LASER BEAMS & LIGHT STREAMS

LETTING HACKERS GO PEW PEW

BUILDING AFFORDABLE LIGHT-BASED SECURITY TOOLING

SAM. BEAUMONT & LARRY TROWELL

Laser Beams & Light Streams: Letting Hackers Go Pew Pew

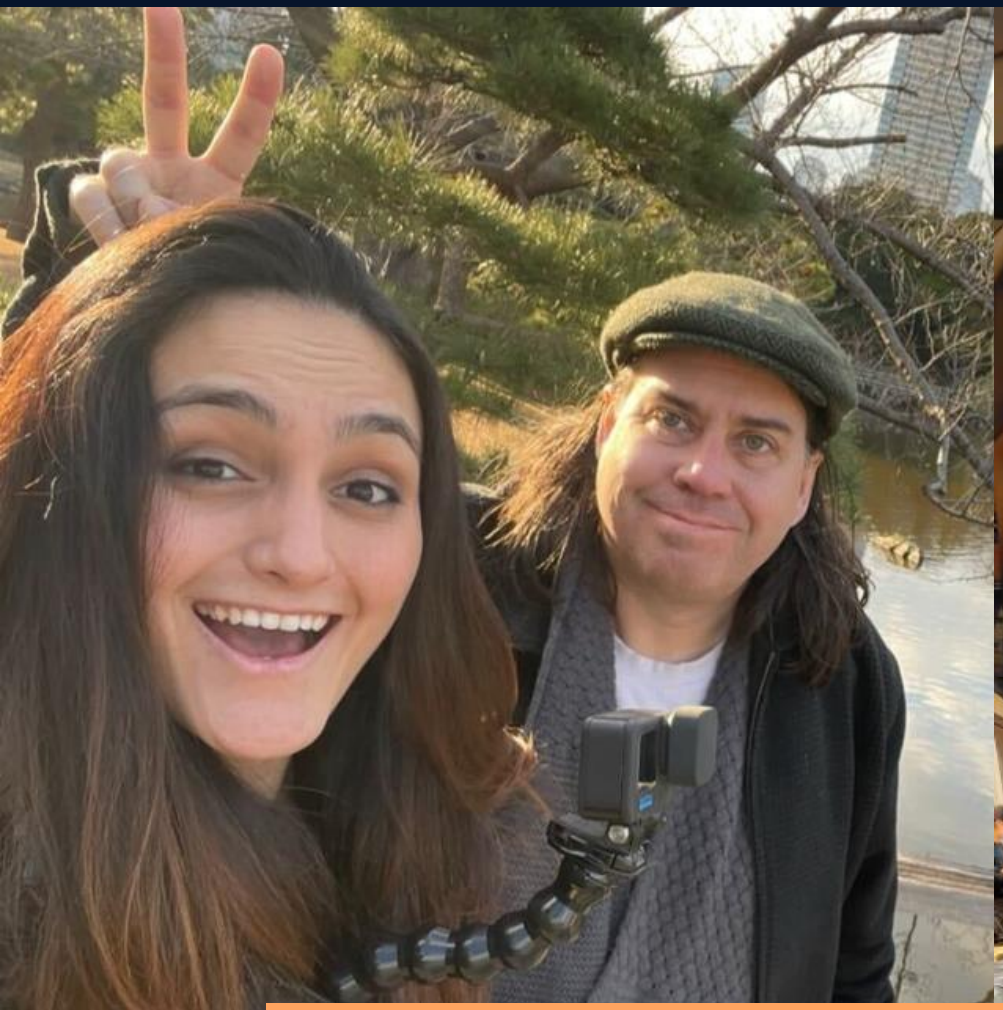
Building Affordable Light-Based Hardware Security Tooling

Sam. Beaumont & Larry Trowell

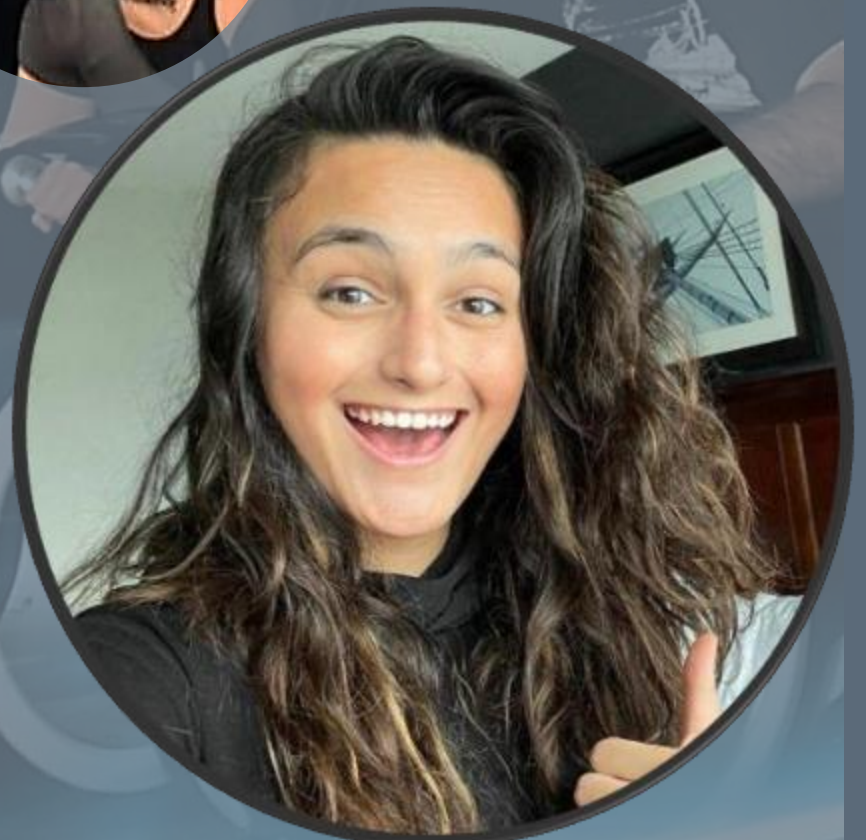
aka. PANTH13R & PATCH

#BHUSA #BlackHatEvents

Project “L.O.R.E.M”



“Laser Oscillation for Retrieving Electronic Memory”



Samantha Isabelle Beaumont (Sam. Beaumont)

a.k.a. “PANTH13R”

- Perpetually Tired
- Terrible with Nouns
- Specialist in Robotics & Cyber-Physical Systems
- Hacks “**anything that flies, sails or drives**”

Project “L.O.R.E.M”

Larry Q. Trowell

a.k.a. “PATCH”

- Horrible with acronyms
- Navigates same way as Dirk Gently
- Specialist in Embedded Systems
- Hacks “**anything with a chip**”

Project “L.O.R.E.M”

WIZARD	ANDROID	SCIENTIST
		
Chas Becht	Casey Repp	Kurtis Shelton

"If we get to the end of this project, and no member of the team has been murdered by another…it will be a miracle.“ – Chas Becht

CHAS BECHT
“The WISARD”

- Instrumental to this research and should be here on stage with us
- Electrical Engineering wisard
- Circuit Father
- Aliases:
  - Chaz
  - Chase
  - Chasssssseeeee
  - Chas

CASEY REPP
“The ANDROID”

- The detailer
- “Silent Third Party” android
- Our third musketeer
- Aliases:
  - Sam
  - KC
  - Who?
  - Story Teller
  - Puppeteer

KURTIS SHELTON

“The ~~actual~~ SCIENTIST”

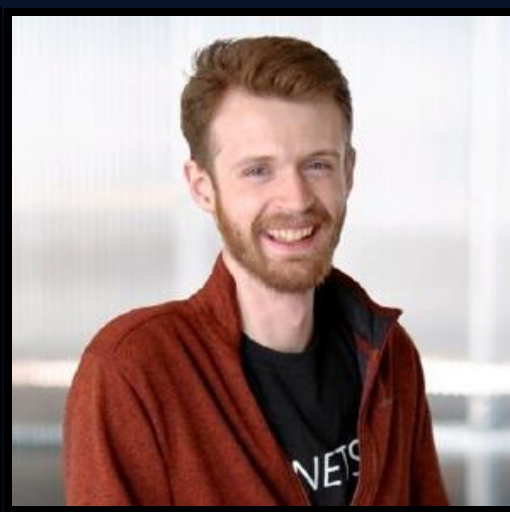
- Machine Learning Madman
- “Mathematics First”
- Modelling Father of all
- Research Scientist
- Aliases:
  - Juice Daddy
  - Mr. Smiles
  - Giggle Meister
  - Birdie
  - SHELDER

NetSPI: The Proactive Security Solution

Hardware & Integrated Systems







Artificial Intelligence & Machine Learning

NetSPI: The Proactive Security Solution





APPLICATION PENTESTING
Web & API Application
Mobile Application
Thick Application

NETWORK PENTESTING
Internal Network
External Networks

CLOUD PENTESTING
AWS
Azure
Google Cloud

ATTACK SURFACE MANAGEMENT (ASM)

AI/ML PENTESTING
Large Language Models

HARDWARE & INTEGRATED SYSTEMS
Hardware & Embedded Systems
Cyber-Physical Systems

MAINFRAME PENTESTING

SAAS SECURITY ASSESSMENT

BREACH AND ATTACK SIMULATION (BAS)

RED TEAM

BLOCKCHAIN PENTESTING

SECURE CODE REVIEW

CYBERSECURITY MATURITY ASSESSMENT
Security Program Advisory
Incident Response
Benchmarking

THREAT MODELING

Very Special Thanks

EMERGENCY ACID

John McMaster

EMERGENCY LASERS

Dr. Matt Lindley

“You don't need a group of superstars; you need a team working together to bring you better results” - Brian Lara

LASERS

PEW PEW PEW

DISCLAIMER & LEGALESE

Lasers used in this device and this presentation are Class 4 lasers based on American National Standards Institute Z136.1, Safe Use of Lasers. Please review this standard and applicable OSHA standards (e.g., https://www.osha.gov/laser-hazards/standards and associated standards) prior to using any laser and comply with the appropriate OSHA standards and protective measures. In addition, if accessing computer hardware please follow all manufacturer's guidelines for such hardware.

The device being demonstrated, and the presentation of its use at this seminar, are intended for educational purposes only (i.e., to demonstrate a specific use in a seminar setting) and not for purposes of instructing any person or entity in how to build or use the demonstrated device, even for the purpose described in this presentation. Any person attempting to develop the demonstrated device, or its use, or any similar device or use thereof, or to duplicate any element of this presentation assumes all risks of harm to themselves, other persons and property associated with such use, and the demonstrators and NetSPI, LLC are not responsible for any of the foregoing.

Without limiting the foregoing, please be aware that lasers can cause injury or death to persons and damage to property, including without limitation:

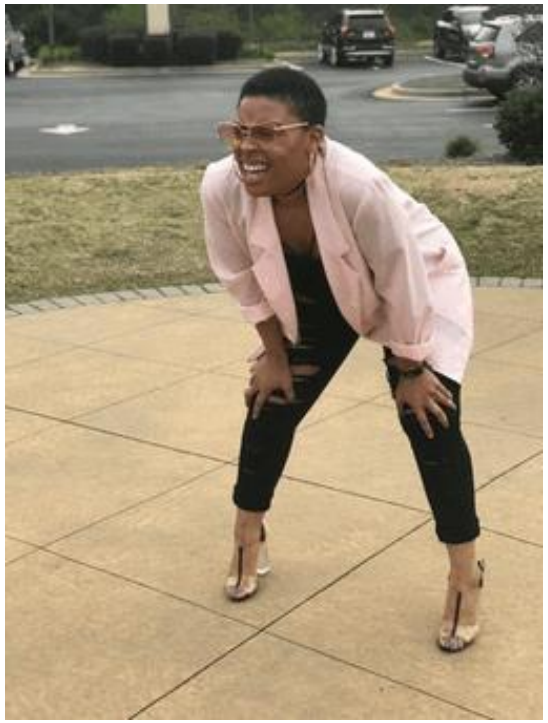
Eye injury (including corneal or retinal burns, opacities, i.e., cataracts), from having a laser shone at the eye, reflected from a surface into the eye, or from looking at the laser source or its impact point. Do not view a laser beam through the use of an optical instrument (such as binoculars, microscope, etc.).

Skin injury (including without limitation burns and carcinogenesis) from having a laser shone at the skin, reflected from a surface onto the skin, or from touching the laser source or any surface heated by the laser (even after the laser has been turned off).

Heating, inflammation and damage to objects, and potential toxic exposure hazards to persons, from combustion and smoke from heating of objects by exposure to lasers (which may involve release of toxic gas, smoke or particles in a laser plume), due to a laser shone at the object, reflected from a reflective surface onto the object, or from the object touching the laser source or any object heated by the laser (even after the laser has been turned off). Without limiting the foregoing, personal injuries may include inhalation hazards, inflammation, irritation or exposure to cancer causing substances.

Exposure to toxins from hazardous substances used in or released by lasers (such as chemical dye, some of which is flammable), or improper handling of high voltage equipment used in laser equipment (which may also result in shock and be potentially lethal). Exposure to hazardous substances and electric shock (which may be potentially lethal) may also arise when accessing and using computer hardware of any kind.

Without limiting any of the foregoing, use appropriate protective gear and take appropriate protective measures (all as advised by OSHA, see above) when using lasers, such as (but not limited to) the correct eye protection (which varies for the Class and wavelength of laser being used).



DISCLAIMER & LEGALESE

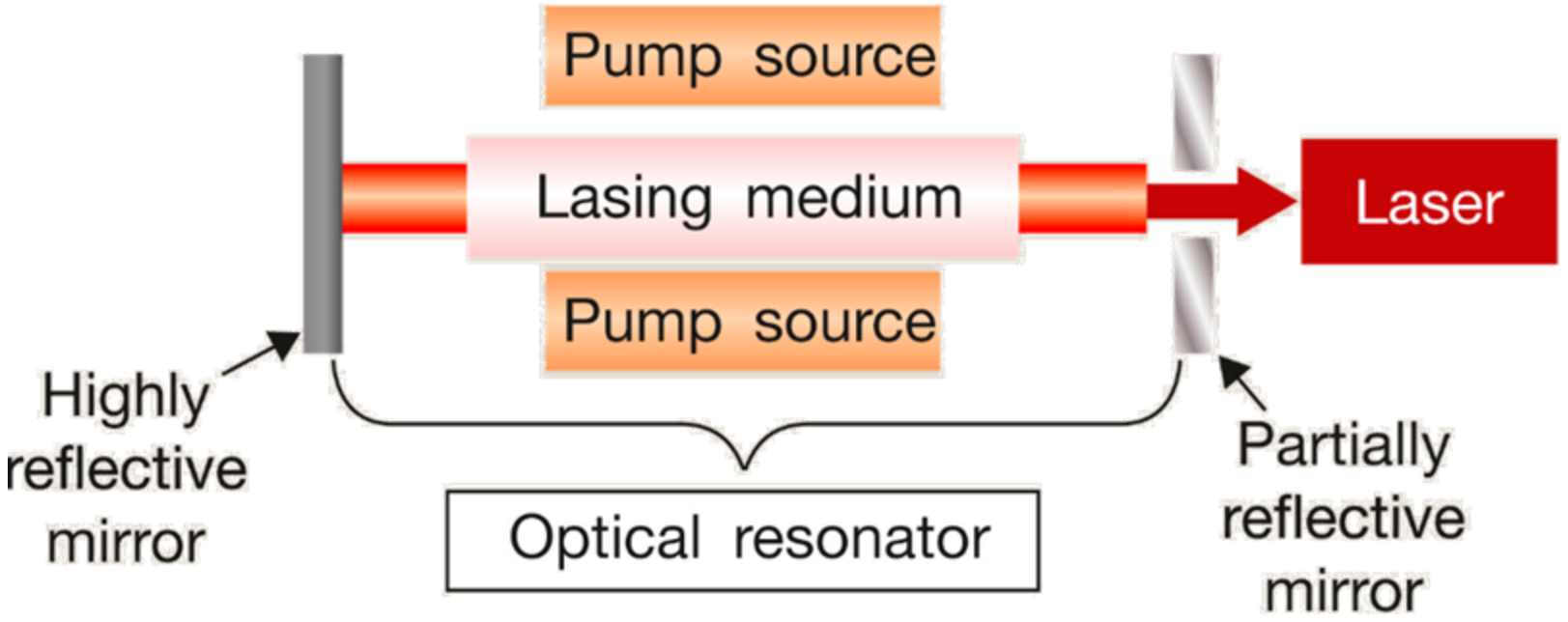
- YOU CAN BE BLINDED, OR WORSE
- INVISIBLE LIGHT, IS STILL LIGHT
- WEAR (THE RIGHT) PROTECTION
- Remember, you only get two chances to protect your eyes

LASERS ARE DANGEROUS

What is a L.A.S.E.R.?

- L.A.S.E.R.
  - **L**ight
  - **A**mplification by
  - **S**timulated
  - **E**mission of
  - **R**adiation

- Bouncing photons inside a medium until they all face one way



Why LASERS?

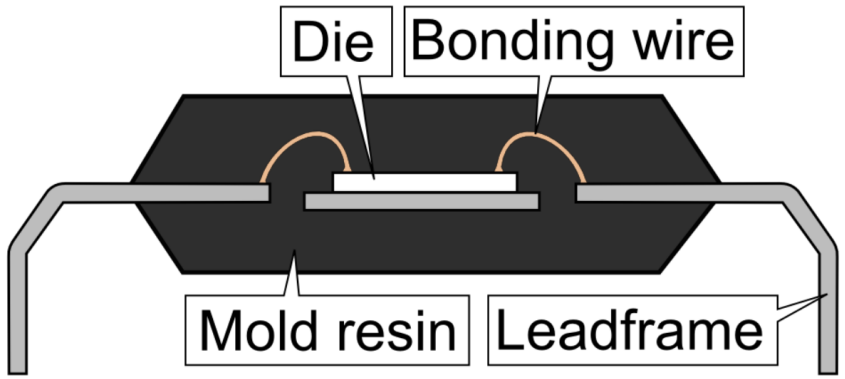
- Light is easy to source
- Transistors have an inherent weakness to light
- Contactless
- Non-Damaging (physically to the target)
- Typically considered a “Semi-invasive” technique

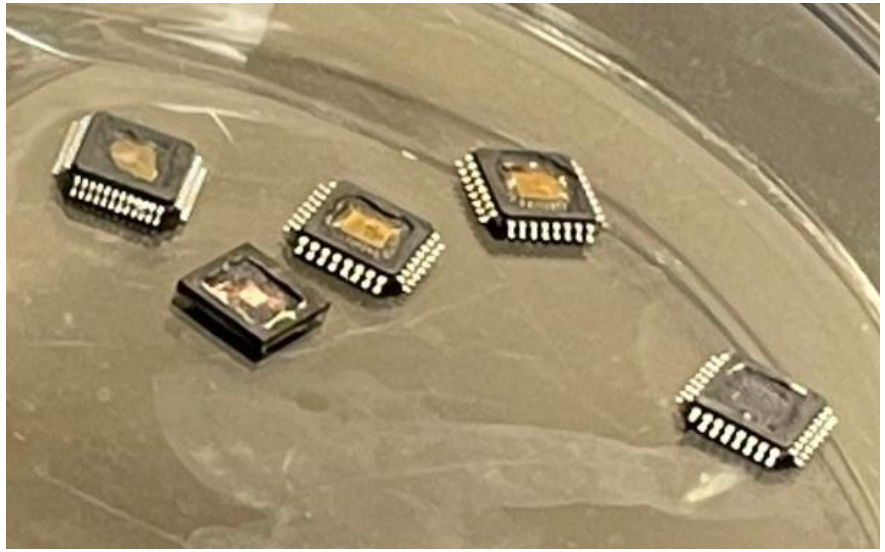
“Semi-Invasive”

