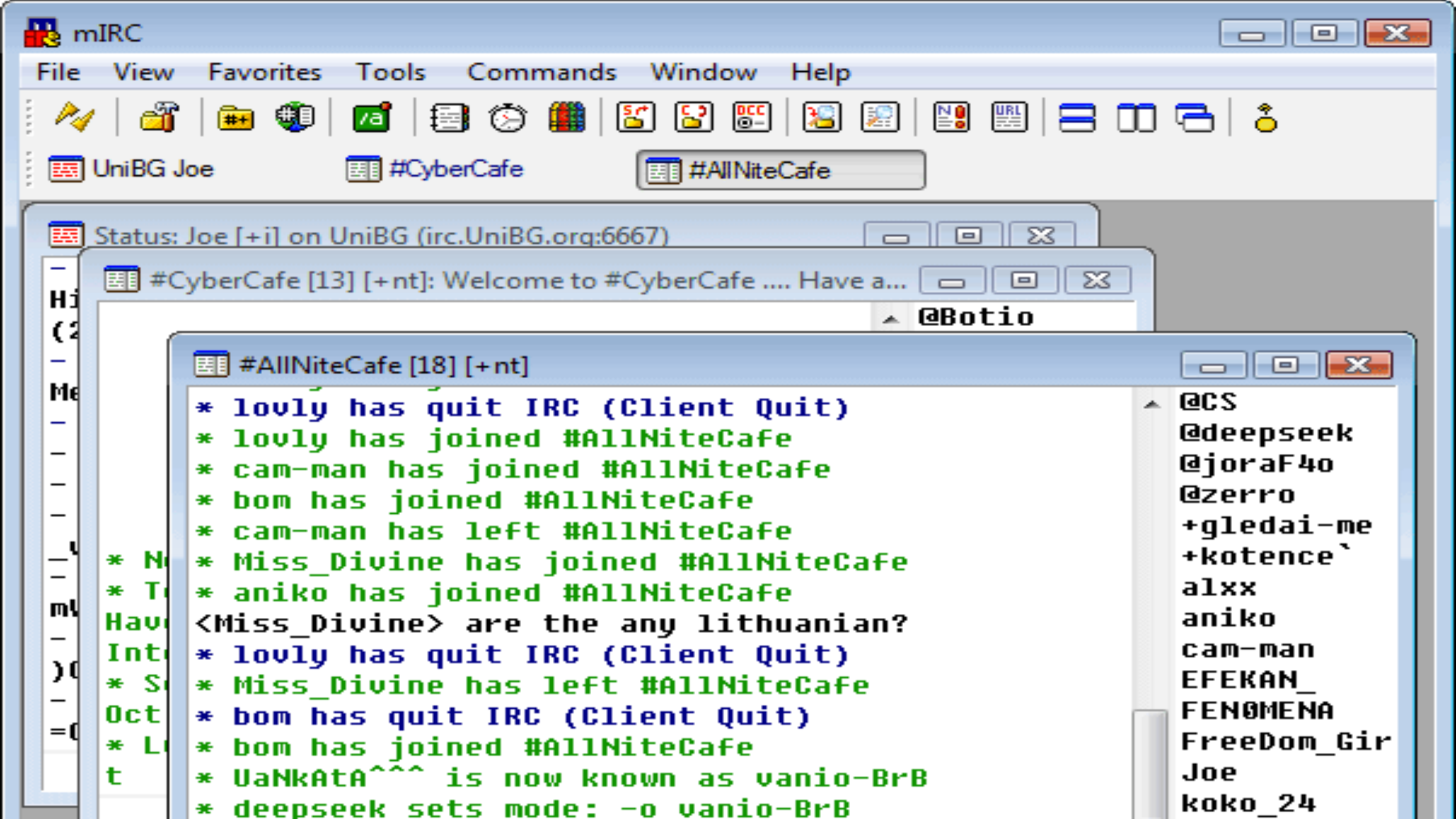
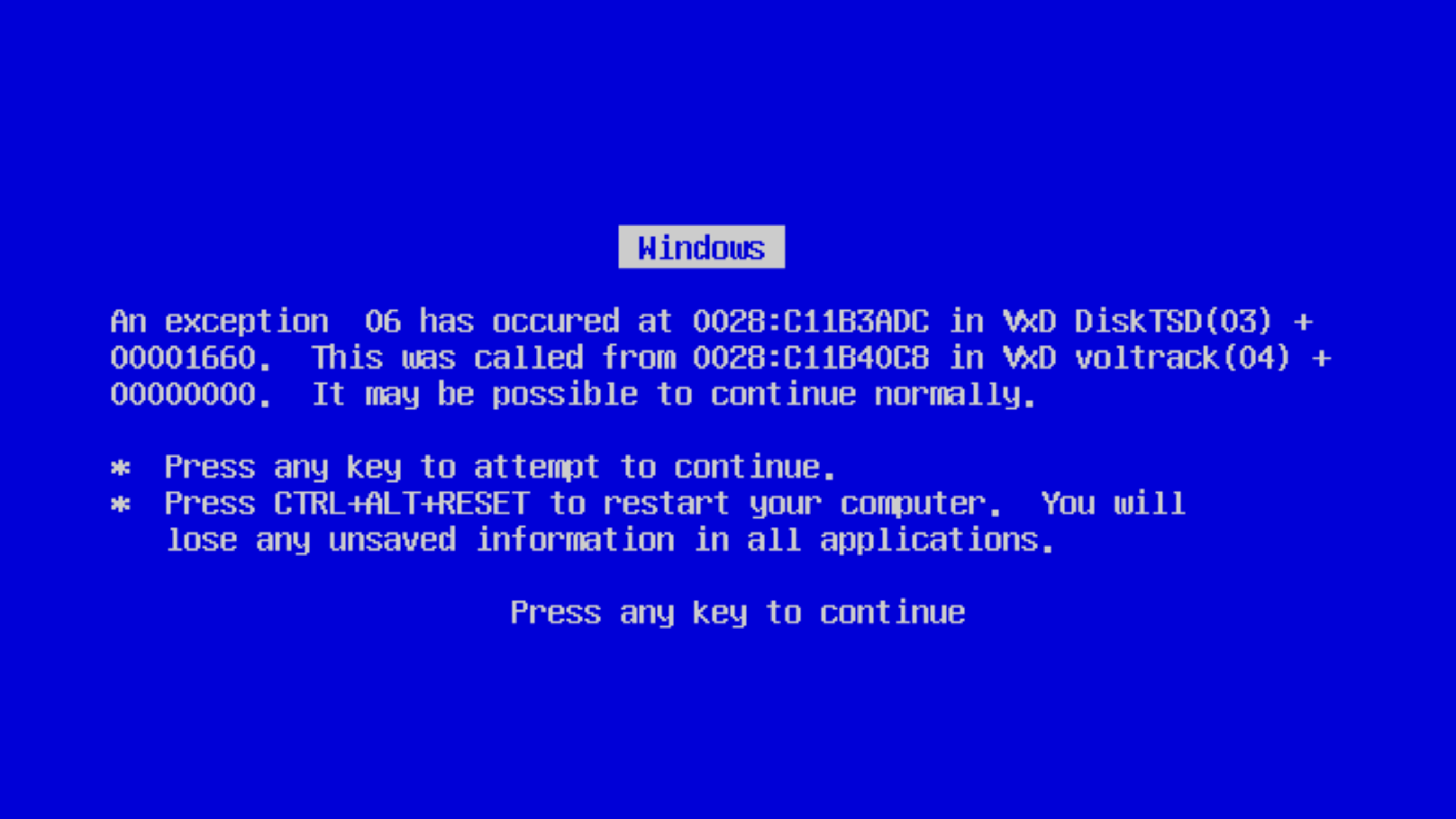
Optical Espionage

(and other fun ways to exploit physics)

@samykamkar
samy.pl


C90
Videon
speed


mIRC
File View Favorites Tools Commands Window Help
UniBG Joe
#CyberCafe
#AllNiteCafe
Status: Joe [+i] on UniBG (irc.UniBG.org:6667)
#CyberCafe [13] [+nt]: Welcome to #CyberCafe .... Have a...
@Botio
#AllNiteCafe [18] [+nt]
* lovly has quit IRC (Client Quit)
* lovly has joined #AllNiteCafe
* cam-man has joined #AllNiteCafe
* bom has joined #AllNiteCafe
* cam-man has left #AllNiteCafe
* Miss_Divine has joined #AllNiteCafe
* aniko has joined #AllNiteCafe
<Miss_Divine> are the any lithuanian?
* lovly has quit IRC (Client Quit)
* Miss_Divine has left #AllNiteCafe
* bom has quit IRC (Client Quit)
* bom has joined #AllNiteCafe
* UaNkAtA^^^ is now known as vanio-BrB
* deepseek sets mode: -o vanio-BrB
@CS
@deepseek
@joraF4o
@zerro
+gledai-me
+kotence`
alxx
aniko
cam-man
EFEKAN_
FEN0MENA
FreeDom_Gir
Joe
koko_24


Windows
An exception 06 has occured at 0028:C11B3ADC in VxD DiskTSD(03) +
00001660. This was called from 0028:C11B40C8 in VxD voltrack(04) +
00000000. It may be possible to continue normally.
* Press any key to attempt to continue.
* Press CTRL+ALT+RESET to restart your computer. You will
lose any unsaved information in all applications.
Press any key to continue

An exception
00001660. T
00000000. I

* Press any
* Press CTR
lose any

skTSD(03) +
ltrack(04) +

will

WinnukeV95



WinNuke V95
(c)1997 BurntBogus of the Den
Greets to Hound Dog

Nuke ME 95

NUKE IP ADDRESS
10.0.0.1

NUKE WITH MESSAGE
Greetings !

Exit



.:: Introduction ::.

Issues: [1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] [15] [16] [17] [18] [19] [20] [21] [22] [23]
[24] [25] [26] [27] [28] [29] [30] [31] [32] [33] [34] [35] [36] [37] [38] [39] [40] [41] [42] [43] [44] [45]
[46] [47] [48] [49] [50] [51] [52] [53] [54] [55] [56] [57] [58] [59] [60] [61] [62] [63] [64] [65] [66] [67]
[68] [69] [70]

