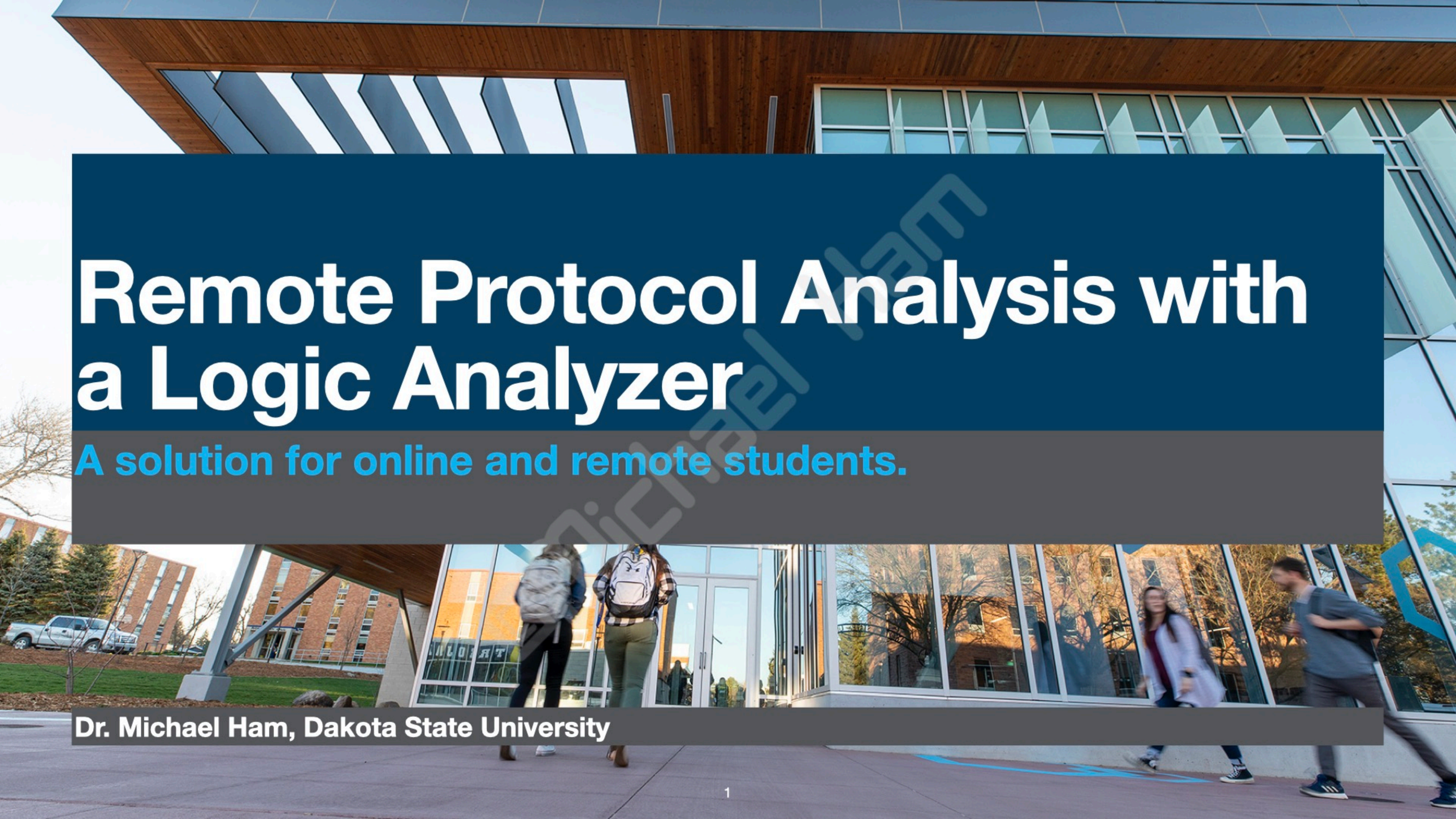


Remote Protocol Analysis with a Logic Analyzer

A solution for online and remote students.

Dr. Michael Ham, Dakota State University

Dakota State University

@Michael Ham

Who we are:

DSU Professors

- Dr. Michael Ham
  - Cyber Operations
  - 14 years at DSU
  - Malware / Reverse Engineering
- Shawn Zwach
- Dr. Kyle Cronin
- We are all DSU alumni!

Dr. Mike Ham

Shawn Zwach

Dr. Kyle Cronin

©Michael Ham

Dakota State University

Madison, SD

We're a little ways away from here.

Overview of DSU

Madison, SD

- 3,509 students (online and on-campus) - a new record for us!
  - 2,951 undergraduate and 558 graduate
  - ~59% (2,086) are online
- Cybersecurity has been the fastest-growing area and largest on campus
- B.S. through Ph.D. in Cyber Operations, Cyber Defense, and CS
- Articulation agreements
- NSA designations in CAE-CO, CAE-CD, CAE-R

©Michael Ham

Background

©Michael Ham

Protocol Analysis in Cybersecurity

A need for practitioners and students.

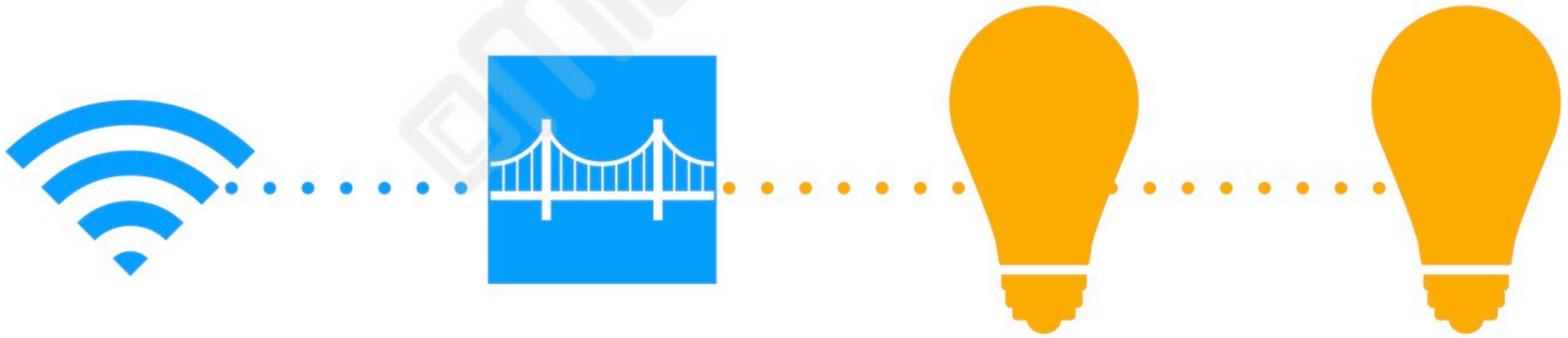
- Importance of protocol analysis for cybersecurity engineers
  - Expanding threat landscape with interconnected devices
- NSA-CAE designation and its focus on networking and communication protocols
  - Computer Networks
  - Software Reverse Engineering
  - Hardware Reverse Engineering
  - WIreless and Mobile Security

