实验吧隐写术WP（四）

原创

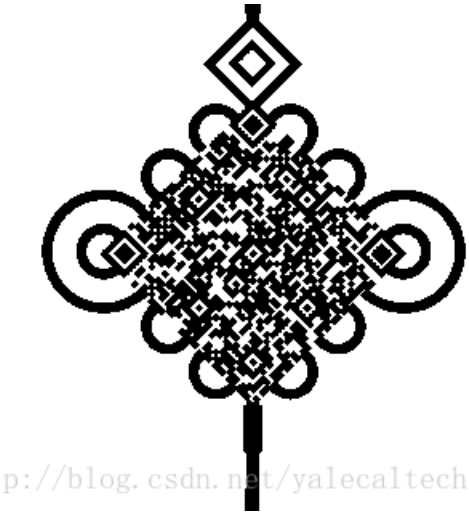
Neil-Yale 于 2017-04-02 12:13:44 发布 5849 收藏 1

文章标签： 二维码 unicode base64 CTF

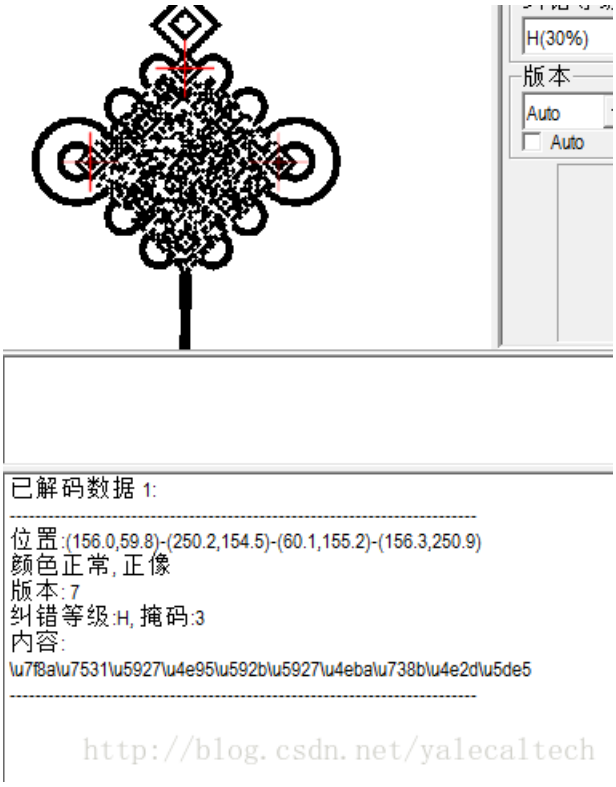
本文链接：https://blog.csdn.net/yalecaltech/article/details/68951550