Current issue : #49 | Release date : 1996-11-08 | Editor : daemon9 Get tar.gz

ground truth

energy

energy / time

==

power

1 horsepower lifts 550lbs 1ft in 1sec

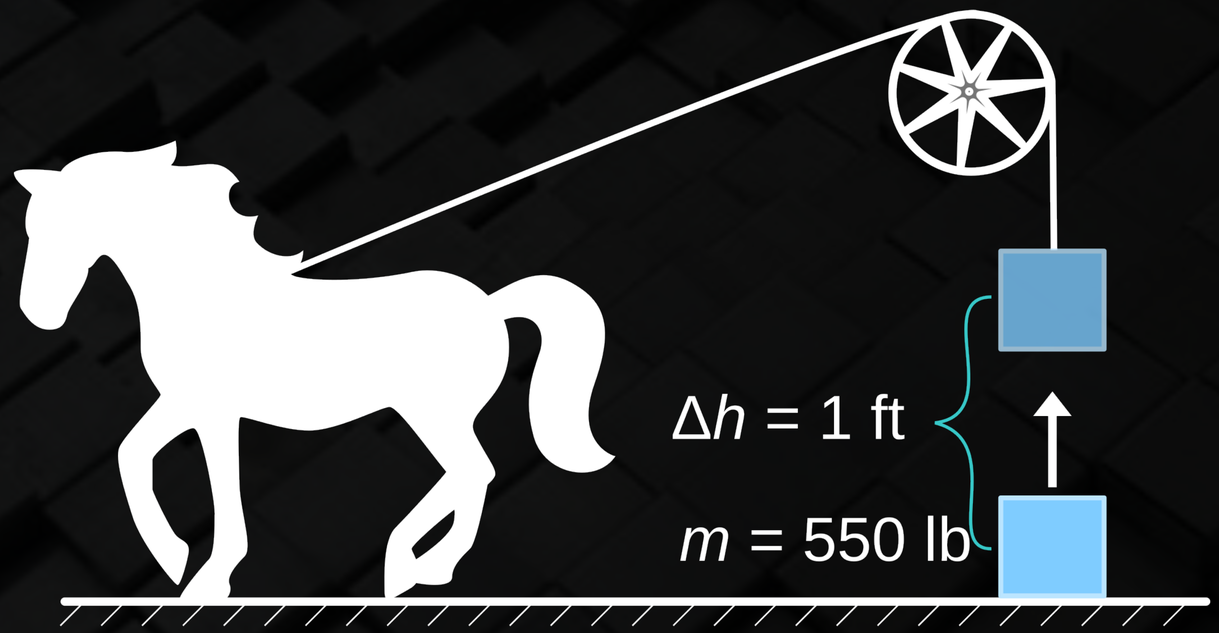


1 imperial horsepower
lifts 550lbs 1ft in 1sec



1 imperial horsepower

lifts 550lbs 1ft in 1sec



1 metric horsepower

lifts 542lbs 1ft in 1sec



energy / time

==

power

energy

==

information

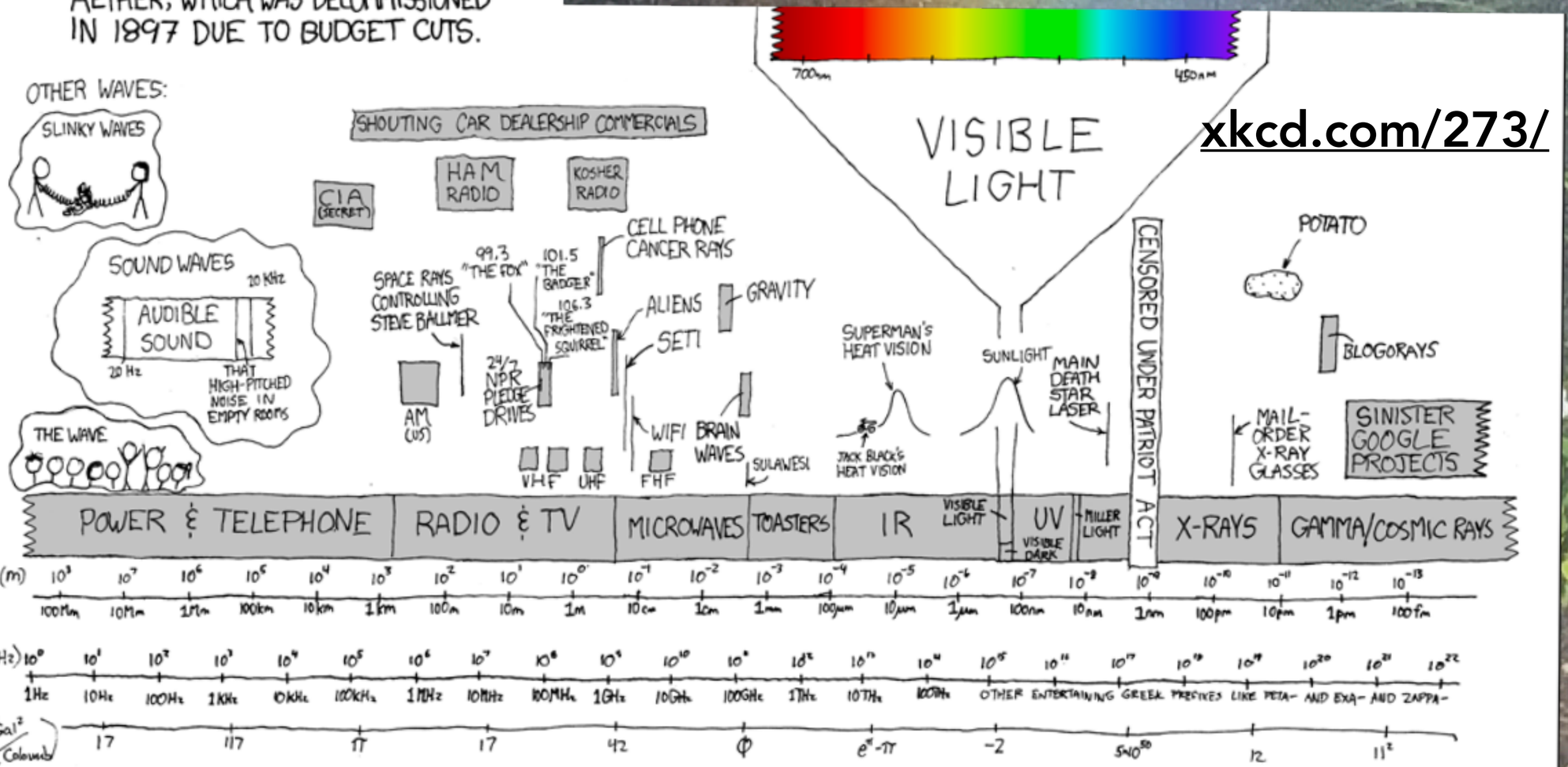
light





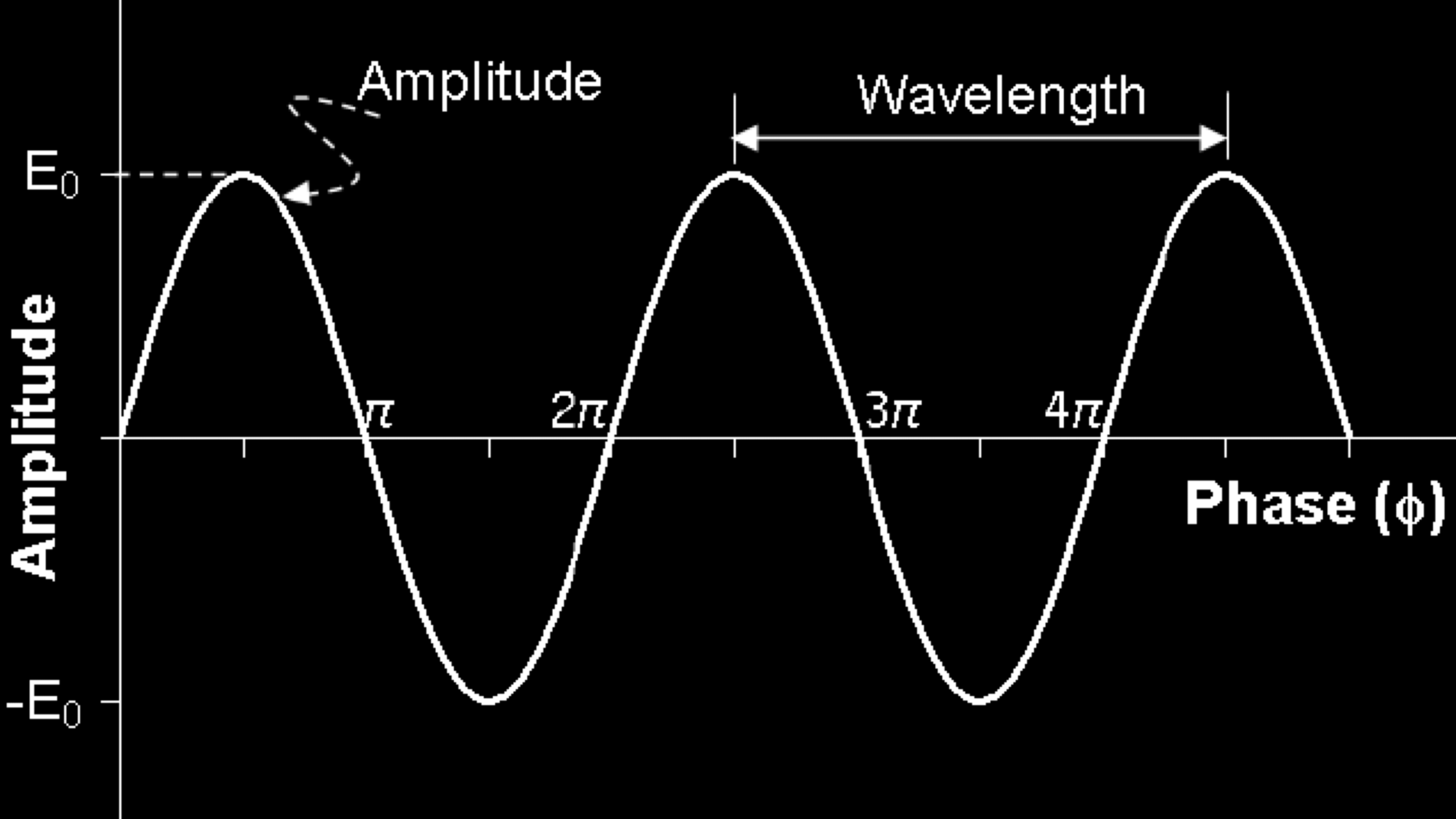
THE ELECTROMAGNETIC SPECTRUM

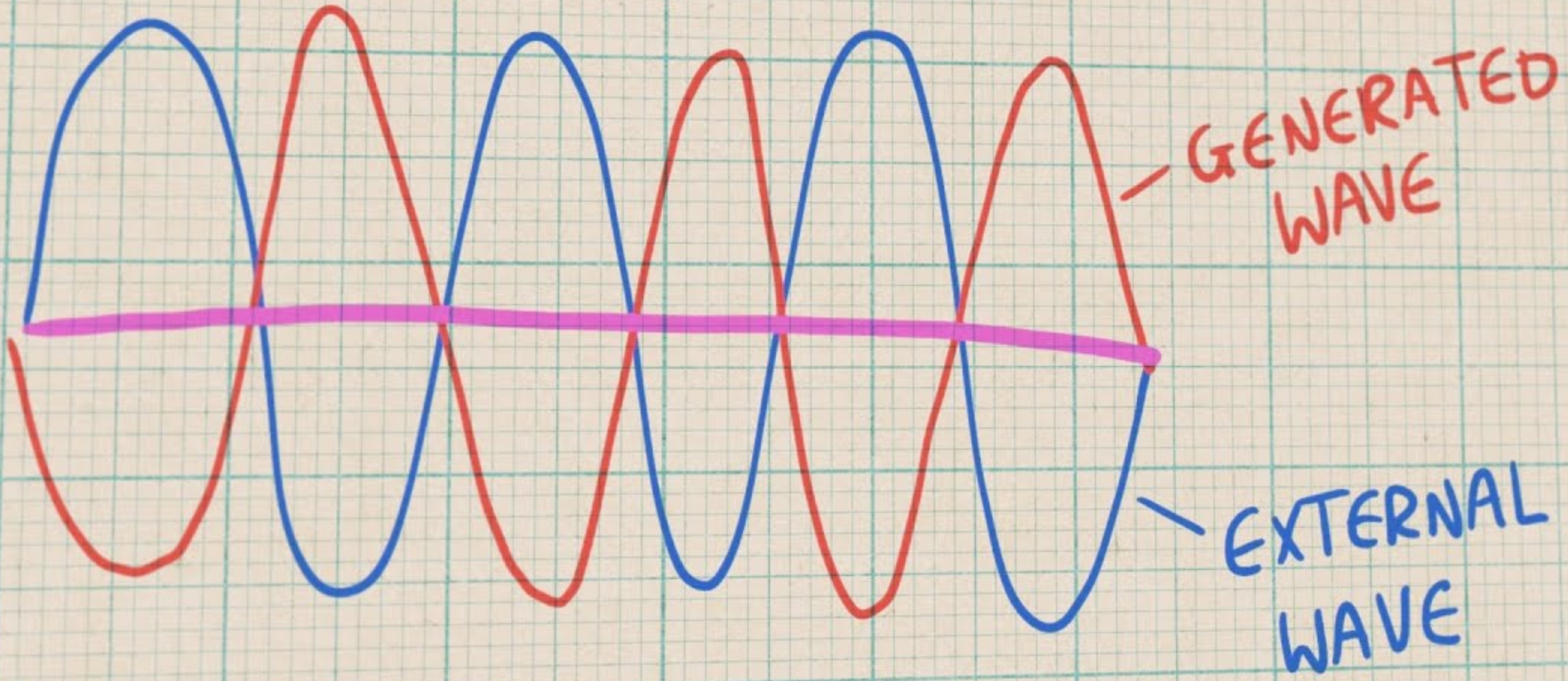
THESE WAVES TRAVEL THROUGH THE ELECTROMAGNETIC FIELD. THEY WERE FORMERLY CARRIED BY THE AETHER, WHICH WAS DECOMMISSIONED IN 1897 DUE TO BUDGET CUTS.



xkcd.com/273/

waves


Amplitude
Wavelength
E_0
$-E_0$
Amplitude
π
2π
3π
4π
Phase (ϕ)


GENERATED WAVE
EXTERNAL WAVE

SCI
HUB



youtube.com/watch?v=Iuv6hY6zsd0 (/Veritasium)

light

visible

STEM
@stem_feed

Isaac Newton designing the cover for Pink Floyd's album.



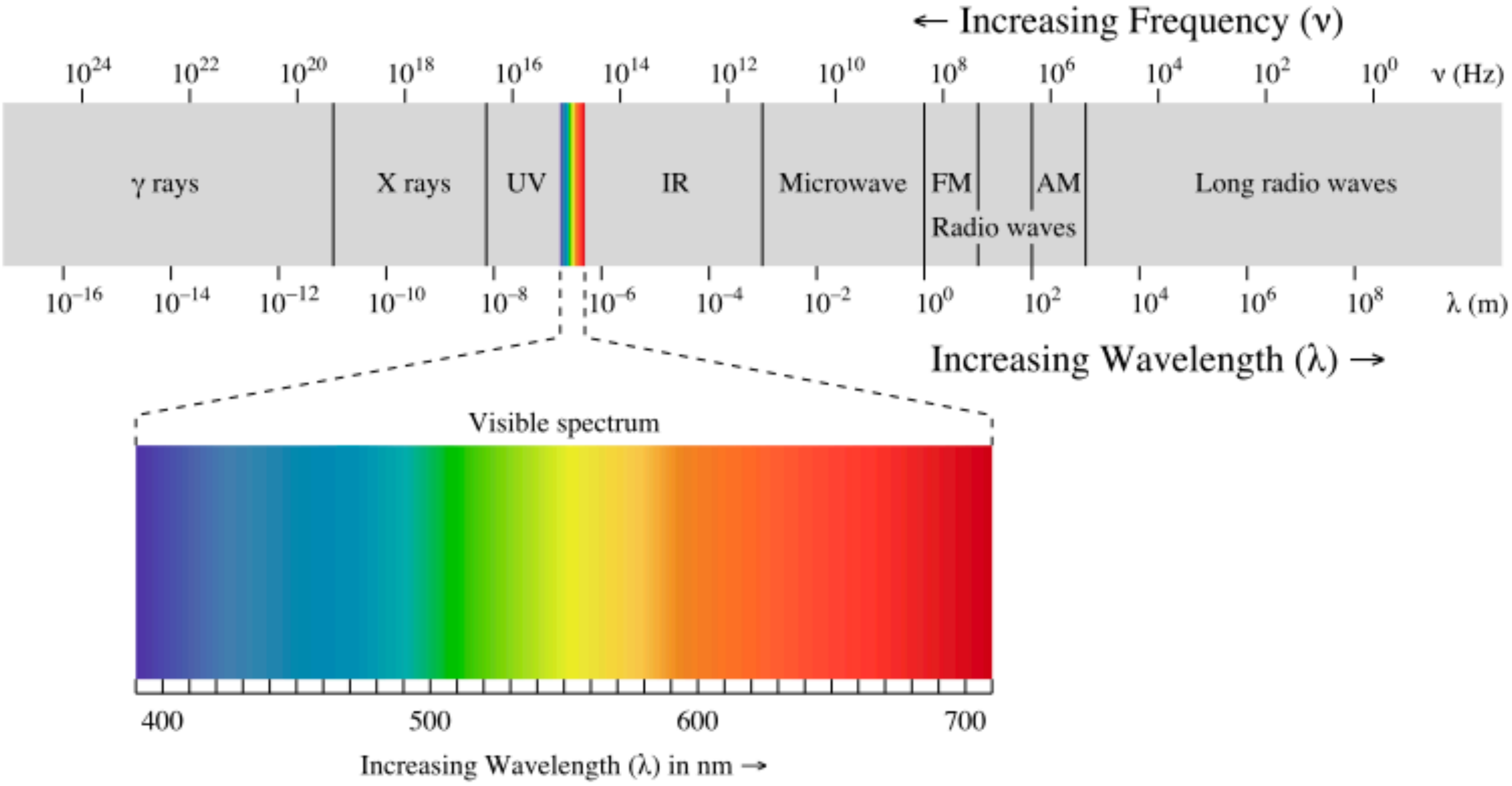
twitter.com/stem_feed/status/1533465304654700544

The Dark Side of the Moon

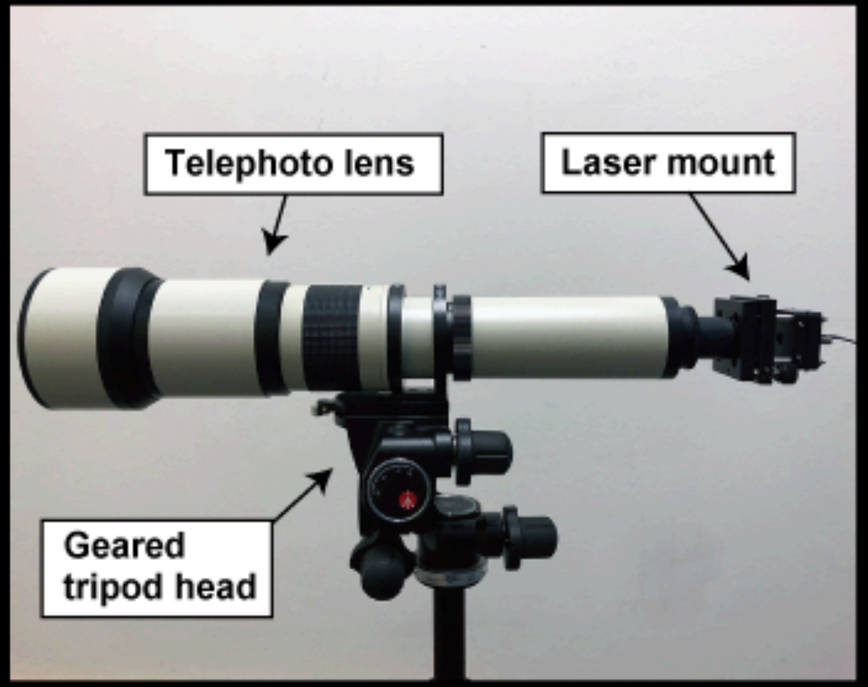


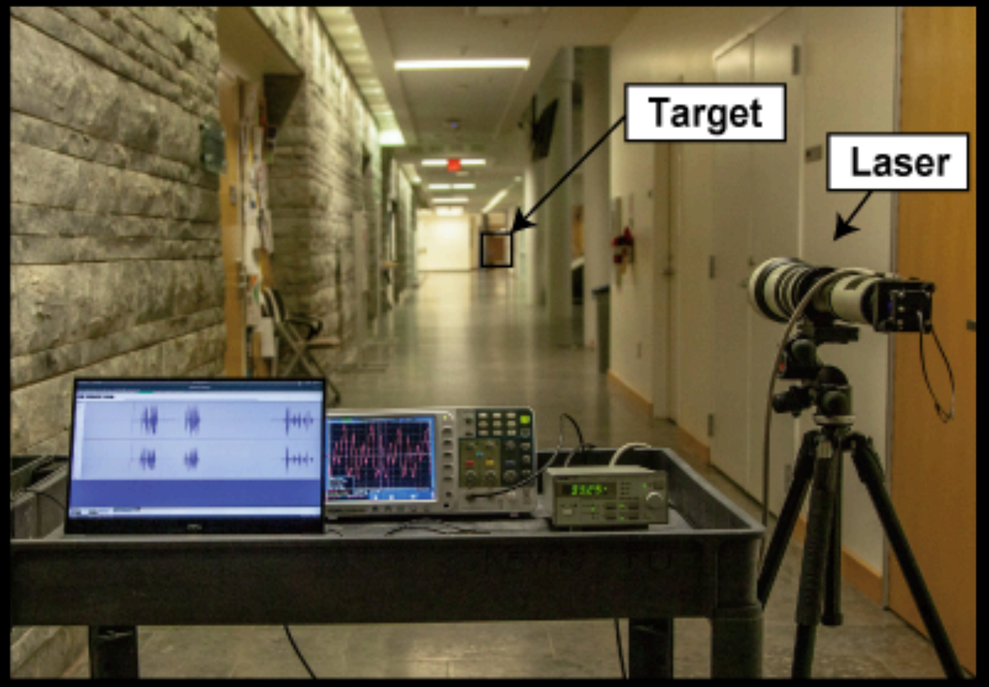
Studio album by Pink Floyd

Released	1 March 1973
Recorded	31 May 1972 – 9 February 1973[1]


← Increasing Frequency (ν)
10^{24} 10^{22} 10^{20} 10^{18} 10^{16} 10^{14} 10^{12} 10^{10} 10^{8} 10^{6} 10^{4} 10^{2} 10^{0} ν (Hz)
γ rays
X rays
UV
IR
Microwave
FM
AM
Radio waves
Long radio waves
10^{-16} 10^{-14} 10^{-12} 10^{-10} 10^{-8} 10^{-6} 10^{-4} 10^{-2} 10^{0} 10^{2} 10^{4} 10^{6} 10^{8} λ (m)
Increasing Wavelength (λ) →
Visible spectrum
400 500 600 700
Increasing Wavelength (λ) in nm →

visible light fault injection







lightcommands.com/20191104-Light-Commands.pdf

fault injection



example from @jzvw


TILT


MISSED
MISSED
HOW TO OPERATE
SCORE VOIDED IF MACHINE HAS BEEN TILTED
2 - Push RED knob to elevate ball to playing surface.
3 - Pull back BLACK knob on plunger and release.
example from @jzvw

light

—

infrared

infra- from Latin, “below”

“In my experience, once data becomes invisible, something magical happens: they forget about security”

