

# MISC-3

原创

Re1y0n  于 2021-08-10 18:19:02 发布  276  收藏 3

分类专栏: [CTF](#) 文章标签: [其他](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/qdlws/article/details/119392688>

版权



[CTF 专栏收录该内容](#)

12 篇文章 0 订阅

订阅专栏

## 题目目录

**SimpleRAR:**

**embarrass:**

**pure\_color:**

**a\_good\_idea:**

**快乐游戏题:**

**Test-flag-please-ignore:**

**glance-50:**

**hit-the-core:**

**Training-Stegano-1:**

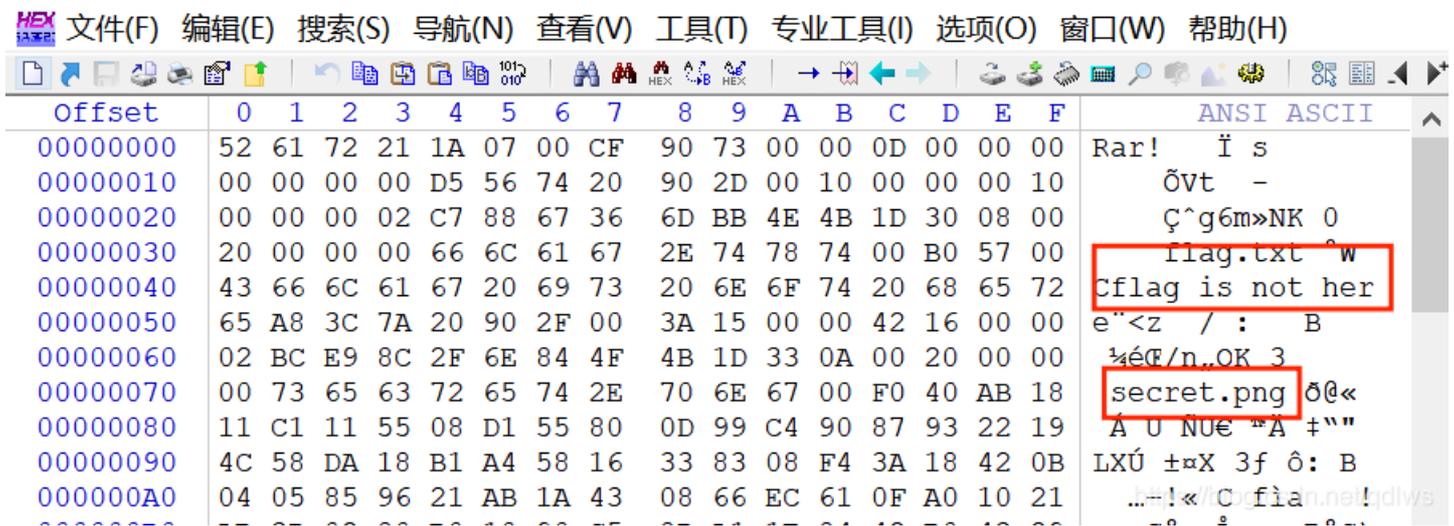
## SimpleRAR:

菜狗最近学会了拼图, 这是他刚拼好的, 可是却搞错了一块(ps:双图层)