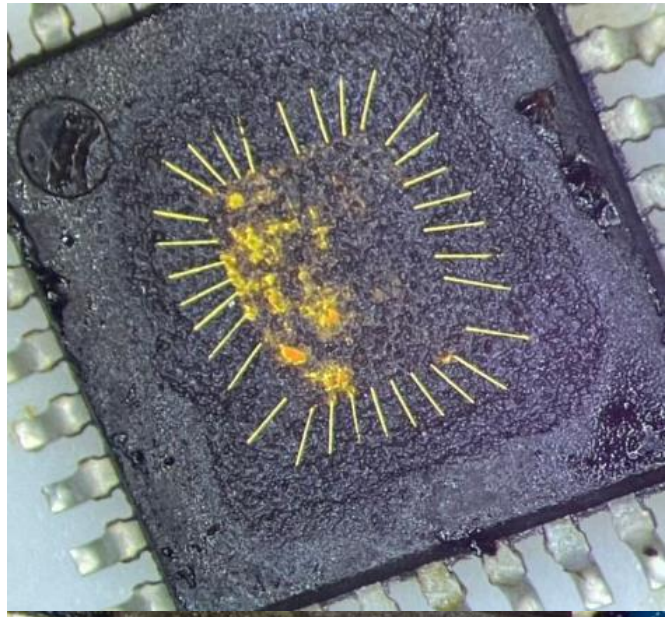
A visceral experience

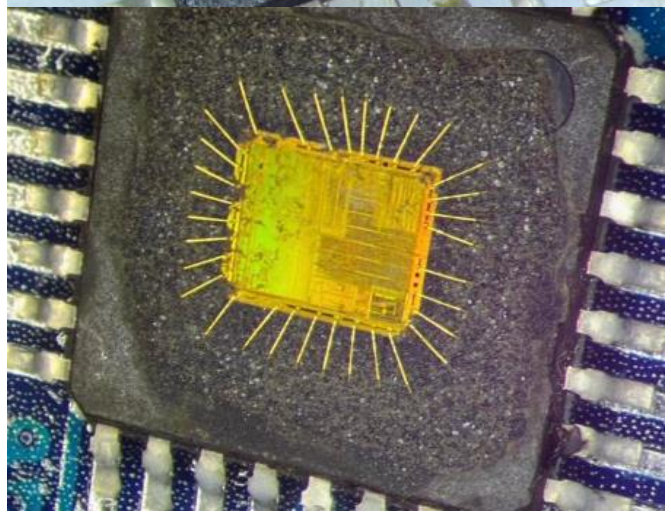
Method 1: Chemical Decapsulation

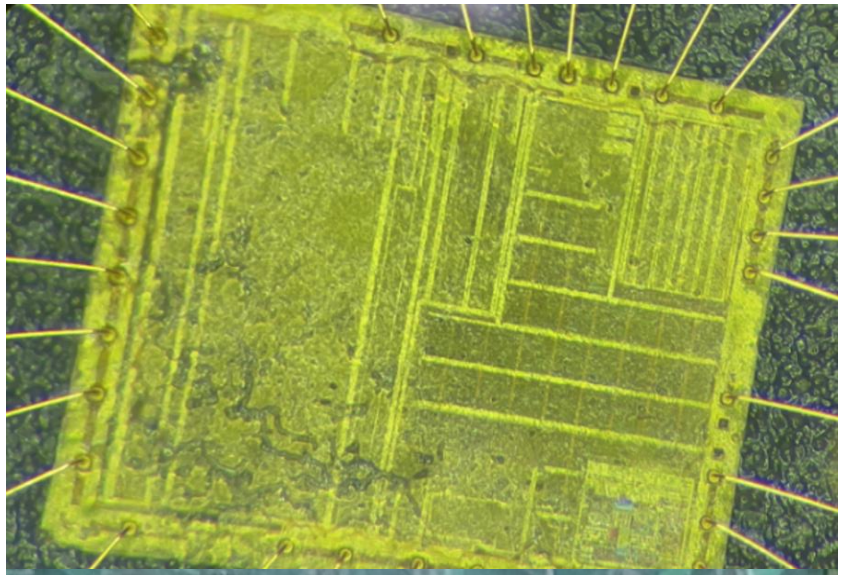
ACID

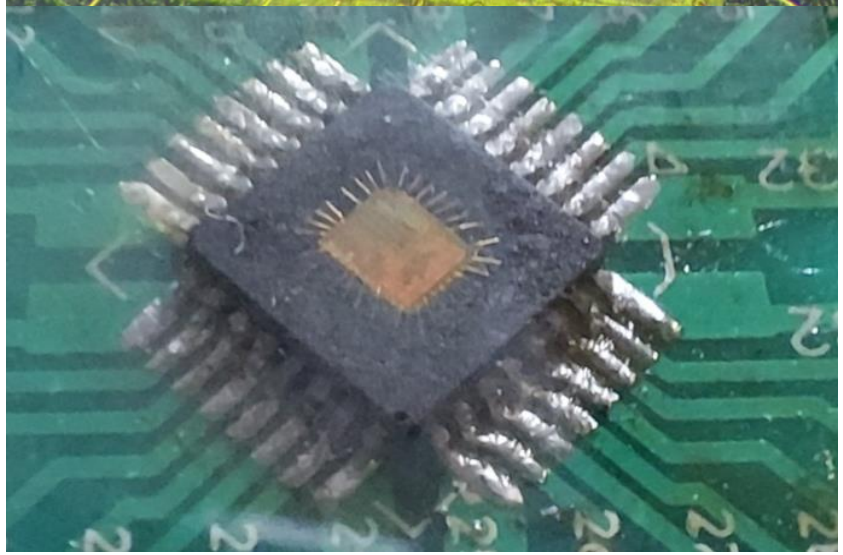




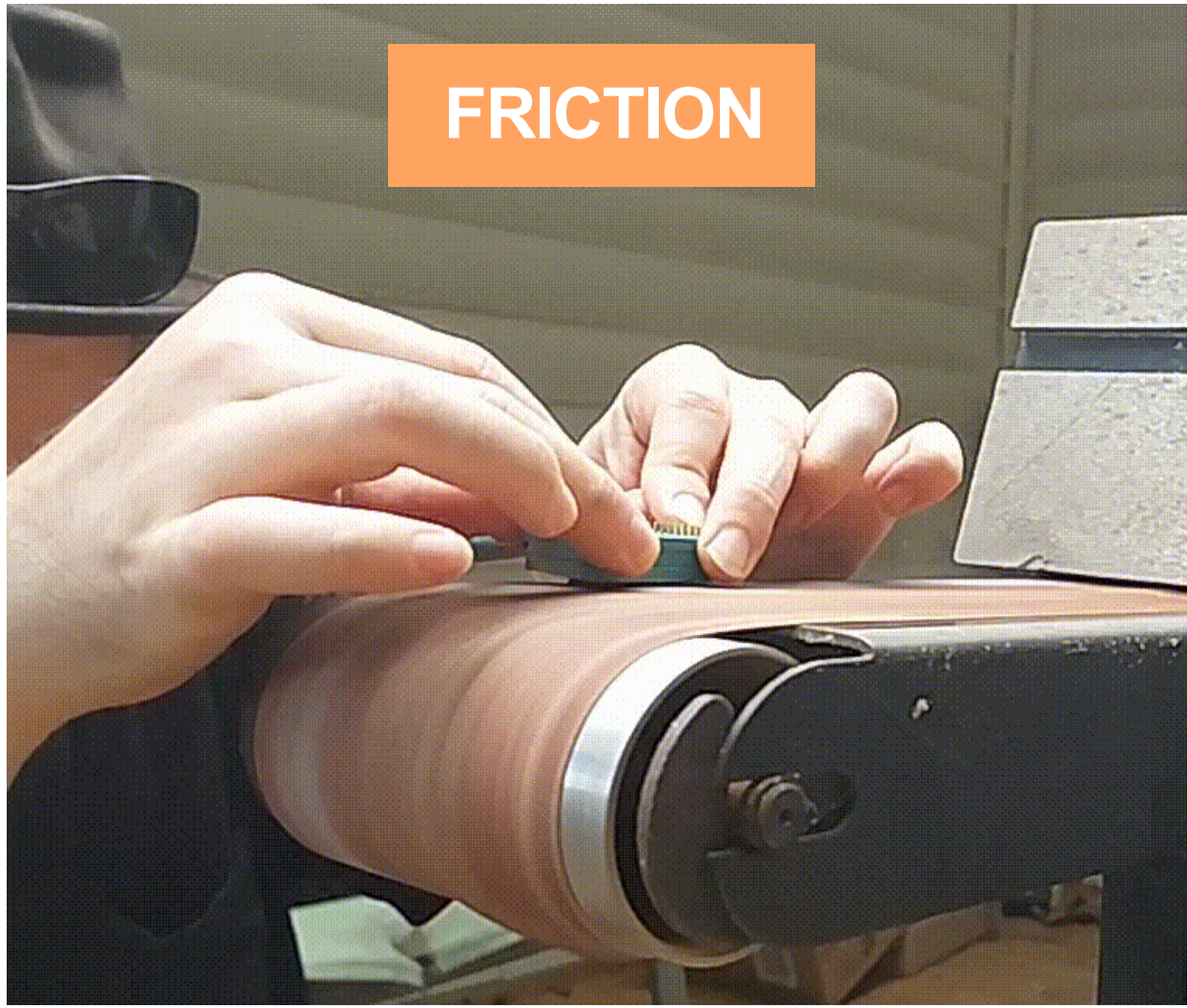




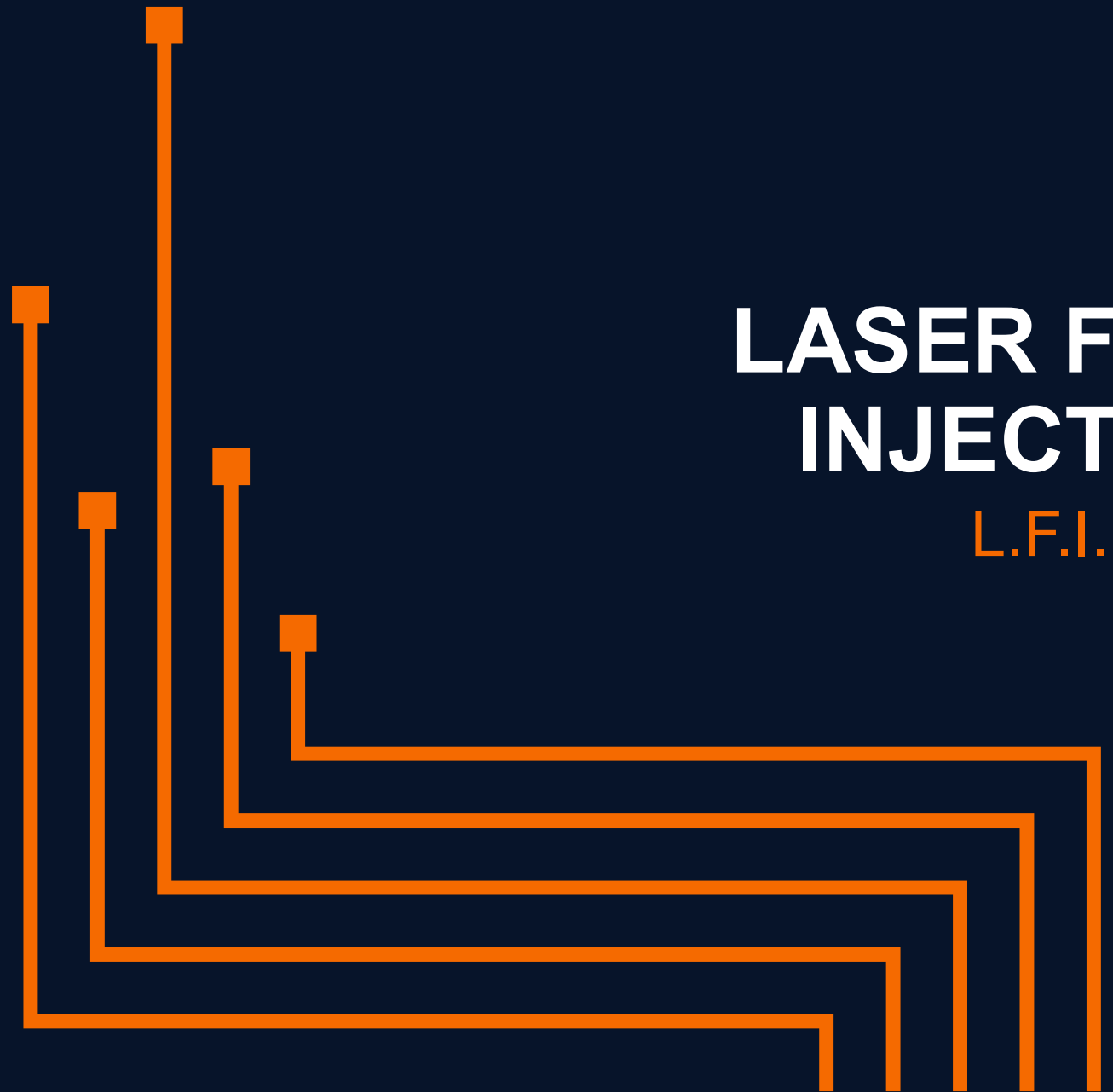




Method 2: “Creative” Destruction



“On one hand, I'm sad to see the standard bigger-hammer method go.. in the other though.. belt sanders and lasers!!!” – Casey Repp

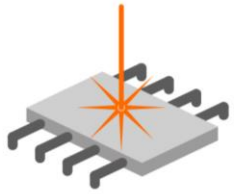


LASER FAULT INJECTION

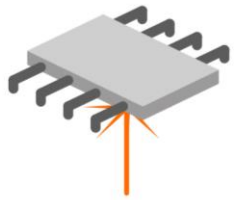
L.F.I.

What, Why, and How?

- Fault injection is traditionally used to cause a processor to skip functions
- LFI is a technique that allows you to affect processor functions with nothing more than light
- Very useful when achieving bypasses of security mechanisms



FRONTSIDE



BACKSIDE

LATERAL

Let’s Axolotl Questions…

Drinks are on that …person!

New:

- 150,000 USD
- 200,000 EUR
- 180,000 GBP

Used, or Decrepit:

- 5,000 - 20,000 USD

Return on investment

- ??????????????????????

Operation: Expense Report Cost Reduction

Objective: Domestication of Laser Tooling

LFI: The Essentials

An imaging system ➢To focus the laser

A positioning system ➢To position the laser, target, or both

A laser (obviously) ➢To fire, because they're cool

Traditional Imaging Systems

- Traditionally these are microscopes
- Reference researchers used the "Trinocular Leitz SM-LUX HL"
- Refurb Price: $4,000 USD
- Uh…Can we make one?

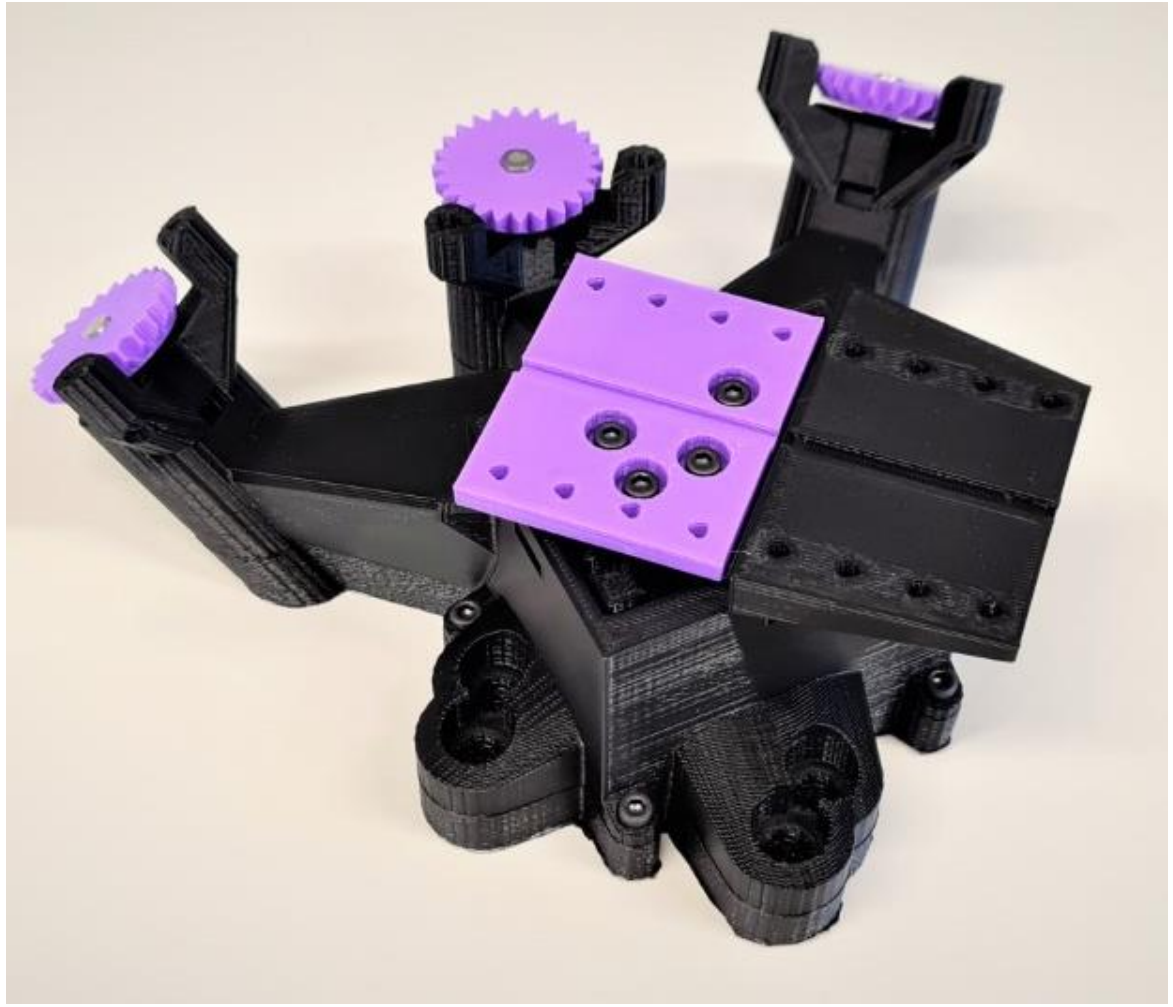
The OpenFlexure Project: Body

- 3D printable, high precision mechanical positioning housing
- For use in microscopes, micromanipulators, and more.
- Cost: ~$3.00 USD

Traditional Positioning Systems

- Next, we need a positioning table how much is one of those?
- Refurb Price: $3,000 USD
- Uh…Can we make one?

The OpenFlexure Project: Stage



- 3D printable, high precision mechanical positioning housing
- For use in microscopes, micromanipulators, and more.
- Cost: ~$1.00 USD

Traditional Laser Systems

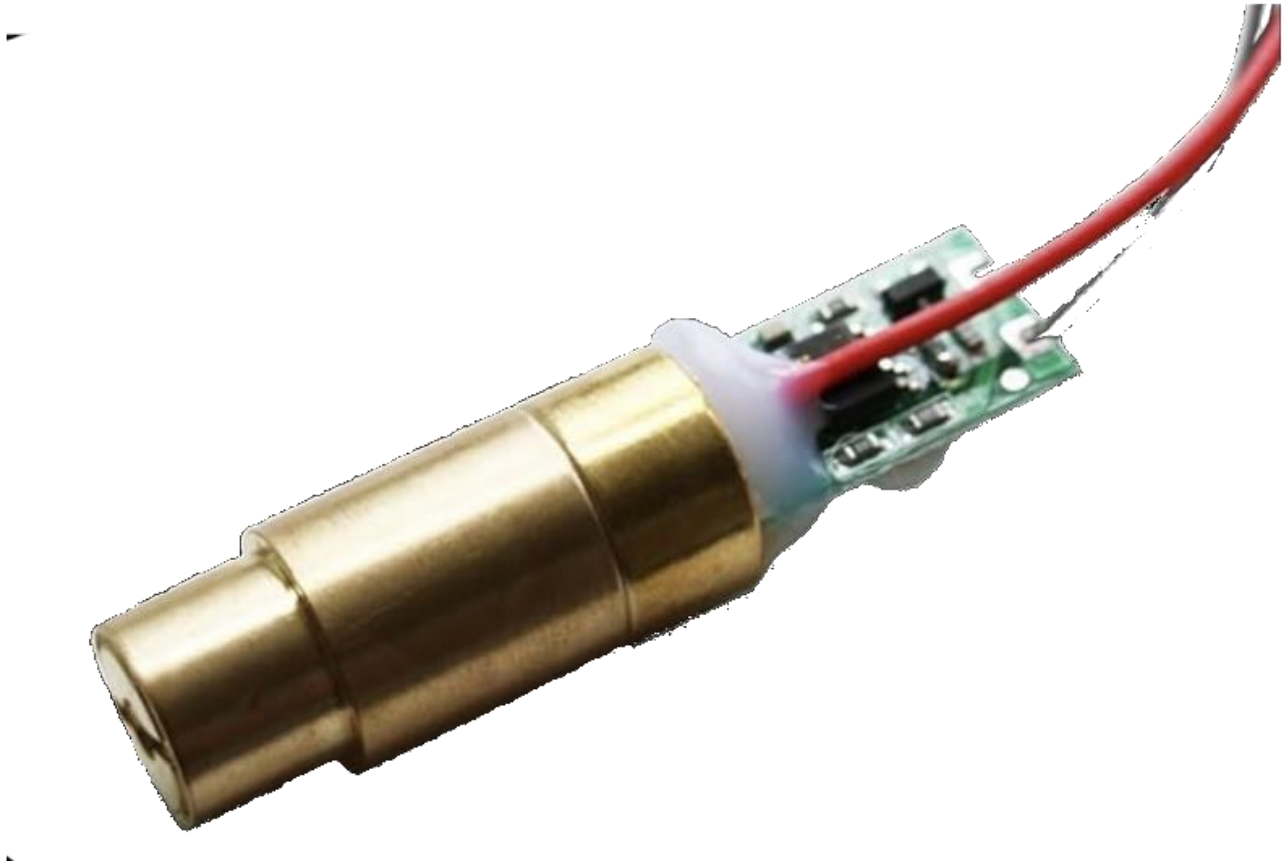
- That leaves a laser…so how does LFI work?
- Traditionally: firing a highly powerful laser in a very shot amount of time
- Do we really need that much power in a short amount of time?

- YAG laser provides 680MJ in 4ns
- They also cost over 30k, just for the laser
- How much power is needed to cause a glitch?

"I bought a laser pointer online that claimed for entertaining a housecat. Turns out it was a tiny, green, illegal alien weapon. The ATF is probably on their way to my house right now."

Photoelectric effect

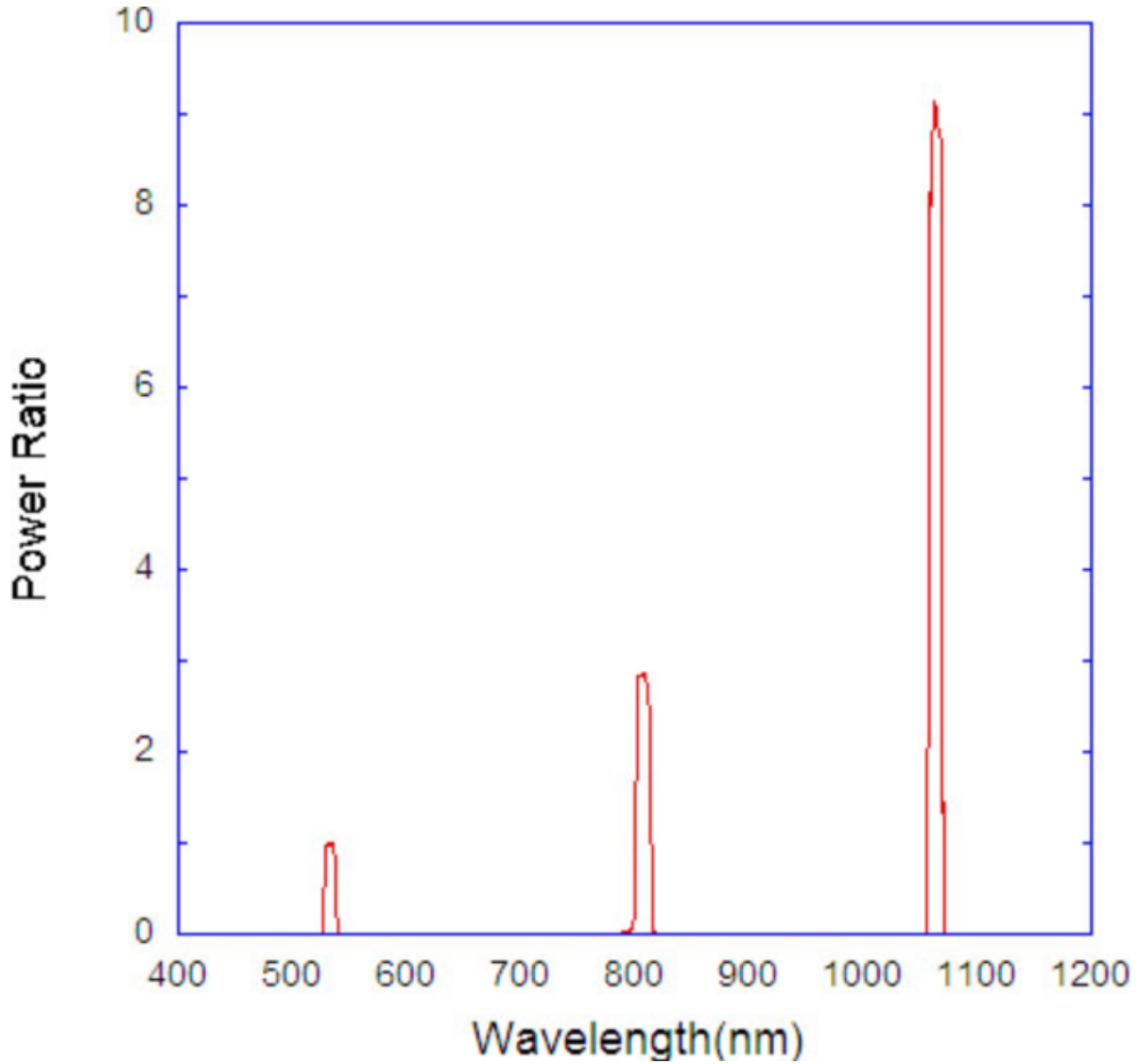
- Between 42.5 and 80 nJ
- Can we find a laser like that?
- We can use a 2.5W laser over 25ns … or
- We can use a less powerful laser for longer..