1.小苹果（http://www.shiyanbar.com/ctf/1928）

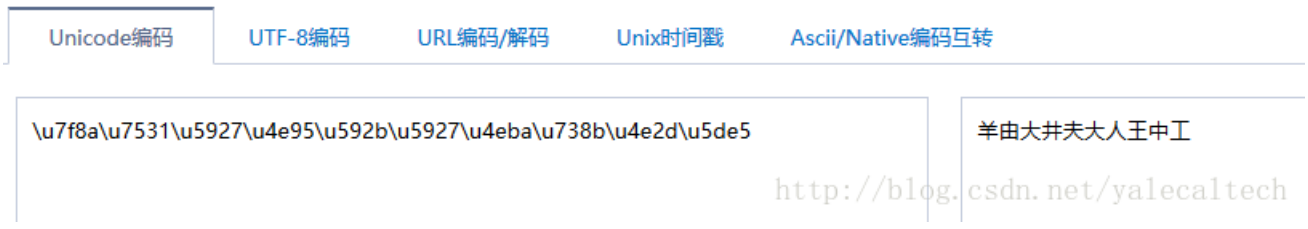
stegsolve发现了二维码



扫描得到unicode



unicode解密得到当铺



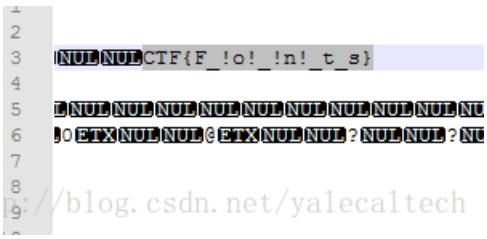
当铺解码得到数字9158753624

这条线结束了，再binwalk发现图片是zip
解压得到mp3,尝试mp3stego
得到txt，打开就是flag了

```
Microsoft Windows [版本 10.0.14393]
(c) 2016 Microsoft Corporation。保留所有权利。

C:\Users\hasee>cd C:\Users\hasee\Desktop\CTF工具\MP3Stego_1_1_16\MP3Stego_1_1_16\Development\MP3Stegos
系统找不到指定的路径。

C:\Users\hasee>cd C:\Users\hasee\Desktop\CTF工具\MP3Stego_1_1_16\MP3Stego_1_1_16\Development\MP3Stego

C:\Users\hasee\Desktop\CTF工具\MP3Stego_1_1_16\MP3Stego_1_1_16\Development\MP3Stego>Decede.exe -X -P 9158753624 apple.mp
3
'Decede.exe' 不是内部或外部命令，也不是可运行的程序
或批处理文件。

C:\Users\hasee\Desktop\CTF工具\MP3Stego_1_1_16\MP3Stego_1_1_16\Development\MP3Stego>Decode.exe -X -P 9158753624 apple.mp
3
MP3StegoEncoder 1.1.16
See README file for copyright info
Input file = 'apple.mp3'  output file = 'apple.mp3.pcm'
Will attempt to extract hidden information. Output: apple.mp3.txt
the bit stream file apple.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 1213]Avg slots/frame = 417.617; b/smp = 2.90; br = 127.895 kbps
Decoding of "apple.mp3" is finished
The decoded PCM output file name is "apple.mp3.pcm"

C:\Users\hasee\Desktop\CTF工具\MP3Stego_1_1_16\MP3Stego_1_1_16\Development\MP3Stego>
```

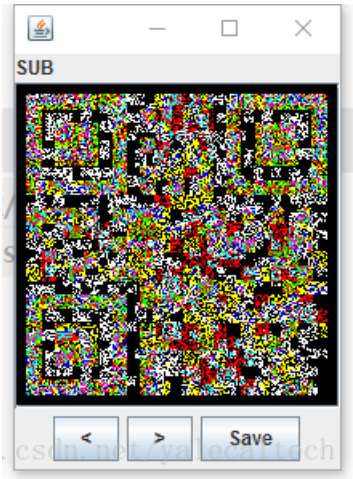

这个flag是base64过的，解码就可以了

2.Fonts(http://www.shiyanbar.com/ctf/1927)
连word都不放过，太没有人性了，打开居然是空白。。
notepad++打开直接搜索字符串CTF

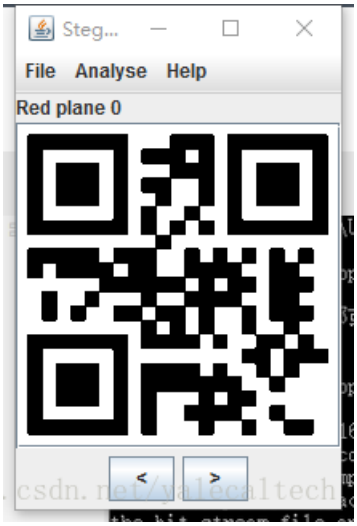


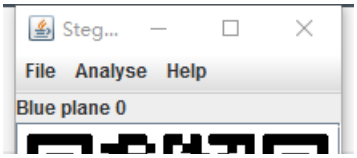
得到flag

3.男神一般都很低调很低调的！！（http://www.shiyanbar.com/ctf/1926）
打开后是两张图片，stegsolve来combine一下，发现了疑似二维码的东西



