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

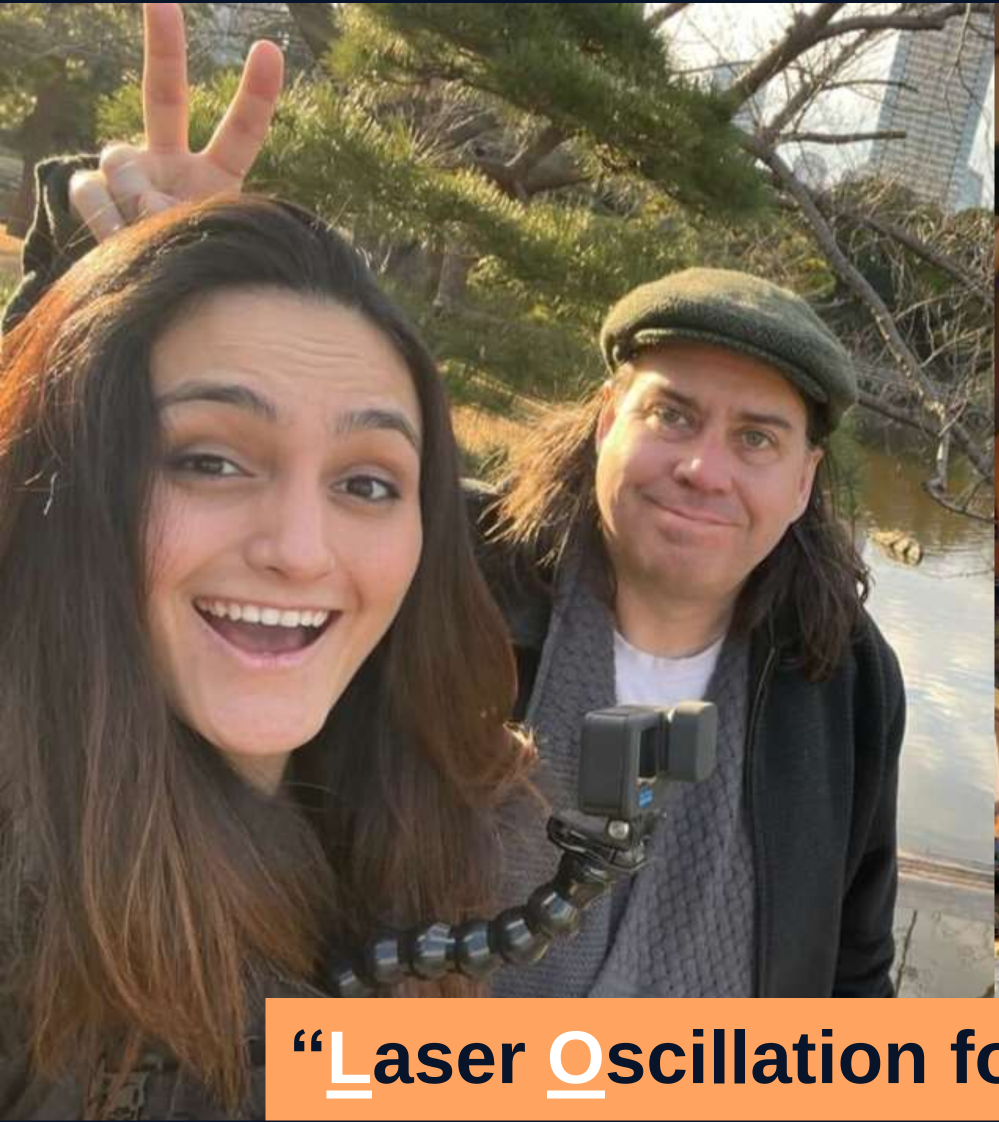
Building Affordable Light-Based Hardware Security Tooling

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

Chas Becht

ANDROID

Casey Repp

SCIENTIST

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
    - Chassssseeeee
    - 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

Project L.O.R.E.M

Director, Transportation, Mobility & Cyber-Physical Systems

Director, Hardware & Embedded Systems

Principal Consultant

AI Practice Lead

Principal AI Researcher

Project L.O.R.E.M

Hardware & Integrated Systems





Artificial Intelligence & Machine Learning

“A jack of all trades is a master of none, but often times better than a master of one” - William Shakespeare

NetSPI: The Proactive Security Solution





APPLICATION PENTESTING
Web & API Application
Mobile Application
Thick Application

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

NETWORK PENTESTING
Internal Network
External Networks

MAINFRAME PENTESTING

BLOCKCHAIN PENTESTING

CLOUD PENTESTING
AWS
Azure
Google Cloud

SAAS SECURITY ASSESSMENT

SECURE CODE REVIEW

ATTACK SURFACE MANAGEMENT (ASM)

BREACH AND ATTACK SIMULATION (BAS)

CYBERSECURITY MATURITY ASSESSMENT
Security Program Advisory
Incident Response
Benchmarking

AI/ML PENTESTING
Large Language Models

RED TEAM

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).

Lorem ipsum dolor sit amet, consectetur adipiscing elit. This is a placeholder section because I need more little text. Quisque vitae tincidunt libero, at feugiat sapien. Praesent sed scelerisque justo. Maecenas laoreet, mauris vel auctor suscipit, magna turpis feugiat ligula, in convallis libero risus eget odio. Ut facilisis ex nec nisl vehicula, ac luctus justo placerat. Integer sit amet turpis nec neque interdum ultrices. Vestibulum et scelerisque metus. Nulla facilisi.Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Ut vel nisl in metus facilisis feugiat. Proin faucibus, nunc non fermentum gravida, libero erat consectetur lectus, eget pretium magna nisl a libero. Integer commodo sem nec arcu ultrices scelerisque. Lasers are still dangerous, I can't believe you're still reading. Nam eget ex ac sem scelerisque laoreet. Nulla interdum justo non lacus efficitur, ac tincidunt ex pulvinar.Aenean non vestibulum urna. Vestibulum eu erat vel elit lacinia convallis. Mauris nec metus in sapien iaculis dignissim.

Vestibulum tempor libero at odio convallis, a hendrerit nunc sollicitudin. Vivamus gravida enim sed magna dictum, non ultrices tortor pharetra. Nam vehicula libero eu dolor suscipit, sit amet dignissim eros venenatis. Phasellus rutrum, justo at condimentum dignissim, erat ex efficitur risus, ut dictum elit metus in ex. Sed auctor interdum tellus sit amet blandit.In feugiat, ex non dignissim ullamcorper, metus magna dapibus leo, id scelerisque purus arcu vel dui. Quisque imperdiet erat sit amet nisi dictum, nec aliquam lectus ultrices. Integer nec lacinia nisl. Curabitur tincidunt, ipsum ut convallis ultricies, turpis sapien aliquam quam, at vulputate nisi nulla vel libero. Curabitur et ante sit amet mauris posuere mollis non et lacus. Vestibulum dapibus send help orci non orci lacinia, ac facilisis odio fermentum. Nam id sagittis dolor, vel consequat mauris.Cras auctor ligula quis augue volutpat cursus.

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

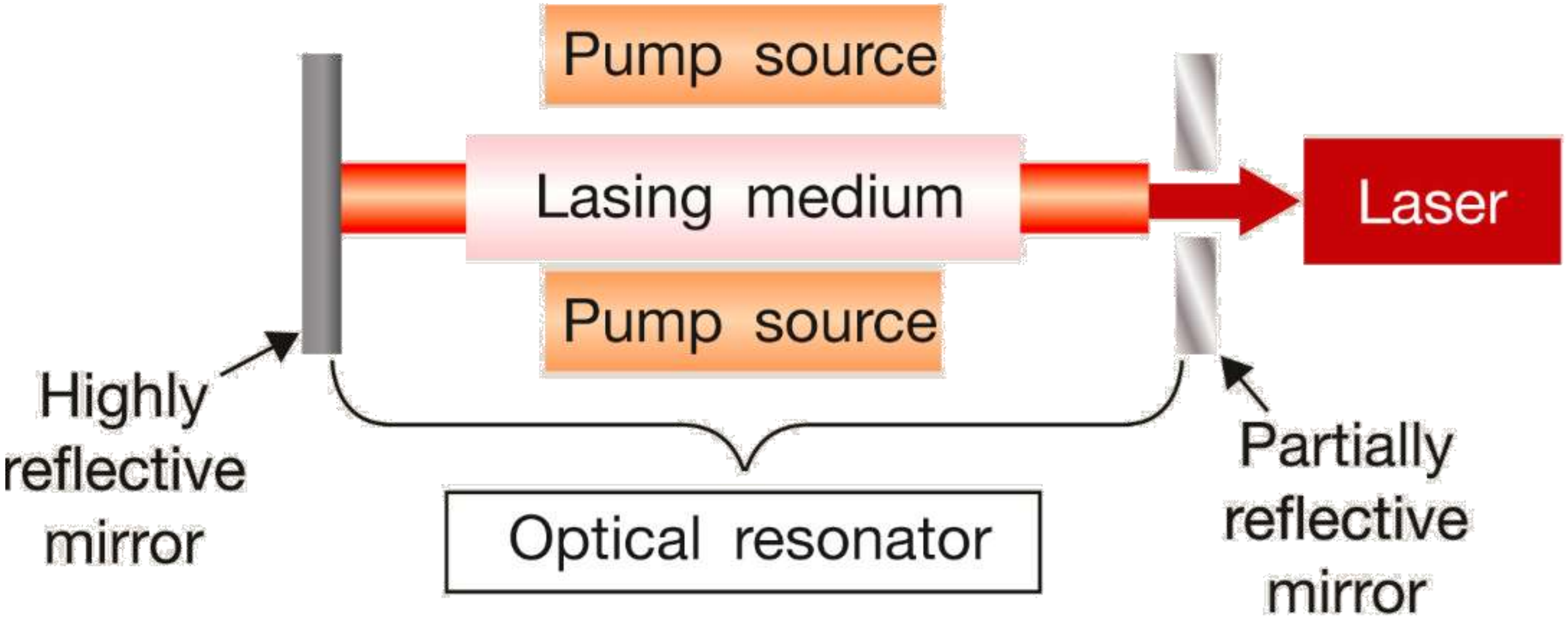
“Why are we putting on the glasses of extreme headache?” – Larry Trowell

LASERS ARE DANGEROUS

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

- L.A.S.E.R.
  - Light
  - Amplification by
  - Stimulated
  - Emission of
  - Radiation

- Bouncing photons inside a medium until they all march in lockstep



Why LASERS?

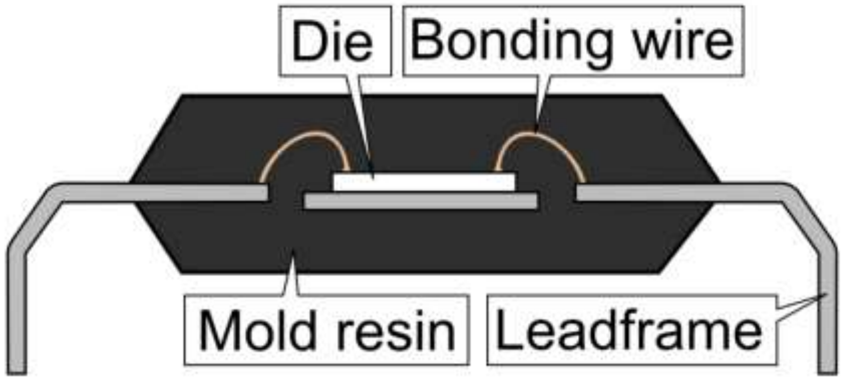
- Light is easy to source
- Transistors have an inherent weakness to light
- Contactless
- Non-Damaging (physically to the target)
- Typically considered a “Semi-invasive” technique

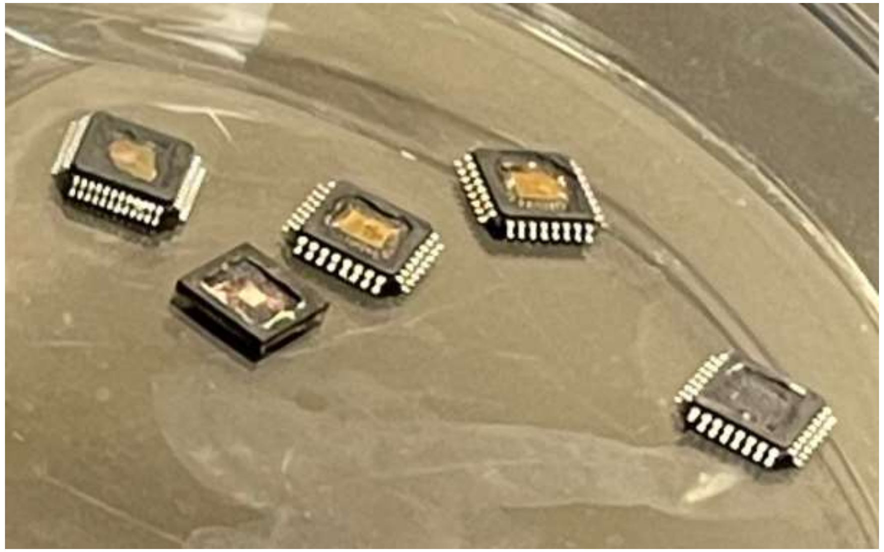
“Semi-Invasive”

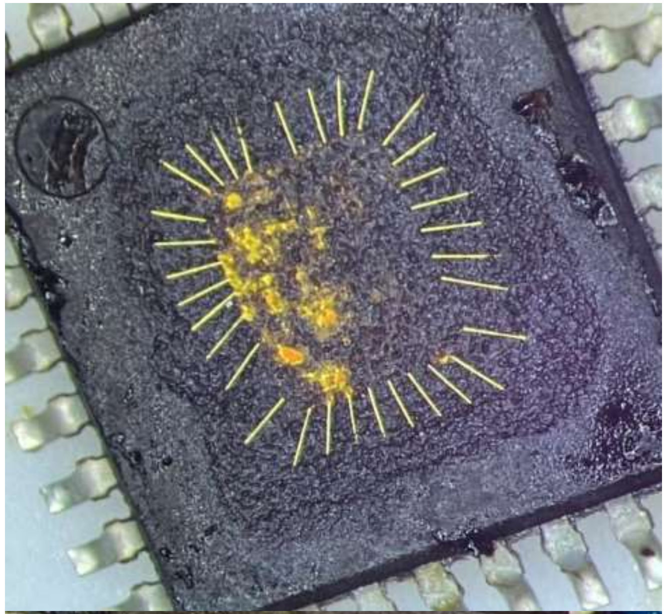
A visceral experience

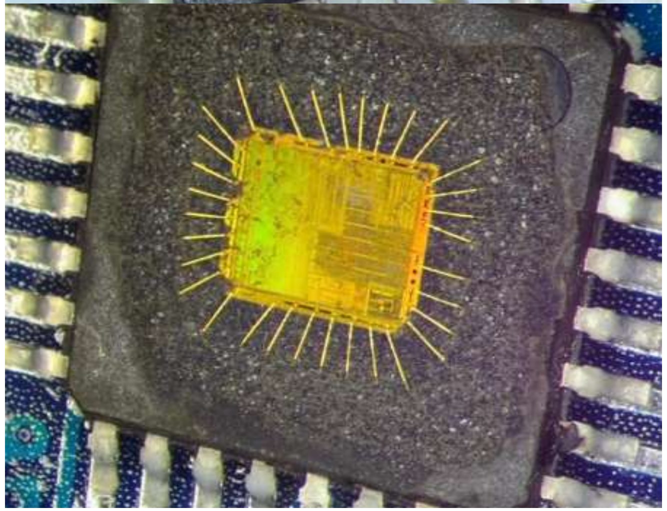
Method 1: Chemical Decapsulation

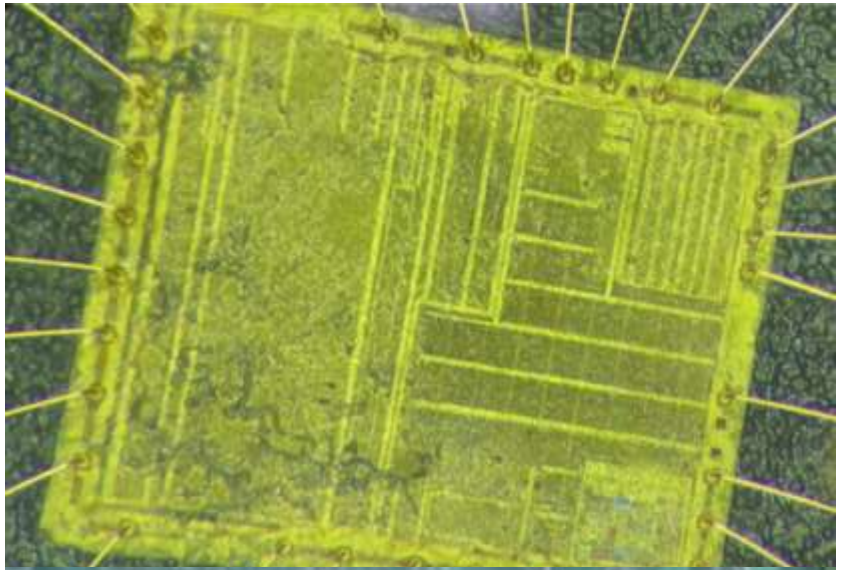
ACID

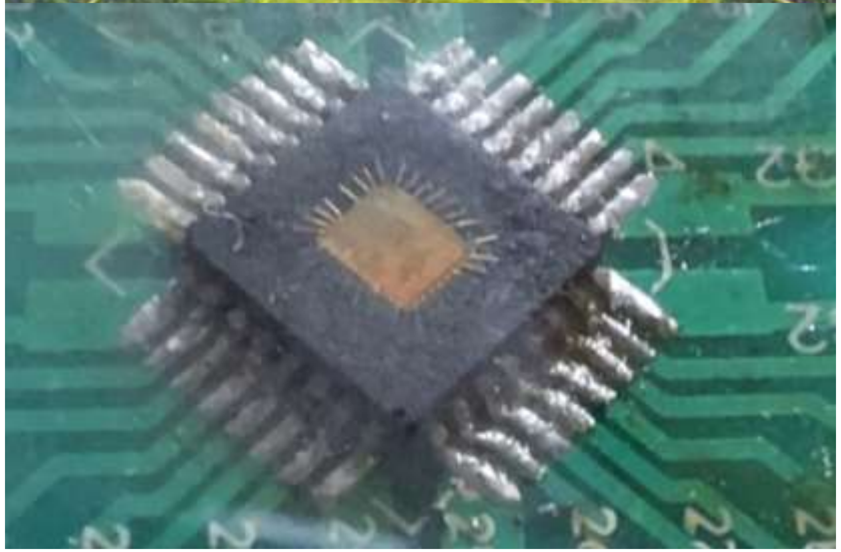




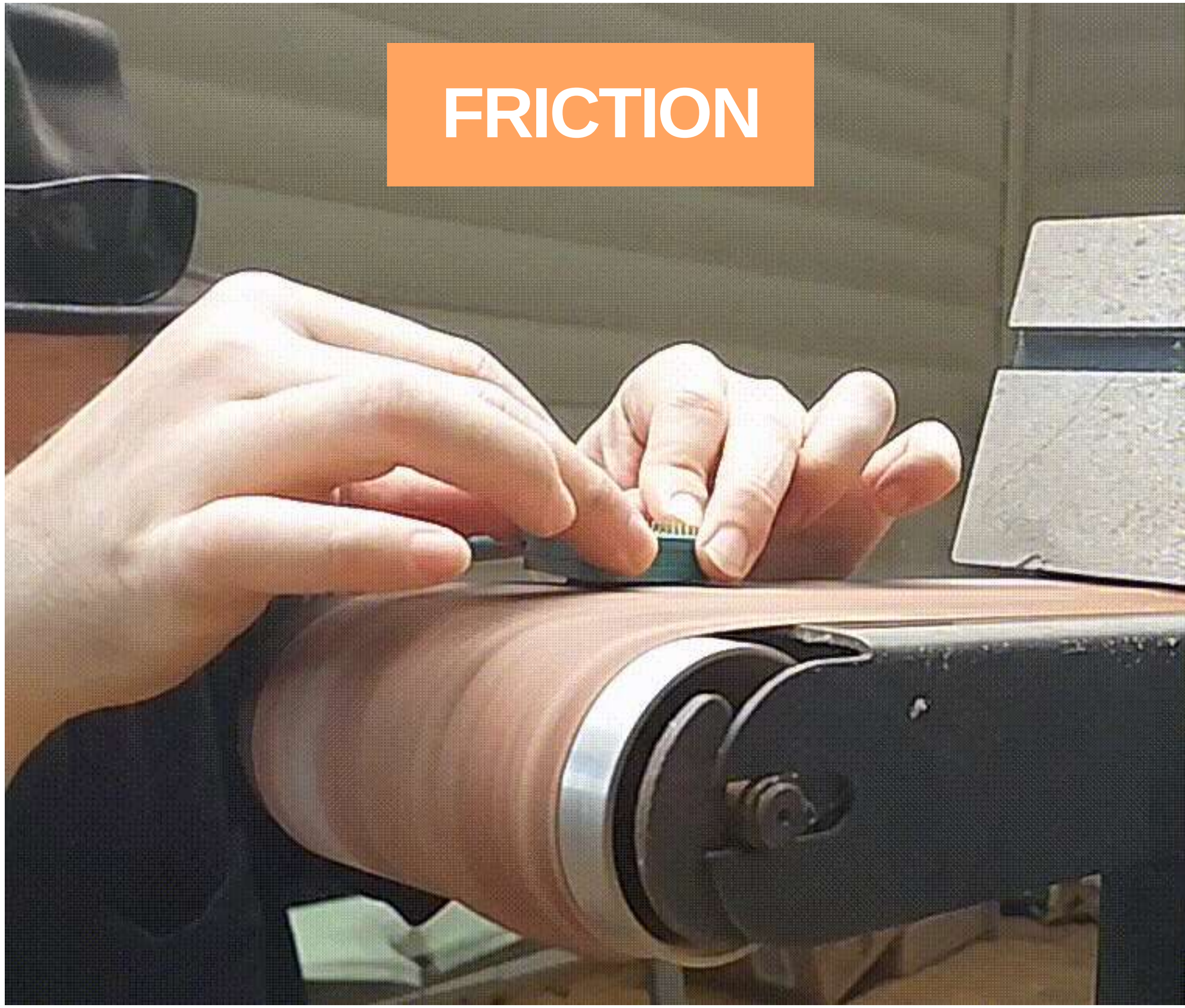








Method 2: “Creative” Destruction



“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

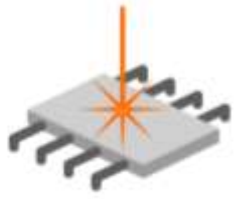
L.F.I.

What, Why, and How?

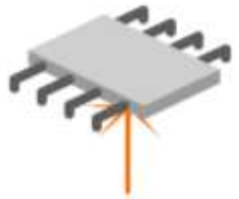
- Fault injection is traditionally used to **cause a processor to skip instructions**

- 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…

We did this not because it was easy…we did this because we thought this would be easy

Drinks are on that …person!

New (lowball):

- $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 $\boldsymbol{they're\ cool^{TM}}$

Traditional Imaging Systems

- Typically, these are microscopes
- Used for **targeting** for the laser, and **identification** for the target
- Reference researchers used the “Trinocular Leitz SM-LUX HL”
- Refurb Price: **$4,000 USD**

Traditional Positioning Systems

- Typically, these tables are specialised, purpose-built units with steppers and dials
- Used for **nano-positioning** of the **target**, or the **laser**
- Refurb Price: **$3,000 USD**

The OpenFlexure Project: 2-in-1

- **3D printable**, high precision mechanical positioning housing
- Contains a **microscope** body….**and positioning stage**
- Total Cost: **~$280 USD**
  - Approximate Savings: **~$6,720 USD**

Traditional Laser Systems

- Traditionally LFI stations work by firing a **highly powerful laser** for **a very short amount of time**
- For example: a YAG laser can provide **tens of millijoules (mJ)** in **less than 10 nanoseconds (ns)**
- Where some can cost **over $30,000 USD**, just for the laser

- How much energy is *actually* needed to cause a glitch?
- Do we *really* need that much energy in a short amount of time?
- How much “time” can we get away with?

"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."

