

BUUCTF MISC 50分以上题目

原创

[ruokeqx](#) 于 2020-08-01 00:33:13 发布 1442 收藏 10

分类专栏: [CTF入坑](#)

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/weixin_45485719/article/details/107662696

版权



[CTF入坑](#) 专栏收录该内容

33 篇文章 1 订阅

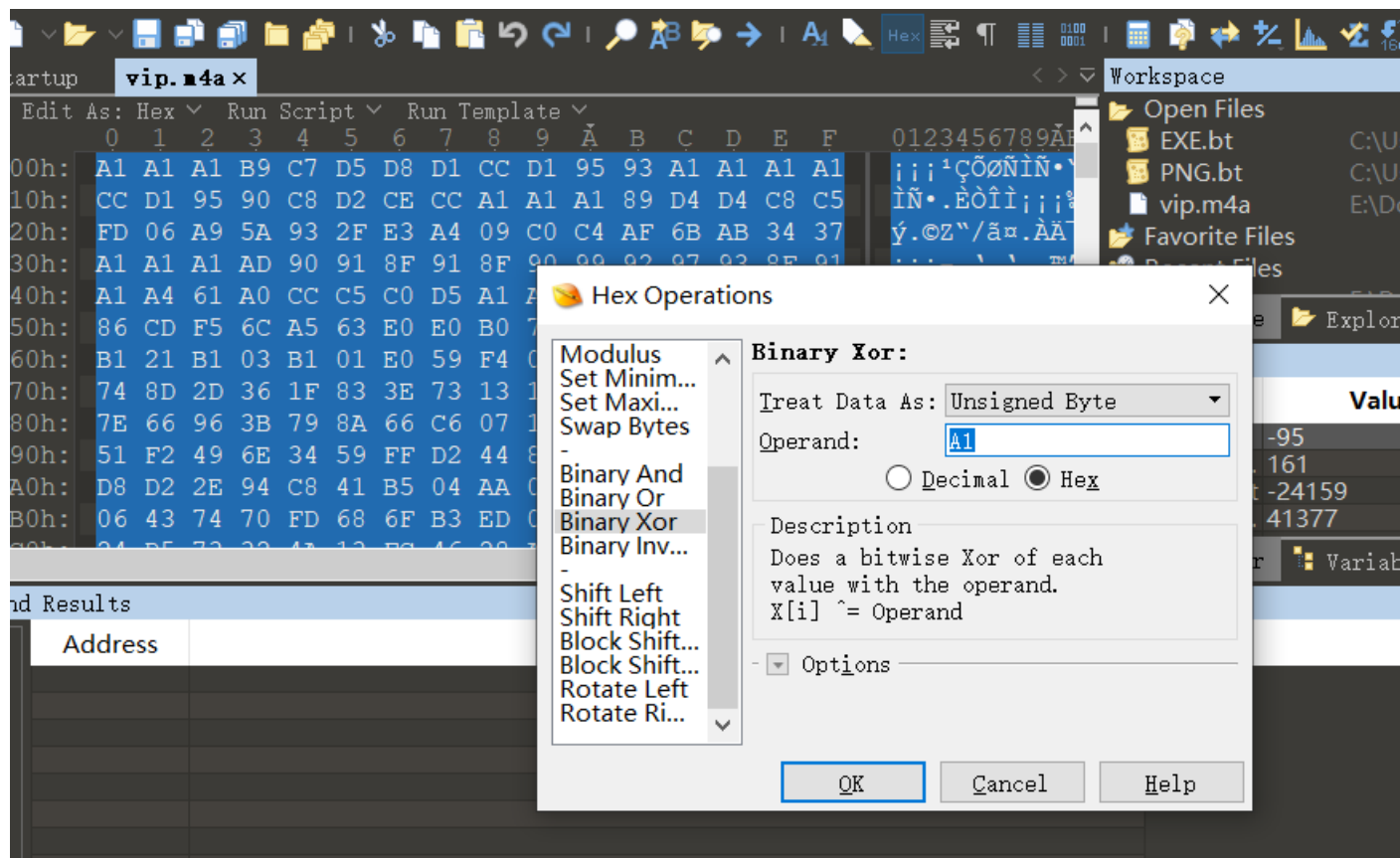
订阅专栏

文章目录

- [\[ACTF新生赛2020\]music](#)
- [\[GUET-CTF2019\]soul sipse](#)
- [\[GWCTF2019\]huyao](#)
- [\[湖南省赛2019\]Findme](#)
- [\[RCTF2019\]disk](#)
- [\[UTCTF2020\]docx 72pt](#)
- [\[QCTF2018\]X-man-A face 72pt](#)
- [\[UTCTF2020\]file header 76pt](#)
- [\[UTCTF2020\]basic-forensics 74pt](#)
- [\[UTCTF2020\]zero 74pt](#)
- [\[UTCTF2020\]sstv 76pt](#)
- [\[MRCTF2020\]pyFlag 77pt](#)
- [greatescape 78pt](#)
- [\[watevrCTF 2019\]Evil Cuteness 80pt](#)
- [\[INSHack2017\]sanity 81pt](#)
- [\[INSHack2019\]INSAnity 82pt](#)
- [\[BSidesSF2019\]table-tennis 81pt](#)
- [\[UTCTF2020\]File Carving 82pt](#)
- [\[UTCTF2020\]spectrogram 86pt](#)
- [\[INSHack2018\]Self Congratulation 85pt](#)
- [Beautiful_Side 90pt](#)
- [很好的色彩呢? 91pt](#)

[\[ACTF新生赛2020\]music](#)

