

ctf--隐写术(持续更新)

原创

小健健健 于 2020-10-19 20:09:40 发布 1161 收藏 11

分类专栏: [ctf](#) 文章标签: [安全](#)

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/superprintf/article/details/108994847>

版权



[ctf](#) 专栏收录该内容

7 篇文章 0 订阅

订阅专栏

[有写的不全的看看大佬的文章](#)

基础视频

链接: https://pan.baidu.com/s/13aiUAaBtRH76aZk_OYIM0Q

密码: 2094

工具

编辑 16 进制文件

1. winhex

2. 010Editor

分离图片中隐藏的文件

1. binwalk: binwalk -e file (不加 -e 为仅查看)

2. foremost: foremost file -o outfile

3. 7z

4. dd: dd if=file of=outfile bs=bs_size count=n skip=m

输入文件为 file, 输出文件为 outfile, 块大小为 bs_size (往往设置成 1), 读写块的个数为 n, 跳过前 m 块

使用 dd 时结合 binwalk 判断块的大小

5. 010editor 手动分离

打印文件中可显示的字符串 (ascii 转义后可显示)

strings filename

查看 gif 图像每帧

[stegsolve](#)

网盘密码: iwhf

音频软件

[adobe audition](#)

密码: 6ppg

一. 概念与历史

隐写术与加密的区别:

希腊单词隐写术(stegnos)加密(crypt)

英文单词隐写术(covered)加密(hidden)

加密(hidden)之后的内容是可见的,只不过顺序被打乱了,不经过分析就无法理解。隐写术中信息是不可见的,所以也叫隐蔽(covered)

古时候的隐写术

隐形墨水(酸性物质受热后颜色会变重)

缩影术(信息缩小成一个点,需放大查看)

水印(类似于人民币透光才能看到的信息)

