

BUUCTF-杂项-1

原创

[eeknight](#) 于 2020-09-12 22:05:48 发布 889 收藏 1

分类专栏: [ctf 杂项 BUUCTF](#) 文章标签: [信息安全](#)

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/m0_46383107/article/details/108555800

版权



[ctf 同时被 3 个专栏收录](#)

1 篇文章 0 订阅

订阅专栏



[杂项](#)

1 篇文章 0 订阅

订阅专栏



[BUUCTF](#)

1 篇文章 0 订阅

订阅专栏

BUUCTF

杂项

文章目录

BUUCTF

杂项

[N种方法解决](#)

[wireshark](#)

[被嗅探的流量](#)

[easycap](#)

[FLAG](#)

[另外一个世界](#)

[假如给我三天光明](#)

[A_Beautiful_Picture](#)

[神秘龙卷风](#)

[来首歌吧](#)

N种方法解决

打开后下载文件key.exe

放到010Editor.exe里面可以看到一段文本

The screenshot shows a web browser at <https://the-x.cn/base64/>. The page title is "The X" and it features a navigation bar with options like "加密", "格式化", "Base64", etc. The main content is "Base64 在线解码、编码". A long Base64 string is entered and decoded into a hex dump. A context menu is open over the hex dump, showing options to save the file as a PNG image. The hex dump shows a sequence of bytes including '89 50 4E 47 0D 0A 1A 0A' which is a valid PNG signature.

由于前面是image/jpg 和base64加密 就直接去网上解密并弄成图片形式

网站: <https://the-x.cn/base64/> (注意要把前面的data:image/jpg;base64,这一段去掉才可以编译)

得到一个二维码 扫完就有flag

wireshark

The screenshot shows a challenge page for "wireshark" with 1864 solves. It features a download button for a file named "7fc3e8a0-69...", a "Flag" input field, and a "Submit" button. The page also includes a "Challenge" tab and a "1864 Solves" indicator.

这里要用到wireshark这个工具-虚拟机上有

下载后打开看到一堆东西

File Edit View Go Capture Analyze Statistics Help

Apply a display filter: 表达式...

No.	Time	Source	Destination	Protocol	Length	Info
25	2.740345	115.231.236.116	192.168.1.102	TCP	590	80 → 22494 [PSH, ACK] Seq=994 Ack=810 Win=31744 Len=536 [TCP segment of a reassembled PDU]
26	2.740374	115.231.236.116	192.168.1.102	HTTP	74	HTTP/1.1 200 OK (text/html)
27	2.740390	192.168.1.102	115.231.236.116	TCP	54	22494 → 80 [ACK] Seq=810 Ack=1550 Win=66240 Len=0
28	2.743289	192.168.1.102	220.181.57.241	TCP	66	22495 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
29	2.751960	115.231.236.116	192.168.1.102	TCP	74	[TCP spurious Retransmission] 80 → 22494 [PSH, ACK] Seq=1530 Ack=810 Win=31744 Len=20 [Reassembly error, p...
30	2.752017	192.168.1.102	115.231.236.116	TCP	66	[TCP Dup ACK 27#1] 22494 → 80 [ACK] Seq=810 Ack=1550 Win=66240 Len=0 SLE=1530 SRE=1550
31	2.777173	220.181.57.241	192.168.1.102	TCP	66	80 → 22495 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 WS=128 SACK_PERM=1
32	2.777245	192.168.1.102	220.181.57.241	TCP	54	22495 → 80 [ACK] Seq=1 Ack=1 Win=66240 Len=0
33	2.777385	192.168.1.102	220.181.57.241	HTTP	1094	GET /hm.gif?cc=1&ck=1&cl=24-bit&ds=1366x768&ep=48625%2C13747&et=3&fl=18.0&ja=1&n=zh-CN&o=0<=143559054...
34	2.809099	220.181.57.241	192.168.1.102	TCP	54	80 → 22495 [ACK] Seq=1 Ack=1041 Win=7936 Len=0
35	2.812445	220.181.57.241	192.168.1.102	HTTP	310	HTTP/1.1 200 OK (GIF89a)

> Frame 30: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
 > Ethernet II, Src: LiteonTe_8d:1f:98 (74:de:2b:8d:1f:98), Dst: Tp-LinkT_a6:82:df (80:89:17:a6:82:df)
 > Internet Protocol Version 4, Src: 192.168.1.102, Dst: 115.231.236.116
 > Transmission Control Protocol, Src Port: 22494, Dst Port: 80, Seq: 810, Ack: 1550, Len: 0

```

0000  80 89 17 a6 82 df 74 de 2b 8d 1f 98 08 00 45 00  .....t.+.
0010  00 34 61 19 40 00 40 06 b7 40 c0 a8 01 66 73 e7  .4a@.@.@...fs.
0020  ec 74 57 de 00 50 9c da dc 7e 4f 88 2d 97 80 10  .tw..P...O....
0030  40 b0 cd d0 00 00 01 01 05 0a 4f 88 2d 83 4f 88  @.....O...O.
0040  2d 97  ..
  
