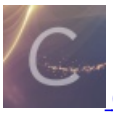
CTF show STEGA系列

原创

yu22x 于 2020-02-19 21:01:24 发布 2661 收藏 6

分类专栏： CTF show STEGA系列 文章标签： python linux 安全 密码学

本文链接：https://blog.csdn.net/miuzzx/article/details/104397527



题目地址：https://ctf.show

一般我做图片隐写类的题目有以下几个步骤：

1.如果是在压缩包中的图片，首先查看压缩包的二进制，没有异常，解压压缩包。

2.查看图片的属性，是否有附加的信息。

3.尝试打开图片，不能打开可能文件头缺少或其他原因。能打开，查看图片二进制。

4.在二进制中查看是否有其他类型的文件头。有则分离出来。

4.放入stegsolve中查看是否是LSB隐写。

5.最后实在没有办法就隐写工具挨个尝试吧

0x01 stega1

这道题就不啰嗦了，使用隐写工具jphs

链接：https://pan.baidu.com/s/1Oq8Wektf-JQSmJOwSYb8BA 提取码：4qks

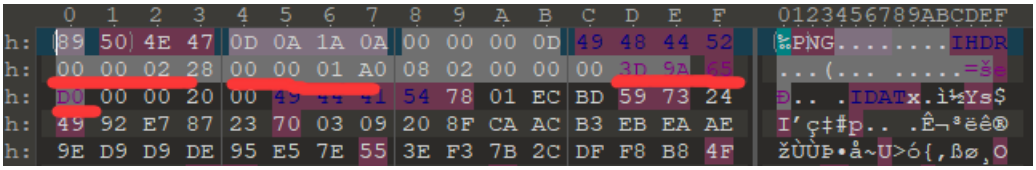
题目中没有任何提示，直接尝试空密码解密，成功获取flag。

0x02 stega2

一般图片的宽高被修改过，放到linux中是打不开的，对于这张图，可以直接爆破宽高，附上脚本：

```
import struct
import binascii
import os
p=0
m = open("flag.png","rb").read()
for i in range(5000):
    if(p==1):
     break
    for j in range(5000):
        c = m[12:16] + struct.pack('>i', i) + struct.pack('>i', j)+m[24:29]
        crc = binascii.crc32(c) & 0xffffffff
        if crc == 0x3d9a65d0:
            p=1
            #print(c)
            print(hex(i),hex(j))
            break
```