二. ctf

word隐藏

1.word自带隐藏文字功能

隐藏文字:选中文字右键选择字体,勾选隐藏文字,即可隐藏。

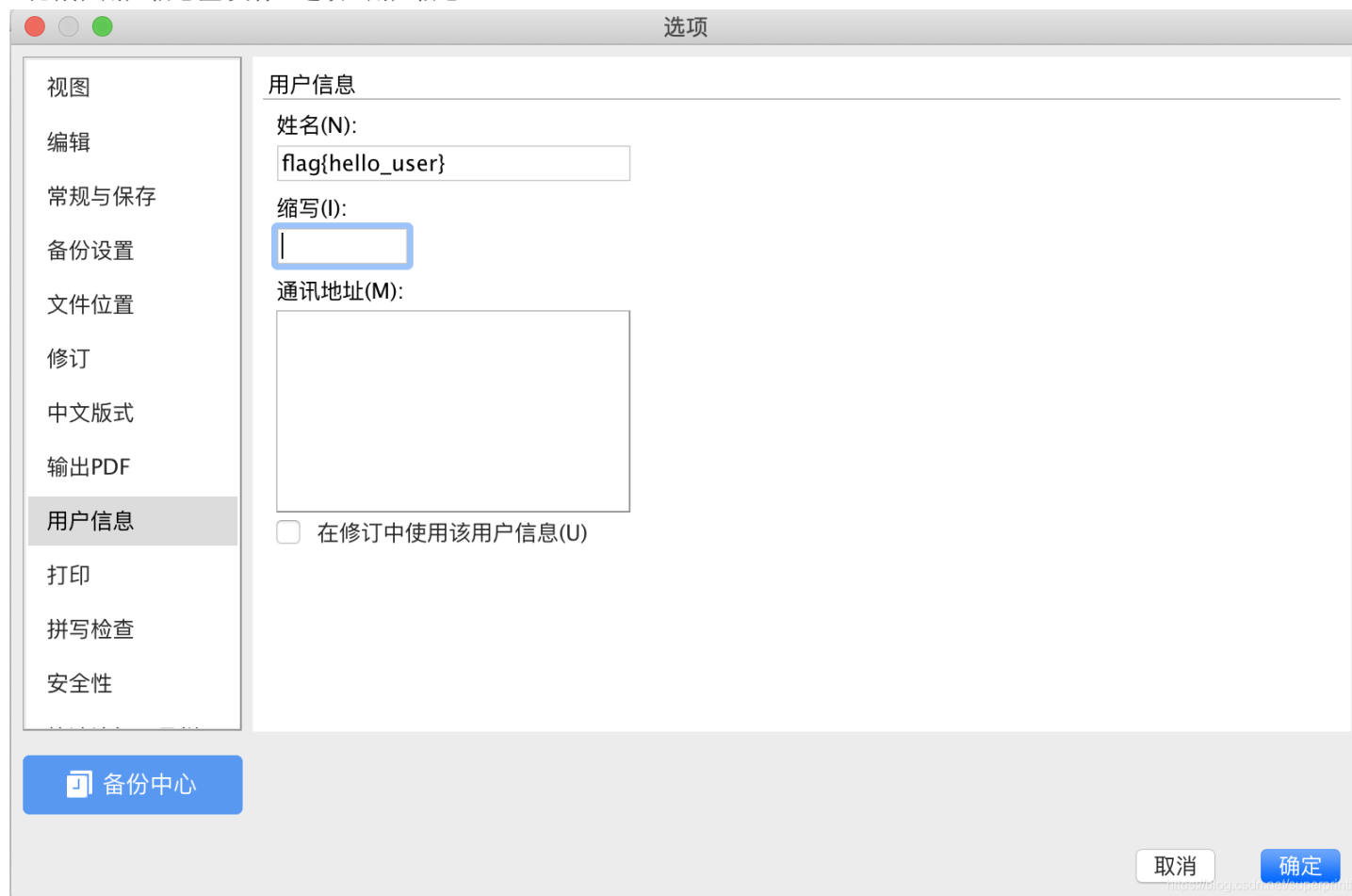
显示文字:文件->选项->视图->隐藏文字



2.白色字体隐藏,修改背景颜色



3.隐藏在用户信息里:文件->选项->用户信息



图像隐藏

细微颜色差别

stegsolve工具

gif多帧隐藏

用stegsolve

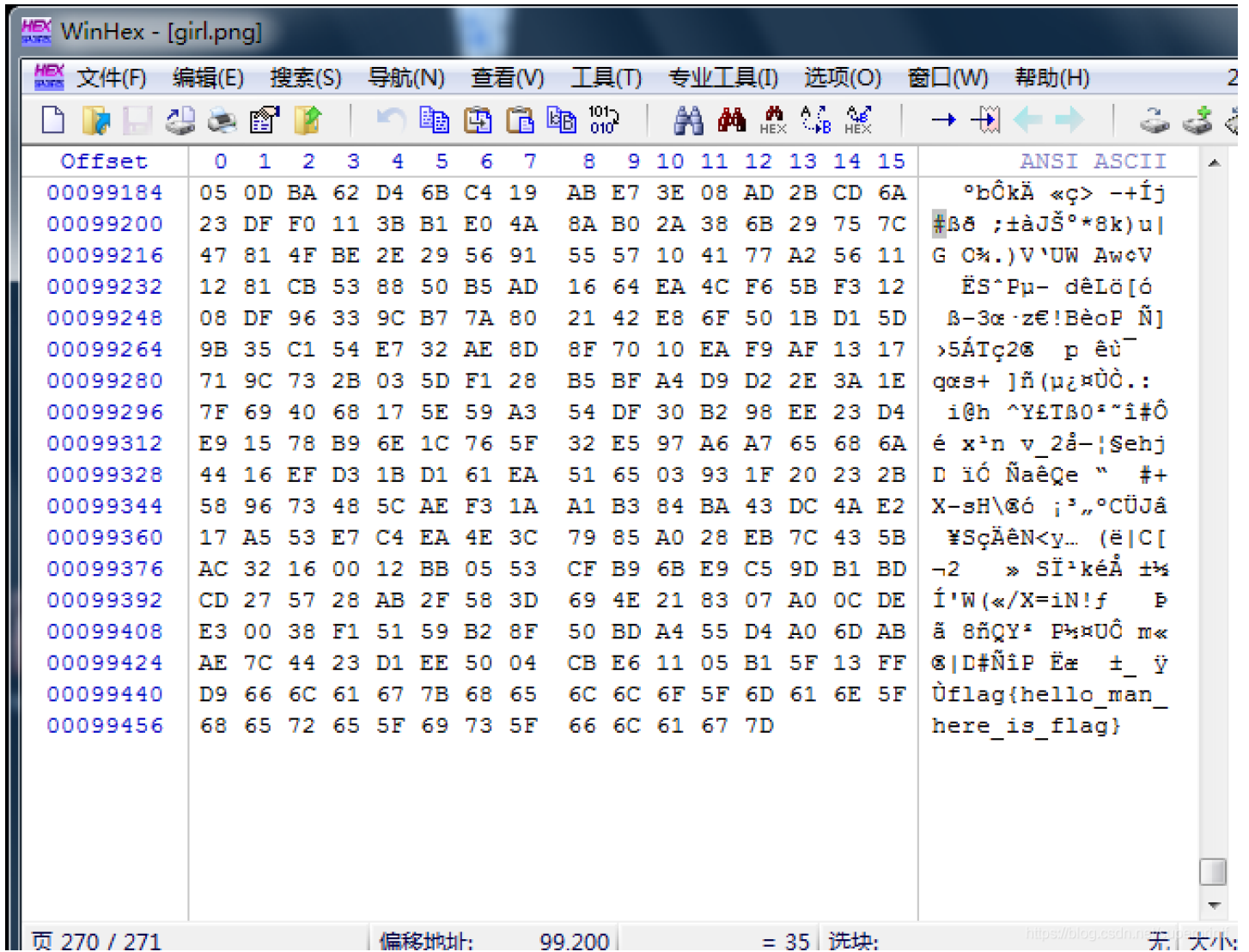
java -jar stegsolve.jar启动，查看gif动图中每一张图的信息

