DJBCTF MISC writeup(部分)

原创

时间大幻剧 于 2021-01-26 14:21:10 发布 208 收藏

分类专栏： CTF 文章标签： 信息安全

本文链接：https://blog.csdn.net/qq_43349910/article/details/113178051

目录

牛年大吉

十八般兵器

碑寺六十四卦

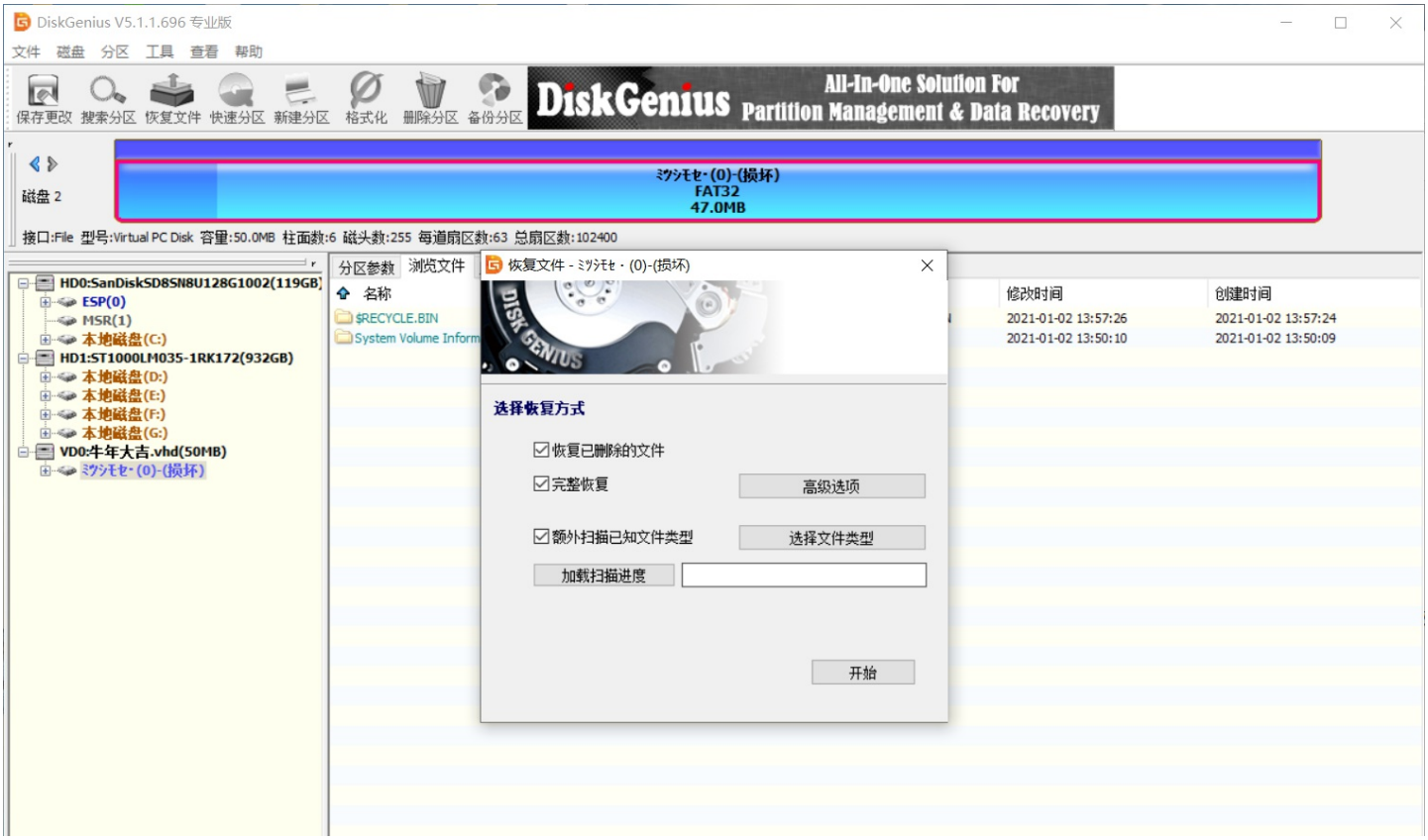
AA86

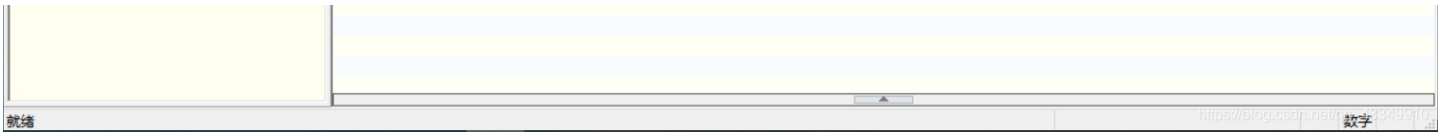
请问大吉杯的签到是在这里签吗

拼图v2.0

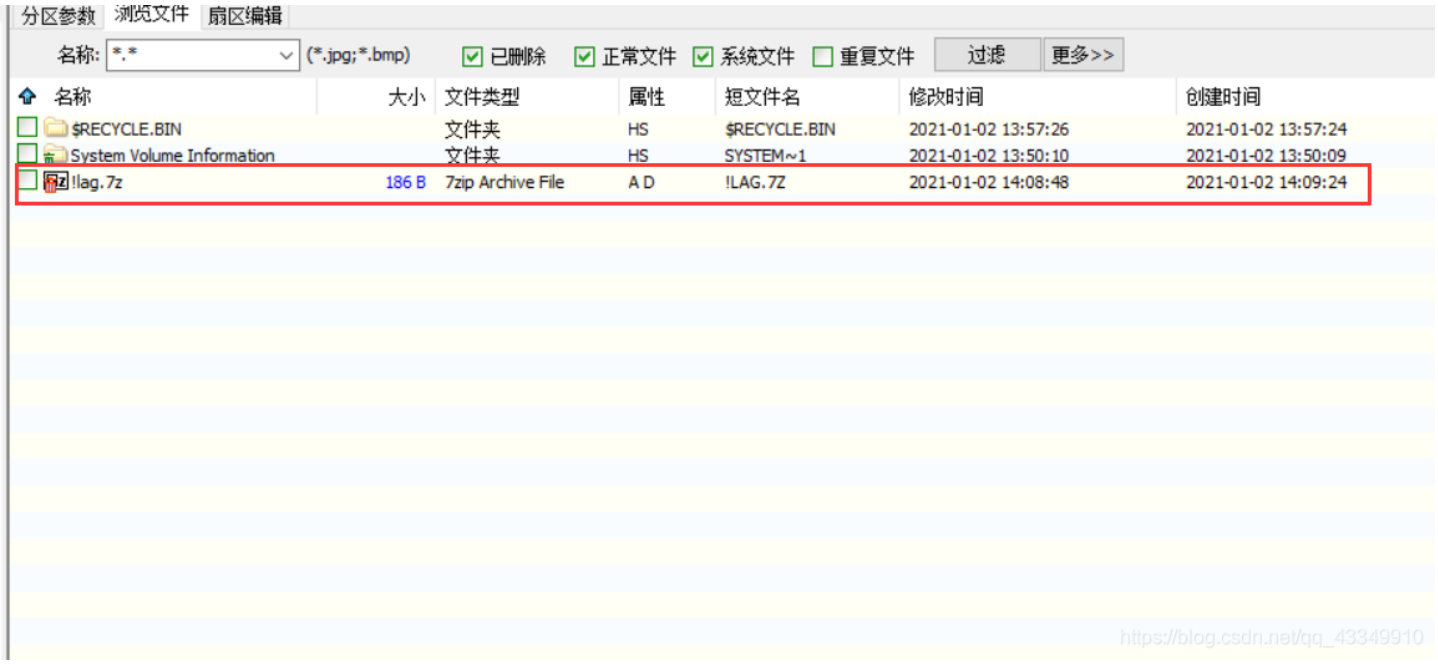
牛年大吉

首先下载下来一个vhd文件，是硬盘镜像文件，那就拖到DiskGenius恢复一下。





