Infrared: Old Threat Meets New Devices

Authors

- Wang Kang, Alibaba Group

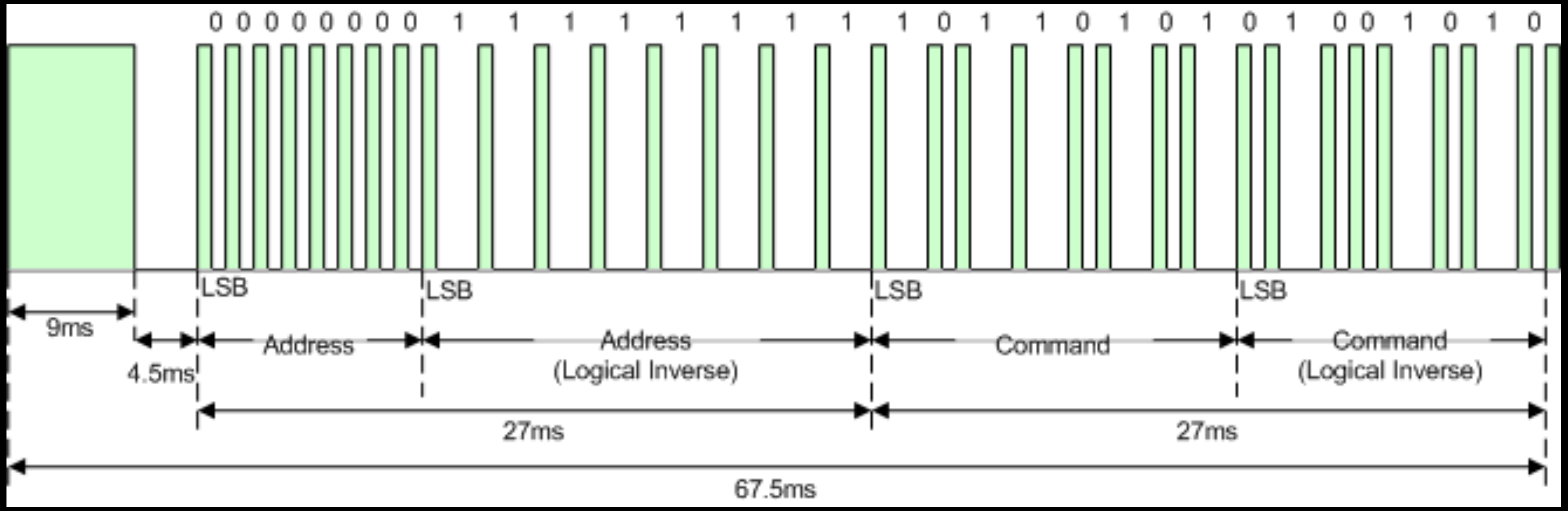
  Wang Kang is a security expert of Alibaba Group, focusing on security issues of IoT, cyber-physical system, V2X, and trusted computing. He was a speaker at Black Hat {EU15, USA17/18, ASIA19}. He is a contributor of Linux Kernel, as well as a founder of the Tsinghua University Network Administrators.

- Yang Bo, CAICT

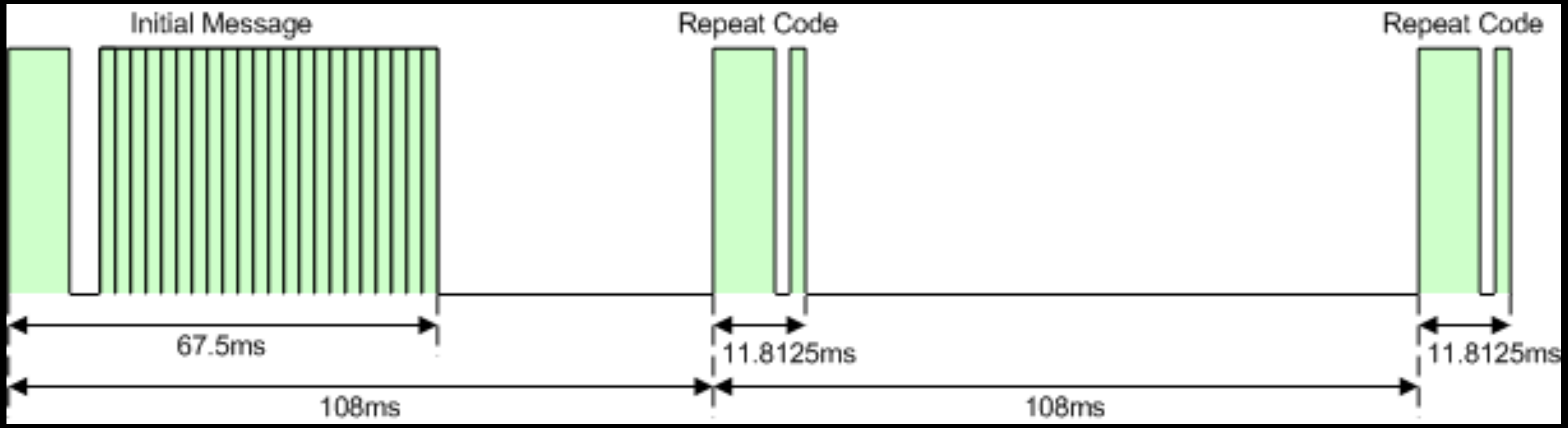
  Yang Bo is a telecommunication specialist in the China Telecommunication Technology Labs in CAICT. He has also been worked on ultrasonic transducers and measurements for several years. His main research interests include sensors/transducers, wireless communication, and related measurement technologies. He was a speaker of Black Hat USA 2017.

Introduction & Outline

- Devices still using IR as control interface
  - Air conditioner / TV / Camera / Speaker / DVD / TV Box / Projector
- Devices that are transmitting IR nowadays
  - Remote controllers are not the only devices that are able to transmit IR signals
  - IR filling light for night-vision purposes on cameras, clock-in machines, ...
- CMOS - Slow motion camera
  - Or we can simply see it with a cellphone
  - Slow motion camera
- High Power IR transmitter as remote controller
  - If the IR transmitting power is powerful enough...
  - How underground industry may make use of this...



- NEC standard.
- “Duty cycle modulation” 25% vs 50%



The NEC IR transmission protocol uses pulse distance encoding of the message bits. Each pulse burst (mark – RC transmitter ON) is 562.5μs in length, at a carrier frequency of 38kHz (26.3μs). Logical bits are transmitted as follows:

- Logical '0' – a 562.5μs pulse burst followed by a 562.5μs space, with a total transmit time of 1.125ms
- Logical '1' – a 562.5μs pulse burst followed by a 1.6875ms space, with a total transmit time of 2.25ms

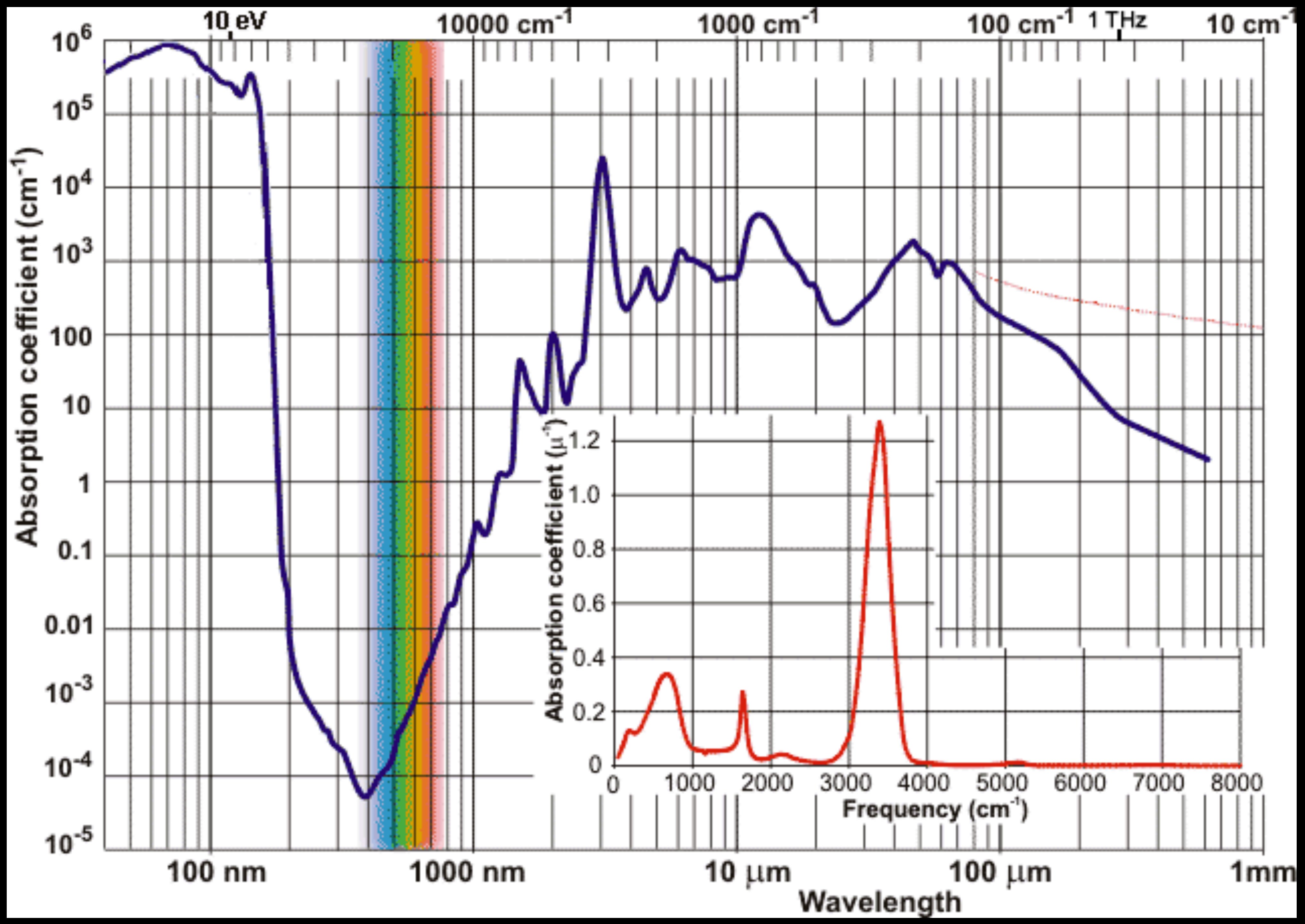
When a key is pressed on the remote controller, the message transmitted consists of the following, in order:

