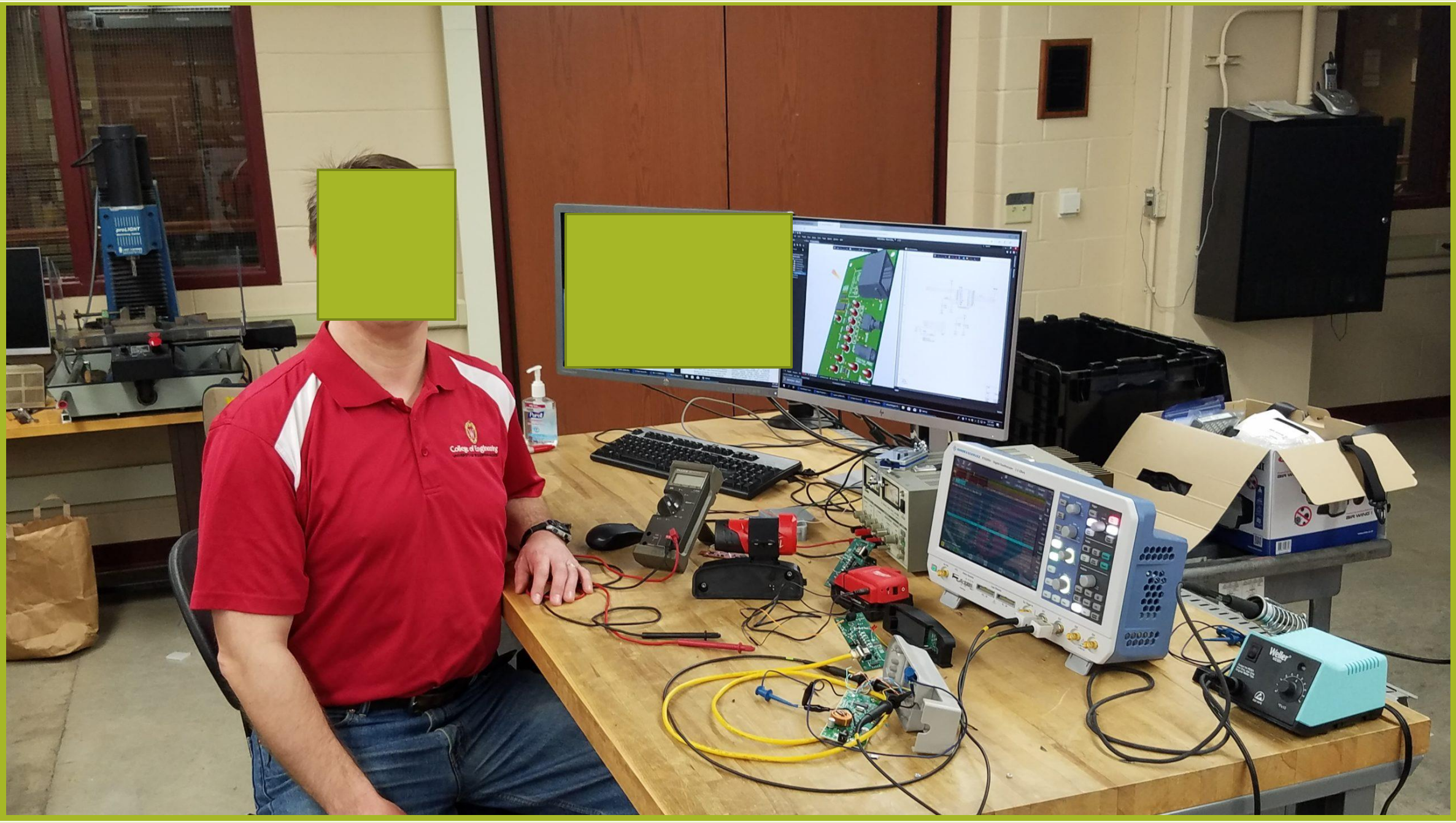
HARDWARE BEFREIEN

Briefbeschwerer, oder gehoert die Hardware wirklich mir?

