实验吧-ctf-misc

原创

逃课的小学生 于 2018-07-22 18:28:18 发布
分类专栏： misc ctf 实验吧 文章标签： ctf 实验吧 misc

本文链接：https://blog.csdn.net/zhang14916/article/details/81152167

1.欢迎来到地狱

用winhex对第一个jpg文件补头，获取网址https://pan.baidu.com/s/1i49Jhlj，打开得到音乐文件,用Audacity打开获取摩斯电码，破解，获得密码KEYLETUSGO，打开word文档，查看隐藏字符获得image steganography提示，用网页版image steganography解密文档中的哈士奇图片，获得key{you are in finally hell now}，解密zip文件，获得txt与jpg文件，打开txt获得二进制数字，转为字符是“弱口令”，用binwalk检查jpg文件发现zip部分，取出，根据弱口令爆破，得到txt，根据提示
对“VTJGc2RHVmtYMTIwRG9yWjJoVFArNXcweINBOWJYaFZlekp5MnVtRlRTcDZQZE42elBLQ01BPT0=“依次做base64,rabbit,凯撒解密获得唯一一个正常的句子为flag

2.stegas 300

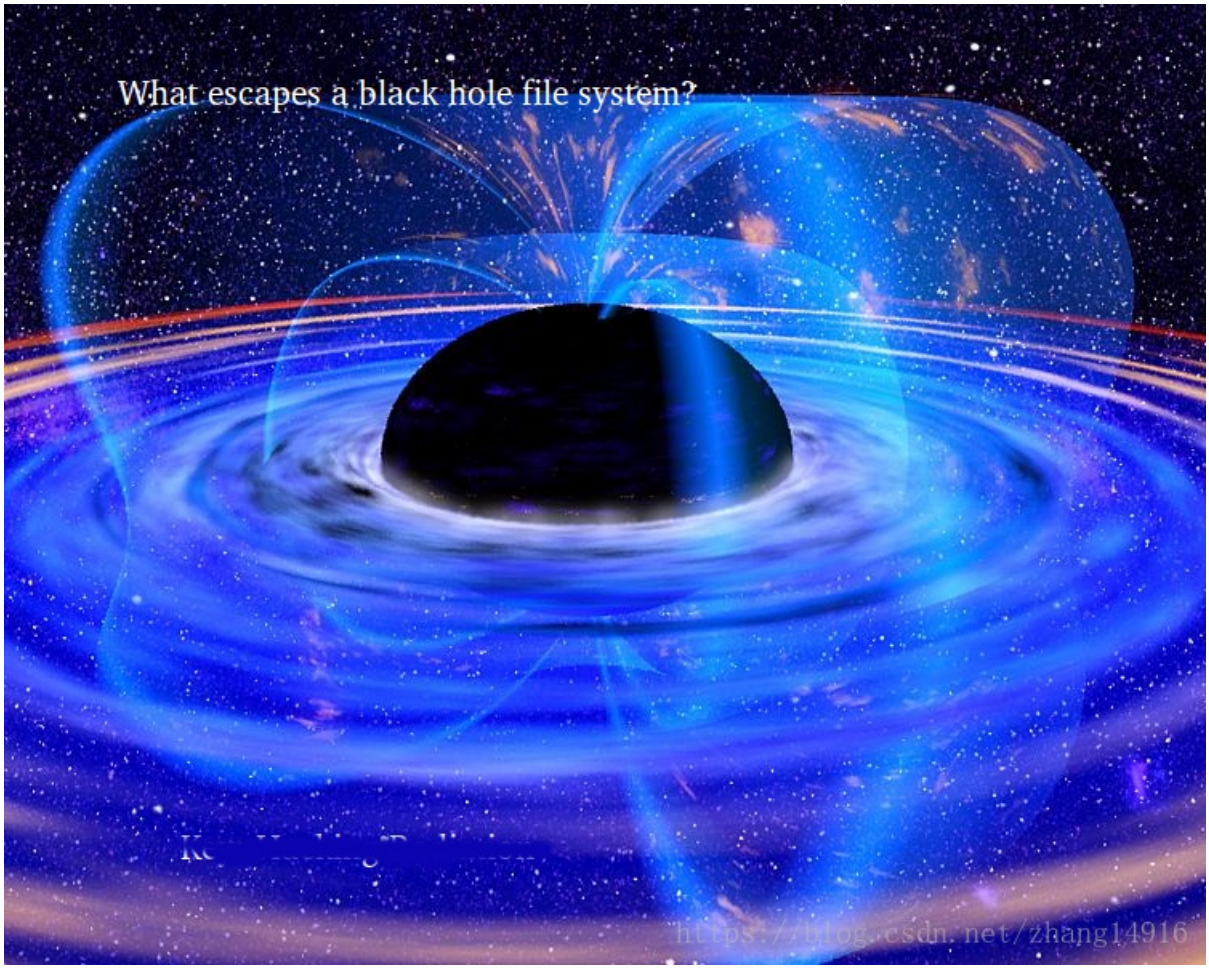
用Audacity打开观察波形发现是（在提示下）曼彻斯特编码（由低到高为0）获得二进制，转为字符是bakdor，然后将其md5加密后的结果输入（题目略有问题）