exif信息隐藏

windows上，图片右键，信息

1.windows下命令 `copy /b pic.jpg+file.rar hidden.jpg` 将file.rar藏在图片的末尾

用winhex查看二进制图片发现flag



图片修复

- 1.修复图片的宽和高
- 2.修复IDAT数据长度
- 3.修复CRC
- 4.构造RGB图片

不同格式的文件头

jpg头: FFD8FF

png头: 89504E47

gif头: 47494638

pdf头: 255044462D312E

zip头: 504B0304

rar头: 52617221

先学习一下png格式

crc校验49484452...08040000并得到四位数字

```

00000000: 8950 4e47 0d0a 1a0a 0000000d 4948 4452 .PNG.....IHDR
00000010: 0000001a 0000001a 0804 0000 00000004 .....C.
00000020: 4500 0000 0467 414d 4100 00b1 8f0b fc61 E....gAMA.....a
00000030: 0500 0000 2063 4852 4d00 007a 2600 0080 ....cHRM..z&...
00000040: 8400 00fa 0000 0080 e800 0075 3000 00ea .....u0...

```

```

3:0000h: 0E E2 8D 00 00 00 00 49 44 41 54 BA 43 5E BE .âv.....IDAT°C^¾
3:0010h: EF B4 25 54 DD CB 4A B4 13 74 A2 4A 6E 14 09 B0 i' %TÿËJ'.tçJn.)°
3:0020h: B0 8F EF CF 19 36 C6 40 6A EF EE F2 39 79 3E B1 °.iï.6Æ@jiiò9y>±

```

1题修改图片高度

修改图片宽度和高度来暴露隐藏的部分(winhex工具)

链接: <https://pan.baidu.com/s/1y22OzQ6Z381LWkibTXoYZA>

密码: nsdi



Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	.PNG IHDR
00000016	00	00	01	F3	00	00	02	80	08	06	00	00	00	99	DA	A9	ó e ¯ú©
00000032	F6	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00	ö sRGB @Î é
00000048	00	09	70	48	59	73	00	00	B1	8F	0B	FC	61	05	00	00	gAMA ± üa
00000064	00	09	70	48	59	73	00	00	0B	13	00	00	0B	13	01	00	pHYs
00000080	9A	9C	18	00	00	FF	A5	49	44	41	54	78	5E	94	FD	85	šœ ¾IDAT@家为
00000096	97	25	5B	76	DD	8D	B6	2D	5B	92	2D	68	B5	24	4B	AD	-%[vÝ ¶-['-hp\$K-



2题修复IDAT长度

[网盘下载图片](#)

密码: uvhf



IDAT数据长度部分为0，我们需要修复，这一段的IDAT是从30004h - 36273h

除去内容部分有4h的CRC，4h的长度，4h的IDAT标示， $3627h - 30004h + 1h - 4h - 4h - 4h = 6264h$ ，填写在数据长度部分，显示原图片

```
00030000: 0ee2 768d 0000 0000 4944 4154 ba43 5ebe ..v.....IDAT.C^.
00030010: efb4 2554 ddc8 4ab4 1374 a24a 6e14 29b0 ..%T..J..t.Jn.).
00030020: b08f efcf 1936 c640 6aef eef2 3979 3eb1 .....6.@j...9y>.
.....

00036250: a029 f3fb 0142 1cbf 22a1 5f1e 2dfd e8d5 .)...B.."._.-...
00036260: 2381 a379 3d15 213f 3fdf fe3f 3003 6bc1 #..y=.!??..?0.k.
00036270: cd56 d230 0000 00a0 4944 4154 5532 4673 .V.0.....IDATU2Fs
.....
```



3题修复CRC校验

[crc在线工具网站](#)

windows下图片可以打开(不用修复CRC校验)其他系统下图片不能打开则有一定概率存在CRC校验码错误的问题
爆破图片修改前的宽和高来匹配CRC校验码，并用正确的宽和高来修复图片

```
import binascii
def str2num(s):
    return int(s, 16)
dic = '''abcdefghijklmnopqrstuvmnopqrstuvwxyz0123456789!#$%&'()*+,-./:;<=>?@[\\]^_`{|}~''
crc1 = str2num("BBB16F8C")#crc值
for x in dic:
    for a in dic:
        for b in dic:
            for c in dic:
                for d in dic:
                    str = x+a+b+c+d
                    str_crc = binascii.crc32(str.encode()) & 0xffffffff
                    if (str_crc == crc1):
                        print("crc1:", str)
```

4题构造RGB图片

[我的另一篇博客](#)

[pdf隐写](#)

音频隐写

视频隐写

adobe audition

密码: 6ppg

数据包隐写

wireshark