"I tried to power my electric car with nanojoules. It got about as far as an ant on a treadmill."

Its only 5mW, isn't that safe?

- These Green lasers are supposed to be 5mw, and they may be, for the 532nm (green) beam.
- However, there is not just 532nm
- There are other frequencies it emits



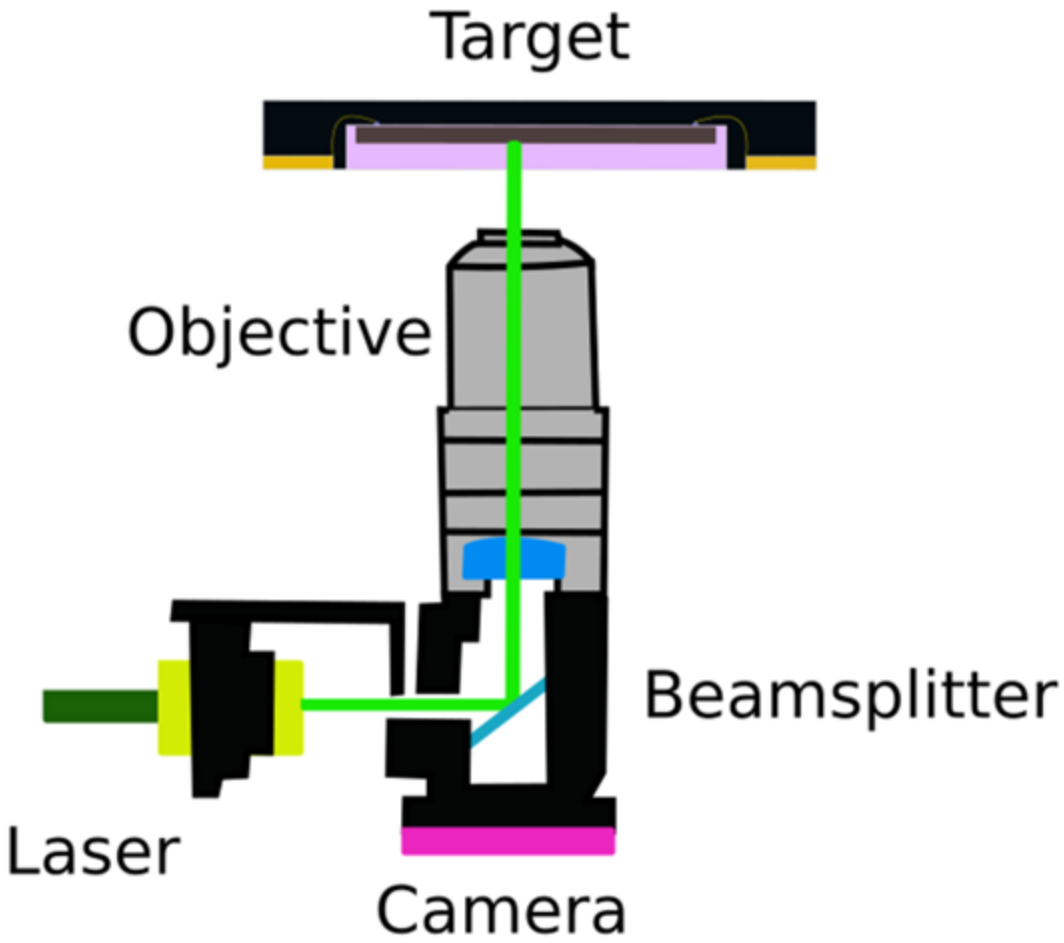
"I bought a laser pointer online that claimed to be a harmless 5mW. Turns out it was more like a miniature death ray disguised as a pen. It's like buying a puppy and getting a dragon instead."

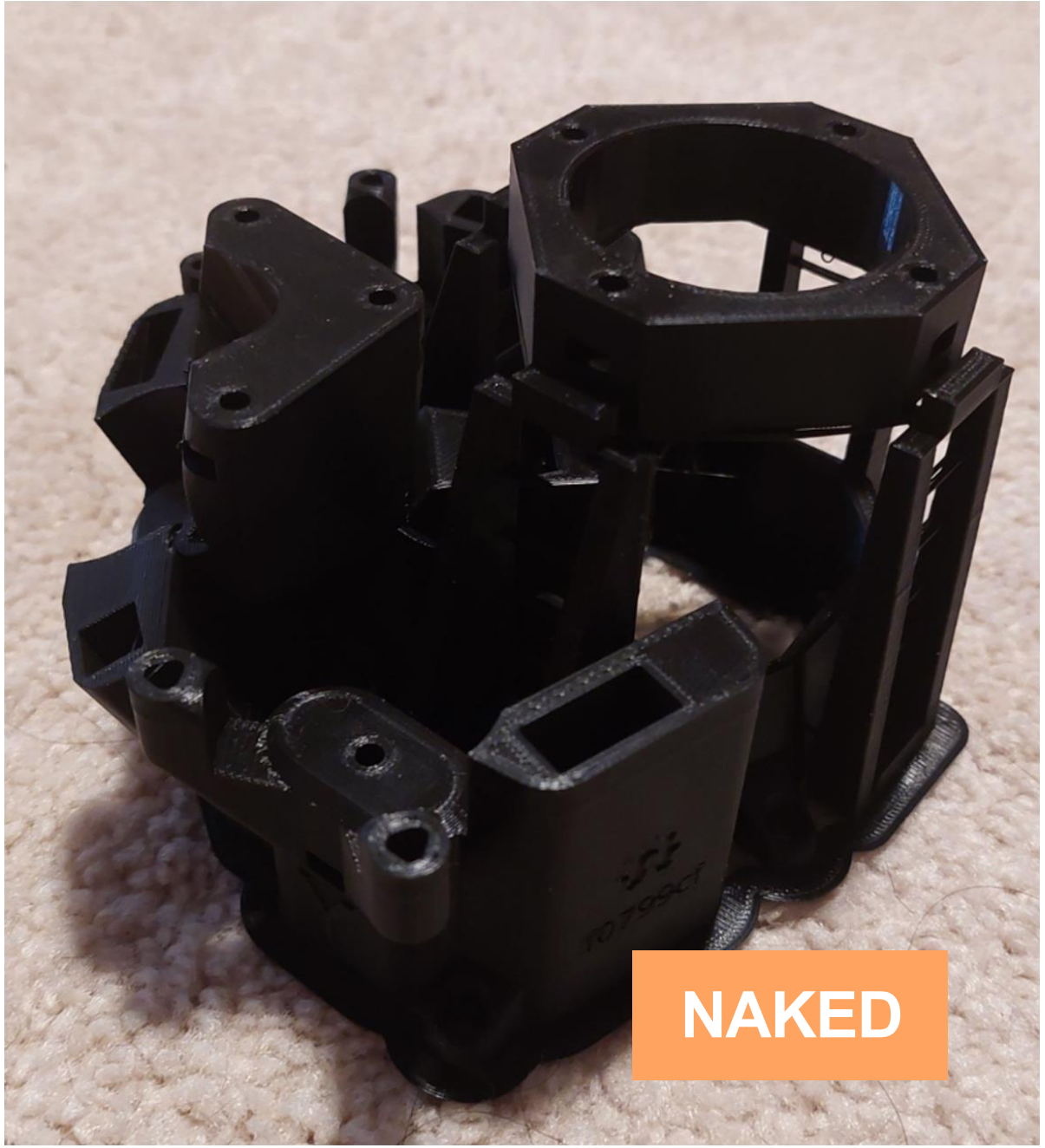
RayV-Lite

Everything Assembled

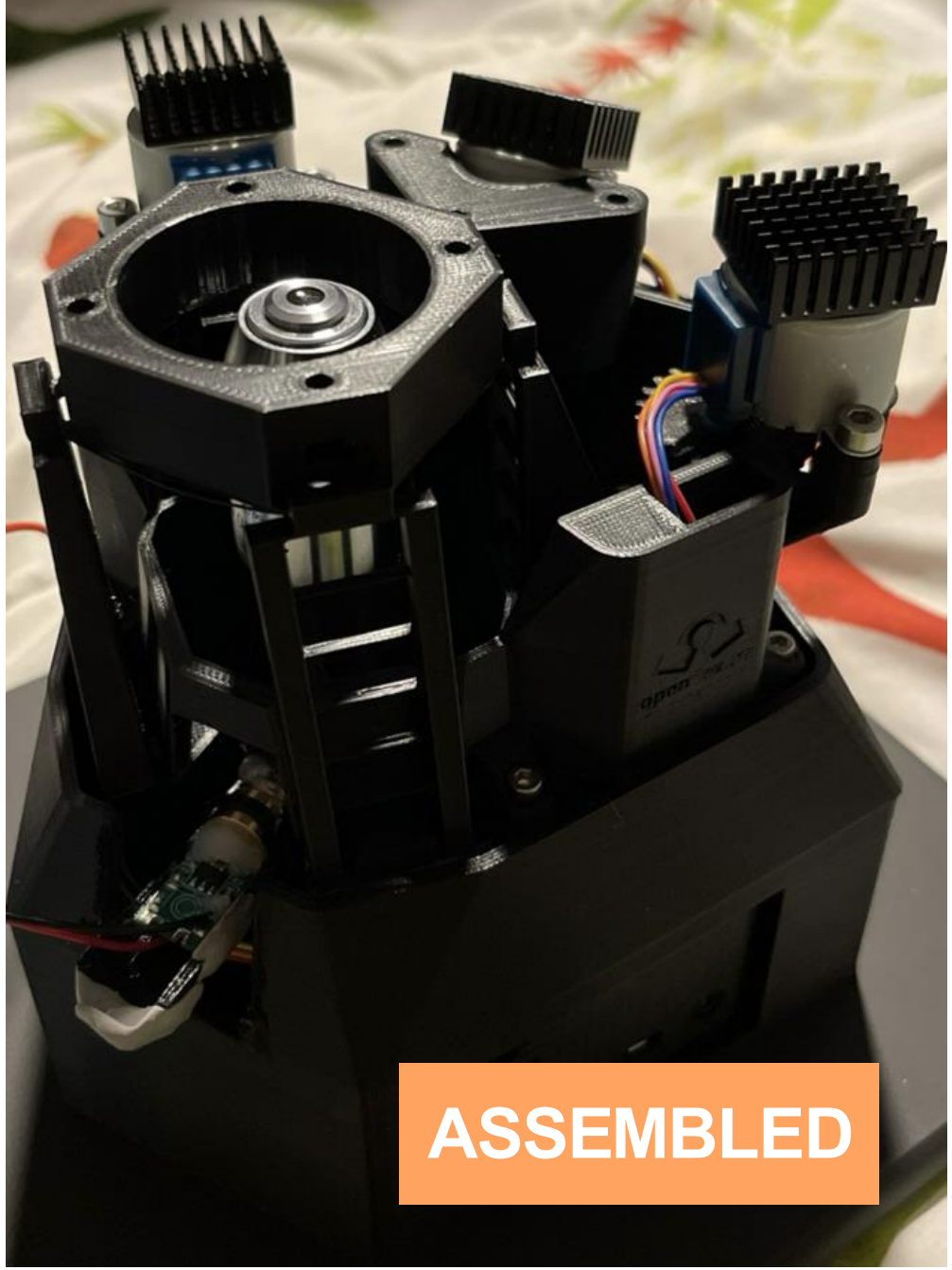
Putting it all together

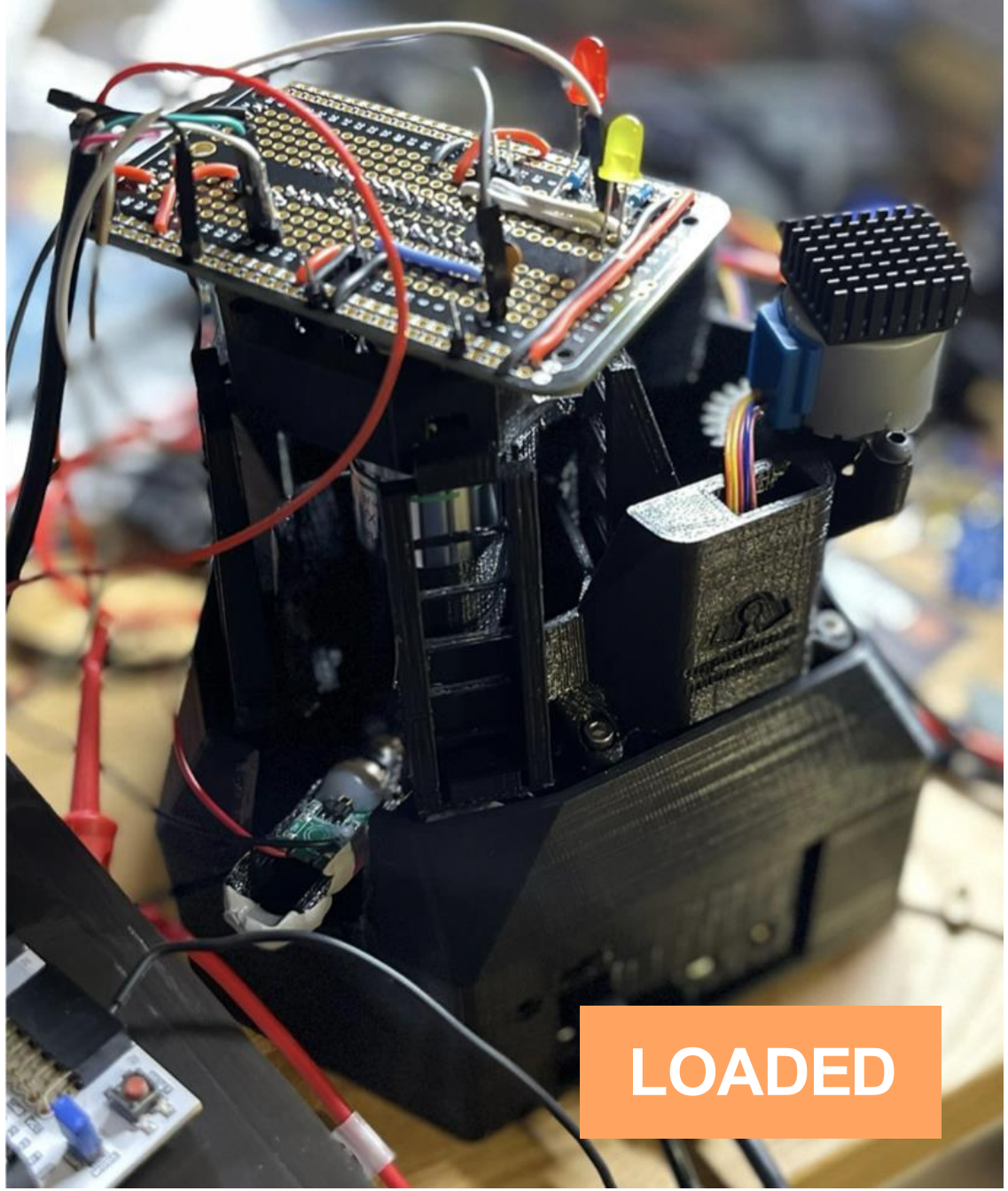
- An FPGA to slow target clock
- An LED to see the target (1050nm, more on this later)
- “Green” Laser pointer to fire, and glitch
- Objective to focus the laser




NAKED


ASSEMBLED

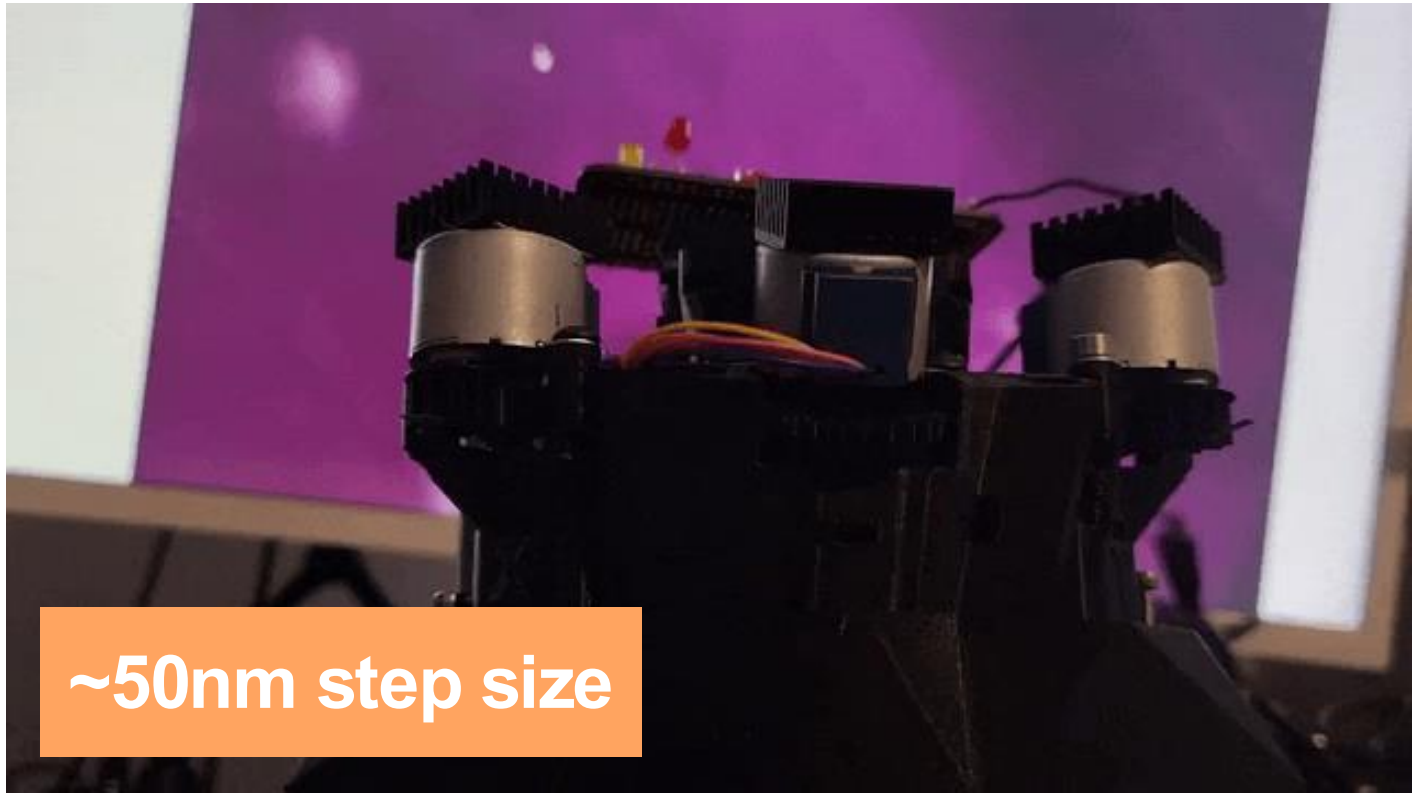

ASSEMBLED

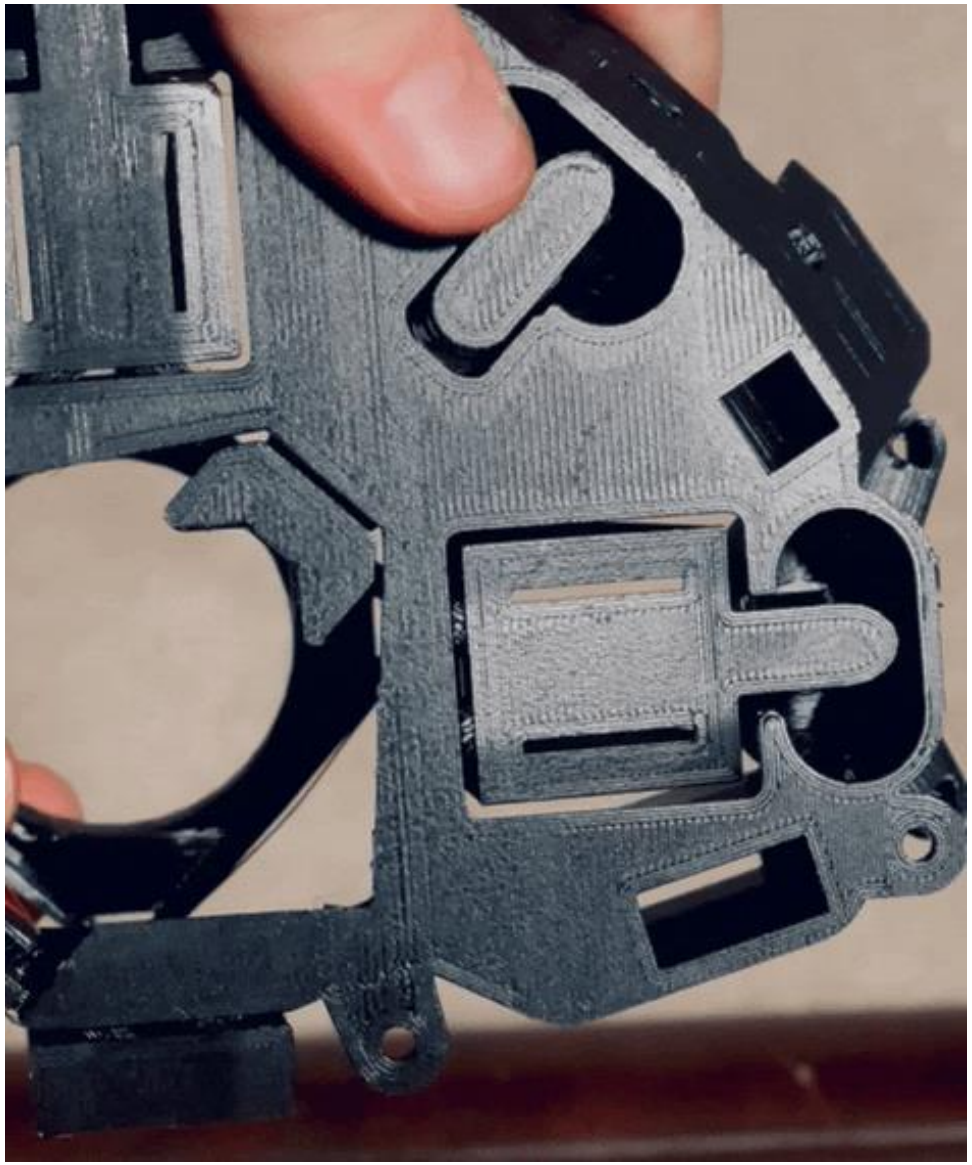

LOADED

Poetry in Motion

The beauty of plastic….

