
杂项题目练习（四）

杂项题目练习（四）	1
杂项第二十五题: 乌云邀请码	4
杂项第二十六题: CTF 之隐写术--LSB 一张图片隐藏的信息	6
杂项第二十七题: convert.....	9
杂项第二十八题: 听首音乐	13
杂项第二十九题: ctf 练习---摩斯密码.....	16
杂项第三十题: 好多数值	17
杂项第三十一题: 神秘的文件	20
杂项第三十二题: zip 明文攻击	22
杂项第三十三题: 论剑	23

前言：

以下是在 bugku 练习的解题思路，编号跟我前面分享的基础是对应的，理论基础结合实践。

所有题目目录如下：

题目练习	1
杂项第一题: 签到题	3
杂项第二题: 这是一张单纯的图片	4
杂项第三题: 隐写	6
杂项第四题: telnet	8
杂项第五题: 眼见非实(ISCCCTF)	9
杂项第六题: 啊哒	12
杂项第七题: 又一张图片, 还单纯吗	14
杂项第八题: 猜	17
杂项第九题: 宽带信息泄露	19
杂项第十题: 隐写 2	20
杂项第十一题: 多种方法解决	23
杂项第十二题: 闪的好快	25
杂项第十三题: come_game	26
杂项第十四题: 白哥的鸽子	28
杂项第十五题: linux	30
杂项第十六题: 隐写 3	30
杂项第十七题: 做个游戏(08067CTF)	33
杂项第十八题: 想蹭网先解开密码	35
杂项第十九题: Linux2	39
杂项第二十题: 细心的大象	42
杂项第二十一题: 爆照(08067CTF)	47
杂项第二十二题: 猫片(安恒)	51
杂项第二十三题: 旋转跳跃	57
音频工具 MP3stego 使用 (一)	59
音频工具 MP3stego 使用 (二)	60
杂项第二十四题: 普通的二维码	61
CTF 杂项之音频及视频隐写补充	64
杂项第二十五题: 乌云邀请码	71
杂项第二十六题: CTF 之隐写术--LSB 一张图片隐藏的信息	73
杂项第二十七题: convert	76
杂项第二十八题: 听首音乐	80
杂项第二十九题: ctf 练习---摩斯密码	83
杂项第三十题: 好多数值	84
杂项第三十一题: 神秘的文件	87
杂项第三十二题: 三十 zip 明文攻击	90
杂项第三十三题: 论剑	91

杂项第三十四题: 图穷匕见.....	94 ^u
杂项第三十五题: 很普通的数独(ISCCTF).....	99 ^u
杂项第三十六题: PEN_AND_APPLE	103 ^u
NTFS 数据流及高级文件隐藏.....	105 ^u
杂项第三十七题: color	107 ^u
杂项第三十八题: 小明的密码.....	110 ^u
杂项第三十九题: 仿射加密.....	111 ^u
仿射密码解析与实例.....	113 ^u
杂项第四十题: 黑客的机密信息	117 ^u
杂项第四十一题: 远控木马.....	118 ^u
杂项第四十二题: Web 漏洞	118 ^u
bugku-ctf 第四十三题: 颜文字	120 ^u
杂项第四十四题: 磁盘镜像.....	120 ^u
杂项第四十五题: 神奇的图片	121 ^u
杂项第四十六题: 怀疑人生	122 ^u
杂项第四十七-CTF 加密篇之 ok (Ook!)	129 ^u
杂项第四十八题: 红绿灯.....	131 ^u
杂项第四十九题: 不简单的压缩包.....	136 ^u



以下是对 24-33 题的介绍

杂项第二十五题: 乌云邀请码

Challenge

1330 Solves

×

乌云邀请码

100

来源: XJNU

misc50.zip

Flag

Submit

<https://ctf.bugku.com/files/69fed30501c47ddd56250587d359e7d9/misc50.zip>

下载压缩包并解压

里面是个图片

您好：

这是来自于WooYun的一封邀请邮件，非常高兴你通过WooYun发布有价值的漏洞，很荣幸的邀请阁下为WooYun白帽子中的一员，你可以通过如下的链接来注册

http://www.wooyun.org/user.php?action=register&code=b6d75821211e338dd56623c8825456ab&invite_email=504038236@qq.com&invite_type=0

