从CTF比赛真题中学习压缩包伪加密与图片隐写术

转载

士别三日wyx 于 2021-11-19 20:52:10 发布 10395 收藏 3
文章标签： linux 安全 运维
原文链接：https://admin-root.blog.csdn.net/article/details/115277128

先讲个笑话，刚刚打完`MAR DASCTF明御攻防赛`，一如往常，很轻松便拿到了两个`flag`（签到与问卷），哈哈，一个脑细胞都不用消耗

好了下面通过其中的一道misc题，一起学习一下伪加密与图片隐写的破解

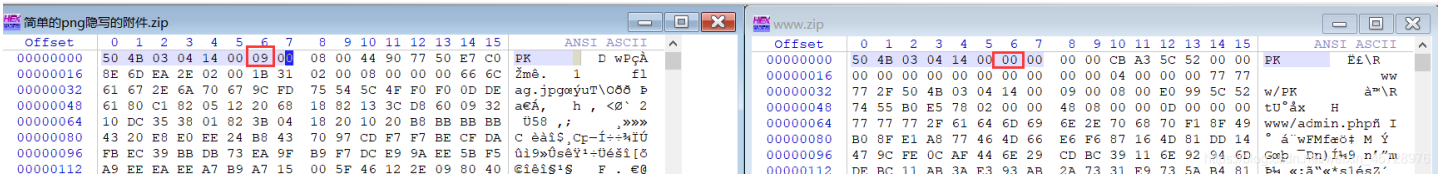
本文知识点：

