Fins协议通讯

2021-09-01 | Challenge， 2021， 工业信息安全技能大赛， 线上赛-第一场

Challenge | 2021 | 工业信息安全技能大赛 | 线上赛-第一场 | Fins协议通讯

点击此处获得更好的阅读体验

WriteUp来源

来自 Venom 战队

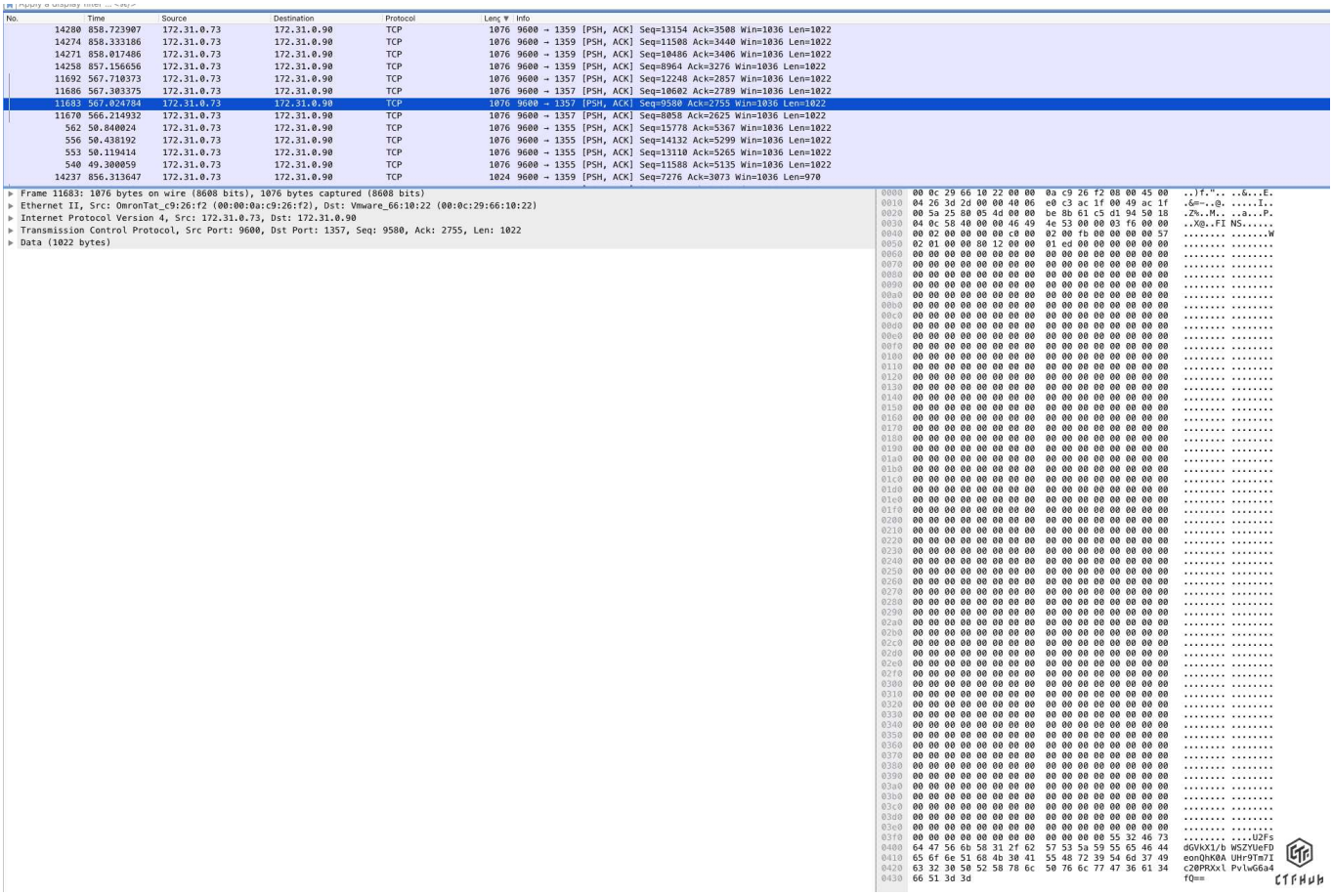
题目描述

> 工程师小夏在工控日志流量审计设备中发现某台PLC设备通讯异常，请您帮助小夏分析出相关异常的加密数据。flag格式为：flag{}

