CTF misc 风信子靶场

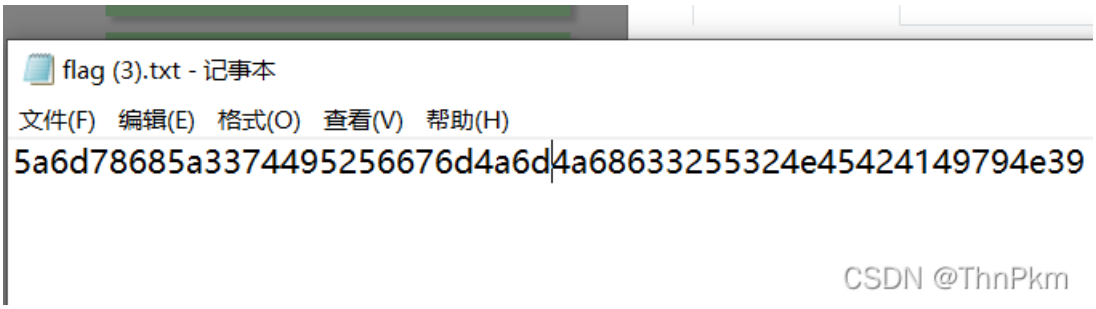
原创

ThnPkm 于 2021-12-09 13:02:52 发布 2557 收藏
分类专栏： 刷题 wp 文章标签： wpf linq gnu web安全 安全

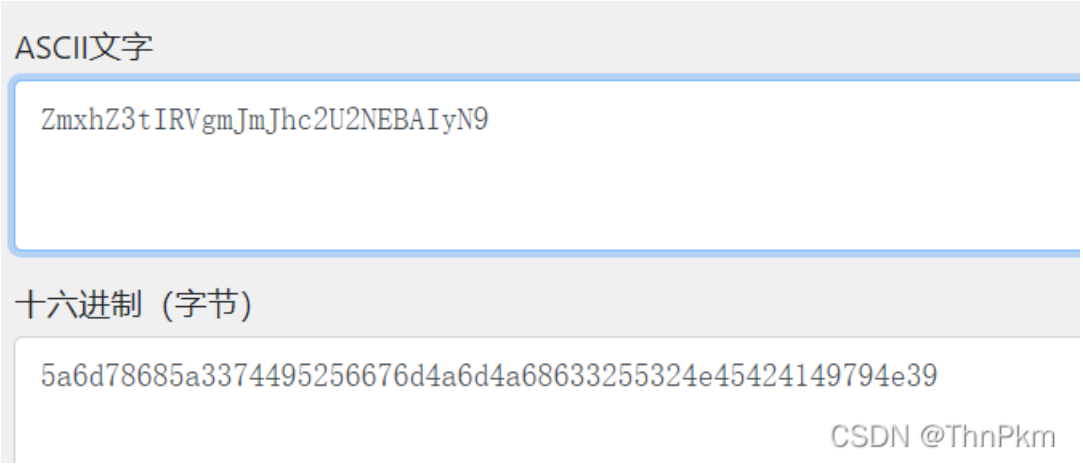
回顾一下写过的misc，风信子靶场，梦开始的地方

目录

1.简单的编码：



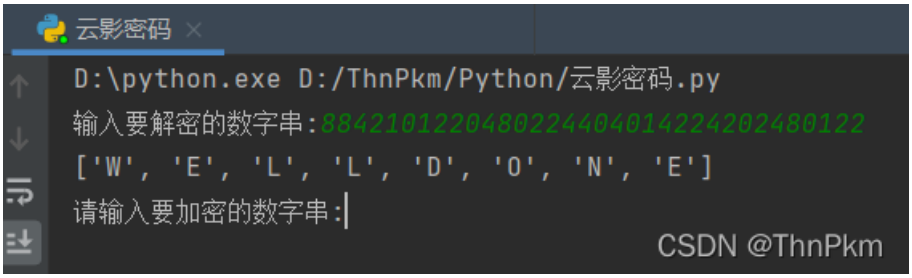
得到一堆像是16进制的编码，转ASCII码看看



Zmxh，再转base64

2.云影密码

题目是云影密码，所搜索一下云影密码，得到是用Python脚本来解密



得到flag

3.滴答滴答

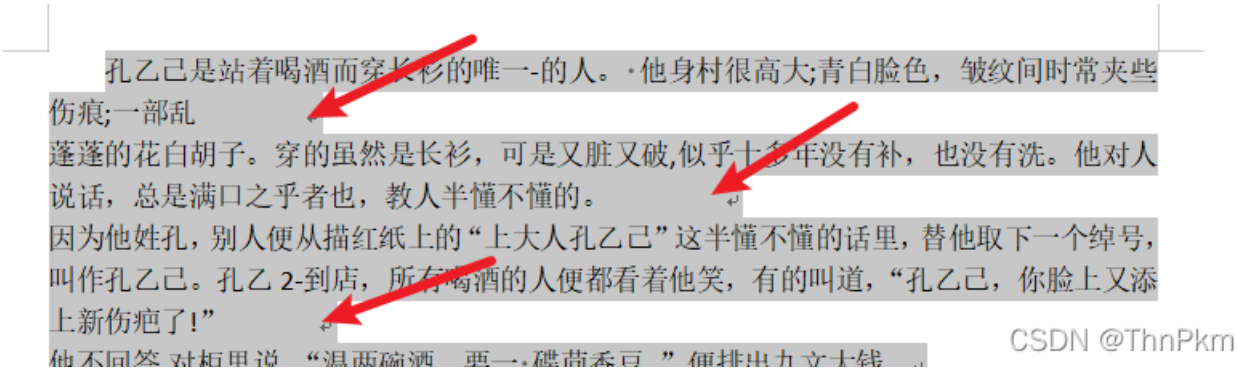
战场传来了一段这样的密文，请你把他解密出来，结果为大写字母，用flag{}包裹，

