

BugkuCTF~Misc~WriteUp

转载

[weixin_30515513](#) 于 2019-07-03 00:06:00 发布 249 收藏

原文链接: <http://www.cnblogs.com/qftm/p/11037200.html>

版权

1、签到

签到题

50

关注微信公众号: Bugku
即可获取flag

下面也有二维码

qrcode_for_gh_...

get flag:

Qftm{You should sign in}

2、这是一张单纯的图片

这是一张单纯的图片

50

<http://123.206.87.240:8002/misc/1.jpg>

FLAG在哪里??

查看图片十六进制

71	E3	18	D4	2D	7D	3B	43	14	00	31	43	14	00	37	3B	q0.0-,B..QB..wz
DA	78	3A	2D	0F	E2	C3	EB	FA	54	0D	0D	BE	AF	03	A5	Úx:-.âÑéúT..¼-.¥
E7	95	1E	E5	33	0F	98	97	FE	EE	ED	AA	43	72	01	57	ç•.đ3.~-pîíªCr.W
1D	64	06	8A	28	03	D0	A8	A2	8A	00	28	A2	8A	00	28	.d.Š(.Đ`çŠ.(çŠ.(
A2	8A	00	FF	26	23	31	30	37	3B	26	23	31	30	31	3B	çŠ.ÿke
26	23	31	32	31	3B	26	23	31	32	33	3B	26	23	31	32	y{
31	3B	26	23	31	31	31	3B	26	23	31	31	37	3B	26	23	1;ou&#
33	32	3B	26	23	39	37	3B	26	23	31	31	34	3B	26	23	32;ar&#
31	30	31	3B	26	23	33	32	3B	26	23	31	31	34	3B	26	101; r&
23	31	30	35	3B	26	23	31	30	33	3B	26	23	31	30	34	#105;gh
3B	26	23	31	31	36	3B	26	23	31	32	35	3B	D9	D9		t}ÙÙ

提去特殊字符串进行解码

ASCII转换到 ASCII (例: a b c)

```
key{you are right}
```

添加空格

删除空格

将空白字符转换

十六进制转换到十六进制 (例: 0x61或61或61/62) 删除 0x

```
0x6b 0x65 0x79 0x7b 0x79 0x6f 0x75 0x61  
0x72 0x65 0x72 0x69 0x67 0x68 0x74 0x7d
```

十进制转换到十进制 (例: 97 98 99)

```
107 101 121 123 121 111 117 32 97 114 101 32  
114 105 103 104 116 125
```

get flag:

```
key{you are right}
```

3、隐写

隐写

50

2.rar

解压压缩包得到一张图片



打开图片发现只有一个“BU”可能缺少了什么东西，尝试更改其宽高，得到flag

2. png

Edit As: Hex Run Script Run Template

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000h:	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG.....IHDR															
0010h:	00	00	01	F4	00	00	11	A4	08	06	00	00	00	CB	D6	DF	...ô...π.....ËÖß															
0020h:	8A	00	00	00	09	70	48	59	73	00	00	12	74	00	00	12	Š...pHYs...t...															
0030h:	74	01	DE	66	1F	78	00	00	0A	4D	69	43	43	50	50	68	t.Bf.x...MiCCPPh															
0040h:	6F	74	6F	73	68	6F	70	20	49	43	43	20	70	72	6F	66	otoshop ICC prof															
0050h:	69	6C	65	00	00	78	DA	9D	53	77	58	93	F7	16	3E	DF	ile..xÚ.SwX".>ß															
0060h:	F7	65	0F	56	42	D8	F0	B1	97	6C	81	00	22	23	AC	08	÷e.VB00±-l.."#-.															
0070h:	C8	10	59	A2	10	92	00	61	84	10	12	40	C5	85	88	0A	È.Yç.'a,,...@Å...^.															
0080h:	56	14	15	11	9C	48	55	C4	82	D5	0A	48	9D	88	E2	A0	V...œHUA,Ö.H.^â															
0090h:	28	B8	67	41	8A	88	5A	8B	55	5C	38	EE	1F	DC	A7	B5	(,gAŠ^Z<U\8i.Üšµ															
00A0h:	7D	7A	EF	ED	ED	FB	D7	FB	BC	E7	9C	E7	FC	CE	79	CF)ziíiû×û*çççüÿÿ															
00B0h:	0F	80	11	12	26	91	E6	A2	6A	00	39	52	85	3C	3A	D8	.E..&'æçj.9R...<:Ø															
00C0h:	1F	8F	4F	48	C4	C9	BD	80	02	15	48	E0	04	20	10	E6	..OHÄÉ*ç..Hà. .æ															
00D0h:	CB	C2	67	05	C5	00	00	F0	03	79	78	7E	74	B0	3F	FC	ÈÄg.Å..ö.yx~t°?ü															
00E0h:	01	AF	6F	00	02	00	70	D5	2E	24	12	C7	E1	FF	83	BA	.-o...pÖ.Ş.Çáÿf°															

PS: 从第二行开始，前四位是宽，后四位是高。

BU

BUGKU{a1e5aSA}

get flag:

BUGKU{a1e5aSA}

4. telnet

telnet

50

<http://123.206.87.240:8002/misc/telnet/1.zip>

key格式flag{xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx}

wires hark打开数据包进行分析，根据提示对telnet进行过滤，get flag。

No.	Time	Source	Destination	Protocol	Length	Info
33	16.785629	192.168.221.128	192.168.221.164	TELNET	55	Telnet Data ...
34	16.801229	192.168.221.164	192.168.221.128	TELNET	60	Telnet Data ...
36	17.924431	192.168.221.128	192.168.221.164	TELNET	56	Telnet Data ...
37	17.940031	192.168.221.164	192.168.221.128	TELNET	60	Telnet Data ...
39	17.986831	192.168.221.164	192.168.221.128	TELNET	64	Telnet Data ...
41	18.423632	192.168.221.128	192.168.221.164	TELNET	92	Telnet Data ...
43	19.921235	192.168.221.128	192.168.221.164	TELNET	56	Telnet Data ...
45	19.968035	192.168.221.164	192.168.221.128	TELNET	60	Telnet Data ...
47	21.886838	192.168.221.164	192.168.221.128	TELNET	109	Telnet Data ...
49	26.317246	192.168.221.128	192.168.221.164	TELNET	55	Telnet Data ...
50	26.332846	192.168.221.164	192.168.221.128	TELNET	60	Telnet Data ...
52	27.924049	192.168.221.128	192.168.221.164	TELNET	55	Telnet Data ...
53	27.939649	192.168.221.164	192.168.221.128	TELNET	60	Telnet Data ... [Malformed Packet]
54	27.986449	192.168.221.164	192.168.221.128	TELNET	60	Telnet Data ...
55	27.986449	192.168.221.164	192.168.221.128	TELNET	60	Telnet Data ...

```

> Frame 41: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
> Ethernet II, Src: Vmware_84:86:5f (00:0c:29:84:86:5f), Dst: Vmware_26:7e:0e (00:0c:29:26:7e:0e)
> Internet Protocol Version 4, Src: 192.168.221.128, Dst: 192.168.221.164
> Transmission Control Protocol, Src Port: 1146, Dst Port: 23, Seq: 83, Ack: 124, Len: 38
▼ Telnet
  Data: flag{d316759c281bf925d600be698a4973d5}

```

0000	00 0c 29 26 7e 0e 00 0c 29 84 86 5f 08 00 45 00	..)&~...)..._..E.
0010	00 4e 07 b0 40 00 80 06 00 00 c0 a8 dd 80 c0 a8	·N··@··········
0020	dd a4 04 7a 00 17 46 01 d4 4e 68 f0 2a 7a 50 18	···z··F· ·Nh·*zP·
0030	01 00 3c b7 00 00 66 6c 61 67 7b 64 33 31 36 37	··<...f} ag{d3167
0040	35 39 63 32 38 31 62 66 39 32 35 64 36 30 30 62	59c281bf 925d600b
0050	65 36 39 38 61 34 39 37 33 64 35 7d	e698a497 3d5}

get flag:

flag{d316759c281bf925d600be698a4973d5}

5、眼见非实(ISCCCTF)

眼见非实(ISCCCTF)

