Misc-RAR隐写

原创

why you learn hard? 于 2021-10-13 17:59:57 发布 99 收藏
分类专栏： misc 文章标签： ctf misc

本文链接：https://blog.csdn.net/hacker_zrq/article/details/120748731

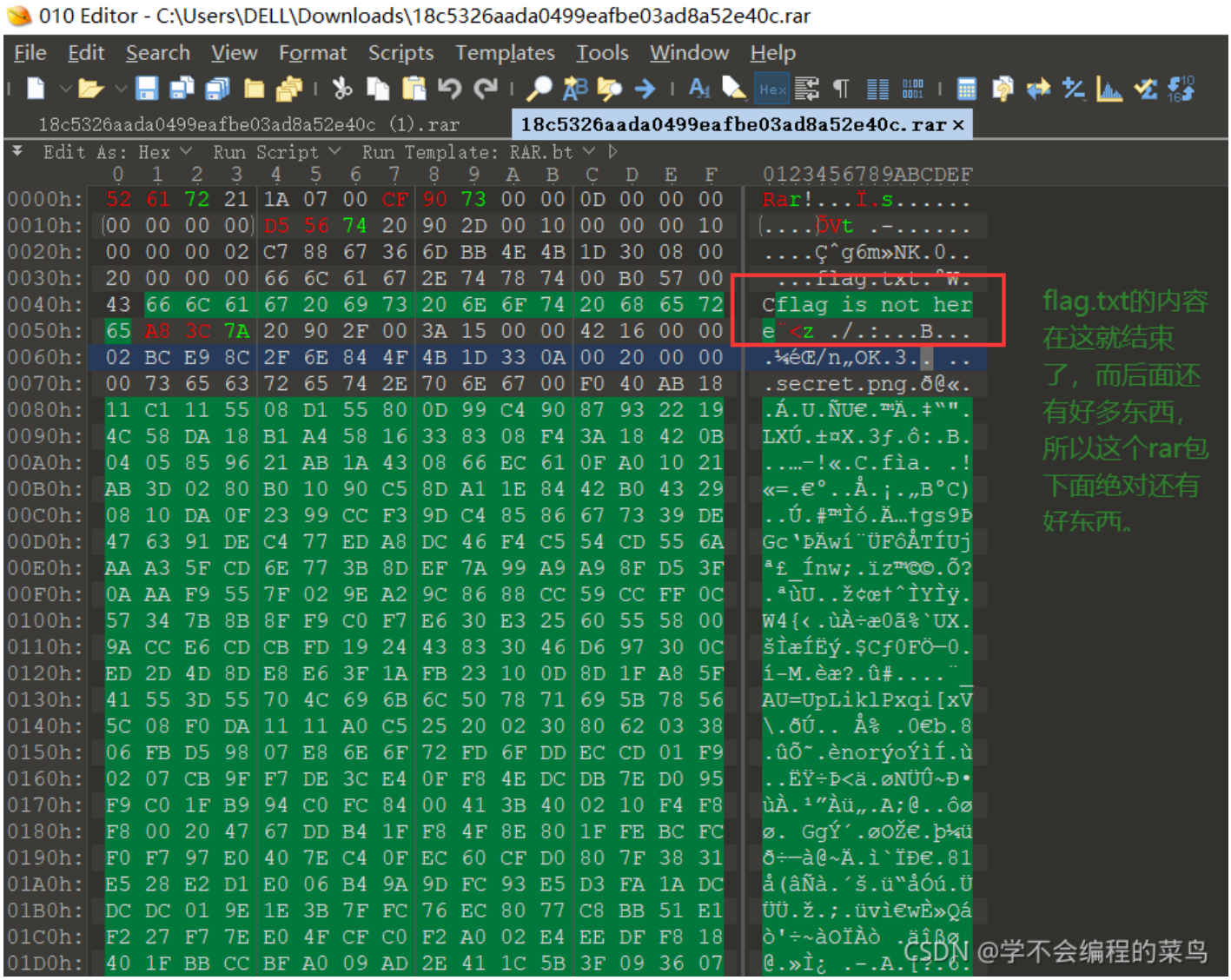

misc 专栏收录该内容
16 篇文章 0 订阅
订阅专栏

> 题目来自于：XCTF的SimpleRAR，由于涉及到许多新知识，所以写篇小文子记录一下。

一、下载完后是一个压缩包。

> 里面就有一个flag.txt，打开之后发现有一串字符是flag is not here，而且我们查看他的文件大小，只要十六字节，绝对不可能再藏着什么信息了。

> 然后把压缩包拉到010editor里面，发现一下子出来好多新的内容，很明显是有夹杂着的附加文件。


010 Editor - C:\Users\DELL\Downloads\18c5326aada0499eafbe03ad8a52e40c.rar
File Edit Search View Format Scripts Templates Tools Window Help
18c5326aada0499eafbe03ad8a52e40c (1).rar
18c5326aada0499eafbe03ad8a52e40c.rar
Edit As: Hex Run Script Run Template: RAR.bt
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 7A 20 90 2F 00 3A 15 00 00 42 16 00 00 e¨<z ./.:...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;.ïz™©©.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˜.ènorýoÝìÍ.ù