-- ----- .-. ..... .-. -... .-. ..... .- -.... . -

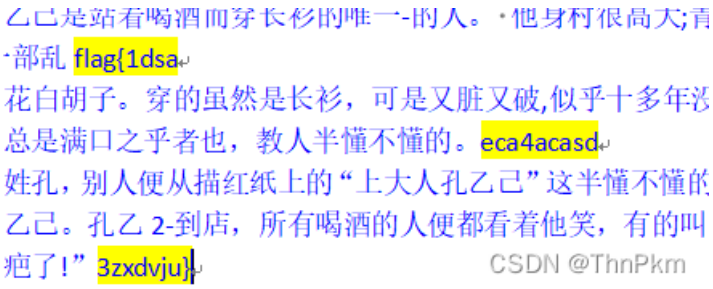
这个大家都晓得了，摩斯密码，转码后大写就是flag

4.孔乙己

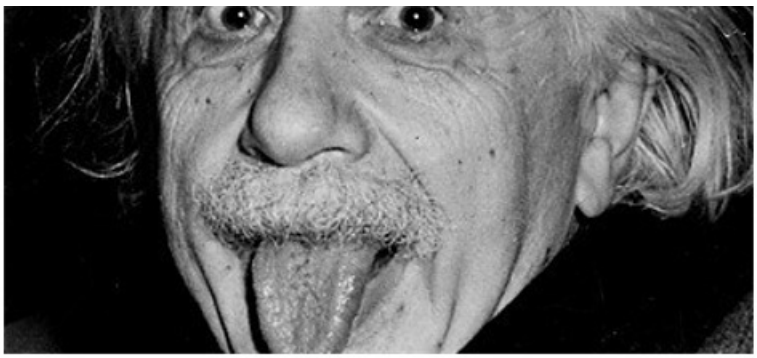
这题是word隐写


孔乙己是站着喝酒而穿长衫的唯一-的人。·他身材很高大;青白脸色，皱纹间时常夹些伤痕;一部乱
蓬蓬的花白胡子。穿的虽然是长衫，可是又脏又破,似乎十多年没有补，也没有洗。他对人说话，总是满口之乎者也，教人半懂不懂的。
因为他姓孔，别人便从描红纸上的“上大人孔乙己”这半懂不懂的话里，替他取下一个绰号，叫作孔乙己。孔乙 2-到店，所有喝酒的人便都看着他笑，有的叫道，“孔乙己，你脸上又添上新伤疤了!”
他不回答 对柜里说 “温两碗酒 要一·碟茴香豆 ”便排出九文大钱

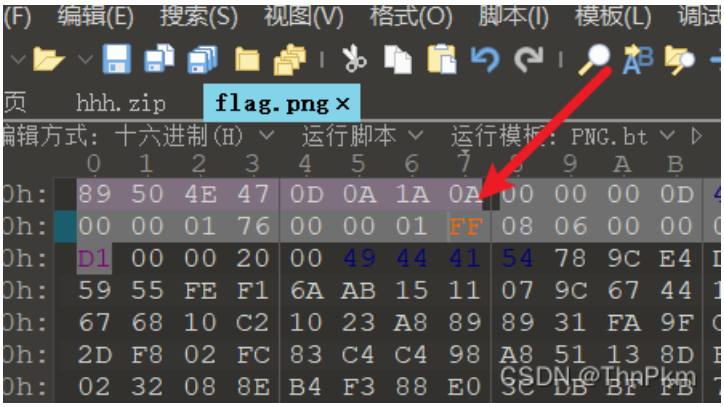
改变字体背景颜色


乙己是站着喝酒而穿长衫的唯一-的人。·他身材很高大;青
·部乱 flag{1dsa
花白胡子。穿的虽然是长衫，可是又脏又破,似乎十多年没
总是满口之乎者也，教人半懂不懂的。eca4acasd
姓孔，别人便从描红纸上的“上大人孔乙己”这半懂不懂的
乙己。孔乙 2-到店，所有喝酒的人便都看着他笑，有的叫
疤了!” 3zxdvju}

