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入坟

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入坟 专栏收录该内容

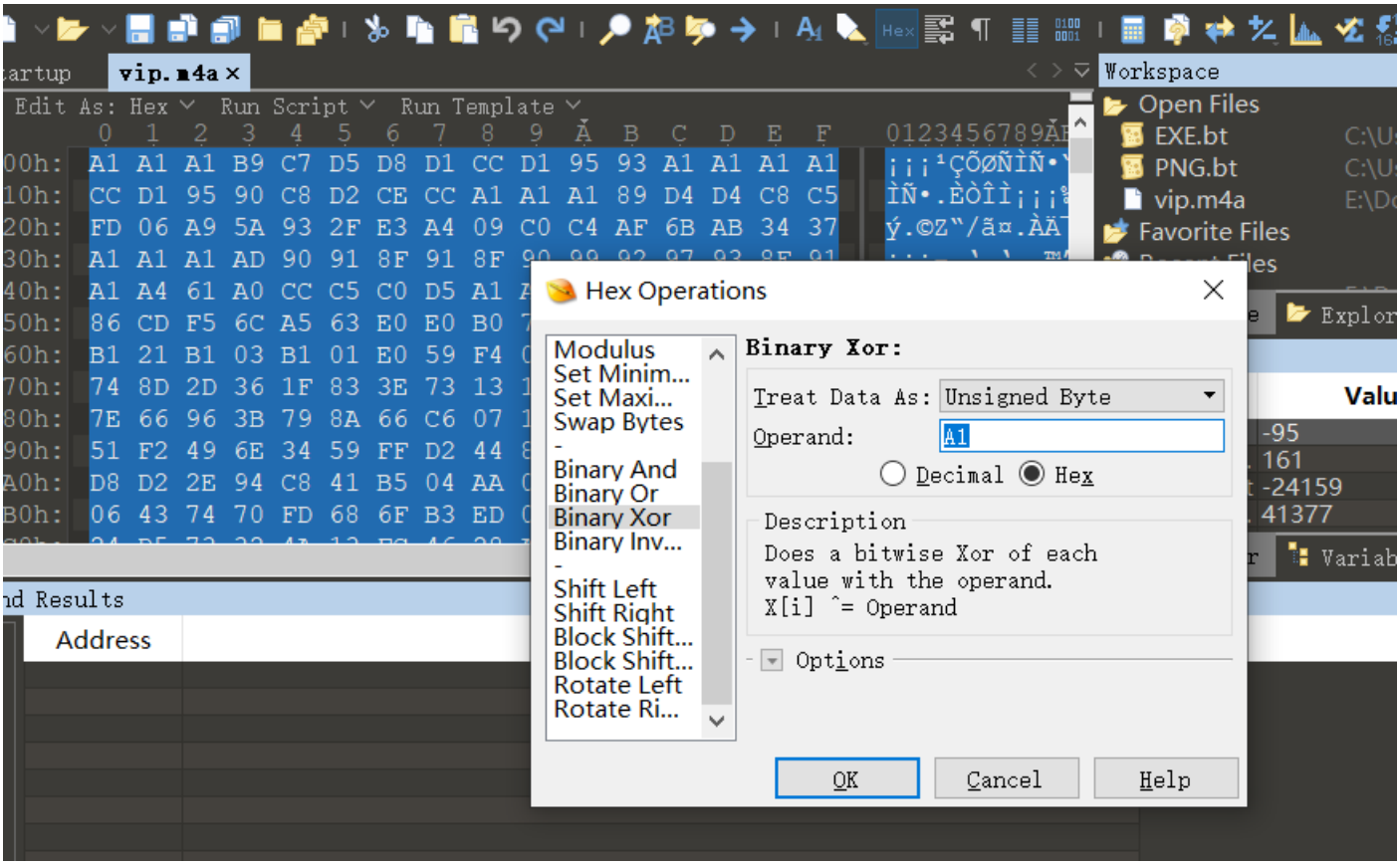
33 篇文章 1 订阅

订阅专栏

文章目录

[ACTF新生赛2020]music

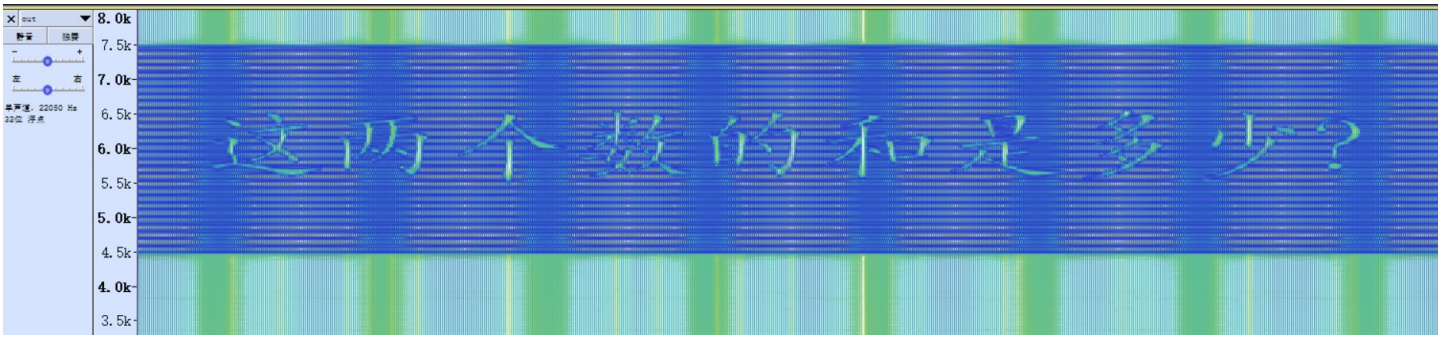
得到一个wav 文件异常 且有很多 A1
对A1进行异或



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

