高级收音机与不智能台灯

申奥

2022 年 10 月 22 日

某厂商高级不智能台灯

The Best Operating Desktop Dial

With the shuttle dial, you can easily switch between brightness and color temperature as well as fine-tuning the light you want in precise.

Turn on the smart-dimming mode with one simple click.

The dial is also ergonomically designed with a slight tilt to enhance comfort.

升级!

The Wireless Controller with the Highest Tech

The wireless controller increases placement flexibility with precise operation of brightness and color temperature adjustment, my favorites setting, 3 light mode switching and auto dimming within one meter range. Industrial precision bearings gives you a smoothing adjustment feeling; optical sensor counting makes operations more precise.
*Keep at least 20 cm above the controller clear to avoid false activation.
*To save power, the controller hibernates automatically when not in

升级？

无线控制器带来了一系列的 UX 问题

- 从 best operating 到 highest tech (but not *best operating*)
- 为了无线，控制器现在需要单独的电池供电
- 于是控制器需要省电
- 为了省电，控制器需要休眠功能
- 先激活控制器后开灯
- 即使如此……

Close

[redacted]

May 1, 2021

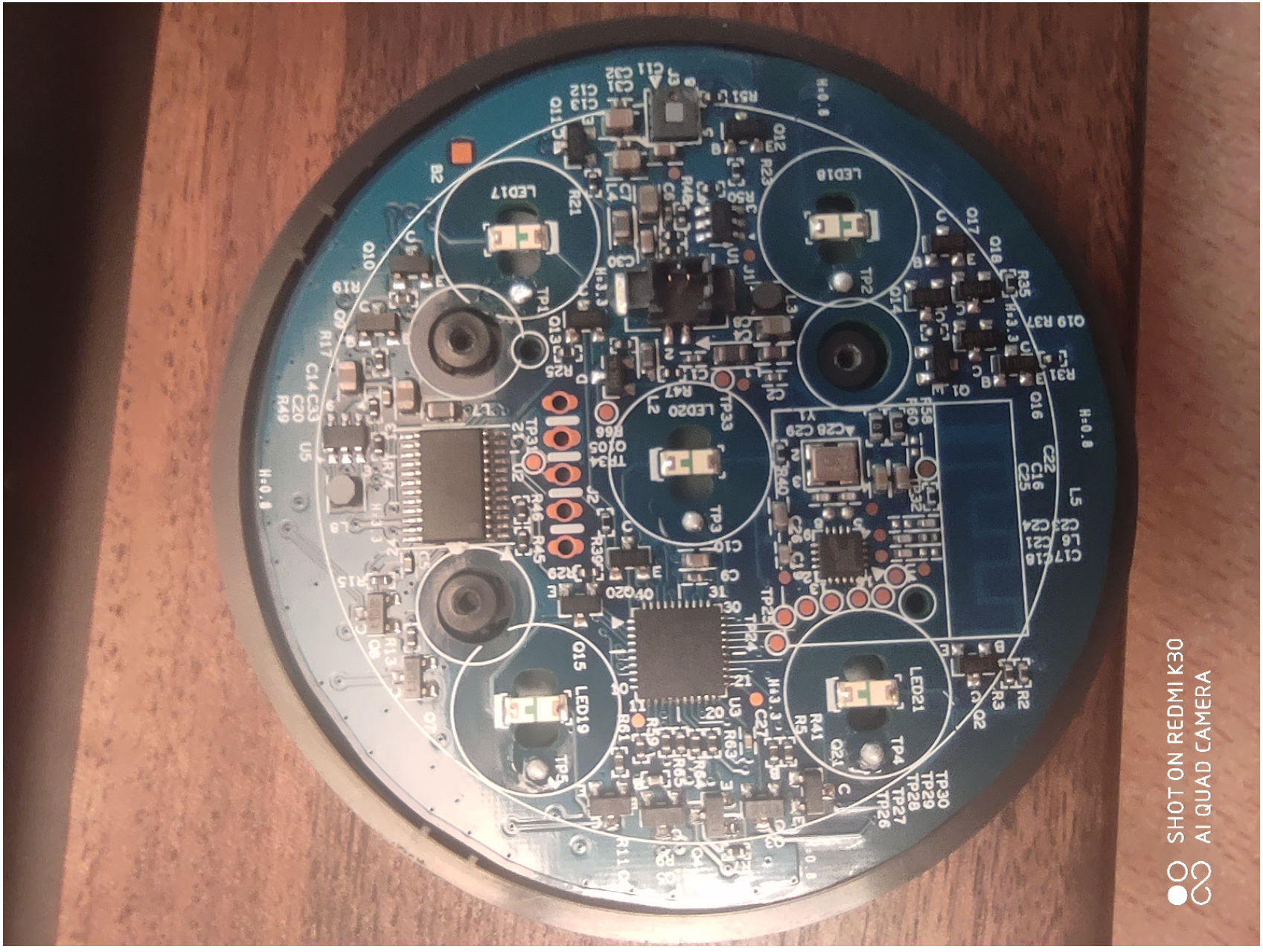
呜呜呜我想念卖你的 screenbar plus 了（ 19:24

halo 不好用吗 19:35

需要七号电池 19:36

现在我无法开灯 19:36

首先拆开看看



- A J2 4-pin connector probably for debugging?
- TCA9539 I/O chip
  - 可能是用来连接按钮灯光的 GPIO
- HOLTEK BC5602 2.4GHz wireless transceiver
- CY8C4125 Cortex-M0 microcontroller

- A J2 4-pin connector probably for debugging?
- TCA9539 I/O chip
  - 可能是用来连接按钮灯光的 GPIO
- HOLTEK BC5602 2.4GHz wireless transceiver
- CY8C4125 Cortex-M0 microcontroller

逆向固件？当时虽然有逻辑分析仪，但是没有合适的夹具

逆向无线？

信息收集

- 该产品在美国上市——它必然取得了 FCC 的相关许可。