5.图片隐写1



是少了一截图片，010修改图片高度，这是第一次使用010印象很深

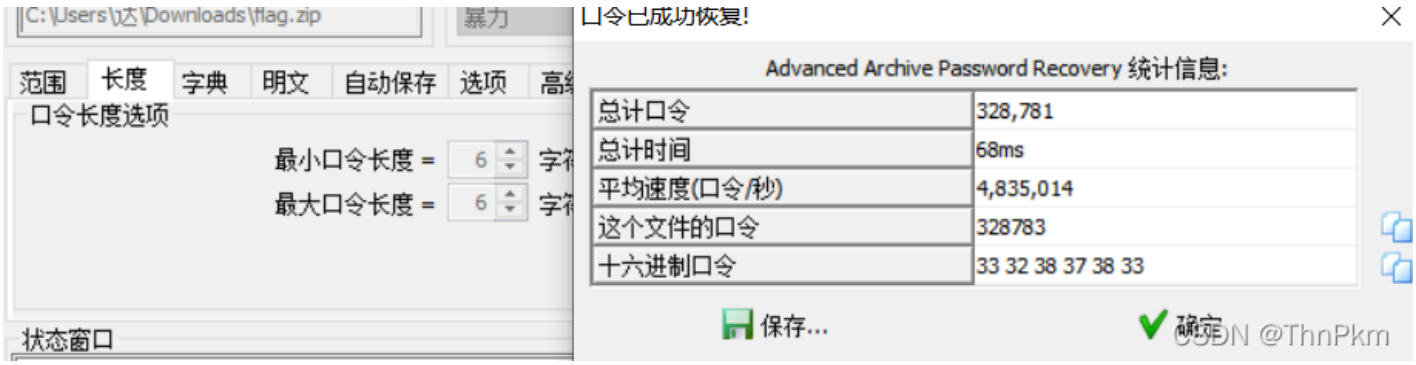


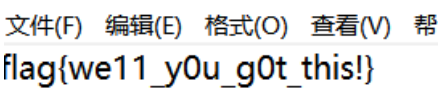
6.ZIP

这个压缩包加密了，听小明说密码好像是六位数的数字

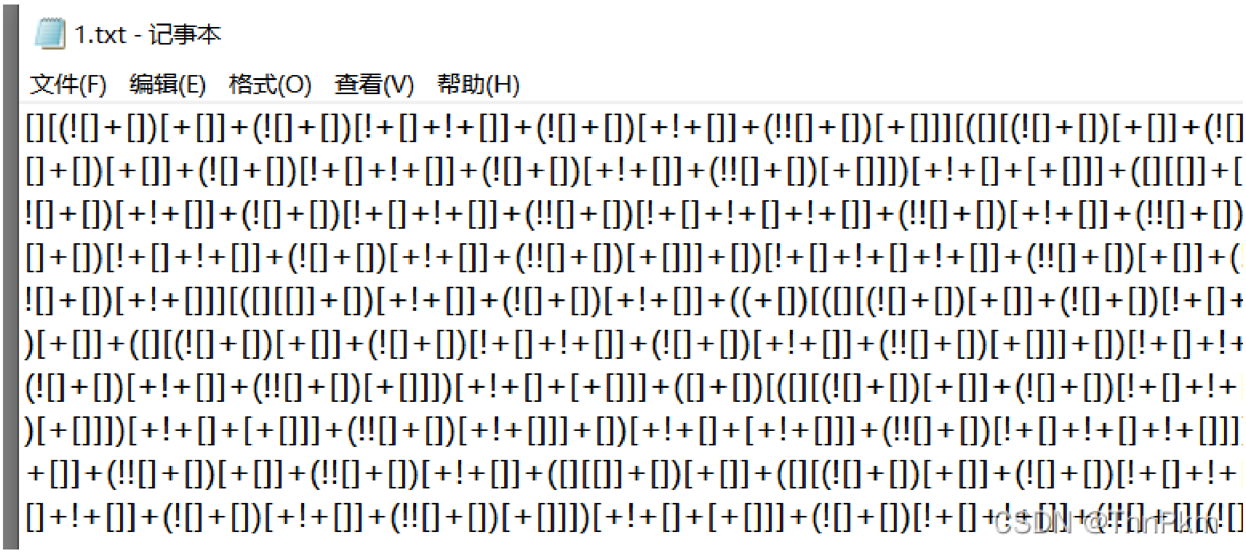
flag.zip

看来是爆破密码了，六位数字给的很贴心（爱了）

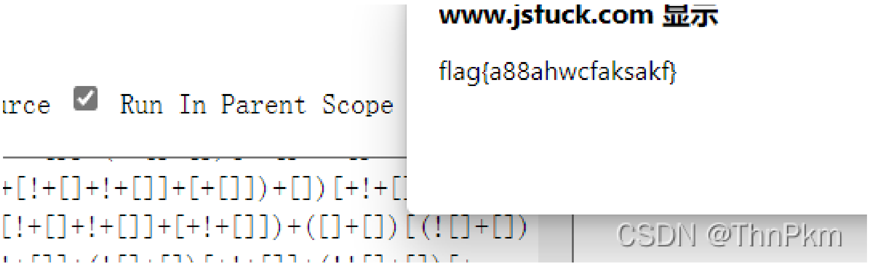




7.奇怪的编码

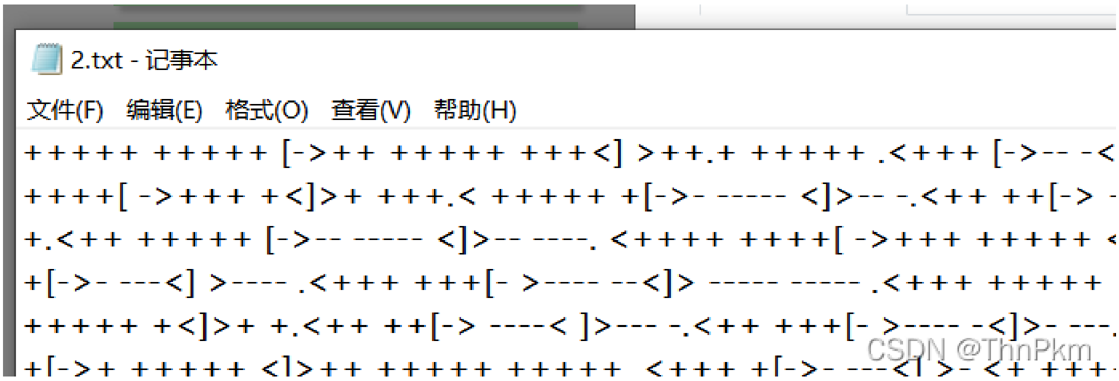


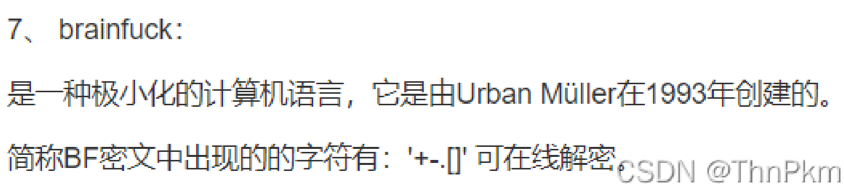
学长讲过的 jsfuck



解密平台JSFuck - Write any JavaScript with 6 Characters: []()!+

8.奇怪的编码2





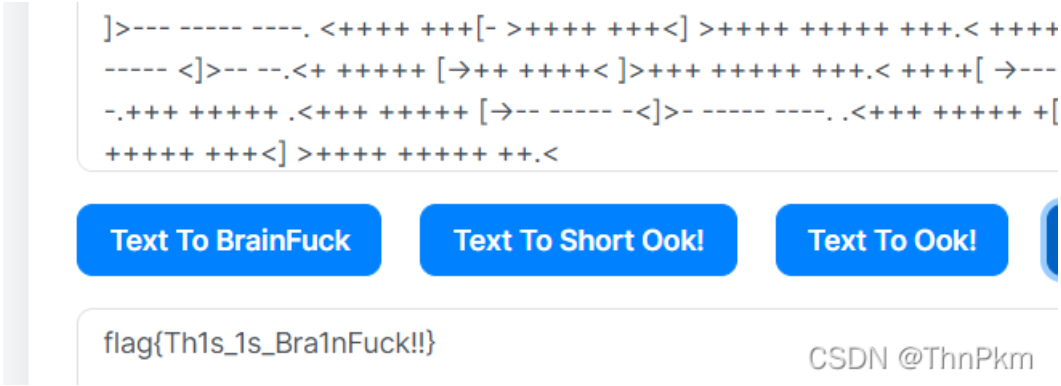
7、 brainfuck:

是一种极小化的计算机语言，它是由Urban Müller在1993年创建的。

简称BF密文中出现的的字符有：'+-.[]' 可在线解密。

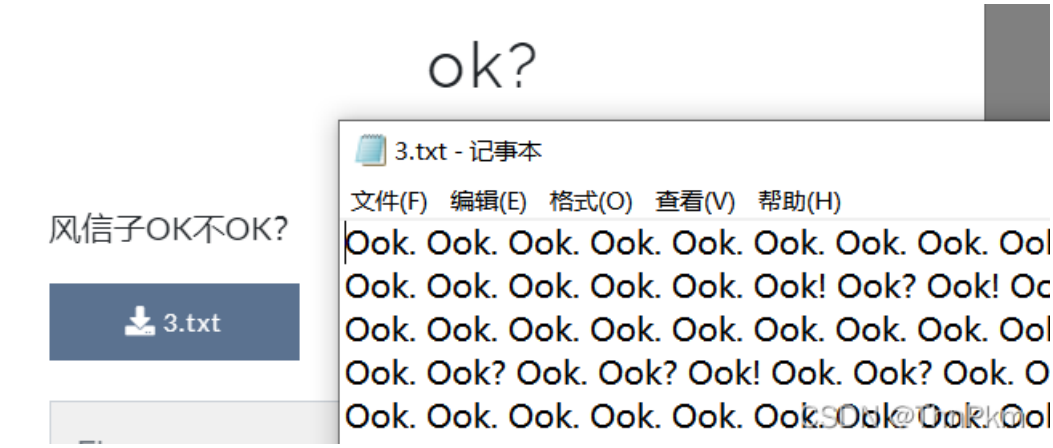
某种编码，去搜搜看

去试试

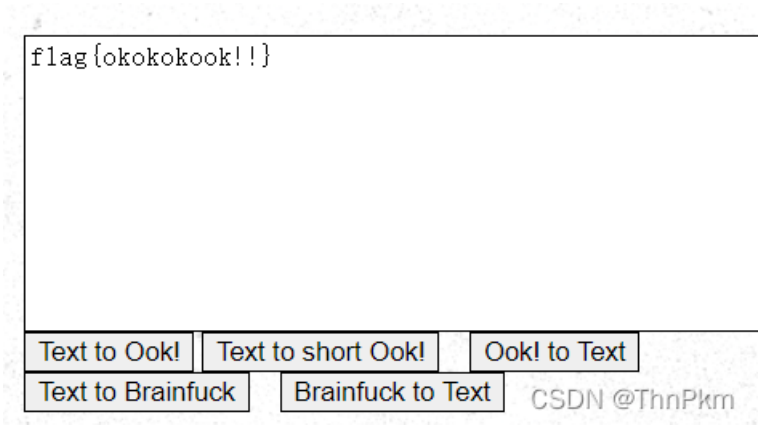


运气不错，解码平台Brainfuck/OoK加密解密 - Bugku CTF

9.ok?