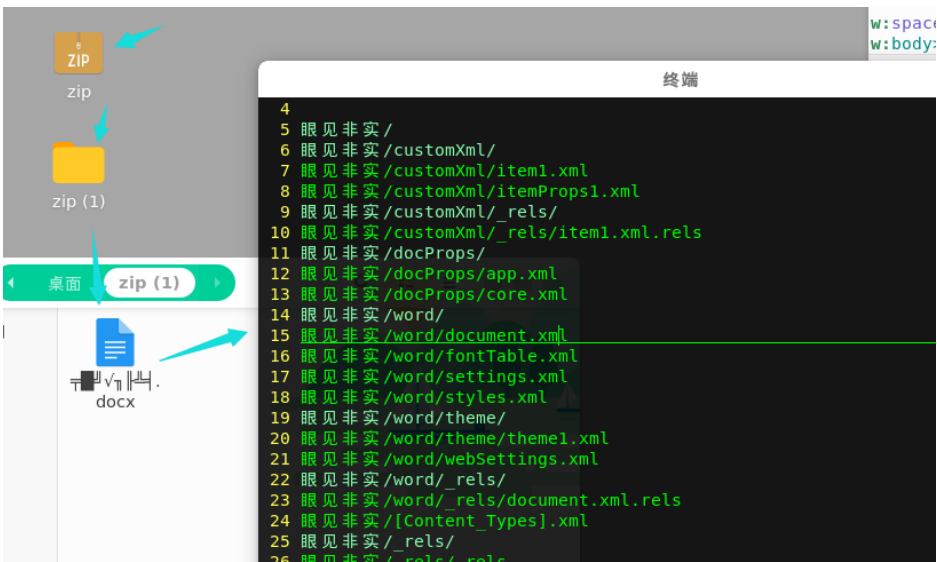
50

zip

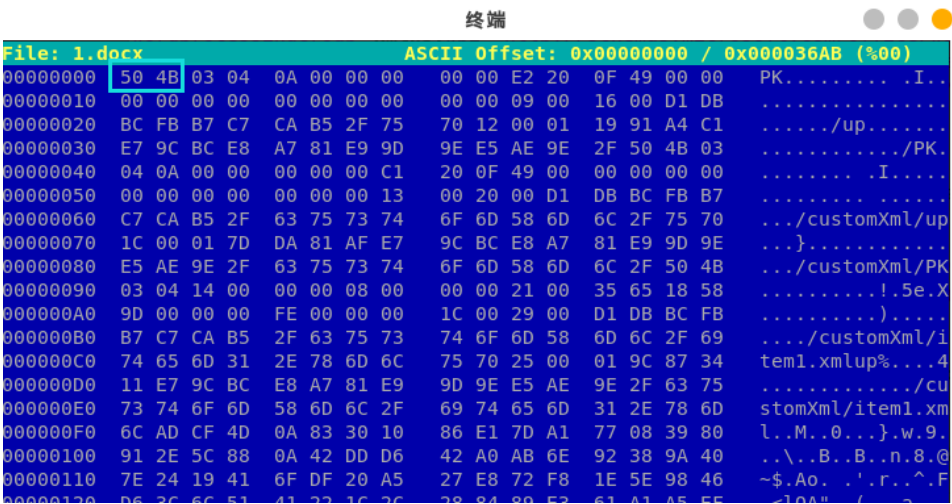
Flag

Submit

解压得到一个word，vi查看文件内容，可以看到有许多目录，猜测word是一个压缩包



word---->zip



解压word压缩包，得到许多xml文件，遍历内容得到flag



get flag:

flag{F1@g}

6、啊哒

啊哒

50

有趣的表情包

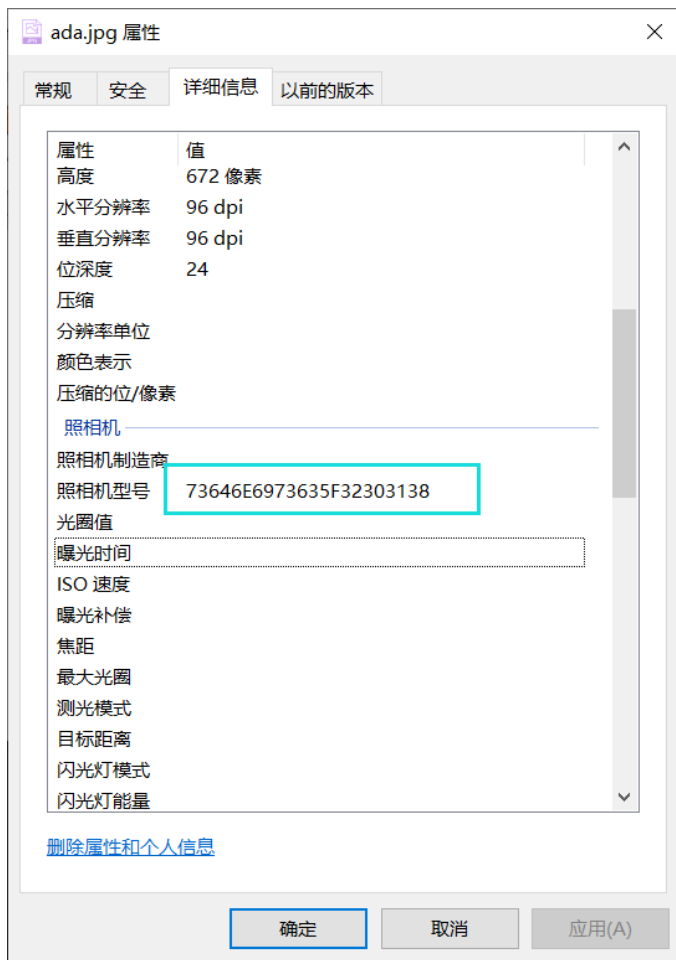
来源：第七届山东省大学生网络安全技能大赛

1cdf3a75-21ed-...

Flag

Submit

查看图片属性，得到特殊数据



解码十六进制得到一个字符串

ASCII转换到 ASCII (例: a b c)

sdnisc 2018

添加空格 删除空格 将空白字符转换

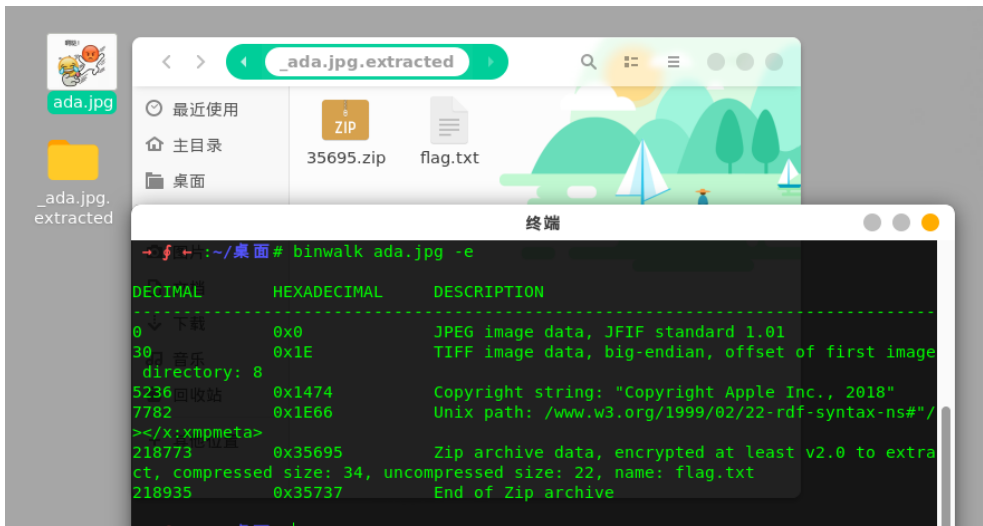
十六进制转换到十六进制 (例: 0x61或61或61/62) 删除 0x

0x730x640x6e0x690x730x630x5f0x320x300x310x38

十进制转换到十进制 (例: 97 98 99)

