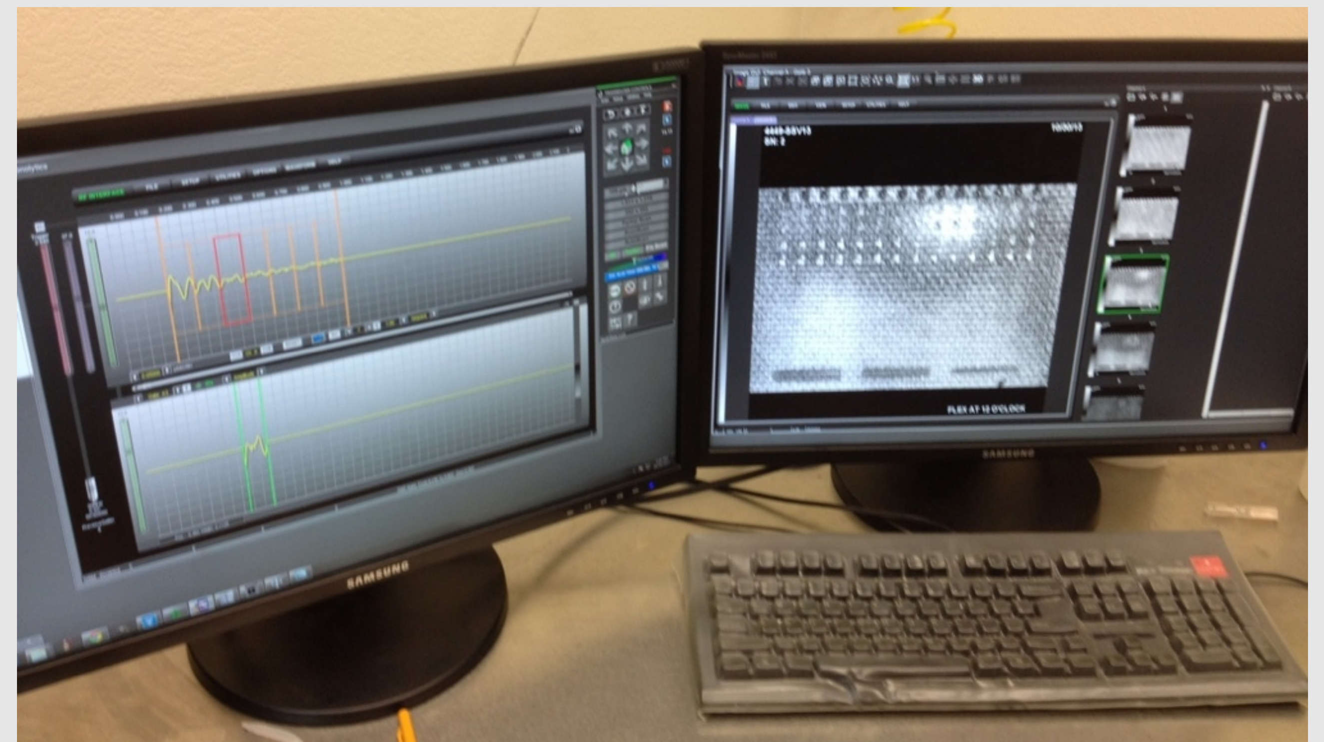
- Typically used for non-destructive failure analysis & reliability testing/verification of ICs, components, packaging, wafers
  - Can identify air gaps/voids, delamination, cracks/mechanical stress, counterfeits
- Ultrasound emitted into target (15-300MHz)
- Return echoes are captured (reflection)
- Transmission through the target is measured (thru scan)

www.sonoscan.com

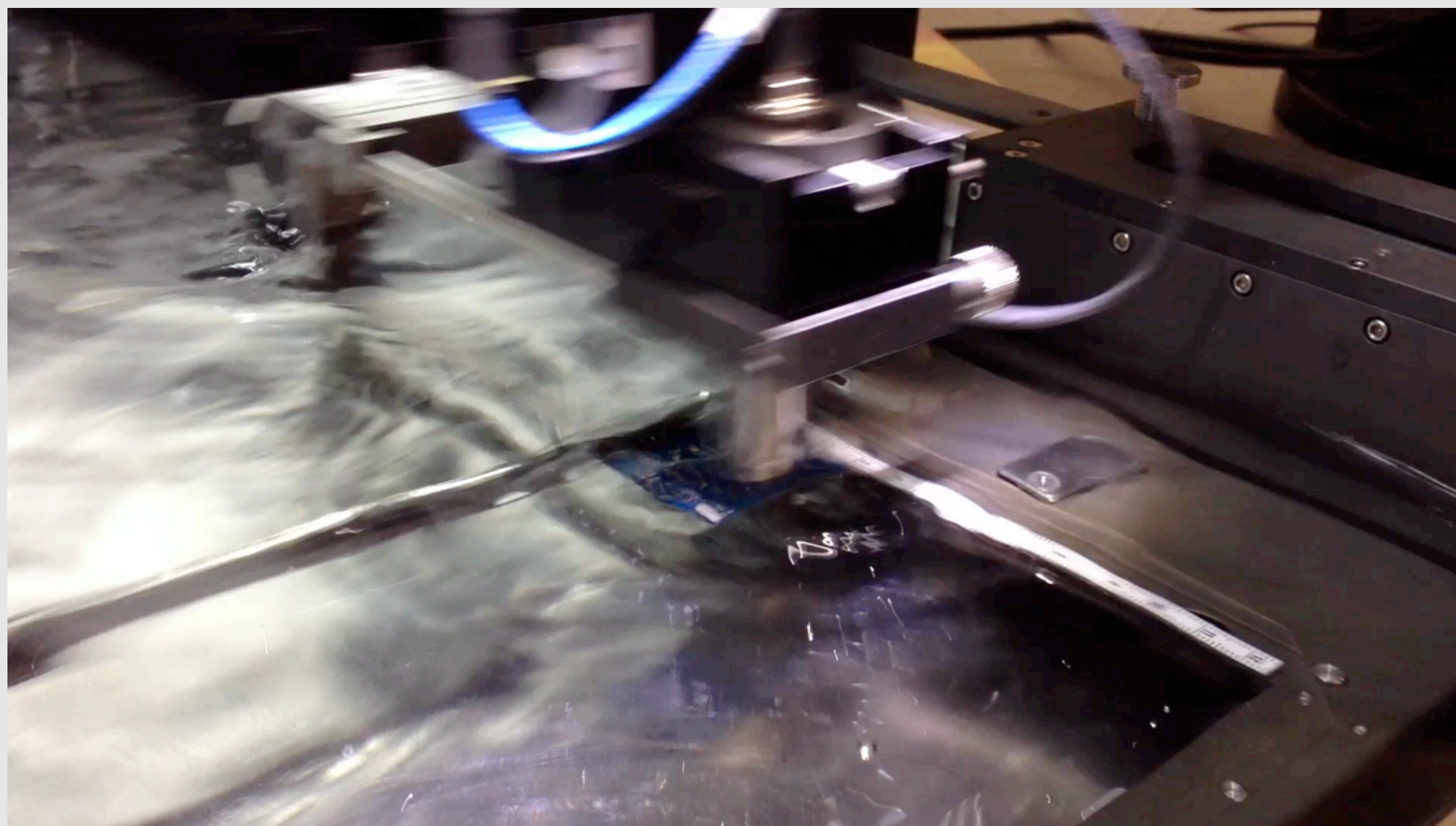
Acoustic Microscopy 2

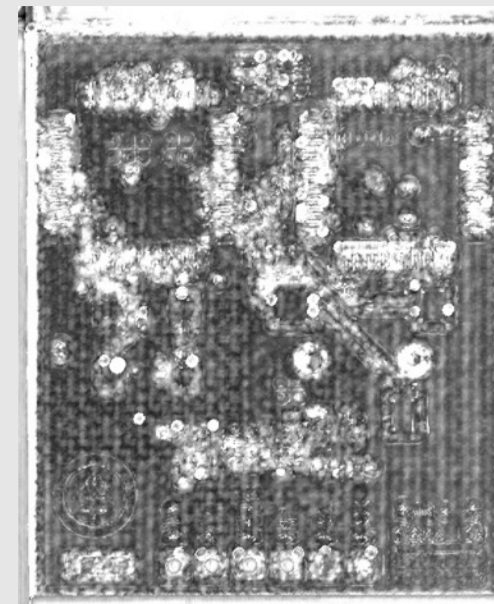
- SonoScan Gen6 C-Mode Scanning Acoustic Microscope @ SonoLab, Santa Clara, CA
- Target placed into bath of DI water or alcohol
  - Serves as liquid coupling medium to transfer sound waves to target

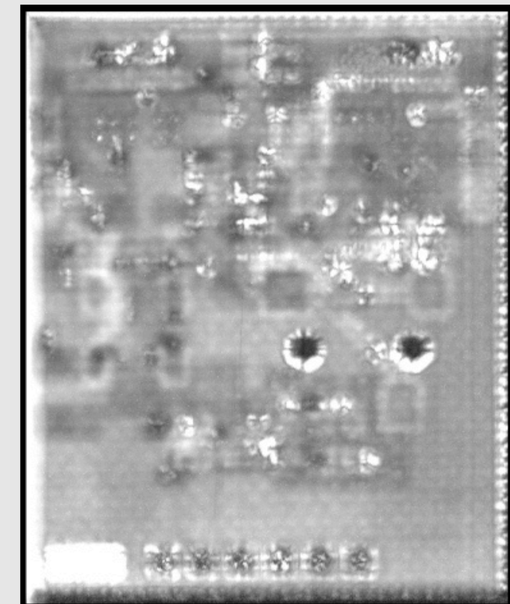


Acoustic Microscopy: Full PCB Layer Imaging

- Emic 2 Text-to-Speech Module
- Resulting inner layer images yielded no useful information
  - AMI works best on devices containing one or two thin interfaces
  - Multiple interfaces (e.g., layers of PCB) can cause undesirable refractions, difficult to identify signal from noise

