攻防世界misc高手进阶篇教程（3）

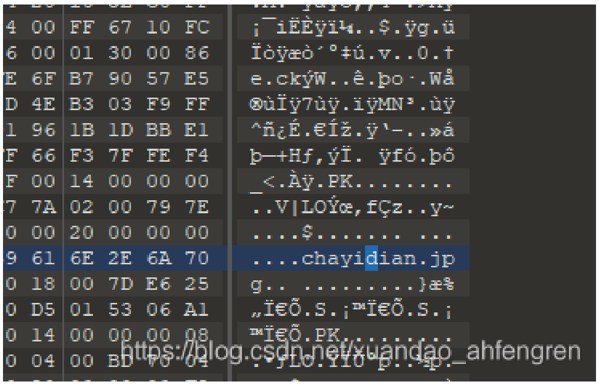
原创

锋刃科技 于 2020-05-27 14:13:57 发布 3662 收藏 7
文章标签： ctf 攻防世界

本文链接：https://blog.csdn.net/xuandao_ahfengren/article/details/106380209

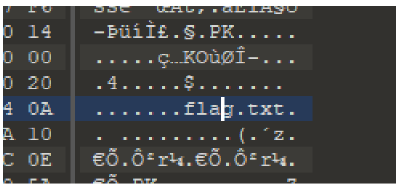
Miscmisc

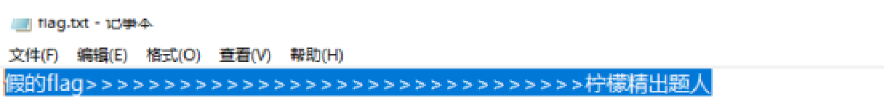
用010editor打开图片，然后看到jpg图片，把后缀修改成zip



有个压缩包是加密过的，还有张图片，我们看看图片

看到了flag.txt，再次把图片后缀修改成zip



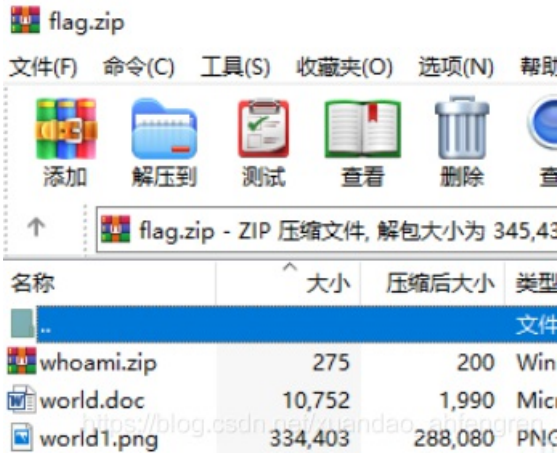


发现可以解压，得到一个 flag.txt 文件，咦，，，，，刚才解压chayidian.zip文件时，目录下也有一个flag.txt 文件，很明显这是一个明文攻击，又已知

是.zip加密，上工具 Advanced Zip Password Recover。

在这里我跑出密码 z$^58a4w

Fial.zip里面的文件



打开whoami.zip文件，发现有个加密文本，需要密码，猜想flag就在里面。

说就差一点点了

打开 world/media/task/writeup/cn/miscmisc/1.png图片

根据提示 pass in world 猜想 world.doc 文件里不可能那么简单 可能还会有隐藏文字，ctrl+A 全选，右击—字体—取消勾选隐藏。发现了隐藏字符。

最后的密码是 pass内容+world里每行字符串的最后一个字符

解压后就得到flag{12sad7eaf46a84fe9q4fasf48e6q4f6as4f864q9e48f9q4fa6sf6f48}

flag_universe

数据里面有一些图片

```
 90 Response: 226 Directory send OK.
 72 Request: PASV
114 Response: 227 Entering Passive Mode (172
 86 Request: RETR /universe.png
142 Response: 150 Opening BINARY mode data c
 90 Response: 226 Transfer complete.
 72 Request: PASV
114 Response: 227 Entering Passive Mode (172
```

复制原始数据存到一个txt文档中，用010编辑器导入十六进制在存为png图片即可

把图片都dump下来后有一张图片lsb隐写，得到flag

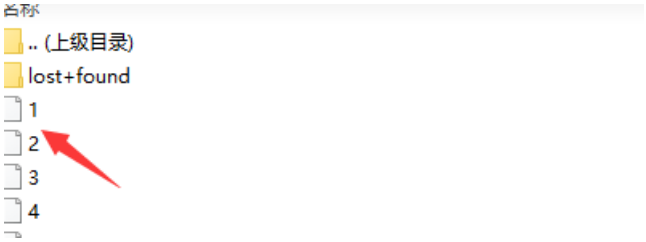
```
zsteg 1.png
..  text: "\n\n\n111???"
..  text: "F2&*rq 9Qz"
..  text: "flag{Plate_err_klaus_Mail_Life}\n"
..  file: PGP Secret Sub-key -
..  text: "zC`)XUWS"
```