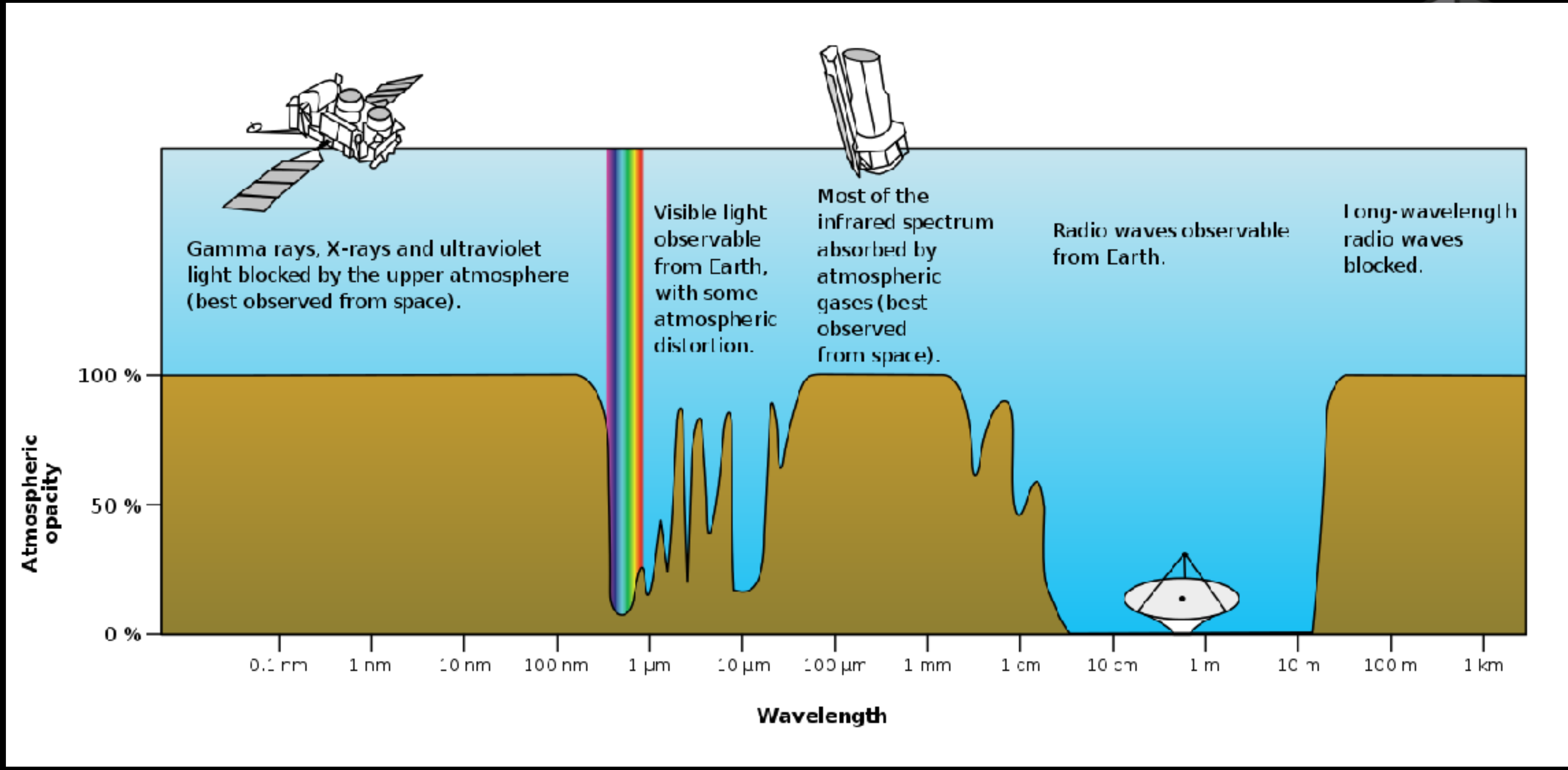
- a 9ms leading pulse burst (16 times the pulse burst length used for a logical data bit)
- a 4.5ms space
- the 8-bit address for the receiving device
- the 8-bit logical inverse of the address
- the 8-bit command
- the 8-bit logical inverse of the command
- a final 562.5μs pulse burst to signify the end of message transmission.

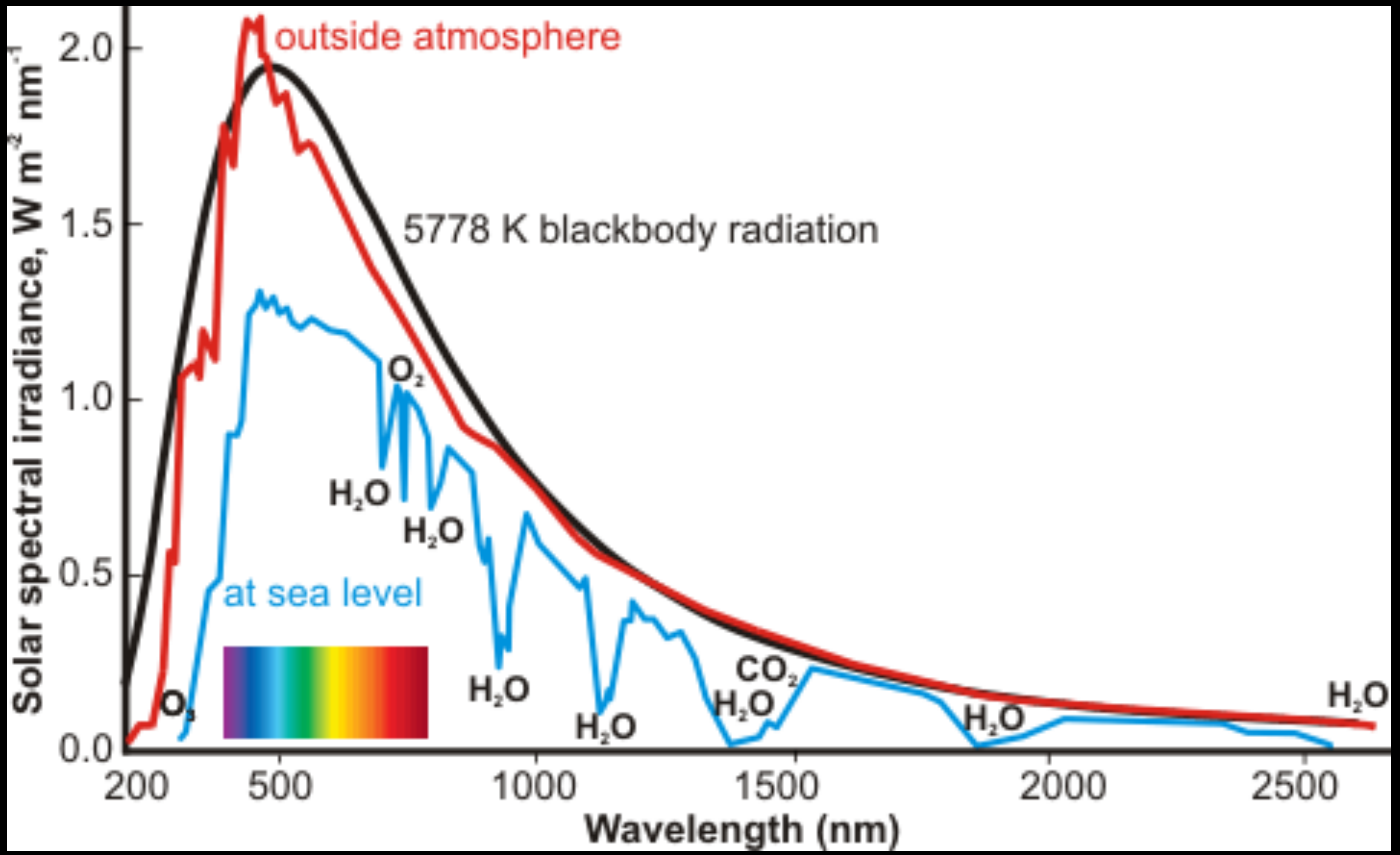
The four bytes of data bits are each sent least significant bit first. Figure 1 illustrates the format of an NEC IR transmission frame, for an address of 00h (00000000b) and a command of ADh (10101101b).

https://techdocs.altium.com/display/FPGA/NEC+Infrared+Transmission+Protocol

“Tell me something I don’t know.”







Why 940nm -- spectrum of solar light

Why 38kHz -- high pass filter to avoid interference

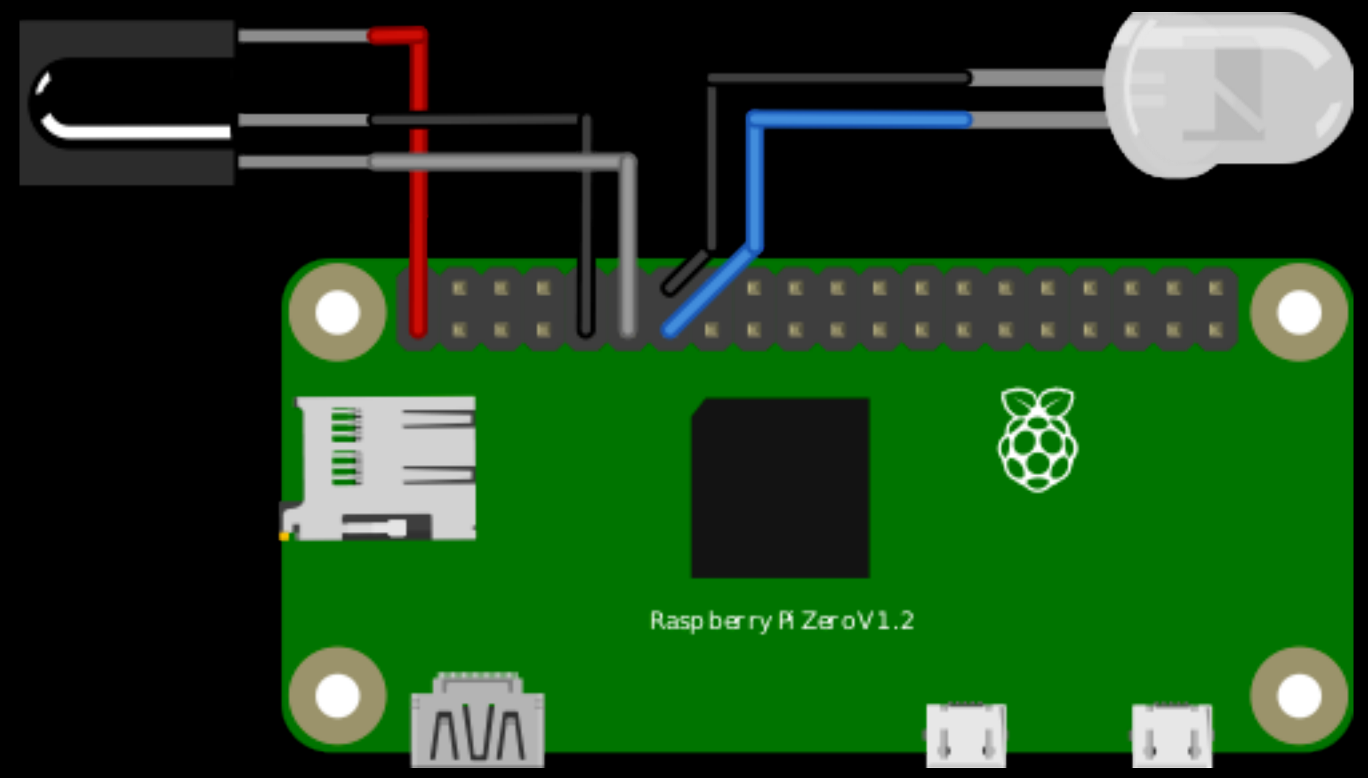
http://www1.lsbu.ac.uk/water/water_vibrational_spectrum.html

How can we get the code?