下面介绍一下png格式图片的16进制，第一处标注为宽度，第二处为高度，第三处为crc32



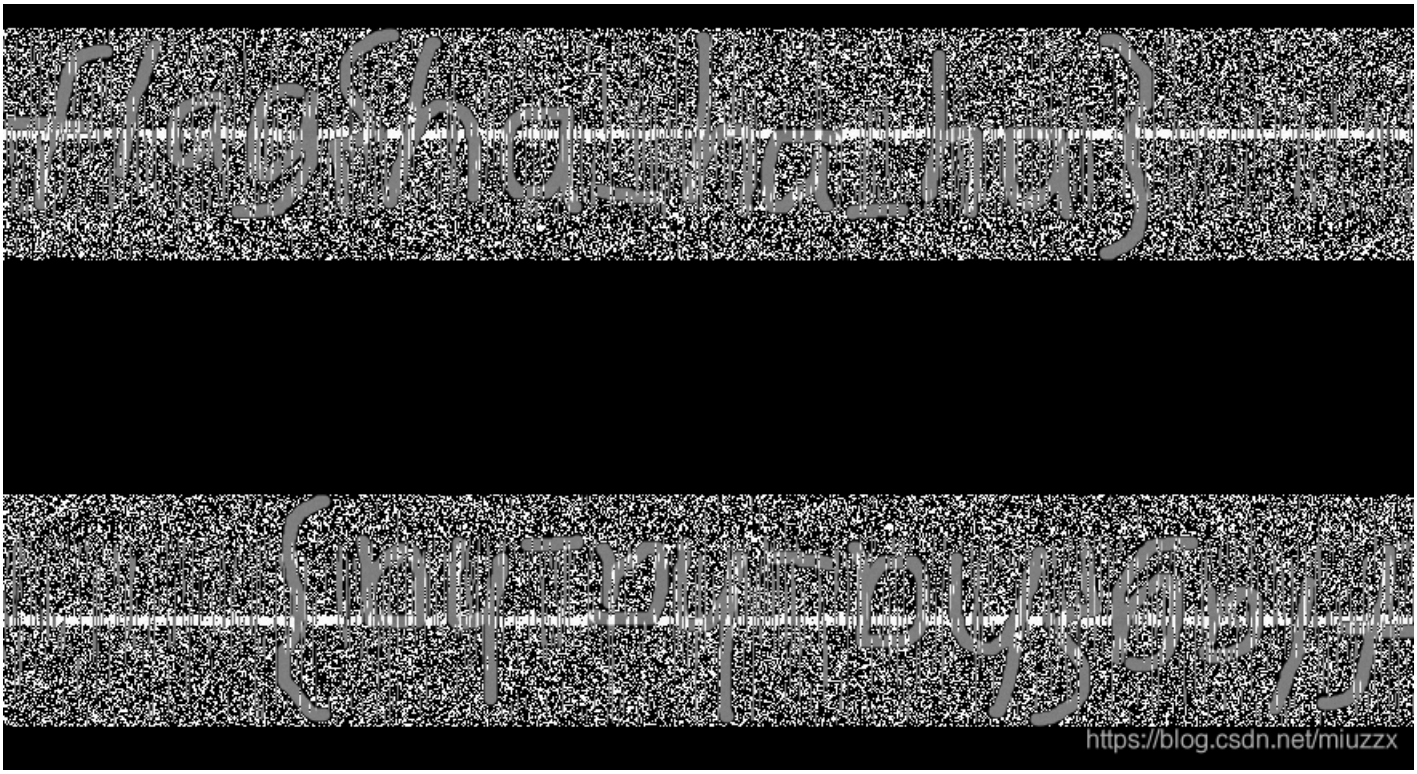
所以对于上面的脚本，不同的图片只要修改crc32的值即可。

0x03 stega3

解压得到一张图片，010editor查看，16进制的末尾有提示是ntfs隐写（前提必须用winrar解压），所以直接上工具（链接：https://pan.baidu.com/s/1Nw70ASUv-sgurDZnFDte4w 提取码：zbw4 ）得到flag.txt文档，打开得flag。

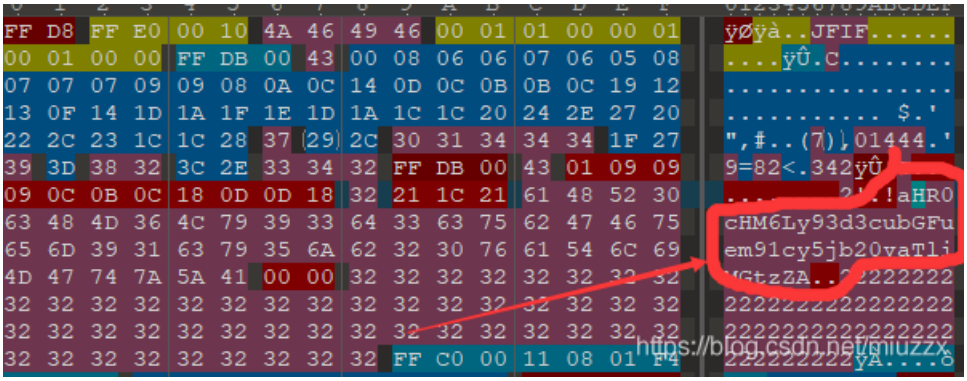
0x04 stega4

两张相同的图片，首先尝试放入stegsolve中，在stegsolve中有图片混合（image combiner）的功能如下图，尝试无果，采用盲水印解密。这里附上工具（链接：https://pan.baidu.com/s/1BoWao6bJ5wvmQqqYJtF-ew 提取码：3tba），对于python脚本，提取图片中的盲水印：`python bwm.py decode 0.png 1.png 2.png` 其中0.png和1.png为得到得两张相同的图片，2.png为解密生成的图片。得到结果如下：



0x05 stega10

在图片的二进制中获取了一串疑似base64的字符串如下，尝试解码，失败，观察到字符串后面还有两个空位，果断添加上两个等于号，成功解密base64，获得一个下载地址。



下载下来以后有一个密码文件夹，一个加密的压缩包。打开密码文件夹，我们发现每一个文档都是一字节，这时我们可以根据文档的crc32爆破里面的值,运行如下脚本得到密码为447^*5#)7

```
import string
import binascii
s=string.printable
c =[0xF3B61B38,0xF3B61B38,0X6ABF4A82,0X5ED1937E,0X09b9265b,0x84b12bae,0x70659eff,0x90b077e1,0x6abf4a82]
password = ''
for crc in c:
    for i in s:
        if crc==(binascii.crc32(i.encode())&0xffffffff):
            password =password + i
 print(password)
```

我在这里再多说一句话，万一我们碰上文件夹中有很多txt怎么办呢，不可能一个一个自己输入吧，我再附上一个比较实用的脚本：

```
import zipfile
import binascii
import string
s=string.printable
f = zipfile.ZipFile("flag.zip")
l = f.namelist()
for i in l:
    for j in s:
        if ".txt" in i:
            if(f.getinfo(i).CRC==binascii.crc32(j.encode())):
                print(j)
```

我们用得到的密码解压加密的压缩包，得到一张图片，但是无法打开，用010editor打开，发现是将图片的16进制逆序了 ，修复脚本如下：

```
f = open("n.png","rb")
f1 = open("m.png","wb")
s = f.read()
s= s[::-1]
f1.write(s)
f.close()
f1.close()
```

得到一张二维码，扫码得到flag

0x06 stega11

我们直接用010editor打开，发现图片中还包含一张图片（字节搜索ffd8），更有趣的是两个图片之间隐藏了一段base32，直接解密得flag