Michael Ham

Non-Routable Protocol Analysis

It's not just 802.11.

- IoT and other devices *do* connect to 802.11 networks
  - They also use underlying communications to support their architecture
- Several of these protocols exist and have flaws
  - Infrared, Zigbee, Bluetooth, etc.



Michael Ham

Logic Analyzer

Measuring signals and decoding secrets.

Saleae Logic Pro 8

- Captures, debugs, and measures digital signals
- Multi-channel capability for circuit connection and waveform display

Saleae Logic 2 analyzing an IR NEC signal.

Michael Ham

Remote Learning

We learn best by doing.

- Direct device intervention is necessary for capturing protocol data
  - Real-time analysis
- Barriers to entry for remote learners
  - Lack of physical access
  - Financial costs and regulatory restrictions
  - Encapsulating non-routable protocols for internet transmission
- Need: an Internet-accessible lab platform

Michael Ham

Artifact

©Michael Ham

Design Requirements

You can’t not follow a plan that doesn’t exist.

- Easily scalable and reproducible
- Web interface for remote control and data visualization
  - Allows remote interaction with the target device
  - Real-time analysis data (i.e., not encapsulated over the Internet)
  - Adaptable for various target hardware devices/wireless transmitters
- Low-cost/no-cost for student support

©Michael Ham

Scalability and Reproducibility

Docker.

- **Images** - like a snapshot of an application at a specific state
  - Dockerfile
- **Containers** - Standardize how applications are packaged, deployed, and run
  - Isolation and consistency - can run multiple simultaneously
- **Scalability** - Docker Compose facilitates multi-container applications
  - Web interface and Logic 2 software
- **Other Benefits** - resource usage, version control, portability

Michael Ham

Logic Analyzer

Real-time analysis and protocol visualization.

- Docker Container: **logic2**
  - Exposes port 8080 for a noVNC connection
- A logic analyzer is used to tap directly into a transmitter or receiver
  - Data (wireless transmissions) are visualized in the Logic 2 software
- Logic 2
  - Electron-based application functions best with a GUI
  - Students can write plugins, configure the hardware, etc.
  - A virtual display is generated for Logic 2