- 遇到加密压缩文件怎么办？需要哪些工具
- 遇到图片隐写怎么办？需要哪些工具
- 十六进制数据还原文件

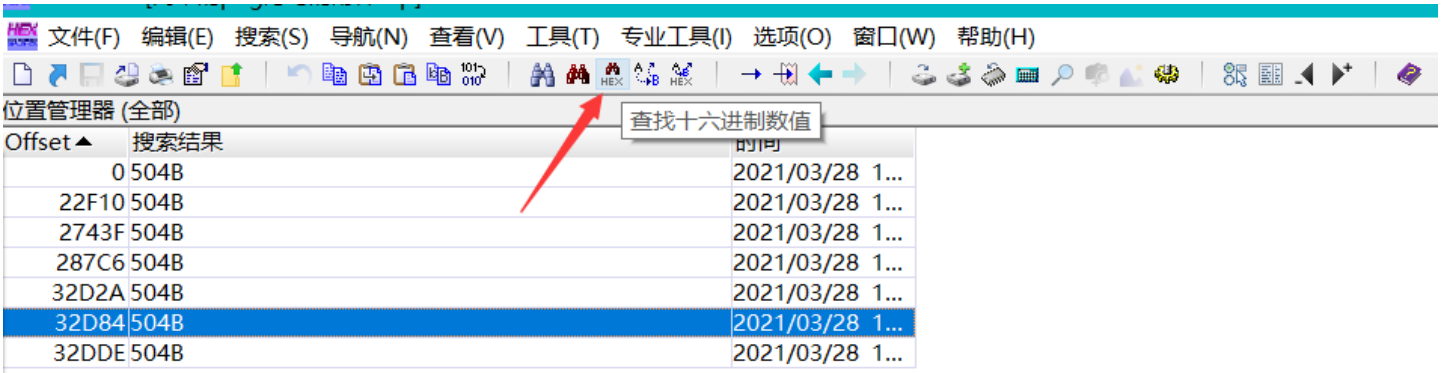
大佬就不用看了，全是小白操作

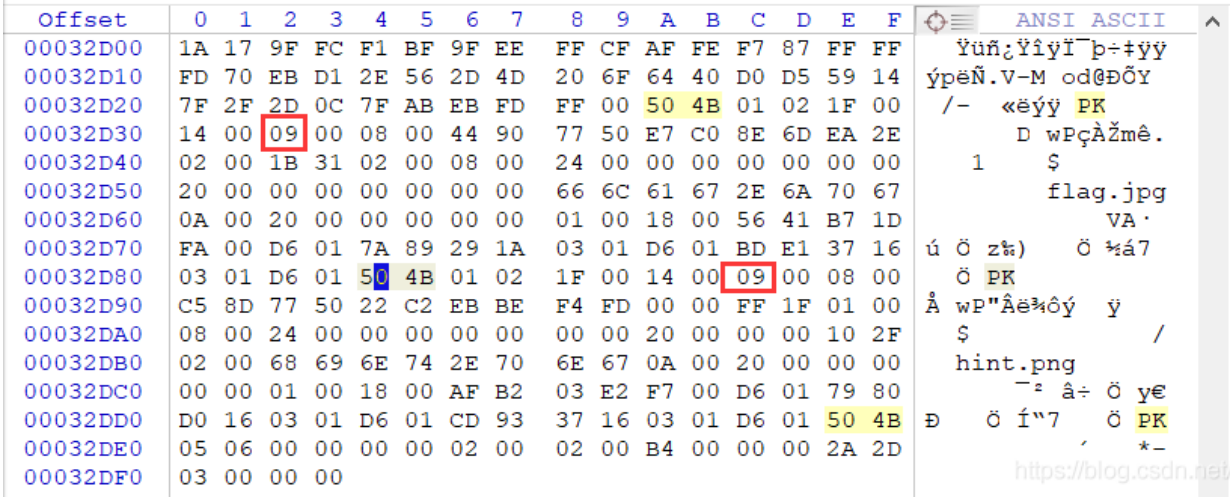
压缩包类的解题思路

如遇加密压缩包，在没有密码提示的情况下，先判断是不是伪加密
最简单的方法就是看十六进制数据，第一行如果有`09`多半就是了



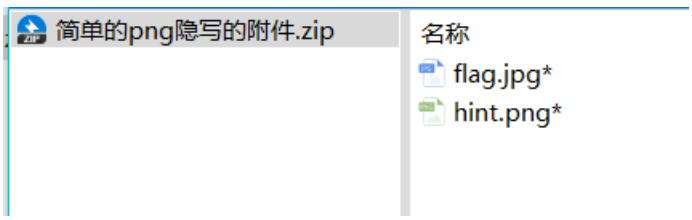
点击查找十六进制数值搜索`504B`，最后如果有`09`那基本就是了，改为`00`完活





