攻防世界Misc入门题之SimpleRAR

原创

沐一 · 林 于 2021-08-18 16:16:14 发布 94 收藏

分类专栏： CTF 杂项 文章标签： unctf

本文链接：https://blog.csdn.net/xiao__1bai/article/details/119781695

CTF 同时被 2 个专栏收录

167 篇文章 6 订阅

订阅专栏

杂项

19 篇文章 0 订阅

订阅专栏

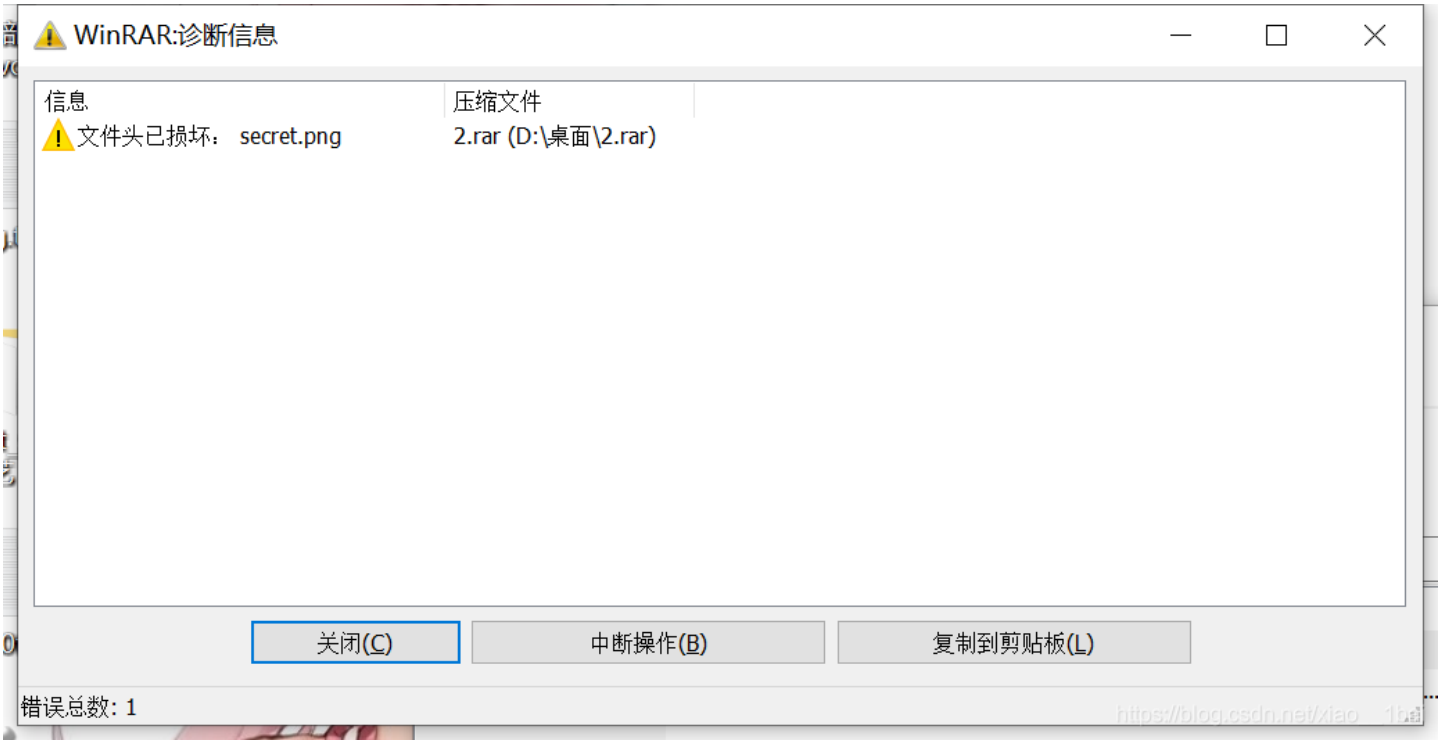
攻防世界Misc入门题之SimpleRAR

继续开启全栈梦想之逆向之旅~