We have the Power

- Traditional practices believe you need energy in the scope of **millijoules (mJ)**
- Research shows you can do it in **nanojoules (nJ)**
- That is an energy reduction of $1e^{-6}$

Photoelectric Effect

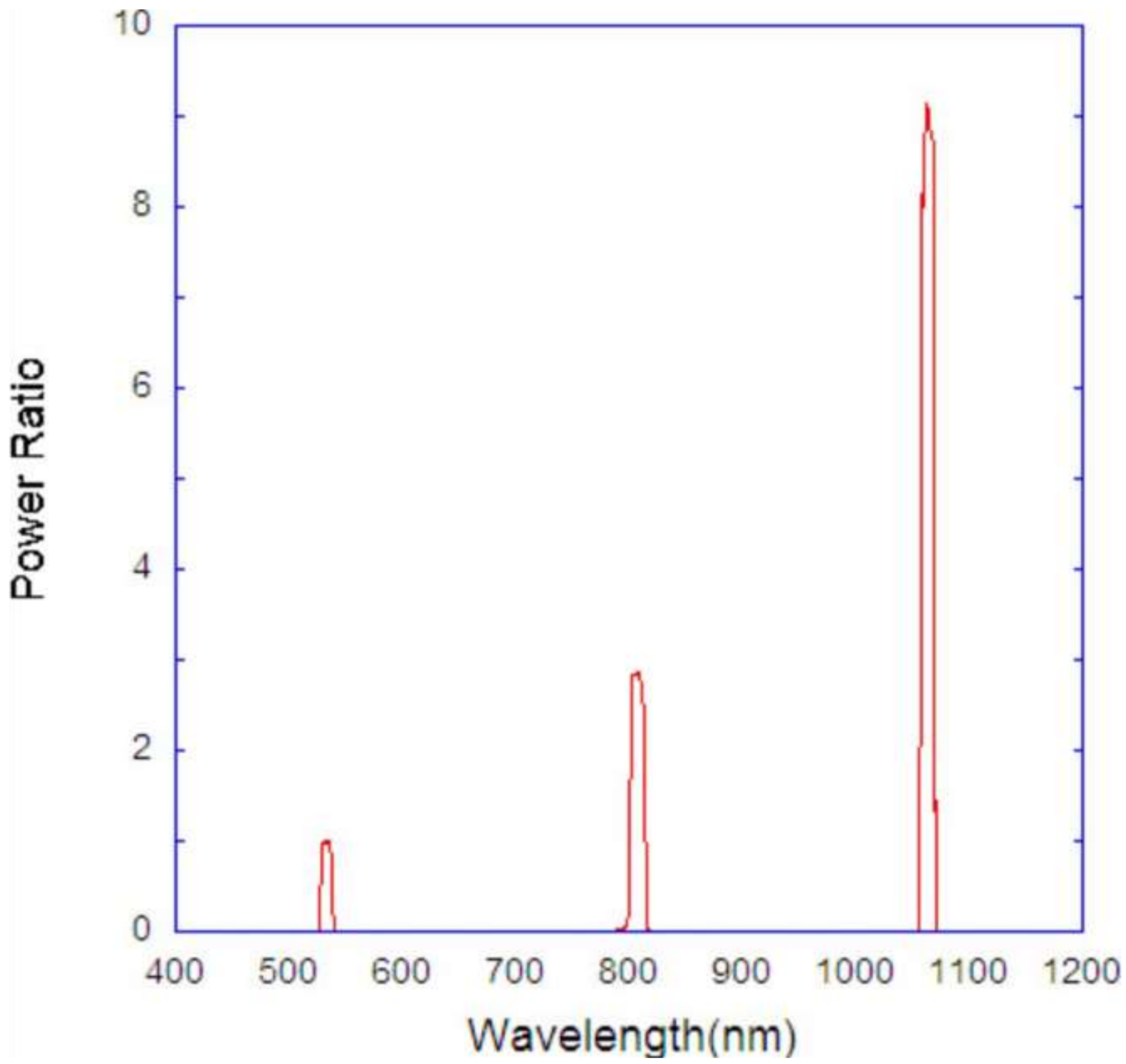
- Further research discovered that **glitching** can happen between **42.5 nJ and 80 nJ**
- The trick is to use **low power over time** instead of instantly
- Thus a **2.5W laser over 25ns** will hit accumulate to **40nJ**
- That’s a lot easier to source

Winner, winner, chicken dinner

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

More Possibilities than those that "meet the eye"

- Remember all those news stories about green laser pointers…
- These "green" lasers are "supposed" to be 5mW
- There are other wavelengths it emits, among them, a lot more than 5mW in the 1064nm range



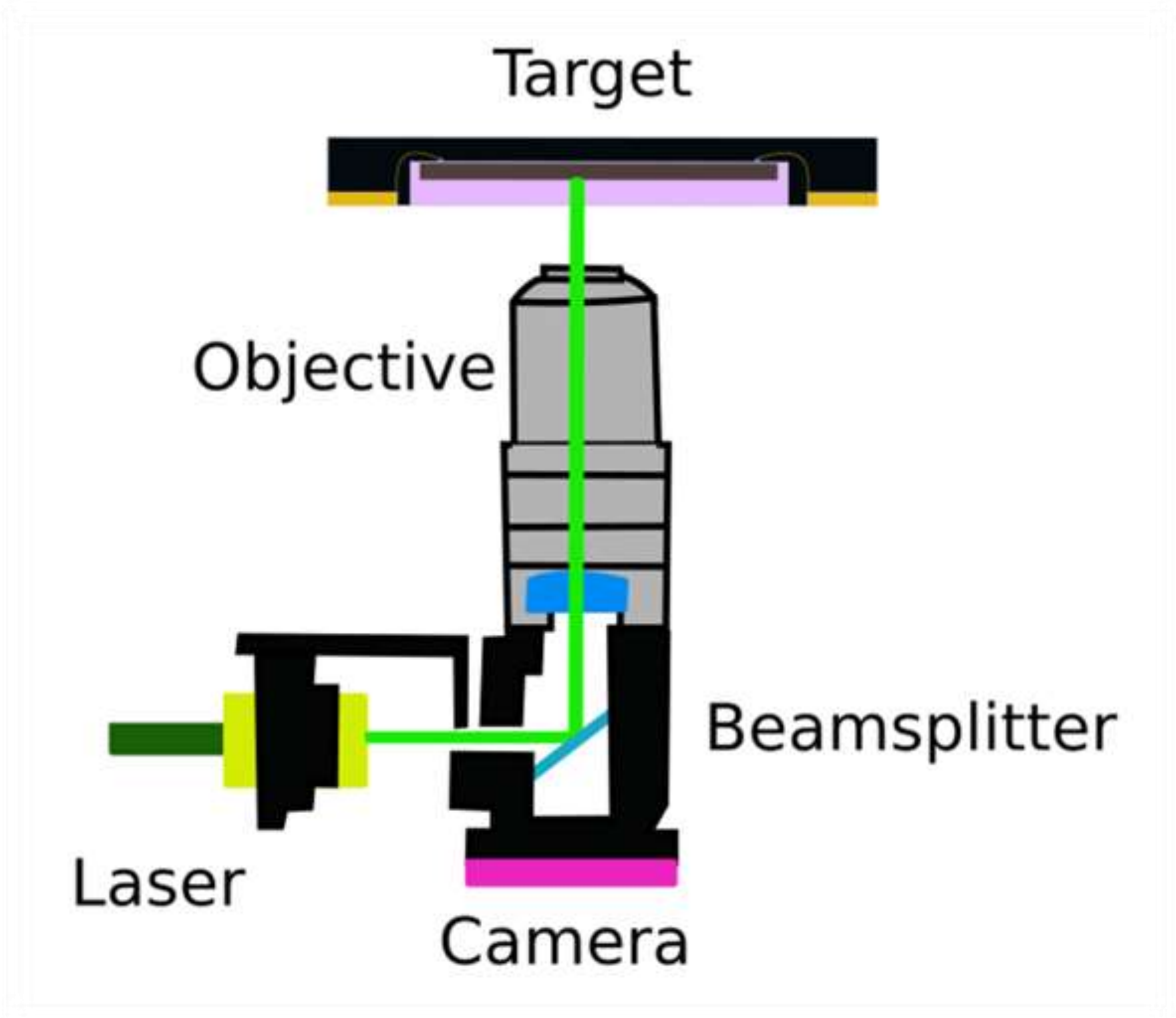
I bought a laser pointer online that claimed to be a harmless 5mW. Turns out it was more like a miniature death ray disguised as a pen. It's like buying a puppy and getting a dragon instead.

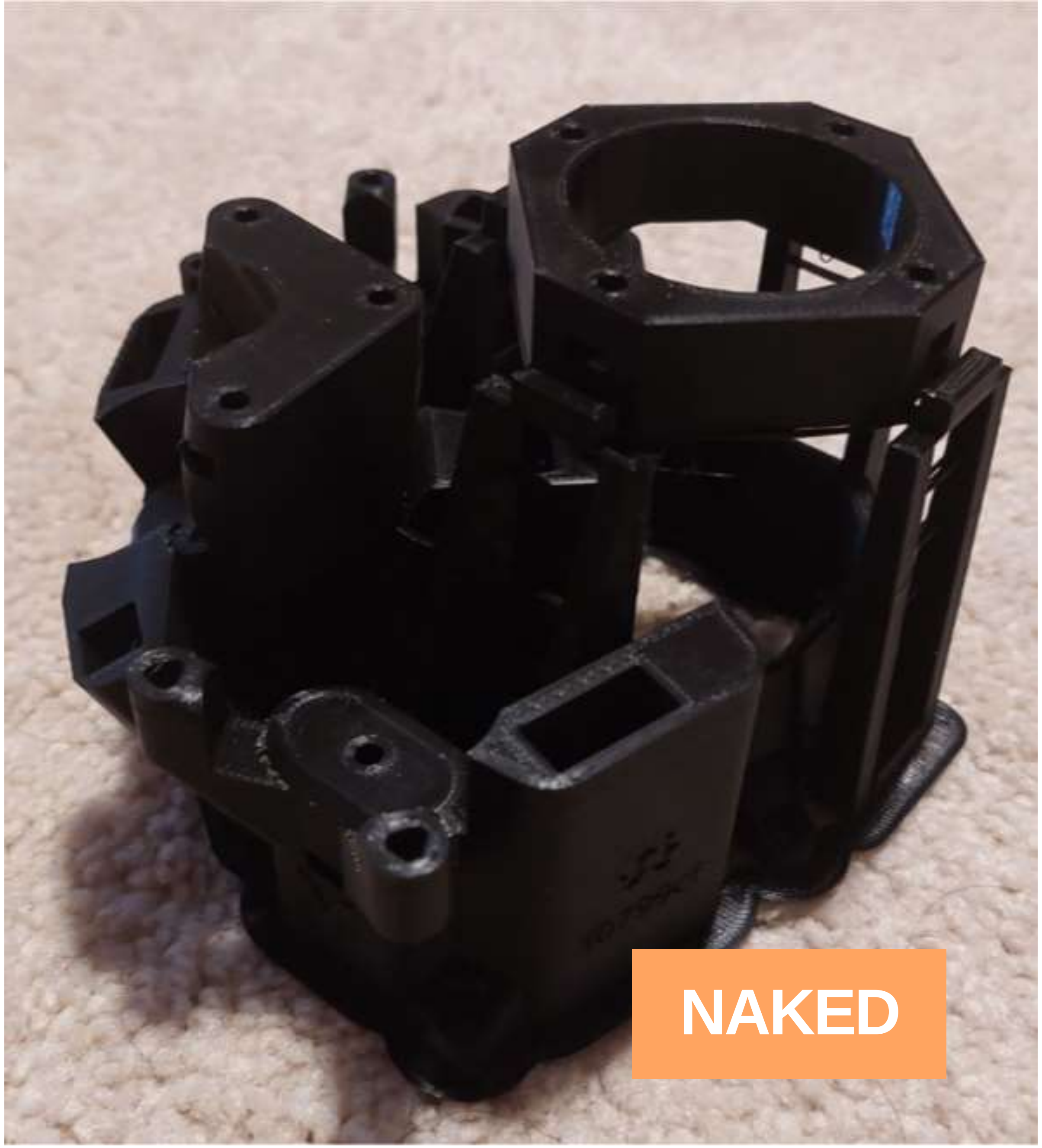
RayV-Lite

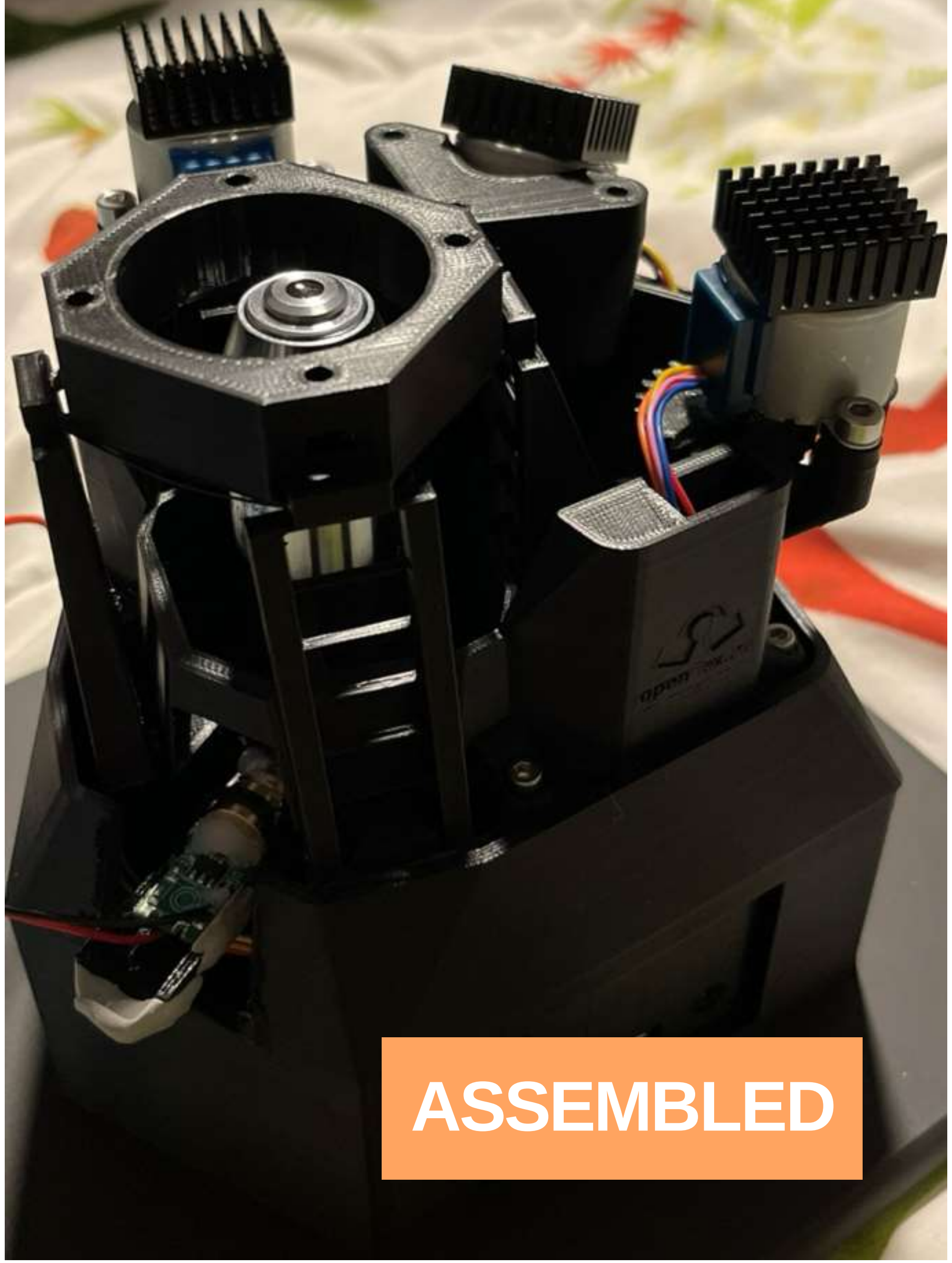
Everything Assembled

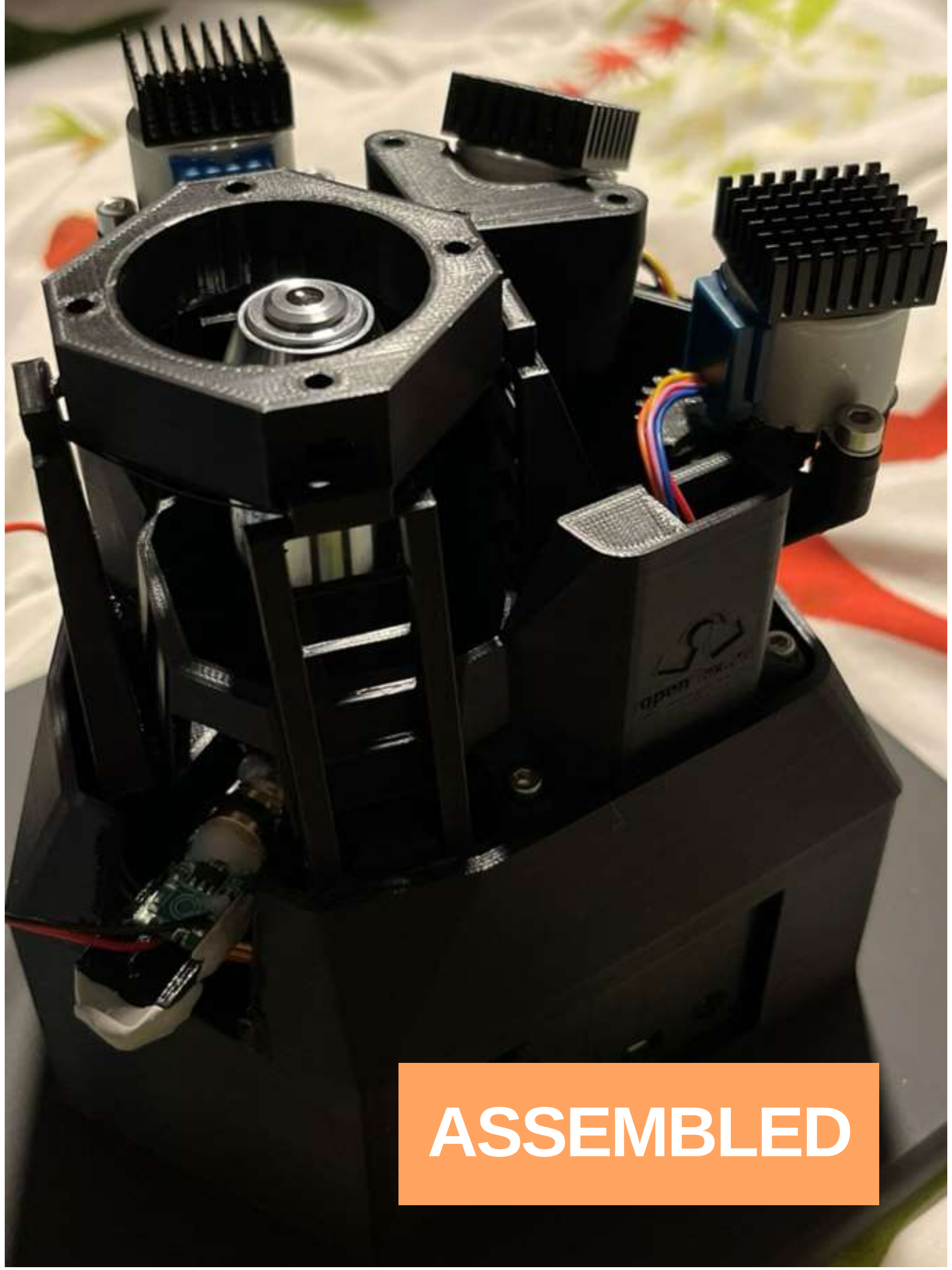
Putting it all together

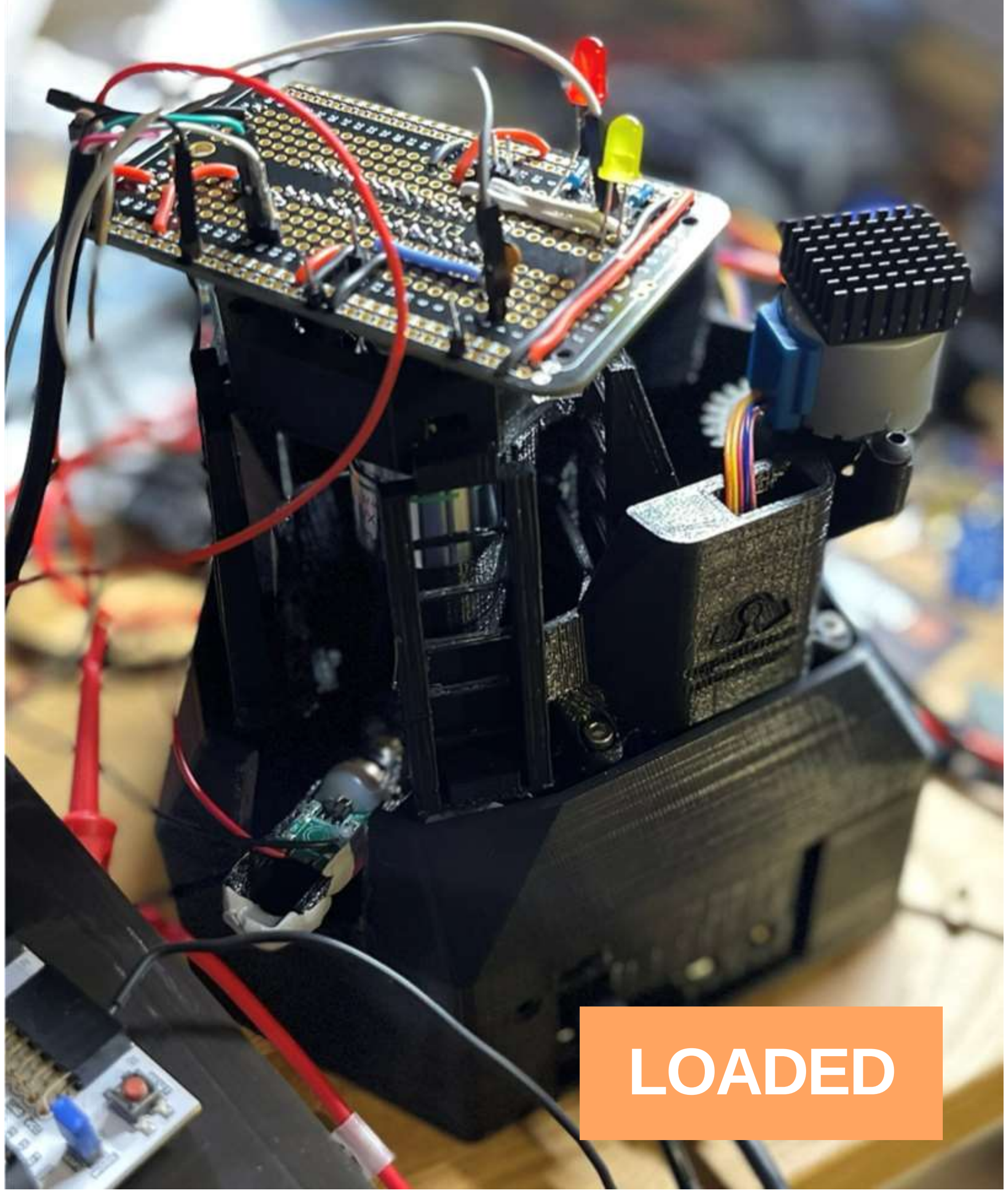
- An FPGA to slow target clock
- An LED to see the target (1050nm, more on this later)
- “Green” Laser pointer to fire, and glitch
- Objective to focus the laser