Get-the-key.txt

看到txt文件，把后缀修改成zip

```
00 00 00  ................
00 00 00  ................
00 00 00  ................
00 00 00  ................
31 35 38  .‹..M˜+T..key158
F6 57 F2  .txt..vuvö÷«ÖöWò
AD E5 02  .ÕÓ.TuOH*+³ÐQ-å.
00 00 00  .fÔé‰...........
00 00 00  ................
00 00 00  ................
00 00 00  ................
00 00 00  ................
00 00 00  ................
```

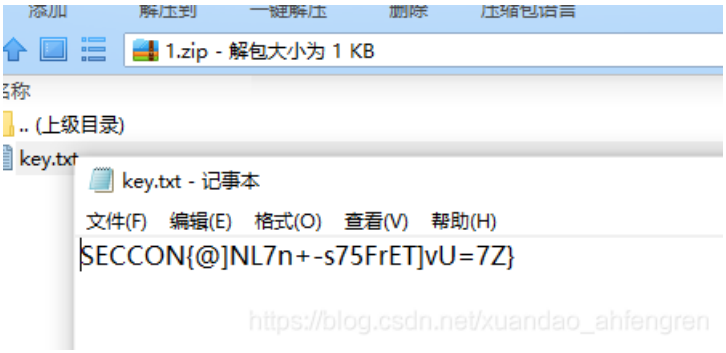

我这里把1解压出来



又看到了.txt文件,再次把1修改后缀

```
  D  E  F    0123456789ABCDEF
9 2E 74 78   .‹..“˜+T..key.tx
8 31 CF D3   t..vuvö÷«v^ÕóÏÏÓ
5 8F AA E5   Ö-67u+r.‰-.µ5.ªå
             ..M.É.....
```

里面就是flag了



奇怪的TTL字段

把每个TTL值二进制码的高两位拿下来，每4个TTL值凑出一个字节的二进制数来

用脚本实现

```
with open('ttl.txt') as f:
    lines = f.readlines()
n_num = []#分析出所有的数for i in lines:
    if i!='\n':
        n_num.append(int(i.replace('TTL=','')))#拿到每个TTL值的高位
rlt = ''for i in range(0,len(lines)):
    tmp = bin(n_num[i])[2:]
    tmp = '0'*(8-len(tmp)) + tmp
    rlt += tmp[0:2]#得到最终的结果并存到文件中
rlt2 = ''for i in range(0,len(rlt),8):
    rlt2 += chr(int(rlt[i:i+8],2))with open('fi.txt','w') as f:
f.write(rlt2.rstrip())
```

得到文件

以FFD8开头，FFD9结束。所以，是jpeg格式的图片无疑了

把这些16进制字符粘贴到winhex里并保存为jpeg格式的图片，得到了一张残缺二维码。于是就搜了下FFD8和FFD9的数量，正好6对

可以用替换搜索，这样可以计数

接着就是把图片拆出来了，使用binwalk，会分出6张二维码图片，用PPT的插图和对齐的功能拼接一下，得到一个二维码

使用autokey解开密文

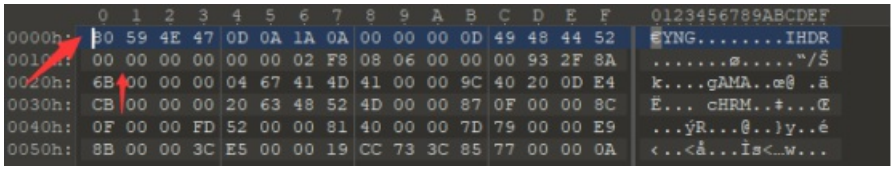
http://www.practicalcryptography.com/ciphers/classical-era/autokey

flag{2028ab39927df1d96e6a12b03e58002e}

2-1

打开发现图片损坏了，用010editor打开

发现头部和宽度都不对



恢复png头为 89 50 4e 47 0d 0a 1a 0a

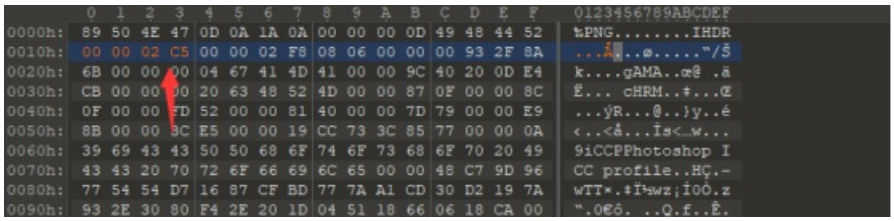
宽度通过pyhton跑出来

```
import os
import binascii
import struct

misc = open("12.png","rb").read()

for i in range(1024):
    data = misc[12:16] + struct.pack('>i',i)+ misc[20:29]
    crc32 = binascii.crc32(data) & 0xffffffff
    if crc32 == 0x932f8a6b:
        print (i)
```