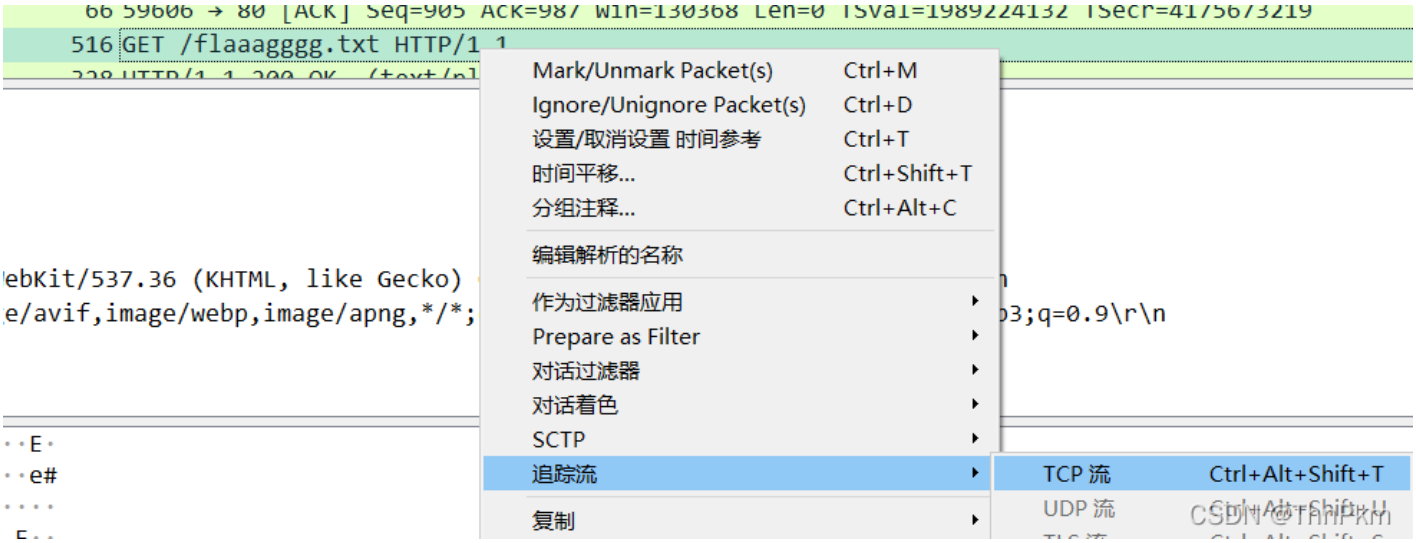
Ook编码，风信子必然ok啊



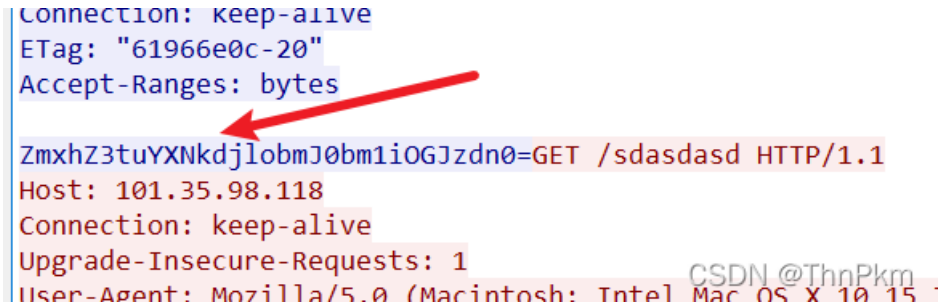
解码：Brainfuck/Ook! Obfuscation/Encoding [splitbrain.org]