[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_c00l}

[湖南省赛2019]Findme

初步分析

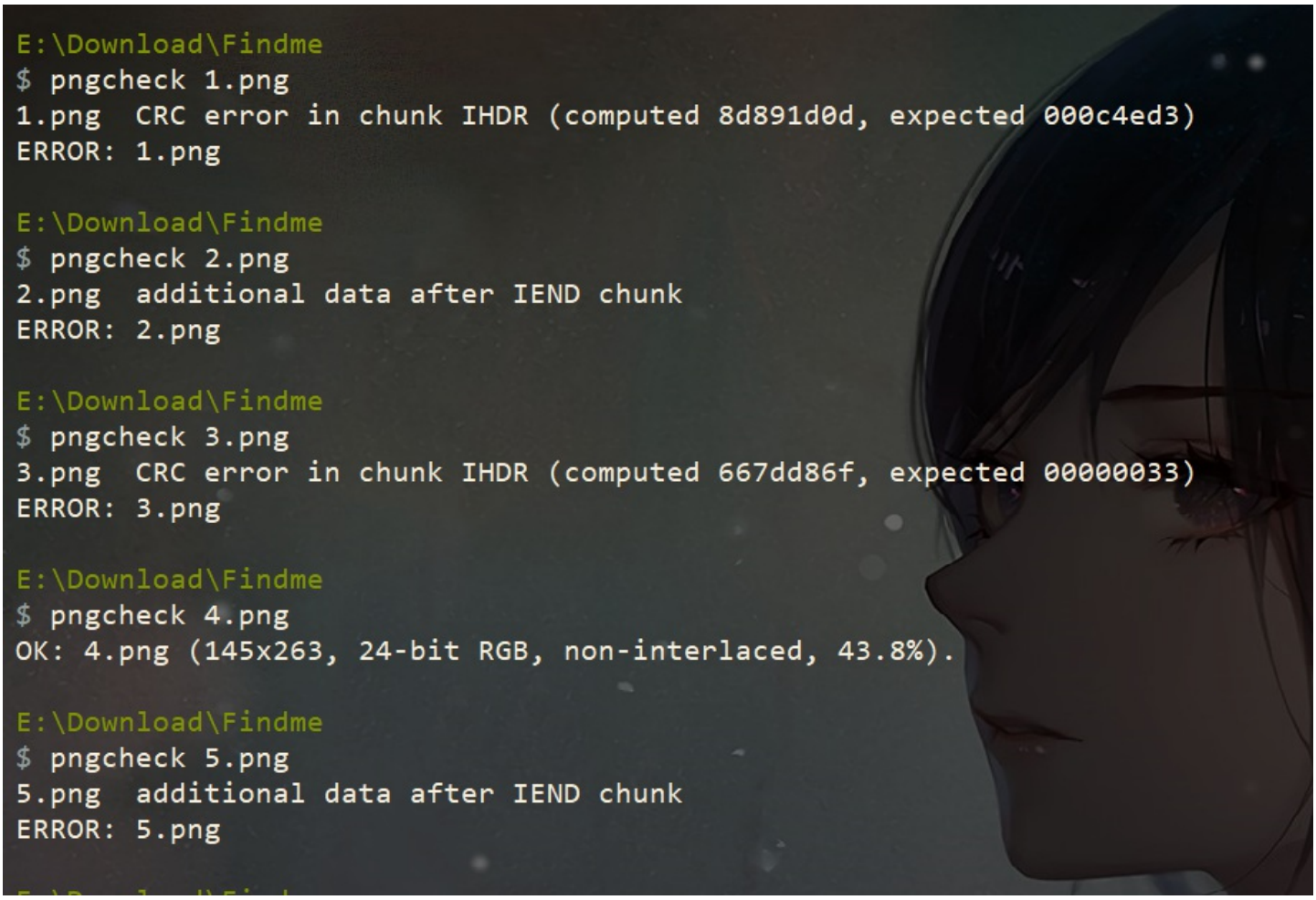
p1宽高crc爆破

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？

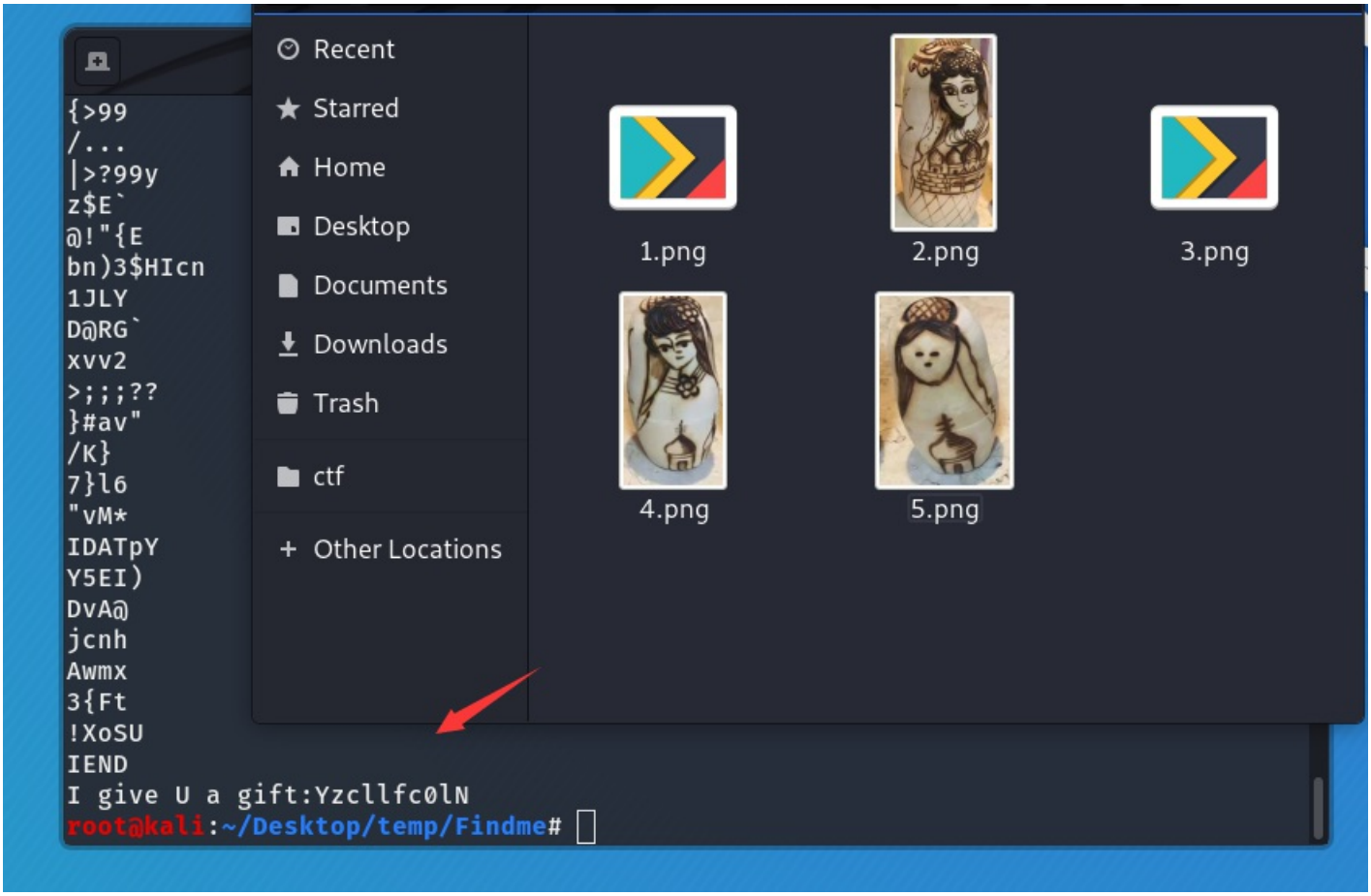
p4这里看不出

p5可能隐藏文件或者信息



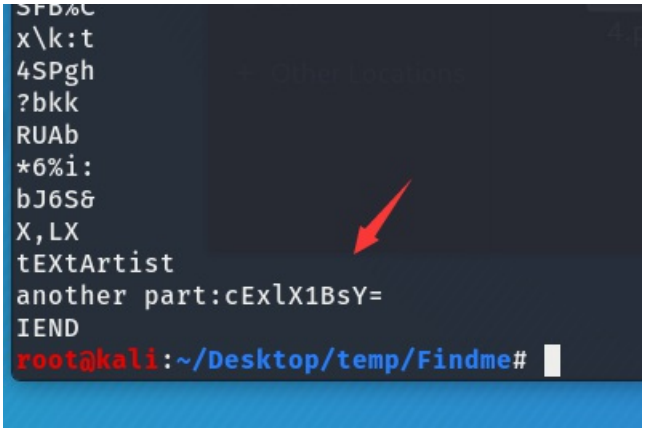
托linux直接strings * 全部文件看到hint 一开始以为可能是某个压缩包密码 先存着

