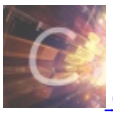
【XCTF 攻防世界】MISC 杂项 新手练习区 SimpleRAR

原创

Kal1 于 2020-08-05 23:59:59 发布 1064 收藏 2

分类专栏： CTF刷题 杂项 文章标签： 信息安全 zip 安全

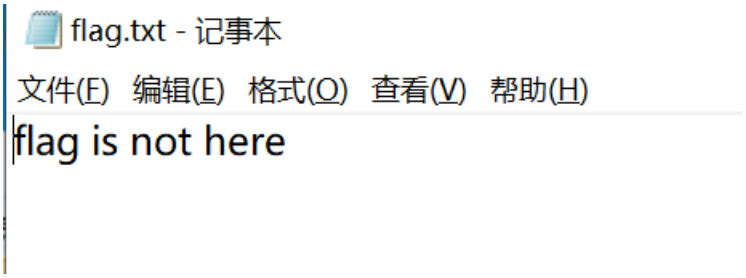
本文链接：https://blog.csdn.net/weixin_45844670/article/details/107828191



题目入口：https://adworld.xctf.org.cn/task/answer?type=misc&number=1&grade=0&id=5102&page=1

下载附件，得到一个rar压缩包，用2345好压和7z打开都是只有一个flag.txt文件

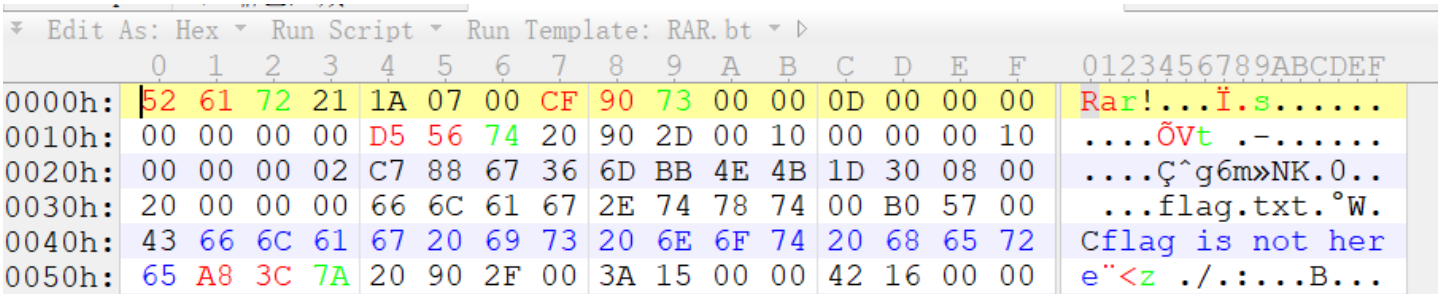
但是flag里面并没有flag



插一句：看到别人wp里面写的，用WinRAR好像可以直接识别一个破损文件（secret.png）但是无法打开。我由于没有下载WinRAR就用kali解压，给我报错，说该压缩文件中有一个破损文件无法打开

回归正题

既然只给了压缩包，说明肯定是压缩包出了问题，用010EDitor打开该压缩包（用notepad++，winhex或者vscode打开都可以，不过vscode需要插件hexdump）果然发现有一个文件

