All Things Security

Bypass Touch ID

With a Forged Fingerprint

9am - noon

Ivy Thomas
@ivydigital

All Things Security

Agenda

9 am - 10:15	Bypass TouchID with a Forged Fingerprint Lecture & Demo
10:15 - 10:45	Break
10:45 - 12 pm	Bypass TouchID with a Forged Fingerprint Lab Exercises
12 - 1:30	Lunch
1:30 - 2:45	Locking down Mac OS. Lecture
2:45 - 3:15	Break
3:15 - 4:30	Physical Security & The Art of Lockpocking Lecture & Lab Exercise
5 pm	Dinner Evening Activities

Security Team

Pam Lefkowitz

@alwaysdns

Jennifer Unger

@quovadimus82

Ivy Thomas

@ivydigital

Shannon Barragan

@shan2104

Welcome!

- ★ Overview
- ★ Meet the Team
- ★ Today's Agenda
- ★ Lab Safety / Code of Conduct

Conduct and Safety

★ Warning: Activities covered in today's workshop are for educational purposes only and are not for use or re-production outside of the classroom

★ Lab methods include heating processes and use of chemicals

★ Laws regarding lock picks may vary per state http://toool.us/laws.html

★ Please maintain caution and awareness when participating in lab activities accordingly

Security. Right at your fingertip.

Touch ID

All Things Security

Bypass Touch ID

With a Forged Fingerprint

9am - noon

Ivy Thomas
@ivydigital

The Goals of the Forgery

★ Collect the fingerprint enrolled to Touch ID

★ Make a high accuracy 3D forgery of the fingerprint

★ Fool Touch ID into interpreting a live finger

The Tradecraft of Forgery

- ★ Forensics "Crime Scene Investigation" methodologies
- ★ Scanning and Digitizing
- ★ Photo retouching
- ★ DIY Printed Circuit Board (PCB) Etching
- ★ Materials analysis, conductivity assessment
- ★ Moulding skin-like material

Wild Fingerprints

Latent Fingerprint

- composed of trace deposits of fat and sweat
- is not visible to the naked eye

Patent Fingerprint

- is visible to the eye
- marked by a substance on the fingers

If I can get the fingerprint, then I can bypass Touch ID

Fingerprinting Methods

The "10-print"

- old ink and card methodology
- civilian, juvenile, and criminal fingerprints

LiveScan Fingerprint

- An ink-less, electronic means of processing fingerprints
- high resolution scans

If I can get the fingerprint, then I can bypass Touch ID

Let’s get some prints.

Find a Latent Print…

- On the glassware
- On iPhone Home Button

Fingerprint Repositories

- Civilian 10-print
- Criminal 10-print
- Child Identification

Digital Photography Archives (Facebook, Websites, etc)

- Public speakers who gesture
- Surveillance tapes

If I can get the fingerprint, then I can bypass Touch ID

Integrated Automated Fingerprint Identification System (AFIS)

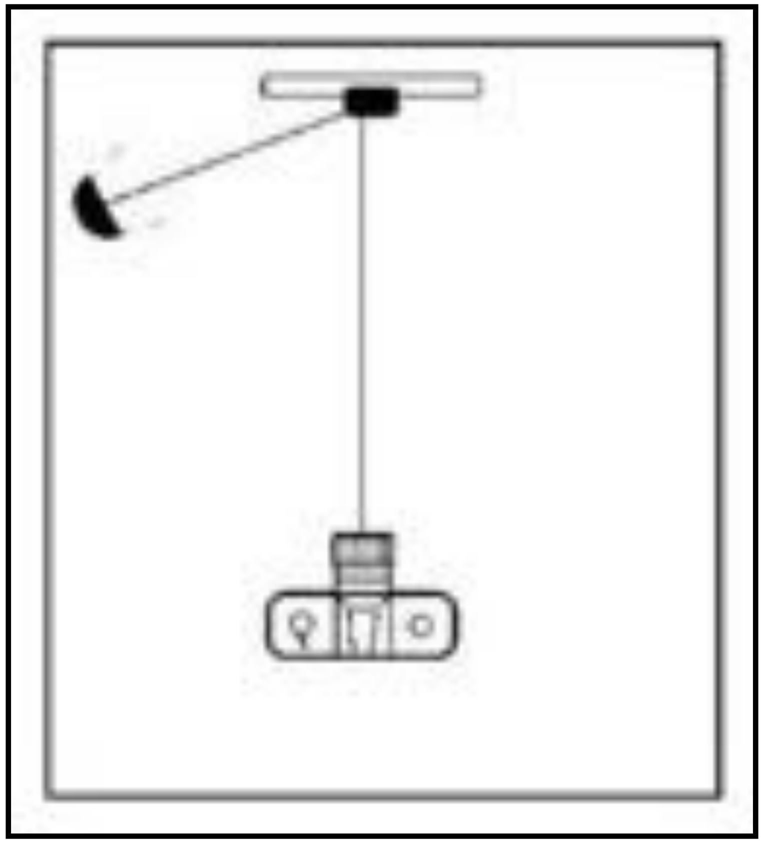
- 76 million criminal subjects
- 34 million civilian 10-prints
- e-exchange to +18,000 entities internationally
- 24 / 7 / 365 access
- no apparent retention policy

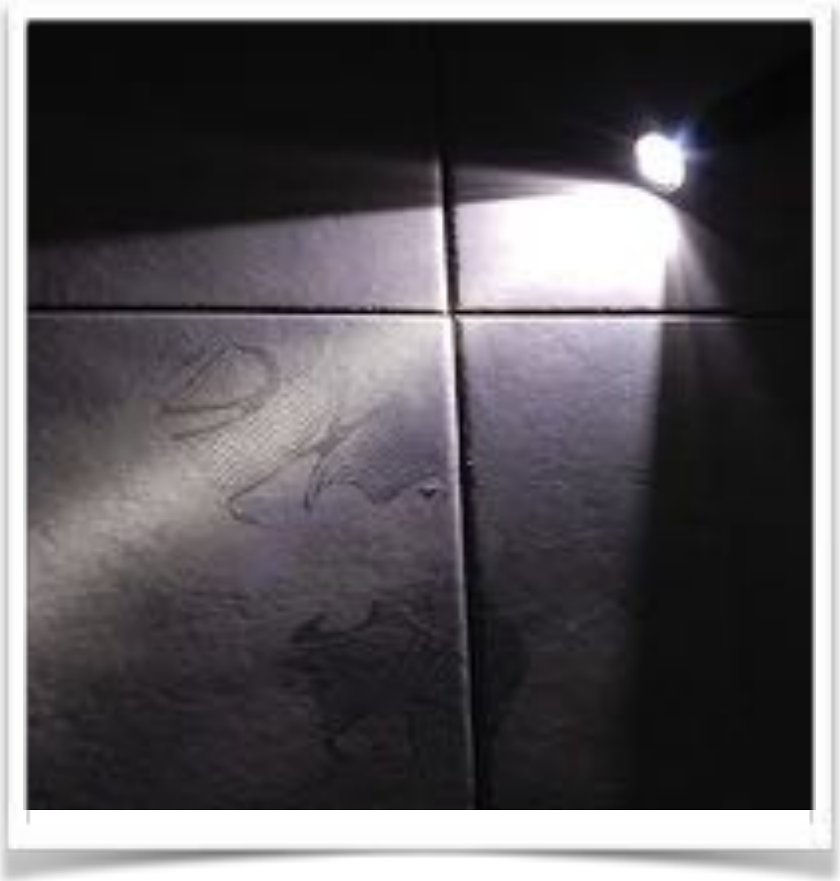
If I can get the fingerprint, then I can bypass Touch ID

The Nuance of Illusion

But latent fingerprints on the iPhone are invisible. Now what?