- Adam "Major Malfunction" Laurie

adamsblog.aperturelabs.com/2013_03_01_archive.html

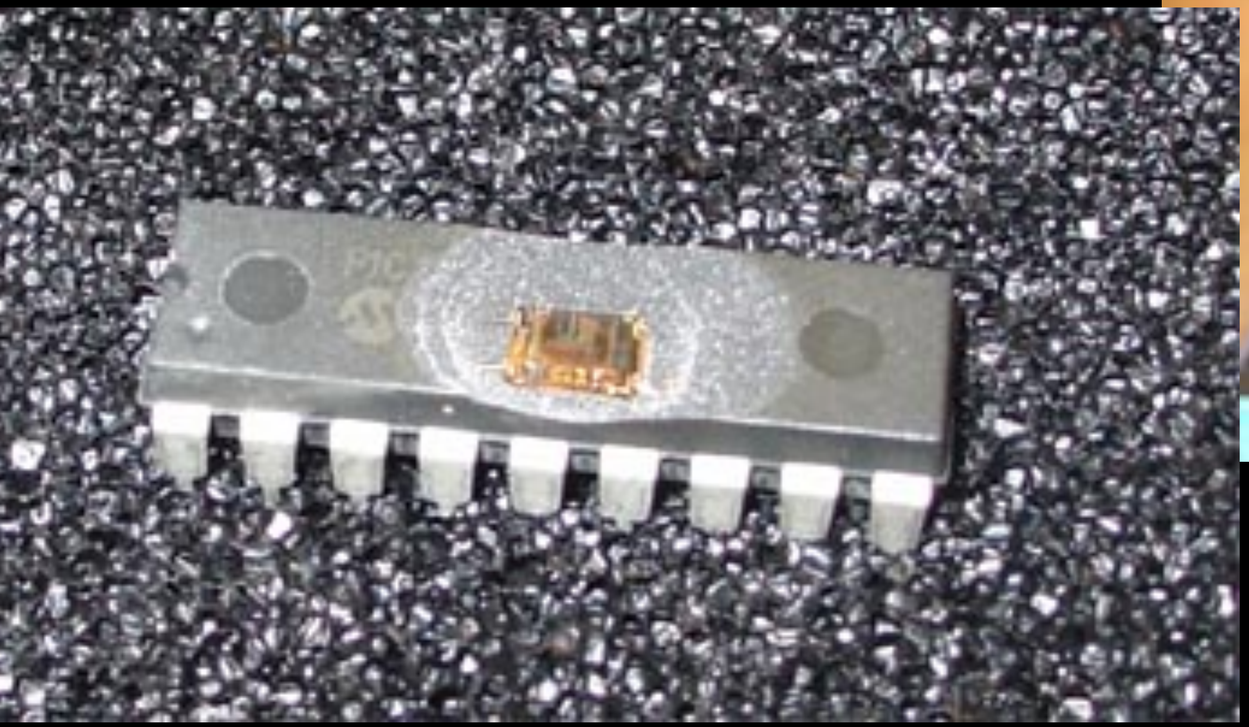
light

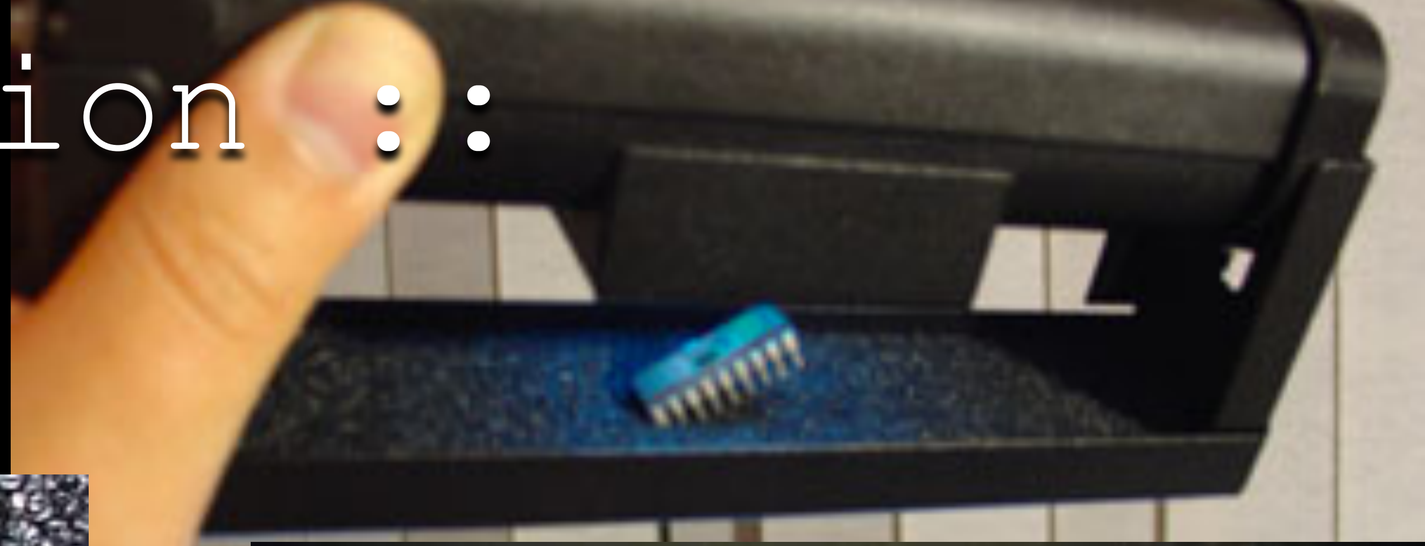
---

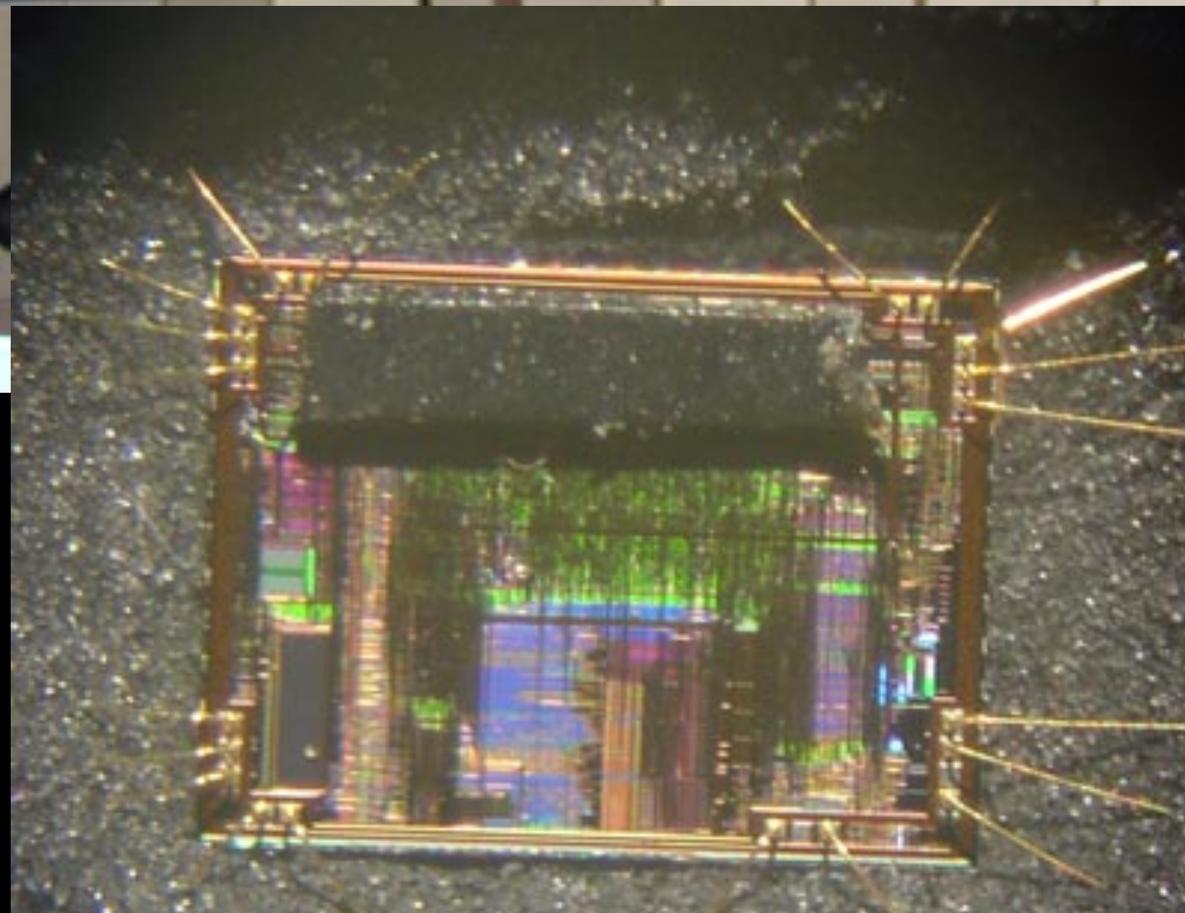
ultraviolet

ultra- from Latin
“beyond” or “on the far side of"

fault injection :: ultraviolet

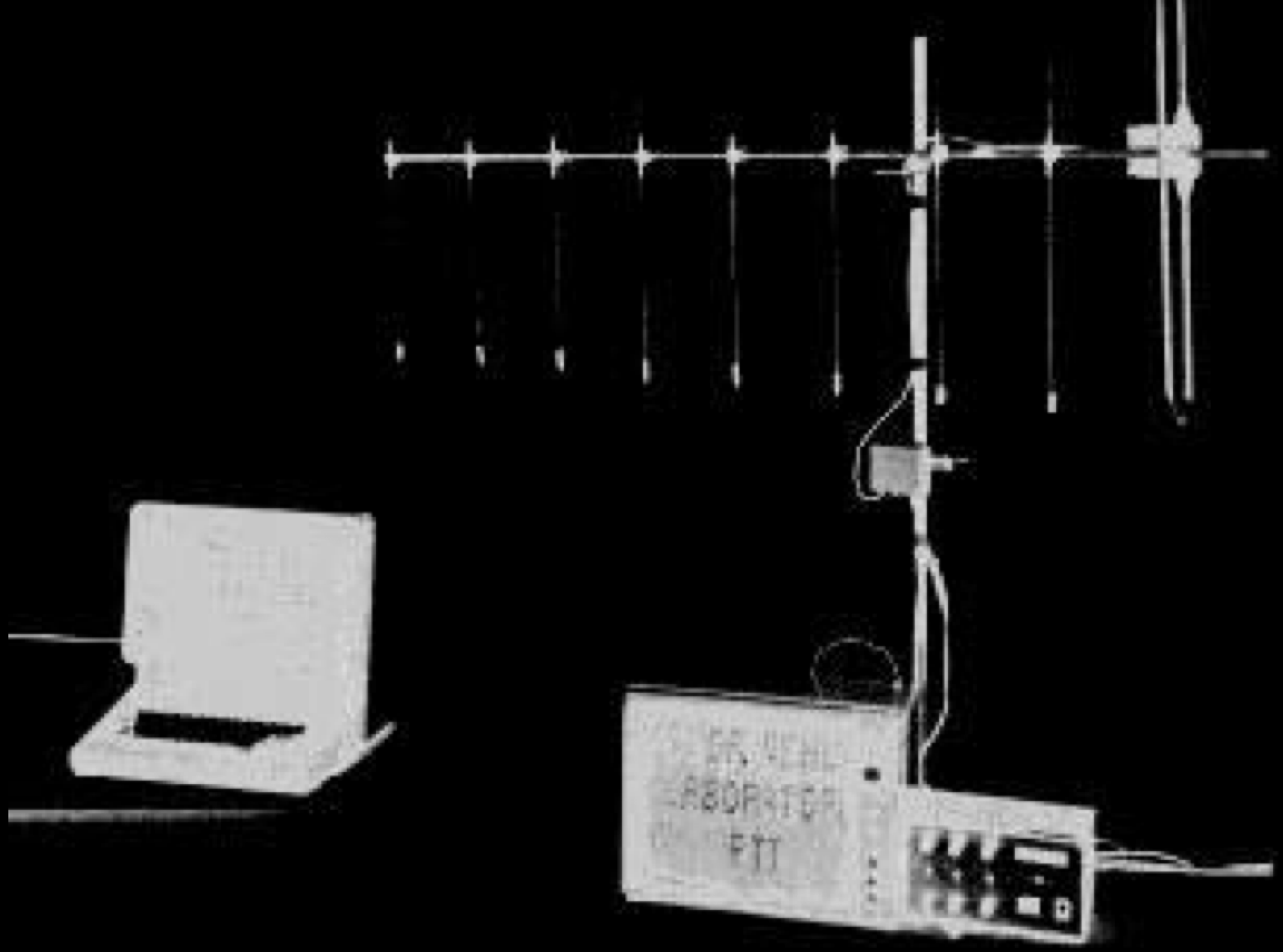






www.bunniestudios.com/blog/?page_id=40

radio



nsa.gov/ REDACTED frequency/ REDACTED pdf

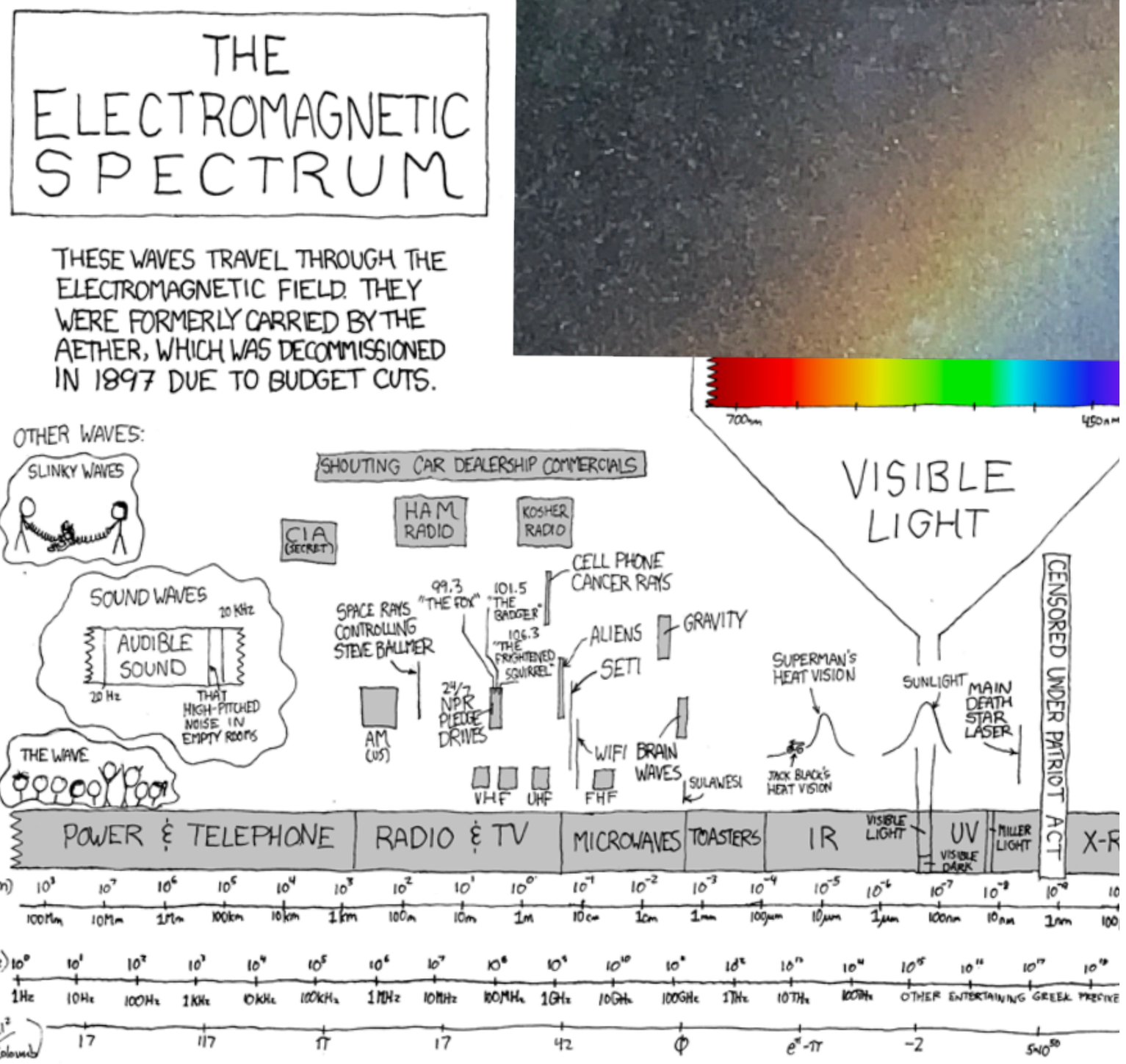
electro-magnetism

electro-magnetism

electro- from Greek ‘ēlektron’, “amber”

electro-magnetism

electro- from Greek ‘ēlektron’, “amber”
magnetism from ‘magnētis lithos’, "Magnesian stone"



Class			Wave-length λ	Freq-uency f	Energy per photon E
Ionizing radiation	γ	Gamma rays	1 pm	300 EHz	1.24 MeV
	HX	Hard X-rays	10 pm	30 EHz	124 keV
	SX	Soft X-rays	100 pm	3 EHz	12.4 keV
			1 nm	300 PHz	1.24 keV
	EUV	Extreme ultraviolet	10 nm	30 PHz	124 eV
	NUV	Near ultraviolet, visible	100 nm	3 PHz	12.4 eV
			1 μm	300 THz	1.24 eV
	NIR	Near infrared	10 μm	30 THz	124 meV
	MIR	Mid infrared	100 μm	3 THz	12.4 meV
	FIR	Far infrared	1 mm	300 GHz	1.24 meV
Micro-waves	EHF	Extremely high frequency	1 cm	30 GHz	124 μeV
	SHF	Super high frequency	1 dm	3 GHz	12.4 μeV
	UHF	Ultra high frequency	1 m	300 MHz	1.24 μeV
Radio waves	VHF	Very high frequency	10 m	30 MHz	124 neV
	HF	High frequency	100 m	3 MHz	12.4 neV
	MF	Medium frequency	1 km	300 kHz	1.24 neV
	LF	Low frequency	10 km	30 kHz	124 peV
	VLF	Very low frequency	100 km	3 kHz	12.4 peV
	ULF	Ultra low frequency	1 Mm	300 Hz	1.24 peV
	SLF	Super low frequency	10 Mm	30 Hz	124 feV
	ELF	Extremely low frequency	100 Mm	3 Hz	12.4 feV

Sources: File:Light spectrum.svg[1][2][3]



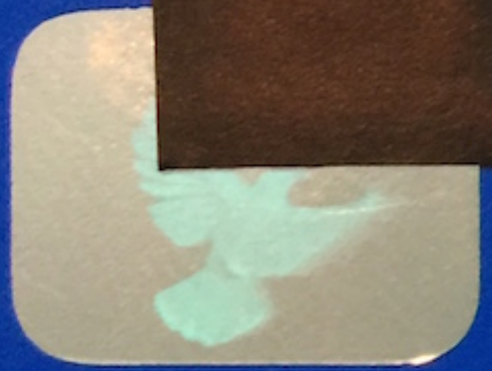
samy.pl/magspoof

Use of this card is subject to the cardmember agreement. 140259H 04/14 4147-12-170-52

chase.com/freedom | 1-800-524-3880 | Int'l Collect: 1-302-594-8200 | Español: 1-888-446-3308



Not



CHASE

samy.pl/magspoof



samy.pl/magspoof

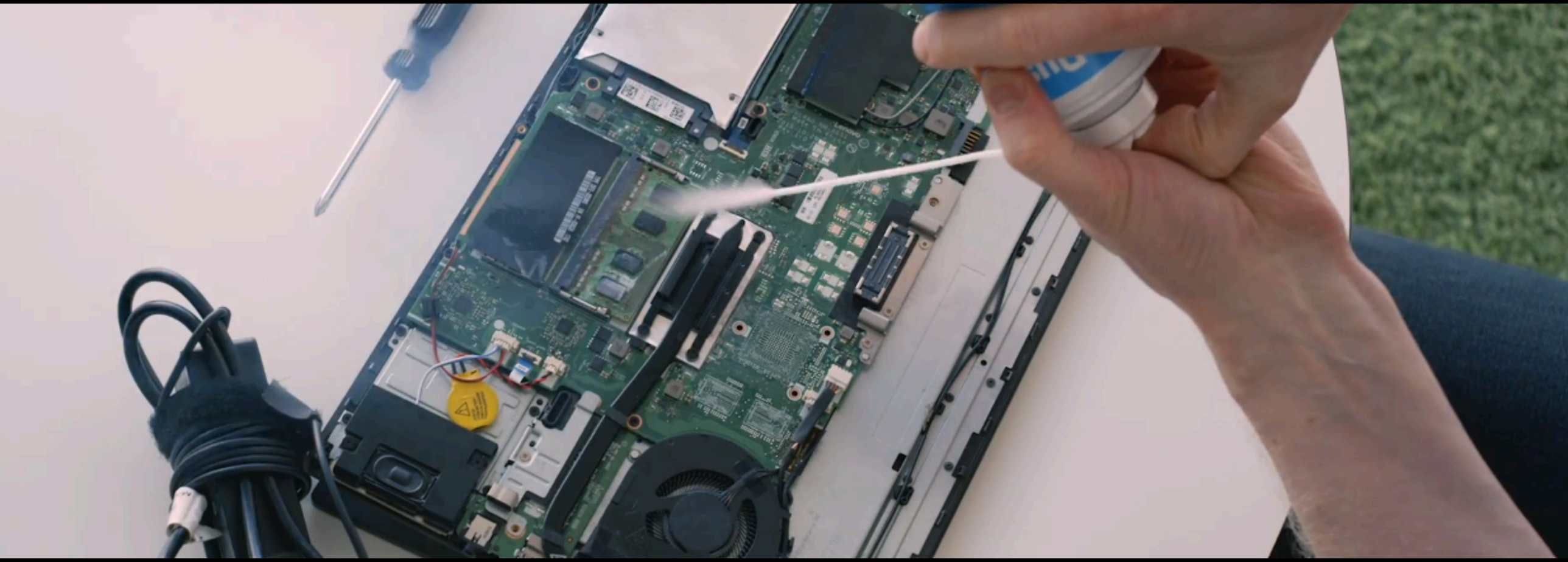
temperature

side channel :: infrared (IR)