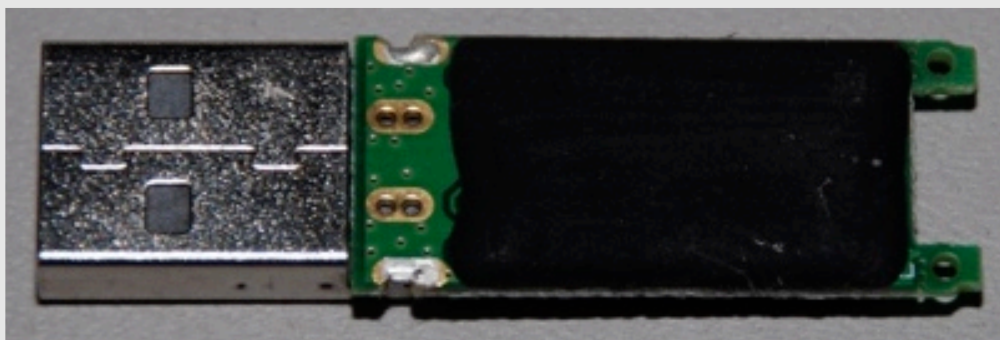


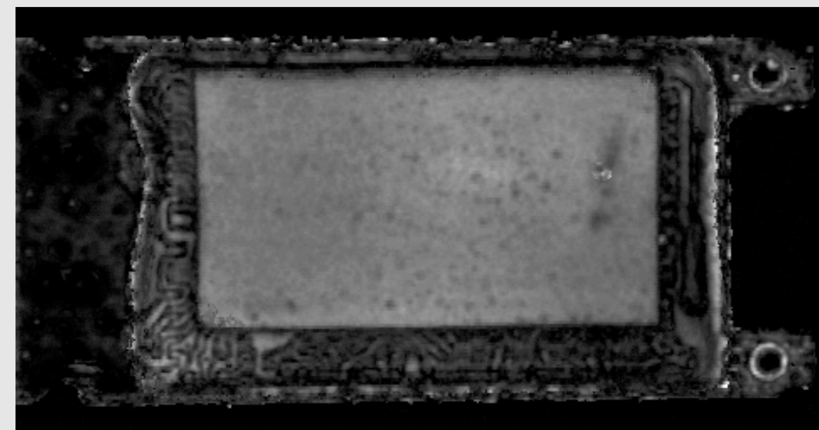


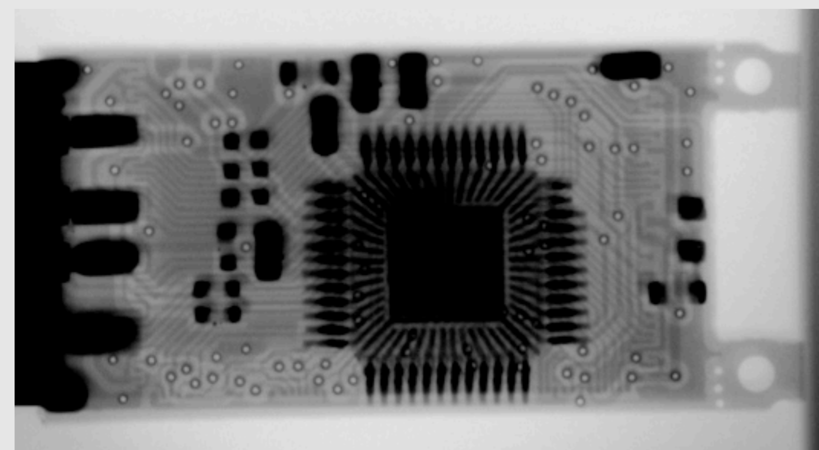


Acoustic Microscopy: Examining Epoxy Encapsulation

- Identify key components, connections, or locations
- Could also get clues about silicon die internal to package
- USB thumb drive w/ epoxy-potted bare die (memory)
  - X-ray (thru scan) doesn't detect glass/silicon die
  - Ultrasound reflects off of silicon, producing a result

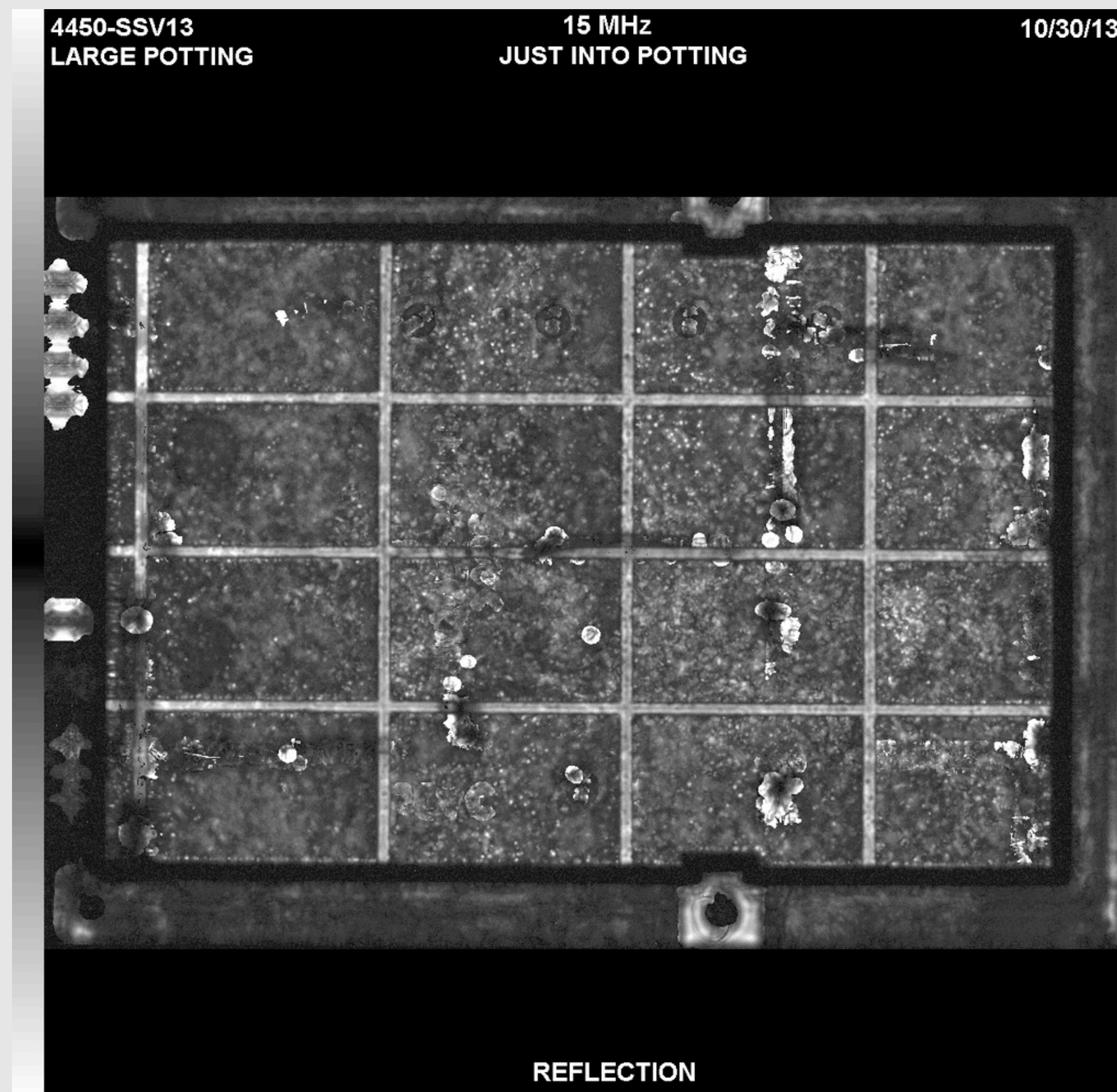






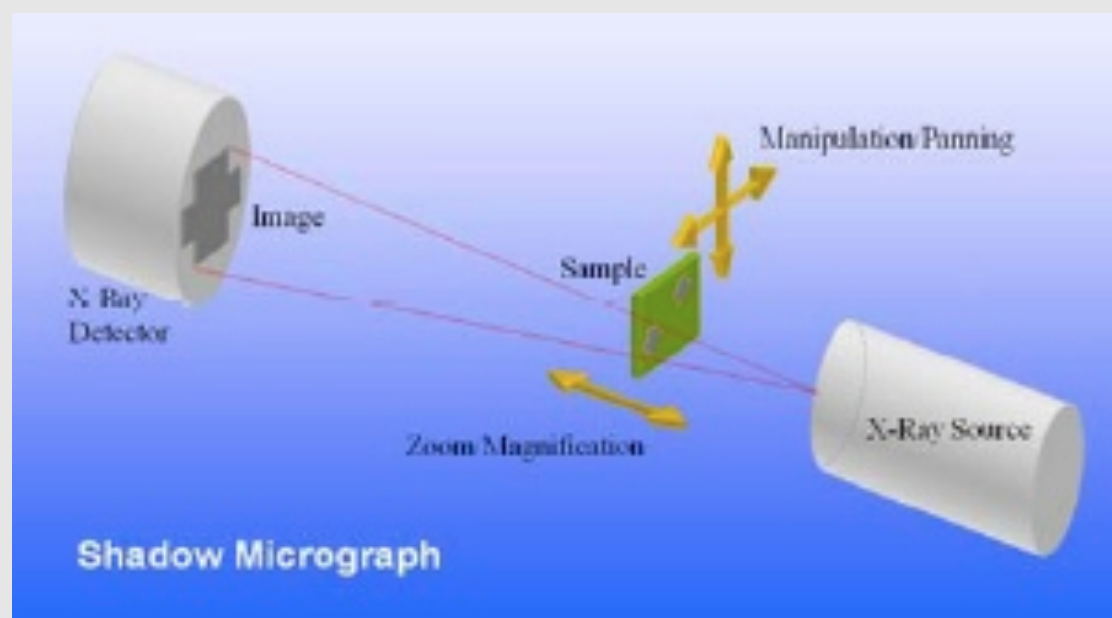
Acoustic Microscopy: Examining Epoxy Encapsulation 2