- Existing Libraries
  - LIRC
  - http://irdb.tk/find/ | http://irdb.tk/codes/
- Self designed gadgets
- Cell phones

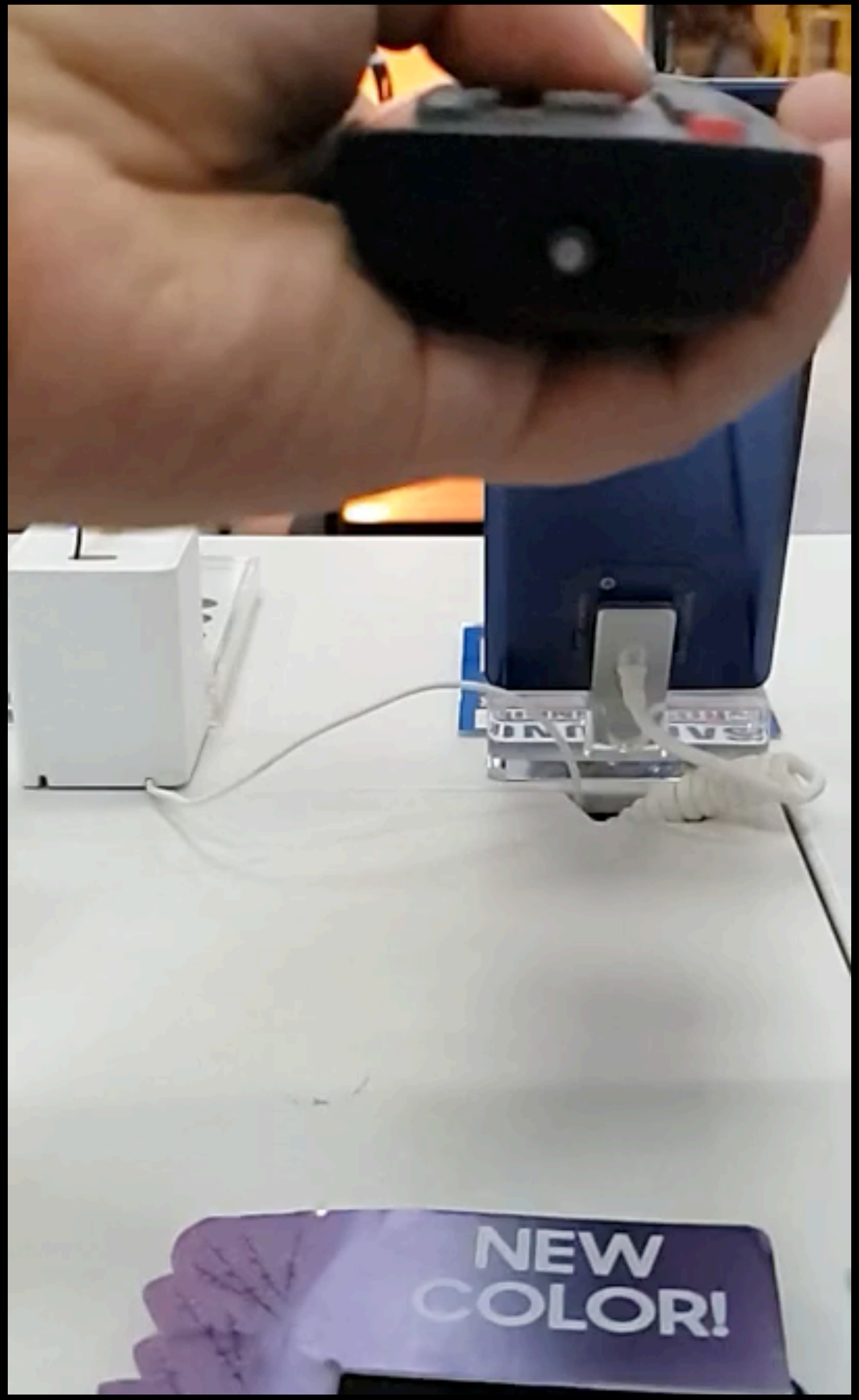
LIRC example

- http://lirc.sourceforge.net/remotes/sharp/GA339WJSA
  - **KEY_POWER 0x41A2**
- TSOP Series - Photo Modules for PCM Remote Control Systems
  - TSOP1738： 38KHz
  - TSOP1736： 36KHz
  - TSOP1730： 30KHz
- 100 0001 1010 0010 x : 41A2 <— — Bingo!



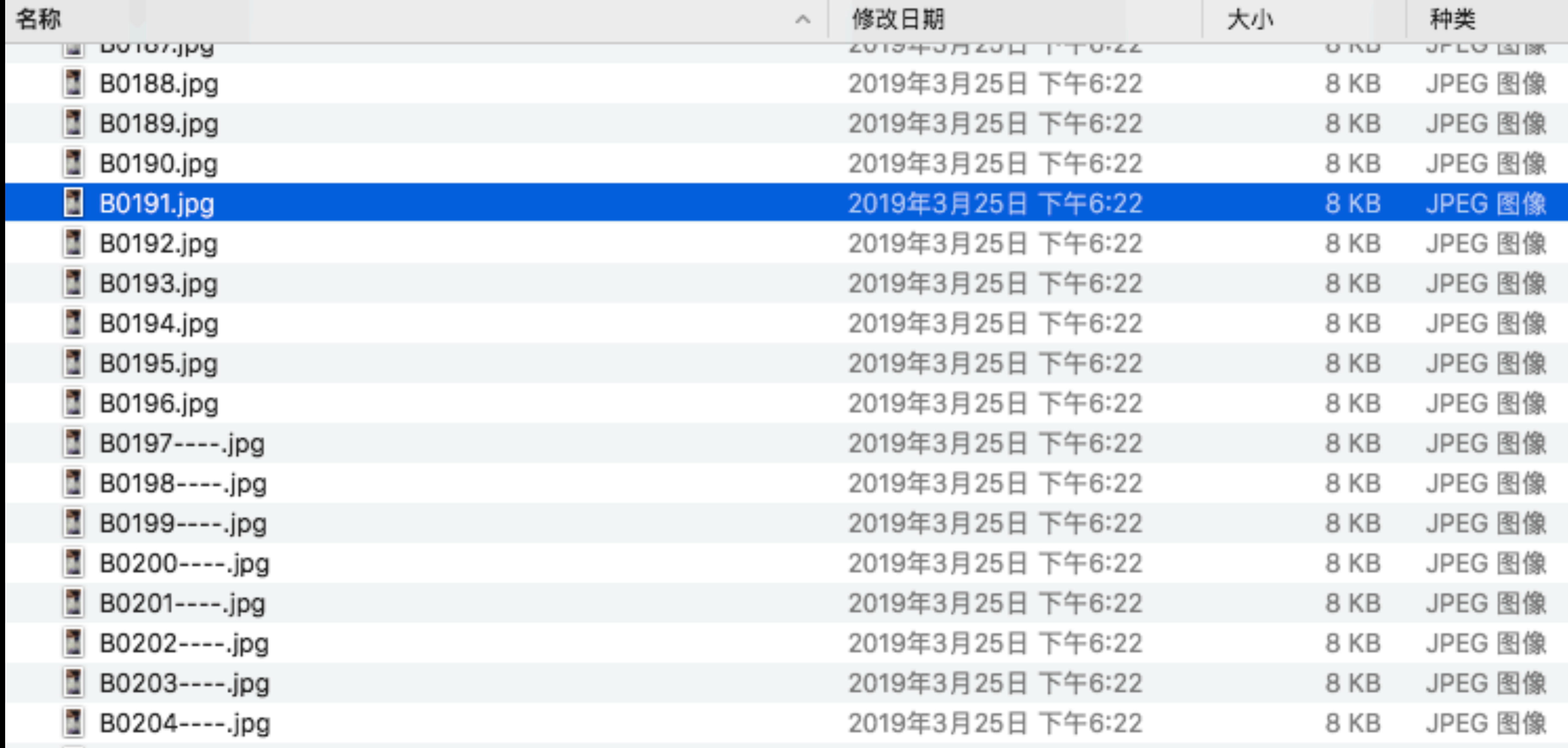
```
# mode2 -d /dev/lirc0

Using driver default on device /dev/lirc0
Trying device: /dev/lirc0
Using device: /dev/lirc0
...

space 366
pulse 1738
space 369
pulse 685
space 371
pulse 683
space 369
pulse 685
space 344
```

Chapter 1
Slow mo



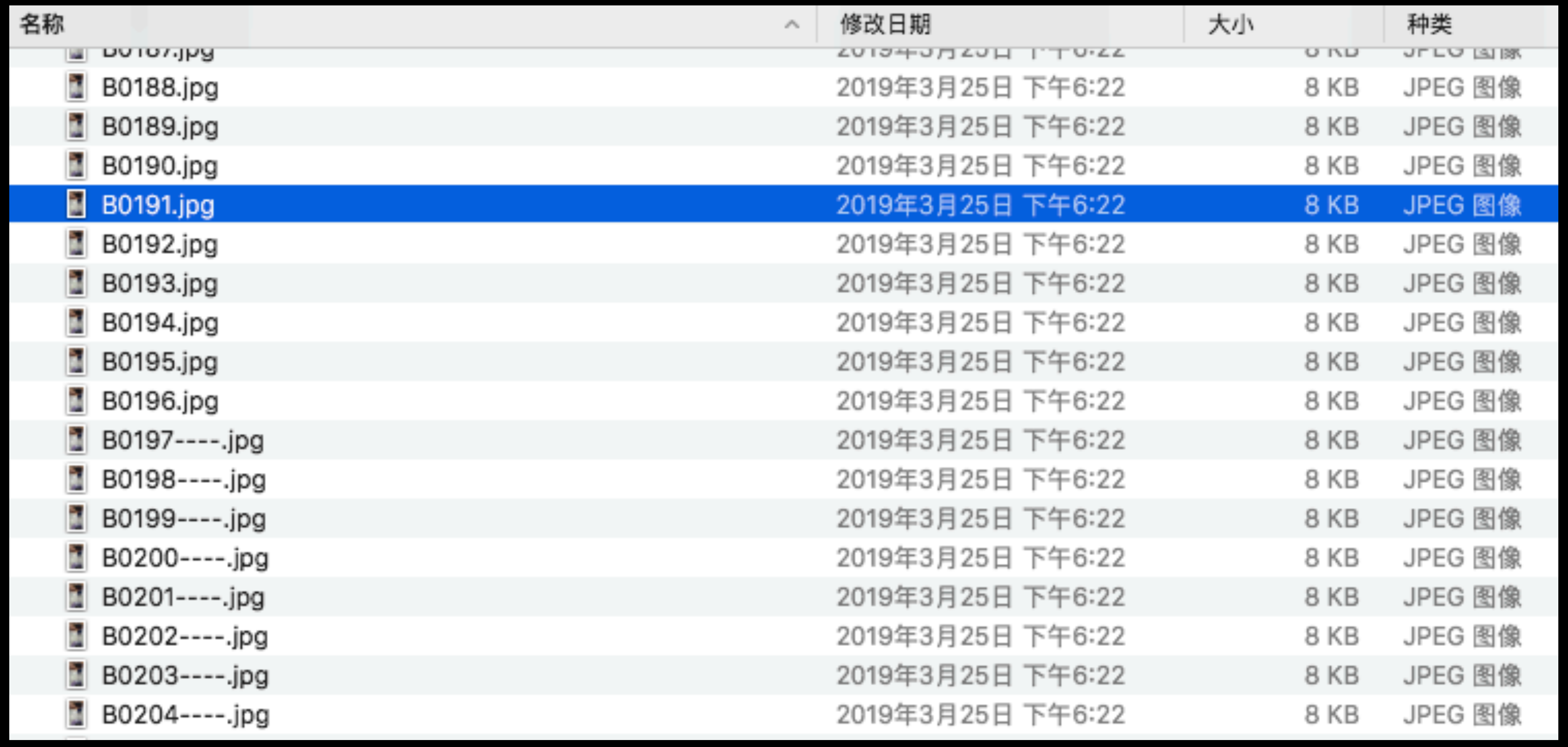
Record: 960 FPS

Playback: 30 FPS



名称	修改日期	大小	种类
B0188.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0189.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0190.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0191.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0192.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0193.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0194.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0195.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0196.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0197----.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0198----.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0199----.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0200----.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0201----.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0202----.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0203----.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0204----.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像

