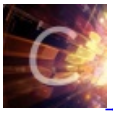
【Writeup】华山杯CTF2016 Forensics部分

原创

KAlbertLee 于 2016-09-12 20:31:44 发布 2812 收藏 1
分类专栏： CTF 文章标签： CTF 攻防 writeup

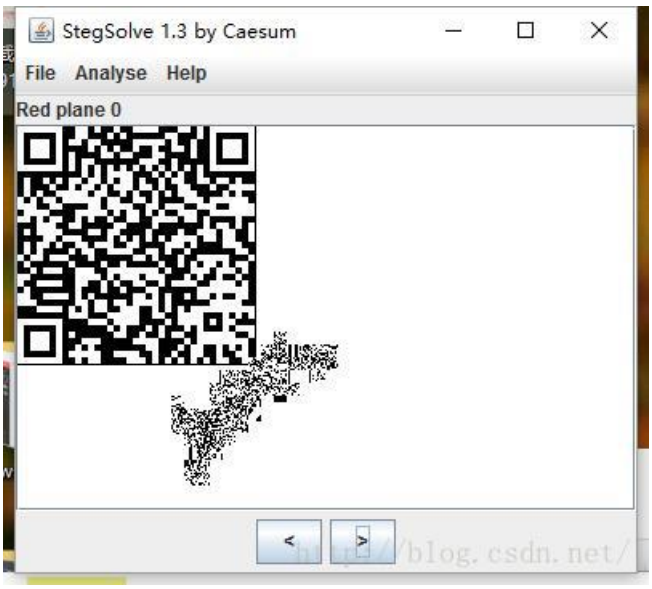


来自2016.09.10的华山杯，新鲜滚热辣的writeup Forensics部分

*0x01.*蒲公英的约定

很简单的图片隐写

使用StegSolve，查看Red plane0（Blue0，Green0都可以），可以看见一个二维码



反色一下可扫

得到一串编码，使用base32解密

base32.py

```
from base64 import *
print b32decode('MZWGCZ27LBSHW2CTNBPWG5DGHJKTE4ZQL5RW63ZRPU======')
```

得到flag

*0x02.*什么鬼

首先是一个暴漫图片

修改后缀成.zip压缩包，发现里面有图片，压缩包被加密，指示密码长度为4位

使用zip破解软件爆破密码，得到密码19bZ

得到一幅二维码

右上角缺失了一个标志块，使用PS修复一下

扫描得到flag：flag_Xd{hSh_ctf:H@ve_fun.}

*0x03.*洪荒之力

Famous: The interview with journalists from CCTV was shared thousands of times online

得到名为fuyuanhui.jpg的图片

不会做。。。。。。现场只做出来4组，期待大神解答

*0x04.*客官，听点小曲儿？

得到一首歌，是周董的《分裂》，猜测里面是不是有其他文件，需要“分裂”开，但是使用binwalk无果

查看下载页面的数据包头，发现有一个key：cheers

Response Header Name	Response Header Value
Status	OK - 200
Server	nginx/1.4.6 (Ubuntu)
Date	Mon, 12 Sep 2016 08:38:26 G
Content-Type	text/html
Content-Length	105
Connection	keep-alive
X-Powered-By	PHP/5.5.9-1ubuntu4.19
key	cheers
Vary	Accept-Encoding
Content-Encoding	gzip

猜测是MP3Stego，遂解密

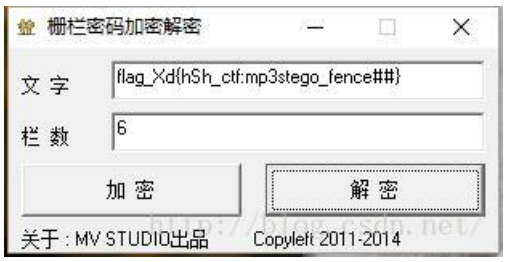
Decode.exe -X -P cheers song.mp3

```
E:\学习资料\CTF\工具\解密\隐写MP3Stego_1_1_18\MP3Stego>Decode.exe -X -P cheers song.mp3
MP3StegoEncoder 1.1.17
See README file for copyright info
Input file = 'song.mp3'  output file = 'song.mp3.pcm'
Will attempt to extract hidden information. Output: song.mp3.txt
the bit stream file song.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=0, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=stereo, sblim=32, jsbd=32, ch=2
[Frame 9747]Avg slots/frame = 417.917; b/smp = 2.90; br = 127.987 kbps
Decoding of "song.mp3" is finished
The decoded PCM output file name is "song.mp3.pcm"
```


得到一个txt，里面有一段字符，很像flag，只不过是顺序乱了

fdc3_#l{tsf#ahfte}gS:en_hmgcX_poe

使用栅栏密码解密，栏数为6



得到flag：flag_Xd{hSh_ctf:mp3stego_fence##}