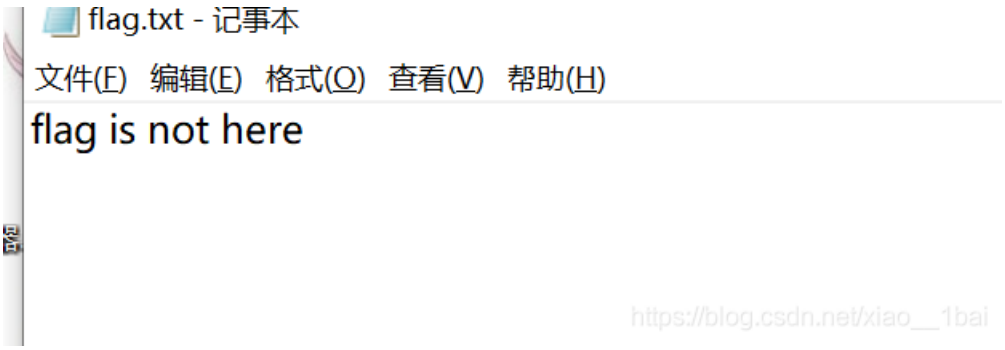
这题是攻防世界Misc入门题之SimpleRAR

我一直很讨厌做二维码拼接类的题，真的，每次都要拼好久~

下载了个RAR压缩包，压缩包解压不开，提示损坏了，第一个考点就是压缩包的文件结构错误，导致解压不了secret.png，只解压出了flag.txt：



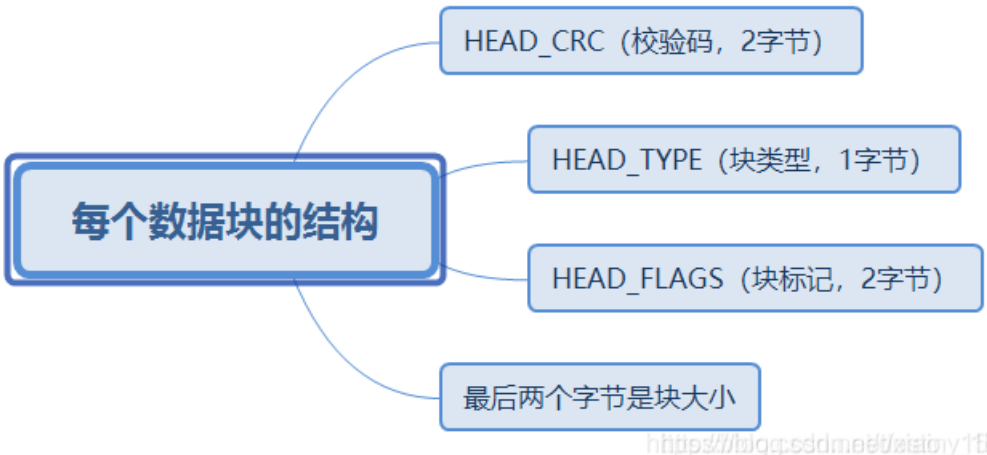
flag.txt打开后里面还是啥都没有的：



然后查资料，一篇看上去是软妹的好博客：

```
https://blog.csdn.net/destiny1507/article/details/89928234
```