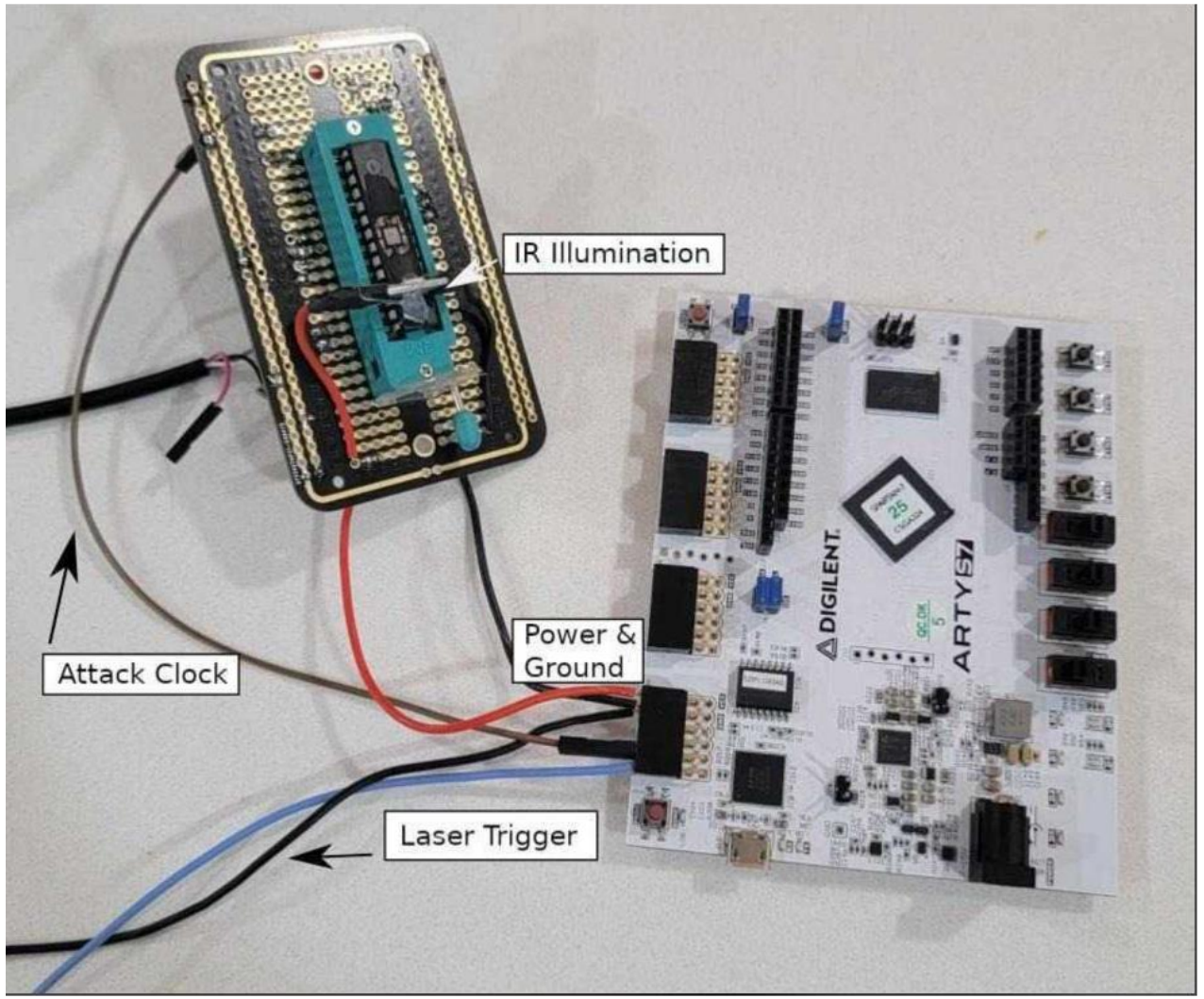
….is that it bends

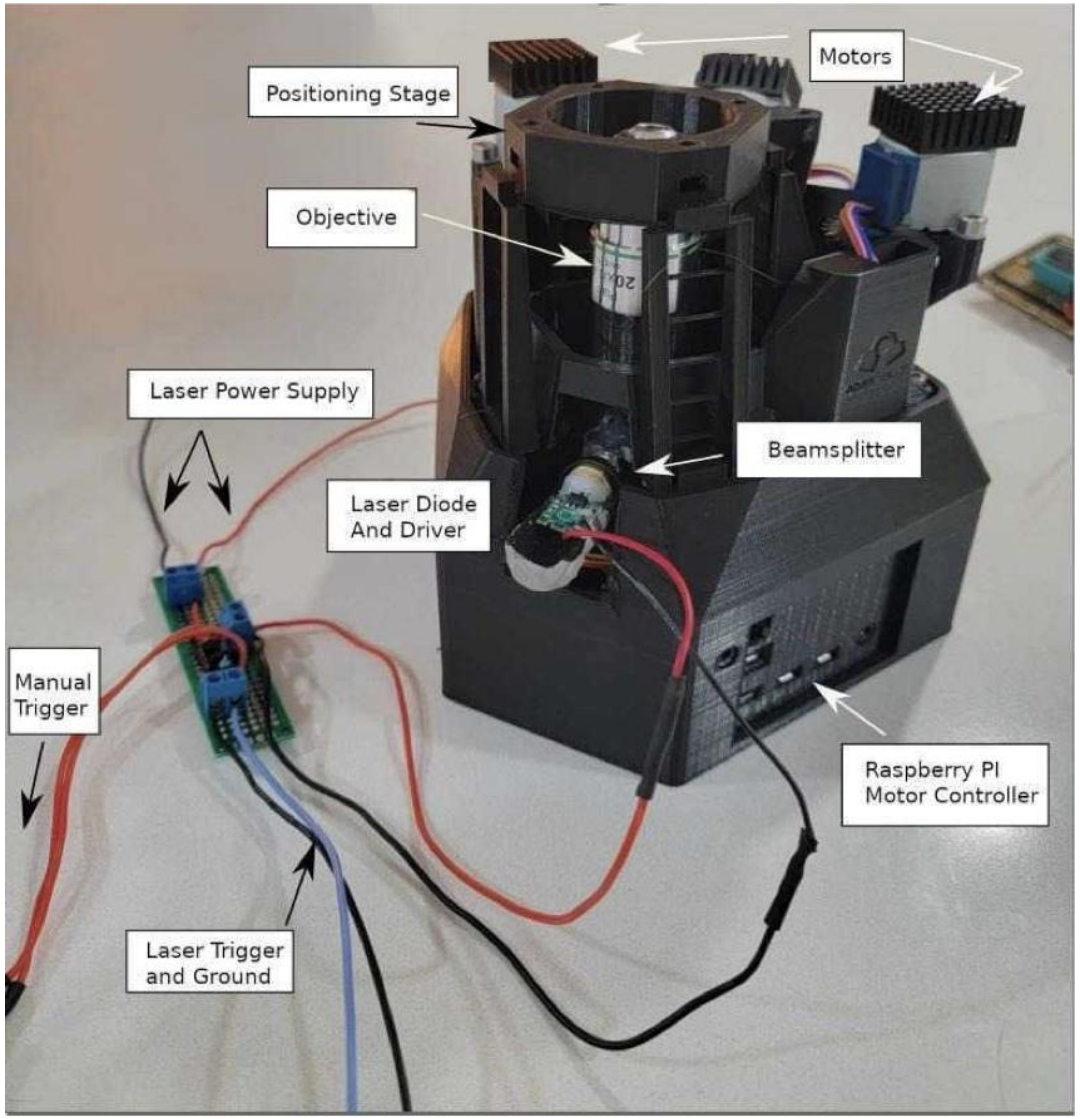




"Sometimes moving backwards is forwards, forwards is backwards, and none can be positive" – Casey Repp

Component Breakdown





"You spend 3 months chewing glass…just to arrive at how to use hot glue, to solve the problem" – Chas Becht

But does it work?

FIRE ZE LASERS!!!

THE END.

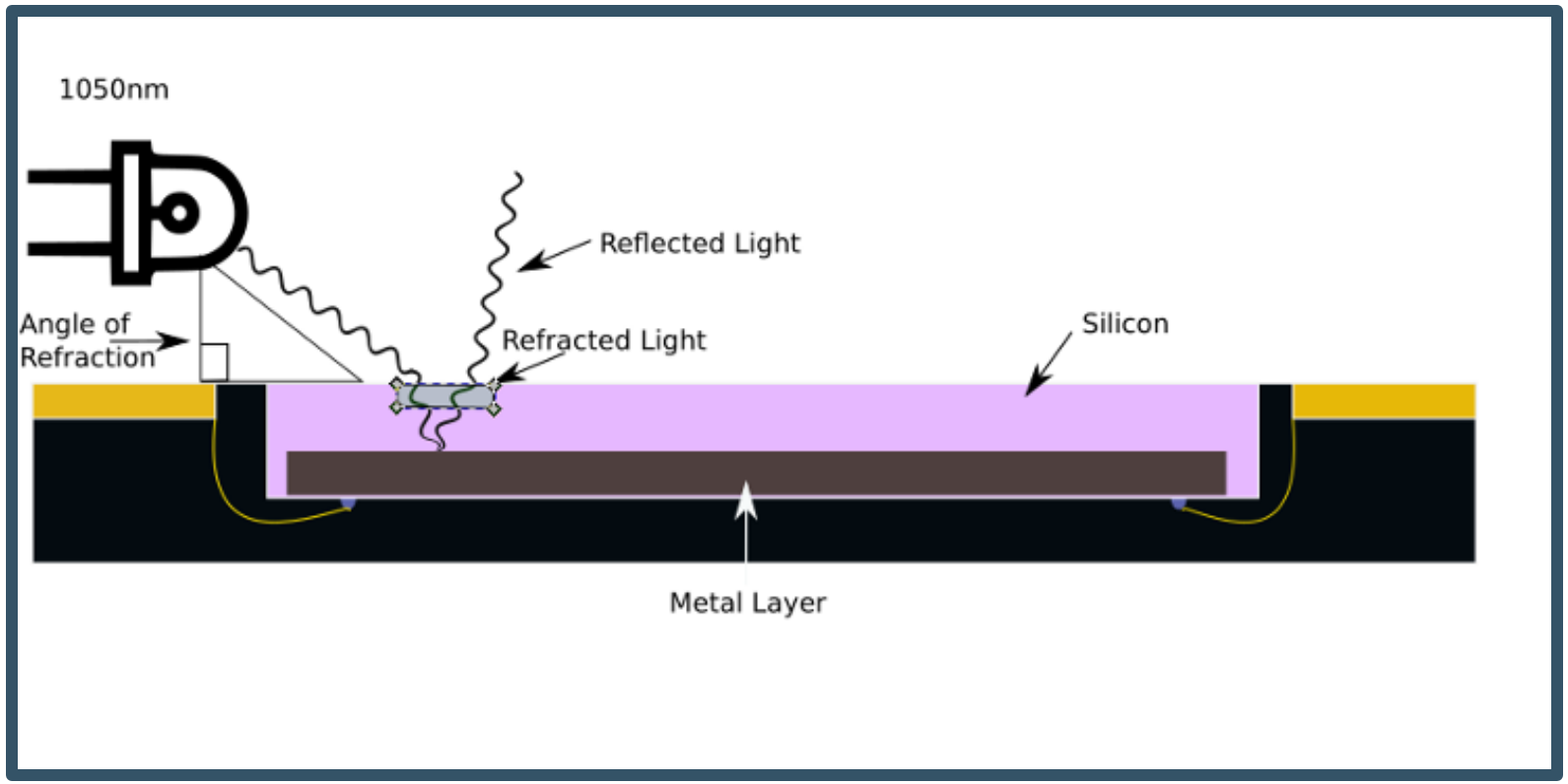
?


AND NOW FOR SOMETHING
COMPLETELY DIFFERENT

Infra-Red, In-Situ Inspection of Silicon

I.R.I.S.

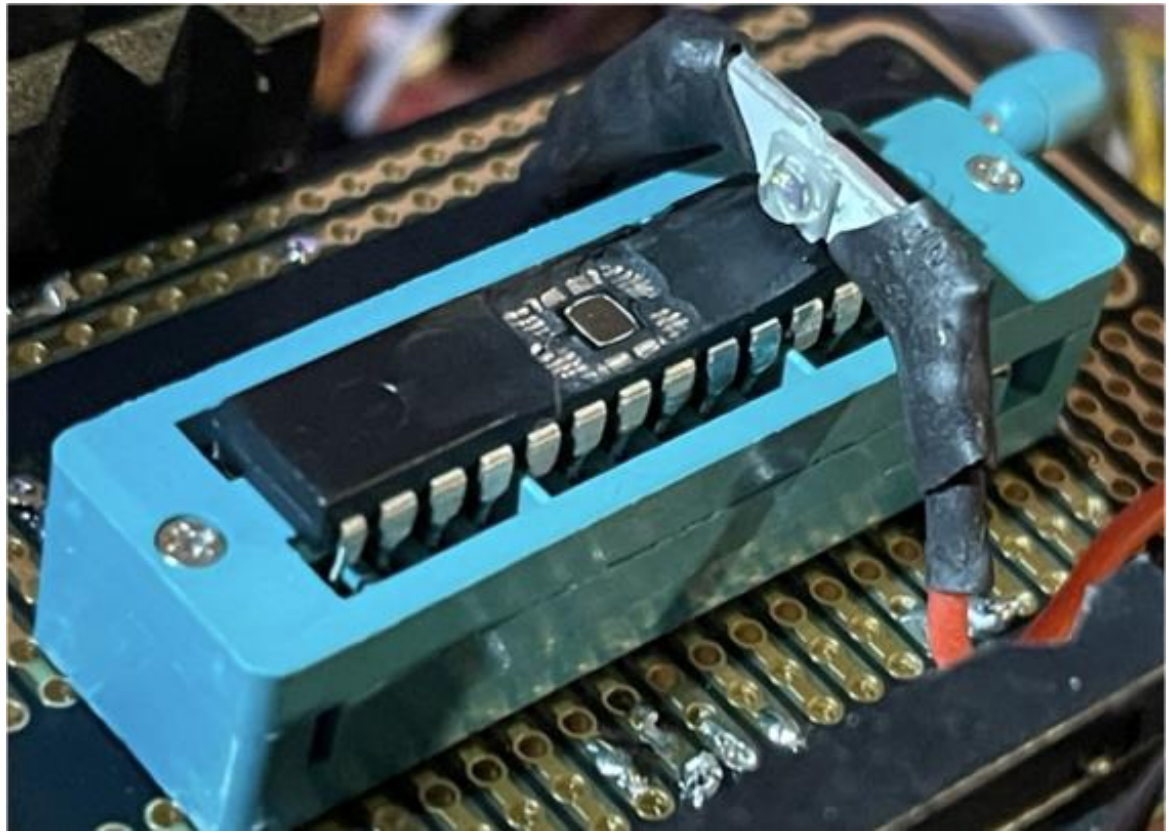
Visual Laser Targeting



1050nm Light on a "800nm" sensor

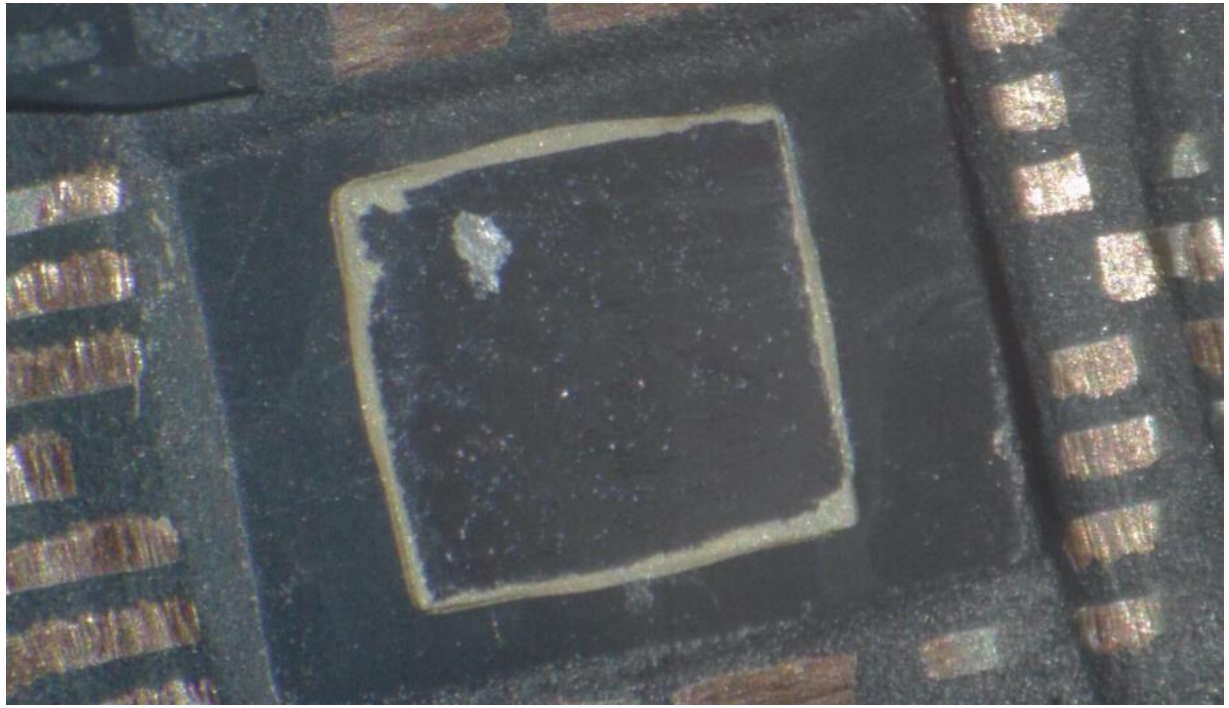
RayV + I.R.I.S.

"Visible Light Camera"



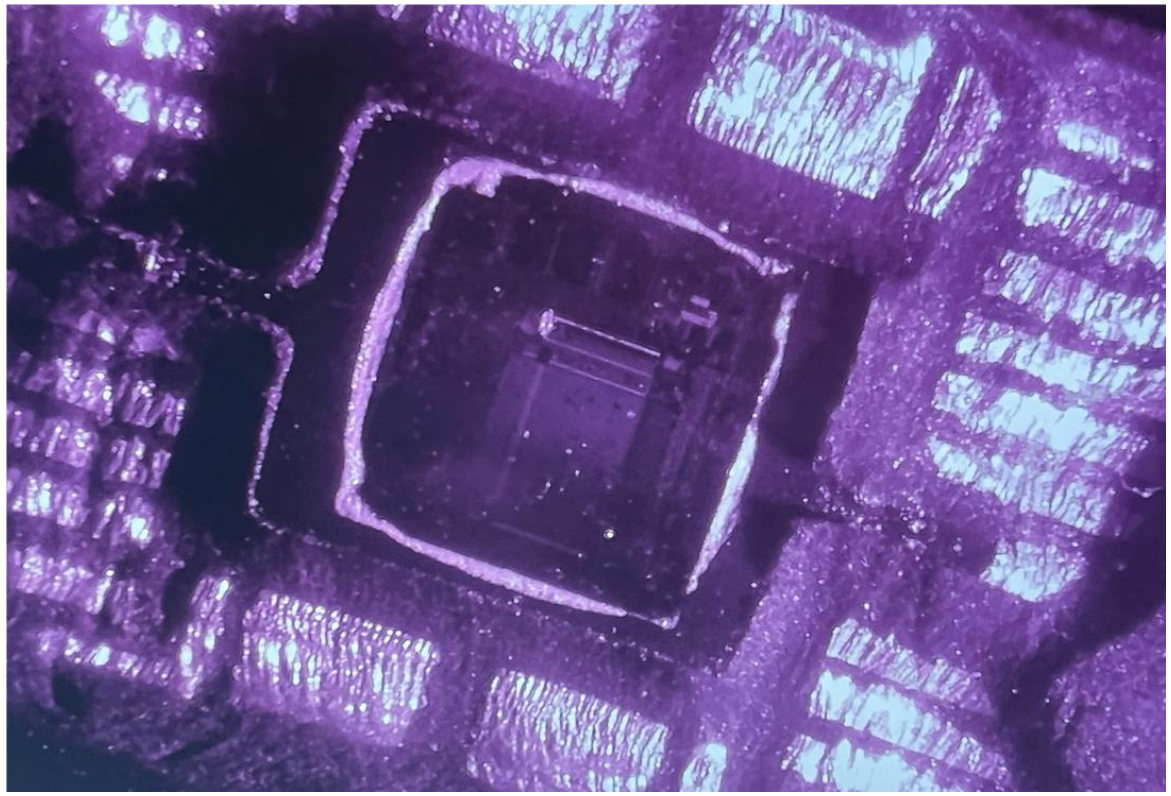
RayV + I.R.I.S.