p5：I give U a gift:YzcIlfc0IN



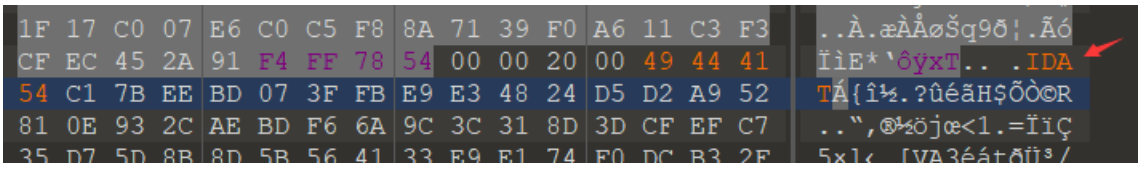
逐个strings * p4有信息

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

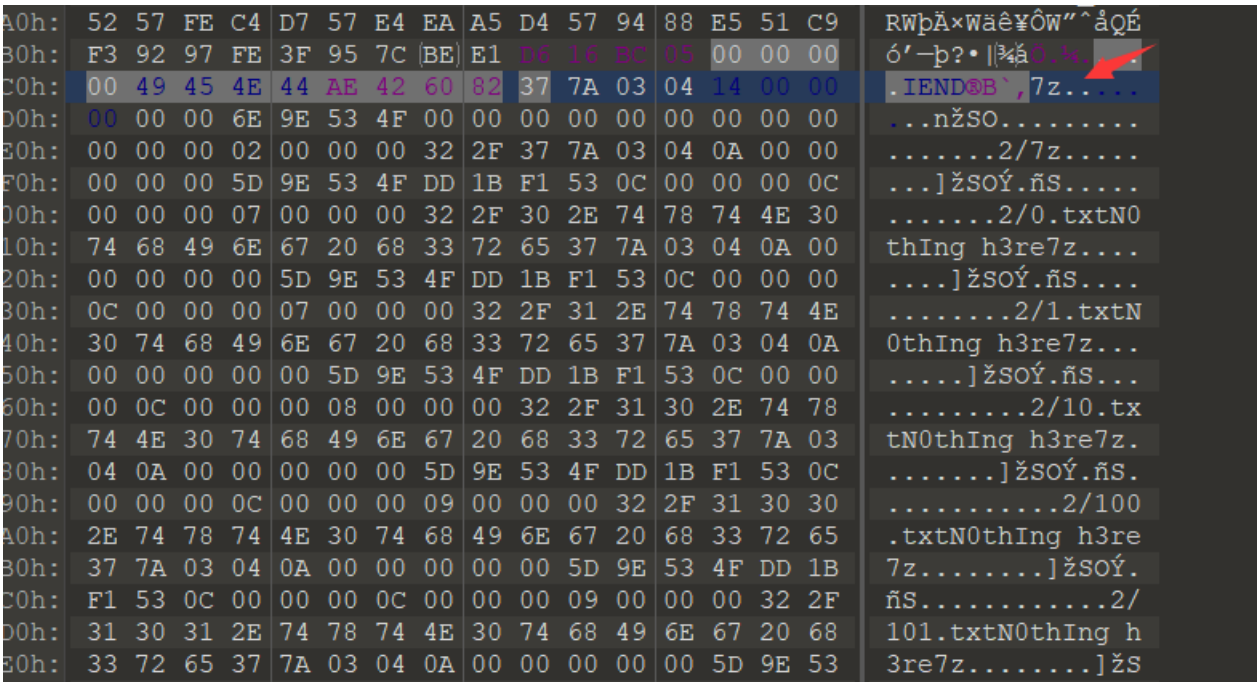
stegsolve blue2得到二维码

扫码得到

P1：ZmxhZ3s0X3

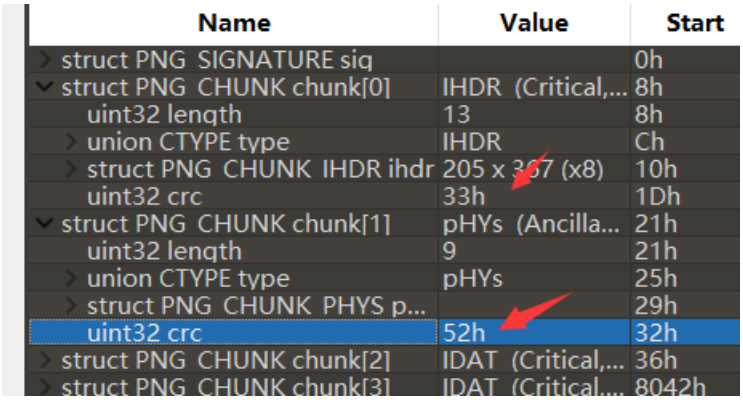
p2文件结束后就出现7z我一开始还以为是7z的压缩包呢 但是打不开

导出仔细看后是 504b0304 zip包文件头 果断全改



P2：You find it: 1RVcmVfc

p3每个chunk的crc都很短很奇怪 取出来连在一起



P3：3RlZ30=

汇总

5.I give U a gift:YzcllfcOlN

4.another part:cExlX1BsY=

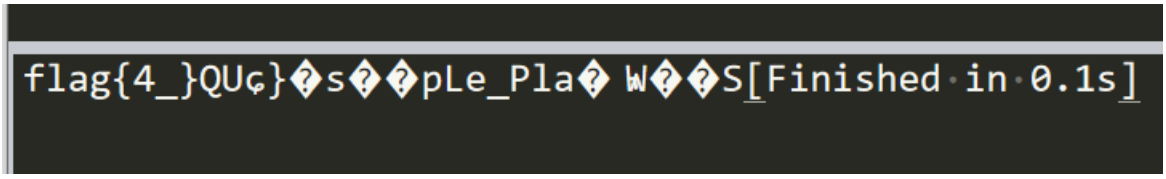
3.3RlZ30=

2.You find it: 1RVcmVfc

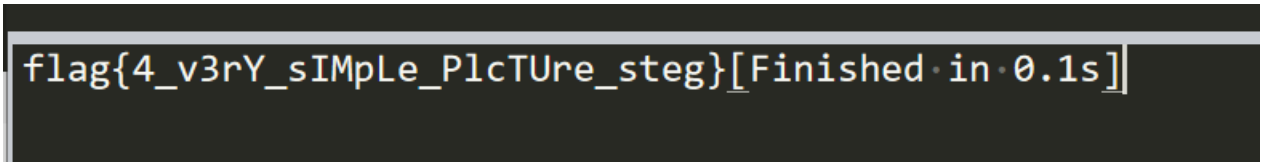
1.ZmxhZ3s0X3

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



经过排序15423

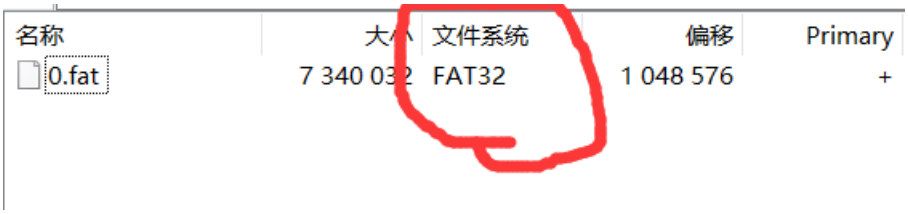


[RCTF2019]disk

拿到一个 encrypt.vmdk

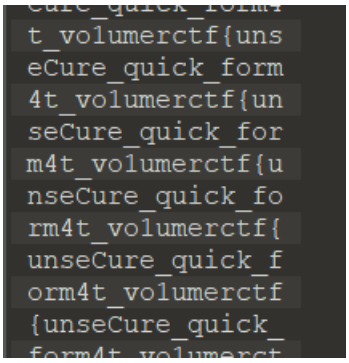
之前做过一个 vmdk的题buu面具下的flag是7z解压的方式

尝试7z打开看到是一个 0.fat 是一个FAT32的 文件系统