得到709,十六进制转换后得到，0x2c5。



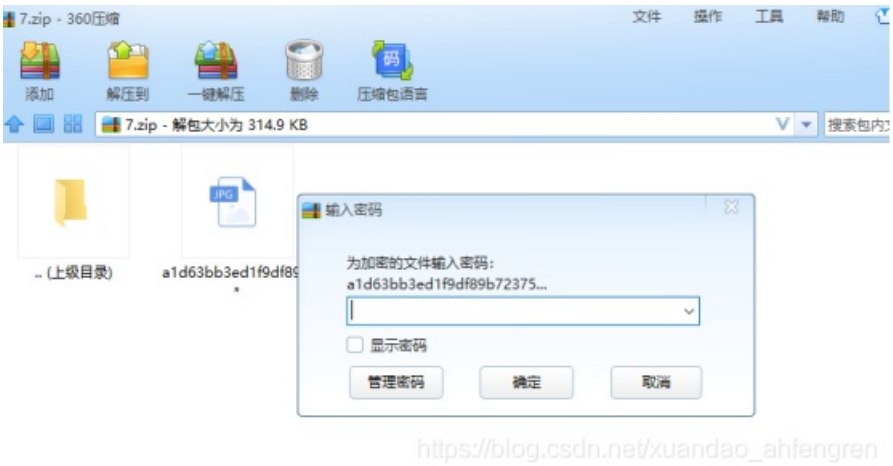
互相伤害!!!

从wireshark打开，导出图片，发现一二维码，图片说了AES加密密码CTF，我们解密出来

668b13e0b0fc0944daf4c223b9831e49

接着发现这张图有密码，把后缀改成zip，输入密码


来啊 互相伤害啊

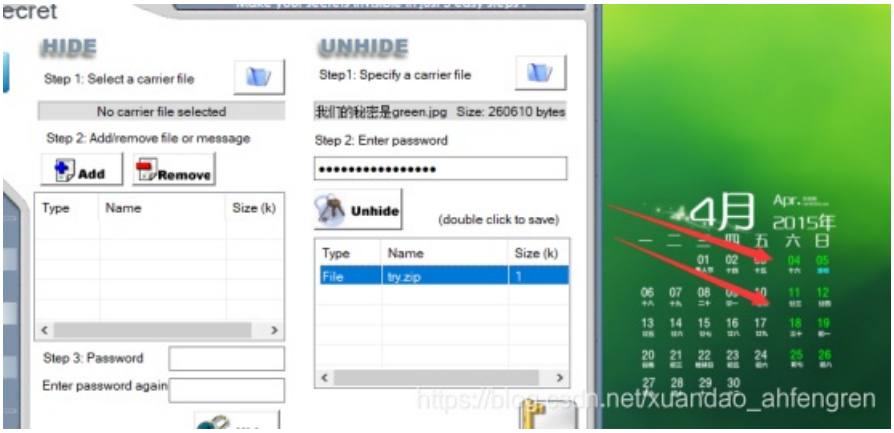

7.zip - 360压缩
文件
操作
工具
帮助
添加
解压到
一键解压
删除
压缩包语言
7.zip - 解包大小为 314.9 KB
.. (上级目录)
输入密码
为加密的文件输入密码:
显示密码
管理密码
确定
取消