- `fccid.org` 收集了 FCC 的各种公开信息

信息收集

Exhibits

All

Document	Type	Submitted Available
Test Setup Photos	Test Setup Photos Adobe Acrobat PDF (743 kB)	2021-04-08 2021-10-06
Users Manual	Users Manual Adobe Acrobat PDF (3886 kB)	2021-04-08 2021-10-06
ID Label/Location Info	ID Label/Location Info Adobe Acrobat PDF (167 kB)	2021-04-08 2021-04-09
Internal Photos	Internal Photos Adobe Acrobat PDF (1044 kB)	2021-04-08 2021-10-06
External Photos	External Photos Adobe Acrobat PDF (476 kB)	2021-04-08 2021-10-06
Test Report	Test Report Adobe Acrobat PDF (820 kB)	2021-04-08 2021-04-09
Letter STC	Cover Letter(s) Adobe Acrobat PDF (354 kB)	2021-04-08 2021-04-09
Letter POA	Cover Letter(s) Adobe Acrobat PDF (254 kB)	2021-04-08 2021-04-09
Schematics	Schematics Adobe Acrobat PDF (379 kB)	2021-04-08
Block Diagram	Block Diagram Adobe Acrobat PDF (45 kB)	2021-04-08
Operational Description	Operational Description Adobe Acrobat PDF (227 kB)	2021-04-08

信息收集

- 内部照片：https://fccid.io/JVPCR20CCTR/Internal-Photos/Internal-Photos-5195232.pdf
- 测试报告：https://fccid.io/JVPCR20CCTR/Test-Report/Test-Report-5195228.pdf
- 企业可以要求对材料当中的原理图等可能涉及商业秘密的信息不予公布（Long-term Confidentiality）
- 可以要求延后一些材料的公布时间防止未上市产品信息泄漏（Short-term Confidentiality）

那不保密的东西有什么用呢？

1.1 Information

1.1.1 Specification of the Equipment under Test (EUT)

RF General Information				
Frequency Range (MHz)	Modulation	Ch. Freq. (MHz)	Channel Number	Data Rate
2400-2483.5	GFSK	2405-2475	0-2 [3]	125kbps

1.1.2 Antenna Details

Ant. No.	Type	Connector	Gain (dBi)
1	PIFA	No	-4.09

1.1.3 Power Supply Type of Equipment under Test (EUT)

Power Supply Type	1.5Vdc, 0.2A (AAA battery*3)

