XCTF-MISC-新手区-SimpleRAR

原创

1stPeak 于 2021-06-18 16:33:29 发布 72 收藏

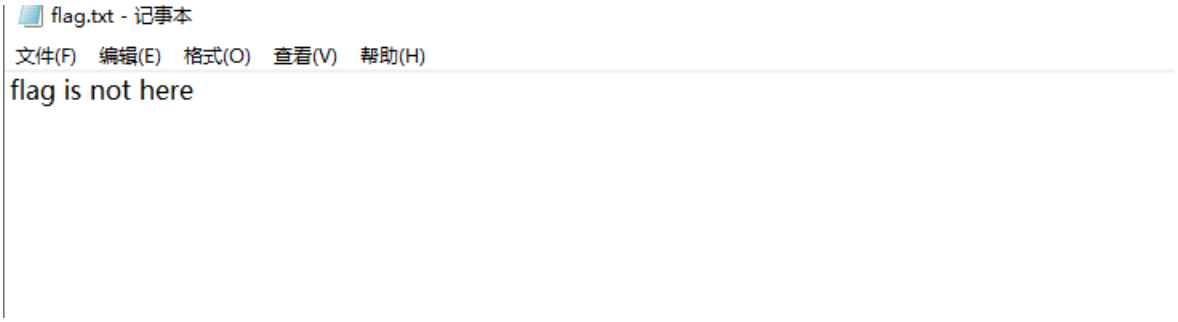
分类专栏： CTF刷题 文章标签： XCTF

本文链接：https://blog.csdn.net/qq_41617034/article/details/118028248

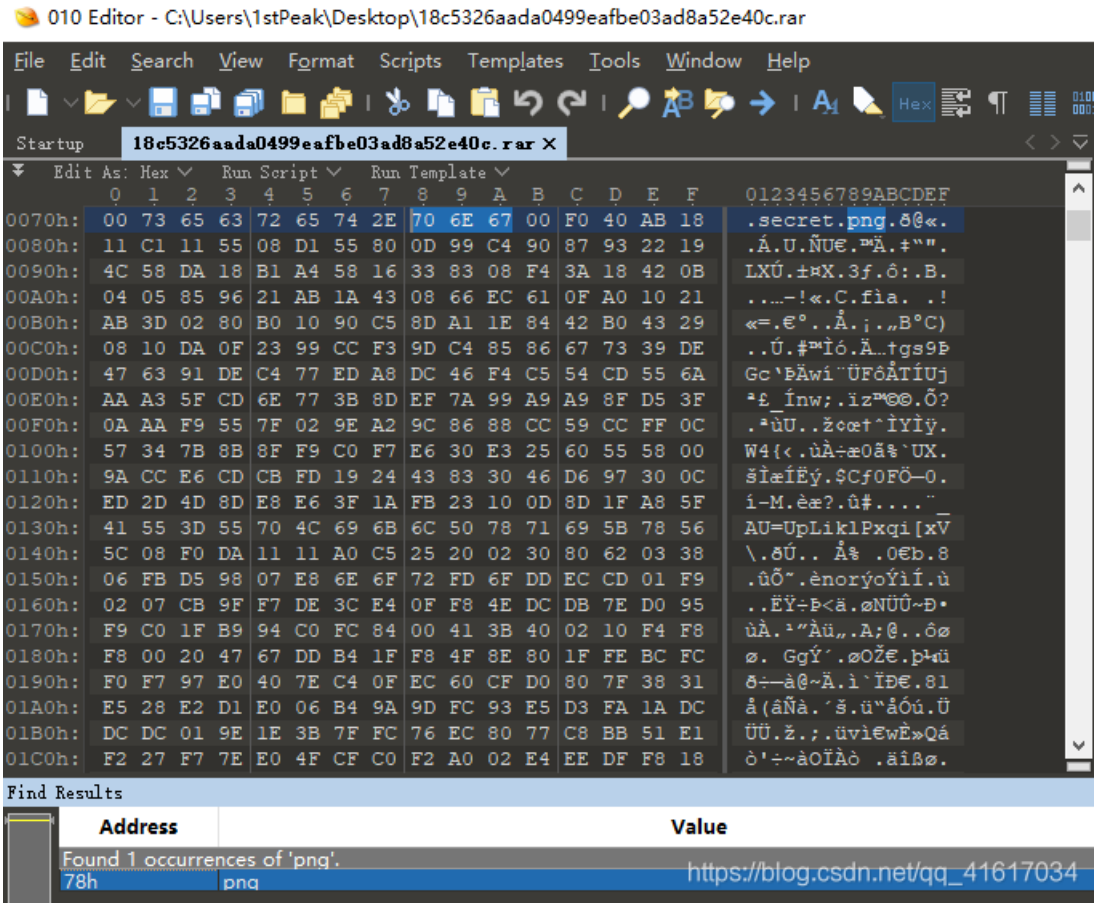
题目

解题思路

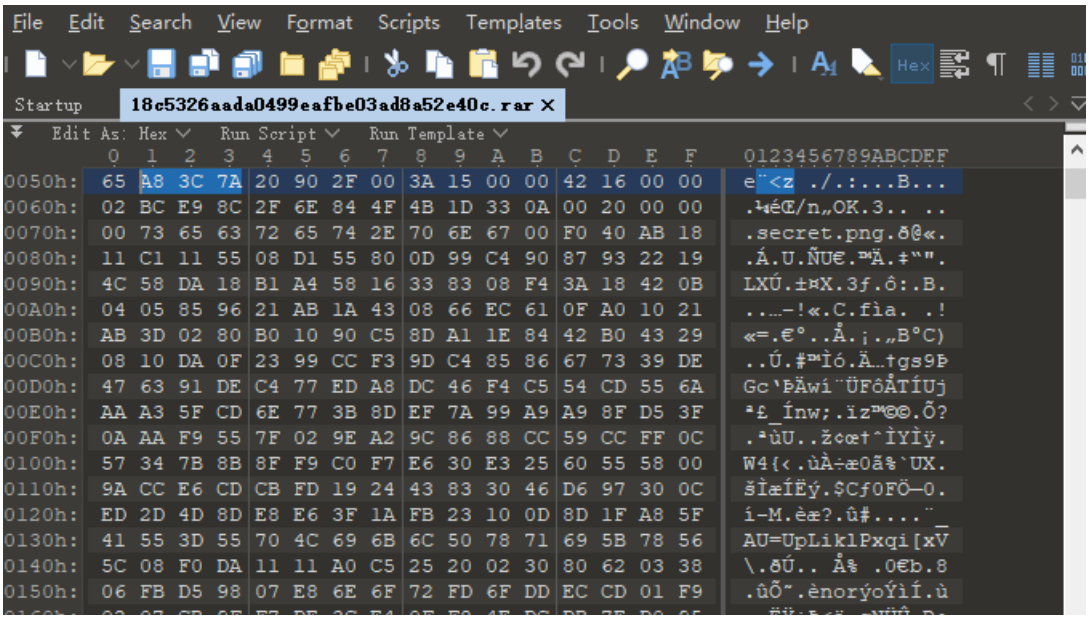
1、将附件解压

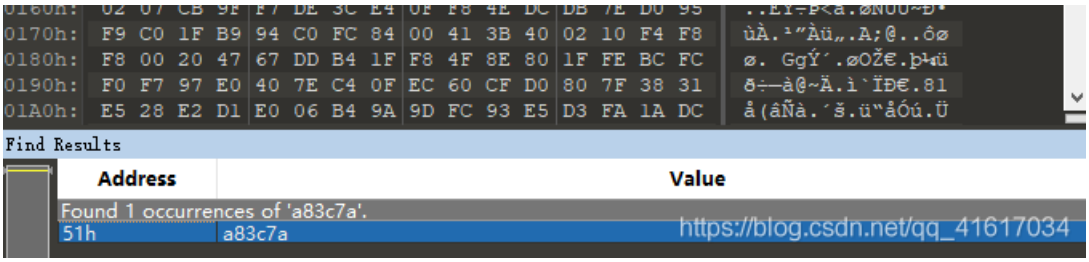