010打开看到一大串

rctf{unseCure_quick_form4t_vo1ume



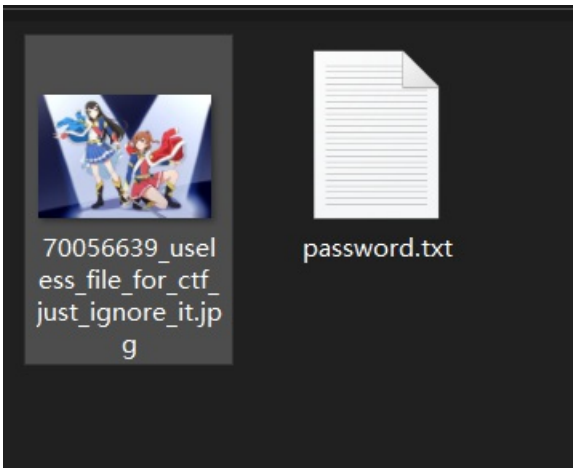
尝试挂载磁盘 但是需要密码 试了一下上面的半个flag 但是不对

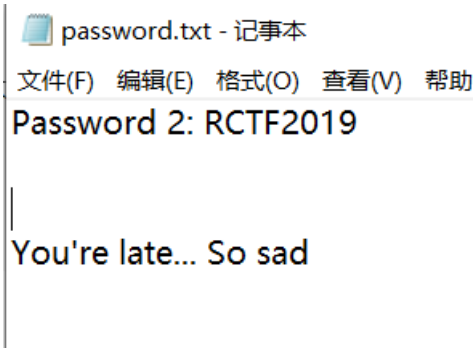
看了一下wp 这个开局给的password buu里是没用提示的。。。

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



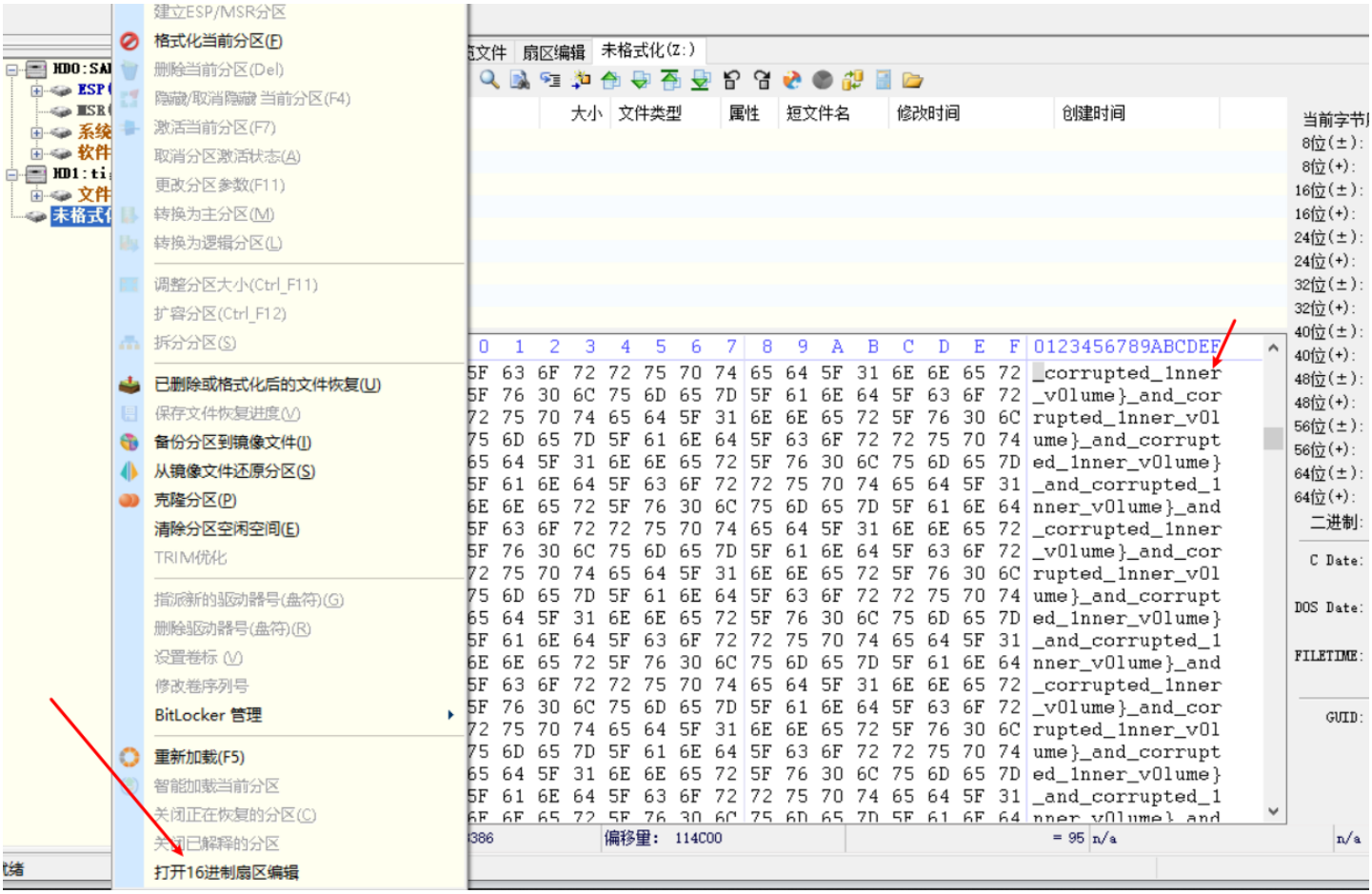


第一反应是图片里有压缩包 这个password是压缩包的密码 但是不是

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

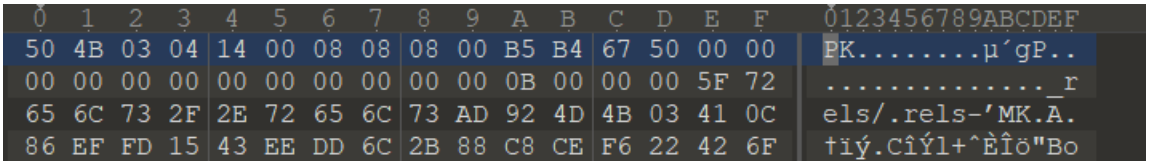
DiskGenius打开16进制编辑发现另一半flag

_and_corrupted_1nner_v0lume}



[UTCTF2020]docx 72pt

下载一个docx 010打开pk头



0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
50	4B	03	04	14	00	08	08	08	00	B5	B4	67	50	00	00	PK.....µ´gP..
00	00	00	00	00	00	00	00	00	00	0B	00	00	00	5F	72	.............._r
65	6C	73	2F	2E	72	65	6C	73	AD	92	4D	4B	03	41	0C	els/.rels-'MK.A.
86	EF	FD	15	43	EE	DD	6C	2B	88	C8	CE	F6	22	42	6F	†ïý.CîÝl+ˆÈÎö"Bo