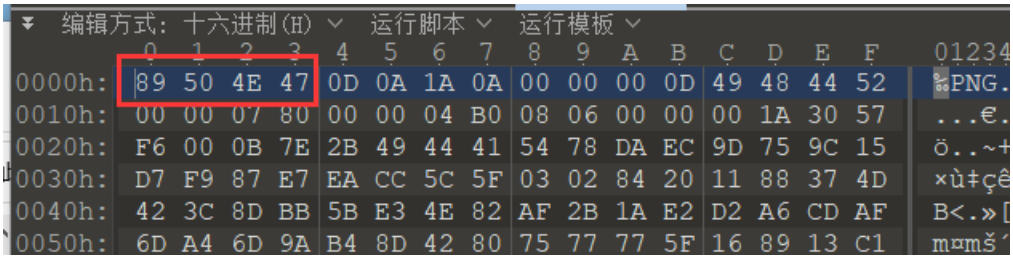
得到一个!lag.7z的文件。



翻阅一下里面的文件，还能找到一个png图片。

将两个文件都拿出来，打开压缩包，发现里面的文件是加密的，hint提示密码在文件头里（注意是文件头里，不是文件里头！）

然后拿png图片捣鼓了半天，最后发现密码真的就是PNG文件头。

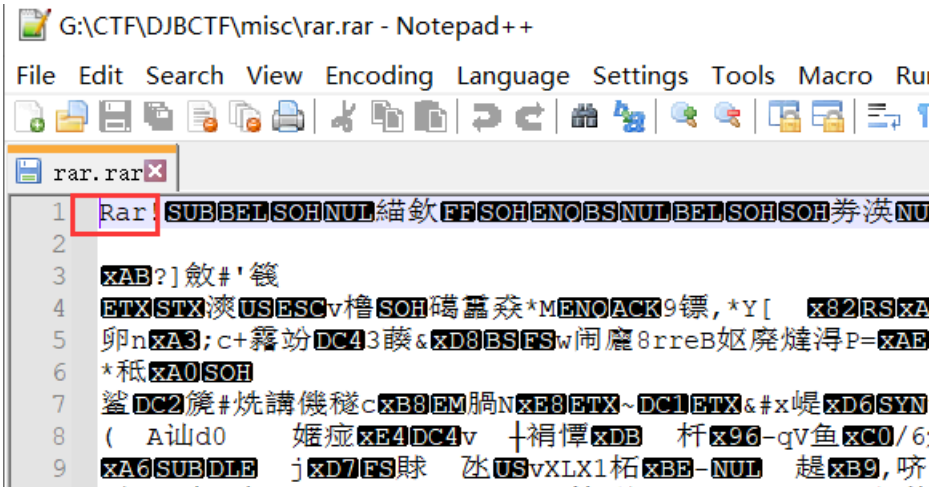


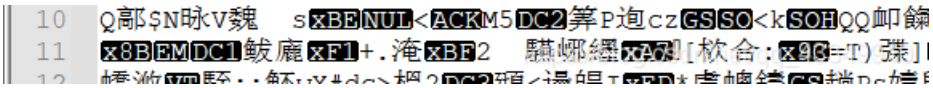
最后拿到flag。

flag{CTFshow_The_Year_of_the_Ox}

十八般兵器