```

https://blog.csdn.net/m0_46383107

根据提示直接过滤出POST包（好像flag一般在POST这里）

File Edit View Go Capture Analyze Statistics Help

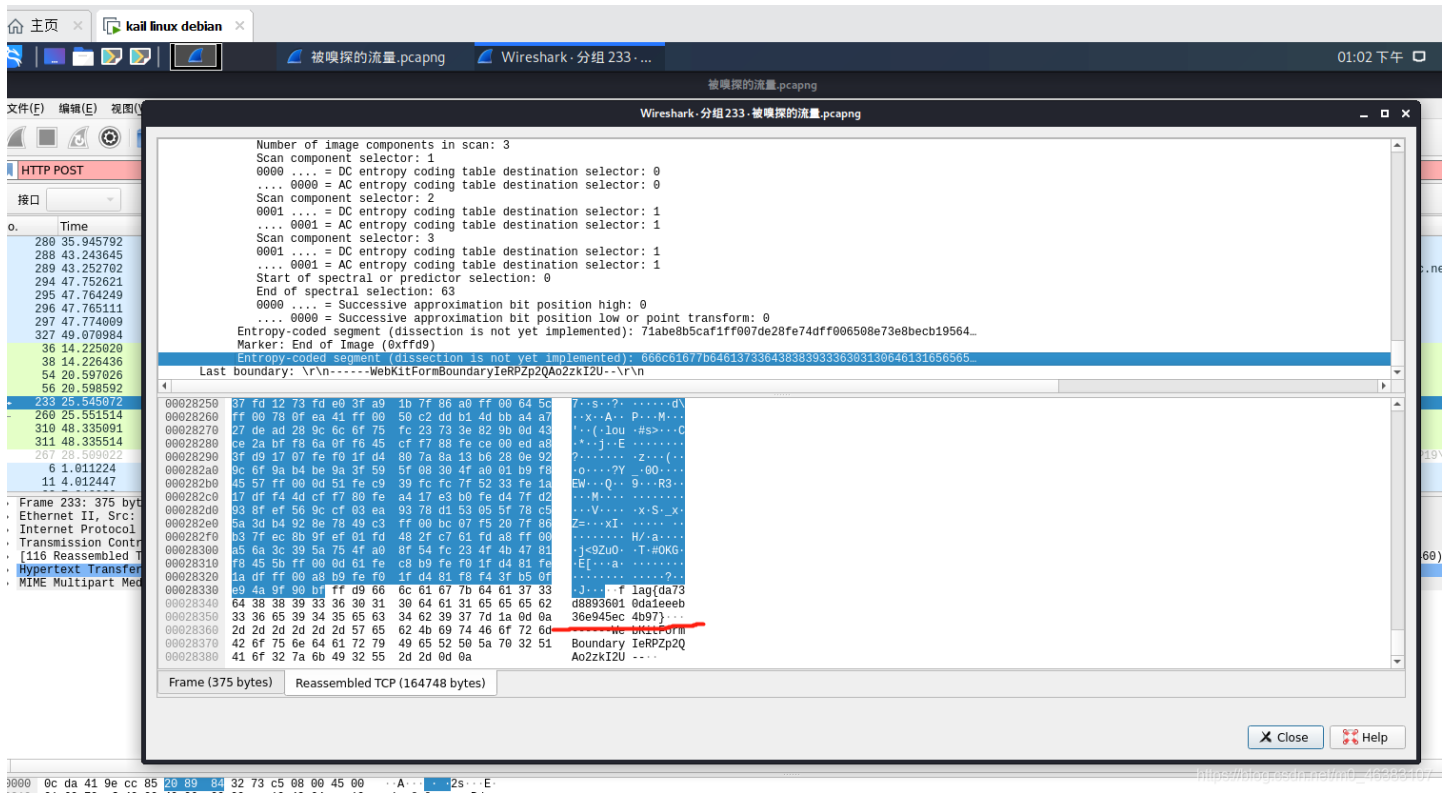
Apply a display filter: 表达式...

No.	Time	Source	Destination	Protocol	Length	Info
20	2.684925	192.168.1.102	115.231.236.116	HTTP	863	POST /user.php?action=login&do=login HTTP/1.1 (application/x-www-form-urlencoded)

> Frame 20: 863 bytes on wire (6904 bits), 863 bytes captured (6904 bits)
 > Ethernet II, Src: LiteonTe_8d:1f:98 (74:de:2b:8d:1f:98), Dst: Tp-LinkT_a6:82:df (80:89:17:a6:82:df)
 > Internet Protocol Version 4, Src: 192.168.1.102, Dst: 115.231.236.116
 > Transmission Control Protocol, Src Port: 22494, Dst Port: 80, Seq: 1, Ack: 1, Len: 809
 > Hypertext Transfer Protocol
 > HTML Form URL Encoded: application/x-www-form-urlencoded