2、用010Editor打开查看，使用text搜索，发现存在png文件



3、将A8 3C 7A中的7A改为74

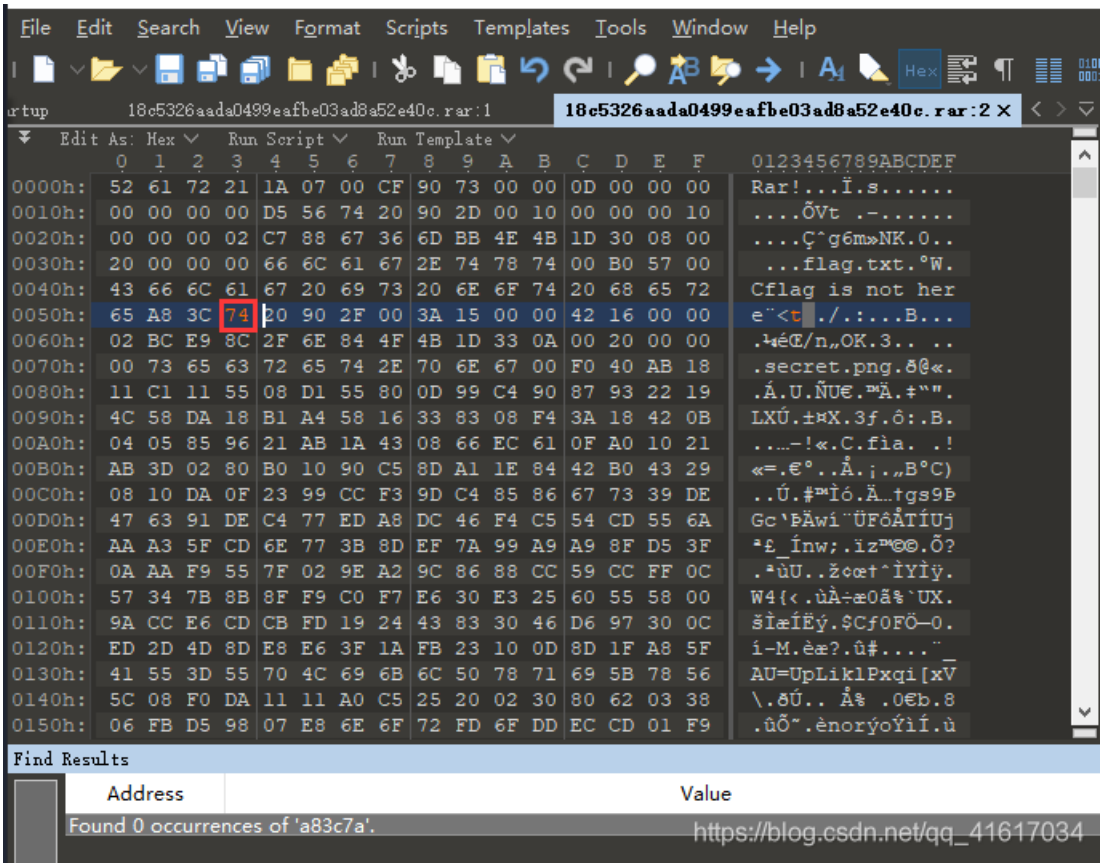




```
0160h:  02 07 CB 9F F7 DE 3C E4 0F F8 4E DC DB 7E D0 95  ..Ëÿ÷Þ<ä.øNÜÛ~Ð•
0170h:  F9 C0 1F B9 94 C0 FC 84 00 41 3B 40 02 10 F4 F8  ùÀ.¹”Àü„.A;@..ôø
0180h:  F8 00 20 47 67 DD B4 1F F8 4F 8E 80 1F FE BC FC  ø. GgÝ´.øOŽ€.þ¼ü
0190h:  F0 F7 97 E0 40 7E C4 0F EC 60 CF D0 80 7F 38 31  ð÷—à@~Ä.ì`ÏĐ€.81
01A0h:  E5 28 E2 D1 E0 06 B4 9A 9D FC 93 E5 D3 FA 1A DC  å(âÑà.´š.ü“åÓú.Ü
```

Find Results

Address	Value
Found 1 occurrences of 'a83c7a'.	
51h	a83c7a



File Edit Search View Format Scripts Templates Tools Window Help

rtup 18c5326aada0499eafbe03ad8a52e40c.rar:1 | 18c5326aada0499eafbe03ad8a52e40c.rar:2 ×