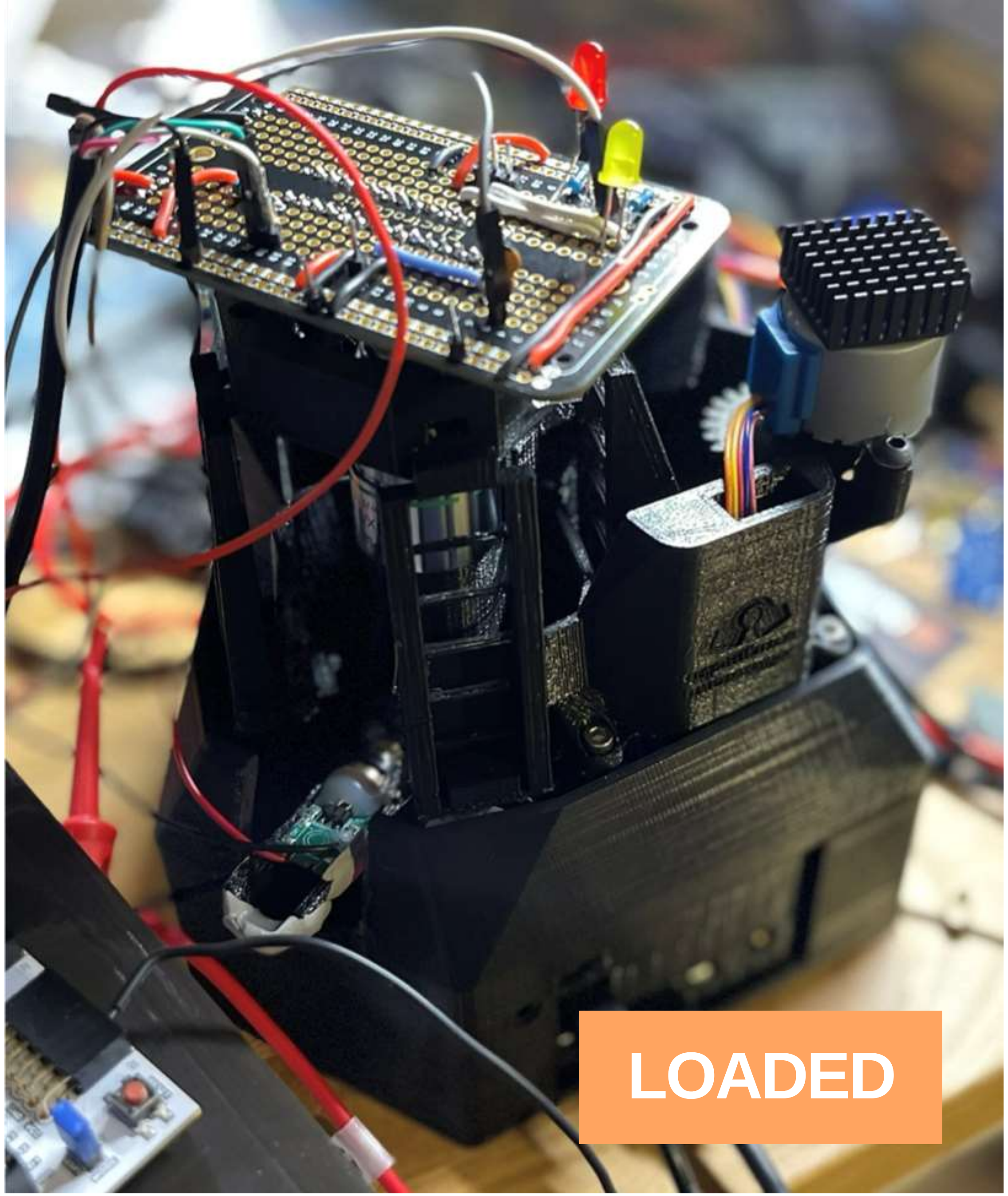


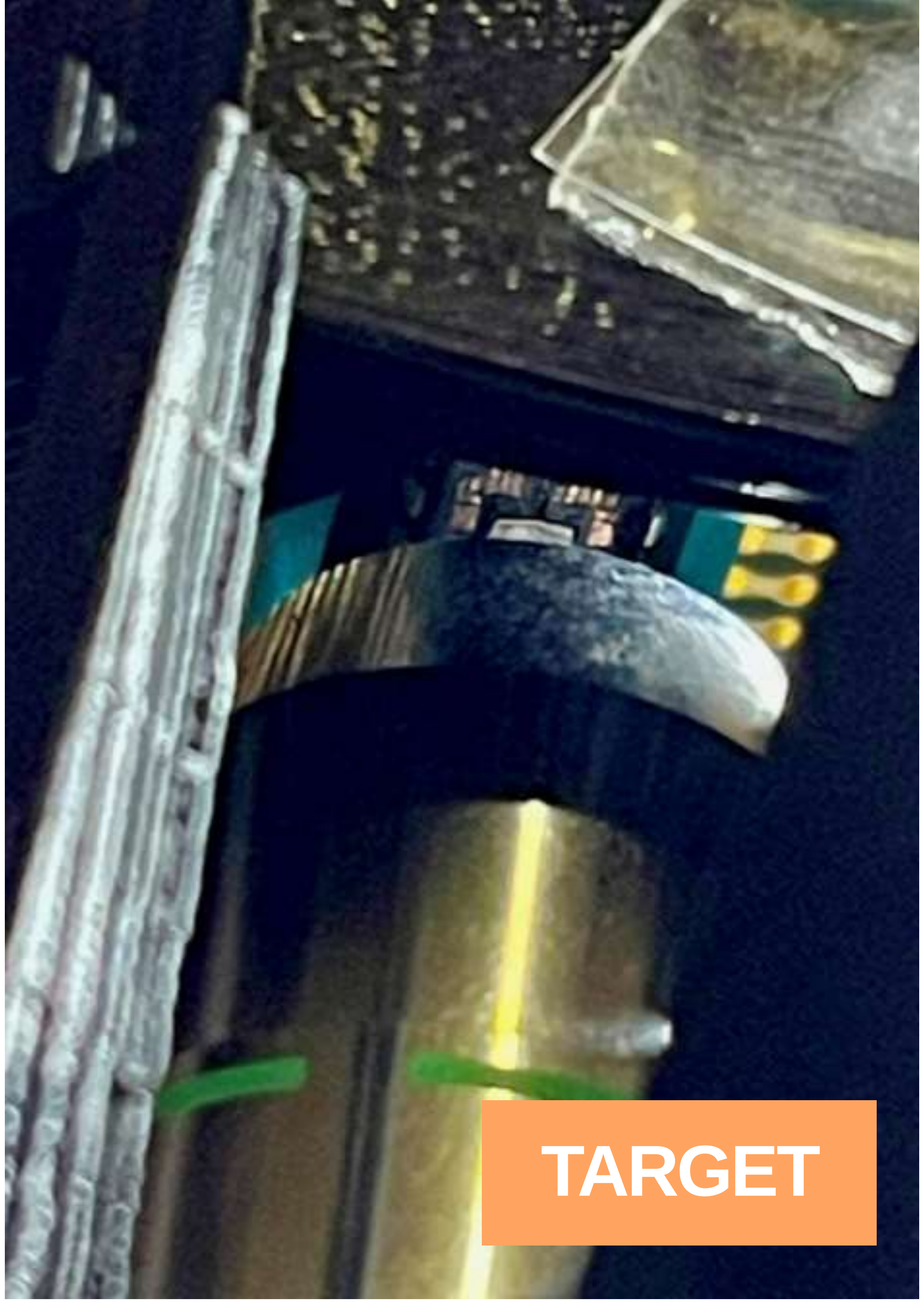

NAKED


ASSEMBLED


ASSEMBLED

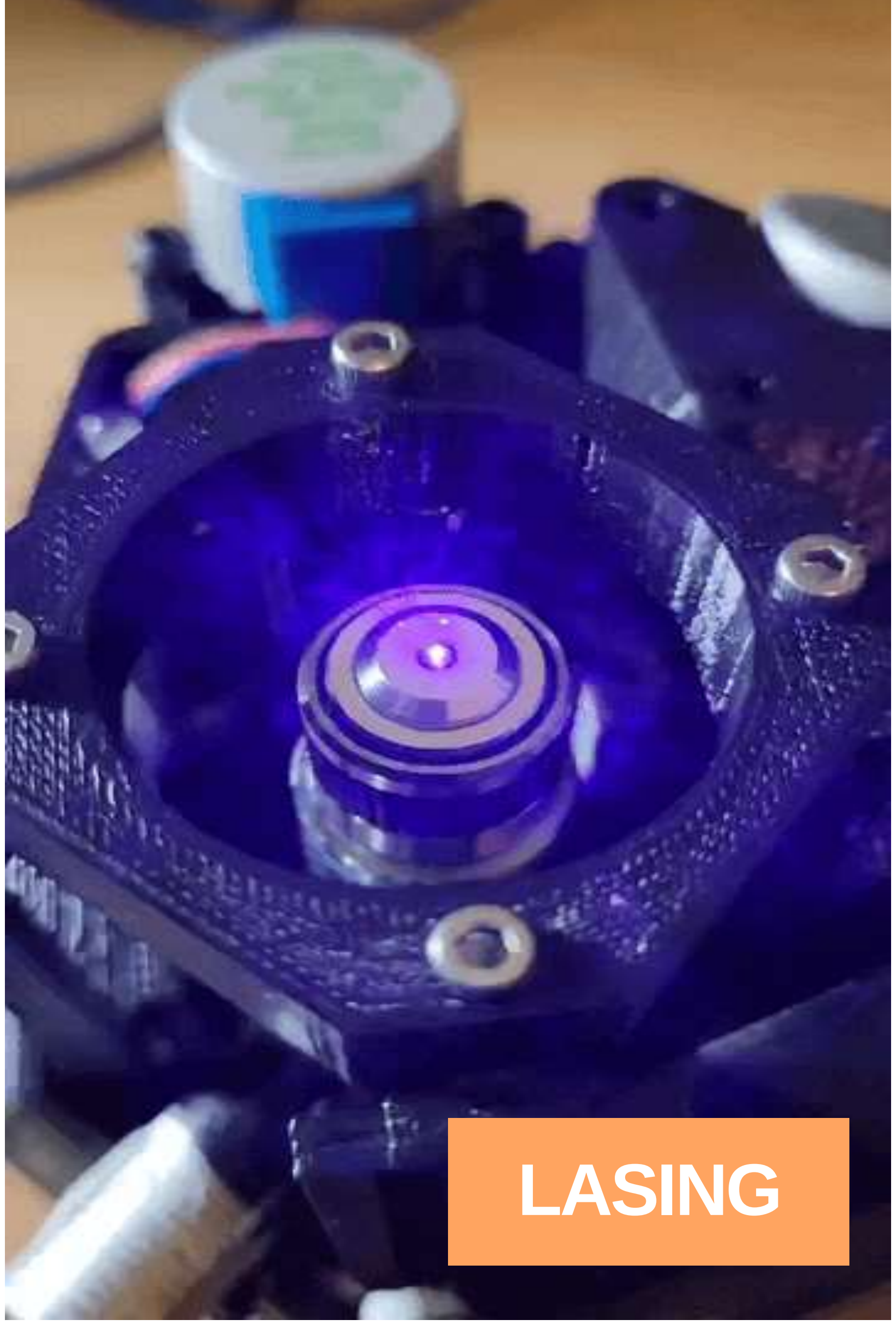

LOADED





“If you don’t move, you’re still” – Chas Becht

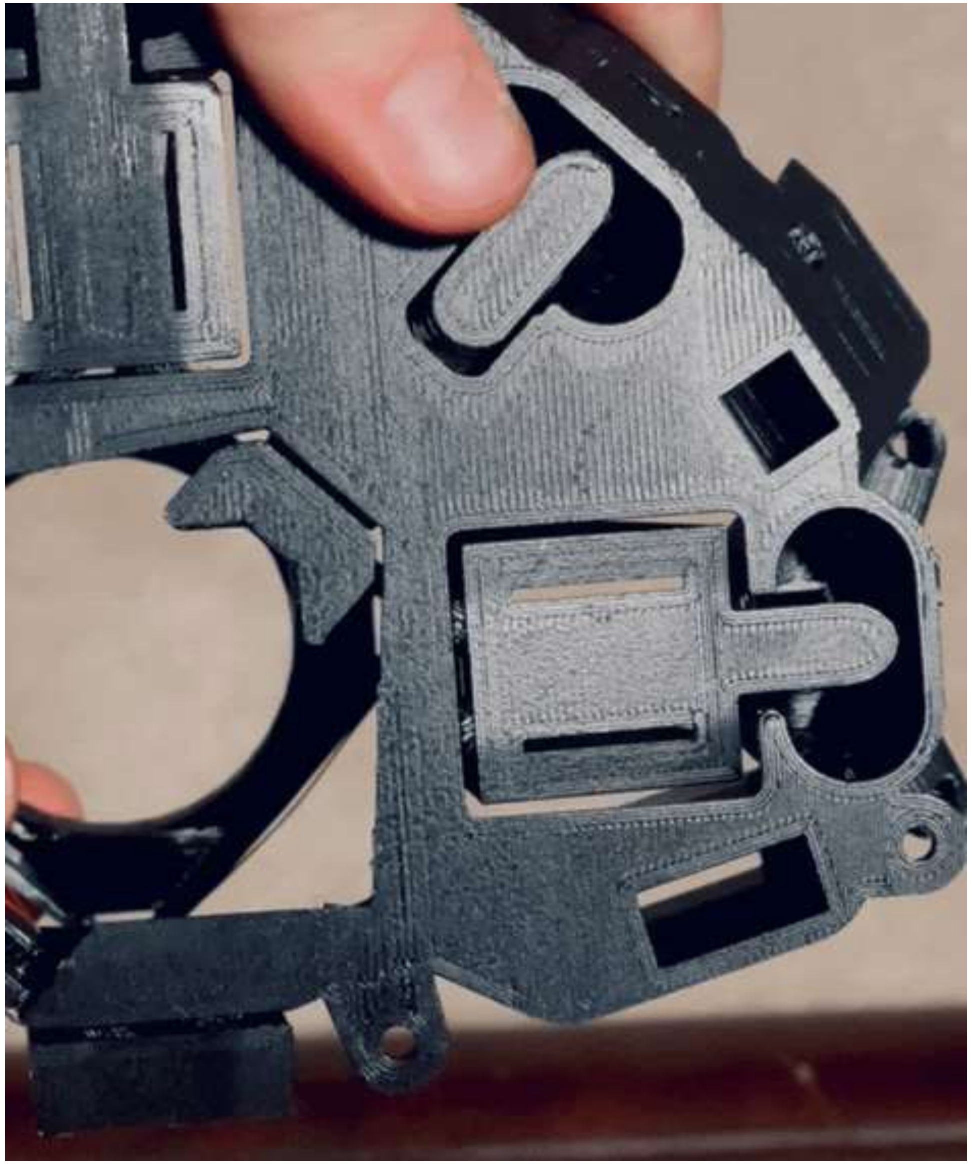

TARGET


LASING

Poetry in Motion

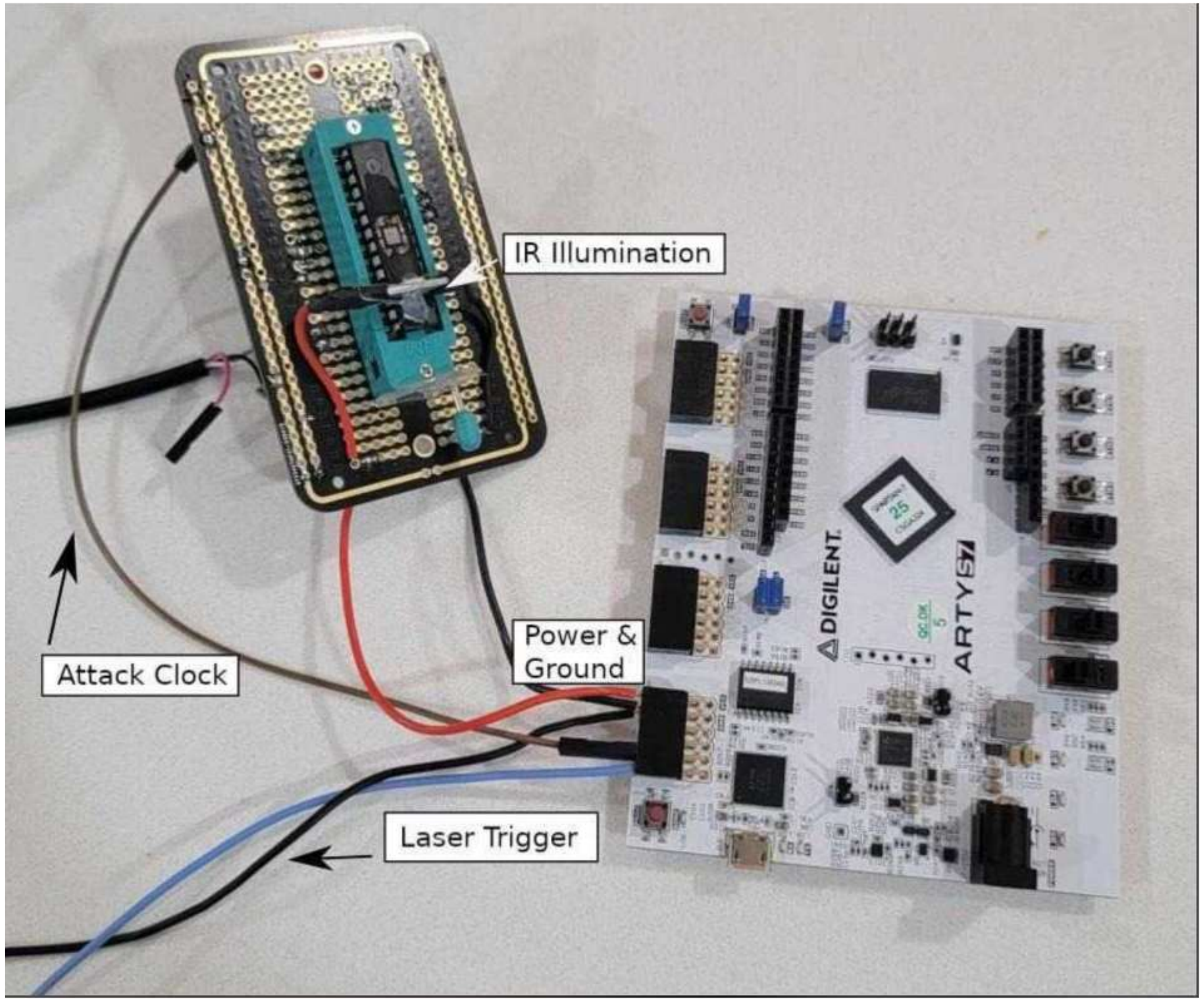
The beauty of plastic….

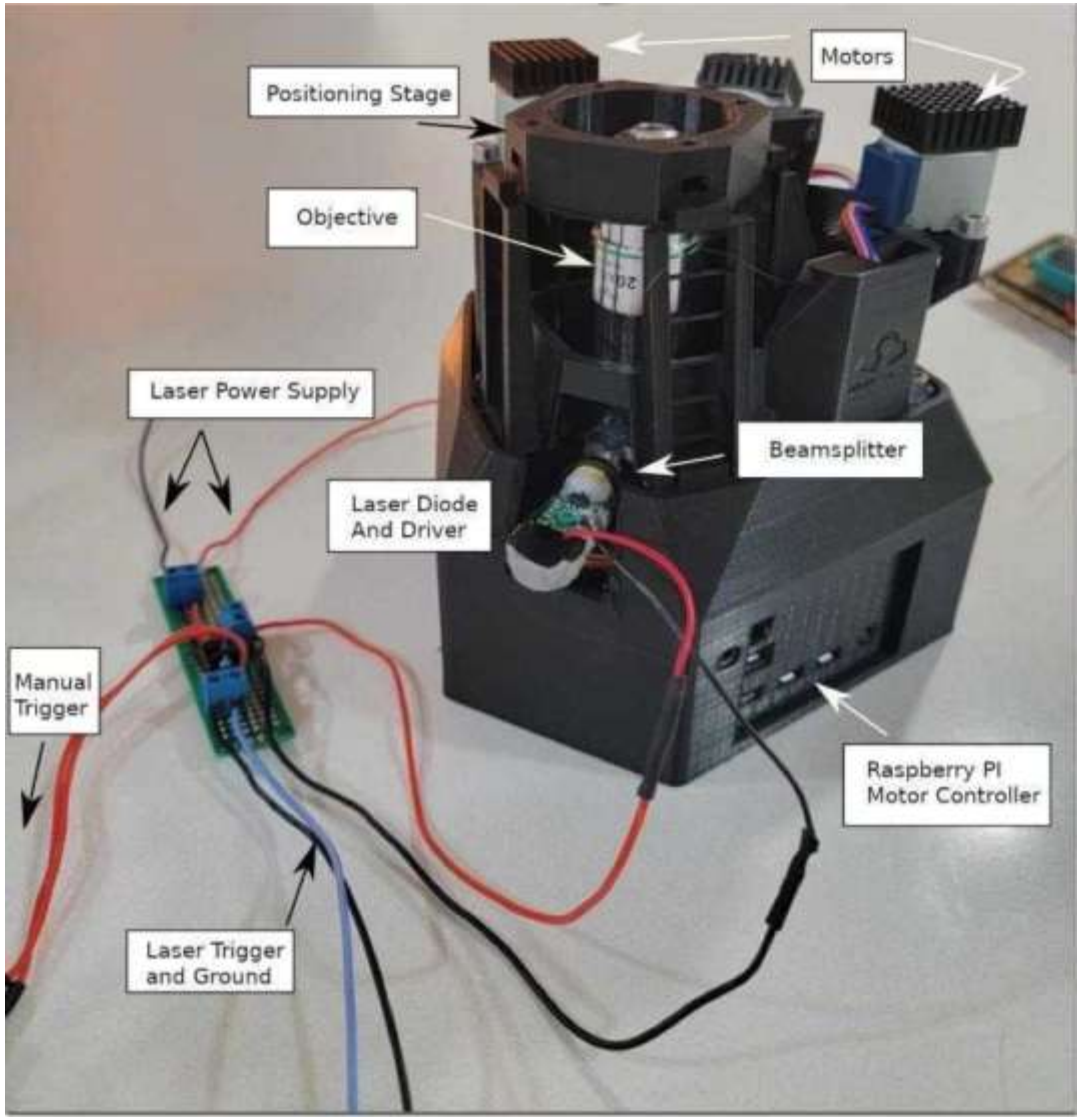
….is that it bends



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

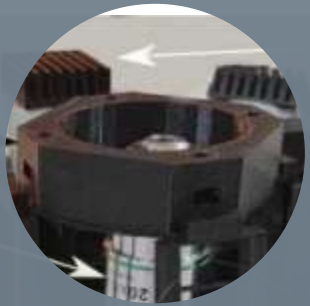
Component Breakdown





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

Positioning Stage

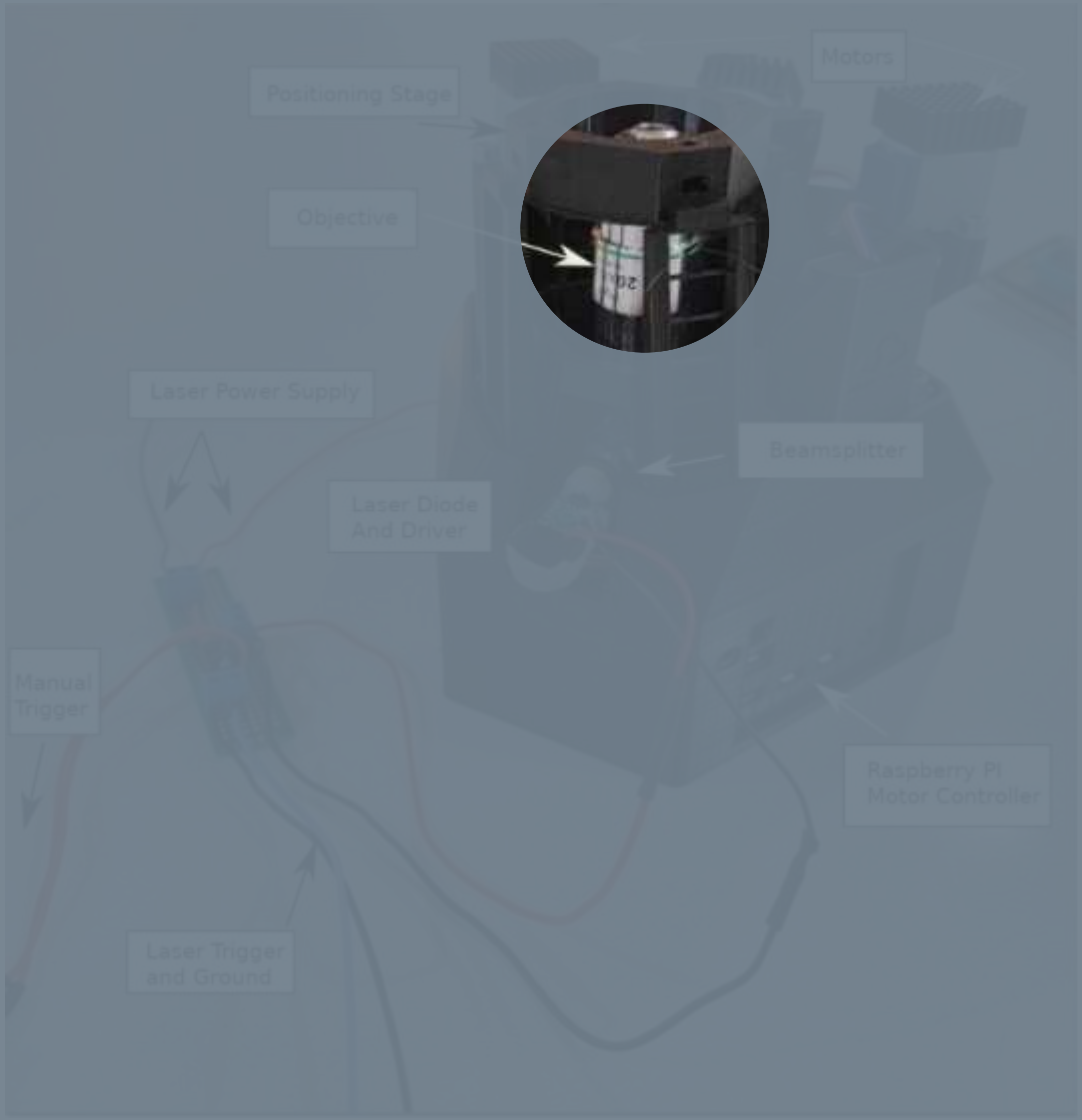


- Target Affixation Location
- Target Movement (for laser positioning)