3.Chromatophoria

根据图片名称使用stegsolve，使用Data Extract,同时选择r,g,b的0获得答案

4.Black Hole

下载获得img，我的Ubuntu无法正常加载，实验吧的writeup也无法使用，使用DiskGenius打开镜像，发现DiskGenius最新版可以找到png文件，但需要专业版才能修复出来。于是就将整个镜像文件打开后去除二进制放入winhex打开，对照DiskGenius将文件取出（先按图片存储位置将图片所在的二进制拿出，在根据文件数据所在簇文件将其中的无用二进制删去，无用二进制大部分是一些\x00组成的字节块），该方法比较麻烦，但最后获得图片可以看到key：



5.心中无码：

使用stegsolve发现b0不太对（在提示下），根据题意去掉图片上的码（即黄色部分）

```
from PIL import Image
lena = Image.open('Lena.png')
pixsels = lena.load()
width=lena.size[0]
height=lena.size[1]
list1=[]
for x in range(0,width):
  for y in range(0,height):
    r,g,b=pixsels[x,y]
    if r==255 and g==255:
      pass
    else:
      if int(bin(b)[-1])==1:
        list1.append(0)
      else:
        list1.append(1)
print len(list1)
im=Image.new("1",(300,300))
i=0
while i<len(list1):
   im.putpixel((i%300,i/300),list1[i])
   i=i+1

im.save("2.png")
```

获得二维码，二维码有些模糊扫描不太成功，对其腐蚀

```
from PIL import Image
lena = Image.open('2.png')
im=Image.new('1',(300,300))
pixsels = lena.load()

for x in range(0,lena.width):
    im.putpixel((x,0),255)
    im.putpixel((x,lena.height-1),255)
for x in range(0,lena.height):
    im.putpixel((lena.width-1,x),255)
    im.putpixel((0,x),255)
for x in range(1,lena.width-1):
  for y in range(1,lena.height-1):
    if (pixsels[x-1, y] == 255) or (pixsels[x, y-1] == 255) or (pixsels[x, y] == 255) or (pixsels[x+1, y] =
        im.putpixel((x,y),255)


im.save("2.bmp")
```

再次扫描获得Brainfuck，在线解码即可

6.黑与白

打开图片获得二维码，下方有一网址，打开网址，没信息，但网址是用大小写字母混合写的，想到培根加密，获得字符“TACP”

将图片放入stegdetect中检测，发现图片可能由jphide加密，使用jphide解密，将刚刚得到的字符串作为密码放入，不行改为小写放入，成功获得结果

7.最低位的亲吻

使用诸多图像无果，想到题目是最低位，从LSB中寻找答案，在看stegsolve中低位中有二维码迹象，决定将图像低位提出组成图片，获得二维码，扫描获得结果（附python代码）：

```
from PIL import Image
lena = Image.open('01.bmp')
im=Image.new('1',lena.size)
pixsels = lena.load()
width=lena.size[0]
height=lena.size[1]

for x in range(0,width):
  for y in range(0,height):
      g=pixsels[x,y]
      im.putpixel((x,y),int(bin(g)[-1]))


im.save("2.bmp")
```

