

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	10	D4	2D	7D	3B	43	14	00	31	43	14	00	37	9B	q0.0-;/B..QB..w2
DA	78	3A	2D	0F	E2	C3	EB	FA	54	0D	0D	BE	AF	03	A5	Úx:-.âÃëúT..¾-.¥
E7	95	1E	E5	33	0F	98	97	FE	EE	ED	AA	43	72	01	57	ç•.đ3.~-þîíªCr.W
1D	64	06	8A	28	03	D0	A8	A2	8A	00	28	A2	8A	00	28	.d.Š(.Ð"¢Š.(¢Š.(
A2	8A	00	FF	26	23	31	30	37	3B	26	23	31	30	31	3B	¢Š.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}ÛÛ

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

50

2.rar

解压压缩包得到一张图片

Bu

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

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	...<...f1 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)

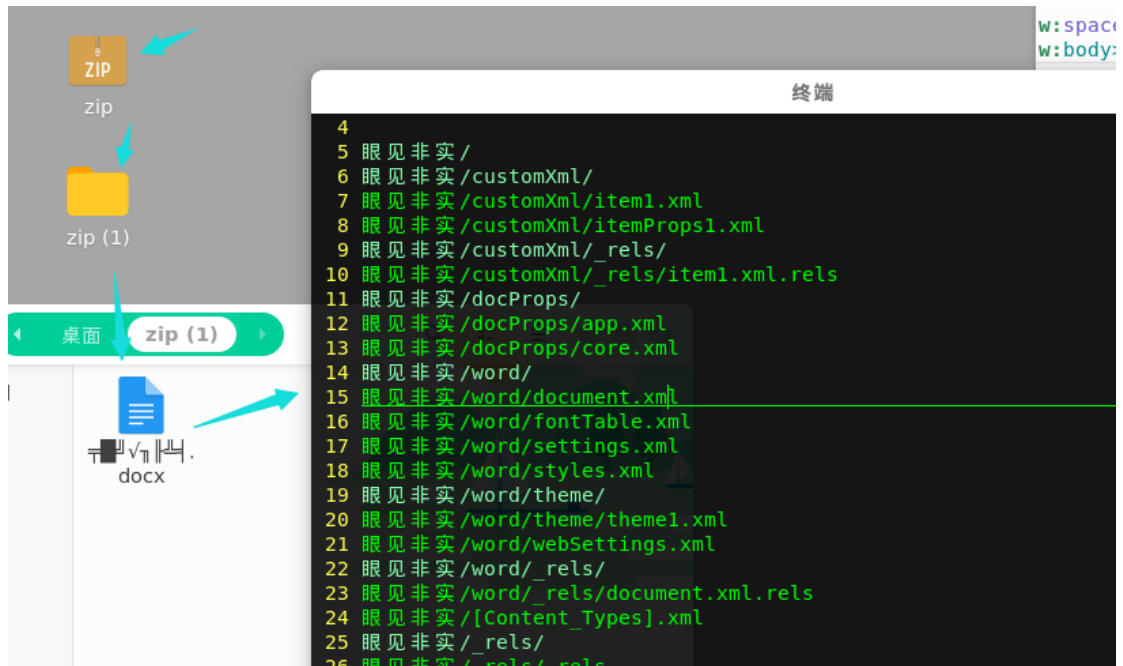
50

zip

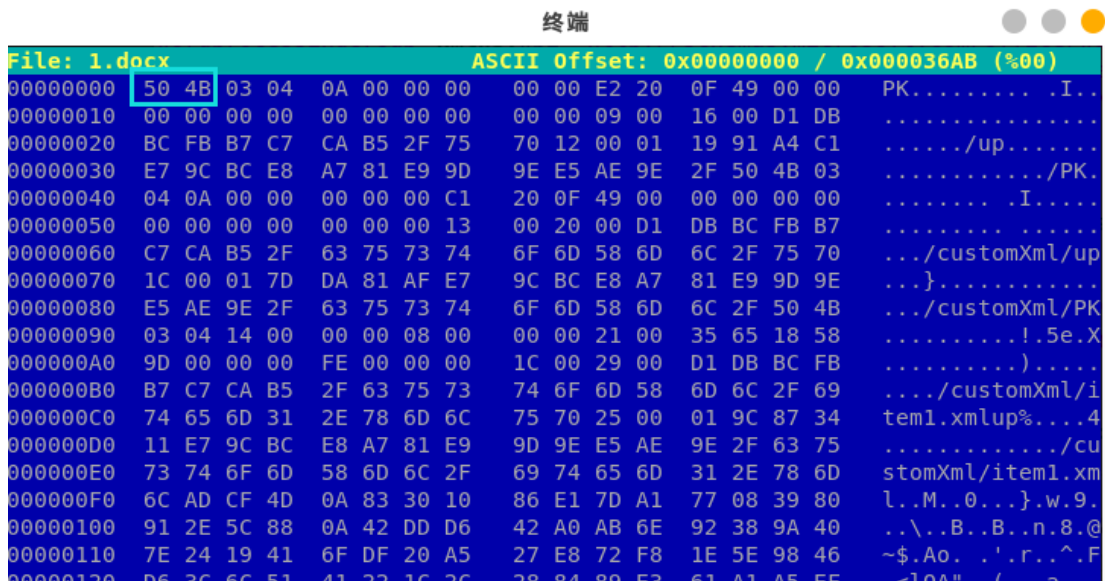
Flag

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

● ● ●

```
-> $ - ~/.桌面/zip (1)/1/1# cd word/  
-> $ - ~/.桌面/zip (1)/1/1/word# cat *.xml | grep flag  
<w:document xmlns:wpc="http://schemas.microsoft.com/office/word/2010/wordprocessingCanvas" xmlns:mc="http://schemas.openxmlformats.org/markup-compatibility/2006" xmlns:o="urn:schemas-microsoft-com:office:office" xmlns:r="http://schemas.openxmlformats.org/officeDocument/2006/relationships" xmlns:m="http://schemas.openxmlformats.org/officeDocument/2006/math" xmlns:v="urn:schemas-microsoft-com:vml" xmlns:wpg="http