使用360压缩打开



使用winhex打开，在右边的框框的内容全部看了一遍，只找到了secret.png，secret.png就在here后面



百度rar的文件头

每一个块都是由以下域开始的：

HEAD\_CRC 2 bytes: 整个块或者某个部分的CRC

HEAD\_TYPE 1 bytes: 块类型

已经声明过的快类型包括：

HEAD\_TYPE = 0x72: 标志块

HEAD\_TYPE = 0x73: 归档头部块

HEAD\_TYPE = 0x74: 文件块

HEAD\_TYPE = 0x75: 老风格的 注释块

HEAD\_TYPE = 0x76: 老风格的 授权信息块/用户身份信息块

HEAD\_TYPE = 0x77: 老风格的 子块

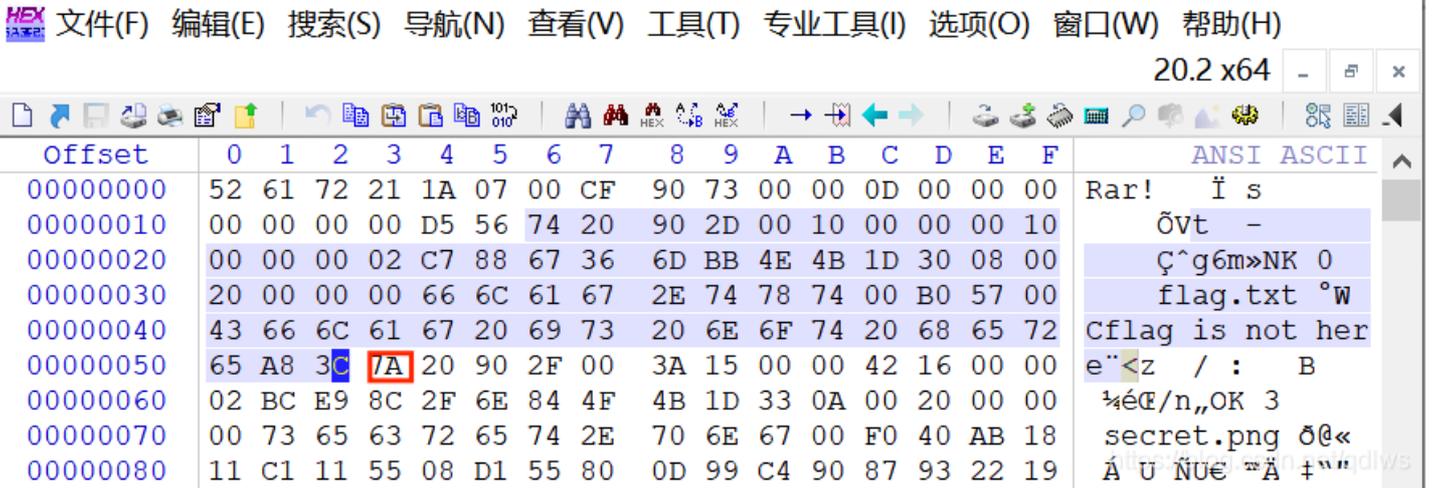
HEAD\_TYPE = 0x78: 老风格的 恢复记录块

HEAD\_TYPE = 0x79: 老风格的 授权信息块/用户身份信息块

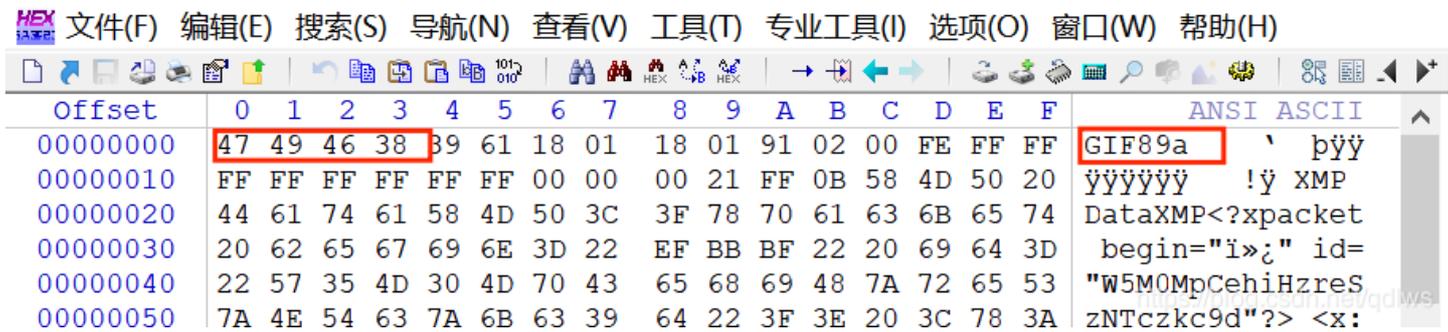
HEAD\_TYPE = 0x7a: 子块

HEAD\_TYPE = 0x7b: 结束块

我们需要的是文件块而不是子块，所以将7a改为74后保存



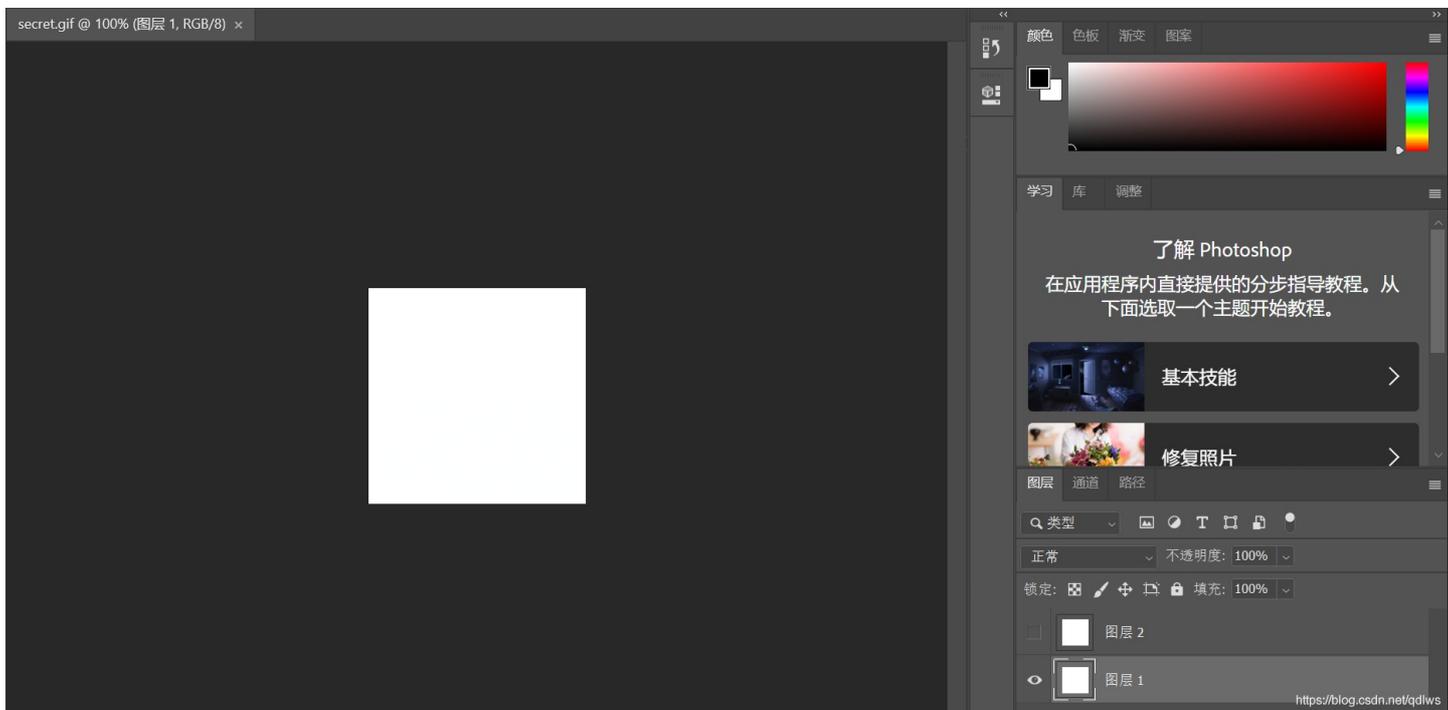
再次查看rar，发现secret.png出现了，但是无法正常打开，使用winhex打开secret.png，发现这是GIF格式



