【ZJNU】Misc集训

原创

sheepbotany 于 2022-04-25 15:47:29 发布 51 收藏

文章标签： misc ctf zjnu misc基础

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/lllwky/article/details/124397160

版权

文章目录

来做几道Misc题吧

图片隐写

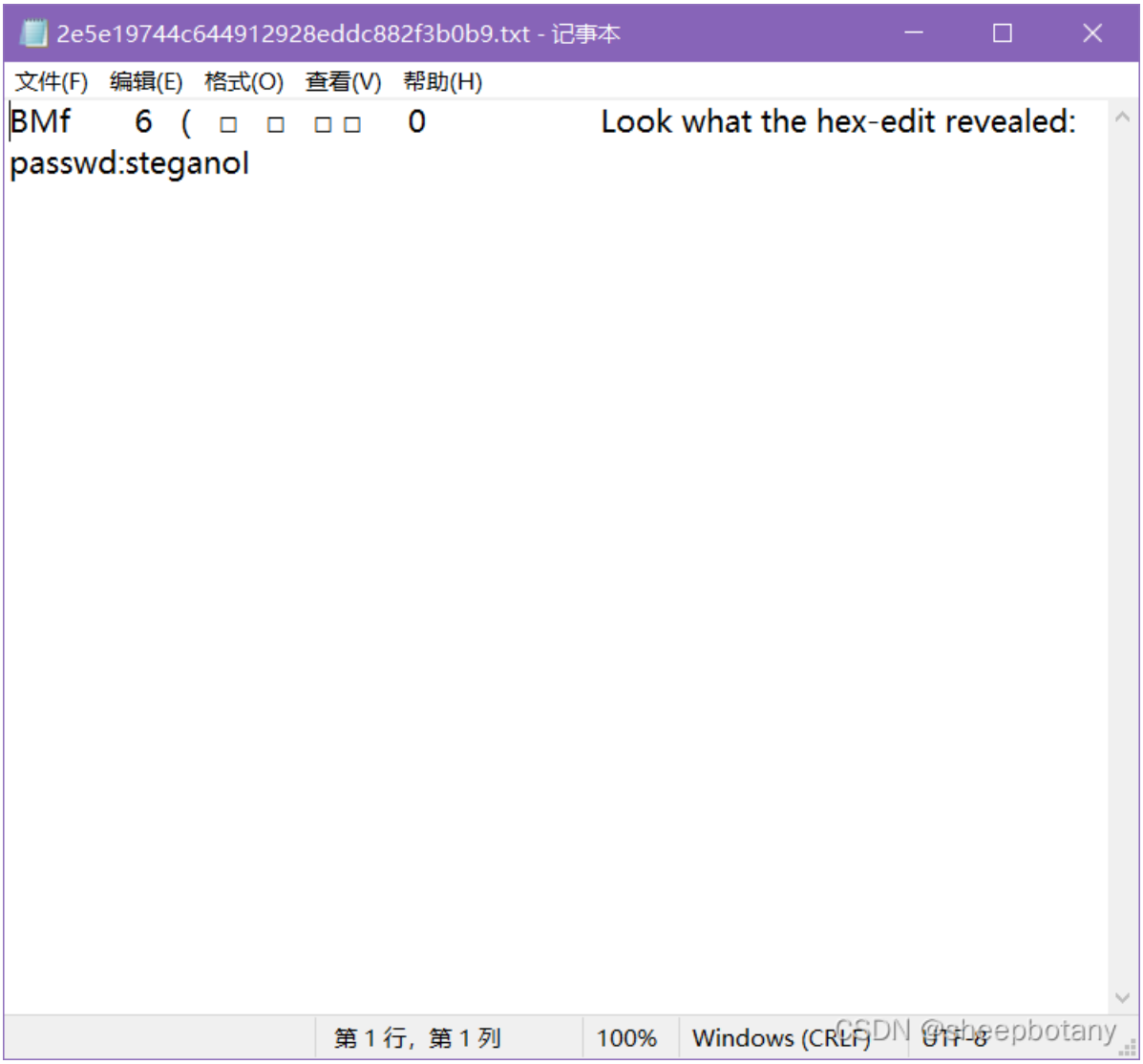
JPEG (jpg),	文件头：FFD8FF	文件尾：FF D9
PNG (png),	文件头：89504E47	文件尾：AE 42 60 82
GIF (gif),	文件头：47494638	文件尾：00 3B
ZIP Archive (zip),	文件头：504B0304	文件尾：50 4B
TIFF (tif),	文件头：49492A00	文件尾：
Windows Bitmap (bmp),	文件头：424D	文件尾：
CAD (dwg),	文件头：41433130	文件尾：
Adobe Photoshop (psd),	文件头：38425053	文件尾：
Rich Text Format (rtf),	文件头：7B5C727466	文件尾：
XML (xml),	文件头：3C3F786D6C	文件尾：
HTML (html),	文件头：68746D6C3E	
Email [thorough only] (eml),	文件头：44656C69766572792D646174653A	
Outlook Express (dbx),	文件头：CFAD12FEC5FD746F	
Outlook (pst),	文件头：2142444E	
MS Word/Excel (xls.or.doc),	文件头：D0CF11E0	
MS Access (mdb),	文件头：5374616E64617264204A	
WordPerfect (wpd),	文件头：FF575043	
Adobe Acrobat (pdf),	文件头：255044462D312E	
Quicken (qdf),	文件头：AC9EBD8F	
Windows Password (pwl),	文件头：E3828596	
RAR Archive (rar),	文件头：52617221	
Wave (wav),	文件头：57415645	
AVI (avi),	文件头：41564920	
Real Audio (ram),	文件头：2E7261FD	
Real Media (rm),	文件头：2E524D46	
MPEG (mpg),	文件头：000001BA	
MPEG (mpg),	文件头：000001B3	
Quicktime (mov),	文件头：6D6F6F76	
Windows Media (asf),	文件头：3026B2758E66CF11	
MIDI (mid),	文件头：4D546864	

CSDN @sheepbotany

1：【XCTF】Training-Stegano-1

打开来看是这样的

而且是bmp结尾的，我们改为txt结尾好了

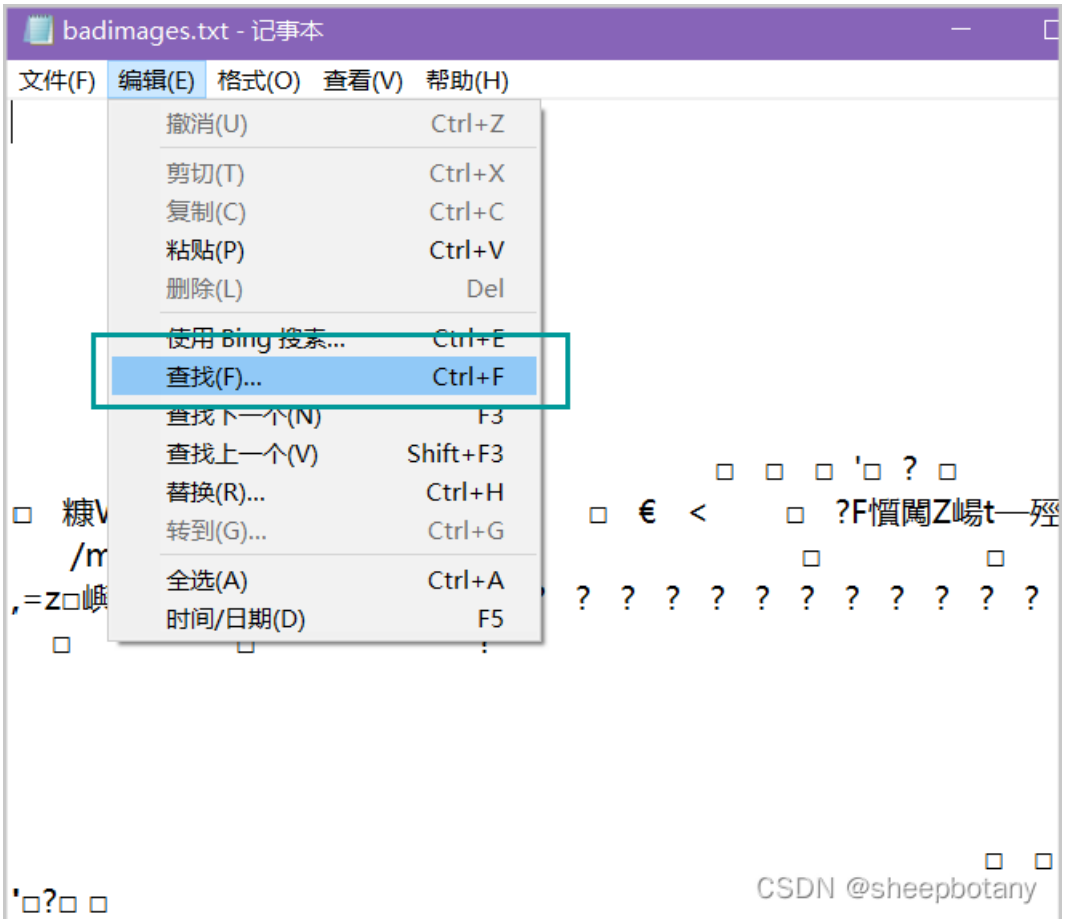


flag就是steganol

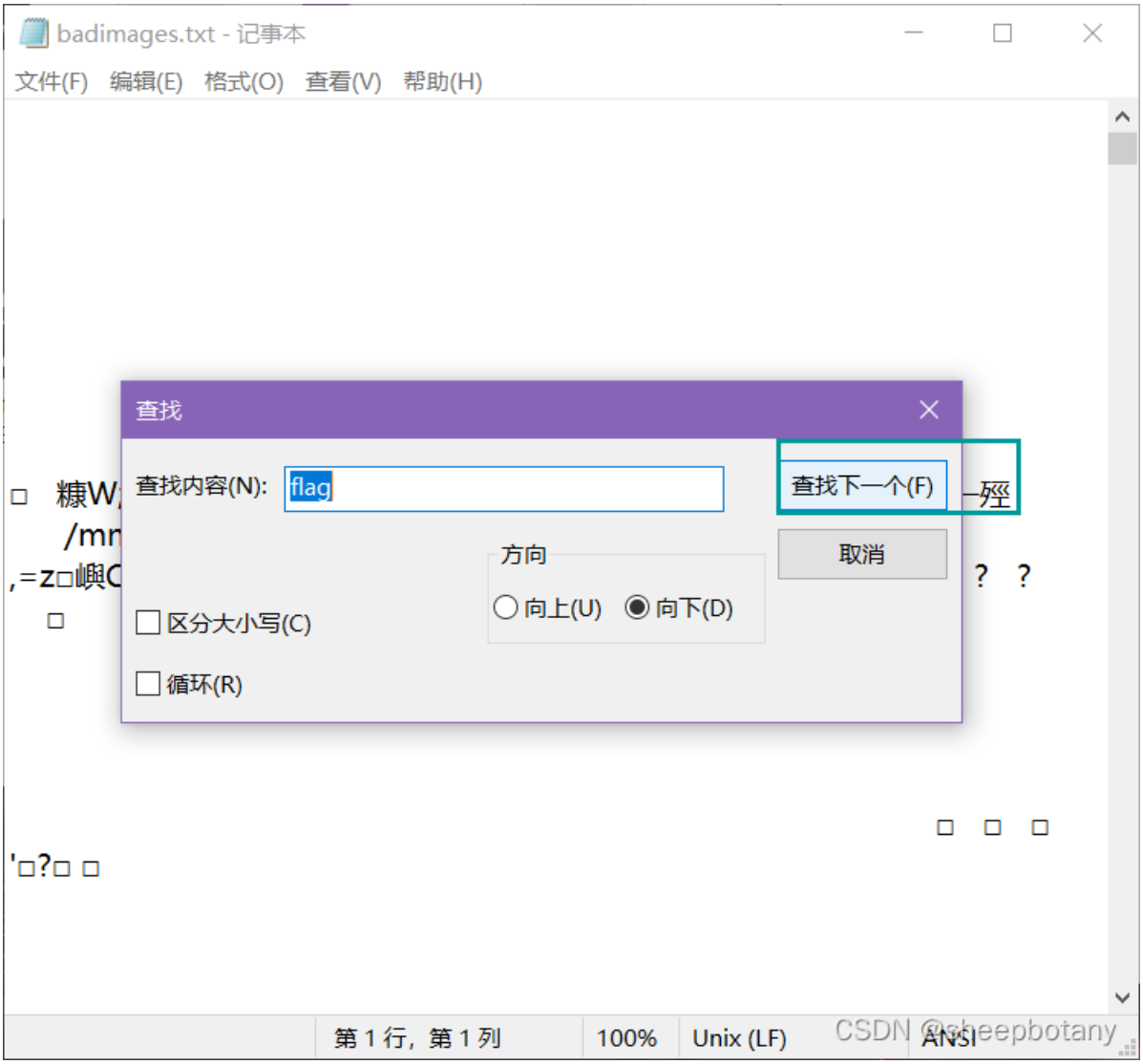
2：【XCTF】Something-in-image

打开来看是一个叫bigimages的文件，但是没有后缀

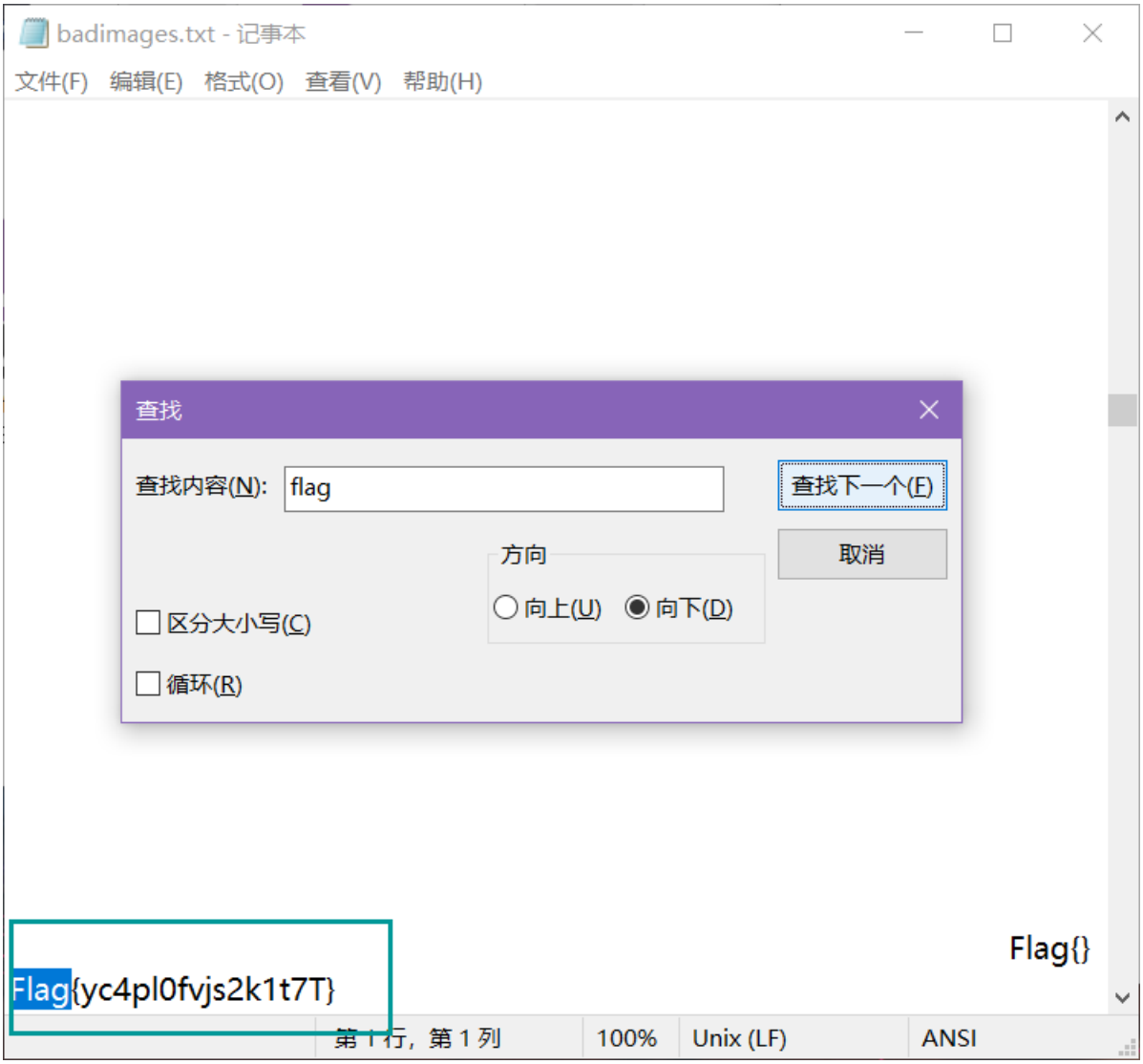
我们还是把后缀改为txt


badimages.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
撤消(U) Ctrl+Z
剪切(T) Ctrl+X
复制(C) Ctrl+C
粘贴(P) Ctrl+V
删除(L) Del
使用 Bing 搜索... Ctrl+E
查找(F)... Ctrl+F
查找下一个(N) F3
查找上一个(V) Shift+F3
替换(R)... Ctrl+H
转到(G)... Ctrl+G
全选(A) Ctrl+A
时间/日期(D) F5
CSDN @sheepbotany