115100110105115999550484956

提交，发现并不是flag，binwalk分析得到压缩包里面有一个flag.txt被加密，使用上面解出的字符串作为密码得到flag



get flag:

flag{3XiF_iNf0rM@ti0n}

7、又一张图片，还单纯吗

又一张图片，还单纯吗

60

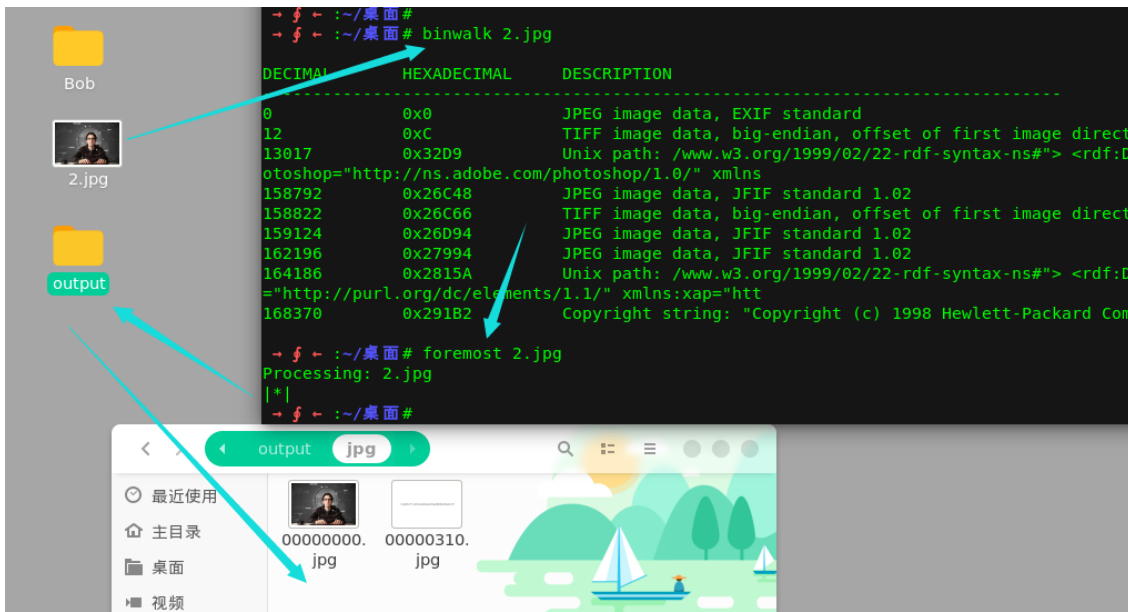
<http://123.206.87.240:8002/misc/2.jpg>

好像和上一个有点不一样

Flag

Submit

binwalk分析可知里面存在其它图片，利用foremost快速得到其中的图片



get flag:

```
fa1g{NSCTF_e6532a34928a3d1dadd0b049d5a3cc57}
```


8、猜

猜
60

<http://123.206.87.240:8002/misc/cai/QQ20170221-132626.png>

flag格式key{某人名字全拼}

Flag

Submit

根据提示，尝试进行图片识别



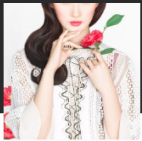
识图得到：刘亦菲

Baidu 识图

拖拽图片到此处或粘贴图片网址

识图一下

本地上传



图中可能是 刘亦菲

更多尺寸推荐

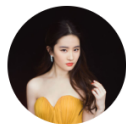
1080x1080 高清

580x1031

1000x562

422x453

+2张



刘亦菲(华语影视女演员、...

刘亦菲，1987年8月25日出生于湖北省武汉市，华语影视女演员、歌手，毕业于北京电影学院2002级表演系本科班。2002年主演个人首部电视剧《金粉世家》，从而踏入演艺圈。2003年因主演武侠剧《天龙八部》崭露头角。2004年凭借仙侠剧《仙剑奇侠传》赵灵儿一角获得了高人气与关注度。2005年因在武侠剧《神雕侠侣》中饰演小龙女受到广泛关注。2006年发行首张国语专辑《刘亦菲》和日文专辑《A...》 [百度百科](#)

[搜索更多相关结果](#) →

get flag:

key{liuyifei}

9、宽带信息泄露

宽带信息泄露

60

flag格式:

flag{宽带用户名}

conf.bin

Flag

Submit

根据提示，则需要找到某个用户，下载的文件是一个配置文件，可能是路由器的配置文件，使用工具 RouterPassView 打开查看宽带用户

```
File Edit View Options Help
[Icons]
<AddressingType val=DHCP />
<ExternalIPAddress val=0.0.0.0 />
<SubnetMask val=0.0.0.0 />
<DefaultGateway val=0.0.0.0 />
<DNSServers val=0.0.0.0,0.0.0.0 />
<MACAddress val=D0:C7:C0:43:53:69 />
<X_TP_IfName val=eth1 />
</WANIPConnection>
<WANIPConnection nextInstance=3 />
<WANPPPOConnection instance=1 >
  <Enable val=1 />
  <DefaultGateway val=10.177.144.1 />
  <Name val=pppoe_eth1_d />
  <Uptime val=671521 />
  <Username val=053700357621 />
  <Password val=210265 />
  <X_TP_IfName val=ppp0 />
  <X_TP_L2IfName val=eth1 />
  <X_TP_ConnectionId val=1 />
  <ExternalIPAddress val=10.177.150.82 />
  <RemoteIPAddress val=10.177.144.1 />
  <DNSServers val=0.0.0.0,0.0.0.0 />
```

PS: RouterPassView可以帮助你从你的路由器恢复您丢失密码的文件。

get flag;

flag{053700357621}

10、隐写2

eTB1IEFyZSBhIGhAY2tIciE=

加密 解密 解密结果以16进制显示

y0u Are a h@cker!

get flag:

flag{y0u Are a h@cker!}

11、多种方法解决

多种方法解决

60

在做题过程中你会得到一个二维码图片

<http://123.206.87.240:8002/misc/3.zip>

查看key.exe十六进制得到二维码，扫描get flag

```

Startup  KEY.exe
Edit As: Text /wrap  Run Script  Run Template
0          10         20         30         40         50         60         70         80
1 data:image/jpeg;base64,iVBORw0KGgoAAAANSUUhEUgAAAIUAAACFCAYAAAB12js8AAAAAXNSR0IArs4c6QAAA
  ARnQU1BAACxjwvOYQAAAAUcEhZcwAADsMAAA7DAcdvqGQAAARZSURBVHhe7ZKBitxIFgTv/396Tx564G1Uouic
  Kg19hwPCDcrMJ9m7/7n45zfdxe5Z3sJ7prHbf9rXO3P41LvYPctbeM80dvtP+3pnDp9yF7tneQvvmcZu/2lf78z
  hu+5i9yxv4T3T200/7eud68OT2H3LCft0l/ae9ZlTo+23pPvX7/rwJHbfcsI+3aW9Z33m1Gj7Len+9bs+PIndt5
  ywT3dp7lmfOTXafku6f/2uD09i9y0n7NNd2nvWZ06Ntt+S7l+/68MJc500OSWpcyexnFjfcSI+JW1ukpRfv+vDC
  XOTtDklqXMnsZxy33LCPiVtbpKUX7/rw1zk7Q5JalZJ7GcWN9ywj4lbW6S1F+/68MJc500OSWpcyexnFjfcSI+
  JW1ukpRfv+vDCXOTWE7a/i72PstJ2zfsHnOTpPz6XR9OmJvEctL2d7H3WU7avmH3mJsk5dfv+nDC3CSWk7a/i73
  PctL2DbvH3CQpv37XhxPmJrGctPld7H2Wk7Zv2D3mJkn59bs+nDA3ieWEfdNImylJnelP7H6bmyTl1+/6cMLcJJ
  YT9k0jbaYkdaansfttbpKUX7/rw1zk1h02DeNtJmS1Jmexu63uU1Sfv2uDyfmTWI5Yd800mZKUmD6Grvf5iZJ+
  fw7PjzJ7v12b33LSdtvsfuW75LuX7/rw5Ps3m/31rectP0Wu2/5Lun+9bs+PMnu/XZvfctJ22+x+5bvku5fv+vD
  k+zeb/fWt5y0/Ra7b/ku6f71+++HT0v+5l3+tK935vApyd+8y5/29c4cPiX5m3f5077emcOnJH/zLn/ar3d+/fl
  BpI+cMDeNtJkSywn79BP5uK+yfzTmppE2U2I5YZ9+Ih/3VfaPxtw00mZKLCfs00/k477K/tGYm0baTInlhH36iS
  xflT78TpI605bdPbF7lhvct54mvOaWJ6m4Z0kdaYtu3ti9yw3uG89TxrHNLE8Tcm7SepMW3b3xO5ZbnDfepR0j
  mlieZqGd5LUmbbs7onds9zgvvU06R3TxPXcSxPrW07YpyR1pqTNKUmDKUmDK5LUaXzdWB/eYX3LCfuUpM6UtDkl
  qTm1qXNSkjQnrxvrwzusbz1hn5LUmZ2pyR1piR1TkpsP/FLY314h/UtJ+xTkjpt0uaUpM6UpM5JSeo0ft34+v0
  