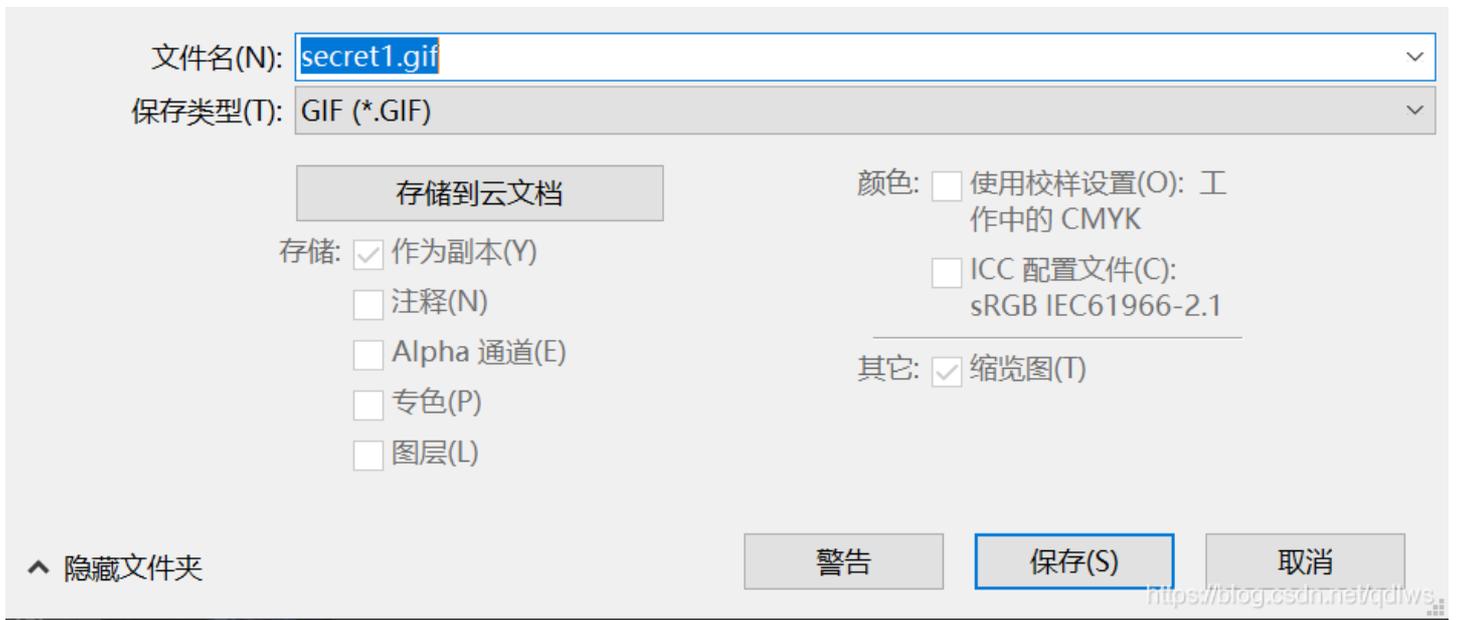
文件头文件尾总结：<https://www.cnblogs.com/lwy-kitty/p/3928317.html>.

常见文件文件头：<https://blog.csdn.net/zhembrace/article/details/52717559>.

由题目已知有两个图层，将后缀改成GIF用ps打开



将两个图层都保存下来，保存图层1，点击图层 - 复制图层 - 确定，再点击文件 -> 储存 -> 保存



将保存的两个图层用stegsolve打开，stegsolve下载地址<http://www.caesum.com/handbook/Stegsolve.jar>.

如果Java环境配置没有问题，但是双击打不开的话，打开cmd

```
java -jar 下载路径\stegsolve.jar
```

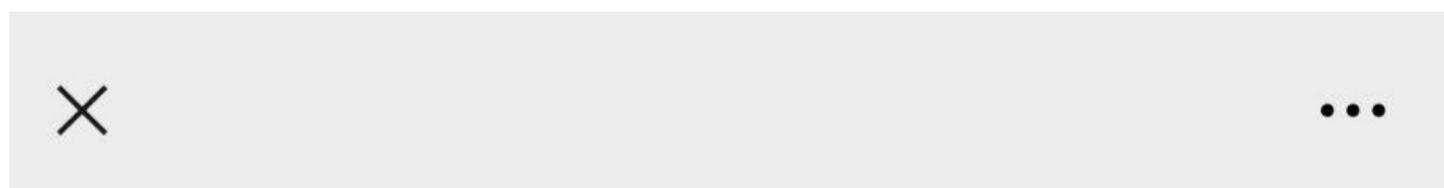
将两个图层都打开，点击箭头，出现半个二维码



然后就是拼接了，使用PPT拼接更方便一些



微信扫一扫得到flag



flag{yanji4n\_bu\_we1shi}

<https://blog.csdn.net/qdlws>

为我的学长的公众号打个广告，关注公众号ScienceCloud 科学云，对话框回复Adobe2020即可获得Adobe全家桶的百度网盘链接：<https://mp.weixin.qq.com/s/IVy7pVLnQiedakderQZdFg>。全家桶中所有的软件均已破解，我用的就是全家桶中的ps

**embarrass:**



**embarrass**  31 最佳Writeup由随便娶一个 • jerrita提供

难度系数:  1.0

题目来源: [ciscn-2017](#)

题目描述: 暂无

题目场景: 暂无

题目附件: [附件1](#)

<https://blog.csdn.net/qdlws>

用notepad++打开->CTRL+F->输入flag->点击find next，最后找到flag

**pure\_color:**

pure\_color  最佳Writeup由老乐与涛·Sla提供

难度系数: 

题目来源: [school-ctf-winter-2015](#)

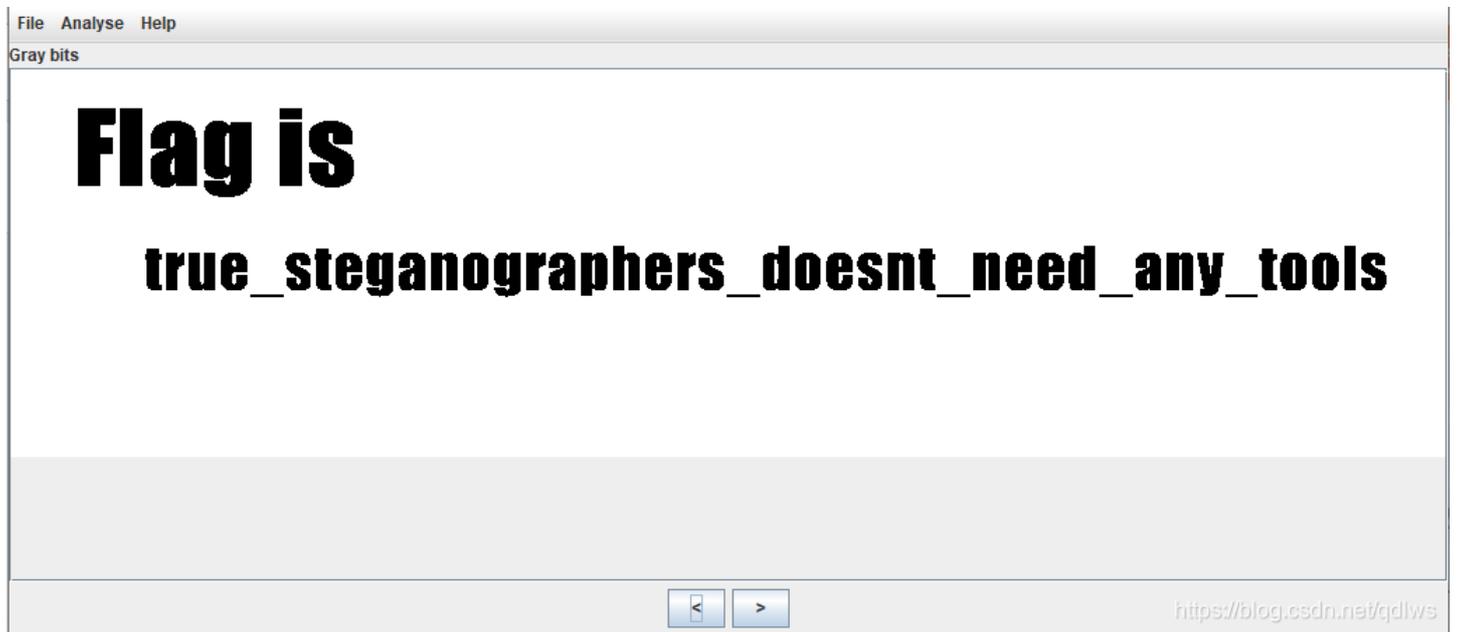
题目描述: 格式为flag{xxxxxx}

题目场景: 暂无

题目附件: [附件1](#)