查找flag

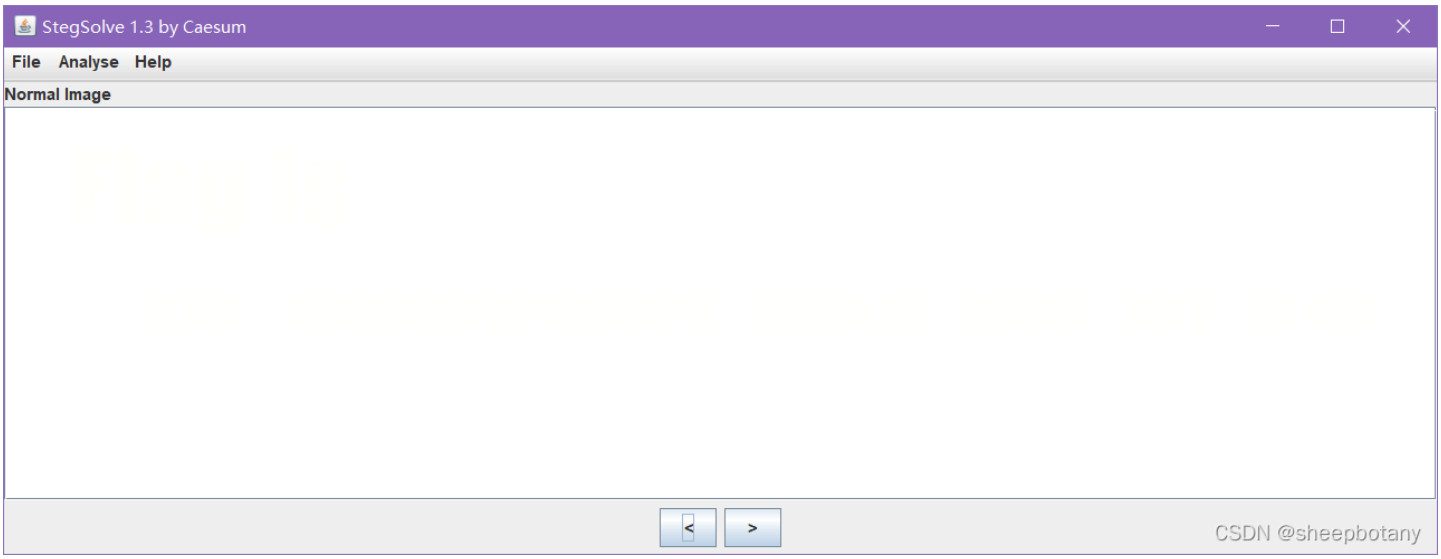


CSDN @sheepbotany



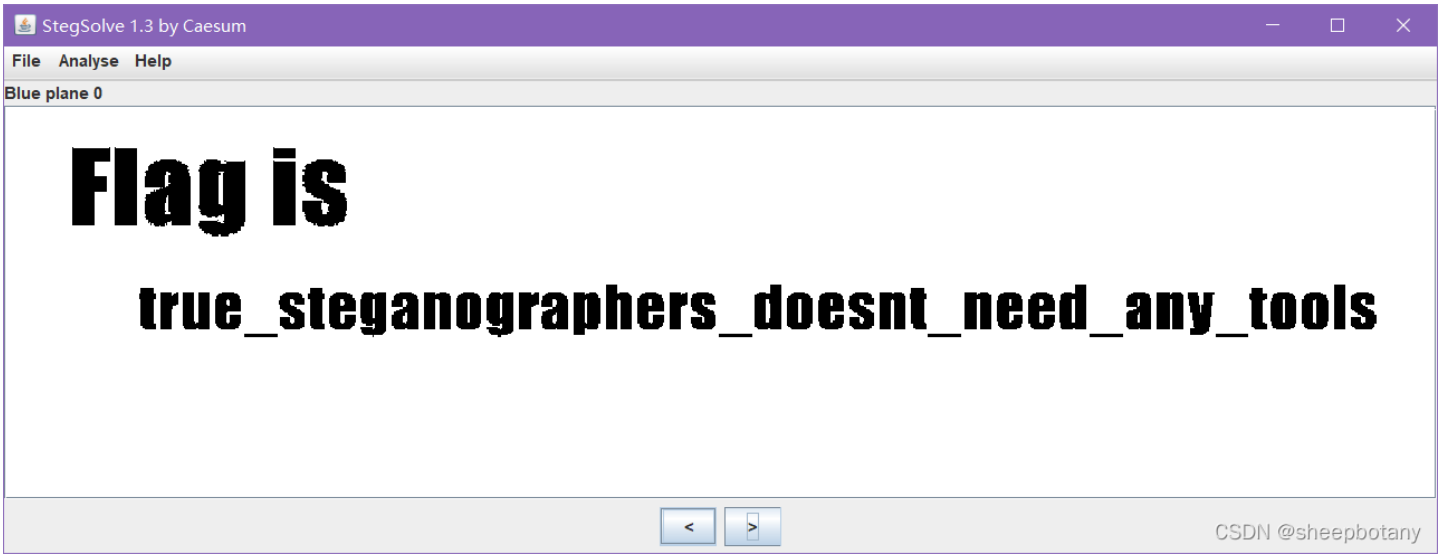
3：【XCTF】pure_color

打开来看是一张图片，我们用stegsolve打开



往左右翻可以查看关闭不同颜色后图片的变化

最终翻到：



4：【XCTF】a_good_idea

打开来看

不知道用010Editor可以看出什么，使用foremost分离一下吧

得到一个zip包里有两张图片

还有一个txt文件写着

try to find the secret of pixels

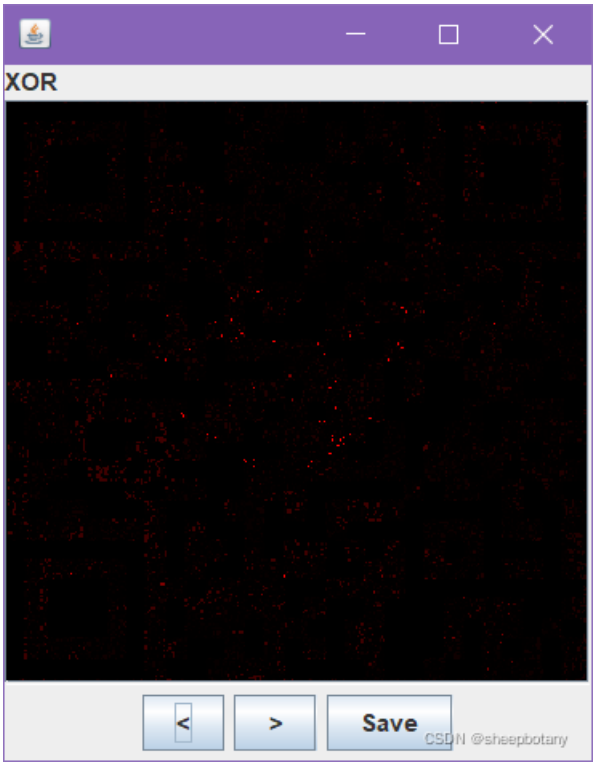
我们将两张图片合成

先用stegSolve打开其中一张图片

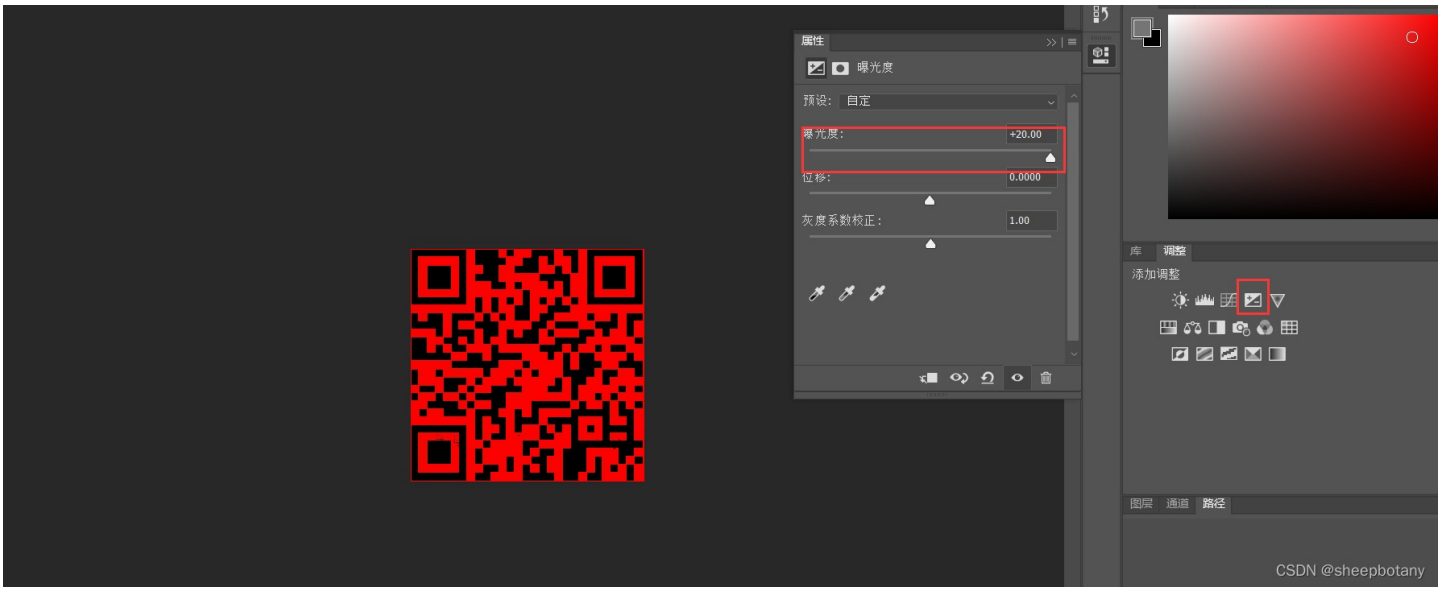

StegSolve 1.3 by C...
File
Analyse
Help
Normal Image
我有一个很大胆的想法
<
>
CSDN @sheepbotany


StegSolve 1.3 by C...
File
Analyse
Help
File Format
Data Extract
Stereogram Solver
Frame Browser
Image Combiner
我有一个很大胆的想法
<
>
CSDN @sheepbotany

合成后保存，记住保存为png文件



使用ps打开图片，调节曝光度



使用PSQREdit进行扫码

NCTF{m1sc_1s_very_funny!!!}

5：【XCTF】Erik-Baleog-and-Olaf

打开发现是stego100

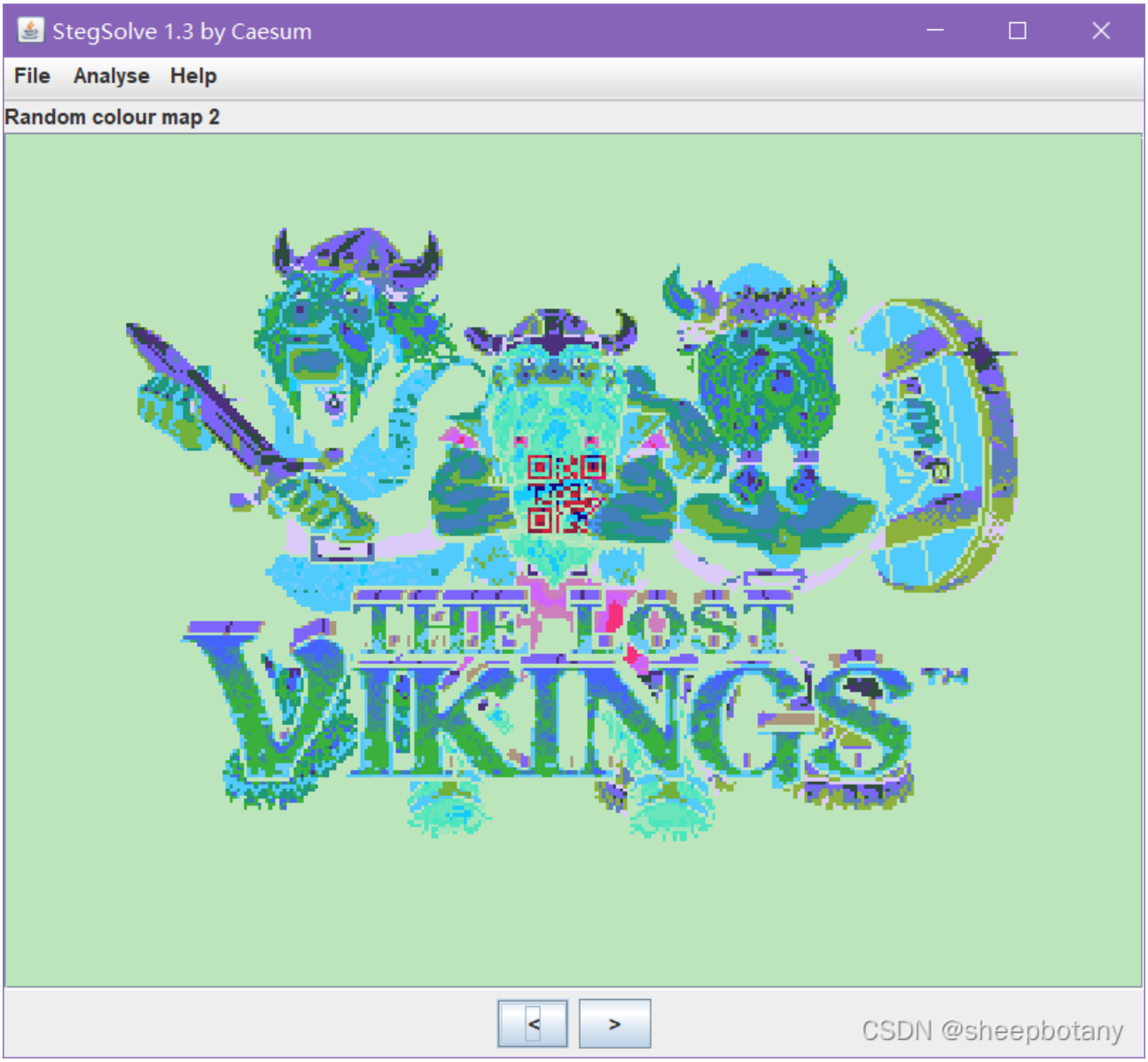
我们用010Editor打开

```
6860h: 84 10 42 08 21 84 10 42 08 21 84 10 42 08 21 84  „.B.!„.B.!„.B.!„
6870h: 10 42 08 21 84 10 42 08 21 84 10 42 08 21 84 10  .B.!„.B.!„.B.!„.
6880h: 42 08 21 84 10 42 08 21 84 10 42 08 21 84 10 42  B.!„.B.!„.B.!„.B
6890h: 08 21 84 10 42 08 21 84 10 42 08 21 84 10 42 08  .!„.B.!„.B.!„.B.
68A0h: 21 C4 BB E7 FF 07 13 EC 56 32 A2 FF D8 6C 00 00  !Ä»çÿ..ìV2¢ÿØl..
68B0h: 00 23 74 45 58 74 68 69 6E 74 00 68 74 74 70 3A  .#tEXthint.http:
68C0h: 2F 2F 69 2E 69 6D 67 75 72 2E 63 6F 6D 2F 32 32  //i.imgur.com/22
68D0h: 6B 55 72 7A 6D 2E 70 6E 67 0E AF FD 3E 00 00 00  kUrzm.png.¯ý>...
68E0h: 00 49 45 4E 44 AE 42 60 82                       .IEND®B`‚
```