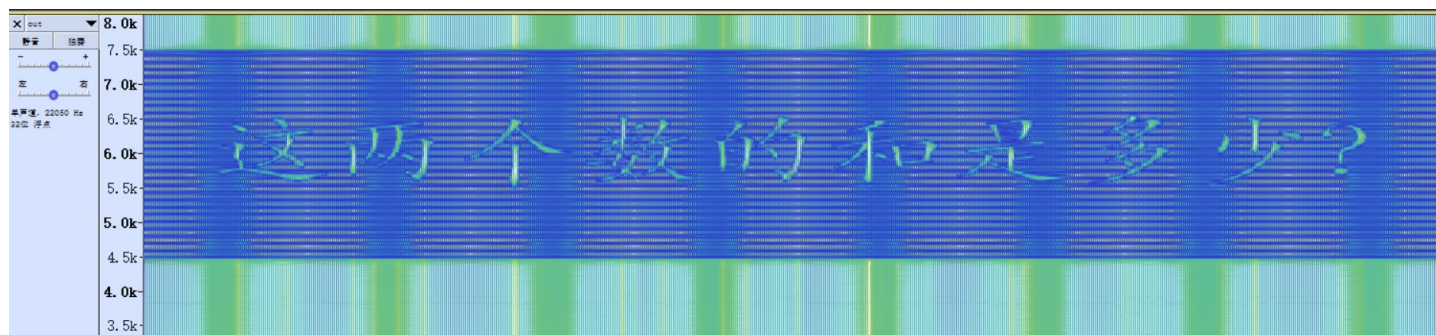
得到一个wav文件异常 且有很多A1
对A1进行异或



得到正常音频听到 actfabcdghijk
buu的flag要改一下 所以是
flag{abcdghijk}

[\[GUET-CTF2019\]soul sipse](#)

一个wav拖audacity调到频谱图 采样频率22050Hz 得到hint
这两个数的和是多少



wav文件steghide提取出一个txt 微云链接

```
root@kali:~/Desktop/temp# steghide extract -sf out.wav
Enter passphrase:
wrote extracted data to "download.txt".
root@kali:~/Desktop/temp# cat download.txt
https://share.weiyun.com/5wVTIN3root@kali:~/Desktop/temp#
```

下载得到一个破损png 文件头损坏 修改文件头得到 unicode 解码得到两个数 相加得到flag

[GWCTF2019]huyao

下载得到两个肉眼看着一样的图片 盲猜盲水印
用github上那个最常见的脚本和stegsolve没用
用1的脚本

```
python decode.py --original huyao.png --image stillhuyao.png --result res.png
```



flag{BWM_1s_c00}

[湖南省赛2019]Findme

初步分析

p1宽高crc爆破

p2可能是隐藏文件或者信息

p3应该也是crc? 但是这样不是重复考?

p4这里看不出

p5可能隐藏文件或者信息

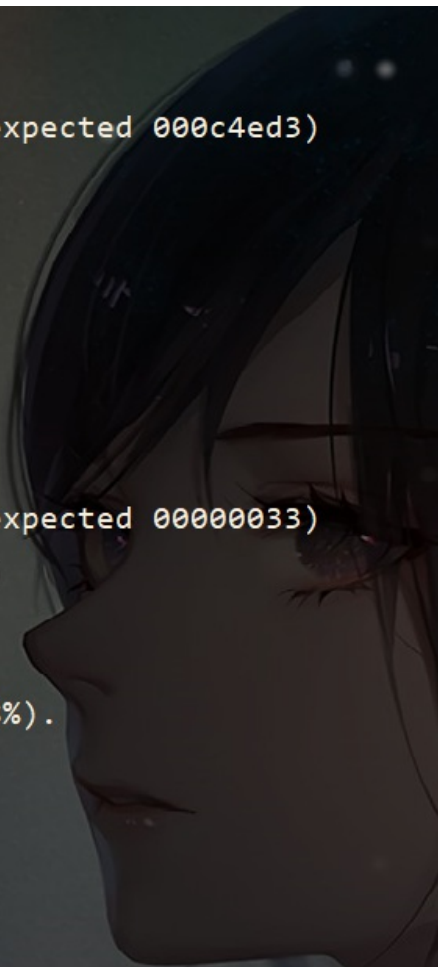
```
E:\Download\Findme
$ pngcheck 1.png
1.png CRC error in chunk IHDR (computed 8d891d0d, expected 000c4ed3)
ERROR: 1.png

E:\Download\Findme
$ pngcheck 2.png
2.png additional data after IEND chunk
ERROR: 2.png

E:\Download\Findme
$ pngcheck 3.png
3.png CRC error in chunk IHDR (computed 667dd86f, expected 00000033)
ERROR: 3.png

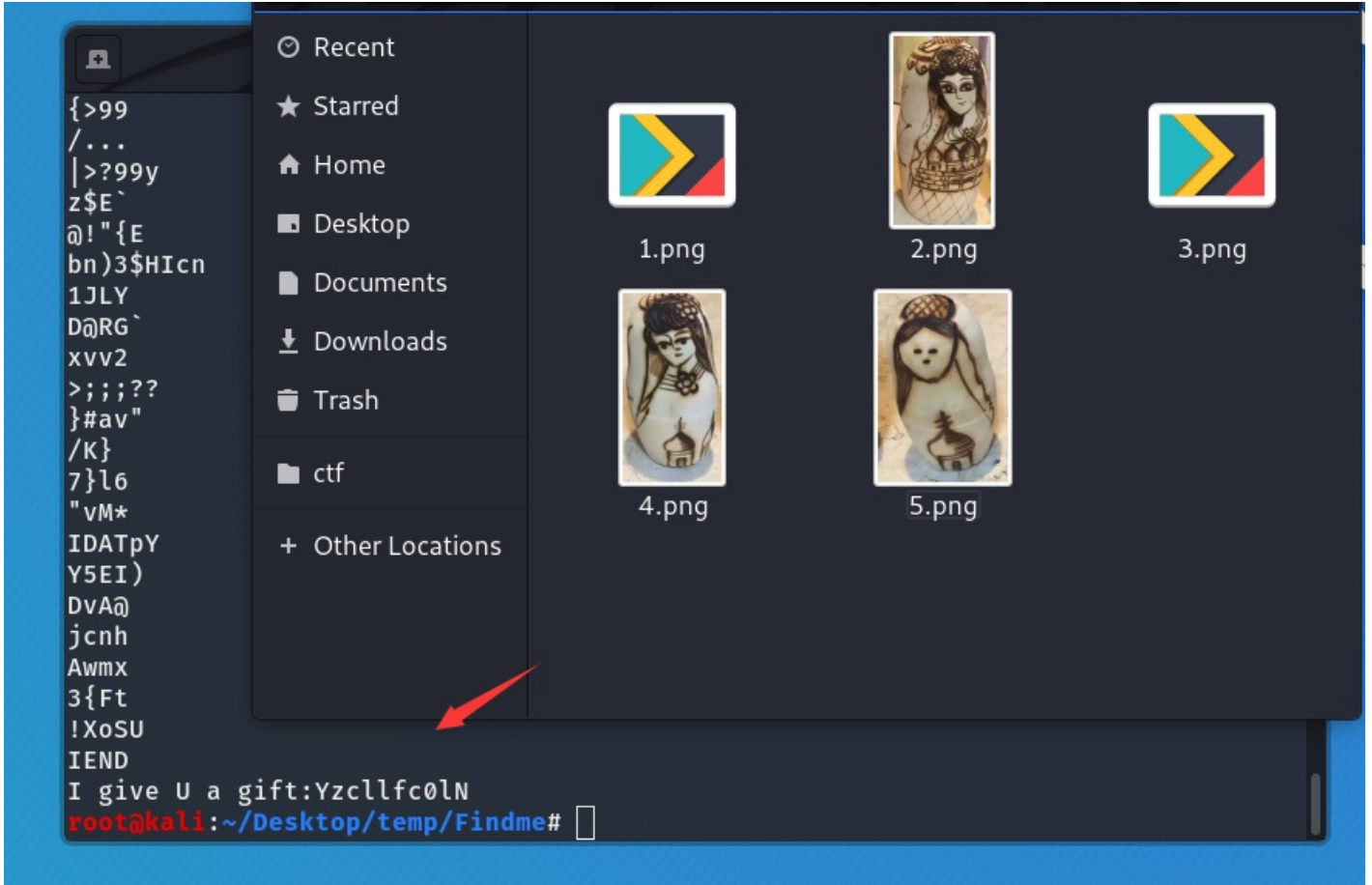
E:\Download\Findme
$ pngcheck 4.png
OK: 4.png (145x263, 24-bit RGB, non-interlaced, 43.8%).

E:\Download\Findme
$ pngcheck 5.png
5.png additional data after IEND chunk
ERROR: 5.png
```