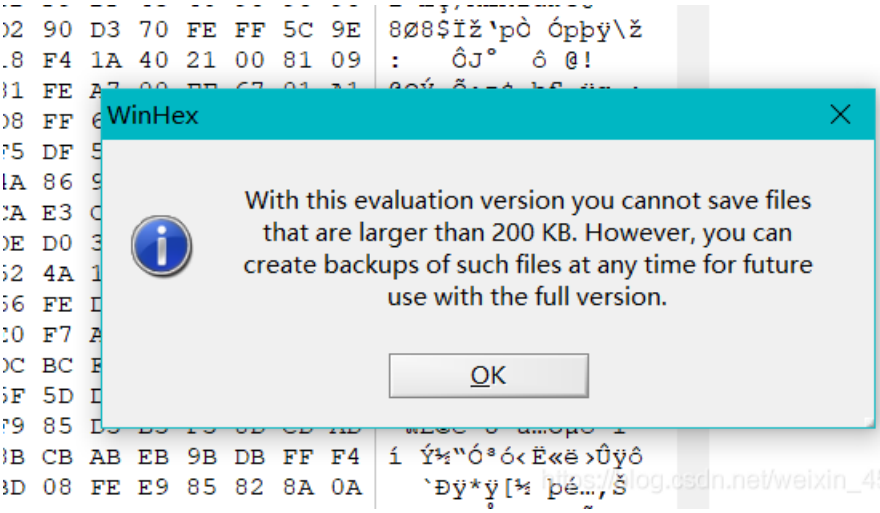
伪加密破解

比如这道misc题，结合了压缩包伪加密与图片隐写技术，我们就以它为例学习一下这两种常见技术的解决方法



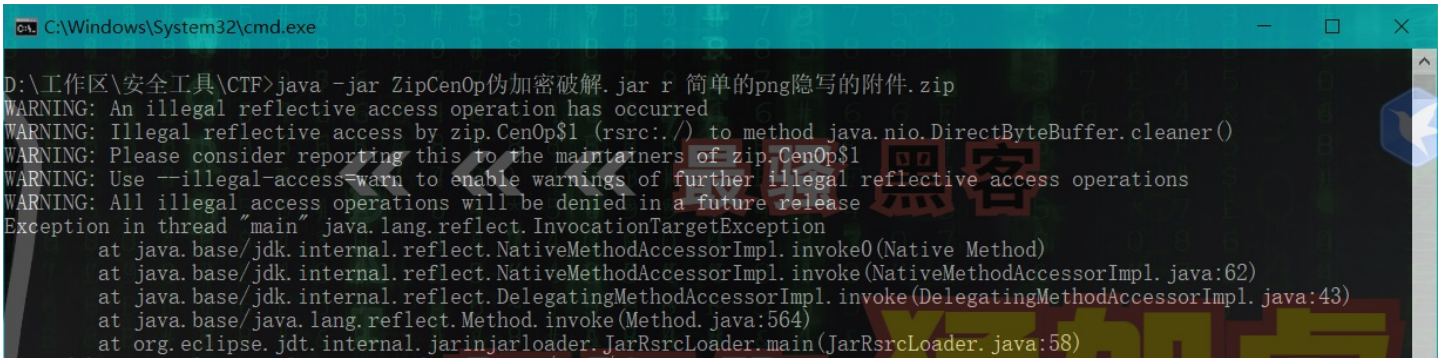
就是这个压缩文件，后面带`*`说明需要密码，但是题中没有任何密码提示，ctf中不可能让你无脑爆破，因为时间是有限的，但也有可能是弱口令，反正无从下手先爆破一下试试呗

当时我也想到了伪加密，用`WinHex`打开压缩包，将全局方位标记中的`09`改为`00`保存即可解除密码限制，这里有两个文件所以要改两处，但提示我试用版超过200kb不能保存，怎么回事，我记得是破解的啊



比赛结束后我才找到破解伪加密的工具——`ZipCenOp`

命令`java -jar ZipCenOp伪加密破解.jar r 简单的png隐写的附件.zip`



图片隐写破解

图片隐写的方式很多样，用到的工具也多，文件名已经提示的很明显了，是png隐写，所以朝着这方面想就行了

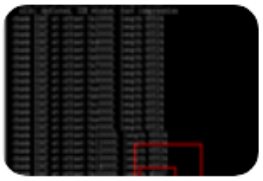
flag.jpg

hint.png

`binwalk` 和 `Stegsolve` 都没能找到什么有用的东西

所以百度一下，当当当，学到两个新工具 `pngcheck` 和 `TweakPNG`

PNG图片隐写IDAT分析(3)_tdcoming blog-CSDN博客_idat

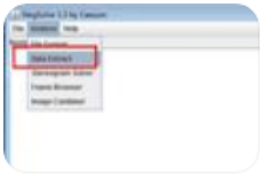


2018年8月20日 使用工具pngcheck命令:pngcheck.exe -v sctf.png 发现有个异常的IDAT 0X15aff7 一共提权138位。使用zlib进行压缩,代码如下: #! /usr/bin/env pythonimport zlib...

CSDN技术社区 百度快照

为您推荐: png图片隐写 pngcheck vim下一页 zlib是什么文件 idata知识检索 png隐写zlib nga f5隐写 图片隐写 png图片 github

PNG隐写model.png(1)_tdcoming'blog-CSDN博客_png隐写



2018年8月8日 这只是一道png的隐写题目,当看到png的图片进行隐写的时候,我们要去考虑IHDR隐写,和lsb的隐写。 0X00准备 实验工具Stegsolve 0X01实验操作 ...

CSDN技术社区 百度快照

Misc 总结 ---隐写术之图片隐写(二) - 先知社区

23条回复 - 发帖时间: 2017年12月24日

2017年12月24日 我们这里重点先了解一下,png图片文件头数据块以及png图片IDAT块,这次的隐写也是以这两个地方位基础的。 png...

xz.aliyun.com/t/1... 百度快照

隐写技巧——PNG文件中的LSB隐写 - 知乎

2016年12月2日 本文分别介绍如何通过Python和C++实现对PNG文件的LSB隐写,参照文中的分析思路也可对常见的LSB隐写数据进行提取分析。注:修改好的PNG_stego工程已上传至github: githu...