https://blog.csdn.net/m0_46383111

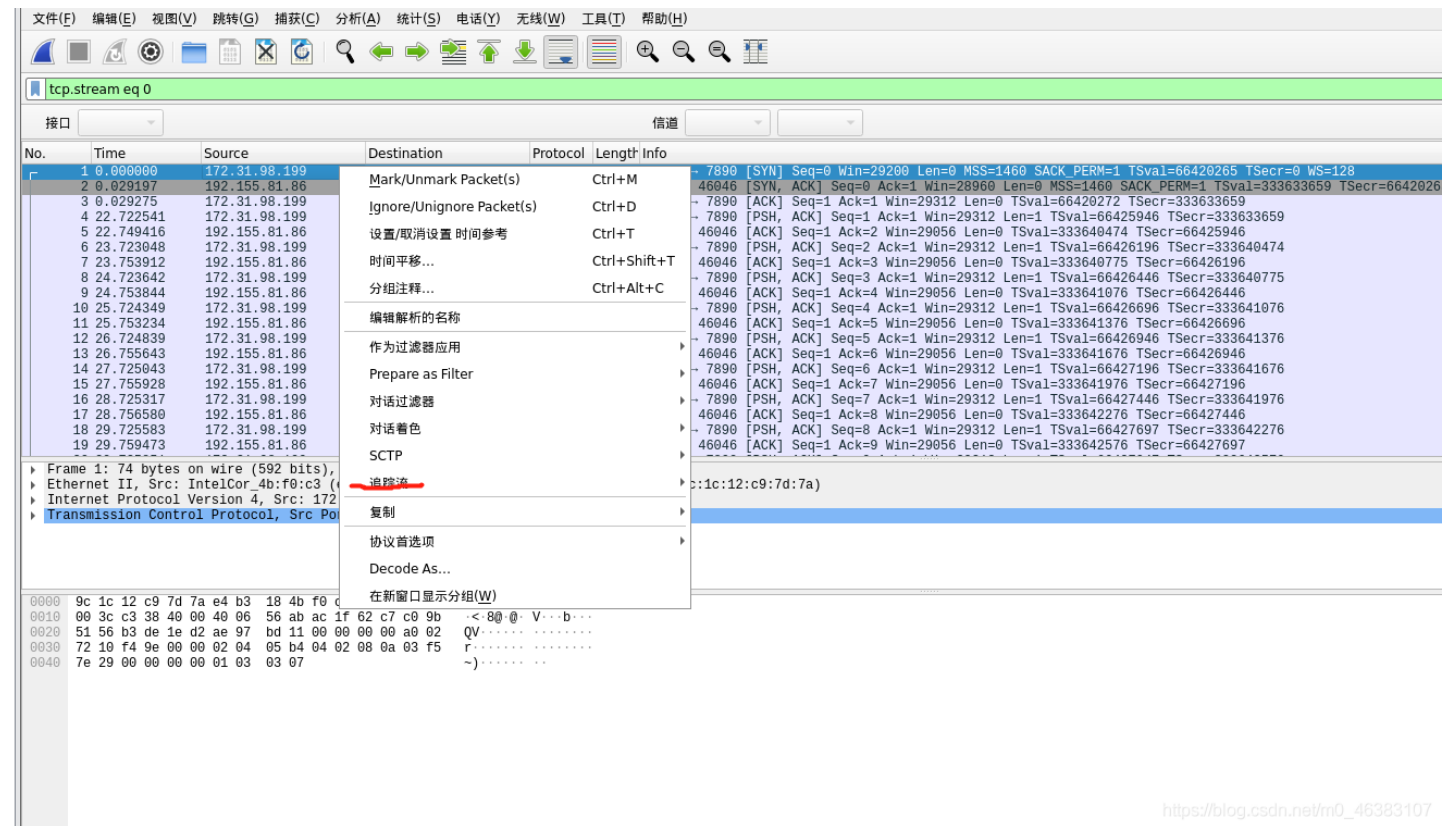
找到flag-value里面的数据就是flag



easycap

下载后直接丢到wireshark里面

看第一个的追踪流直接出flag



https://blog.csdn.net/m0_46383107

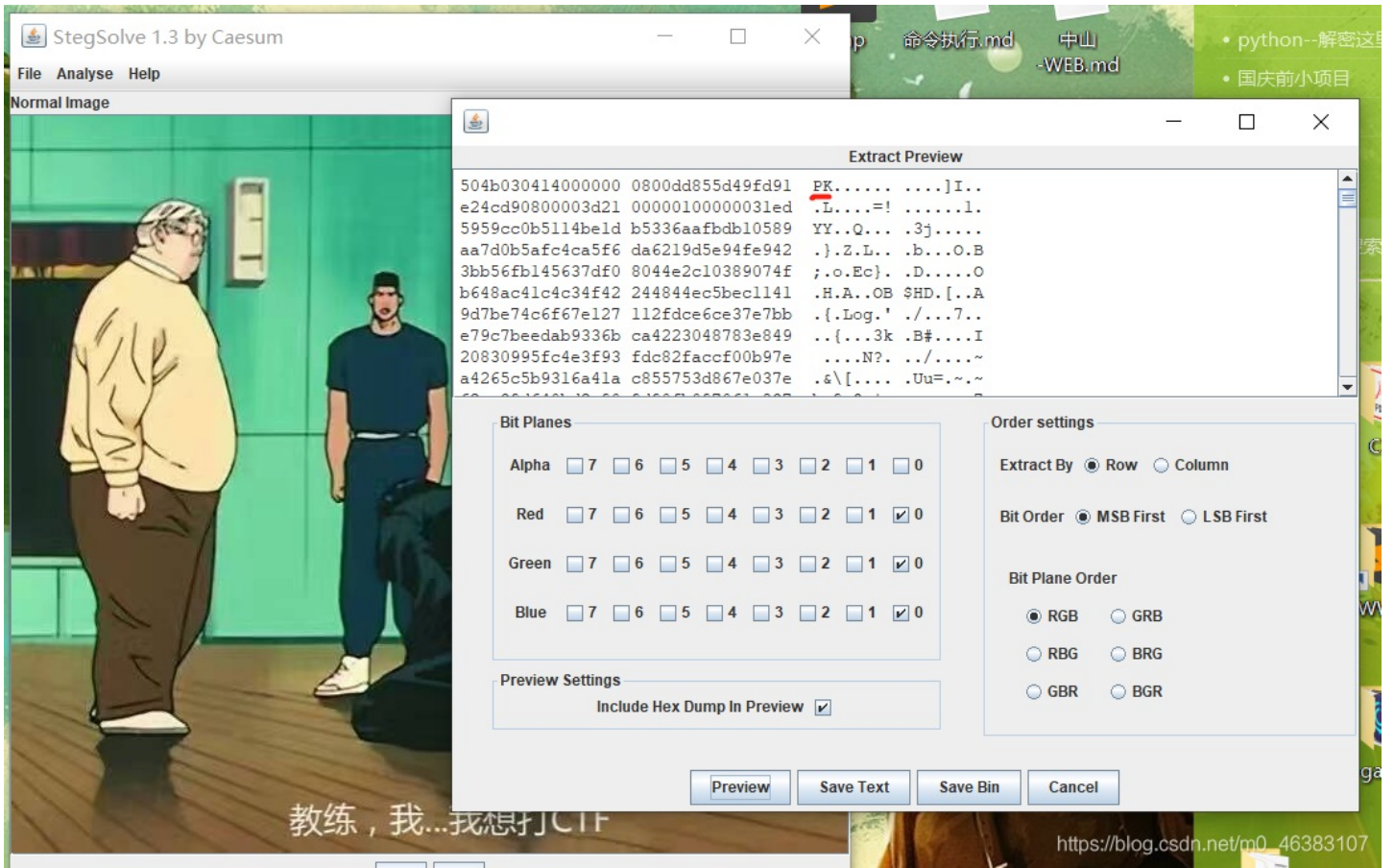
FLAG

下载后是这个图片



教练，我...我想打CTF

https://blog.csdn.net/m0_46383107



看到pk 用zip去解压

解压后丢进010editor

题目说的是hctf 所以去找hctf

```

起始页 1 x
编辑方式: 十六进制(H) 运行脚本 运行模板
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
04D0h: 89 C6 BF 40 10 60 00 FF E2 0F 1F 80 00 00 00 00 %Æ¿@.`.ÿâ..€....
04E0h: 80 3D 59 0B 20 00 00 75 11 55 48 89 E5 E8 7E FF €=Y. .u.UH%âè~ÿ
04F0h: FF FF 5D C6 05 46 0B 20 00 01 F3 C3 0F 1F 40 00 ÿÿ]Æ.F. .óÃ..@.
0500h: 48 83 3D 18 09 20 00 00 74 1E B8 00 00 00 00 48 Hf=.. .t.,....H
0510h: 85 C0 74 14 55 BF 20 0E 60 00 48 89 E5 FF D0 5D ...Àt.U¿ .`.H%áÿÐ]
0520h: E9 7B FF FF FF 0F 1F 00 E9 73 FF FF FF 55 48 89 é{ÿÿÿ...ésÿÿÿUH%
0530h: E5 BF D8 05 40 00 B8 00 00 00 00 E8 D0 FE FF FF å¿ø.@.,....èÐþÿÿ
0540h: 5D C3 66 2E 0F 1F 84 00 00 00 00 00 0F 1F 40 00 ]Ãf.....@.
0550h: 41 57 41 89 FF 41 56 49 89 F6 41 55 49 89 D5 41 AWA%ÿAVI%øAUI%øA
0560h: 54 4C 8D 25 A8 08 20 00 55 48 8D 2D A8 08 20 00 TL.%". .UH.-". .
0570h: 53 4C 29 E5 31 DB 48 C1 FD 03 48 83 EC 08 E8 5D SL)å1ÛHÁÿ.Hfì.è]
0580h: FE FF FF 48 85 ED 74 1E 0F 1F 84 00 00 00 00 00 þÿÿH...it.....
0590h: 4C 89 EA 4C 89 F6 44 89 FF 41 FF 14 DC 48 83 C3 L%êL%øD%ÿAY.ÛHfÃ
05A0h: 01 48 39 EB 75 EA 48 83 C4 08 5B 5D 41 5C 41 5D .H9ëuêHfÃ.[|A\A]