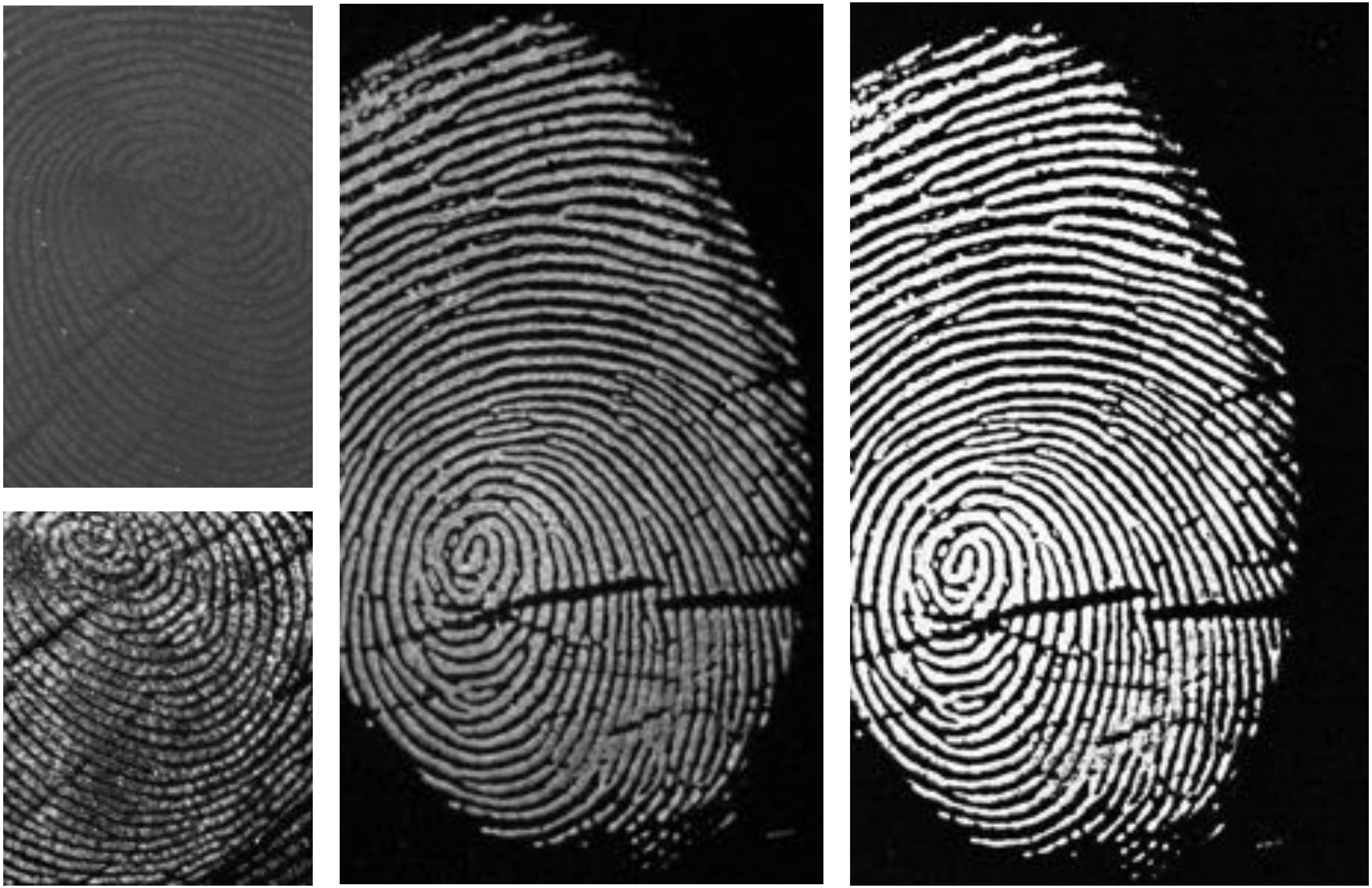
- Oblique lighting uses a light source positioned at a low angle
- Shows detail by creating shadows on the surface





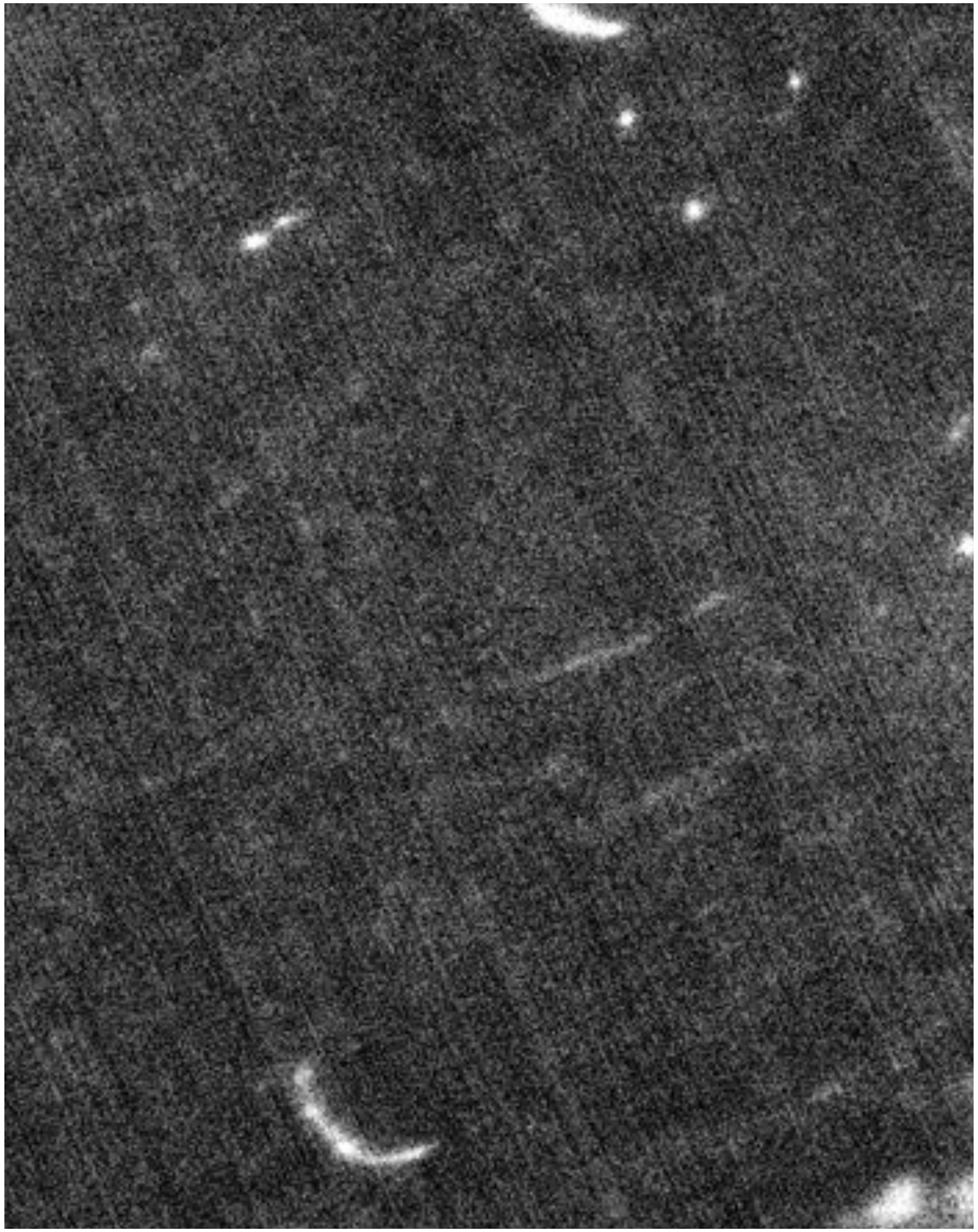
Between subtle shading and the absence of light…