WooYun会给你发送一封确认邮件，可以点击其中的链接完成注册，希望你继续支持WooYun

漏洞处理流程：<http://www.wooyun.org/help#bug>

白帽注意事项：<http://www.wooyun.org/help#whitehat>

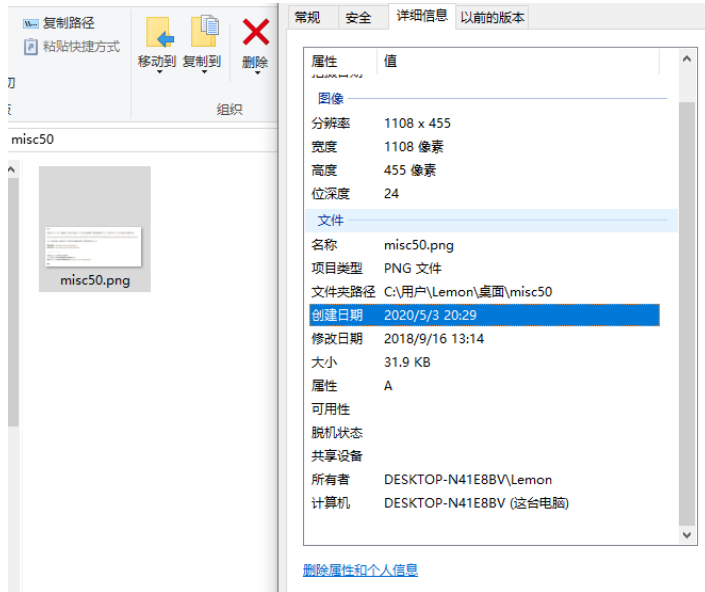
本邮件由WooYun自动发送，请勿回复

WooYun是一个自由平等的漏洞和安全信息报告平台

其他关于WooYun的更多信息请访问<http://www.wooyun.org/about.php>

谢谢！

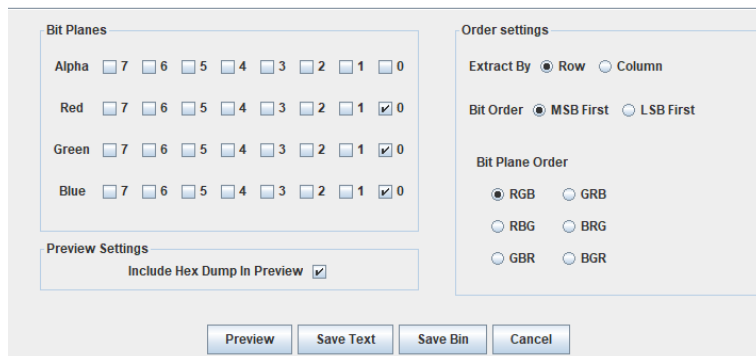
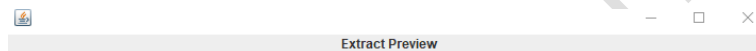
查看属性没什么发现



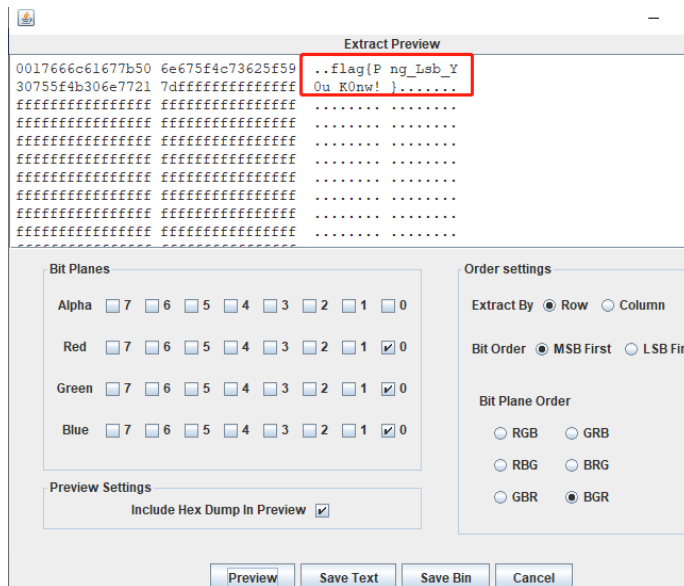
Blue plane 0

您好：

打开 Stegsolve->Analyse->Data Extract，选取相应颜色通道



更改 Bit Plane Order，就得到 flag 了



flag{P ng_Lsb_Y0u_K0nw! }

顺便总结一下图片隐写常用套路

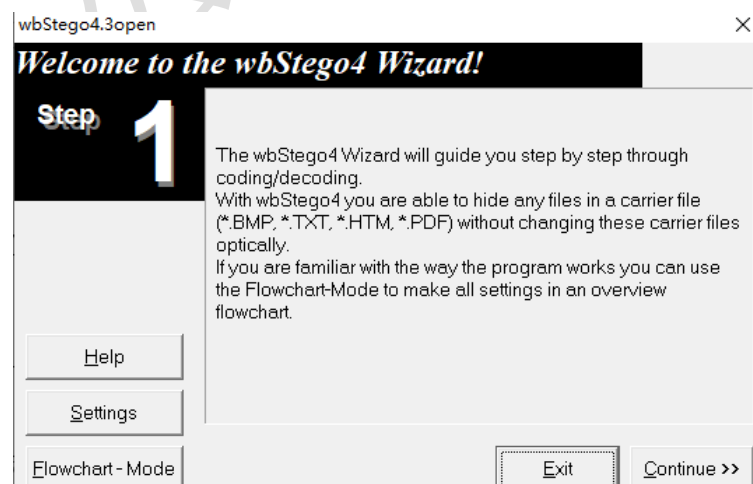
- 1、能打开的先用 stegsolve 看一下各个颜色通道有没有隐藏信息，或者是不是 LSB 隐写。
- 2、打不开的在十六进制下看一下是不是缺少头标记
- 3、用解压、Linux 下的 binwalk、foremost 看一下有没有隐藏文件
- 4、查看文件属性、修改图片的长宽比例。
- 5、用记事本查看图片，查看图片的十六进制。

