23121677-范舒舰-6 月 9 日 misc 作业 WP

接下来我四个步骤讲解如何得到最终 flag

一：提取文件

先使用 shu_lib@challenge.ctf 解压压缩包“技能练习题.zip”得到“chall.zip”
直接解压“chall.zip”得到“chall.jpg”

二：得到二层文件

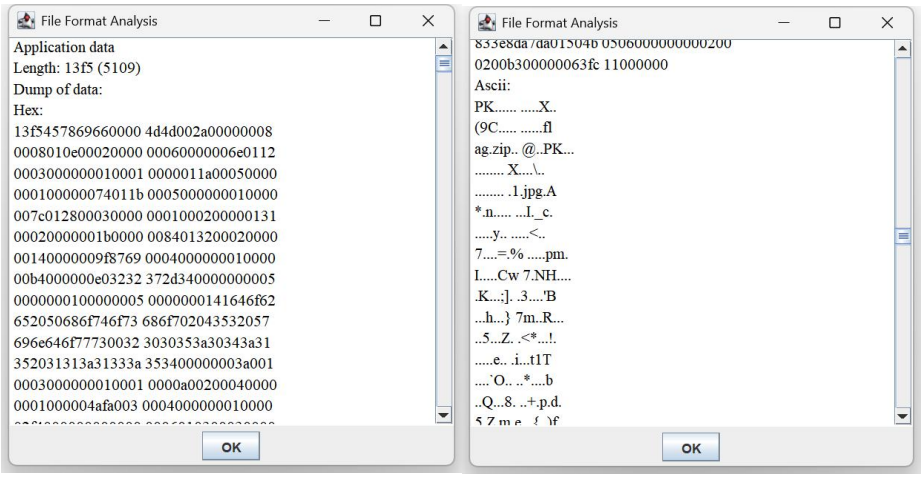
此时来到了解法的分歧点：

图片分析法：

使用“Stegsolve”打开“chall.jpg”

先使用“Stegsolve”“Analyse”里的“File Format”查看信息

约十分钟后得到隐含的 Application data



Length: 13f5 (5109)

Dump of data:

Hex: 13f5457869660000 4d4d002a00000008 0008010e00020000 00060000006e0112 0003000000010001 0000011a00050000 0001000000074011b 0005000000010000....

Ascii: PK..... .....X.. (9C..... ......fl ag.zip.. @..PK... ..... X....\.. ..... .1.jpg.A *.n..... ...l._c. ....

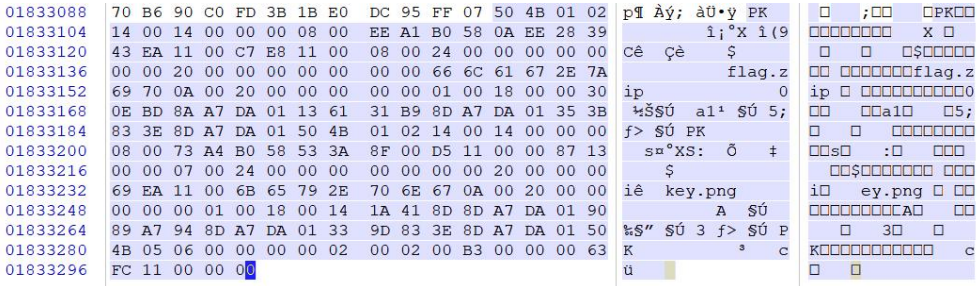
观察 Ascii 可得 PK 头是 ZIP 文件的标准开头，存在隐藏信息 flag.zip 等

直接将后缀名.jpg 改为.zip 解压得下一步

文件分析法：

使用“WinHex”打开“chall.jpg”

可以在文件最后找到



504B0102140014000000080 0EEA1B0580AEE283943EA1100C7E81100080024000000000000002000000000000000000666C61672E7A69700A0020000000000000100180000300EBD8AA7DA01136131B98DA7DA01353B

UTF-8:PK X $ flag.zip 0 a1 5;

观察可得 PK 头是 ZIP 文件的标准开头，存在隐藏信息 flag.zip 等

直接将后缀名.jpg 改为.zip 解压得下一步

瞪眼法：

题目只给出了一个图片文件，由于题目是套娃题，一定存在下一步

修改文件后缀为.zip 尝试，尝试成功，进入下一步

三：解压 flag.zip

直接尝试解压 flag.zip 发现存在密码，key.png 一眼就是解题关键

图片分析法：

使用“Stegsolve”打开“key.png”

直接从“File Format”中找到

Ascii:

VGlwOiB UaGUgeml wIHBhc3N 3b3JkIGl zIDYgY2h hcmFjdGV ycyBsb25 nIGFuZCB jb250YWl ucyBvbmx 5IGxvd2V yY2FzZSB sZXR0ZXJ zIGFuZCB udW1iZXJ zOik=

一眼盯真得出是 base64 编码（字符串长度是 4 的倍数 =出现在字符串最后）

解码得 Tip: The zip password is 6 characters long and contains only lowercase letters and numbers:)

