第四届“强网”拟态防御国际精英挑战赛MISC-mirror

原创

末 初 于 2021-11-01 01:14:01 发布 421 收藏 3

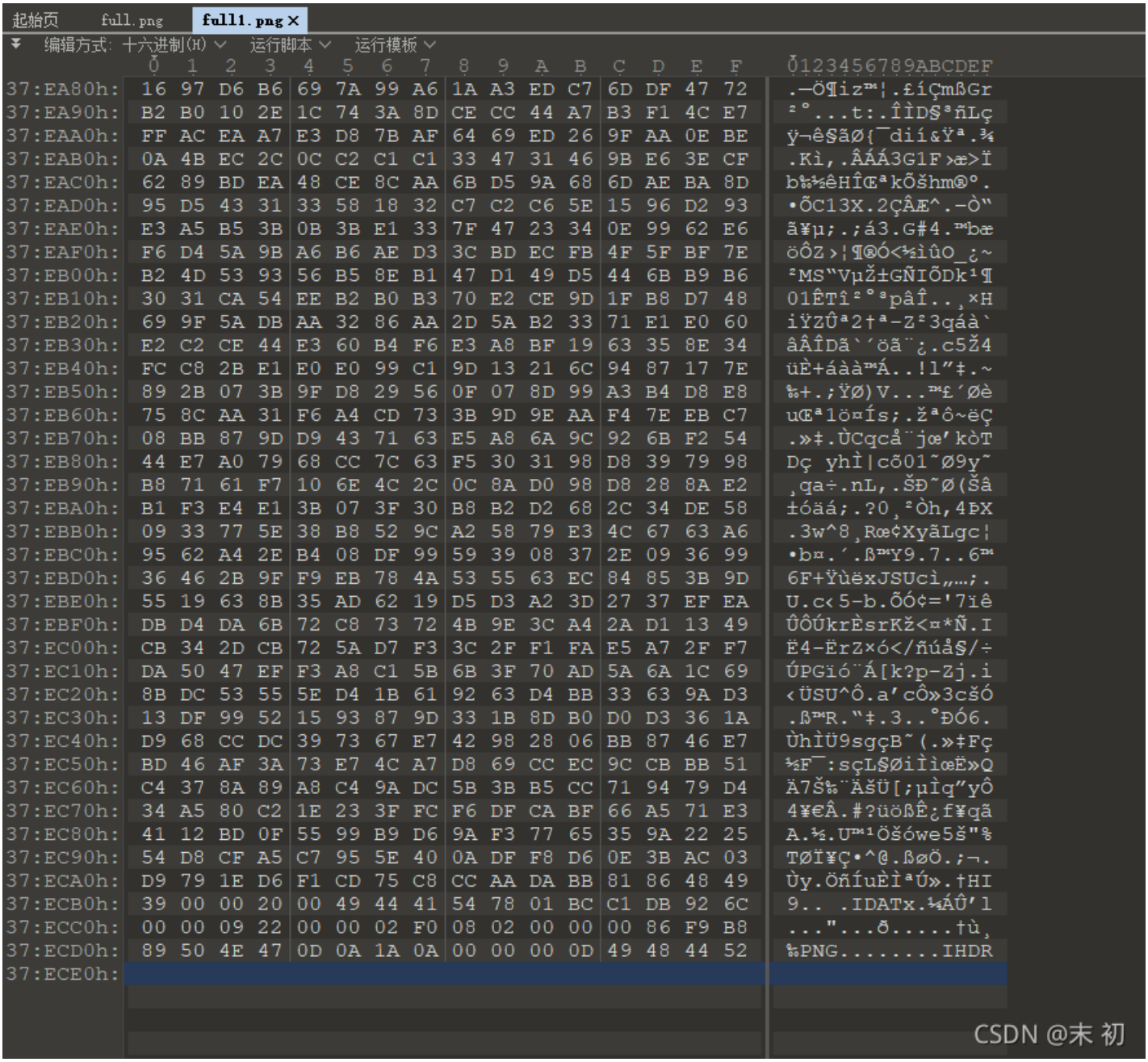
分类专栏： CTF_MISC_Writeup 文章标签： 强网“拟态”

本文链接：https://blog.csdn.net/mochu7777777/article/details/120945321


```
题目附件请自取
链接：https://pan.baidu.com/s/18K00ClgwJsqmKphPmqMpHw
提取码：6r3j
```

