

实验吧——(stega)打不开的文件 writeup

原创

嗯哼哈嘿 于 2019-05-21 18:00:12 发布 158 收藏

分类专栏: [CTF](#) 文章标签: [CTF 实验吧 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/qq_39480875/article/details/90412020

版权



[CTF 专栏收录该内容](#)

16 篇文章 0 订阅

订阅专栏

题目链接: <http://ctf5.shiyanbar.com/423/stego/xx.gif>

可以先看我的另一篇博客https://blog.csdn.net/qq_39480875/article/details/90408674

下载下来的gif打不开。

- 1.查看文件属性的详细信息, 没有发现隐藏的信息。
- 2.使用010editor 打开gif文件查看文件的结构(开始标志和结束标志)

开始标志:

```
启动 x 打不开的文件.gif x 打不开的文件2.gif
编辑为: 十六进制(H) 运行脚本 运行模板
0000h:  B9 61 C2 01 52 01 F7 FF 00 ED ED EC F7 F7 F7 9C 9aÂ.R.÷ÿ.íì÷÷÷œ
```

结束标志:

```
B420h:  35 87 94 49 68 94 4B C9 94 4D A9 8C 01 01 00 3B 5+”Ih”KÉ”Mœ...;
```

正常的开始标志和结束标志为:

gif图像开始标志: 47 49 46 38 39 61 (GIF89)结束标志: 01 01 00 3B

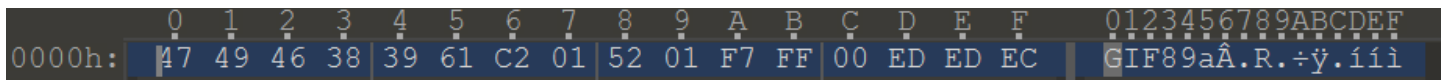
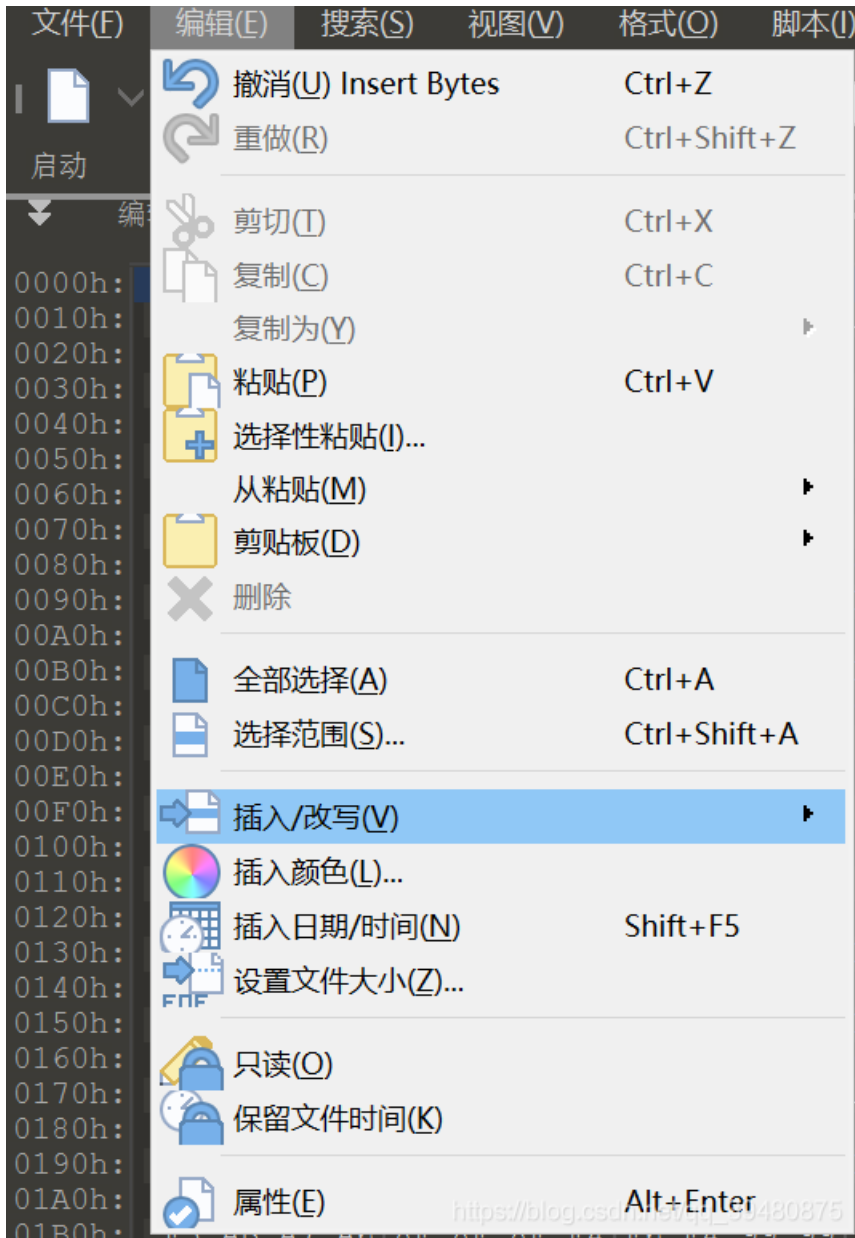
题目的gif图像的结束标志正常, 问题出现在开始标志

于是我刚开始尝试修改开始标志:

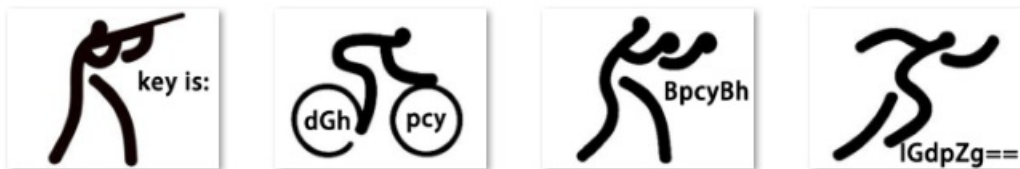
```
编辑为: 十六进制(H) 运行脚本 运行模板
0000h:  47 49 46 38 39 61 C2 01 00 ED ED EC F7 F7 F7 9C GIF89aÂ..íì÷÷÷œ
```

这样修改的结果还是打不开gif文件。

后来我自己查看原来文件的开始标志，发现他是39 61开头，于是我尝试插入4字节：



这样保存后的gif就可以打开了。我们可以看到



但这个还是base64加密过的，需要进行解密才能得到flag。