Component Breakdown

Objective

- Focusing element for laser
- Firing “housing” for laser



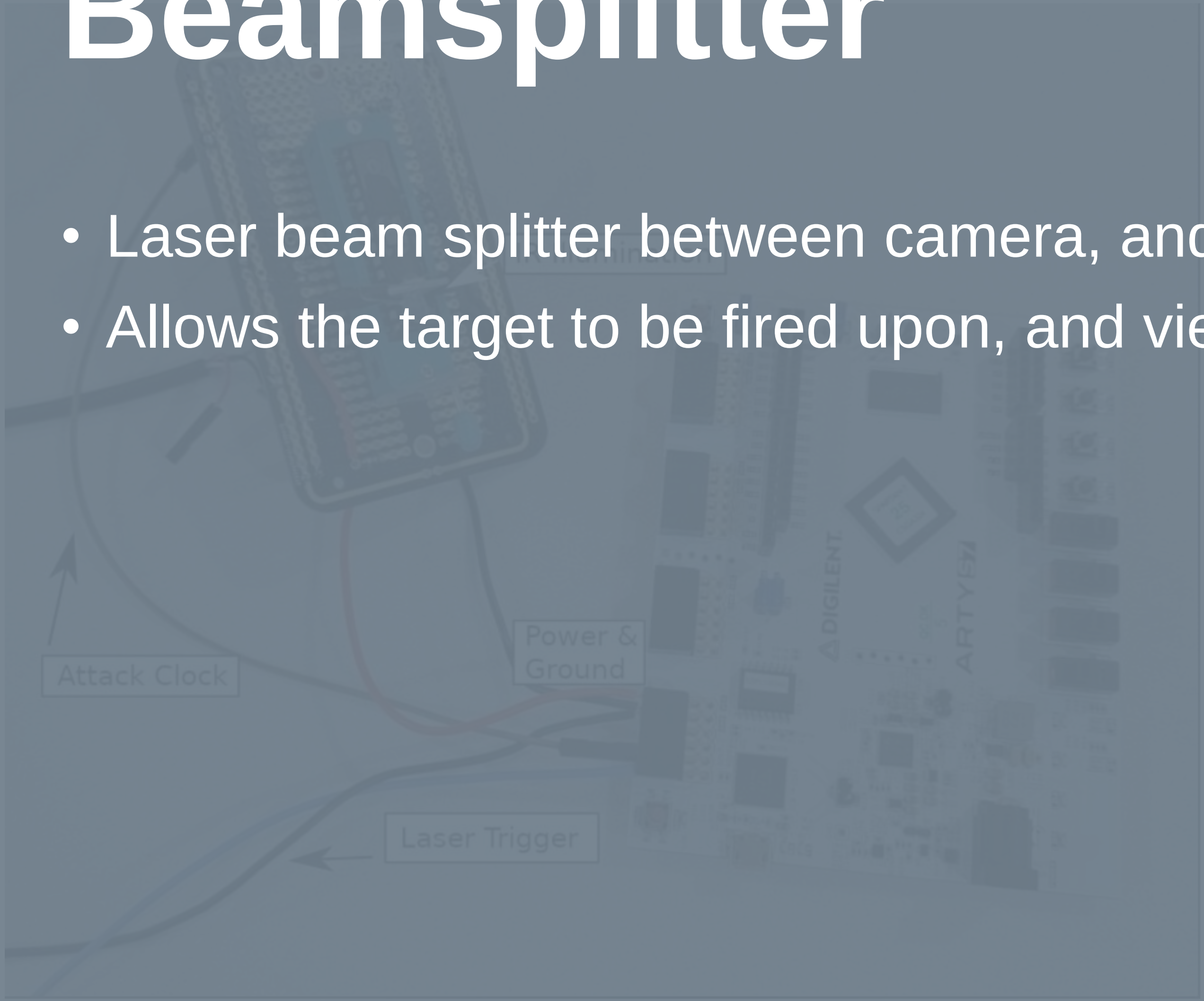
Motors

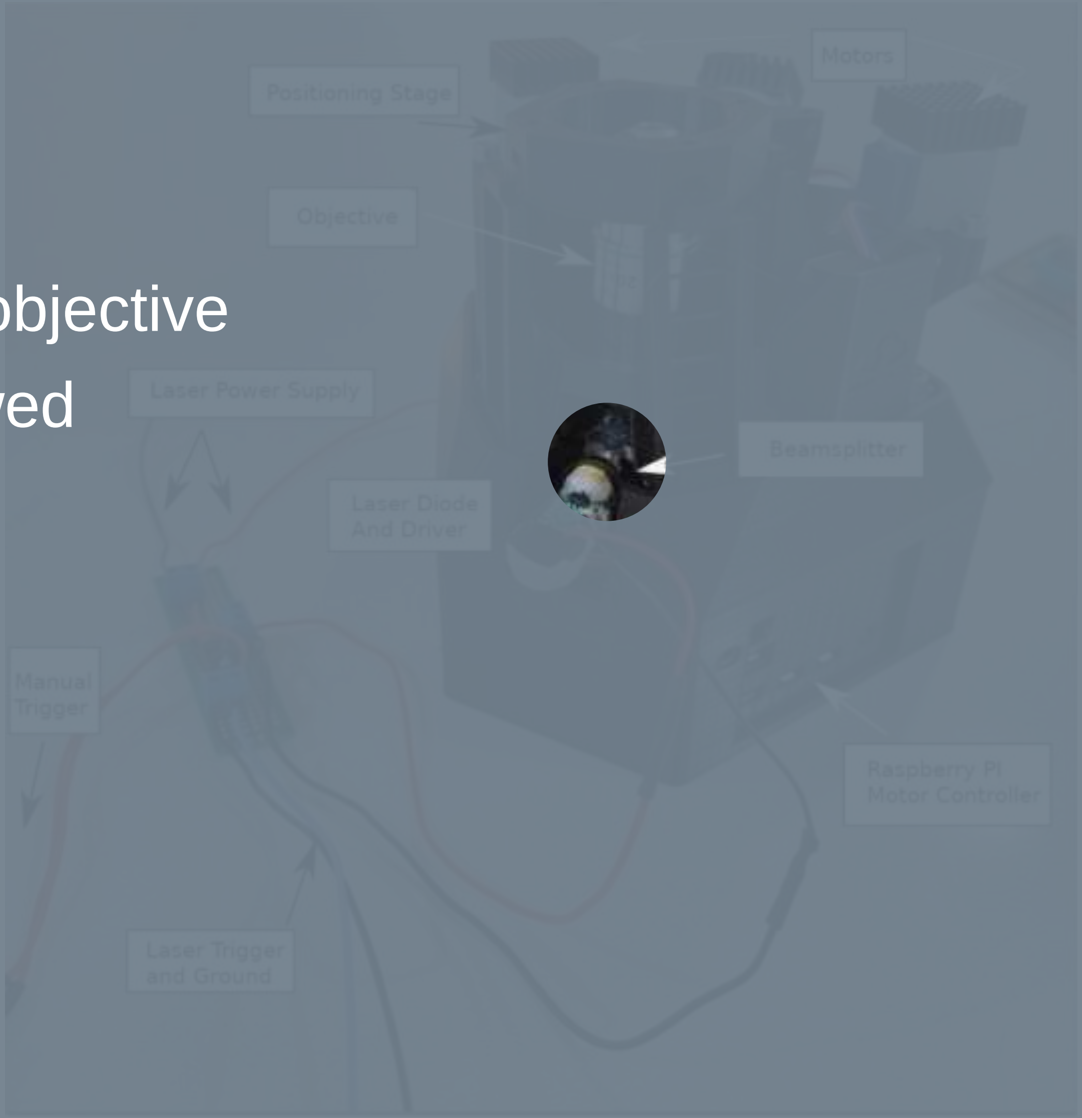
- Mechanical movement of positioning stage
- Gear/stepper driver
- Full X & Y plane

Component Breakdown

Beamsplitter

- Laser beam splitter between camera, and objective
- Allows the target to be fired upon, and viewed

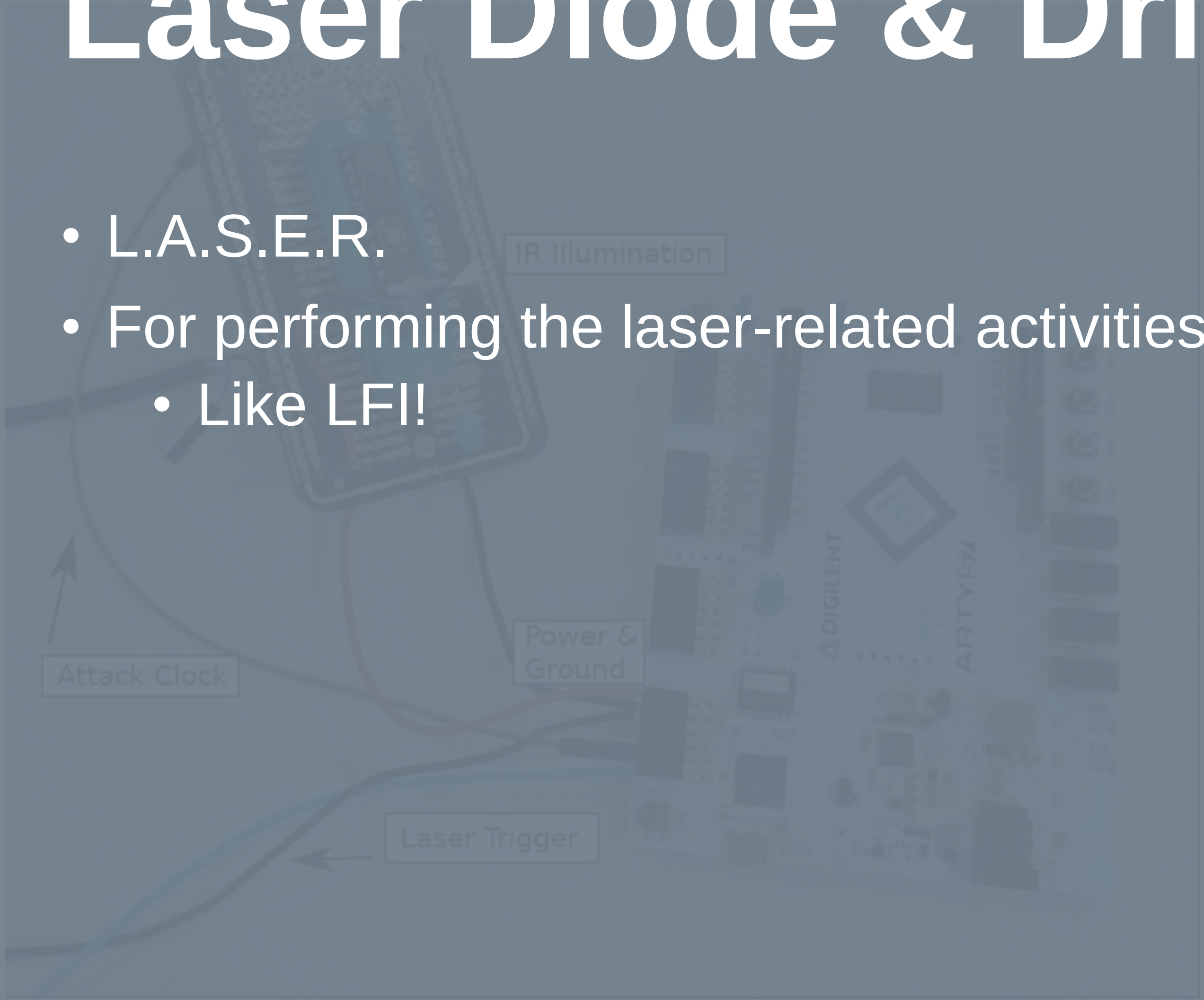


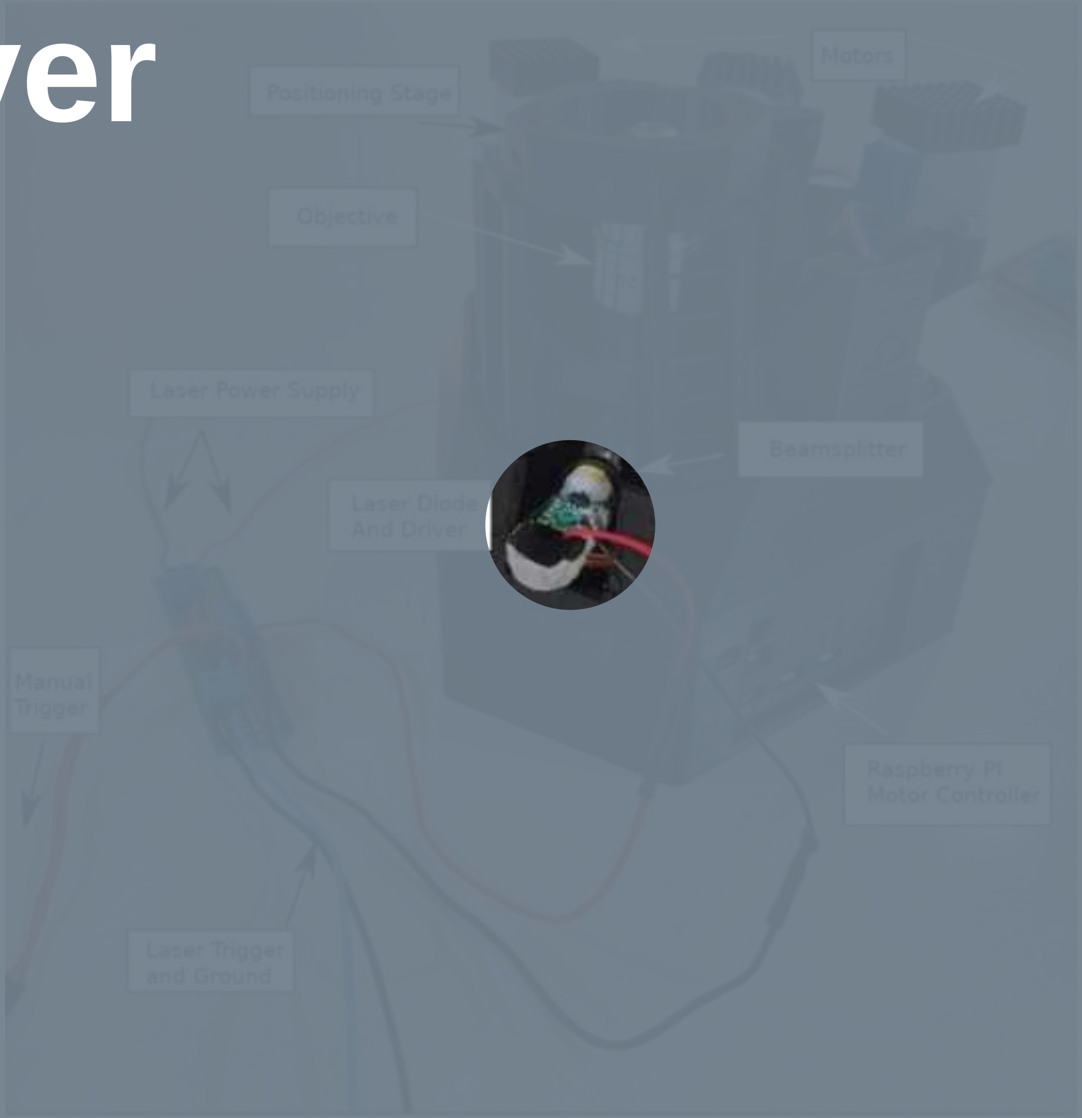


Component Breakdown

Laser Diode & Driver

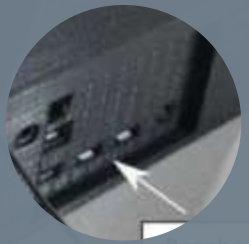
- L.A.S.E.R.
- For performing the laser-related activities
  - Like LFI!





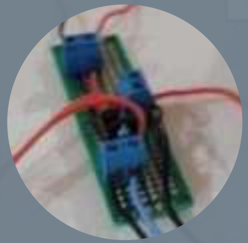
Motor Controller

- The controller for the stepper motors
- Currently a Raspberry Pi 4 and a Sangaboard
- Connects to OpenFlexure software for motor movement
- Let’s an end user control the RayV targeting system

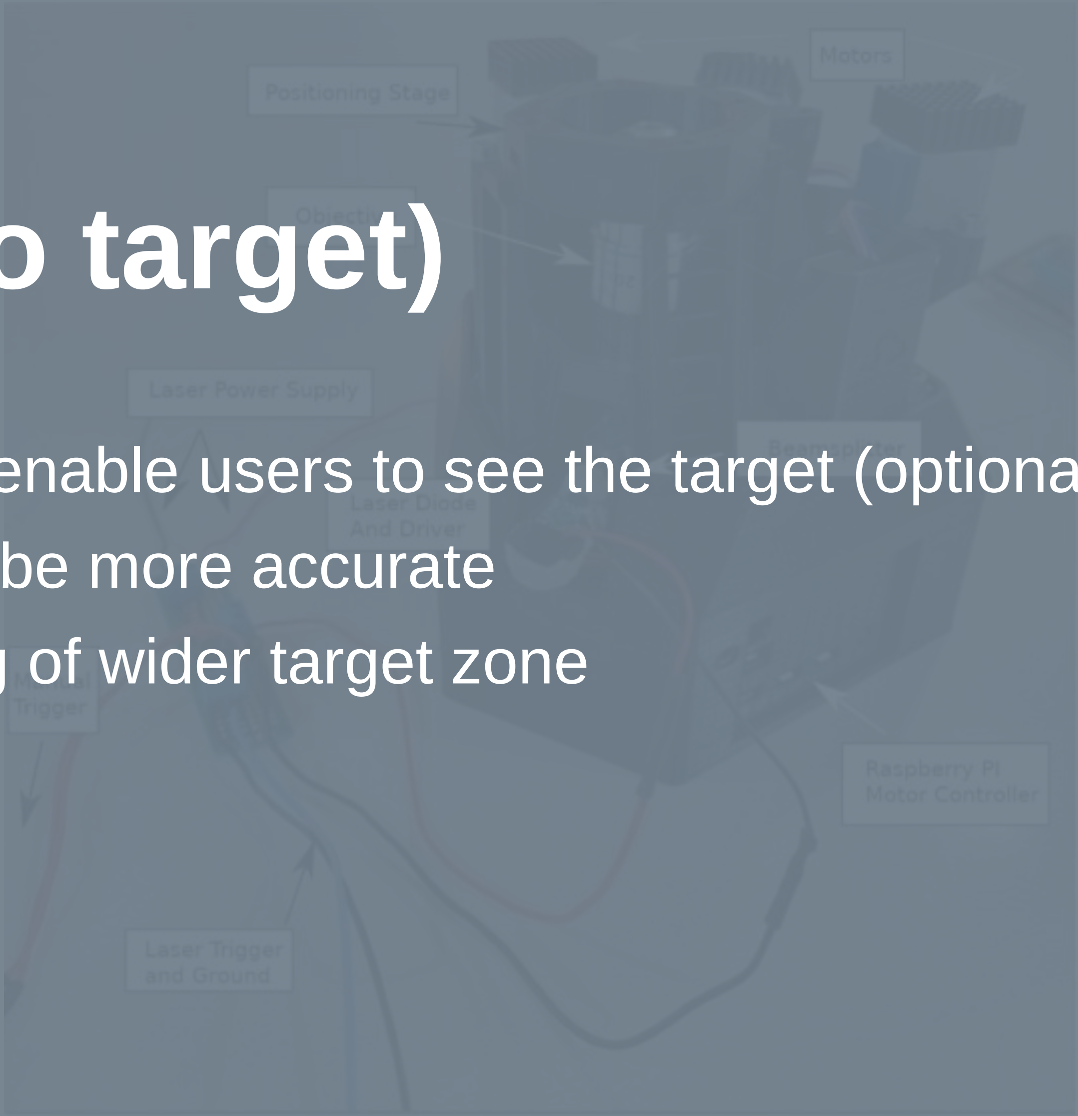


Laser Controller

- Provides Laser power
- Processes Laser trigger
- Provides Manual Laser trigger
- Grounding



Component Breakdown



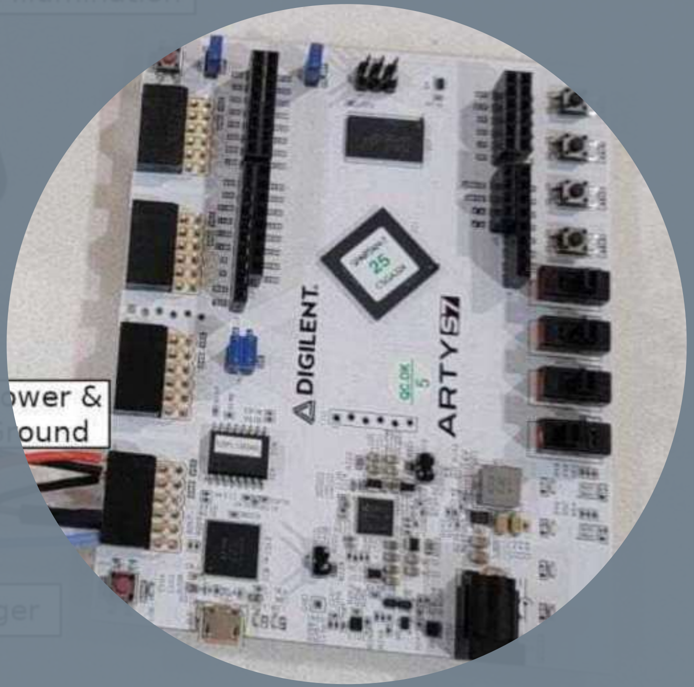
IR LED
(affixed to target)

- Infrared LED to enable users to see the target (optional)
- Enable users to be more accurate
- Enables imaging of wider target zone

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

Component Breakdown

FPGA Board



- Used to trigger and measure when to trigger the laser
- Slows the target clock down to enable the lase to cover its time requirement
- Determines if the laser lased successfully

But does it work?

FIRE ZE LASERS!!!

THE END.

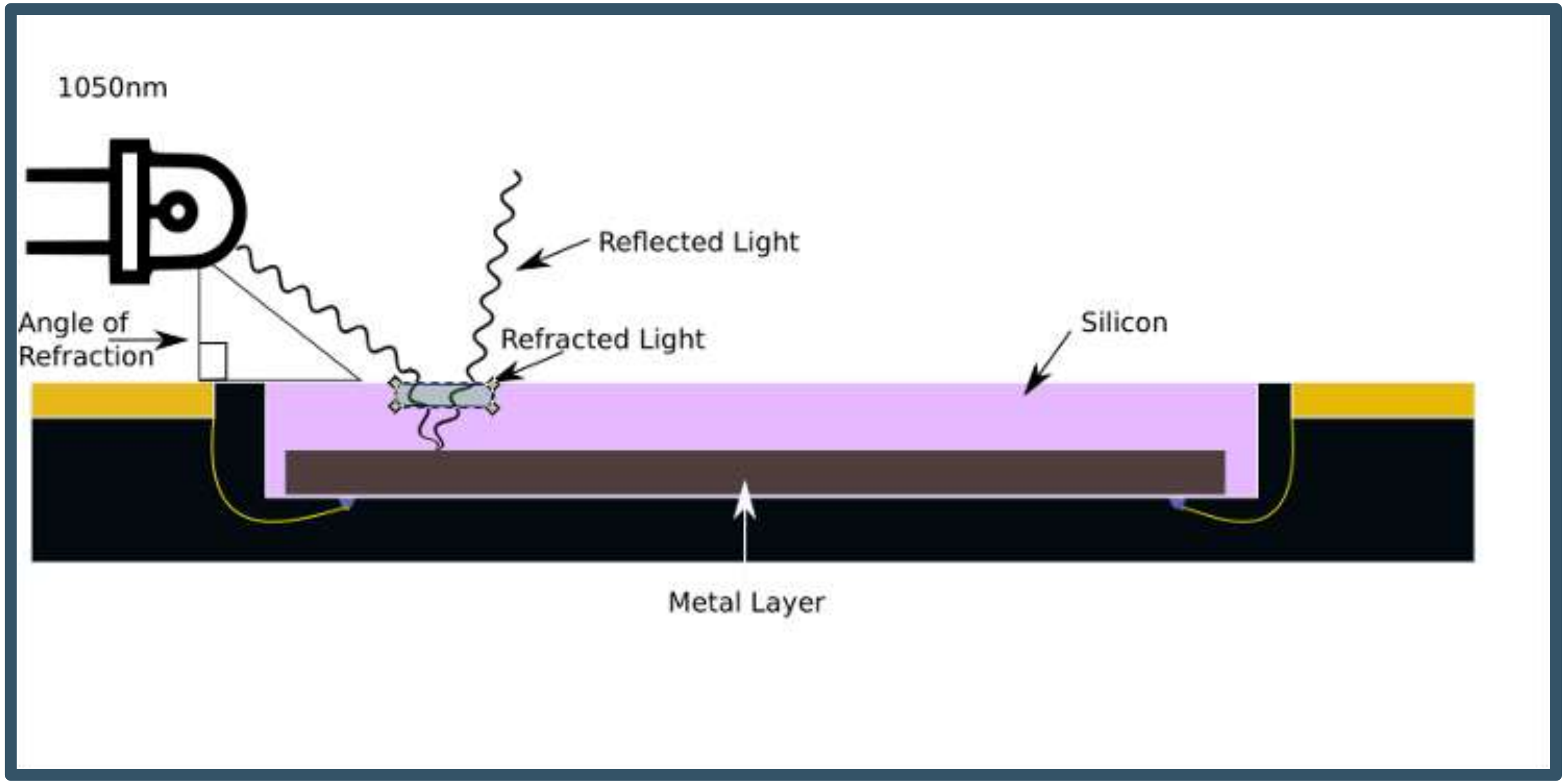
(ok not really)


AND NOW FOR SOMETHING
COMPLETELY DIFFERENT

Infra-Red, In-Situ Inspection of Silicon

I.R.I.S.