05B0h: 41 5E 41 5F C3 66 66 2E 0F 1F 84 00 00 00 00 00 A^A_Ãff.....
05C0h: F3 C3 00 00 48 83 EC 08 48 83 C4 08 C3 00 00 00 óÃ..Hfì.HfÃ.Ã...
05D0h: 01 00 02 00 00 00 00 00 68 63 74 66 7B 64 64 30 .....hctf{dd0
05E0h: 67 66 34 63 33 74 6F 6B 33 79 62 30 61 72 64 34 gf4c3tok3yb0ard4
05F0h: 67 34 31 6E 7E 7E 7E 7D 00 00 00 00 01 1B 03 3B g41n~~~}.....;
0600h: 30 00 00 00 05 00 00 00 04 FE FF FF 7C 00 00 00 0.....þÿÿ|...
0610h: 44 FE FF FF 4C 00 00 00 31 FF FF FF A4 00 00 00 DþÿÿL...lÿÿÿª...
0620h: 54 FF FF FF C4 00 00 00 C4 FF FF FF 0C 01 00 00 TÿÿÿÃ...Ãÿÿÿ....
0630h: 14 00 00 00 00 00 00 00 01 7A 52 00 01 78 10 01 .....zR..x..
0640h: 1B 0C 07 08 90 01 07 10 14 00 00 00 1C 00 00 00 .....
0650h: F0 FD FF FF 2A 00 00 00 00 00 00 00 00 00 00 00 øÿÿÿ*.....
0660h: 14 00 00 00 00 00 00 00 01 7A 52 00 01 78 10 01 .....zR..x..
0670h: 1B 0C 07 08 90 01 00 00 24 00 00 00 1C 00 00 00 .....$.
0680h: 80 FD FF FF 40 00 00 00 00 0E 10 46 0E 18 4A 0F eÿÿÿ@.....F...J.
0690h: 0B 77 08 80 00 3F 1A 3B 2A 33 24 22 00 00 00 00 .w.€.?.;*3$"....
06A0h: 1C 00 00 00 44 00 00 00 85 FE FF FF 15 00 00 00 ....D.....þÿÿ....
06B0h: 00 41 0E 10 86 02 43 0D 06 50 0C 07 08 00 00 00 .A..†.C..P.....
06C0h: 44 00 00 00 64 00 00 00 88 FE FF FF 65 00 00 00 D...d...^þÿÿe...
06D0h: 00 42 0E 10 8F 02 45 0E 18 8E 03 45 0E 20 8D 04 .B....E..Ž.E. .
06E0h: 45 0F 20 0C 05 40 0F 20 06 06 40 0F 20 02 07 4D E.(T.V.0†.V.0ç.M