B0300.jpg
B0301----.jpg
B0302----.jpg
B0303----.jpg
B0304----.jpg
B0305----.jpg
B0306----.jpg
B0307----.jpg
B0308----.jpg
B0309----.jpg
B0310.jpg
B0311.jpg
B0312----.jpg



名称	修改日期	大小	种类
B0187.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0188.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0189.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0190.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0191.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0192.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0193.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0194.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0195.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0196.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0197----.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0198----.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0199----.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0200----.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0201----.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0202----.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0203----.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像
B0204----.jpg	2019年3月25日 下午6:22	8 KB	JPEG 图像

312.jpg

309.jpg

301.jpg

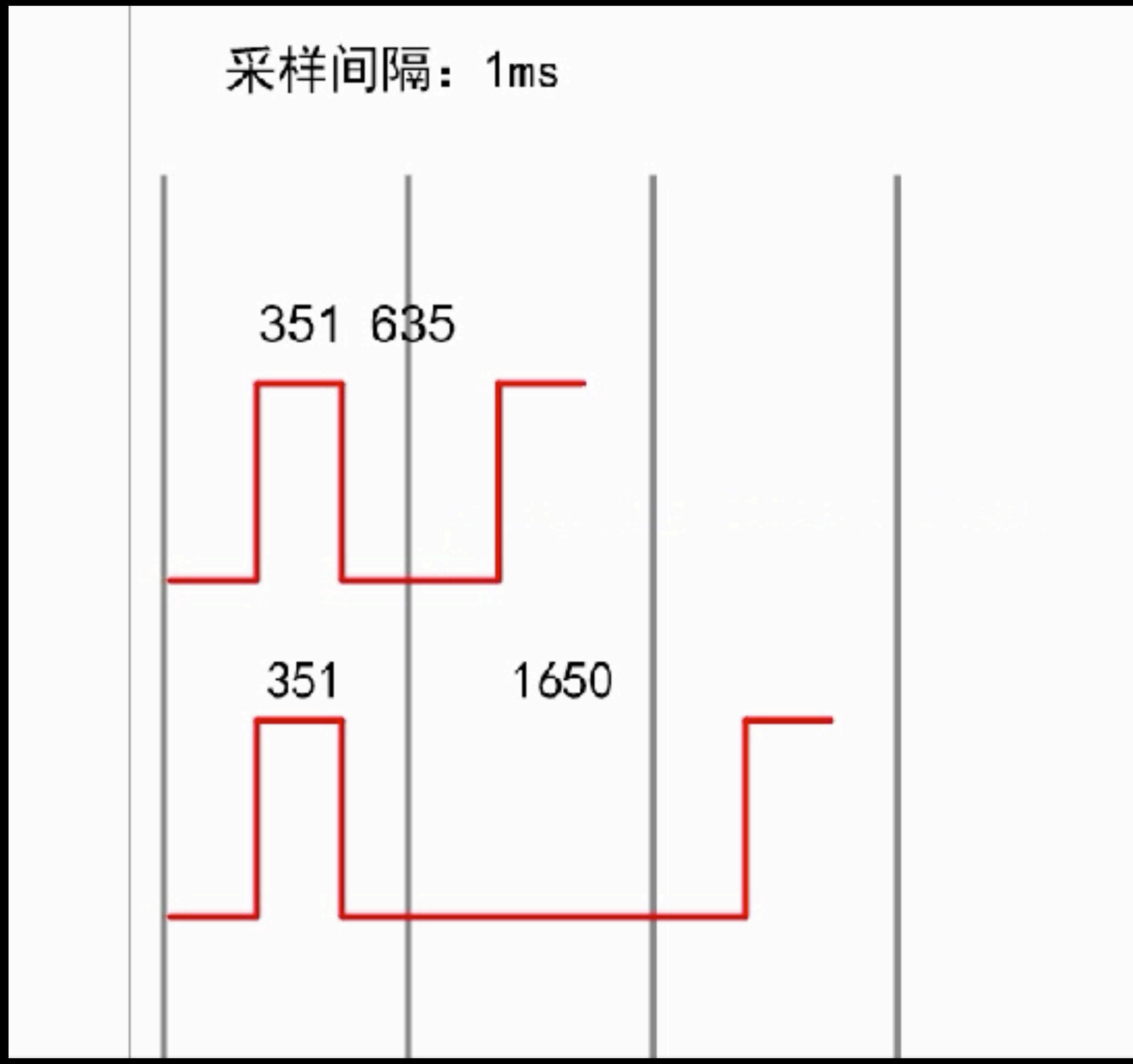
197.jpg

(301-197) / 960 FPS = 108.33 ms 108 ms (from spec.)

(312-301) / 960 FPS = 11.45 ms 11.8125 ms (from spec.)

Another not-so-lucky example

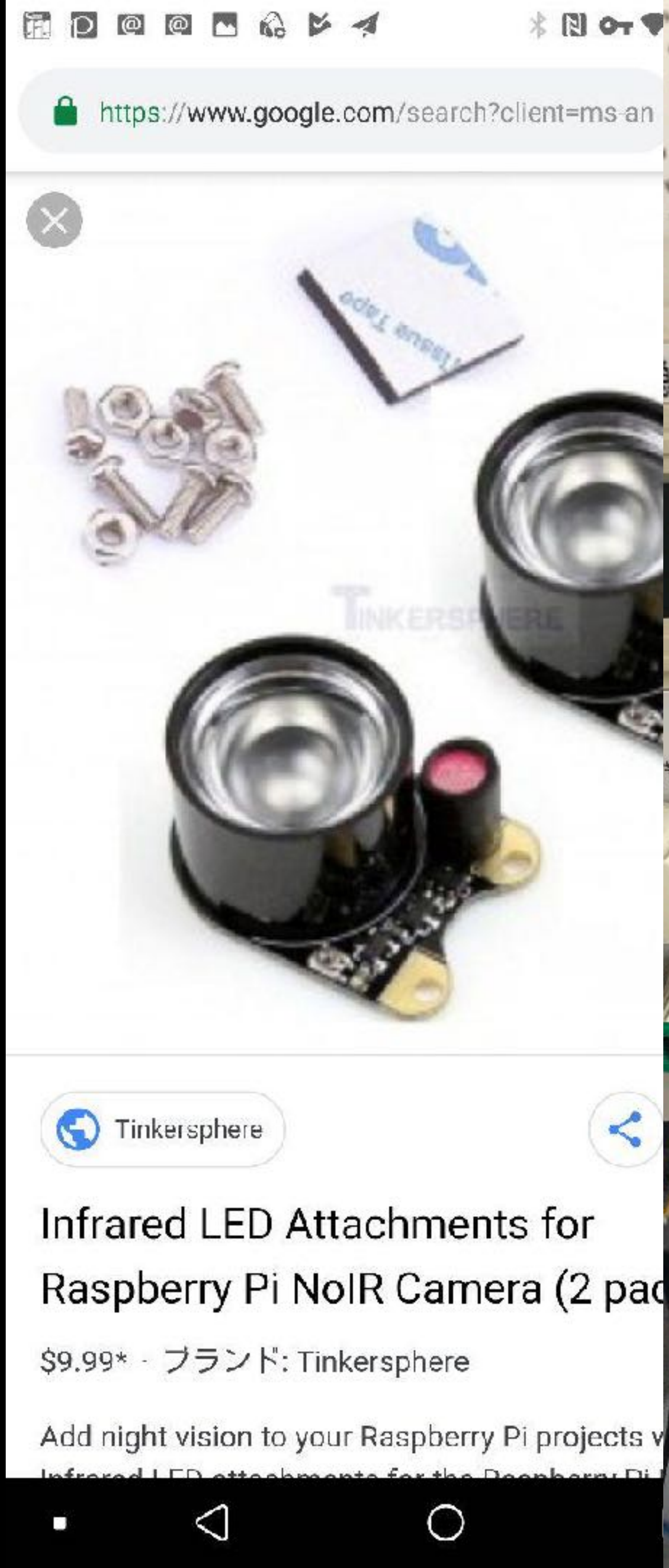
- “one” 351μs (space) 1650μs (pulse)
- “zero” 351μs (space) 635μs (pulse)
- Undersampled Signal Recovery
  - Video edge trigger
  - Multiple-pass samples
  - Silva A J. Reconstruction of undersampled periodic signals[J]. 1986.MLA