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

找到flag

啊？72pt就这？

utflag{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

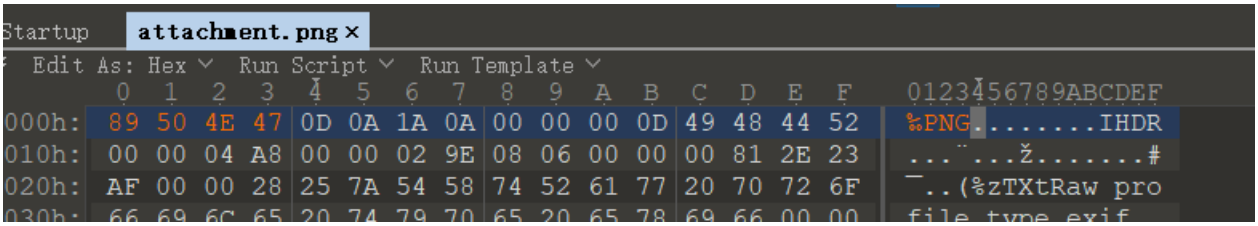
KFBVIRT3KBZGK5DUPFPVG2LTORSXEX2XNBXV6QTVPFZV6TLFL5GG6YTTORSXE7I=

base32解码

QCTF{Pretty_Sister_Who_Buys_Me_Lobster}

[UTCTF2020]file header 76pt

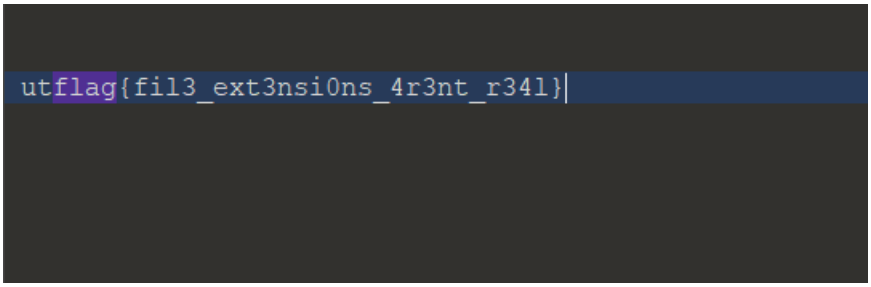
题目名为文件头 一个明显png 换上头就有flag。。啊？？这？？



utflag{3lit3_h4ck3r}

[UTCTF2020]basic-forensics 74pt

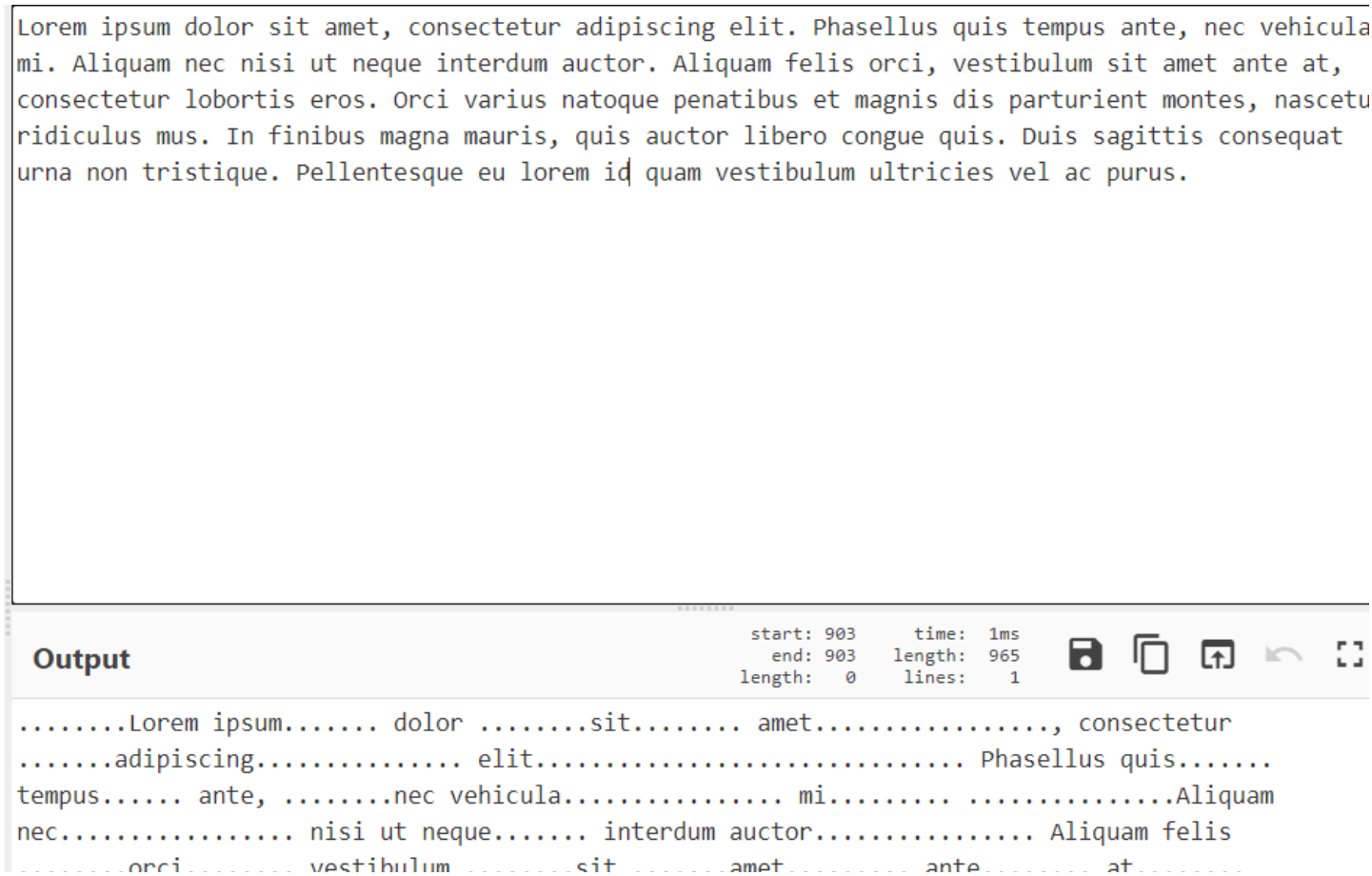
一个文本。很多东西 以为是某种方式隐藏信息。。结果一搜就出来了。。。。。。。。啊？？？这？？？



utflag{fil3_ext3nsi0ns_4r3nt_r34l}

[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



```
.....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.....
```

