



# 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

No.	Time	Source	Destination	Protocol	Length	Info
14280	858.723987	172.31.0.73	172.31.0.90	TCP	1076	6600 → 1359 [PSH, ACK] Seq=13154 Ack=3508 Win=1036 Len=1022
14274	858.333186	172.31.0.73	172.31.0.90	TCP	1076	6600 → 1359 [PSH, ACK] Seq=13508 Ack=3440 Win=1036 Len=1022
14271	858.017486	172.31.0.73	172.31.0.90	TCP	1076	6600 → 1359 [PSH, ACK] Seq=10406 Ack=3406 Win=1036 Len=1022
14258	857.156556	172.31.0.73	172.31.0.90	TCP	1076	6600 → 1359 [PSH, ACK] Seq=8964 Ack=3276 Win=1036 Len=1022
11692	567.710373	172.31.0.73	172.31.0.90	TCP	1076	6600 → 1357 [PSH, ACK] Seq=12248 Ack=2857 Win=1036 Len=1022
11686	567.303375	172.31.0.73	172.31.0.90	TCP	1076	6600 → 1357 [PSH, ACK] Seq=10602 Ack=2789 Win=1036 Len=1022
11653	567.021724	172.31.0.73	172.31.0.90	TCP	1076	6600 → 1357 [PSH, ACK] Seq=10587 Ack=2755 Win=1036 Len=1022
11670	566.214922	172.31.0.73	172.31.0.90	TCP	1076	6600 → 1357 [PSH, ACK] Seq=8055 Ack=2625 Win=1036 Len=1022
562	50.840024	172.31.0.73	172.31.0.90	TCP	1076	6600 → 1355 [PSH, ACK] Seq=15778 Ack=5367 Win=1036 Len=1022
556	50.438192	172.31.0.73	172.31.0.90	TCP	1076	6600 → 1355 [PSH, ACK] Seq=14132 Ack=5299 Win=1036 Len=1022
553	50.119414	172.31.0.73	172.31.0.90	TCP	1076	6600 → 1355 [PSH, ACK] Seq=13110 Ack=5265 Win=1036 Len=1022
540	49.300059	172.31.0.73	172.31.0.90	TCP	1076	6600 → 1355 [PSH, ACK] Seq=11580 Ack=5135 Win=1036 Len=1022
14237	856.313647	172.31.0.73	172.31.0.90	TCP	1024	6600 → 1359 [PSH, ACK] Seq=7276 Ack=3073 Win=1036 Len=970

▶ Frame 11683: 1076 bytes on wire (8608 bits), 1076 bytes captured (8608 bits) on interface 0

▶ Ethernet II, Src: OmronTat\_c9:26:f2 (00:00:0a:c9:26:f2), Dst: Vmware\_66:10:22 (00:0c:29:66:10:22)

▶ Internet Protocol Version 4, Src: 172.31.0.73, Dst: 172.31.0.90

▶ Transmission Control Protocol, Src Port: 6600, Dst Port: 1357, Seq: 9580, Ack: 2755, Len: 1022

▶ Data (1022 bytes)

0000 00 0c 29 66 10 22 00 00 0a c9 26 f2 00 00 45 00 ..)T... ..E.

0010 04 26 3d 2d 00 00 40 06 e0 c3 ac 1f 00 49 ac 1f .6=-...@...I.