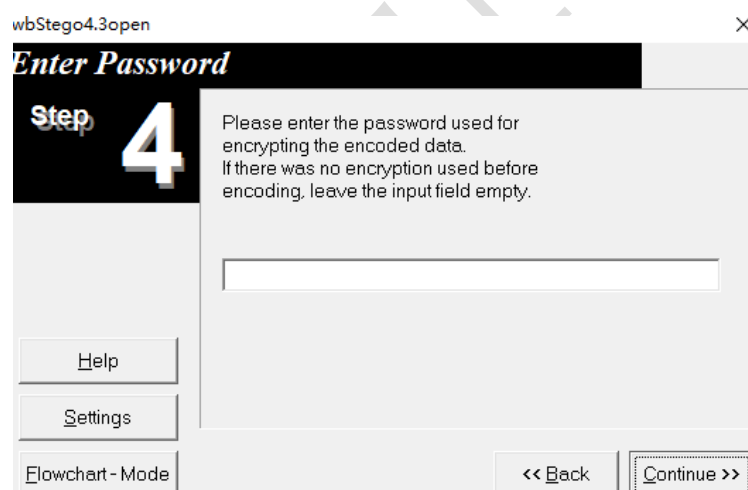
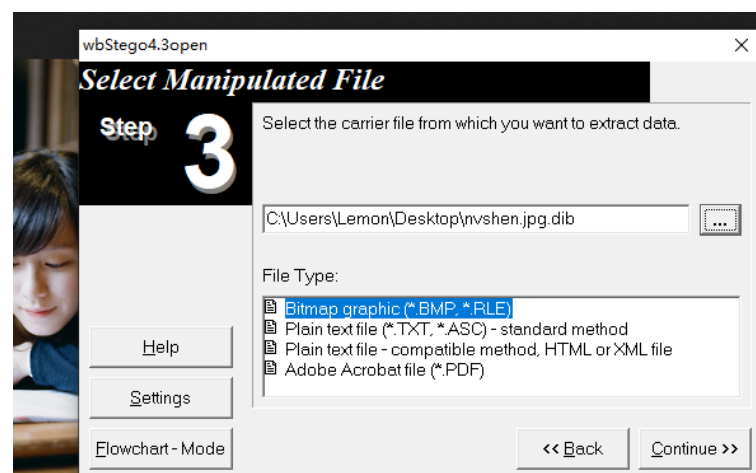
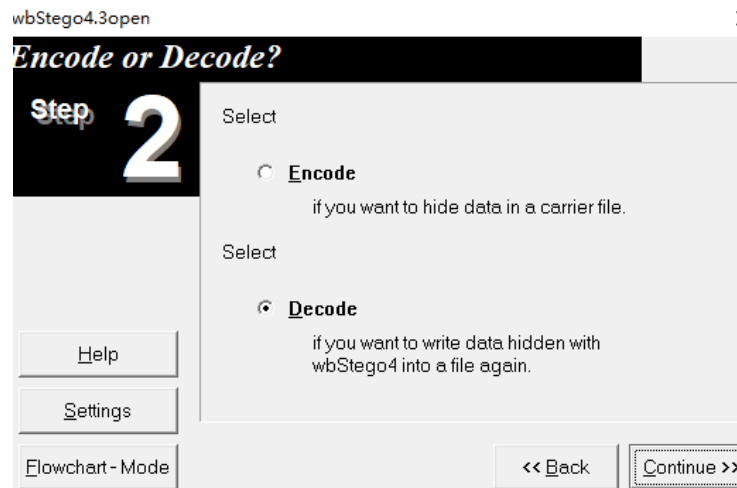
杂项第二十六题: CTF 之隐写术--LSB 一张图片隐藏的信息

实验吧图片链接: <http://ctf5.shiyanbar.com/stega/nvshen.jpg>

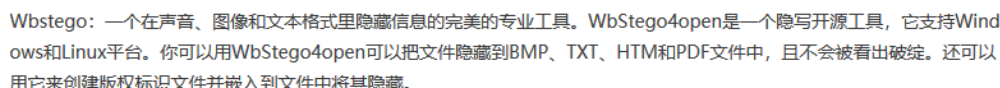
使用工具进行操作如下:

- 1、图片另存为桌面:
- 2、使用 wbStego4.3 对图片进行操作，步骤如下:





评分 ★★★★★



进制转换

A screenshot of a CTF challenge interface. At the top, there's a header bar with 'Challenge' on the left and '1332 Solves' on the right, with a close button 'X' on the far right. Below the header, the challenge content is displayed: the word 'convert' in a blue box, followed by the number '150'. Below this, the author is listed as '作者: NIPC'. There is a button labeled '1.txt' and a 'Flag' input field. A 'Submit' button is also visible.

<https://ctf.bugku.com/files/de3b517a9b83b2d35f1a8751e9b80c08/1.txt>

里面全是二进制

[illegible]

```
f1=open('1.txt','r')
```

#二进制转 10 进制

```
oct1=int(f1.read().2)
```

#十进制转 16 进制

```
hex1=hex(oct1)
```

```
#将十六进制文件写入文件
```

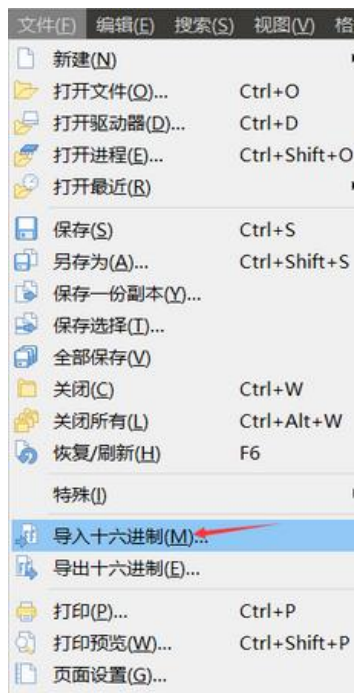
```
1 f1=open('l.txt','r')
2 oct1=int(f1.read(),2)
3 hex1=hex(oct1)
4 f2=open('out.txt','w')
5 f2.write(hex1)
6 f1.close()
7 f2.close()
8
```

A screenshot of a Windows Notepad application window. The title bar reads "1.txt - 记事本". Below the title bar is a menu bar with options: "文件(F)", "编辑(E)", "格式(O)", "查看(V)", and "帮助(H)". The main text area contains approximately 28 lines of binary code, consisting of long strings of '0's and '1's separated by spaces every four bits. The text is black on a white background.