知乎 百度快照

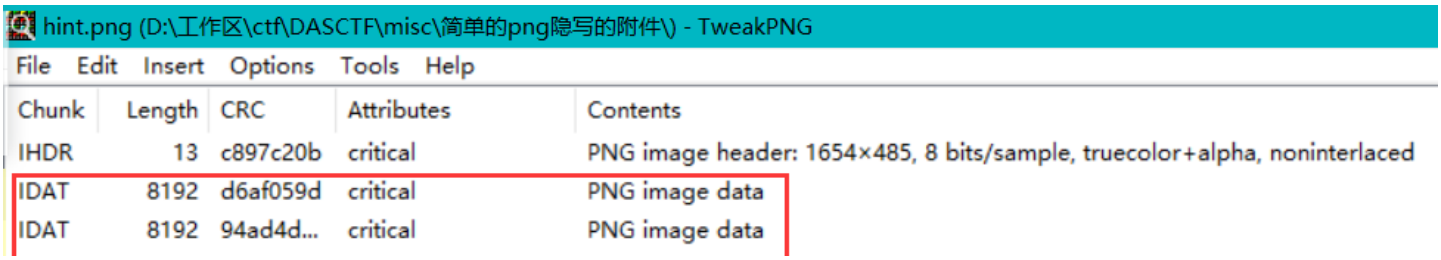
它们的功能是差不多的，只不过一个是命令行模式一个是图形化界面，但`pngcheck`可以识别多个图像类型，而另一个只能是`png格式`

pngcheck

Hacking Tools 1.31k 阅读

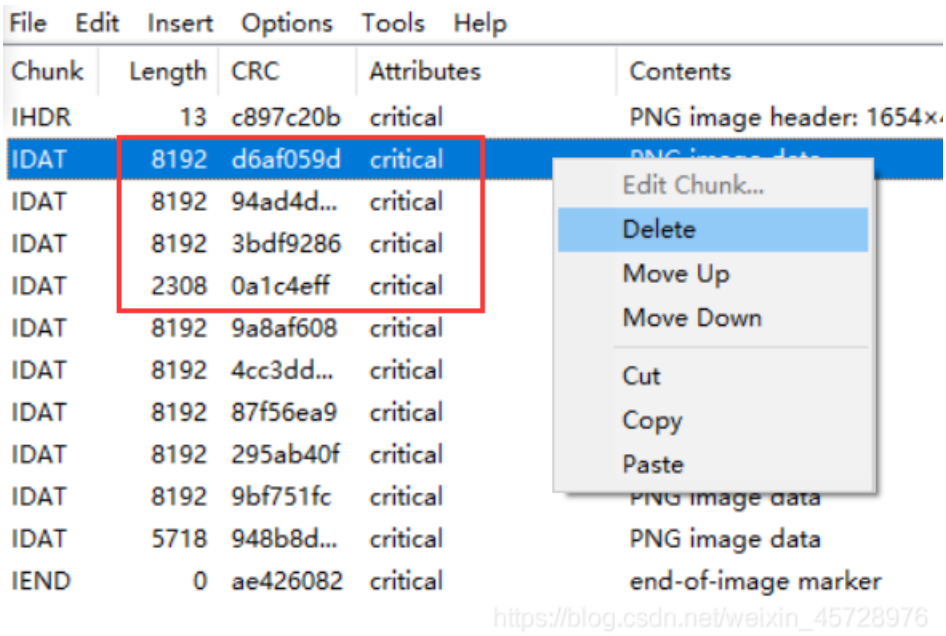
描述：通过检查CRC和解压缩图像数据来验证PNG、JNG和MNG文件的完整性。

复制一张`hint.png`然后用`TweakPNG`打开，可以看到两个`IDAT块`，正常的图片应该只有一条IDAT数据不同，而这里有两条不一样的，可以判断是两张图片

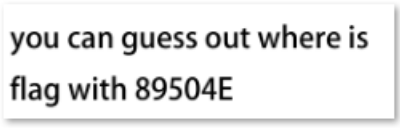


IDAT	8192	3bdf9286	critical	PNG image data
IDAT	2308	0a1c4eff	critical	PNG image data
IDAT	8192	9a8af608	critical	PNG image data
IDAT	8192	4cc3dd...	critical	PNG image data
IDAT	8192	87f56ea9	critical	PNG image data
IDAT	8192	295ab40f	critical	PNG image data
IDAT	8192	9bf751fc	critical	PNG image data
IDAT	5718	948b8d...	critical	PNG image data
IEND	0	ae426082	critical	end-of-image marker