```

另外一个世界

下载后是一张图片

丢进010里面 看到后面有101010这些二进制很可疑

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
2540h:	5A	34	F2	39	EE	47	0C	6F	D0	7E	DB	0E	4A	B6	AE	CD	Z4ò9iG.òÐ~Û.J¶@I
2550h:	53	80	95	00	42	F2	9F	0E	CA	DC	7A	0F	DB	6A	5E	27	se•.Bòÿ.ÊÛz.Ûj^!
2560h:	36	BE	CF	50	FE	1C	2B	83	DF	97	75	77	04	FF	00	EA	6¾iPp.+fß-uw.ÿ.é
2570h:	55	DC	3E	2A	AD	87	0F	0F	95	53	E4	91	26	97	D1	C2	UÛ>*+..•Sä`&-ÑÄ
2580h:	FF	00	E4	4E	D6	52	8B	AA	DA	BB	3D	6F	AB	F3	94	2C	ÿ.änÖR<^Û>=o«ó",
2590h:	47	BA	84	3F	F0	FB	B6	14	B5	1F	BF	AC	A1	46	48	E8	G°,?ðû¶.µ.¿-jFHè
25A0h:	D5	F4	AF	A0	13	F9	7B	FE	55	81	C3	C3	E5	41	CD	B3	õó~.ù{pU.ÄÄáÁí³
25B0h:	2A	47	12	4F	A1	0D	AA	84	80	36	BD	8F	02	AE	A2	F3	*G.Oj.ª.„€6½.„@çó
25C0h:	20	77	76	54	87	D0	B6	D7	2A	52	95	B6	AC	D2	09	C4	wvT+Ð¶×*R•¶-ò.Ä
25D0h:	A0	96	D7	99	1F	DA	BB	49	E3	E3	F3	AC	2F	D5	57	71	-x™.Û>Iääó-/õwç
25E0h:	F9	D3	7C	B3	40	71	4F	D1	C6	5D	F4	2D	B5	D4	94	A1	ùó ³@qOÑE]ô-µô"j
25F0h:	BD	AF	64	80	91	21	3D	1A	B3	3C	3C	2B	A1	6E	1E	EE	½~de(')!.=.ª<<+jn.î
2600h:	5C	EE	AE	EE	33	B2	AE	AE	9B	B9	79	0E	B8	E1	71	A0	\i@i3²@®>¹ÿ.ág
2610h:	40	21	46	78	F7	D5	A0	FE	F0	79	E7	51	35	FB	F5	7E	@!F×-õ pðÿçQ5ûó.
2620h:	48	F8	0A	59	E4	94	BB	1A	29	30	31	31	30	31	30	31	Hø.Yä"».)0110101
2630h:	31	30	31	31	30	31	31	31	31	30	31	31	30	30	31	30	1011011110110010
2640h:	31	30	31	31	30	31	30	31	31	30	31	31	30	31	30	31	1011010110110101
2650h:	30	30	30	31	31	30	30	31	31	30	31	31	31	30	30	31	0001100110111001
2660h:	31	2E	00	00	00												1....