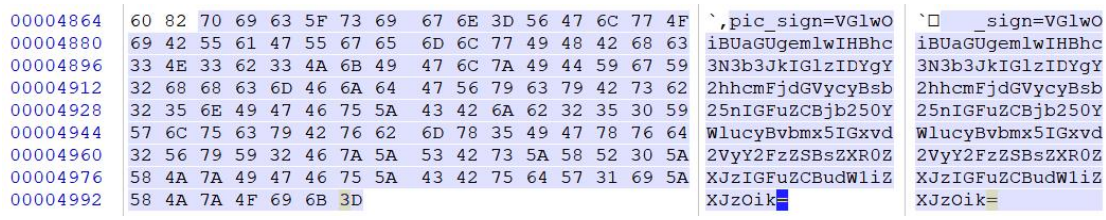
使用“ARCHPR”暴力破解 6 位小写+数字得到密码“s1h2u3”

解压“flag.zip”进入下一步

文件分析法：

使用“WinHex”打开“key.png”

同样的可以在文件最后找到



7069635F7369676E3D56476C774F69425561475567656D6C774948426863334E3362334A6B49476C7A4944596759326868636D466A64475679637942736232356E494746755A43426A6232353059576C7563794276626D7835494778766432567959324675A5A5342735A5852305A584A7A494746755A434275645731695A584A7A4F696B3D

UTF-8：

pic_sign=VGlwOiBUaGUgemlwIHBhc3N3b3JkIGlzIDYgY2hhcmFjdGVycyBsb25nIGFuZCBjb250YWlucyBvbmx5IGxvd2VyY2FzZSBsZXR0ZXJzIGFuZCBudW1iZXJzOik=

一眼盯真得出 pic_sign 后是 base64 编码（字符串长度是 4 的倍数 =出现在字符串最后）

解码得 Tip: The zip password is 6 characters long and contains only lowercase letters and numbers:)

使用“ARCHPR”暴力破解 6 位小写+数字得到密码“s1h2u3”

解压“flag.zip”进入下一步

四：得到 flag

得到两张图片“1.jpg”和“2.jpg”

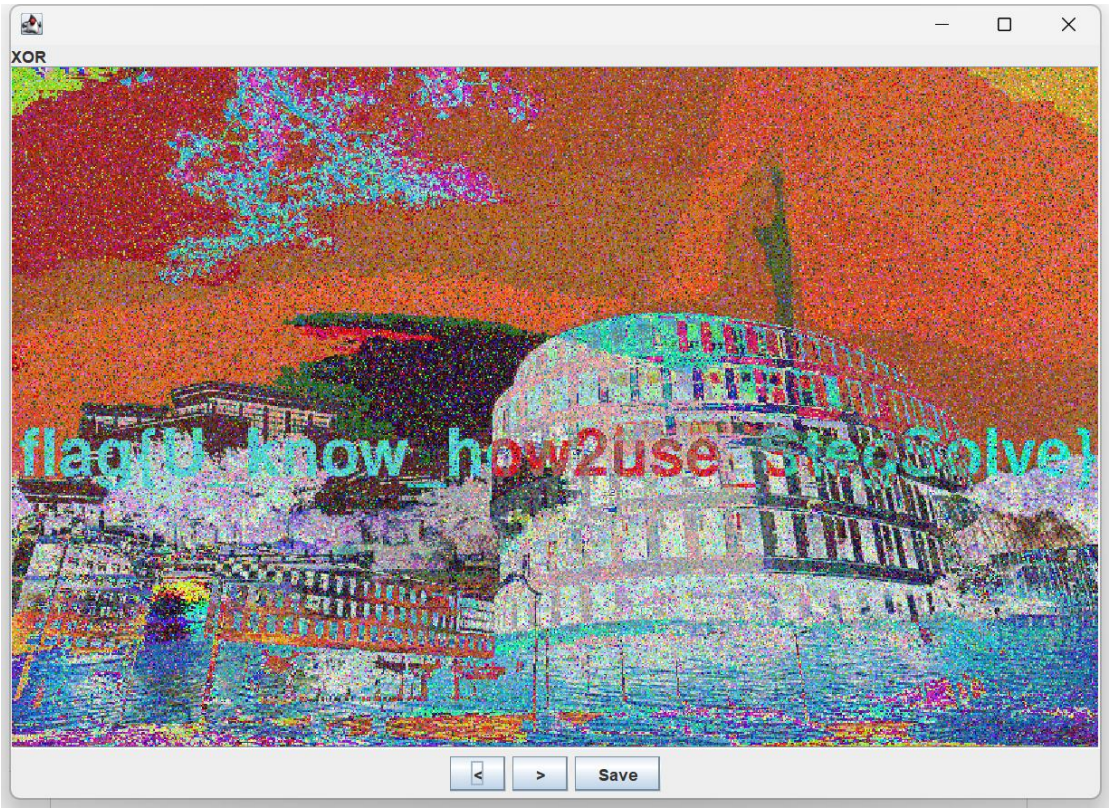
很容易看出需要叠加两张图片

使用“Stegsolve”打开“1.png”

使用“Stegsolve”“Analyse”里的“Image Combiner”叠加图片

直接在 XOR 里看得到

flag{U_know_how2use_StegSolve}



五：图寻题

使用“flag{U_know_how2use_StegSolve}”解压素养练习题

得到“challenge.png”

图中给出两个信息：

1. 地图：某山石靠近水域，边上有一条小道名为“???nore Trail”
2. 文字：地图处于美国加利福尼亚州的一个州公园，Shorebirds nesting on rocks 表明有岸禽筑巢，有很大可能该公园位于海岸线边缘

之后就无法获得更多信息了

只能丢给 chatgpt，询问加州海岸边的保护区，直接给出位于海岸线上的公园 Point Lobos State Natural Reserve：一处沿海礁石鸟类筑巢保护区。

flag{36.515,-121.949}