右键将上面四条`Delete`，然后`Ctrl+s`保存



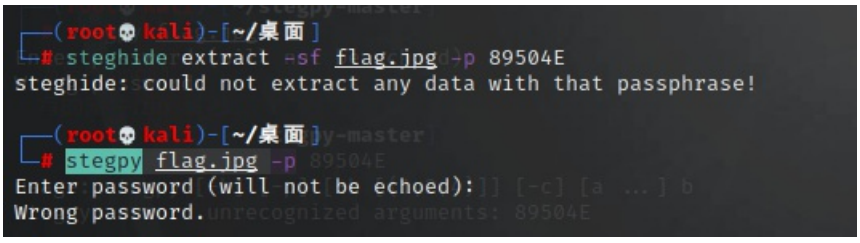
这样隐藏的图片就出来了，这句意思是`你可以用89504E猜出旗子在哪里`



hint - 副本.png

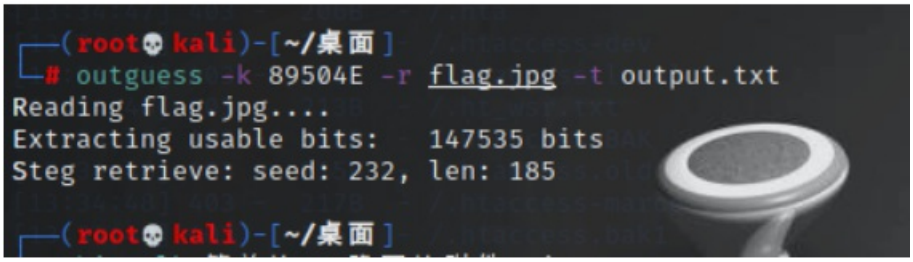
hint.png

`89504E`应该是个密码，而需要密码解图片隐写的工具有很多，如：`steghide`和`stegpy`，然而都没用，看了大佬的wp才知道用的是`outguess`，又学了一个工具