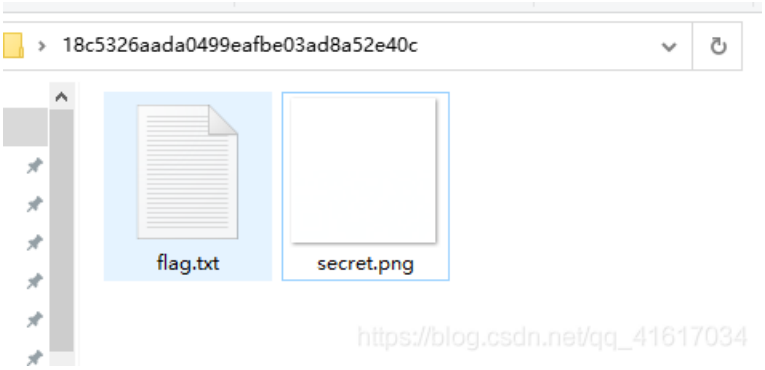
Edit As: Hex | Run Script | Run Template

```
          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   ....Ç^g6m»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 5F CD 6E 77 3B 8D EF 7A 99 A9 A9 8F D5 3F   ª£_Ínw;.iz™©©.Õ?
00F0h:   0A AA F9 55 7F 02 9E A2 9C 86 88 CC 59 CC FF 0C   .ªùU..ž¢œ†ˆÌYÌÿ.
0100h:   57 34 7B 8B 8F F9 C0 F7 E6 30 E3 25 60 55 58 00   W4{‹.ùÀ÷æ0ã%`UX.
0110h:   9A CC E6 CD CB FD 19 24 43 83 30 46 D6 97 30 0C   šÌæÍËý.$Cƒ0FÖ—0.
0120h:   ED 2D 4D 8D E8 E6 3F 1A FB 23 10 0D 8D 1F A8 5F   í-M.èæ?.û#....¨_
0130h:   41 55 3D 55 70 4C 69 6B 6C 50 78 71 69 5B 78 56   AU=UpLiklPxqi[xV
0140h:   5C 08 F0 DA 11 11 A0 C5 25 20 02 30 80 62 03 38   \.ðÚ.. Å% .0€b.8
0150h:   06 FB D5 98 07 E8 6E 6F 72 FD 6F DD EC CD 01 F9   .ûÕ˜.ènoryoÝìÍ.ù
```

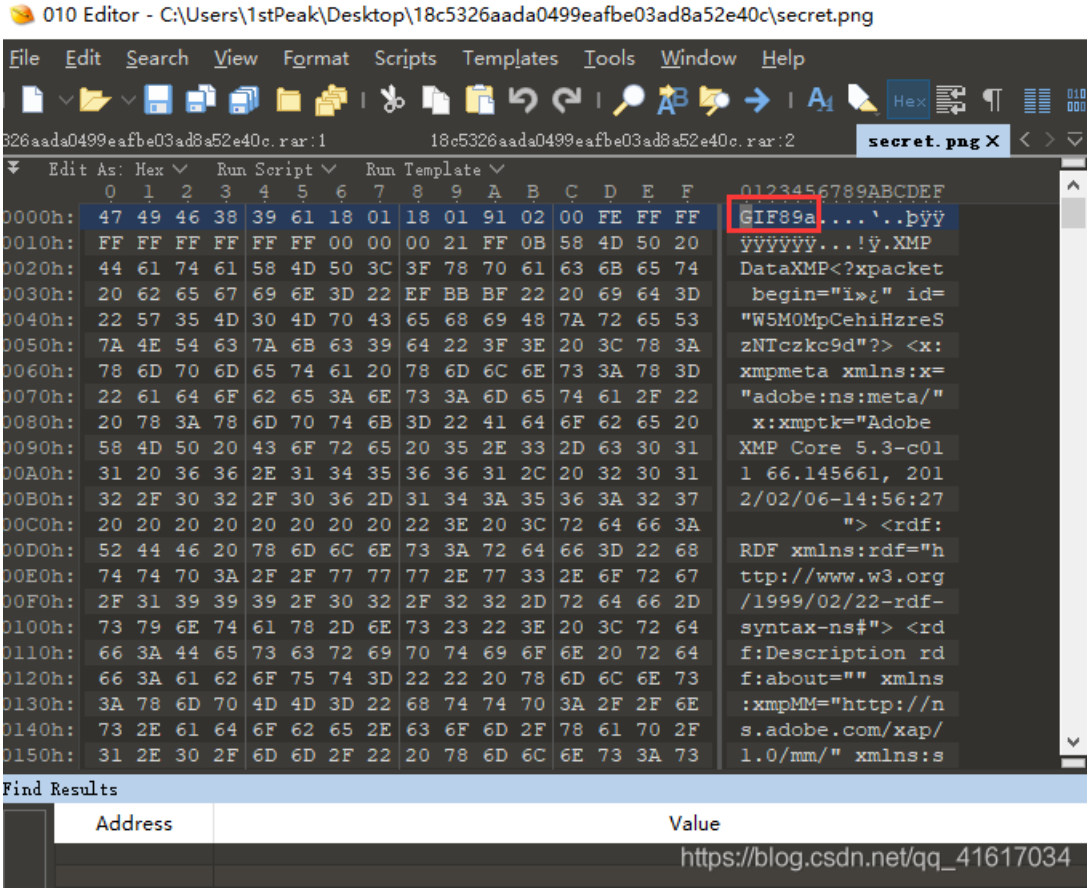
Find Results

Address	Value
Found 0 occurrences of 'a83c7a'.	