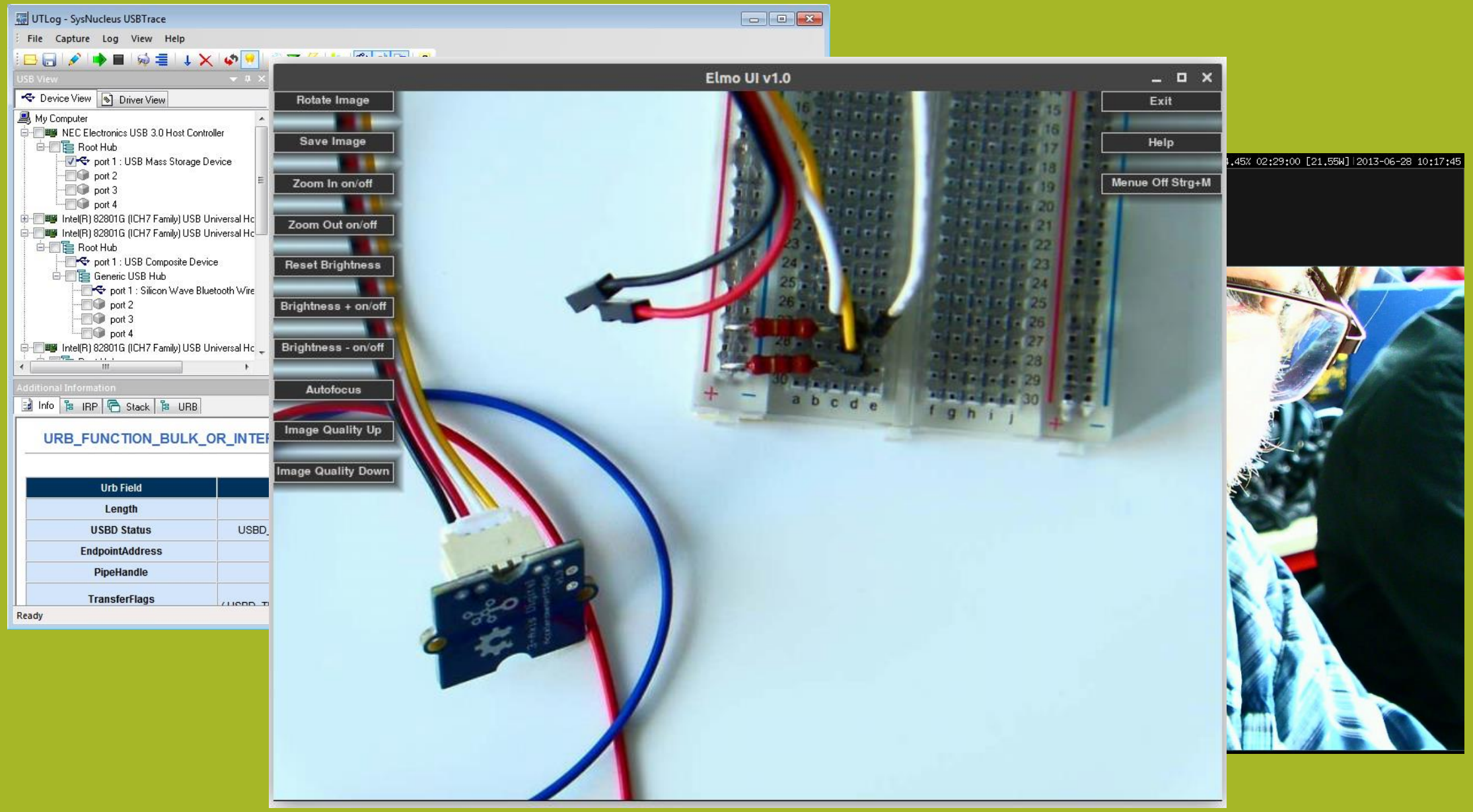

proLIGHT
College of Engineering
Weller

Beispiel #1

ELMO L-12

Problem:

- Kein Linux Client.


UTLog - SysNucleus USBTrace
File Capture Log View Help
USB View
Device View
Driver View
My Computer
NEC Electronics USB 3.0 Host Controller
Root Hub
port 1 : USB Mass Storage Device
port 2
port 3
port 4
Intel(R) 82801G (ICH7 Family) USB Universal Hc
Intel(R) 82801G (ICH7 Family) USB Universal Hc
Root Hub
port 1 : USB Composite Device
Generic USB Hub
port 1 : Silicon Wave Bluetooth Wire
port 2
port 3
port 4
Intel(R) 82801G (ICH7 Family) USB Universal Hc
Additional Information
Info
IRP
Stack
URB
URB_FUNCTION_BULK_OR_INTER
Urb Field
Length
USBD Status
USBD_
EndpointAddress
PipeHandle
TransferFlags
Ready
Elmo UI v1.0
Rotate Image
Save Image
Zoom In on/off
Zoom Out on/off
Reset Brightness
Brightness + on/off
Brightness - on/off
Autofocus
Image Quality Up
Image Quality Down
Exit
Help
Menue Off Strg+M
1.45% 02:29:00 [21.55W] 2013-06-28 10:17:45