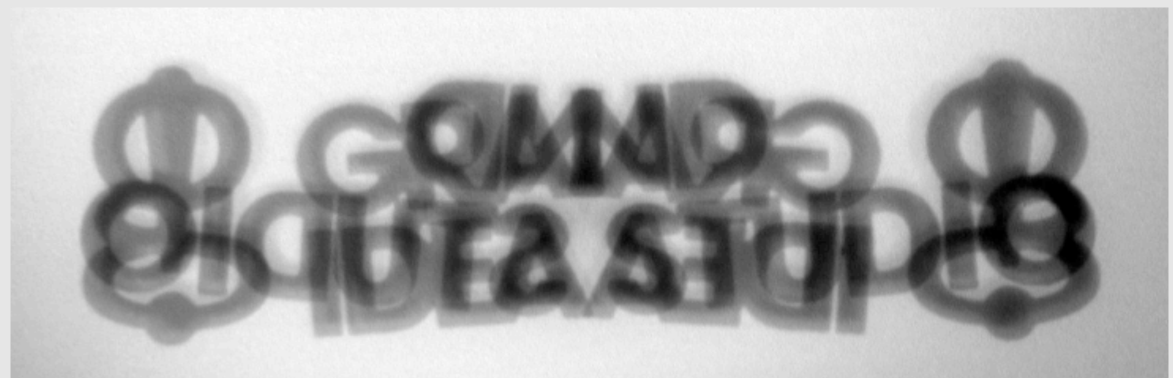
- Locate voids/gaps that may signify weakened areas



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





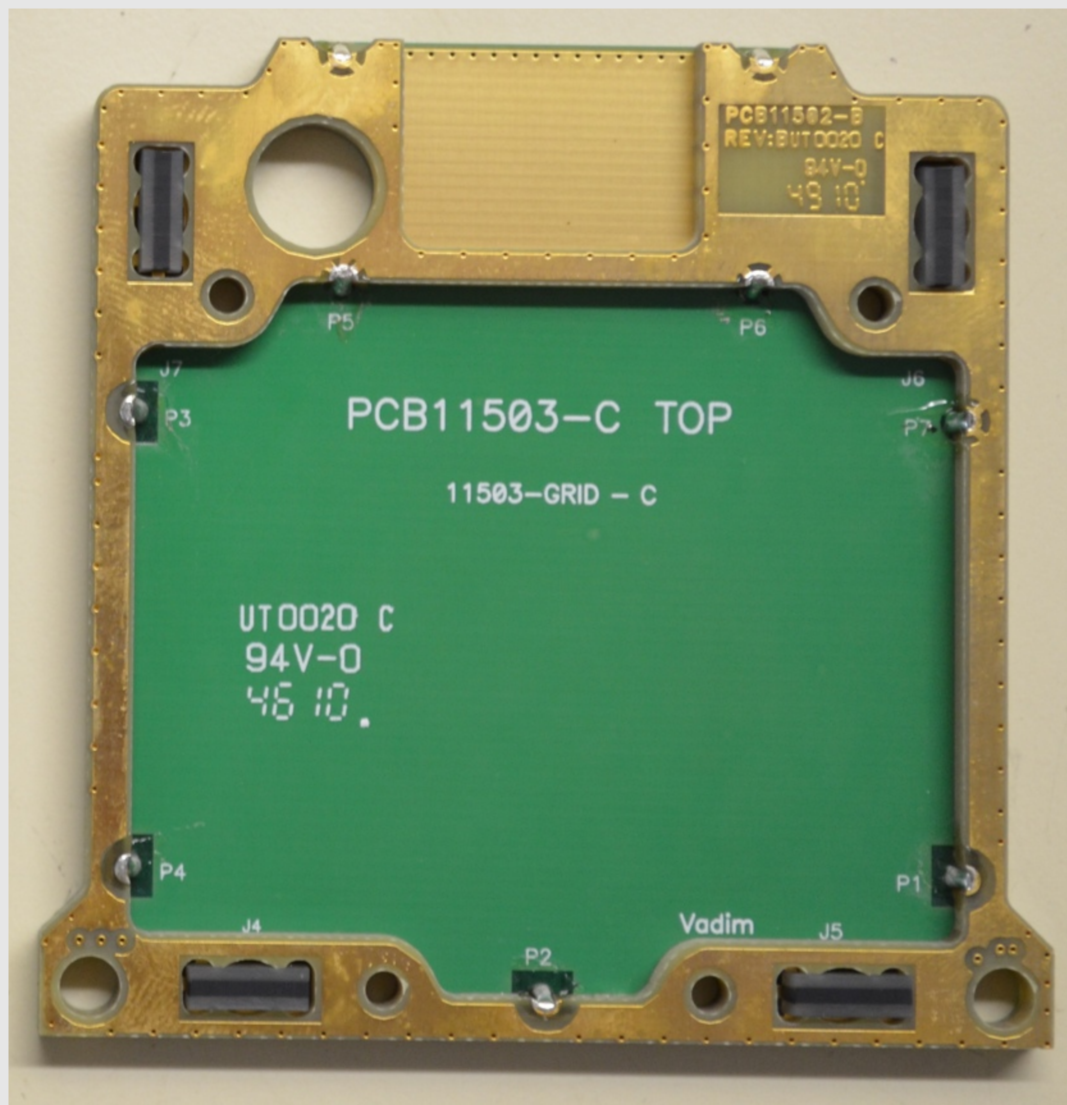
http://datest.com/resources-boardtestmeth-primer2d3d.php