扫描里面的二维码即可

97d1-0867-2dc1-8926-144c-bc8a-4d4a-3758

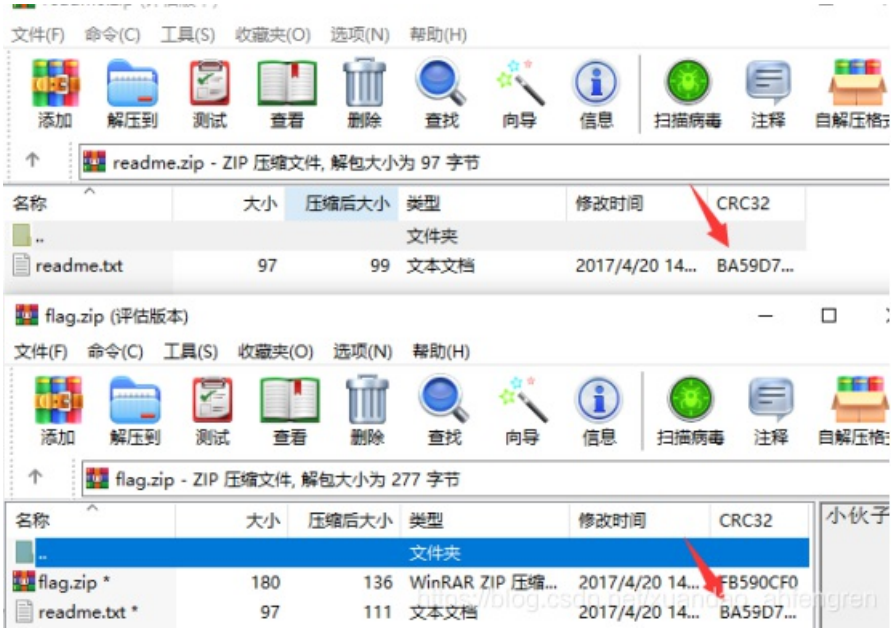
我们的秘密是绿色的

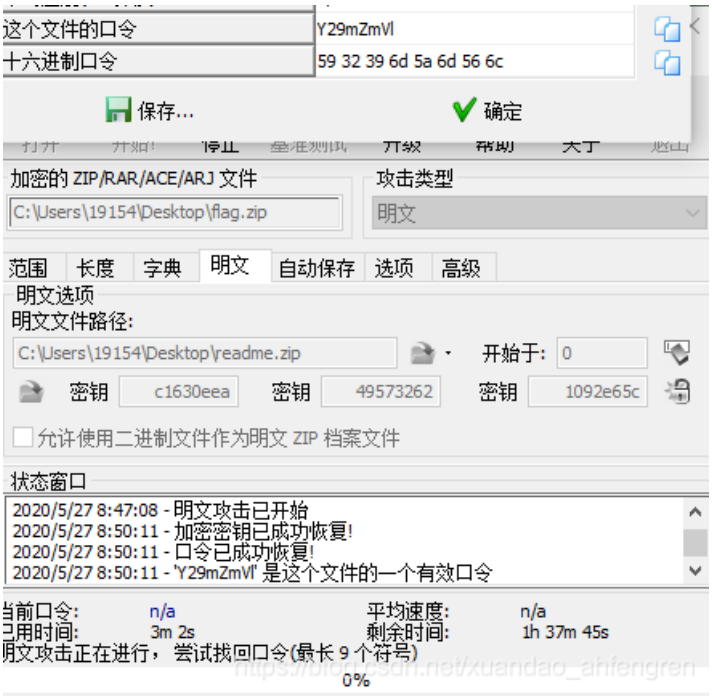
我们用oursecret分解出压缩包，密码是图片的绿色的数字



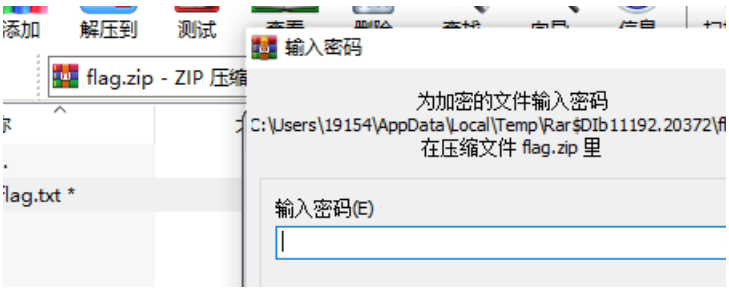
根据提示生日，爆破压缩包，密码19950822

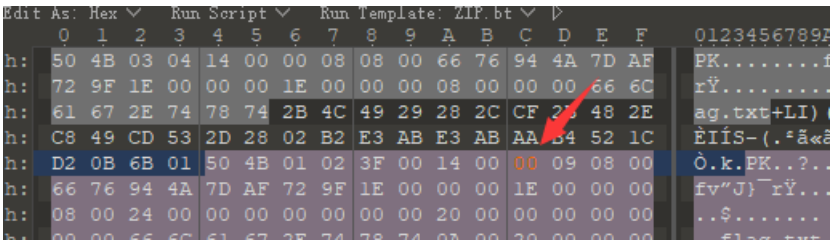
发现txt文件和flag.zip压缩包里的txt文件CRC32一样即可用明文爆破





发现里面有flag.txt，这里用的是伪加密，在PK处把01修改成00即可





爆破栅栏密码

```
第1栏: qdqnclnpqn{z*@qdpwppe%rw__zdg}
第2栏: qpnpnrn_*qdqp!%q_zdqdwcepw{z@}
第3栏: qwlr{ddneq_@dpnwzgpc%nzqqpp_*}
第4栏: qnnn*qp%_qdcp{@ppr_gqlqzqwewz}
第5栏: ql{de_dnzp%zqp*wrdnq@pwgcnqp_}
第6栏: qrdqdwpnq_w{n_pzczp*!de@ng%qp}
```

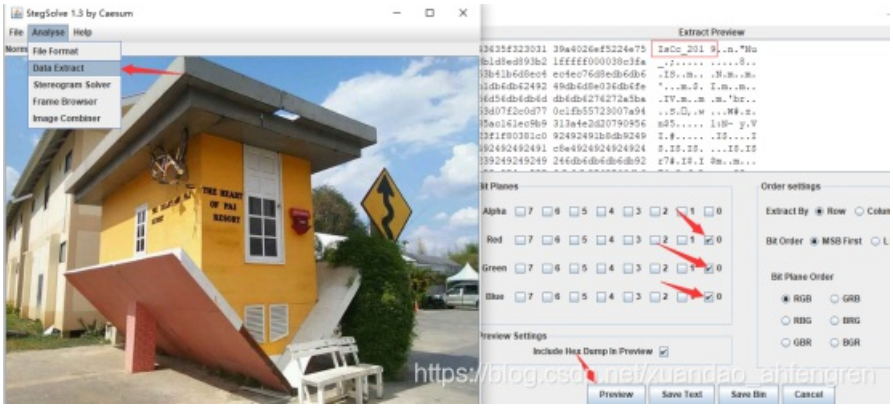
爆破凯撒密码

```
wcrx{jjtkw_@jvtcfmvi%tfwwvv_*}
xdsy{kkulx_@kwudgnwj%ugxxww_*}
yetz{llvmy_@lxvehoxk%vhyyxx_*}
zfua{mmwnz_@mywfipyl%wizzyy_*}
agvb{nnxoa_@nzxgjqzm%xjaazz_*}
bhwc{ooypb_@oayhkran%ykbbaa_*}
cixd{ppzqc_@pbzilsbo%zlccbb_*}
djye{qqard_@qcajmtcp%amddcc_*}
ekzf{rrbse_@rdbknudq%bneedd_*}
flag{ssctf_@seclover%coffee_*}
gmbh{ttdug_@tfdmpwfs%dpggff_*}
hnci{uuevh_@ugenqxgt%eqhhgg_*}
iodj{vvfwi_@vhforyhu%friihh_*}
jpek{wwgxj_@wigpsziv%gsjjii_*}
kqfl{xxhyk_@xjhqtajw%htkkjj_*}
lrgm{yyizl_@ykirubkx%iullkk_*}
```