<https://blog.csdn.net/qdlws>

打开附件，是一个png图片，纯白，果然是纯净的颜色，使用Stegsolve打开，点箭头得到flag



[a\\_good\\_idea:](#)

a\_good\_idea

👍 10

最佳Writeup由admin提供

难度系数:

★ 1.0

题目来源:

2019\_NJUPT\_CTF

题目描述: 汤姆有个好主意

题目场景: 暂无

题目附件:

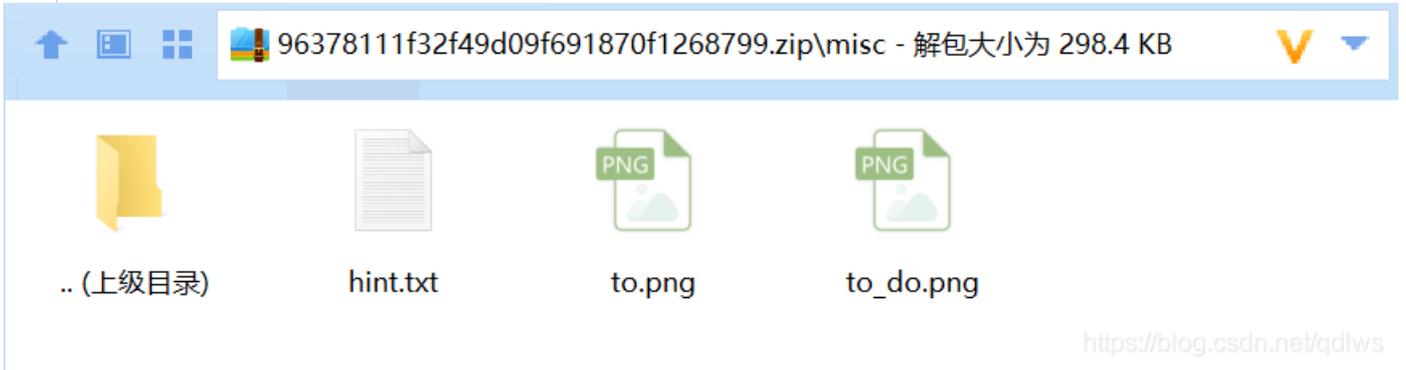
附件1

<https://blog.csdn.net/qdlws>

直接打开和改成zip再打开非常不同（这个是十几年前流行过的技巧，原理就是利用命令行下的copy来合并不同的文件，合并后的文件实际上内部包含了多个不同的文件，解压缩软件会跳过其中与扩展名不符的内容）



<https://blog.csdn.net/qdlws>



<https://blog.csdn.net/qdlws>

## try to find the secret of pixels

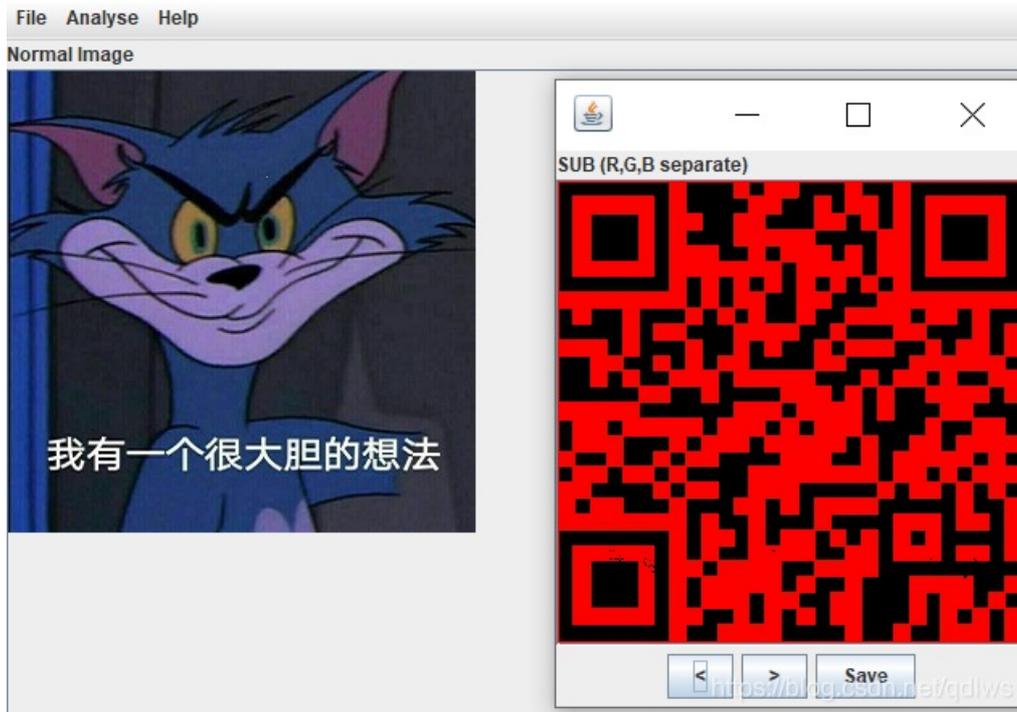
### 翻译

试着找到像素的秘密

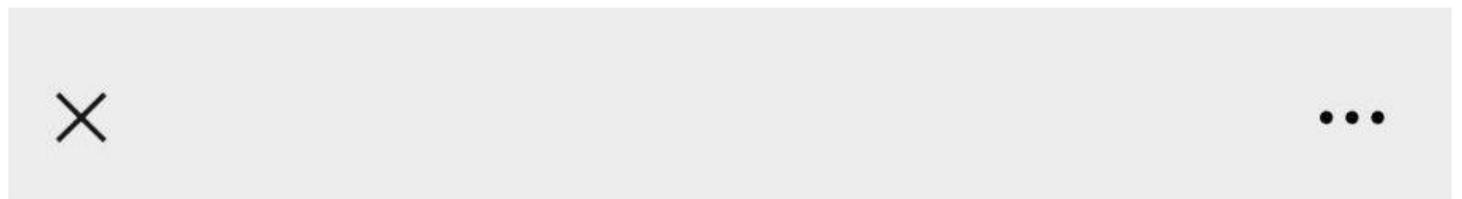


<https://blog.csdn.net/qdlws>

使用stegsolve打开to\_do.png，Analyse->Image Combiner->to.png，箭头...箭头得到二维码（先打开to.png再拼接to\_do.png得不到二维码）