Animation courtesy cyxu

Chapter 2
IR Filling Light

MENU
0
未检测到人脸
F1
F2
F3
F4
F5
F6



https://www.google.com/search?client=ms-an

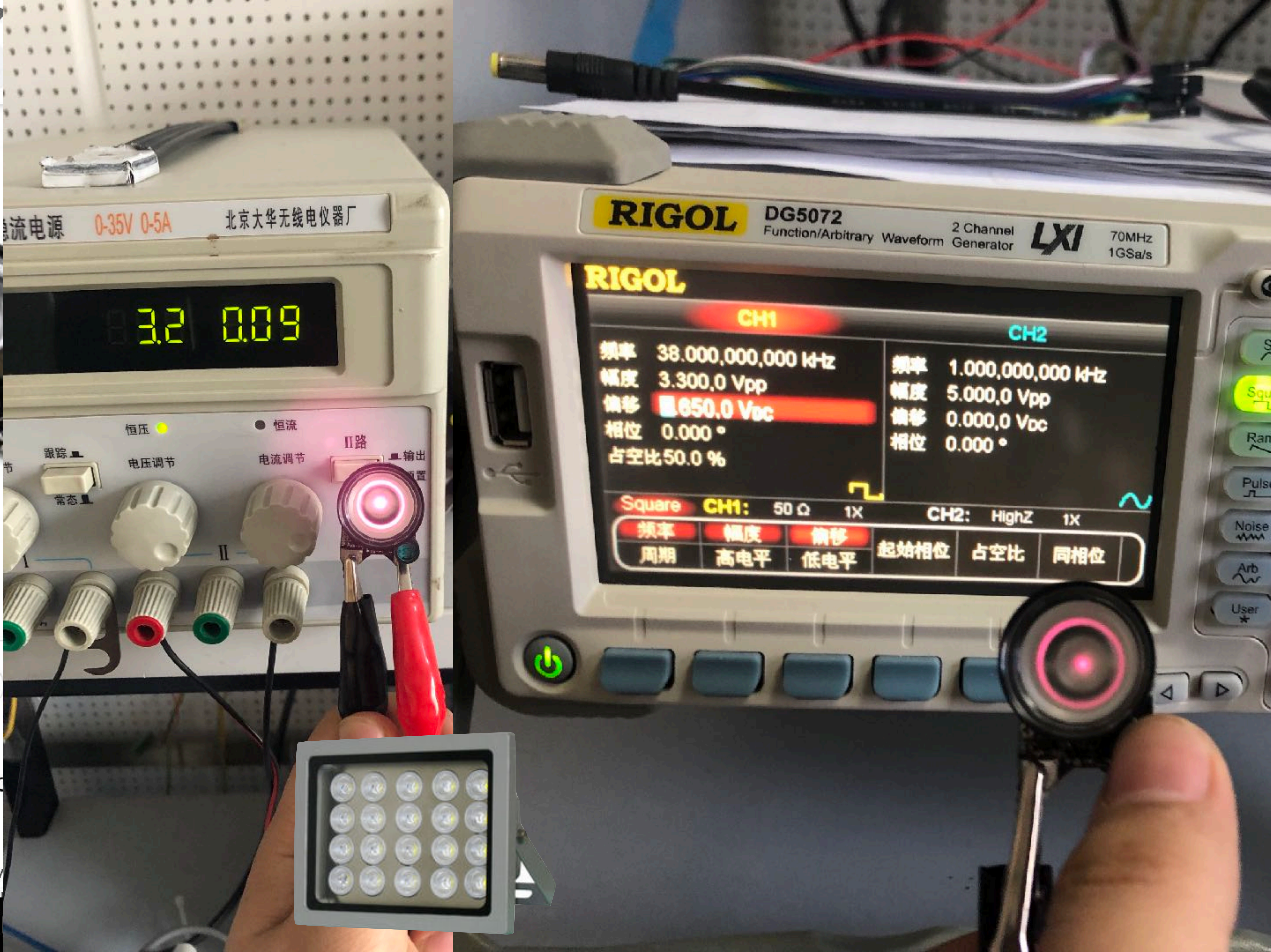
Tinkersphere

Infrared LED Attachments for Raspberry Pi NoIR Camera (2 pac

$9.99* · ブランド: Tinkersphere

Add night vision to your Raspberry Pi projects w

Infrared LED attachments for the Raspberry Pi



RIGOL

CH1
频率 38.000,000,000 kHz
幅度 3.300,0 Vpp
偏移 1.650,0 Vdc
相位 0.000 °
占空比 50.0 %

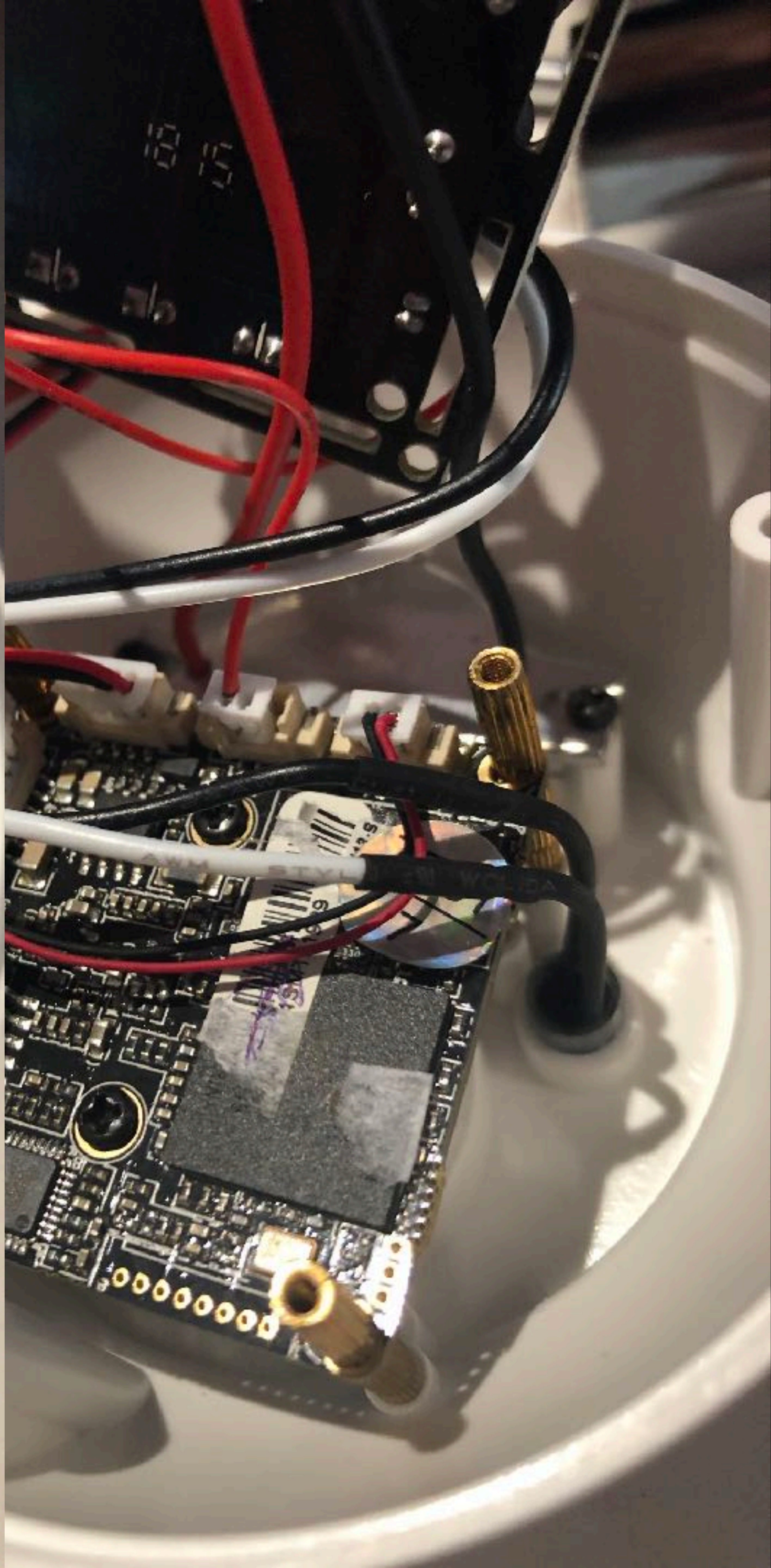
CH2
频率 1.000,000,000 kHz
幅度 5.000,0 Vpp
偏移 0.000,0 Vdc
相位 0.000 °