转成十六进制

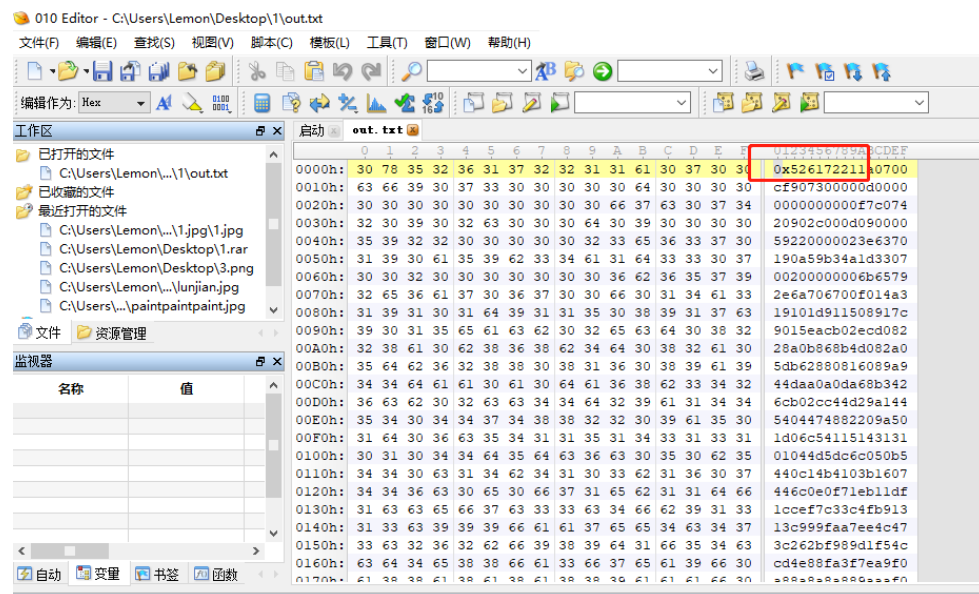
```
1 0x526172211a0700cf907300000d00000000000000f7c07420902c000d090000592200000
ld330700200000006b65792e6a706700f014a319101d911508917c9015eacb02ecd08228a
2880816089a944daa0a0da68b3426cb02cc44d29a1445404474882209a501d06c54115143
b5440c14b4103b1607446c0e0f71eb11df1cccf7c33c4fb91313c999faa7ee4c473c262bf
3f7ea9f0a88a8a8a89aaaf09889c7f463fec0d2adabad2b8036580df85e031fd3a5ac567
281200f0cde031c943050297464341e070cbb4ad050f80202966e146372501f14fb13a3e0
91a06fc683c257b22568f8162c5b23eba3e058b64559980e407c03704f4b03c01ec0b8065
99c6854dc72570c946017729ff72d881bc03efd8cab0565ccfb702a04f5d0a7e63e0e4afa
24fe3e30072ab02b2a312eb0278a20d692e0ead84053d6c52860a4722f0dee798d696d605
4814d6d8da3c8f05e453b111fc16f79246a1748b09b66e7979754f162dcde1287b5ba701b
615a05814073e3a8f6a716c2f3fac90cd45451bdf494a8c29bdaf3032ecd7062e3aaab637
89a9f5c5a939ad18729690d541f13df1c9d5c8bd878afa7c1cd6b32a8a17dafc9e17be84e
1b757fe0a850971ff1f18f796253da5a53a3b90ce153b24163068b1a352422a92f049ccb
2ffe2404ae2bfb01a3e4058b6473fb8d1f202c58b647affec83f1a55b63985a497b0b48ac
3212232c3434126a6e77a437363637d569b4e72767fab4140cbcf8f852225230a424843cc
841464e514d1aa09497b21ba16018d3242f6373dd2690f46eb0fb5837267e3d300e848164
cbb1fc00410ba930c836547df63d0c601cc4cb3b012686a6c1149ed29761758730310e646
e8cb4dadcd8aa19e9d7c78842763b1b0315d31287b6ec77b50c15b7c8897c077822fcd49e1
bf65b34cda26a727aaedd595d6165696d85898d919777bc666a0b60d20dcdee0f0f245e9e
1f8bc68b8ce5c6f323b9bcee7c97524e53ab2b2d2f31d9ed4ecf4fd050d151d3f7fc1e1a8
e7b1f45959fa49dc5cdd7abd7777852ff03f7c1f87c708afcb0f4319cf38386fb8cade759
27bd028745c39eb19e99517c40f76d3a1161277b6cf672434434b60bed416adcf551365e9
a82c9ebc9cfe319b301b87c90c0eb3a700e06161a3c9401afffacd54751096d052d73da3e
df576ff9526b3d394b3e1dfa8cb07a5d5e372fc8a74b070b691f71aac3b099fcd19faa47
c6bba969ab27717714d58acece713ebf7a47a3d7b58711832df30dd55c9469f63d76b61c2
```

删除开头的 0x，之后将这些十六进制数放到编辑器中



导入这个文件后 发现

文件头 为 52617221 正好为 rar 文件



RAR Archive (rar),

文件头: 52617221

那么将他另存为 q.rar

解压后发现一张图片



q.rar



blog key.jpg

修改后缀之后，解压得到图片 key.jpg，接下就是图片隐写相关的常规操作(查看属性、010 editor、stegsolve 等)，在图片属性“主题”里面发现一串 base64 编码的字符串：
ZmxhZ3swMWEyNWVhM2ZkNjM0OWM2ZTYzNWExZDAxOTZlZmYnO=
解码，得到 flag
flag{01a25ea3fd6349c6e635a1d0196e75fb}