扫一扫得到flag



NCTF{m1sc\_1s\_very\_funny!!!}

<https://blog.csdn.net/qdlws>

快乐游戏题:

# 快乐游戏题

👍 17

最佳Writeup由admin提供

难度系数: ★ 1.0

题目来源: 2019\_UNCTF

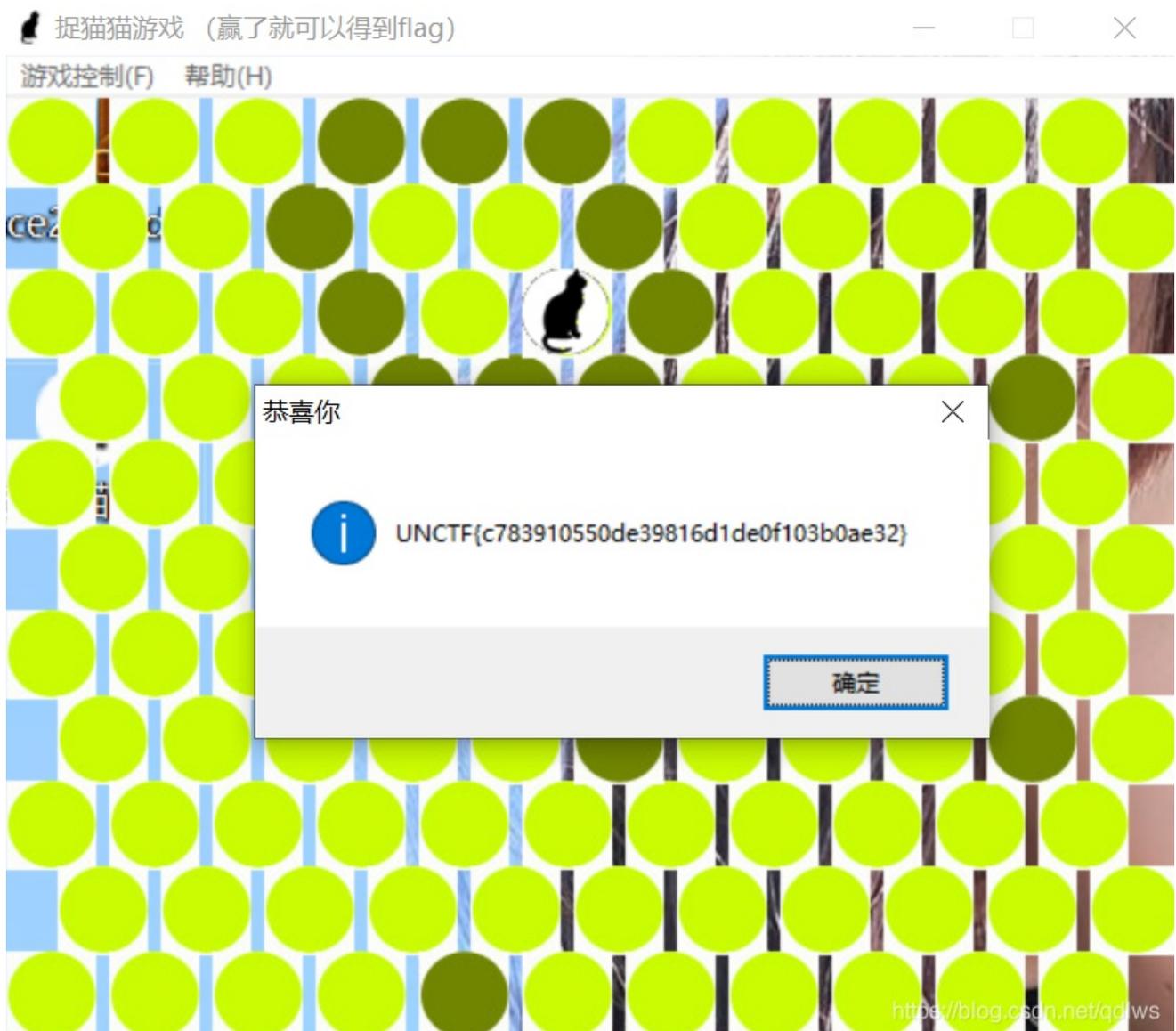
题目描述: 暂无

题目场景: 暂无

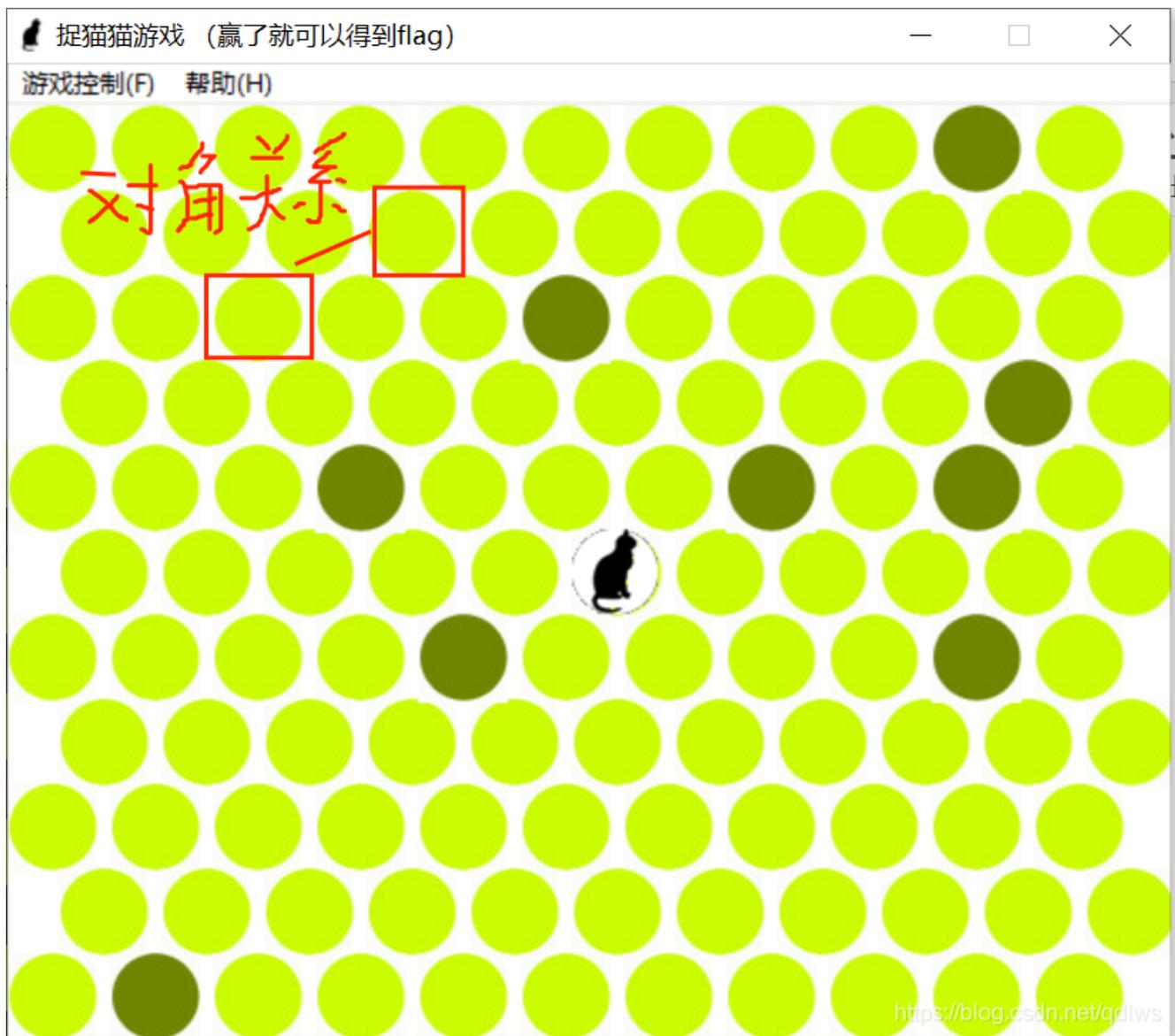
题目附件: 附件1

<https://blog.csdn.net/qdlws>

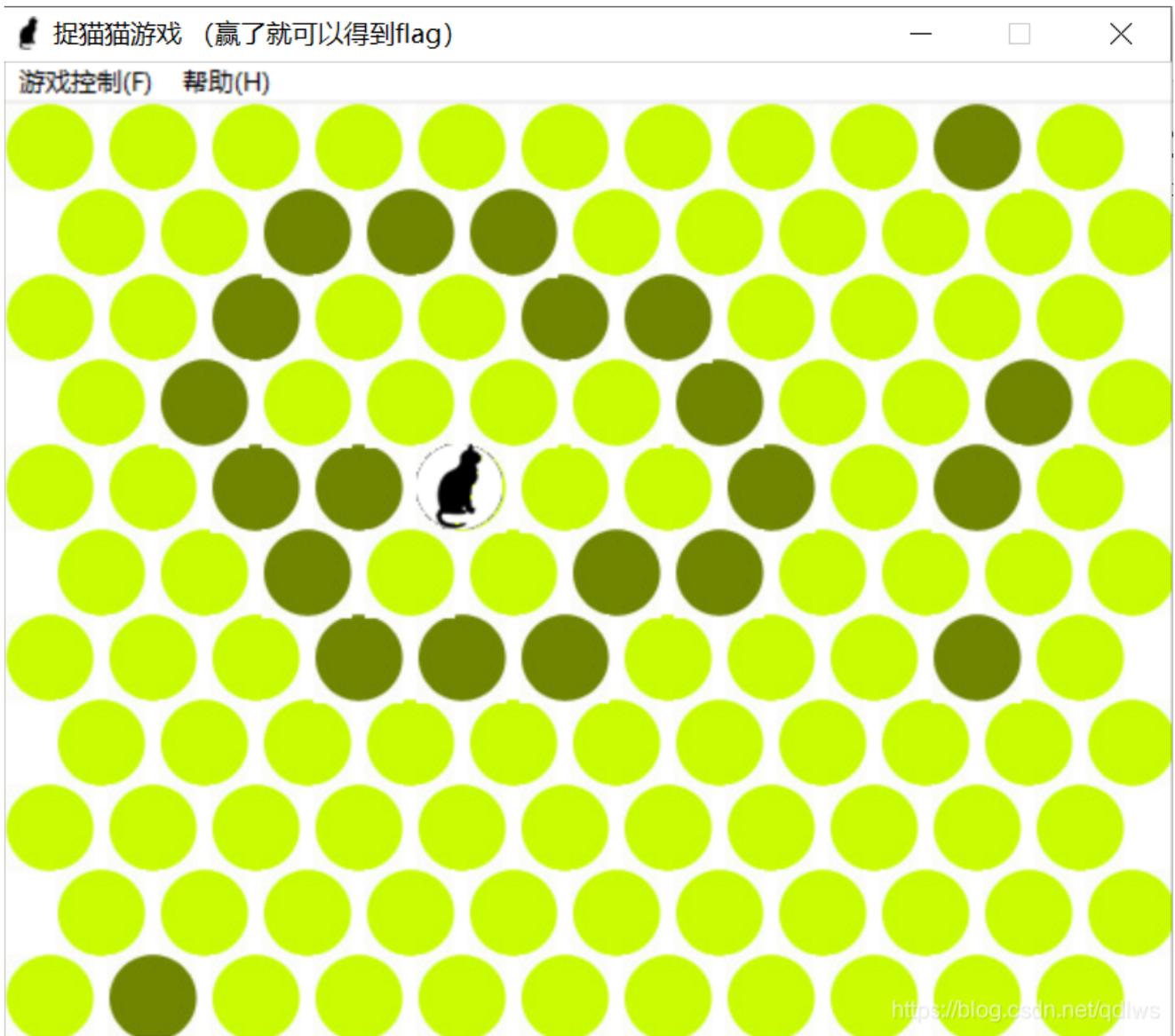
附件1解压得到一个‘捉猫猫.exe’文件，是一个小游戏，试了三次通关了



太快乐了，又忍不住玩了十几次，猫猫会优先往左上跑



在猫猫往左上角跑之前先在左上角建立许多的对角关系，等猫猫跑到一半再封锁其他三个角



最后形成合围之势，势不可挡

**Test-flag-please-ignore:**

## Test-flag-please-ignore

最佳Writeup由 **B301** • dals 提供

难度系数: ★ 1.0

题目来源: `tinyctf-2014`

题目描述: 暂无

题目场景: 暂无

题目附件: `附件1`

<https://blog.csdn.net/qdlws>

附件1是一个没有后缀的文件，添加.txt打开

\*misc10.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

666c61677b68656c6c6f5f776f726c647d

将这一串字符串进行两两分组，每一组的第一个字符在5到7之间，是ASCII码没错了，与ASCII对照表进行对照得到flag

\*misc10.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

66 6c 61 67 7b 68 65 6c 6c 6f 5f 77 6f 72 6c 64 7d  
f l a g { h e l l o \_ w o r l d }