Visual Laser Targeting

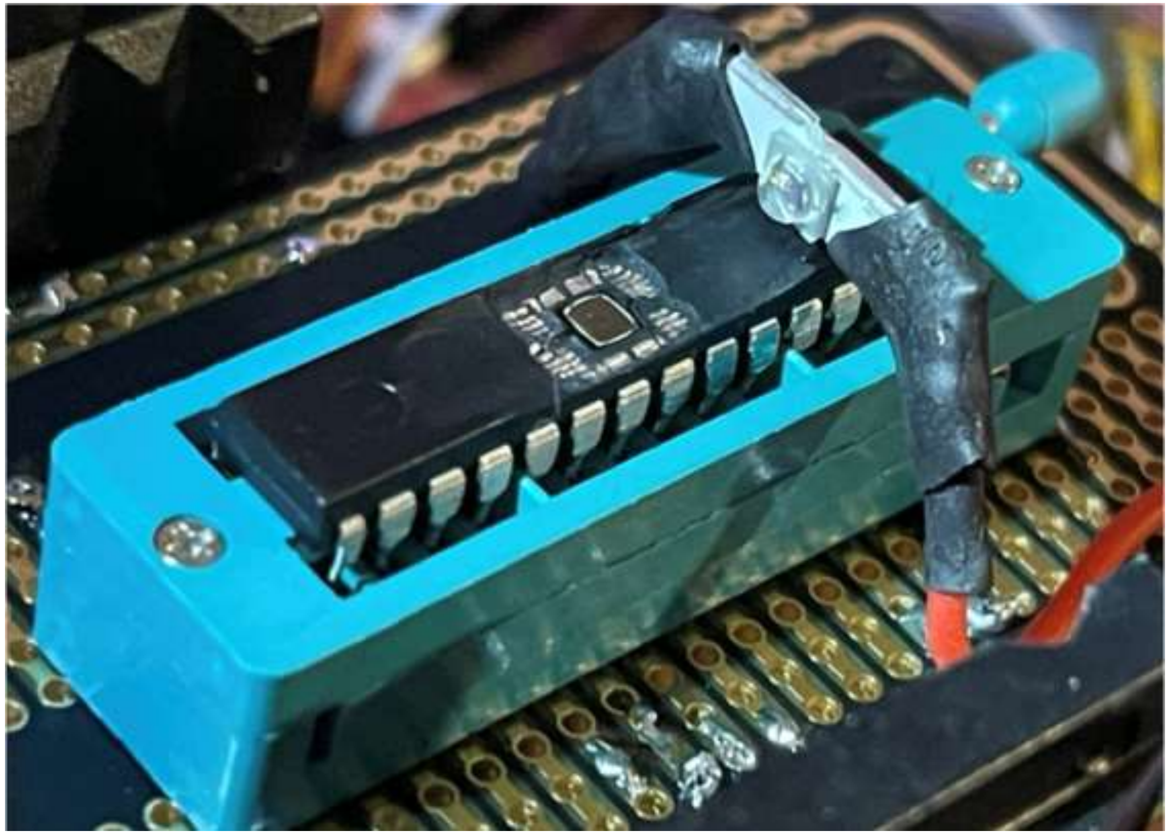


RayV + I.R.I.S.

1050nm Light on a
“800nm” sensor

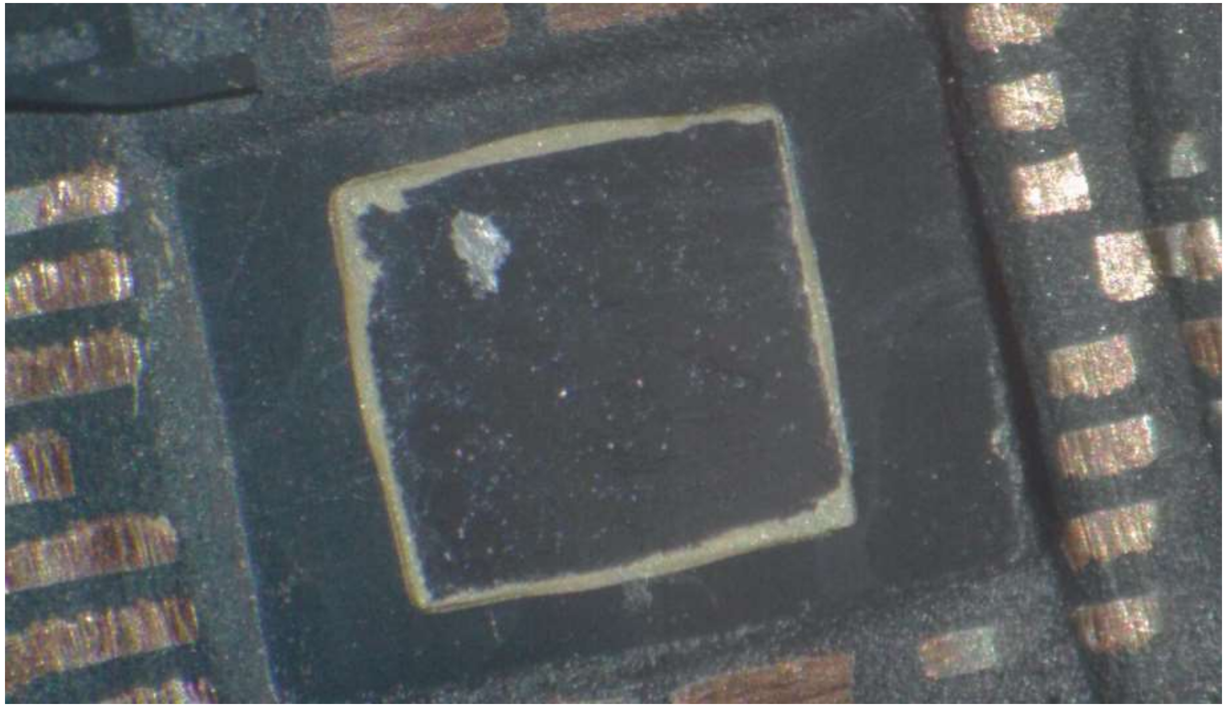
“You can do IRIS with a simple halogen lamp and an IR-pass filter on your SLR” – Phillippe Teuwen

"Visible Light Camera"



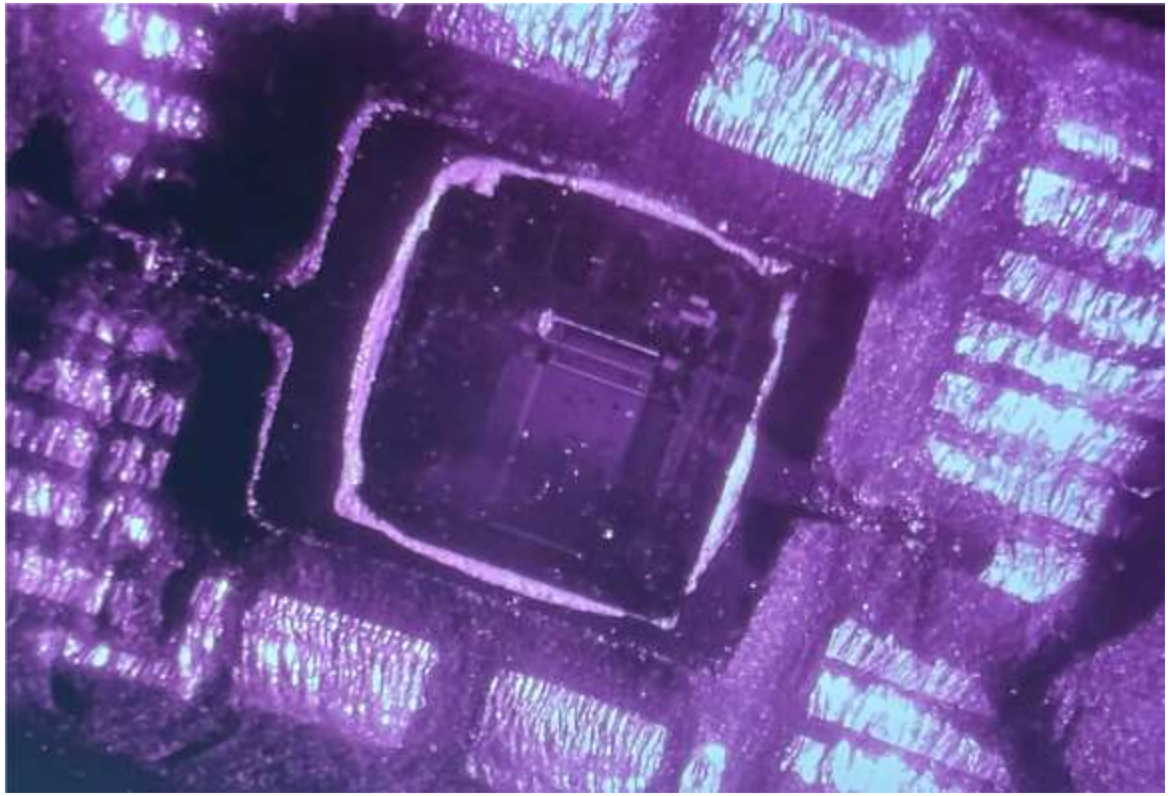
RayV + I.R.I.S.

Visible Spectrum



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

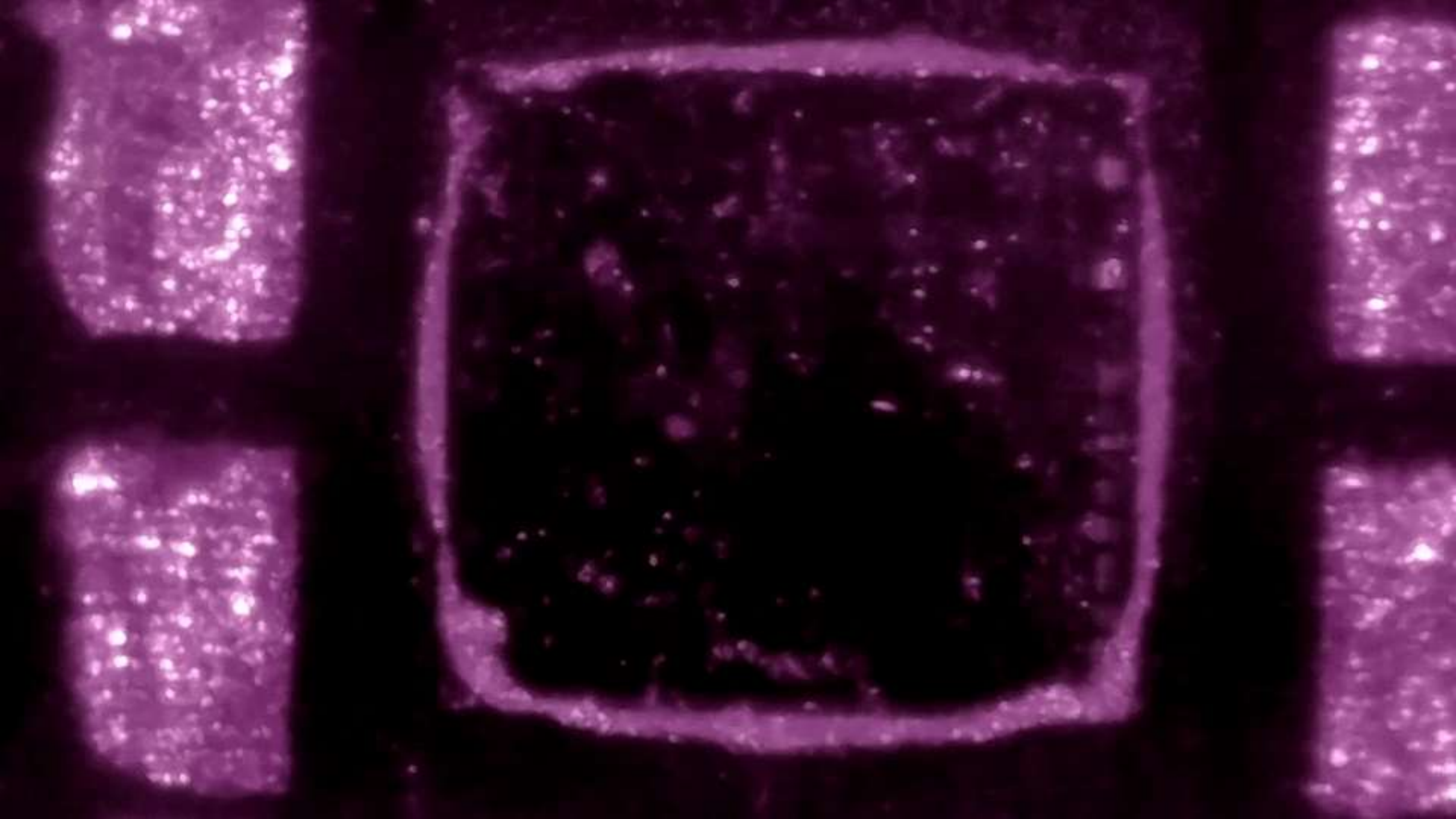
"Invisible Light Camera"



Infared Spectrum

Zoomed In

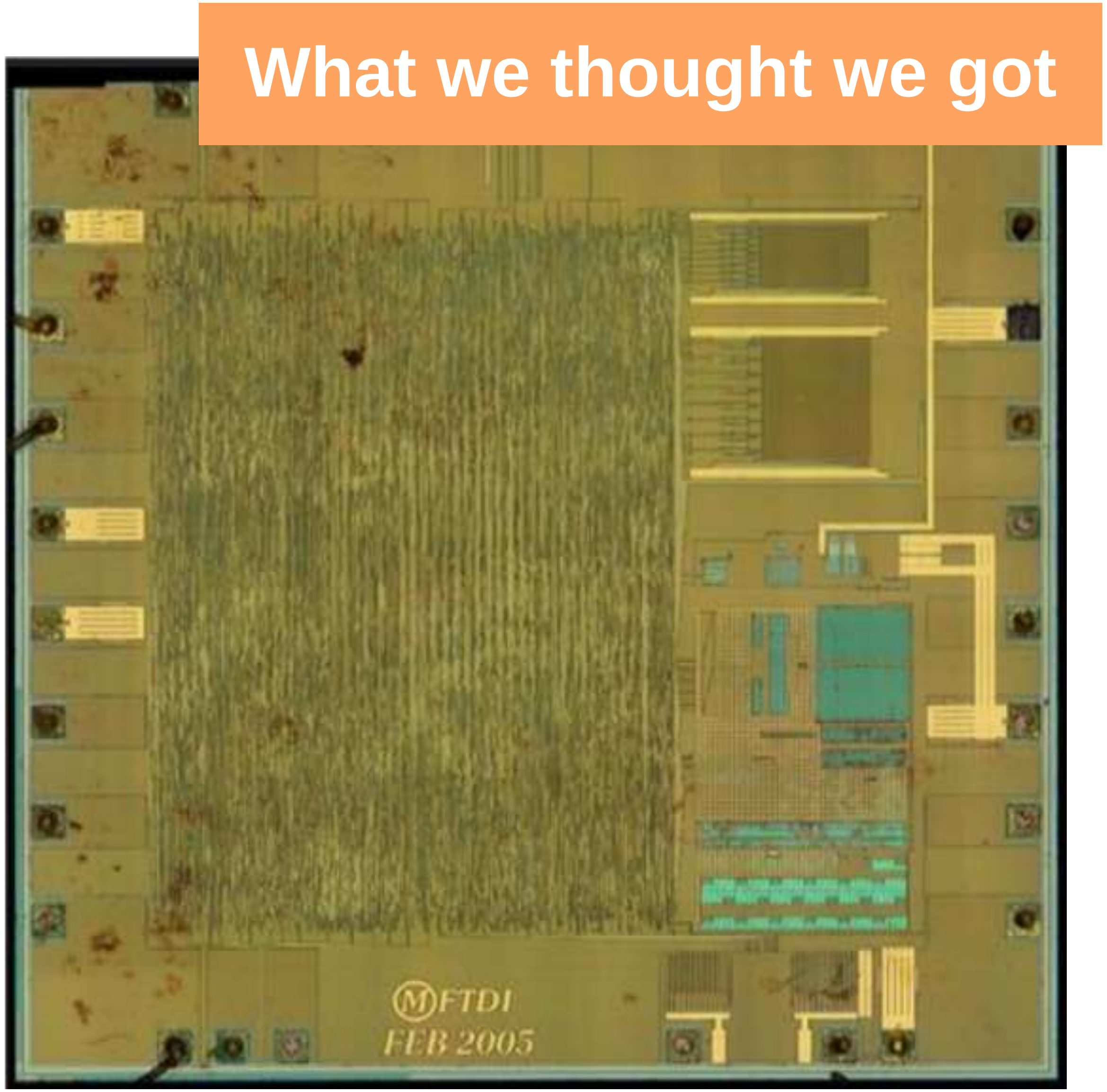
“What are those lines? …I don’t know, seems like some kind of circuitry!” – Team LOREM



But wait, there’s more!

Happy Accidents can happen

FT232r "Alternative"



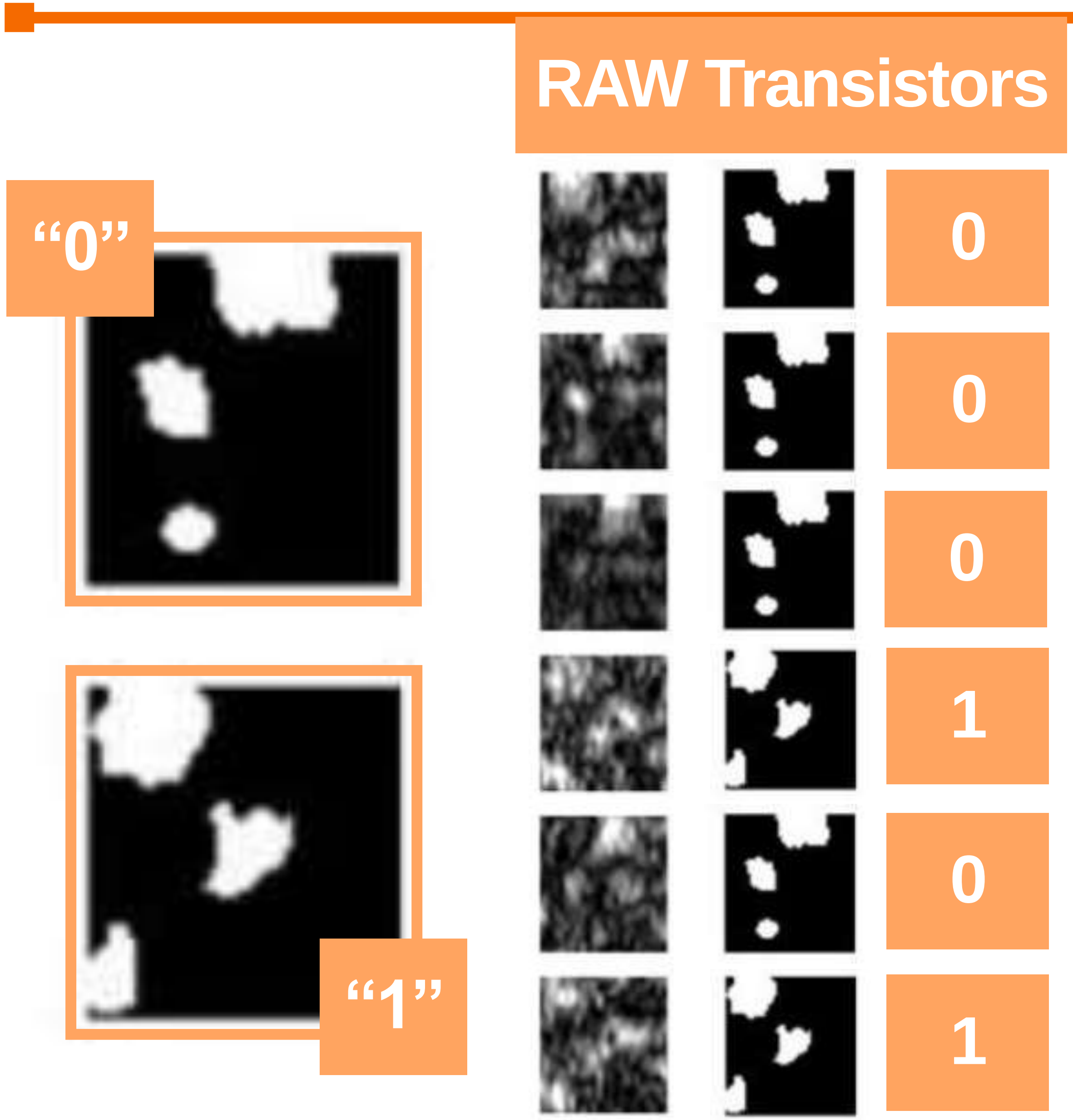
"Yeah…Huge advantage to backside is that you just don't have to be gentle" – Chas Becht

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)



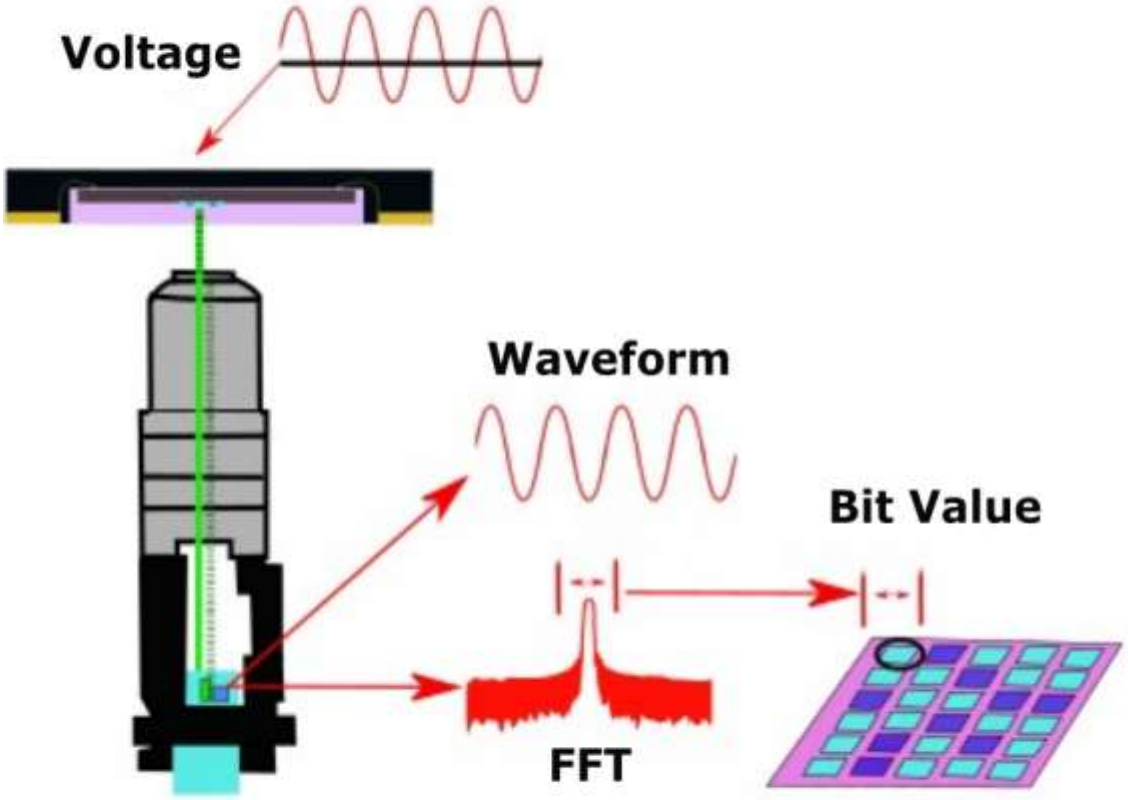
In the beginning the Universe was created. This has made a lot of people very angry and been widely regarded as a bad move. – Douglas Adams

How?

- Changes in **voltage**, changes the **absorption** (and reflection) **rate of silicon**

- **Electro-Optical Frequency Mapping** (EoFM) can be used to detect these fluctuations in absorption via **state changes**

- In LLSI, causing a **voltage ripple** on the target's active transistors acts as a readable **modulated signal**



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.