flag{ssctf_@seclover%coffee_*}

倒立屋

用Stegsolve打开图片，相应操作，然后第一串就是，根据题目所说是倒写的



flag{9102_cCsl}

隐藏的信息

首先8进制转换ascii码，然后base64转换即可

Become_a_Rockstar

首先安装rockstar

pip3 install rockstar-py

然后获取python代码。跑一下即可

```
Leonard_Adleman = "star"
Problem_Makers = 76
Problem_Makers = "NCTF{"
def God(World):
    a_boy = "flag"
    the_boy = 3
def Evil(your_mind):
    a_girl = "no flag"
    the_girl = 5
Truths = 3694
Bob = "ar"
Adi_Shamir = "rock"
def Love(Alice, Bob):
    Mallory = 13
    Mallory = 24
Everything = 114514
Alice = "you"
def Reality(God, Evil):
    God = 26
    Evil = 235
Ron_Rivest = "nice"
def You_Want_To(Alice, Love, Anything):
    You = 5.75428
your_heart = input()
You = 5
your_mind = input()
Nothing = 31
if Truths * Nothing == Everything:
    RSA = Ron_Rivest + Adi_Shamir + Leonard_Adleman
if Everything / Nothing == Truths:
    Problem_Makers = Problem_Makers + Alice + Bob
print(Problem_Makers)
the_flag = 245
the_confusion = 244
print(RSA)
Mysterious_One = "}"
print(Mysterious_One)
This = 4
This = 35
This = 7
This = 3
This = 3
This = 37
```

NCTF{youarnicerockstar}

小小的PDF

用binwalk发现还有图片没有显示出来

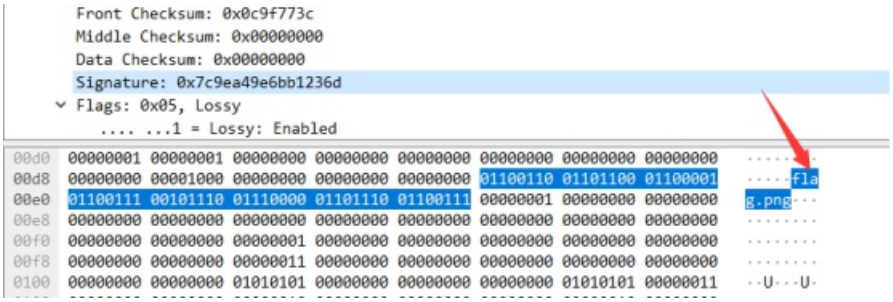
```
root@kali:~/test# binwalk a4f37ec070974eadab9b96abd5ddffed.pdf

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PDF document, version: "1.4"
452           0x1C4           JPEG image data, JFIF standard 1.01
73254         0x11E26         JPEG image data, JFIF standard 1.01
81606         0x13EC6         Zlib compressed data, default compression
82150         0x140E6         JPEG image data, JFIF standard 1.01
104469        0x19815         Zlib compressed data, default compression
105134        0x19AAE         Zlib compressed data, default compression
```