https://blog.csdn.net/m0_46383107

去这个网站解密<http://ctf.ssleye.com/jinzhi.html>

ASCII与2进制、10进制和16进制之间相互转; 2进制、8进制、10进制、16进制及任意进制相互转换

ASCII = 进制 进制转换 (常用) 进制转换 (任意) ●

文本 koekj3s

清空

二进制 01101011 01101111 01100101 01101011 01101010 00110011 01110011

https://blog.csdn.net/m0_46383107

得到的结果加上flag{koekj3s}

假如给我三天光明



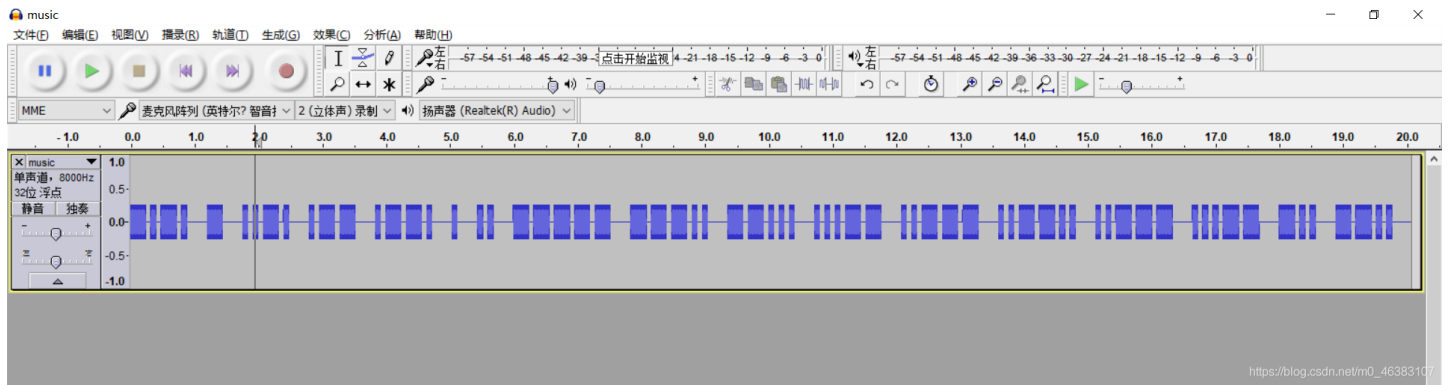
有两个东西 zip是加密文件，应该是要用jpg去找到密码

在图片下面有黑点（盲文）

对比解密后是kmdonowg

里面是音频

用Audacity打开



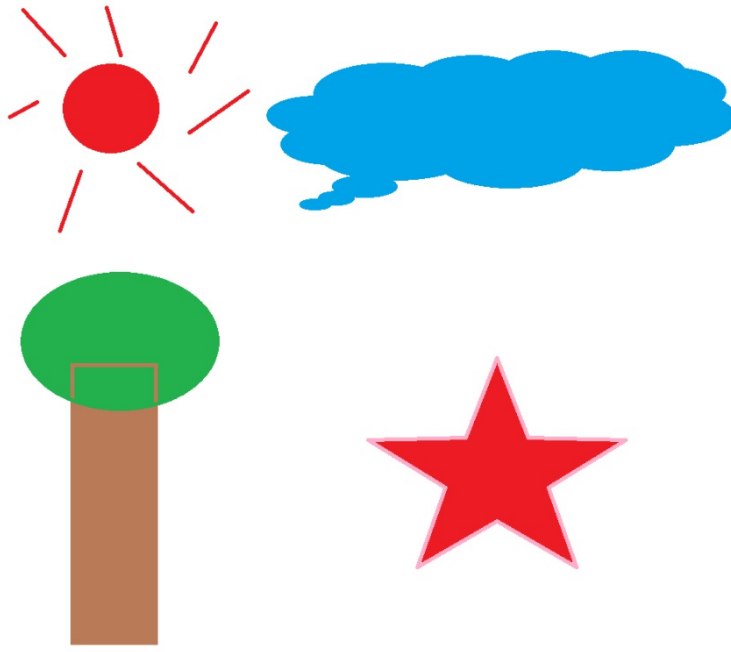
看出来是摩斯密码

.....- - - - -

去解密得到的可能是大写字母 最后要改一下

flag{wpei08732?23dz}

[A_Beautiful_Picture](#)