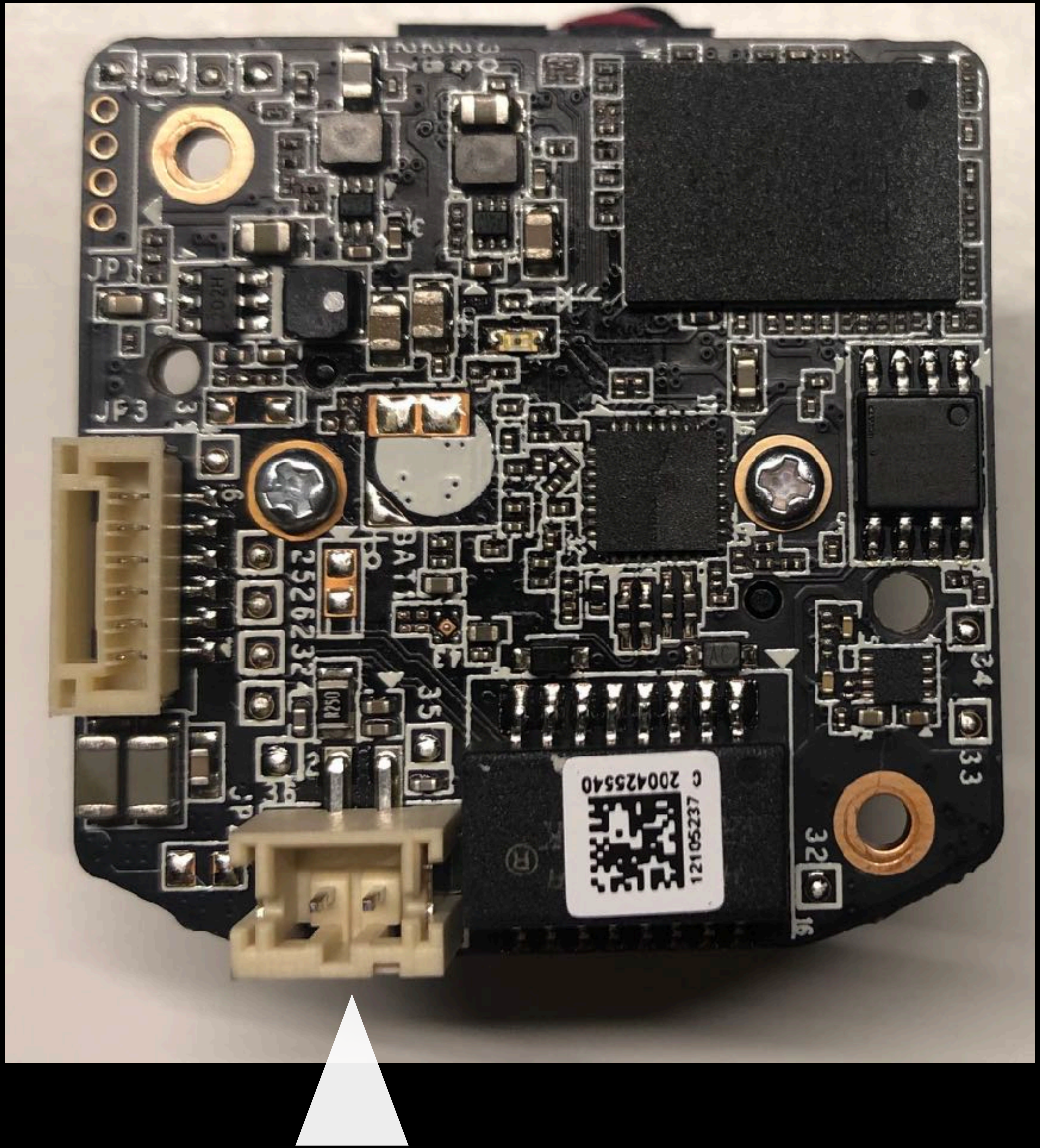
Square CH1: 50 Ω 1X CH2: HighZ 1X

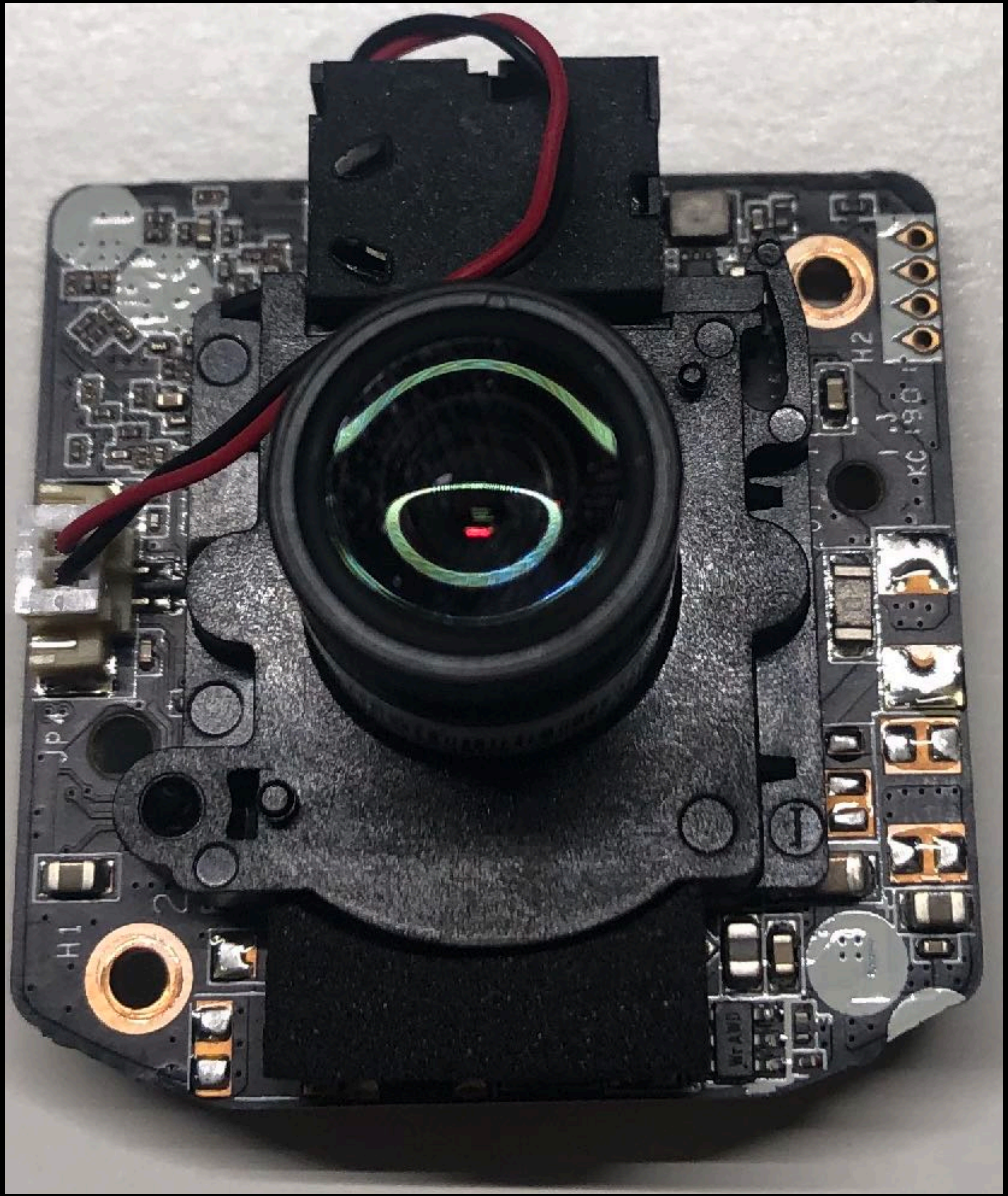
频率 幅度 偏移 起始相位 占空比 同相位
周期 高电平 低电平

(Pictures taken in Amsterdam)

C6
LED+
LED-




JP1
JP3
BAT
C 200425540
12105237
32
33
34
35

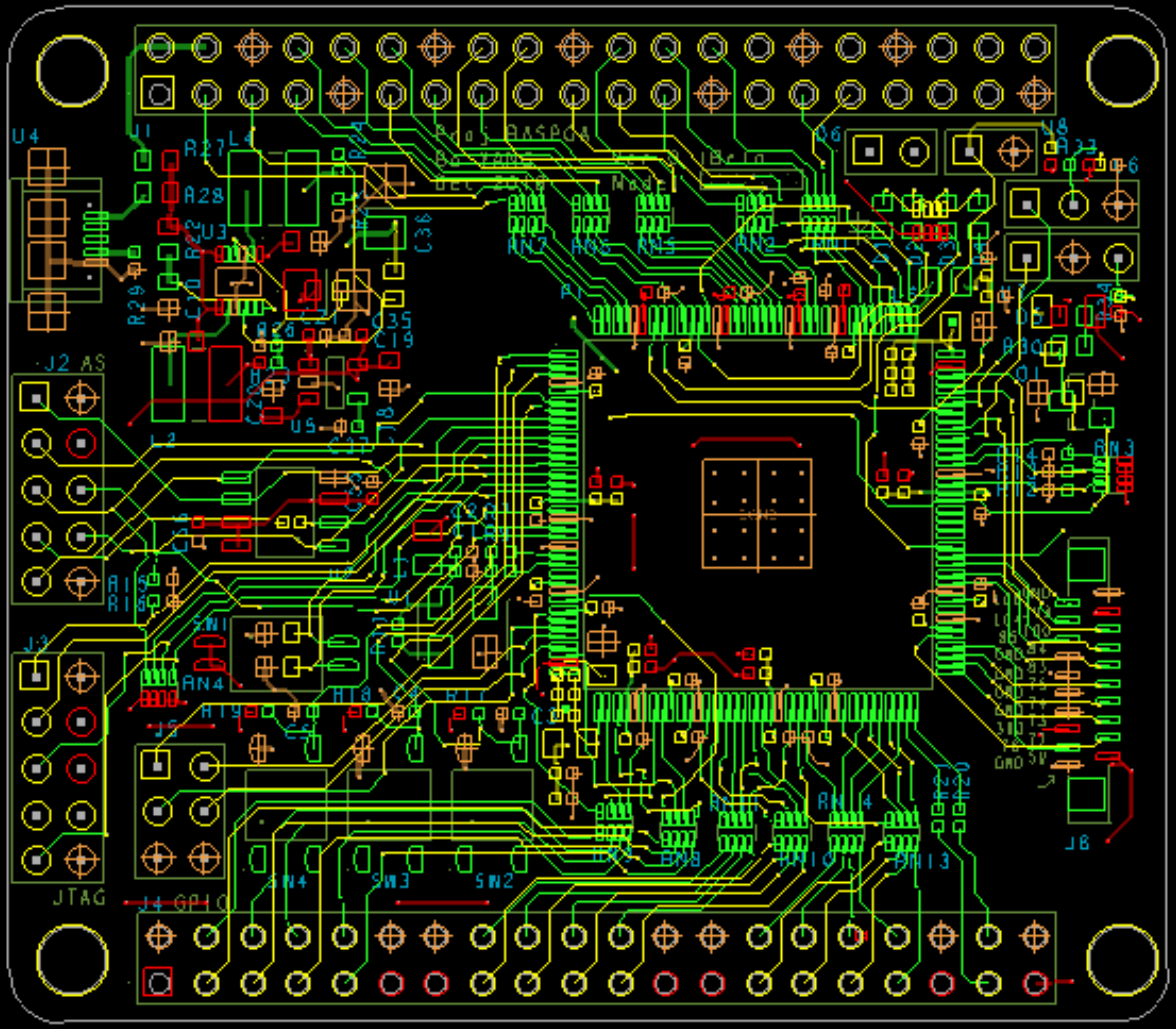

JP4
H1
H2

What we don’t know yet

- 940 nm or not?
- Switching speed can be as fast as 38 kHz ?
- Will higher TX power make a difference?

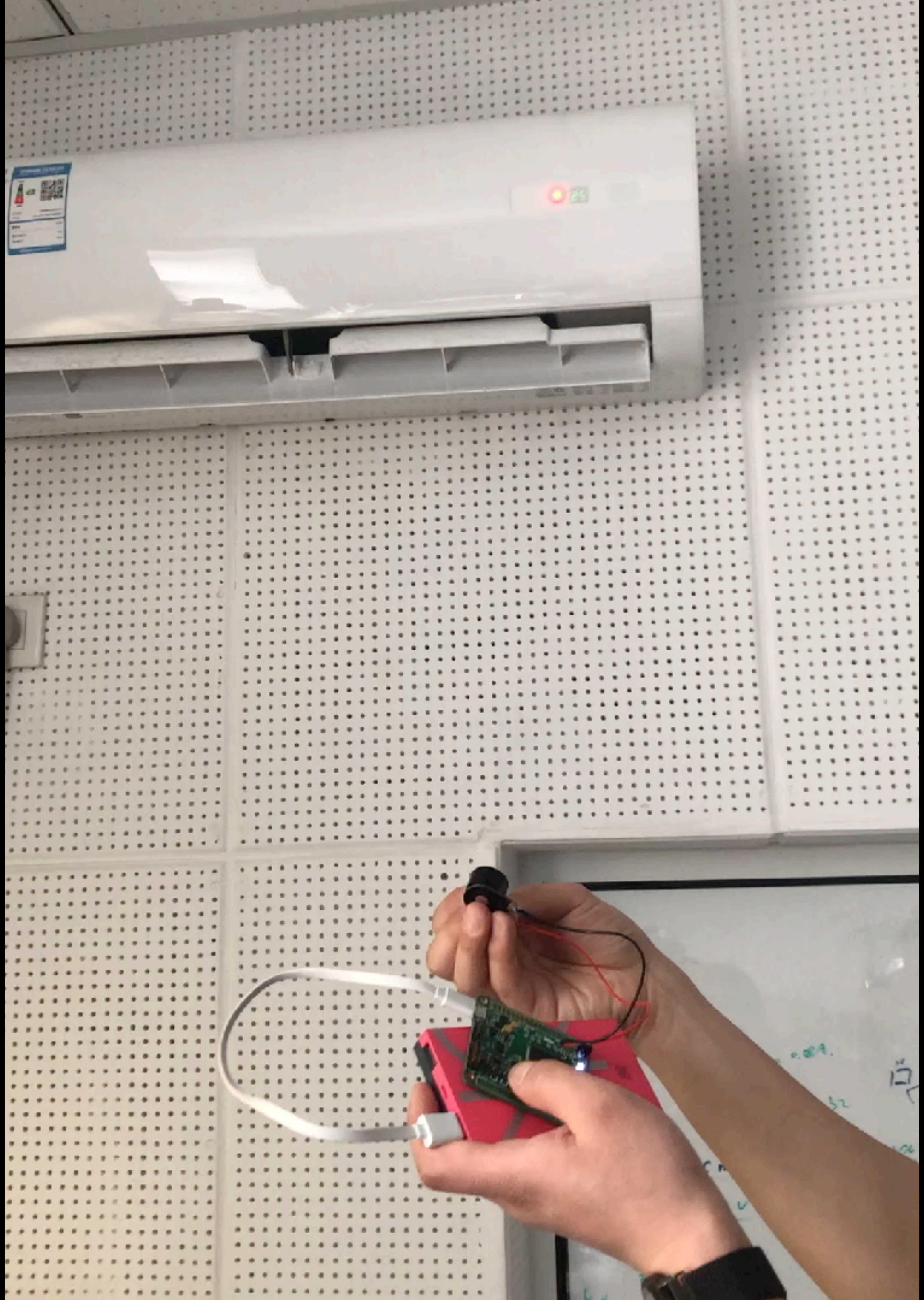
- Several experiments are needed.

- A self-designed FPGA hat for Raspberry Pi
- With interfaces for transmitting and receiving IR signals
- Can be easily programmed into an “IR recorder”.