CSDN @sheepbotany

告诉我们有一张png图片，修改后缀为png

调试后发现有个二维码

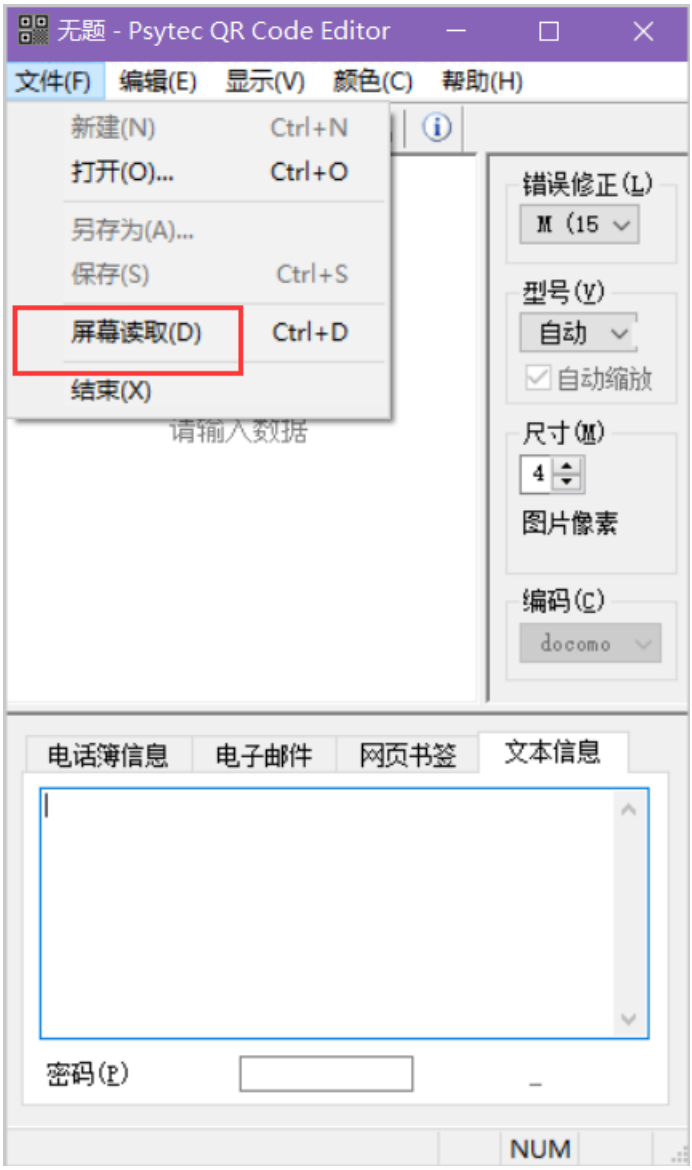


截图保存

使用photoshop改变颜色并补全

但是最后仍然扫不出来，我试过网上所有版本的二维码，没有一个扫得出来，只能说不可思议。

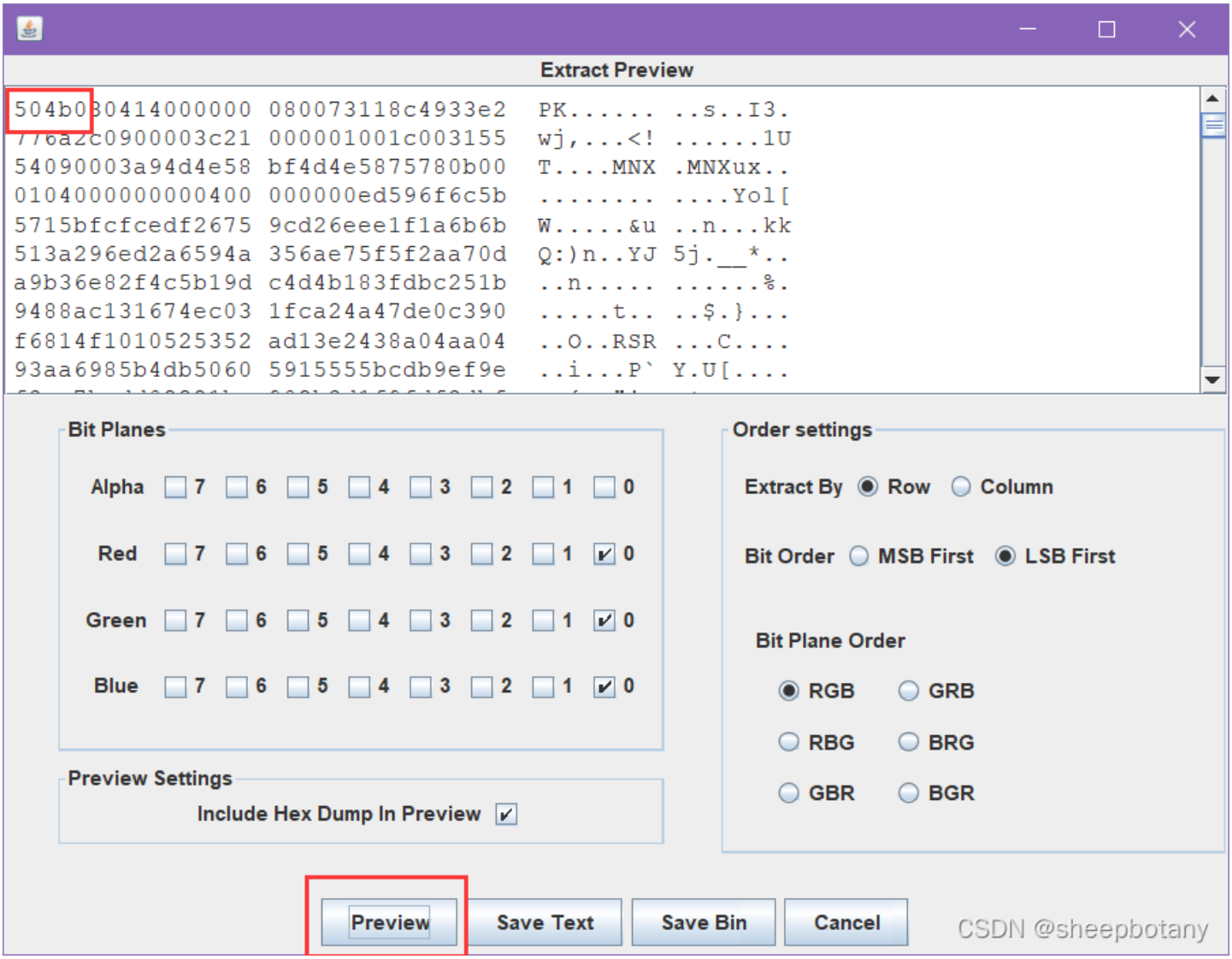
使用PsQREdit读取



扫不出来，即使使用QRResearch

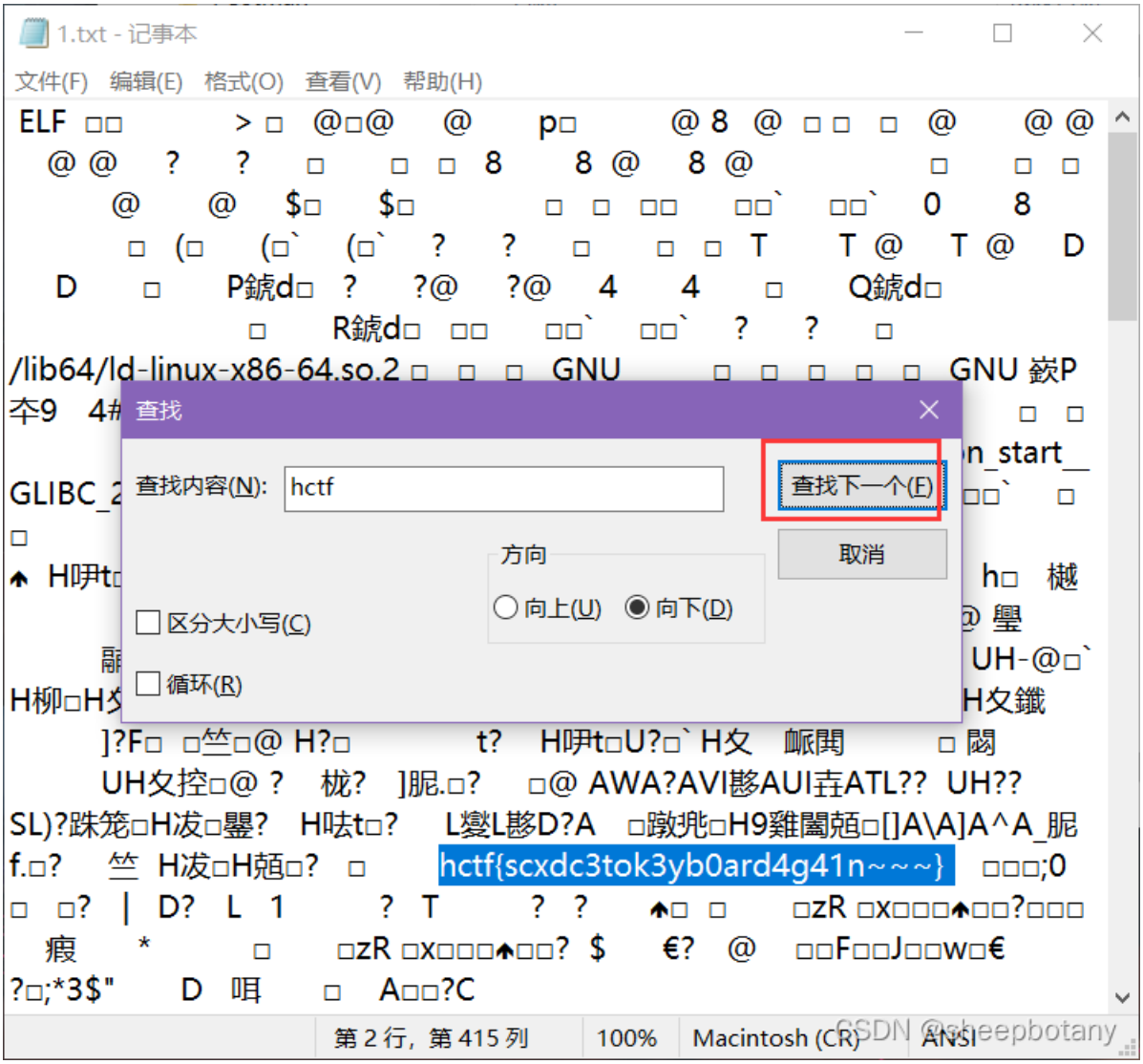
6：【XCTF】misc_pic_again

打开来看是一张图片，扔到stegolve



代表有一个zip 选择save Bin，保存为1.zip

打开后发现是elf文件，修改其后缀为.txt,根据题目描述，查找题目描述：flag = `hctf{[a-zA-Z0-9~]*}`



所以flag为：hctf{scxdc3tok3yb0ard4g41n~~~}

7：【XCTF】normal_png

打开发现是png图片

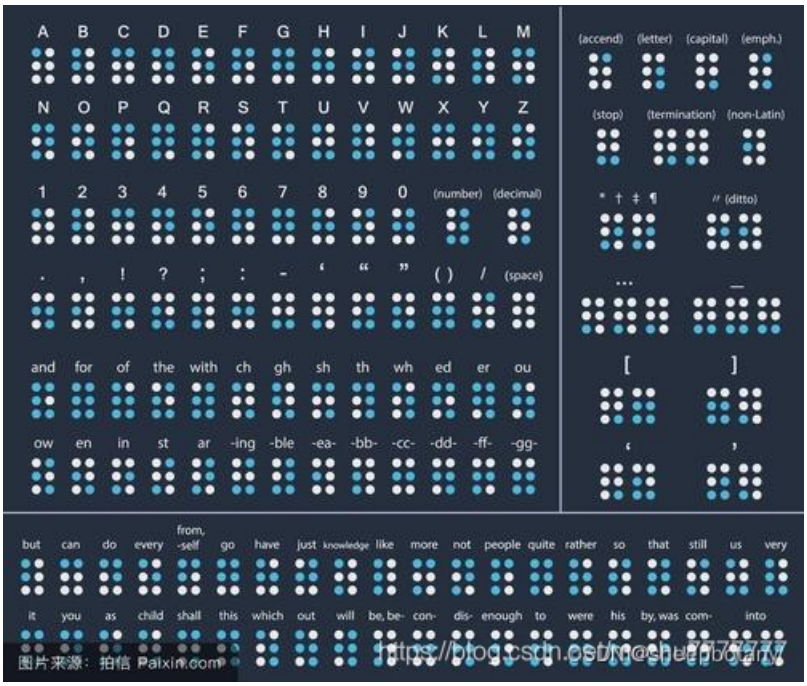
有印象，是高度问题，所以修改高度，丢到010Editor里

flag{B8B68DD7007B1E406F3DF624440D31E0}

音频隐写

8：【BUUCTF】假如给我三天光明

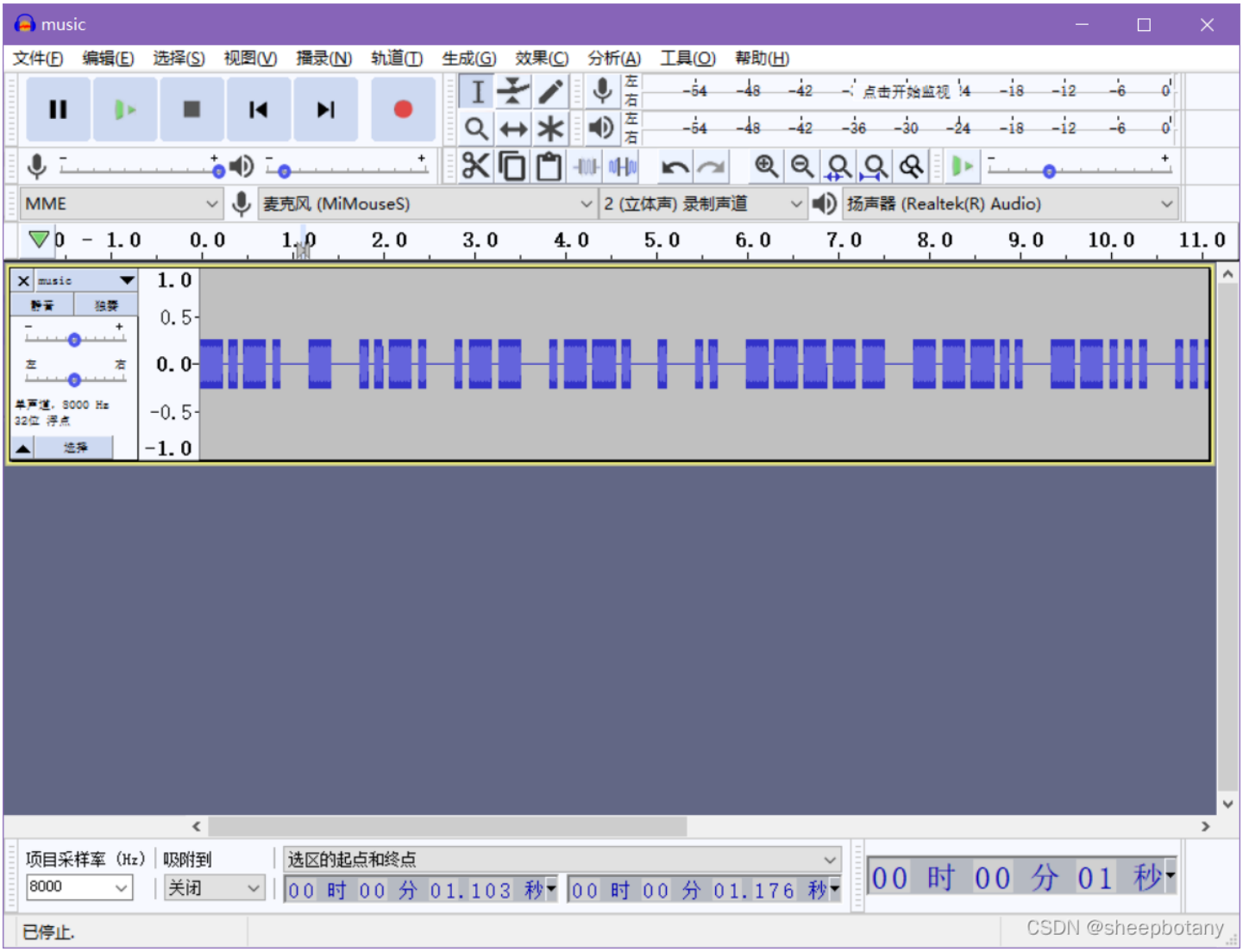
打开来看是一张图片，用到crypto中的解密知识



kmdonowg

在输入密码对zip包进行解压得到一段音频

使用audacity打开



当作摩斯密码，长的为- 短的为.

手动解密

-.-. - …-. .-- .-. . … ----- —… --… …-- …— …–… …— …-- -… --…

CTFWPEI08732?23DZ

要转换为小写

ctfwpei08732?23dz

习惯去掉ctf后包上flag

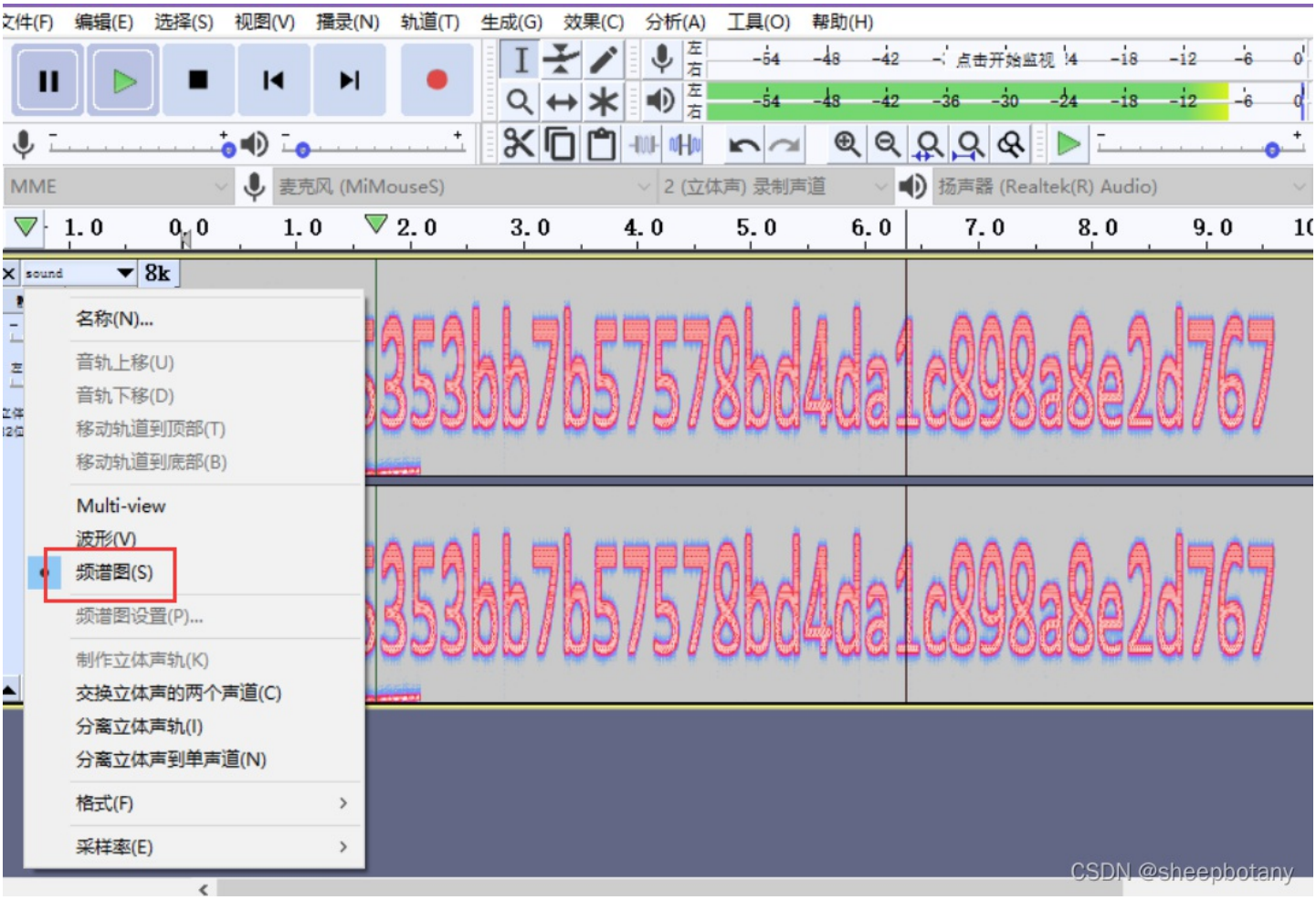
flag{wpei08732?23dz}

频谱隐写

9：【XCTF】Hear-with-your-Eyes

打开看是一段音频，拖到audacity中：

打开波频图可以看到flag



e5353bb7b57578bd4da1c898a8e2d767

LSB音频隐写

10：【攻防世界】funny_video

下载出来是一段视频，视频中提示音频有问题，我们使用MKVToolnixPortable进行分离，或者在线网站：MKV轉MP3轉換器。在线自由 — Convertio