©Michael Ham

Logic 2 Virtual Display

It’s really picky about having a GUI

Xtigervnc

Display 0, Port 5900

Michael Ham

Logic 2 Virtual Display

It’s really picky about having a GUI

Michael Ham

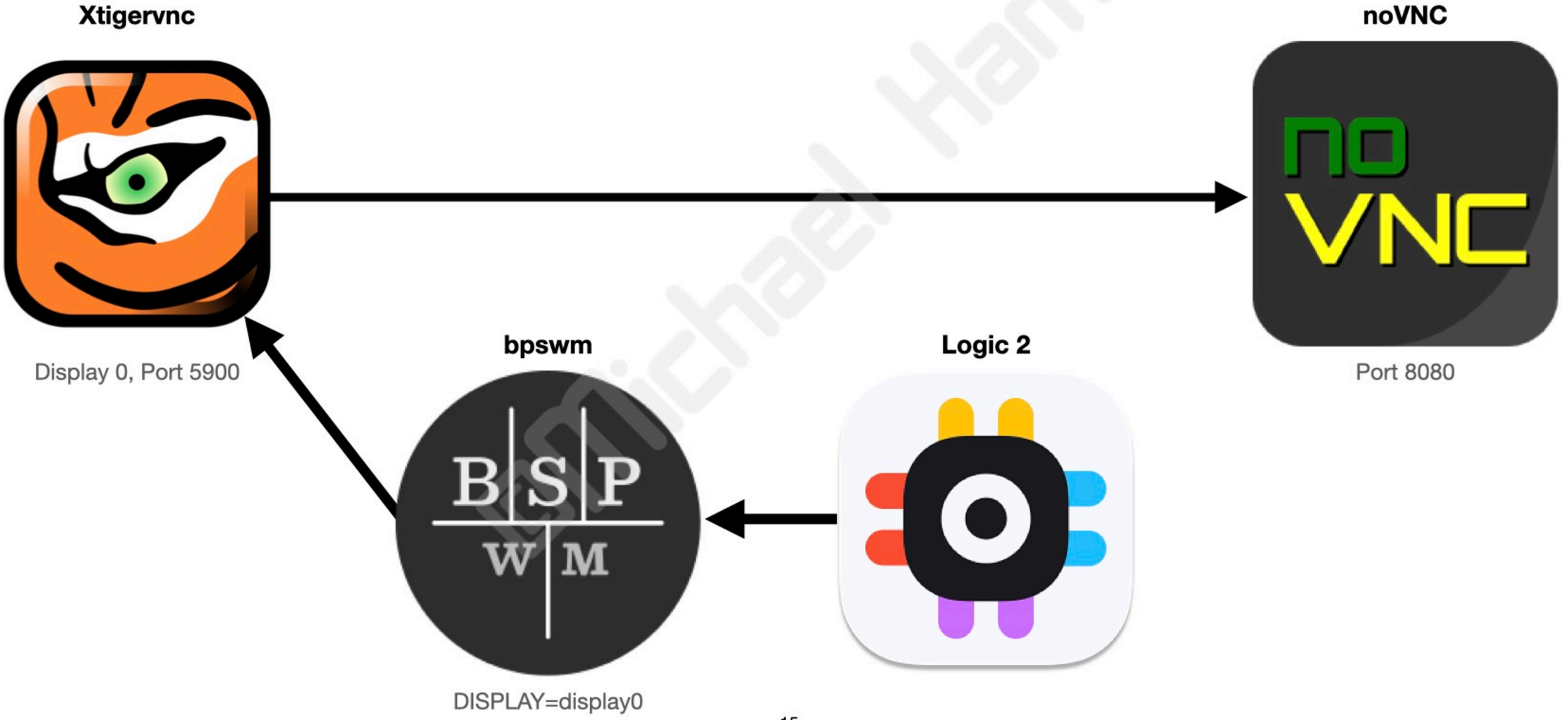
Logic 2 Virtual Display

It's really picky about having a GUI

Michael Ham

Logic 2 Virtual Display

It's really picky about having a GUI



Michael Ham

Web Interface

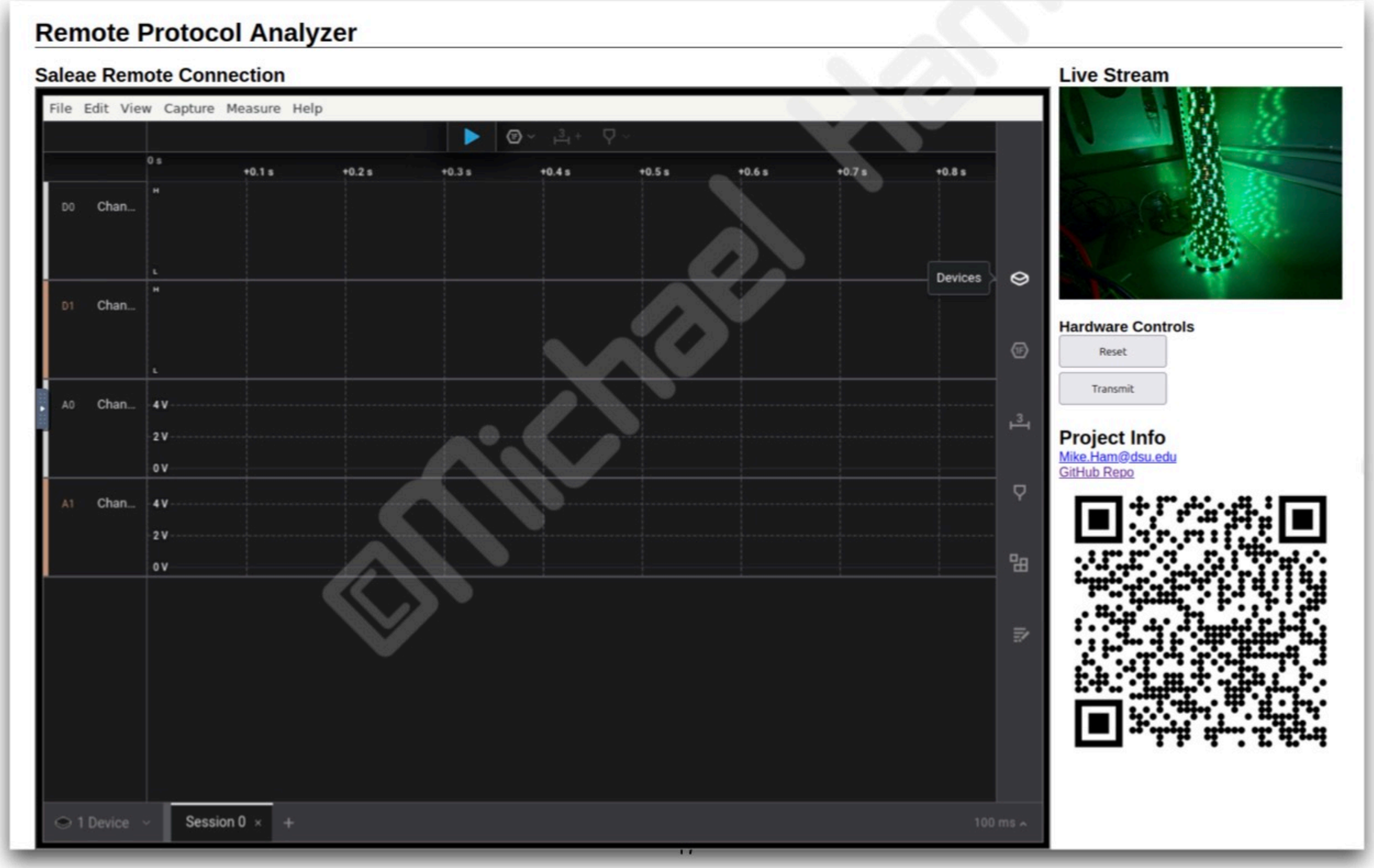
Remote control and data visualization.

- Docker container: **rpa-app**
  - Exposes port 5000 for the Flask app
  - Maps the webcam, Arduino, and Logic 2's noVNC session
- Flask App - written in Python and a small amount of JS, HTML, and CSS templates
  - Send serial commands via Python
  - View a webcam for the live status of the target hardware platform
  - Interact with the Logic 2 software directly on the host

Michael Ham

Resulting Interface

It's not *super* pretty, but it works.