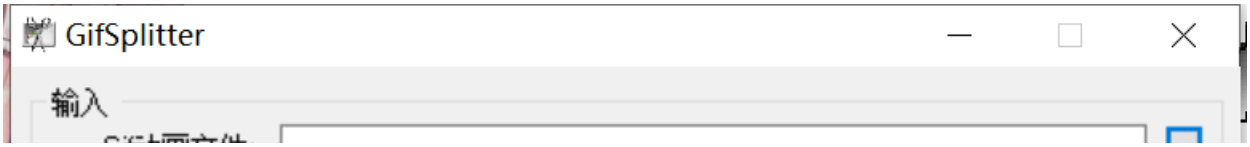
根据她的思维导图：

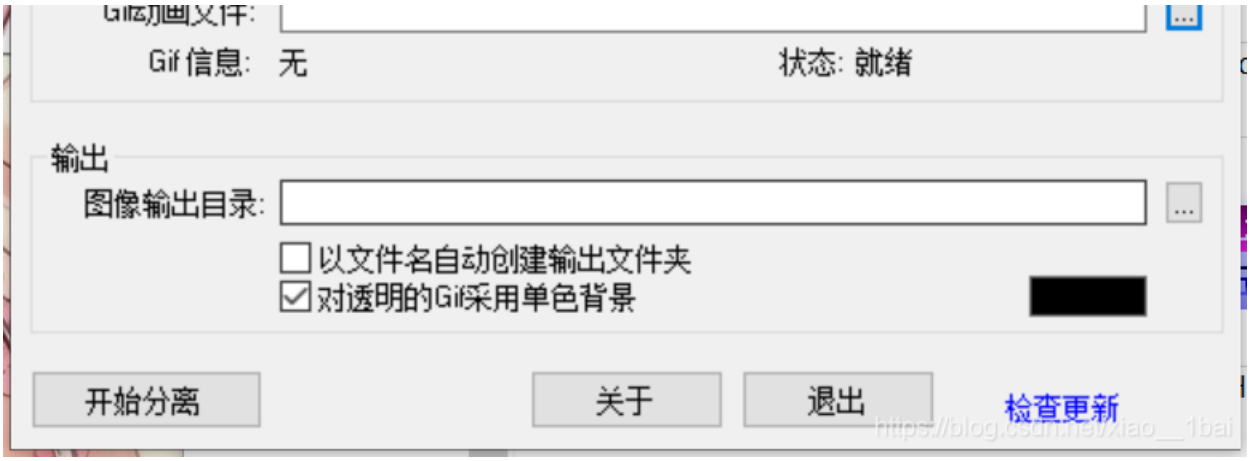


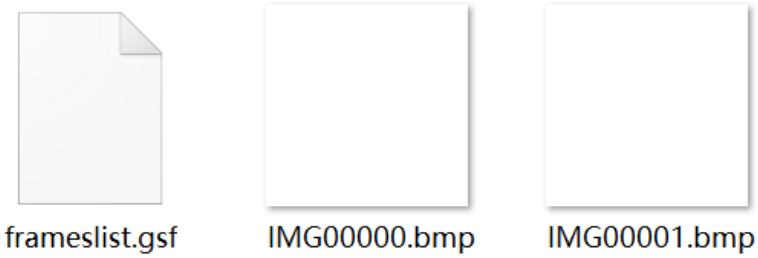
把压缩包扔入winhex64中，在secrypt.png的头部看到一个7A，表明是子块，改为74，作为一个独立文件即可解压。

```
7 00 43 66 6C  61 |  flag.txt °W Cfla
2 65 A8 3C 74  20 | g is not here¨<t
2 BC E9 8C 2F  6E |  / :   B    ¼éŒ/n
3 65 63 72 65  74 | ..OK 3      secret
```