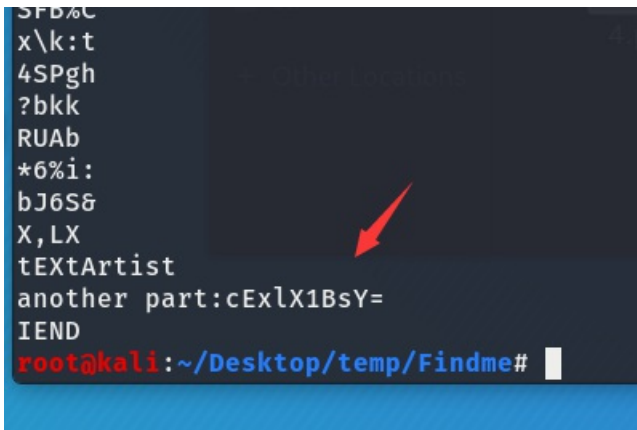
托linux直接strings * 全部文件看到hint 一开始以为可能是某个压缩包密码 先存着

p5: I give U a gift:Yzclfc0IN



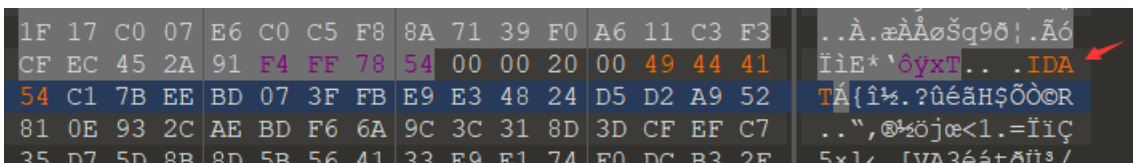
逐个strings * p4有信息

p4: another part:cExlX1BsY=



p1明显宽高 遂爆破crc

脚本可借鉴: 1



得到图片在chunk2, 3对应位置改49 44 41 54 得到正常图片

stegsolve blue2得到二维码



扫码得到

P1: ZmxhZ3s0X3

p2文件结束后就出现7z我一开始还以为是7z的压缩包呢 但是打不开
导出仔细看后是 504b0304 zip包文件头 果断全改

```
A0h: 52 57 FE C4 D7 57 E4 EA A5 D4 57 94 88 E5 51 C9 RwpÄ×wäê¥ôw^^âQÉ
B0h: F3 92 97 FE 3F 95 7C BE E1 D6 16 BC 05 00 00 00 ó' -p? • ||%á 0.4.
C0h: 00 49 45 4E 44 AE 42 60 82 37 7A 03 04 14 00 00 .IEND@B ,7z.....
D0h: 00 00 00 6E 9E 53 4F 00 00 00 00 00 00 00 00 ...nžSO.....
E0h: 00 00 00 02 00 00 00 32 2F 37 7A 03 04 0A 00 00 .....2/7z.....
F0h: 00 00 00 5D 9E 53 4F DD 1B F1 53 0C 00 00 00 0C ...]žSOÝ.ňS....
00h: 00 00 00 07 00 00 00 32 2F 30 2E 74 78 74 4E 30 .....2/0.txtN0
10h: 74 68 49 6E 67 20 68 33 72 65 37 7A 03 04 0A 00 thIng h3re7z....
20h: 00 00 00 00 5D 9E 53 4F DD 1B F1 53 0C 00 00 00 ....]žSOÝ.ňS....
30h: 0C 00 00 00 07 00 00 00 32 2F 31 2E 74 78 74 4E .....2/1.txtN
40h: 30 74 68 49 6E 67 20 68 33 72 65 37 7A 03 04 0A 0thIng h3re7z...
50h: 00 00 00 00 00 5D 9E 53 4F DD 1B F1 53 0C 00 00 ....]žSOÝ.ňS...
60h: 00 0C 00 00 00 08 00 00 00 32 2F 31 30 2E 74 78 .....2/10.tx
70h: 74 4E 30 74 68 49 6E 67 20 68 33 72 65 37 7A 03 tN0thIng h3re7z.
80h: 04 0A 00 00 00 00 00 5D 9E 53 4F DD 1B F1 53 0C .....]žSOÝ.ňS.
90h: 00 00 00 0C 00 00 00 09 00 00 00 32 2F 31 30 30 .....2/100
A0h: 2E 74 78 74 4E 30 74 68 49 6E 67 20 68 33 72 65 .txtN0thIng h3re
B0h: 37 7A 03 04 0A 00 00 00 00 00 5D 9E 53 4F DD 1B 7z.....]žSOÝ.
C0h: F1 53 0C 00 00 00 0C 00 00 00 09 00 00 00 32 2F ňS.....2/
D0h: 31 30 31 2E 74 78 74 4E 30 74 68 49 6E 67 20 68 101.txtN0thIng h
E0h: 33 72 65 37 7A 03 04 0A 00 00 00 00 00 5D 9E 53 3re7z.....]žS
```