```

点击这里选择选择要转换成Base64的图片

复制 清空

```
n7FPD+pa1TK9O71S1T3Mv7WD3L5TS08P0pOZ107VvXfXcy/tyFcu+xtw/qwk/ZPTU9bE9dZL+1g9y0n7FPD+pa1TK9O
71sT1/P7EnOTWG5wb5LUmRptn3D/6b6+eX04YW4Syw3uTZI6U6PtE+4/3dc3rw8nzE1iucG9SVJnarR9ww2n+/rm9eGE
uUksN7g3SepMjibZPuP90X9+8PpwwN0mb72pYfzcn1rf8NHwffXXWhxPmJmnzXQ3r7+bE+pafhu+jr876cMLcJG2+q2
H93ZxY3/LT8H301VkfTpiBPm13Nay/mxPrW34avo++OuvDCXOT7OZGu7e+5YT9XYnlhH36DlffvsTcJLu50e6tbzlhfdi
OWGfvsPVux8xN8lubrR761tO2N+VWE7Yp+9w9e5HzE2ymxvt3vqWE/Z3JZY9uk7XL1+1GD3LX8avt8klhu2t5yc6F+/6
8OT2H3Ln4bvN4nlhu0tJyf61+/68CR23/Kn4ftNYrlhe8vjf71uz48id23/Gn4fpNYbtjecnKif/3+++HTnub0fd4zieUtvLfr01
y9PH7K05y+z3smbYF93Z9h6uXx095mtP3ec8klrfw3q7vcPXy+CIPc/o+75nE8hbe2/Udzv9X+sv/OP/881/SqvtcdpBh+
wAAAABJRU5ErkJggg==
```

还原生成的Base64编码为图片:



get flag:

```
KEY{dca57f966e4e4e31fd5b15417da63269}
```

12、闪的好快

闪的好快

60

这是二维码吗? 嗯。。。是二维码了, 我靠, 闪的好快。。。

题目来源: 第七季极客大挑战

masterGO.gif

打开图片发现是动图, 并且每一帧的动画都是一个二维码, 尝试分离每一帧, 使用工具GifSplitter进行分离, 但是分离出来的二维码不完整



此时可以利用工具Stegsolve进行每一帧的浏览



通过扫码发现每一帧都存在一个字符，将这18个字符进行拼接得到flag

get flag:

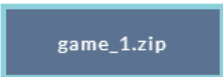
SYC{F1aSh_so_f4sT}

13、come_game

come_game

60

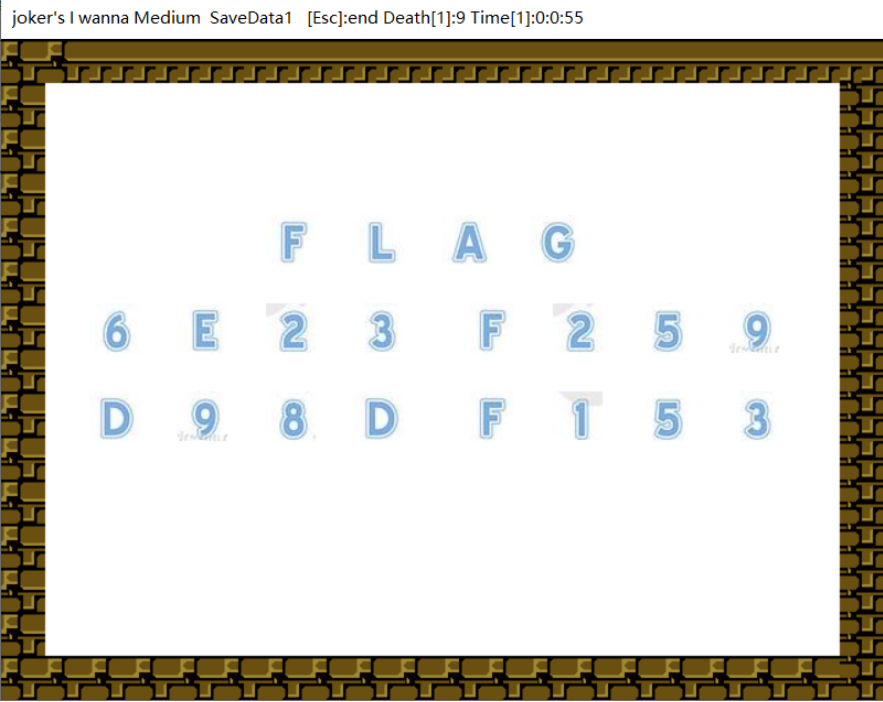
听说游戏通关就有flag
 题目来源：第七季极客大挑战



通过玩游戏(当游戏玩到第二关的时候)可以得到游戏配置文件 save1，十六进制查看save1，猜测字符2为通关的数字

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
:	00	01	32	00	00	41	00	05	43	00	00	00	00	00	00	00	.	2	
:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		

尝试将其修改为33 34 35，当到了第5关的时候可以拿到flag，游戏通关



get flag:

```
SYC{6E23F259D98DF153} #flag格式有问题
```

14、白哥的鸽子

白哥的鸽子

60

咕咕咕



将文件放入十六进制编辑器中，在后面得到一串特殊字符串

8D 47 DA 3E D1 EE CF 94 1A E6 2A C5 8E 3C F8 00	.GÚ>Ñiï".æ*Ăž<ø.
EA 03 A8 35 12 39 F0 8E 6C A2 9E 1D 66 E2 BB 87	è."5.9ðž1çž.fâ»†
74 F7 4B 65 B0 58 2F 01 3A 92 BF 1E 73 2A C7 49	t÷Ke°X/.'¿.s*ÇI
E6 03 A7 9D 14 11 1D 79 D0 9D 28 0E A5 1D 40 20	æ.s...yĐ.(.¥.©
78 DC 59 69 DA 8F 64 6E E6 7B A3 57 31 EE 8D DC	xŪYiŪ.dnæ{£Wlî.Ū
CB 62 45 62 89 EE 5B DC B6 73 01 E3 FF D9 66 67	ĔbEb&i[ŪŪs.ăyŪfg
32 69 76 79 6F 7D 6C 7B 32 73 33 5F 6F 40 61 77	2ivyo}l{2s3 o@aw
5F 5F 72 63 6C 40	rcl@

将字符串进行栅栏解密得到flag

栅栏密码

在下面的文本框输入明文或密文，点加密或解密，文本框中即可出现所得结果

加密 解密 列举加密 列举解密 栏数: 2 只列举完整匹配的

密文框:

```
fg2ivyo}l{2s3_o@aw__rc1@  
2栏:  
f3g_2oi@vaywo_}_lr{c2ls@  
3栏:  
flag{w22_is_v3ry_cool}@@  
4栏:  
fo3_g}__2lori{@cv2alysw@  
6栏:  
fv13argy{ _wc2o2o_li}s@_@  
8栏:  
fio{3@_cgv}2_a_l2ylsowr@  
12栏:  
f2vol23oa_rlgiy}{s_@w_c@
```

get flag:

flag{w22_is_v3ry_cool}

15、linux

linux 80

<http://123.206.87.240:8002/misc/1.tar.gz>
linux基础问题

终端下cat flag得到flag



get flag:

key{feb81d3834e2423c9903f4755464060b}

16、隐写3

隐写3

80

58d54bd3e134...

下载图片发现图片高度不正常，尝试更改，得到flag

```

it As: Hex | Run Script | Run Template
  0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
1: 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 %PNG.....IHDR
1: 00 00 02 A7 00 00 11 00 08 06 00 00 00 6D 7C 71 ...$.m|q
1: 35 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00 5...sRGB.@i.e..
1: 00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00 ..gAMA..t..ta...
1: 00 09 70 48 59 73 00 00 0E C4 00 00 0E C4 01 95 ..pHYs...A...A.
1: 2B 0E 1B 00 00 FF A5 49 44 41 54 78 5E EC BD 07 +...yIDATx^i%
1: A0 A5 57 59 EE FF EE BE 4F 9B DE 93 4C 7A 0F 84 WYiyi%O>B"Lz,,
1: 24 24 60 0C 04 A5 2B 20 45 10 10 BB 88 8A A8 57 $$.Y+ E..»`S`W
1: BD FC EF BD 7A F5 5A AE 7A BD 5E CB BD 2A 62 05 %iiz6Z@z^E%+b.
1: 04 69 52 04 E9 01 42 48 48 42 7A EF 7D 52 A6 CF .i.r.e.BHHBz1}R;I
1: 9C 7E 76 FD 3F BF F7 DB EF 39 6B 76 F6 4C 26 C9 e~vy?ç+0i9kv0L&E
1: 4C 32 E5 7B CE 59 7B F5 DE 9E 6F 7D 6B AD AF D0 L2â{îY{ôpžo}k-Đ
1: 15 2C 47 8E 1C 39 72 1C 90 60 88 2E 14 0A 3D DD .,Gž.9r...`=Y
1: DE 63 6F FD A5 53 C0 93 8D A7 D3 E9 F4 54 66 C5 pcoyWSÀ`.s0é0TfÅ
1: 62 D1 E5 34 BC 34 0D AD 56 CB 1A 8D 86 35 9B 4D bNâ4%4.-VE..+5>M
1: 17 R3 R3 R3 36 37 37 F7 72 98 21 70 87 DC 6E R7 **$677cr~lnifln.