10.流量包1

wireshark打开



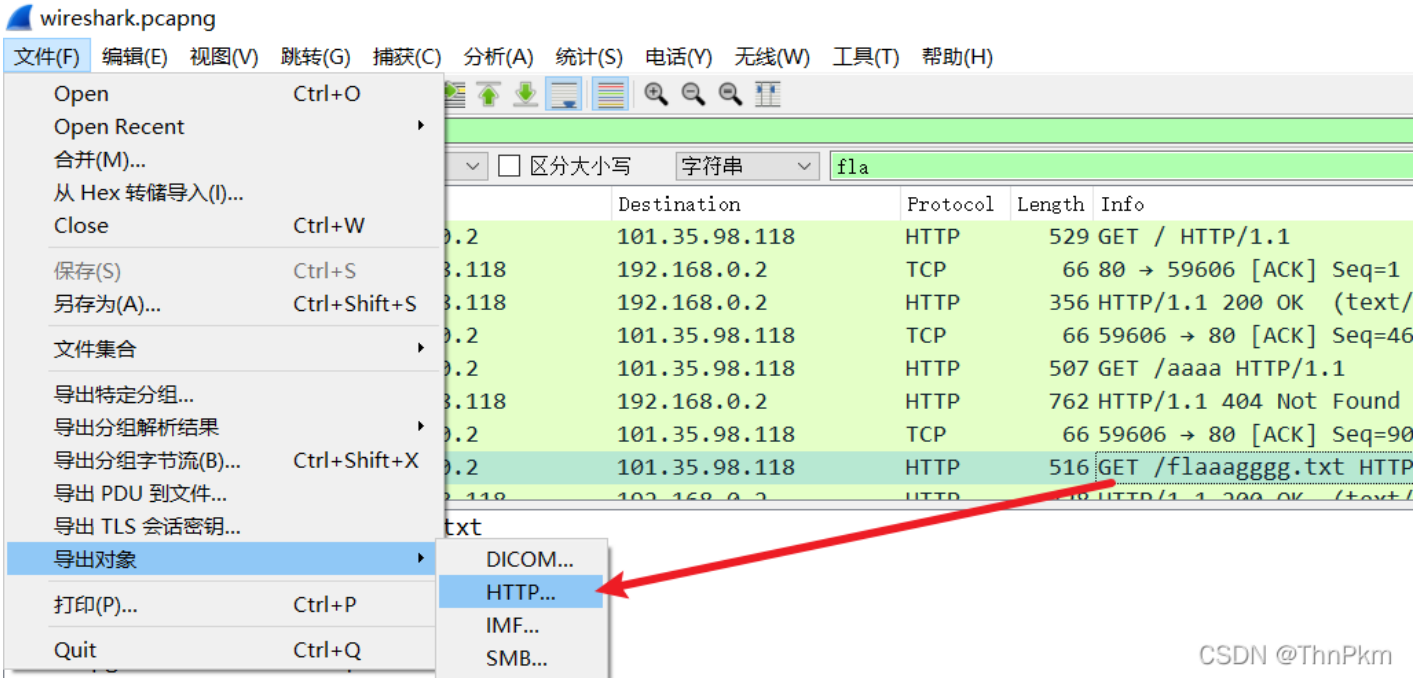
追踪流打开，里面的东西很多，找了一会看见base64了，



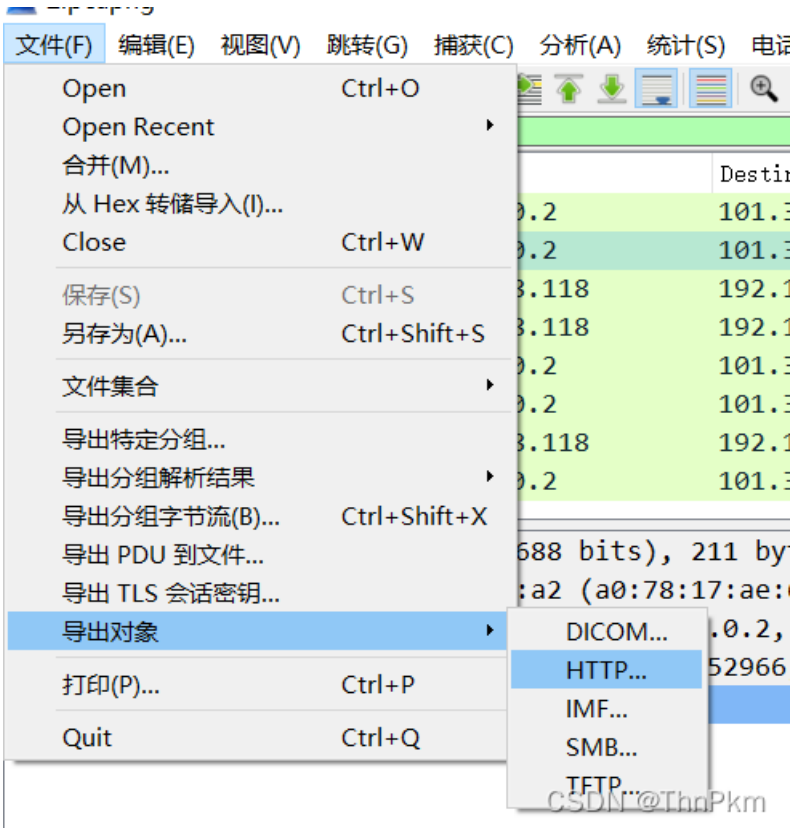
解码就是flag。

像我所说的追踪流里面的东西很多，靠眼神找，我还找错过，

有另外的方法更简洁



11.流量包2



导出对象 HTTP 意外发现了这个

分组	主机名	内容类型	大小	文件名
86	101.35.98.118	text/html	146 bytes	9
96	101.35.98.118	text/html	146 bytes	f
106	101.35.98.118	text/html	146 bytes	l
116	101.35.98.118	text/html	146 bytes	a
126	101.35.98.118	text/html	146 bytes	g
136	101.35.98.118	text/html	146 bytes	%7B
146	101.35.98.118	text/html	146 bytes	T
156	101.35.98.118	text/html	146 bytes	h
166	101.35.98.118	text/html	146 bytes	1
176	101.35.98.118	text/html	146 bytes	s
186	101.35.98.118	text/html	146 bytes	_
196	101.35.98.118	text/html	146 bytes	1
206	101.35.98.118	text/html	146 bytes	s
216	101.35.98.118	text/html	146 bytes	_
226	101.35.98.118	text/html	146 bytes	y
236	101.35.98.118	text/html	146 bytes	0
246	101.35.98.118	text/html	146 bytes	u
256	101.35.98.118	text/html	146 bytes	r