## glance-50:

### glance-50

👍 28 最佳Writeup由 **Kyrie** • **KyrieKiki** 提供

难度系数: ★ 1.0

题目来源: [mma-ctf-2nd-2016](#)

题目描述: 暂无

题目场景: 暂无

题目附件: [附件1](#)

<https://blog.csdn.net/qdlws>

附件1是一个GIF动态图



使用GIF动态图分解得到flag

本地上传  网络图片

浏览... 9266eadf3...0c50.gif



hit-the-core:

# hit-the-core

👍 13

最佳Writeup由0xfafu-1 • giun提供

难度系数: ★ 1.0

题目来源: alexctf-2017

题目描述: 暂无

题目场景: 暂无

题目附件: 附件1

<https://blog.csdn.net/qdlws>

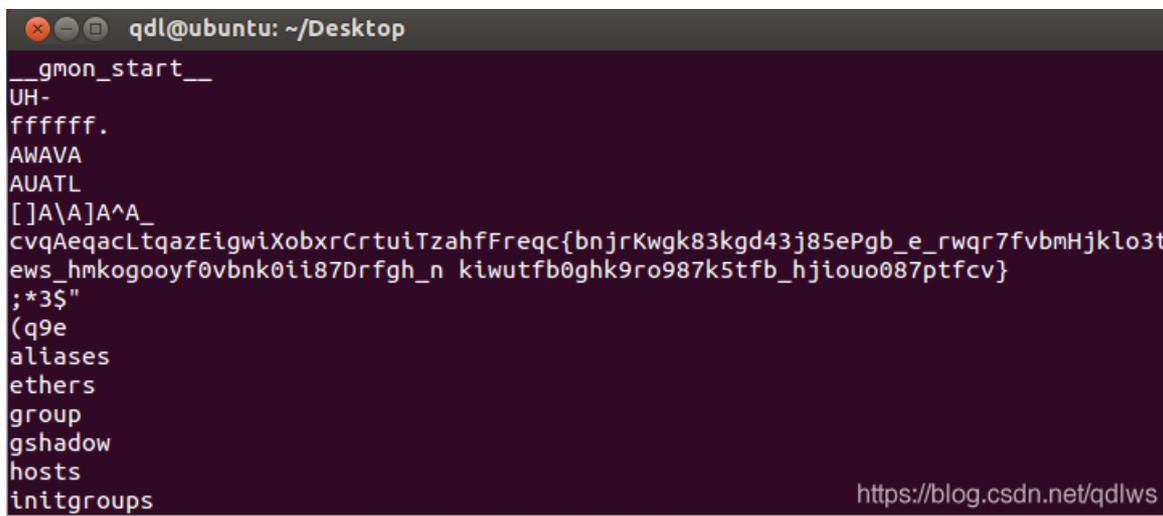
附件1是一个.core文件

[Linux下 core dump](#)

基本概念:

当程序运行的过程中异常终止或崩溃，操作系统会将程序当时的内存状态记录下来，保存在一个文件中，这种行为就叫做Core Dump（中文有的翻译成“核心转储”）。我们可以认为 core dump 是“内存快照”，但实际上，除了内存信息之外，还有些关键的程序运行状态也会同时 dump 下来，例如寄存器信息（包括程序指针、栈指针等）、内存管理信息、其他处理器和操作系统状态和信息。

strings命令查看字符串内容，strings 文件名



```
qdl@ubuntu: ~/Desktop
__gmon_start__
UH-
ffffff.
AWAVA
AUATL
[]A\A]A^A_
cvqAeqacLtqazEigwiXobxrCrtuiTzahfFreqc{bnjrKwgk83kgd43j85ePgb_e_rwqr7fvbmHjkl03tews_hmkogooyf0vbnk0ii87Drfgh_n kiwutfb0ghk9ro987k5tfb_hjiouo087ptfcv}
;*3$"
(q9e
aliases
ethers
group
gshadow
hosts
initgroups
```

<https://blog.csdn.net/qdlws>

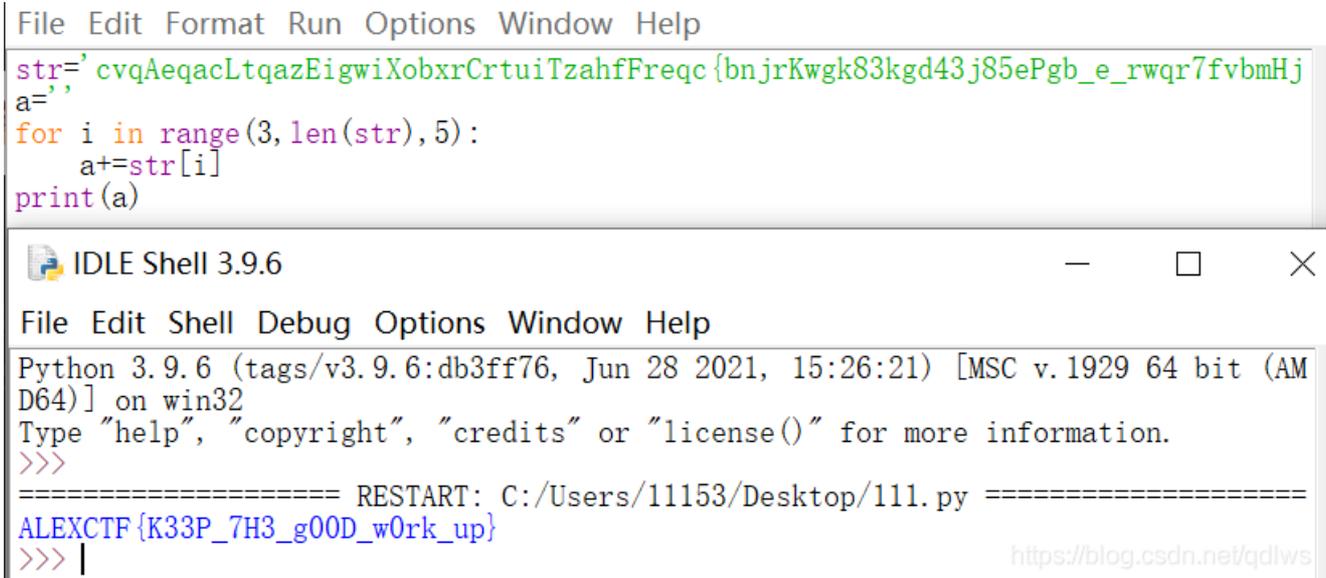
每隔四个小写字母就能看到一个大写字母，按照这个规律找下去就得到flag



```
*Untitled Document (~/Desktop) - gedit
cvqAeqacLtqazEigwiXobxrCrtuiTzahfFreqc{bnjrKwgk83kgd43j85ePgb_e_rwqr7fvbmHjkl03tews_hmkogooyf0vbnk0ii87Drfgh_n kiwutfb0ghk9ro987k5tfb_hjiouo087ptfcv}
A L E X C T F { K 3 3 P _ 7 H 3 _ g 0 0 D _ w 0 r k _ u p }
```