Sample Target Device

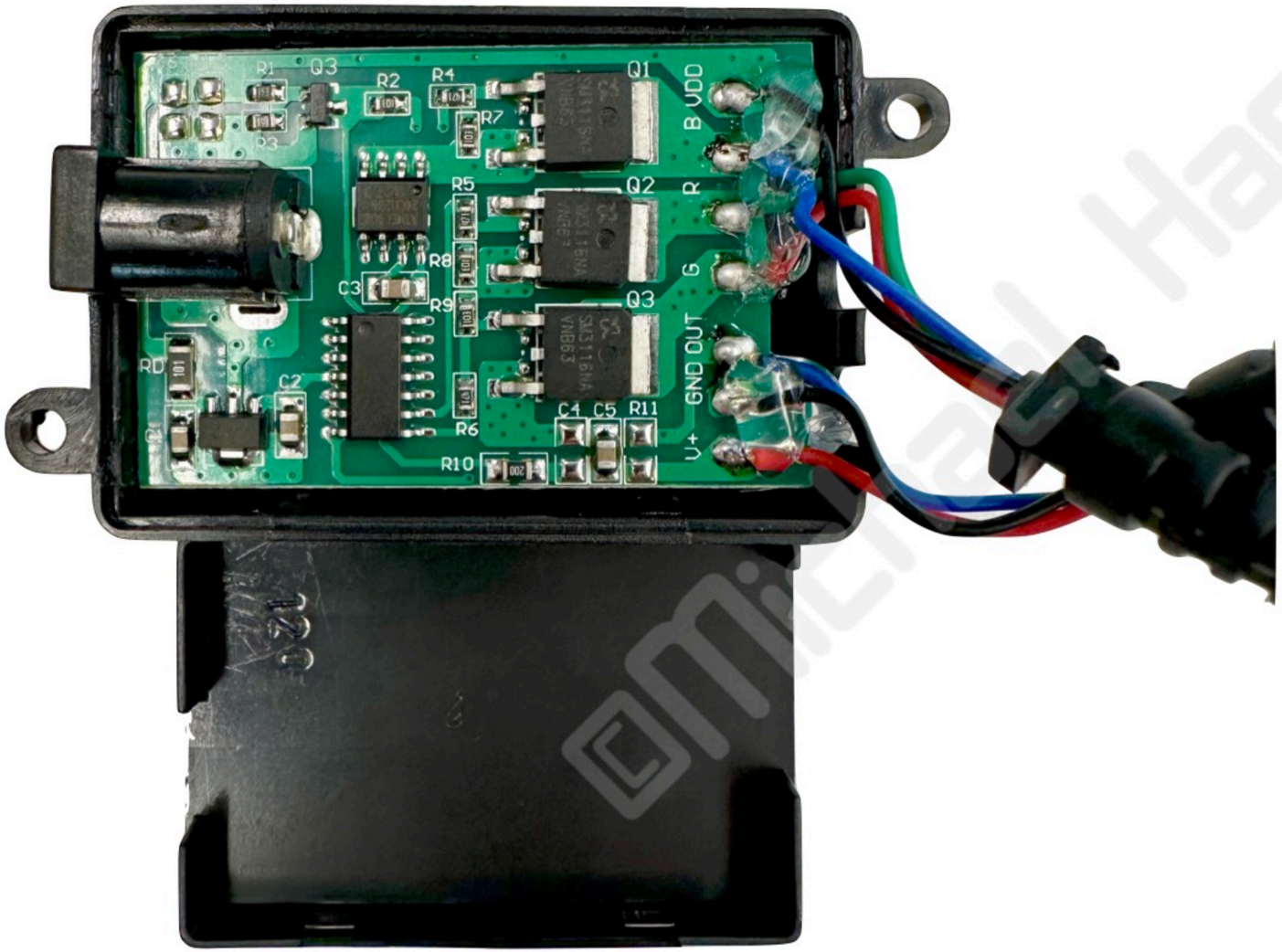
Building a blinky tree with a message.

Cone

Cheap IR LED light strip

Hot glue gun

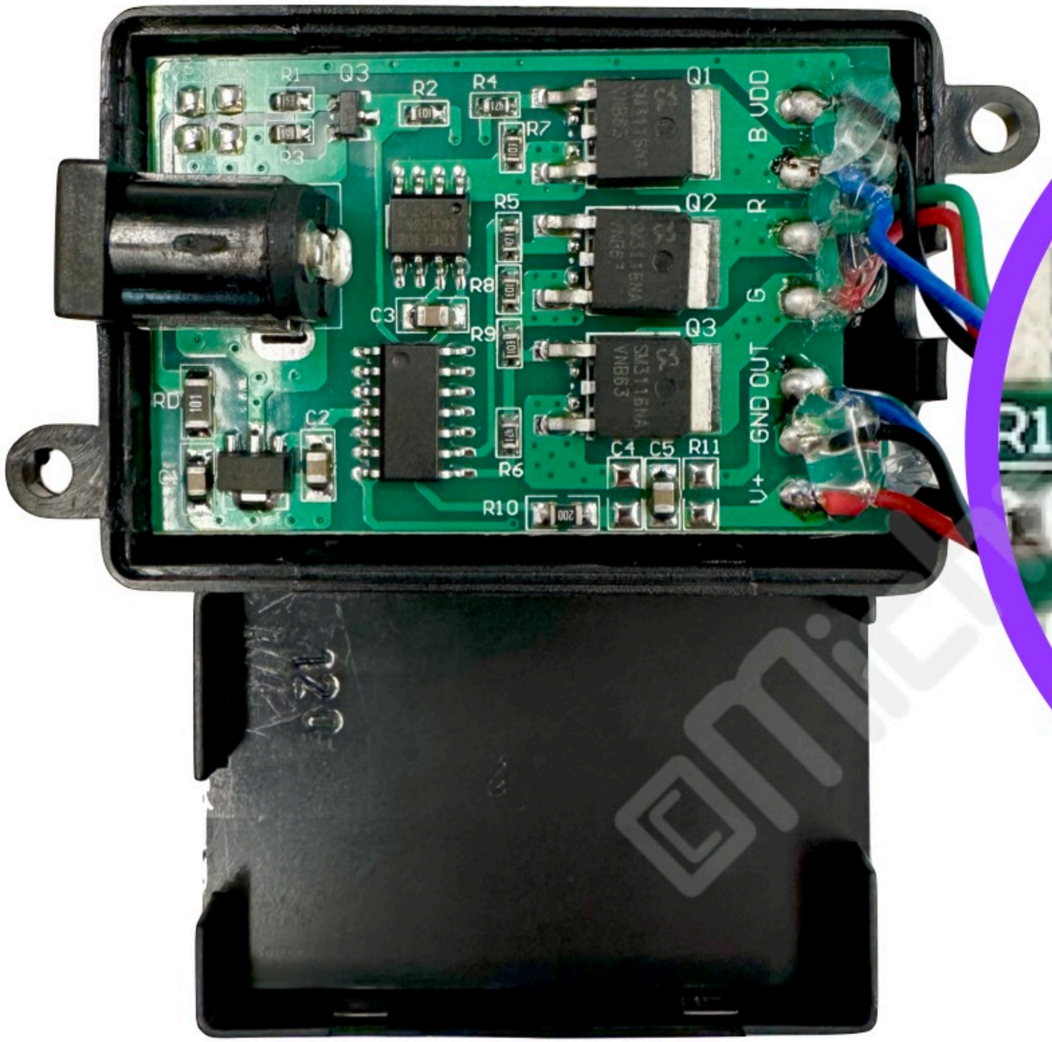
Mike (nerd)