```

Address	Value



get flag:

flag{He110_d4_ba1}

17、做个游戏(08067CTF)

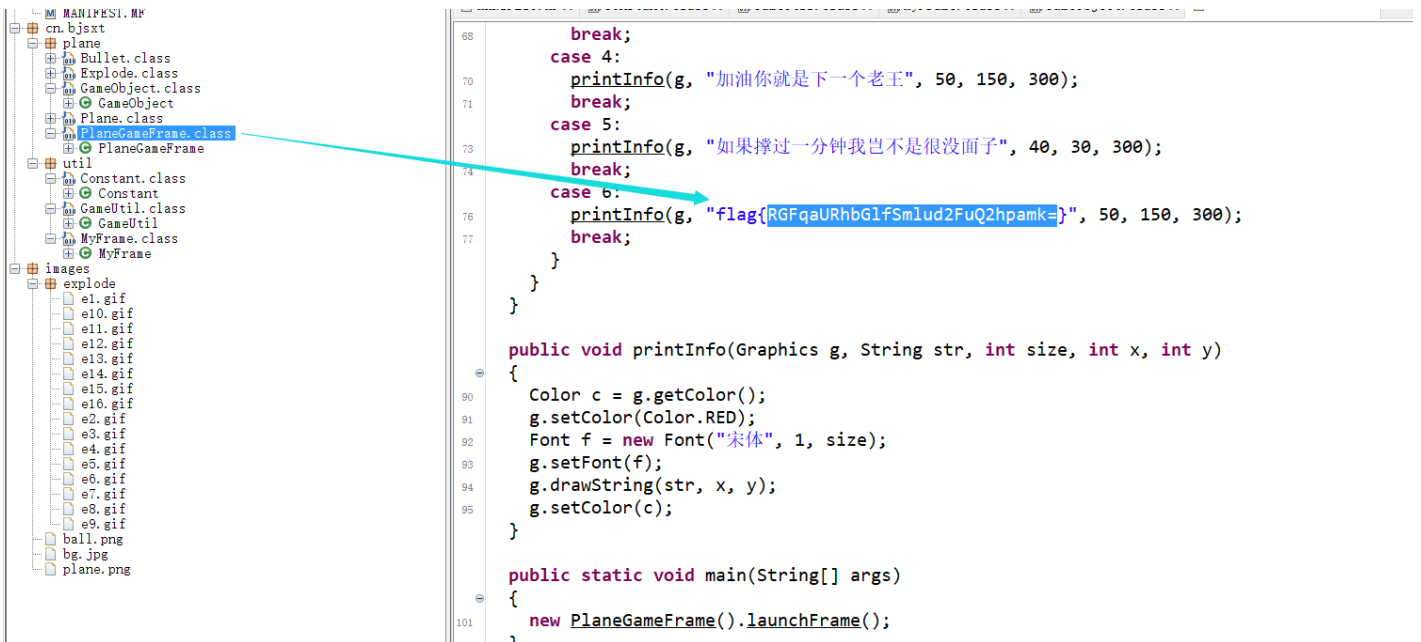
做个游戏(o8o67CTF)

80

坚持60秒

heiheihei.jar

懂点Android逆向的人都会很快做出来，使用jd-gui查看Java代码，在PlaneGameFrame.class文件中得到flag



get flag:

```
flag{DajiDali_JinwanChiji}
```

18、想蹭网先解开密码

想蹭网先解开密码

100

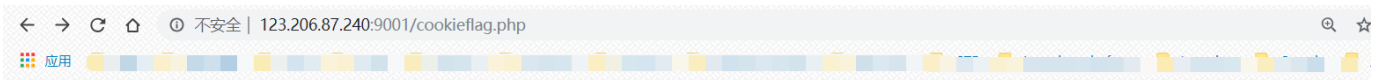
flag格式: flag{你破解的WiFi密码}

tips: 密码为手机号, 为了不为你, 大佬特地让我悄悄地把前七位告诉你

1391040**

Goodluck!!

作者@NewBee



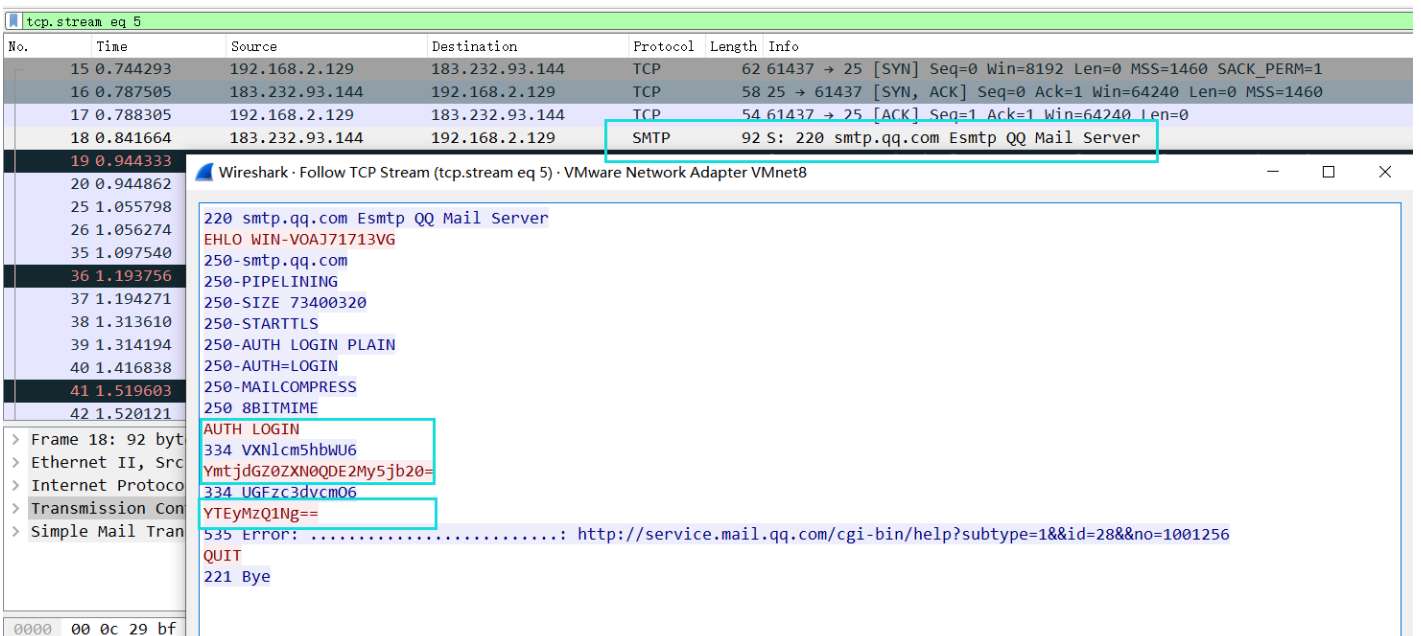
http://123.206.87.240:9001/123.exe

Login游戏界面



填写信息进行抓包，真的可以刷枪，你信不233333

过滤TCP可以看到特殊流量



可以看到，上面base64编码内容是某账号账户和密码

YmtjdGZ0ZXN0QDE2My5jb20=

加密 解密 解密结果以16进制显示

bkctftest@163.com

YTEyMzQ1Ng==

加密 解密 解密结果以16进制显示

a123456

利用账号登陆163邮箱得到flag



get flag:

flag{182100518+725593795416}

21、细心的大象

细心的大象

100

<https://share.weiyun.com/9287be0a629971ac53d97f39727eee18>

Flag

Submit

查看图片属性



foremost分离处压缩包，利用图片备注信息base64解码进行解密得到图片，修改图片高度得到flag

89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52	%PNG.....IHDR
00 00 01 F4 00 00 11 A4 08 06 00 00 00 CB D6 DF	...ö...ä...EÖ8
8A 00 00 00 09 70 48 59 73 00 00 12 74 00 00 12	Š...pHYs...t...
74 01 DE 66 1F 78 00 00 0A 4D 69 43 43 50 50 68	t.Łf.x...MiCCPPh
6F 74 6F 73 68 6F 70 20 49 43 43 20 70 72 6F 66	otoshop ICC prof
69 6C 65 00 00 78 DA 9D 53 77 58 93 F7 16 3E DF	ile...xÜ.SwX"+.>ß
F7 65 0F 56 42 D8 F0 B1 97 6C 81 00 22 23 AC 08	÷e.VB00±-l..">#-
C8 10 59 A2 10 92 00 61 84 10 12 40 C5 85 88 0A	È.Yc.'a...0Á...^.
56 14 15 11 9C 48 55 C4 82 D5 0A 48 9D 88 E2 A0	V...œHUÀ,Ö.H.^â
28 B8 67 41 8A 88 5A 8B 55 5C 38 EE 1F DC A7 B5	(,gAS`Z<U\8i.Ü\$u
7D 7A EF ED ED FB D7 FB BC E7 9C E7 FC CE 79 CF)ziíiûx0%çœçüïY
0F 80 11 12 26 91 E6 A2 6A 00 39 52 85 3C 3A D8	.e..š`æej.9R...<:Ø
1F 8F 4F 48 C4 C9 BD 80 02 15 48 E0 04 20 10 E6	..OHÄÉ%e..Hà. .æ
CB C2 67 05 C5 00 00 F0 03 79 78 7E 74 B0 3F FC	EÄg.Ä..ð.yx~t"?ü
01 AF 6F 00 02 00 70 D5 2E 24 12 C7 E1 FF 83 BA	.°...pô.š.Çáÿf°
50 26 57 00 20 91 00 E0 22 12 E7 0B 01 90 52 00	P&W ` `à" c R

BU

BUGKU{a1e5aSA}

get flag:

BUGKU{a1e5aSA}

22、爆照(08067CTF)

爆照(08067CTF)

100

flag格式 flag{xxx_xxx_xxx}

8.jpg

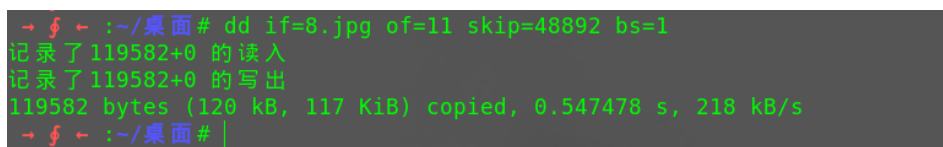
Flag

Submit

binwalk分析图片发现隐藏文件，利用binwalk和foremost分离隐藏文件，只能得到88文件其他的不到，此时利用dd命令进行分离



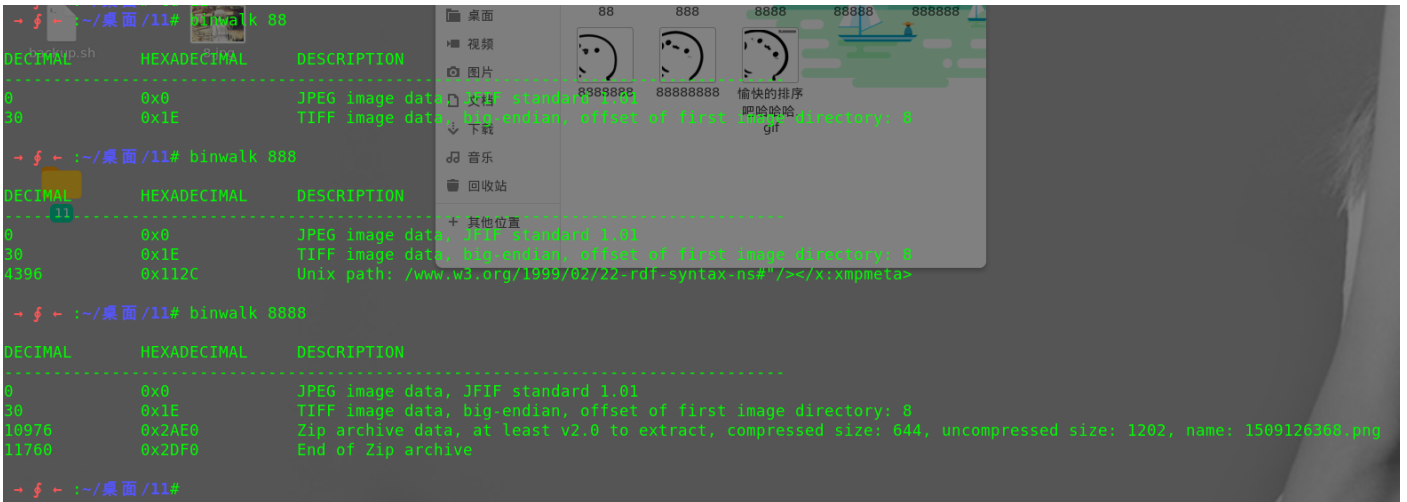
dd if=8.jpg of=11 skip=48892 bs=1



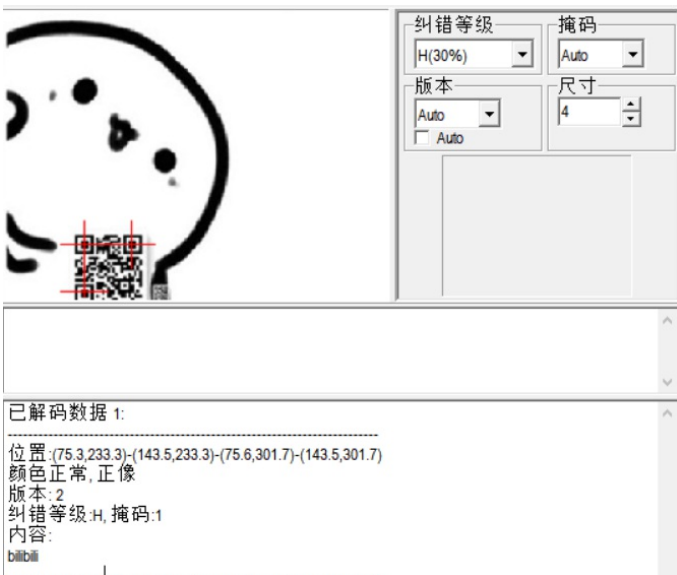
得到几张图片



binwalk分析这几张图片，发现前三张存在被修改的记录



第一张包含二维码直接扫描得到：bilibili



第二张图片属性中存在特殊字符串，对其进行解码



第三张图片binwalk分析，分离出压缩包，得到一张二维码，扫描得到：panama



根据题目flag提示，将上述得到的三个字符串组合成最终的flag

get flag:

```
flag{bilibili_silisili_panama}
```

23、猫片(安恒)

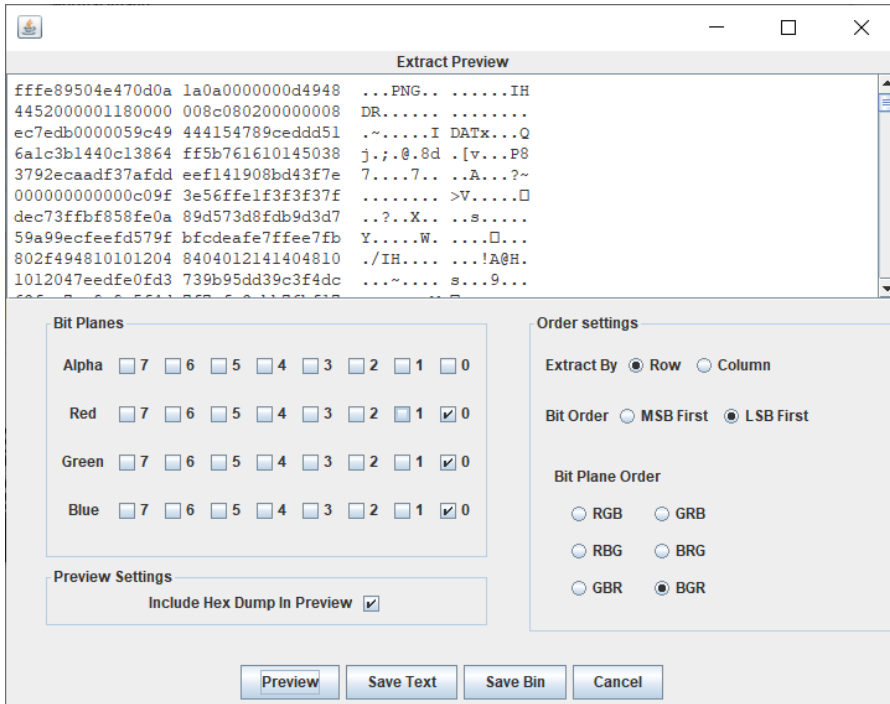
猫片(安恒)