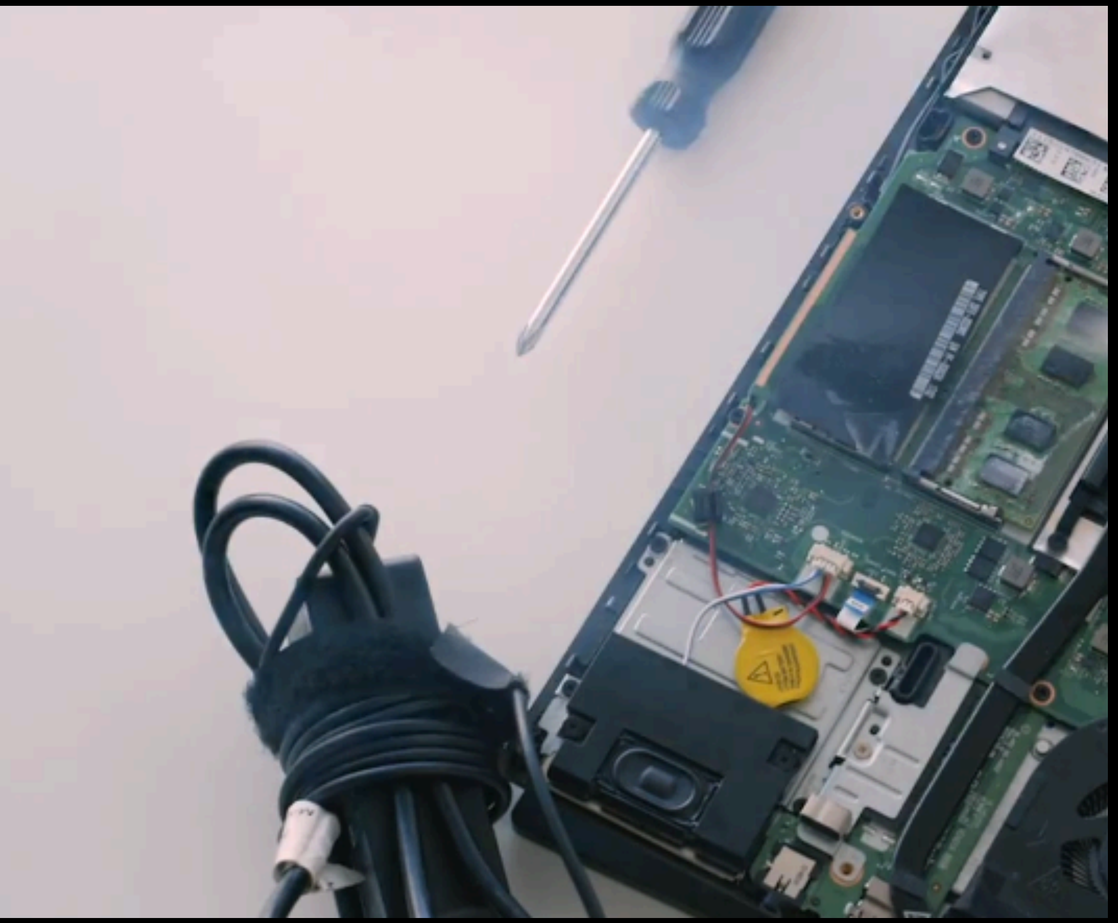
youtu.be/8Vc-69M-UWk

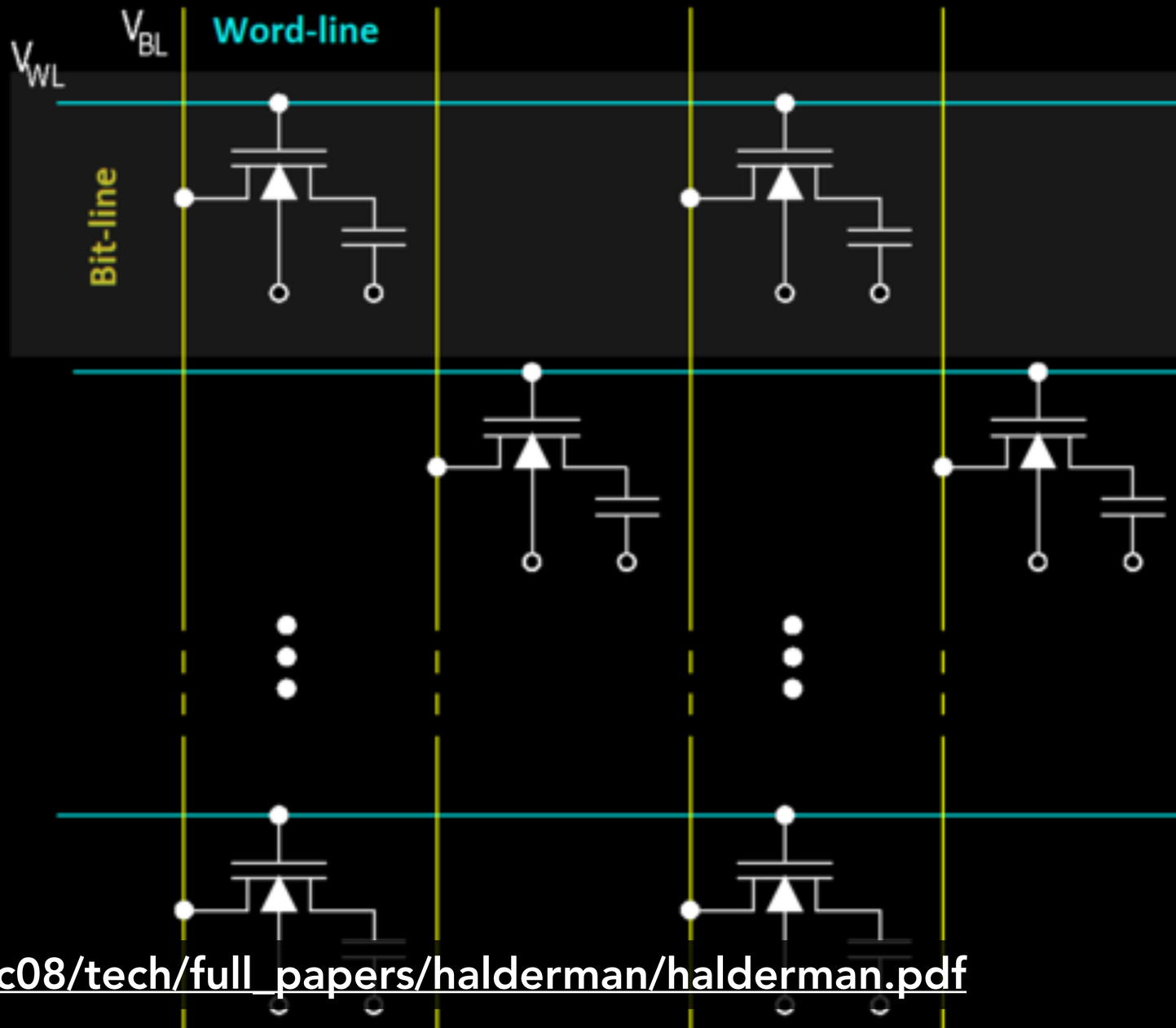
fault injection :: temperature



www.usenix.org/legacy/event/sec08/tech/full_papers/halderman/halderman.pdf

fault injection :: temperature





www.usenix.org/legacy/event/sec08/tech/full_papers/halderman/halderman.pdf

sound

sound

—

audible

(meaning, to most humans)

side channel :: audible sound





people.eecs.berkeley.edu/~tygar/papers/Keyboard_Acoustic_Emanations_Revisited/TISSEC.pdf

sound

—

ultrasound

ultra- from Latin

“beyond” or “on the far side of"



cs.tau.ac.il/~tromer/acoustic

fault injection :: ultrasound



www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-son-updated.pdf

energy conversion

Leon Theremin



Lev Termen demonstrating the theremin, December 1927

Born	Lev Sergeyevich Termen 27 August [O.S. 15 August] 1896 Saint Petersburg, Russian Empire
Died	3 November 1993 (aged 97) Moscow, Russia
Occupation(s)	Engineer, physicist
Known for	Theremin, The Thing

Theremin



Leon Theremin



Lev Termen demonstrating the theremin, December 1927

Born	Lev Sergeyevich Termen 27 August [O.S. 15 August] 1896 Saint Petersburg, Russian Empire
Died	3 November 1993 (aged 97) Moscow, Russia
Occupation(s)	Engineer, physicist
Known for	Theremin, The Thing

k g b

Leon Theremin



Lev Termen demonstrating the theremin, December 1927

Born	Lev Sergeyevich Termen 27 August [O.S. 15 August] 1896 Saint Petersburg, Russian Empire
Died	3 November 1993 (aged 97) Moscow, Russia
Occupation(s)	Engineer, physicist
Known for	Theremin, The Thing

The Thing



light + sound

—

~~laser~~ optical microphone

Sniffing Keystrokes With Lasers/Voltmeters



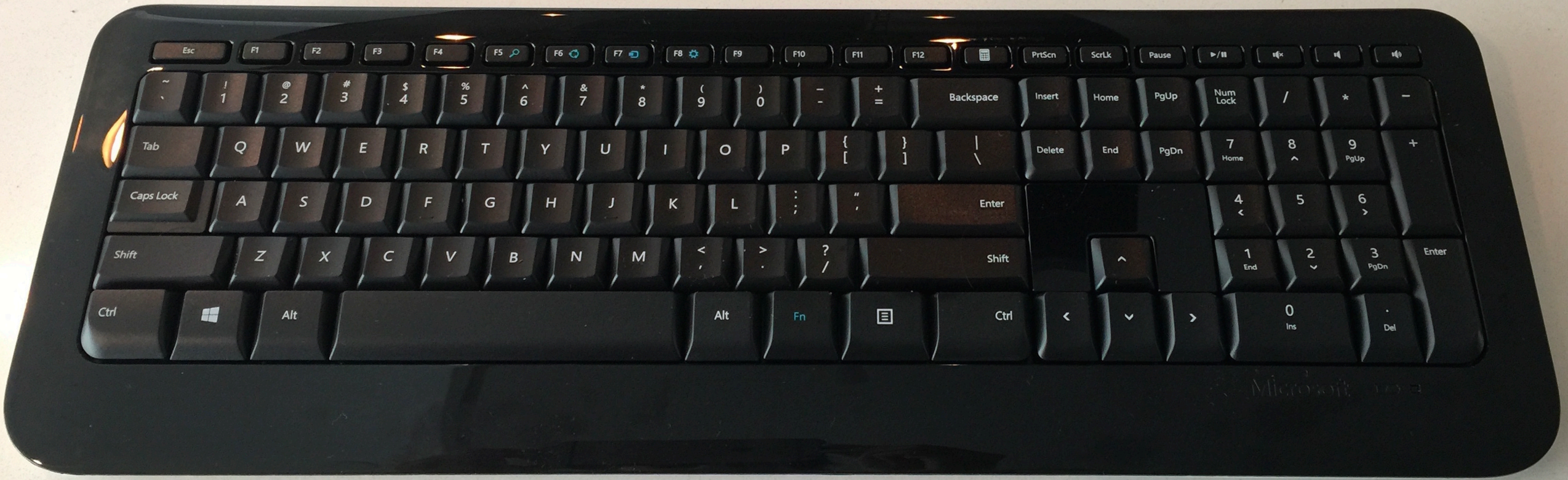
Side Channel Attacks Using Optical Sampling Of Mechanical Energy And Power Line Leakage

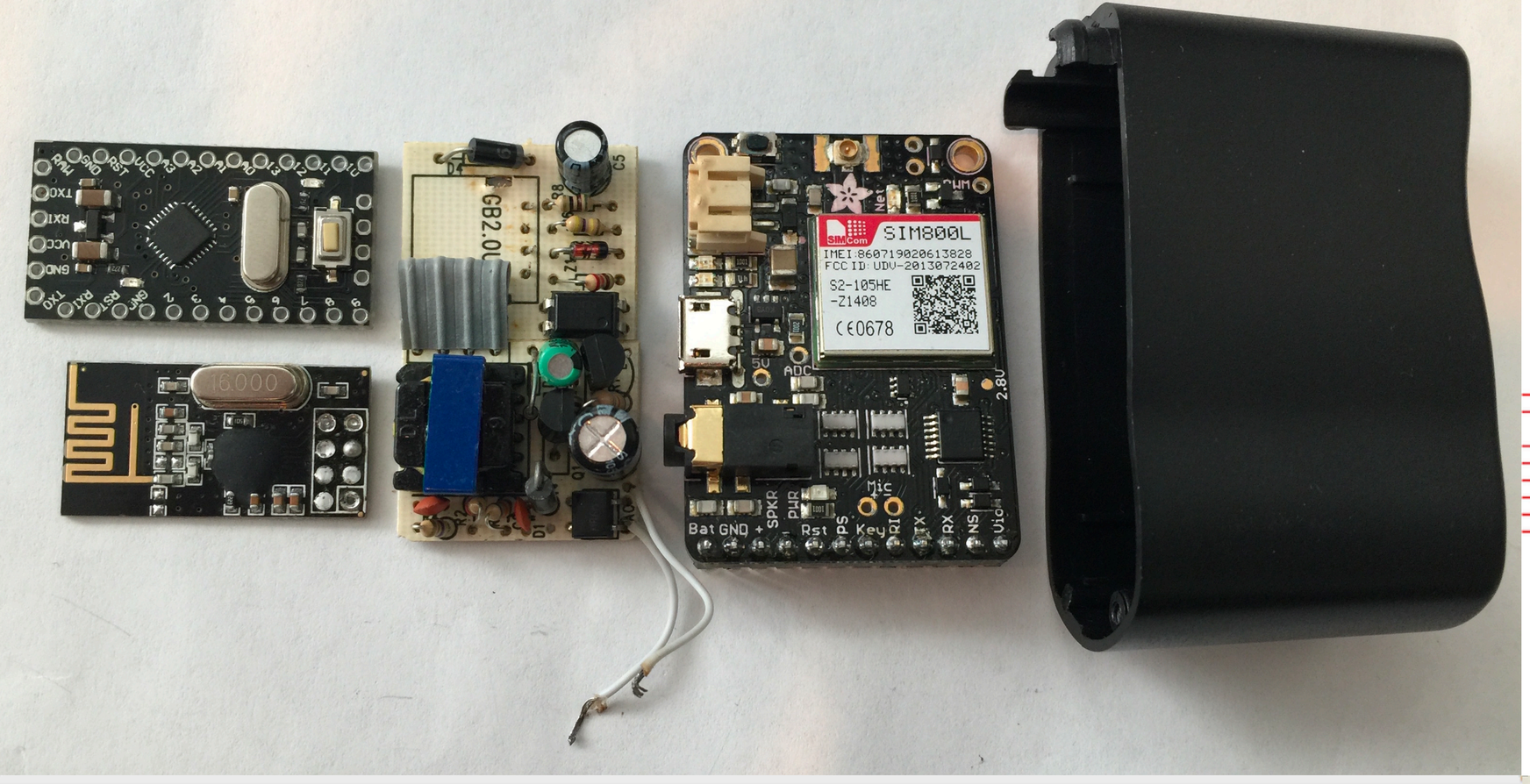
Andrea Barisani
Chief Security Engineer
<*andrea@inversepath.com*>

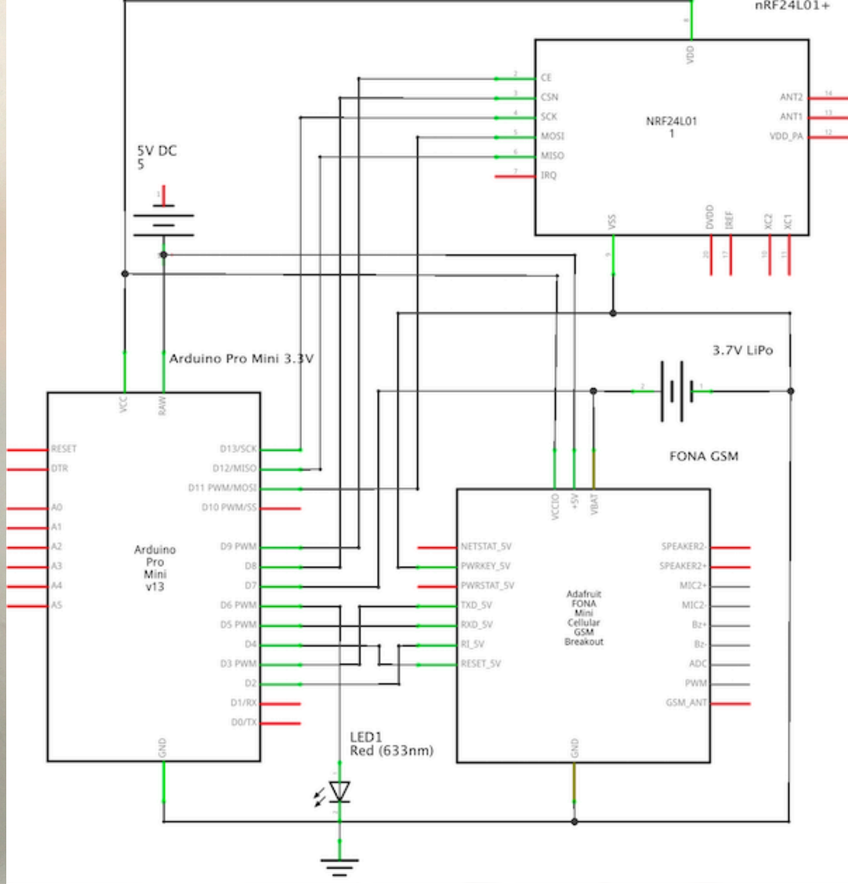
Daniele Bianco
Hardware Hacker
<*daniele@inversepath.com*>

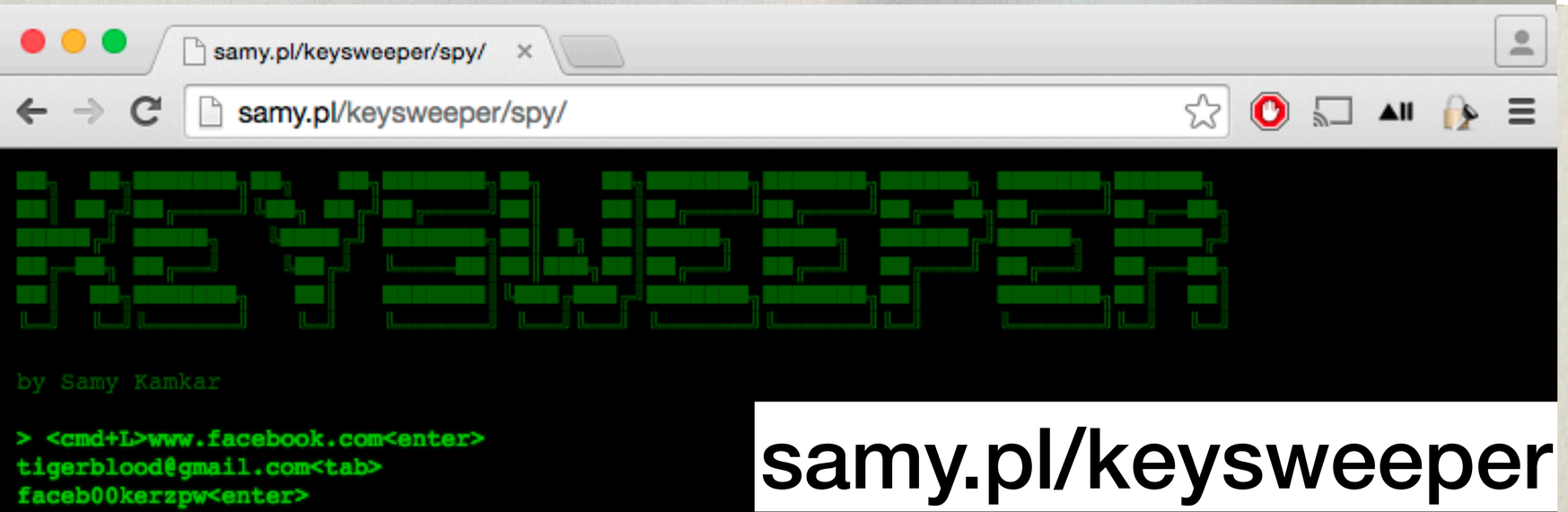
INVERSE PATH
http://www.inversepath.com

Copyright 2009 Inverse Path Ltd.