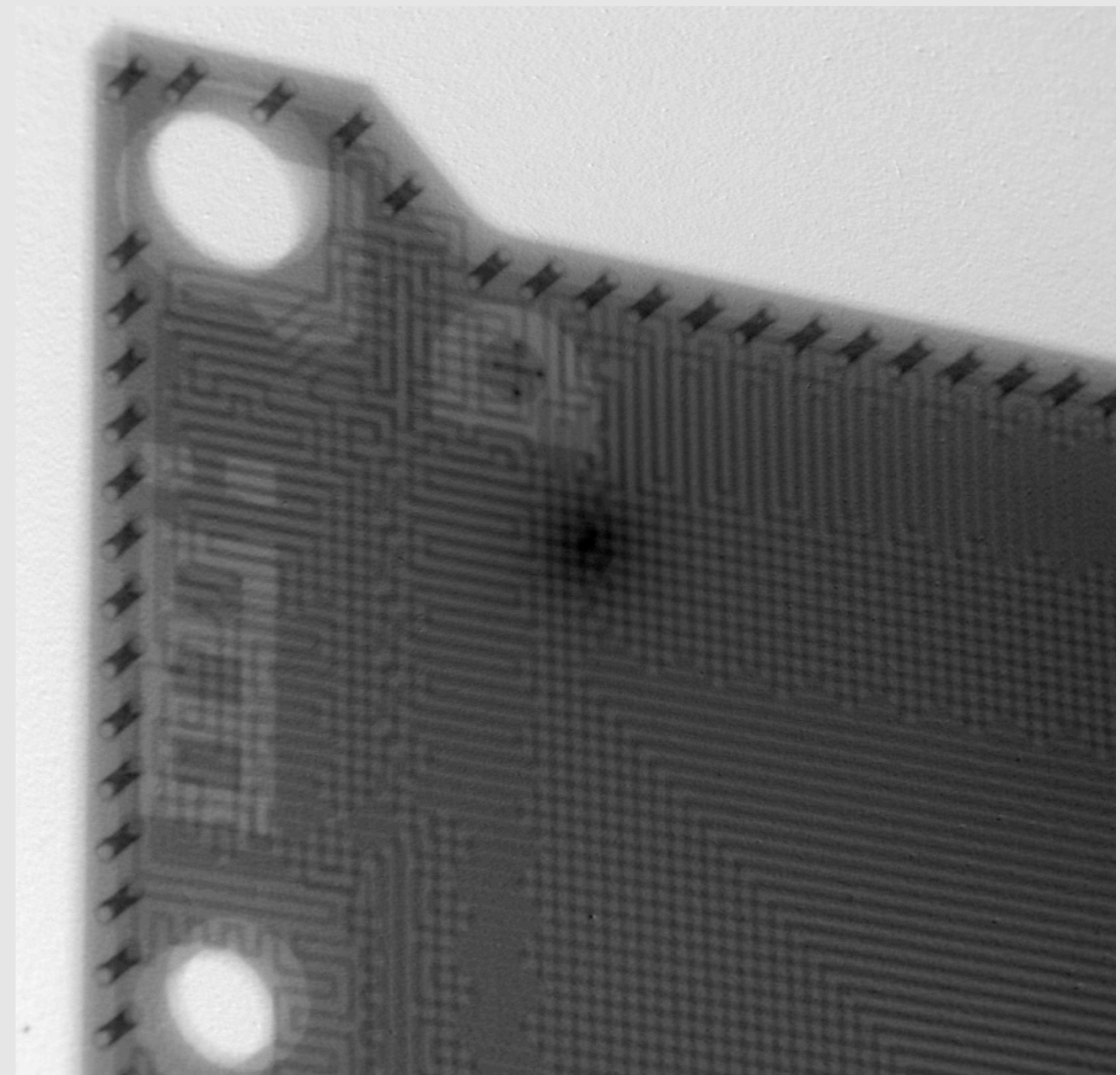
X-Ray (2D) 2

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

X-Ray (2D): General PCB Inspection

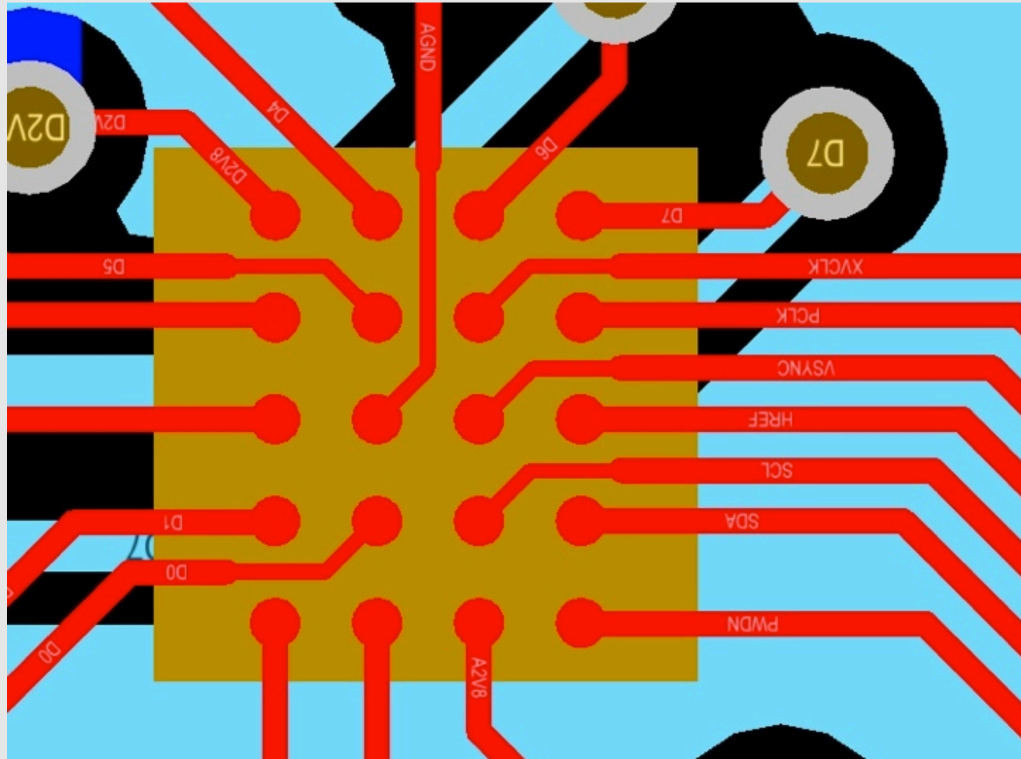
- Can get clues of PCB fabrication techniques, component location, layer count, hidden/embedded features
- VeriFone PINpad 1000SE active security envelope

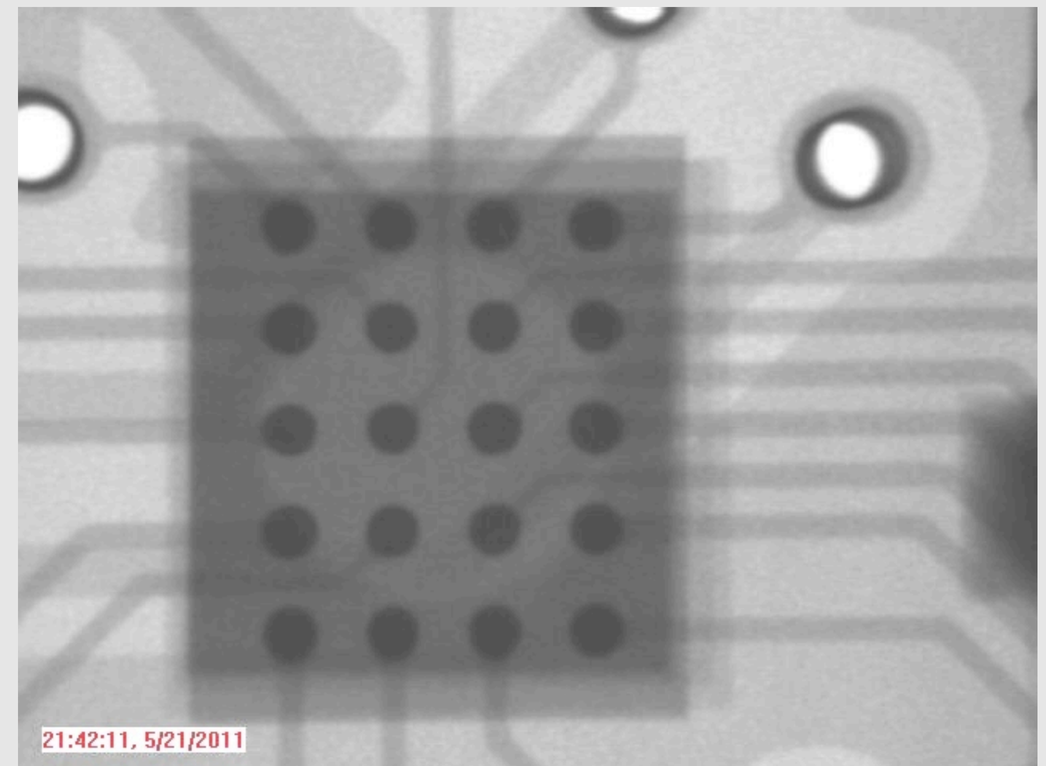




X-Ray (2D): General PCB Inspection 2

- 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

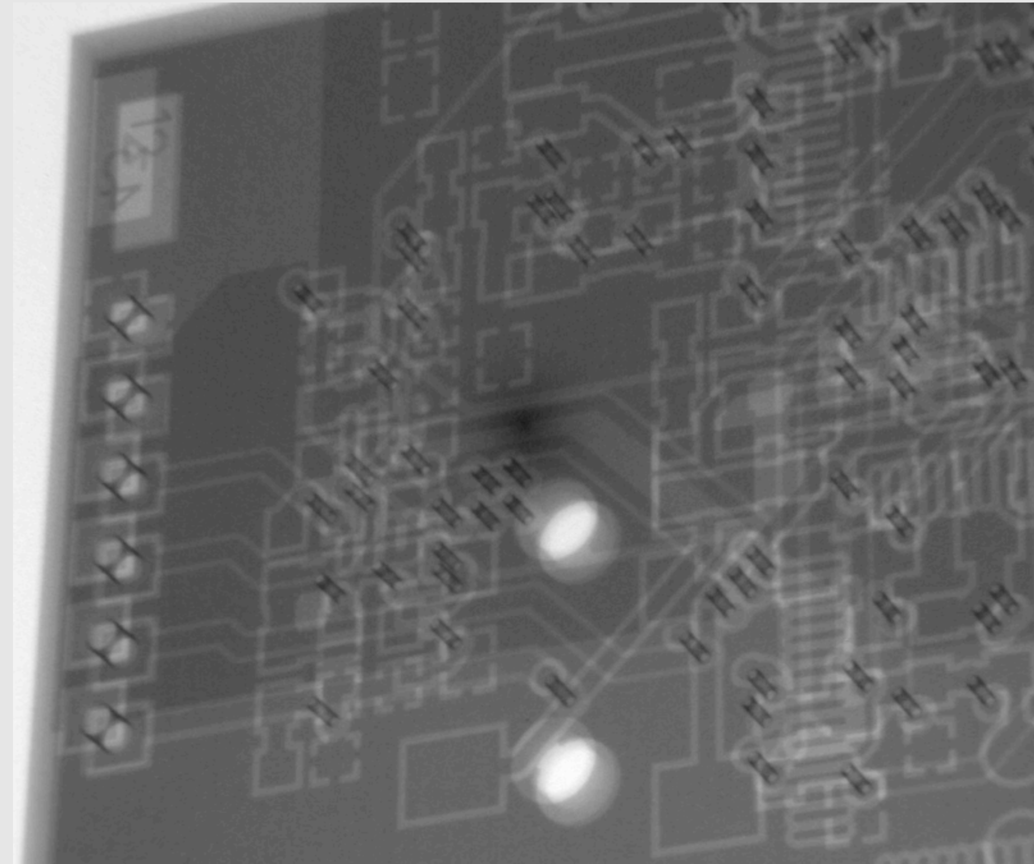




20-pin uBGA (CSP3)