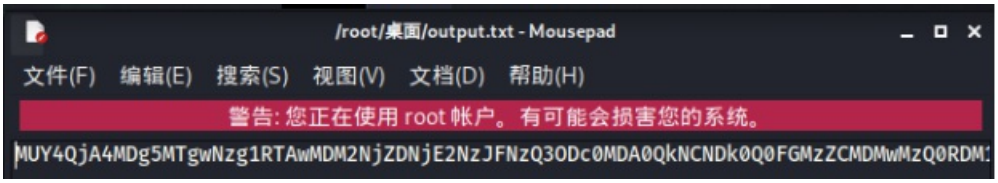


这个kali里是没有的，输入`apt install outguess`安装即可

用命令`outguess -k 89504E -r flag.jpg -t output.txt`导出加密内容



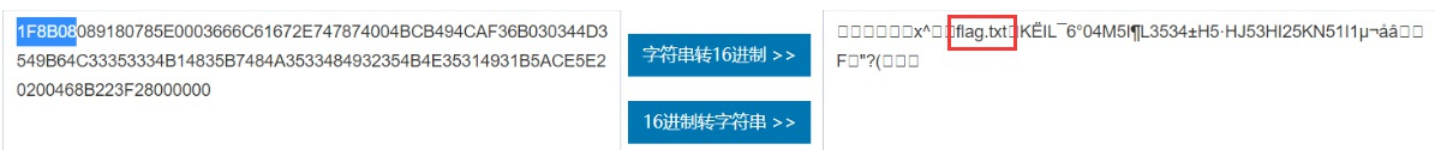
里面有一行编码字符，看着像`Base64`



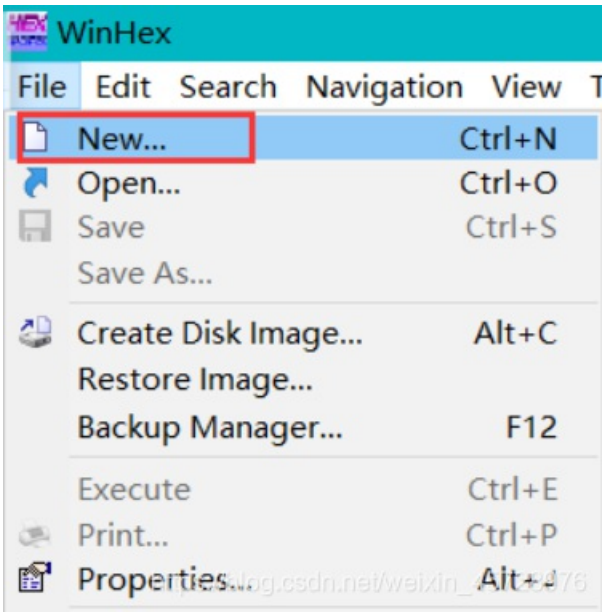
十六进制数据还原文件

解密得到一串好像十六进制的东西

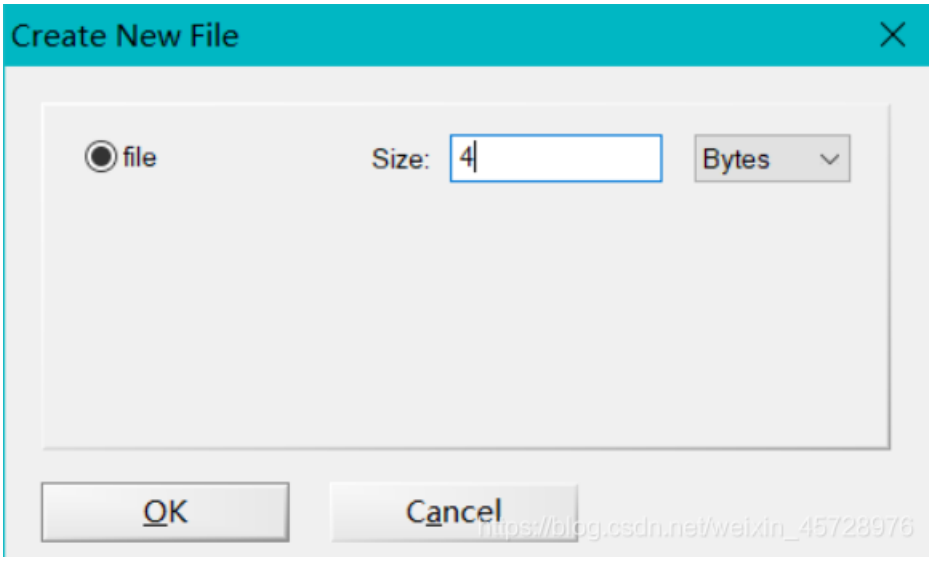
十六进制再转字符串发现有个`flag.txt`字样，有经验的已经想到了，这可能是个压缩文件，那怎样将十六进制数据变成文件呢？大神用的Python导出成文件，那咱这种菜鸡不会，只能用笨办法喽