://schemas.microsoft.com/office/word/2010/wordprocessingDrawing" xmlns:wp="http://schemas.openxmlformats.org/drawingml/2006/wordprocessingDrawing" xmlns:w10="urn:schemas-microsoft-com:office:word" xmlns:w="http://schemas.openxmlformats.org/wordprocessingml/2006/main" xmlns:w14="http://schemas.microsoft.com/office/word/2010/wordml" xmlns:w15="http://schemas.microsoft.com/office/word/2012/wordml" xmlns:wpg="http://schemas.microsoft.com/office/word/2010/wordprocessingGroup" xmlns:wpi="http://schemas.microsoft.com/office/word/2010/wordprocessingInk" xmlns:wne="http://schemas.microsoft.com/office/word/2006/wordml" xmlns:wps="http://schemas.microsoft.com/office/word/2010/wordprocessingShape" mc:Ignorable="w14 w15 wp14"><w:body><w:p w:rsidR="002B3D8D" w:rsidRDefault="002B3D8D"><w:t>Flag</w:t></w:r><w:r><w:t>在这里啦！ </w:t></w:r></w:p><w:p w:rsidR="002B3D8D" w:rsidRPr="002B3D8D" w:rsidRDefault="002B3D8D"><w:pPr><w:rPr><w:rFonts w:hilite="eastAsia"/><w:vanish/></w:rPr></w:pPr><w:r w:rsidRPr="002B3D8D"><w:rPr><w:vanish/></w:rPr><w:t>flag{F1@g}</w:t></w:r><w:bookmarkStart w:id="0" w:name="GoBack"/><w:bookmarkEnd w:id="0"/></w:p><w:sectPr w:rsidR="002B3D8D" w:rsidRPr="002B3D8D"><w:pgSz w:w="11906" w:h="16838"/><w:pgMar w:top="1440" w:right="1800" w:bottom="1440" w:left="1800" w:header="851" w/footer="892" w:gutter="0"/><w:cols w:
```

