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

本文链接：https://blog.csdn.net/qq_39480875/article/details/90412020

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

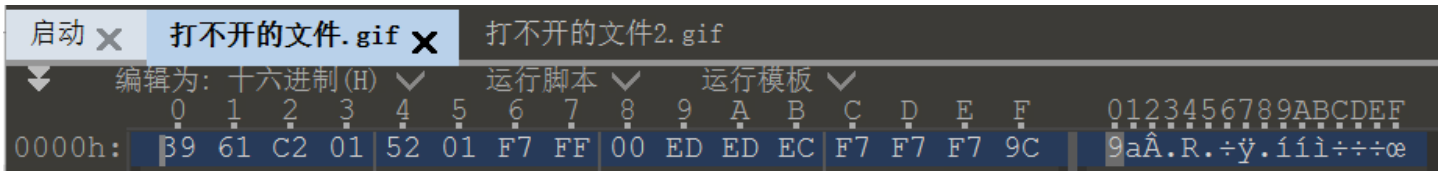
可以先看我的另一篇博客https://blog.csdn.net/qq_39480875/article/details/90408674

下载下来的gif打不开。

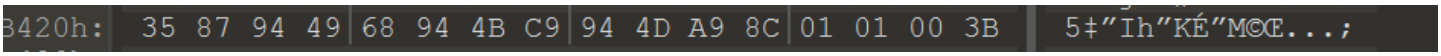
1.查看文件属性的详细信息，没有发现隐藏的信息。

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：



结束标志：

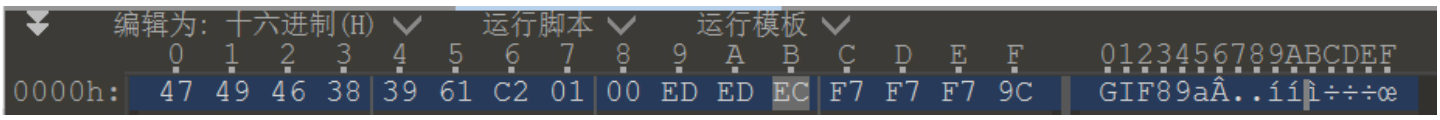


正常的开始标志和结束标志为：

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

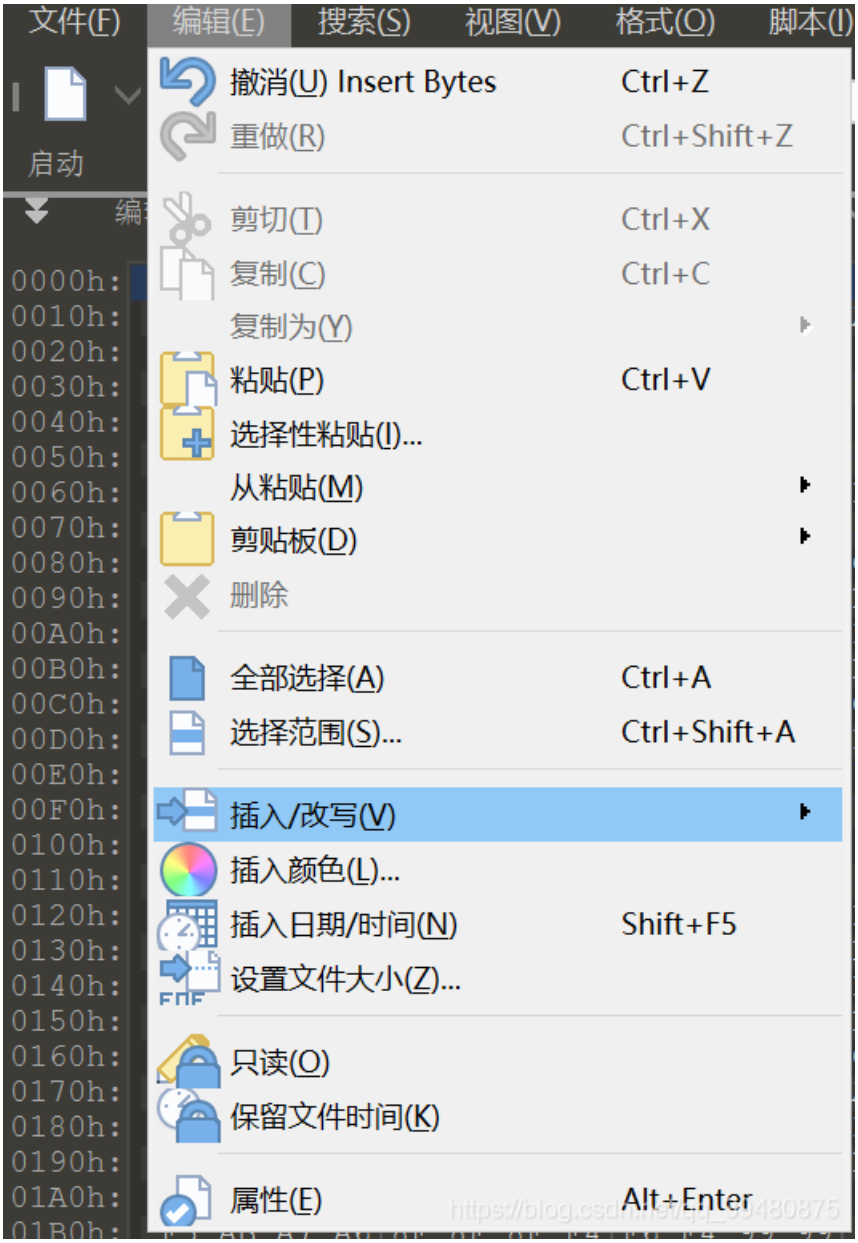
题目的gif图像的结束标志正常，问题出现在开始标志

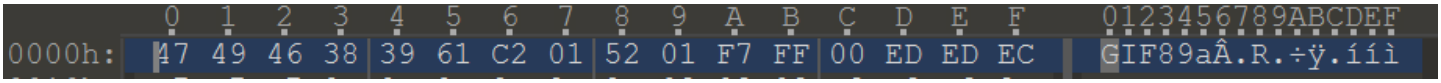
于是我刚开始尝试修改开始标志：



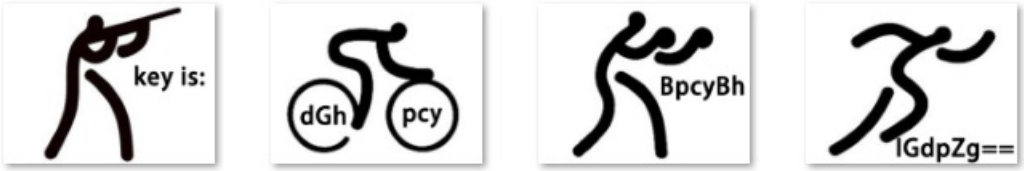
这样修改的结果还是打不开gif文件。

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。