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
01B0h: DC DC 01 9E 1E 3B 7F FC 76 EC 80 77 C8 BB 51 E1 ÜÜ.ž.;.üvì€wÈ»Qá
01C0h: F2 27 F7 7E E0 4F CF C0 F2 A0 02 E4 EE DF F8 18 ò'÷~àOÏÀò .äîßø.
01D0h: 40 1F BB CC BF A0 09 AD 2E 41 1C 5B 3F 09 36 07 @.»Ì¿ .-.A.[?.6.
flag.txt的内容在这就结束了，而后面还有好多东西，所以这个rar包下面绝对还有好东西。
CSDN @学不会编程的菜鸟

二、rar文件头信息。

```
rar 是由一个一个 block 组成的，每个 block 有以下几个部分

HEAD_CRC    2   全部块或块部分的CRC

HEAD_TYPE   1   块类型

HEAD_FLAGS  2   阻止标志

HEAD_SIZE   2   块大小

ADD_SIZE    4   可选字段 - 添加块大小
```

而 HEAD_TYPE一般是下面这些值：

```
标记块：HEAD_TYPE=0x72
压缩文件头：HEAD_TYPE=0x73
文件头：HEAD_TYPE=0x74
旧风格的注释头：HEAD_TYPE=0x75
旧风格的用户身份信息：HEAD_TYPE=0x76
旧风格的子块：HEAD_TYPE=0x77
旧风格的恢复记录：HEAD_TYPE=0X78
旧风格的用户身份信息：HEAD_TYPE=0X79
子块：HEAD_TYPE=0x7A
最后的结束块：HEAD_TYPE=0x7B
```

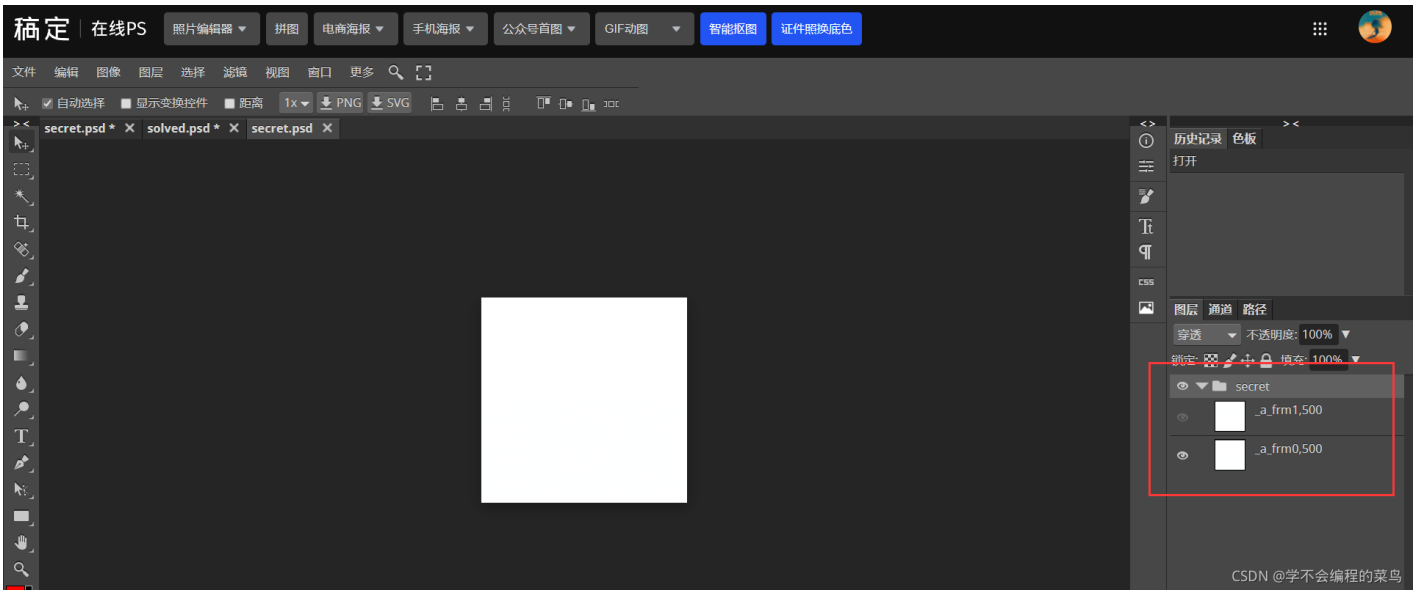
回到这道题，我们想要的是文件块，而非文件子块，所以我们得把位于子块第三个字节的0x7A子块标识改成0x74的文件块标识，然后保存。52好压很坑壁，文件头损坏他压根不提醒。