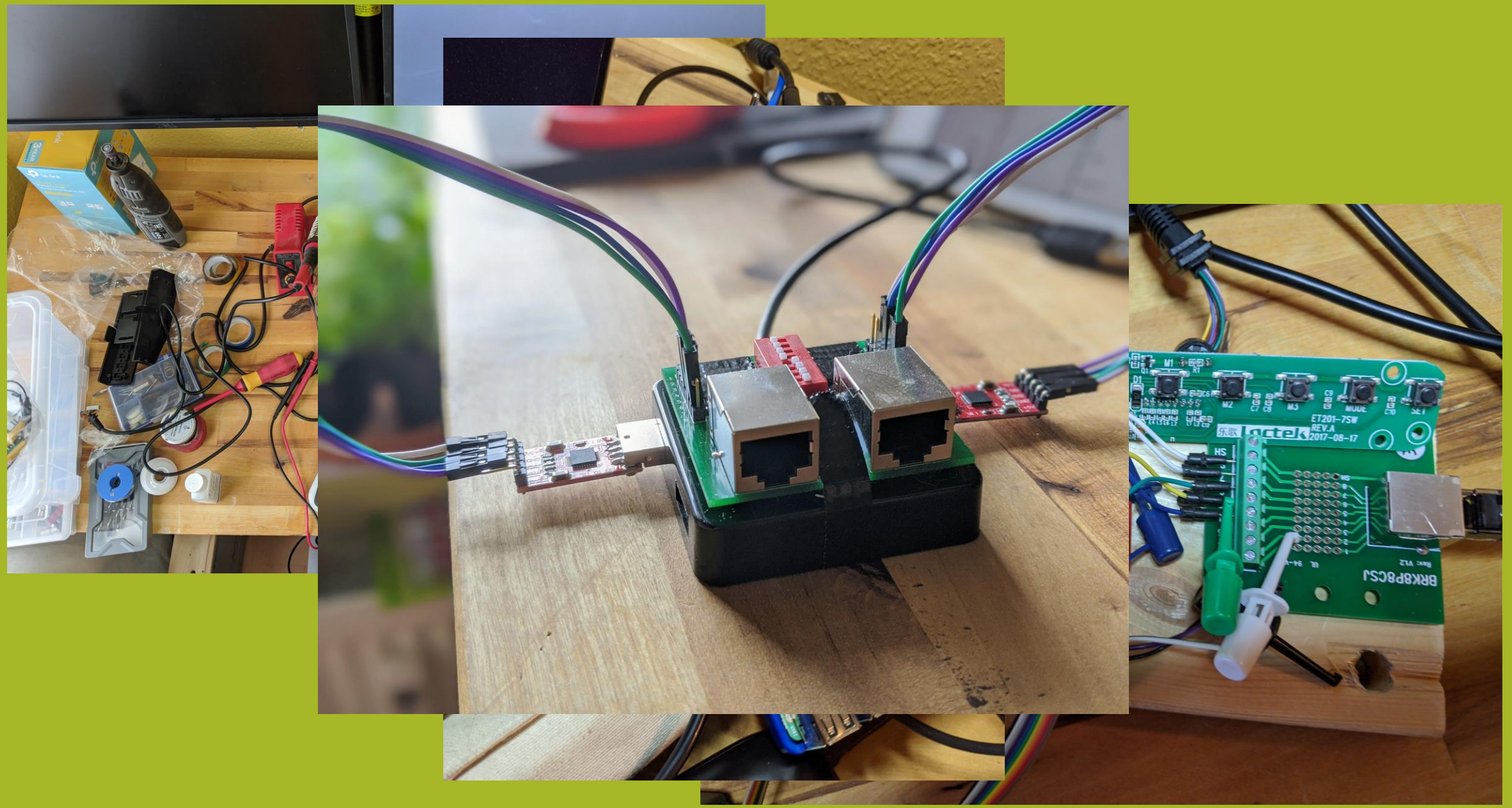
Projekt wurde nach 8 Jahren auf Github vor 1.5 Jahren auf Python 3 portiert.
Es wird aktiv an einigen Schulen und Unis eingesetzt.