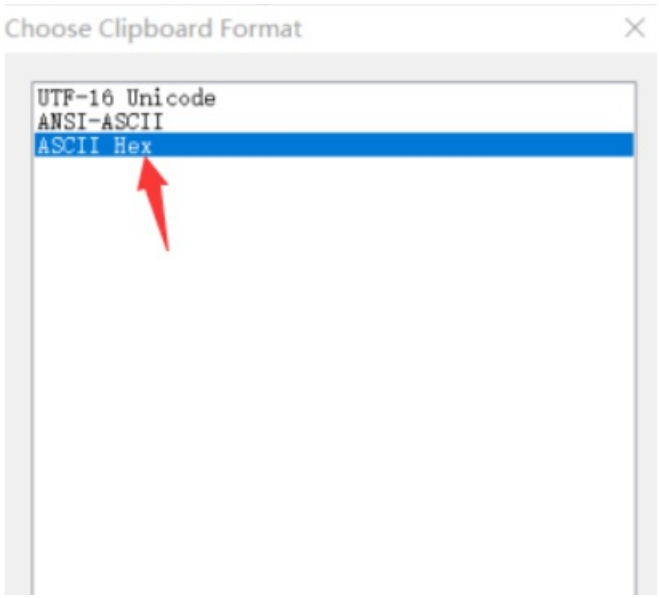
打开`WinHex`点击左上角新建

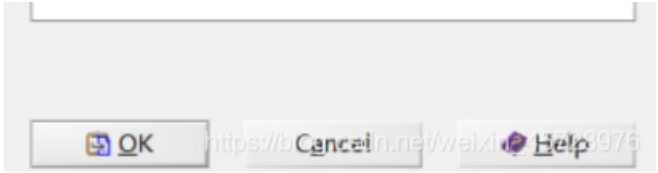


输入4个字符，OK

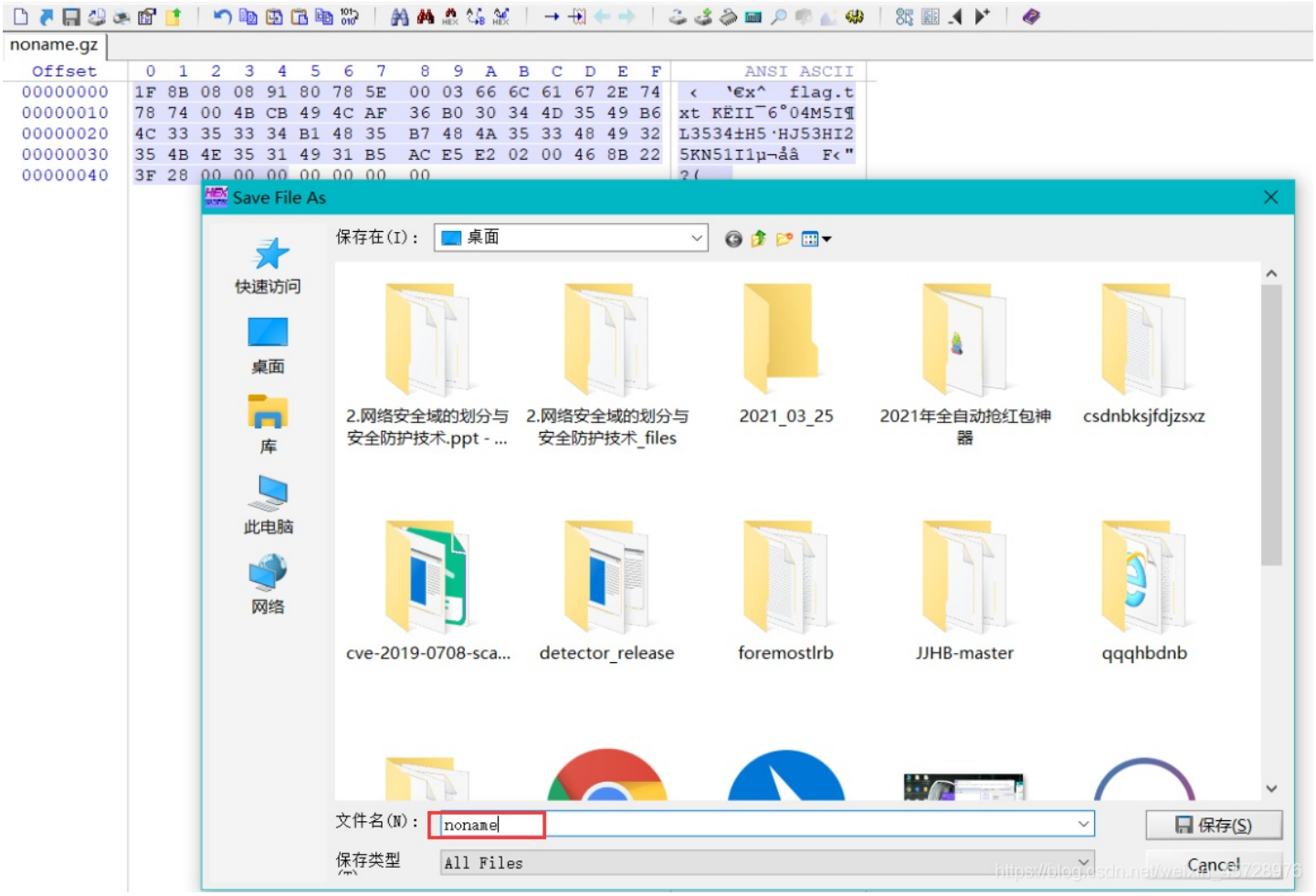


将十六进制字符粘贴进去，选择第三个

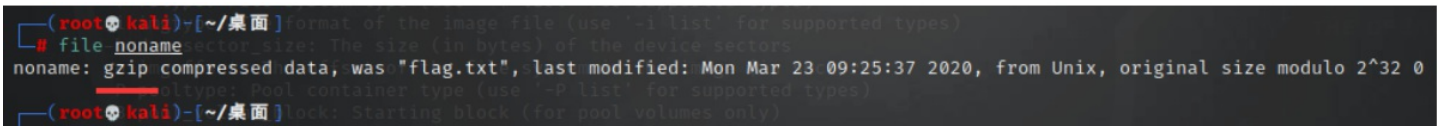




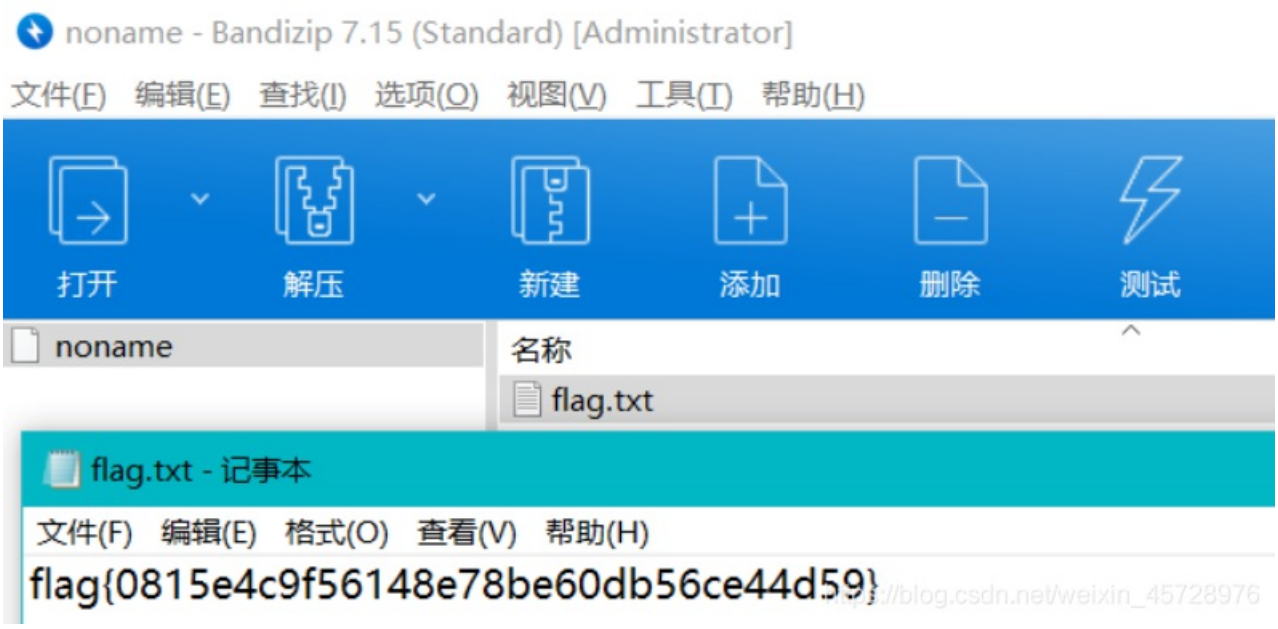
然后保存到桌面即可，其实现在这个文件可以用压缩软件直接打开



或者将后缀改为gz、zip都可以，假如你不知道这是什么文件，那就将它拖到Linux系统中用file命令验证一下



打开后flag就在txt文件中



看完你会发现其实这道题没有多难，只是很多工具我们不知道，没见过罢了，总之还是要多学多看，不要做井底之蛙

文章提到的工具都已打包，公众号回复“`CTF`”获取下载链接

参考文章：

- zip伪加密原理及操作
- [MAR DASCTF明御攻防赛] 个人（or团队）writeup

> 欢迎关注公众号，原创不易，转载请注明来源【爱国小白帽】


```
</article>
```