> 会发现压缩包里多了一个secret.png。

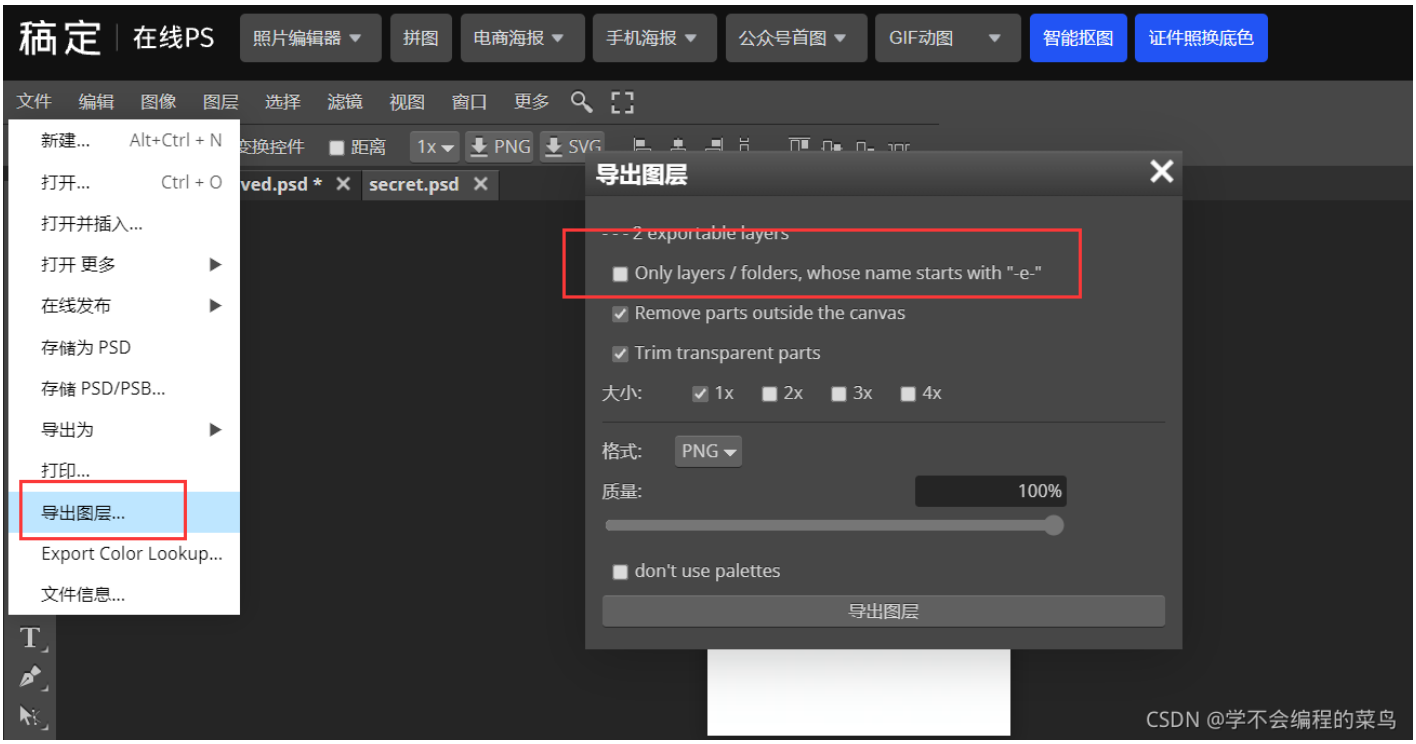
> 但是无法打开。 根据题意说是双图层，那我们先把双图层分解出来。这里使用在线PS网站，不用去下载繁杂的PS软件。
>
> 【在线PS】PS软件网页版，ps在线图片处理工具photopea-稿定设计PS (gaoding.com)