杂项第二十八题: 听首音乐

摩斯密码

Challenge

1252 Solves

×

听首音乐

150

听首音乐放松放松吧~

下载地址: 链接: <http://pan.baidu.com/s/1gfvezBl> 密码: y6gh

Flag

Submit

下载地址 <https://pan.baidu.com/share/init?surl=gfvezBl>
密码 y6gh
看题目是跟音频相关的题目，
下载下来是个压缩包，解压得一个 wav 文件，点击播放下（电脑先安装了一个 Cool Edit）。

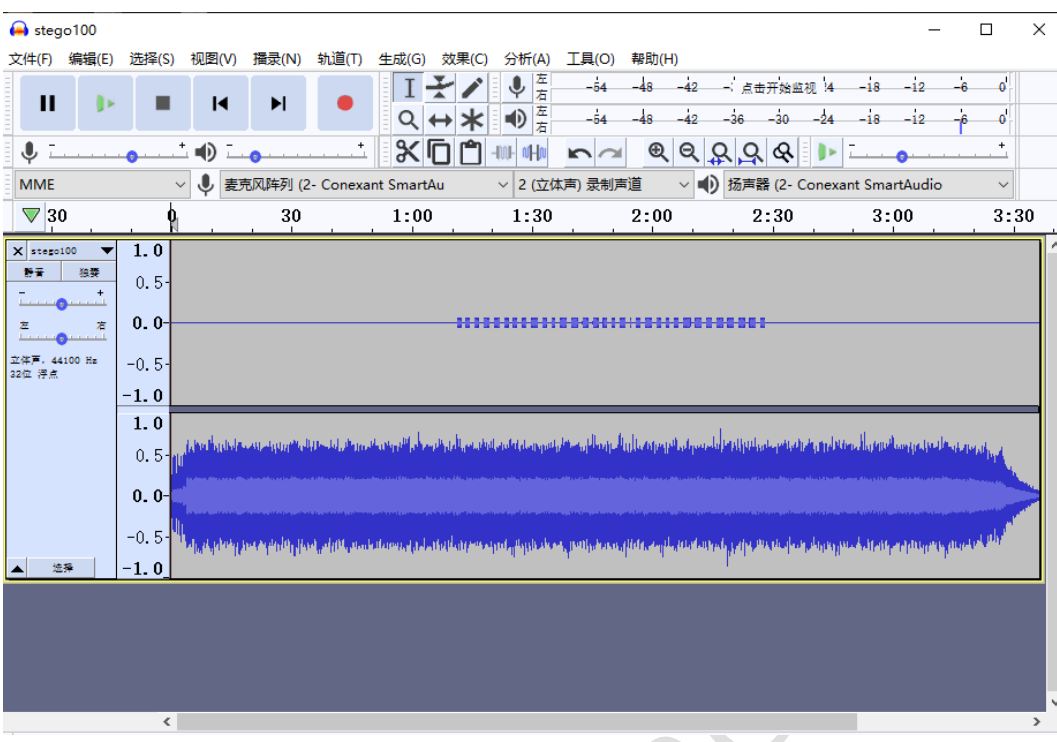


cool edit 编辑

★ 收藏 | 4481 |

Adobe Audition(前Cool Edit Pro) 是美国Adobe Systems 公司 (前Syntrillium Software Corporation) 开发的一款功能强大、效果出色的多轨录音和音频处理软件。

关于音频工具，也可以用 Audacity 分析



关于摩斯密码：

摩尔斯电码（又译为摩斯密码，Morse code）是一种时通时断的信号代码，通过不同的排列顺序来表达不同的英文字母、数字和标点符号。它发明于 1837 年，发明者有争议，是美国人塞缪尔·莫尔斯或者阿尔菲德·维尔。摩尔斯电码是一种早期的数字化通信形式，但是它不同于现代只使用零和一两种状态的二进制代码，它的代码包括五种：点、划、点和划之间的停顿、每个字符之间短的停顿、每个词之间中等的停顿以及句子之间长的停顿。

标准摩尔斯电码对照表

Morse-Alphabet (Punkt = kurz blinken, Strich = lang blinken.)			
a · -	i · ·	r · · ·	1 · - - -
ä · · ·	j · - -	s · · ·	2 · · - -
b - · ·	k - · -	t -	3 - · - -
c · · · ·	l · · ·	u · · ·	4 · · · ·
ch - - - -	m - -	ü · · · ·	5 · · · ·
d · ·	n - ·	v · · ·	6 - · · ·
e ·	o - - -	w · - -	7 - · · ·
f · · ·	ö - - -	x - · ·	8 - - · ·
g - -	p · · ·	y - - ·	9 - - - ·
h · · · ·	q - - ·	z - - ·	0 - - - -
Verstanden · · - · ·			
Schlusszeichen · - · - ·			

摩尔斯电码由两种基本信号组成：短促的点信号“·”，读“滴”；保持一定时间的长信号“—”，

读“嗒”。间隔时间：滴=1t，嗒=3t，滴嗒间=1t，字符间=3t，单词间=7t。

杂项第二十九题: ctf 练习---摩斯密码

摩斯密码

题目：

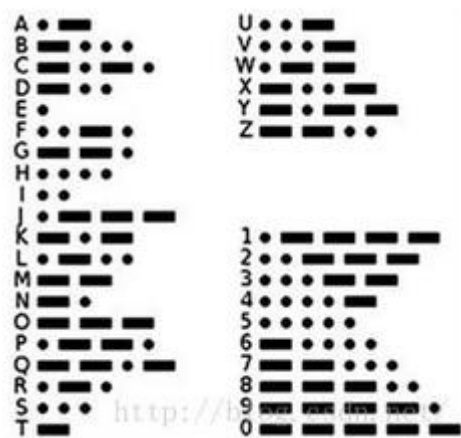
嘀嗒嘀嗒嘀嗒嘀嗒 时针它不停在转动

-- --- .-

嘀嗒嘀嗒嘀嗒嘀嗒 小雨它拍打着水花

-. - --- -.. .