get flag:

```
flag{F1@g}
```

6、啊哒

啊哒

50

有趣的表情包

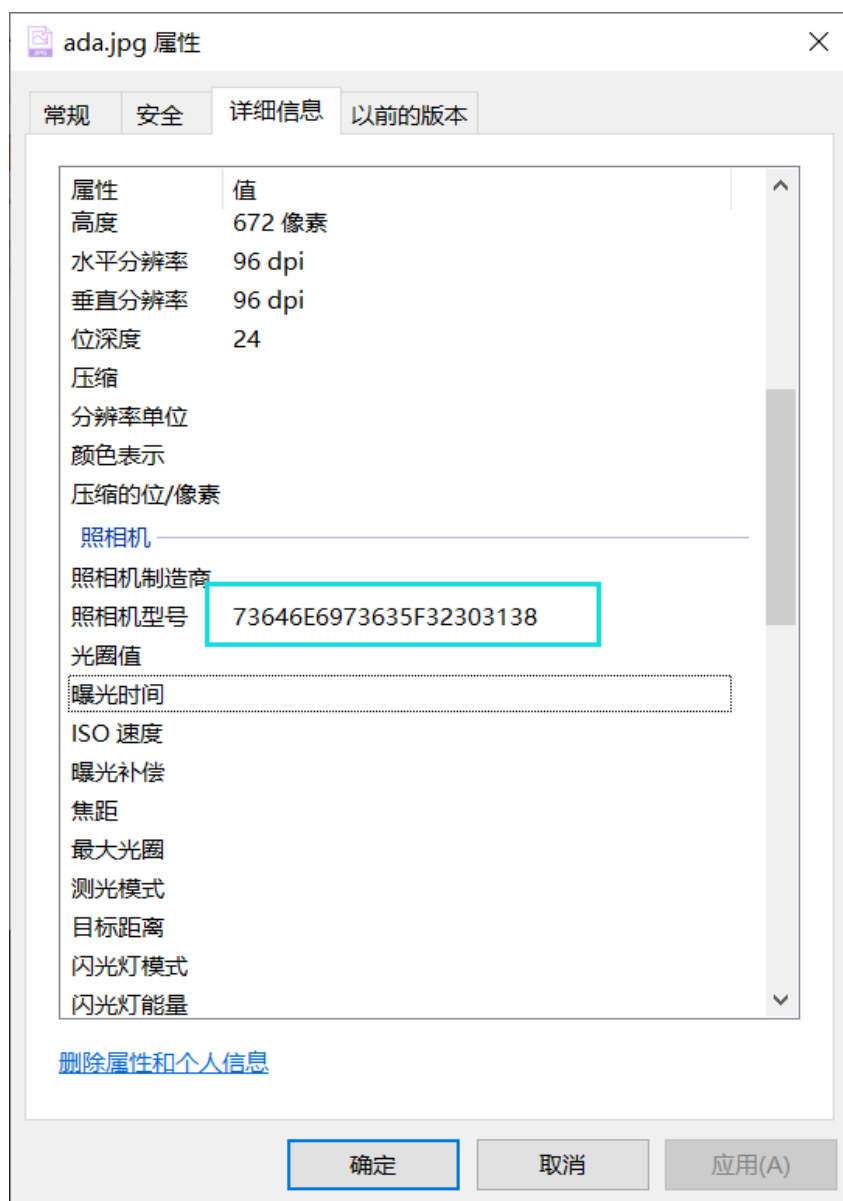
来源：第七届山东省大学生网络安全技能大赛

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

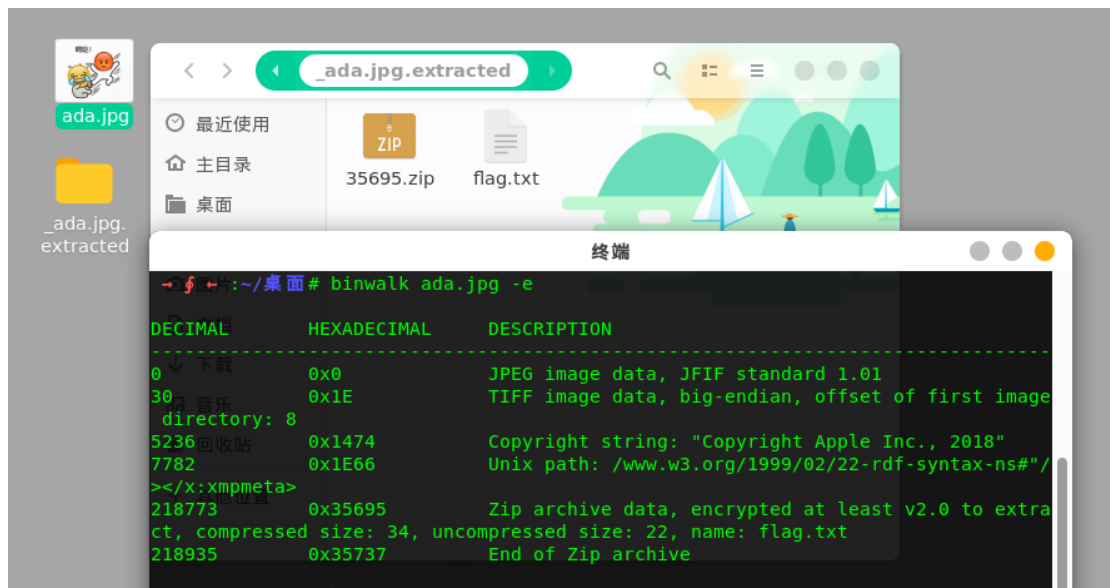
0x730x640x6e0x690x730x630x5f0x320x300x310x38