Esc
F1
F2
F3
F4
F5
F6
F7
F8
F9
F10
F11
F12
PrtScn
ScrLk
Pause
Backspace
Insert
Home
PgUp
Num Lock
Tab
Delete
End
PgDn
Caps Lock
Enter
Shift
Shift
Ctrl
Alt
Alt
Fn
Ctrl
Enter
Microsoft


SIM800L
IMEI:860719020613828
FCC ID: UDV-2013072402
S2-105HE
-Z1408
16.000


nRF24L01+
NRF24L01
1
5V DC
5
Arduino Pro Mini 3.3V
3.7V LiPo
FONA GSM
Arduino
Pro
Mini
v13
Adafruit
FONA
Mini
Cellular
GSM
Breakout
LED1
Red (633nm)


samy.pl/keysweeper/spy/
samy.pl/keysweeper/spy/
KEYSWEEPER
by Samy Kamkar
> <cmd+L>www.facebook.com<enter>
tigerblood@gmail.com<tab>
faceb00kerzpw<enter>
samy.pl/keysweeper



Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION



The KeySweeper device in use.

Wireless Keystroke Logger Disguised as USB Device Charger Targets Wireless Keyboards

Summary

KeySweeper is a covert device that resembles a functional Universal Serial Bus (USB) enabled device charger which conceals hardware capable of harvesting keystrokes from certain wireless keyboards. If placed strategically in an office or other location where individuals

info.publicintelligence.net/FBI-KeySweeper.pdf

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Additional best practices to prevent a compromise could include but are not limited to office policies that address mobile device chargers:

- Limiting which outlets are available for device charging
- Knowing whose chargers are currently being used
- Immediate removal of an unknown charger from the office facility (although the optional backup battery can allow data theft even when unplugged)

The KeySweeper device in use.

placed strategically in an office or other location where individuals

entially

erty.

info.publicintelligence.net/FBI-KeySweeper.pdf

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Additional best practices to prevent a compromise could include but are not limited to office policies that address mobile device chargers:

- Limiting which c[illegible] are available for device charging
- Knowing whose [illegible] are currently being used
- Immediate removal of an unknown [illegible] from the office facility (although the optional backup battery can allow data theft even when unplugged)

The KeySweeper device in use.

placed strategically in an office or other location where individuals

[illegible]entially

[illegible]erty.

info.publicintelligence.net/FBI-KeySweeper.pdf

Sniffing Keystrokes With Lasers/Voltmeters



Side Channel Attacks Using Optical Sampling Of Mechanical Energy And Power Line Leakage

Andrea Barisani
Chief Security Engineer
<andrea@inversepath.com>

Daniele Bianco
Hardware Hacker
<daniele@inversepath.com>

INVERSE PATH
http://www.inversepath.com

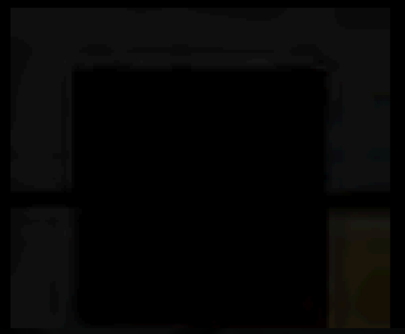
Copyright 2009 Inverse Path Ltd.

Laser Microphone Assembly

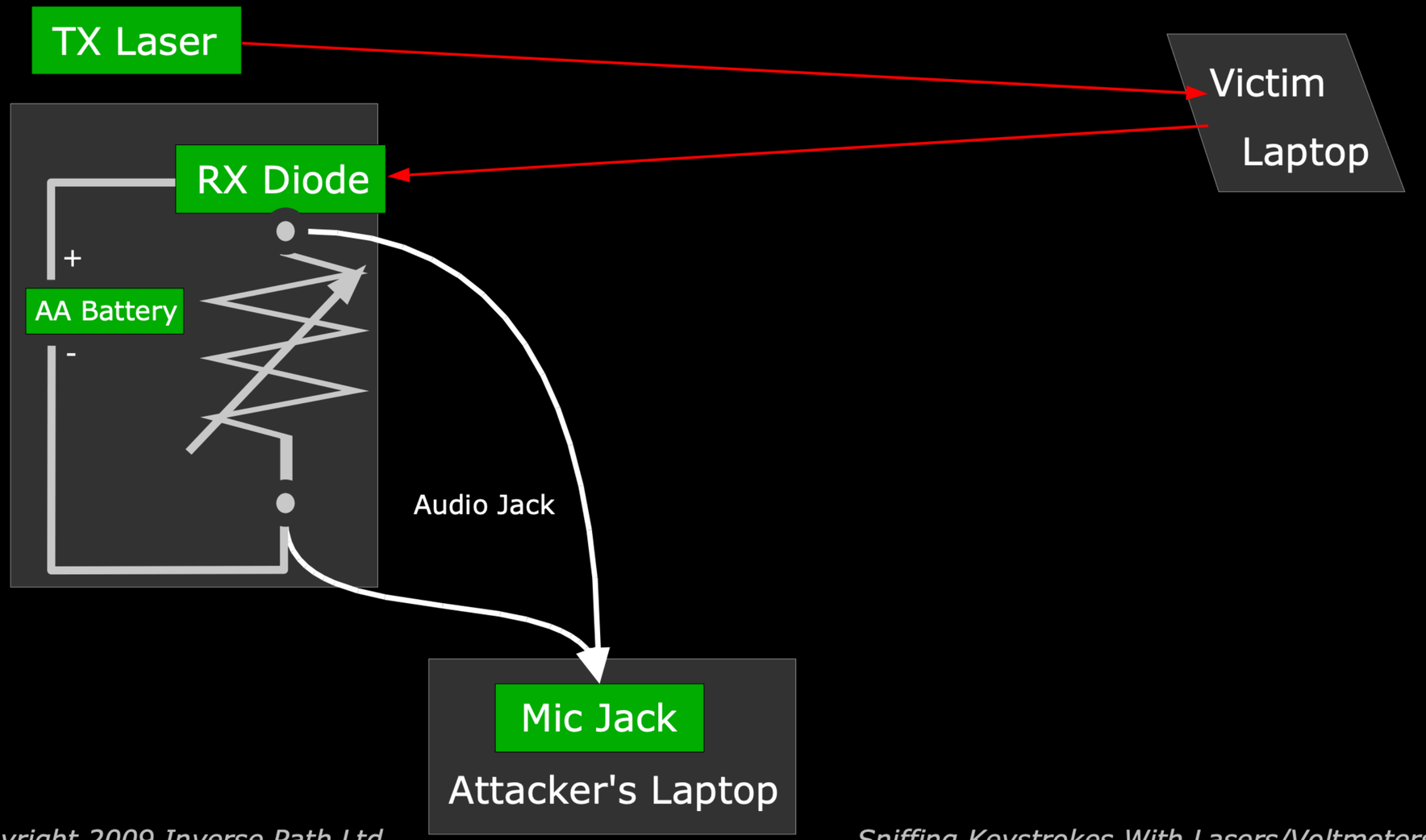


- 1 x Laser (more expensive lasers means more range)
- 1 x Photoresistor or Photodiode
- 1 x Resistor
- 1 x AA Battery
- 1 x Universal Power Adapter
- 1 x Jack Cable
- 1 x Laptop with sound card
- 2 x Tripod
- 1 x Focusing lens (for long distances)

$ 79.99



Diagram



Copyright 2009 Inverse Path Ltd.

more amazing research

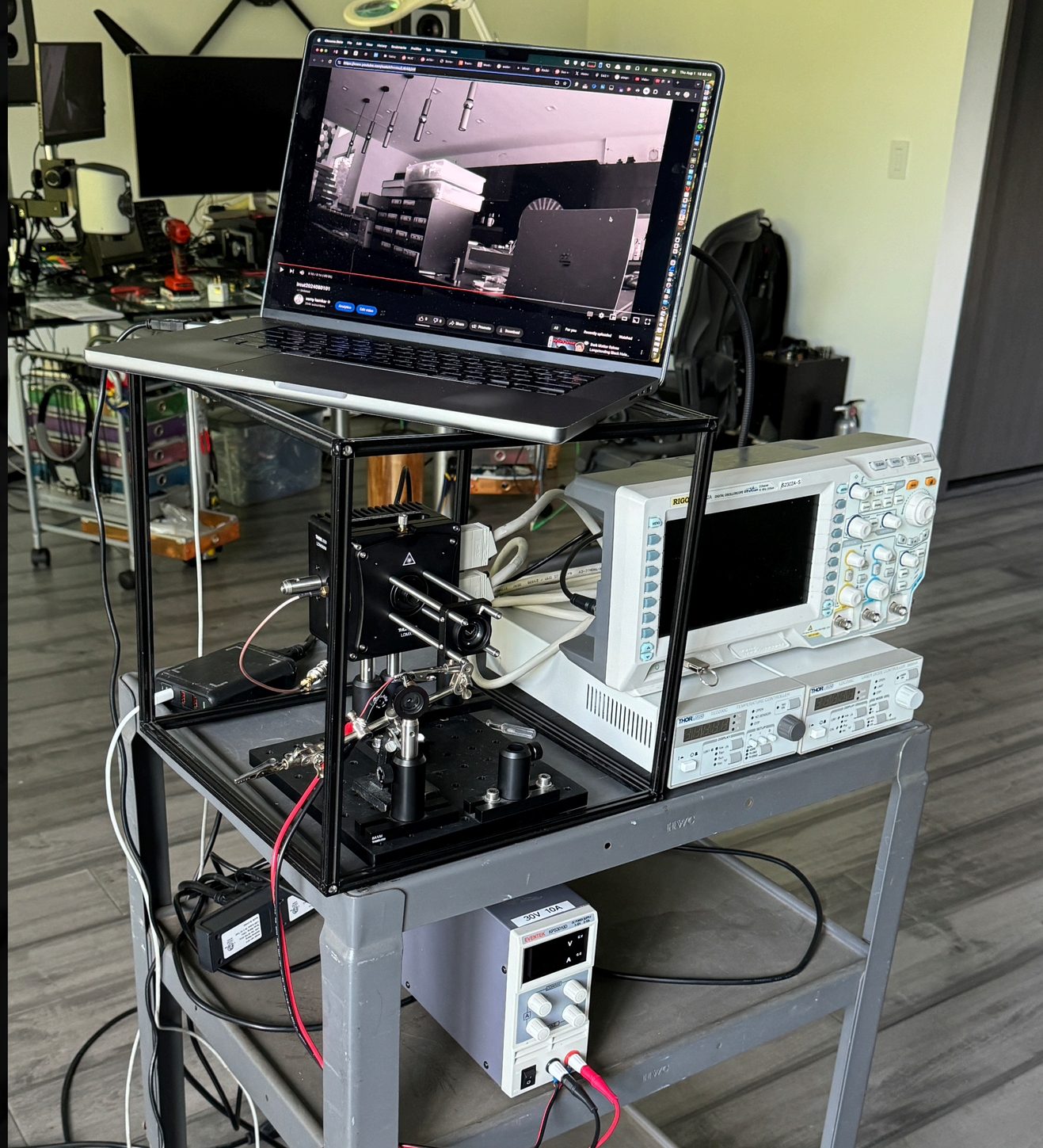
- Ben Nassi - Lampoon, Glowworm, …
- Andrea Barisani & Daniele Bianco: Sniffing Keystrokes With Lasers
- Joshua Harrison, Ehsan Toreini, and Maryam Mehrnezhad - Keyboard Acoustic Side Channels
- Daniel Genkin, Adi Shamir, Eran Tromer - Acoustic Cryptanalysis
- Li Zhuang, Feng Zhou, J. D. Tygar - Keyboard Acoustic Emanations Revisited
- NSA - ANT catalog, XKeyscore, …
- KGB - The Thing, …