这题首先下载到一个没有后缀名的文件，但是文件名是rar，用notepad++打开发现里面的头也是rar，说明这是一个rar压缩包，添加rar后缀。





打开压缩包后发现里的图片都是加密的，找了半天发现压缩包的注释就是密码（压缩包的注释很重要！）

根据hint JPHS，将所有的图片放到stegdetect.exe的目录下，使用命令

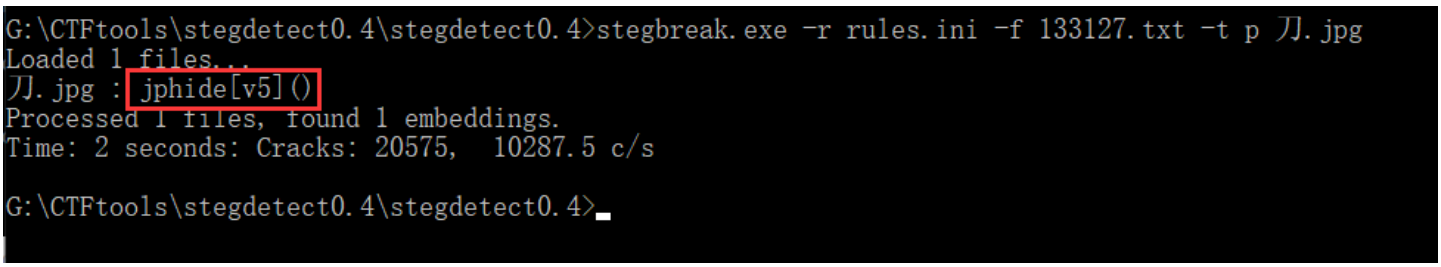
```
stegdetect.exe -tjopi -s 10.0 文件名
```

来判断文件什么加密

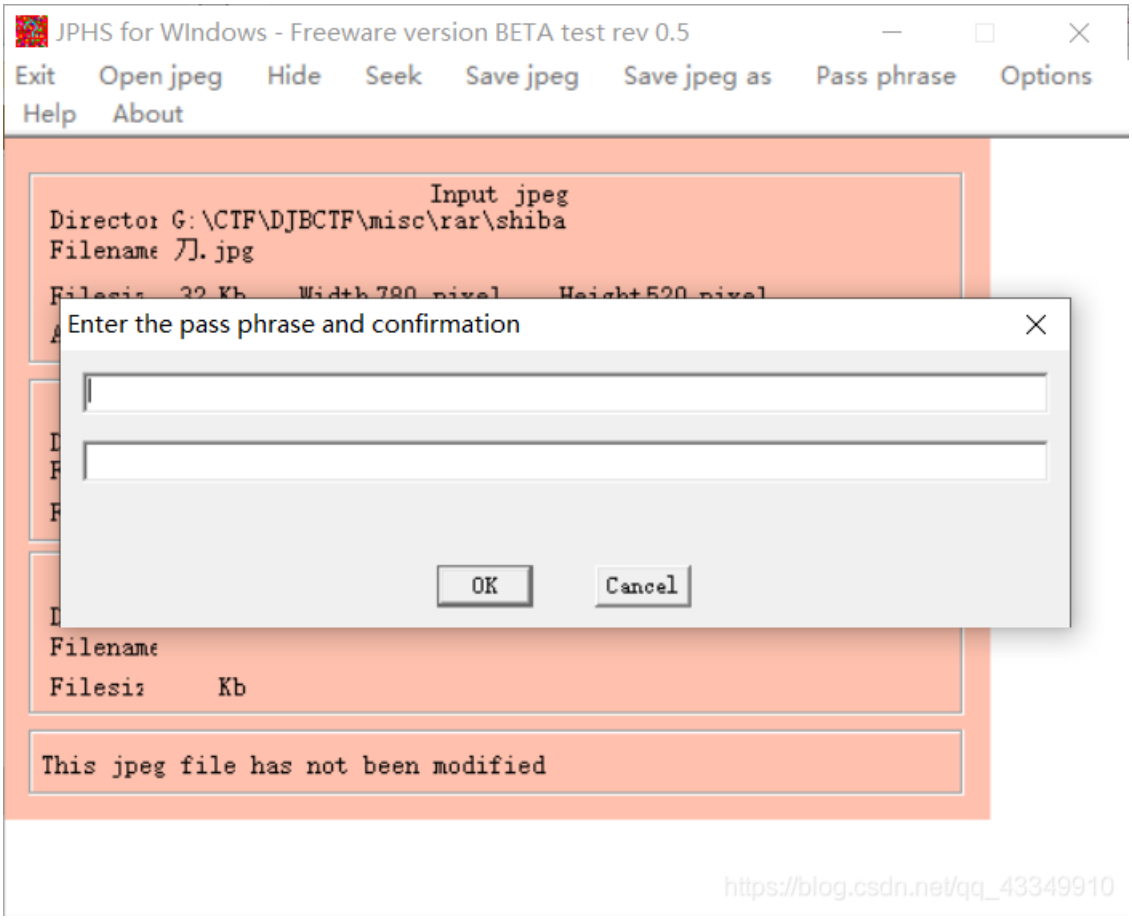
可以看到是jphide，接着用stegbreak.exe 来爆破密码。

```
stegbreak.exe -r rules.ini -f password.txt -t p 文件名
```