P2: You find it: 1RVcmVfc

p3每个chunk的crc都很短很奇怪 取出来连在一起

Name	Value	Start
> struct PNG SIGNATURE sig		0h
▼ struct PNG CHUNK chunk[0]	IHDR (Critical,...	8h
uint32 length	13	8h
> union CTYPE type	IHDR	Ch
> struct PNG CHUNK IHDR ihdr	205 x 337 (x8)	10h
uint32 crc	33h	1Dh
▼ struct PNG CHUNK chunk[1]	pHYs (Ancilla...	21h
uint32 length	9	21h
> union CTYPE type	pHYs	25h
> struct PNG CHUNK PHYS p...		29h
uint32 crc	52h	32h
> struct PNG CHUNK chunk[2]	IDAT (Critical,...	36h
> struct PNG CHUNK chunk[3]	IDAT (Critical,...	8042h

P3: 3RIZ30=

汇总

5.I give U a gift:Yzclfc0IN

4.another part:cExlX1BsY=

3.3RIZ30=

2.You find it: 1RVcmVfc

1.ZmxhZ3s0X3

接下来任何人都知道要干嘛了

12345连在一起 出来这个 可以看出 1是开始的, 2或者3是最后的

```
flag{4_QUc}??pLe_Pla?W??S[Finished in 0.1s]
```

经过排序15423

```
flag{4_v3rY_sIMpLe_PlCTure_steg}[Finished in 0.1s]
```

[RCTF2019]disk

看了一下wp 这个开局给的password buu里是没用提示的。。。

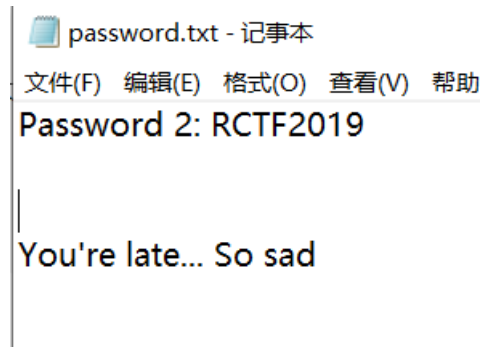
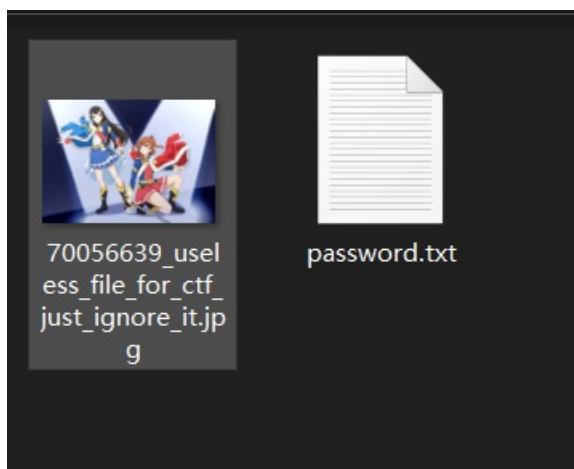
题目设定如下:

An otaku used VeraCrypt to encrypt his favorites.