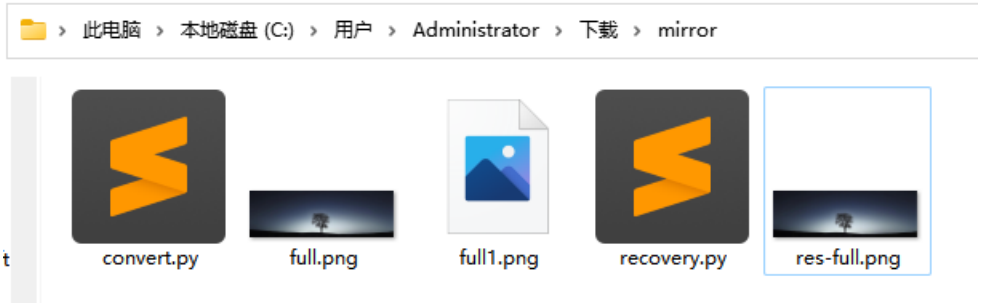
`full.png` 使用 `010 Editor` 打开出现CRC校验报错，猜测需要修复宽高，其次发现了文件末尾附加了镜像翻转的 `png` 字节流数据

将附加数据提取出来另存为`png`文件，通过分析不难发现将字节流数据逆序然后每十六个字节流翻转一下即为正常的`png`数据



使用Python简单处理

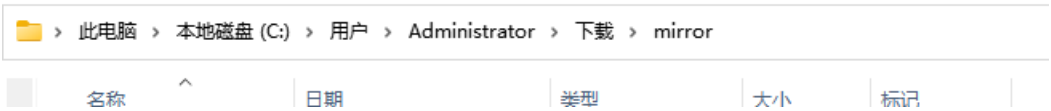
```python
from binascii import *

with open('full1.png', 'rb') as f:
 with open('res-full.png', 'wb') as f1:
  hex_data = hexlify(f.read()).decode()[::-1]
  for i in range(0, len(hex_data), 32):
   data = hex_data[i:i+32][::-1]
   f1.write(unhexlify(data))
```



即得到`full.png`和`res-full.png`两张图片，两张图片使用`010 Editor`打开都会出现CRC报错，使用脚本还原宽高

```
import binascii
import struct
import sys

file = 'full.png'
fr = open(file,'rb').read()
data = bytearray(fr[0x0c:0x1d])
crc32key = eval('0x'+str(binascii.b2a_hex(fr[0x1d:0x21]))[2:-1])
#原来的代码: crc32key = eval(str(fr[29:33]).replace('\\x','').replace("b'",'0x').replace("'",''))
n = 4095
for w in range(n):
    width = bytearray(struct.pack('>i', w))
    for h in range(n):
        height = bytearray(struct.pack('>i', h))
        for x in range(4):
            data[x+4] = width[x]
            data[x+8] = height[x]
        crc32result = binascii.crc32(data) & 0xffffffff
        if crc32result == crc32key:
            print(width,height)
            newpic = bytearray(fr)
            for x in range(4):
                newpic[x+16] = width[x]
                newpic[x+20] = height[x]
            fw = open(file+'.png','wb')
            fw.write(newpic)
            fw.close
            sys.exit()
```