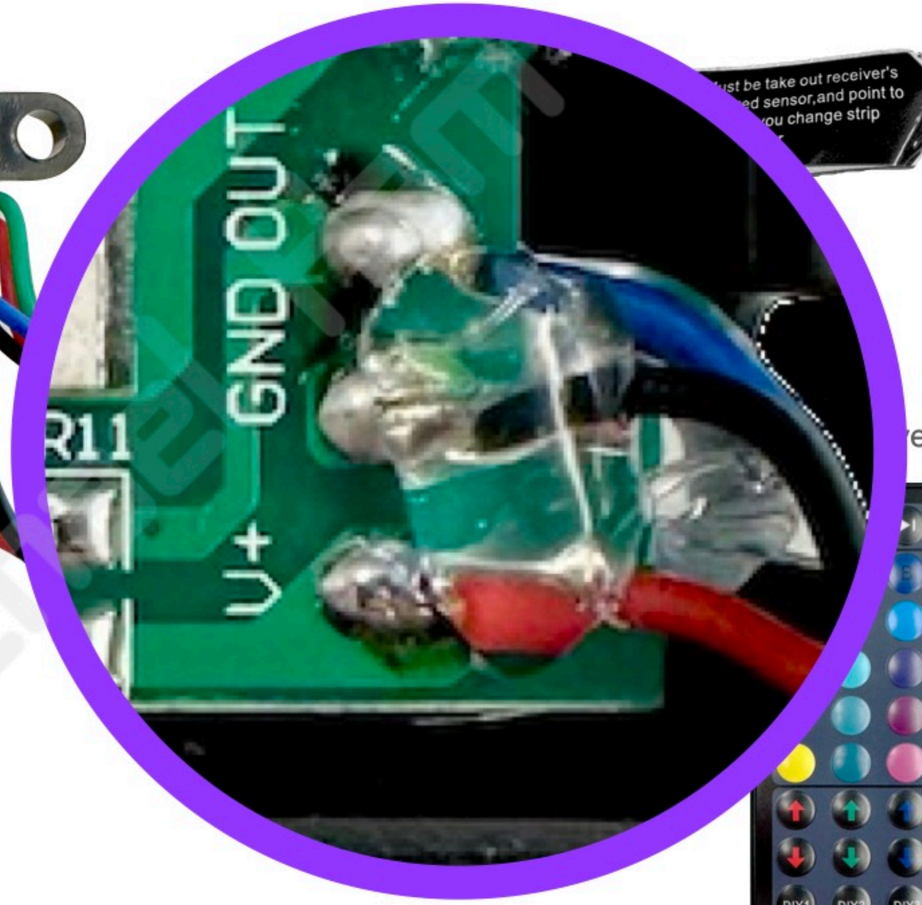


Power supply, microcontroller, and wiring for IR receiver and LED strip

IR Receiver

Remote





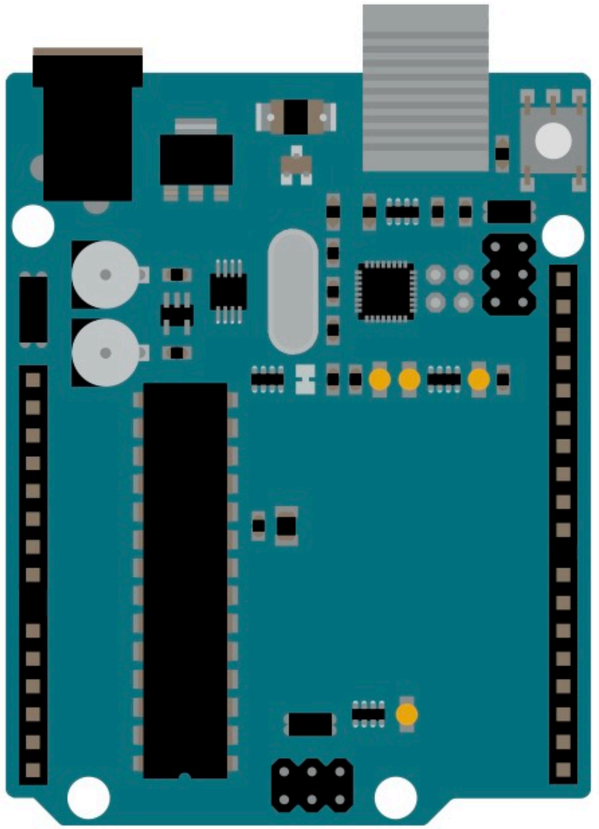
Power supply, microcontroller, and wiring for IR receiver and LED strip

Remote

Bypassing IR Entirely

Better for reliable signaling.