直接foremost分离出来

Cephalopod

有个flag.png图片，但是foremost分离不出来,这里我们用tcpxtract分离

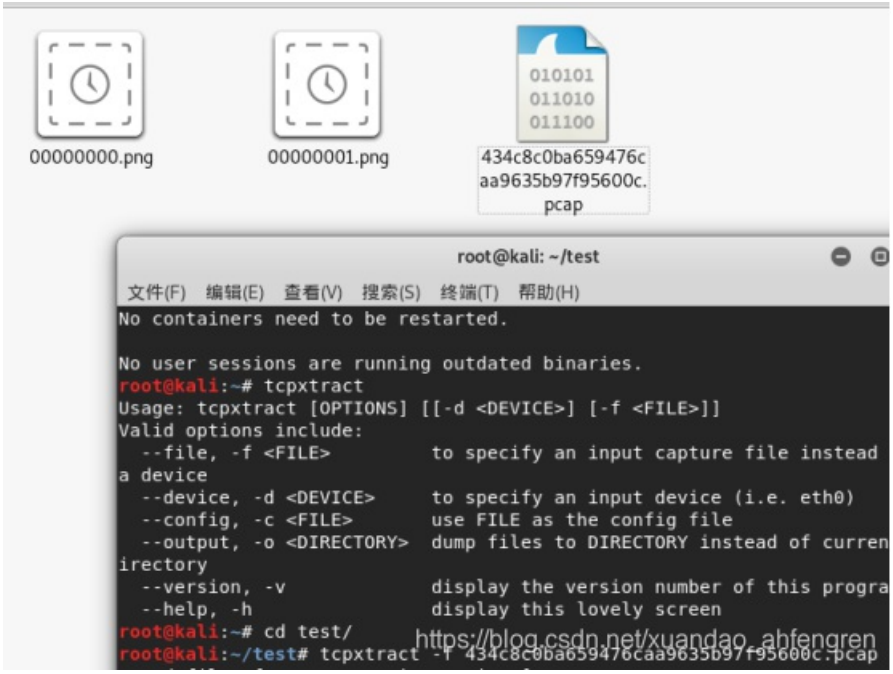


先安装

apt-get install tcpxtract

Tcpxtract -f

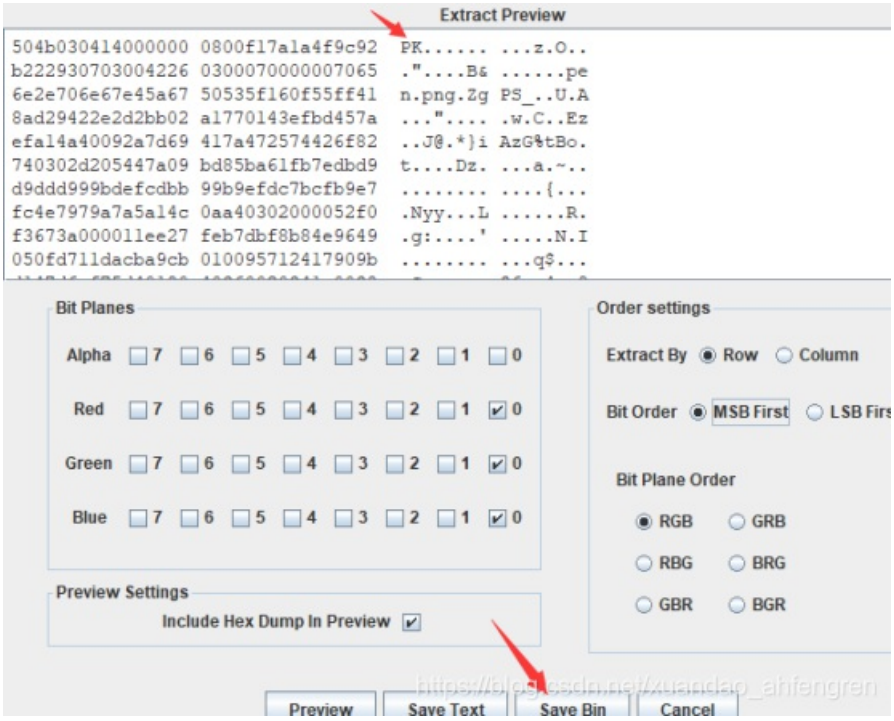
分离出来，flag就出来了



HITB{95700d8aefdc1648b90a92f3a8460a2c}

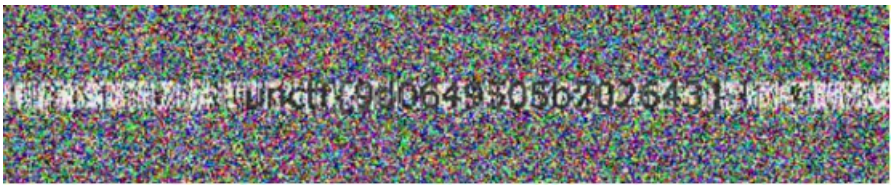
信号不好先挂了

用stegsolver打开，发现PK头，于是分离出zip文件



发现一样的图片，于是利用盲水印

python bwm.py decode apple.png pen.png apple_pen.png

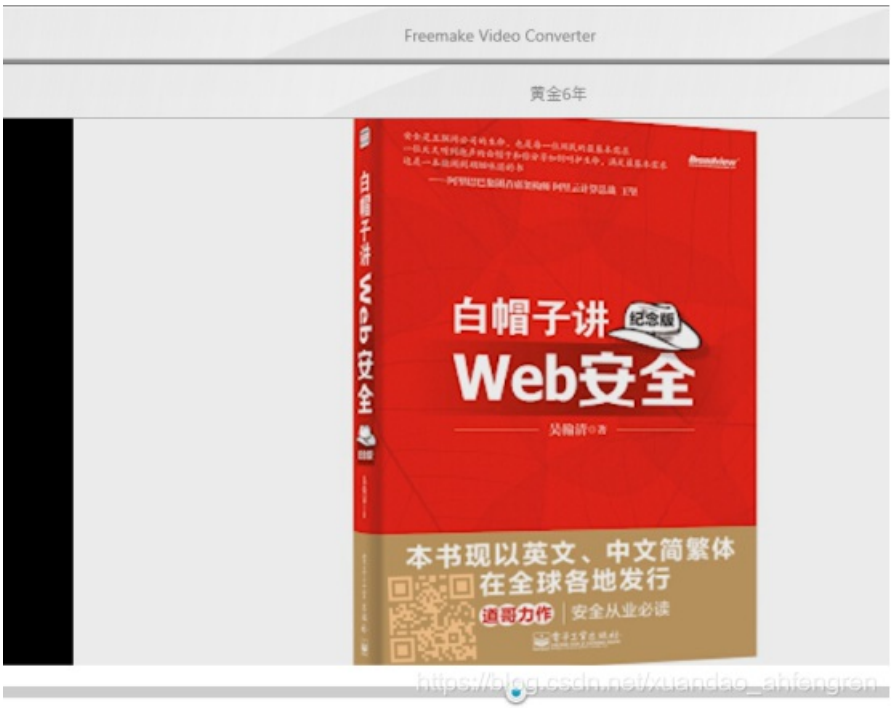


unctf{9d0649505b702643}

我们用工具Freemake Video Converter慢慢打开，发现两个二维码拿去扫描下

黄金六年

我们用工具Freemake Video Converter慢慢打开，发现两个二维码拿去扫描下



解密出来

key2:want

key3:play

接着我们用winhex打开发现一串base64加密的字符串

黄金6年.mp4

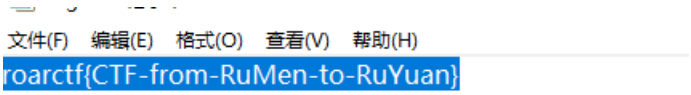
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00C4BB20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00C4BB30	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00C4BB40	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00C4BB50	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00C4BB60	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00C4BB70	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00C4BB80	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00C4BB90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00C4BBA0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00C4BBB0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00C4BBC0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00C4BBD0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00C4BBE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00C4BBF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00C4BC00	00	00	00	00	00	00	00	00	00	00	00	00	00	DE	18	00	Þ