the new laser microphone / keystroke snooper

laser safety

hardware

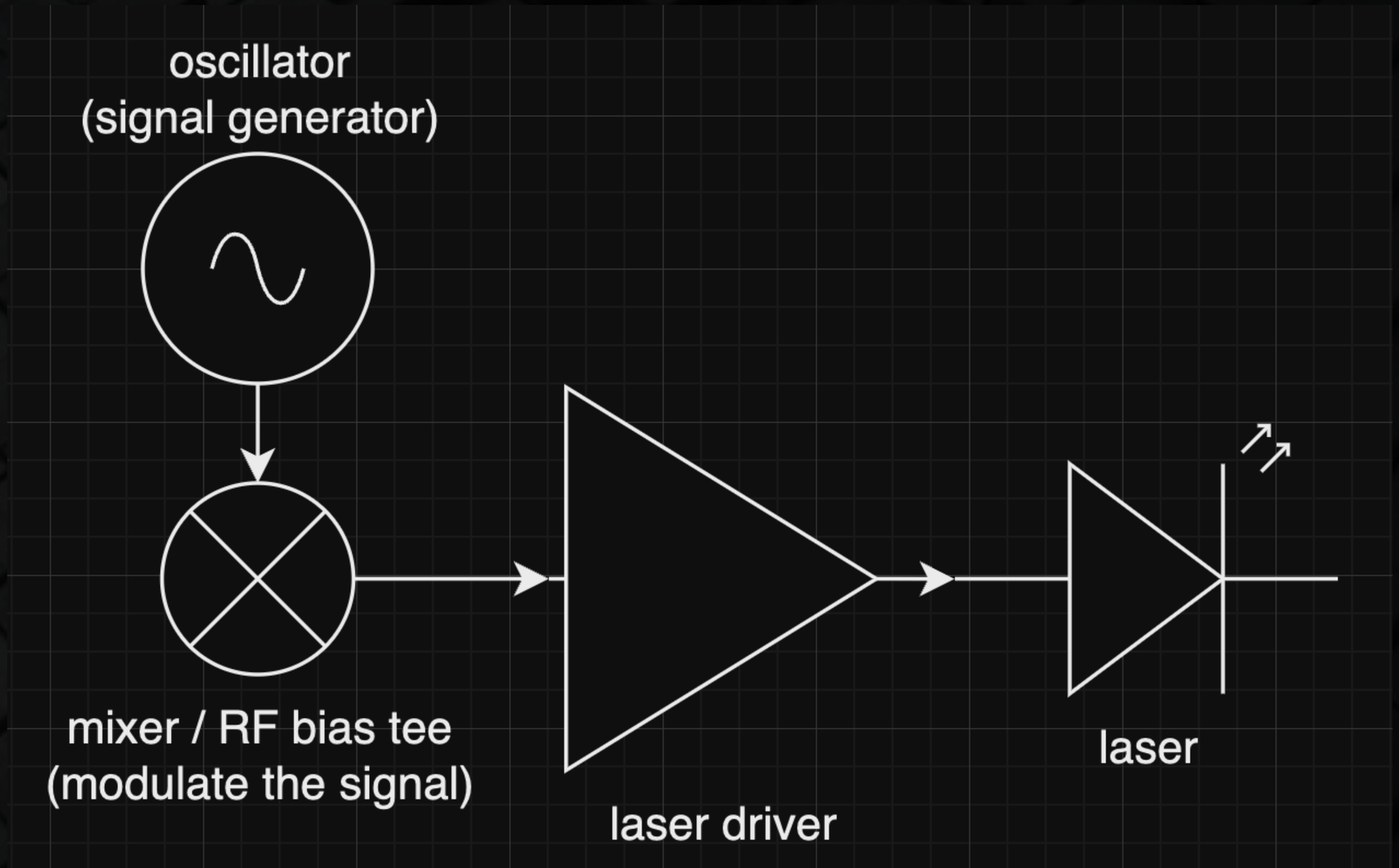
hardware tx side



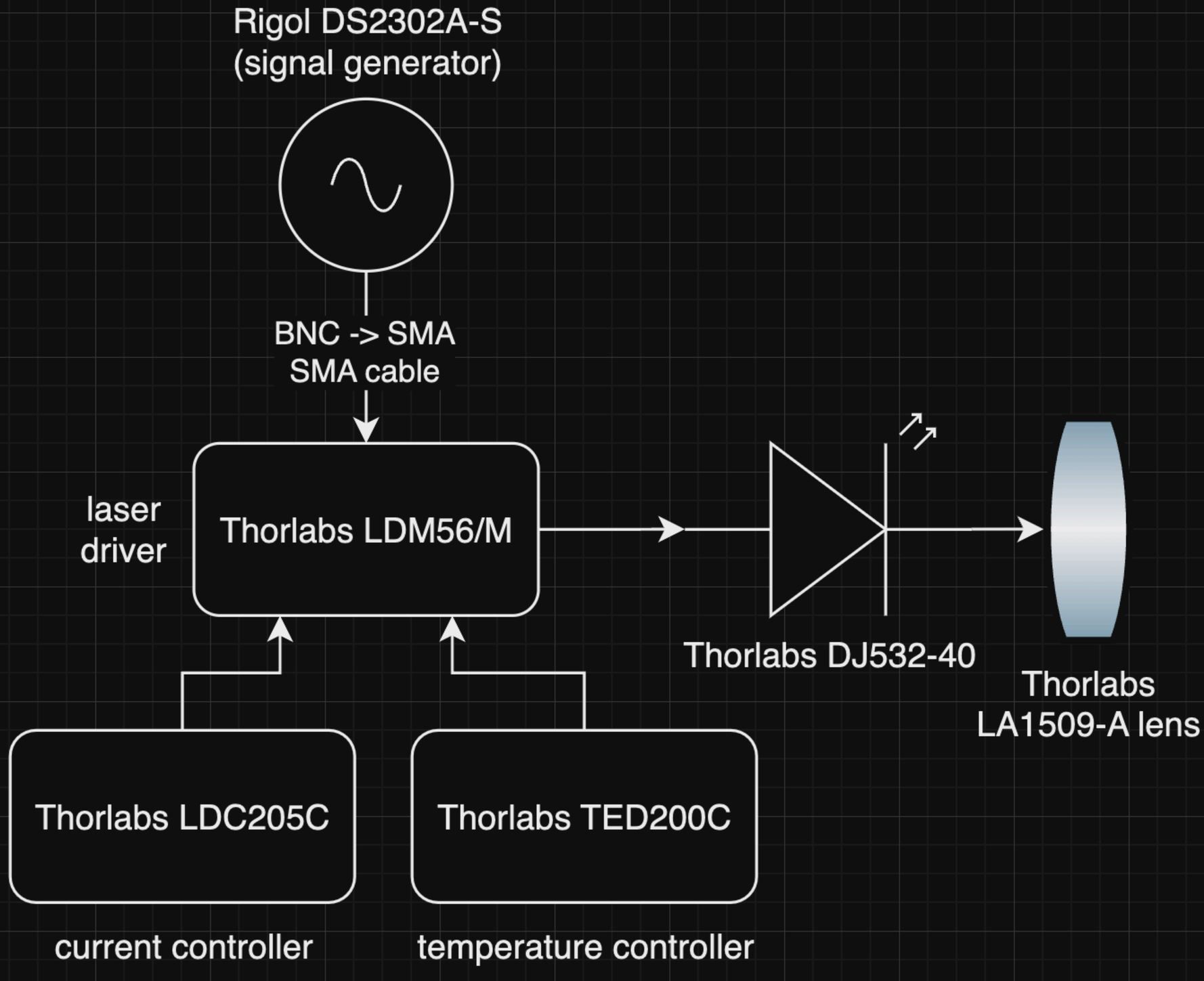
hardware
rx side

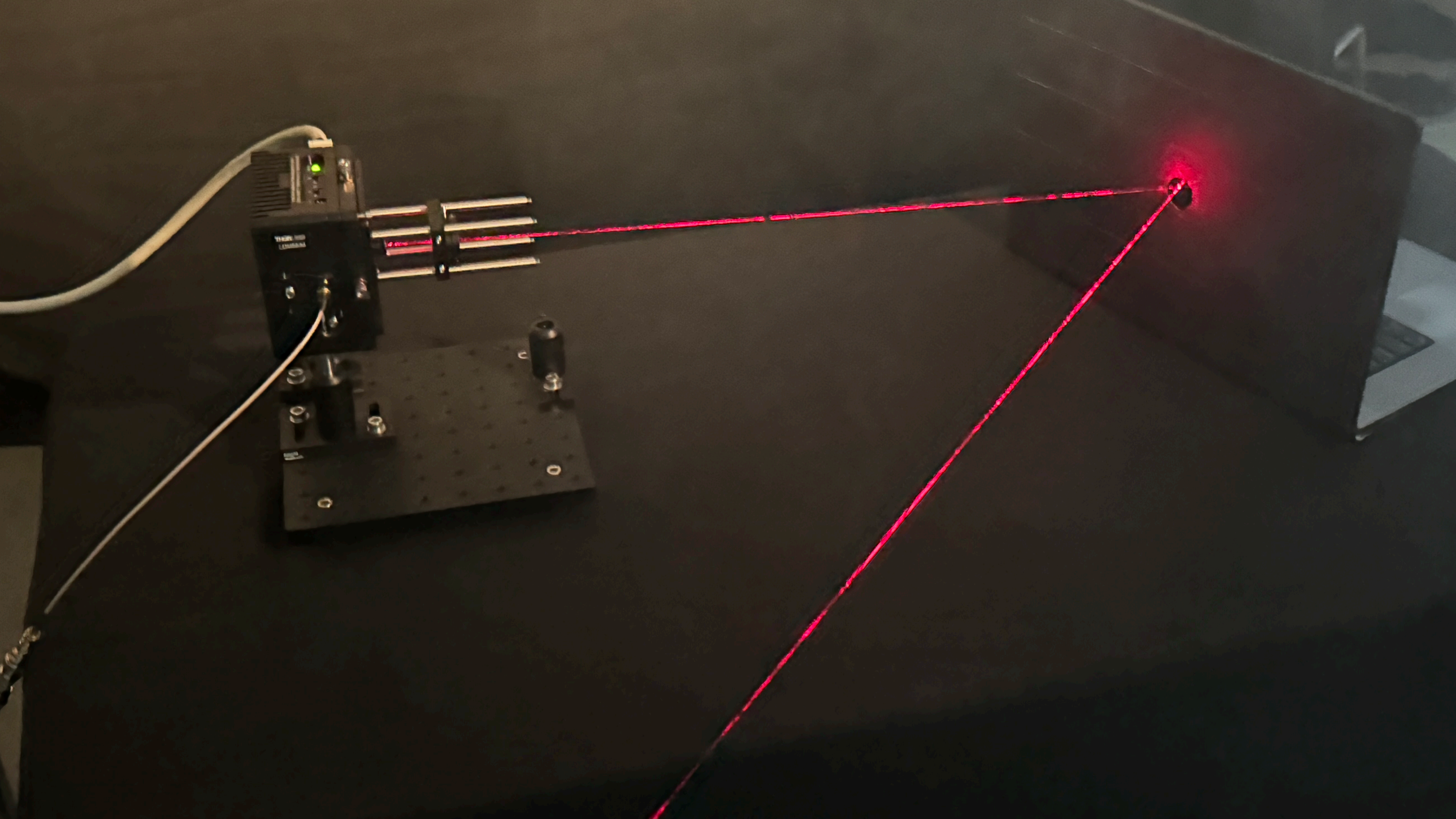


hardware (tx)


oscillator
(signal generator)
mixer / RF bias tee
(modulate the signal)
laser driver
laser

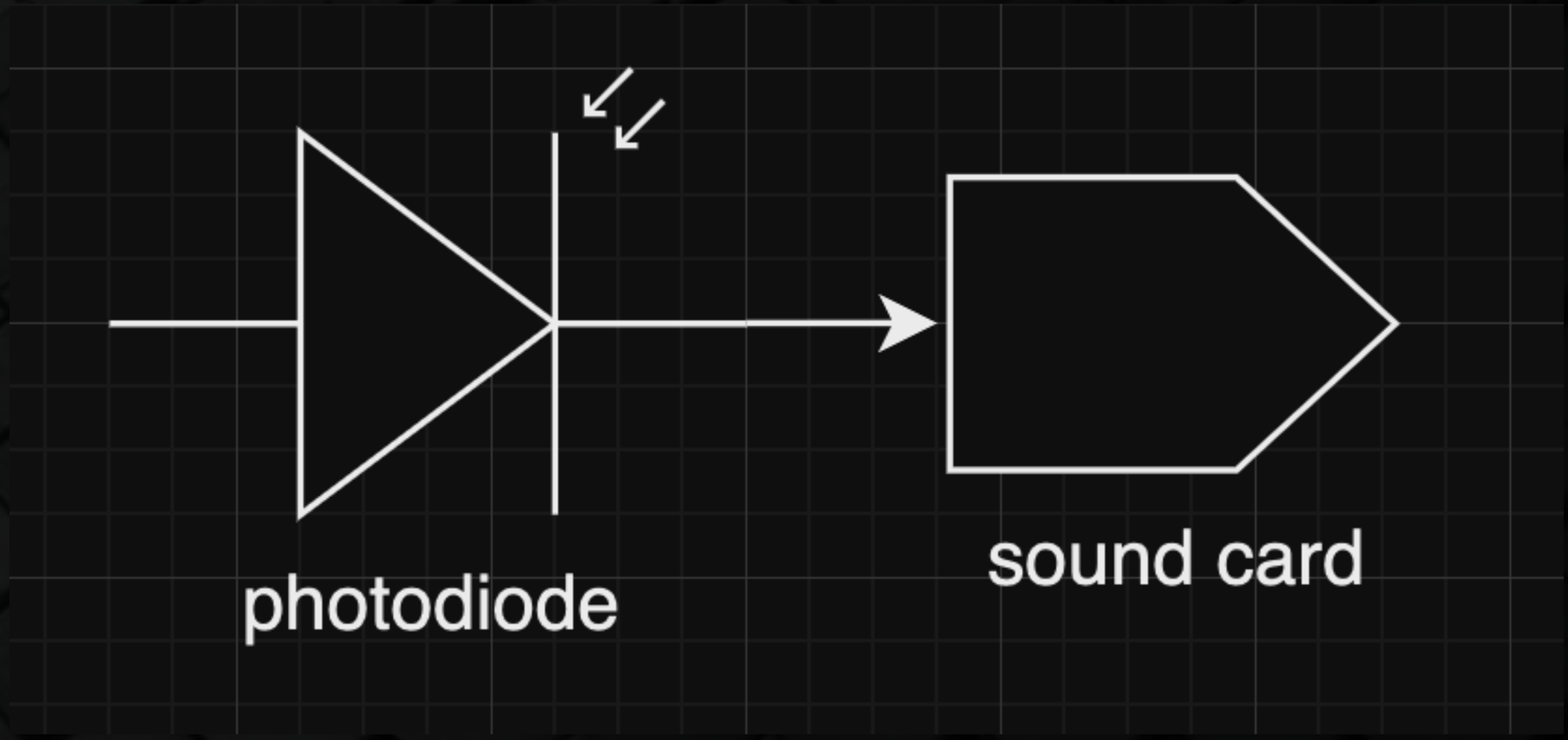
our tx side


Rigol DS2302A-S
(signal generator)
BNC -> SMA
SMA cable
laser
driver
Thorlabs LDM56/M
Thorlabs DJ532-40
Thorlabs
LA1509-A lens
Thorlabs LDC205C
Thorlabs TED200C
current controller
temperature controller

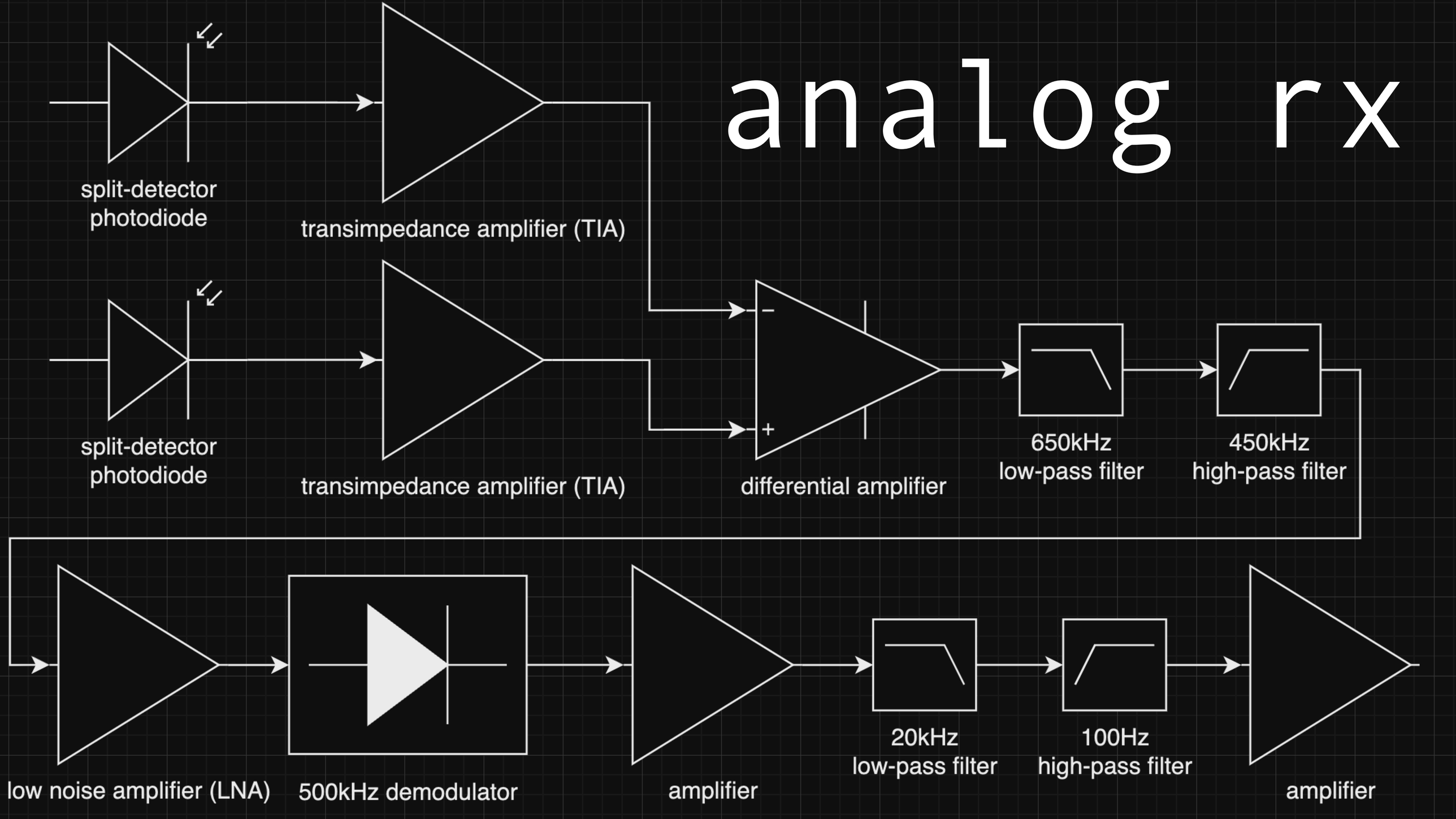


hardware (rx)

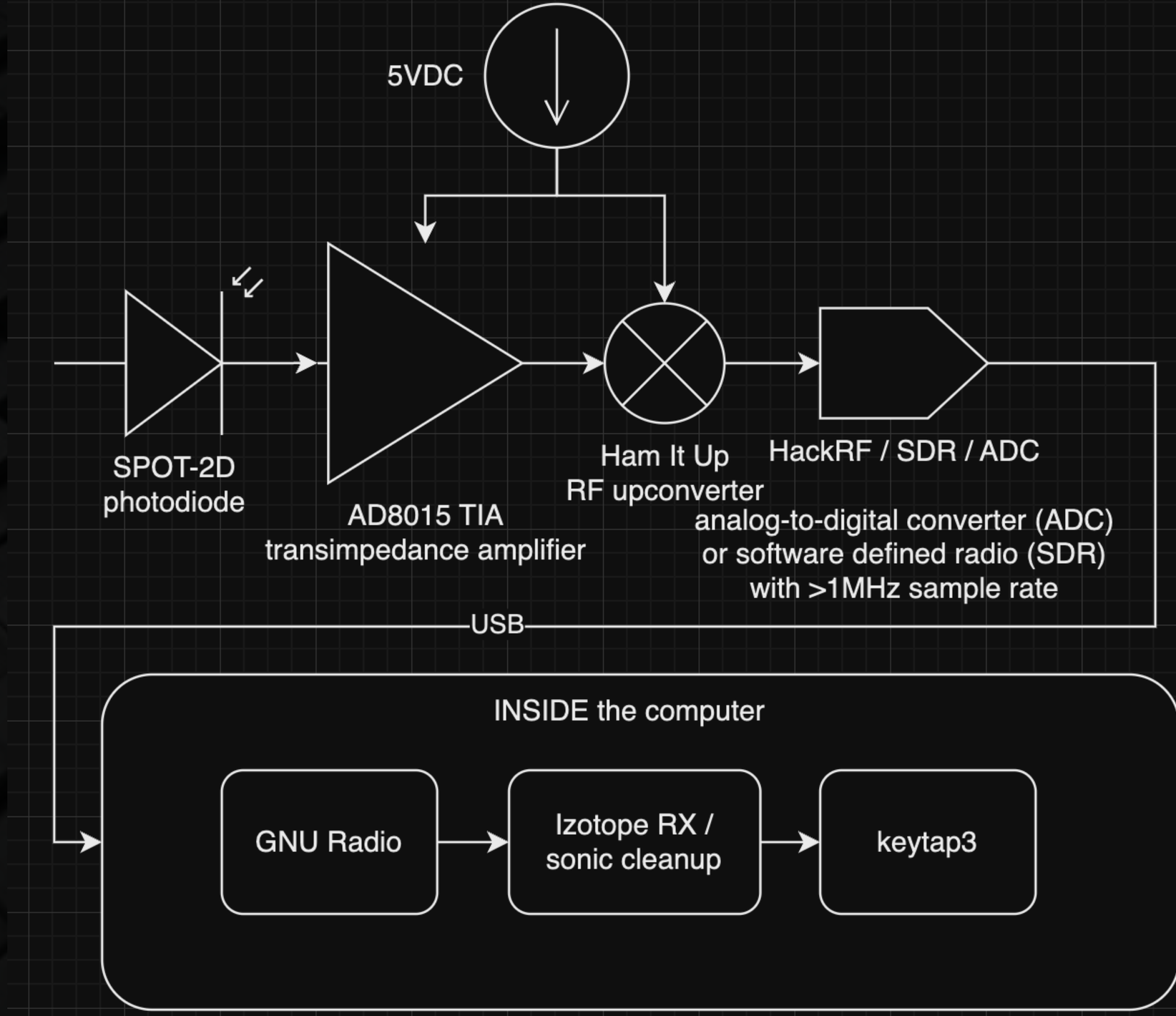
typical setup



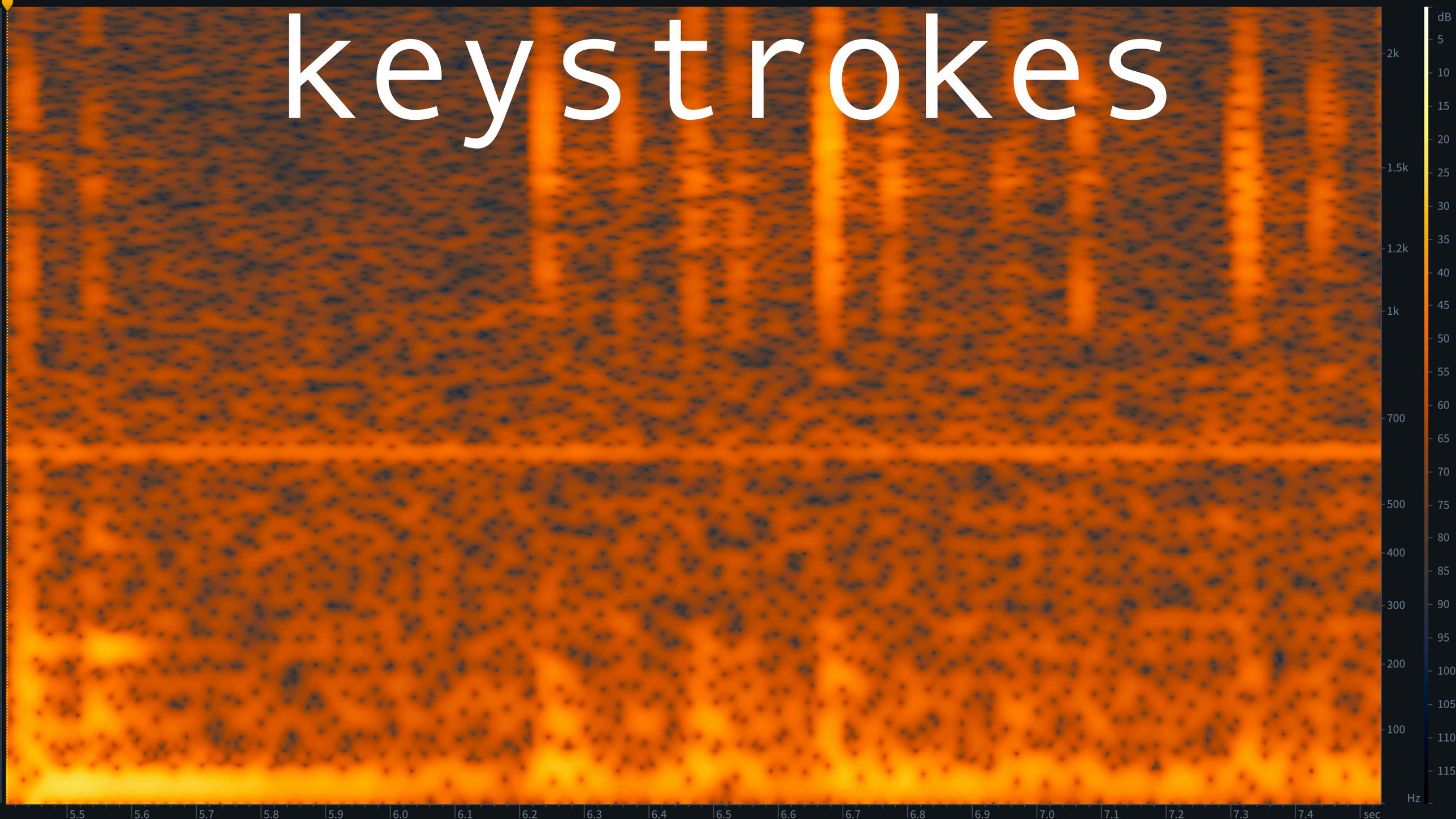
analog rx


split-detector photodiode
transimpedance amplifier (TIA)
split-detector photodiode
transimpedance amplifier (TIA)
differential amplifier
650kHz low-pass filter
450kHz high-pass filter
low noise amplifier (LNA)
500kHz demodulator
amplifier
20kHz low-pass filter
100Hz high-pass filter
amplifier