100

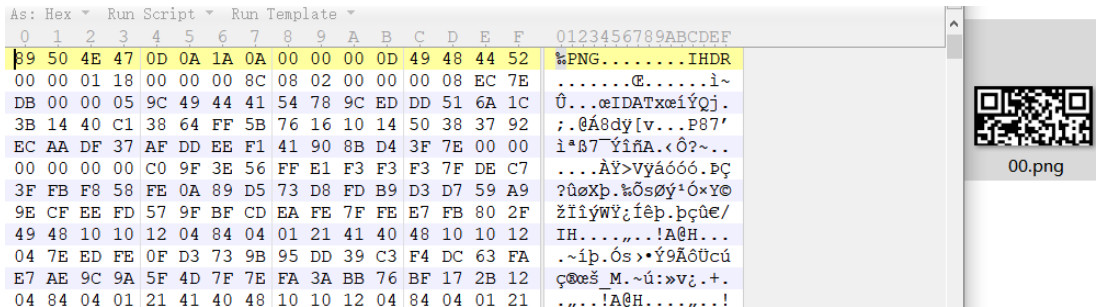
hint:LSB BGR NTFS

png

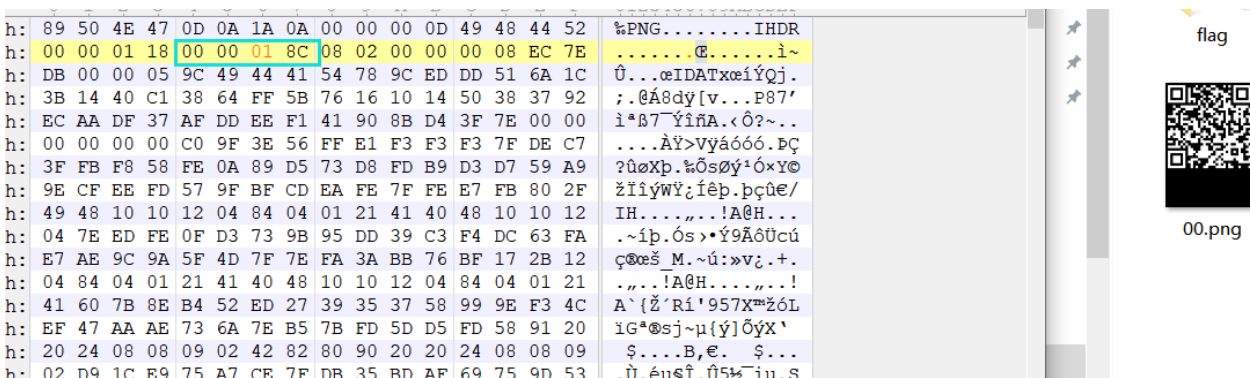
根据提示LSB隐写得到新的二维码



修改图片头部得到二维码



下意识修改图片高度，得到完整二维码



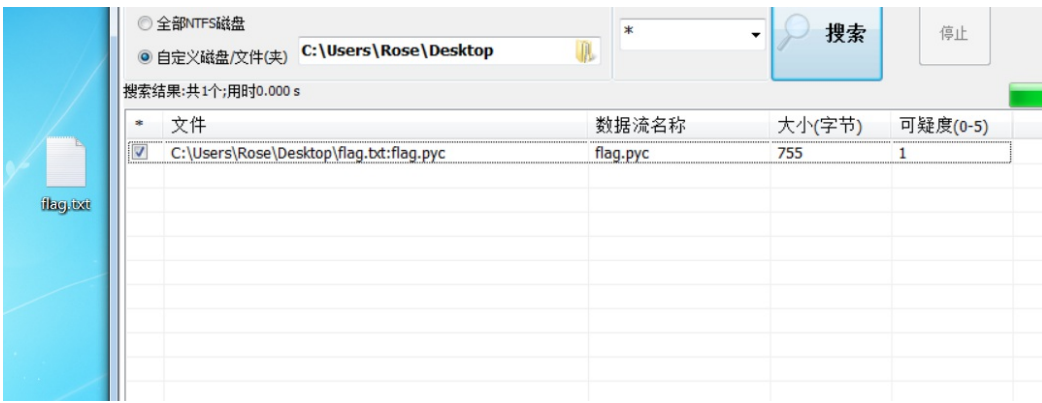
扫描二维码得到云盘连接: <https://pan.baidu.com/s/1pLT2J4f>



链接下载得到flag.rar压缩包,使用WinRAR解压,得到flag.txt,发现并不是flag,依据题目提示还有一个提示NTFS没有用到,于是利用工具ntfsstreamseditor进行提取,得到一个pyc文件,将pyc反编译回去,得到一个python的flag加密函数。



NTFS数据提取



pyc反编译

```

C:\WINDOWS\system32\cmd.exe
...loads>uncompyle6 flagg.pyc
# uncompyle6 version 3.3.4
# Python bytecode 2.7 (62211)
# Decompile from: Python 3.7.0 (v3.7.0:1bf9cc5093, Jun 27 2018, 04:06:47) [MSC v.1914 32 bit (Intel)]
# Embedded file name: flag.py
# Compiled at: 2017-12-05 23:42:15
import base64

def encode():
    flag = '*****'
    ciphertext = []
    for i in range(len(flag)):
        s = chr(i + ord(flag[i]))
        if i % 2 == 0:
            s = ord(s) + 10
        else:
            s = ord(s) - 10
        ciphertext.append(str(s))

    return ciphertext[::-1]

ciphertext = [
    '96', '65', '93', '123', '91', '97', '22', '93', '70', '102', '94', '132', '46', '112', '64', '97', '88', '80', '82',
    '137', '90', '109', '99', '112']
# okay decompiling flagg.pyc

```

编写相应的解密函数得到解密的flag

```

Python 3.7.0 (v3.7.0:1bf9cc5093, Jun 27 2018, 04:06:47) [MSC v.1914 32 bit (Intel)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: C:\Users\Joker\Downloads\encode.py =====
f
fl
fla
flag
flag{
flag{Y
flag{Y@
flag{Y@e
flag{Y@e_
flag{Y@e_C
flag{Y@e_C1
flag{Y@e_C13
flag{Y@e_C13v
flag{Y@e_C13ve
flag{Y@e_C13veR
flag{Y@e_C13veR_
flag{Y@e_C13veR_C
flag{Y@e_C13veR_C1
flag{Y@e_C13veR_C1E
flag{Y@e_C13veR_C1Ev
flag{Y@e_C13veR_C1Eve
flag{Y@e_C13veR_C1Ever
flag{Y@e_C13veR_C1Ever!
flag{Y@e_C13veR_C1Ever!}
>>>

# uncompyle6 version 3.3.4
# Python bytecode 2.7 (62211)
# Decompile from: Python 3.7.0 (v3.7.0:1bf9cc5093, Jun 27 2018, 04:06:47) [MSC v.1914 32 bit (Intel)]
# Embedded file name: flag.py
# Compiled at: 2017-12-05 23:42:15
import base64

def encode():
    flag = '*****'
    ciphertext = []
    for i in range(len(flag)):
        s = chr(i + ord(flag[i]))
        if i % 2 == 0:
            s = ord(s) + 10
        else:
            s = ord(s) - 10
        ciphertext.append(str(s))

    return ciphertext[::-1]

ciphertext = ['96', '65', '93', '123', '91', '97', '22', '93', '70', '102', '94', '132', '46', '112', '64', '97', '88', '80', '82', '137', '90', '109', '99', '112']
# okay decompiling flagg.pyc

def decode():
    ci = ['96', '65', '93', '123', '91', '97', '22', '93', '70', '102', '94', '137', '90', '109', '99', '112']
    flag = ""
    ci.reverse()
    for i in range(len(ci)):
        if i % 2 == 0:
            s = int(ci[i]) - 10
        else:
            s = int(ci[i]) + 10
        s = chr(i + s)
        flag += s
    print(flag)

decode()

```

get flag:

```
flag{Y@e_C13veR_C1Ever!}
```

24、多彩

多彩

100

lipstick.png

Flag

Submit

该题脑洞很大!!!!