即得到完整的图片`full.png.png`以及`res-full.png.png`

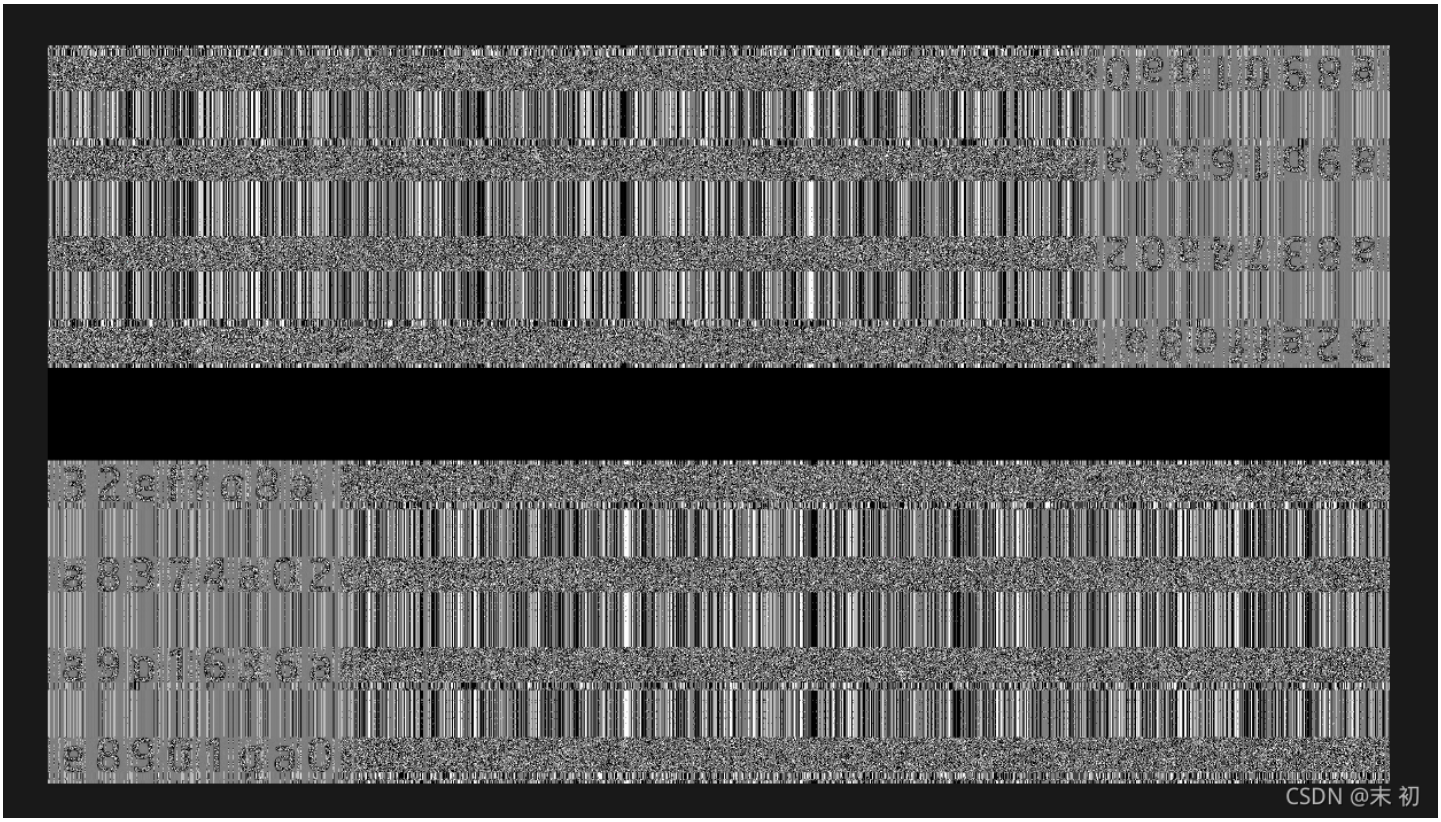


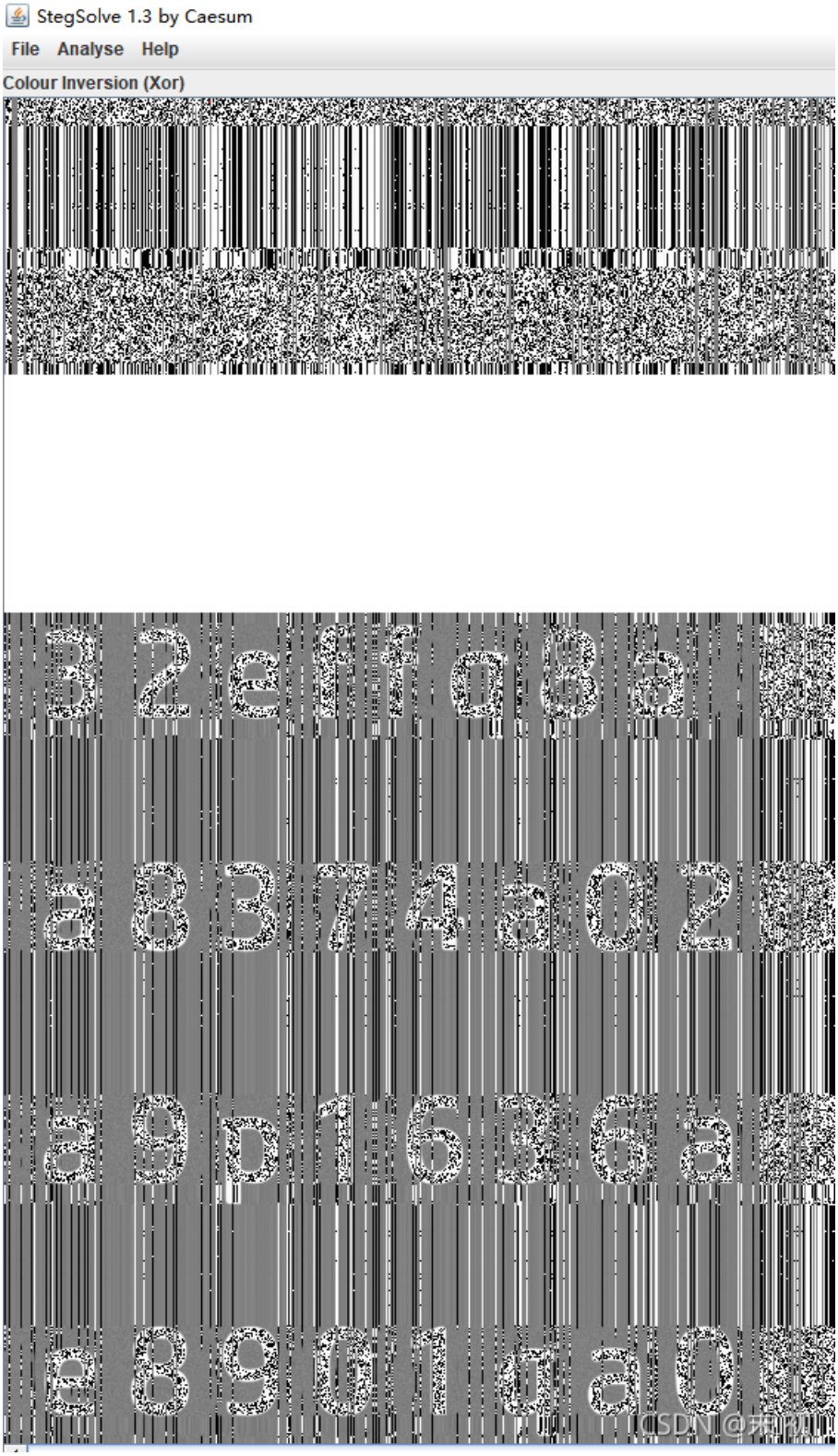
convert.py	2021/10/25 8:45	PY 文件	1 KB
full.png	2021/10/12 10:41	PNG 文件	2,695 KB
full.png.png	2021/10/25 8:54	PNG 文件	2,695 KB
recovery.py	2021/10/25 8:36	PY 文件	1 KB
res-full.png	2021/10/25 8:47	PNG 文件	3,580 KB
res-full.png.png	2021/10/25 8:55	PNG 文件	3,580 KB

很明显`res-full.png.png`可能存在盲水印

```
PowerShell
PS D:\Tools\Misc\BlindWaterMark> ls

    Directory: D:\Tools\Misc\BlindWaterMark

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          2021/9/4     9:56                blindwatermark
d-----         2021/9/25    11:51                JavaBlindWatermark
-a---          2020/8/30    12:58           1493 blind.py
-a---          2020/8/27    12:24           5776 bwm.py
-a---          2020/8/27    12:24           7242 bwmforpy3.py
-a---         2021/10/25     8:54        2759225 full.png.png
-a---          2020/8/27    12:24          35815 LICENSE