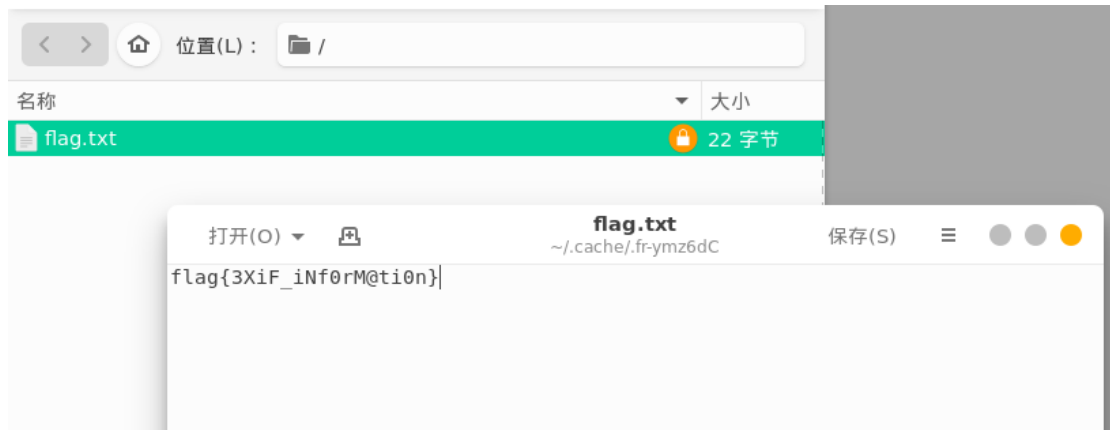
十进制转换到

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

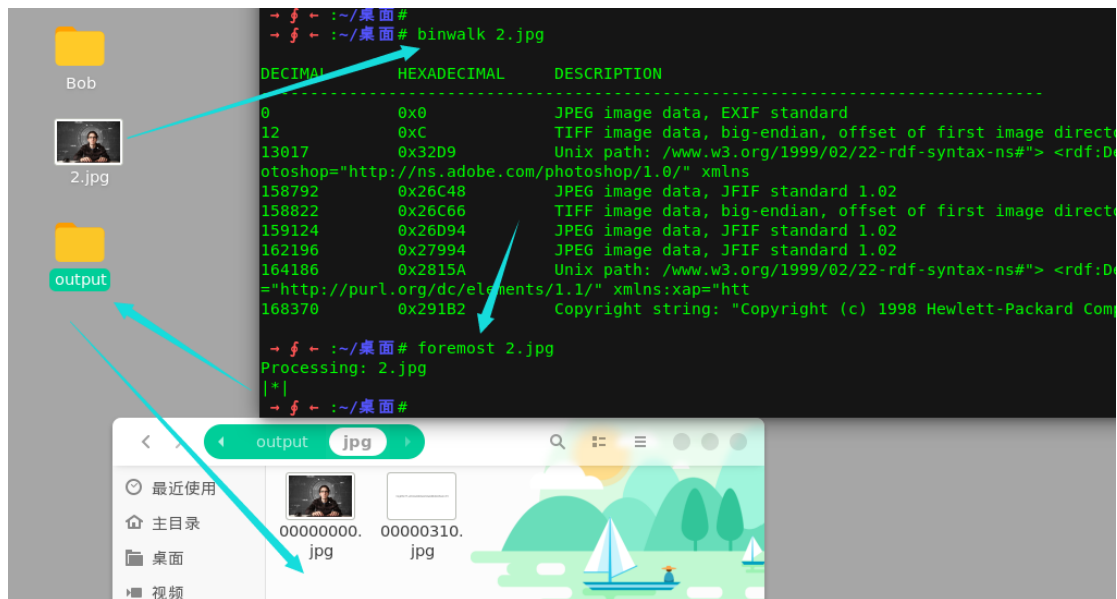
<http://123.206.87.240:8002/misc/2.jpg>

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:

```
falg{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}

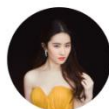
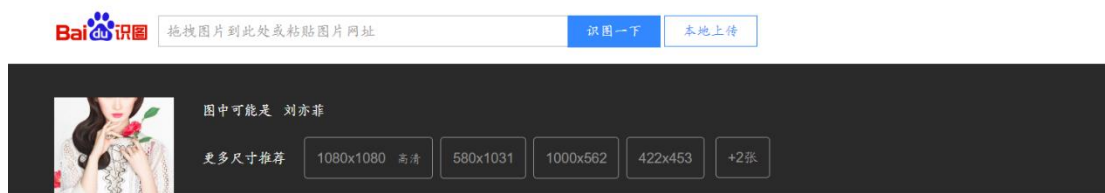
Flag

Submit

根据提示，尝试进行图片识别



识图得到：刘亦菲



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 />
<WANPPPConnection 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

隐写2

60

Welcome_.jpg

Flag

Submit

foremost 分离图片中存在文件，根据提示进行压缩包爆破

告诉你们一个秘密，密码是3个数哦。

查理曼：

查理曼，法兰克王国国王，征服了西欧与中欧大部分土地，具有了至高无上的权威，下令全国人民信仰基督教，查理重振了西罗马帝国。

雅典娜：

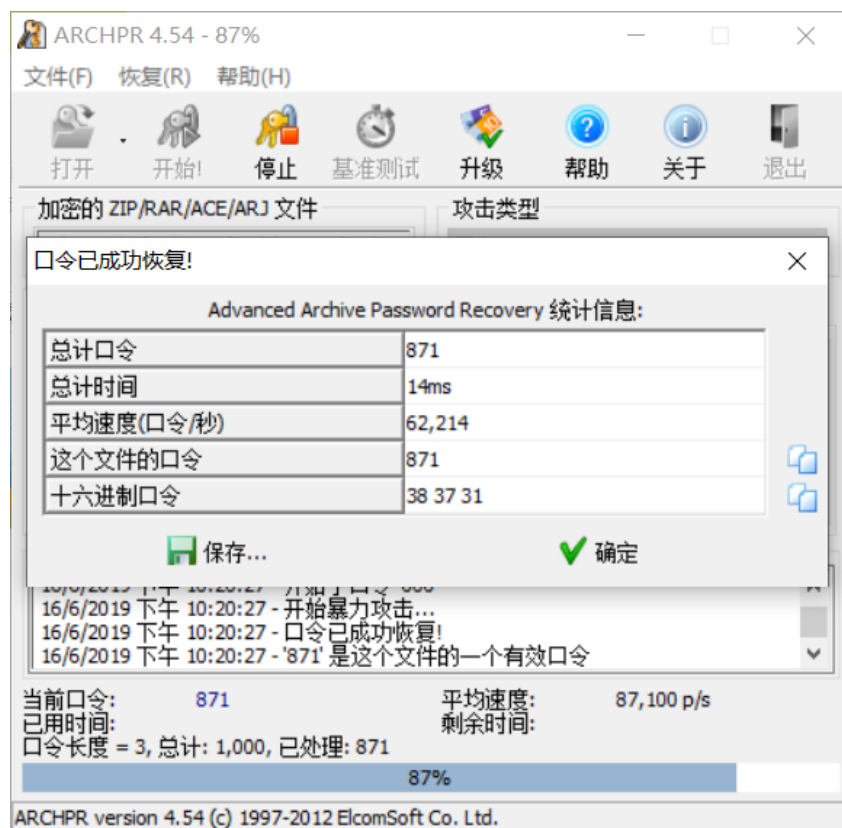
女神帕拉斯·雅典娜，是希腊神话中的女战神也是智慧女神，雅典是以她命名的。

兰斯洛特，

英格兰传说中的人物，是亚瑟王圆桌骑士团中的一员。看上去就是一个清秀年轻的帅小伙儿，由于传说中他是一名出色的箭手，因此梅花J手持箭支。兰斯洛特与王后的恋爱导致了他与亚瑟王之间的战争。

Hint:

其实斗地主挺好玩的。



取出图片查看其十六进制得到 flag

t As: Hex ▾ Run Script ▾ Run Template ▾																	0123456789ABCDEF													