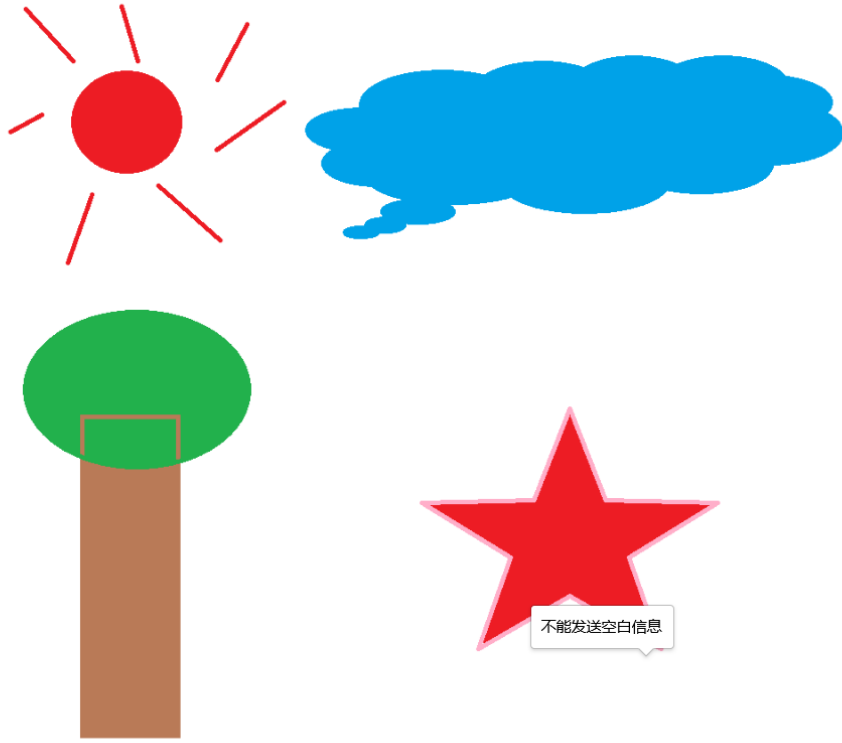


https://blog.csdn.net/m0_46383107

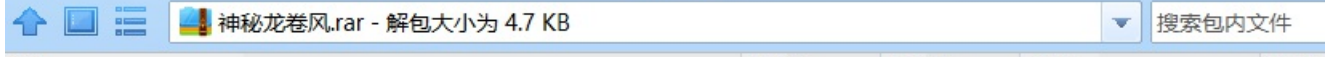
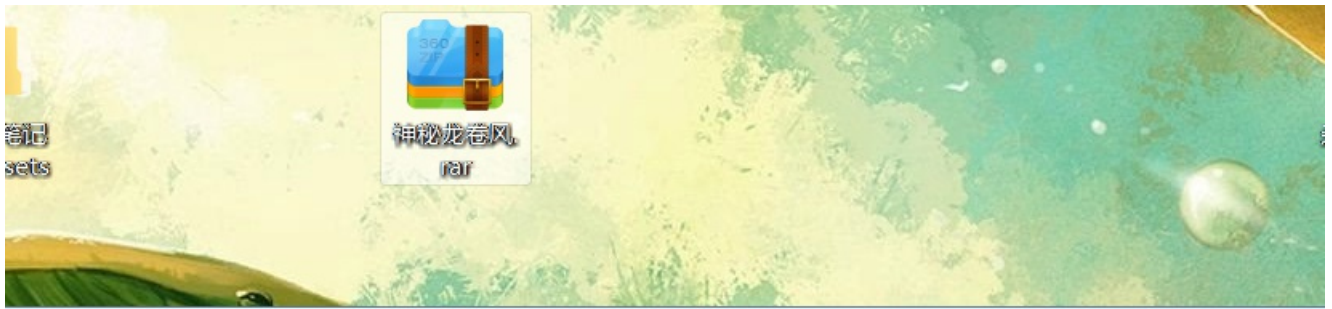
看上去没什么东西，可能长度有点问题，尝试去修改一下，改成长宽一样就出来flag

```

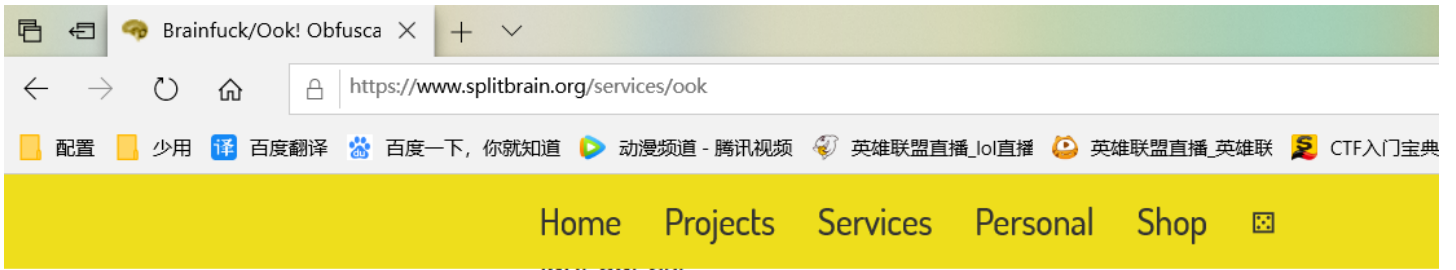
Misc_A_Beautiful_Picture_DreamerJack.png
编辑方式: 十六进制(H) 运行脚本 运行模板: PNG.bt
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0000h: 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 %PNG.....IHDR
0010h: 00 00 03 E8 00 00 03 E8 08 02 00 00 00 00 C2 C1 43 ...è.è.....ÂÁC
0020h: B3 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00 s....sRGB.@î.é...
0030h: 00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00 ..gAMA..±..üa...
0040h: 00 09 70 48 59 73 00 00 0E C3 00 00 0E C3 01 C7 ..pHYs...Ï...Ï.Ç
0050h: 6F A8 64 00 00 43 F2 49 44 41 54 78 5E ED DD 3D o'd..CòIDATx^íÝ=
0060h: AC 5B E9 79 E0 F1 91 DB 74 6E B6 4A 15 C9 85 31 -[éyàñ`Ûtn¶J.É...1
0070h: 75 16 D0 F4 06 34 83 2C 26 4D 60 60 B1 70 27 21 u.Đô.4f, &M` `±p'!
0080h: CD CE 34 AE EC D2 AE DC 48 69 02 A9 0B 16 01 0C íî4@ìò@ÛHi.©....
0090h: 37 6B 64 61 09 70 2F 01 D9 7A 30 C5 DC BB 55 AA 7kda.p/.Ùz0ÅÛ»Uª
00A0h: 6D DC 6D 7D F7 90 3C BA E2 25 CF 7B 3E C8 F3 F1 mÛm}÷.<°â%î{>Èóñ
00B0h: 3E EF FB FB 61 90 A1 9C 91 C4 7B 3E C8 3F 1F BE >iûûa. ;æ`Ã{>È?..¼
00C0h: 87 7C 74 77 77 F7 19 00 00 90 B7 1F B5 FF 06 00 #|tww÷.....î.ÛÝ.6383107
00D0h: 00 32 26 DC 01 00 20 00 F1 0E 00 00 01 08 77 00 .2&Û...á...w.
    
```