our rx side


5VDC
SPOT-2D
photodiode
AD8015 TIA
transimpedance amplifier
Ham It Up
RF upconverter
HackRF / SDR / ADC
analog-to-digital converter (ADC)
or software defined radio (SDR)
with >1MHz sample rate
USB
INSIDE the computer
GNU Radio
Izotope RX /
sonic cleanup
keytap3




keystrokes
2k
1.5k
1.2k
1k
700
500
400
300
200
100
Hz
dB
5
10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95
100
105
110
115
5.5
5.6
5.7
5.8
5.9
6.0
6.1
6.2
6.3
6.4
6.5
6.6
6.7
6.8
6.9
7.0
7.1
7.2
7.3
7.4
sec

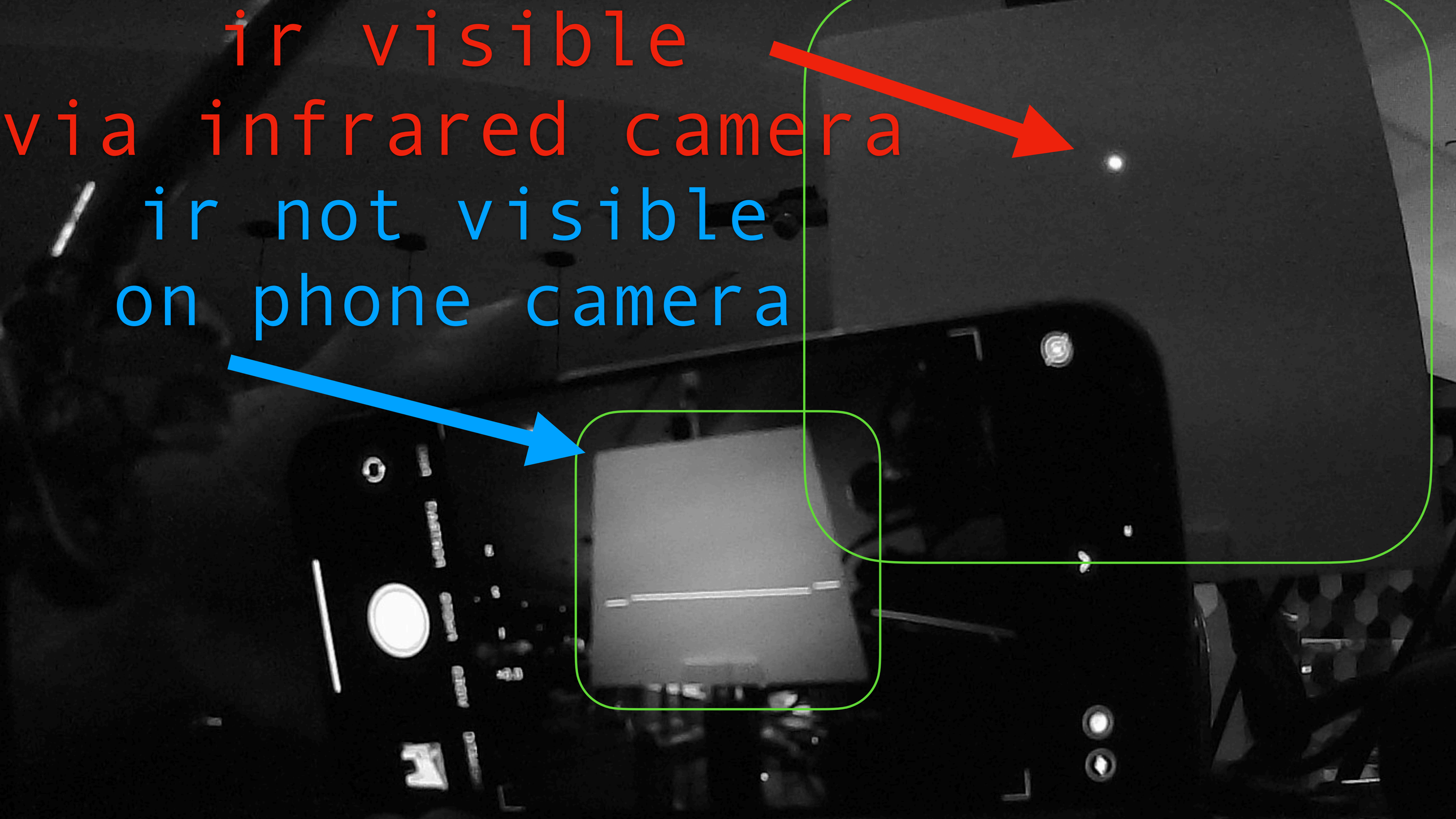
hardware (tx)

- red laser diode: L650P007 (7mW! DANGER!)
- IR laser diode: HL8338MG (50mw! DANGER!)
- Collimating lens: LT230260P-B
- Laser driver (w/bias tee+TEC): LDM56/M
- Current controller: LDC205C
- Signal generator/oscope: Rigol DS2302A-S
- Flexure adapter (optional): LDMXY
- Temp controller (optional): TED200C

hardware (SDR rx)

- UV+Vis+IR camera (for locating+aligning IR laser): XNiteUSB2S-M
- Focusing Lens: LB1471
- Split-cell photodiode: SPOT-2D
- Transimpedance amp (TIA): AD8015 or AMP145
- MF (350-450kHz) band pass filter: ZFBP-400K-S+
- HF upconverter: Ham It Up Plus v2
- SDR: USRP B210
- Software: GNU Radio + iZotope RX + ffmpeg + keytap
- USB battery