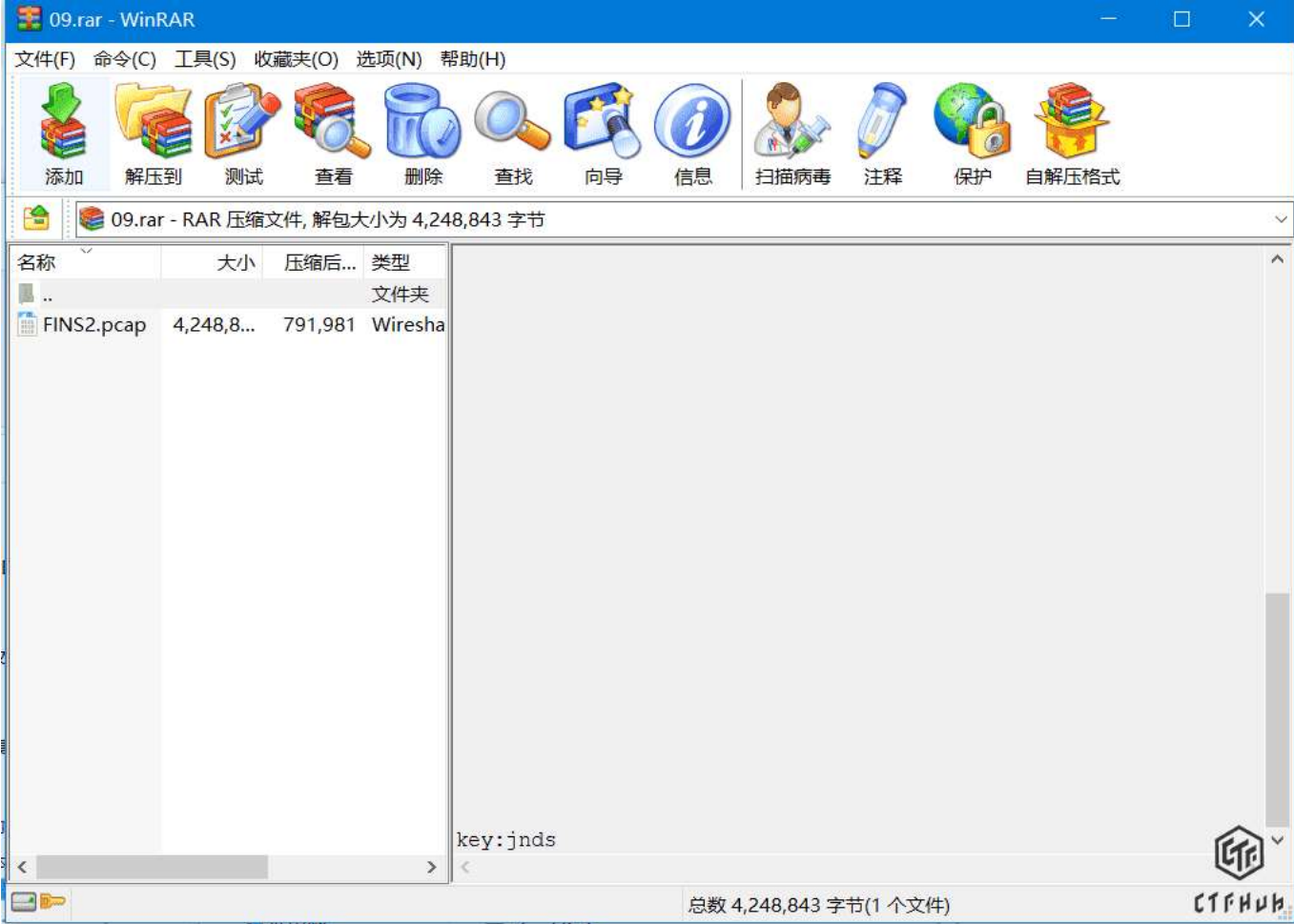
0020 00 5a 25 00 05 4d 00 00 0e 61 c5 a1 94 50 18 .Z...M...S...P.

0030 04 0c 5b 40 00 00 46 49 4e 53 00 00 03 f6 00 00 .Xb..FfNS.....

0040 00 02 00 00 00 c0 00 00 02 00 7b 00 00 00 57 .....W

0050 02 01 00 00 00 12 00 00 01 cd 00 00 00 00 00 .....  
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
01a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
01b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
01c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
01d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
01e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
01f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0230 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0250 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0260 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0270 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0280 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0290 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
02a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
02b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
02c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
02d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
02e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
02f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0310 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0320 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0330 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0340 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0350 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0360 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0370 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0380 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0390 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
03a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
03b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
03c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
03d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
03e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
03f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0400 64 47 56 6b 58 31 2f 62 57 53 5a 59 55 65 46 44 dGVuK1I/b W5ZYueFD  
0410 05 6f 6e 51 6b 4b 30 41 55 48 72 39 54 6d 37 49 eonQnK8A UIR9Tn7I  
0420 63 32 30 50 52 58 78 6c 50 76 6c 77 47 36 61 34 C2BR0XkL PwLw66A  
0430 66 51 3d 3d f0=

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

加密/解密

AES加密/解密

DES加密/解密

RC4加密/解密

Rabbit加密/解密

TripleDes加密/解密

MD5加密/解密

Base64加密/解密

Hash加密/解密

JS 加密

JS 解密

flag{J6voaW20VjnrS2}

jnds

密码是可选项，也就是可以不填。

< 解密

加密 >

U2FsdGVkX1/bWSZYUeFDeonQhK0AUHr9Tm7lc20PRXlPvIwG6a4fQ==

PayPal

PayPal

CTFHub

## Flag

```
1  flag{J6voaW20VjnrS2}
```

**本文作者：**CTFHub

**本文链接：**<https://writeup.ctfhub.com/Challenge/2021/工业信息安全技能大赛/线上赛-第一场/ckf7NEvr3fYBjwZmZWNm2M.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！

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

[< Modbus采集分析](#)

[Attack >](#)

© 2019 – 2022 ❤ CTFHub

由 [Hexo](#) & [NexT.Gemini](#) 强力驱动