.wav异或提取png 提取blue通道数值并转换写成zip文件（2022DASCTF x SU 三月春季挑战赛 书鱼的秘密）

原创

Hardworking666 于 2022-03-28 21:15:54 发布 189 收藏

分类专栏： CTF 文章标签： 2022DASCTF x SU

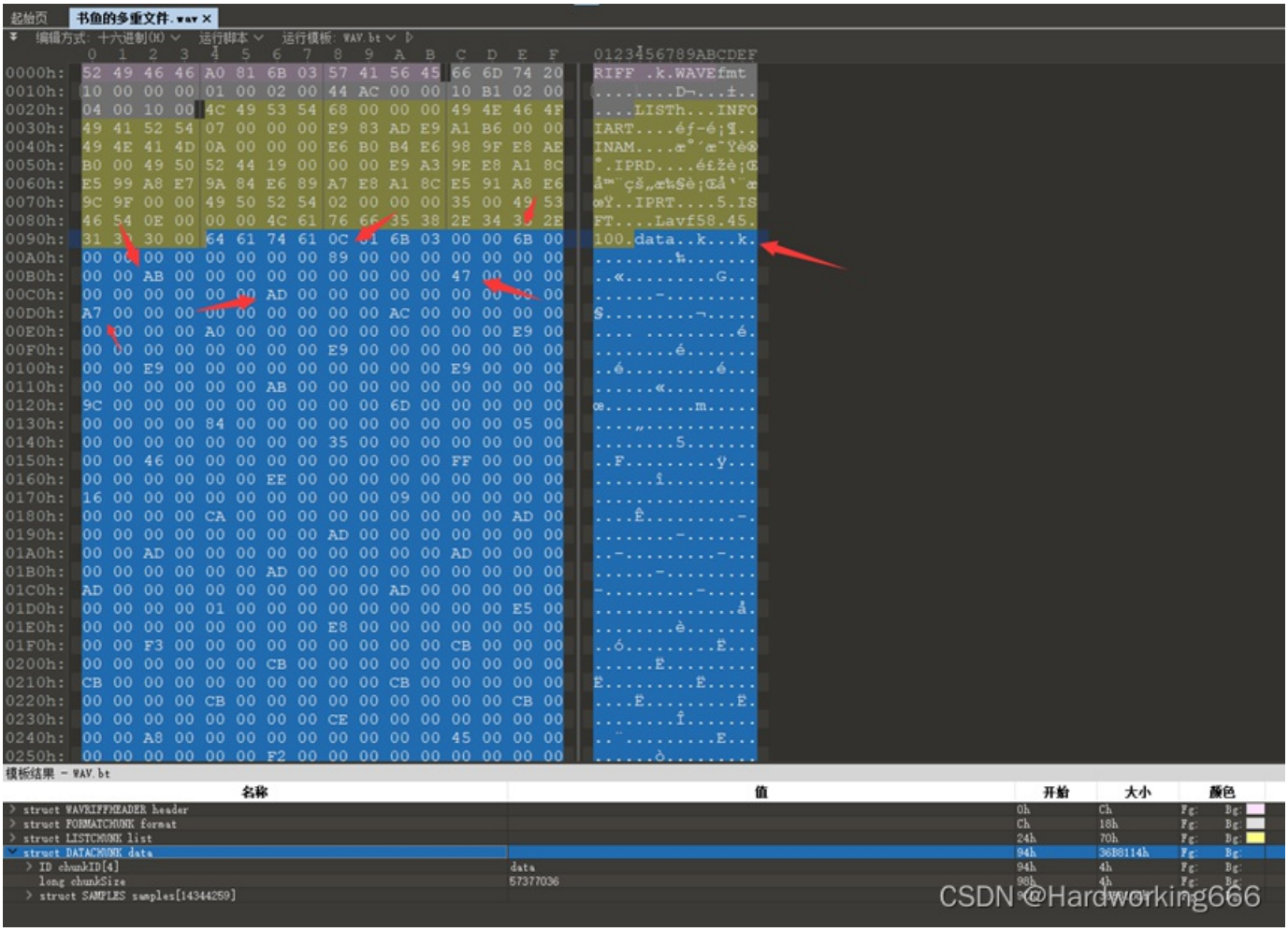
文章目录

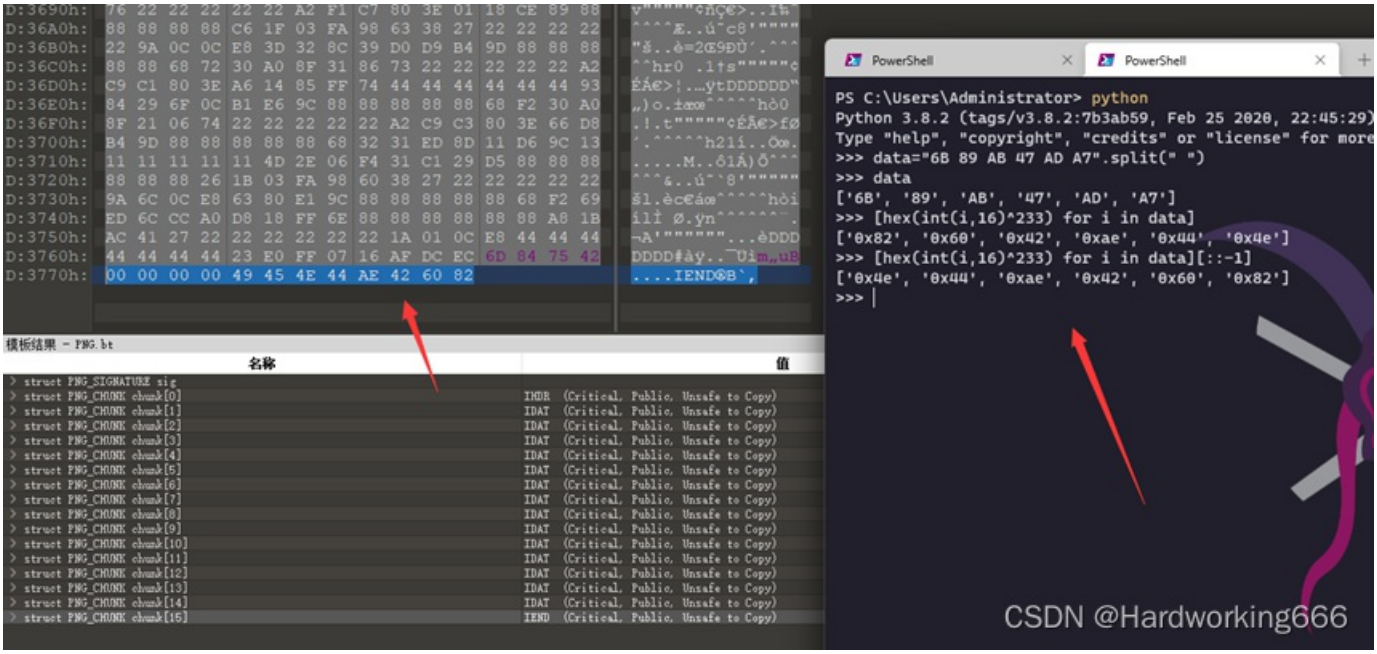
2022DASCTF x SU 三月春季挑战赛 书鱼的秘密
题目wp参考来源：
2022DASCTF x SU 三月春季挑战赛wp–WHT战队