发现密码为空。



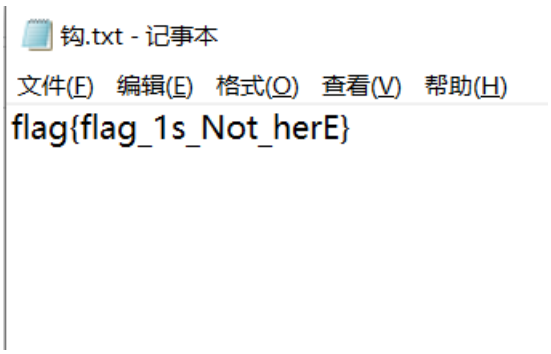
接着将所有的图片用jphswin.exe中的seek输入空密码，将里面的txt提取出来。



鞭.txt	2021/1/24 13:33	文本文档	1 KB
叉.txt	2021/1/24 13:33	文本文档	1 KB
锤.txt	2021/1/24 13:34	文本文档	1 KB
刀.txt	2021/1/24 13:30	文本文档	1 KB
斧.txt	2021/1/24 13:32	文本文档	1 KB
戈.txt	2021/1/24 13:34	文本文档	1 KB
钩.txt	2021/1/24 13:33	文本文档	1 KB
棍.txt	2021/1/24 13:35	文本文档	1 KB
戟.txt	2021/1/24 13:31	文本文档	1 KB
剑.txt	2021/1/24 13:31	文本文档	1 KB
锏.txt	2021/1/24 13:34	文本文档	1 KB
矛.txt	2021/1/24 13:36	文本文档	1 KB
耙.txt	2021/1/24 13:36	文本文档	1 KB
枪.txt	2021/1/24 13:31	文本文档	1 KB

类型: 文本文档
大小: 124 字节
修改日期: 2021/1/24 13:30

打开txt文档，每个都是



但往下翻一翻可以看到，每个txt都带有一个不同的数字，根据题目里兵器的顺序以及所给的hint，前十个兵器是十进制，后八个兵器是八进制，想到应该是把这些数字转换成字符串就是flag，但是具体怎么转需要尝试一下。

先将前十组十进制数放在一起，转成十六进制，然后将后八组八进制数放在一起转成十六进制（可以看到转换出来的十六进制两两一组都是7f一下的那就肯定能转换成字符），最后十六进制转字符串就是flag。