00C4BC10	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00C4BC20	00	00	00	00	00	00	00	00	01	F5	55	6D	46	79	49	52	õUmFyIR
00C4BC30	6F	48	41	51	41	7A	6B	72	58	6C	43	67	45	46	42	67	oHAQAzkrXlCgEFBg
00C4BC40	41	46	41	51	47	41	67	41	44	68	37	65	6B	35	56	51	AFAQGAgADh7ek5VQ
00C4BC50	49	44	50	4C	41	41	42	4B	45	41	49	45	76	73	55	70	IDPLAABKEAIEvsUp
00C4BC60	47	41	41	77	41	49	5A	6D	78	68	5A	79	35	30	65	48	GAAwAIZmxhZy50eH
00C4BC70	51	77	41	51	41	44	0A	44	78	34	33	48	79	4F	64	4C	QwAQAD Dx43HyOdL
00C4BC80	4D	47	57	66	43	45	39	57	45	73	42	5A	70	72	41	4A	MGWfCE9WEsBZprAJ
00C4BC90	51	6F	42	53	56	6C	57	6B	4A	4E	53	39	54	50	35	64	QoBSVlWkJNS9TP5d
00C4BCA0	75	32	6B	79	4A	32	37	35	4A	7A	73	4E	6F	32	39	42	u2kyJ275JzsNo29B
00C4BCB0	6E	53	5A	43	67	4D	43	33	68	2B	55	46	56	39	70	31	nSZCgMC3h+UFV9p1
00C4BCC0	51	45	66	0A	4A	6B	42	50	50	52	36	4D	72	59	77	58	QEf JkBPPR6MrYwX
00C4BCD0	6D	73	4D	43	4D	7A	36	37	44	4E	2F	6B	35	75	31	4E	msMCMz67DN/k5u1N
00C4BCE0	59	77	39	67	61	35	33	61	38	33	2F	42	2F	74	32	47	Yw9ga53a83/B/t2G
00C4BCF0	39	46	6B	47	2F	49	49	54	75	52	2B	39	67	49	76	72	9FkG/IITuR+9gIvr
00C4BD00	2F	4C	45	64	64	31	5A	52	41	77	55	45	41	41	3D	3D	/LEdd1ZRAwUEAA==
00C4BD10	0A																

用python跑出压缩包

```
import base64a='UmFyIRoHAQAzkrXlCgEFBgAFAQGAgADh7ek5VQIDPLAABKEAIEvsUpGAAwAIZmxhZy50eHQwAQADDx43HyOdLMGWfCE
f=open('111.rar','wb')
f.write(base64.b64decode(a))
f.close()
```