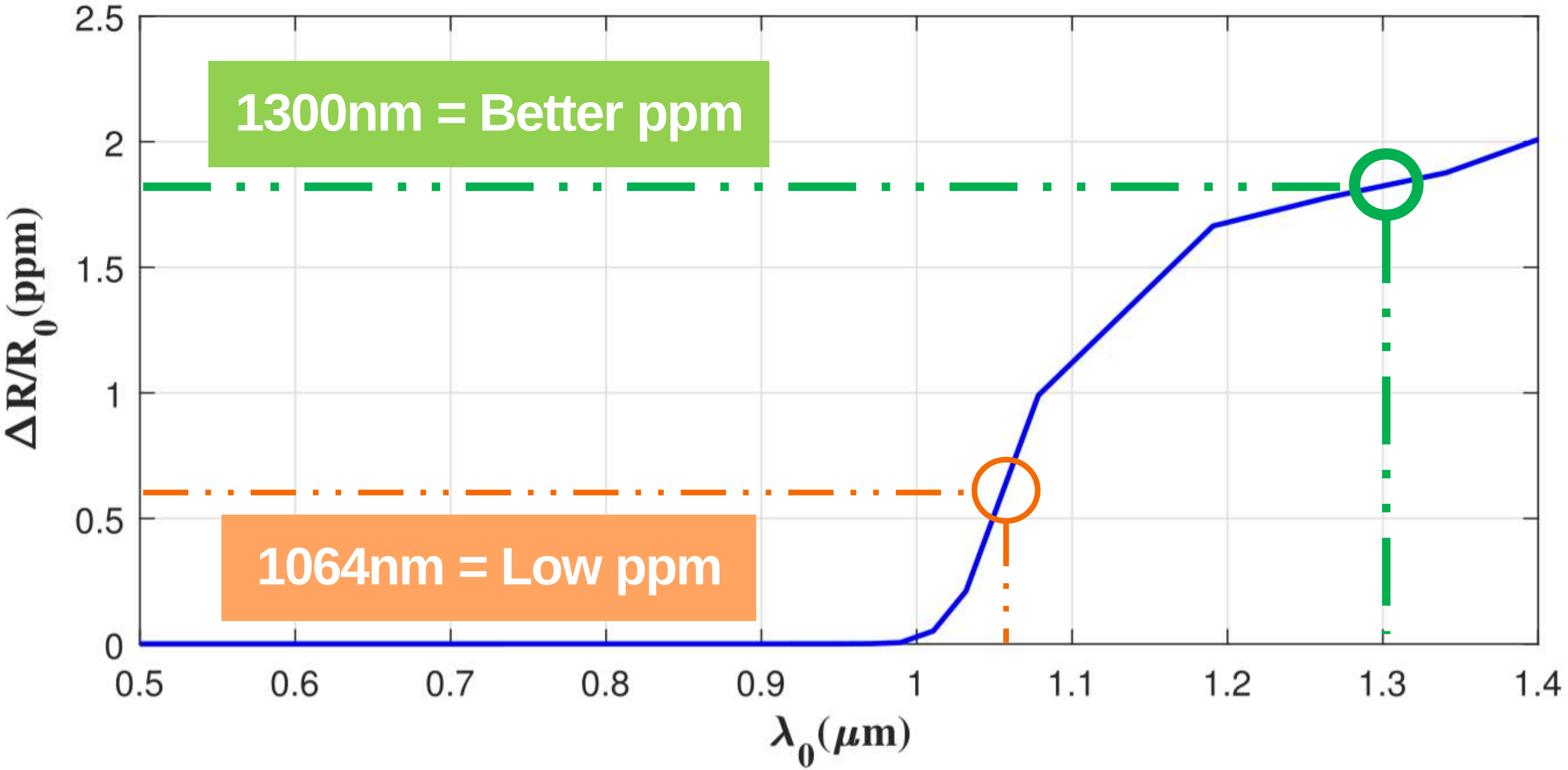
Operation: Over Achiever

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

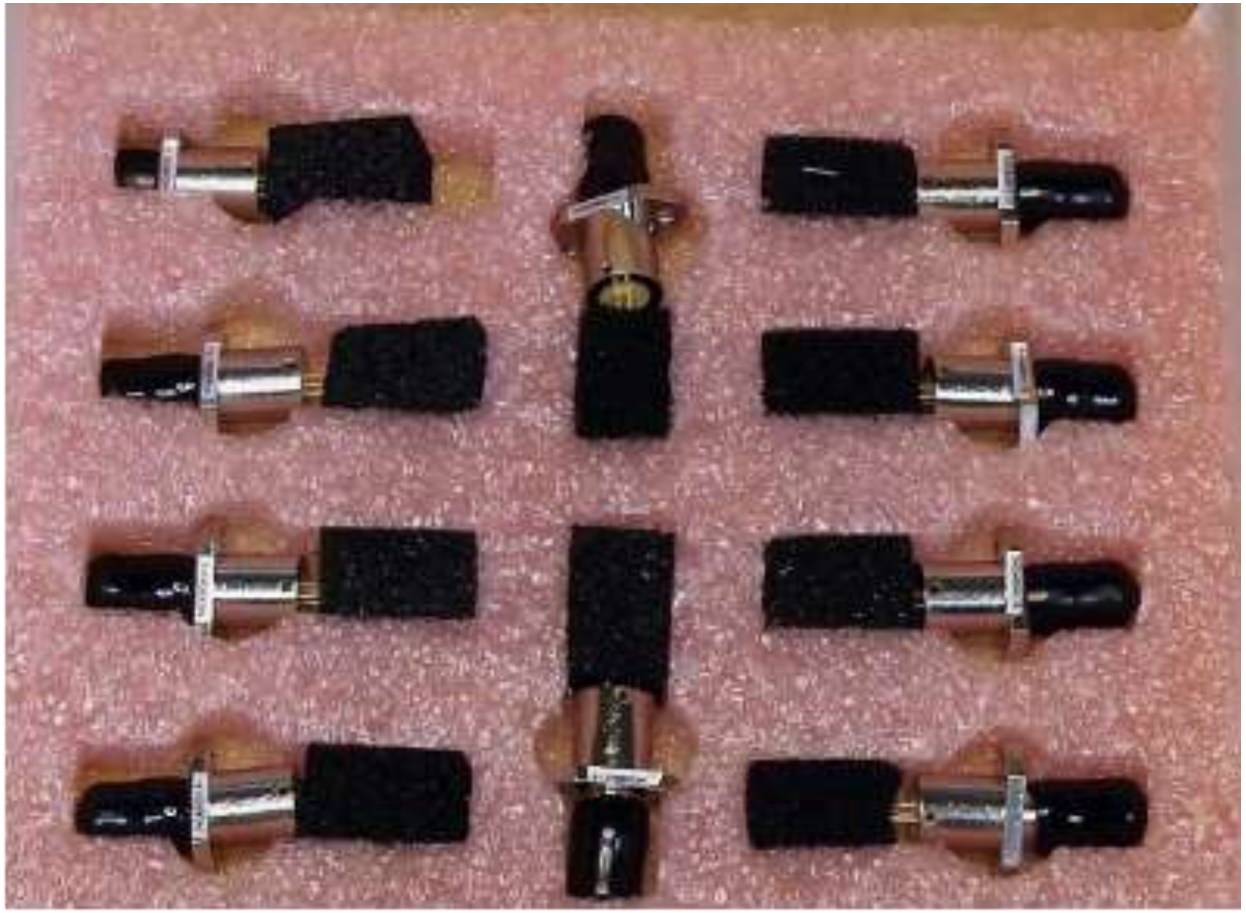
Which Laser?



1300nm = Better ppm
1064nm = Low ppm
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
$\Delta R/R_0$(ppm)
$\lambda_0(\mu m)$

Why 1300nm, Specifically?

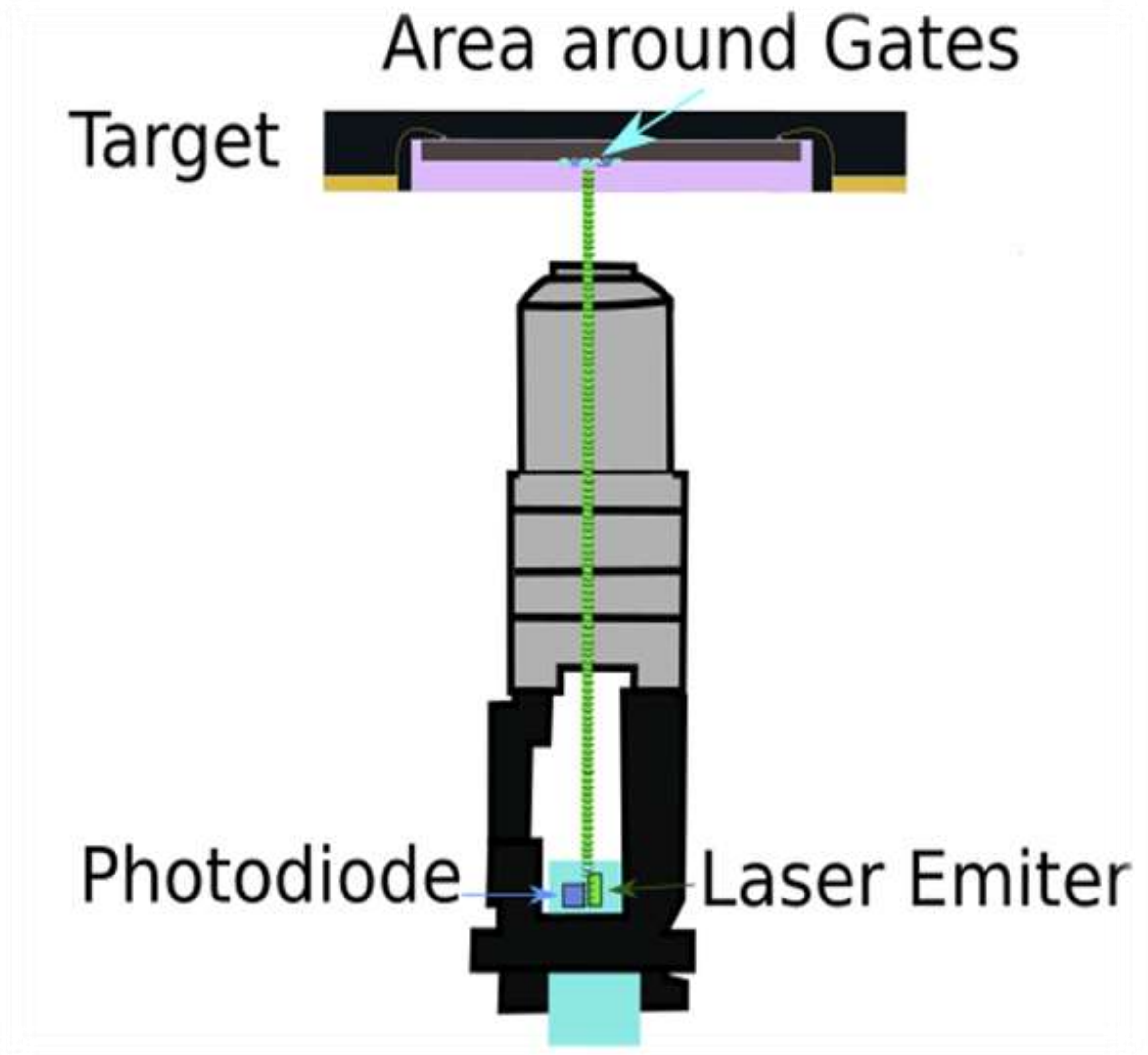
- Incredibly high in supply, and very inexpensive ($6.00 USD)
- Lasers come with their own sensor for self-regulation
- For $6 USD we can get a 1300nm laser **WITH** a photodiode
- Two birds, one stone



Self-Mixing Interferometer

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

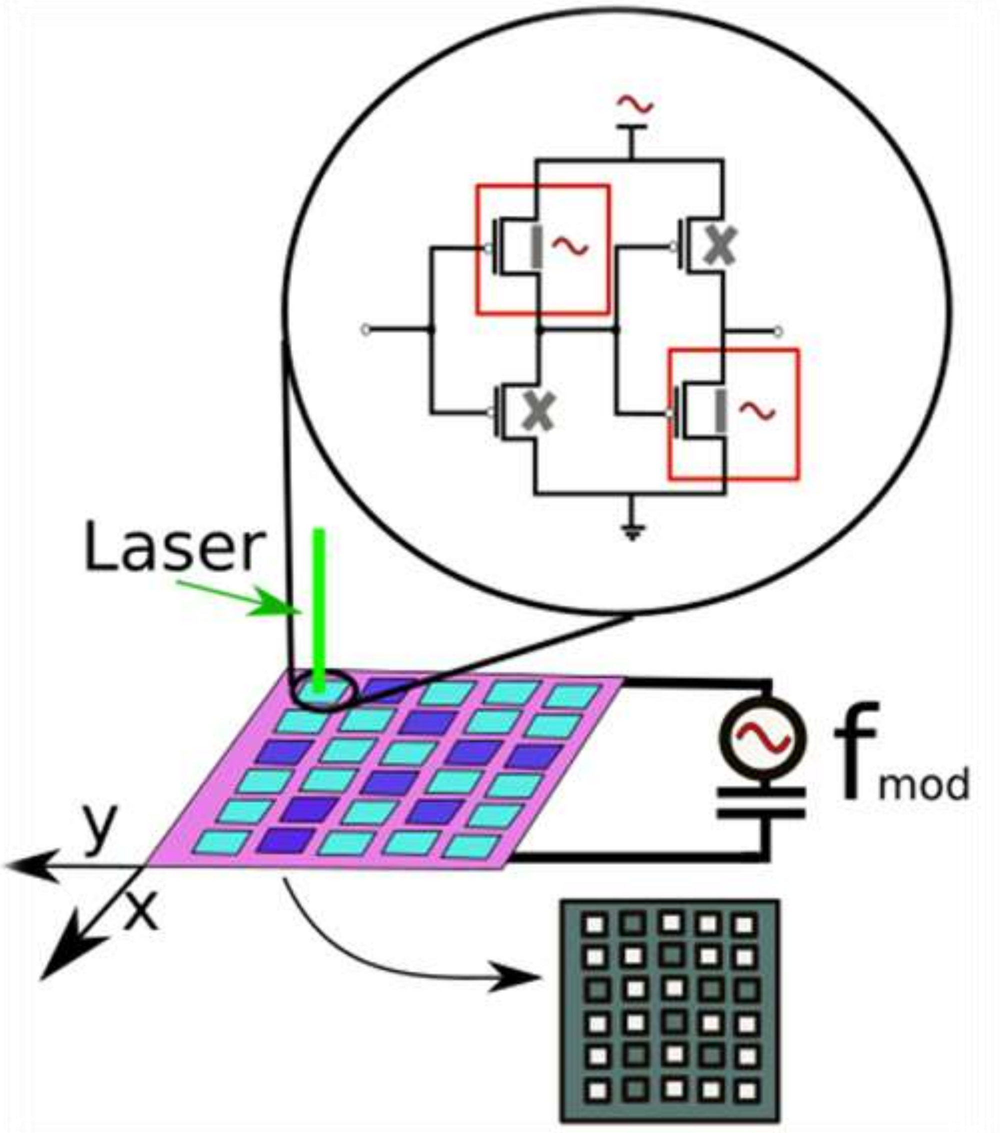
- If it can measure changes equal to the size of its wavelength, it can also **measure variations** in silicon absorption



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

Putting it all together

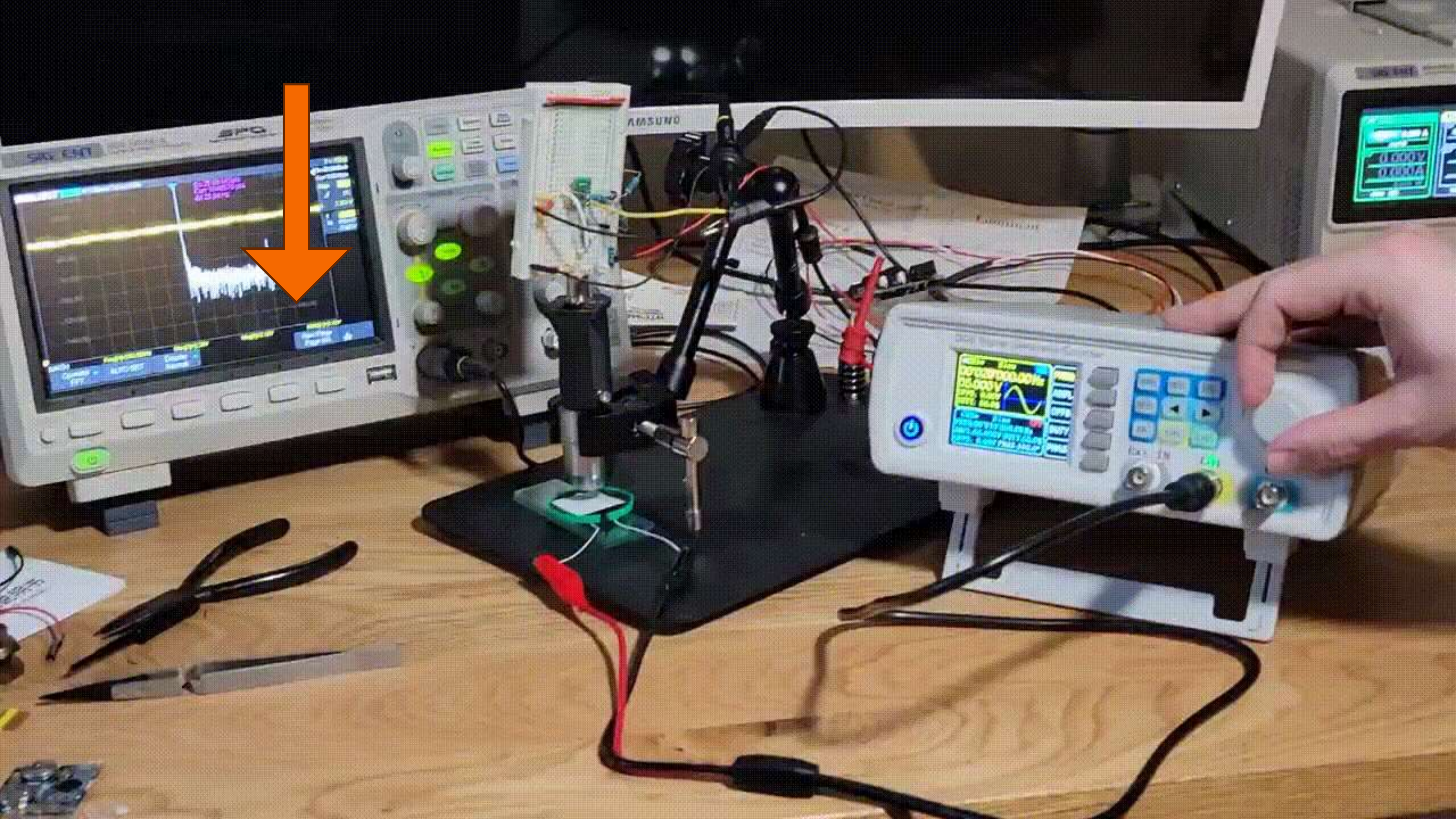
- Pause instructions and memory in the transistors
- Send a signal through the active transistors (via modulation of voltage)
- Activate laser beam and scan beam over target
- Read the sent signal through the beam's reflection



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 Convolutional Neural Networks

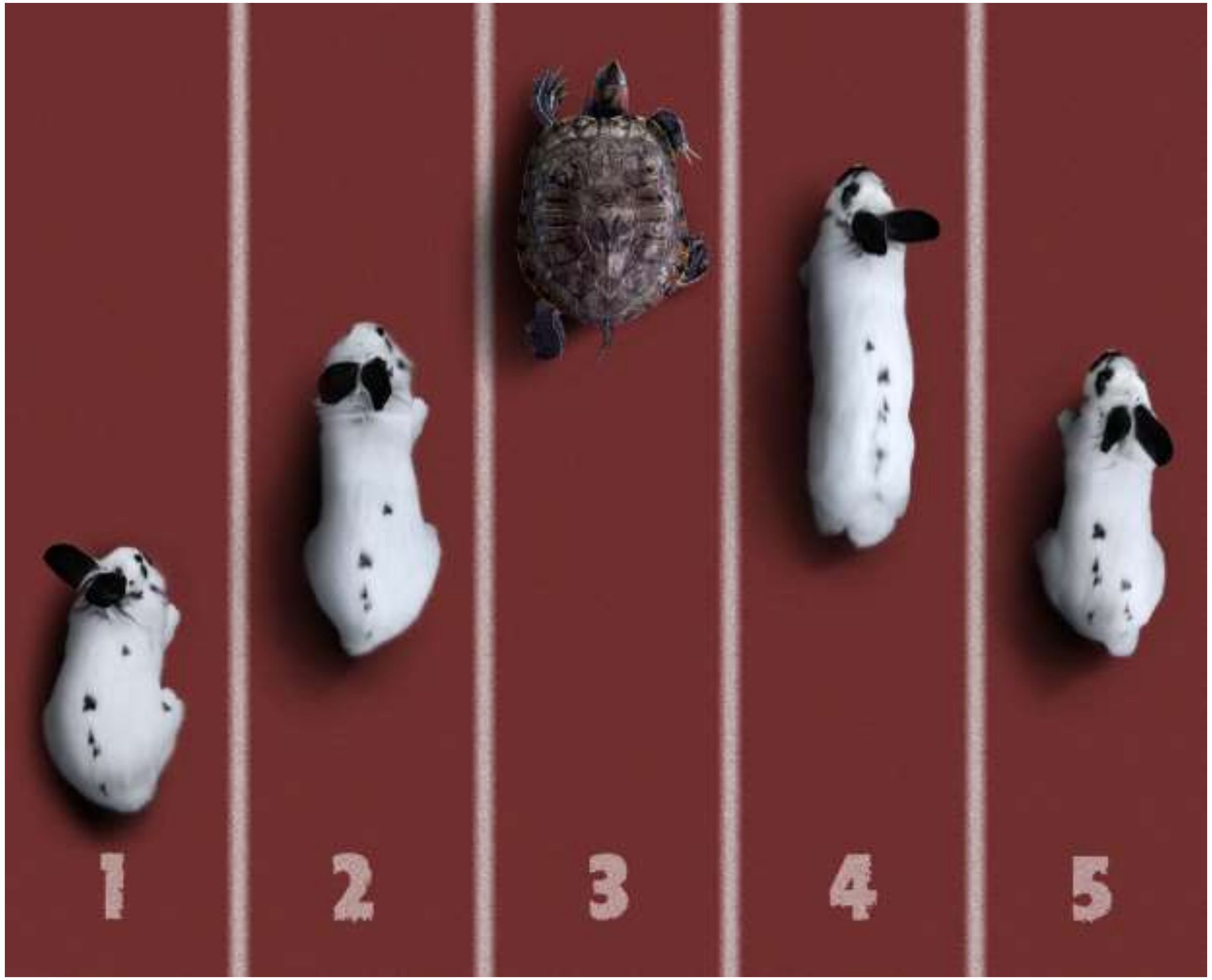
Statistical Matrices & Math

- The signals received from an LLSI need to be **mapped to the chip**
- Every chips **memory is unique specific to itself**: not all transistor gates 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

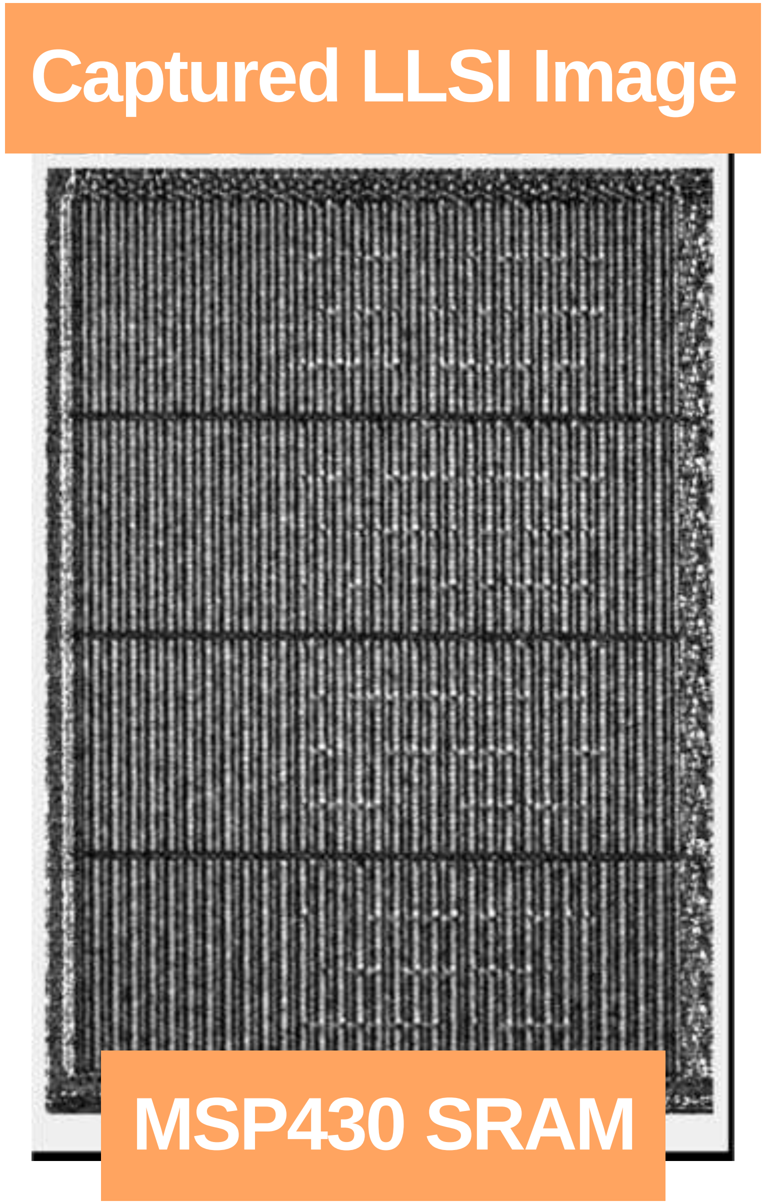
Black Hat has deadlines

- Scanning a chip with Laser Scanning Microscope (LSM) is slow
- The process to design a low noise, band pass filter and demodulator to isolate signals around 1ppm is slow
- Combining an active LLSI and LSM to train a model, is really, really, slow