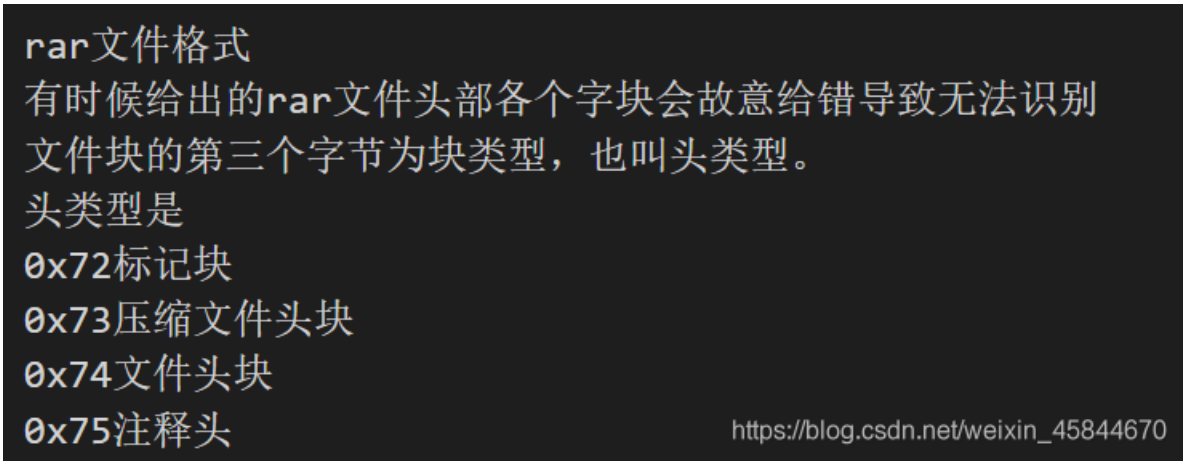


```
0060h: 02 BC E9 8C 2F 6E 84 4F 4B 1D 33 0A 00 20 00 00  .¼éŒ/n„OK.3.. ..
0070h: 00 73 65 63 72 65 74 2E 70 6E 67 00 F0 40 AB 18  .secret.png.ð@«.
0080h: 11 C1 11 55 08 D1 55 80 0D 99 C4 90 87 93 22 19  .Á.U.ÑU€.™Ä.‡"".
0090h: 4C 58 DA 18 B1 A4 58 16 33 83 08 F4 3A 18 42 0B  LXÚ.±¤X.3ƒ.ô:.B.
00A0h: 04 05 85 96 21 AB 1A 43 08 66 EC 61 0F A0 10 21  ....–!«.C.fìa. .!
00B0h: AB 3D 02 80 B0 10 90 C5 8D A1 1E 84 42 B0 43 29  «=.€°..Å.¡.„B°C)
00C0h: 08 10 DA 0F 23 99 CC F3 9D C4 85 86 67 73 39 DE  ..Ú.#™Ìó.Ä…†gs9Þ
00D0h: 47 63 91 DE C4 77 ED A8 DC 46 F4 C5 54 CD 55 6A  Gc'ÞÄwí¨ÜFôÅTÍUj
00E0h: AA A3 5E CD 6E 77 3B 8D EE 7A 99 A9 A9 8E D5 3E  ª£^ÍnwÌ;.îz™©©.Õ>
```

Template Results - RAR.bt

Name	Value	Start	Size	Color	Comment
struct RarBlock Ma…		0h	7h	Fg: Bg	
struct RarBlock Ar…		7h	Dh	Fg: Bg	
struct RarBlock bl…		14h	3Dh	Fg: Bg	
struct RarBlock bl…		51h	1569h	Fg: Bg	
struct RarBlock bl…		15BAh	7h	Fg: Bg	