直接手打提交了

追踪tcp没搞懂怎么写

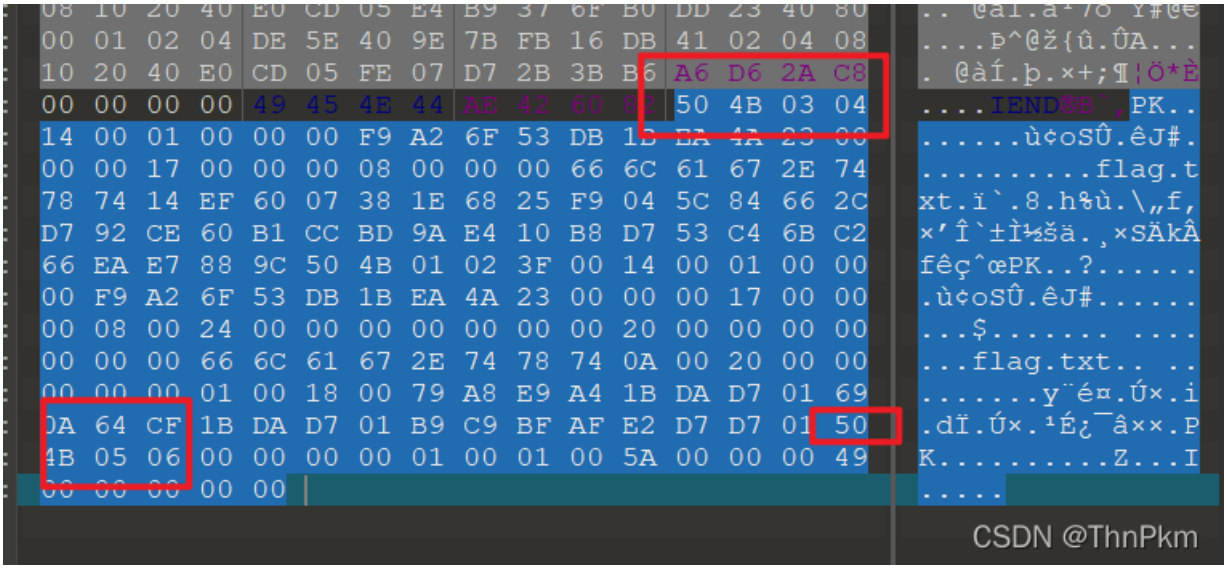
12.图片隐写2

提示png藏文件，所以去百度了怎么分离文件

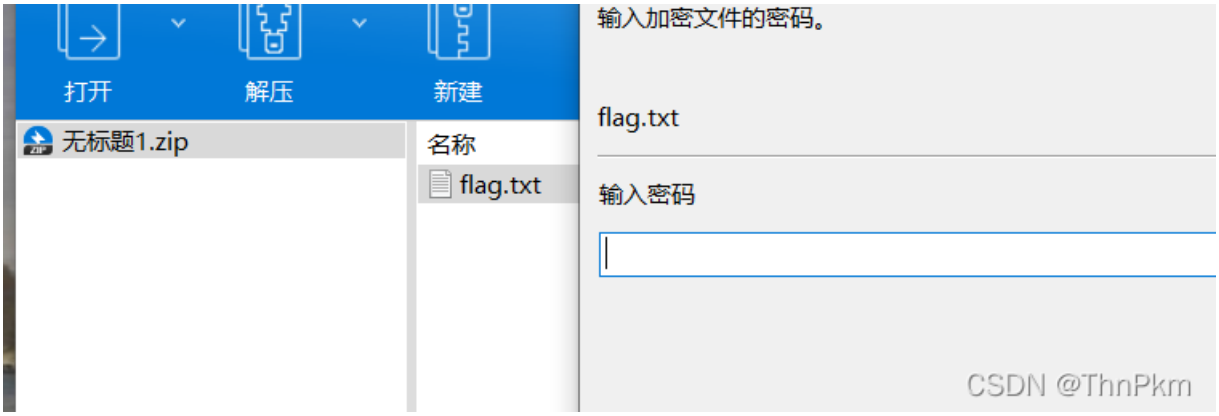
我用010来分离的

了解了文件头尾的相关16进制码

例如：ZIP　文件头：504B0304　　文件尾：50 4B



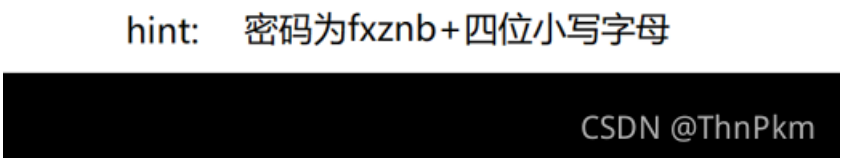
可以知道是藏了个zip，所以分离出来（选中右击后保存选择，写上zip后缀名就可以了）



得到一个加密txt，刚开始试了很久爆破，弄不出来

学长说有个细节没注意到，一直以为伪加密，最后给提示了，图片宽高还藏东西了

继续010修改高度得到



掩码爆破，fxznb？？？？ 就可以啦

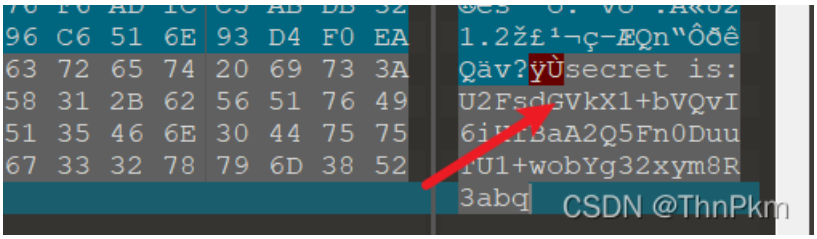
之前写了个用kali虚拟机 binwalk分离的方法，很详细

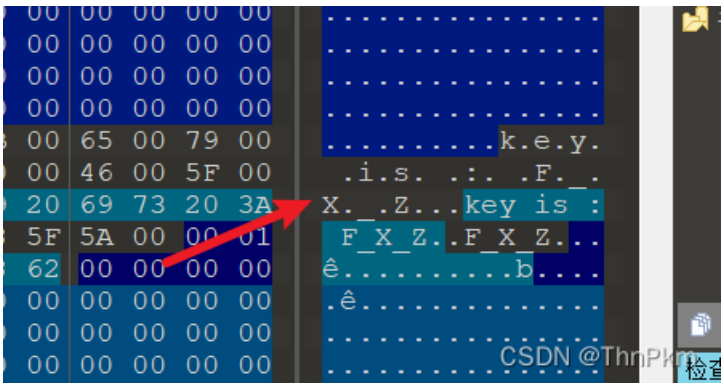
ctf kali虚拟机初体验_ThnPkm的博客-CSDN博客

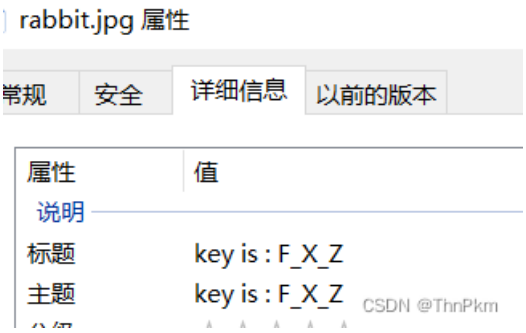
13.Rabbit!

给了一个jpg文件，010打开

发现些条件







secret，key，只要去解相应的编码就应该可以了

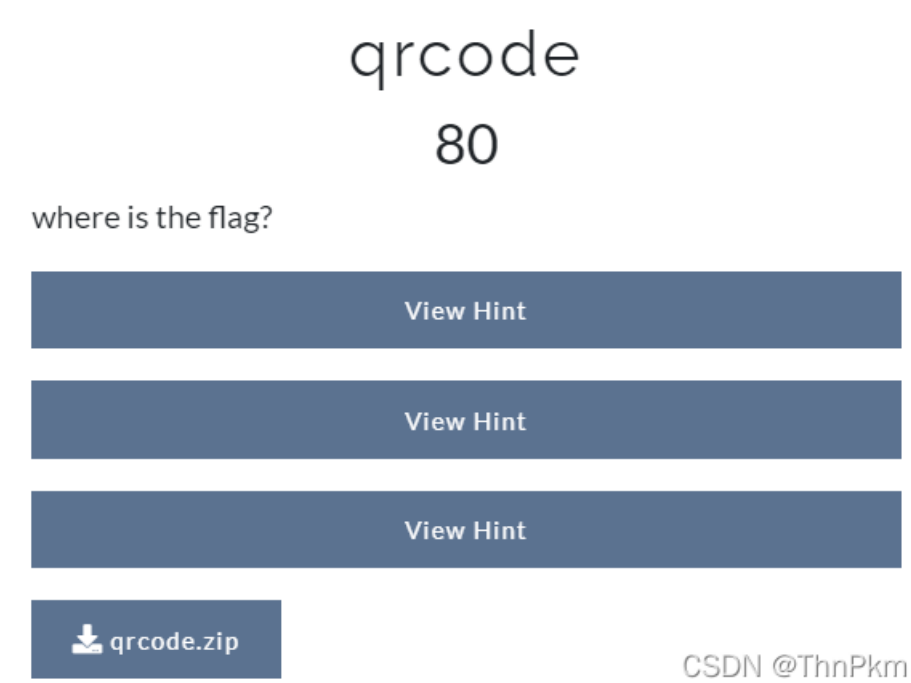
对应着编码样式找了找

> AES：
>
> 密码学中的高级加密标准（Advanced Encryption Standard，AES），又称Rijndael加密法，是美国联邦政府采用的一种区块加密标准。这个标准用来替代原先的DES，已经被多方分析且广为全世界所使用。做题过程中遇到过一个aes加密，题目给了提示，是AES加密。
>
> 密码样式：U2FsdGVkX1+qtU8KEGmMJwGgKcPUK3XBTdM+KhNRLHSCQL2nSXaW8++yBUkSylRp