进行分离，拖进Audacity得到的结果都是

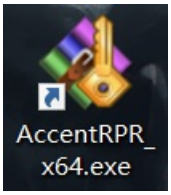
在这里插入图片描述

看不清楚，不知道是怎么得出最后的falg的

flag{fun_v1d30_mu51c}

11：【BUUCTF】基础破解

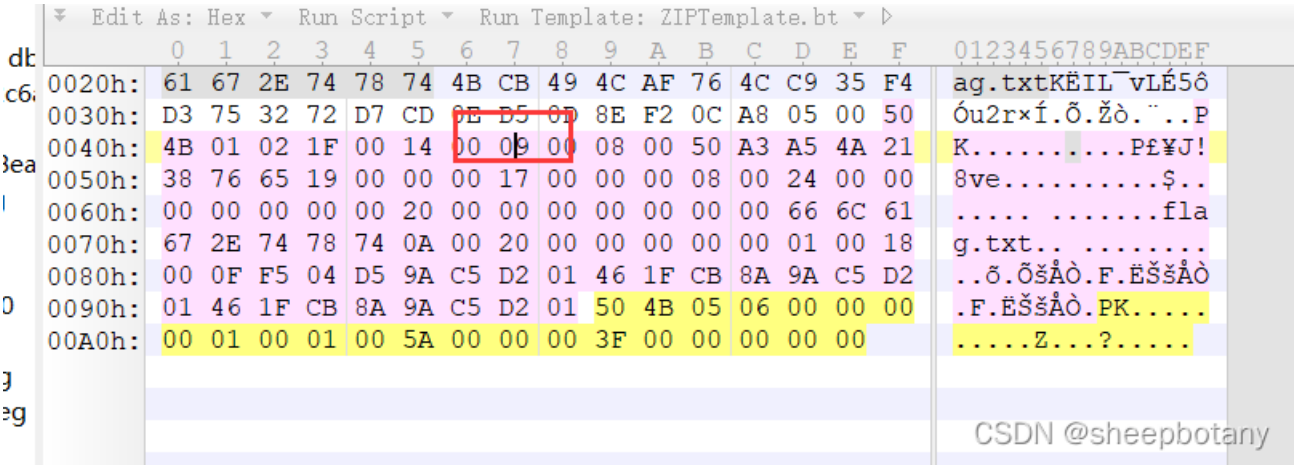
这题写过，直接上工具：



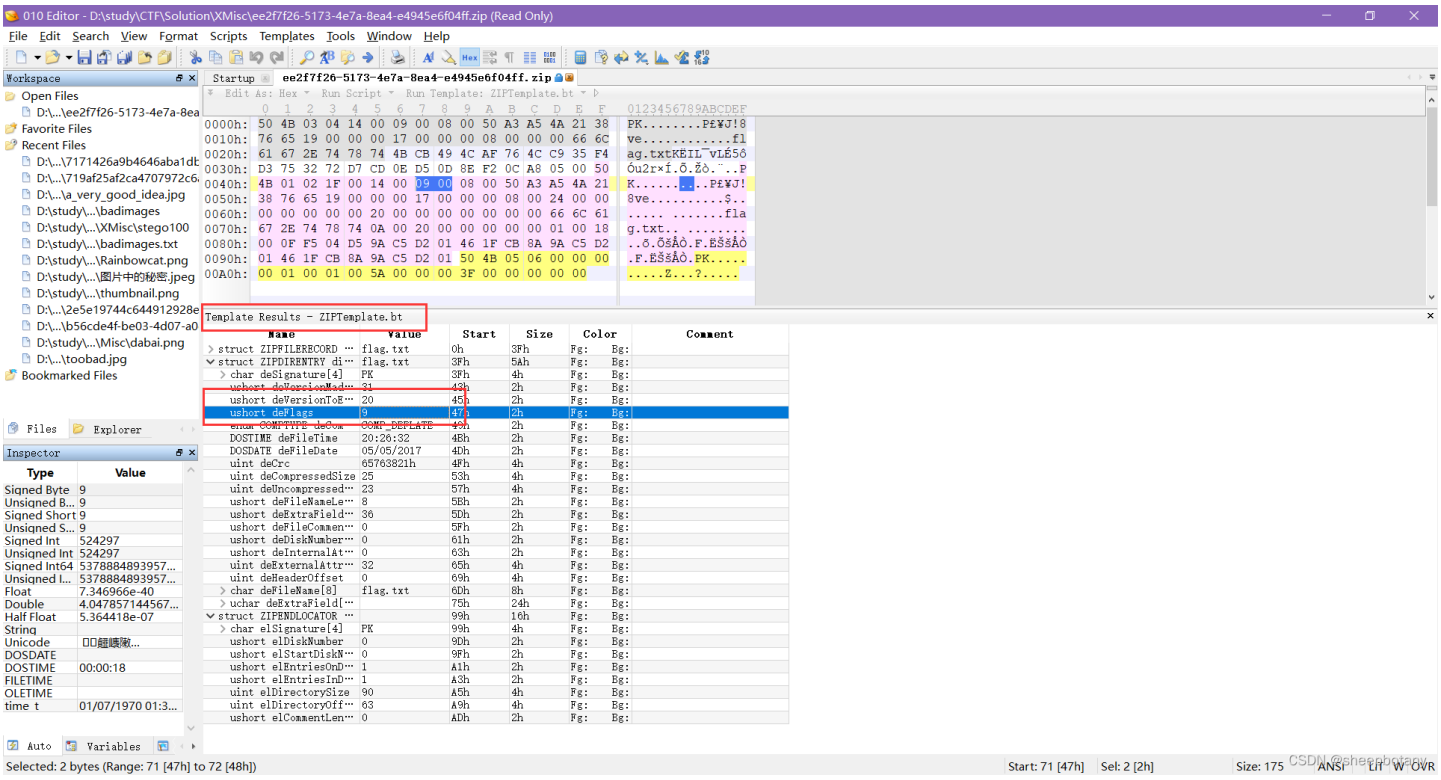
zip伪加密

12. 【BUUCTF】zip伪加密

此题无法直接爆破，拖到010Editor中

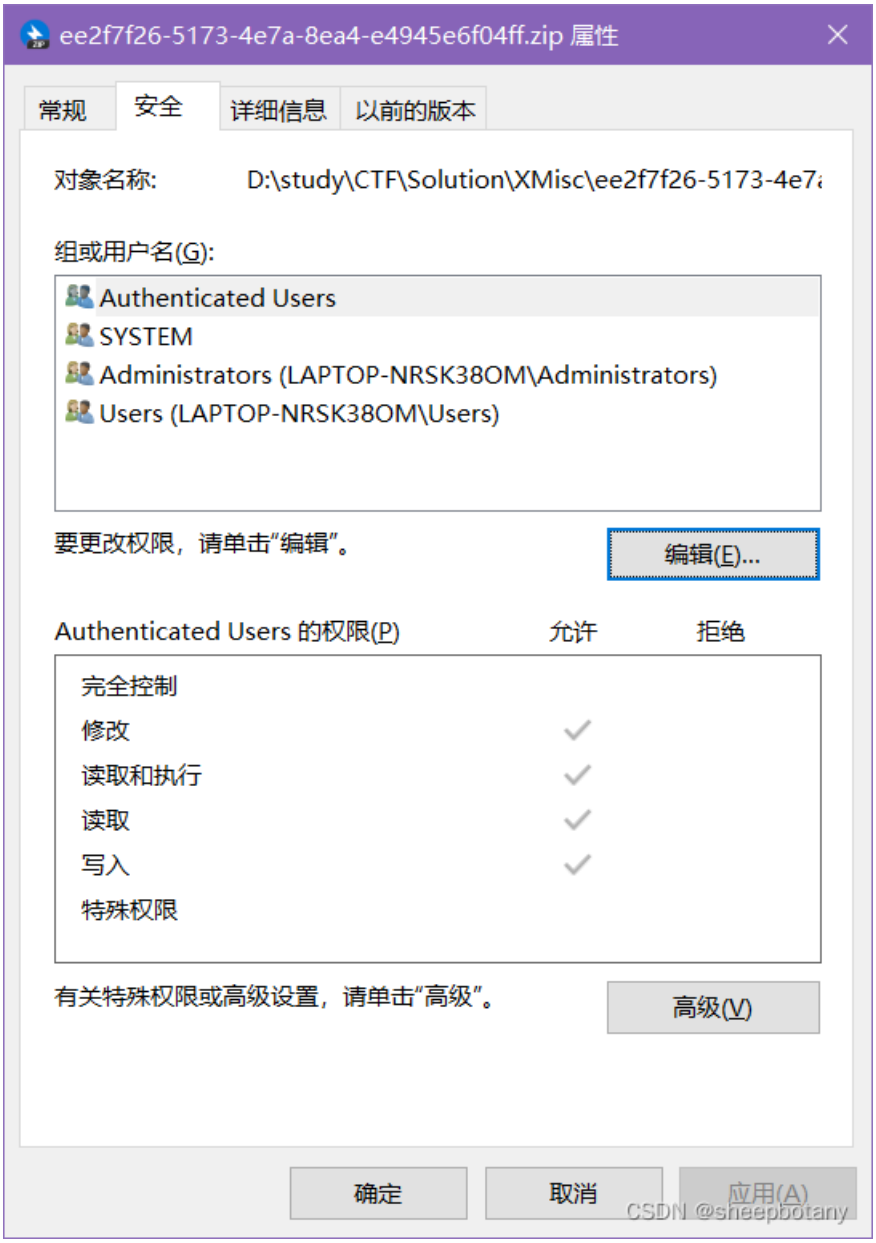


无法直接修改，打开下方的struct

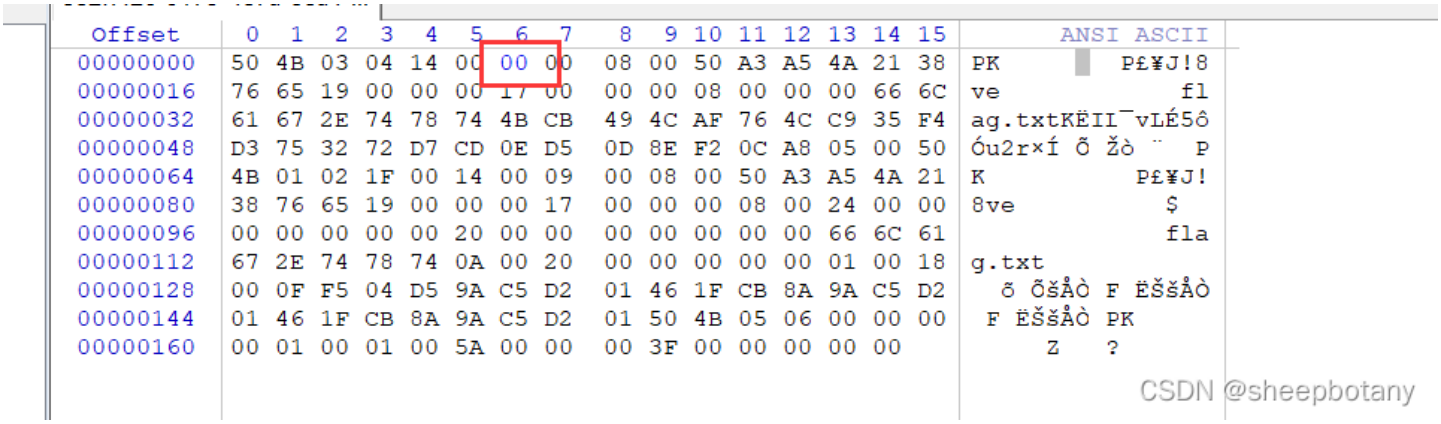


将9改为0即可。

发现只能读取无法修改，于是点击属性更改权限



然后按上述修改即可得到flag



法二：使用binwalk解压

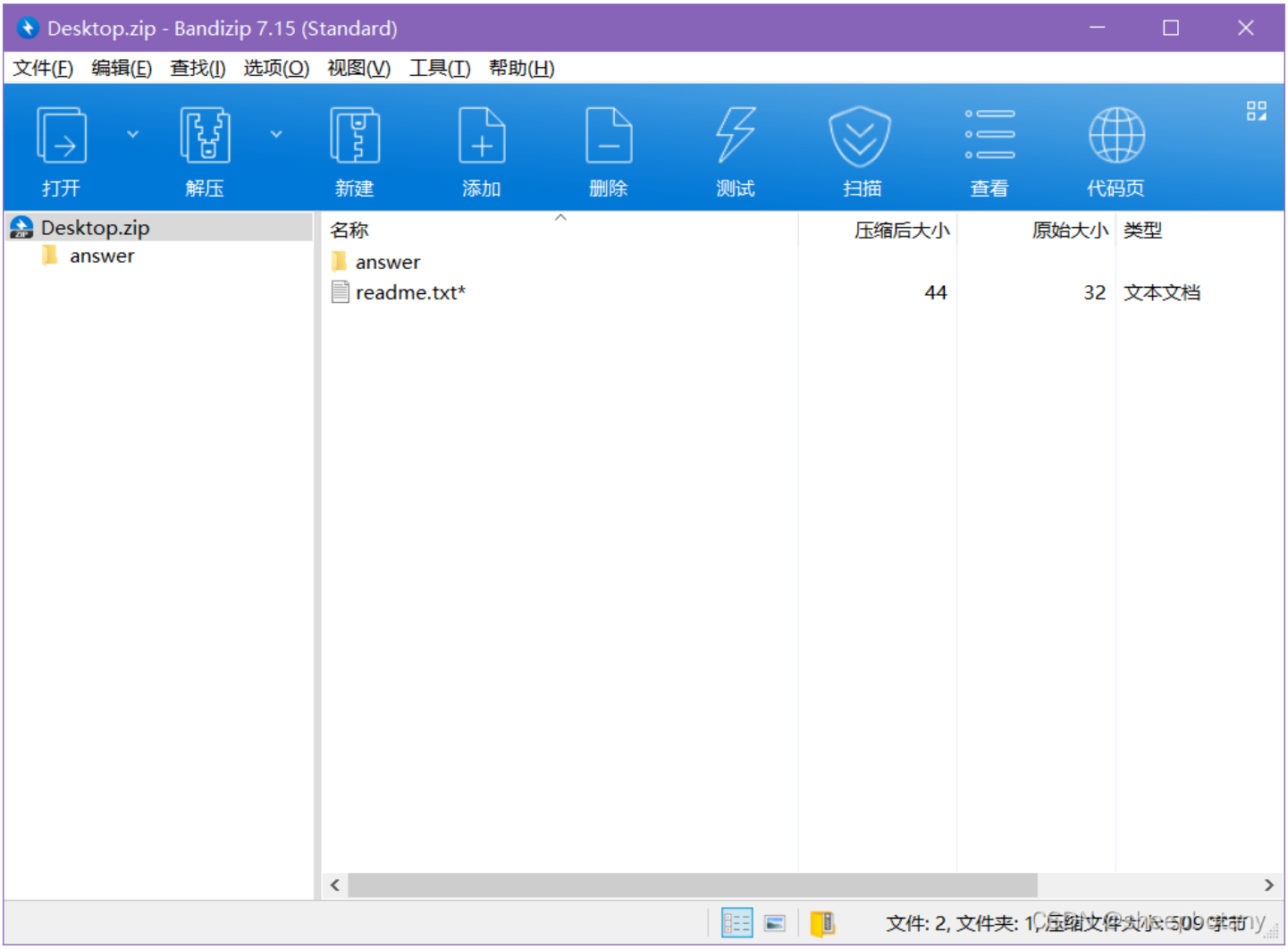
```
root@ubuntu:/home/bi0x/BuuCtf/misc# binwalk -e 1.zip

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v2.0 to extract, compre
ssed size: 25, uncompressed size: 23, name: flag.txt
153           0x99            End of Zip archive, footer length: 22

root@ubuntu:/home/bi0x/BuuCtf/misc#
```

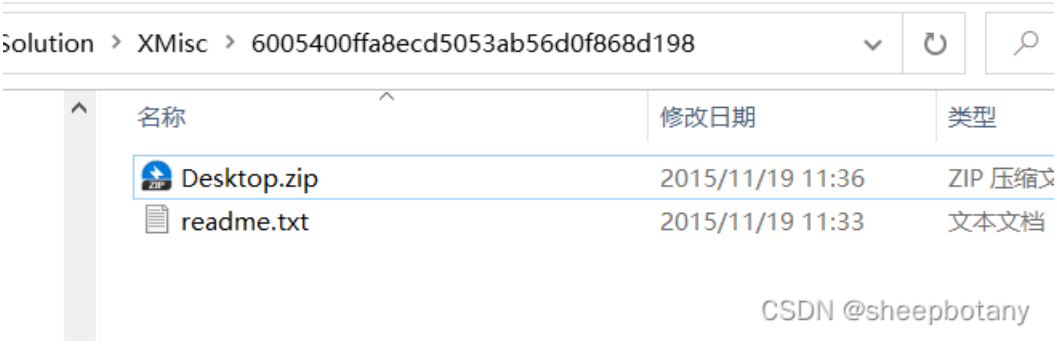
明文攻击

13：广州强网杯：爆破？

https://static2.ichunqiu.com/icq/resources/ctf/qwb/6005400ffa8ecd5053ab56d0f868d198.zip

