




CTF-隐写术-九连环 writeup

原创

湖zz  于 2019-07-16 11:13:49 发布  521  收藏 1

文章标签: [CTF 隐写术](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/zhz444614971/article/details/96114851>

版权

1.使用foremost对 123456cry.jpg 进行文件分离

foremost -i 传入的文件 -o 输出文件位置

得到:加密的 00000038.zip 文件

2.00000038.zip 这是个伪加密的zip

使用WinHex打开修改倒数第三个504B 里的0108 为0000

解压得到:good-宸插惜蹇.jpg 以及 qwe.zip两个文件

3.将 good-宸插惜蹇.jpg 改名为 good.jpg

打开可以看到是一张图片,因为qwe.zip的解压需要密码,图片中肯定包含密码

使用steghide去提取图片中的隐藏信息

steghide.exe extract -sf good.jpg

得到:ko.txt文件,文件中包含解压密码

4.解压qwe.zip文件

最终的得到flag.txt,里面包含flag