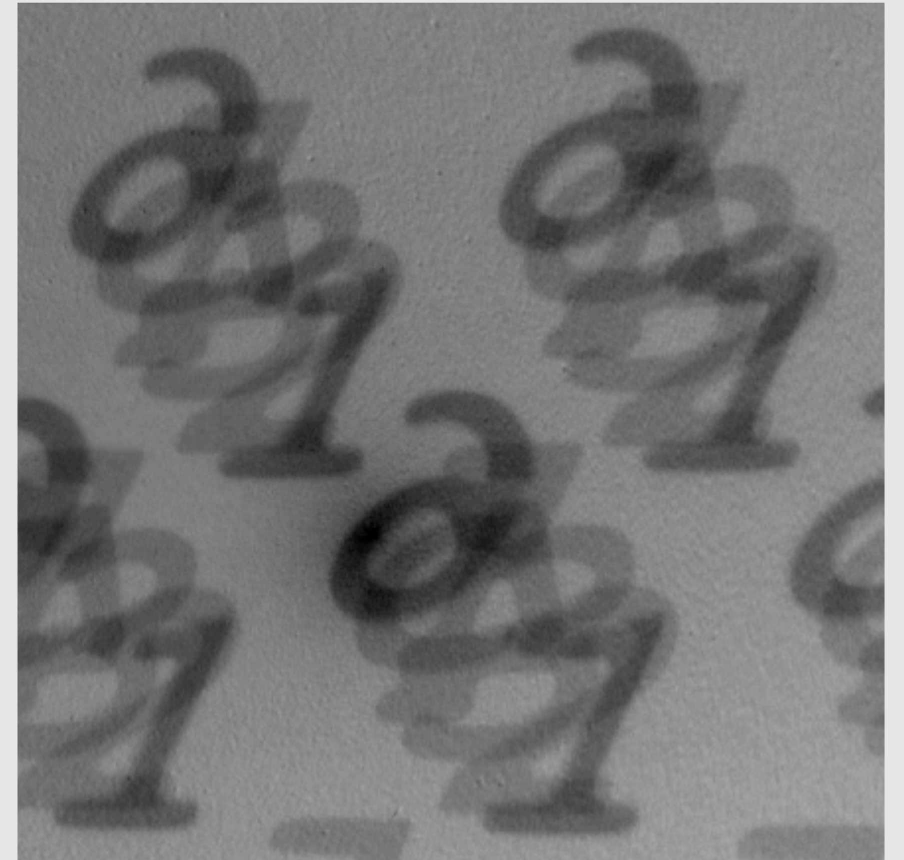
X-Ray (2D): General PCB Inspection 3

Emic 2 Text-to-Speech Module



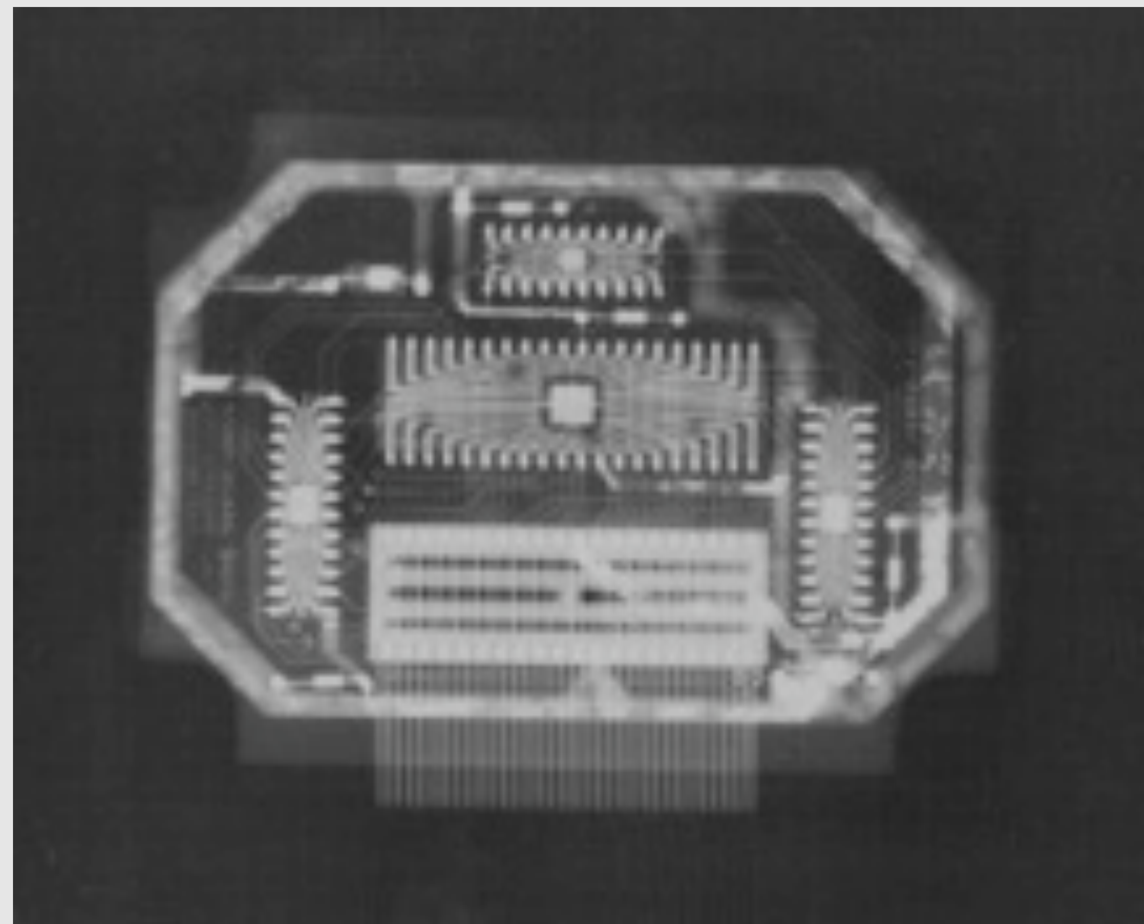
iPhone 4 16GB Assembled

X-Ray (2D): General PCB Inspection 4



X-Ray (2D): Examining Epoxy Encapsulation

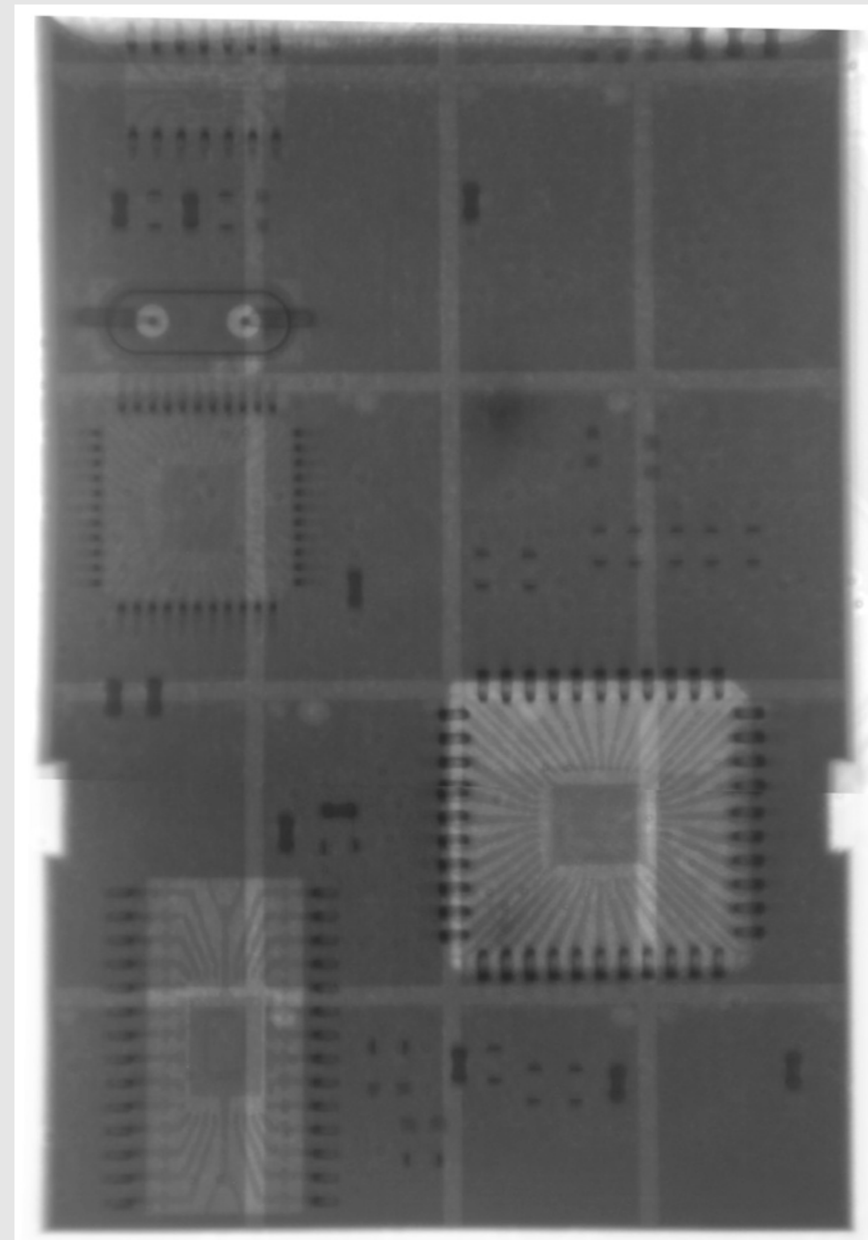
- Can help identify key components, connections, or locations
- Bally/Midway Pac Man Plus conversion module (1982)



