



# IEC104

📅 2021-09-05 | 📁 Challenge , 2021 , 第七届全国工控系统信息安全攻防竞赛 , 四类

Challenge | 2021 | 第七届全国工控系统信息安全攻防竞赛 | 四类 | IEC104

[点击此处](#)获得更好的阅读体验

## WriteUp来源

来自 毕方安全实验室 战队及 bad\_cat 战队

## 题目描述

查看压缩包内隐藏的信息，flag格式：flag{xxx}

## 提示信息

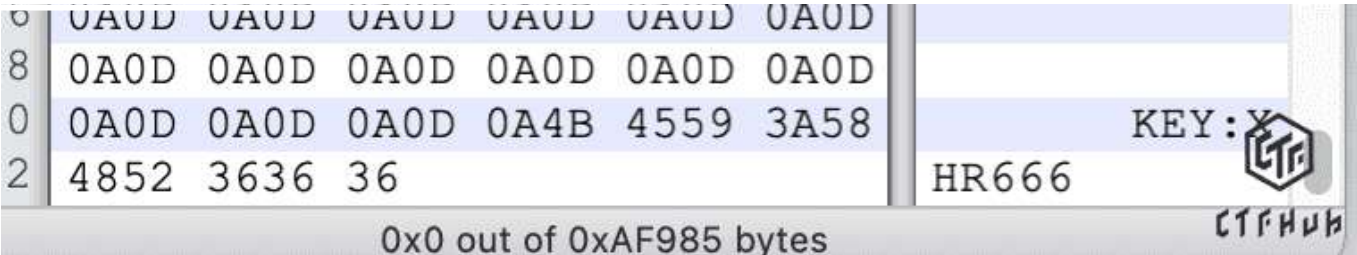
无

## 题目考点

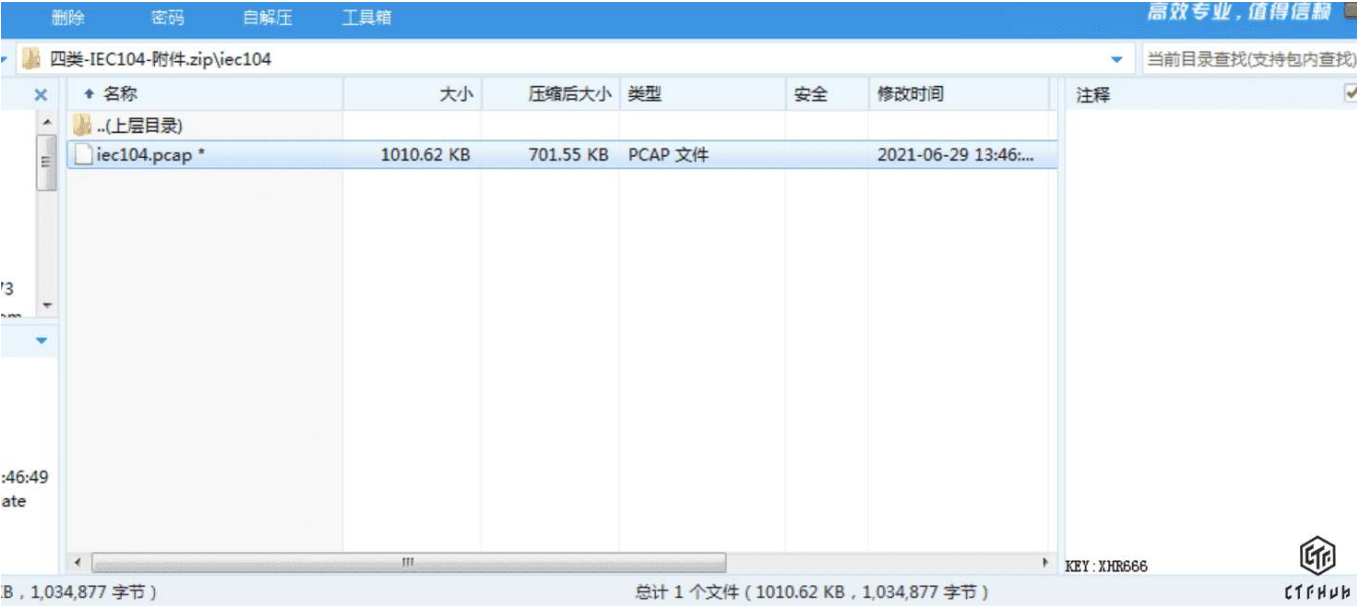
- Zip伪加密
- 流量分析
- IEC104

## 解题思路

在ZIP末尾发现一串字符伪 KEY:XHR666



打开压缩包发现有密码，



尝试使用 `zipCenOp.jar` 处理伪加密，之后成功解压出ice104.pcap流量包

进一步使用binwalk分析流量包得到 `FLAG.txt`



flag.txt里面是加密的flag，利用第一步得到的key(XHR666)解密

```
1 U2FsdGVkX1/A8ta0AedfEebXcmYznwA2U4SXuZ9oW2NQ1AuJbF9dmg==
```

根据经验，U2Fsd开头为AES、DES、3DES等算法，挨个以 `XHR666` 作为密码尝试，发现算法为3DES

对称加密/解密

AES加密/解密

DES加密/解密

RC4加密/解密

Rabbit加密/解密

Tri

TripleDES算法在线加密解密工具（实现TripleDES在线加密解密）

U2FsdGVkX1/A8ta0AedfEebXcmYznwA2U4SXuZ9oW2NO1AuJbF9dmg==

XHR666

TripleDES加密

TripleDES解密

清空输入框

复制结果文本

flag{QgcMT\_zqMpXG\_7DMs}



## Flag




```
1 flag{QgcMT_zqMpXG_7DMs}
```

**本文作者：** CTFHub

**本文链接：** <https://writeup.ctfhub.com/Challenge/2021/第七届全国工控系统信息安全攻防竞赛/四类/5HMAXfhNLXeuuUnBuc2QnL.html>

**版权声明：** 本博客所有文章除特别声明外，均采用 [CC BY-NC-SA](#) 许可协议。转载请注明出处！

© 2019 – 2022  CTFHub  
由 [Hexo](#) & [NexT.Gemini](#) 强力驱动