1.1.4 Channel List

Channel	Frequency (MHz)
0	2405
1	2446
2	2475

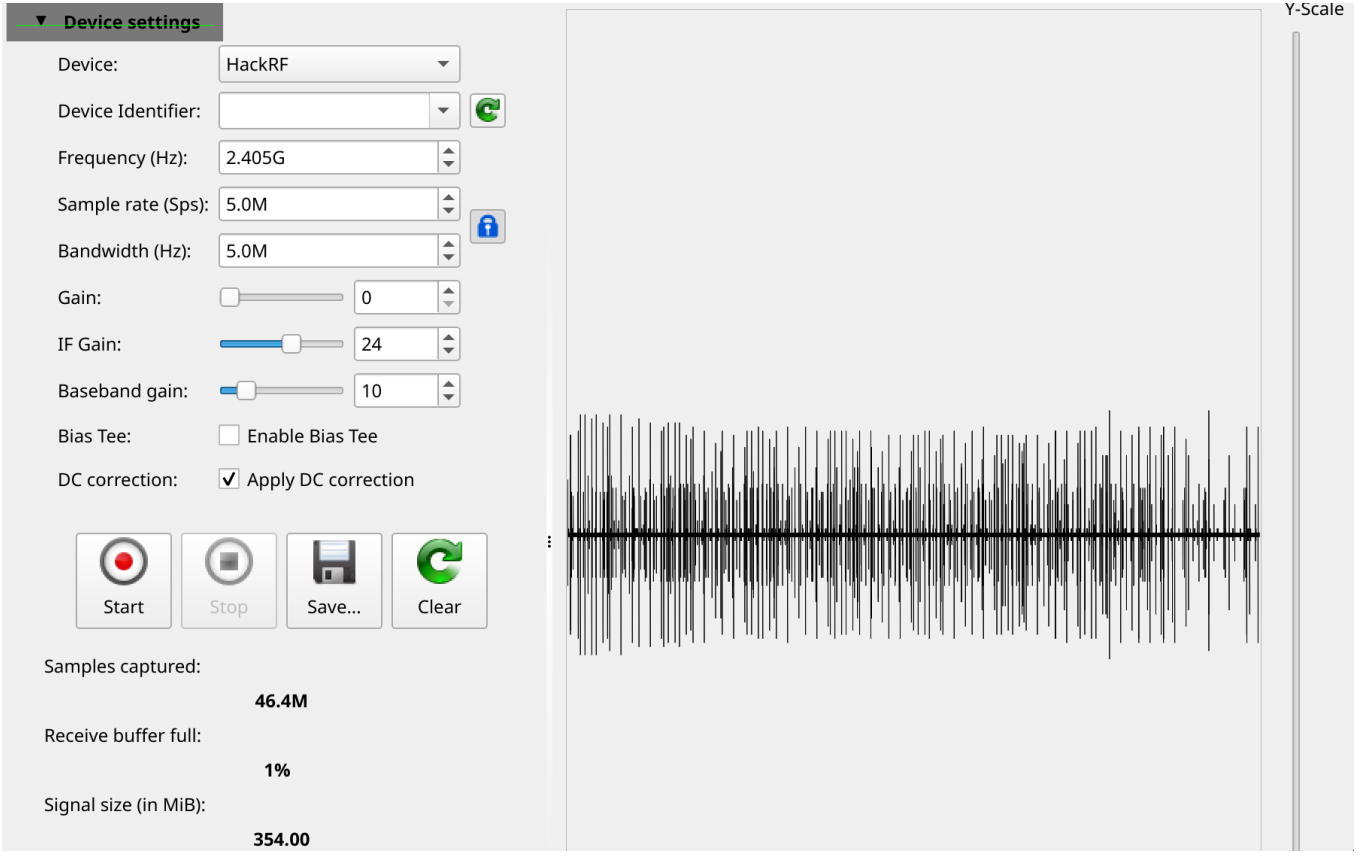
免责声明

- 操作无线电收发设备时，请务必遵守当地法律法规！
- 以下描述的信息仅为个人观察的结果，仅供研究学习等用途，对于尝试使用这些信息所带来的一切直接与间接后果，本人不承担任何直接或连带的责任。