Beispiel #2

STEHSCHREIBTISCH

Problem:

- Freie Wahl der Hoehe
- (Vielleicht vom Laptop steuerbar?)


M1
M2
M3
ET201-7SW
REV.A
2017-08-17
HS

Eine Person hat sich das genommen, was ich oeffentlich geteilt habe und hat das Projekt "Deskmatik" gestartet

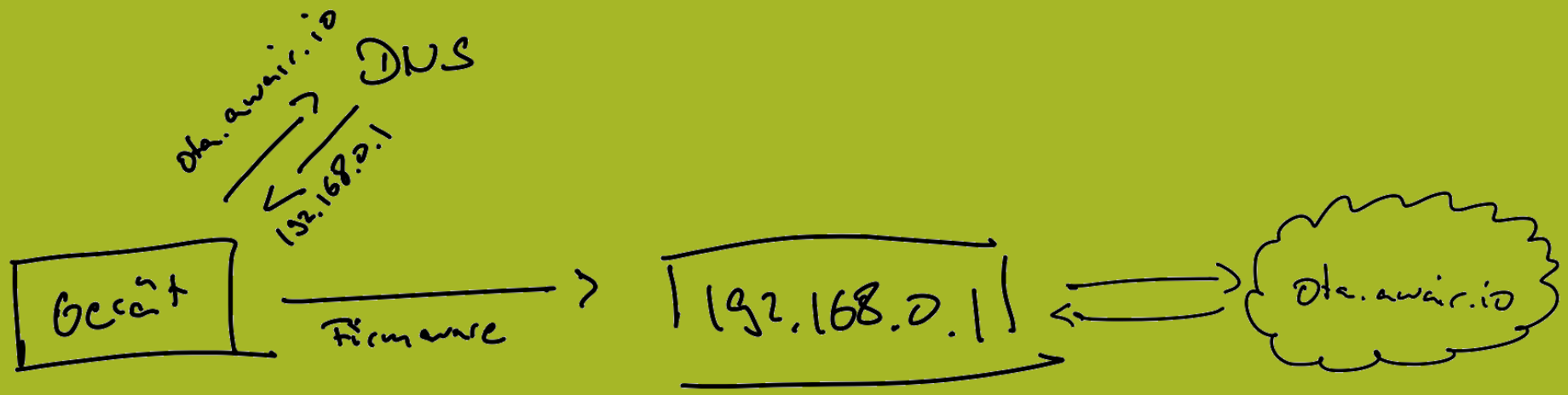
https://github.com/deskmatik/deskmatik

Beispiel #3

LUFTSENSOR

Problem:

- Eigentlich hatten wir kein Problem
- Aber es waere schoen auf dem "Bildschirm" was eigenes ausgeben zu koennen.