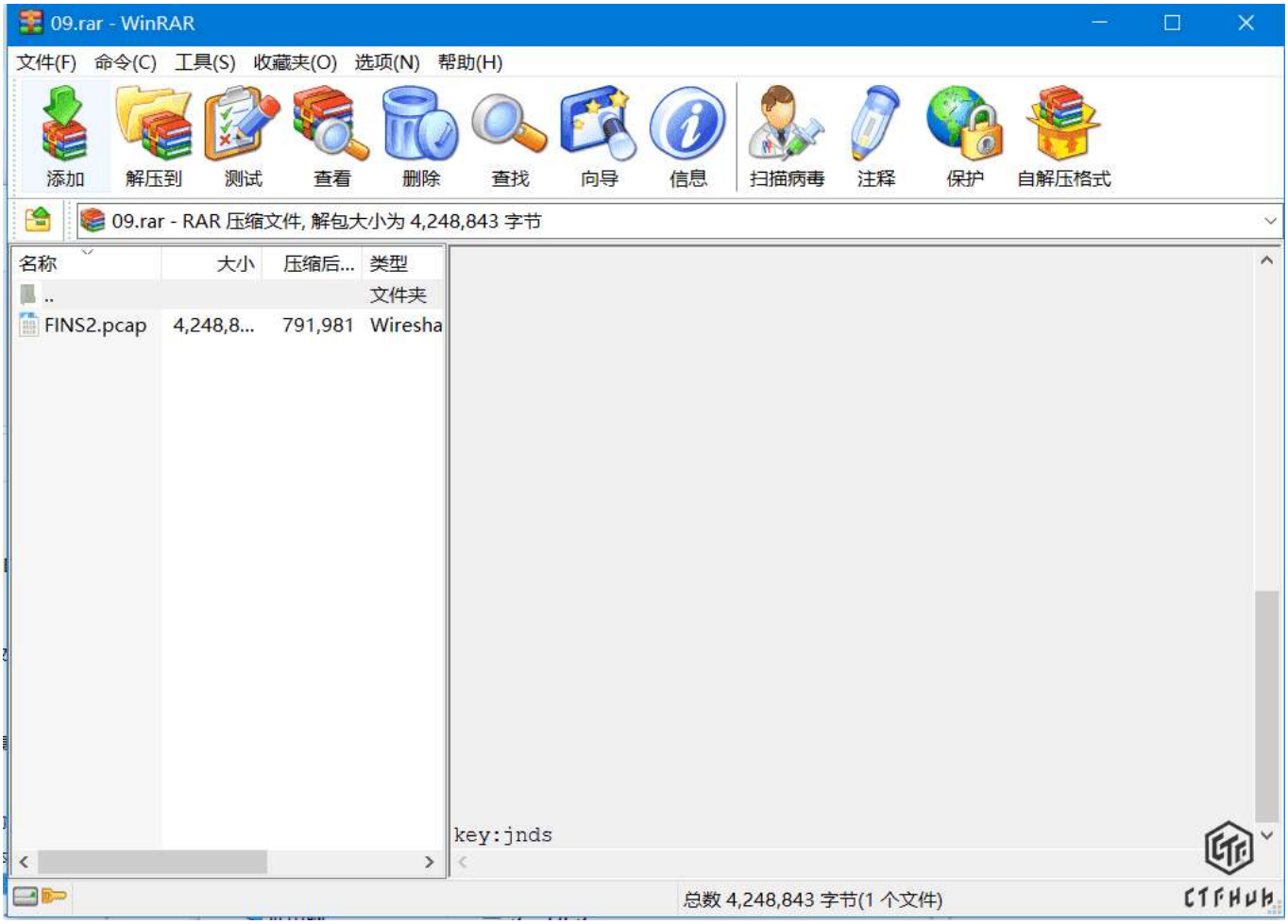
题目考点

解题思路

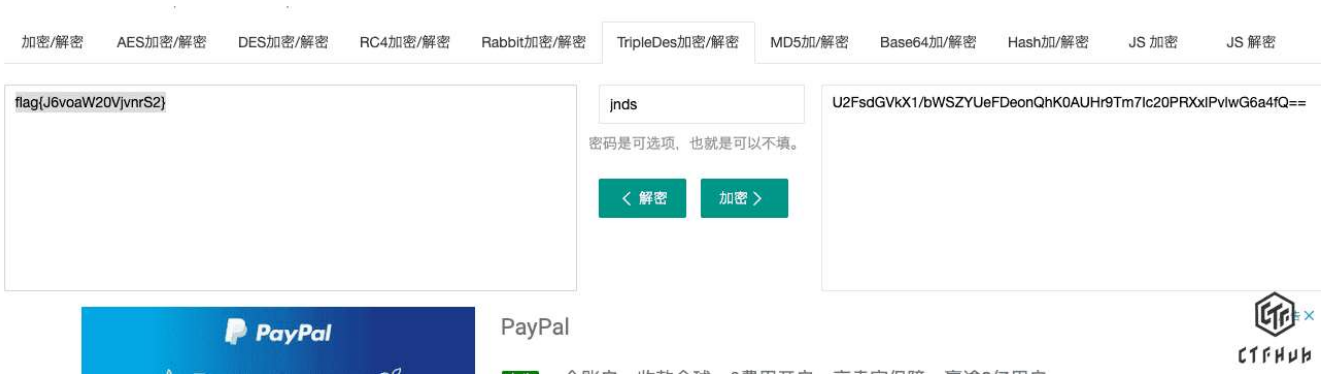
翻看流量，在11683 号数据包发现异常数据



在压缩包注释中发现密钥 `jnds`



对U2Fsd开头的这串数据进行3DES解密，得到flag



Flag

```
1  flag{J6voaW20VjnrS2}
```


Challenge # 2021 # 工业信息安全技能大赛 # 线上赛-第一场

Modbus采集分析 Attack