Visible Spectrum



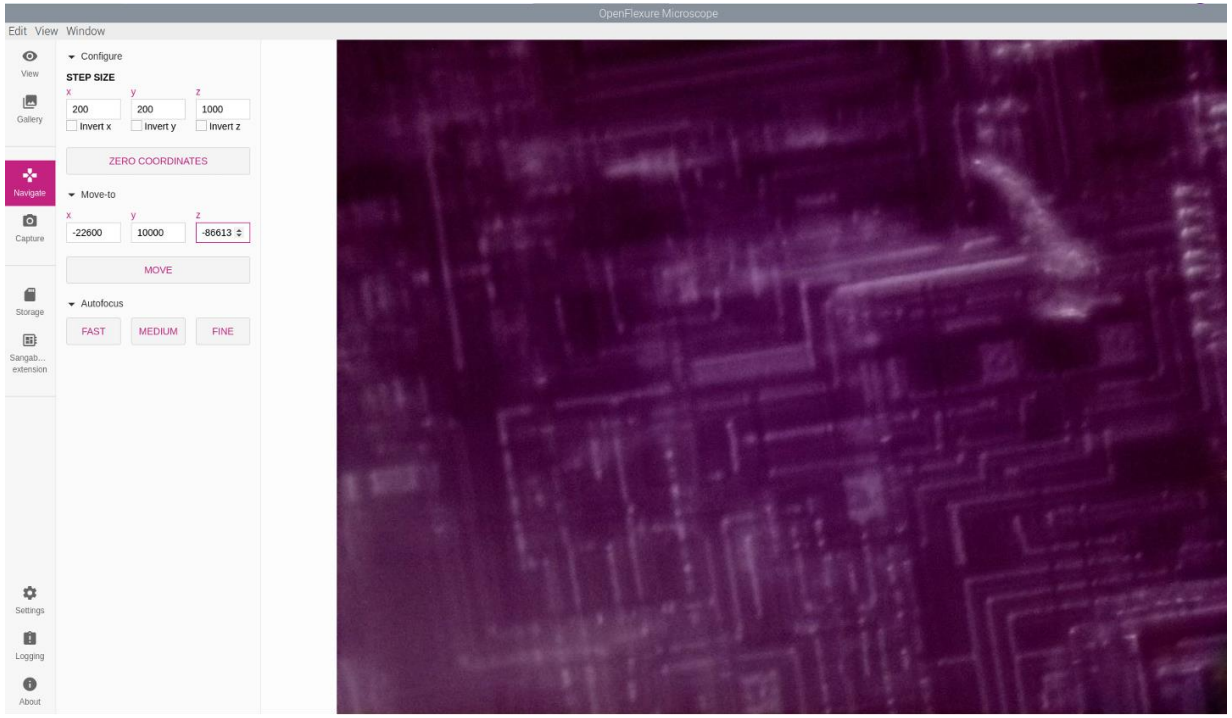
"How are we meant to see invisible light? ...With our invisible light camera"
– Team LOREM

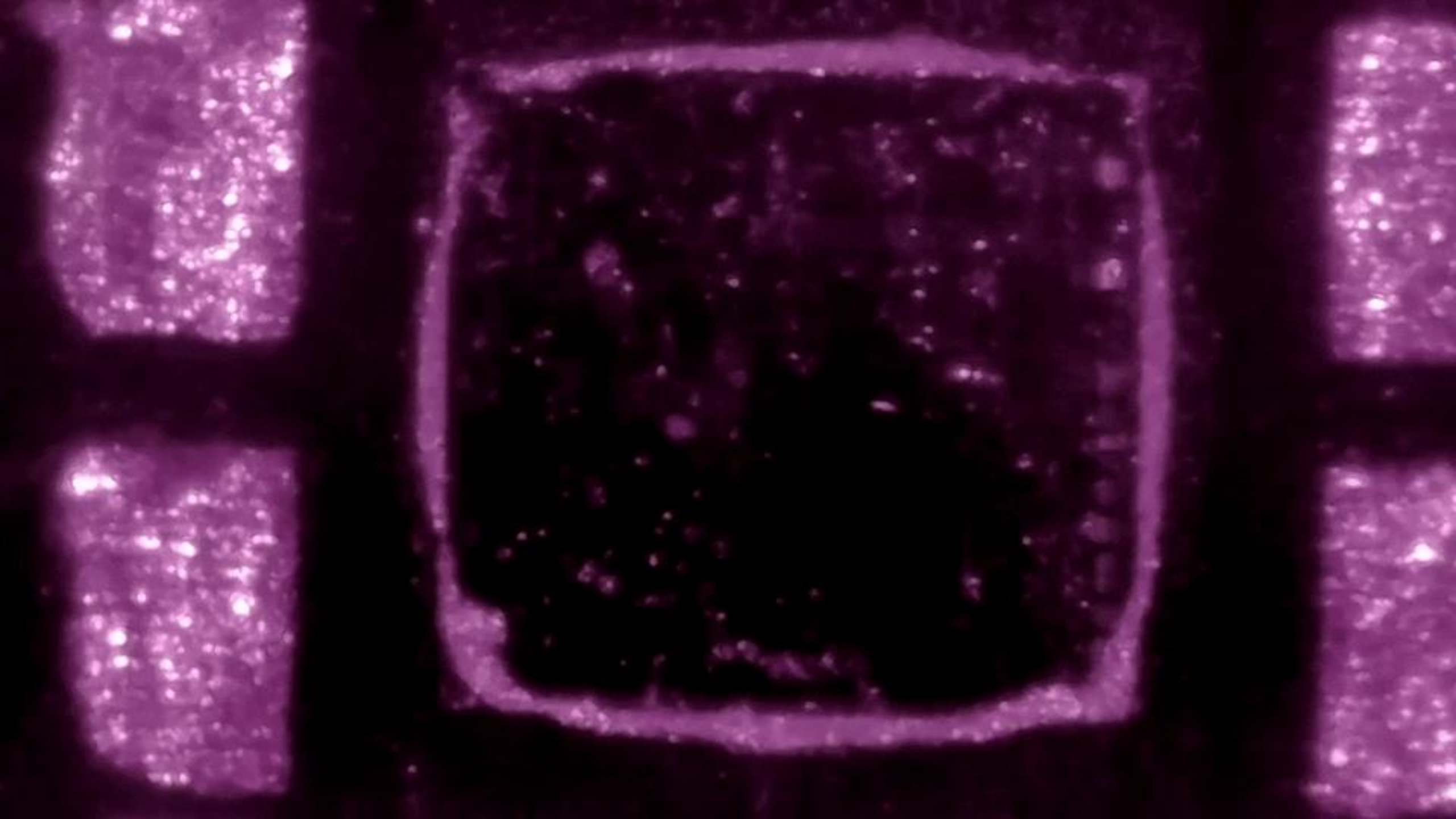
"Invisible Light Camera"



Infared Spectrum

Zoomed In





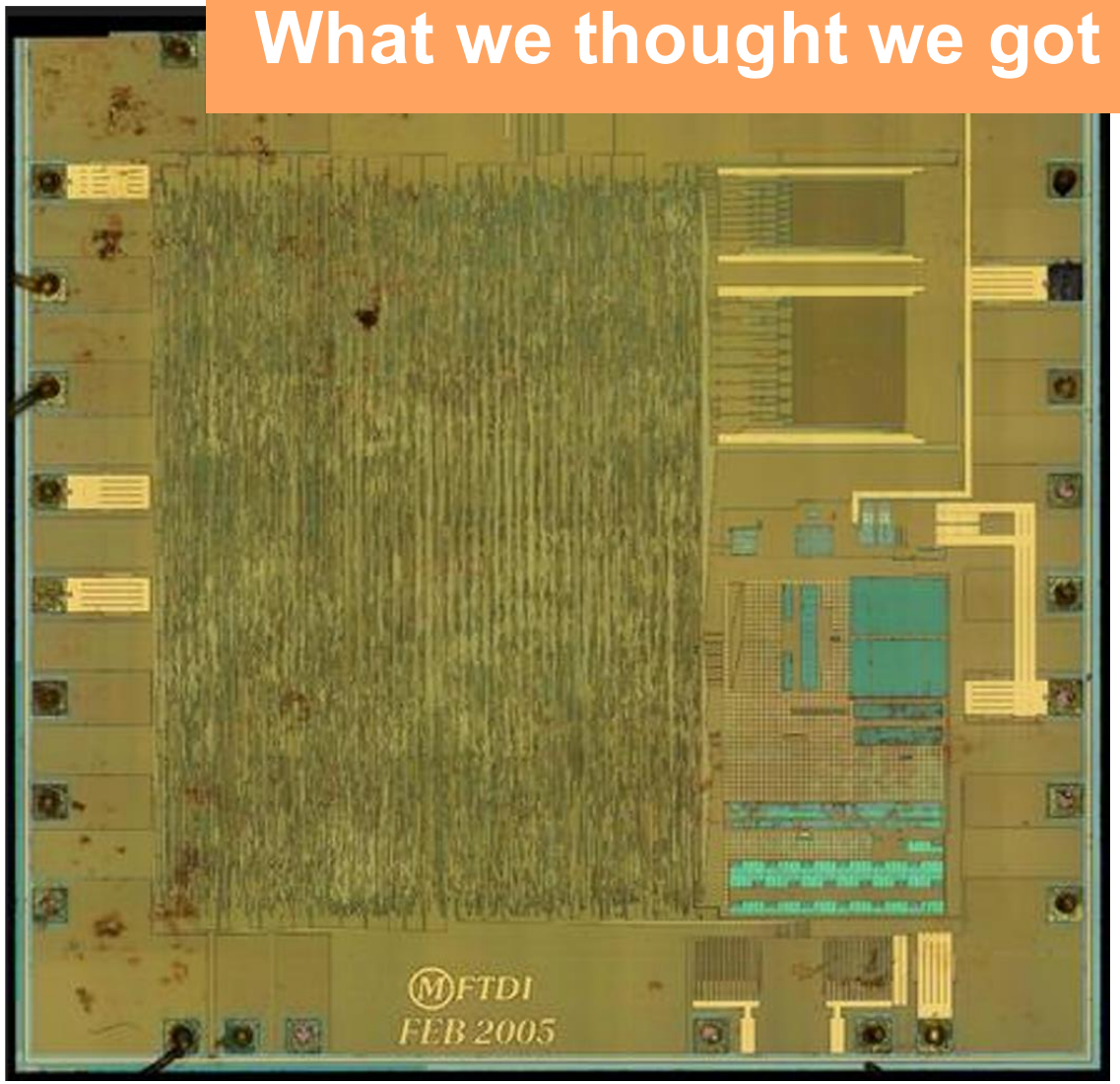
But wait, there’s more!

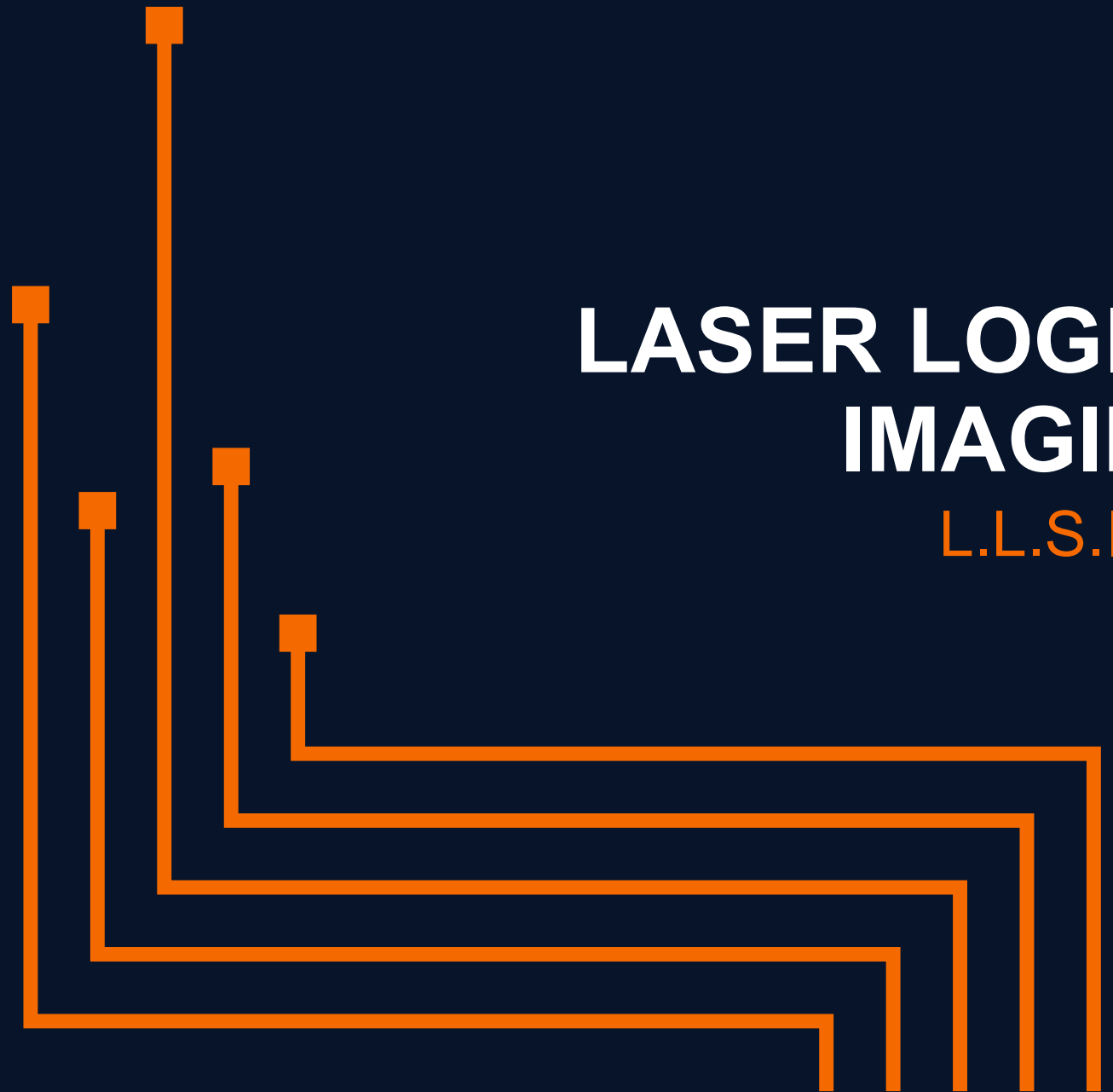
Happy Accidents can happen

FT232r “Alternative”

What we actually got

What we thought we got



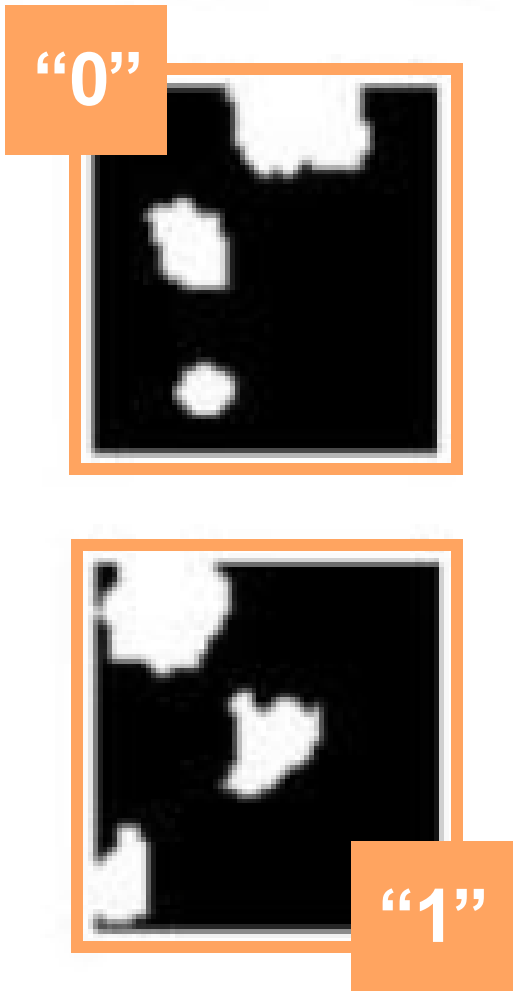


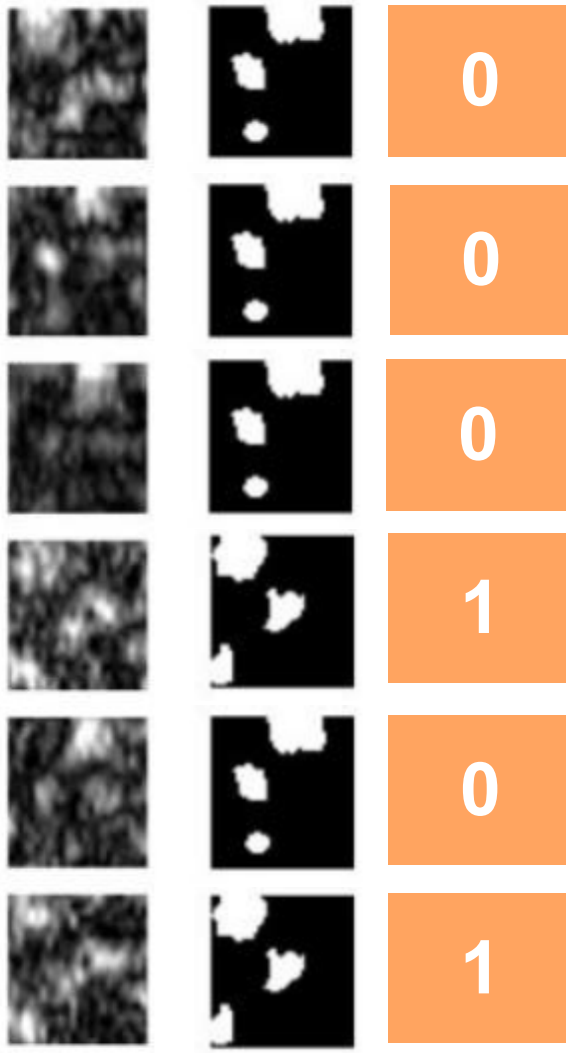
LASER LOGIC STATE IMAGING

L.L.S.I.

What, and Why?

- Imaging dynamic data
- Transistors are arranged in gates
- Gate states determine as a cluster what is a “**1**” and what is a “**0**”
- Each chip is different, so you need to map a victim before Side Channel Analysis (SCA)

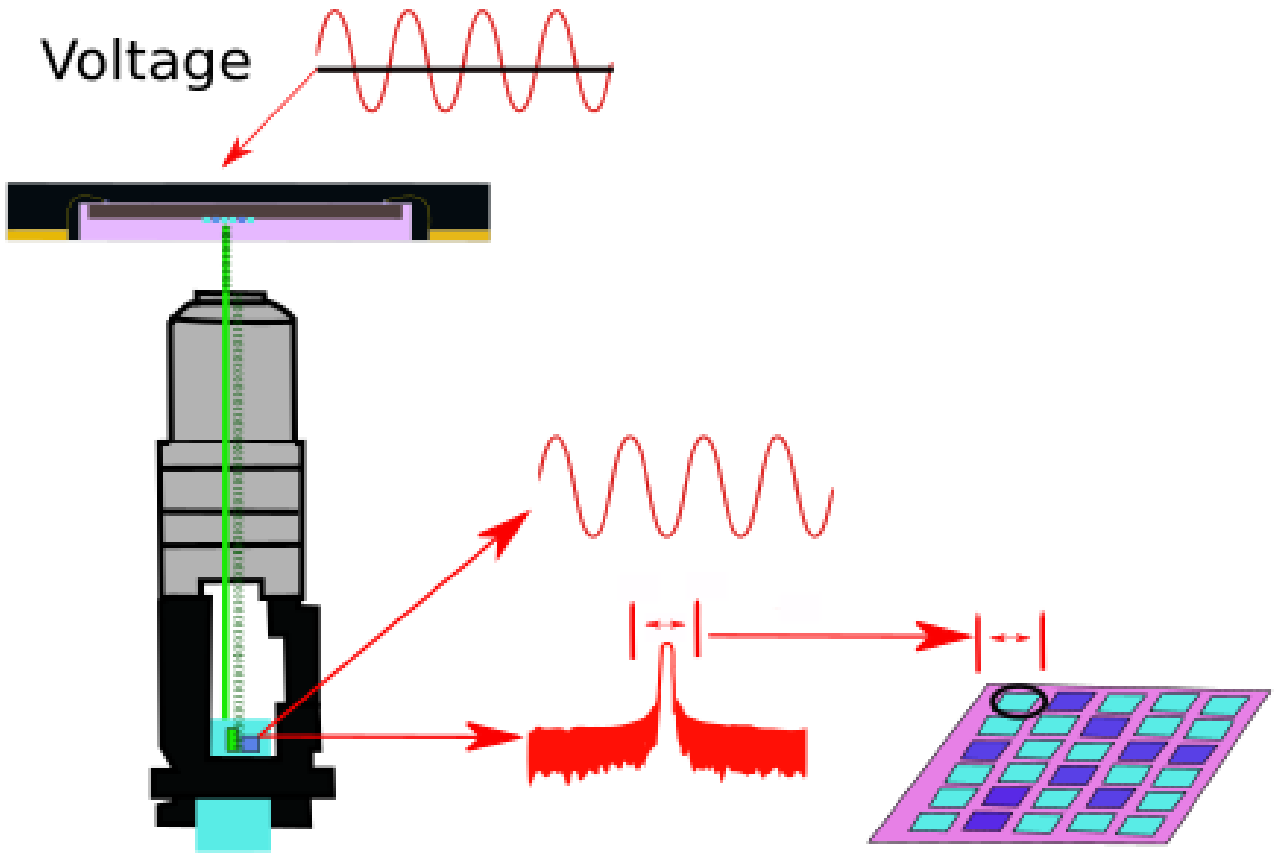




I tried to read my computer's mind, but it was all in binary. I think it's plotting against me, but I can’t decode its plans.

How?

- Changes in energy, change the absorption rate of silicon
- Electro-Optical Frequency Mapping (EoFM) does this as chip runs
- The modulated signal will travel through the powered transistors



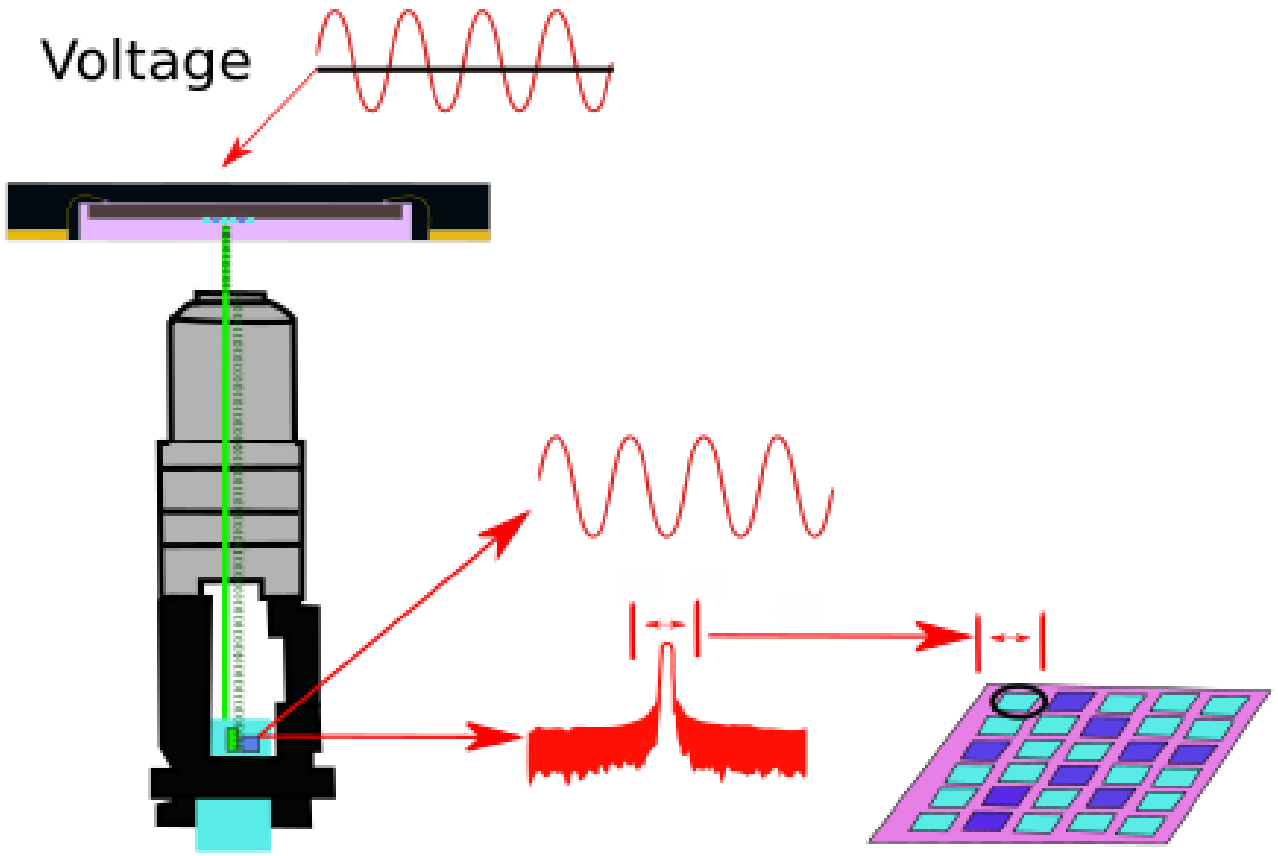
I tried to read my computer's mind, but it was all in binary. I think it's plotting against me, but I can't decode its plans.