附上安全脉搏一篇详细的writeup

<https://www.secpulse.com/archives/69465.html>

25、旋转跳跃

旋转跳跃

100

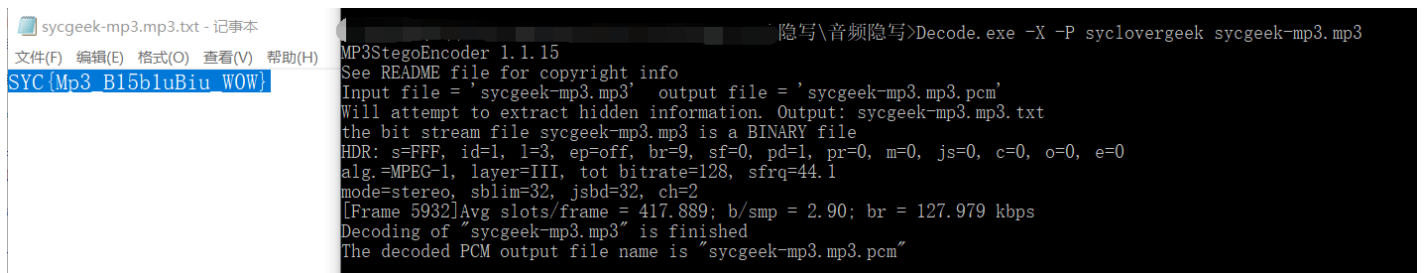
熟悉的声音中貌似又隐藏着啥, key: syclovergeek

题目来源: 第七季极客大挑战

sycgeek-mp3_2....

利用音频分析工具MP3Steno, 结合key直接进行解码得到 sycgeek-mp3.mp3.txt

```
Decode.exe -X -P syclovergeek sycgeek-mp3.mp3
```

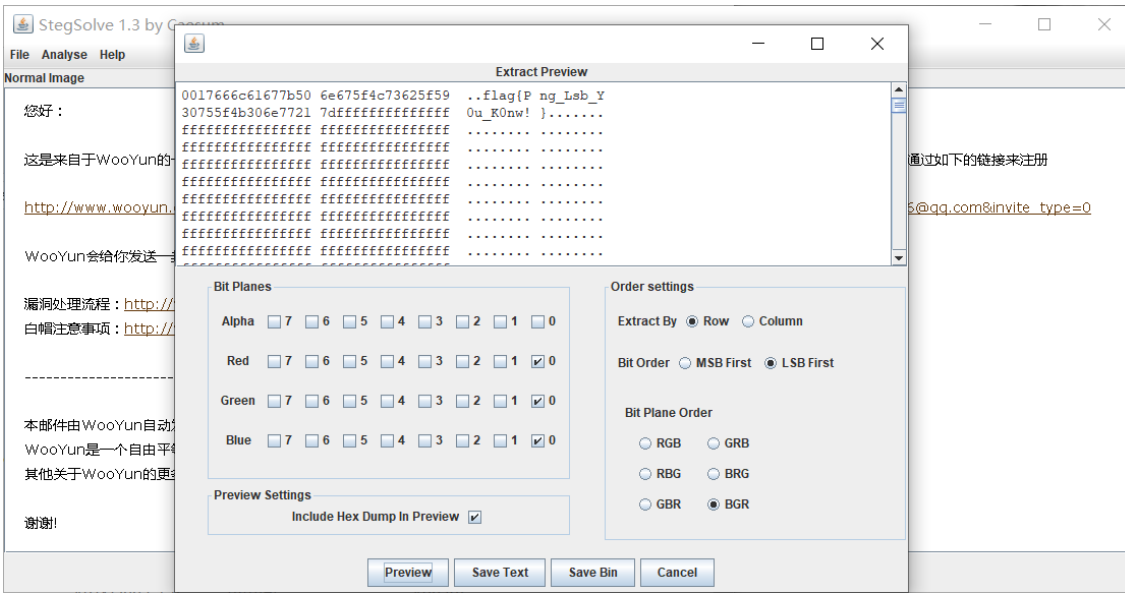


```
sycgeek-mp3.mp3.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
SYC{Mp3_B15b1uBiu_W0W}
MP3StegoEncoder 1.1.15
See README file for copyright info
Input file = 'sycgeek-mp3.mp3' output file = 'sycgeek-mp3.mp3.pcm'
Will attempt to extract hidden information. Output: sycgeek-mp3.mp3.txt
the bit stream file sycgeek-mp3.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=0, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=stereo, sblim=32, jsbd=32, ch=2
[Frame 5932]Avg slots/frame = 417.889; b/smp = 2.90; br = 127.979 kbps
Decoding of "sycgeek-mp3.mp3" is finished
The decoded PCM output file name is "sycgeek-mp3.mp3.pcm"
```

get flag:

```
SYC{Mp3_B15b1uBiu_W0W}
```

26、普通的二维码



get flag:

flag{Png_Lsb_Y0u_K0nw!}

28、神秘的文件

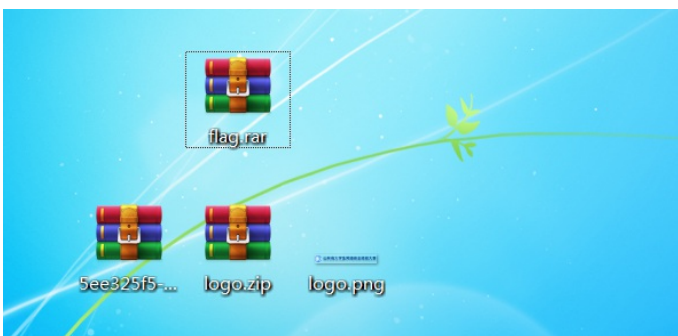
神秘的文件

100

来源：第七届山东省大学生网络安全技能大赛

5ee325f5-44c6-...

分析压缩包，可知明文攻击，利用WinRAR解压，并且压缩图片logo.png作为明文攻击





得到口令：q1w2e3r4，解压得到word文档发现并没有什么



哪有什么 WriteUP，别想了，老老实实做题吧！

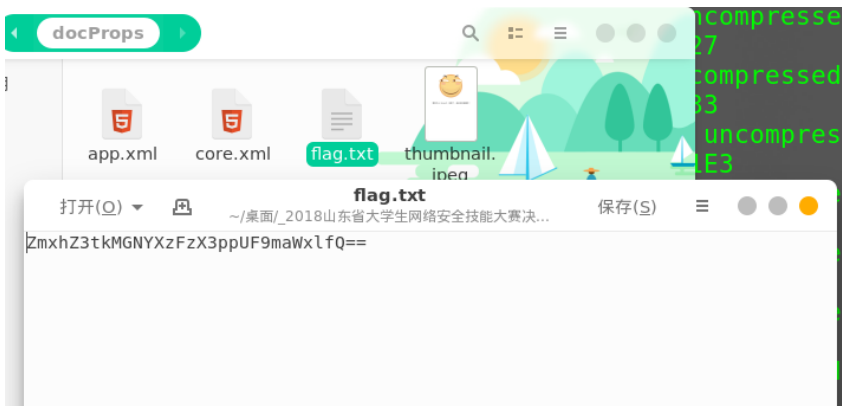
利用binwalk分析word文档得到发现存在隐藏文件


```

-> $ - ~/桌面# binwalk 2018山东省大学生网络安全技能大赛决赛writeup.docx
Bob
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         Zip archive data, at least v2.0 to extract, compressed size:
678         0x2A0      Zip archive data, at least v2.0 to extract, compressed size:
1370        0x55A      Zip archive data, at least v1.0 to extract, compressed size:
11.jpeg
37875       0x93F3     Zip archive data, at least v2.0 to extract, compressed size:
39207       0x9927     Zip archive data, at least v2.0 to extract, compressed size:
39751       0x9B33     Zip archive data, at least v1.0 to extract, compressed size:
ge1.png
262627      0x401E3    Zip archive data, at least v2.0 to extract, compressed size:
263791      0x4066F    Zip archive data, at least v2.0 to extract, compressed size:
266755      0x41204    Zip archive data, at least v2.0 to extract, compressed size:
xml
266759      0x4181F    Zip archive data, at least v2.0 to extract, compressed size:
266857      0x41970    Zip archive data, at least v2.0 to extract, compressed size:
xml.rels
269244      0x41BBC    Zip archive data, at least v2.0 to extract, compressed size:
270175      0x41F5F    Zip archive data, at least v2.0 to extract, compressed size:
270991      0x4228F    Zip archive data, at least v2.0 to extract, compressed size:
272048      0x426B0    End of Zip archive

```

分离文件找到flag.txt解码得到flag



ZmxhZ3tkMGNYXzFzX3ppUF9maWxlfQ==

加密 解密 解密结果以16进制显示

flag{d0cX_1s_ziP_file}

get flag:

flag{d0cX_1s_ziP_file}

update+ing

转载于:<https://www.cnblogs.com/qftm/p/11037200.html>