Password: `rctf`

Flag format: `rctf{a-zA-Z0-9_}`

使用 VeraCrypt 成功挂载
两个文件



第一反应是图片里有压缩包 这个password是压缩包的密码 但是不是

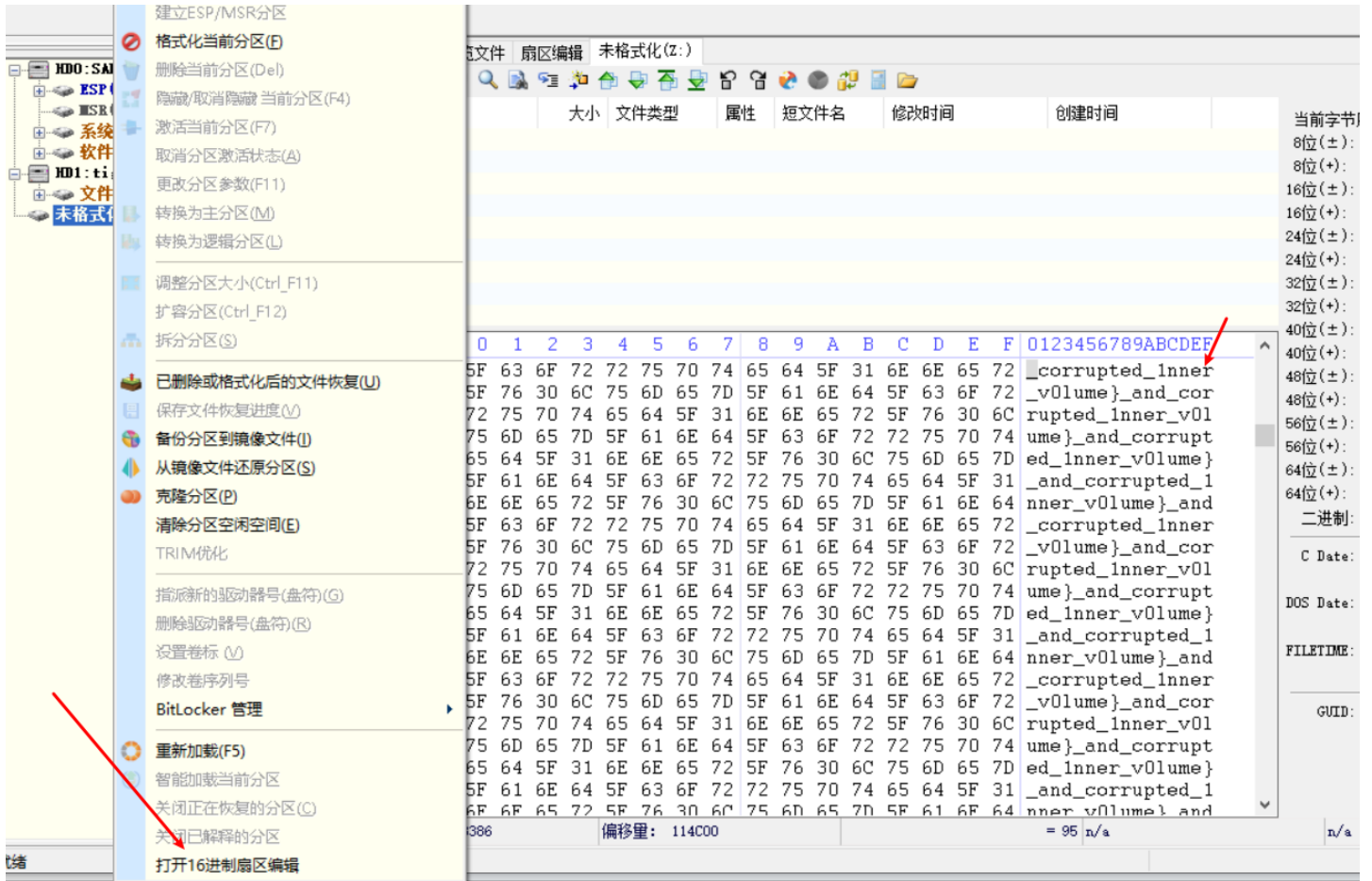
再次瞟一眼wp居然可以拿这个password重新挂载磁盘

不同密码对应不同文件 挺神奇的

想要自己复现一个这样的vmdk 发现使用VeraCrypt跟着指引走就可以直接创建了
重新挂载发现是无法访问的磁盘

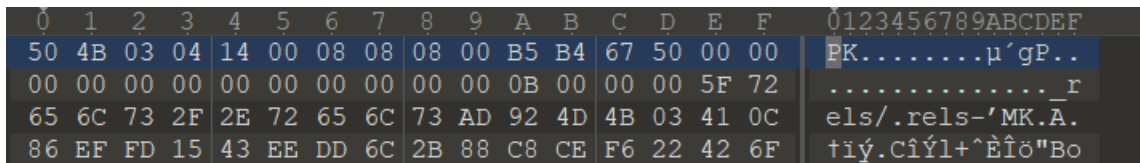
DiskGenius打开16进制编辑发现另一半flag

and_corrupted_1nner_v0lume}



[UTCTF2020]docx 72pt

下载一个docx 010打开pk头



foremost得到zip打开zip /word/media 里面有很多图片

找到flag

啊? 72pt就这?

utf_lag{unz1p_
3v3ryth1ng}

[QCTF2018]X-man-A face 72pt

挺简单一个题

下载一个破损二维码 每发现别的 尝试修复二维码



修复好之后cqr和qrazyboz都扫不出来 有点自闭 看了一下wp, 那个补的比我的差多了但是说能扫出来 拿微信扫了一下 还真扫出来了。。。挺神奇的

KFBVIRT3KBZGK5DUPFPVG2LTORSXEX2XNBXV6QTVPFZV6TLFL5GG6YTTORSXE7I=

base32解码

QCTF{Pretty_Sister_Who_Buys_Me_Lobster}

[UTCTF2020]file header 76pt

题目名为文件头 一个明显png 换上头就有flag。。啊?? 这??

```
Startup attachment.png x
Edit As: Hex Run Script Run Template
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
000h: 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 %PNG.....IHDR
010h: 00 00 04 A8 00 00 02 9E 08 06 00 00 00 81 2E 23 ..."....ž.....#
020h: AF 00 00 28 25 7A 54 58 74 52 61 77 20 70 72 6F ..(%zTXtRaw pro
030h: 66 69 6C 65 20 74 79 70 65 20 65 78 69 66 00 00 file type exif
```

utflag{3lit3_h4ck3r}

[UTCTF2020]basic-forensics 74pt

一个文本。很多东西 以为是某种方式隐藏信息。。结果一搜就出来了。。。。。。。。啊?? 这??

```
utflag{fil3_ext3nsi0ns_4r3nt_r34l}
```

utflag{fil3_ext3nsi0ns_4r3nt_r34l}

[UTCTF2020]zero 74pt

一个文本文件 刚开始以为类似凯撒之类的，用自己写的脚本跑出来奇奇怪怪的结果
放cyberchef 贴进去就可以看到很多点 猜测零宽字节

```
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus quis tempus ante, nec vehicula mi. Aliquam nec nisi ut neque interdum auctor. Aliquam felis orci, vestibulum sit amet ante at, consectetur lobortis eros. Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. In finibus magna mauris, quis auctor libero congue quis. Duis sagittis consequat urna non tristique. Pellentesque eu lorem id quam vestibulum ultricies vel ac purus.
```