思路：百度一张摩斯密码表，然后根据摩斯密码表把相应的符号翻译出来即可。



A	·—	U	··—
B	—···	V	···—
C	—·—·	W	··—·
D	—···	X	—·—·
E	·	Y	—··—
F	···—	Z	—··—
G	—·—·		
H	····		
I	··		
J	·—·—		
K	—·—·	1	·—·—·—
L	—···	2	···—·—
M	—·—	3	··—·—·
N	—·	4	···—·—
O	—·—	5	··—·—·
P	··—·—	6	··—·—·
Q	—·—·—	7	—·—·—·
R	··—·	8	—·—·—·
S	····	9	—·—·—·
T	—	0	—·—·—·

翻译后的结果是 morsecode
所以答案为 wct{morsecode}。

杂项第三十题: 好多数值

Challenge

952 Solves

好多数值

150

flag格式 flag{}

1.txt

Flag

Submit

打开连接: <https://ctf.bugku.com/files/093d4073de2c7bfac7466fd166c5d990/1.txt>

里面都是 255, 255

[illegible]

先复制出来

```
61343 255,255,255
61344 255,255,255
61345 255,255,255
61346 255,255,255
61347 255,255,255
61348 255,255,255
61349 255,255,255
61350 255,255,255
61351 255,255,255
61352 255,255,255
61353 255,255,255
61354 255,255,255
61355 255,255,255
61356 255,255,255
61357 255,255,255
61358 255,255,255
61359 255,255,255
61360 255,255,255
61361 255,255,255
61362 255,255,255
61363 255,255,255
61364 255,255,255
61365 255,255,255
61366 255,255,255
61367
```

这里我百度了大佬的解题思路：

打开文件发现好多行类似 255,255,255 的数据，直接想到 RGB 值，估计是画图。

用 yafu 分解一下因数,yafu 自行下载

yafu暴力分解

评分 ★★★★★



当RSA中的n过大并且在线的网站无法分解时，可以尝试一下yafu。暴力分解n非常有效。方法：下载后运行yafu-x64.exe 然后输入factor(n),接下来就等着n被分解咯。

然后进行爆破

```
P1 = 3
P1 = 5
P2 = 17

ans = 1

=== Starting work on batchfile expression ===
factor(255,255,255)
=====
fac: factoring 255
fac: using pretesting plan: normal
fac: no tune info: using qs/gnfs crossover of 95 digits
div: primes less than 10000
Total factoring time = 0.0040 seconds

***factors found***

P1 = 3
P1 = 5
P2 = 17

ans = 1

=== Starting work on batchfile expression ===
factor(255,255,255)
=====
fac: factoring 255
fac: using pretesting plan: normal
```

爆破中。

分解因数，有 503、61、2

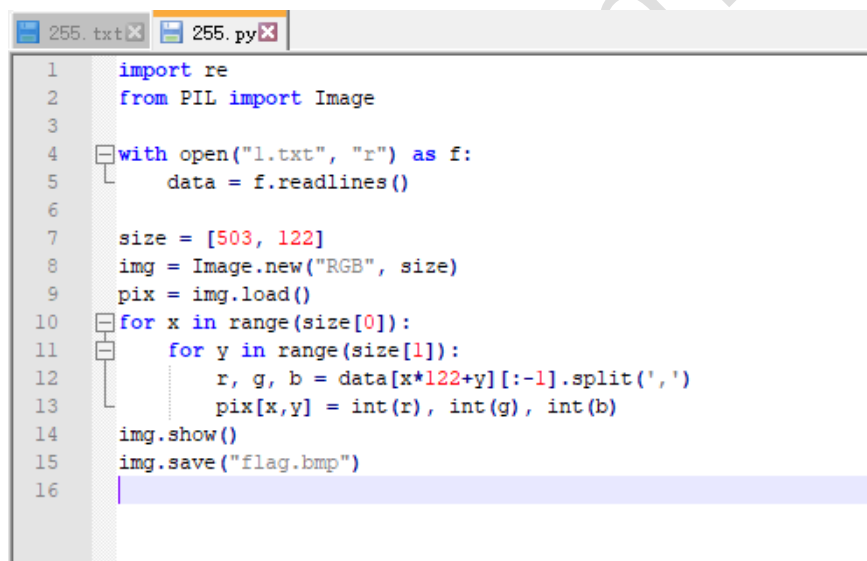
即图像无非 $503 * 122, 1006 * 61, 30683 * 2$ 这三个 size，可以先排除第三个，即试前两个即可

文件总共 61366 行，分解一下是 $122 * 503$ ，猜测要画一个宽 503，高 122 的图，拿 Python 写个脚本如下：

```
import re
from PIL import Image

with open("1.txt", "r") as f:
    data = f.readlines()

size = [503, 122]
img = Image.new("RGB", size)
pix = img.load()
for x in range(size[0]):
    for y in range(size[1]):
        r, g, b = data[x*122+y][:-1].split(',')
        pix[x,y] = int(r), int(g), int(b)
img.show()
img.save("flag.bmp")
```



```
1 import re
2 from PIL import Image
3
4 with open("1.txt", "r") as f:
5     data = f.readlines()
6
7 size = [503, 122]
8 img = Image.new("RGB", size)
9 pix = img.load()
10 for x in range(size[0]):
11     for y in range(size[1]):
12         r, g, b = data[x*122+y][:-1].split(',')
13         pix[x,y] = int(r), int(g), int(b)
14 img.show()
15 img.save("flag.bmp")
16
```