URH: Universal Radio Hacker

`https://github.com/jopohl/urh`

- 提供了很多分析无线传输数字数据的实用工具
- 问题：2.4GHz 频段用的东西非常多，所以很多自动化功能通常都没用（x



先直接回放一遍

先直接回放一遍

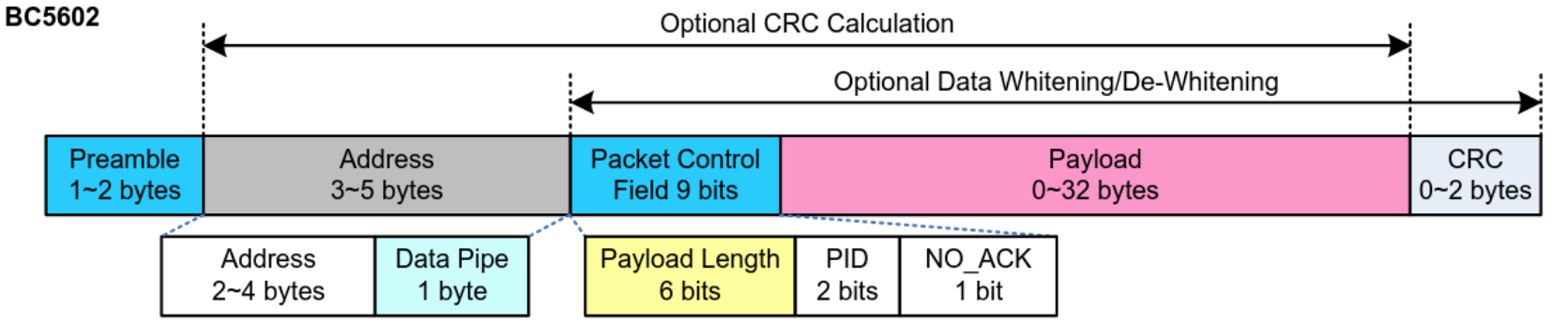
- 非常幸运的是，直接重放就可以看到遥控器的效果
- 这意味着：
- 测试报告列出的几个频道之间没有跳频操作
- 没有加密（或者至少没有足以抗重放的加密）