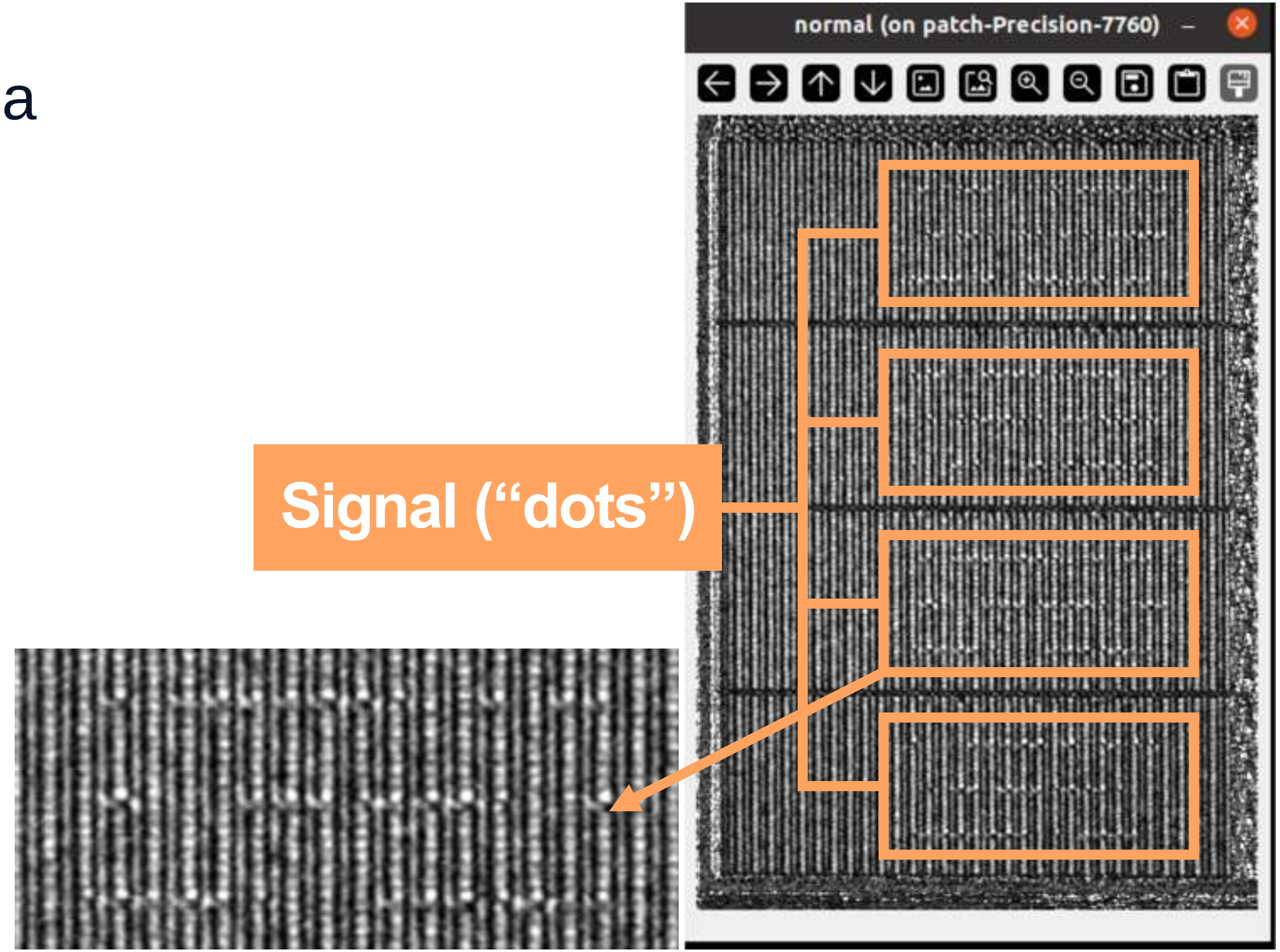
Training with Published Data Sets

- Each instance of training data has a **known, programmed, 512 bits** of data stored in memory
- Working with **known data points that are user programmed**, allow the model to later identify in unknown data sets (once trained)
- Collection contains randomized and zeroed data sets, outside of the 512 bits
- This is a faster method to train for a POC



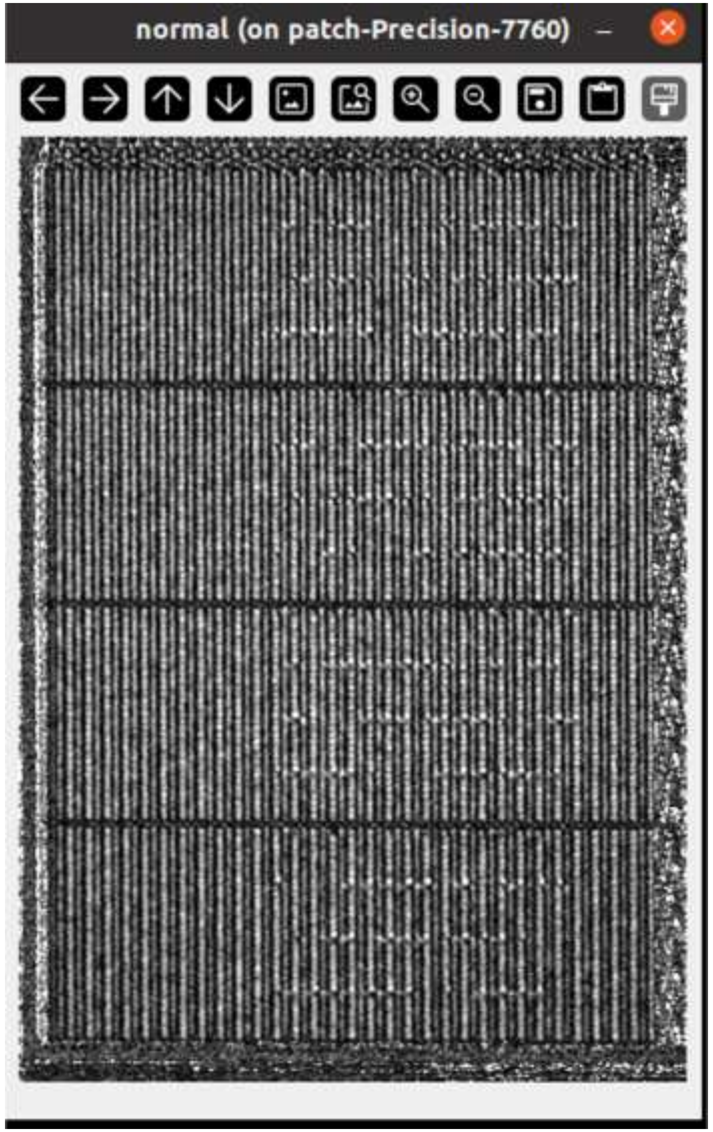
Identifying Data in LLSI

- This is an LLSI capture of a **MSP430 SRAM** block
- The SRAM block contains **512 bits** of **known programmed memory**
- The "**dots**" are the **modulated signal representing** the 512 bits



The data needs to be seen

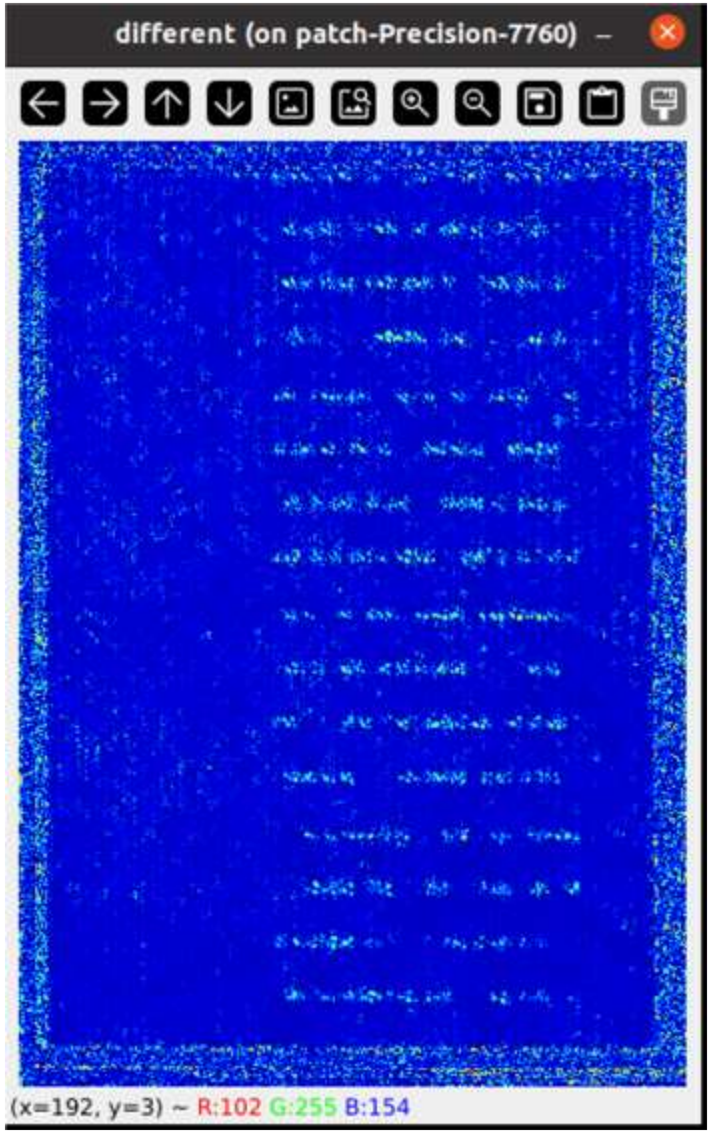
- We need to make the data more readable
- Subtract a random LLSI image from it (to isolate the 512 bits)
- Put the results in the blue channel…



I tried to find a quiet place in a library, but it was like looking for Waldo in a crowd of identical twins.

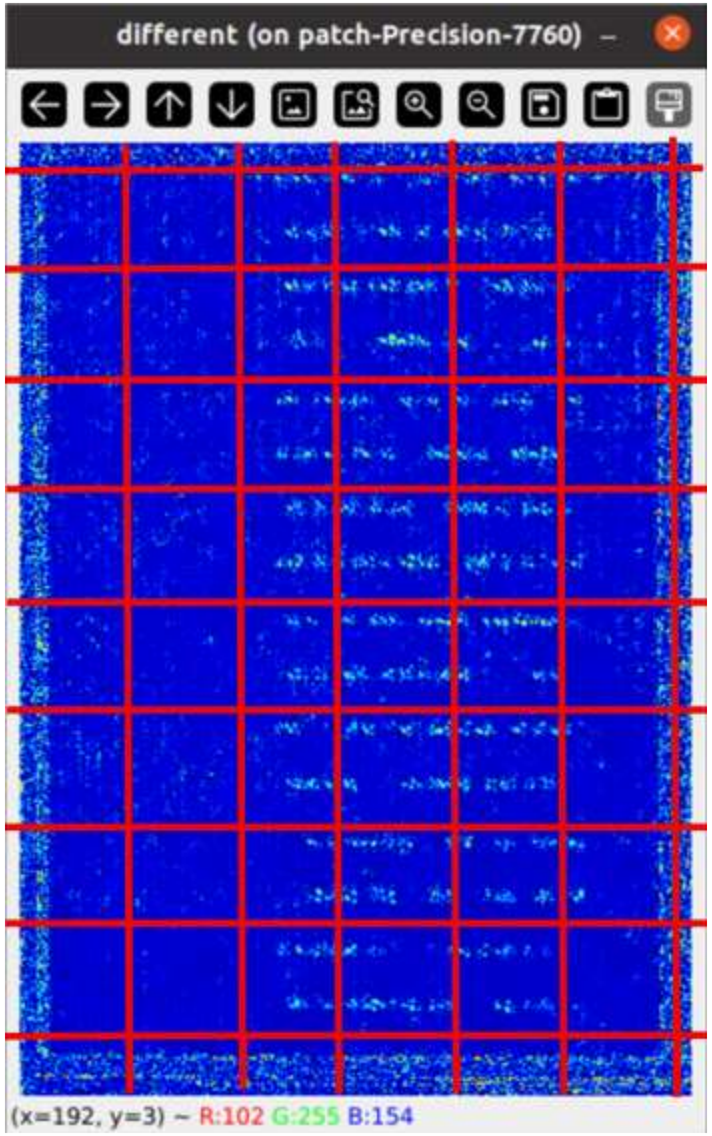
The data needs to be seen

- We need to make the data more readable
- Subtract a random LLSI image from it (to isolate the 512 bits)
- Put the results in the blue channel…
- ….and Voila!



I can see, but I don't understand

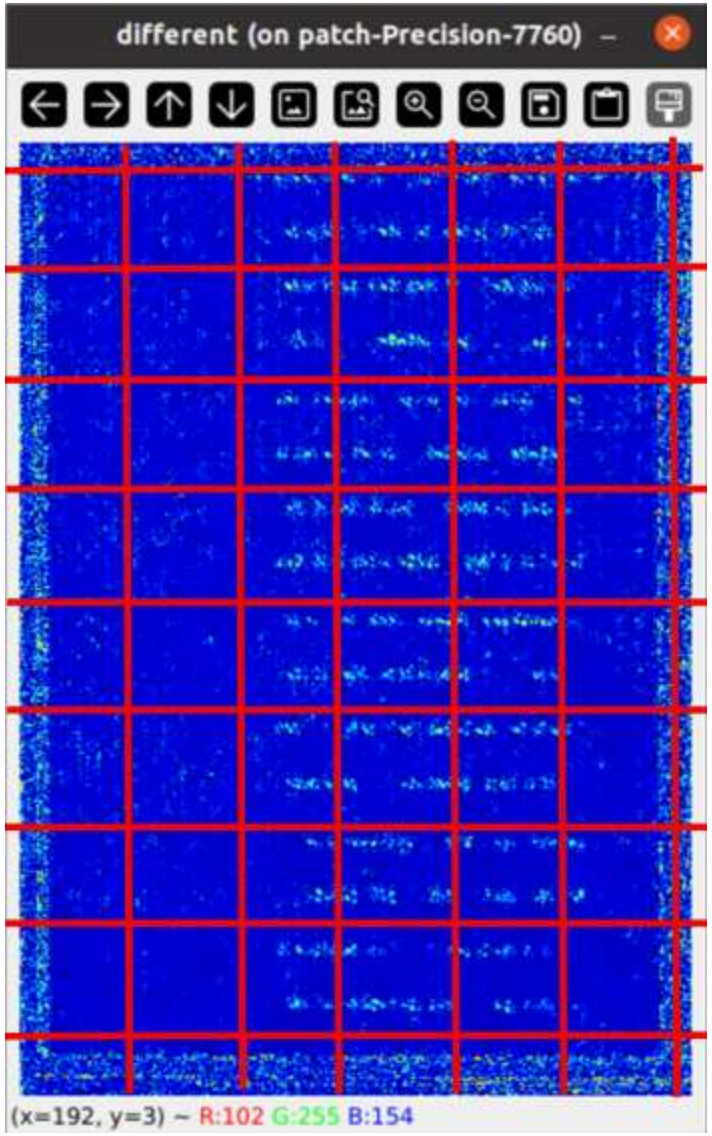
- Next is to help the model identify **where** the user programmed 512 **bits are stored**
- Divide the SRAM into a **search grid** so that we can minimize the chance of bit collisions
- The **red squares are areas that we can search** that should aid in isolation of bit similarities



“Special Thanks to all the Wi-Fi endpoints you crashed as a result of having to serve this PowerPoint to SharePoint” – KMAP

Finding the Right Segment

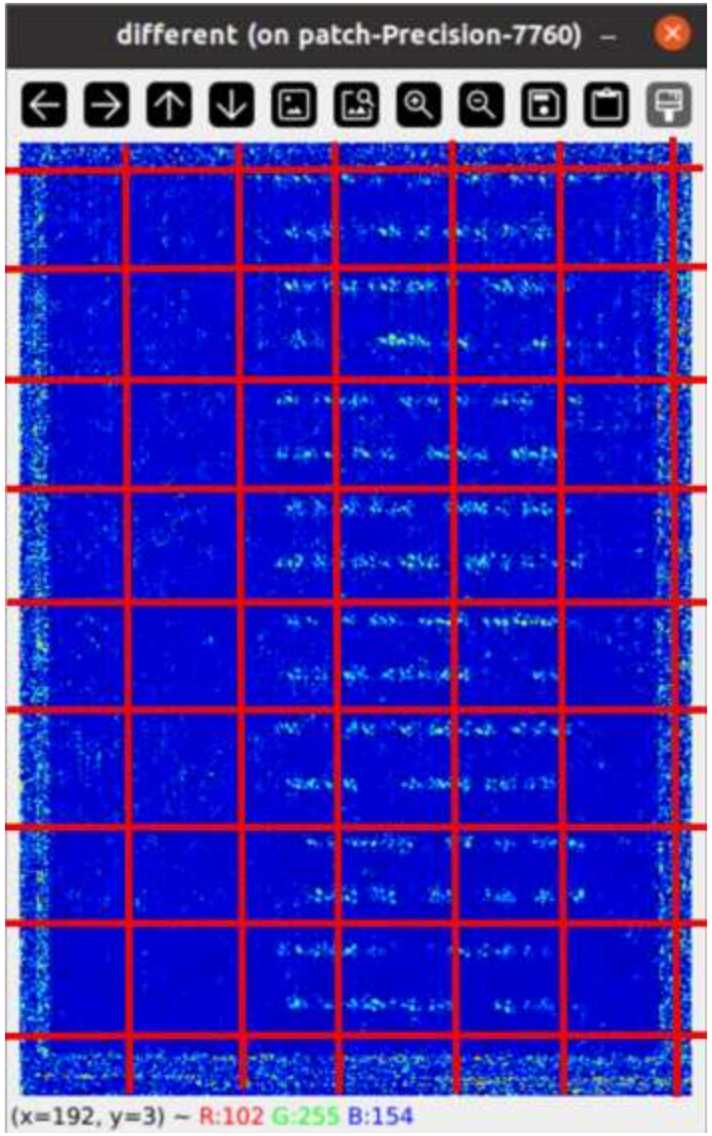
- Each segment will have a number of bits.
- We need to know which segment has the bits we are looking for.
- Here is how we search the segments



“I may not have gone where I intended to go, but I think I have ended up where I needed to be.” – Douglas Adams

Segment Searching

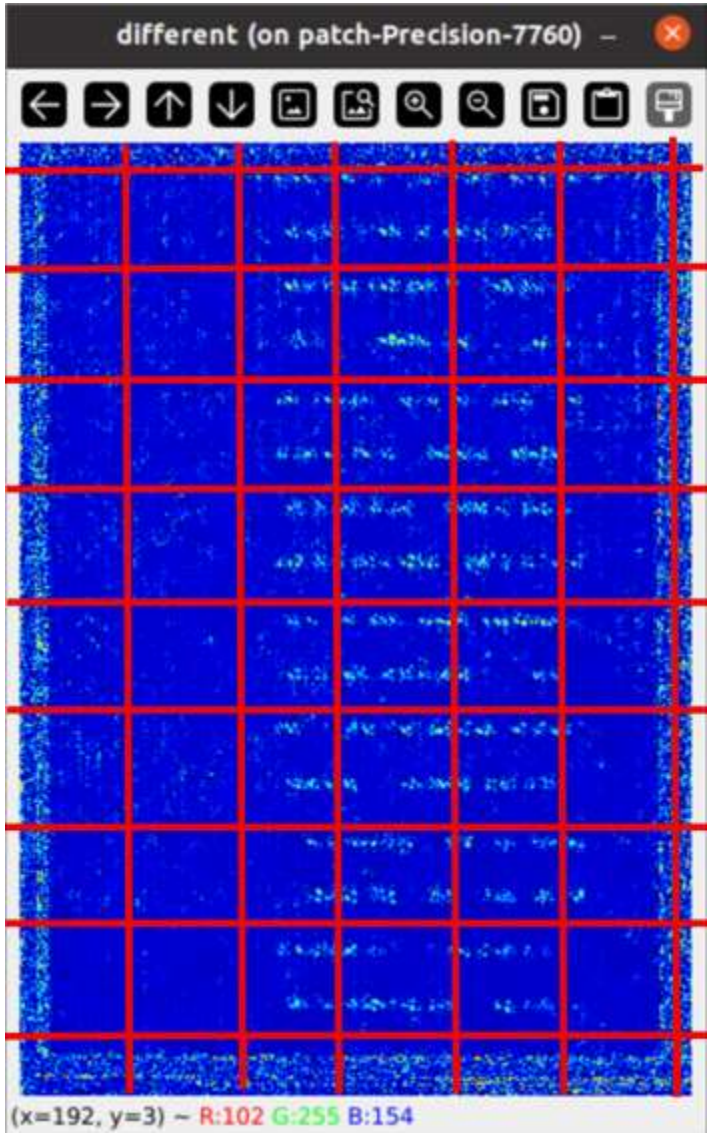
- The model can isolate bit locations by identifying segments with similar binary values, **except for 1 bit**
- Example: the 512 bits contains a segment that contains **1101011** and **1110111**
- By using an absolute diff, **001000** would cause an **observable change**, representing **1** or **0**
- Change represents location of **where** a 1 or 0 is in SRAM



"I may not have gone where I intended to go, but I think I have ended up where I needed to be." – Douglas Adams

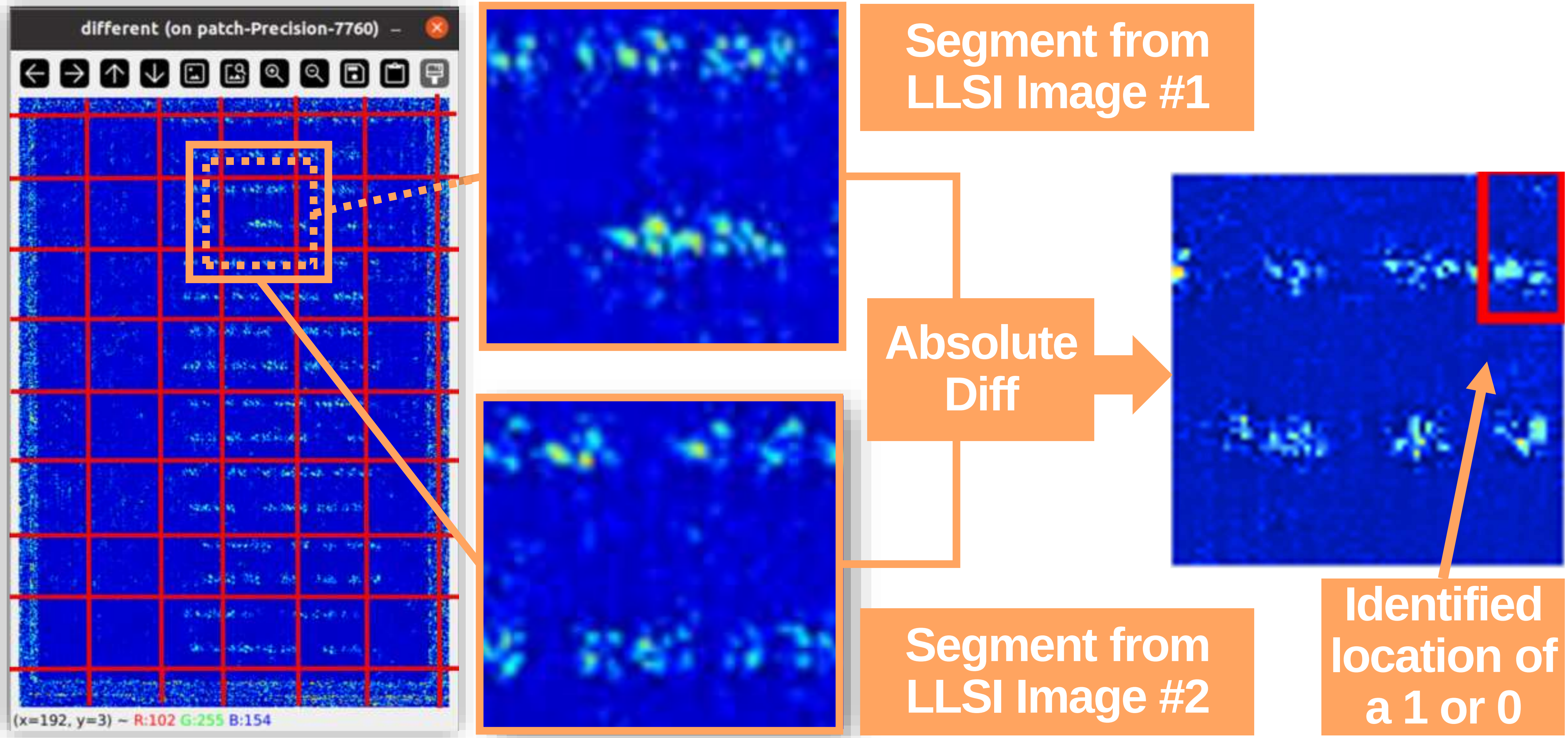
Segment Searching

- If time is not an issue, there are other ways to identify **bit placements**
- Example: flashing one 512 bits with all **11111111** and the other with all **00000010** where the 1 would be the image to help the model identify **that specific bit location**
- By using an absolute diff, only a **specific segment pair** would cause an **observable change**, representing the **location** of that **1** or **0**
- **Repeat** 512 times to cover all areas (or use maths to make this more efficient)



"I may not have gone where I intended to go, but I think I have ended up where I needed to be." – Douglas Adams

