flag在哪

发表于 2021-01-25 更新于 2021-02-17 分类于 Challenge ， 2019 ， 工业信息安全技能大赛 ， 哈尔滨站
Challenge | 2019 | 工业信息安全技能大赛 | 哈尔滨站 | flag在哪

点击此处获得更好的阅读体验

WriteUp来源

https://www.cnpanda.net/ctf/415.html

题目描述

> *某队在审核一起工业间谍案件中的邮件收发记录时，发现一张可疑图片，初步怀疑这张图片中隐藏了关键秘钥信息，你能找出隐藏的秘钥信息吗？找出的秘钥信息即为flag。*

题目考点

- *图片隐写*

解题思路

使用 binwalk查看图片，发现存在隐藏的 ZIP 文件，再使用 foremost 分离出来：

得到一个 PNG 图片和压缩包：

打开压缩包发现存在另一张图片，且需要解压密码

观察另一张图片发现存在残缺的条形码图文：

使用 PS 工具将其修复完整：

发现熊猫的颜色颠倒过来，因此对图片进行反相处理：

扫描可得到字符串：`This_n0t_fl4g`

使用该字符串解压刚才的压缩包，得到3.jpg文件，使用 binwalk 查看依旧存在 ZIP 文件，于是继续分离出来：

最终得到两个一模一样的图片，使用Stegsolve工具进行图片对比：

发现出现很多像素点，确定是像素隐写，保存该图片为：solved.bmp，发现和原图对比数据杂乱因此尝试使用像素隐写解密工具进行解密

GitHub 搜索尝试几个工具后，最终发现此工具可以成功解密：https://github.com/HFO4/HideByPixel

之后somd5解密即可

Flag

```
flag{this_is_fl4g_icsc-^_^}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2019/工业信息安全技能大赛/哈尔滨站/iVADyVy29t1WTEL2ZRSWZH.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 # 2019 # 工业信息安全技能大赛 # 哈尔滨站
神奇的数据
协议分析又来了