

XCTF-SimpleRAR

原创

r0b1n_9070 于 2020-11-03 21:54:08 发布 167 收藏

分类专栏: [web](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_45707441/article/details/109480209

版权



[web](#) 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

考察知识点:

RAR文件结构
Winhex工具的简单使用
Stegsolve
PS抠图

解题过程:

SimpleRAR

👍 50 最佳Writeup由它山提供

难度系数: ★★★★★ 5.0

题目来源: 08067CTF

题目描述: 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)

题目场景: 暂无

题目附件: 附件1

https://blog.csdn.net/qq_45707441

看题目描述有个提示 ps:双图层, 想到可能要用到PS, 双图层当时没看懂, 完全没接触过PS...

然后下载附件得到了一个rar压缩文件, 打开后发现只有一个flag.txt文件

名称

flag.txt

flag.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

flag is not here

但题目提示了PS，双图层，我想到附件里怎么着也得有张图片文件吧,接下来用Winhex打开压缩文件

00000000	52 61 72 21 1A 07 00 CF 90 73 00 00 0D 00 00 00	Rar! ĩ s
00000010	00 00 00 00 D5 56 74 20 90 2D 00 10 00 00 00 10	Övt -
00000020	00 00 00 02 C7 88 67 36 6D BB 4E 4B 1D 30 08 00	Ç^g6m»NK 0
00000030	20 00 00 00 88 8C 81 87 2E 74 78 74 00 B0 57 00	flag.txt w
00000040	43 66 6C 61 67 20 69 73 20 6E 6F 74 20 68 65 72	Cflag is not her
00000050	65 A8 3C 7A 20 90 2F 00 3A 15 00 00 42 16 00 00	e`<z / : B
00000060	02 BC E9 8C 2F 6E 84 4F 4B 1D 33 0A 00 20 00 00	4éG/n,,OK 3
00000070	00 73 65 63 72 65 74 2E 70 6E 67 00 F0 40 AB 18	secret.png δ@«
00000080	11 C1 11 55 08 D1 55 80 0D 99 C4 90 87 93 22 19	Á U ÑUe ¯Ä ±""
00000090	1C 50 DA 10 B1 A4 50 16 03 03 00 F4 0A 10 42 0D	lXó i-X 0f 0. B
000000A0	04 05 85 96 21 AB 1A 43 08 66 EC 61 0F A0 10 21	...-!« C fia !
000000B0	AB 3D 02 80 B0 10 90 C5 8D A1 1E 84 42 B0 43 29	<= e° Å ; „B°C)
000000C0	08 10 DA 0F 23 99 CC F3 9D C4 85 86 67 73 39 DE	Ú #™i6 Ä...tgs9B
000000D0	47 63 91 DE C4 77 ED A8 DC 46 F4 C5 54 CD 55 6A	Gc`PÄwi`ÜFóÁTÍUj
000000E0	AA A3 5F CD 6E 77 3B 8D EF 7A 99 A9 A9 8F D5 3F	ª£_ínw; iz™@@ Ö?
000000F0	0A AA F9 55 7F 02 9E A2 9C 86 88 CC 59 CC FF 0C	ªùU žçst4iYiy
00000100	57 34 7B 8B 8F F9 C0 F7 F6 30 F3 25 60 55 58 00	w4 /, ñÀ-«03&`UV

发现压缩文件里除了除了.txt文件，还有其他的東西，这里需要用到关于RAR文件结构的一些知识

RAR文件结构

注意到7A代表的含义是子块，需要把7A改成74，74是文件头的标志,用Winhex修改后保存，然后再打开

发现多了一个png文件

名称	大小	压缩后大小	修改时间	创建时间	访问时间
flag.txt	16	16	2017-10-1...		
secret.png	5 698	5 434	2017-10-1...		