开始分析

- 首先，需要抓到一个尽可能干净的信号
- 关闭各种蓝牙设备，无线鼠标键盘，离路由器尽可能远……

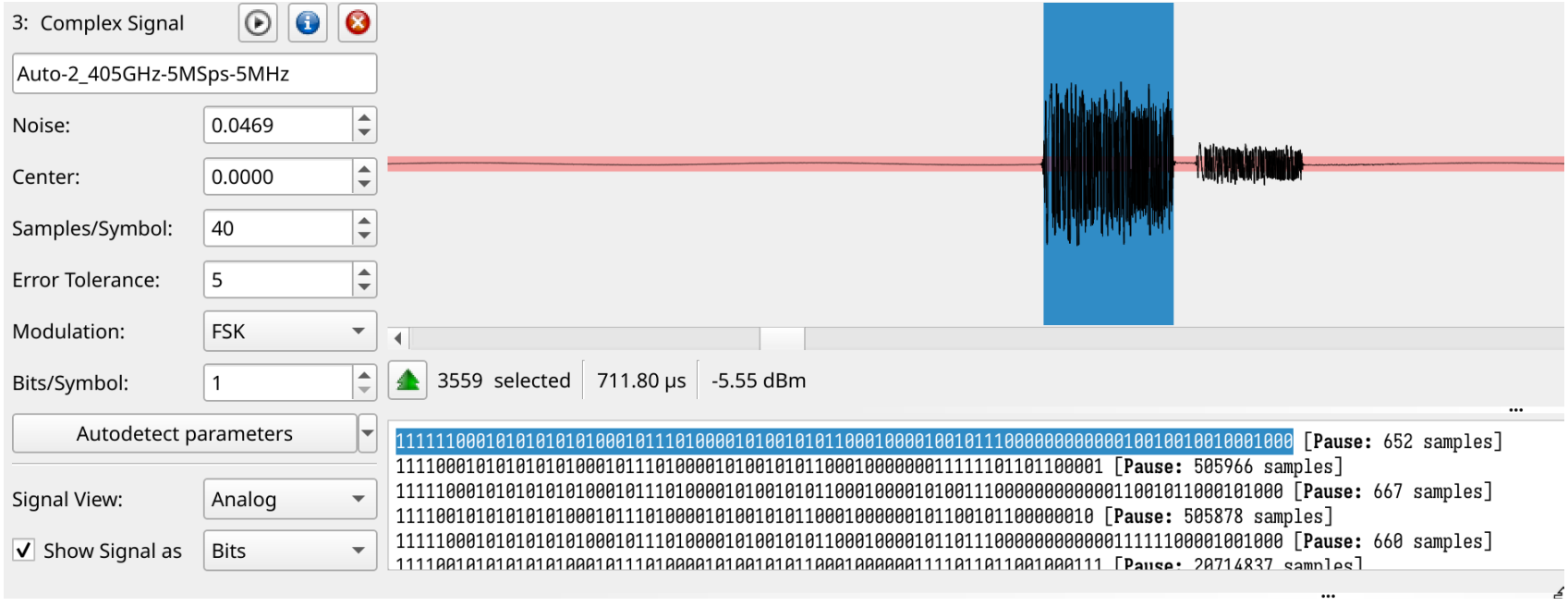
开始分析

- 首先，需要抓到一个尽可能干净的信号
- 关闭各种蓝牙设备，无线鼠标键盘，离路由器尽可能远……

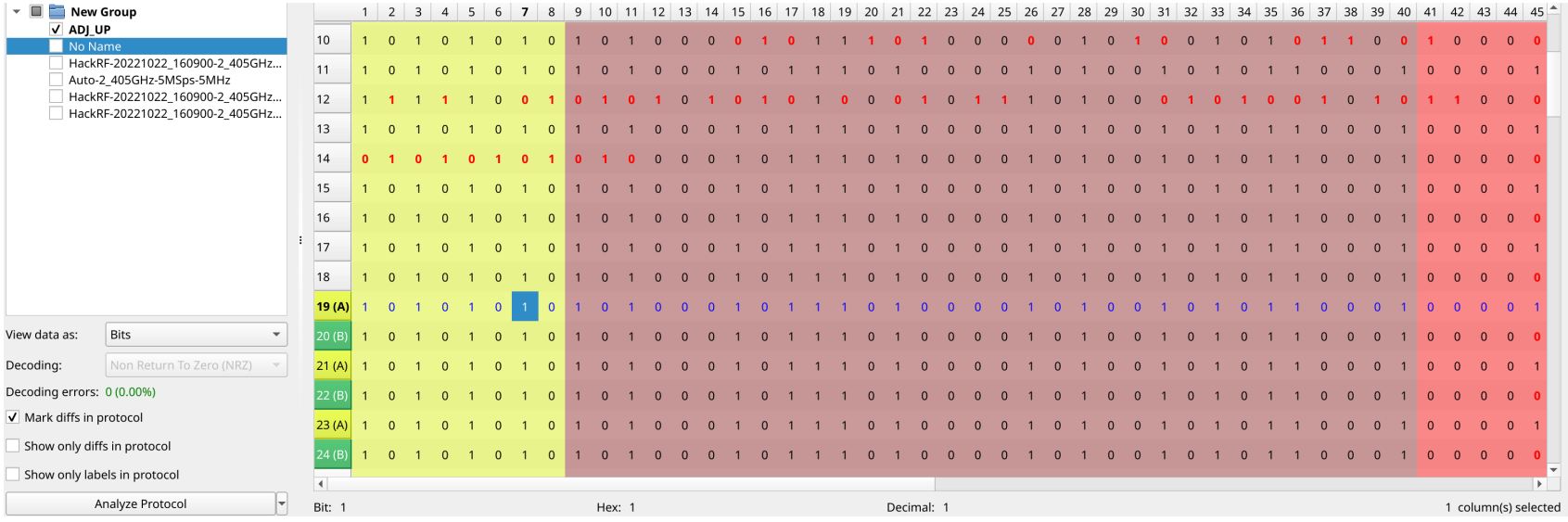


- 了解包格式的信息
- 寻找开头的 01010101 preamble

成功抓到第一个包


3: Complex Signal
Auto-2_405GHz-5MSps-5MHz
Noise: 0.0469
Center: 0.0000
Samples/Symbol: 40
Error Tolerance: 5
Modulation: FSK
Bits/Symbol: 1
Autodetect parameters
Signal View: Analog
Show Signal as Bits
3559 selected
711.80 µs
-5.55 dBm
[Pause: 652 samples]
[Pause: 505966 samples]
[Pause: 667 samples]
[Pause: 505878 samples]
[Pause: 660 samples]