得到最终 flag 如图：

flag{ youc@n'tseeme }

flag{youc@n'tseeme}

ps: flag 没有空格。。。。。。。

杂项第三十一题: 神秘的文件

Challenge 1074 Solves ×

神秘的文件

100

来源: 第七届山东省大学生网络安全技能大赛

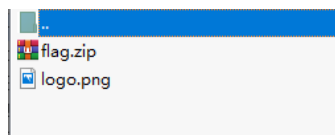
5ee325f5-44c6-...

Flag

Submit

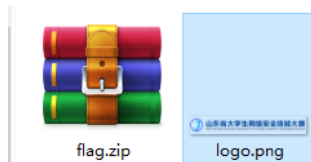
<https://ctf.bugku.com/files/d017f513e8f414cae61bfa3498ea34a8/5ee325f5-44c6-4a0b-b496-a0b11ef6dca1.rar>

下载压缩包后解压

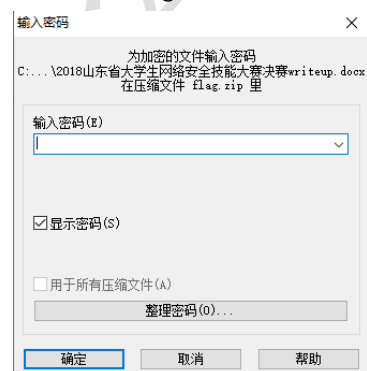


里面是一个压缩包和图片

5ee325f5-44c6-4a0b-b496-a0b11ef6dca1



再次解压 flag, 需要输入密码

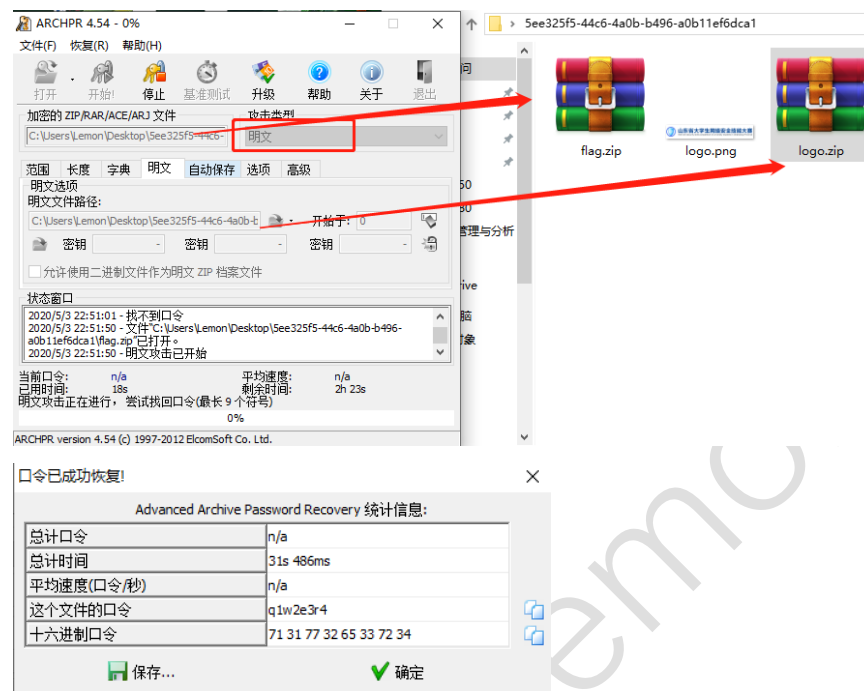


双击压缩包, 发现压缩包中含有 logo.png

名称	大小	压缩后大小
2018山东省大学生网络安全技能大赛决赛writeup.docx *	272,070	259,726
logo.png *	27,870	27,405