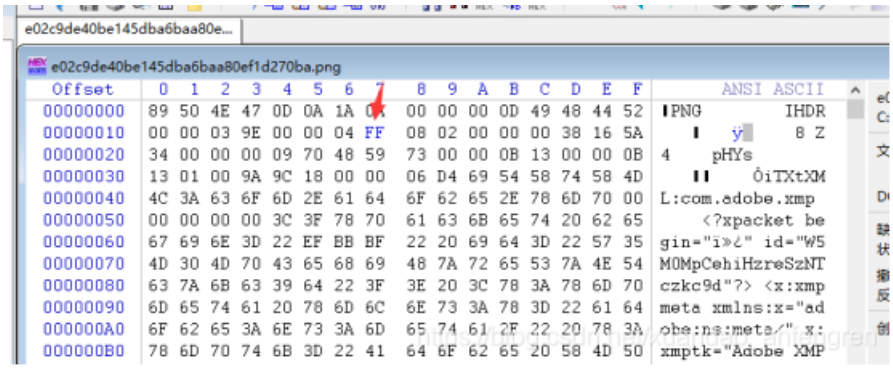
根据给出的2和3的key，我们猜测1和4的key为i、ctf，构成

iwantplayctf

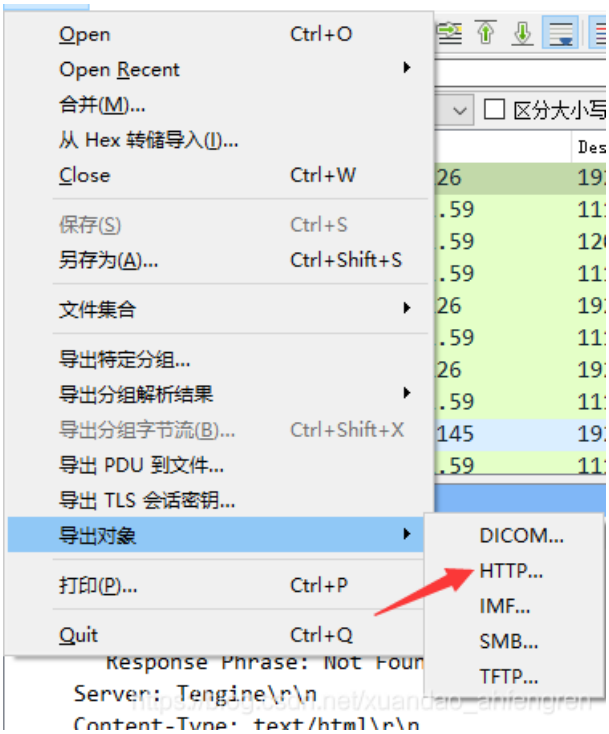


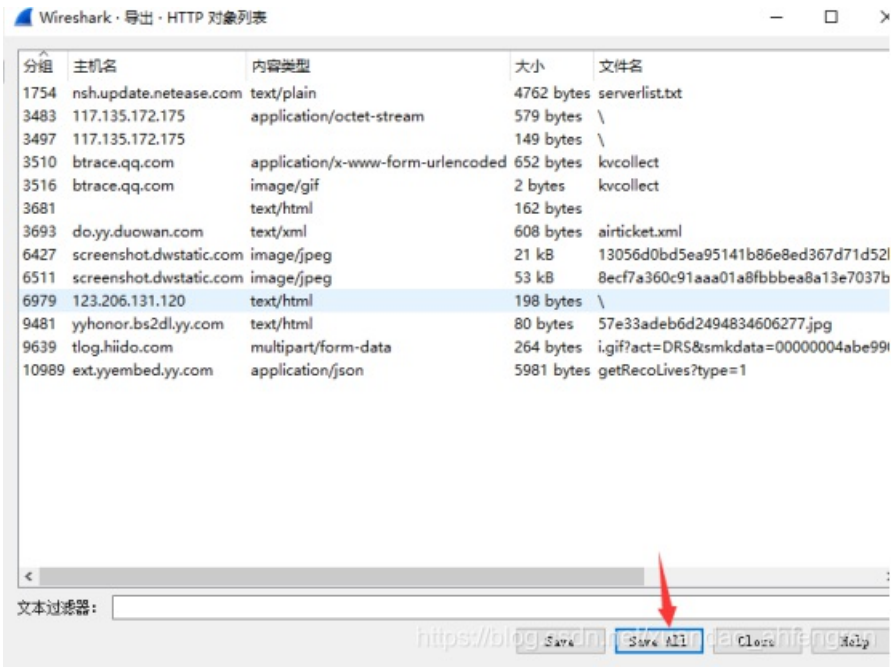
Ditf

把04后面修改成FF



把这张图片后缀修改成zip，然后用这图片下方的密码打开，导出所有的html文件





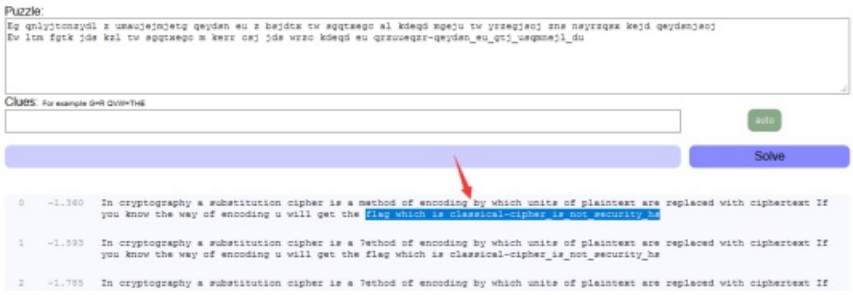
看到了一串base64加密的字符串

flag{Oz_4nd_Hir0_lov3_For3ver}

4-2

直接在线解密

https://quipqiup.com/



flag{classical-cipher_is_not_security_hs}

5-1

```
import os
c = open("cipher",'rb').read()
key = "GoodLuckToYou"
def xor(c,k):
    keylen = len(k)
    res = ""
    for pos,c in enumerate(c):
        res +=chr(ord(c) ^ ord(k[pos % keylen]))
        return res
print xor(c,key)
```

Low

运行代码即可获取二维码

```
import PIL.Image as Image
img = Image.open('low.bmp')
img_tmp = img.copy()
pix = img_tmp.load()
width,height = img_tmp.size
for w in range(width):
   for h in range(height):
      if pix[w,h]&1 == 0:
         pix[w,h] = 0
      else:
         pix[w,h] = 255
img_tmp.show()
```

flag{139711e8e9ed545e}