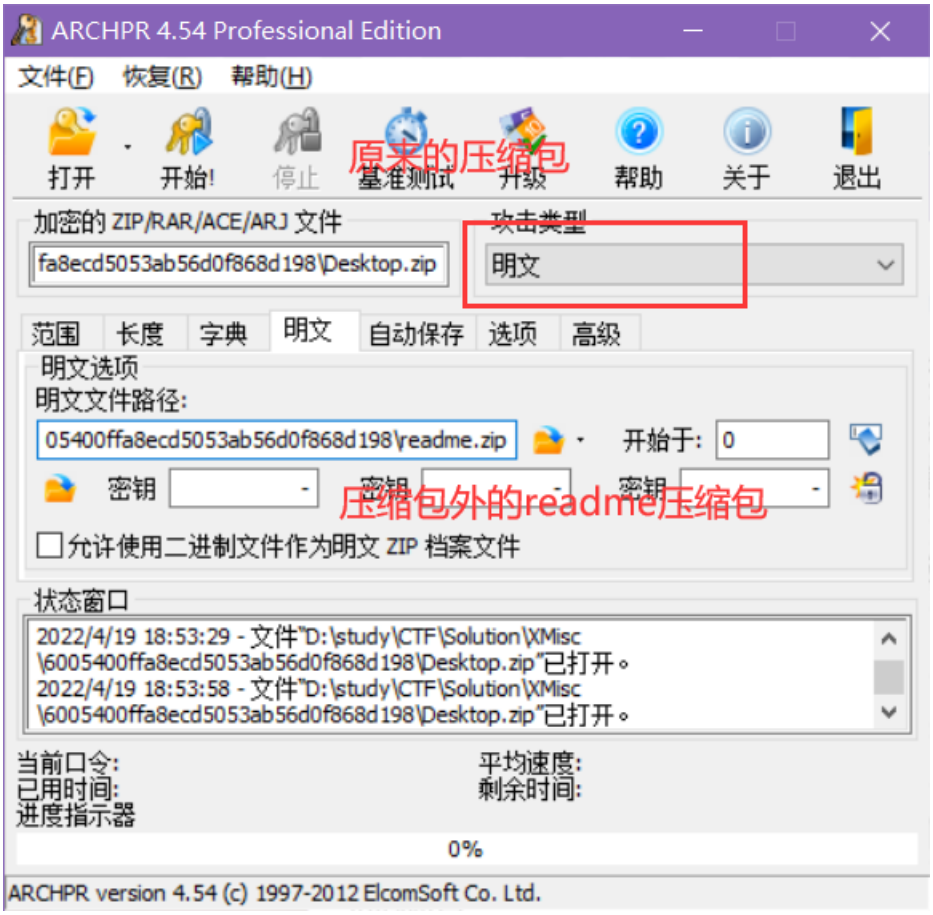
解压后有两个文件，一个是readme，另一个是压缩包Desktop





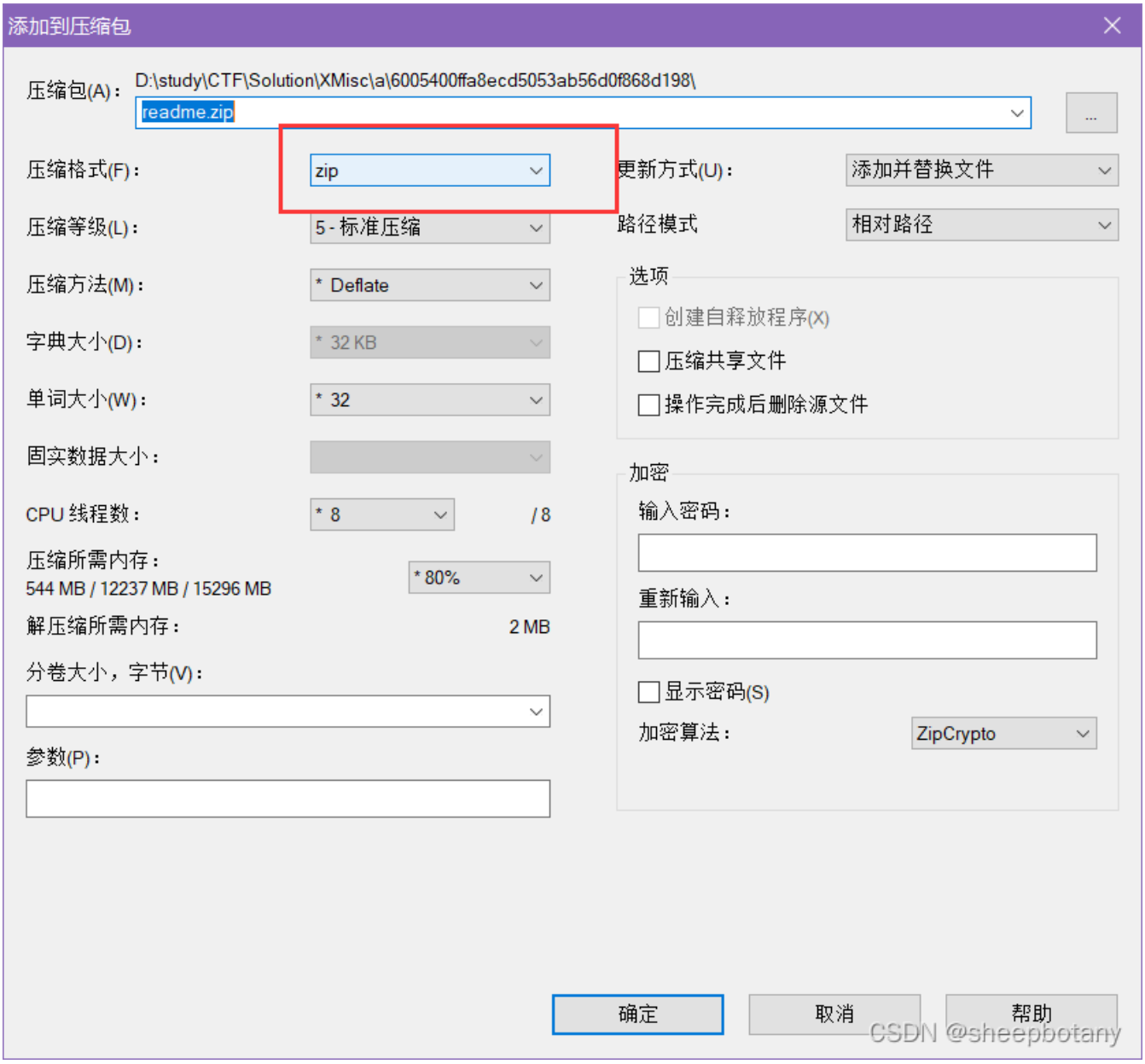
我们把外面的readme.txt进行压缩（需要用winRAR进行加密）

然后打开ARCHPR



但是不知道为啥用了winRAR还是报错

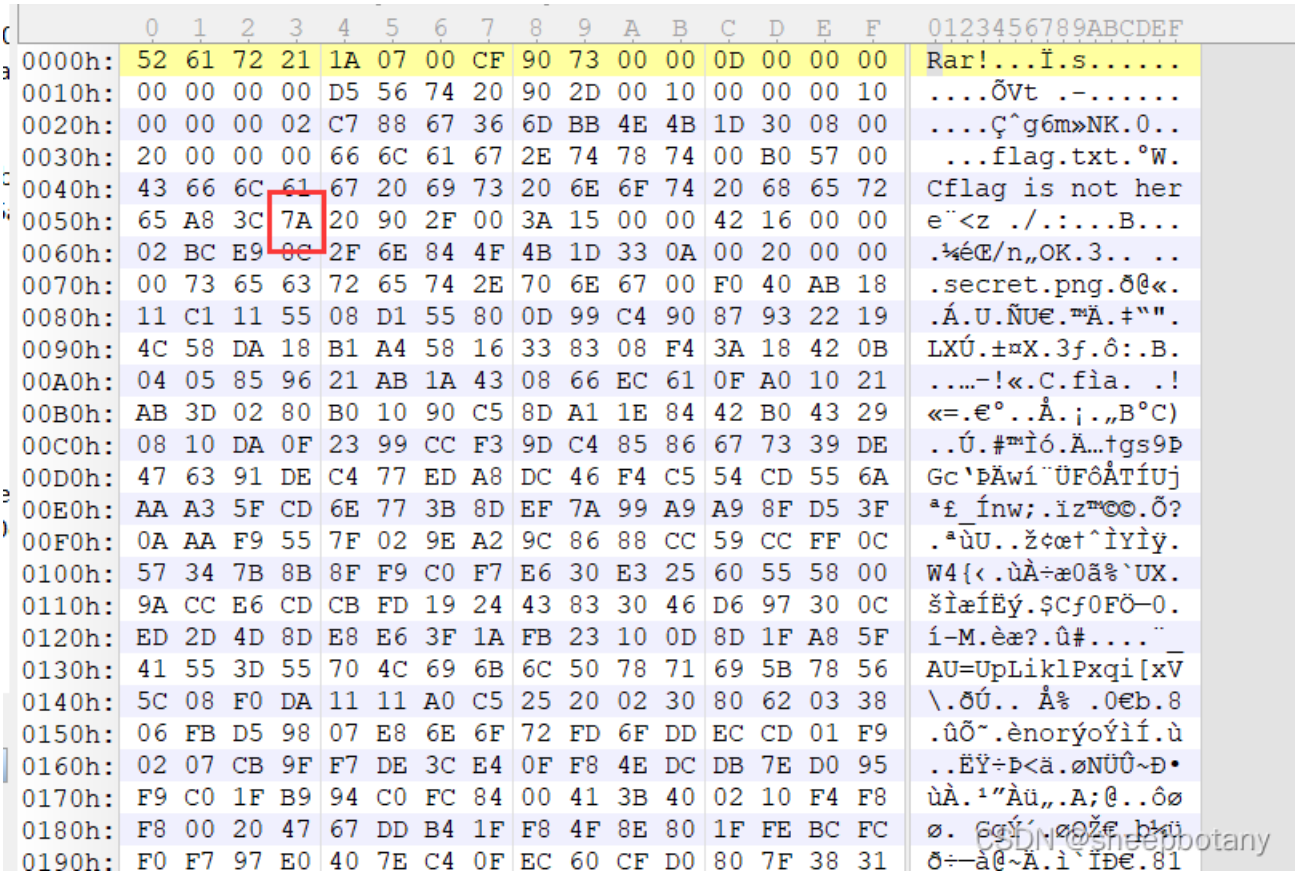
可能是因为我之前用了bandzip的原因，后来换成了7z，注意7z的使用方法：



14：【攻防世界】Simple RAR

打开是文件头损坏的压缩包

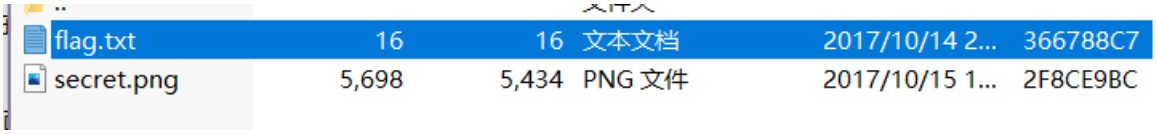
使用010Editor，7A的地方是文件头，本来应该是74



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	52	61	72	21	1A	07	00	CF	90	73	00	00	0D	00	00	00	Rar!...Ï.s.....
0010h:	00	00	00	00	D5	56	74	20	90	2D	00	10	00	00	00	10	....ÕVt .-......
0020h:	00	00	00	02	C7	88	67	36	6D	BB	4E	4B	1D	30	08	00	....Çˆg6m»NK.0..
0030h:	20	00	00	00	66	6C	61	67	2E	74	78	74	00	B0	57	00	...flag.txt.°W.
0040h:	43	66	6C	61	67	20	69	73	20	6E	6F	74	20	68	65	72	Cflag is not her
0050h:	65	A8	3C	7A	20	90	2F	00	3A	15	00	00	42	16	00	00	e¨<z ./.:...B...
0060h:	02	BC	E9	8C	2F	6E	84	4F	4B	1D	33	0A	00	20	00	00	.¼éŒ/n„OK.3.. ..
0070h:	00	73	65	63	72	65	74	2E	70	6E	67	00	F0	40	AB	18	.secret.png.ð@«.
0080h:	11	C1	11	55	08	D1	55	80	0D	99	C4	90	87	93	22	19	.Á.U.ÑU€.™Ä.‡"".
0090h:	4C	58	DA	18	B1	A4	58	16	33	83	08	F4	3A	18	42	0B	LXÚ.±¤X.3ƒ.ô:.B.
00A0h:	04	05	85	96	21	AB	1A	43	08	66	EC	61	0F	A0	10	21	..…–!«.C.fìa. .!
00B0h:	AB	3D	02	80	B0	10	90	C5	8D	A1	1E	84	42	B0	43	29	«=.€°..Å.¡.„B°C)
00C0h:	08	10	DA	0F	23	99	CC	F3	9D	C4	85	86	67	73	39	DE	..Ú.#™Ìó.Ä…†gs9Þ
00D0h:	47	63	91	DE	C4	77	ED	A8	DC	46	F4	C5	54	CD	55	6A	Gc'ÞÄwí¨ÜFôÅTÍUj
00E0h:	AA	A3	5F	CD	6E	77	3B	8D	EF	7A	99	A9	A9	8F	D5	3F	ª£_Ínw;.ïz™©©.Õ?
00F0h:	0A	AA	F9	55	7F	02	9E	A2	9C	86	88	CC	59	CC	FF	0C	.ªùU..ž¢œ†ˆÌYÌÿ.
0100h:	57	34	7B	8B	8F	F9	C0	F7	E6	30	E3	25	60	55	58	00	W4{‹.ùÀ÷æ0ã%`UX.
0110h:	9A	CC	E6	CD	CB	FD	19	24	43	83	30	46	D6	97	30	0C	šÌæÍËý.$Cƒ0FÖ—0.
0120h:	ED	2D	4D	8D	E8	E6	3F	1A	FB	23	10	0D	8D	1F	A8	5F	í-M.èæ?.û#....¨_
0130h:	41	55	3D	55	70	4C	69	6B	6C	50	78	71	69	5B	78	56	AU=UpLiklPxqi[xV
0140h:	5C	08	F0	DA	11	11	A0	C5	25	20	02	30	80	62	03	38	\.ðÚ.. Å% .0€b.8
0150h:	06	FB	D5	98	07	E8	6E	6F	72	FD	6F	DD	EC	CD	01	F9	.ûÕ˜.ènoryoÝìÍ.ù
0160h:	02	07	CB	9F	F7	DE	3C	E4	0F	F8	4E	DC	DB	7E	D0	95	..ËŸ÷Þ<ä.øNÜÛ~Ð•
0170h:	F9	C0	1F	B9	94	C0	FC	84	00	41	3B	40	02	10	F4	F8	ùÀ.¹”Àü„.A;@..ôø
0180h:	F8	00	20	47	67	DD	B4	1F	F8	4F	8E	80	1F	FE	BC	FC	ø. GgÝ´.øOŽ€.þ¼ü
0190h:	F0	F7	97	E0	40	7E	C4	0F	EC	60	CF	D0	80	7F	38	31	ð÷—à@~Ä.ì`ÏĐ€.81

CSDN @sheepbotany

发现有一张图片



flag.txt	16	16	文本文档	2017/10/14 2...	366788C7
secret.png	5,698	5,434	PNG 文件	2017/10/15 1...	2F8CE9BC

继续拖到010Editor中，打开发现是GIF文件

Edit As: Hex ▾ Run Script ▾ Run Template ▾

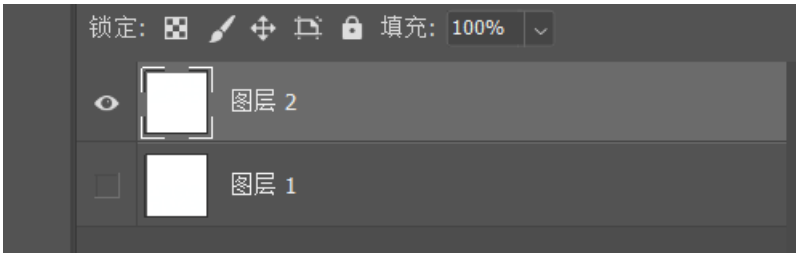
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
000h:	47	49	46	38	39	61	18	01	18	01	91	02	00	FE	FF	FF	GIF89a....'..þÿÿ
010h:	FF	FF	FF	FF	FF	FF	00	00	00	21	FF	0B	58	4D	50	20	ÿÿÿÿÿÿ...!ÿ.XMP
020h:	44	61	74	61	58	4D	50	3C	3F	78	70	61	63	6B	65	74	DataXMP<?xpacket
030h:	20	62	65	67	69	6E	3D	22	EF	BB	BF	22	20	69	64	3D	begin="ï»¿" id=
040h:	22	57	35	4D	30	4D	70	43	65	68	69	48	7A	72	65	53	"W5M0MpCehiHzreS
050h:	7A	4E	54	63	7A	6B	63	39	64	22	3F	3E	20	3C	78	3A	zNTczkc9d"?> <x:
060h:	78	6D	70	6D	65	74	61	20	78	6D	6C	6E	73	3A	78	3D	xmpmeta xmlns:x=
070h:	22	61	64	6F	62	65	3A	6E	73	3A	6D	65	74	61	2F	22	"adobe:ns:meta/"
080h:	20	78	3A	78	6D	70	74	6B	3D	22	41	64	6F	62	65	20	x:xmptk="Adobe
090h:	58	4D	50	20	43	6F	72	65	20	35	2E	33	2D	63	30	31	XMP Core 5.3-c01
0A0h:	31	20	36	36	2E	31	34	35	36	36	31	2C	20	32	30	31	1 66.145661, 201
0B0h:	32	2F	30	32	2F	30	36	2D	31	34	3A	35	36	3A	32	37	2/02/06-14:56:27
0C0h:	20	20	20	20	20	20	20	20	22	3E	20	3C	72	64	66	3A	"> <rdf:
0D0h:	52	44	46	20	78	6D	6C	6E	73	3A	72	64	66	3D	22	68	RDF xmlns:rdf="h
0E0h:	74	74	70	3A	2F	2F	77	77	77	2E	77	33	2E	6F	72	67	ttp://www.w3.org
0F0h:	2F	31	39	39	39	2F	30	32	2F	32	32	2D	72	64	66	2D	/1999/02/22-rdf-
100h:	73	79	6E	74	61	78	2D	6E	73	23	22	3E	20	3C	72	64	syntax-ns#"> <rd
110h:	66	3A	44	65	73	63	72	69	70	74	69	6F	6E	20	72	64	f:Description rd
120h:	66	3A	61	62	6F	75	74	3D	22	22	20	78	6D	6C	6E	73	f:about="" xmlns
130h:	3A	78	6D	70	4D	4D	3D	22	68	74	74	70	3A	2F	2F	6E	:xmpMM="http://n
140h:	73	2E	61	64	6F	62	65	2E	63	6F	6D	2F	78	61	70	2F	s.adobe.com/xap/