How to crack a Pacman Plus!, www.multigame.com/pacplus.html

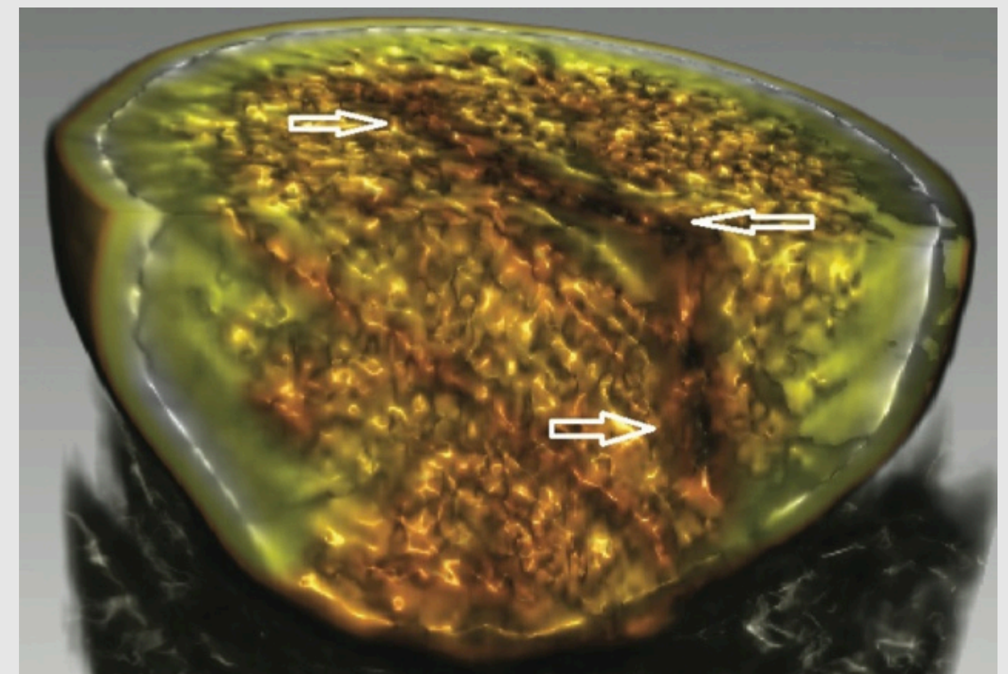
X-Ray (2D): Examining Epoxy Encapsulation 2

- Can help identify key components, connections, or locations
- LinkPoint BankPoint II 8001



X-Ray (3D/CT)

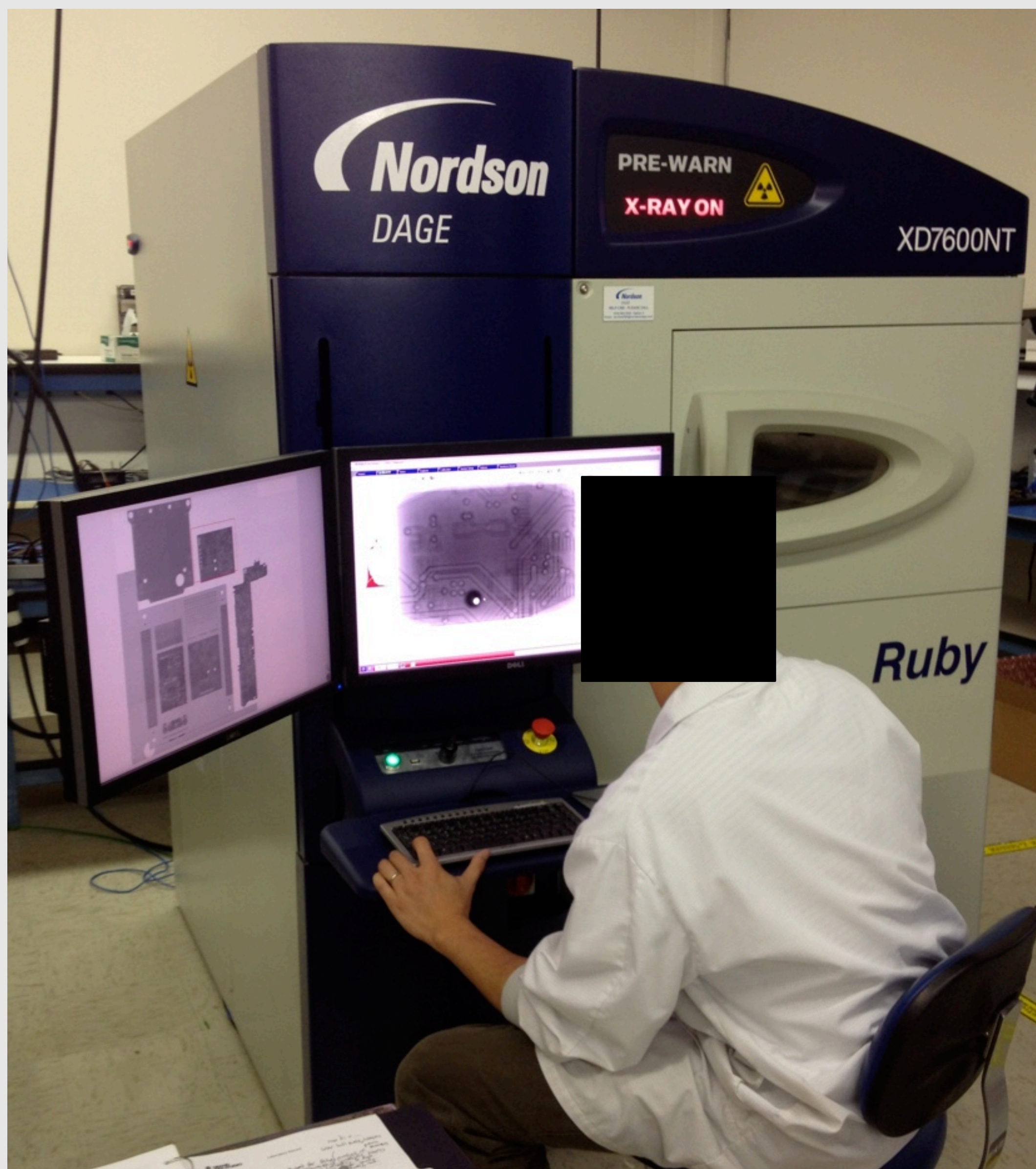
- Computed Tomography (CT)
  - A series of 2D X-ray images post-processed to create cross-sectional slices of the target
  - X-ray beam rotated 360° in a single axis around the target
- Typically used for complex inspection and failure analysis of PCBs, component packaging, solder ball/joint quality
- 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

