

司机的身份

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](#) | [司机的身份](#)

[点击此处](#) 获得更好的阅读体验

WriteUp来源

来自MOIN战队

题目描述

小明是一个卡车公司的管理员，他需要知道其中一辆卡车司机的身份信息，你能帮他找出来吗？Flag格式为：flag{}

题目考点

- T808 协议
- 新约加密

解题思路

根据题目的提示信息，信息隐藏在司机信息中。

找到驾驶员身份信息采集上报报文，将报文内容复制出来。

将报文用T808软件进行解析，将驾驶员姓名复制出来，进行后续解析。

□

驾驶员身份信息采集上报的消息ID: 0x0702

起始字节	字段	数据类型	描述
0	驾驶员姓名长度	BYTE	
1	驾驶员姓名	STRING	驾驶员姓名, 长度n
1+n	驾驶员身份证编码	STRING	长度20位
21+n	从业资格证编码	STRING	长度40位
61+n	发证机构名称长度	BYTE	长度m
61+n+m	发证机构名称	STRING	从业资格证发证机构名称

主要分析在协议中驾驶员的信息，hint中有提示说想要获取驾驶员信息，所以这里只需要分析姓名等一些信息即可，正常人姓名一般不会有84位那么长，所以在流量中分析出协议即可看出端倪，

这里驾驶员姓名是16进制

```
1 8af896b850e7964d543d8af89640646996b850e77f3d85a9985876a4802876a4773e52ab963f621176a46167963f4ea676a4621154c6515c964d56a47957610d76a48fe695cd773e76a496404ea6805e5ba354a48fe
```

□

对16进制转换成字符串即可查看到新佛经密码。

```
1 諸緣僧降叶諸陀摩隸魯鉢薩願轉轉轉眾劫阿我轉慧阿亦轉我哆兜降摩祇瑟轉迦闍眾轉陀亦闍宜吃迦劫薩囉瑟闍須轉塞迦轉諱亦劫亦轉闍願轉吃修闍薩摩宜轉我苦苦轉迦闍諱婆亦闍轉阿薩所願如空如如囑轉囑
```

根据题目可知为佛经解密，但是在与佛论禅的网站解密失败

我们已知有两个版本的与佛论禅，所以猜测为新约

□

根据解密结果分辨为base64

□

发现满足base32的特征

□

Flag

```
1 flag{Crypy01sFuN}
```

- 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/f4HduEHWkwB6bnEEjCqj5.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](#)

[泄露的信号](#)

[工控协议数据分析](#)