数据分析



- 全面手动处理：
- 当你看到 CRC 对上的很多包的时候说明找对了（

推测 payload 结构

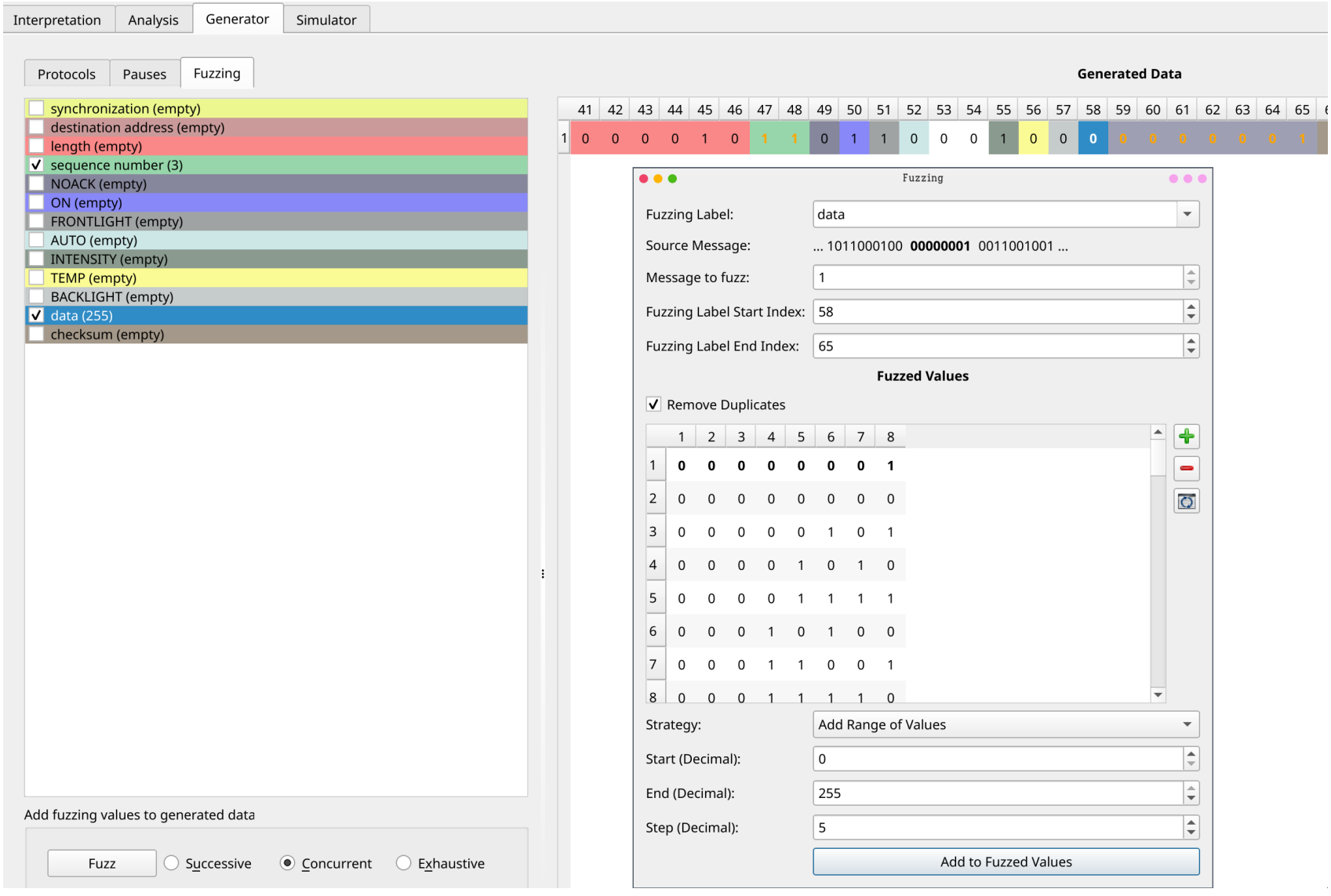
通过抓各种拧旋钮时的无线信息，推测 payload 部分结构如下。注意到里面有两个比特的坑，再加上后面的一些现象，说明这个协议其实还没有完全了解。但是知道这些就可以开关灯了！

payload 共两字节，按发送比特序

[0]	总开关，开启为 1
[1]	前灯，开启为 1
[2]	自动调光，开启为 1
[5]	为 1 代表数据段为亮度
[6]	为 1 代表数据段为色温
[7]	后灯，开启为 1
[8:15]	数据，编码亮度或色温调节