一、.wav异或提取png

从data之后的第二个 k 之后开始，每隔10个字节，有一个字节的数据，其余的都是填充，混淆之类的数据。

把前几个字节提取出来与 233 异或。发现最终结果是png字节流文件尾的逆序。





编写脚本，将这些数据提取出来，异或，然后逆序重新写入成png

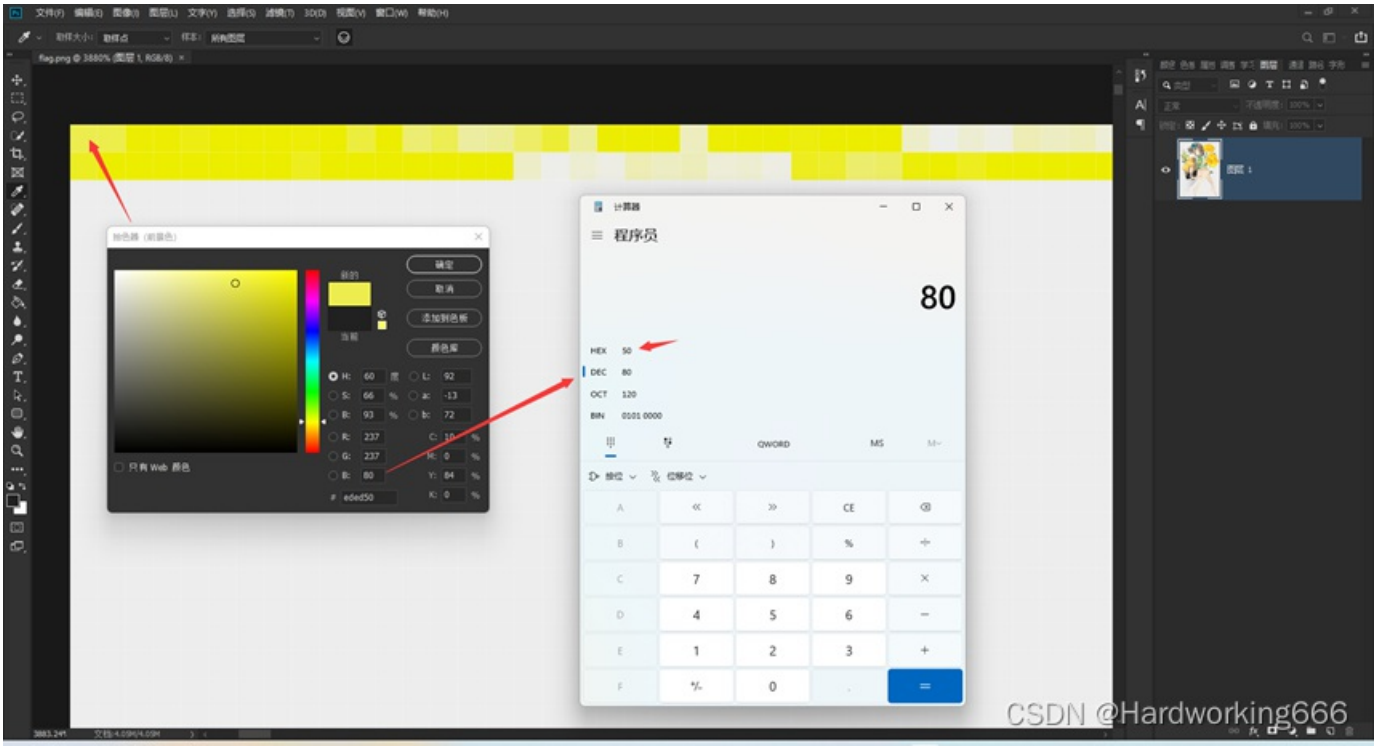
```
from binascii import *

data = ''
with open('书鱼的多重文件.wav', 'rb') as f:
 with open('flag.png', 'wb') as f1:
  for idx in range(0x9e, len(f.read()), 10):
   f.seek(idx)
   data += '{:02x}'.format(ord(f.read(1)) ^ 233)
  data = data[::-1]
  for i in range(0, len(data), 2):
   hex_data = data[i:i+2][::-1]
   f1.write(unhexlify(hex_data))
```

得到的png图片无法正常显示，binwalk分析发现，文件前部分都是无效数据，png图片被附加在了这些无效数据之后，foremost分离即可

二、提取blue通道数值并转换写成zip文件

Stegsolve的Data Extract查看并不像隐写了文件数据，猜测应该是对颜色动了手脚，使用 PS 打开，发现图片的前两行像素确实颜色一场，查看blue通道的数值，发现是 50 的十进制。继续提取前几个像素的blue数值，发现是 50 4B 03 04 的zip文件头。