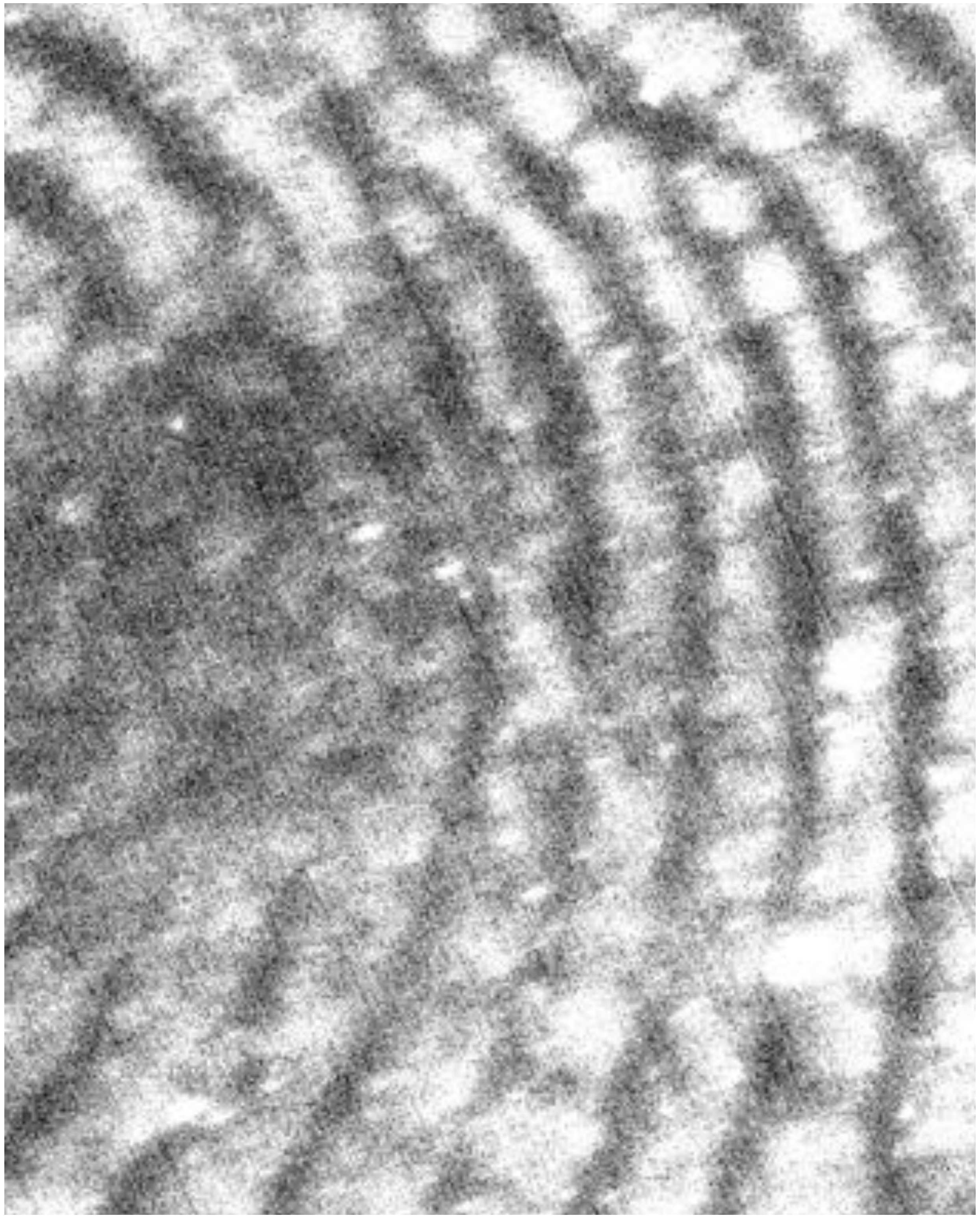
Digital Retouching



Between subtle shading and the absence of light…

Digital Retouching

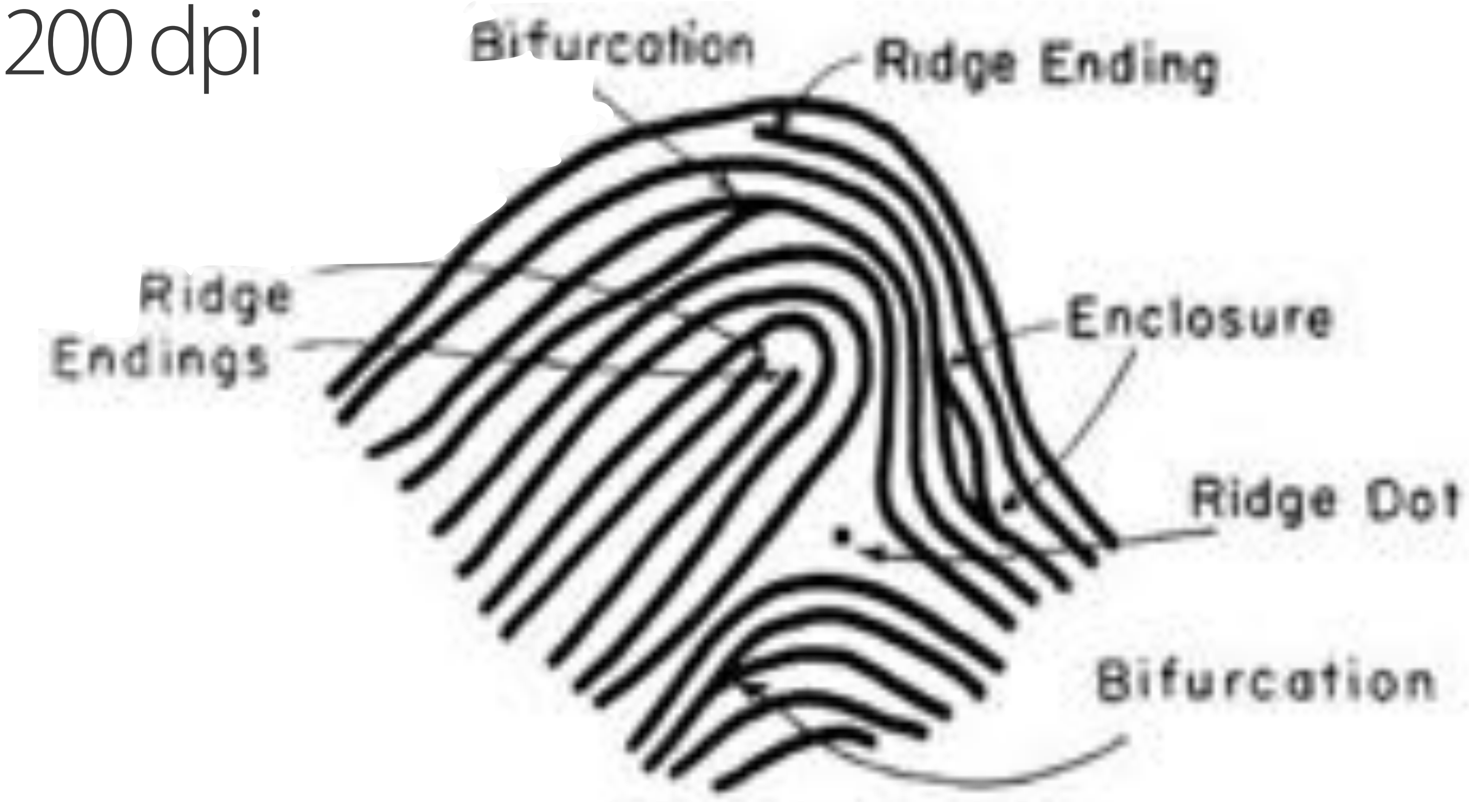




Between subtle shading and the absence of light…

Key Take-aways

- Ridges are white, furrows are black
- Don't destroy the minutiae
- Invert, then Mirror (Flip Horizontally)
- Scan 4800 dpi , Export 1200 dpi