Operation: Over Achiever

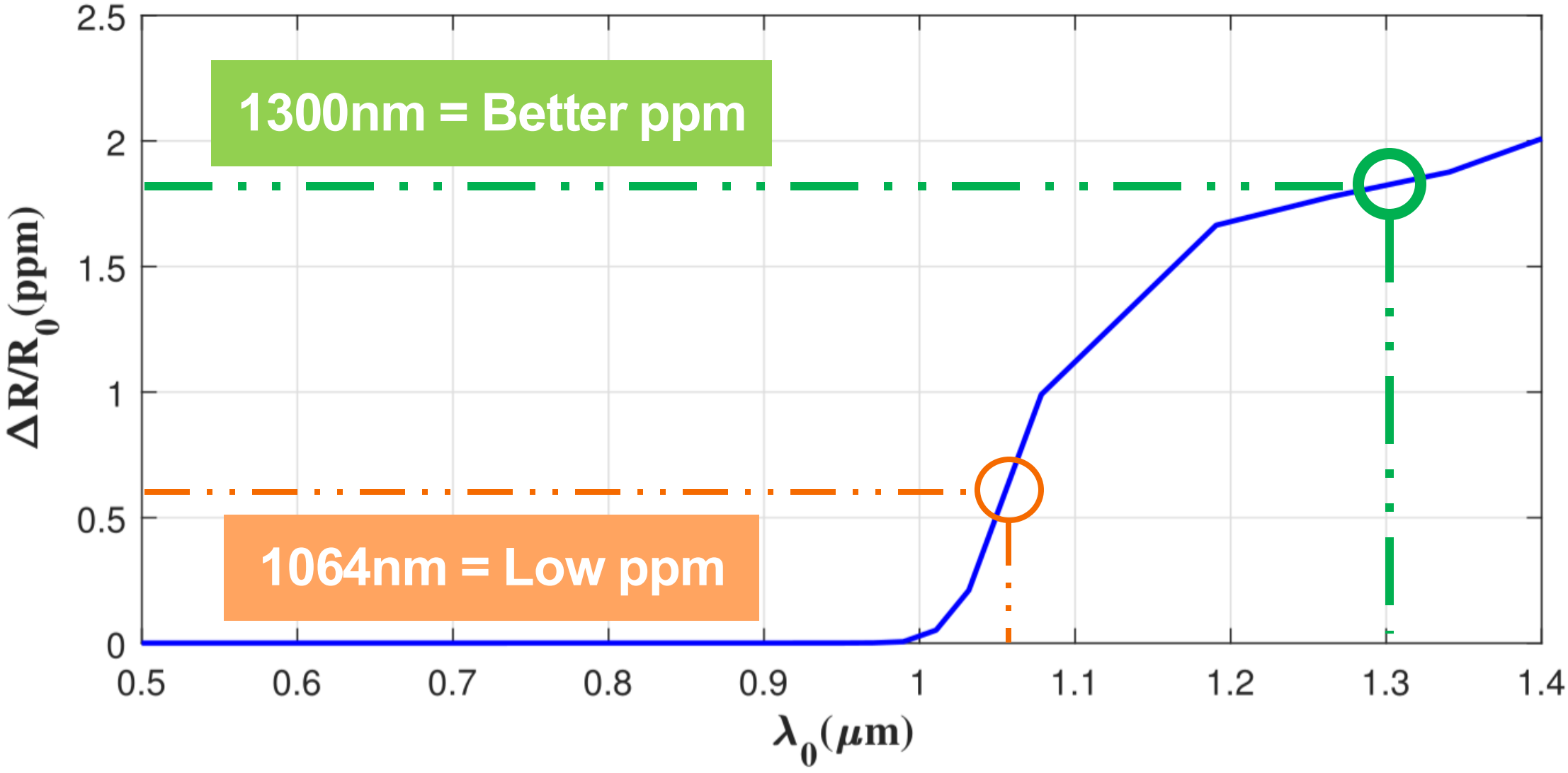
Because telling a hacker “no” is the fastest route to hyper-productivity

LLSI: The Essentials

- Target chip modulation
- A laser that can achieve penetration and reflection
- A laser sensor
- Smooth laser panning
- Signal & noise parsing
- Human Readability

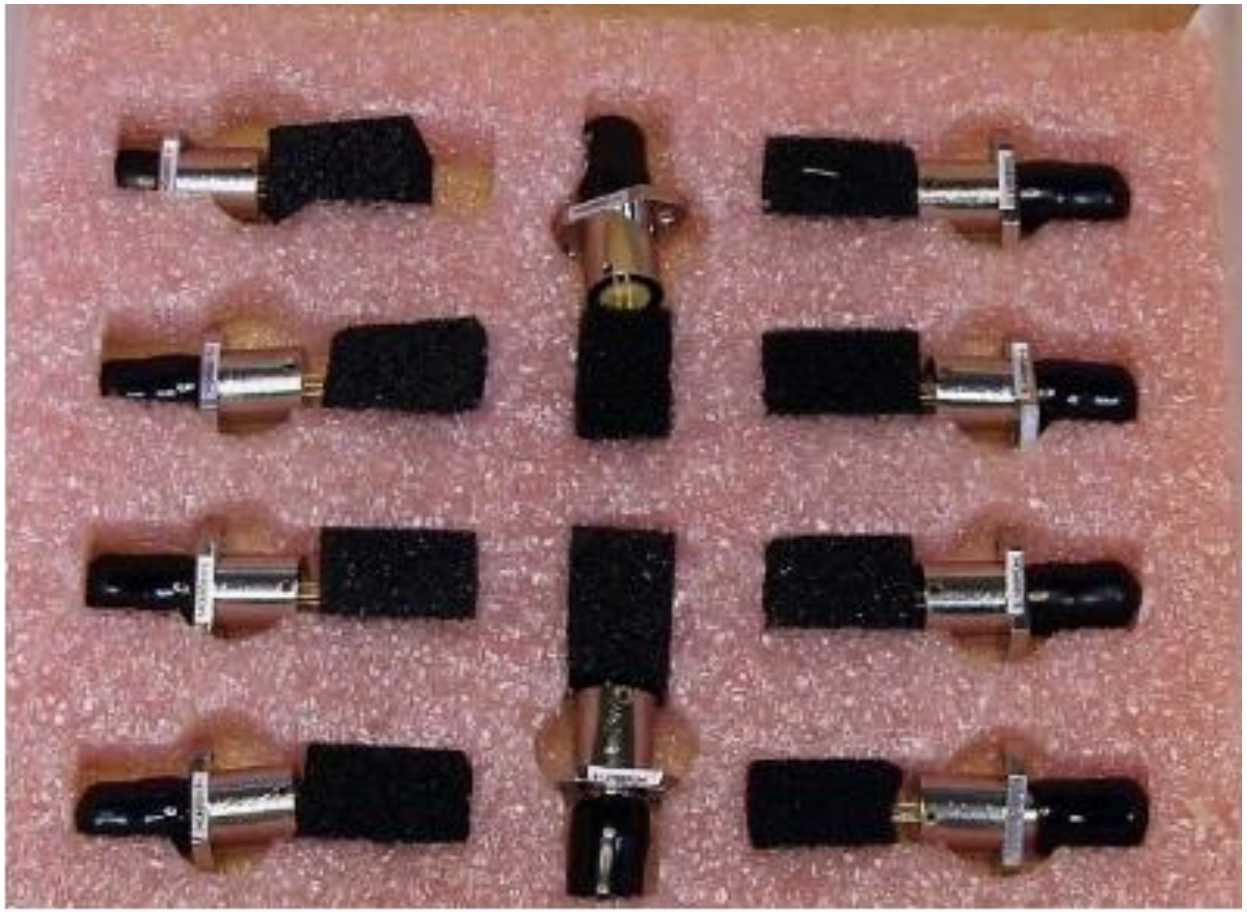


Which Laser?


1300nm = Better ppm
1064nm = Low ppm
$\Delta R/R_0$(ppm)
$\lambda_0(\mu m)$
2.5
2
1.5
1
0.5
0
0.5
0.6
0.7
0.8
0.9
1
1.1
1.2
1.3
1.4

Laser Self-Regulation

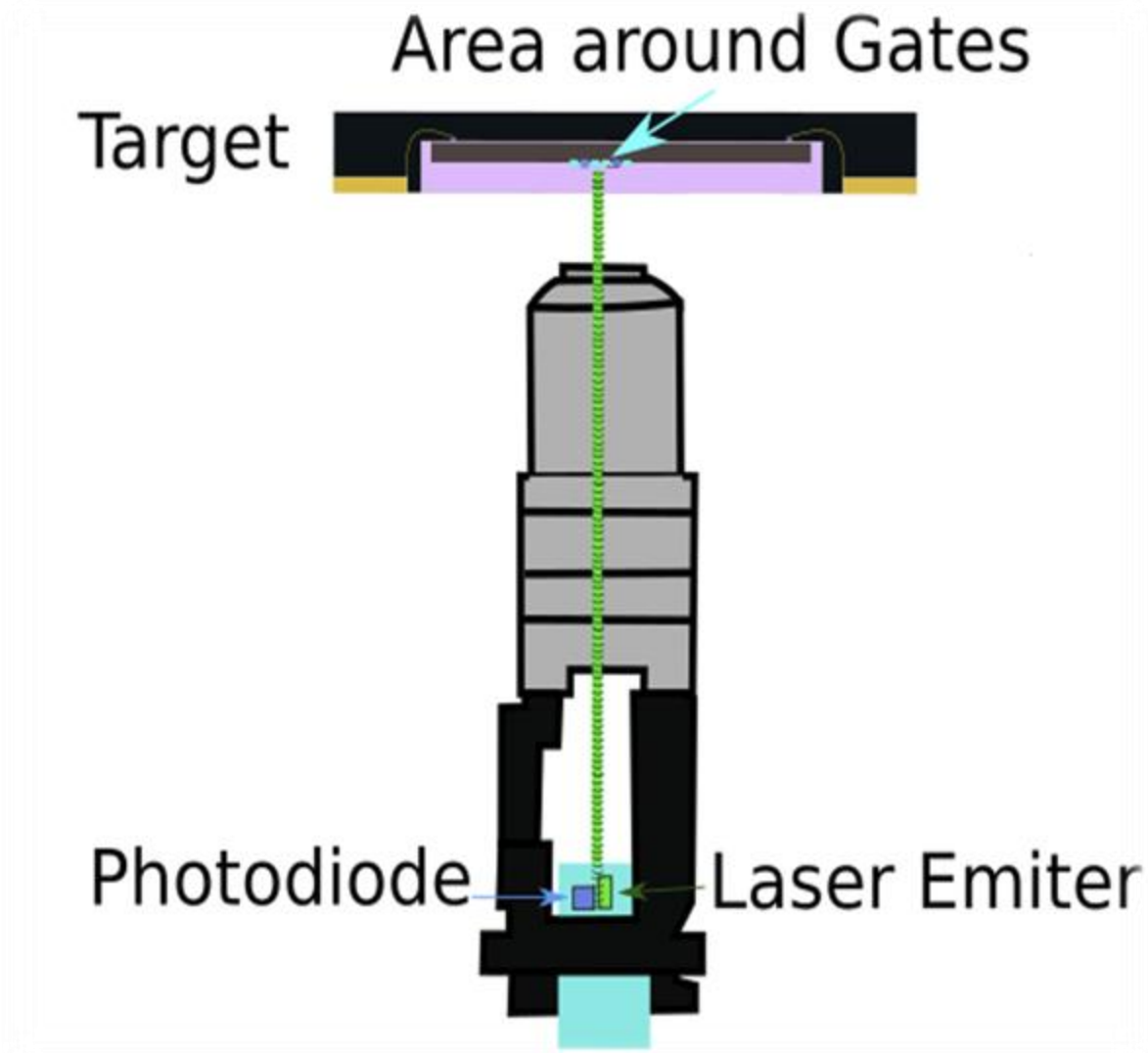
- Lasers come with their own sensor for self-regulation
- 6 Dollar 1300nm lasers WITH a photodiode so it can pull the results independently
- Two birds, one stone



Self Mixing Interferometer

- We can use the **photodiode** in the laser to record how much was reflected

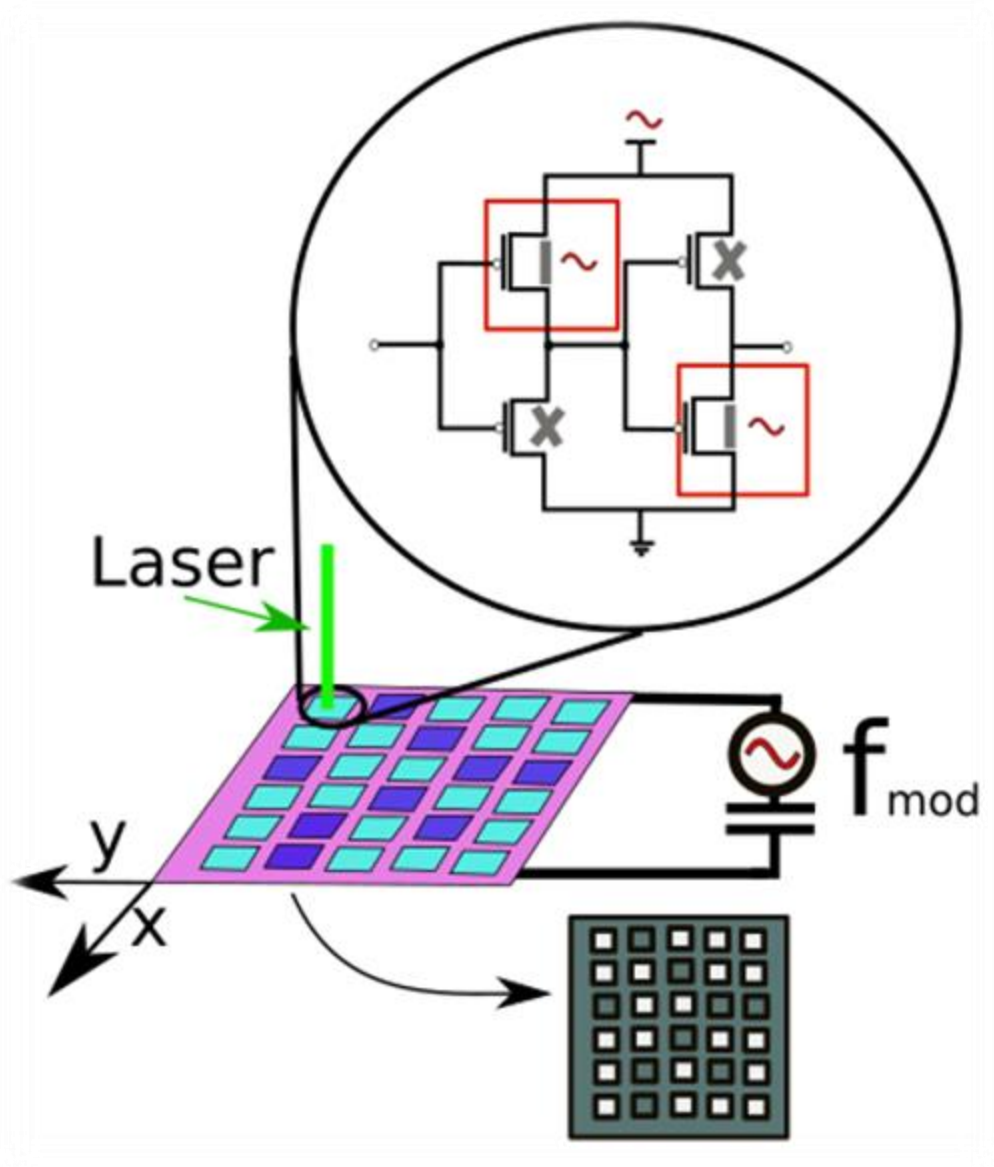
- If it can measure changes equal to the size of its wavelength, it can also **measure variations** in silicon absorption



I tried to measure my iq with a self mixing Interferometer, but it kept saying "error: object too dim".

Putting it all together

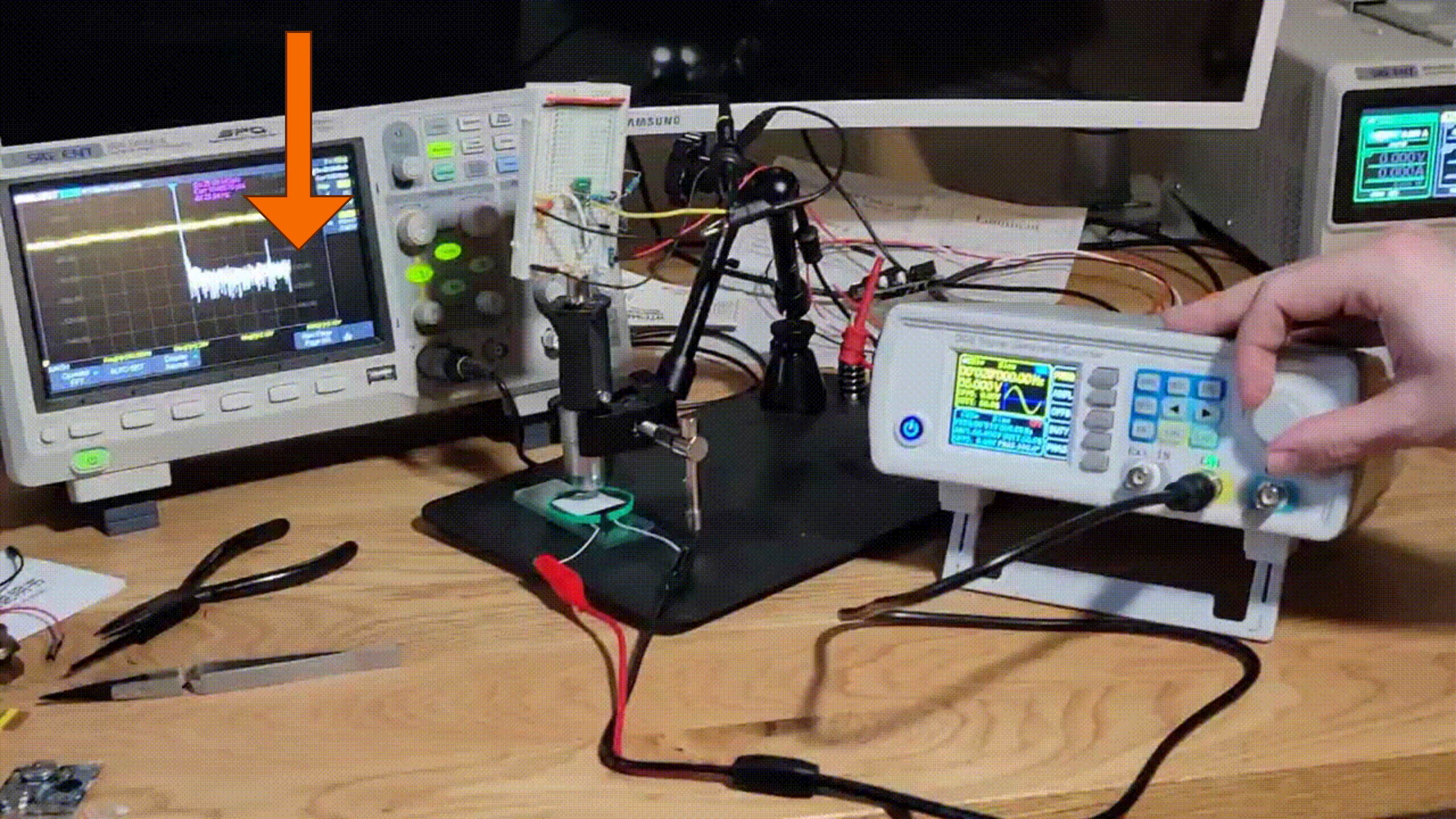
- Pause instructions and memory in the transistors
- Send a signal through the active transistors
- Activate laser beam
- Read the sent signal through the beam's reflection

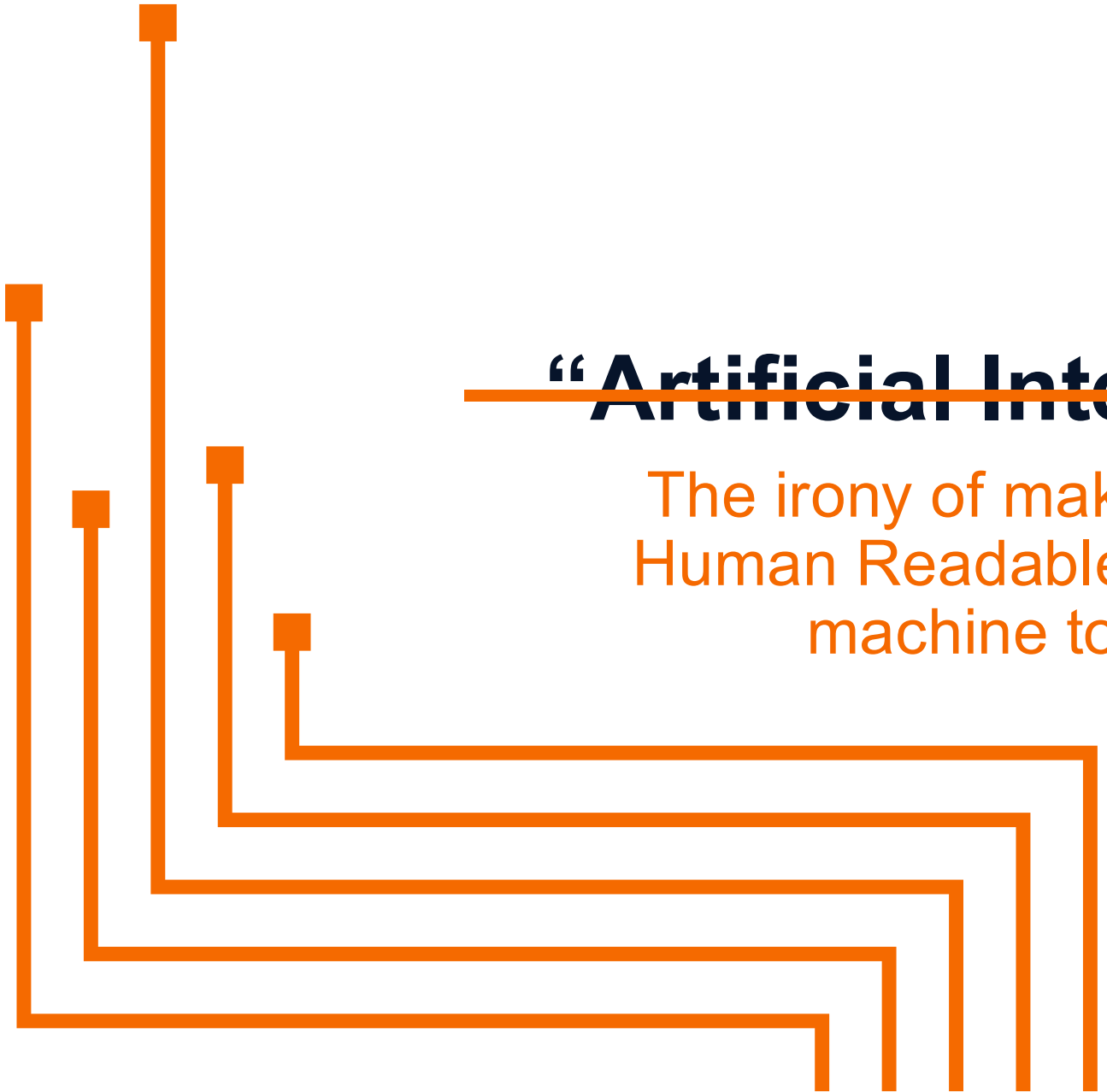


How does a laser feel after a long day of logic state imaging? Exhausted, because it's been working its bits off.