8.无处不在的广告

将图片放在stegsolve中，在通道red plane0中可获得二维码，反色扫描即可

9.想看正面？那就要看仔细了！

根据提示仔细看图片信息，在文件详细信息备注中发现字符串，填入不太对，发现字符串长度为8，然后用base64解码可得

10.打不开的文件

文件无法显示，猜测缺少头部，用winhex补入gif头部“47494638“，发现动态图，放入ps中逐帧查看获得key

11.py的交易

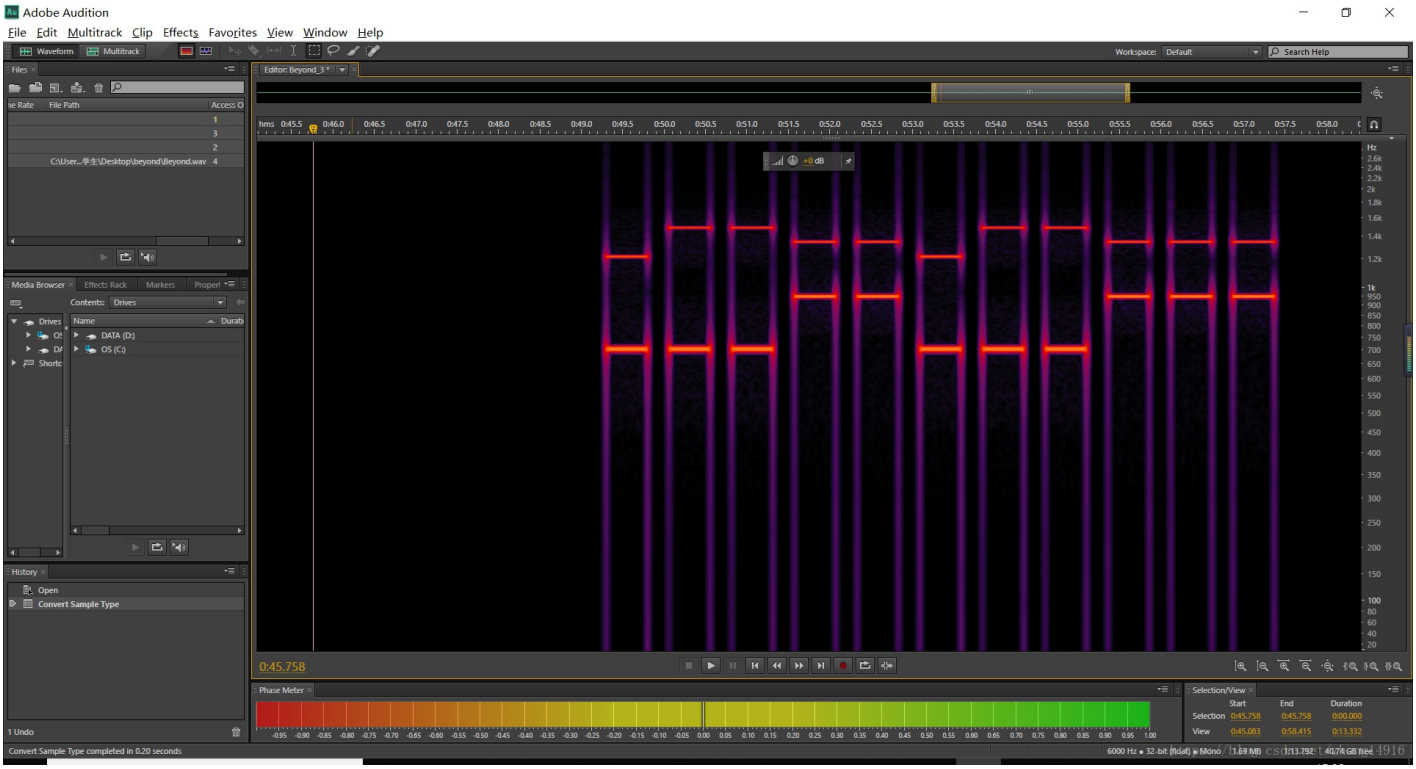
用ps打开图片会提示有adobe fireworks的数据，用adobe fireworks打开图片，发现还有一层是二维码，取出扫描获得16进制字符，看数字头“03f30d0a”可知是pyc文件，进行反编译（可以下工具，也可以在线找python反编译https://tool.lu/pyc/）即可