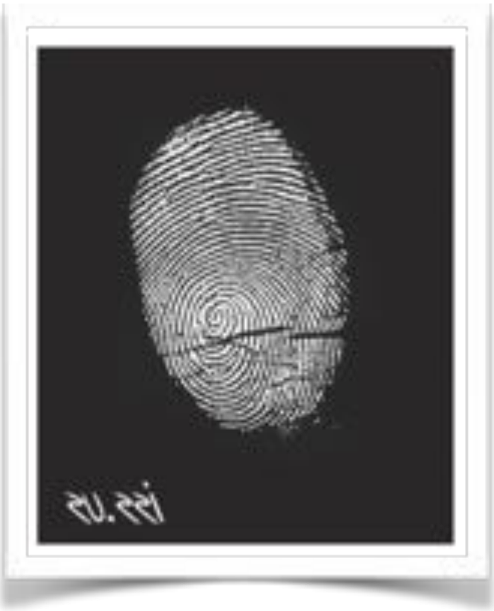


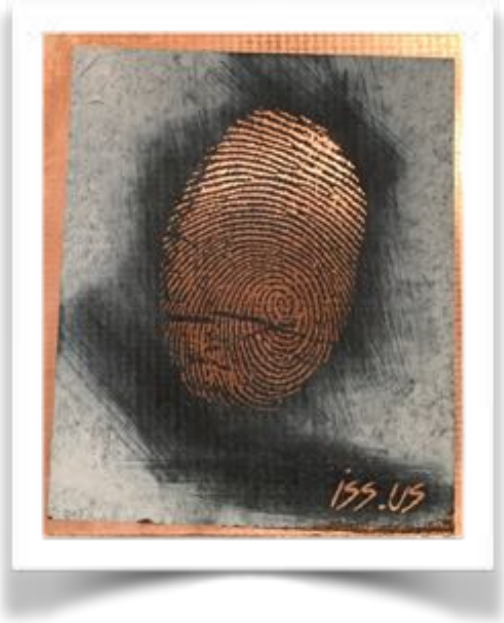
Between subtle shading and the absence of light…

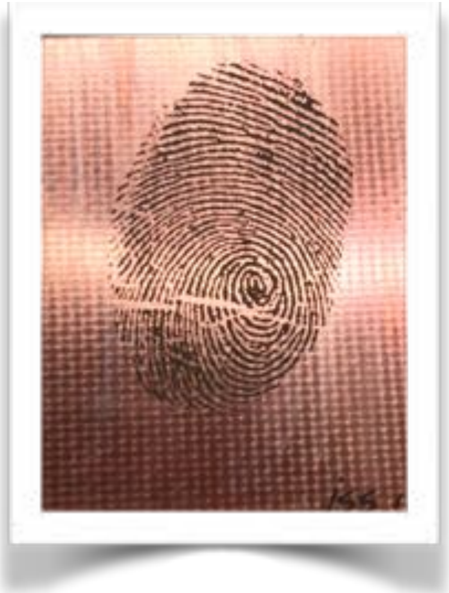
Building the 3D Mould

Challenge: Build a mould capable of producing a 3D replica of the finger pad complete with ridges identical in depth and pattern to the source fingerprint

Response: Dermal fingerprint ridges are 20-50 microns deep. The copper layer of a printed circuit board (PCB) is 34 microns thick, and can be custom etched using a chemical process.

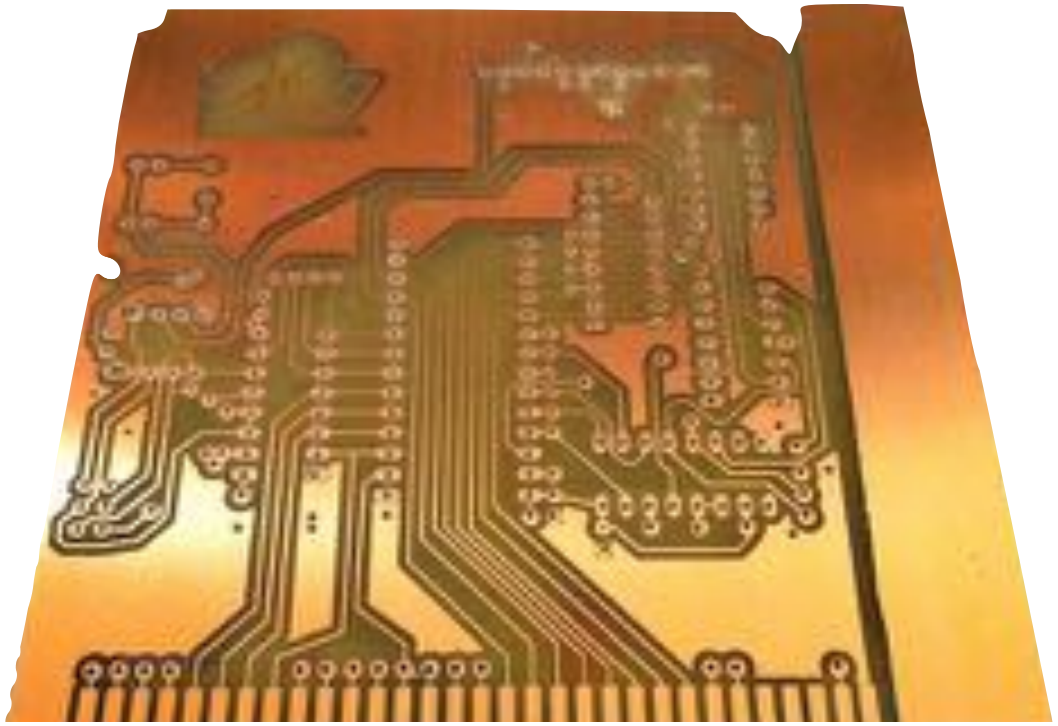






Printed Circuit Boards (PCB)

- Used by DIY computer enthusiasts to prototype unique circuit board designs
- Also great for forgery!