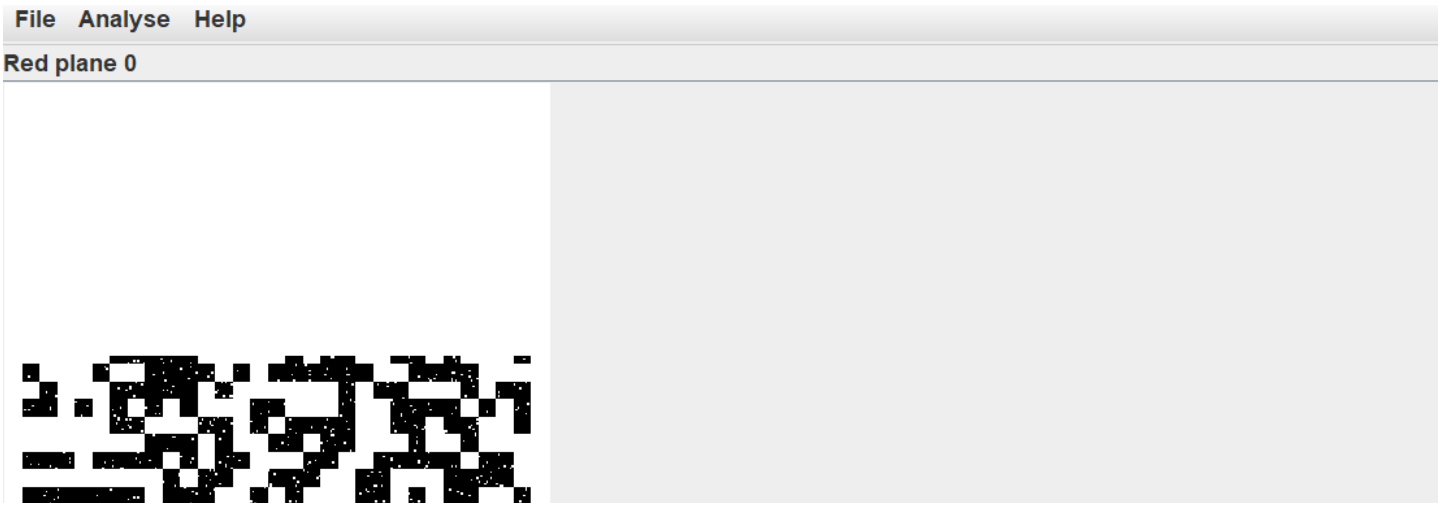
解压后是一个空白的gif图，题目暗示说是双层图，一开始我还以为层是指gif图的桢数，因为刚好也是两桢。后来发现不是的，层图的后缀是bmp，因为不想用ps，太大了，所以用了gifsplitter2.0图层剥离工具：







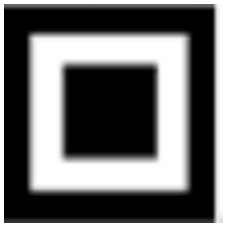
然后又学了Stegsolve的操作，导入图片，按下面的>不断单层显示颜色位平面，找出被隐藏的图片，如图，分别是两个残缺的上下部分二维码：



File Analyse Help

Red plane 0

照例用windows自带的3D画图拼接，补全定位图即可：



扫码即可得flag，吐槽一下，我是怎么拼接的呢，我不会合并，我也不知道其他人是怎么不用PS合并的，我用3D的截图截出只剩上半身的二维码：

然后在3D中用插入方法拖拉到下半部分中去,定位符也是插入后拖拉的,注意定义符要与内容二维码保持两边空行才行,不然扫不了的,我就是很难掌握这个空行的大小尺寸,才一直觉得难做。
唉~说多了都是泪。

总结：

> 1：压缩包解压不开，提示损坏了，第一个考点就是压缩包的文件结构错误，导致解压不了secret.png，只解压出了flag.txt：

> 2：解压后是一个空白的gif图，题目暗示说是双层图，一开始我还以为层是指gif图的桢数，因为刚好也是两桢。后来发现不是的，层图的后缀是bmp，因为不想用ps，太大了，所以用了gifsplitter2.0图层剥离工具：

> 3： 然后又学了Stegsolve的操作，导入图片，按下面的>不断单层显示颜色位平面，找出被隐藏的图片，如图，分别是两个残缺的上下部分二维码：

> 4：在3D中用插入方法拖拉到下半部分中去,定位符也是插入后拖拉的,注意定义符要与内容二维码保持两边空行才行,不然扫不了的,我就是很难掌握这个空行的大小尺寸,才一直觉得难做。

解毕！敬礼！