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F														
:	76	83	BE	19	02	12	19	85	DD	F5	2F	71	D9	F8	ED	F8	vf%.....Yô/qÜøíø													
:	D6	32	7B	25	E4	F1	53	17	8C	80	50	37	D7	1D	BF	9C	Ö2{‰ñS.œP7×.¿œ													
:	A0	2E	B0	29	AC	A6	B1	AD	38	00	A3	62	CF	8C	69	6D	.°)¬!±-8.fbiGim													
:	CB	15	9F	6F	6C	A0	86	25	6E	12	70	EB	BC	69	6B	41	E.Yol †%n.pé%ikA													
:	23	E4	67	D4	FF	D9	20	20	20	20	66	31	40	67	7B	65	#ägÔyÜ f1@g{e													
:	54	42	31	49	45	46	79	5A	53	42	68	49	47	68	41	59	TB1IEFyZSBhIGhAY													
:	32	74	6C	63	69	45	3D	7D	20	20	20	20	20	0D	0A	20	2tlciE=} ..													
:	1A																.													

eTB1IEFyZSBhIGhAY2tlciE=

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,iVBORw0KGgoAAAANSUHEUgAAAIUAAACFCAYAAAB12js8AAAAAXNSR0Iars4c6QAAA
  ARnQv1BAAcXjwv8YQAAAAUcEhZcwAADsMAAA7DAdcvqGQAAARZSURBVHhe7ZKBitxIFgTv/396Tx564G1Uouic
  Kg19hwPCDcrMJ9m7/7n45zfdxe5Z3sJ7prHbf9rXO3P4lLvYPctbeM80dvtP+3pnDp9yF7tneQvvmcZu/2lf78z
  hU+5i9yxv4T3T200/7eud68OT2H3LCft0l/ae9ZlTo+23pPvX7/rwJHbfcsI+3aW9Z33mlGj7Len+9bs+PIndt5