3 Stages:

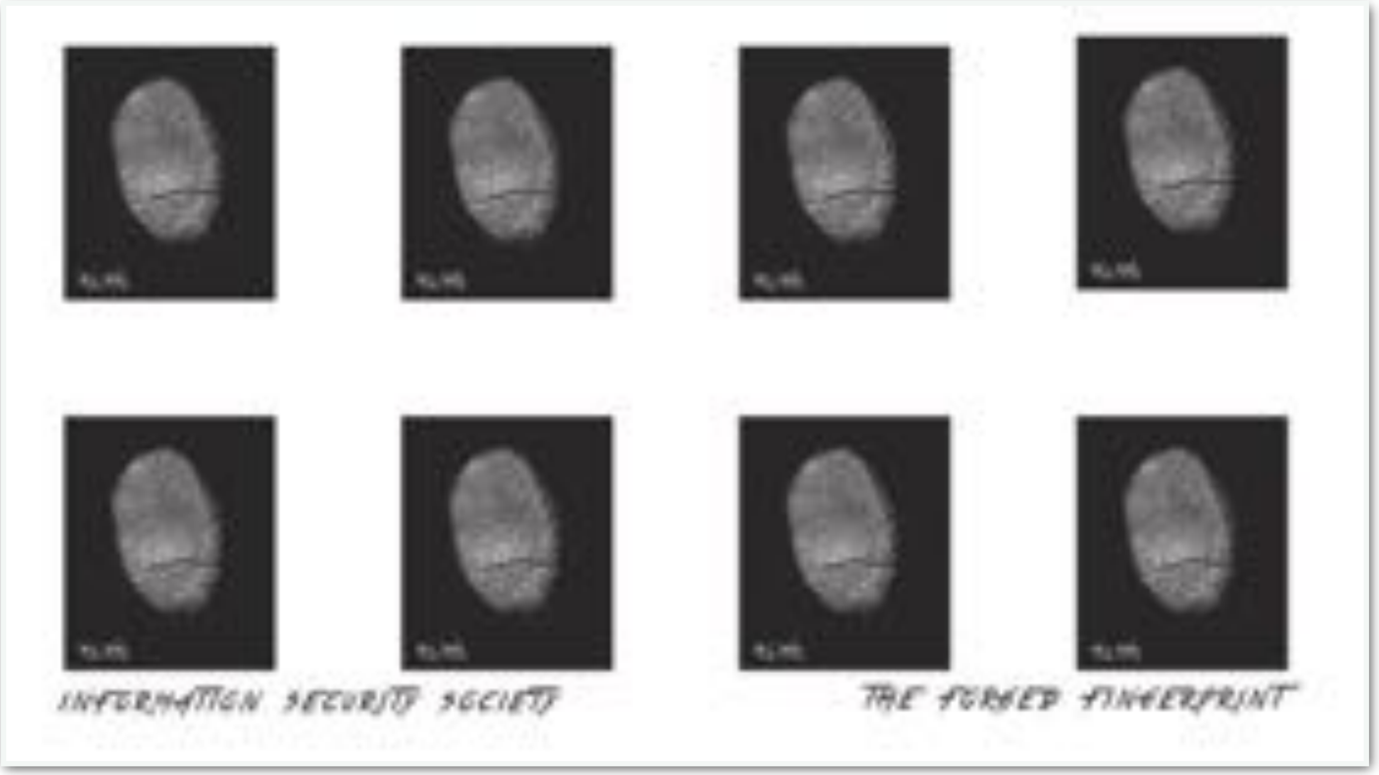
★ Ink Mask

★ Toner Transfer Method

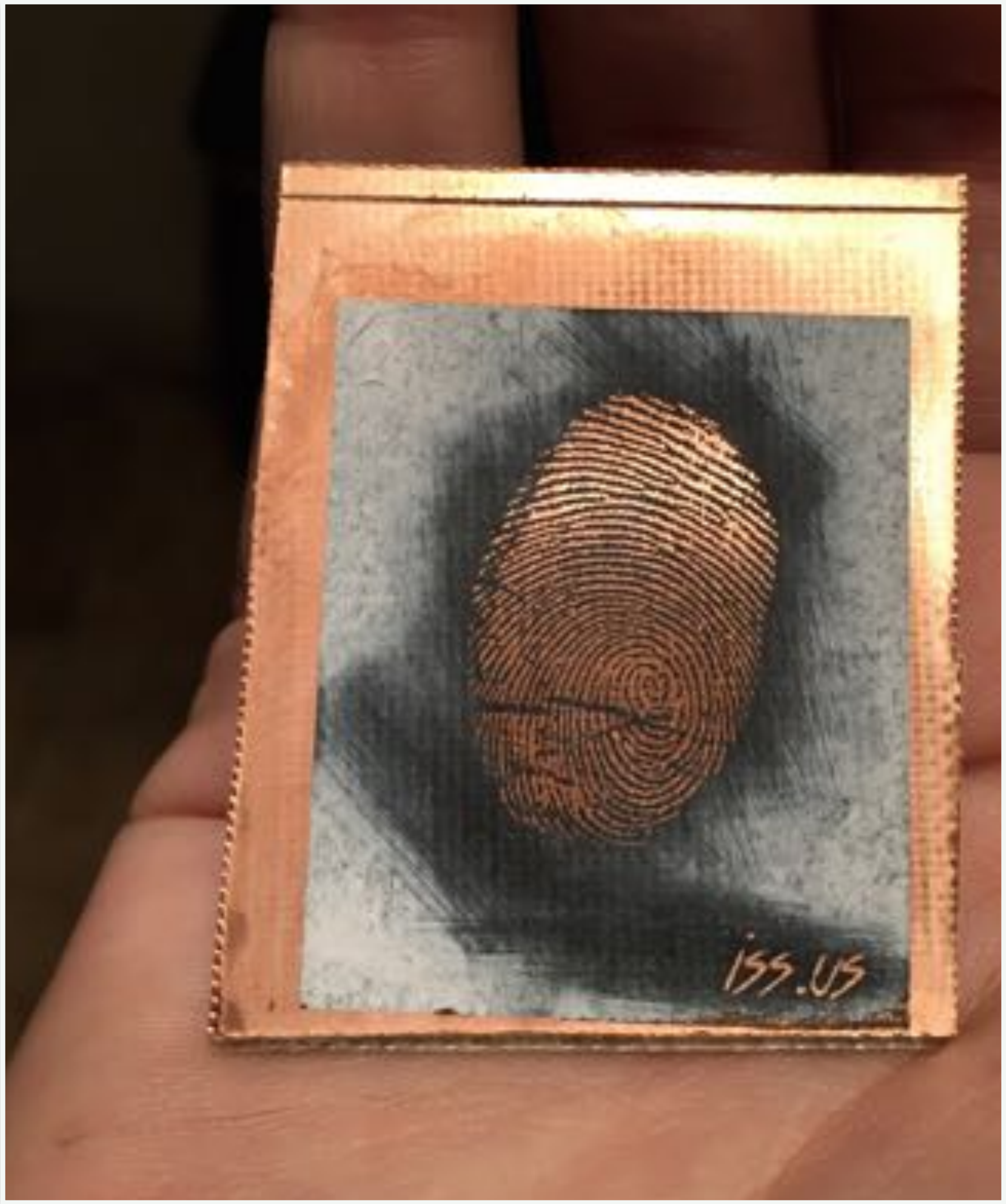
★ Chemical Etching

The Ink Mask

- A laser printed template of the PCB design
- Printed onto "HP Brochure" or glossy paper
- Must be made with a Laser Printer



Toner Transfer



In PCB etching methodology, “toner transfer” is defined as the process of transferring laser toner to copper using thermal conduction

Chemical Etching

- The method by which unmasked copper on the board is corroded and shaped using a chemical bath composed of ferric chloride or other corrosive agents

- PCB is submerged for up to 20 minutes or until all excess copper is gone

Zombie Children and Processes that Fail.

Challenge

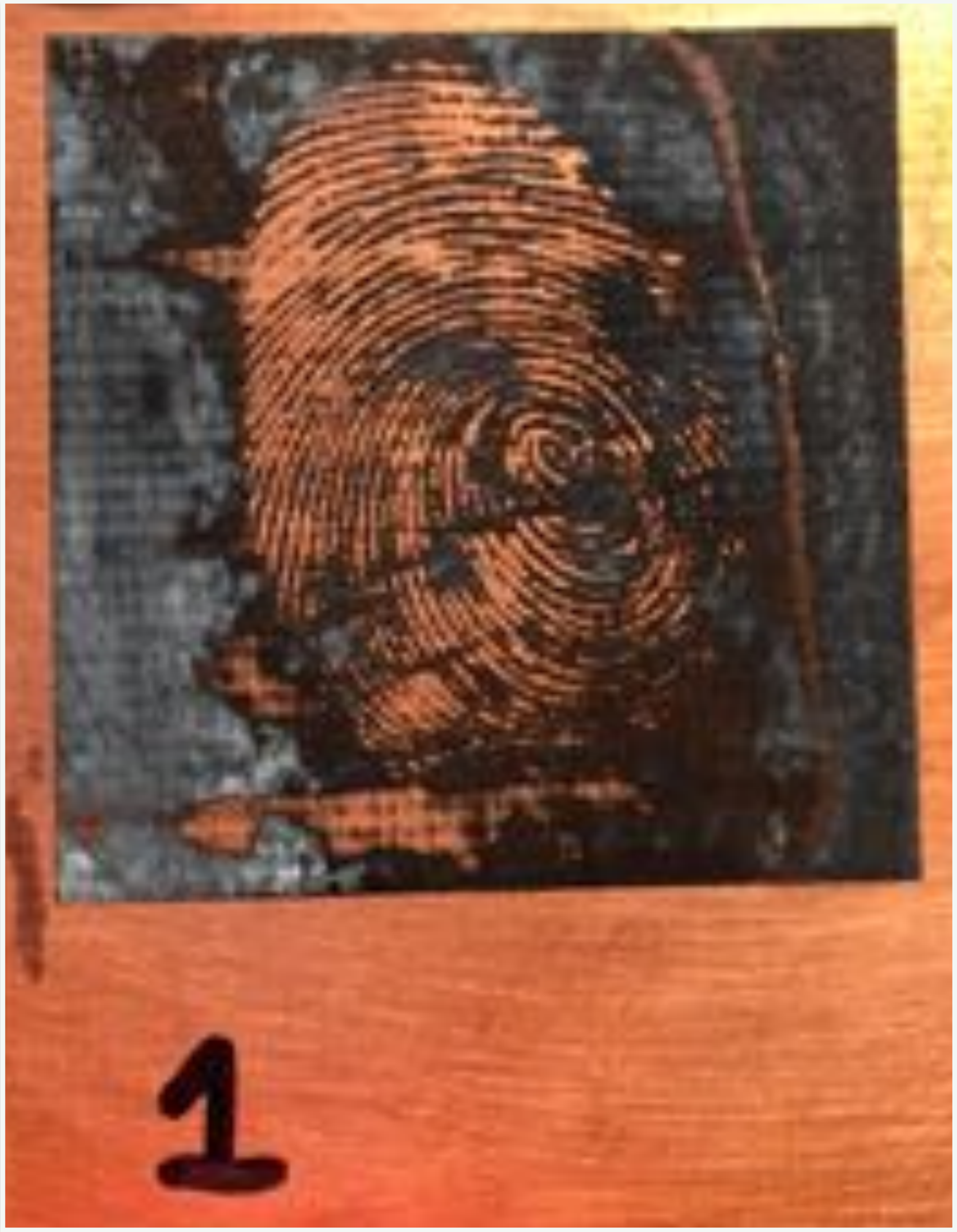
- Ink won't stick to copper board

Response

- Ensure board is heating evenly and to the high temperature required for toner transfer

What we have here is a failure to exfoliate.