Output

start: 903 time: 1ms
end: 903 length: 965
length: 0 lines: 1

```
.....Lorem ipsum..... dolor .....sit..... amet....., consectetur
.....adipiscing..... elit..... Phasellus quis.....
tempus..... ante, .....nec vehicula..... mi..... Aliquam
nec..... nisi ut neque..... interdum auctor..... Aliquam felis
..... orci ..... vestibulum ..... sit ..... amet ..... ante ..... at.....
```

```
.....; vestibulum .....amet..... ac.....  
consectetur..... lobortis eros.....Orci varius.....  
.....natoque .....penatibus et .....magnis..... dis  
.....parturient montes, .....nascetur ridiculus .....mus. In  
finibus..... magna..... mauris, quis..... auctor .....libero congue quis.  
.....Duis..... sagittis consequat urna non tristique. Pellentesque eu lorem  
.....id..... quam vestibulum ultricies vel ac purus.....
```

放vim看看

```
202c> at<200b><200b><200b><200b><200b><200b><200b>, consectetur<200c><  
0c><200c><200d><200c><feff><feff> lobortis eros<200b><200b><200b><200b>  
200b><200b><200b><200b>.<200c><200c><200c><200c><200d><200d><200d><200  
><200c><200c><200c><200d><200c><200c><200c><200b><200b><200b><200b><20  
><200b>Orci varius<200b><200b><200b><200b><200b><200b><200b> <200b><20  
><200b><200b><200b><200b>natoque <200c><200c><200c><200c><200d><feff><fe  
ff>penatibus et <200c><200c><200c><200c><200d><202c><200c><feff><200b>  
00b><200b><200b><200b><200b>magnis<200c><200c><200c><200c><200c><feff>  
00d><200c><200c><200c><200c><200c><feff><200c><200d> dis <200b><200b><  
0b><200b><200b><200b><200c><200c><200c><200c><200d><200d><feff><feff>p  
t montes, <200b><200b><200b><200b><200b><200b><200b><200b>nascetur ridiculus  
200c><200c><200c><200c><feff><200d><200c><200b><200b><200b><200b><200b>  
200b><200b><200b><200b><200b><200b><200b><200b><200c><200c><200c><200c>  
feff><202c><200d>mus. In finibus<200c><200c><200c><200c><200c><feff><2  
c> magna<200b><200b><200b><200b><200b><200b><200c><200c><200c><200c><2  
f><200d><feff> mauris, quis<200c><200c><200c><200c><200d><202c><200c><  
ctor <200c><200c><200c><200c><200d><202c><200c><200d>libero congue qui  
><200c><200c><200c><200d><202c><202c><202c>Duis<200c><200c><200c><200c>  
202c><200c><202c> sagittis consequat urna non tristique. Pellentesque  
<200c><200c><200c><200c><200d><feff><200c><200d>id<200c><200c><200c><  
0d><202c><202c><feff> quam vestibulum ultricies vel ac purus<200c><200  
<200c><200c><feff><200c><200d>.<200c><200c><200c><200c><200c><feff><20
```

果然 遂解密网站

utflag{whyNOT@sc11_4927aajbqk14}

[UTCTF2020]sstv 76pt

qsstv教程

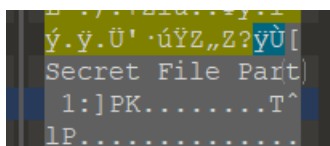
<http://www.srcmini.com/62326.html>

utflag{6bdfcac1e2baa12d6ac5384cdfd166b0}

utflag{6bdfcac1e2baa12d6ac5384cdfd166b0}

[MRCTF2020]pyFlag 77pt

三张图片 结尾有提示part1, 2, 3 提取出一个zip



爆破密码 1234

打开hint 提示很明显了

我用各种baseXX编码把flag套娃加
但我只用了一些常用的base编码哦
提示: 0x10,0x20,0x30,0x55

```
Python 3.8.0 (tag:
Type "help", "copy
>>> 0x10
16
>>> 0x20
32
>>> 0x30
48
>>> 0x55
85
>>> |
```

没有48 32报错 16正确

```
import base64

b85 = base64.b85decode("G&e0hGcg(ZG(t2*H8M3dG&wXiGcg(
print(b85)
b16 = base64.b16decode(b85)
print(b16)
b32 = base64.b32decode(b16)
print(b32)
b16 = base64.b16decode(b32)
print(b16)
b64 = base64.b64decode(b16)
print(b64)
```

```
test x
D:\IDE\python\python3.8\python.exe D:/Project/python
b'475532444B4E525549453244494E4A57475132544B514A5447
b'GU2DKNRUIE2DINJWGQ2TKQJTG42TONJUGQZDGMJVHAZTANBWG4
b'54564A4456455A3757544231583046795A5638305833417A63
b'TVJDVEZ7WTB1X0FyZV80X3AzckZLY3RfZGVjMGRlcn0='
b'MRCTF{Y0u_Are_4_p3rFect_decoder}'

Process finished with exit code 0
```


Wireshark · 追踪 TCP 流 (tcp.stream eq 18) · greatescape.pcap

```
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 1 of 5 allowed.
220-Local time is now 11:51. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
USER bob
331 User bob OK. Password required
PASS toto123
230 OK. Current directory is /
SYST
215 UNIX Type: L8
TYPE I
200 TYPE is now 8-bit binary
PORT 172,17,42,1,171,159
200 PORT command successful
STOR ssc.key
150 Connecting to port 43935
226-File successfully transferred
226 0.001 seconds (measured here), 4.59 Mbytes per second
QUIT
221-Goodbye. You uploaded 4 and downloaded 0 kbytes.
221 Logout.
```