Segment Search-Bit Areas



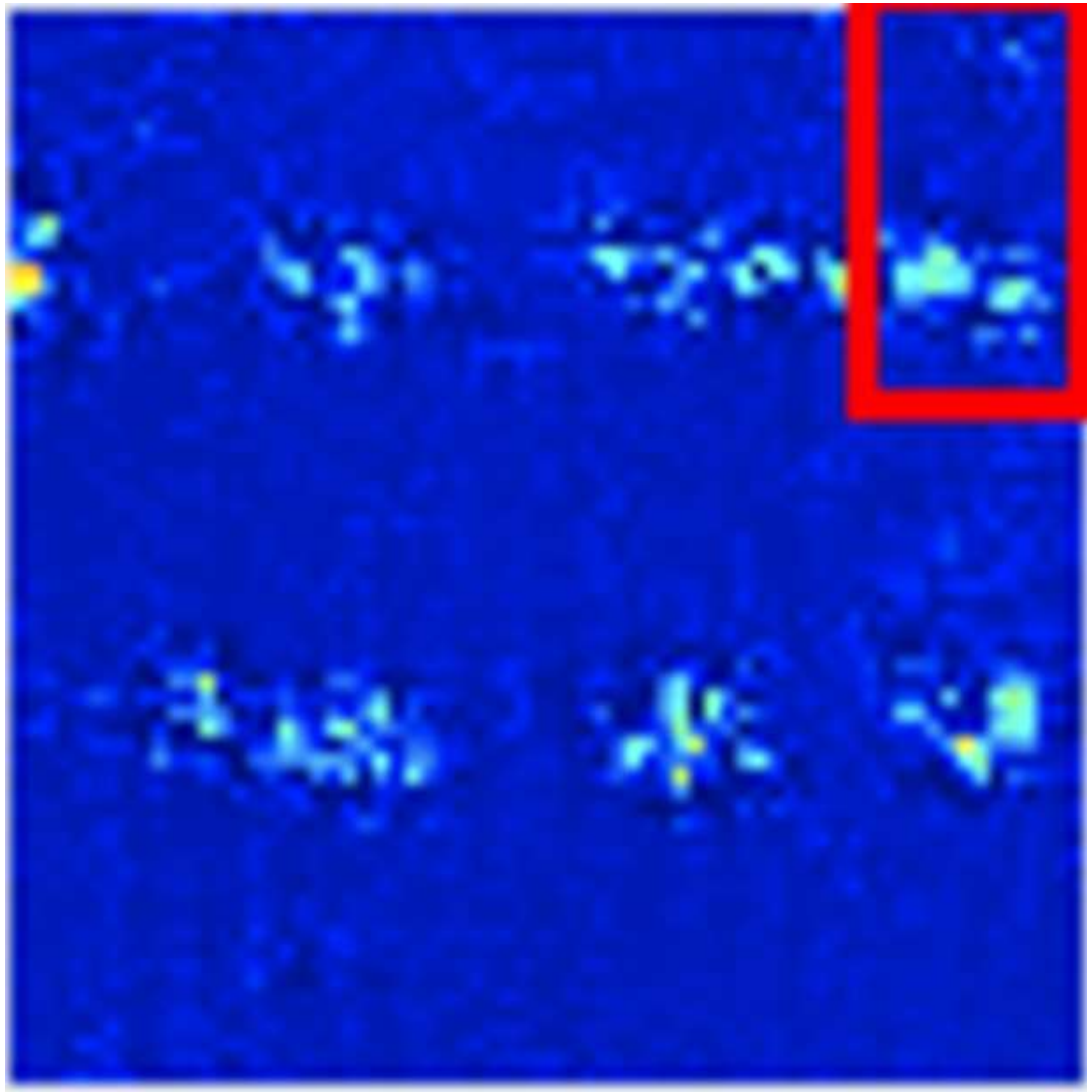
"I may not have gone where I intended to go, but I think I have ended up where I needed to be." – Douglas Adams

Segment Search-Dataset

- With many iterations, and a proper dataset an **understanding of where bits are stored** can be formulated

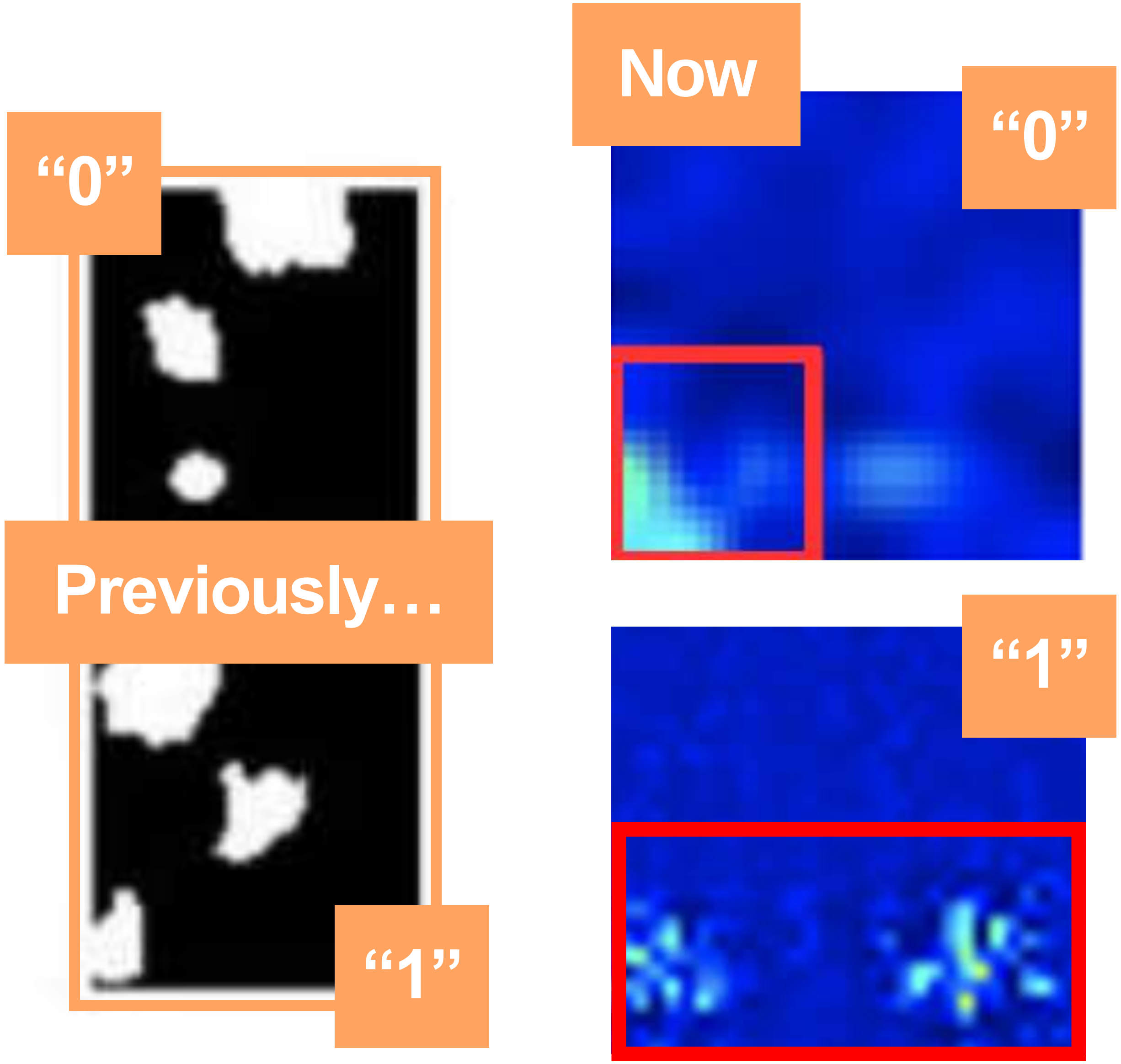
- Next step is to identify **WHICH** bits are “**1**” and “**0**”

- To do this, the model can use **supervised learning**



Success!

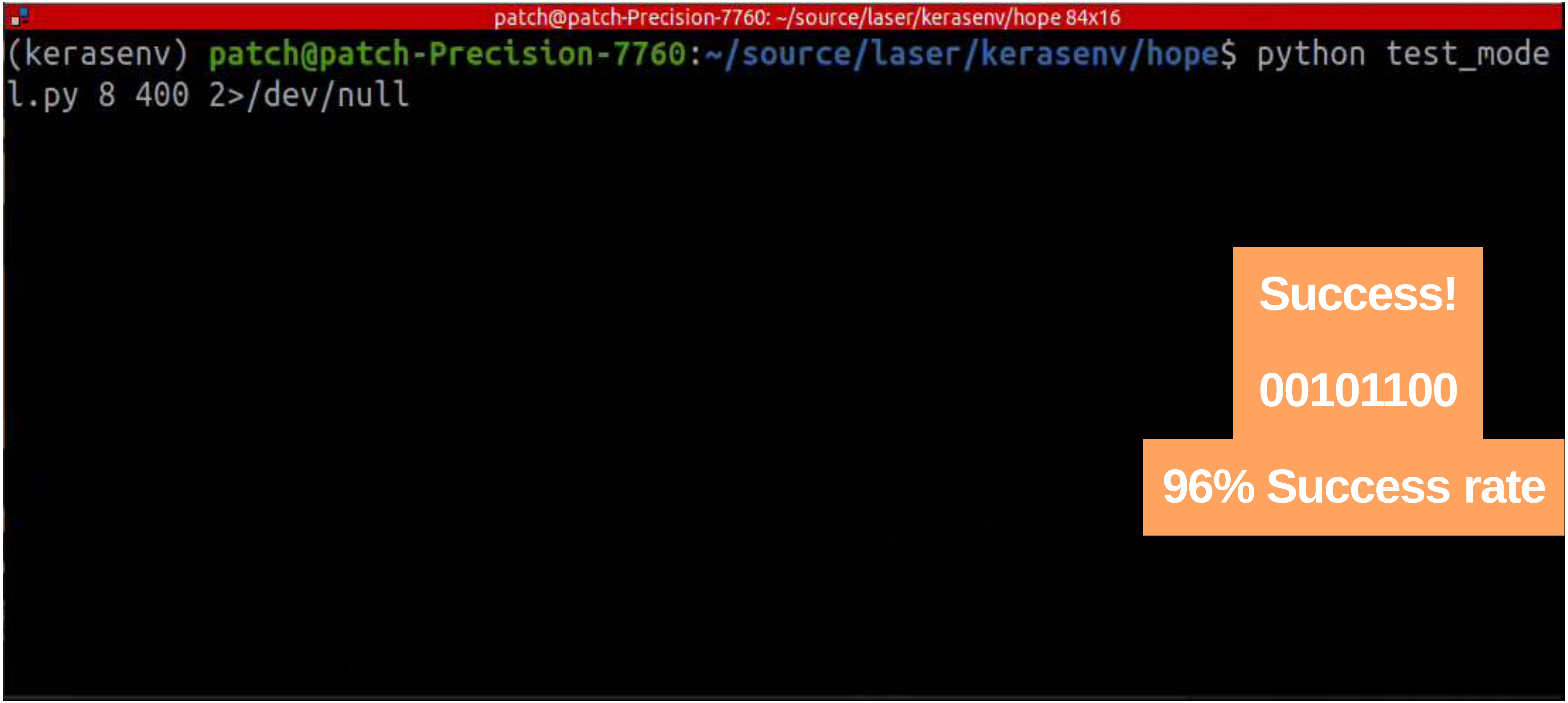
- In time, the model is able to correlate what is the gate representation of “1” and what is “0”
- Previously, we showed this with another data set using a different IC and memory
- Now, we have created a new mapping, **tailored for this specific SRAM and IC**



But does it work?

No lasers to fire this time ☹

Mapping the values



Success!

00101100

96% Success rate

FIN.

…of Gen 1

(we aren't done)

RayV Recap & Use Cases

- Proved building an **LFI** using materials **less than $500** USD was possible
- Proved building an **LLSI** using **affordable materials**, is plausible
- Proved a CNN can be used to **extract data from a live system**
- Learn **chip layout** through **imaging**
- Used to **introduce faults** in Embedded Controllers
- **Portable**, movable and **affordable** at-home **entry-level LFI** (& LLSI) tooling

We stand on the shoulders of so many giants

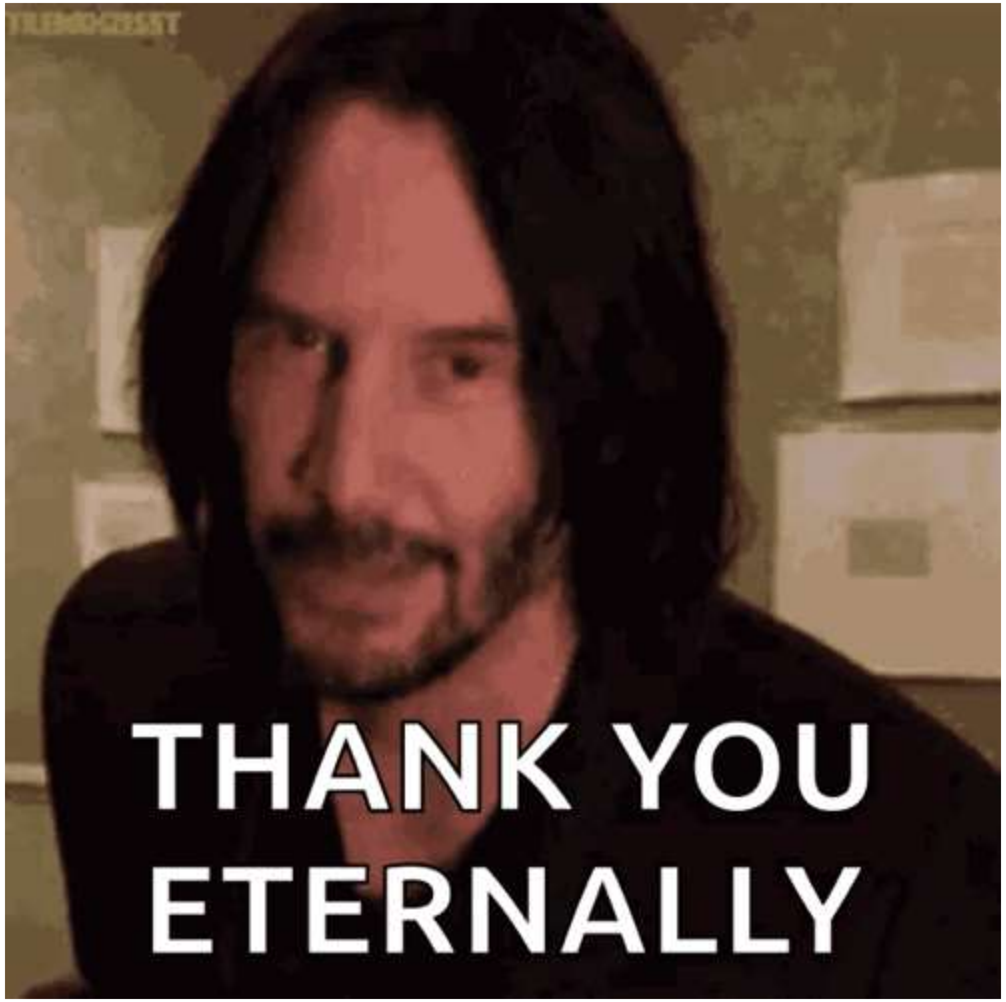
- The OpenFlexure Project
  - Joel T. Collins, Joe Knapper, Julian Stirling, Joram Mduda, Catherine Mkindi, Valeriana Mayagaya, Grace A. Mwakajinga, Paul T. Nyakyi, Valerian L. Sanga, Dave Carbery, Leah White, Sara Dale, Zhen Jieh Lim, Jeremy J. Baumberg, Pietro Cicuta, Samuel McDermott, Boyko Vodenicharski, 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 (some of) us

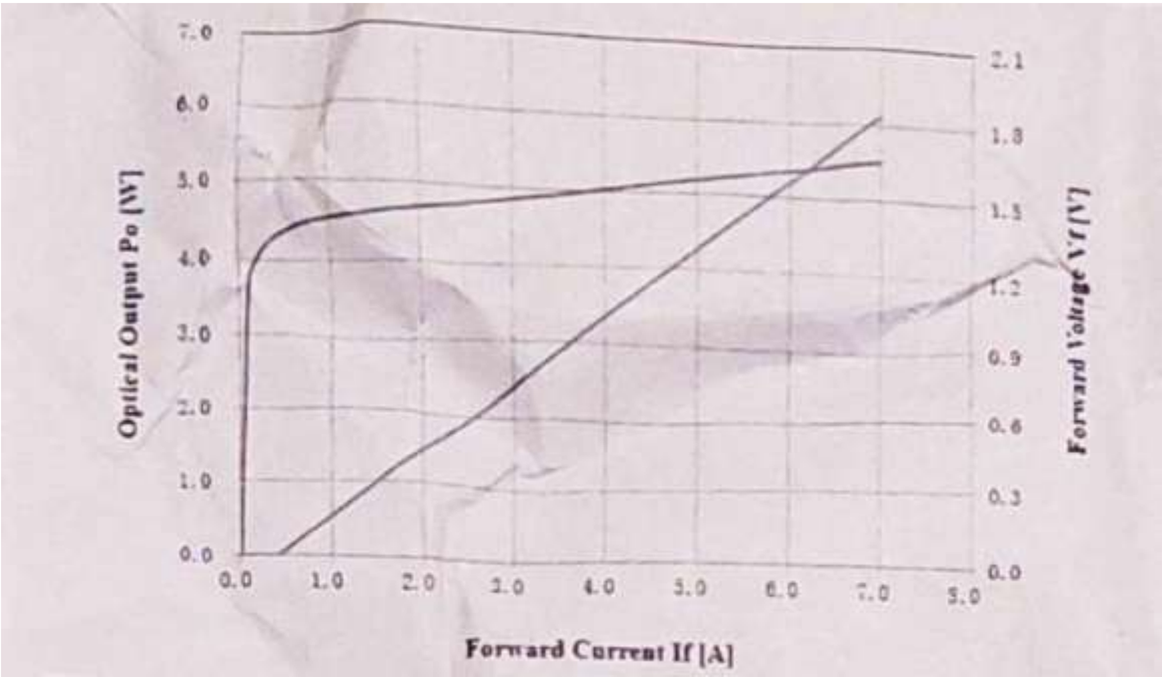
- That “laser” was an acronym
- Hoarding, finally, paid off
- I can do this from my house
- Not all datasheets are real
- That one of us didn’t kill, blind, or maim ourselves

- Open Sourcing and democratizing tooling is **powerful**
- As suspected, **others are doing similar work**. Just 24 hours ago, due to the coverage of this research a Janne Taponen from Fraktal shared with us the details of their rig
- We’ve coordinated our tools to opensource and release at **12:00 GMT-7, today (August 8th, 2024)**

Waldo and Wally walked into a bar. The bartender said, "I can't serve you, you're both too hard to find."

Things that went horribly wrong

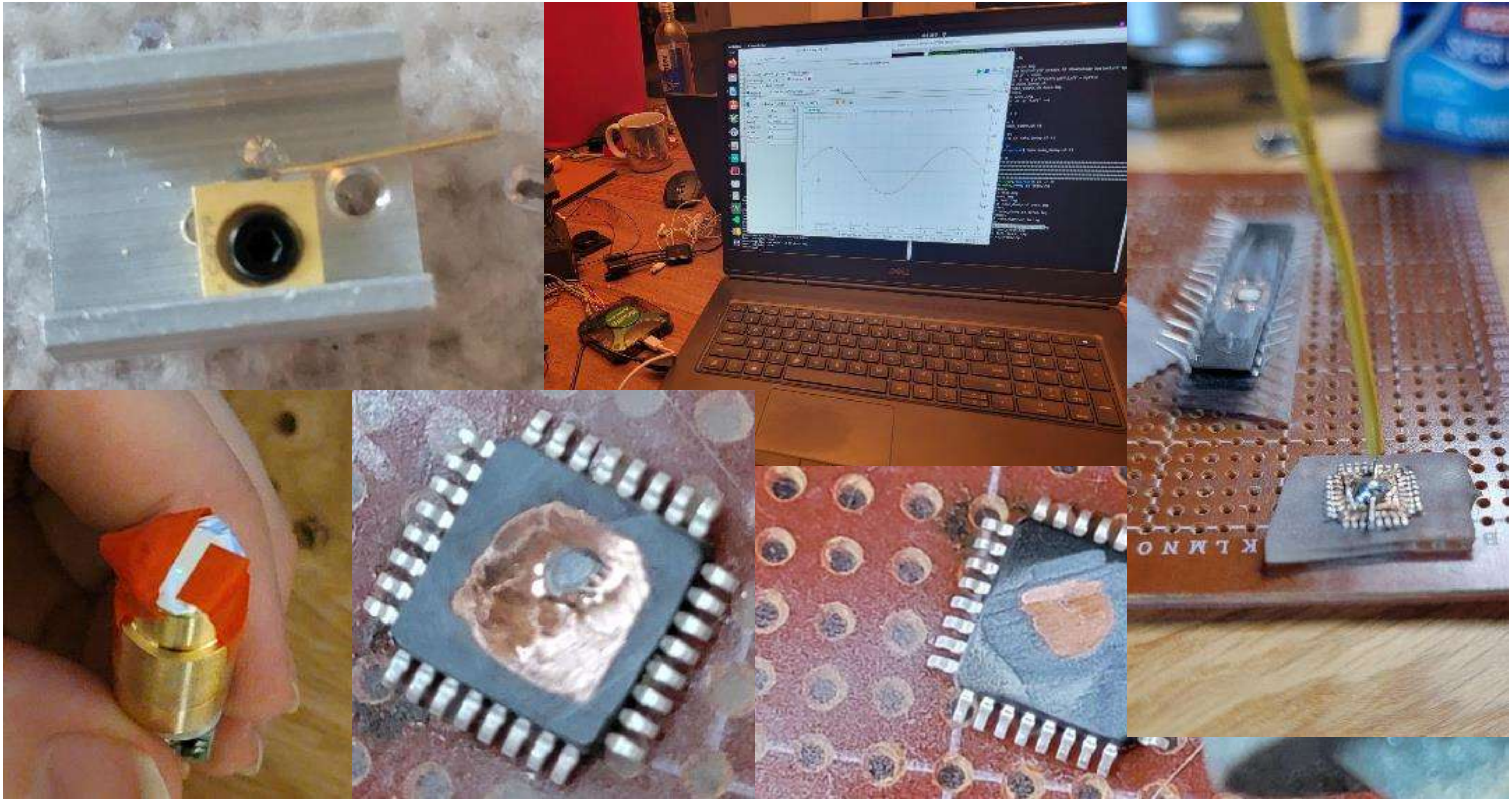
- Supply chains & distributors are hard
- Product Descriptors are a lie
- Practical implementation will always trump theoretical principles (the cake is a lie)
- Deadlines are real



- Graphs that make no sense
- Some parts were very hard to find

Waldo and Wally were on a reality TV show called "Survivor: The Hidden." They lasted about five minutes before the host yelled, "We give up!"

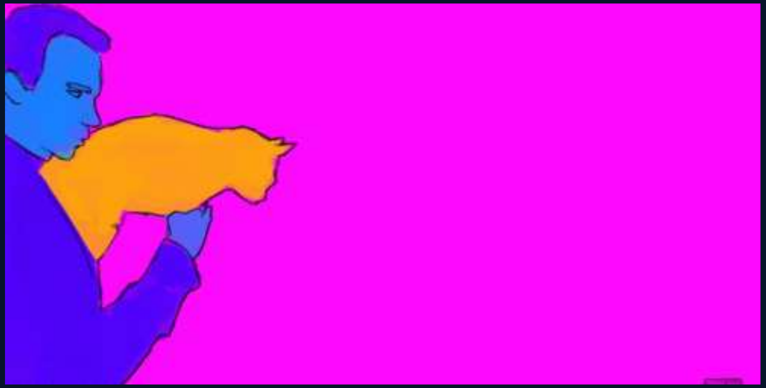
The Cost of RnD (thank you NetSPI)

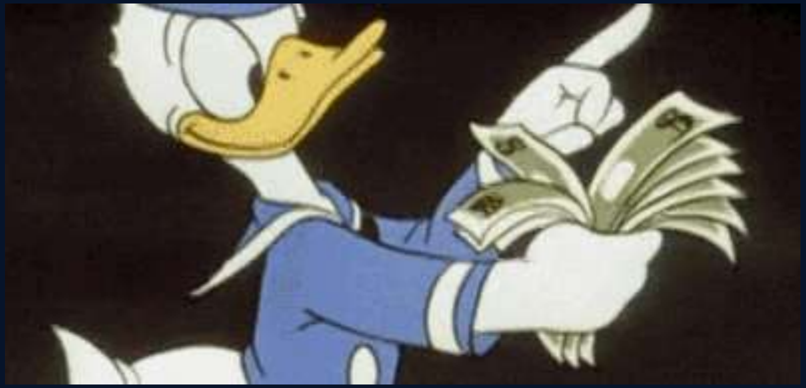


Next time you see us RayV'n

- 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

Thank you!

Welcome to the real-life version of “Where's Wally”

…(or “Where’s Waldo”)

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
(but wear protection.....)
Pew. Pew.