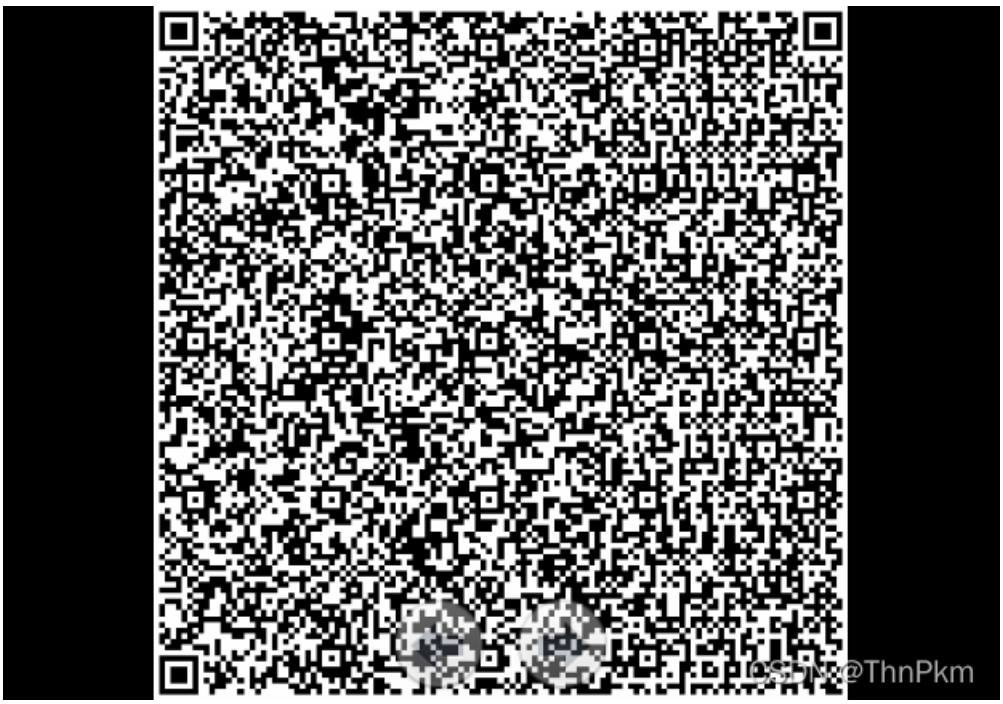
我一看这不就是AES加密吗，然后就去解码了，可惜怎么弄也弄不出来！！！

、最后还是学长给提示要看看题目标题，Rabbit

14.qrcode

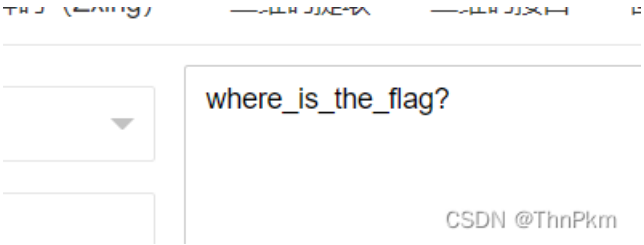


三个提示，不夸张（没有提示大概率全军覆没）



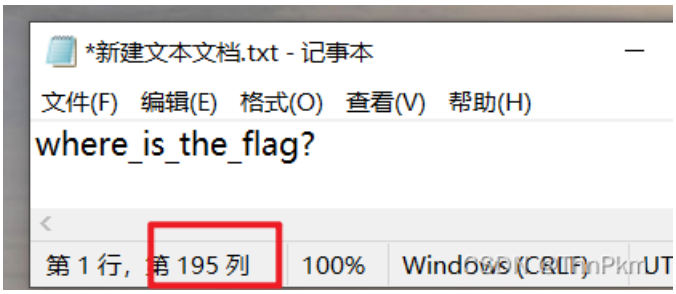
很夸张的二维码，竟然能扫出来

扫出来是这个



正规的思路是 这么密集的二维码怎么才扫出这么几个字

然后放到记事本里瞅瞅



可以看到是195列，说明很多东西我们看不到

Hint

0宽度字符隐写

0宽度字符隐写，学长直接给了，不给这个提示应该也没人会想到，大家都没什么经验

去搜0宽度字符解码，搜了一通终于找到个不错的网站

0宽度字符隐写

Original Text: Clear (length: 18)

where_is_the_flag?

Hidden Text: Clear (length: 22)

flag{zxv9023nvso390jf}

脑洞不小哦，没有提示的话我是不会注意那串where _ is_the _ flag ？

积累经验吧！

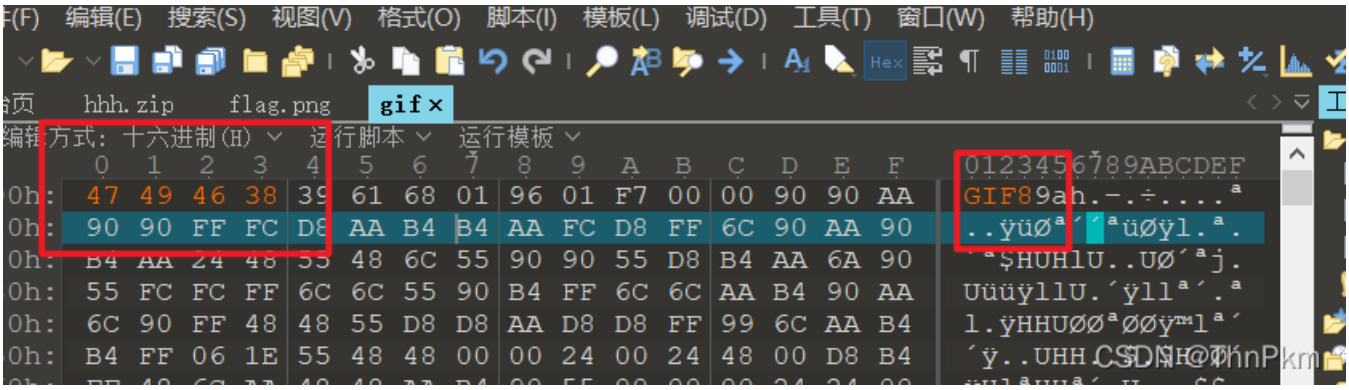
15.哥谭小丑

这题笑死我了，紧随时代潮流

也是放了提示，刚开始我以为还真没传上去呢...

这题比较简单了，gif文件头损坏，010修复一下就好

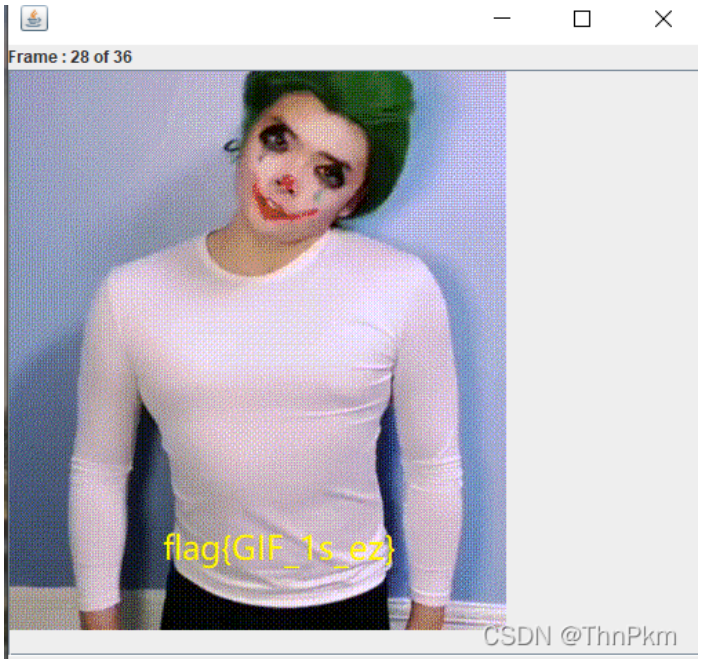
> GIF (gif)
>
> 文件头：47494638
>
> 文件尾：00 3B