流19看到类似ssh key的东西 就是上图的 ssc.key 先保存下来

```
-----BEGIN PRIVATE KEY-----
MIIJQwIBADANBgkqhkiG9w0BAQEFAASCCS0wggkpkAgEAAoICAQC5twyPH+2U6X0Q
uxOKPThSR6MkXGSvAz+Ax+G9DKEiBLuTtfl7dNv4oswdmT9nWlSY1kxZatNwLUF8
WAuGLntO5xTEmOJlMtBFrWGD+DVpCE9KORGvYif8e4xxi6vh4mkw78IxV03VxHM0
mk/cq5kkERfWQW81pVeYm9UAm4dj+LcCwQ9aGd/vfTtcACqS50GtELFbSHJuFVyn
srpp4K6tLTrk2ensSnmXUXNEjqpodfdb/wqGT86NYg7i6d/4Rqa440a6BD7RKrgp
YPaXl7pQusemHQpd248fxsuEfEwhPNDJhIb8fDX9Bwv2xTfBLhGwOh7euzSh2C4o
KSuBAO+bIKL+pGY1z7DFtuJYfTOSJyQ5zQzToxS+jE+2x9/3GpD2LUD0xkA8bwhv
eecq0v6ZWBVYNX54V5ME3s2qxYc6CSQhi6Moy8xwlcSpTSAa7voNQNa9RvQ4/3KF
3gCbKtFvdd7IHvxfn8vcCrCZ37eVkkq0F1ly5UNEJU/Y0Tt8m7UDn3uKNpB841BQa
hiGayCSjsHuTS8B+MnnpnzWCrzD+rAzCB37B599iBK4t/mwSIZZUzaqxTWNofS2Lz
7m0LumZ4Yk8DpDEuWhNs8OUD8FsgAvWfVAvivaaAcif3kMs8pkmNTs2LFBowOshz
SXfONshupgXEwwFrKOOZXnhb+O/WKQIDAQABoICAAT6mFaZ94efft/c9BgnrddC
XmhSJczfXGt6cF3eIc/Eqra3R3H83wzaaHh+rEl8DXqPfdQfD6e0CK5pud1eD6Y8
4bynkKI/63+Ct30PSvdG5sFJqGS7Gb1WIpzErtX+eOzJfr5N5eNOQfxuCqGS3acu
4iG3XWdlzuRjgSFkCgWvFdD4Fg5HVU6ZX+cGhh2sDzTRlr+rilXTMsm4K/E8udIg
yEbv5KqWEI5y+5Eh9gWY7AnGw6TgLNxzfYyt0nhYhI2+Yh4IKRqQd6F8XQARbEhP
yZx1eK4Q/dRPQXOJNY1KkrPl+Cx6tAPVimByRx1hu82qsTstb6rLHemruOPbf5Dw
aqgSFdp7it3uqjJHCWJ2hAZoijAcv1hn1sa1hr/qFFly/weDAi80yvGdCSh30vs6
yazkah85GOnY85rz+s98F9cvIqcRdGJrAeNBUHhNj6+X9qFVtwDpF0V1vlvn2Ggp
7m8hiZ0Y+8T+7qfnS9WsdPh7MkoIEoZ0CPryYvX+YPLYwqzxtCvrRWF8tAScI6H+
XBz3NlCAUaok+Z0kKlZ8ZYMSn/g5EV2jj/mwZVdtYoeQjLaCDuLq8E1Hswnpqg7F
54hHU7voeJ1/TQltLCNFJFQRauD+tPz9R6jVpbqBiXIC2eiGTo1rP4Ii7hsQRFC
W0KKqu+bv69HJAmi06yBAoIBAQDvz+c+3z9njQFFaeUUqyzl31HOzRHmwhJEorIR
nRhWTLzqMyn+RLGrD3DJQj/dGH6tyxHJ7PdI7gtJ3qaF4lCc2dKR3uQW3CBKI9Ys
wz3Bk0Tijcfht+Yh9YEvYB3uPdkcHE3BpTY7QWAFvzDwTD7z34650h166h/um
```


wzjBw0T1JatDCCANaIKEWAR3vHFK+Sb3Zbq1KZQVA3VZFW1FJ1Z3H0E91L000/ur
DS9owYRBmykX1V9Gt91V15cpg3yxPixaELMhqDD2Ebq60FyuacExQHfGUeP0Va/A
IdM9+H5DE13qR2INX+N0kAFyFzW7k8AvY37KGZdoACURDzmmGoilfs/pFAC0kZaZ
tKXoR9iLNxWSBtlI2Fr3qz4gc5nItYb7JSQsdu6Lc92+9z4xAoIBAQQGQFDXVQyk
Q5tswicru5v2c9VoFpLUTBg4Dx3uXOMEV1/S5hZ8jYbUH4dcwKyLCYQLtNSc9aei
8zm18Td0Gm0nCL0o70PMeet+JHyx8uz1l/Sx4ucI/Jq3yVSTqdtXYakxzijTldNQ
M7YnjpbCs0yDk806R7J3xvzxNMbElQH1bP947Ej0sv40cBcA0hdpjuuNI5C20t4P
fUZxfqR34L7aPZPuP82W2WqFgkTyMY8F0235qR+Sy5xrcHSS4L1FdF+PhS5ZjiPN
sudXRvfNFQlKZRUYqB147XY7EDnx6BZW2aoM7AiYPiGhxZev4NHY1ChdB02CSmOA
03FvucMEMUF5AoIBAD2xorA0BuXA5L7Sy1hR4S8SEJ2/LAeyzFhT9F+hpo0tGLY3
h0ohCgQT6NQd8wgSMSTMxTrJd6SPeN/8I6L14f84Gm/kg5FN+BCav5KsdoFnORr/
jlt74et3e+yuSCQ2HuKdkCGScuPOgzYUw54Ea6cyI5v/yx9kcxzLik8xZSzx+/BU
1nF2wBgVXR+T7BOF/CIs+IQd4RebiV0EmqElttI36rec+jNPBFHpyVkIWqvqrDb

分组 661, 0 客户端 分组, 1 服务器 分组, 0 turn(s). 点击选择。

输入对话 (9999) 且二和保存数据为 40000

编辑->首选项->protocols->TLS 把刚才的key导入

流80追踪http可以找到flag

[watevrCTF 2019]Evil Cuteness 80pt

图片解为有zip

取出来 abc里就是flag

[INSHack2017]sanity 81pt

一个tar 里面有个md文件 但是md和tar大小差很大 010看下tar 看到flag。。。

```
0 .....  
3 # Challenge desc  
C ription:...I real  
0 ly hope you are  
4 INSane, but if t  
1 hat's not the ca  
0 se and that you  
1 don't want to va  
1 lidate the "INSA  
0 nity" challenge  
7 then maybe you w  
C ould like to val  
0 idate this one?  
1 Here is your fla  
4 g, you disapoint  
6 ing and boring f  
2 ellow: [INSA{Your  
F e_sane Good for  
0 you}.....
```