- The concept is the nearly the same as wiring and programming an IR LED



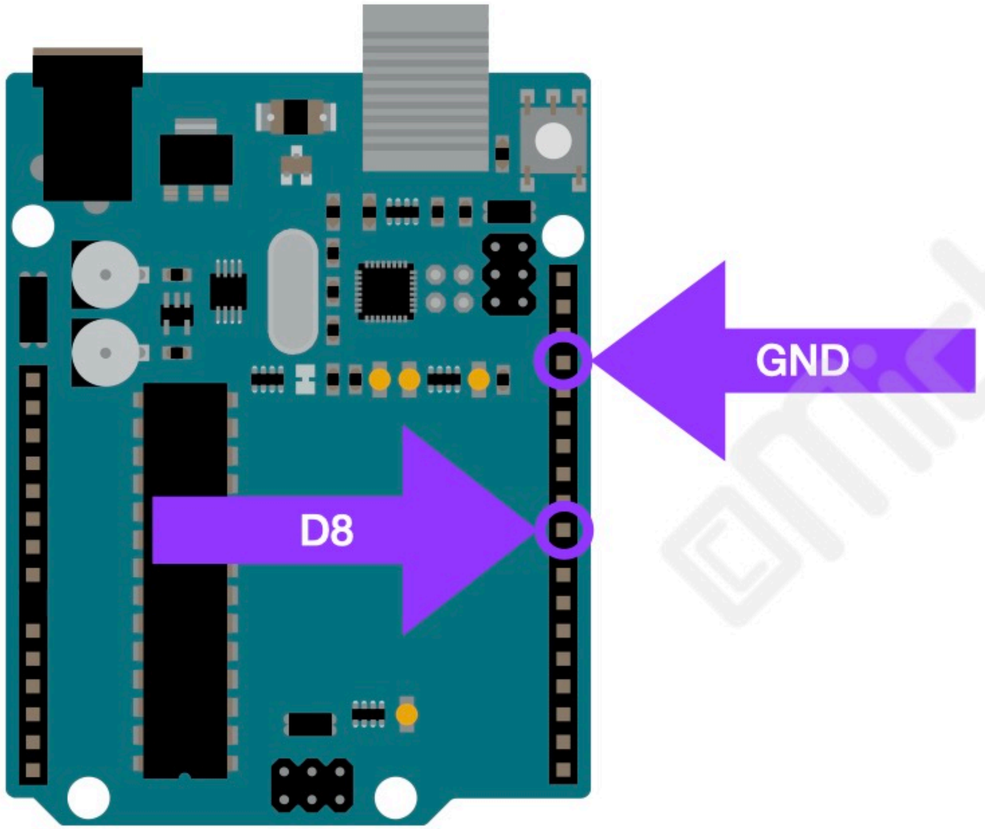
Arduino UNO R3

Michael Ham

Bypassing IR Entirely

Better for reliable signaling.

- The concept is the nearly the same as wiring and programming an IR LED



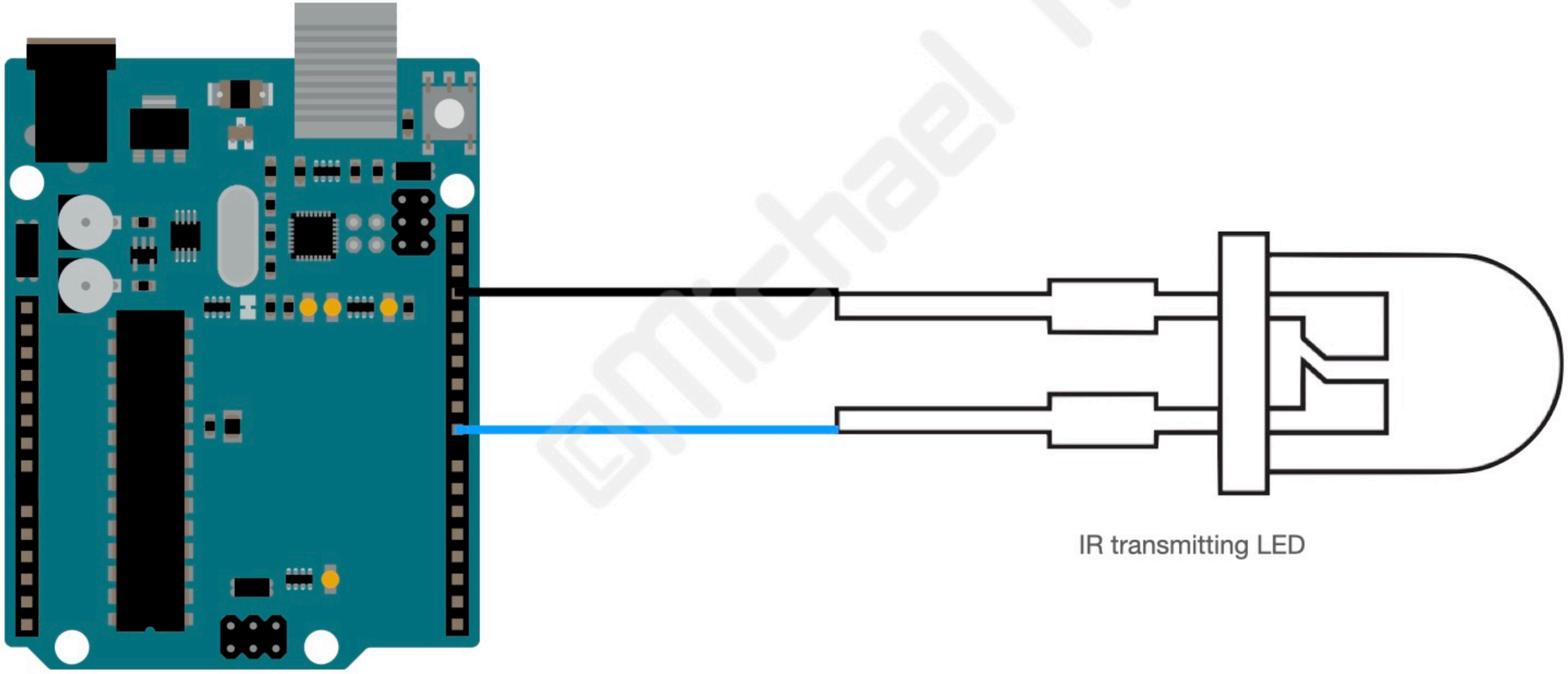
Arduino UNO R3

Michael Ham

Bypassing IR Entirely

Better for reliable signaling.