果然，修改了文件头，我们无法识别



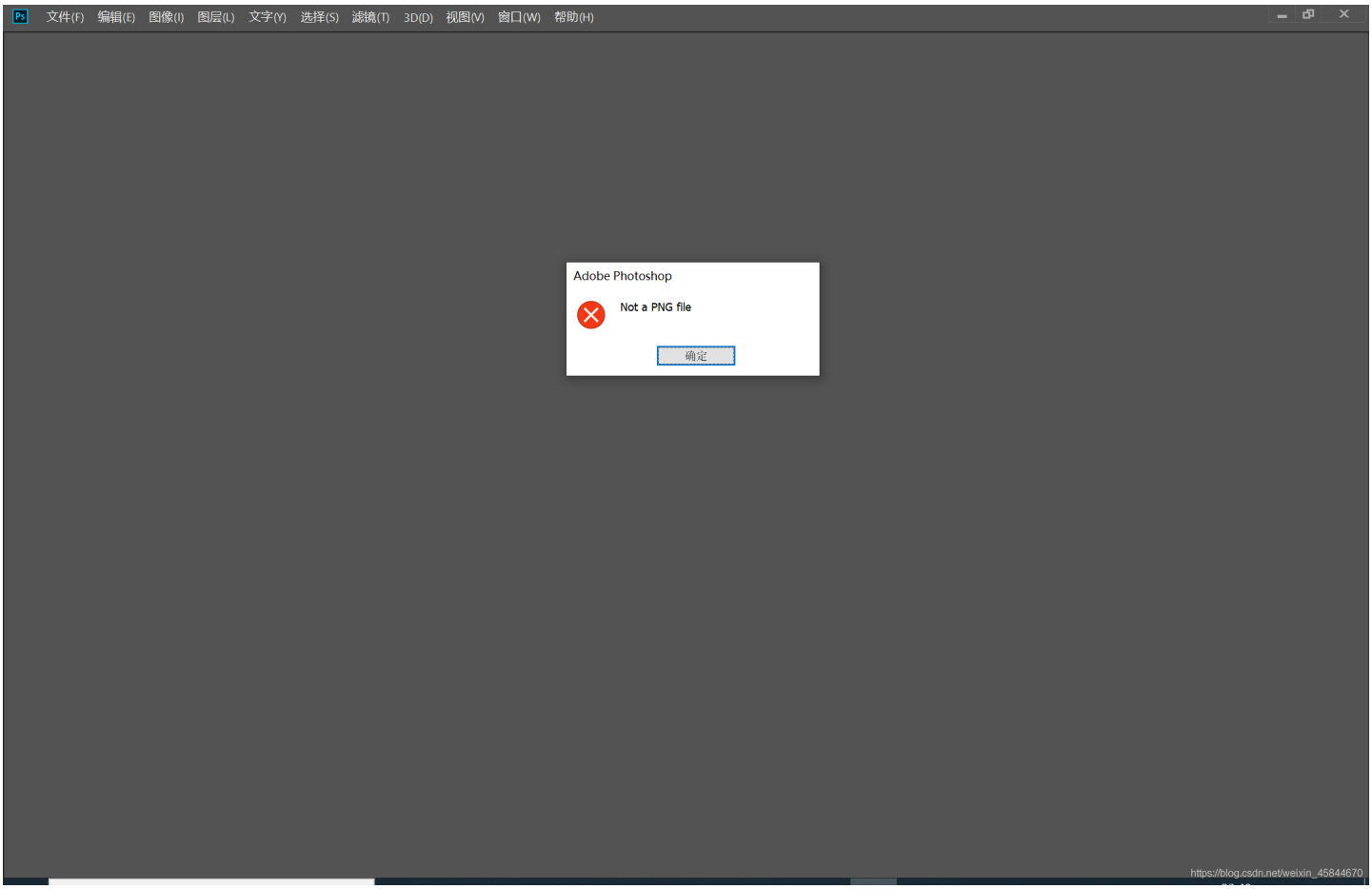
相关知识如下:

我们把0050h那一行第三个字节改为74，保存

```
      0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
0000h: 52 61 72 21 1A 07 00 CF 90 73 00 00 0D 00 00 00  Rar!...Ï.s......
0010h: 00 00 00 00 D5 56 74 20 90 2D 00 10 00 00 00 10  ....ÕVt .-......
0020h: 00 00 00 02 C7 88 67 36 6D BB 4E 4B 1D 30 08 00  ....Çˆg6m»NK.0..
0030h: 20 00 00 00 66 6C 61 67 2E 74 78 74 00 B0 57 00  ...flag.txt.°W.
0040h: 43 66 6C 61 67 20 69 73 20 6E 6F 74 20 68 65 72  Cflag is not her
0050h: 65 A8 3C 74 20 90 2F 00 3A 15 00 00 42 16 00 00  e¨<t ./.:...B...
0060h: 02 BC E9 8C 2F 6E 84 4F 4B 1D 33 0A 00 20 00 00  .¼éŒ/n„OK.3.. ..
0070h: 00 73 65 63 72 65 74 2E 70 6E 67 00 F0 40 AB 18  .secret.png.ð@«.
0080h: 11 C1 11 55 08 D1 55 80 0D 99 C4 90 87 93 22 19  .Á.U.ÑU€.™Ä.‡"".
0090h: 4C 58 DA 18 B1 A4 58 16 33 83 08 F4 3A 18 42 0B  LXÚ.±¤X.3ƒ.ô:.B.
00A0h: 04 05 85 96 21 AB 1A 43 08 66 EC 61 0F A0 10 21  ....–!«.C.fìa. .!
00B0h: AB 3D 02 80 B0 10 90 C5 8D A1 1E 84 42 B0 43 29  «=.€°..Å.¡.„B°C)
00C0h: 08 10 DA 0F 23 99 CC F3 9D C4 85 86 67 73 39 DE  ..Ú.#™Ìó.Ä…†gs9Þ
00D0h: 47 63 91 DE C4 77 ED A8 DC 46 F4 C5 54 CD 55 6A  Gc'ÞÄwí¨ÜFôÅTÍUj
00E0h: AA A3 5E CD 6E 77 3B 8D EE 7A 99 A9 A9 8E D5 3E  ª£^ÍnwÌ;.îz™©©.Õ>
```