Zombie Children and Processes that Fail.

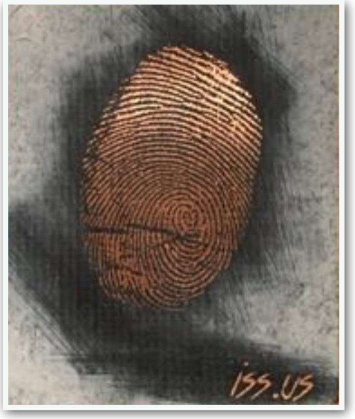


Challenge

- Ink won't stick evenly to copper board

Response

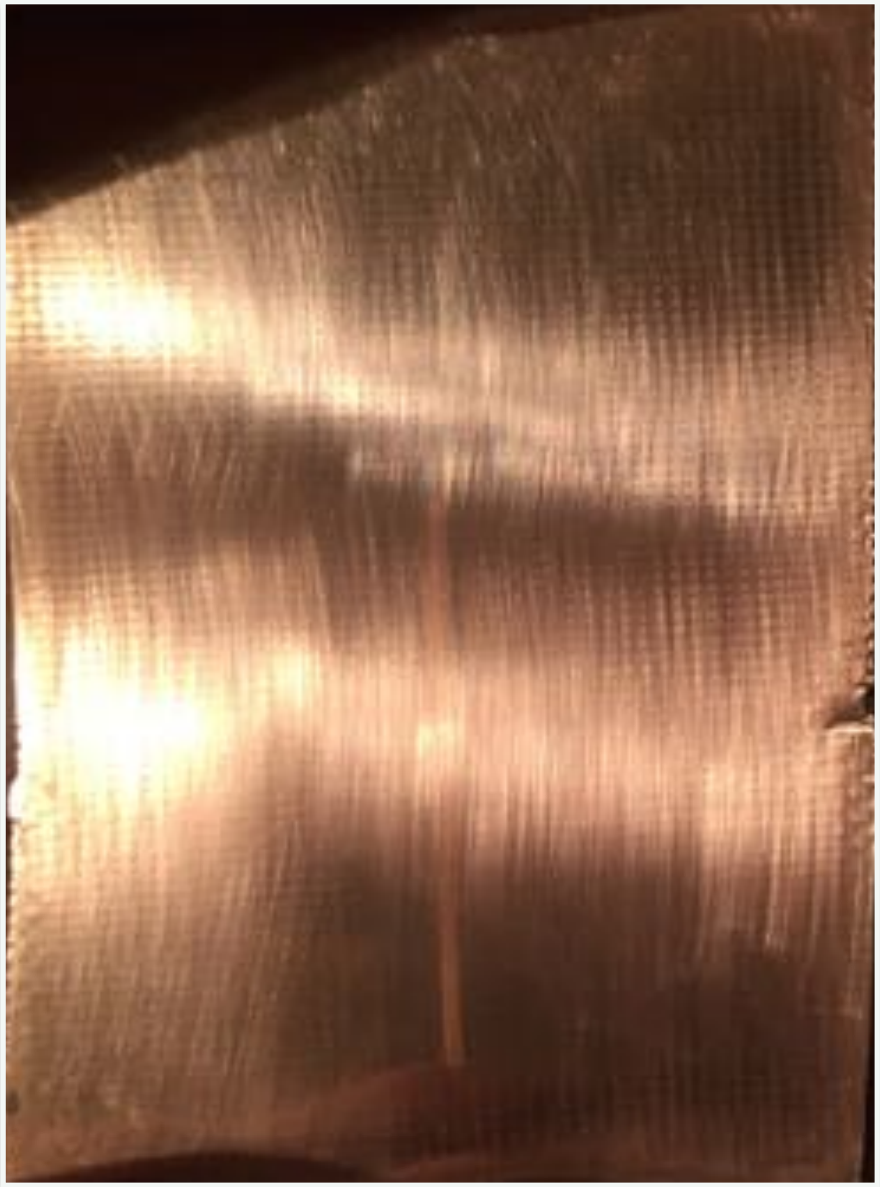
- Wear nitrile gloves at all times
- Ensure board is free of contaminants
- Buff w/ 2000 grain jeweler's sandpaper



What we have here is a failure to exfoliate.

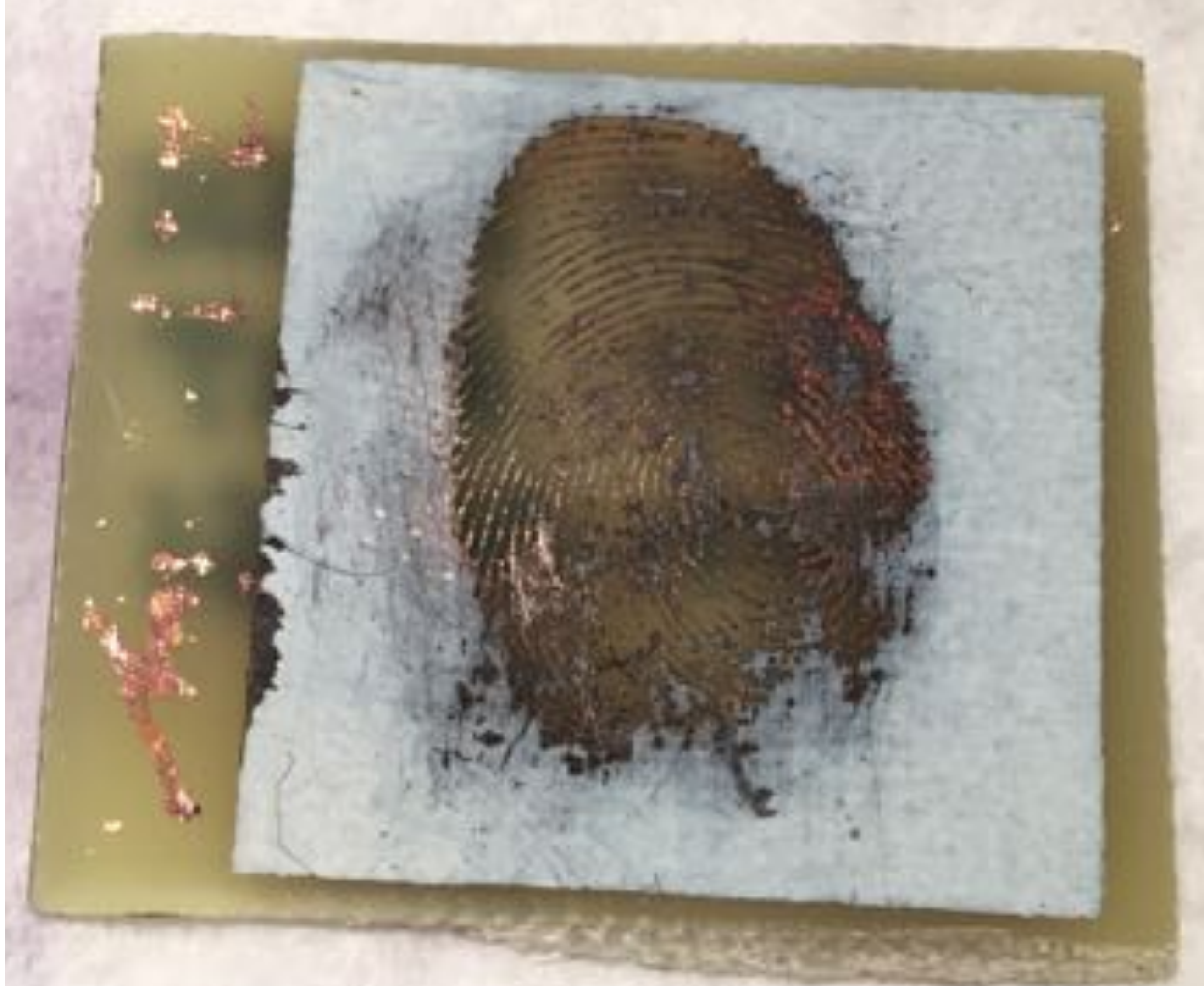
Before and After

actual color



What we have here is a failure to exfoliate.