CSDN @sheepbotany

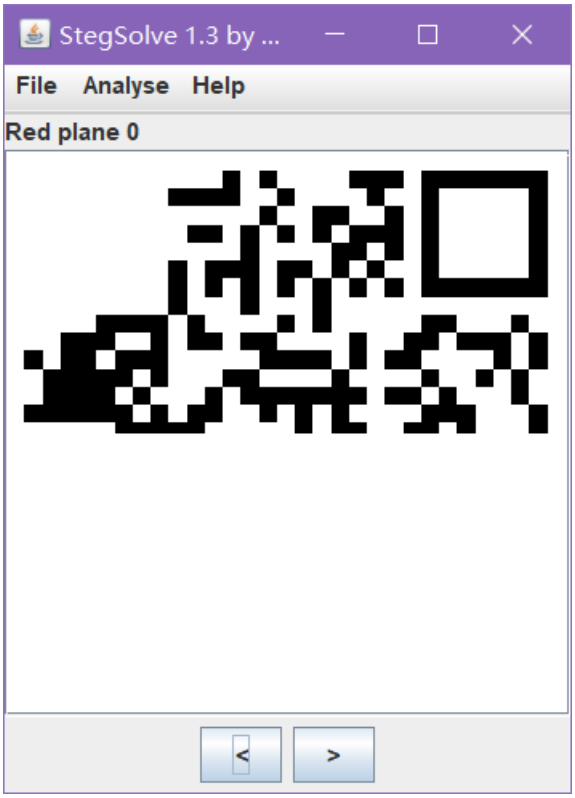
修改文件后缀为gif，然后拖到stegolve中，翻到半张二维码

然后继续翻，发现没有，于是脱到ps中（根据提示是双图层）

选中图层2导出：



继续拖到stegolve中查看：



截图保存后使用ps拼接

CSDN @sheepbotany

用ORCode最后获得flag:

flag{yanji4n_bu_we1shi}

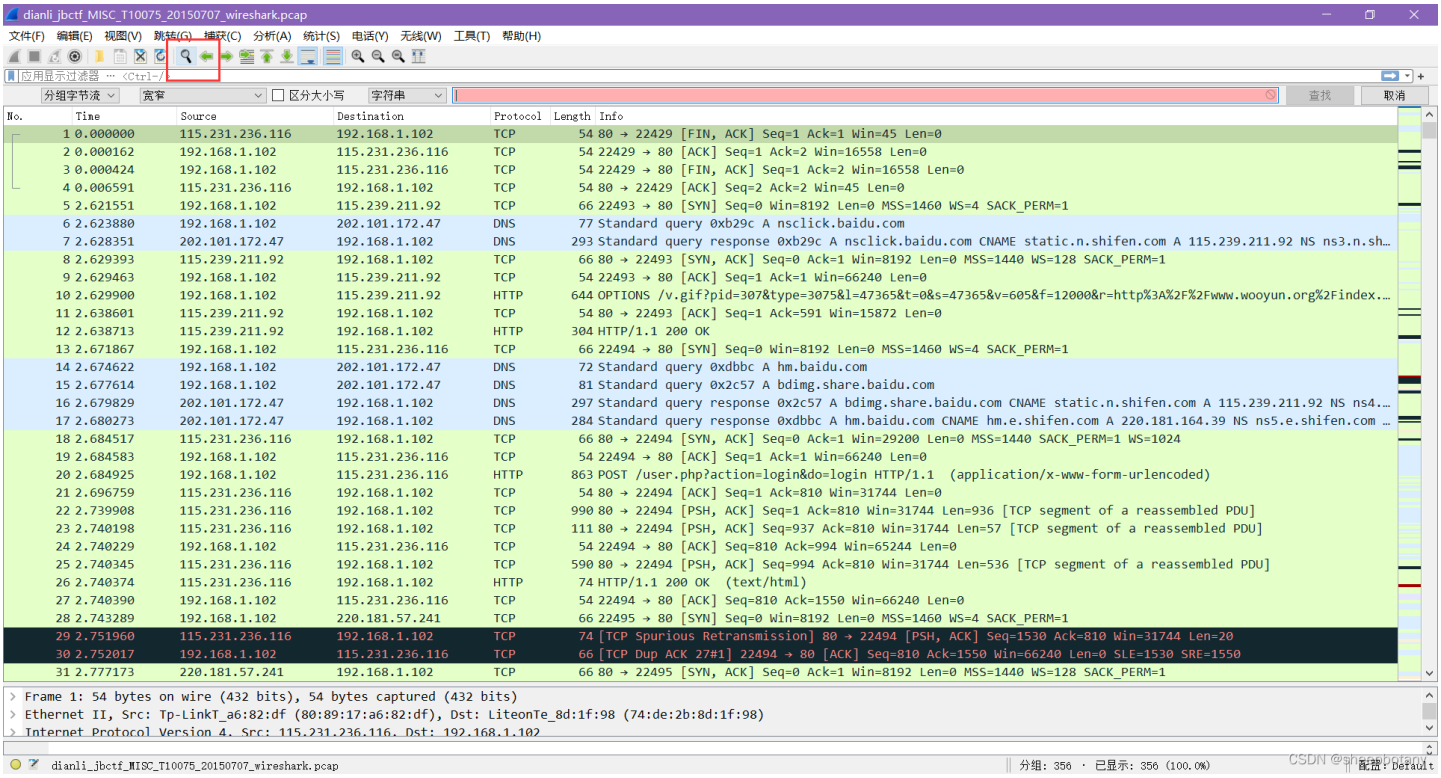
流量分析

15：【BUUCTF】wireshark

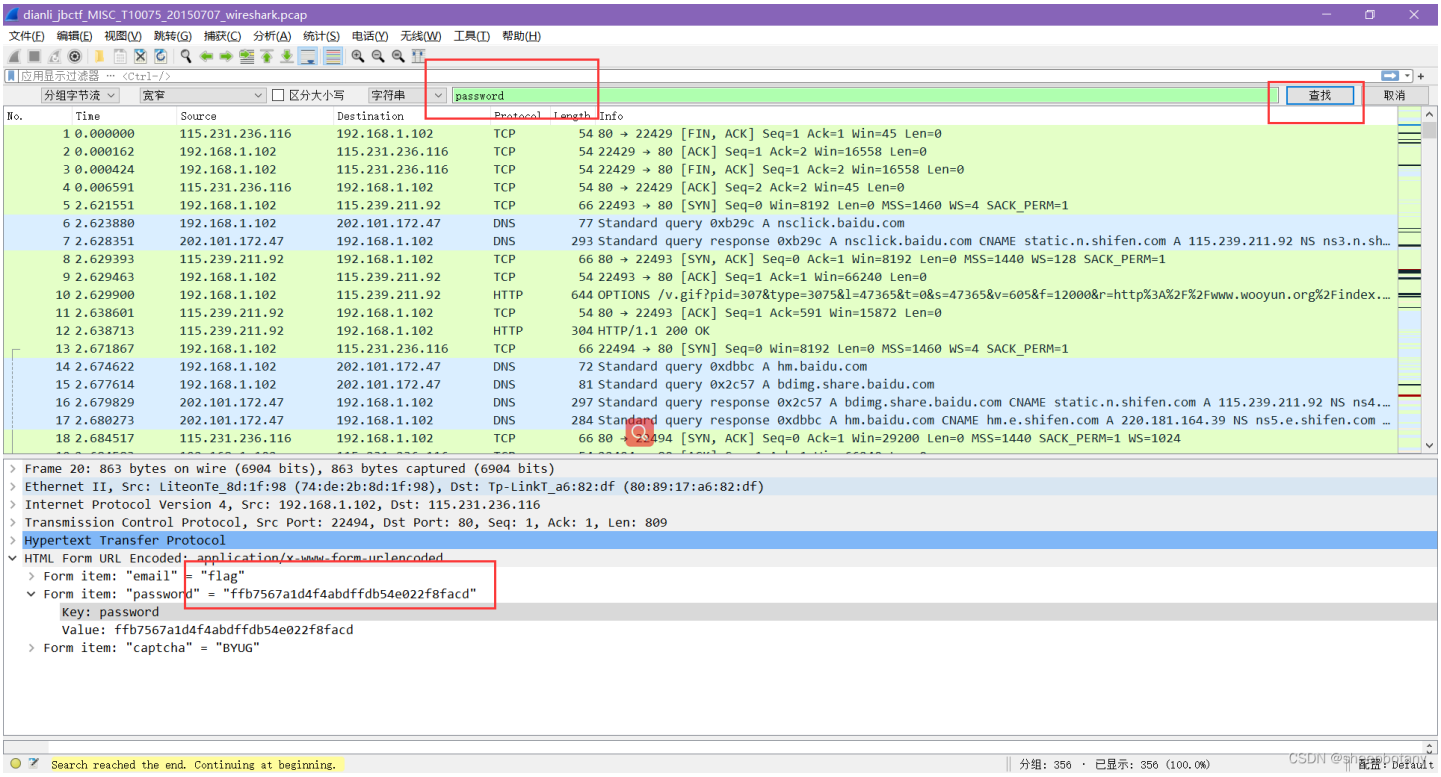
打开发现是wireshark流量包，拖进wireshark看看

题目告诉我们要去找password

黑客通过wireshark抓到管理员登陆网站的一段流量包（管理员的密码即是答案)注意：得到的flag请包上flag{}提交



搜索password



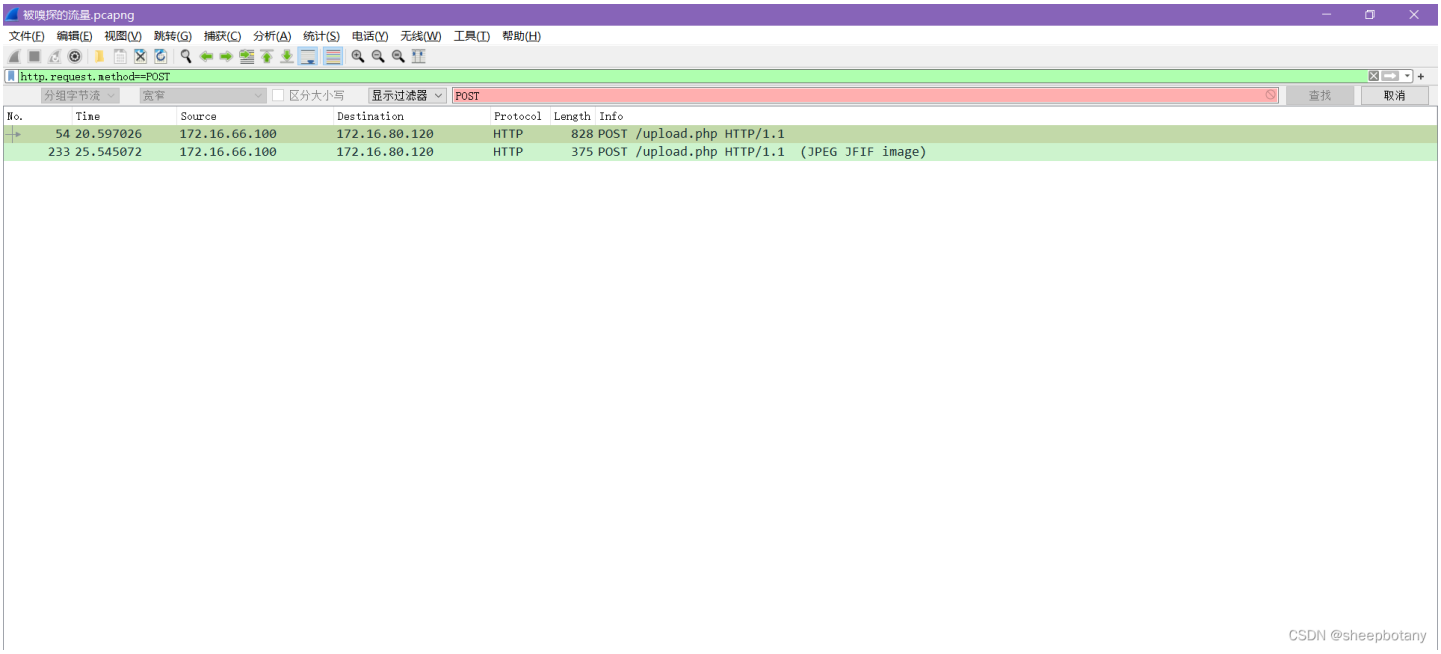
16: 【BUUCTF】被嗅探的流量

拖到wireshark

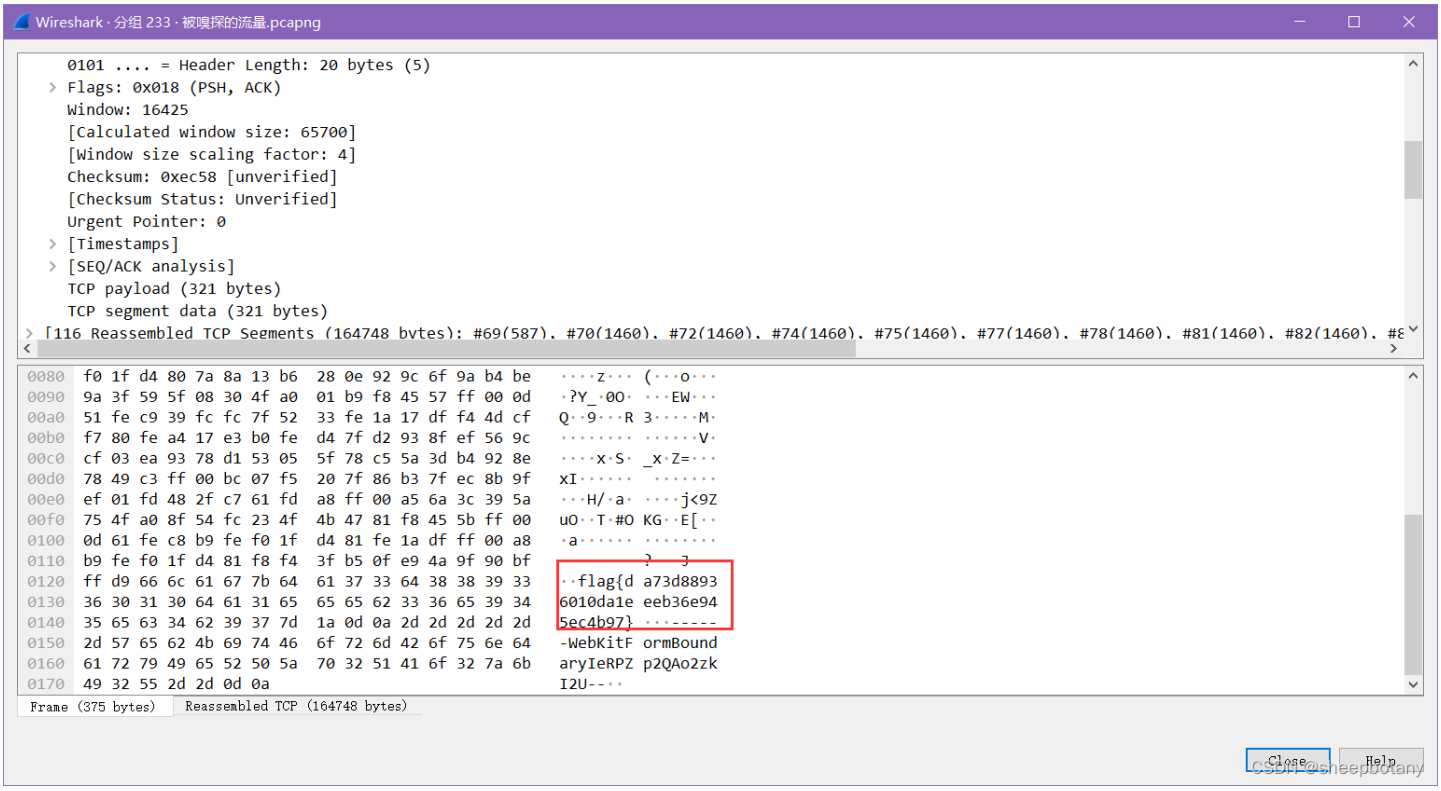
某黑客潜入到某公司内网通过嗅探抓取了一段文件传输的数据，该数据也被该公司截获，你能帮该公司分析他抓取的到底是什么文件的数据吗？注意：得到的 flag 请包上 flag{} 提交