接着打开图片发现是空白，这时候想到题目提示的PS双图层，于是就用PS打开，结果提示Not a PNG file

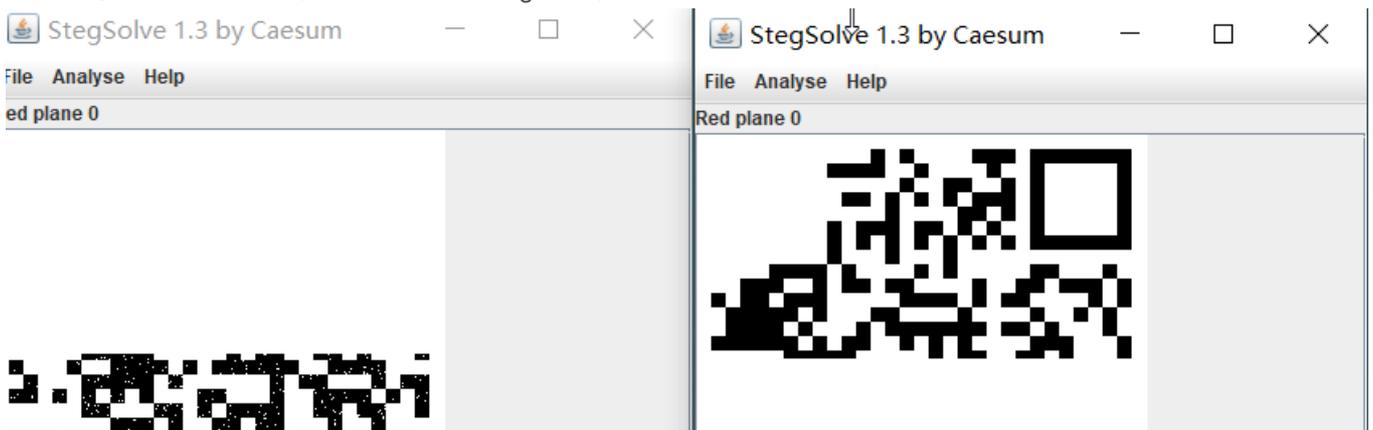
用Winhex再次打开png文件，发现文件头是GIF，于是更改文件后缀名为GIF类型，用PS成功打开，果然有

```

? FF GIF89a \ pÿÿ
) 20 yyyyyy !y XMP
5 74 DataXMP<?xpacket
4 3D begin="i»¿" id=
5 53 "W5M0MpCehiHzreS
3 3A zNTczkc9d"?> <x:

```

两个图层，接下来就是把图层分离出来，再用StegSolve分别打开





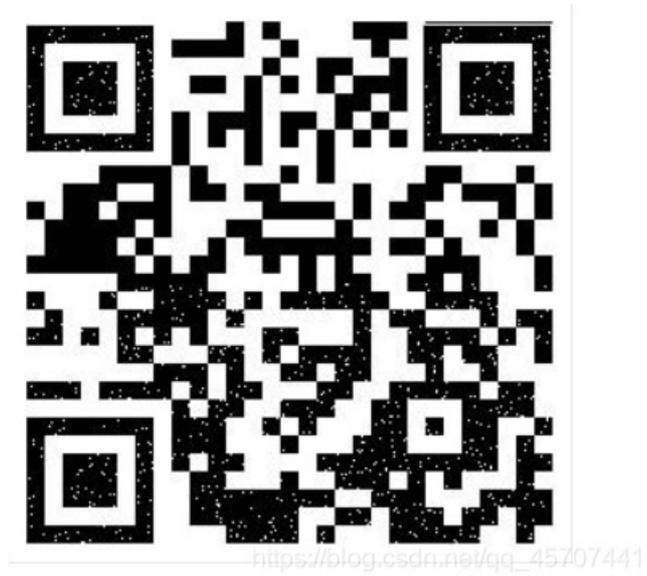
接下来需要用PS把两张图片拼到一起，然后把右上角和左上角的定位方格补齐，这里就需要用到一点PS的知识啦，感谢室友教会了我抠图...

分离图层可看下下面两个链接

[分离图层操作](#)

[分离图层操作](#)

完成后用手机扫描得到flag



[参考博客](#)