

# 工控大楼的道闸怎么坏了

发表于 2021-01-25 更新于 2021-02-16 分类于 [Challenge](#) , [2020](#) , [工业信息安全技能大赛](#) , [济南站](#)  
[Challenge | 2020 | 工业信息安全技能大赛 | 济南站 | 工控大楼的道闸怎么坏了](#)

[点击此处](#)获得更好的阅读体验

## WriteUp来源

来自MO1N战队

## 题目描述

某工控大楼道闸数据分析，你能获取到flag吗？Flag格式为：flag{}

## 题目考点

- 无线信号分析

## 解题思路

无线信号分析题，em1527协议，考点主要在分析32位数据，而32位中8位的同步码位并不需要，所以还剩24位主要数据，而20位为固定码位、4位数据码位。

最后一位为下一帧的无线信号，所以在分析时坑就在这里

□

一帧信号的编码格式为 => 8位同步码 + 20位内码 + 4位数据码

- 0码, 对应1个高电平+3个低电平
- 1码, 对应3个高电平+1个低电平
- 同步码, 对应1个高电平+31个低电平

也就是说，同步码=10000000000000000000000000000000，0码=1000，1码=1110

□

使用urh、Audacity、inspectrum、都可以看到分析出来的数据101010110010110010000001

只需要转换成16进制即可，而且文件名有提示iiiiicccccssssshhhheeeexxxx就是ics hex 一下。

## Flag

```
1 flag{ab2c81}
```

- 本文作者：CTFHub
- 本文链接：<https://writeup.ctfhub.com/Challenge/2020/工业信息安全技能大赛/济南站/HEf85G4esjJx3BmDXiRrh.html>
- 版权声明：本博客所有文章除特别声明外，均采用 [BY-NC-SA](#) 许可协议。转载请注明出处！

[# Challenge # 2020 # 工业信息安全技能大赛 # 济南站](#)  
[COTP](#)  
[泄露的信号](#)