提示我们输入

http.request.method==POST



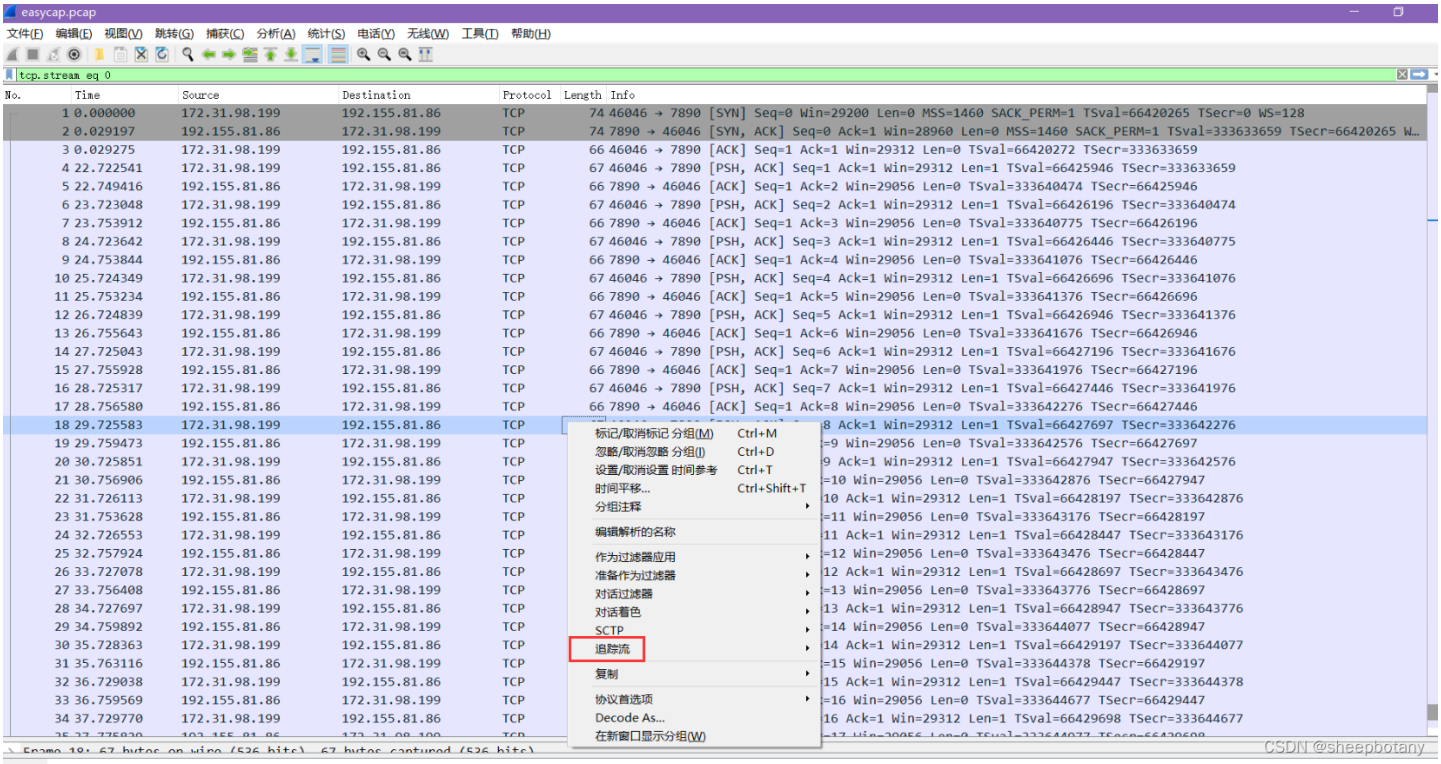
点进去看发现：



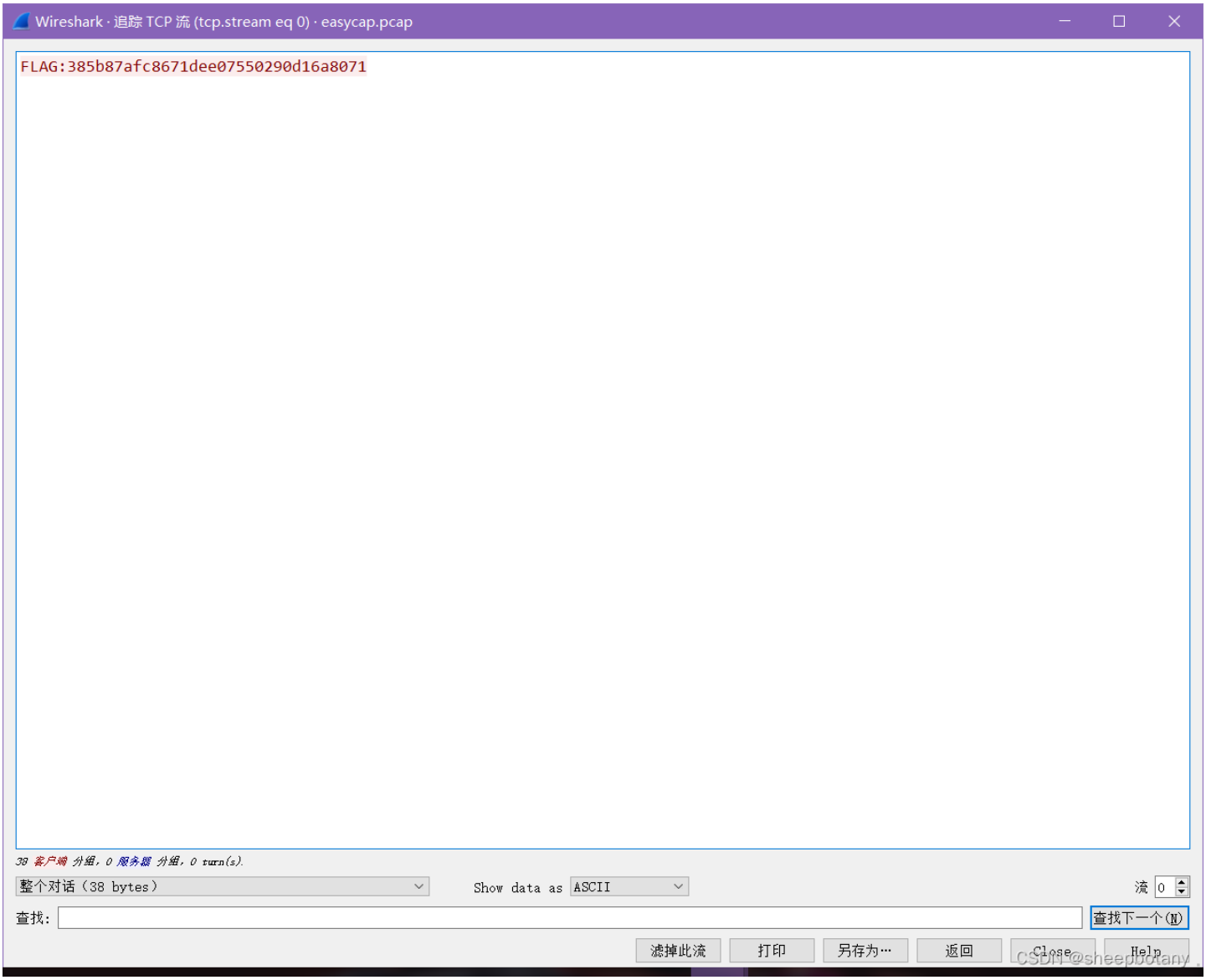
得到flag:flag{da73d88936010da1eeeb36e945ec4b97}

17:【BUUCTF】easycap

因为是流量包，直接在任意TCP处右键，选择TCP流


easycap.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
tcp.stream eq 0
No. Time Source Destination Protocol Length Info
1 0.000000 172.31.98.199 192.155.81.86 TCP 74 46046 → 7890 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=66420265 TSecr=0 WS=128
2 0.029197 192.155.81.86 172.31.98.199 TCP 74 7890 → 46046 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=333633659 TSecr=66420265 W…
3 0.029275 172.31.98.199 192.155.81.86 TCP 66 46046 → 7890 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=66420272 TSecr=333633659
4 22.722541 172.31.98.199 192.155.81.86 TCP 67 46046 → 7890 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=1 TSval=66425946 TSecr=333633659
5 22.749416 192.155.81.86 172.31.98.199 TCP 66 7890 → 46046 [ACK] Seq=1 Ack=2 Win=29056 Len=0 TSval=333640474 TSecr=66425946
6 23.723048 172.31.98.199 192.155.81.86 TCP 67 46046 → 7890 [PSH, ACK] Seq=2 Ack=1 Win=29312 Len=1 TSval=66426196 TSecr=333640474
7 23.753912 192.155.81.86 172.31.98.199 TCP 66 7890 → 46046 [ACK] Seq=1 Ack=3 Win=29056 Len=0 TSval=333640775 TSecr=66426196
8 24.723642 172.31.98.199 192.155.81.86 TCP 67 46046 → 7890 [PSH, ACK] Seq=3 Ack=1 Win=29312 Len=1 TSval=66426446 TSecr=333640775
9 24.753844 192.155.81.86 172.31.98.199 TCP 66 7890 → 46046 [ACK] Seq=1 Ack=4 Win=29056 Len=0 TSval=333641076 TSecr=66426446
10 25.724349 172.31.98.199 192.155.81.86 TCP 67 46046 → 7890 [PSH, ACK] Seq=4 Ack=1 Win=29312 Len=1 TSval=66426696 TSecr=333641076
11 25.753234 192.155.81.86 172.31.98.199 TCP 66 7890 → 46046 [ACK] Seq=1 Ack=5 Win=29056 Len=0 TSval=333641376 TSecr=66426696
12 26.724839 172.31.98.199 192.155.81.86 TCP 67 46046 → 7890 [PSH, ACK] Seq=5 Ack=1 Win=29312 Len=1 TSval=66426946 TSecr=333641376
13 26.755643 192.155.81.86 172.31.98.199 TCP 66 7890 → 46046 [ACK] Seq=1 Ack=6 Win=29056 Len=0 TSval=333641676 TSecr=66426946
14 27.725043 172.31.98.199 192.155.81.86 TCP 67 46046 → 7890 [PSH, ACK] Seq=6 Ack=1 Win=29312 Len=1 TSval=66427196 TSecr=333641676
15 27.755928 192.155.81.86 172.31.98.199 TCP 66 7890 → 46046 [ACK] Seq=1 Ack=7 Win=29056 Len=0 TSval=333641976 TSecr=66427196
16 28.725317 172.31.98.199 192.155.81.86 TCP 67 46046 → 7890 [PSH, ACK] Seq=7 Ack=1 Win=29312 Len=1 TSval=66427446 TSecr=333641976
17 28.756580 192.155.81.86 172.31.98.199 TCP 66 7890 → 46046 [ACK] Seq=1 Ack=8 Win=29056 Len=0 TSval=333642276 TSecr=66427446
18 29.725583 172.31.98.199 192.155.81.86 TCP
19 29.759473 192.155.81.86 172.31.98.199 TCP
20 30.725851 172.31.98.199 192.155.81.86 TCP
21 30.756906 192.155.81.86 172.31.98.199 TCP
22 31.726113 172.31.98.199 192.155.81.86 TCP
23 31.753628 192.155.81.86 172.31.98.199 TCP
24 32.726553 172.31.98.199 192.155.81.86 TCP
25 32.757924 192.155.81.86 172.31.98.199 TCP
26 33.727078 172.31.98.199 192.155.81.86 TCP
27 33.756408 192.155.81.86 172.31.98.199 TCP
28 34.727697 172.31.98.199 192.155.81.86 TCP
29 34.759892 192.155.81.86 172.31.98.199 TCP
30 35.728363 172.31.98.199 192.155.81.86 TCP
31 35.763116 192.155.81.86 172.31.98.199 TCP
32 36.729038 172.31.98.199 192.155.81.86 TCP
33 36.759569 192.155.81.86 172.31.98.199 TCP
34 37.729770 172.31.98.199 192.155.81.86 TCP
标记/取消标记 分组(M) Ctrl+M
忽略/取消忽略 分组(I) Ctrl+D
设置/取消设置 时间参考 Ctrl+T
时间平移... Ctrl+Shift+T
分组注释
编辑解析的名称
作为过滤器应用
准备作为过滤器
对话过滤器
对话着色
SCTP
追踪流
复制
协议首选项
Decode As...
在新窗口显示分组(W)
CSDN @sheepbotany

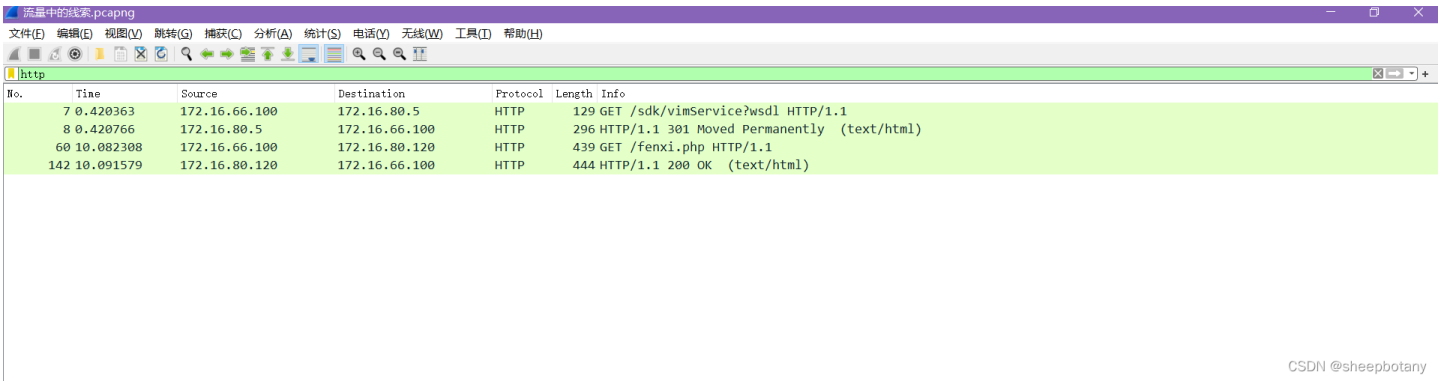
即可得到flag



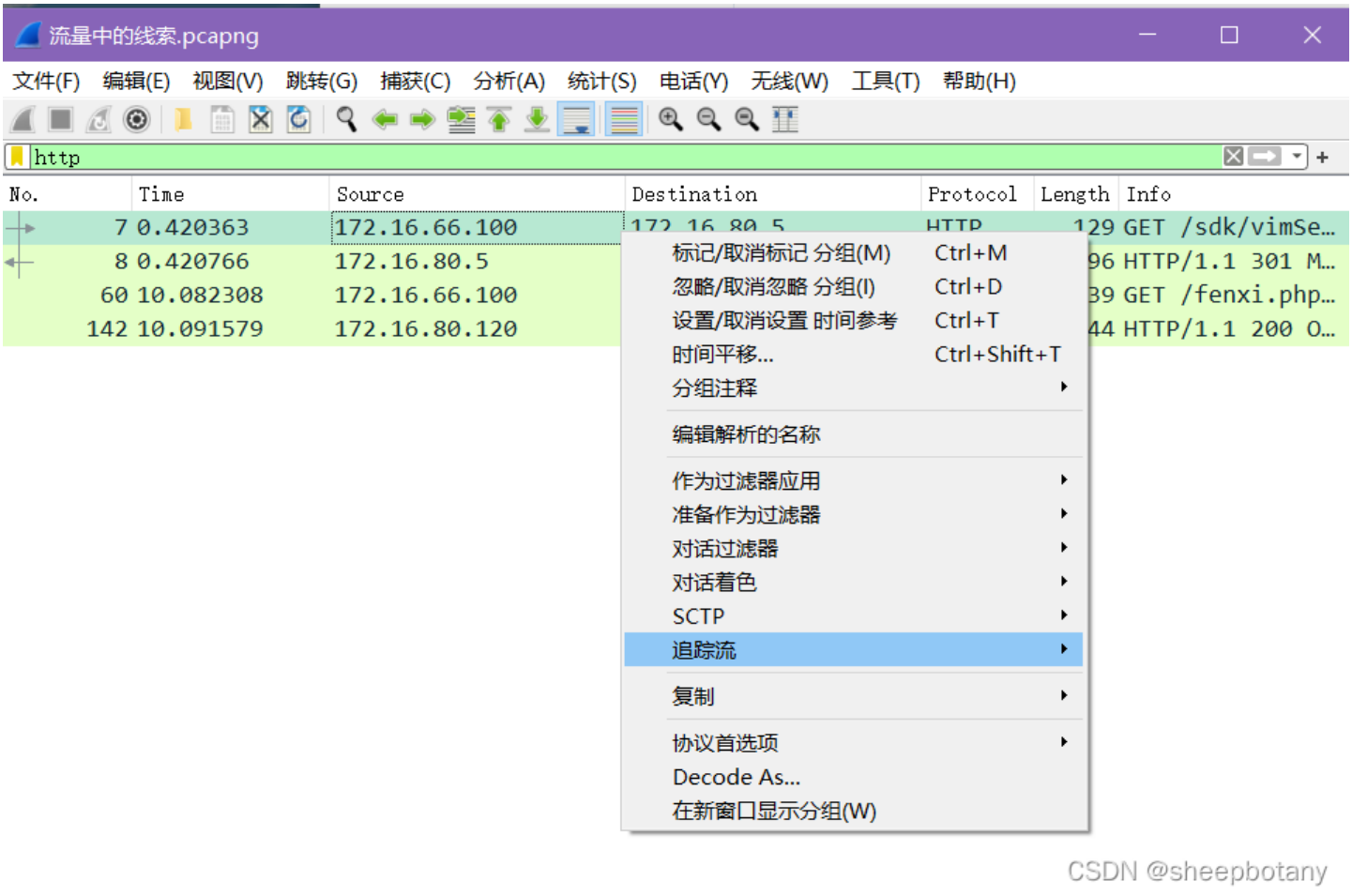
18：【BUUCTF】数据包中的线索

公安机关近期截获到某网络犯罪团伙在线交流的数据包，但无法分析出具体的交流内容，聪明的你能帮公安机关找到线索吗？注意：得到的 flag 请包上 flag{} 提交

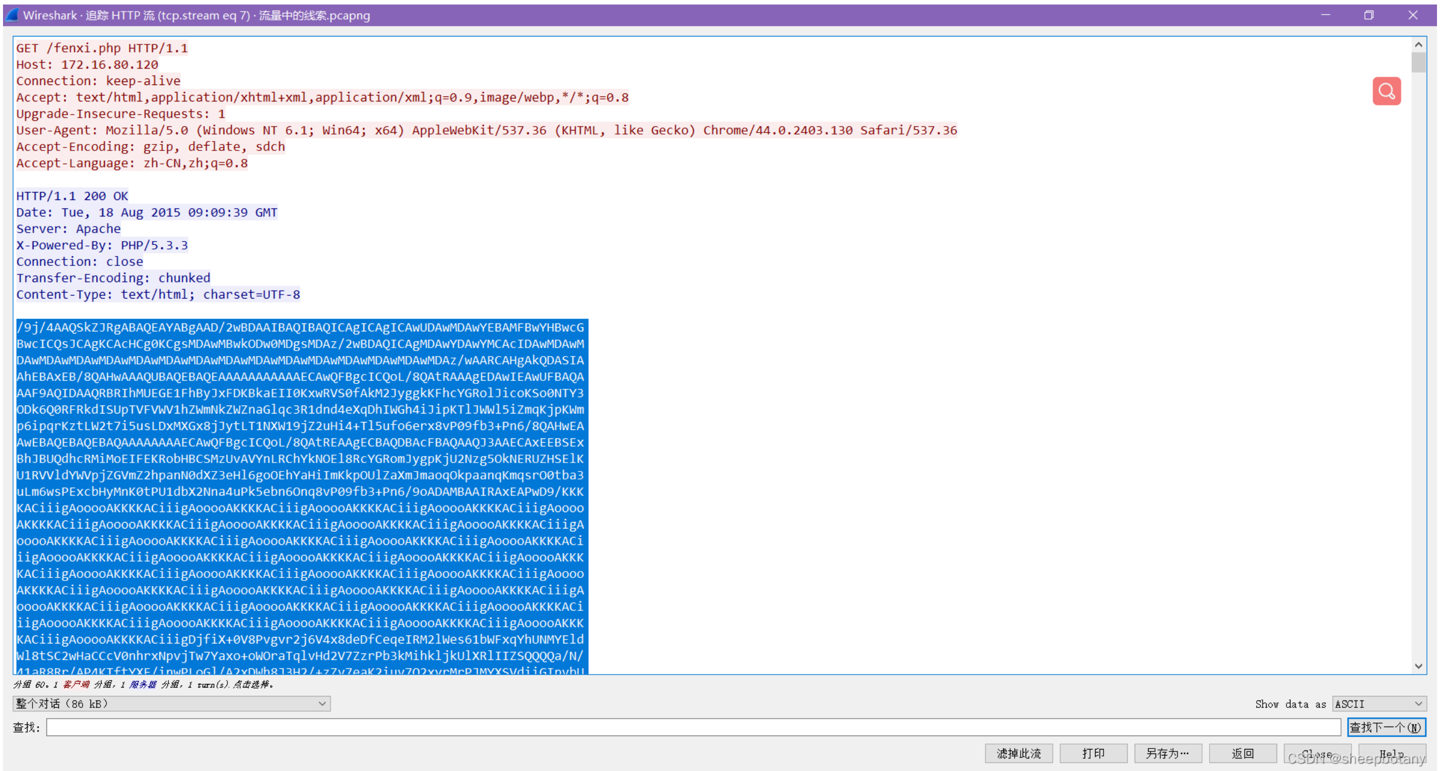
在线交流，提示我们筛选出http



选中一个http右键追踪



每个都追踪一下，最后发现：


Wireshark · 追踪 HTTP 流 (tcp.stream eq 7) · 流量中的线索.pcapng
GET /fenxi.php HTTP/1.1
Host: 172.16.80.120
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2403.130 Safari/537.36
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
HTTP/1.1 200 OK
Date: Tue, 18 Aug 2015 09:09:39 GMT
Server: Apache
X-Powered-By: PHP/5.3.3
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
整个对话 (86 kB)
Show data as ASCII
查找:
查找下一个(N)
滤掉此流
打印
另存为…
返回
CSDN @sheepbotany