- The concept is the nearly the same as wiring and programming an IR LED



Arduino UNO R3

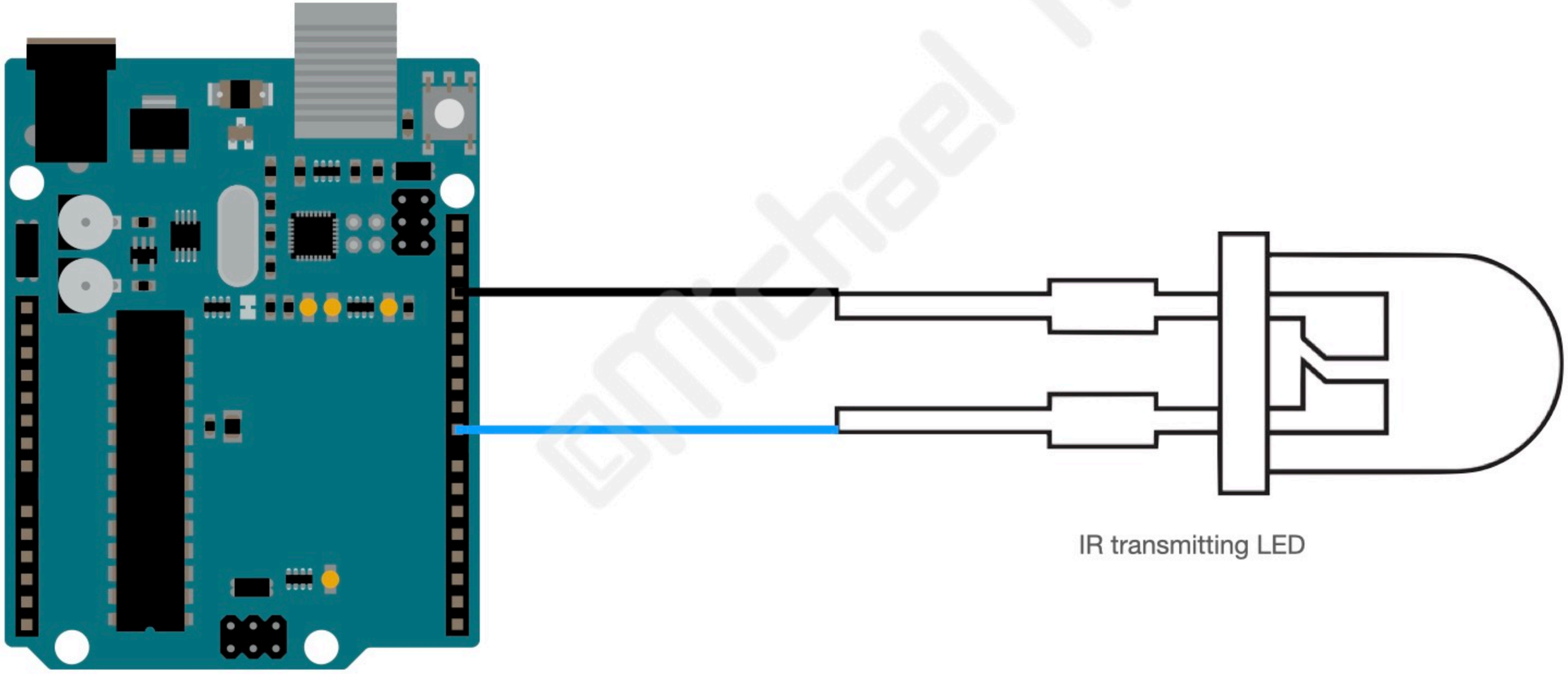
IR transmitting LED

Michael Ham

Bypassing IR Entirely

Better for reliable signaling.