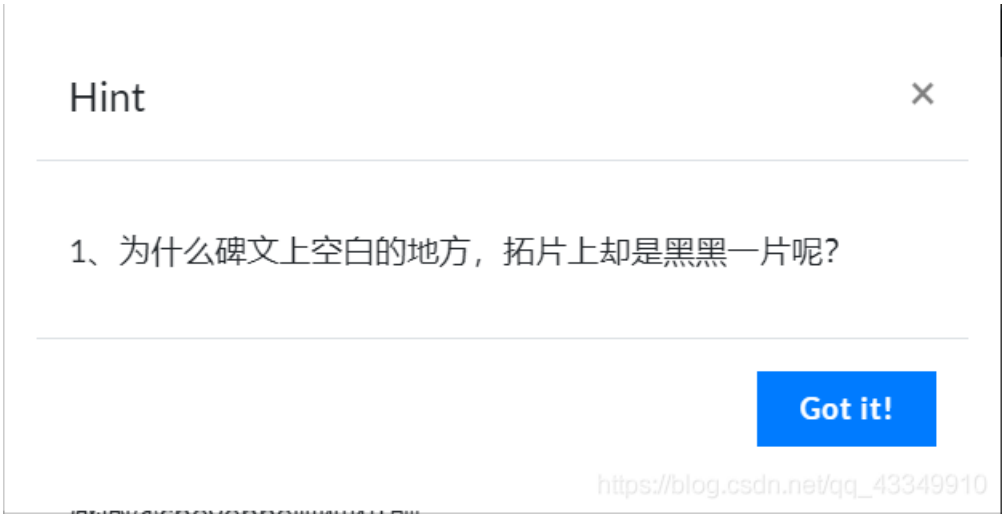
16进制到文本字符串

加密或解密字符串长度不可以超过10M

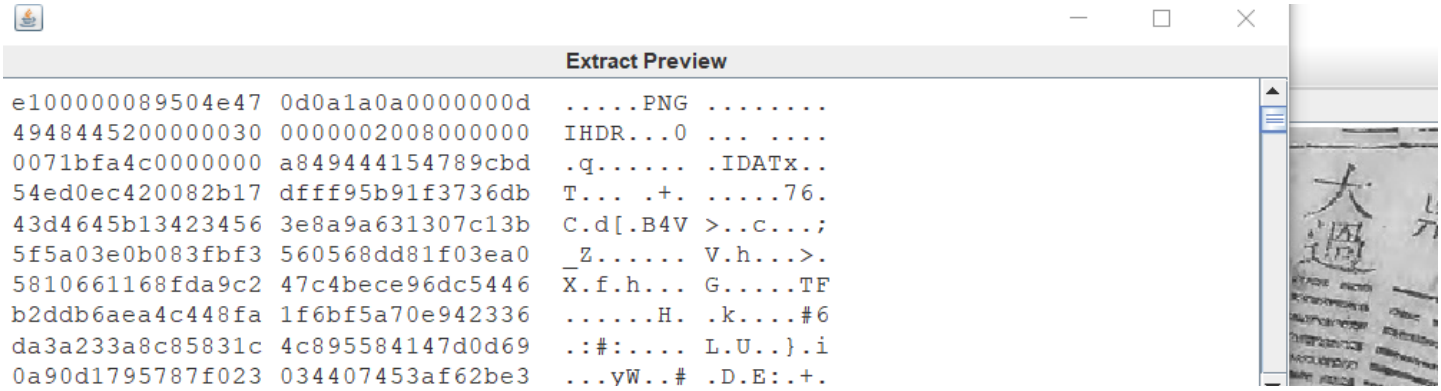
```
1 666c61677b43544673686f775f31305f62415f42616e5f62316e675f51317d
```