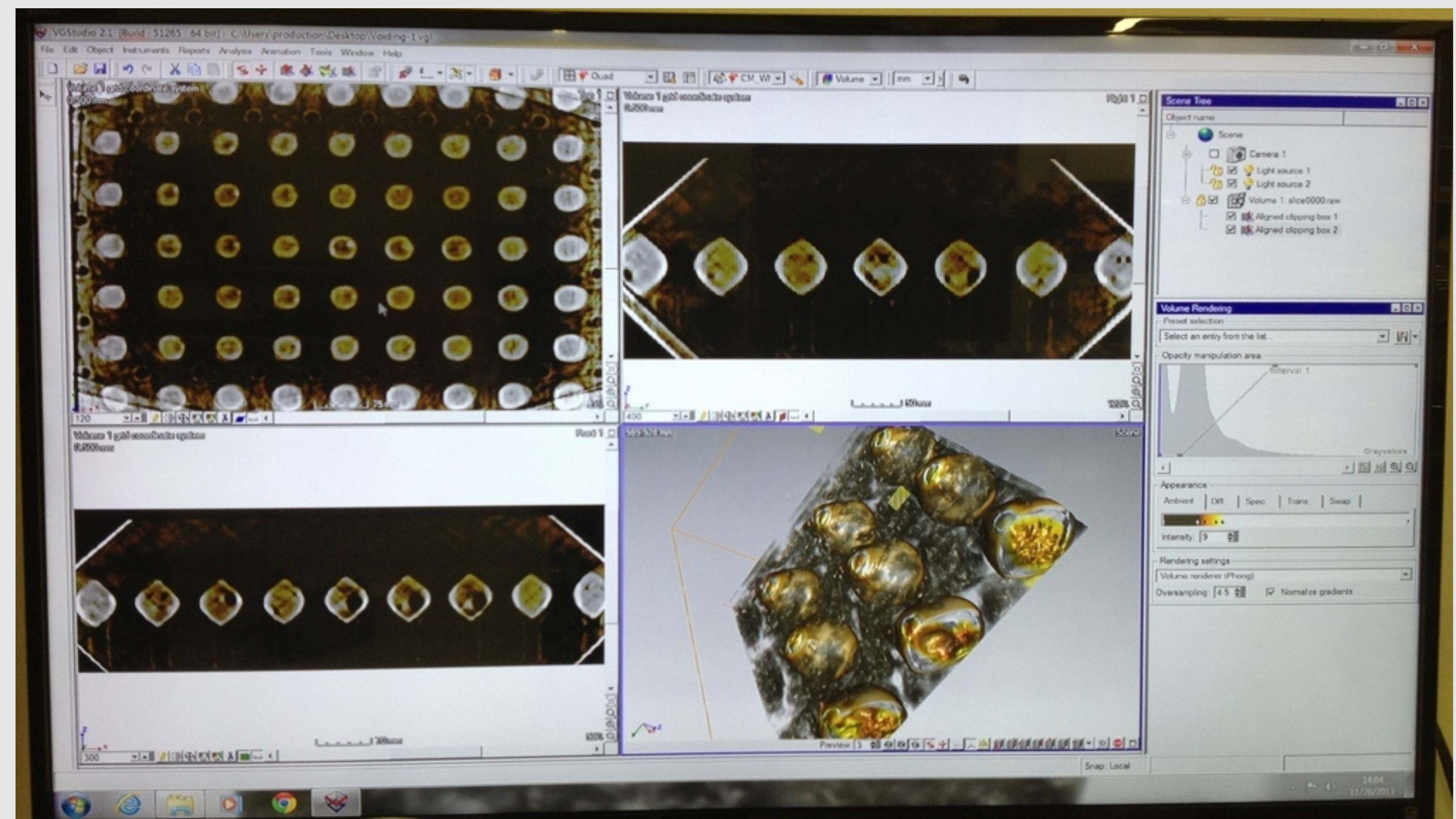


http://datest.com/resources-brochures.php

X-Ray (3D/CT) 2

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

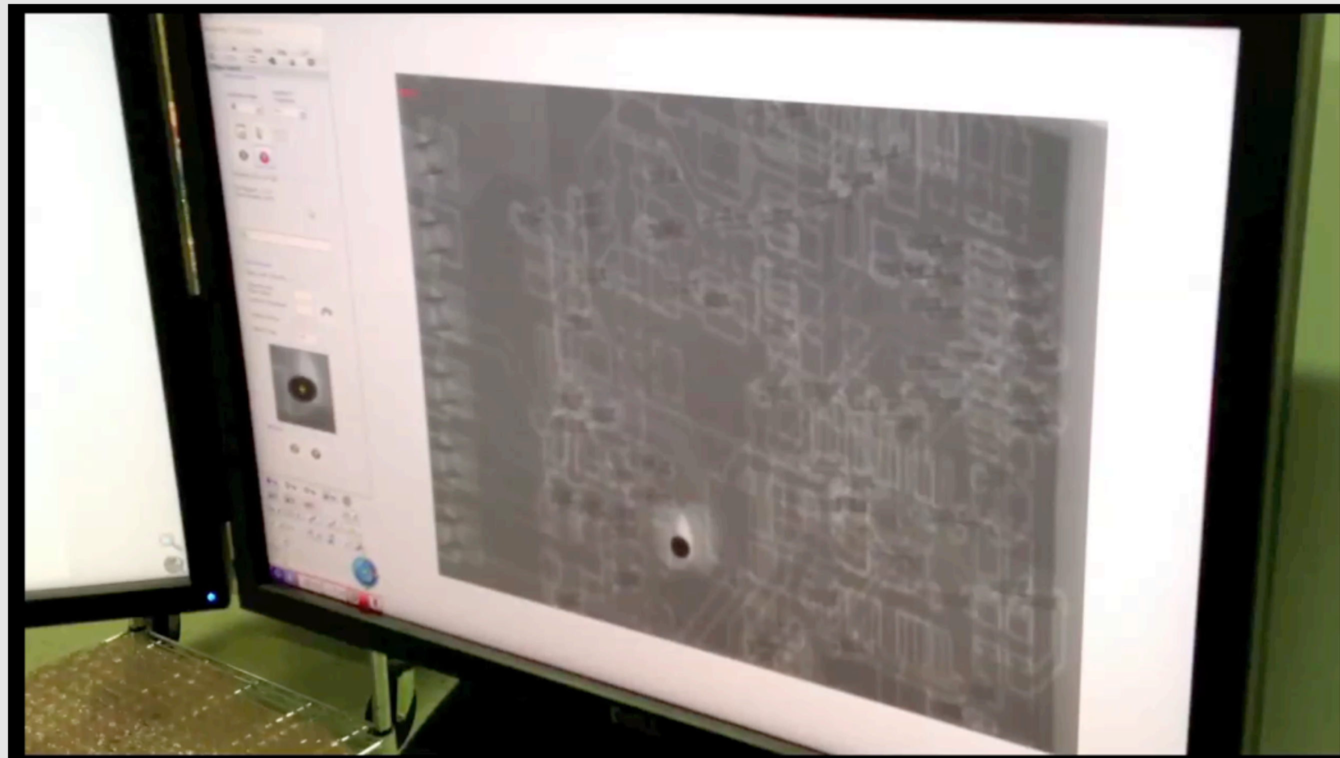




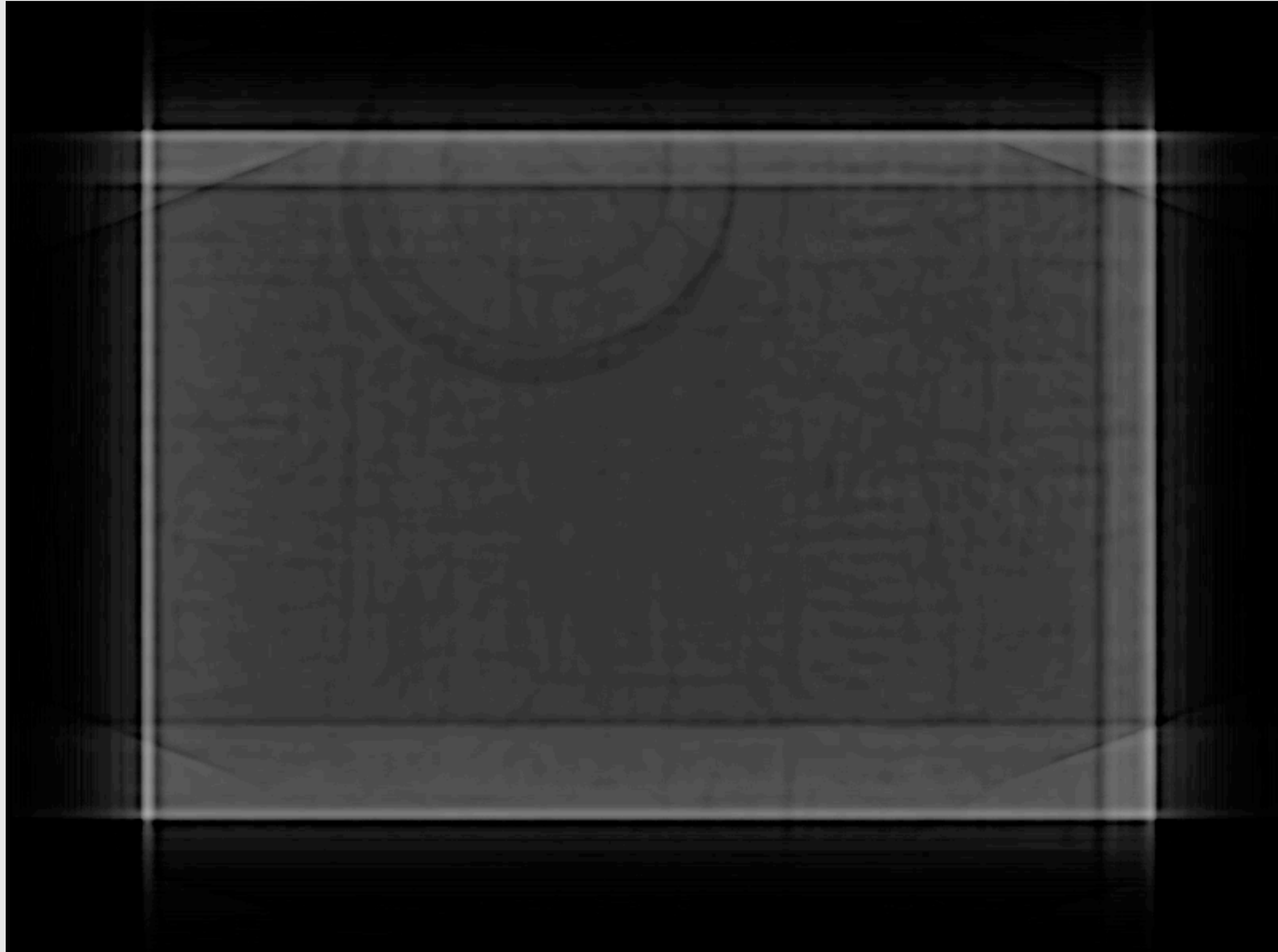
X-Ray (3D/CT): PCB Layer Extraction

- 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

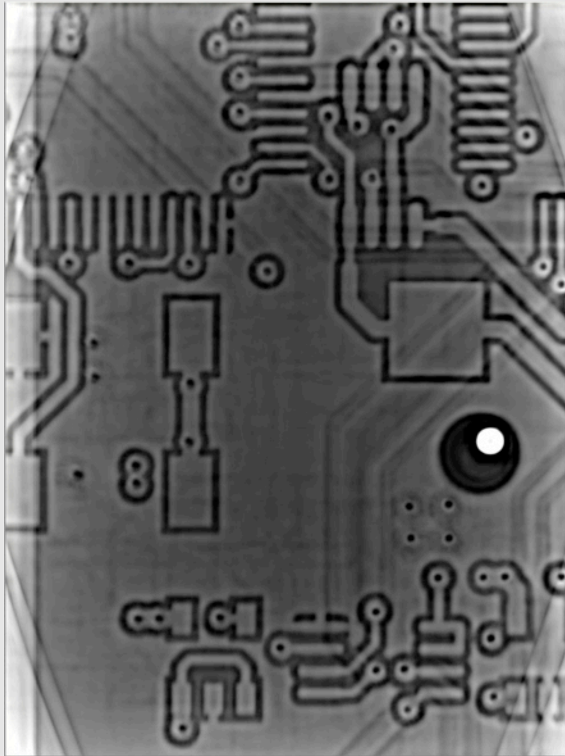