验证

利用 URH 的 Fuzzing 功能



未尽的工作

注意展示里面有一个坑：遥控器是无状态的！
遥控器唤醒时，可以通过某种方式获取台灯当前的状态
可能和 payload 里未知的两个比特有关

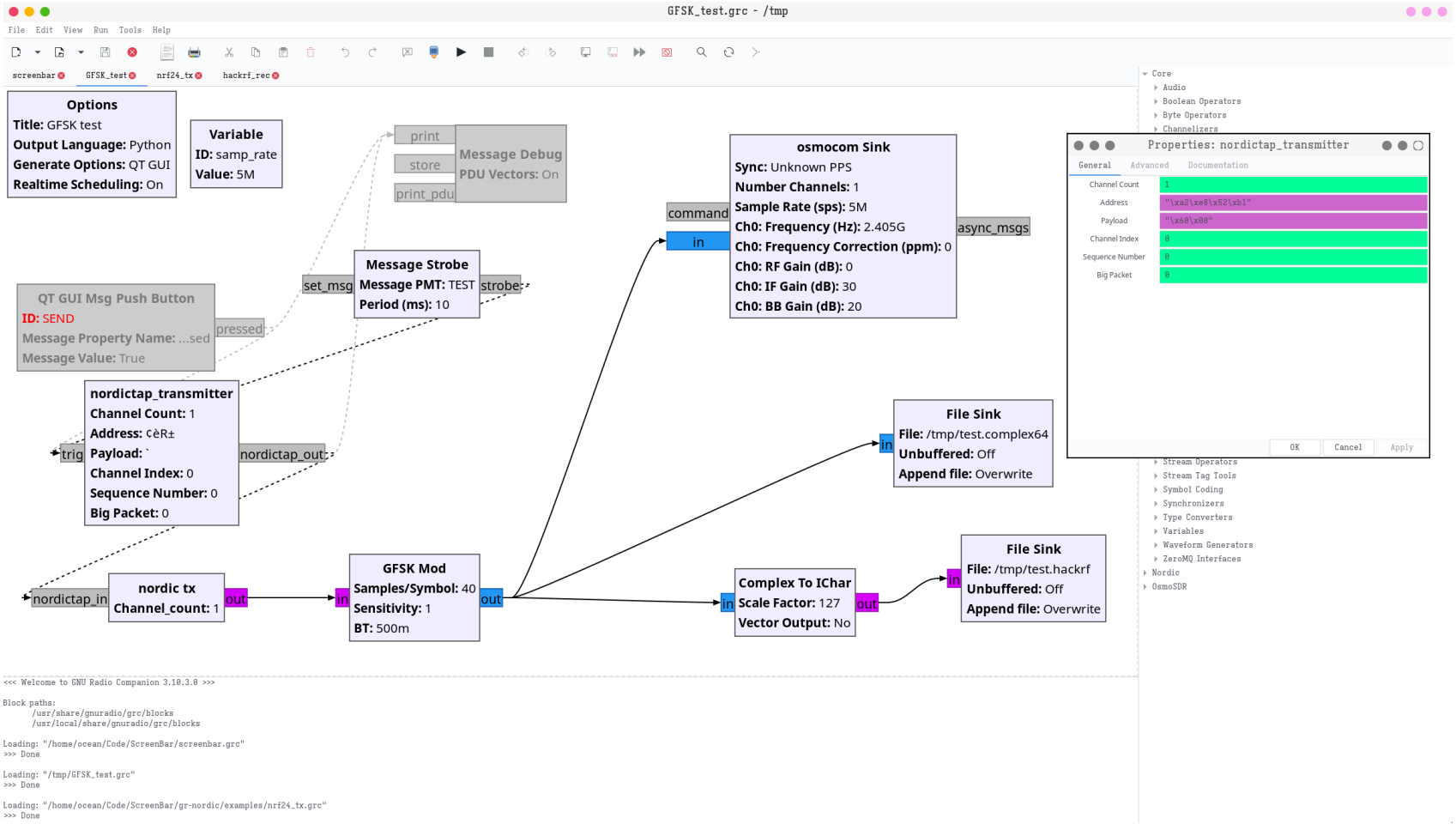
说好的 GNURadio

- 很明显，每次开关灯需要打开 urh 也非常不优雅
- 当然可以把 encode 之后的数据存起来用 `hackrf-transfer` 发送，但是也很不优雅

说好的 GNURadio

- 很明显，每次开关灯需要打开 urh 也非常不优雅
- 当然可以把 encode 之后的数据存起来用 `hackrf-transfer` 发送，但是也很不优雅
- 如何使用 GNURadio 编写脚本控制？
- 熟悉的同学可以看出来，这个包格式（和其它大量 2.4GHz 模块一样）和 nRF24 的 nordic ShockBurst^{TM} 一模一样
- `https://github.com/BastilleResearch/gr-nordic`

年久失修


GFSK_test.grc - /tmp
File Edit View Run Tools Help
screenbar GFSK_test nrf24_tx hackrf_rec
Options
Title: GFSK test
Output Language: Python
Generate Options: QT GUI
Realtime Scheduling: On
Variable
ID: samp_rate
Value: 5M
print
store
print_pdu
Message Debug
PDU Vectors: On
osmocom Sink
Sync: Unknown PPS
Number Channels: 1
Sample Rate (sps): 5M
Ch0: Frequency (Hz): 2.405G
Ch0: Frequency Correction (ppm): 0
Ch0: RF Gain (dB): 0
Ch0: IF Gain (dB): 30
Ch0: BB Gain (dB): 20
command
in
async_msgs
Message Strobe
Message PMT: TEST
Period (ms): 10
set_msg
strobe
QT GUI Msg Push Button
ID: SEND
Message Property Name: ...sed
Message Value: True
pressed
nordictap_transmitter
Channel Count: 1
Address: ĊèR±
Payload: `
Channel Index: 0
Sequence Number: 0
Big Packet: 0
trig
nordictap_out
File Sink
File: /tmp/test.complex64
Unbuffered: Off
Append file: Overwrite
nordictap_in
nordic tx
Channel_count: 1
out
GFSK Mod
Samples/Symbol: 40
Sensitivity: 1
BT: 500m
Complex To IChar
Scale Factor: 127
Vector Output: No
File Sink
File: /tmp/test.hackrf
Unbuffered: Off
Append file: Overwrite
Properties: nordictap_transmitter