修改后导出，保存选择，可以打开了

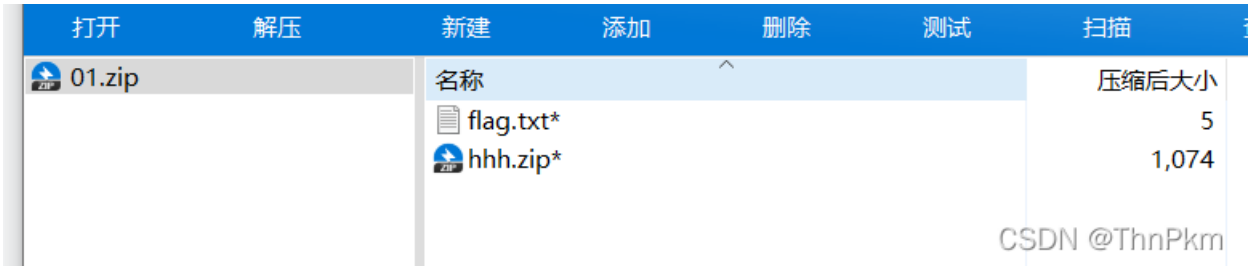

哥谭噩梦笑死了（变装瞬间好像有个flag出来）

放到stegslove里面frame逐帧查看

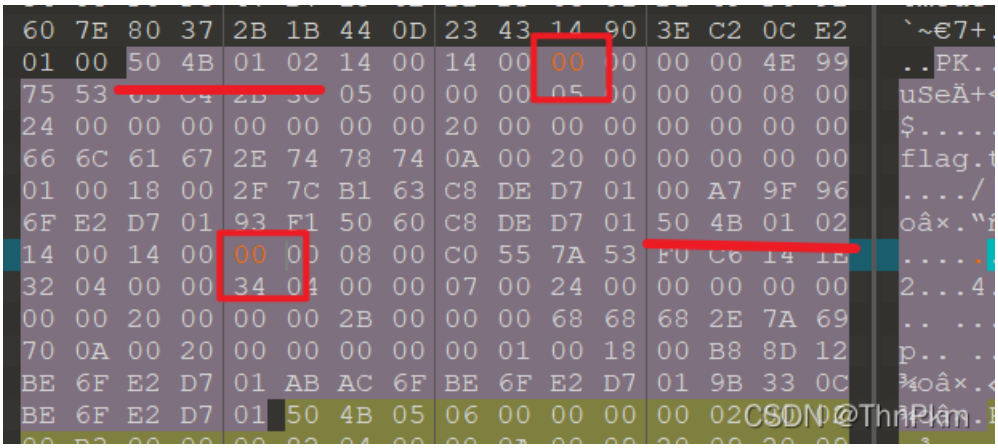


16.眼见为虚

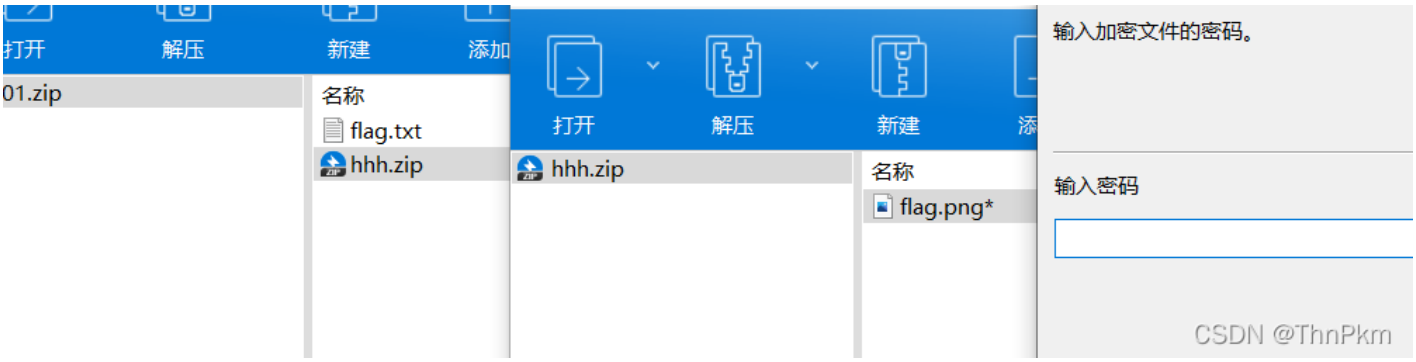
要了老命了，这题写了好几天



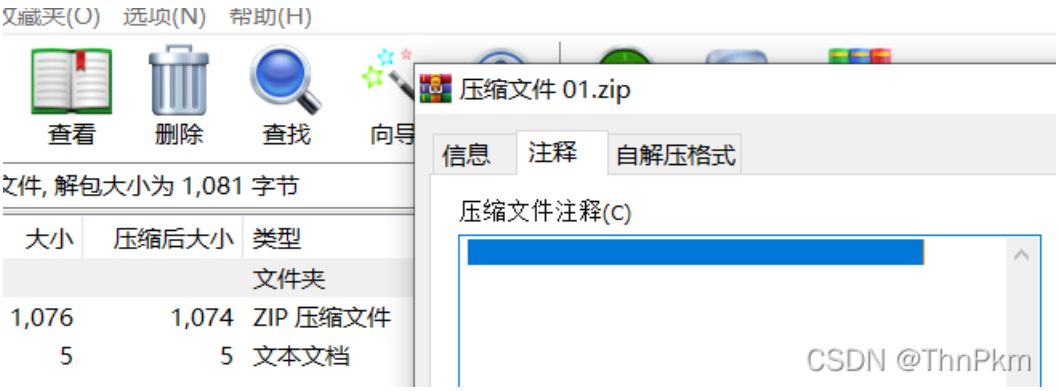
首先想到放进010看有没有隐藏文件，是不是伪加密，



两处伪加密，修复后 得到了flag.png，只要找到密码就行



给了提示看注释，bandzip还看不见，又去拿WinRAR看了



一堆空白，与txt里面blank相呼应，还以为有很大联系呢，其实blank没有用

把这堆空白放到了记事本里没看出啥东西

放到world里，知道了是由5个Tab和空格相间组成的

应该就是密码，然后放进去不行，懵啊

又去搜资料，可能是Tab与空格代表 - 和 . 组成摩斯密码？

可能是 ASCII码？ 试了 依然不行，试了很多

最后放弃了

最后知道了是代表01，阿西吧，就差一丢丢，不过证明我的思路还是正的

还好，写了好几天，看了很多wp，也积累了一些经验

感谢学长对我们的引导与帮助

这些misc题给了我们学习的机会，学长出的题确实对我们很友好，慢慢帮我们积累题型，今天重新写一遍又是不同感受，努力学习吧

以后也要多刷题，争取早日入门