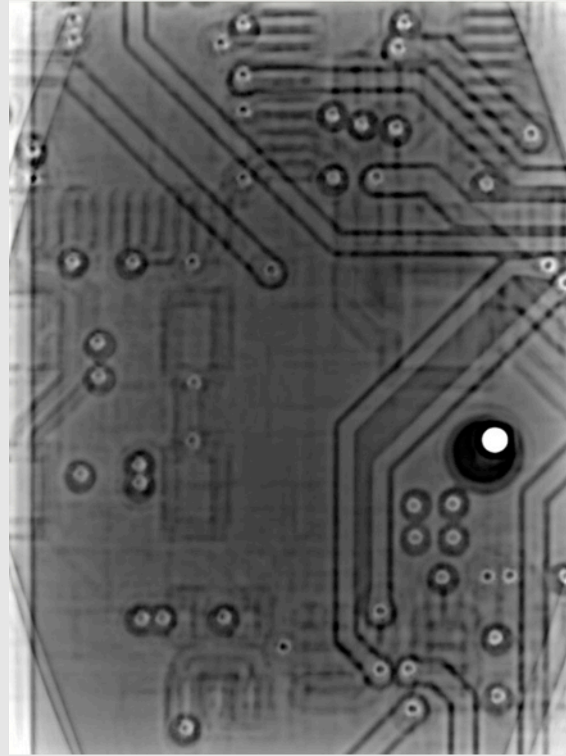
X-Ray (3D/CT): PCB Layer Extraction 2

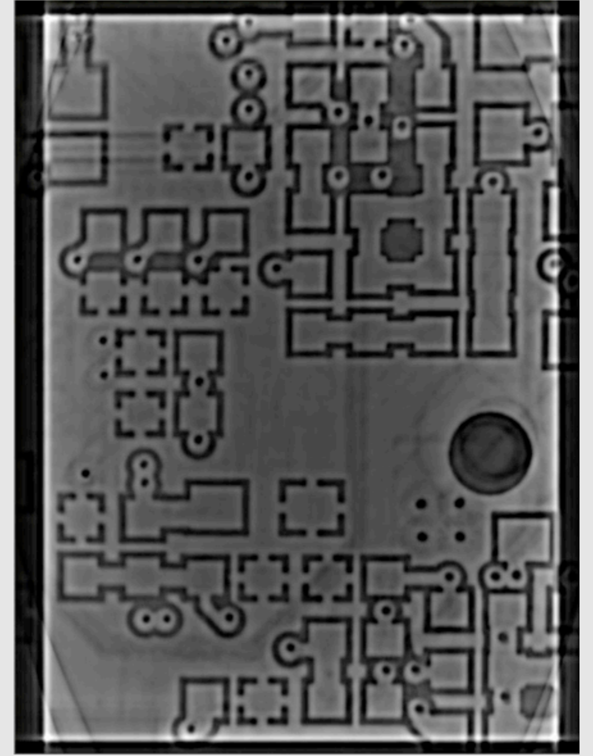
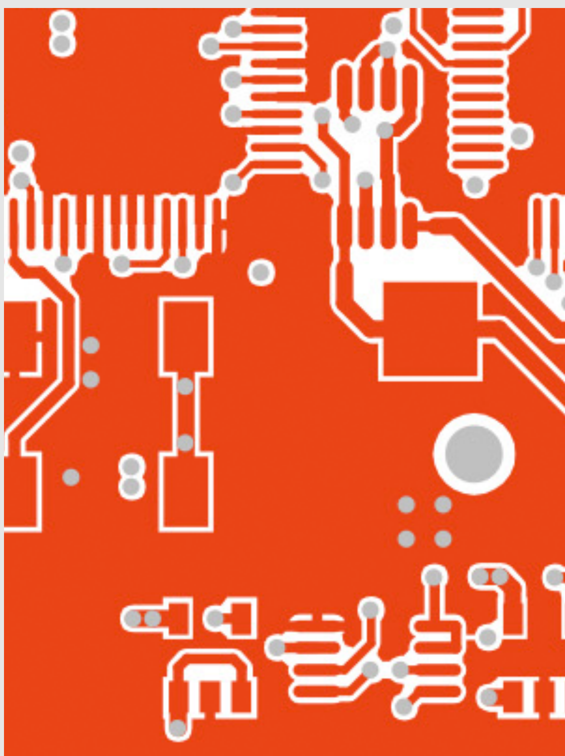
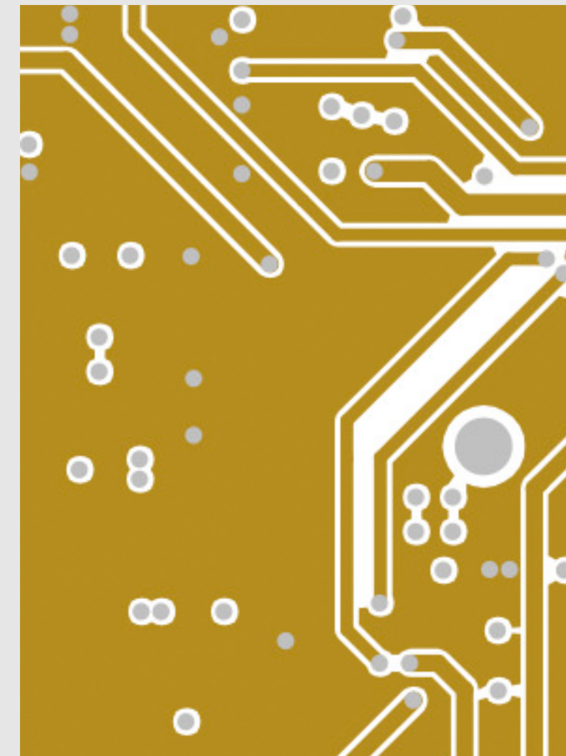
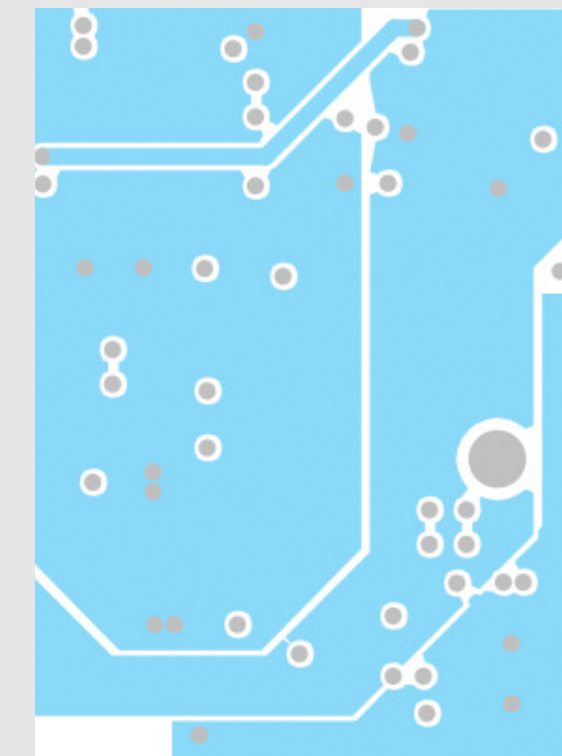
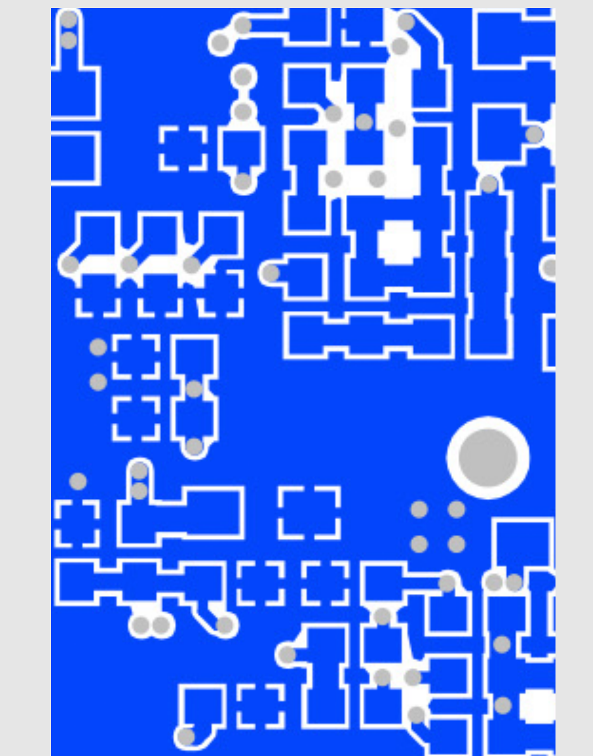


X-Ray (3D/CT): PCB Layer Extraction 3



X-Ray (3D/CT): PCB Layer Extraction 4

The End.