base64的编码

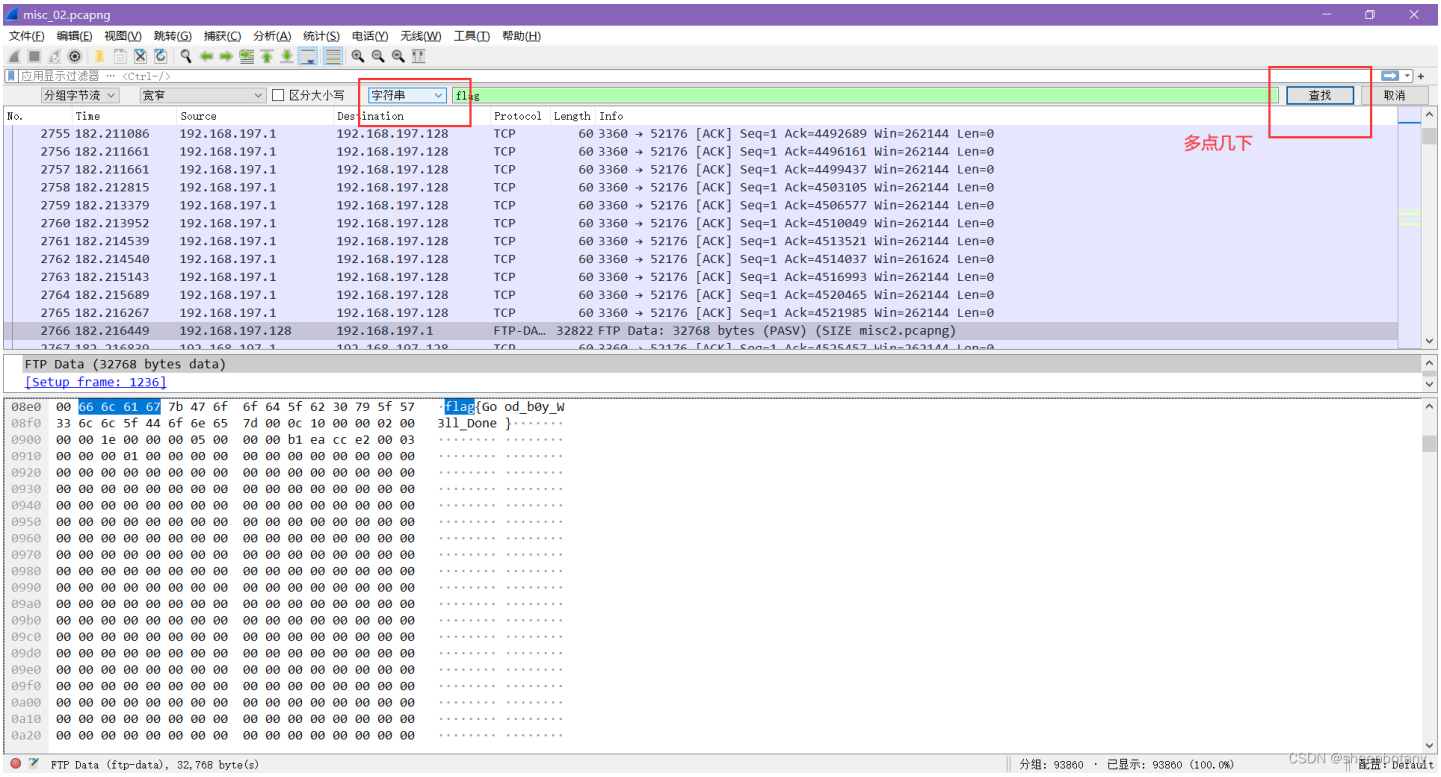

CSDN @sheepbotany

正常解码不行，就选择图片解码

19：【攻防世界】embrass

打开来看是一个数据包

直接搜一下有没有flag



编码相关

20【攻防世界】Test-flag-please-ignore

修改后缀为txt，打开发现是字符串，因为有数字有字符有f，所以应该是十六进制

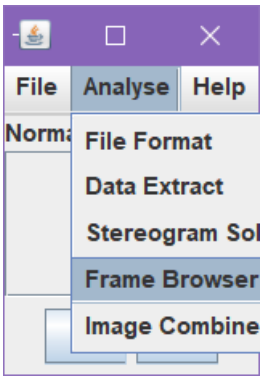
666c61677b68656c6c6f5f776f726c647d

丢进转换器里转换得到flag

flag{hello_world}

21：【攻防世界】Aesop_secret

打开来看是gif文件，放入stegolve中，选择

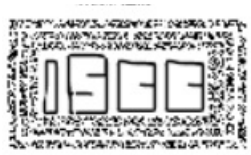


来进行逐帧分析，每一帧对应的图案位置不同，使用ps缝合起来

好吧还是建议不要用ps缝合，我们使用动态图片缝合工具吧

GIF动态图片分解，多帧动态图分解成多张静态图片_图片工具网页版 (sioe.cn)

然后就得到：



我们拖到010Editor中：

得到base64编码

```
820h: 0E 54 40 55 3B B6 26 A1 81 31 0A 34 80 7D E3 0D  .T@U;¶&¡.1.4€}ã.
830h: F0 1E 8C 06 BD 90 49 67 7F 15 00 25 41 54 BD 18  ð.Œ.½.Ig...%AT½.
840h: 60 5B 18 78 C6 08 04 03 E6 B8 65 85 18 1E C1 97  `[.xÆ...æ¸e….Á—
850h: 73 A9 31 17 1D 9A EC E1 87 82 01 4A F2 85 80 67  s©1..šìá‡‚.Jò…€g
860h: 6B B0 38 5E 9C F8 91 93 C9 26 E7 1D 24 DE 9B 49  k°8^œø'"É&ç.$Þ›I
870h: C6 A8 E3 63 1A 84 37 DD 9E F7 7D C9 57 98 7C 8D  Æ¨ãc.„7Ýž÷}ÉW˜|.
880h: 59 A6 A2 56 0D 30 C0 60 E3 51 75 61 A1 84 7D B5  Y¦¢V.0À`ãQua¡„}µ
890h: DC 40 06 D0 A5 D4 8A 98 4D D9 E0 04 C3 4D 48 CE  Ü@.Ð¥ÔŠ˜MÙà.ÃMHÎ
8A0h: 07 26 14 E4 A5 41 AF 26 1F 29 EB AC B4 D6 6A EB  .&.ä¥A¯&.)ë¬´Öjë
8B0h: AD B8 E6 AA EB AE BC F6 EA EB AF C0 06 2B EC B0  -¸æªë®¼öêë¯À.+ì°
8C0h: C4 16 6B EC B1 B2 06 04 00 3B 55 32 46 73 64 47  Ä.kì±²...;U2FsdG
8D0h: 56 6B 58 31 39 51 77 47 6B 63 67 44 30 66 54 6A  VkX19QwGkcgD0fTj
8E0h: 5A 78 67 69 6A 52 7A 51 4F 47 62 43 57 41 4C 68  ZxgijRzQOGbCWALh
8F0h: 34 73 52 44 65 63 32 77 36 78 73 59 2F 75 78 35  4sRDec2w6xsY/ux5
900h: 33 56 75 6A 2F 41 4D 5A 42 44 4A 38 37 71 79 5A  3Vuj/AMZBDJ87qyZ
910h: 4C 35 6B 41 66 31 66 6D 41 48 34 4F 65 31 33 49  L5kAf1fmAH4Oe13I
920h: 75 34 33 35 62 66 52 42 75 5A 67 48 70 6E 52 6A  u435bfRBuZgHpnRj
930h: 54 42 6E 35 2B 78 73 44 48 4F 4E 69 52 33 74 30  TBn5+xsDHONiR3t0
940h: 2B 4F 61 38 79 47 2F 74 4F 4B 4A 4D 4E 55 61 75  +Oa8yG/tOKJMNUau
950h: 65 64 76 4D 79 4E 34 76 34 51 4B 69 46 75 6E 77  edvMyN4v4QKiFunw
960h: 3D 3D 0D 0A                                      ==..
```

CSDN @sheepbotany

选择网站在线AES加密 | AES解密 - 在线工具 (sojson.com)

进行解码，得到一串base64，可以继续解码

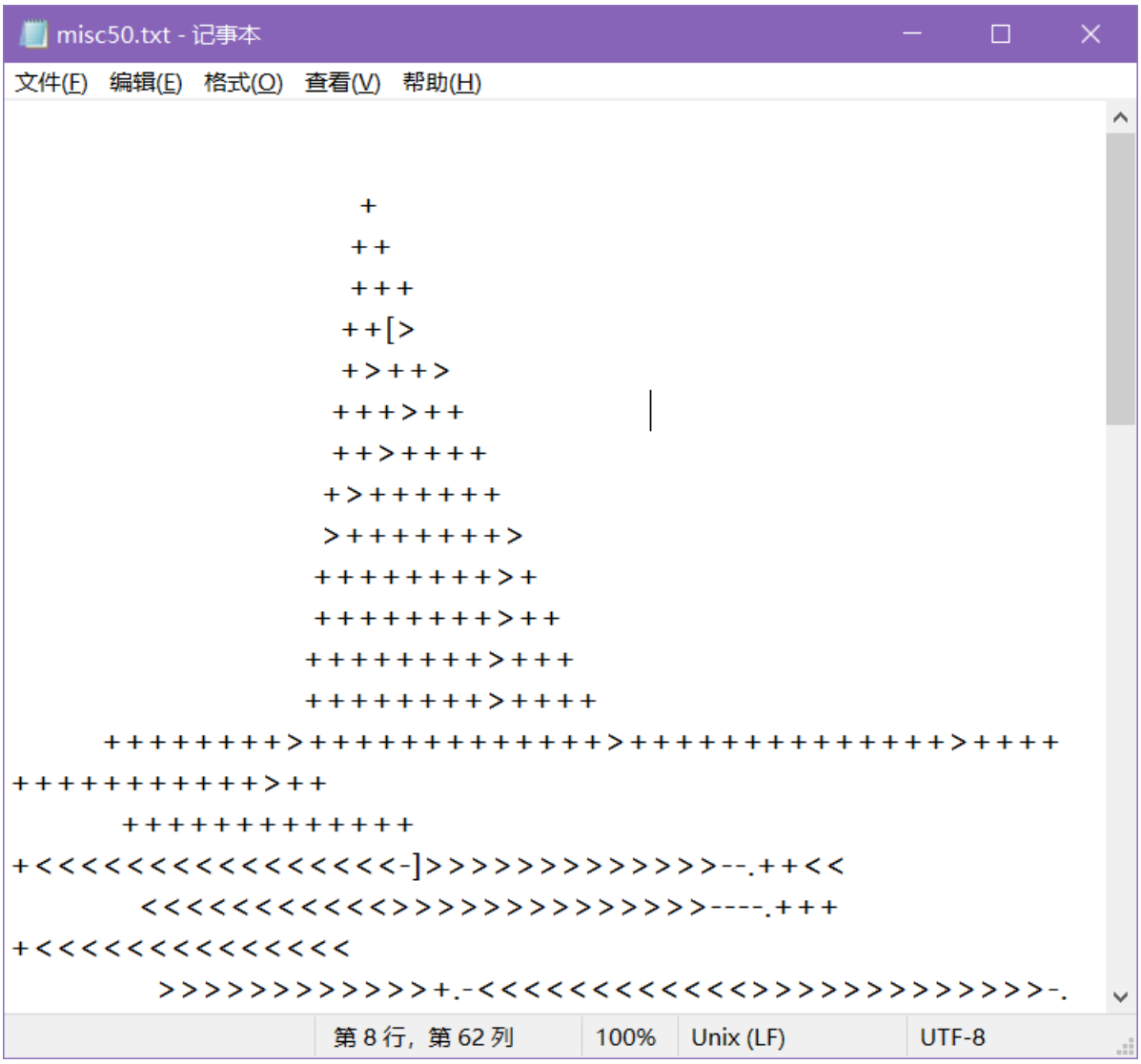
U2FsdGVkX18OvTUlZubDnmvk2lSAkb8Jt4Zv6UWpE7Xb43f8uzeFRUKGMo6QaaNFHZriDDV0EQ/qt38Tw73tbQ==

最后得到flag

flag{DugUpADiamondADeepDarkMine}

22：【攻防世界】can_has_stdio?

得到elf文件，我们还是把后缀改为txt



经典BrainFuck解密：

flag为：flag{esolangs_for_fun_and_profit}

进行解码，得到一串base64，可以继续解码

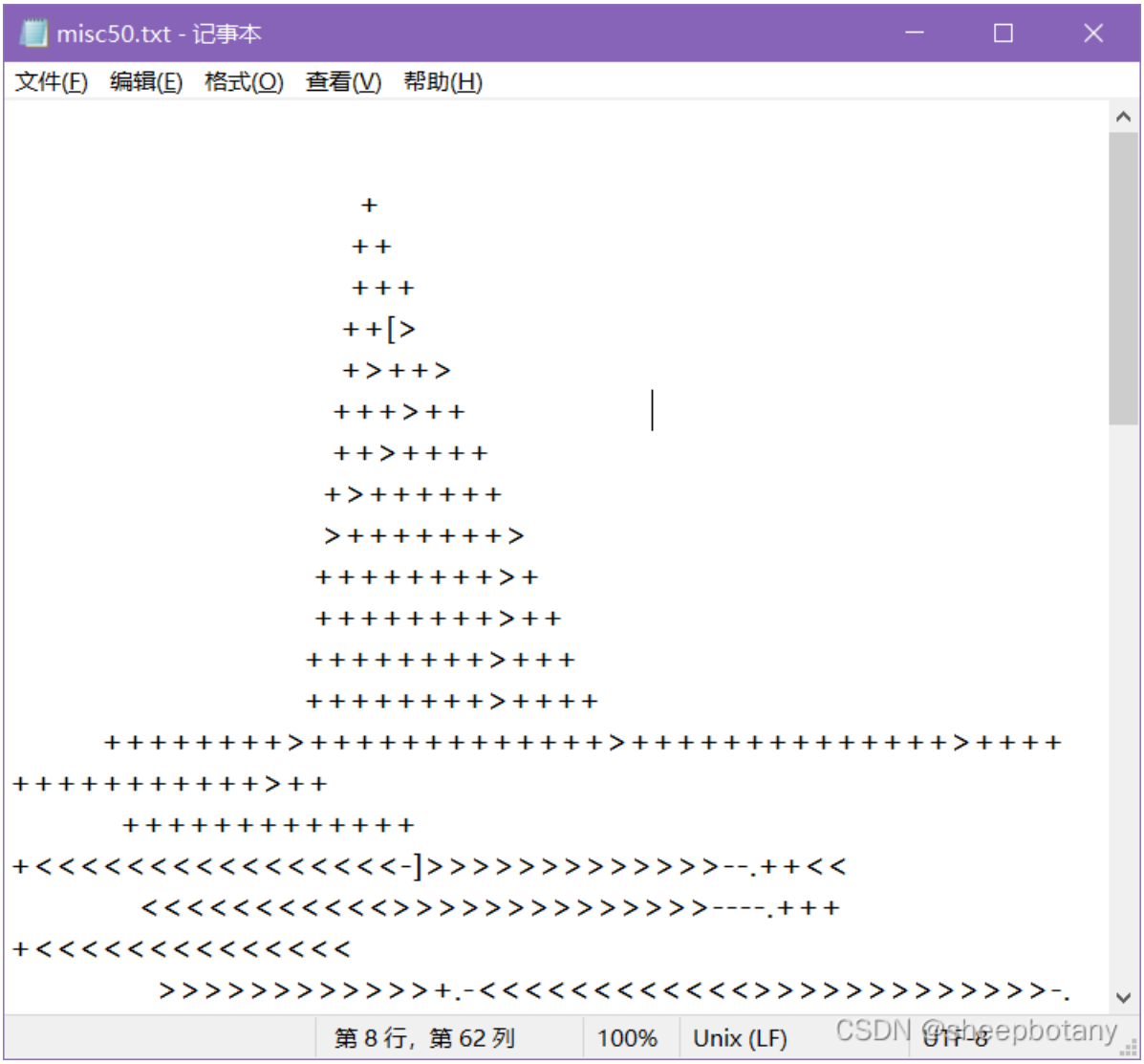
U2FsdGVkX18OvTUlZubDnmvk2lSAkb8Jt4Zv6UWpE7Xb43f8uzeFRUKGMo6QaaNFHZriDDV0EQ/qt38Tw73tbQ==

最后得到flag

flag{DugUpADiamondADeepDarkMine}
选择网站在线AES加密 | AES解密 - 在线工具 (sojson.com)

22：【攻防世界】can_has_stdio?

得到elf文件，我们还是把后缀改为txt



经典BrainFuck解密：

flag为：flag{esolangs_for_fun_and_profit}