- The concept is the nearly the same as wiring and programming an IR LED



Arduino UNO R3

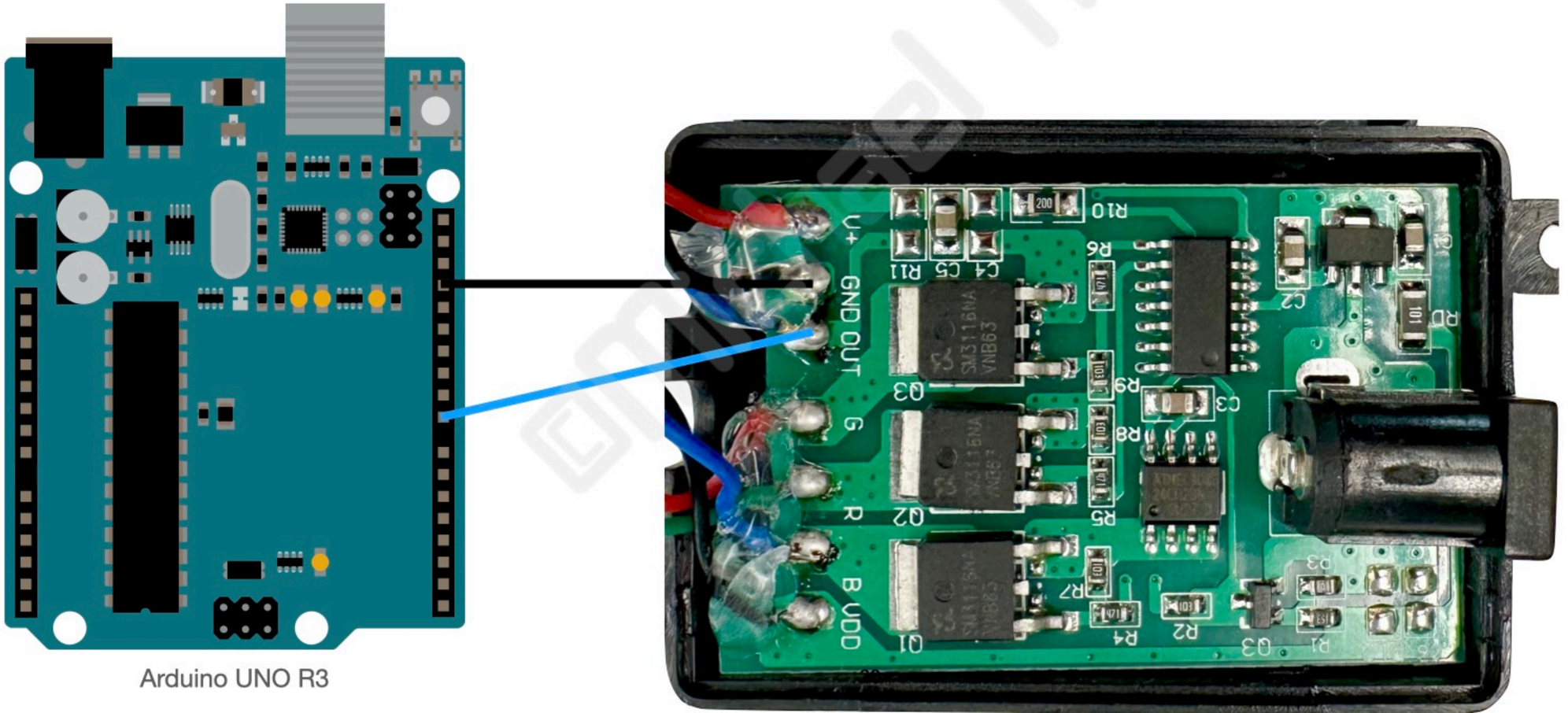
IR transmitting LED

Michael Ham

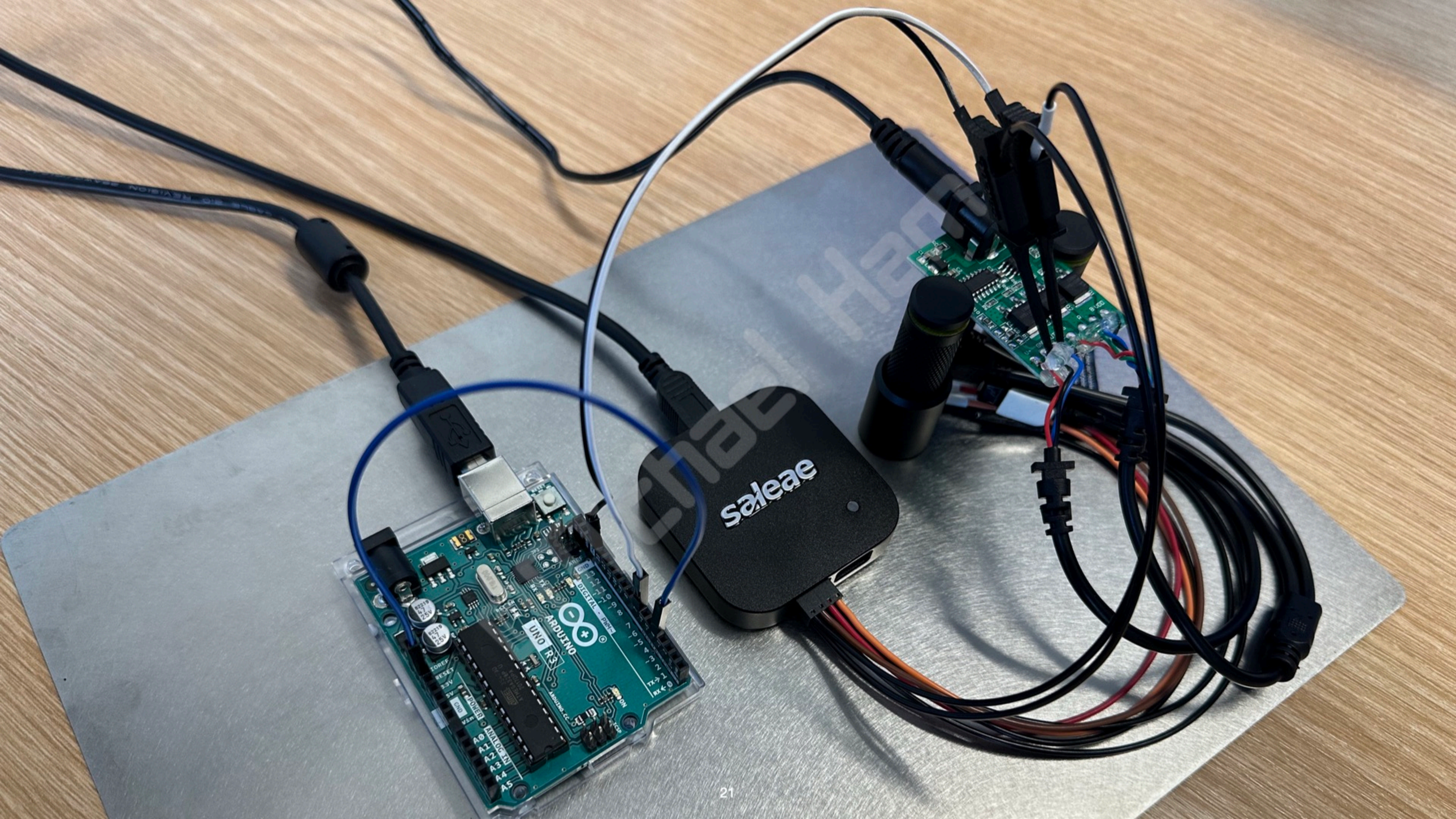
Bypassing IR Entirely

Better for reliable signaling.

- The concept is the nearly the same as wiring and programming an IR LED



Arduino UNO R3


saleae
ARDUINO
UNO R3

Demo

This probably won't blow up in front of everyone while I try to demo it live.

Michael Ham

Getting RPA

Only 3 commands!

1. Clone the repository

```
git clone https://github.com/DSUmjham/remote-protocol-analyzer.git
```

2. Navigate to the docker folder

```
cd remote-protocol-analyzer/docker/
```

3. Bring up the containers

```
docker compose up -d
```

```
dsu@ubuntu:~/remote-protocol-analyzer/docker$ docker ps
CONTAINER ID   IMAGE            COMMAND           CREATED         STATUS         PORTS                                                NAMES
de7629e62f31   docker-rpa-app   "python app.py"   5 minutes ago   Up 5 minutes   0.0.0.0:5000->5000/tcp, :::5000->5000/tcp            rpa-app
8d046201e1cb   docker-logic2    "supervisord"     5 minutes ago   Up 5 minutes   0.0.0.0:8080->8080/tcp, :::8080->8080/tcp            logic2
```

Docker containers running.

Michael Jham

Follow the Project

It's continuing to evolve.

- Updates will be provided via GitHub
  - https://github.com/DSUmjham/remote-protocol-analyzer
- Assessment data will inform how the challenges and teaching techniques will evolve the approach to maximize SLOs toward learning outcomes.

GitHub repository link

Questions?
mike.ham@dsu.edu

©Michael Ham

https://github.com/DSUmjham/remote-protocol-analyzer