12.IHDR

首先发现题目中的图片无法打开，但又好像能看到，而题目中IHDR是png头部一个数据段，由width，height，Bit depth，ColorType，Compression method，Filter method，Interlace method构成（具体请百度)，猜测IHDR有问题，用TweakPNG打开提示crc错误，纠正后打开图片依旧看不到key，更改IHDR中其他数据，更改height发现可以看到key（可以用斌walk的结尾和winhex打开文件实际结尾差好多看出）

13.beygond

用binwalk发现这是一个zip文件，改后缀解压获得wav文件，用Adobe Audition CS6打开发现有一个通道频率比较奇怪，点击文件右键提取通道获得该通道获得取出后查看频率（可以改变下方有个有关频率的地方能看的清楚一些），与DTMF编码对照翻译获得“13300133000”即为flag



14.LSB

使用binwalk检测图片发现是bmp，改后缀，题目提示LSB，而查询stegsolve data extract无果（此时直接使用wbStego运行即可得到答案），即可决定将图片最后一位提取出来观察，由于图片是bmp类型，像素在图片中是倒叙存储，即以b,g,r的方式存储，而且当高度为正时图片中最后一行像素是存储在第一行的位置（对于正常二位坐标系，当以左下角为原点高度才会为正），用PIL的getdata读出的像素只是像素点在图片的相对位置，并非在文本文件的相对位置（试一下就明白了），所以我们以文本文件的方式读取图片

```
bmpfi=open("nvshen.bmp","rb")
bmpstr=bmpfi.read()
bmpfi.close()
bfOffBits=int(bmpstr[13:9:-1].encode("hex"),16)
str1=""
for j in xrange(bfOffBits,len(bmpstr)):
  str1+=bin(ord(bmpstr[j]))[-1]
i=0
lst=""
while i<len(str1):
  str2=str1[i:i+8]
  lst+=chr(int(str2,2))
  i=i+8

fi=open("1",'wb')
fi.write(lst)
fi.close()
```