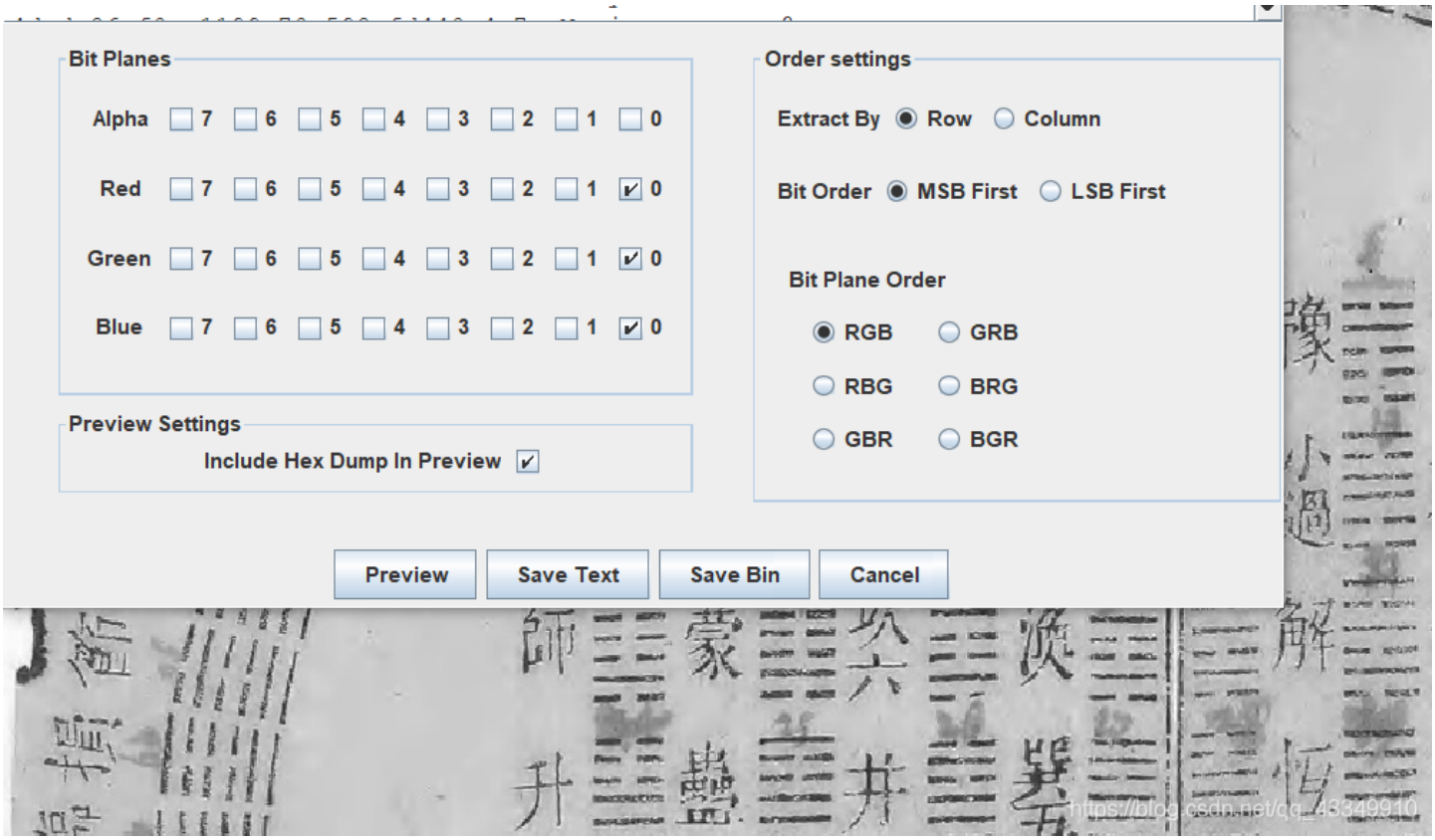
碑寺六十四卦

首先题目是一个碑文拓片的图片，一开始在stegsolve捣鼓了半天没发现什么特别的东西，然后binwalk了一下也没有任何东西，看了这个hint，我也在黑白反色上停留了一会也没想到什么。



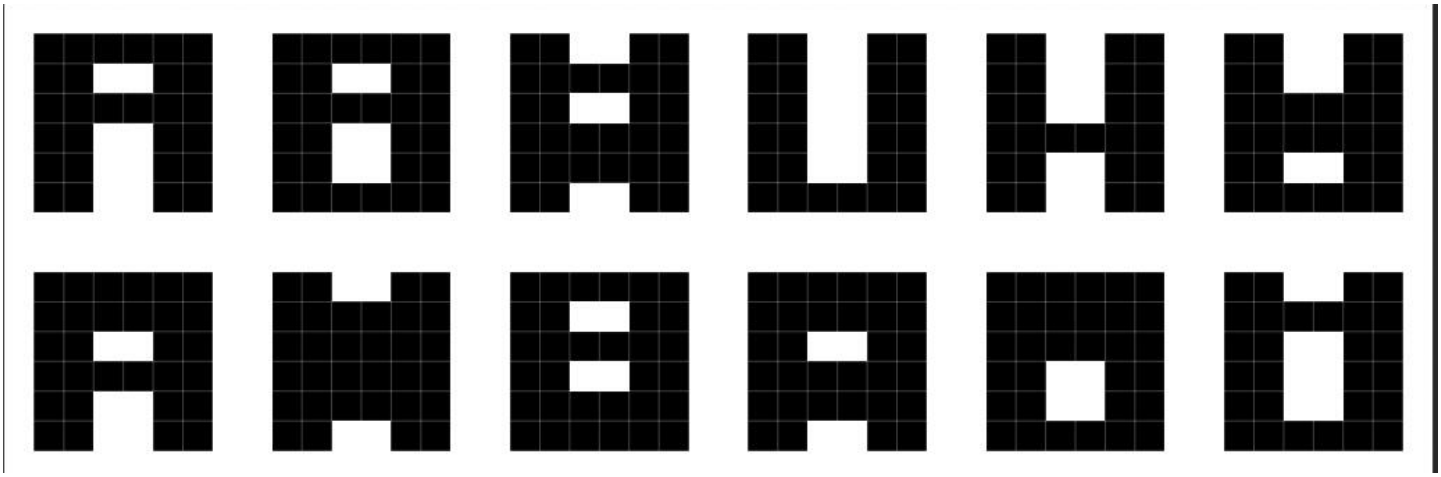
最后在提示下知道了，原来还有图片黑白反色后才能看到隐写的东西。
反色图片LSB隐写，Save Bin导出后还要把PNG头前面的数据删掉。