Zombie Children and Processes that Fail.



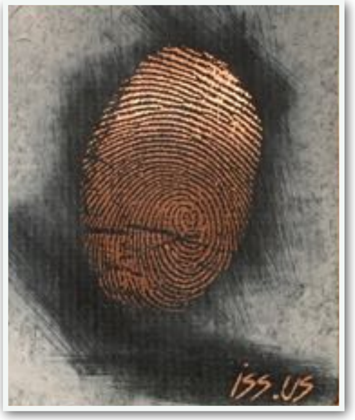
Challenge

- Heavy paper residue sticking to ink

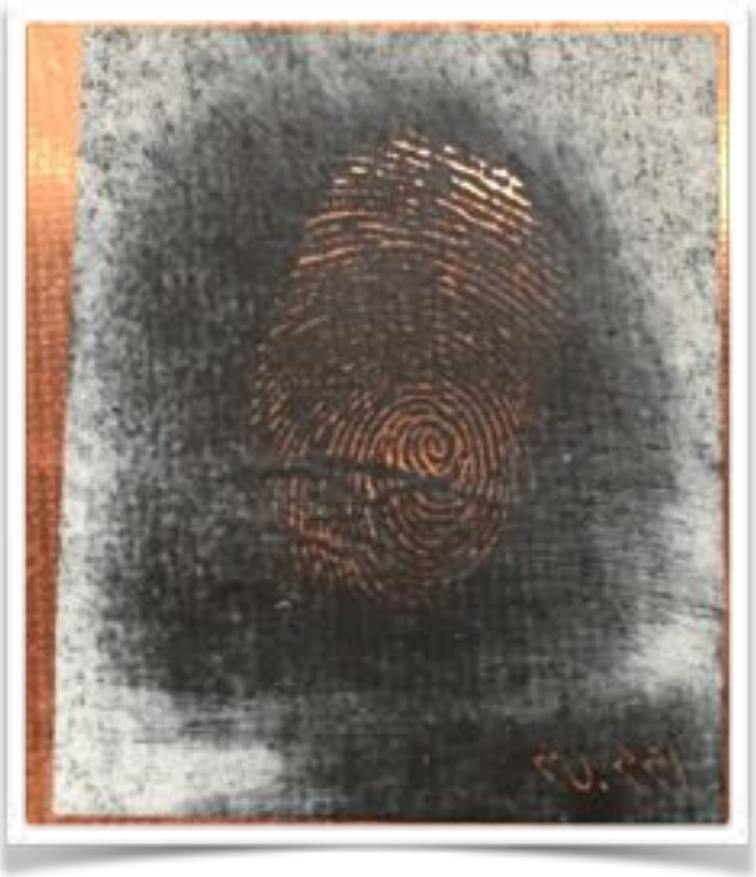
Response

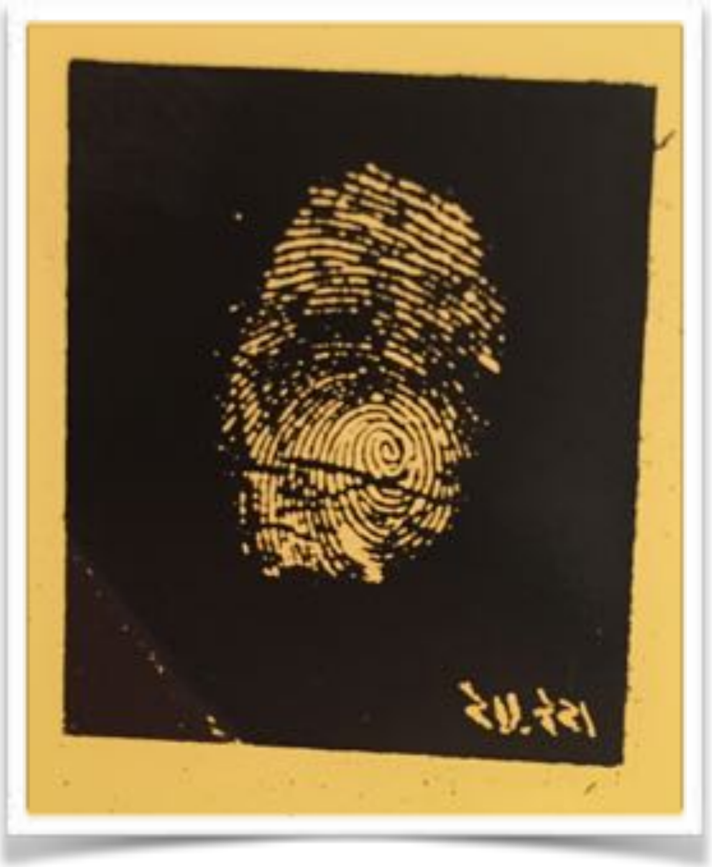
- paper is getting too hot and re-absorbing ink into it's core
- Limit to 90 seconds in the heat press

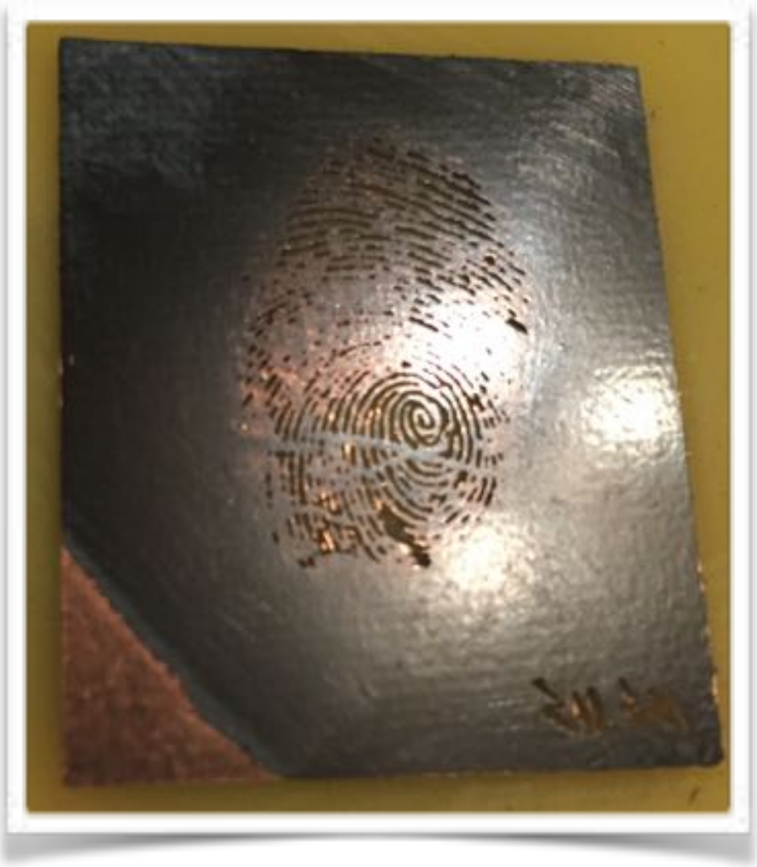
What we have here is a failure to exfoliate.



Zombie Children and Processes that Fail.