tx
infrared

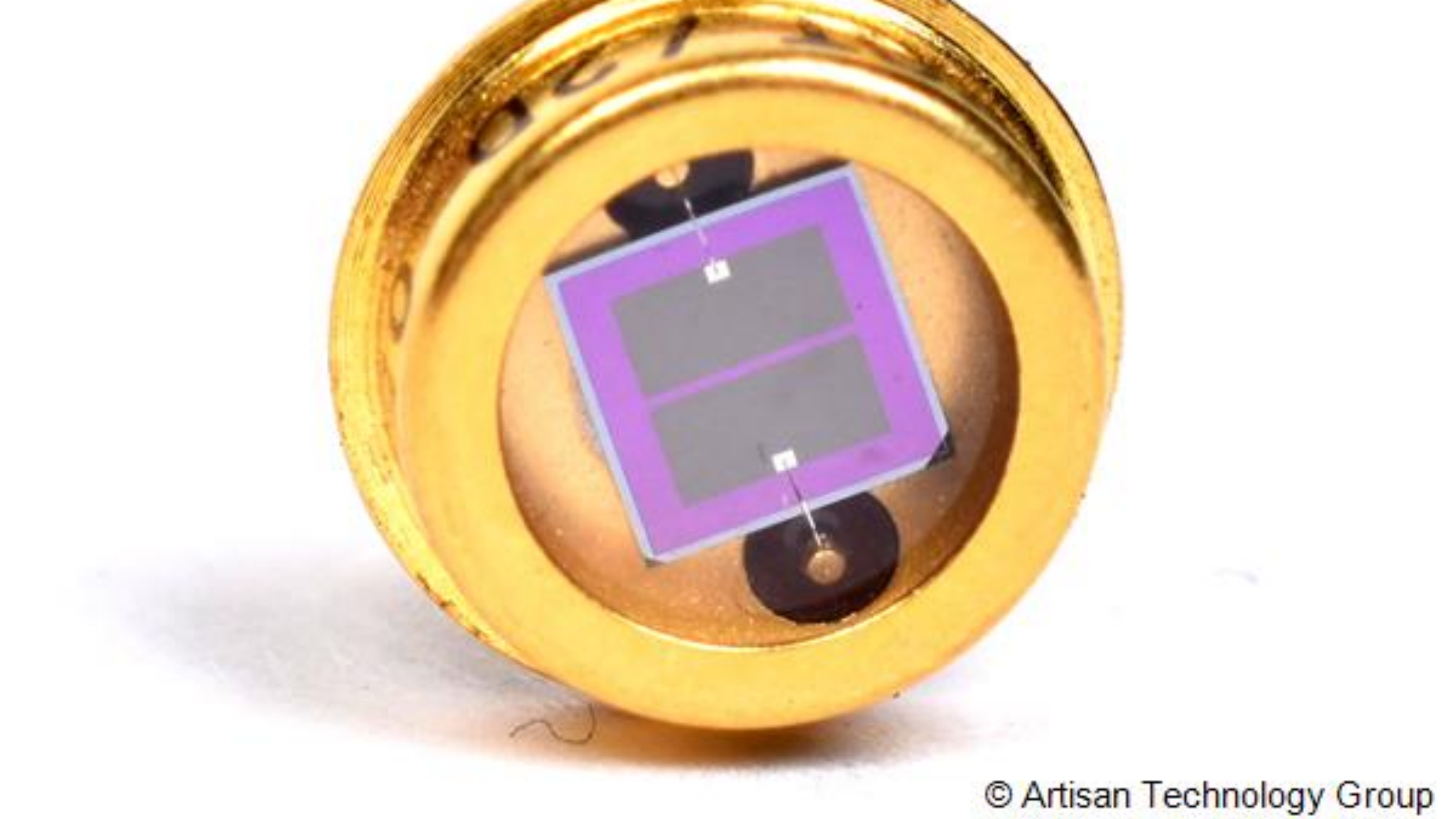

ir visible
via infrared camera
ir not visible
on phone camera



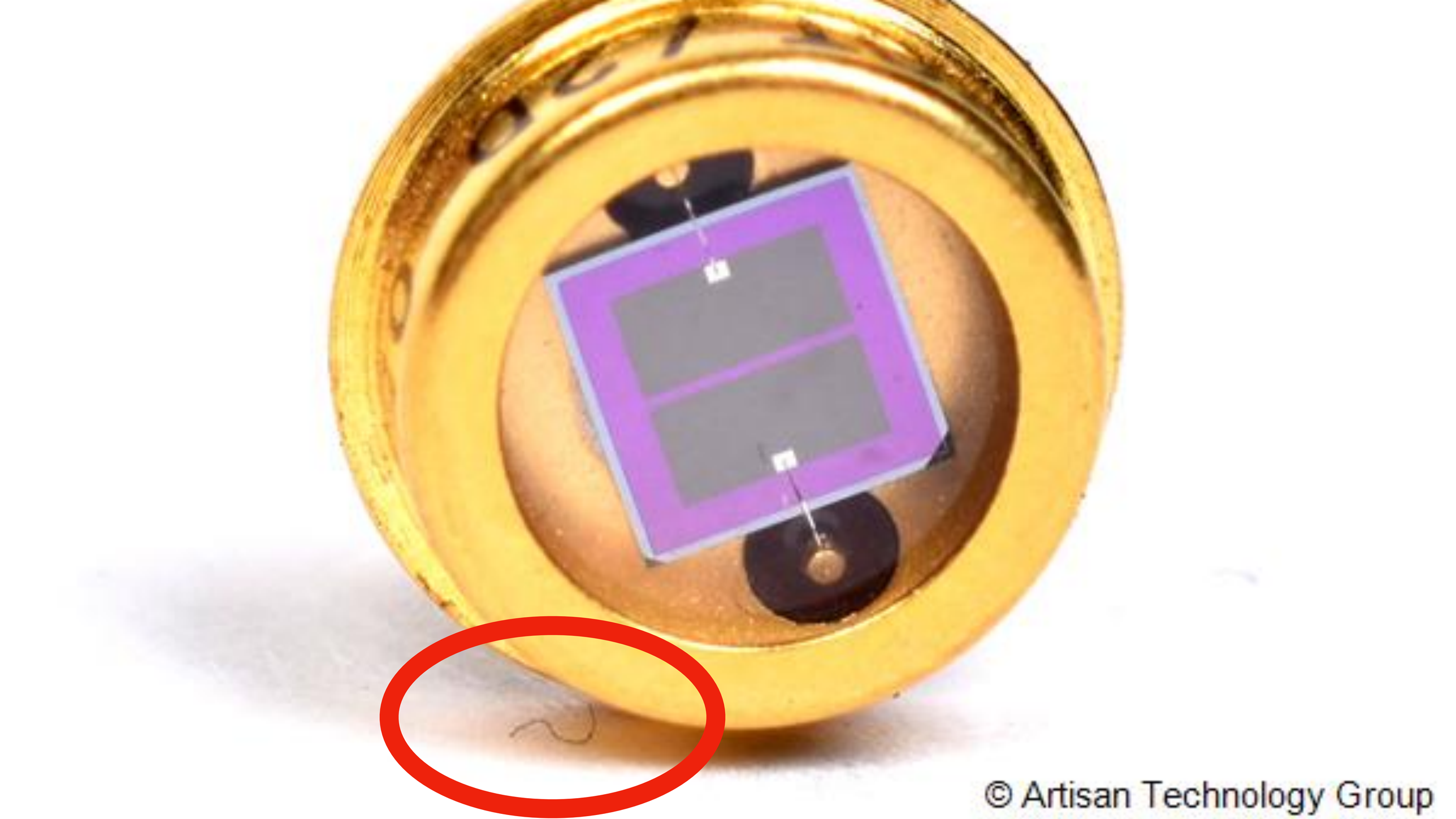


tx RF modulation

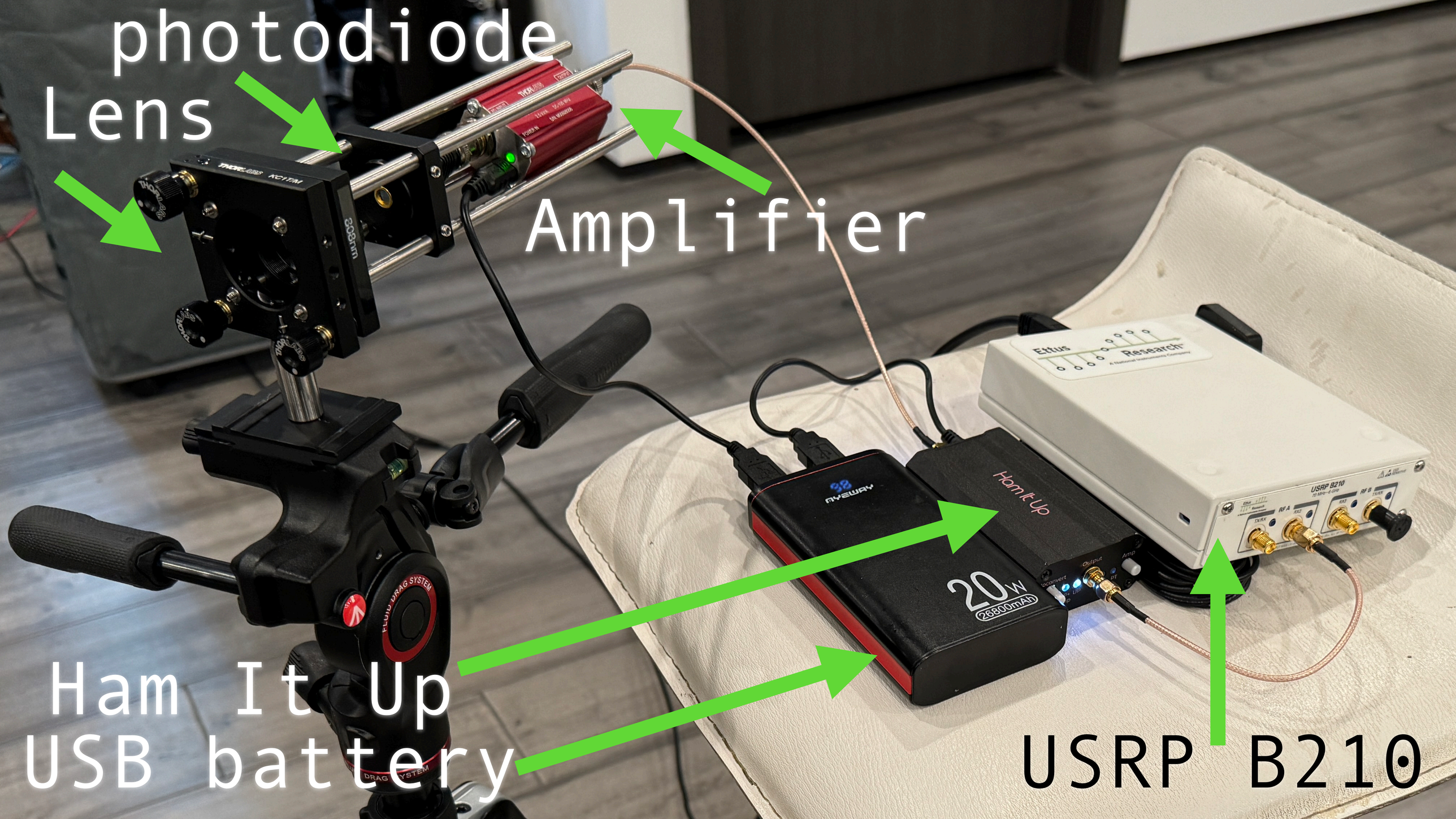
rx split cell photodiode



© Artisan Technology Group

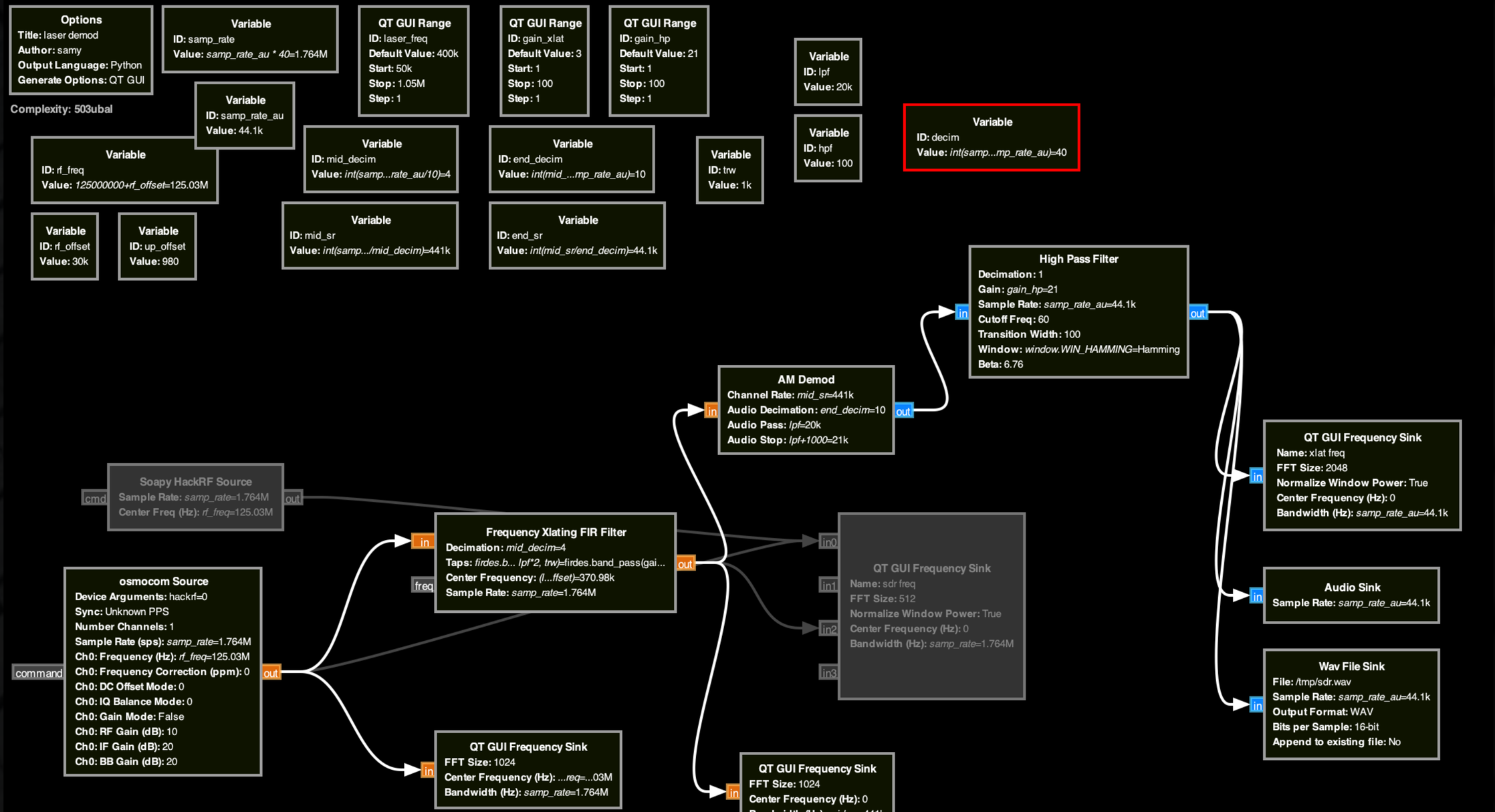


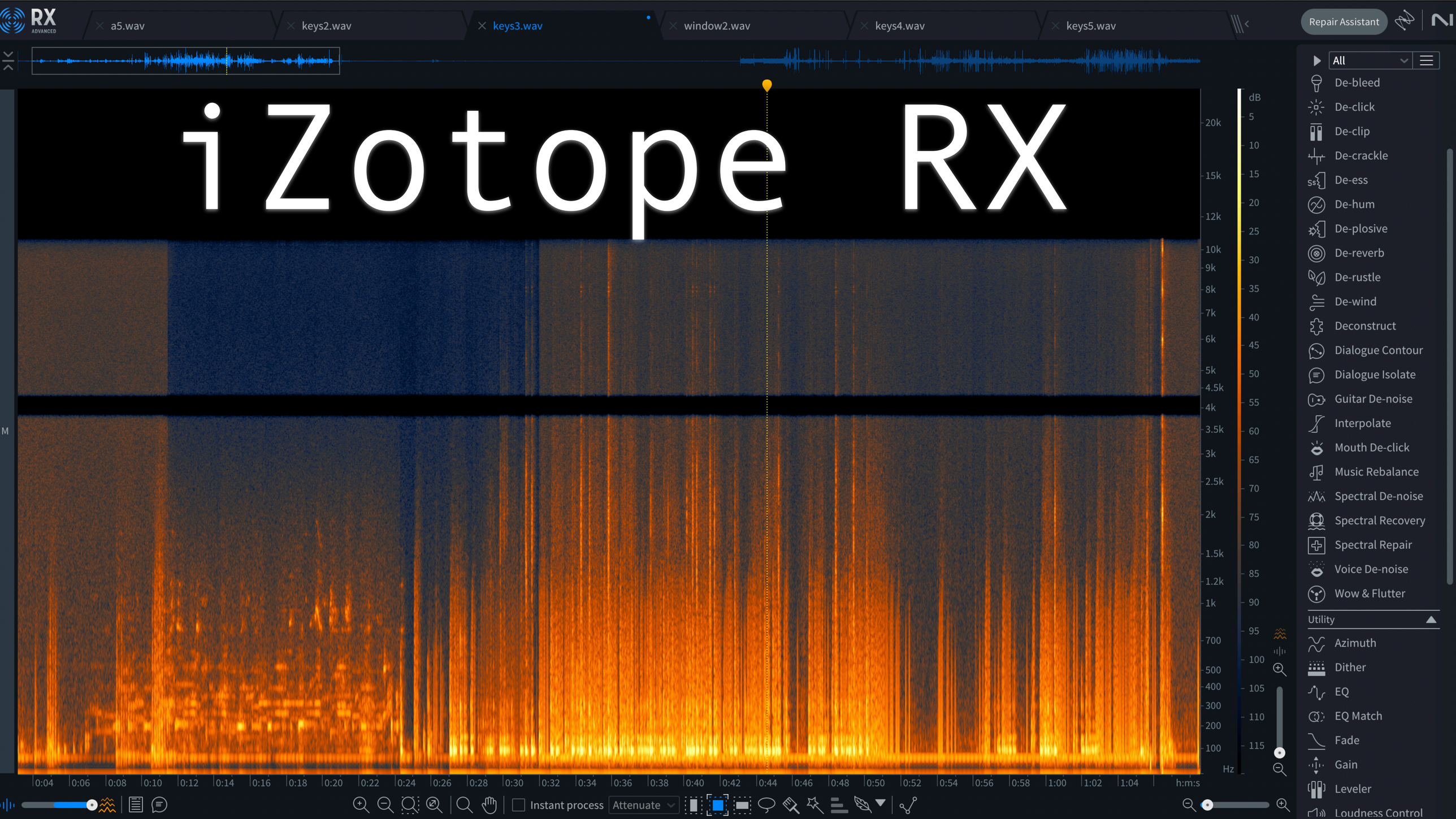
© Artisan Technology Group


photodiode
Lens
Amplifier
Ham It Up
USB battery
USRP B210

software

GNU Radio


Options
Title: laser demod
Author: samy
Output Language: Python
Generate Options: QT GUI
Complexity: 503ubal
Variable
ID: samp_rate
Value: samp_rate_au * 40=1.764M
QT GUI Range
ID: laser_freq
Default Value: 400k
Start: 50k
Stop: 1.05M
Step: 1
QT GUI Range
ID: gain_xlat
Default Value: 3
Start: 1
Stop: 100
Step: 1
QT GUI Range
ID: gain_hp
Default Value: 21
Start: 1
Stop: 100
Step: 1
Variable
ID: lpf
Value: 20k
Variable
ID: hpf
Value: 100
Variable
ID: decim
Value: int(samp...mp_rate_au)=40
Variable
ID: samp_rate_au
Value: 44.1k
Variable
ID: rf_freq
Value: 125000000+rf_offset=125.03M
Variable
ID: mid_decim
Value: int(samp...rate_au/10)=4
Variable
ID: end_decim
Value: int(mid_...mp_rate_au)=10
Variable
ID: trw
Value: 1k
Variable
ID: rf_offset
Value: 30k
Variable
ID: up_offset
Value: 980
Variable
ID: mid_sr
Value: int(samp.../mid_decim)=441k
Variable
ID: end_sr
Value: int(mid_sr/end_decim)=44.1k
High Pass Filter
Decimation: 1
Gain: gain_hp=21
Sample Rate: samp_rate_au=44.1k
Cutoff Freq: 60
Transition Width: 100
Window: window.WIN_HAMMING=Hamming
Beta: 6.76
in
out
AM Demod
Channel Rate: mid_sr=441k
Audio Decimation: end_decim=10
Audio Pass: lpf=20k
Audio Stop: lpf+1000=21k
QT GUI Frequency Sink
Name: xlat freq
FFT Size: 2048
Normalize Window Power: True
Center Frequency (Hz): 0
Bandwidth (Hz): samp_rate_au=44.1k
Soapy HackRF Source
Sample Rate: samp_rate=1.764M
Center Freq (Hz): rf_freq=125.03M
cmd
out
Frequency Xlating FIR Filter
Decimation: mid_decim=4
Taps: firdes.b... lpf*2, trw)=firdes.band_pass(gai...
Center Frequency: (l...ffset)=370.98k
Sample Rate: samp_rate=1.764M
in
freq
out
QT GUI Frequency Sink
Name: sdr freq
FFT Size: 512
Normalize Window Power: True
Center Frequency (Hz): 0
Bandwidth (Hz): samp_rate=1.764M
in0
in1
in2
in3
Audio Sink
Sample Rate: samp_rate_au=44.1k
Wav File Sink
File: /tmp/sdr.wav
Sample Rate: samp_rate_au=44.1k
Output Format: WAV
Bits per Sample: 16-bit
Append to existing file: No
osmocom Source
Device Arguments: hackrf=0
Sync: Unknown PPS
Number Channels: 1
Sample Rate (sps): samp_rate=1.764M
Ch0: Frequency (Hz): rf_freq=125.03M
Ch0: Frequency Correction (ppm): 0
Ch0: DC Offset Mode: 0
Ch0: IQ Balance Mode: 0
Ch0: Gain Mode: False
Ch0: RF Gain (dB): 10
Ch0: IF Gain (dB): 20
Ch0: BB Gain (dB): 20
command
out
QT GUI Frequency Sink
FFT Size: 1024
Center Frequency (Hz): ...req=...03M
Bandwidth (Hz): samp_rate=1.764M
QT GUI Frequency Sink
FFT Size: 1024
Center Frequency (Hz): 0


RX ADVANCED
a5.wav
keys2.wav
keys3.wav
window2.wav
keys4.wav
keys5.wav
Repair Assistant
iZotope RX
All
De-bleed
De-click
De-clip
De-crackle
De-ess
De-hum
De-plosive
De-reverb
De-rustle
De-wind
Deconstruct
Dialogue Contour
Dialogue Isolate
Guitar De-noise
Interpolate
Mouth De-click
Music Rebalance
Spectral De-noise
Spectral Recovery
Spectral Repair
Voice De-noise
Wow & Flutter
Utility
Azimuth
Dither
EQ
EQ Match
Fade
Gain
Leveler
Loudness Control
dB
Hz
h:m:s
Instant process
Attenuate

ffmpeg

NAME

ffmpeg - ffmpeg video converter

SYNOPSIS

ffmpeg [global_options] {[input_file_options] -i input_url} ... {[output_file_options] output_url} ...

DESCRIPTION

ffmpeg is a very fast video and audio converter that can also grab from a live audio/video source. It can also convert between arbitrary sample rates and resize video on the fly with a high quality polyphase filter.

ffmpeg reads from an arbitrary number of input "files" (which can be regular files, pipes, network streams, grabbing devices, etc.), specified by the "-i" option, and writes to an arbitrary number of output "files", which are specified by a plain output url. Anything found on the command line which cannot be interpreted as an option is considered to be an output url.

Each input or output url can, in principle, contain any number of streams of different types (video/audio/subtitle/attachment/data). The allowed number and/or types of streams may be limited by the container format. Selecting which streams from which inputs will go into which output is either done automatically or with the "-map" option (see the Stream selection chapter).

To refer to input files in options, you must use their indices (0-based). E.g. the first input file is 0, the second is 1, etc. Similarly, streams within a file are referred to by their indices. E.g. "2:3" refers to the fourth stream in the third input file. Also see the Stream specifiers chapter.

As a general rule, options are applied to the next specified file. Therefore, order is important, and you can have the same option on the command line multiple times. Each occurrence is then applied to the next input or output file. Exceptions from this rule are the global options (e.g. verbosity level), which should be specified first.

Do not mix input and output files -- first specify all input files, then all output files. Also do not mix options which belong to different files. All options apply ONLY to the next input or output file and are reset between files.



Georgi Gerganov
ggerganov

Unfollow | Sponsor

I like big .vimrc and I cannot lie

github.com/ggerganov/kbd-audio

kbd-audio Public

Acoustic keyboard eavesdropping

C++ 8.4k 583

keytap3



Georgi Gerganov

ggerganov

Unfollow | Sponsor

I like big .vimrc and I cannot lie

github.com/ggerganov/kbd-audio

kbd-audio Public

Acoustic keyboard eavesdropping

C++ 8.4k 583

keytap3


CAST: CASEY
ARMSTRONG + TOSHI











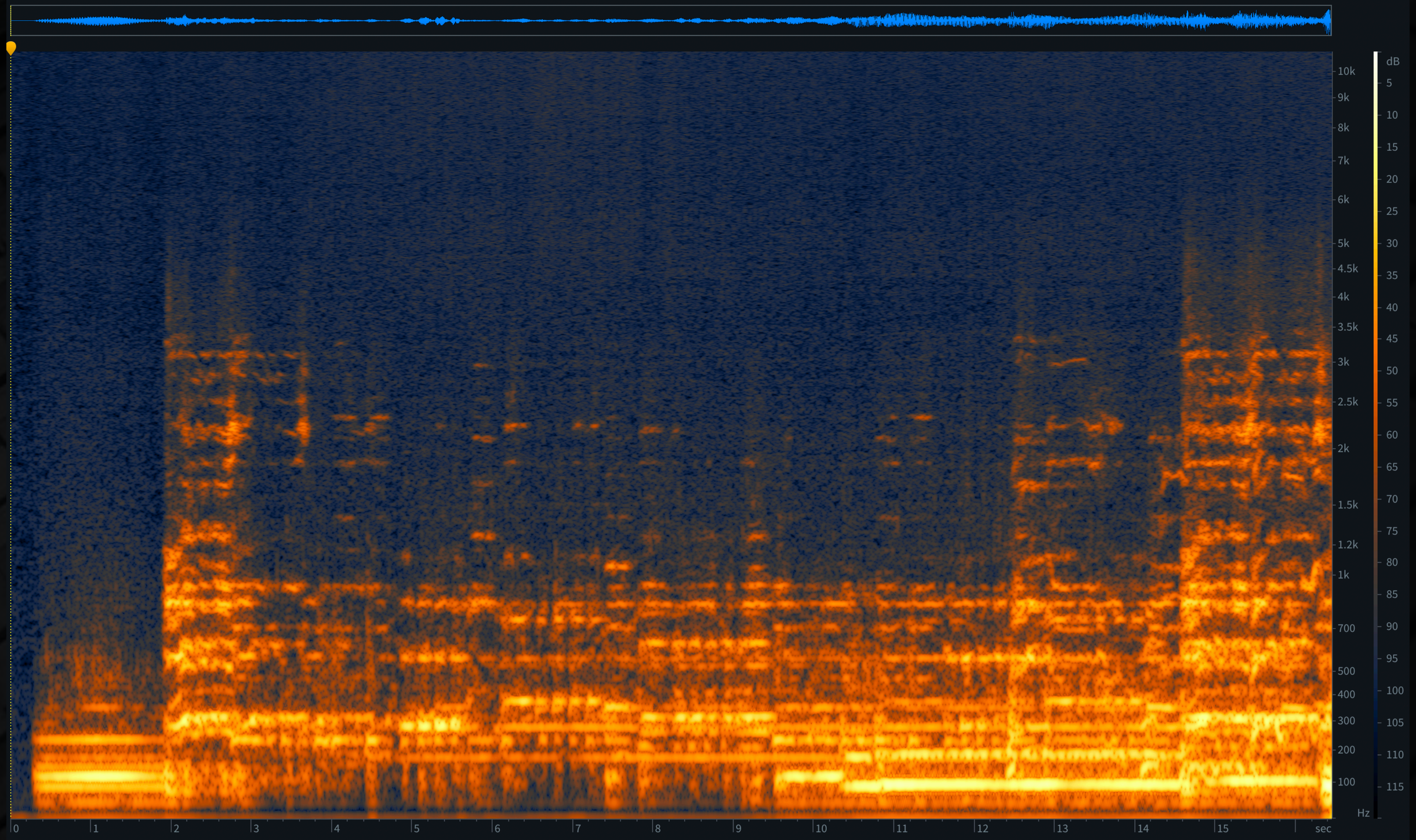
```
➜  keytap git:(master)
```

typed:

hello and welcome to the laser microphone test where we are now converting light to sounds well actually signal as we never technically hear the signal as sound since it does not get directly recorded or played back

keytap3:

hhello and welcome to thheplaser microohone test where we are now converting lightto sounds awelll acitualllysignasl aos we netheir techniciallytreast the sigaal as sound isince int ddoes not get aged intly recolrded or llayedf


10k
9k
8k
7k
6k
5k
4.5k
4k
3.5k
3k
2.5k
2k
1.5k
1.2k
1k
700
500
400
300
200
100
Hz
dB
5
10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95
100
105
110
115
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
sec

challenges

improvements

latest @ samy.pl/dc32

Optical Espionage

thank you!

@samykamkar
samy.pl