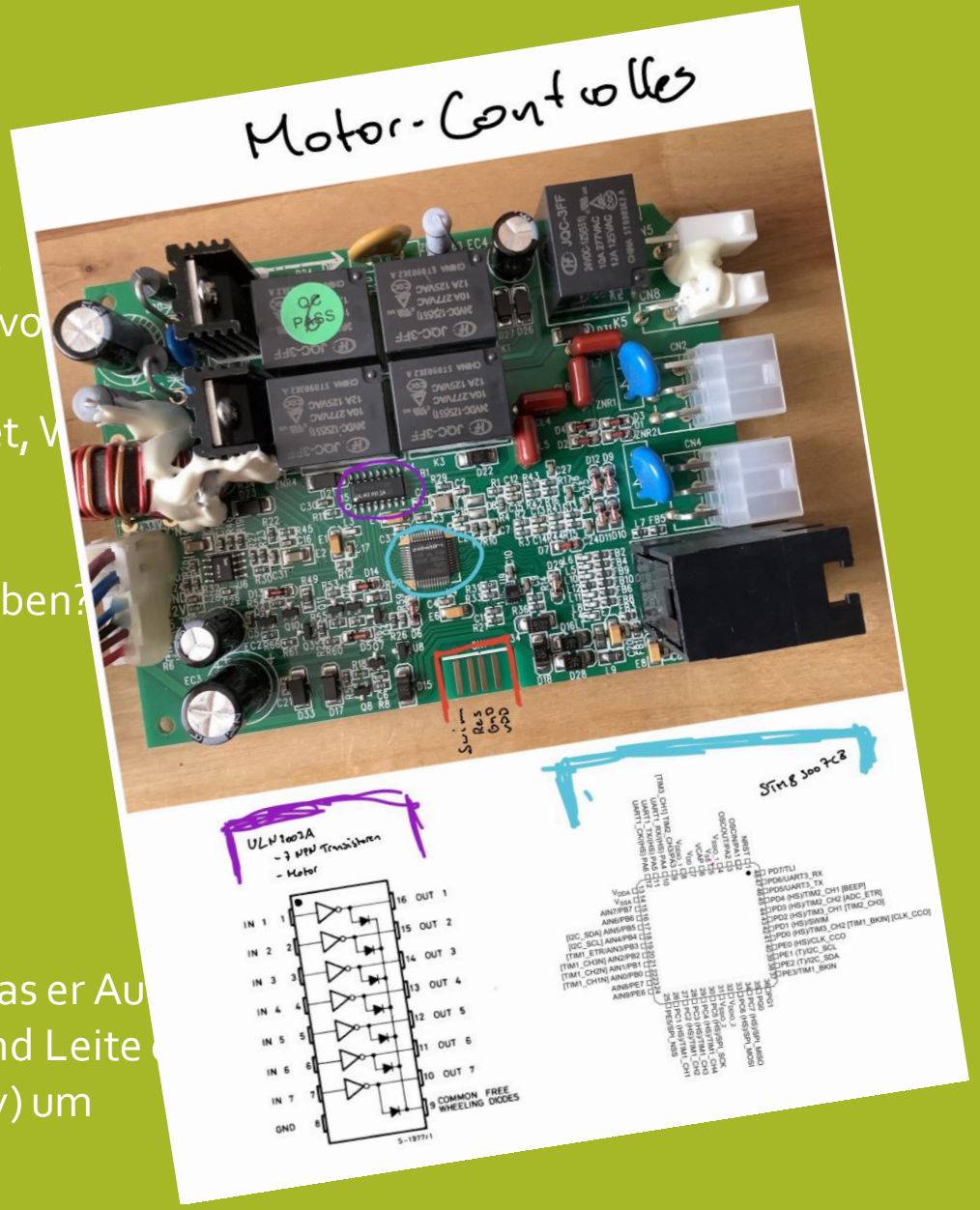

ota.awair.io
DNS
192.168.0.1
Occat
Firmware
192.168.0.1
ota.awair.io

Beispiel #n

GENERALISIERT

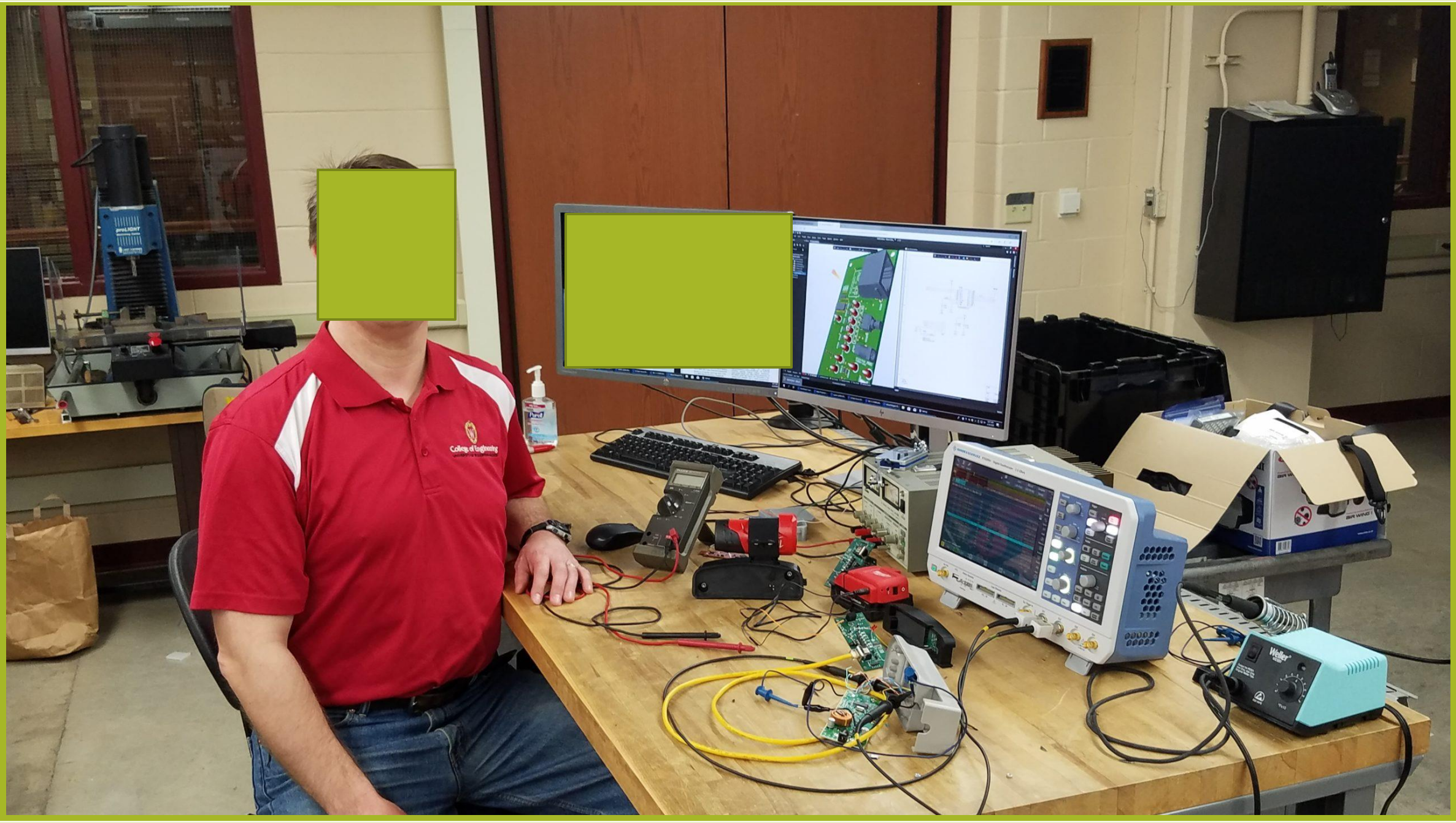
Ohne das Geraet zu oeffnen:

1. Hardware in Betrieb nehmen wie gedacht.
    1. Den "Flow" der Applikation anschauen.
2. Das Geraets dokumentieren. (Mit Bildern vielleicht?)
    1. Sieht man irgendwie seltsame PINs an die man vo
    2. Welche Anschluesse sieht man direkt
    3. Hat es in irgendeiner Weise Netzwerk? (Ethernet, W
    4. Bluetooth?
3. Gibt es FCC Dokumente? (https://fccid.io/)
    1. Was sieht man auf den Bildern aus dem Innenleben?
        1. Die Dokumention der Chips raussuchen
4. Ist die Firmware irgendwo online?
    1. Gibt es ueberhaupt einen Update Prozess?
    2. Laesst sie sich durch binwalk einfach zerlegen?
5. Falls es in deinem Netzwerk haengt:
    1. Portscan (nmap, etc.)
    2. Kontrolliere das DNS (pydns), um zu schauen was er Au
    3. Beantworte die DNS Anfragen selber (pydns) und Leite
       einen Intercepting Proxy (Burp, Zap, mitmproxy) um



Am Offenen Geraet:

1. Wie geht es ueberhaupt auf?
    1. Gibt es Clips die Abbrechen? (ifixit kann hier sehr helfen)
    2. Besondere Schraubendreherkoepfe. (Tri-Wings, etc)
2. Gibt es "Seltsame" Test-Pin Konfigurationen?
    1. Was sagt der "Silk-Layer"? Irgendwas Beschriftet?
    2. Tigard/Buspirate/LogicAnalyzer dranhaengen und schauen was er tut.
3. Welche Chips werden verwendet?
    1. Pin-Layout?
    2. Wo gehen die Traces hin?
    3. Schon mal die Testpins angeschaut?
    4. Haben sie Debugging Protokolle noch an? (SWIM, etc)
    5. Kann man die Chips glitchen? Um Debugging wieder anzuschalten?


proLIGHT
College of Engineering
Weller

Bildet Banden!

https://github.com/nv1t/talks

Twitter: @nv1t