4、解压该文件，获得png图片

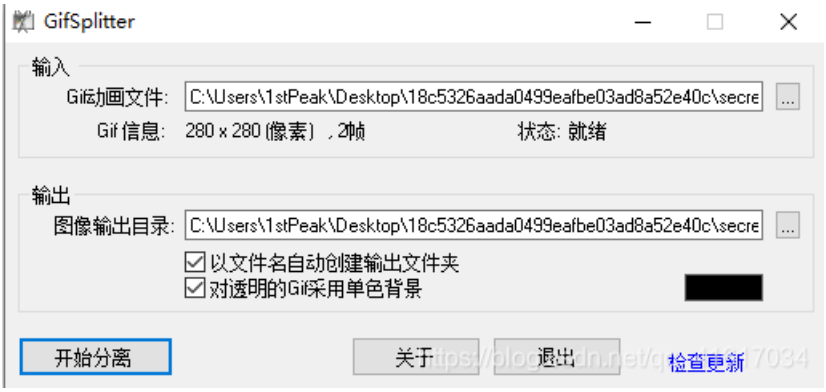


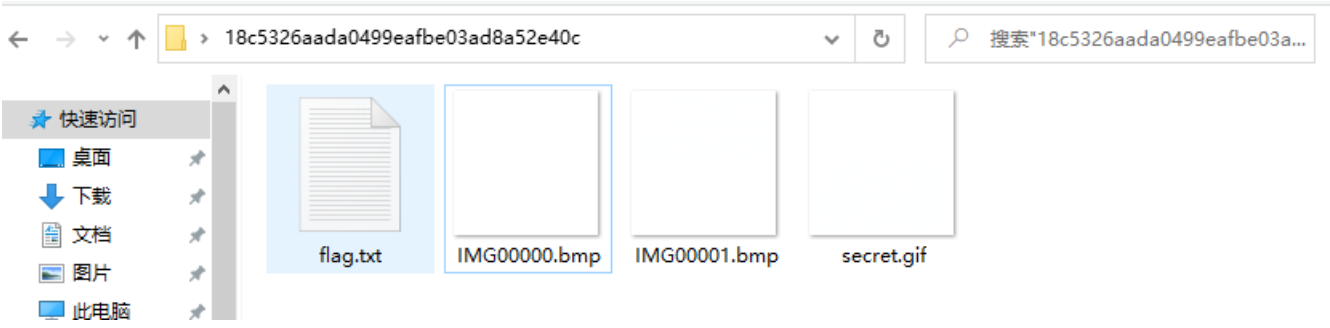
5、将png图片丢入010Editor中发现是gif文件，呢么我们修改一下后缀



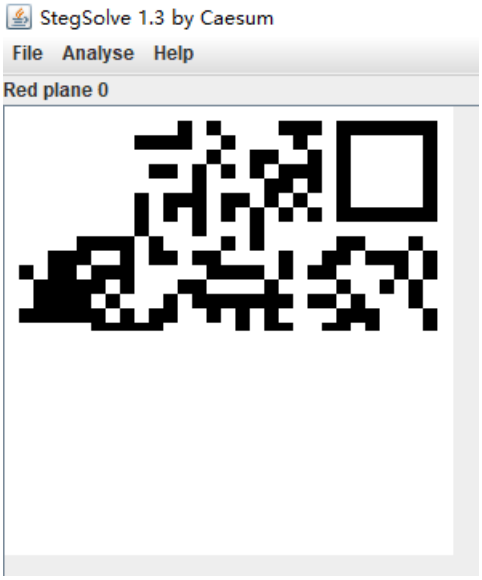
6、因为提示双图层，我们使用ps或gifsplitter进行分离

gifsplitter下载：https://github.com/1stPeak/GIFsplitter2.0





7、使用StegSolve对两个图片进行查看



8、将两个分离的二维码进行拼接，并补全定位符

9、扫描二维码即可获得flag