后者含有前者，想到明文攻击

将 logo.png 压缩做明文。将 logo 文件压缩为 zip



q1w2e3r4

将压缩包里的文件解压出来，打开 doc 文件，没有什么有用的信息，但它是肯定有问题的，



哪有什么 WriteUP，别想了，老老实实做题吧！

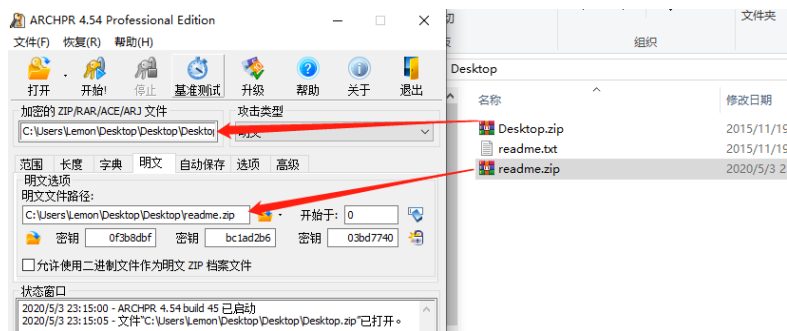
于是用 binwalk 检查一下，果然有问题，用 foremost 分离



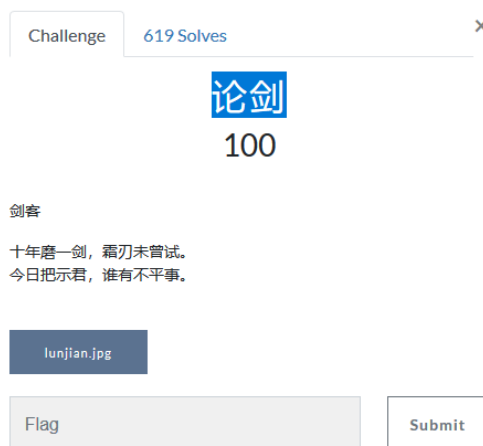
要把 readme.txt 先压缩成 zip

Desktop.zip 是要解压缩的文件

所谓明文攻击就是已经通过其他手段知道 zip 加密文件中的某些内容，这里有百度解说



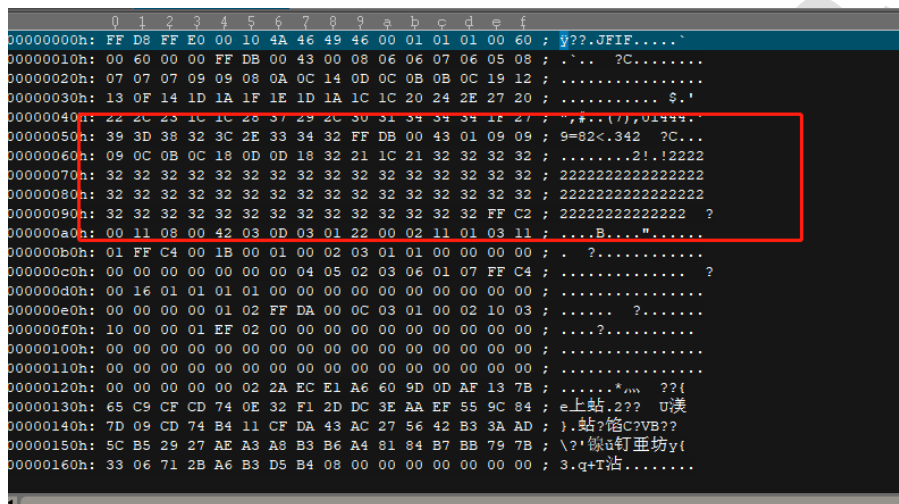
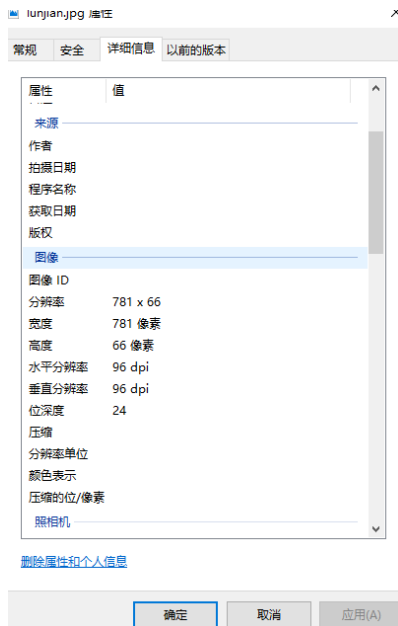
杂项第三十三题: 论剑



<https://ctf.bugku.com/files/934db0621d88bd8b16049c1b795c6a1a/lunjian.jpg>

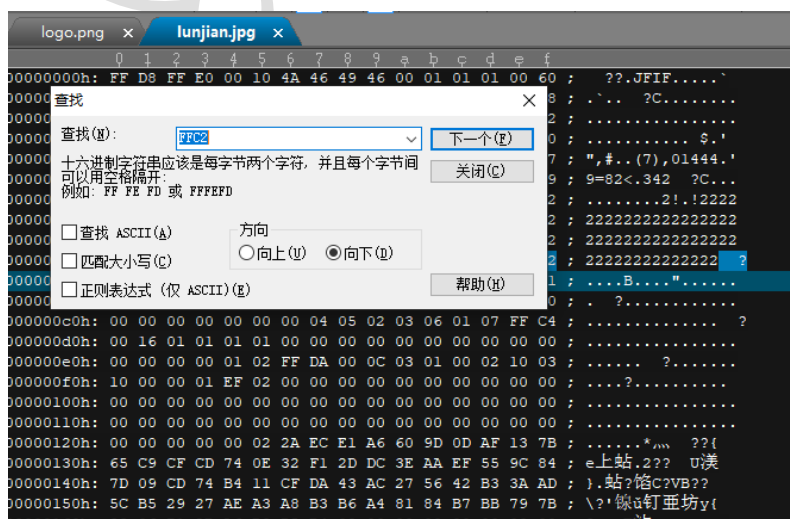
打开图片并保存在本地。

看下属性没什么发现



UE 查看发现了一串奇怪的字符

以前知道如何修改 PNG 格式的圖片的寬高，換到 JPEG 就一臉懵逼，經過百知知道是先尋找 FFC2，3 字節後即圖片的高與寬信息。




```
root@BlueDoor:/mnt/hgfs/BugKu
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@BlueDoor:/mnt/hgfs/BugKu# binwalk -e lunjian.jpg
DECIMAL      HEXADECIMAL    DESCRIPTION
-----
0             0x0            JPEG image data, JFIF standard 1.01
9591          0x2577         7-zip archive data, version 0.4
17569         0x44A1         JPEG image data, JFIF standard 1.01
```

压缩包里面发现一张图片，是加密了的，输入之前解密的 ascii 码，密码正确。又是一张图片，继续修改图片高度，发现这个信息。



结合之前的图片，base16 解密一下，就得到 flag 了。
flag{666C61677B6D795F6E616D655F482121487D}，使用 16 进制解密得到最终
flag{my_name_H!!!H}