结果看了一个md md里就是这个flag 我服了。。。

[INSHack2019]INSAnity 82pt

???跟上面一模一样的。。。这不是直接白给吗
好像2018 2017 2019都有两题送分的 就不写了。。。

[BSidesSF2019]table-tennis 81pt

request末尾连在一起是一个html

手抄得到document.write(Q1RGe0p1c3RBuzBuZ0FiMHV0UDFuZ1Awbmd9)

base64decode 就是flag

```
.217.5.100      ICMP      98 Echo (ping) request i
.168.10.212    ICMP      98 Echo (ping) reply  i
.217.6.36      ICMP      98 Echo (ping) request i
.168.10.212    ICMP      98 Echo (ping) reply  i
.217.5.100     ICMP      98 Echo (ping) request i
.168.10.212    ICMP      98 Echo (ping) reply  i
.217.5.100     ICMP      98 Echo (ping) request i
.168.10.212    ICMP      98 Echo (ping) reply  i
.217.0.36      ICMP      98 Echo (ping) request i
.168.10.212    ICMP      98 Echo (ping) reply  i
.217.5.100     ICMP      98 Echo (ping) request i
```

14:29:36.000000000 中国标准时间

0.175236609 seconds]

```
08 00 45 00    ..^.....K...E.
0a d4 ac d9    .T (@@  .....
74 5c 00 00    .$.....$ ..t\..
65 61 64 3e    ..^.....<head>
65 61 64 3e    ..<head> ..<head>
65 61 64 3e    ..<head> ..<head>
..
```

```
6.36      ICMP      98 Echo (ping) request id=
10.212    ICMP      98 Echo (ping) reply  id=
5.100     ICMP      98 Echo (ping) request id=
10.212    ICMP      98 Echo (ping) reply  id=
5.100     ICMP      98 Echo (ping) request id=
10.212    ICMP      98 Echo (ping) reply  id=
0.36     ICMP      98 Echo (ping) request id=
10.212    ICMP      98 Echo (ping) reply  id=
5.100     ICMP      98 Echo (ping) request id=
```

469746c653e20...

```
0 45 00    ..^.....K...E.
4 ac d9    .T}@@@ ? .....
c 00 00    .d..5:.& ....t\..
4 6c 65    ..=.....<title
4 6c 65    > <title > <title
4 6c 65    > <title > <title
>
```

```
id ac d9 ·T·v@·@· .....
ic 00 00 ·$·.·r·0 ····t\··
id 65 6e ······ ··ocumen
id 65 6e t.ocumen t.ocumen
id 65 6e t.ocumen t.ocumen
t.
```

[UTCTF2020]File Carving 82pt

一张图片 后面一个zip 取出 一个elf文件 丢linux跑 出flag

```
(base) ruoke@ruoke:~/Desktop/tmp$ ./hidden_binary
Ah, you found me!
utflag{2fbe9adc2ad89c71da48cabe90a121c0}
```

[UTCTF2020]spectrogram 86pt

英文名翻译一下是频谱图 托audacity秒出



flag{sp3tr0gr4m0ph0n3}

[INSHack2018]Self Congratulation 85pt

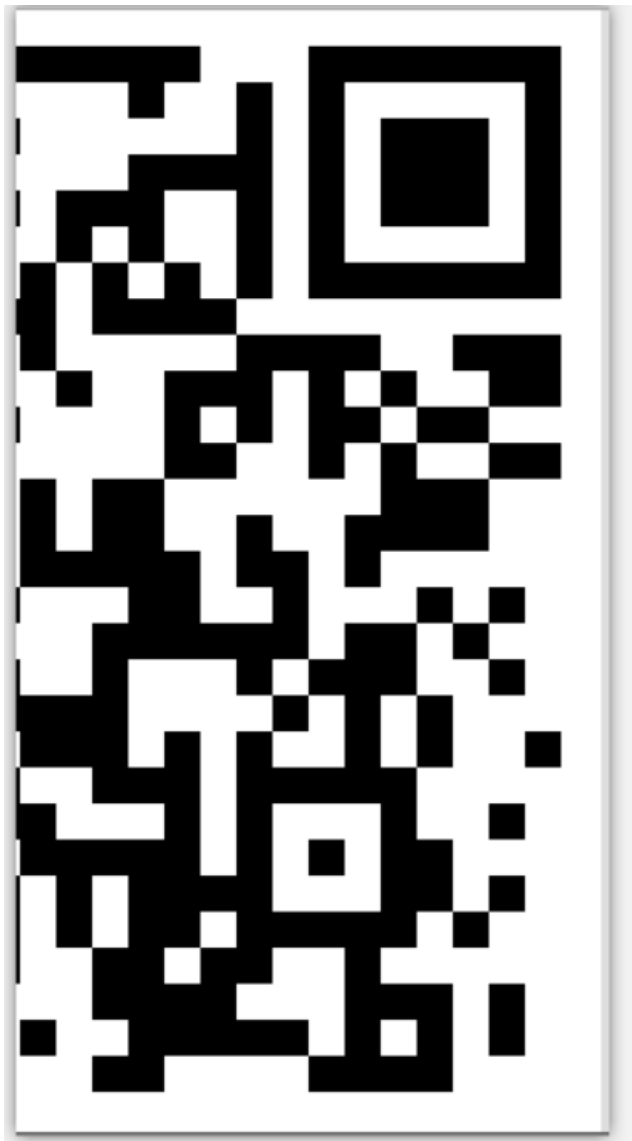
左上角类似二维码 转二进制

```
00110001001
10010001100
11001101000
01101010011
01100011011
10011100000
```



Beautiful_Side 90pt

提取出半个二维码 照经验是可以扫出来的 遂手撸



: Flag{OQWIC_4DS1A_S034S}





很好的色彩呢？ 91pt

六个颜色可以看出来有不一样 ps看16进制 得到



8b8b61

8b8b61

8b8b70

8b8b6a

8b8b65

8b8b73

lsb原理 把后面拿出来转字符串就是flag

flag{aapjes}