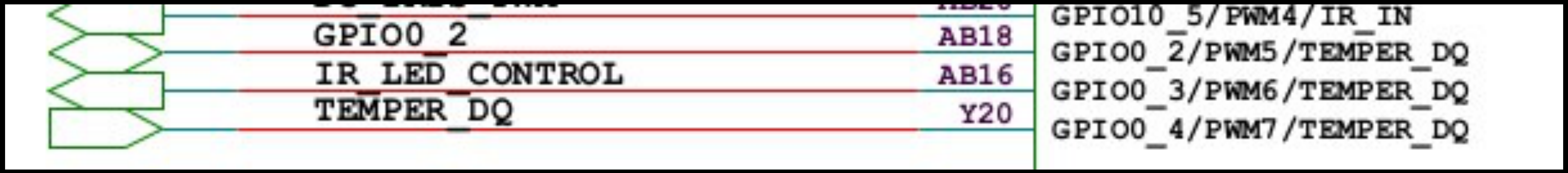
10/100 Fast Ethernet Switch
FeelTech
CH1

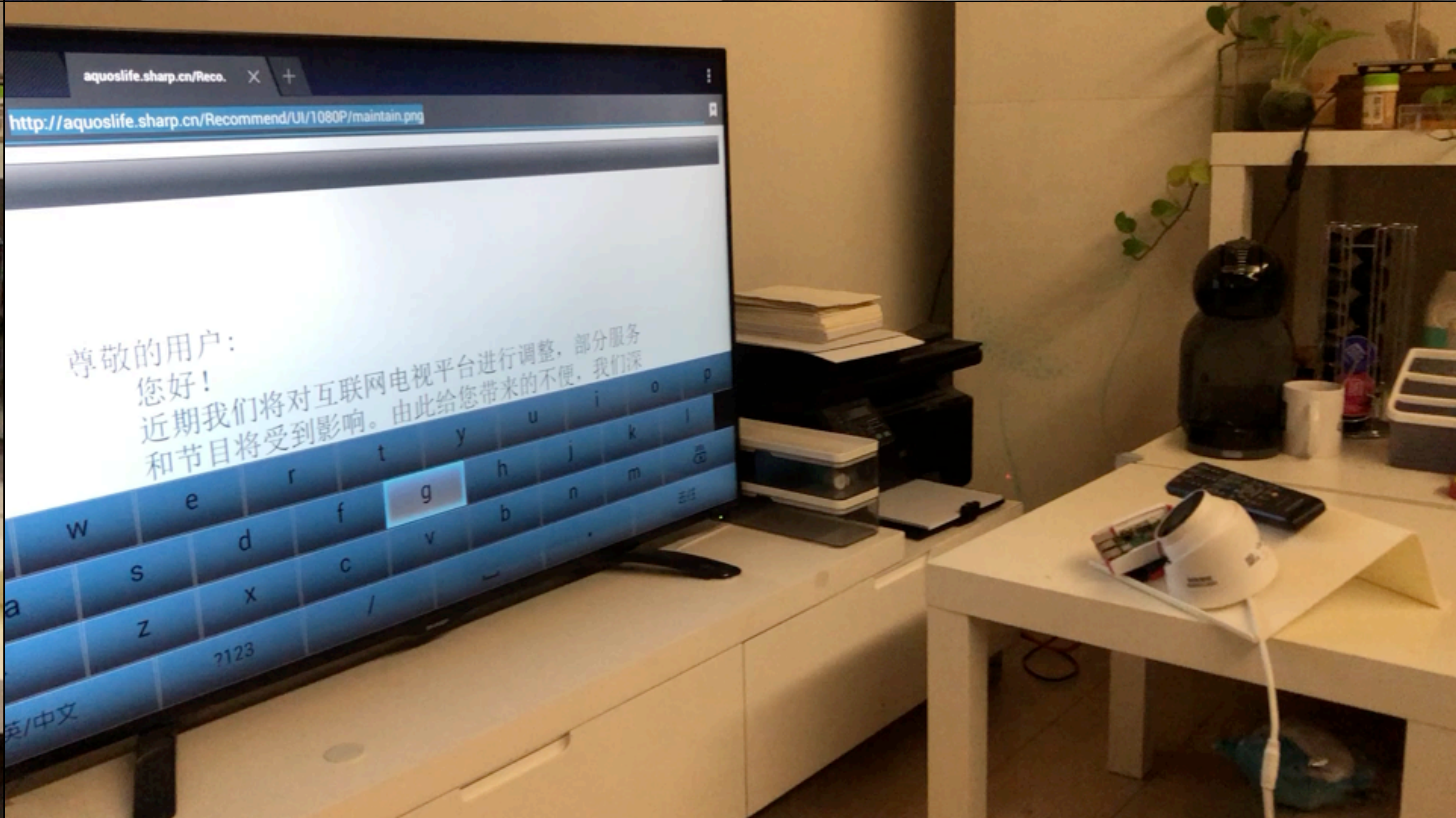
10/100 Fast Ethernet Switch
FeelTech



GPIO, PWM

- Remember PIFM ?
  - https://github.com/rm-hull/pifm
  - DMA Mode





http://aquoslife.sharp.cn/Recommend/UI/1080P/maintain.png

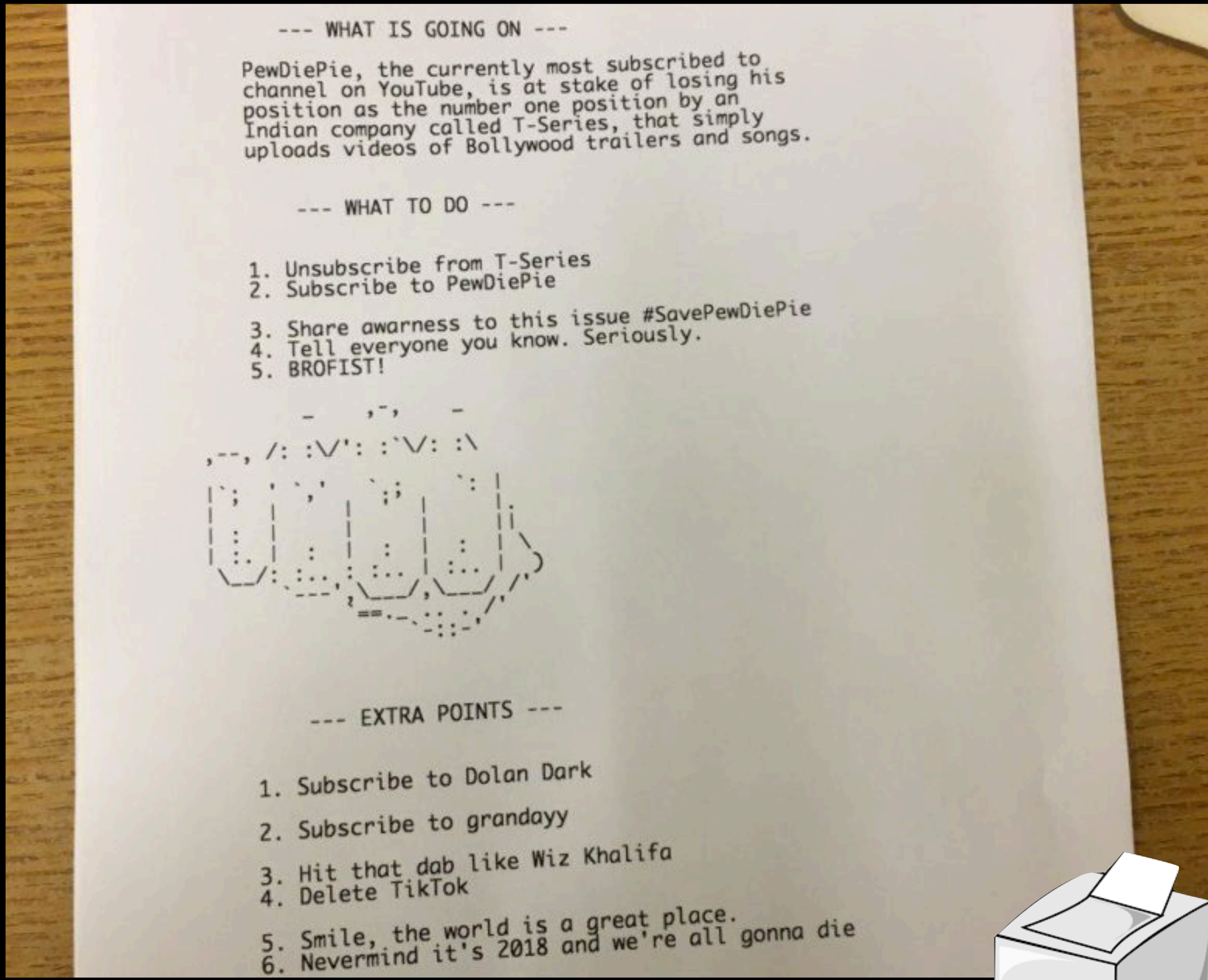
尊敬的用户：

您好！

近期我们将对互联网电视平台进行调整，部分服务和节目将受到影响。由此给您带来的不便，我们深

What could possibly go wrong?

- Turn on millions of ACs at the same time, causing power surge.
- Internet connected TV: unauthorized purchases, botnet-like behaviors



--- WHAT IS GOING ON ---

PewDiePie, the currently most subscribed to channel on YouTube, is at stake of losing his position as the number one position by an Indian company called T-Series, that simply uploads videos of Bollywood trailers and songs.

--- WHAT TO DO ---

1. Unsubscribe from T-Series
2. Subscribe to PewDiePie

3. Share awarness to this issue #SavePewDiePie
4. Tell everyone you know. Seriously.
5. BROFIST!

```
          _     ,-,    _
 ,--, /: :\/': :`\/: :\
|`;  ' `,'   `.;    `: |
|    |     |  '  |     |.
| :  |     |     |     ||
| :. |  :  |  :  |  :  | \
 \__/: :.. : :.. | :.. |  )
      `---',\___/,\___/ /'
           `==._ .. . /'
                `-::-'
```

--- EXTRA POINTS ---

1. Subscribe to Dolan Dark

2. Subscribe to grandayy

3. Hit that dab like Wiz Khalifa
4. Delete TikTok

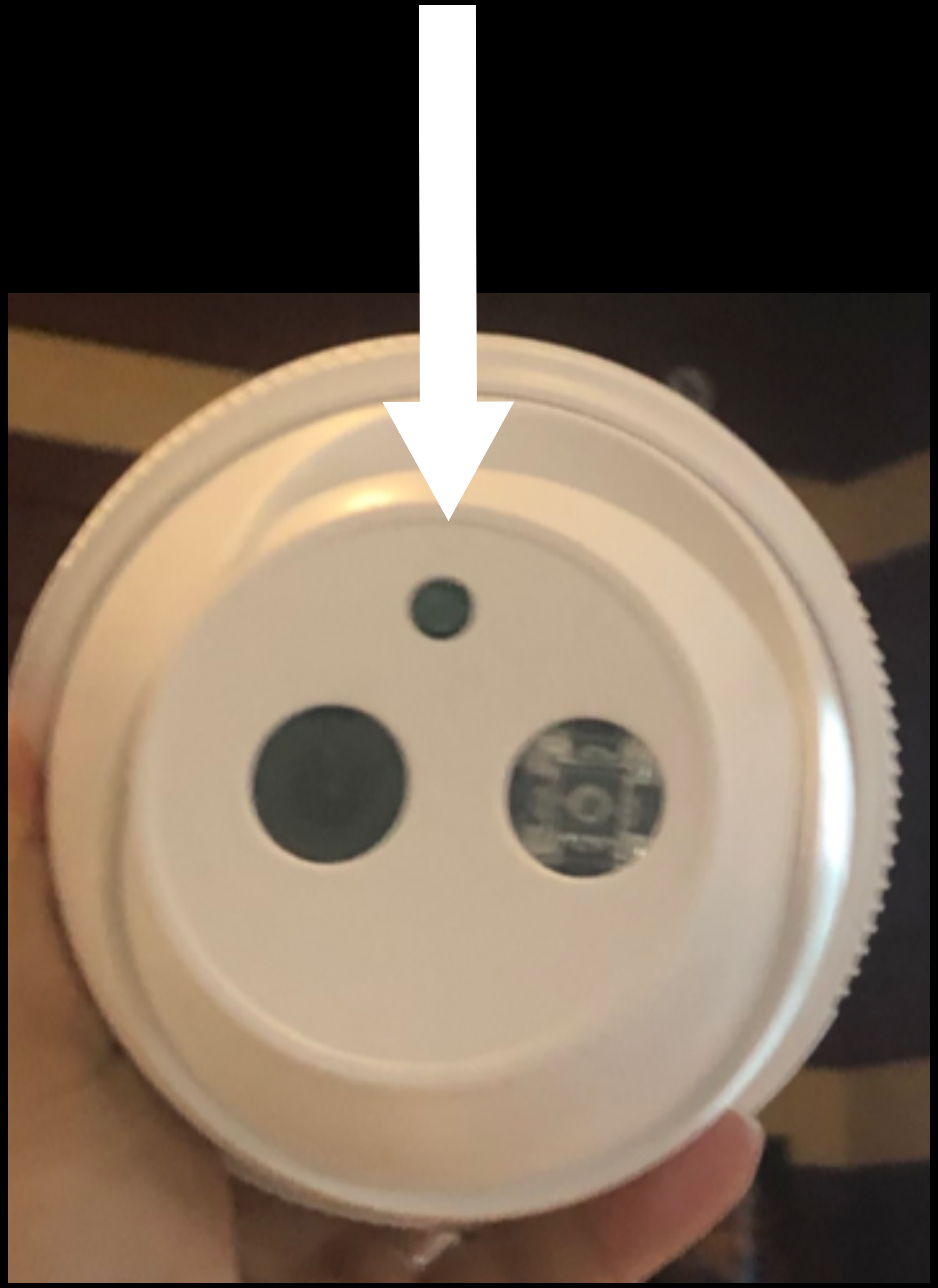
5. Smile, the world is a great place.
6. Nevermind it's 2018 and we're all gonna die