  ywT3dp7lmfOTXafku6f/2uD09i9y0n7NNd2nvWZ06Ntt+S7l+/68MJc500OSWpcyexnFjfcSI+JWlupkRfv+vDC
  XOTtdklqXmnsZxY33LCPiVtbpKUX7/rwwlzk7Q5JalZJ7GcWN9ywj4lbW6S1F+/68MJc500OSWpcyexnFjfcSI+
  JWlupkRfv+vDCXOTWE7a/i72PstJ2zfsHnOTpPz6XR9OmJvBctL2d7H3WU7avmH3mJsk5dfv+nDC3CSWk7a/i73
  PctL2DbvH3CQpv37XhxPmJrGctPlD7H2Wk7Zv2D3mJkn59bs+nDA3ieWEfdNImylJnelP7H6bmyTl1+/6cMLcJJ
  YT9k0jbaYkdaansfttbpKUX7/rwwlzk1hO2DeNtJmslJmexu63uUlsfv2uDYfMTWI5Yd800mZKUmd6Grvf5izJ+
  fw7PjzJ7v12b33LSdtvsfuW75LuX7/rw5Ps3m/3lrectP0Wu2/5Lun+9bs+PMnu/XZvfctJ22+x+5bvku5fv+vD
  k+zeb/fWt5y0/Ra7b/ku6f7l+++HT0v+5l3+tkK935vApyd+8y5/29c4cPiX5m3f5077emcOnJH/zLn/ar3d+/f1
  BpI+cMDeNtJkSywn79BP5uK+yfzTmpeE2U2I5YZ9+Ih/3VfaPxtw00mZKLCfs00/k477K/tGym0baTInlhH36is
  xflT78TpI605bdPbF7lhvct54mvWOaWJ6m4Z0kdaYtu3ti9yw3uG89TXrHNLE8Tcm7SepMW3b3x05ZbnDfepr0j
  mlieZqGd5LUmbbs7onds9zgvvU06R3TxPXCxSxPrW07YpyR1pqTNKUmdKUmdk5LUaXzdWB/eYX3LCfuUpM6UtDkl
  qTMLqXNSkjQNrXvrwzusbz1hn5LUmZi2pyR1piR1TkpsP/FlY314h/UtJ+xTkjpt0uaUpM6UpM5JSeo0ft34+vO
```