放vim看看

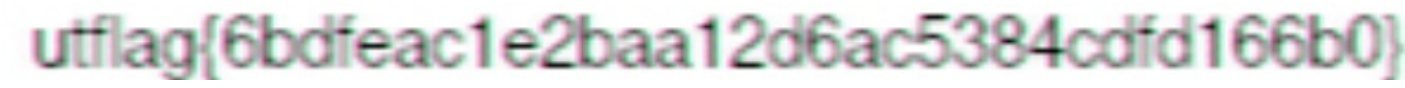
```
202c> at<200b><200b><200b><200b><200b><200b><200b>, consectetur<200c><
0c><200c><200d><200c><feff><feff> lobortis eros<200b><200b><200b><200b
200b><200b><200b><200b>.<200c><200c><200c><200c><200d><200d><200d><200
><200c><200c><200c><200d><200c><200c><200c><200b><200b><200b><200b><20
><200b>Orci varius<200b><200b><200b><200b><200b><200b><200b> <200b><20
><200b><200b><200b><200b>natoque <200c><200c><200c><200c><200d><feff><
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>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

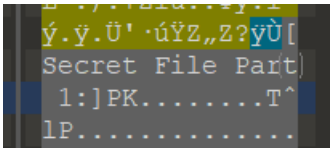
qsstv教程
http://www.srcmini.com/62326.html



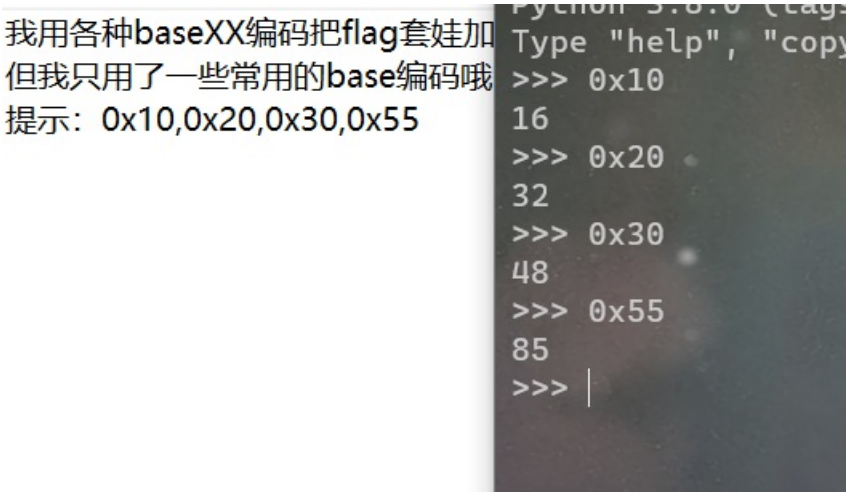
utflag{6bdfeac1e2baa12d6ac5384cdfd166b0}

[MRCTF2020]pyFlag 77pt

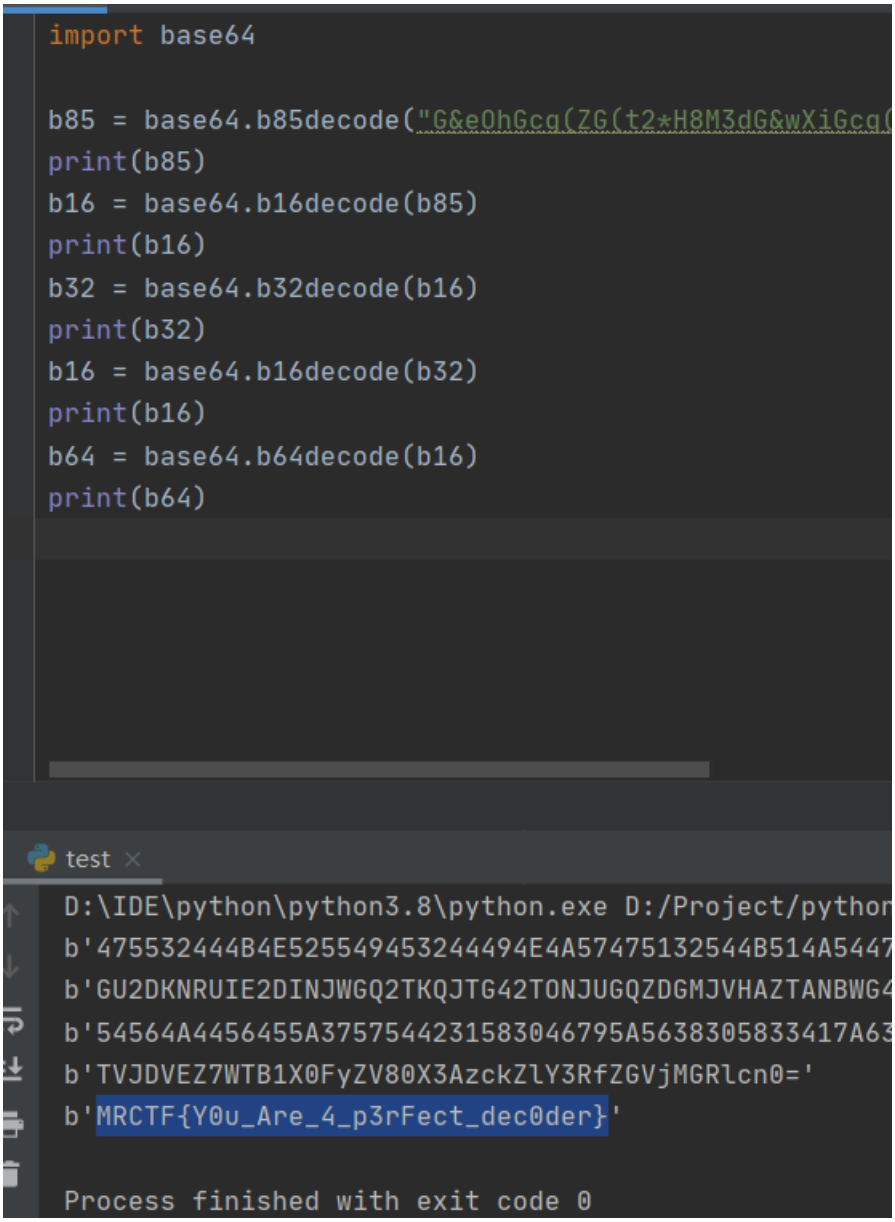
三张图片 结尾有提示part1，2，3 提取出一个zip



爆破密码 1234
打开hint 提示很明显了



没有48 32报错 16正确



greatescape 78pt

流18看到shell流量 FTPD ftp协议

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-----
MIIJQwIBADANBgkqhkiG9w0BAQEFAASCCS0wggkpAgEAAoICAQC5twyPH+2U6X0Q
uxOKPTHSR6MkXGSvAz+Ax+G9DKEiBLuTTfl7dNv4oswdmT9nWlSY1kxZatNwlUF8
WAuGLntO5xTEmOJlMtBFrWGD+DVpCE9KORGvyif8e4xxi6vh4mkW78IxV03VxHM0
mk/cq5kkERfWQW81pVeYm9UAm4dj+LcCwQ9aGd/vfTtcACqS5OGtELFbsHJuFVyn