(Pictures taken in Amsterdam)

(Pictures taken in Amsterdam)

Photoresistance

- Exploitable?
- Response time : 30ms
- meh..



Looking at the bright side ...

(Pictures taken in Amsterdam)

IR Watermark maybe?

One More Chapter

Poor man’s Spatial Light Modulator

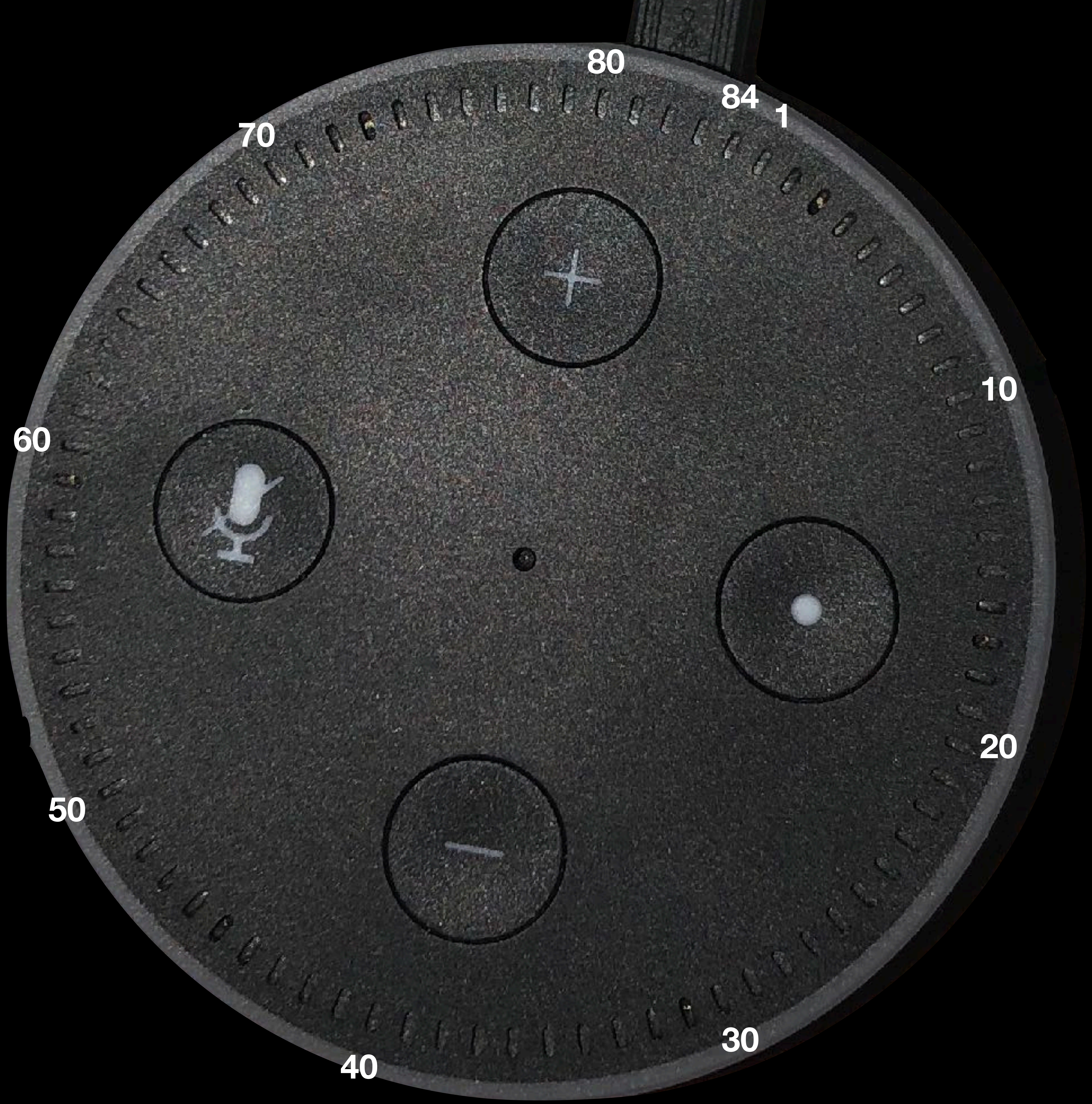
Who said hacking a fan doesn't matter?

Revolutions Per Minute

- DVD: 52x 10400 RPM
- Car: 60mph, 785.3 RPM
- Electric Drill: 10000 ~ 50000 RPM
- Fan: 500 - 1500 RPM
  - Ceiling Fan: 150 ~ 600 RPM
  - Exhaust Fan: 1000 ~ 3000 RPM
  - Server Fan: 20000 RPM
- HDD: 5400/7200 RPM
- Aircraft Propeller: 2400 RPM
- Drones Propeller: 1500-5000 RPM

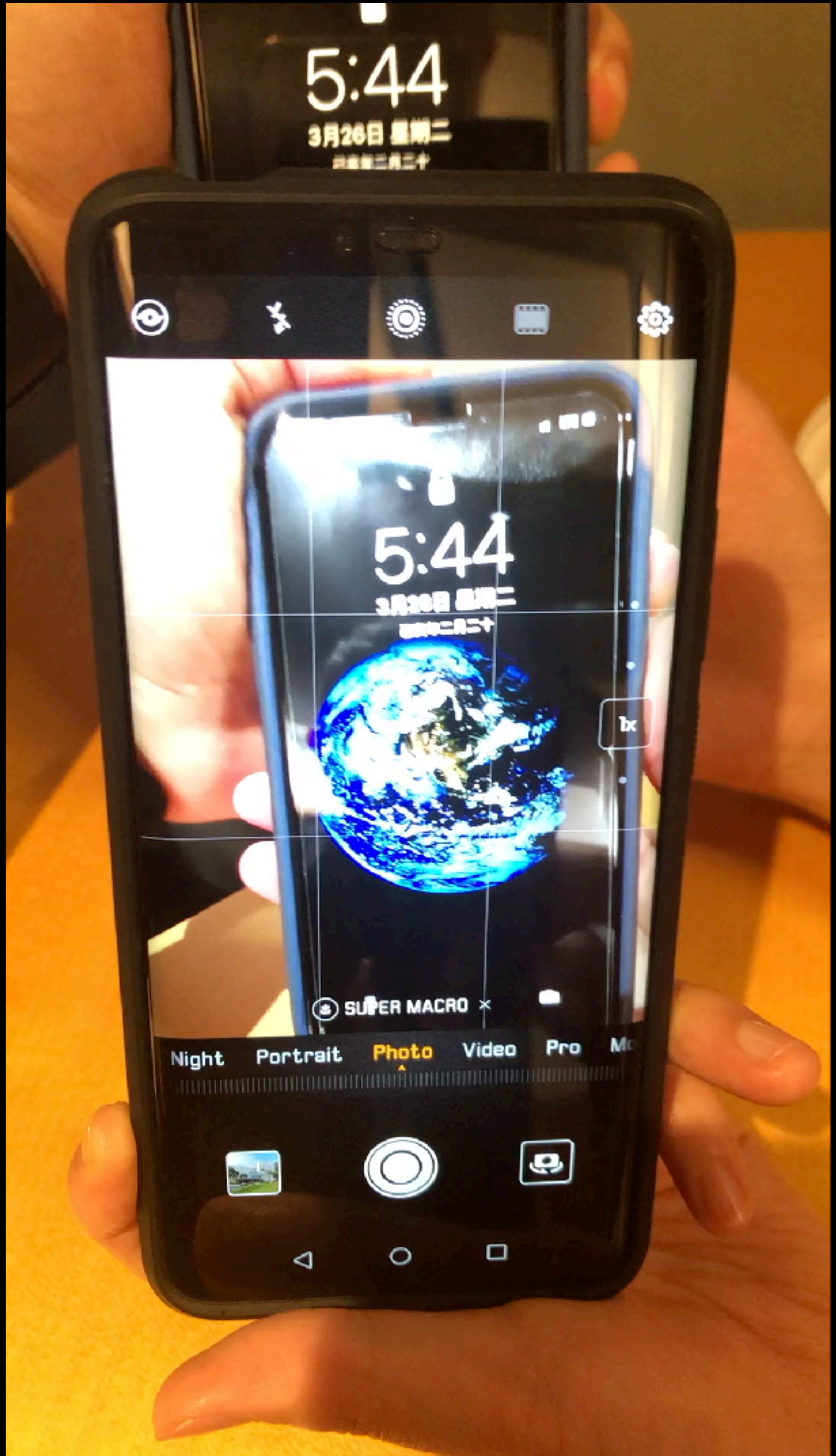
To get 38kHz:

300 Holes, 7600 RPM
150 Holes, 15200 RPM


80
84
1
70
10
60
20
50
30
40

Future Works

- Phantom V25 II   20,000 FPS
- Virtual Frame Technique: Ultrafast Imaging with Any Camera
  - ‘a simple, useful, and accessible form of compressed sensing that increases the frame acquisition rate of any camera by several orders of magnitude by leveraging its dynamic range’
- Spycam detection?
- IR video watermark?


5:44
3月26日 星期二
1x
SUPER MACRO ×
Night
Portrait
Photo
Video
Pro
Mo

Key Takeaways

- Switching rate of IR Filling Light is enough for IR remote controlling.
    - IR Filling light should not be connected to GPIO directly.
- 960FPS COTS cellphone camera is able to work as a logic analyzer.
- Home made light choppers
- Supply chain risk: Regular LED replaced with IR LED. Backdoor.

Thank you!