三、分离双图层。

看到了右侧的双图层。

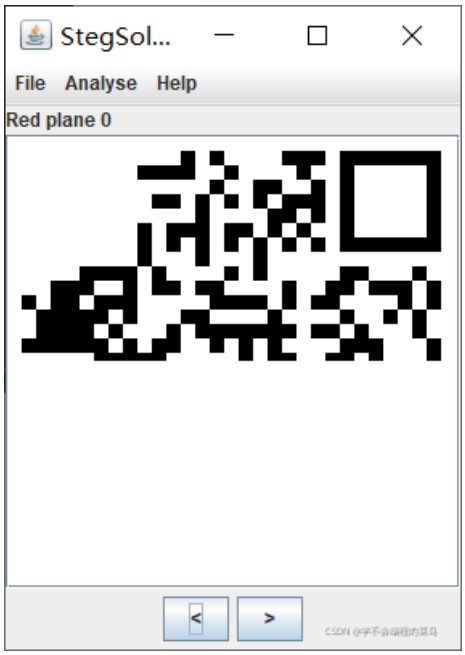


导出图层。

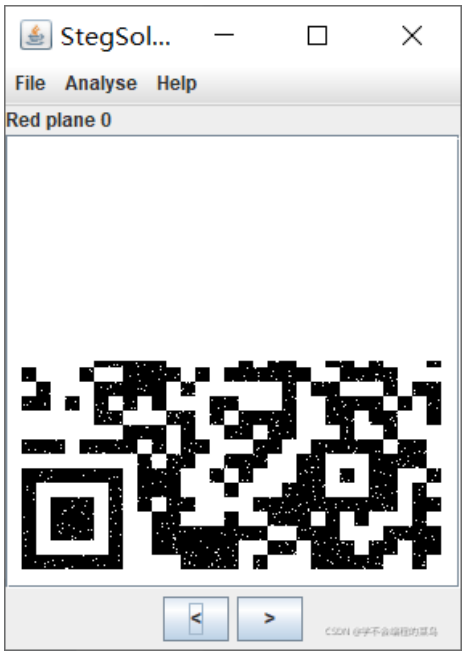


四、接下来就是再stegsolve里面拼接了。

> 先导入一张图层，找到含有二维码部分的那一帧，然后保存为文件名b1。



然后再导入第二个图层。找到含有下半部分二维码的那一帧，然后使用stegsolve的拼接功能Image Combiner，找到我们刚才保存的上半部分b1。



找到拼接好的那一张并保存。可以看出是个半残，我们得把左上角还有右上角的定位块补齐，再次来到在线ps。

五、修复二维码。

> 直接截图左下角那个完整的定位块，拖到左上角还有右上角即可扫码。可以手机扫，也可以电脑在线扫码。这个网站最好用，你不用将照片保存到本地，直接截图，然后ctrl+v即可扫描成功。
>
> 在线二维码解码器 二维码安全检测工具 (wwei.cn)

.

zip隐写汇总：

> 【CTF 攻略】CTF比赛中关于zip的总结 - 安全客，安全资讯平台 (anquanke.com)