再打开，果然可以了

打开PS，准备搞活，**却被告知**



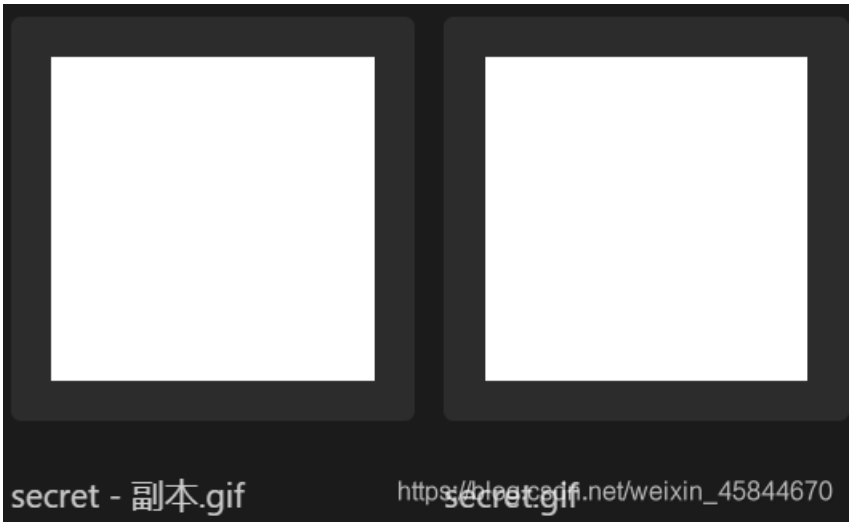
打开Linux终端，发现是gif文件

```
λ file secret.png
secret.png: GIF image data, version 89a, 280 x 280
```

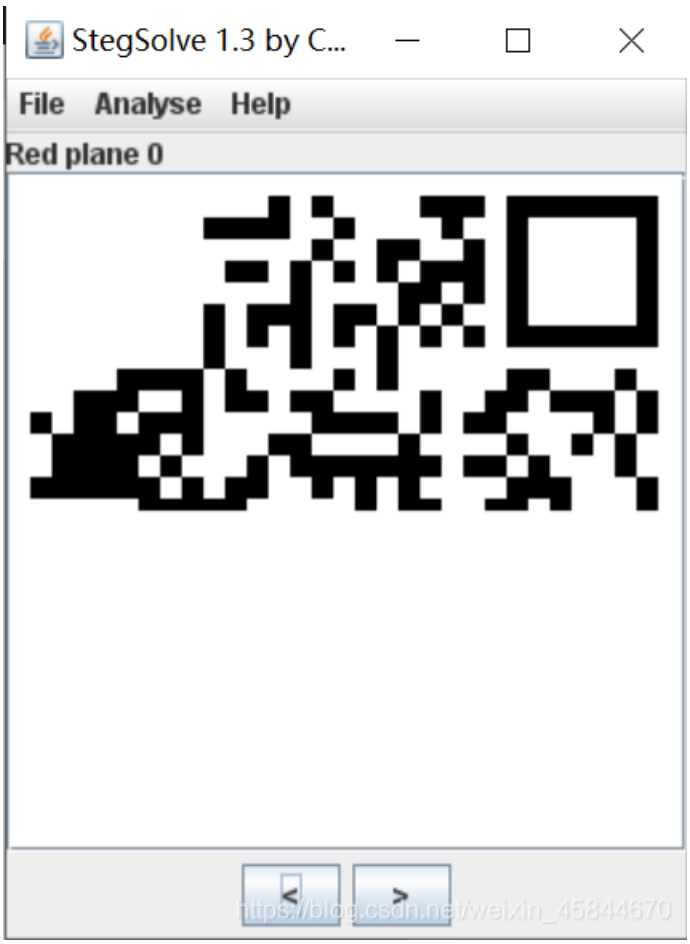
修改后缀后，再用PS打开，发现有两个图层，由于题目给提示

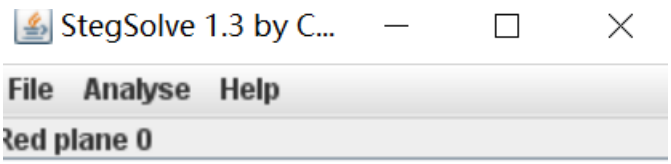
```
菜狗最近学会了拼图，这是他刚拼好的，可是却搞错了一块(ps:双图层)
```

我打算把两个图层分开保存



然后用Stegsolve打开，看看有什么发现





果然各自是一半二维码

用画图合并，并且补充完整二维码定位区

扫描得到flag

这也太绕弯了。。。。。。。。。