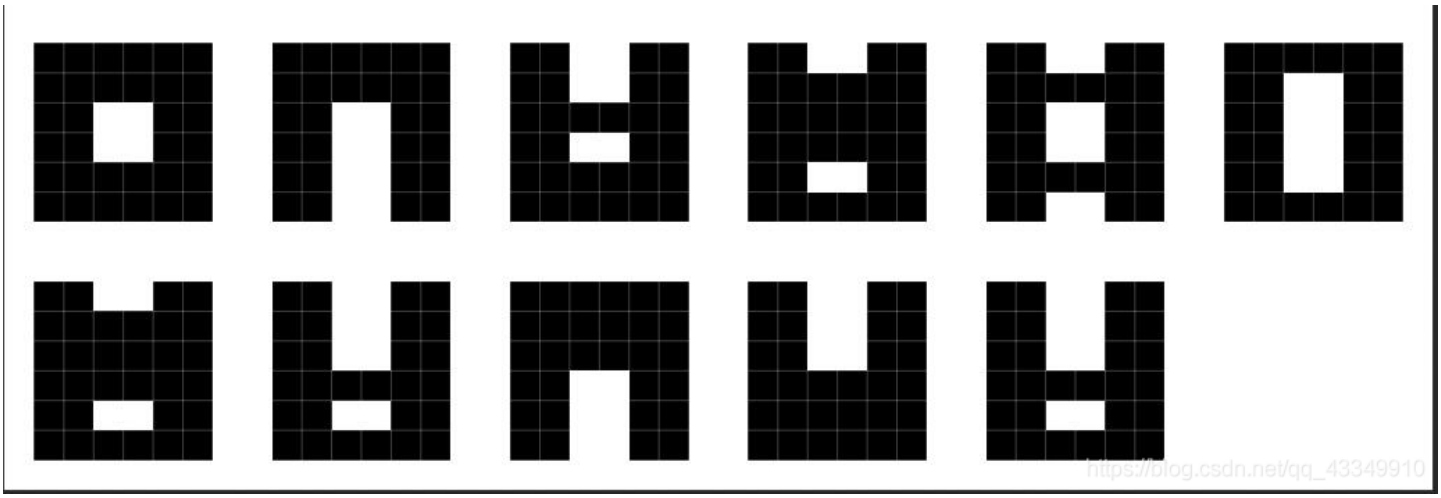




得到了这样的图

这张清楚一些的，可以看到上面的六横刚好对应卦的六横，再根据题目是碑寺六十四卦肯定与base64有所关联，那就把每一个卦用六位二进制表示出来，然后转换成十进制，再与base64的表对照就能得到flag





经过尝试

```
000101 100101 011010 100000 001000 101100 001011 011110 110101 011011 100111 100010 110011 000011 110100 101110
010010 100001 101110 101000 000111 111000 101000
5  37  26  32  8  44  11  30  53  27  39  34  51  3  52  46  18  33  46  40  7  56  40
FiagIsLe1bnizD0uShuoH4o
```

最后得到flag{Le1bnizD0uShuoH4o}

AA86

首先根据这些字符我想到的是jjencode和aaencode，百度搜索一下

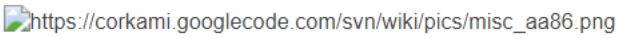
```
%@"%"@,~,%,!`_^[^_^]-;>`_^[^_^]%"!,^,:`_^[^_^]-@{-`{-?:`_[^_^]_-``-``-@@`_^[^_^]-`~-``-@$`_^[^_^]-``-``-@@`_^[^
^]-`~-``-@#`_^[^_^]-+~-/~-?;`_^[^_^]%!~-;-,;`_^[^_^]-"$-@~-@``_^[^_^]-{[-);-@:`_^[^_^]-/*,%`_^[^_^]`_^[^_^]`_^[^
_^]`_^[^_^]%@$-@;-?;`_^[^_^]-/~-`&,#`_^[^_^]-`~-`{,*`_^[^_^]-@@-$!`_^[^_^]-:$,[,<`_^[^_^]-!|-.),!`_^[^_^]-@{-@`-
/(`_^[^_^]`_^[^_^]`_^[^_^]`_^[^_^]-{!-{.,.`_^[^_^]-~/-/``_^[^_^]%""-}@$"`_^[^_^]%@@-!/,!`_^[^_^]-:*-=%`[[[[[[[[`
^^^^^-%+)@@^^^!;@@++,((,.((-$+"@"+&&-,!""+,&-,!""+!&-,!""+'&-,!""++'-,!""+(&-,!""+$'-,!""+$'-,!""+@'-,!""+#'-,!"
"+*#-,!""+_"-,!""+_"-,!""+%'-,!""+$'-,!""+&&-,!""+-"-,!""+(#-,!""+."-,!""+*&-,!""+@'-,!""+_"-,!""+@'-,!""+%'-,!"
"+"&-,!""+,&-,!""+)&-,!""+#&-,!""+_"-,!""+#'-,!""+!&-,!""+#'-,!""+_"-,!""+)&-,!""+.&-,!""+$&-,!""+%&-,!""+('-,!"
"+."-,!""+(&-,!""+$'-,!""+-&-,!""+,&-,!""+-'-,!"(+@@,$-,!"
```

发现这个可能是DOS系统的com文件内容

COM

Not the ActiveX thingy, but the old headerless binaries from DOS (and Windows XP or before)

aa86



Aa86 is a .COM file encoder by Yosuke Hasegawa that encodes binaries using only symbols characters, with a decoder.