编写脚本提取blue通道数值并转换写成zip文件

```
from PIL import Image
from binascii import *


img = Image.open('flag.png')
width, height = img.size
with open('flag.zip', 'wb') as f:
 for h in range(2):
  for w in range(width):
   blue = '{:02x}'.format(img.getpixel((w, h))[2])
   f.write(unhexlify(blue)
```

三、输入法九键+国际区号解密码

既然你这么懂文件,那么你也一定会很懂书鱼吧

书鱼说:如果你想拿到我的血,那么你必须通过我的考验,除了要懂文件还必须要找到我很久之前储存在老手机里的手机号哦。由于年代久远,那部手机里面的内容都被清空了,只有备忘录里留下了许多奇怪的内容,似乎当时是怕自己忘记女神的手机号而特定设定的,此时我再看着这些内容,过去对女神的美好记忆又突然袭来。那年那月那日那夜,我是多么思恋着她,但最终还是明白了她只是我望之而却的白月光。随着时间的推移,我似乎很久没有想起她了,但今天再度看着那青春年少时记录下来的内容,我突然又想起了她。此时,水星记突然萦绕在我的耳畔:

怎么可以 拥有你

还要多远才能进入你的心~

还要多久才能和你接近~

但似乎这些都已经成为了过去,沉默良久,我只是轻轻的叹了一口气:打CTF要什么女朋友。还是让我们来解出我过去存的这个电话号码吧

```
226232   1
23442647826 1
528842   3
5893626874   3
46342    2
6443742  1
473323   2
24462    1-2
6626     2
35426884     3
3782867425 484632    2
2654842      3
2376832      0-3
52726        1
```

我似乎已经知道了我当初是用什么方法存的这个电话号码了,虽然存错了,但是它陪了我渡过了整个青春。已经都无所谓了~

flag为DASCTF{md5(电话号码)}

输入法九键226232是 Canada ， 加拿大

国际手机号码开头，区号：

```
https://cwlwxr.github.io/s3n62u57_/
```

国家或地区	Countries and Regions	国家代码	手机电话号码开头正确格式/区号
中国	China	86	+86 13123456789
香港	Hong Kong	852	+852 61234567
台湾(台湾)	Taiwan	886	+886 912345678
澳门	Macao	853	+853 66123456
新加坡	Singapore	65	+65 81234567
日本	Japan	81	+81 7012345678
泰国	Thailand	66	+66 812345678
马来西亚	Malaysia	60	+60 123456789
菲律宾	Philippines	63	+63 9051234567
澳大利亚(澳洲)	Australia	61	+61 412345678
圣诞岛	Christmas Island	53	+61 812345678
科科斯（基林）群岛	Cocos (Keeling) Islands	-830	+61 891345678
加拿大	Canada	1	+1 2042345678
英国	United Kiongdom	44	+44 7400123456
美国	United States of America	1	+1 2223334444

发现这些国家的区号代码，都有一至三四位数字，对应右边的数字，猜测右边的数字就是这些国家地区的区号代码下标，即得到：

```
226232 1 => 1
 Canada
23442647826 1 => 9
 Afghanistan
528842 3 => 1
 Latvia
5893626874 3 => 2
 Luxembourg
46342 2 => 1
 India
6443742 1 => 2
 Nigeria
473323 2 => 0
 Greece
24462 1-2 => 86
 China
6626 2 => 6
 Oman
35426884 3 => 3
 Djibouti
3782867425 484632 2 => 4
 Equatorial Guinea
2654842    3 => 1
 Bolivia
2376832    0-3 =>  -440
 Bermuda
52726      1 => 8
 Japan
```

```
1912120866341-440
```

```
>>> import hashlib
>>> hashlib.md5('1912120866341-4408'.encode()).hexdigest()
'4d1a3568b2a81c7d958892bf100b3f15

DASCTF{4d1a3568b2a81c7d958892bf100b3f15}
```