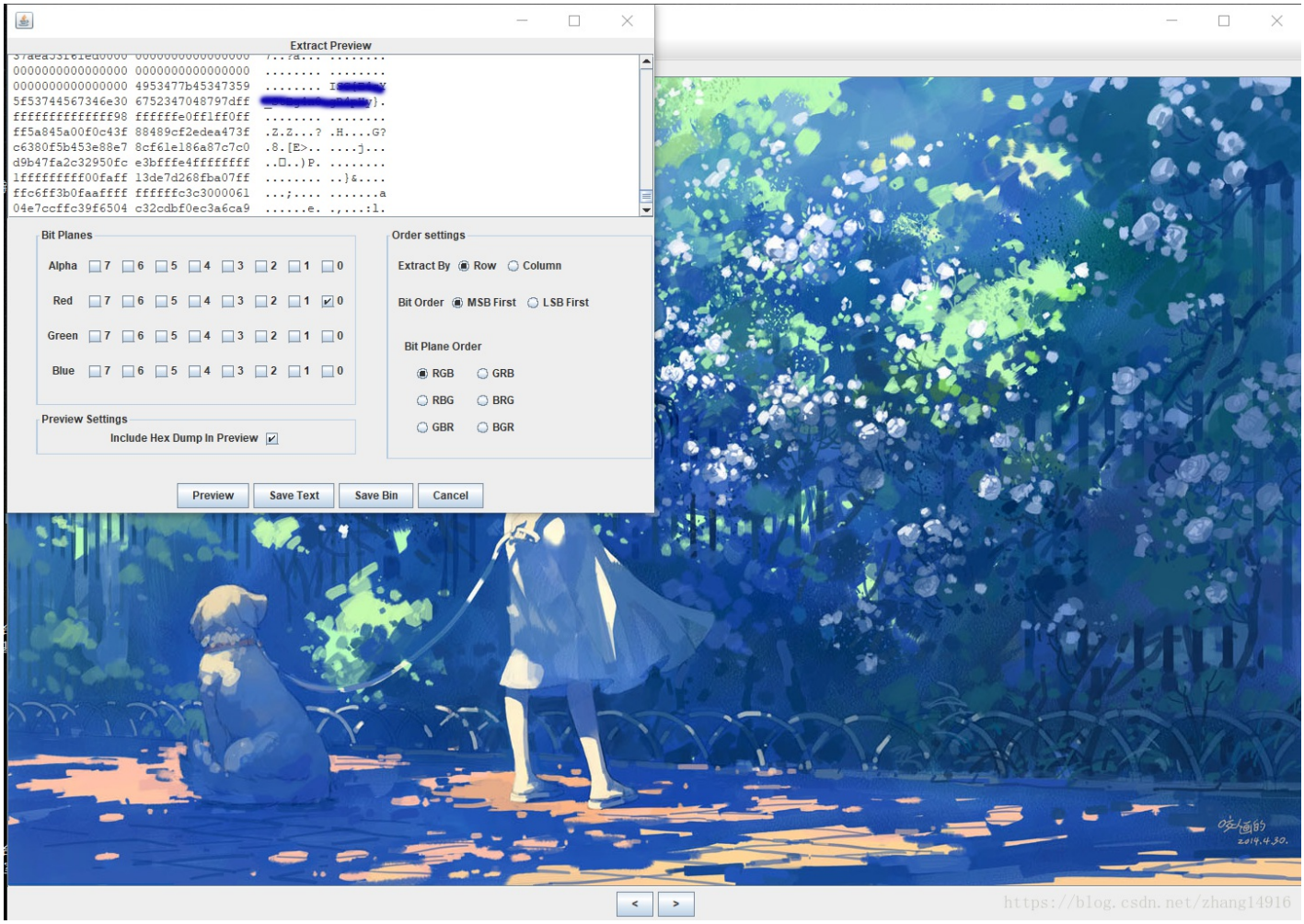
将最后得到的文件放入winhex也可得到结果

15.SB！SB！SB!

直接使用stegsolve，在Red plane 0可获得二维码，扫描即可

16.当眼花的时候，会显示两张图

使用binwalk发现文件是由两张png组合而成的，分开，放在winhex中观察发现两个文件中字节数不同，分别是1d55db和1d5648于是将使用stegsolve对图片做减法，发现得到的图片最下角有一条红色的线，猜想相对大一些的图片可能是在结尾加入了密码字符而导致两个文件字节数不相同，将做完减法的图片放入stegsolve观察发现在Red plane 0处线短的很厉害，基本可以确定在图像结尾处添加了对r使用了低位加密的像素点，将大一点（1d5648）的图像放入stegsolve，用stegsolve的data extract选择red0得到结果观察字符串尾部，即可发现key



17.听会歌吧

这个题和隐写关系不大，打开连接是一个网页和两首歌，对两首歌进行检查没有发现问题，打开网页源代码，发现两首歌的连接url都是base64，解密后与文件名相同。同时在源代码我们只发现了download.php，我们可以尝试打开该文件，于是将url改为download.php的base64，即download.php?url=ZG93bmxvYWQucGhw，获得代码

```php
 <?php
error_reporting(0);
include("hereiskey.php");
$url=base64_decode($_GET[url]);
if( $url=="hereiskey.php" || $url=="buxiangzhangda.mp3" || $url=="xingxingdiandeng.mp3" || $url=="download.
 $file_size = filesize($url);
 header ( "Pragma: public" );
 header ( "Cache-Control: must-revalidate, post-check=0, pre-check=0" );
 header ( "Cache-Control: private", false );
 header ( "Content-Transfer-Encoding: binary" );
 header ( "Content-Type:audio/mpeg MP3");
 header ( "Content-Length: " . $file_size);
 header ( "Content-Disposition: attachment; filename=".$url);
 echo(file_get_contents($url));
 exit;
}
else {
 echo "Access Forbidden!";
}
?>
```

看到可以其中有hereiskey.php文件，用相同方式对该文件访问，得到结果