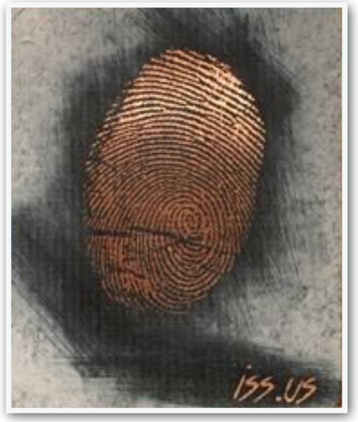


Challenge

- Ink is too thick, ridge data disappearing due to bleeding ink

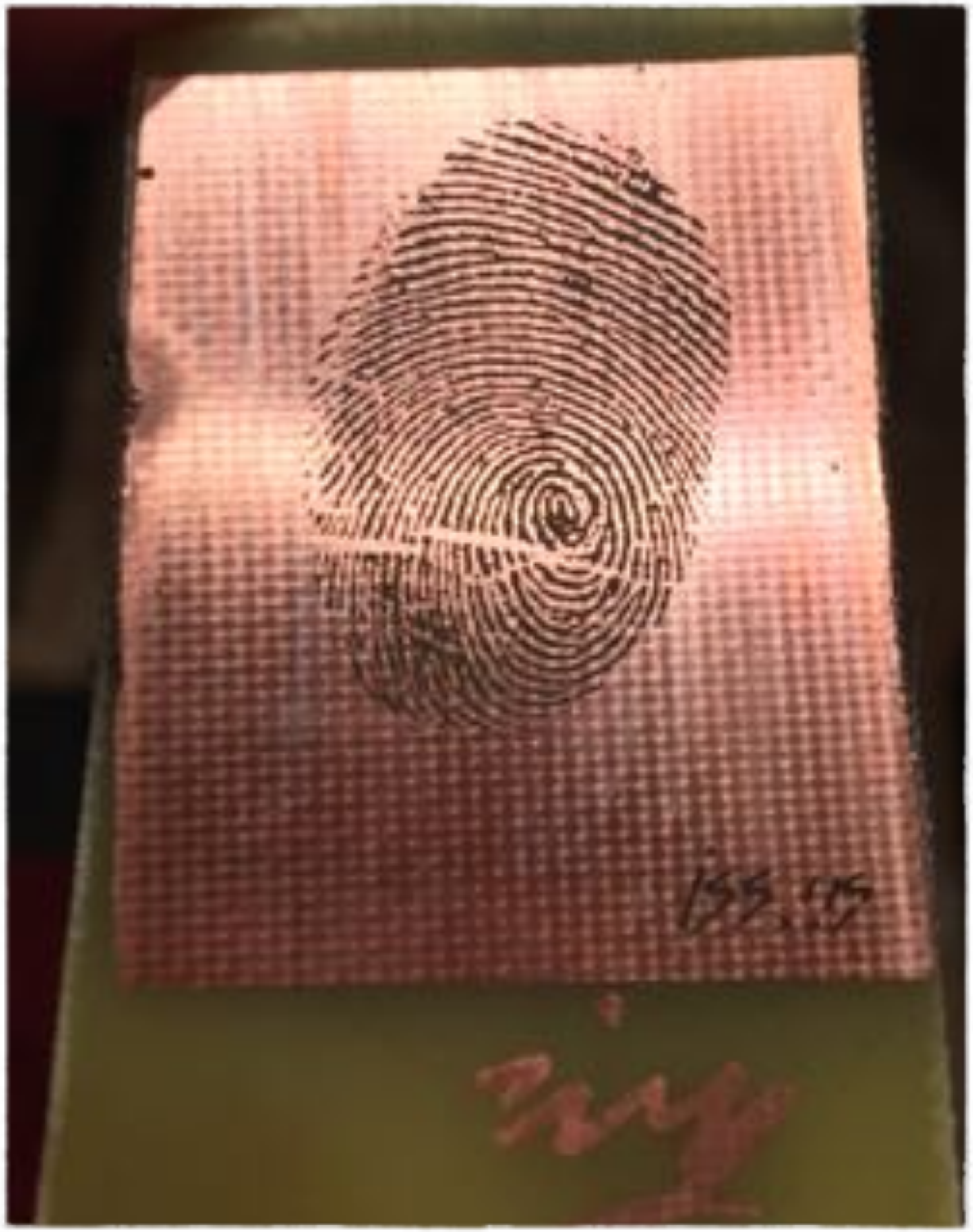
Response

- reduce toner output in printer dialogue



What we have here is a failure to exfoliate.

Mould Prototype



The Forged Fingerprint

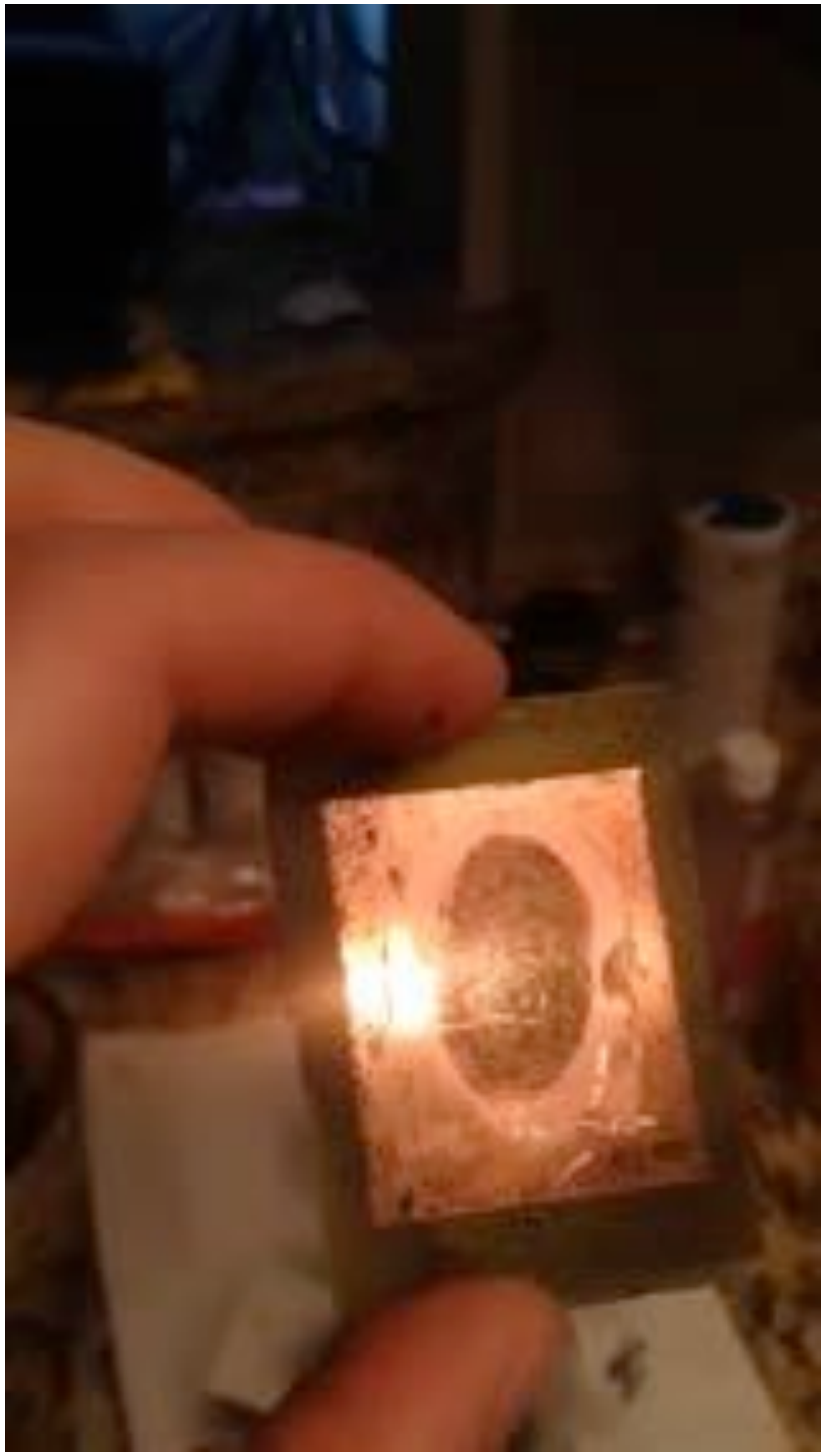
Specifications

- No thicker than a credit card
- Readable surface larger than home button
- Must read as a "live finger"

Materials

- Wood Glue
- Glycerine
- Graphite Lube

The Forged Fingerprint



Touch ID

All Things Security