But does it work?

FIRE ZE LASERS!!! ….AGAIN!





~~“Artificial Intelligence”~~

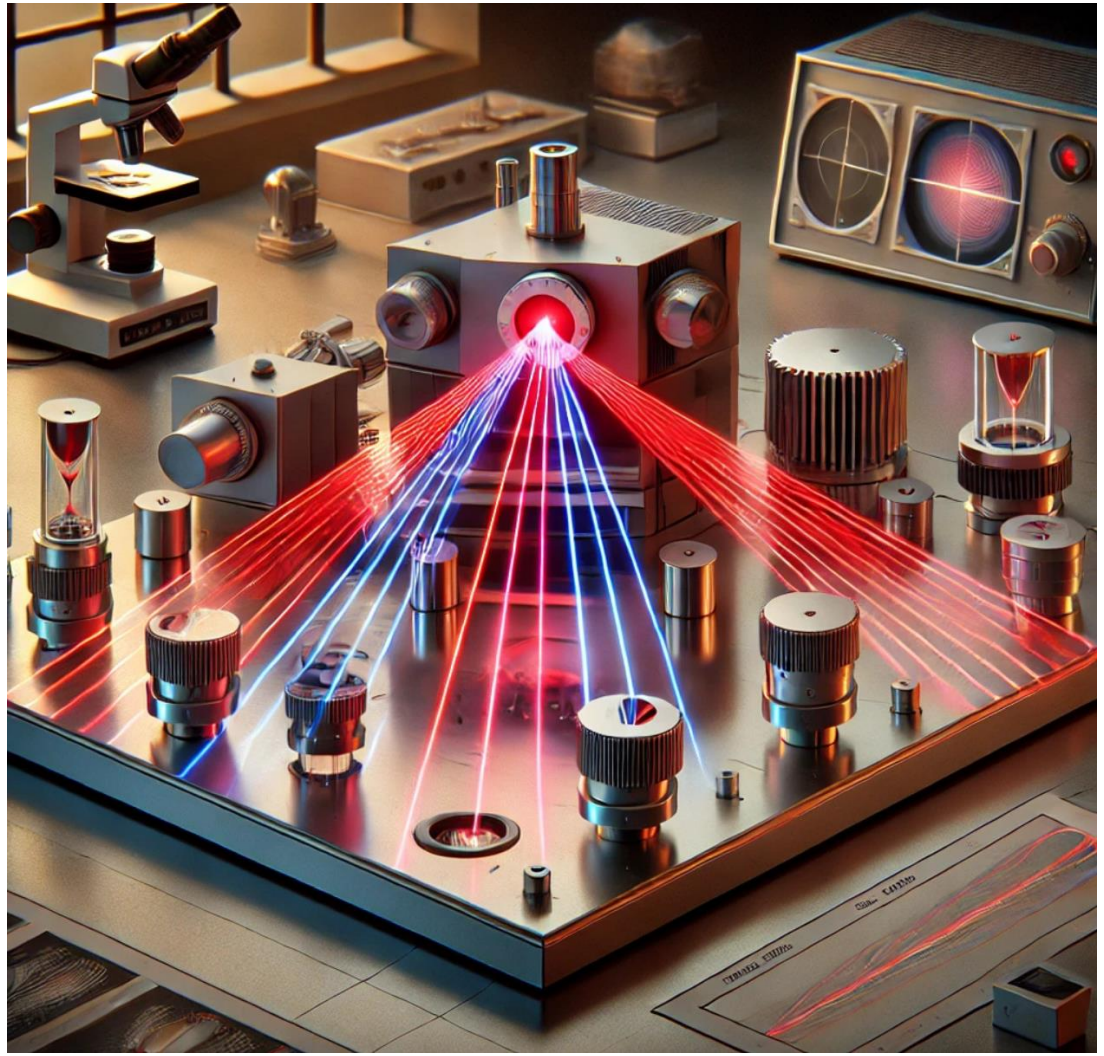
The irony of making signals Human Readable by using a machine to read

Machine Learning

Statistical Analysis using Convoluted Neural Nets

Statistical Matrices & Math

- The signals received from an LLSI setup are pretty abstract
- The abstraction is also specific to the memory being read: not all transistors are created the same
- We need a model that is trained to perform the analysis, so we don’t jump off a cliff

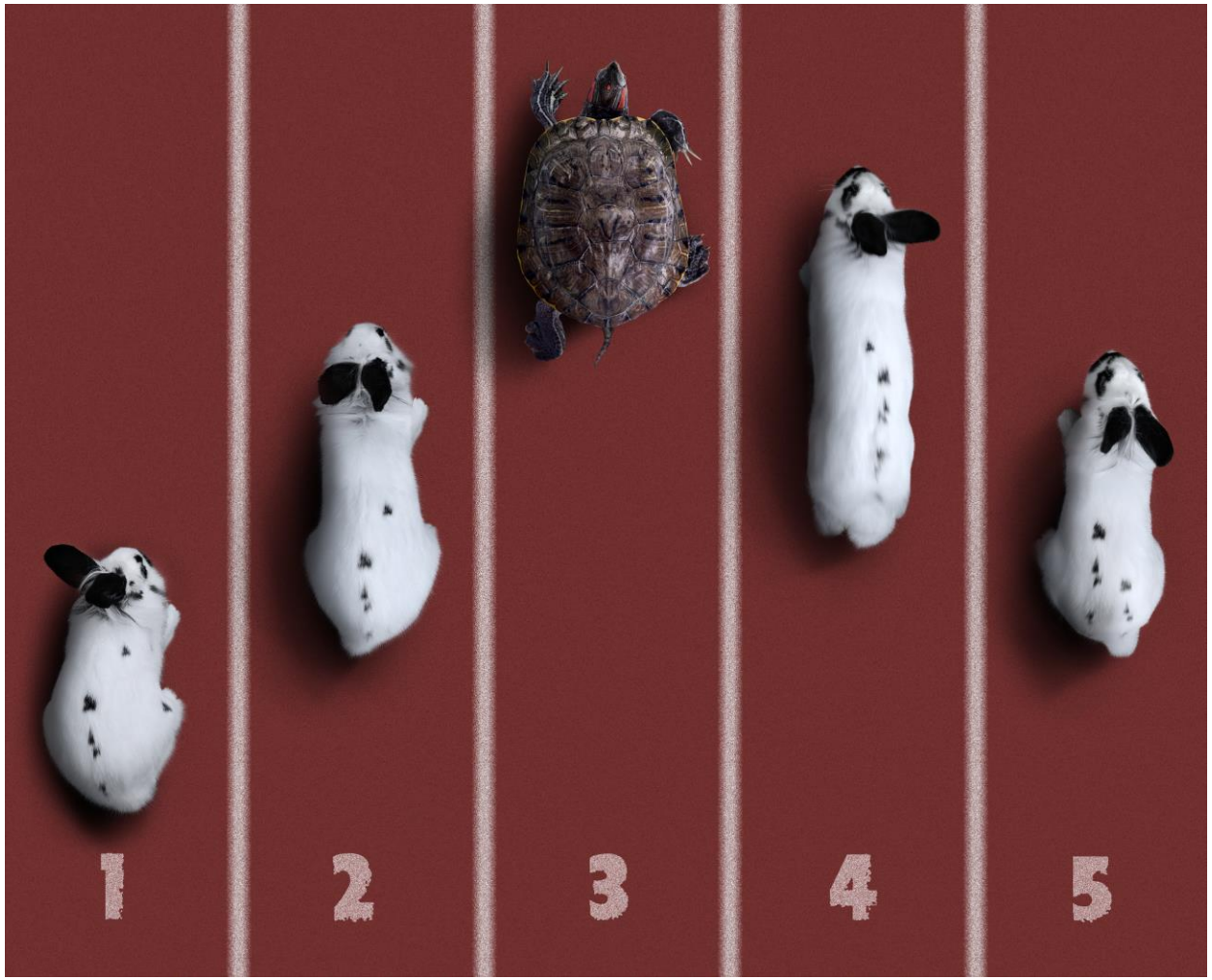


ChatGPT Prompt: Draw me a picture of a laser interferometer

I’m not saying patch is old, but his AI/ML thesis was written with pencil and paper

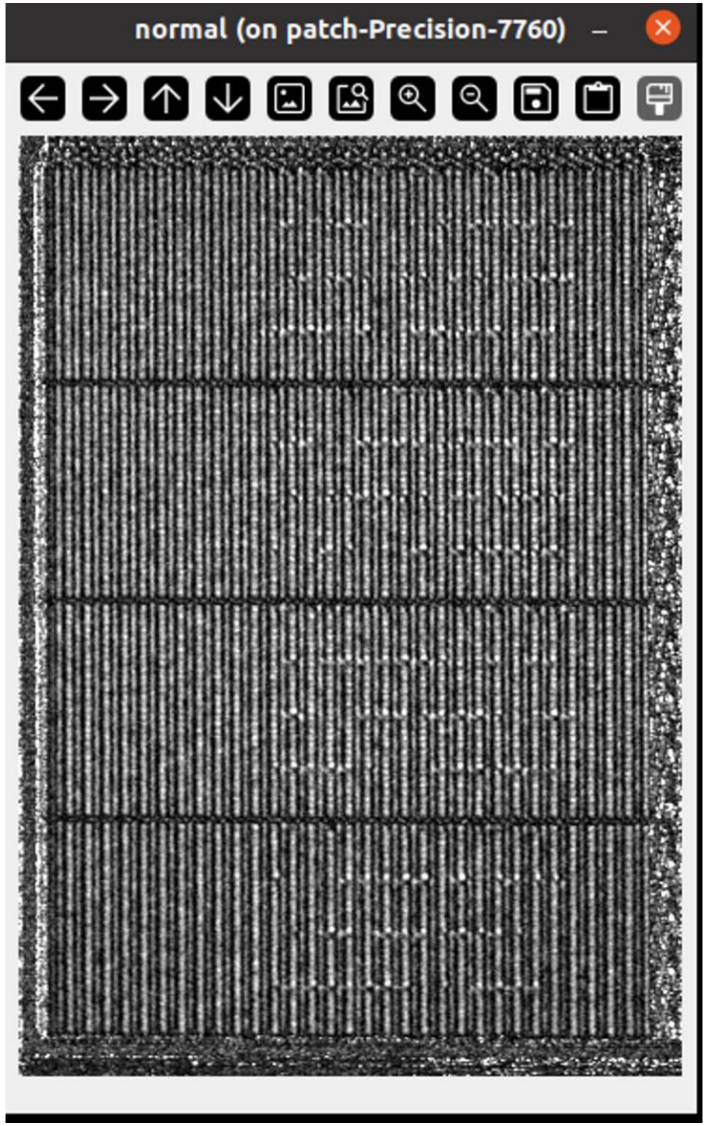
BlackHat has deadlines

- The process to get a working laser microscope to scan an object is slow
- The process to design a low noise, band pass filter to detect 1ppm is slow
- Combining an active LLSI and LSM to train a model, is really slow



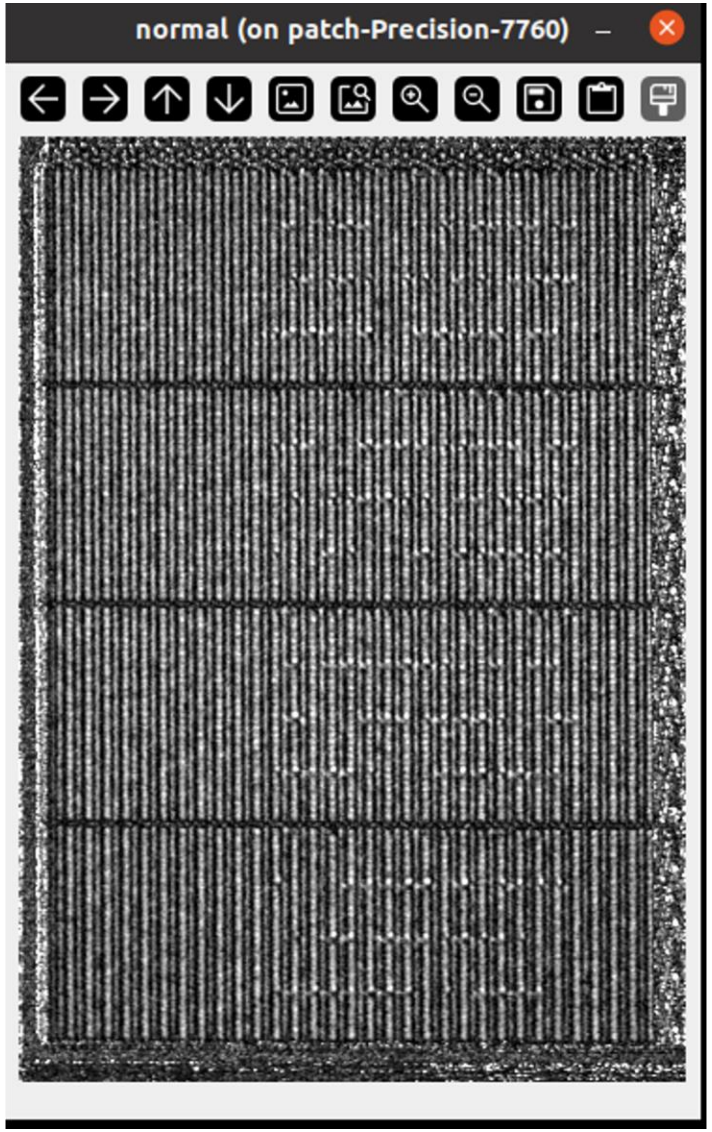
Training with Published Data

- Target was a 512-bit key, stored on data that was zeroed out
- 430 images non-random
- 820 images random
- Faster to train & demonstrate
- We like life



Signal

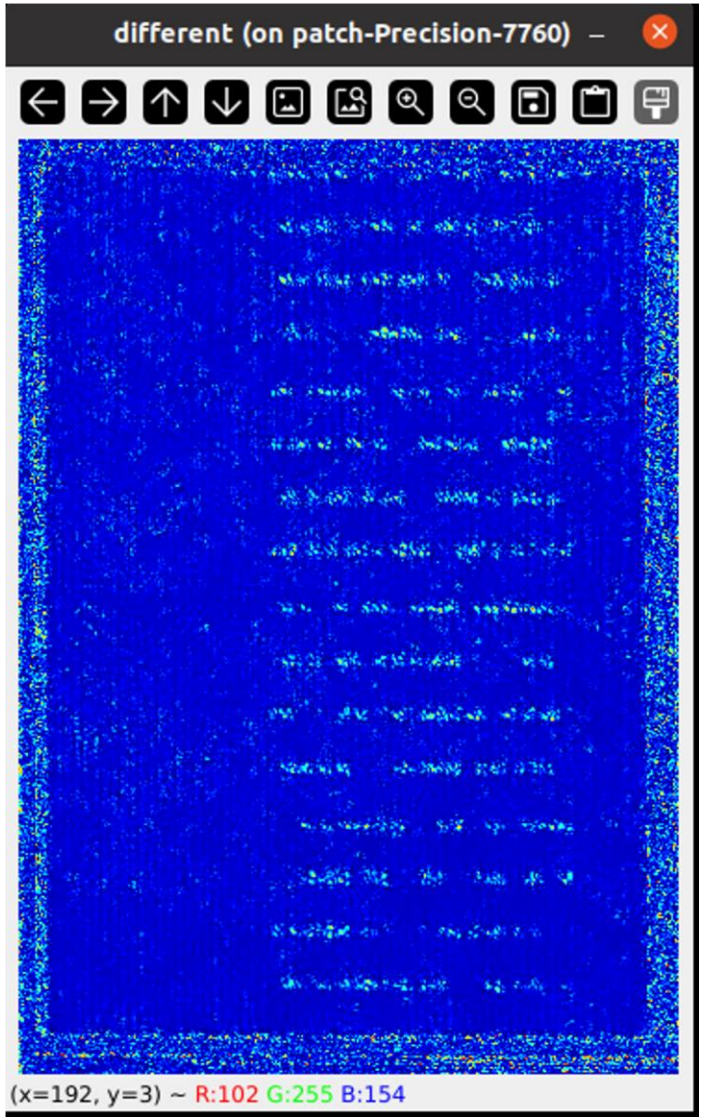
- The “dots” are the signal.
- This image has 512 bits programed
- This process will also work on the randomized images



I tried to have a deep conversation with my computer, but all I got was signal and noise. It was a real buzzkill

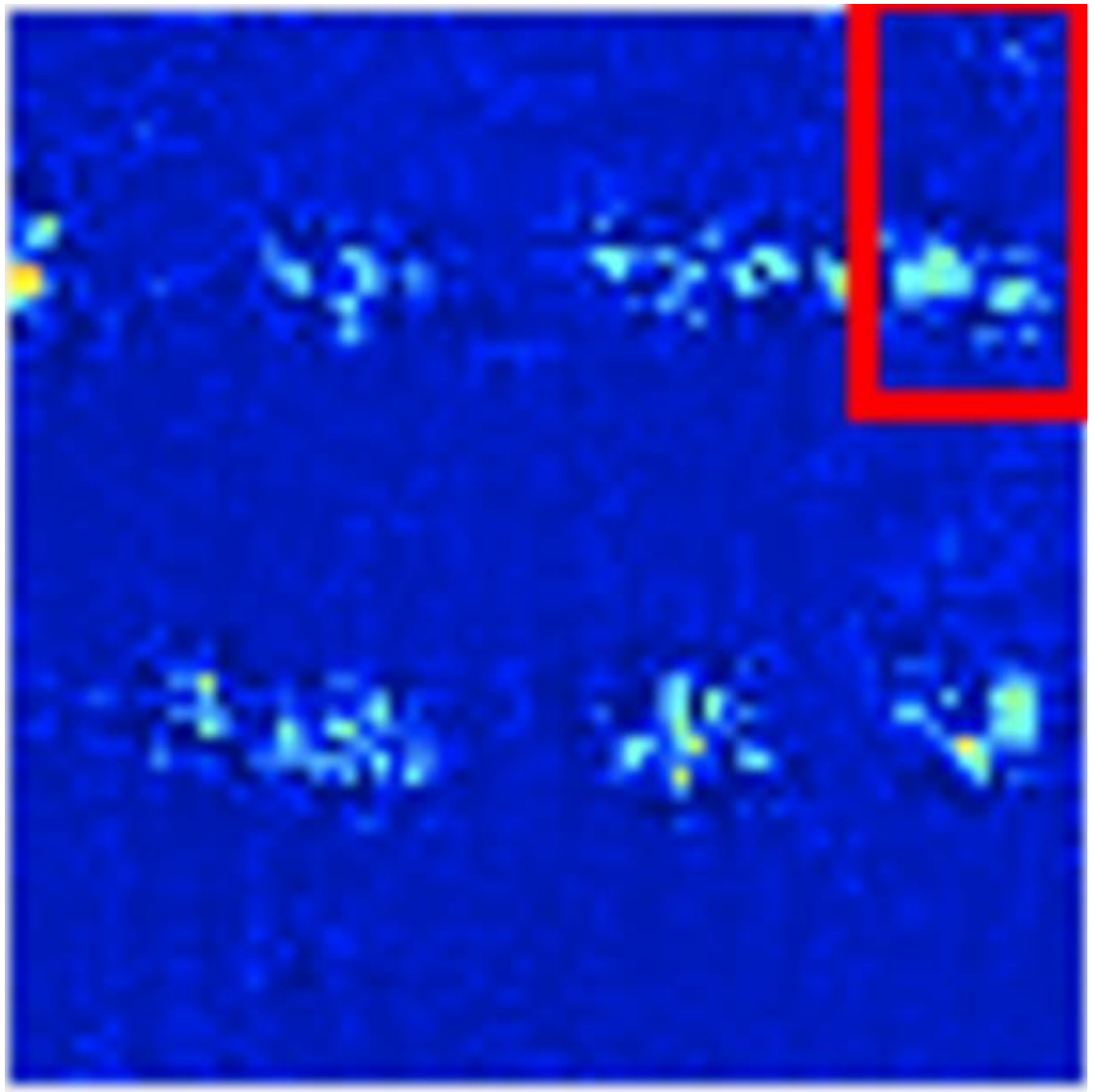
The data needs flair

- First, we need to make the data pop.
- It needs a new wardrobe; blue is always in style.
- Let's subtract a random llsi image from it and put the results in the blue channel
- Also, patch can see blue better than other colors



512 bits on the flash

- Isn't that better…now how is this laid out.
- There are 46 memory sections, each section has a number of bytes, and the pattern is repeating.
- This is one section.
- The red square is a is data we are interested in