-a---          2020/8/27    12:24           2120 README.md
-a---         2021/10/25     8:55        3665120 res-full.png.png

PS D:\Tools\Misc\BlindWaterMark> python .\bwmforpy3.py decode .\full.png.png .\res-full.png.png flag.png
image<.\full.png.png> + image(encoded)<.\res-full.png.png> -> watermark<flag.png>
PS D:\Tools\Misc\BlindWaterMark>
```


`flag.png`使用`PS`水平翻转一下






```
32effq8aa8374a02a9p1636ae8901qa0
```

提示

```
2-5 e-6 9-a p-b q-d
```

一开始以为只是`2->5 e->6 9->a p->b q->d`，替换后发现提交并不对，猜测是都要相互替换即

```
flag='32effq8aa8374a02a9p1636ae8901qa0'

dict1 = {'2':'5','5':'2','e':'6','6':'e','9':'a','a':'9','p':'b','b':'p','q':'d','d':'q'}
flag_list = list(flag)

idx = 0
for char in flag_list:
 for key in dict1:
  if char == key:
   flag_list[idx] = dict1[key]
 idx += 1
res_flag = ''
for i in flag_list:
 res_flag += i
print('flag{{{}}}'.format(res_flag))
```

```
PS C:\Users\Administrator\Downloads\mirror> python .\replace.py
flag{356ffd89983749059ab1e3e968a01d90}
```