（这里需要对它反色处理，不然之后的步骤只能出来一个二维码）
处理后回到stegsolve
发现扫出三张清晰的二维码





分别扫描得到


QR Research
文件(F) 工具(T) 帮助(H)
File Analyse Help
Red plane 0
数据
纠错等级
H(30%)
掩码
Auto
版本
Auto
Auto
尺寸
4
已解码数据 1:
位置:(15.2,81.2)-(202.8,81.2)-(15.2,268.8)-(202.8,268.8)
颜色正常, 正像
版本:1
纠错等级:L, 掩码:2
内容:
DES
解码完成
http://blog.csdn.net/yalecaltech


File Analyse Help
Green plane 0
数据

```
----------------------------------------------------------------

已解码数据 1:

----------------------------------------------------------------
位置:(15.2,81.2)-(202.8,81.2)-(15.2,268.8)-(202.8,268.8)
颜色正常,正像
版本: 1
纠错等级:L,掩码:2
内容:
6XaMMbM7
```



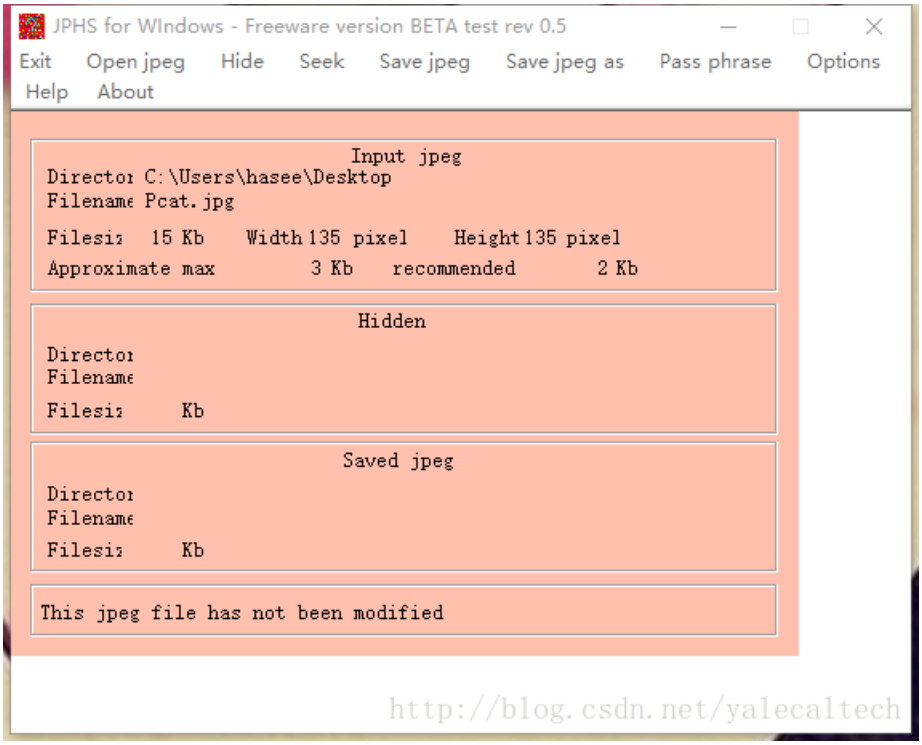
```
----------------------------------------------------------------

已解码数据 1:

----------------------------------------------------------------
位置:(15.5,81.5)-(202.5,81.5)-(15.5,268.5)-(202.5,268.5)
颜色正常,正像
版本: 4
纠错等级:L,掩码:2
内容:
U2FsdGVkX18IBEATgMBe8NqjIqp65CxRjjMxXIIUxIjBnAODJQRkSLQ/+IHBsjpv1BwwEawMo1c=
----------------------------------------------------------------
```


分别是DES（加密方式），密钥，和密文
解密即可

4.黑与白（http://www.shiyanbar.com/ctf/1925）
这题很容易误解，我直接说正确的做法吧
涉及到隐写，那么我们用stegdetect看看是用什么方式隐写的