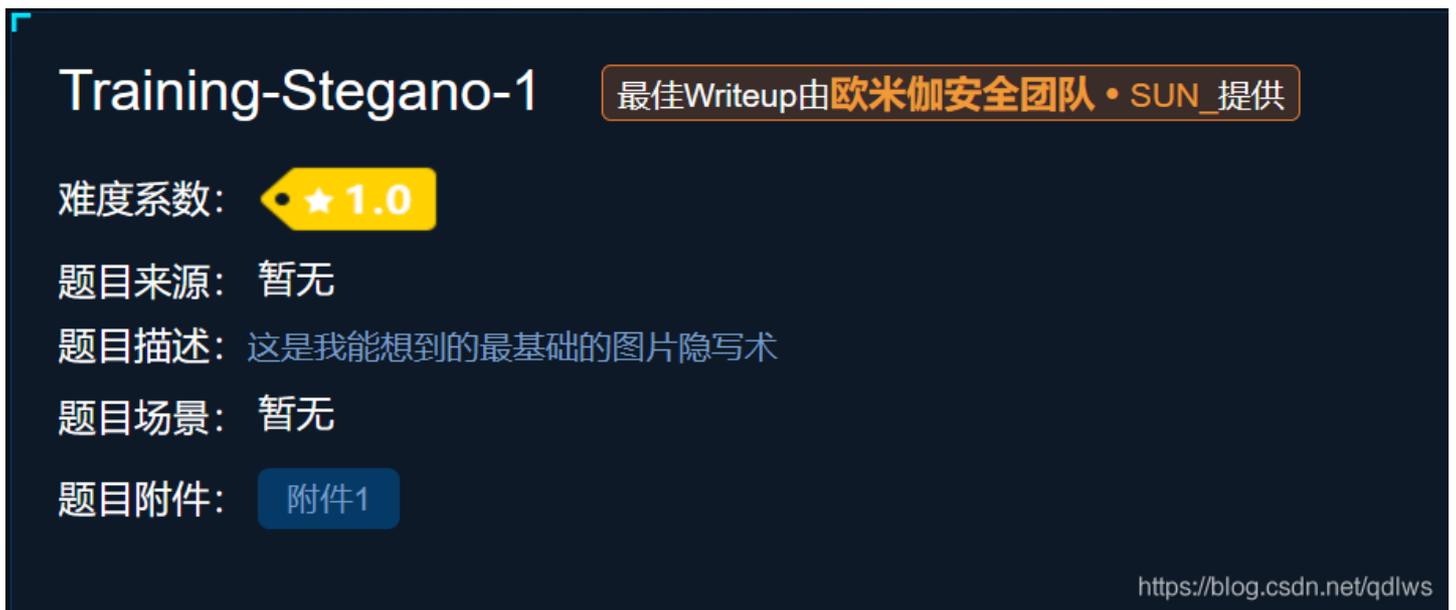
用python实现

```
str='cvqAeqacLtqazEigwiXobxrCrtuiTzahfFreqc{bnjrkWgk83kgd43j85ePgb_e_rwqr7fvbmHjklo3tews_hmkogooyf0vbnk0ii87Drfg  
h_n kiwutfb0ghk9ro987k5tfb_hjiouo087ptfcv}'  
a=''  
for i in range(3,len(str),5):  
    a+=str[i]  
print(a)
```



```
File Edit Format Run Options Window Help  
str='cvqAeqacLtqazEigwiXobxrCrtuiTzahfFreqc{bnjrkWgk83kgd43j85ePgb_e_rwqr7fvbmHj  
a='',  
for i in range(3, len(str), 5):  
    a+=str[i]  
print(a)  
----- RESTART: C:/Users/11153/Desktop/111.py -----  
ALEXCTF{K33P_7H3_g00D_w0rk_up}  
>>> |
```

## Training-Stegano-1:



**Training-Stegano-1** 最佳Writeup由欧米伽安全团队·SUN\_提供

难度系数: ★ 1.0

题目来源: 暂无

题目描述: 这是我能想到的最基础的图片隐写术

题目场景: 暂无

题目附件: 附件1

<https://blog.csdn.net/qdlws>

附件一是一个bmp文件，进行放大，是一块色彩斑斓的thing



<https://blog.csdn.net/qdlws>

于是乎用stegsolve打开进行Data Extract, 无果, 用winhex打开, 看到一个passwd, 把它保存下来

WinHex - [2e5e19744c644912928eddc882f3b0b9.bmp]

文件(F) 编辑(E) 搜索(S) 导航(N) 查看(V) 工具(T) 专业工具(I) 选项(O) 窗口(W) 帮助(H)

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI	ASCII
00000000	42	4D	66	00	00	00	00	00	00	00	36	00	00	00	28	00	BMf	6 (
00000010	00	00	04	00	00	00	04	00	00	00	01	00	18	00	00	00		
00000020	00	00	30	00	00	00	00	00	00	00	00	00	00	00	00	00	0	
00000030	00	00	00	00	00	00	4C	6F	6F	6B	20	77	68	61	74	20		Look what
00000040	74	68	65	20	68	65	78	2D	65	64	69	74	20	72	65	76		the hex-edit rev
00000050	65	61	6C	65	64	3A	20	70	61	73	73	77	64	3A	73	74		ealed: passwd:st
00000060	65	67	61	6E	6F	49												eganoI

新建文本文档.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

steganol

<https://blog.csdn.net/qdlws>

我觉得可能是解压的密码或是啥的, 一番操作无果, 实在想不到这个passwd到底干嘛用, 看了别人的writeup, 淦, 这个passwd的值就是flag, 人傻了都