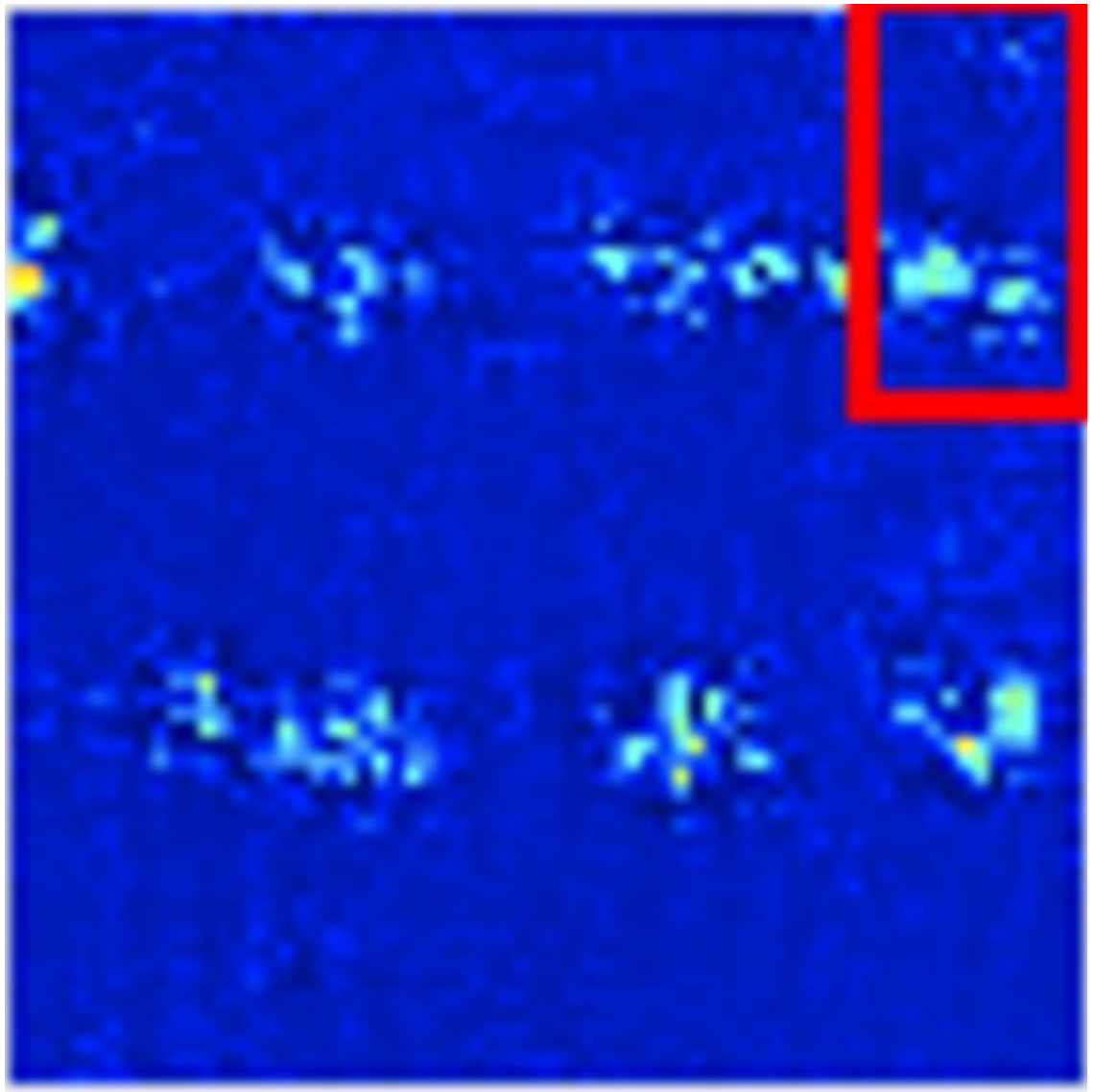


46 Memory Segments

- Each are laid out identically
- We can find which bits are in which block by choosing orthogonal binary values
- 1101011 vs 111011
- If you take absulte diff, you get

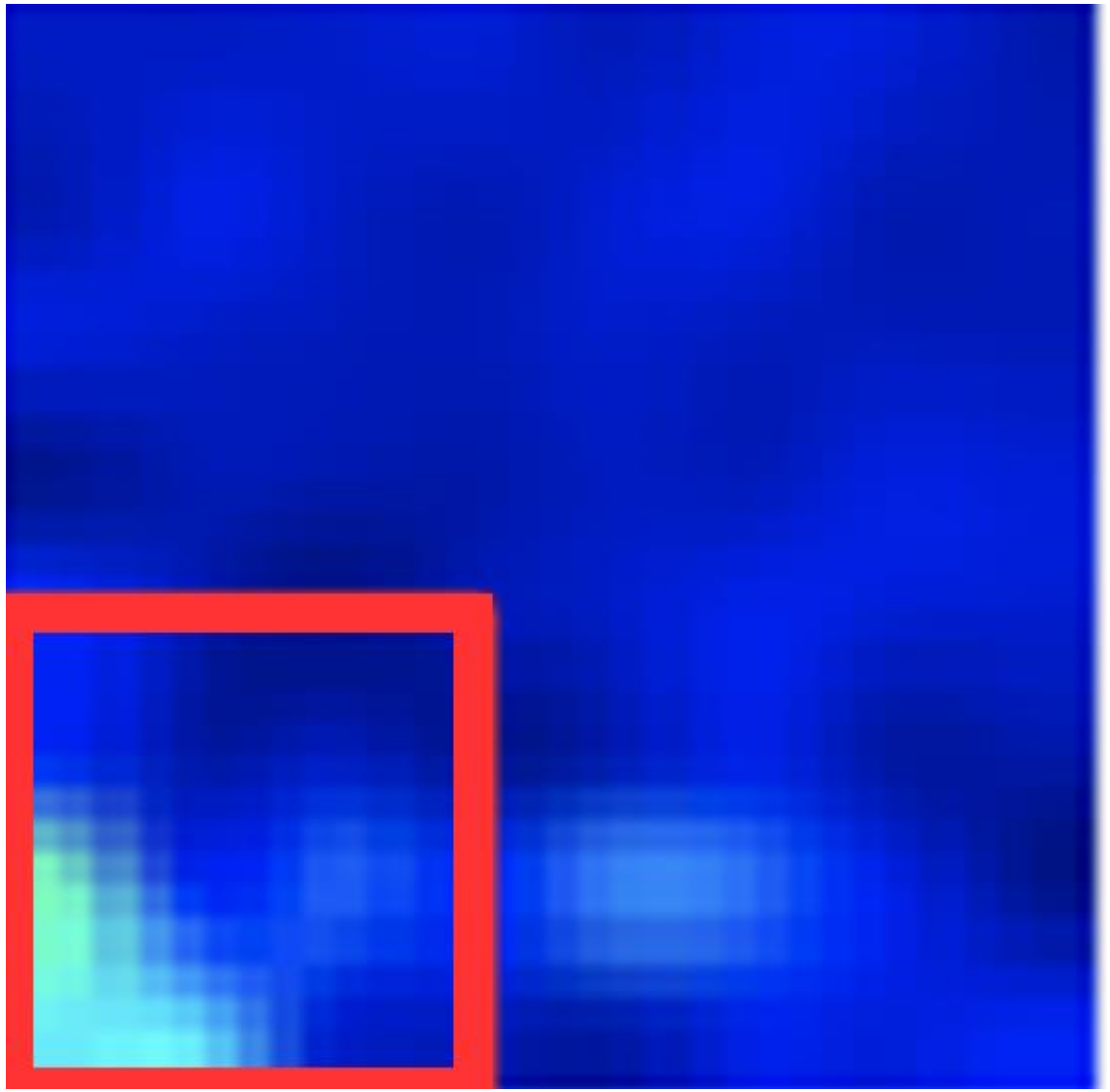
001000

- You still will not be able to read it, but see a change



Piece of eight

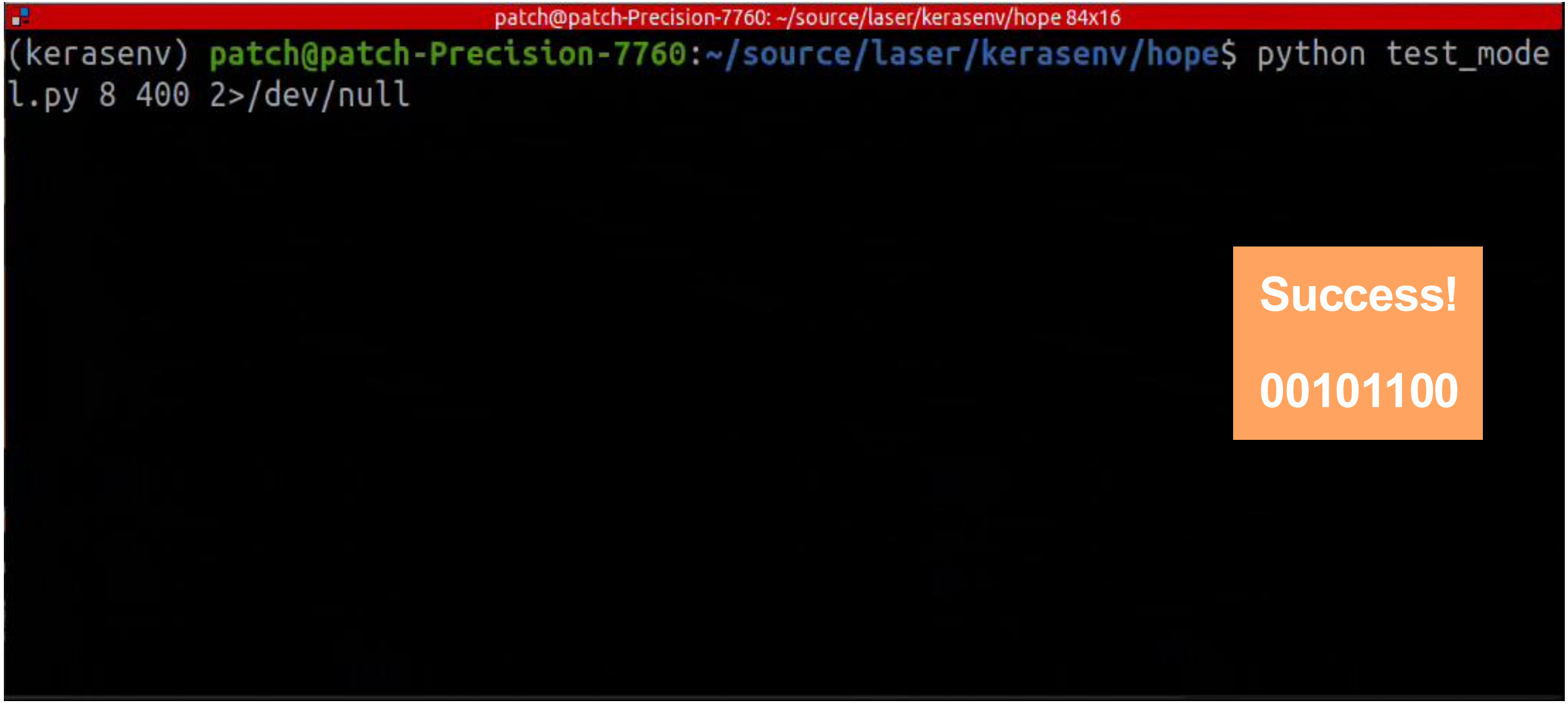
- We made a search grid of 8x8 squares in the section
- We trained the AI on the section that was found to correspond with its value position
- The lighter blue area is what we believe the algorithm triggers on



But does it work?

No lasers to fire this time ☹

Mapping the values



FIN.

…of Gen 1
(we aren’t done)

We stand on the shoulders of so many giants

- The OpenFlexture Project
  - Joel T. Collins, Joe Knapper, Julian Stirling, Joram Mduda, Catherine Mkindi, Valeriana Mayagaya, Grace A. Mwakajinga, Paul T. Nyakyi, Valerian L. Sanga, Dave Carbery, Leah White, Sara Dale, Zhen Jieh Lim, Jeremy J. Baumberg, Pietro Cicuta, Samuel McDermott, Boyko Vodenicharski, and Richard Bowmanm 2020
- High Precision Laser Fault Injection using Low-cost Components
  - Martin S. Kelly, Keith Mayes 2022
- Fault Attack Resilience on Error-prone Devices
  - Martin S. Kelly 2022
- Laser-Based Logic State Analysis in Hardware Security: Threats and Opportunities
  - Thilo Krachenfels 2023

We stand on the shoulders of so many giants

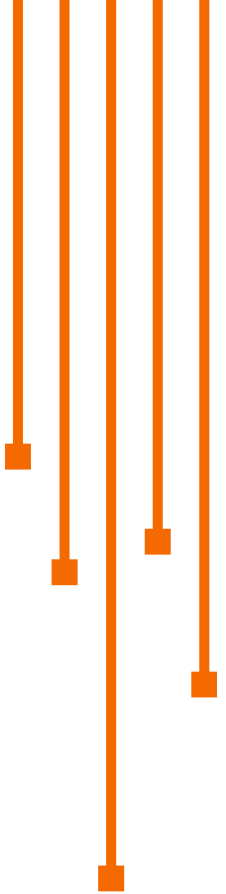
- How Practical Are Fault Injection Attacks, Really?
  - Jakub Breier, Xiaolu Hou 2022
- Trojan Awakener: Detecting Dormant Malicious Hardware Using Laser Logic State Imaging (Extended Version)
  - Thilo Krachenfels, Jean-Pierre Seifert, Shahin Tajik 2023
- Infra-Red, In-Situ (IRIS) Inspection of Silicon
  - Andrew ‘bunnie’ Huang 2023
- Super-resolution laser probing of integrated circuits using algorithmic methods
  - V. K. Ravikumar, Jiann Min Chin, Winson Lua, Nathan Linarto, Gopinath Ranganathan, Jonathan Trisno, K. L. Pey & Joel K. W. Yang 2022

We stand on the shoulders of so many giants

- Preliminary Study on Detecting the Internal Voltage Values of Integrated Circuits Based on Electro-Optical Frequency Mapping
  - Pengcheng Liu, Yingqi Ma, Jianwei Han 2022

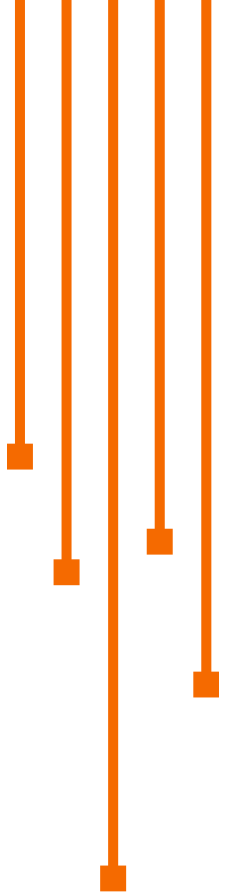
Things that surprised us

- That “laser” was an acronym
- Hoarding, finally, paid off
- I can do this from my house
- Not all datasheets are real
- That one of us didn’t kill, blind, or maim ourselves

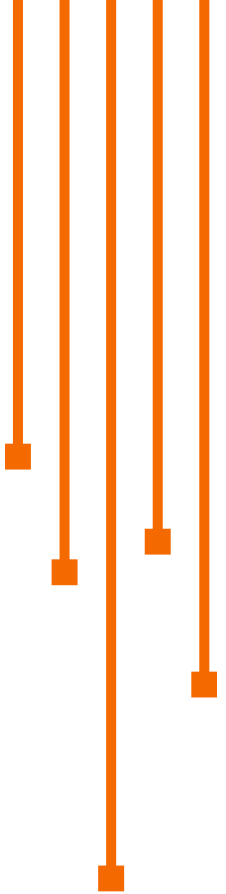


Things that went horribly wrong

- Supply chains & distributors are hard
- Product Descriptors are a lie
- Practical implementation will always trump theoretical principles (the cake is a lie)
- Deadlines are real



How Much RnD costs (thank you NetSPI)

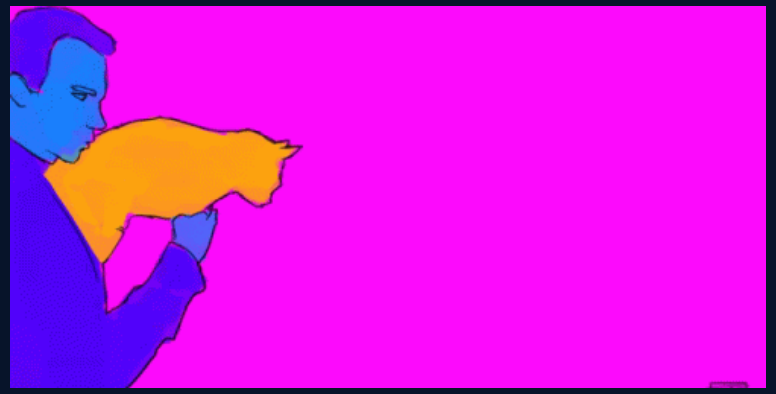


RayV Use Cases

Next time you see us RayV'n

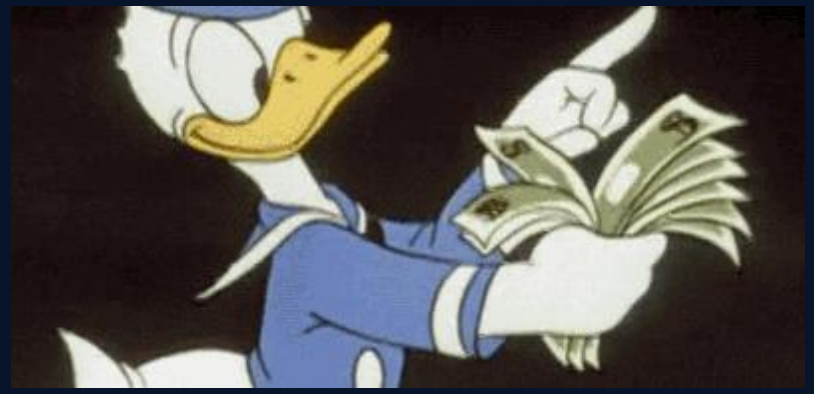
- Increase control & precision of the laser
- Further challenge the cost floor
- Improve 3D Print to optimize speed and panning
- Lower the noise floor for LLSI
- Combine LFI and LLSI to one housing and stage

Key Take Aways?



Lasers are Fun

Wear Protection!



Money is no obstacle

Maker + Hacker mentality = profit

Open Source is King

https://github.com/ProjectLOREM/RayVLite

"The worst thing that could ever happen to you, is that your talk actually gets accepted…because then you need to do your slides" – Phil Young

Thank you!

Catch us at our Booth!

…or in HallwayCon

…or at Hacker Summer Camp

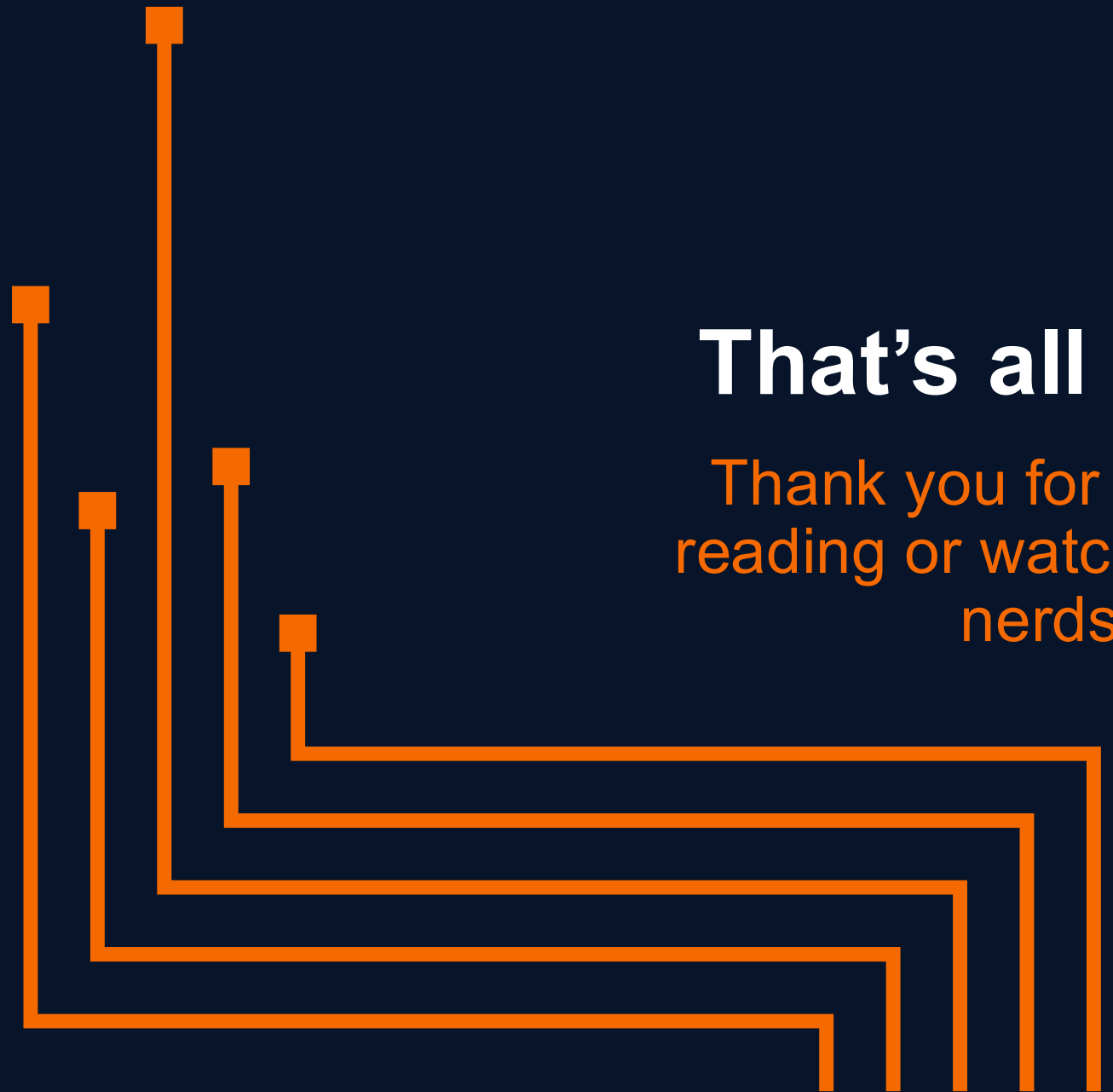
241 N 5th Ave Suite 1200

Minneapolis, MN 55401

netspi.com

Larry.Trowell@netspi.com

Sam.Beaumont@netspi.com



That’s all Folks!

Thank you for listening, reading or watching us be nerds


LASERS ARE COOL
FIRE THE LASER!!!
SHARKS WITH FRICKIN' LASER BEAMS ATTACHED TO THEIR HEADS!
Pew. Pew.