百度jphide
然后使用

然后使用



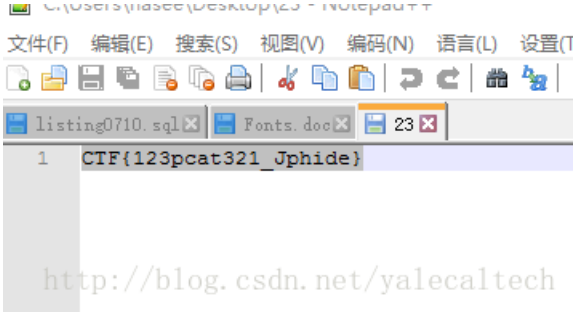
点击seek查找隐藏文件时要求输入密码
密码哪里来呢？我们先扫扫二维码，得到

一个网址还搞什么大小写，肯定有问题
但是我不知道什么问题。。大神提示01
于是想到培根，把大写看作A，小写看作B，或者反之，看看哪个解密出来像就行了
HttPp BAABA t

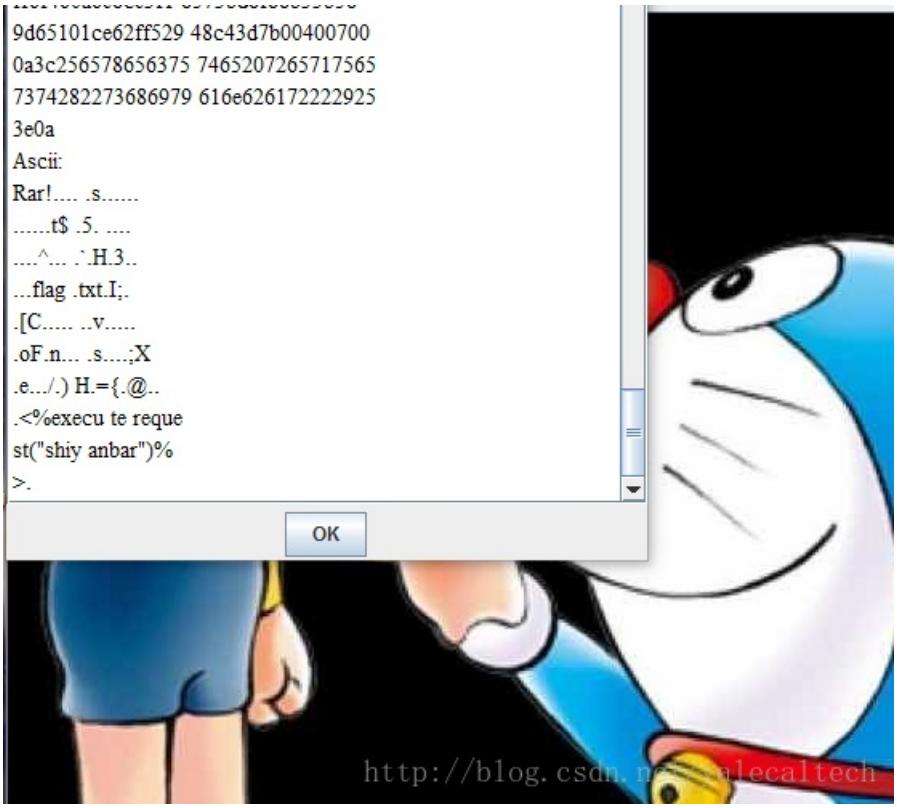
catcn AAAAA a

bloGs AAABA c

cOMHh ABBBA p
密码：tacp
再解密就行了
得到hidden的文件



5.大雄和哆啦A梦（http://www.shiyanbar.com/ctf/1916）
放到stegsolve分析format看到



看到有价值的东西：1.rar2.shiyanbar
改后缀解压时发现需要密码，我们用shiyanbar发现不对，题目是base，于是用base64后的shiyanbar解压，得到flag.txt，里面就是flag