BJD{PnG_He1ghT_1s_WR0ng}



名称	压缩前	压缩后	类型	修改E
.. (上级目录)			文件夹	
神秘龙卷风.txt *	4.7 KB	1 KB	文本文档	2015-



All the hard work (like actually understanding how those language and his Brainfuck interpreter in PHP

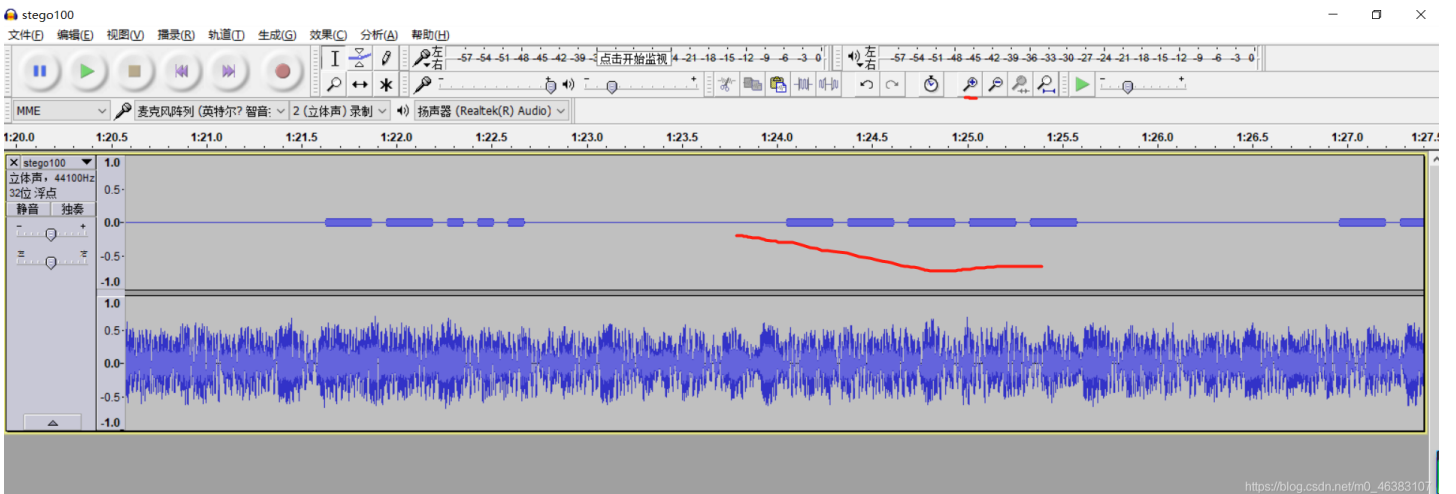
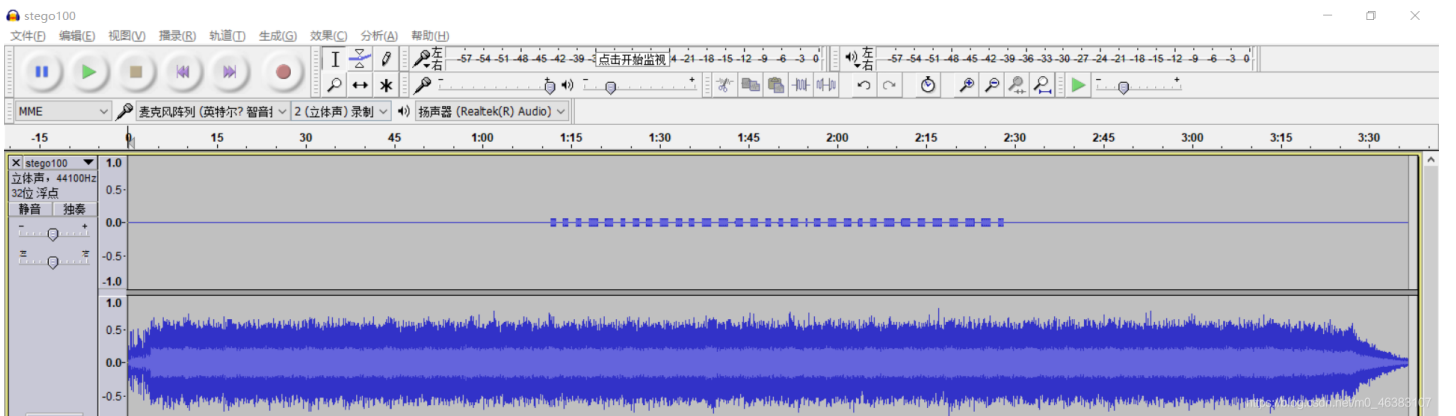
```
f1ag{e4bbef8bdf9743f8bf5b727a9f6332a8}
```

- Text to Ook!
- Text to short Ook!
- Ook! to Text
- Text to Brainfuck
- Brainfuck to Text

https://blog.csdn.net/m0_46383107

来首歌吧

打开是一个音频



https://blog.csdn.net/m0_46383107