General Advanced Documentation
Channel Count
Address
Payload
Channel Index
Sequence Number
Big Packet
OK Cancel Apply
Core
Audio
Boolean Operators
Byte Operators
Channelizers
Stream Operators
Stream Tag Tools
Symbol Coding
Synchronizers
Type Converters
Variables
Waveform Generators
ZeroMQ Interfaces
Nordic
OsmoSDR
<<< Welcome to GNU Radio Companion 3.10.3.0 >>>
Block paths:
/usr/share/gnuradio/grc/blocks
/usr/local/share/gnuradio/grc/blocks
Loading: "/home/ocean/Code/ScreenBar/screenbar.grc"
>>> Done
Loading: "/tmp/GFSK_test.grc"
>>> Done
Loading: "/home/ocean/Code/ScreenBar/gr-nordic/examples/nrf24_tx.grc"
>>> Done

年轻人的第一个 GNURadio 模块

- steaming API：在 work 函数里处理流式数据
- message passing API：利用 `message_port_register_in/out` 和 `set_msg_handler` 异步处理消息
- 支持使用 ZeroMQ 和外部程序收发消息

科学与不太科学

控制流图导出 python 之后可以独立修改使用

```
def main(top_block_cls=GFSK_test, options=None):
    if gr.enable_realtime_scheduling() != gr.RT_OK:
        print("Error: failed to enable real-time scheduling.")

    if StrictVersion("4.5.0") <= StrictVersion(Qt.qVersion()) < StrictVersion("5.0.0"):
        style = gr.prefs().get_string('qtgui', 'style', 'raster')
        Qt.QApplication.setGraphicsSystem(style)
    qapp = Qt.QApplication(sys.argv)

    tb = top_block_cls()

    tb.start()

    tb.show()

    def sig_handler(sig=None, frame=None):
        tb.stop()
        tb.wait()

        Qt.QApplication.quit()

    signal.signal(signal.SIGINT, sig_handler)
    signal.signal(signal.SIGTERM, sig_handler)

    timer = Qt.QTimer()
    timer.start(500)
    timer.timeout.connect(lambda: None)
```