so for example, a simple `hello world` binary is encoded as: `%@"%"@,~,%,!`_^[^_^]-;>`_^[^_^]%"!,^,:`_^[^_^]-@{-`{-?:`_[^_^]_-``-``-@@`_^[^_^]-`~-``-@$`_^[^_^]-``-``-@@`_^[^_^]-`~-``-@#`_^[^_^]-+~-/~-?;`_^[^_^]%!~-;-,;`_^[^_^]-"$-@~-@``_^[^_^]-{[-);-@:`_^[^_^]-/*,%`_^[^_^]`_^[^_^]`_^[^_^]`_^[^_^]%@$-@;-?;`_^[^_^]-/~-`&,#`_^[^_^]-`~-`{,*`_^[^_^]-@@-$!`_^[^_^]-:$,[,<`_^[^_^]-!|-.),!`_^[^_^]-@{-@`-/(`_^[^_^]`_^[^_^]`_^[^_^]`_^[^_^]-{!-{.,.`_^[^_^]-~/-/``_^[^_^]%""-}@$"`_^[^_^]%@@-!/,!`_^[^_^]-:*-=%`[[[[[[[[`^^^^^-%+)@@^^^!;@@_!,((,.((-$+)@*+@!!@-,!"(+@@,$-,!"($%&,&,&_&@"'%_&"',&$&!"-@*@$"`

- commented assembly source
- standalone encoder

将文件后缀名改为com，放到16位虚拟机运行，即可得到flag。

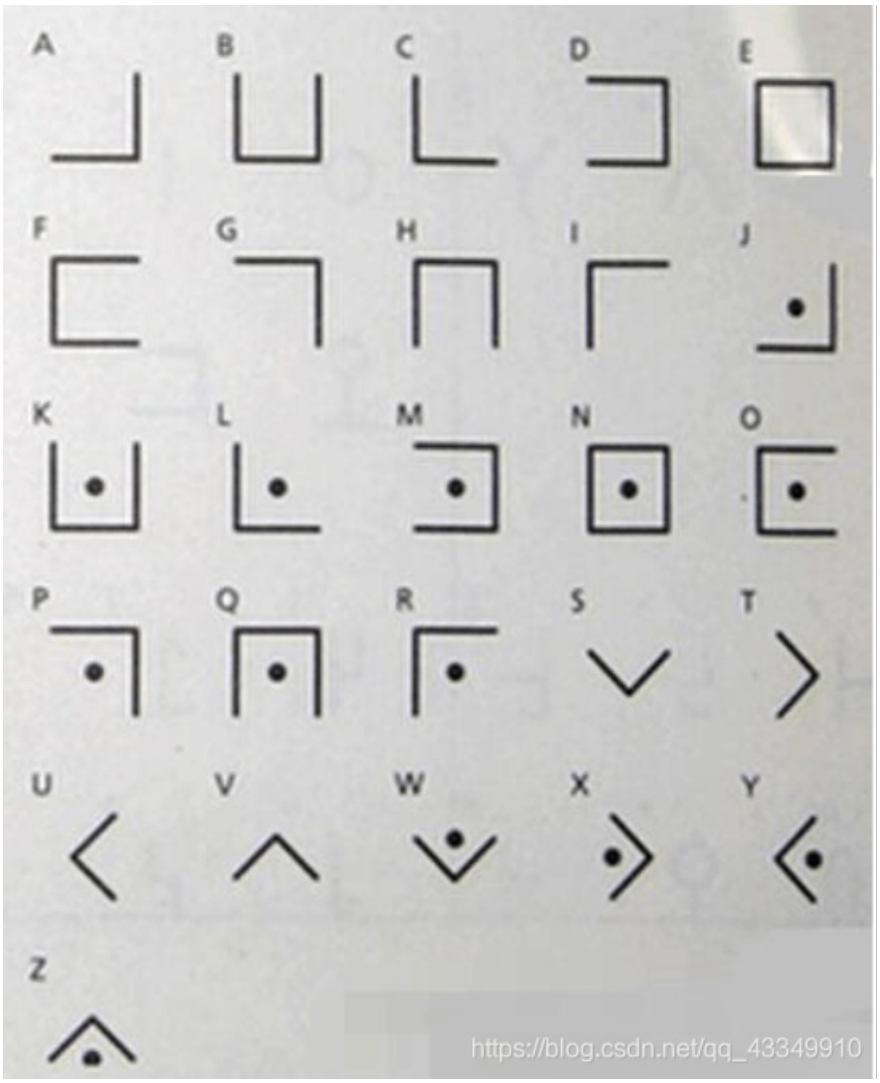
```
C:\>1.com
flag{https://utf-8.jp/public/sas/index.html}
C:\>
```

请问大吉杯的签到是在这里签吗

这题首先得到一个二维码，扫描二维码以为这是一个纯脑洞题，后来还是把二维码下载下来试了一下。

首先binwalk下去到2.png说有岔路口，到4.png发现是死路，回到2.png，在stegsolve捣鼓了一下，发现有特别的东西，

搜了一下发现是猪圈密码，对照密码得到最终flag



FLAG DAJIADOAIDJB

拼图v2.0

这题手撕的，好像可以用gaps来拼。