srpp4K6tLtRk2ensSnmXUXNEjqpodfdb/wqGT86NYg7i6d/4Rqa440a6BD7RKrgp
YPaXl7pQusemHQPd248fxsuEfEwhPNDJhIb8fDX9BWv2xTfBLhGwOh7euzSh2C4o
KSuBAO+bIkL+pGY1z7DFtuJYfTOSJyQ5zQzToxS+jE+2x9/3GpD2LUD0xkA8bWhv
eecq0v6ZWBVYNX54V5ME3s2qxYc6CSQhi6Moy8xWlcSpTSAa7voNQNa9RvQ4/3KF
3gCbKtFvdd7IHvxfn8vcCrCZ37eVkq0Fl1y5UNeJU/Y0Tt8m7UDn3uKNpB841BQa
hiGayCSjsHuTS8B+MnpnzWCrzD+rAzCB37B599iBK4t/mwSIZZUZaqxTWNoFS2Lz
7m0LumZ4Yk8DpDEuWhNs8OUD8FsgAvWFVAvivaaAciF3kMs8pkmNTs2LFBowOshz
SXfONsHupgXEwwFrKOOZXNhb+O/WKQIDAQABAoICAAT6mFaZ94efft/c9BgnrddC
XmhSJczfXGt6cF3eIc/Eqra3R3H83wzaaHh+rEl8DXqPfDqFd6e0CK5pud1eD6Y8
4bynkKI/63+Ct3OPSvdG5sFJqGS7GblWIpzErtX+eOzJfr5N5eNOQfxuCqgS3acu
4iG3XWDlzuRjgSFkCgwvFdD4Fg5HVU6ZX+cGhh2sDzTRlr+rilXTMsm4K/E8udIg
yEbv5KqWEI5y+5Eh9gWY7AnGW6TgLNxzfYyt0nhYhI2+Yh4IkRqQd6F8XQARbEhP
yZx1eK4Q/dRPQxOJNY1KkRpl+Cx6tAPVimByRx1hu82qsTstb6rLHemruOPbf5Dw
aqgSFdp7it3uqjJHCwJ2hAZoijAcvlhn1sa1hr/qFFlY/WeDAi8OyvGdCSh3OvS6
yazkah85GOnY85rz+s98F9cvIqcRdGJrAeNbUHHnj6+X9qFVtwDpF0V1vlvn2Ggp
7m8hiZ0Y+8T+7qfnS9WsdPh7MkoIEoZ0CPryYvX+YPLYWqzxtCvrRWF8tAScI6H+
XBz3NlCAUaOk+ZOkKlZ8ZYMSn/g5EV2jj/mwZVdtYoeQjLaCDuLq8E1Hswnpgq7F
54hHU7vOeJ1/TQltLCNfJFQRaUD+tPz9R6jVpbqBiXxIC2eiGTo1rP4Ii7hsQRFC
W0KKqu+bV69HJAmi06yBAoIBAQDvz+c+3z9njQFFaeUUqyzl31HOzRHmWhJEoriR
nRhWTLzqMyn+RLGrD3DJQj/dGH6tyxHJ7PdI7gtJ3qaF4lCc2dKR3uQW3CBKI9Ys
```

编辑->首选项->protocols->TLS 把刚才的key导入

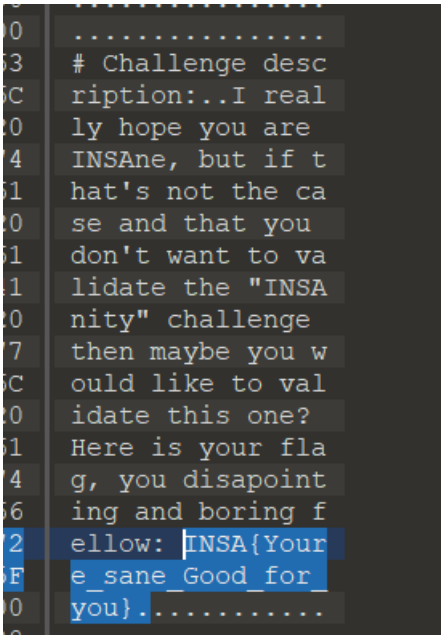
流80追踪http可以找到flag

[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。。。



结果看了一个md md里就是这个flag 我服了。。。

[INSHack2019]INSAnity 82pt

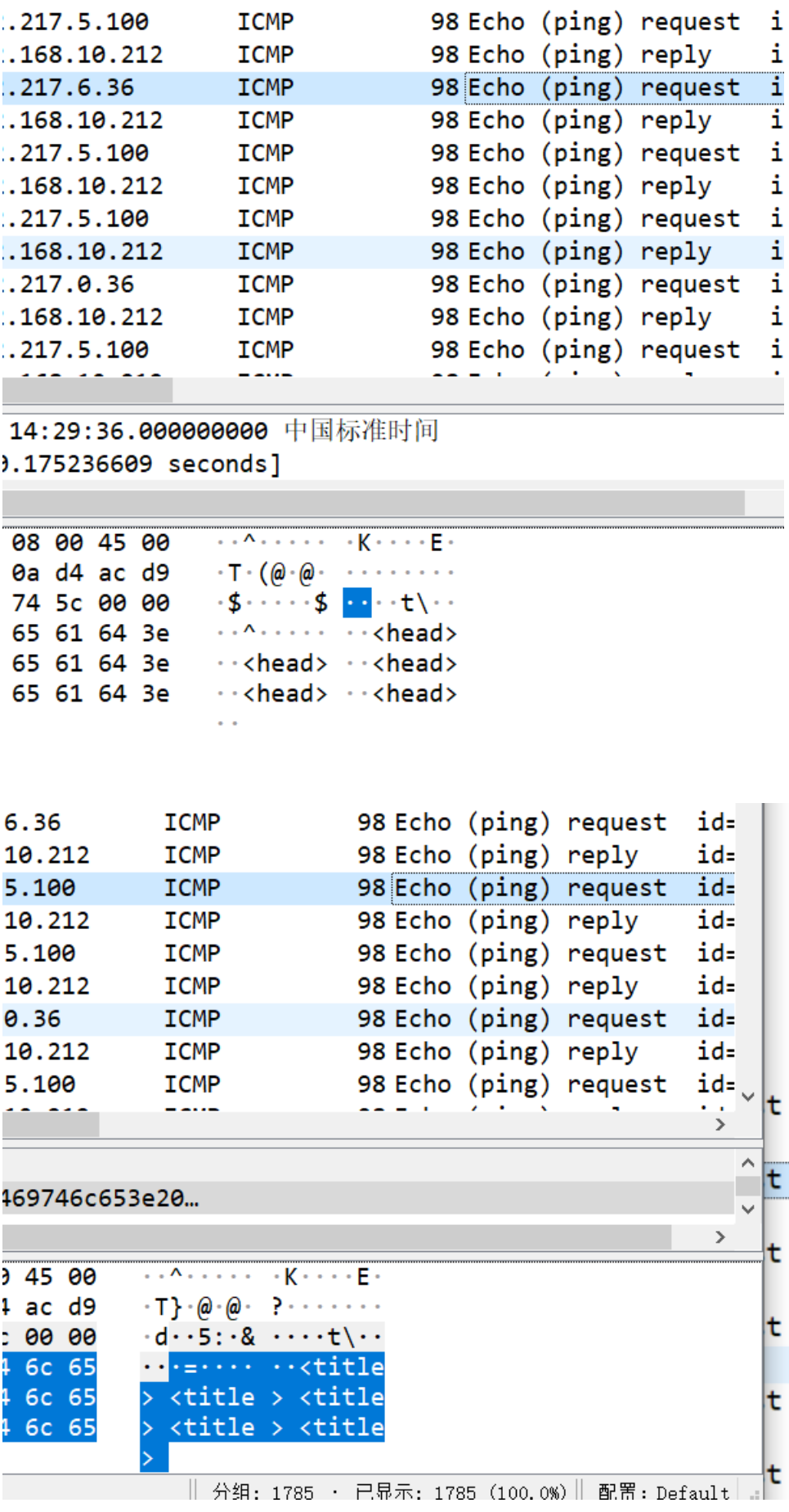
???跟上面一模一样的。。。这不是直接白给吗
好像2018 2017 2019都有两题送分的 就不写了。。。

[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



```
d4 ac d9    ·T·v@·@· ········
5c 00 00    ·$··r·0· ····t\··
5d 65 6e    ········ ··ocumen
5d 65 6e    t.ocumen t.ocumen
5d 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]spectogram 86pt

英文名翻译一下是频谱图 托audacity秒出

flag{sp3tr0gr4m0ph0n3}

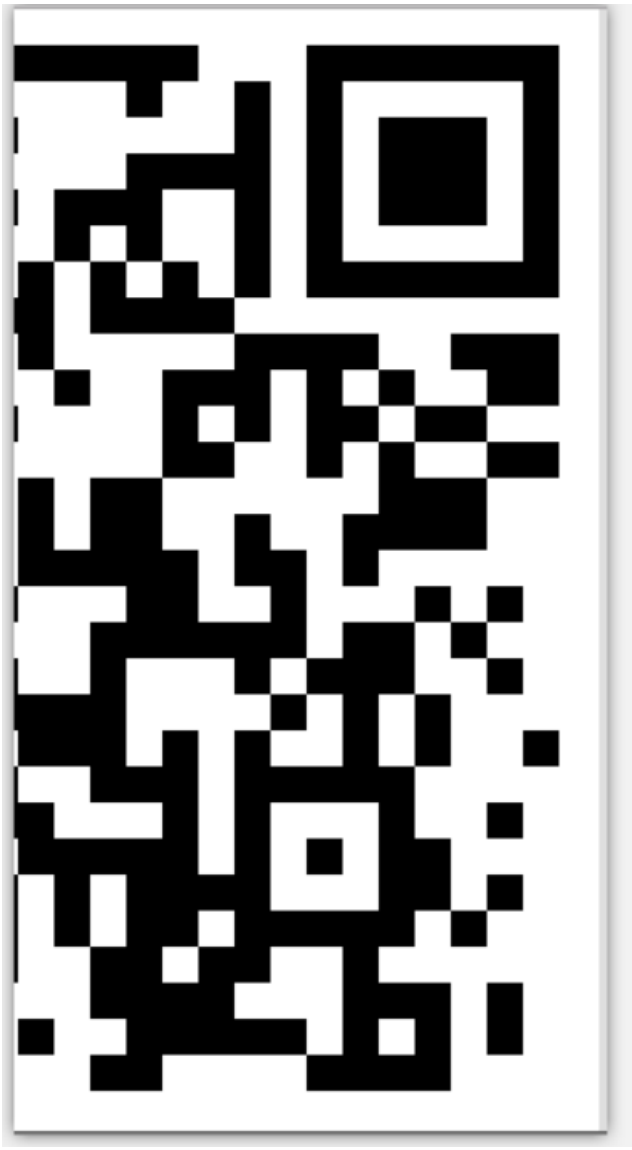
[INSHack2018]Self Congratulation 85pt

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}

很好的色彩呃？ 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}