点击这里选择要转换成Base64的图片

复制 清空

```
n/FPD+paITK9O/TS13Mv/WU3LSTsU8P6ipQZ10/vvwxPxcy/TYPCU+XTW/qWk/ZP1U9DE9aZL+I9gyun/FPD+paITK9O
71sT1/P7EnOTWG5wb5LUmRptn3D/6b6+eX04YW4Sww3uTz16U6PtE+4/3dc3rw8nzE1iucG9SVJnarR9ww2n+/rm9eGE
uUksN7g3SepMjbZPuP90X9+8PpwwN0mb72pYfzcn1rf8NHwffXXWhxPmJmnzXQ3r7+bE+pafhu+jr876cMLCJG2+q2
H93ZxY3/LT8H301VkfTibpM13Nay/mxPrW34avo++OuvDCXOT7OZGu7e+5YT9XynlhH36DlFvTsCjLu50e6tbzlh1di
OWGfvsPVux8xN8lubrR761tO2N+VWE7Yp+9w9e5He2ymxvt3vqWE/Z3lZYT9uk7XL1+1GD3LX8avt8klhu2t5yc6F+/6
8OT2H3Ln4bvN4nlhu0tYf61+/68CR23/Kn4ftNYrlhe8vJif71uz48id23/Gn4fpNYbtjecnKif/3+++HTnub0fd4zieUtlfrO1
y9PH7K05y+z3smsbyF93Z9h6uXx095mtP3ec8klrfw37vcPxy+CIPc/o+75nE8hbe2/Udzv9X+sv/OP/881/SqtvcdpBh+
wAAAABJRUErkkggg==
```

还原生成的Base64编码为图片:



get flag:

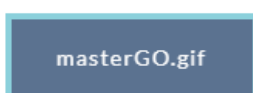
```
KEY{dca57f966e4e4e31fd5b15417da63269}
```

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



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{FlaSh_so_f4sT}
```

13、come_game

come_game
60

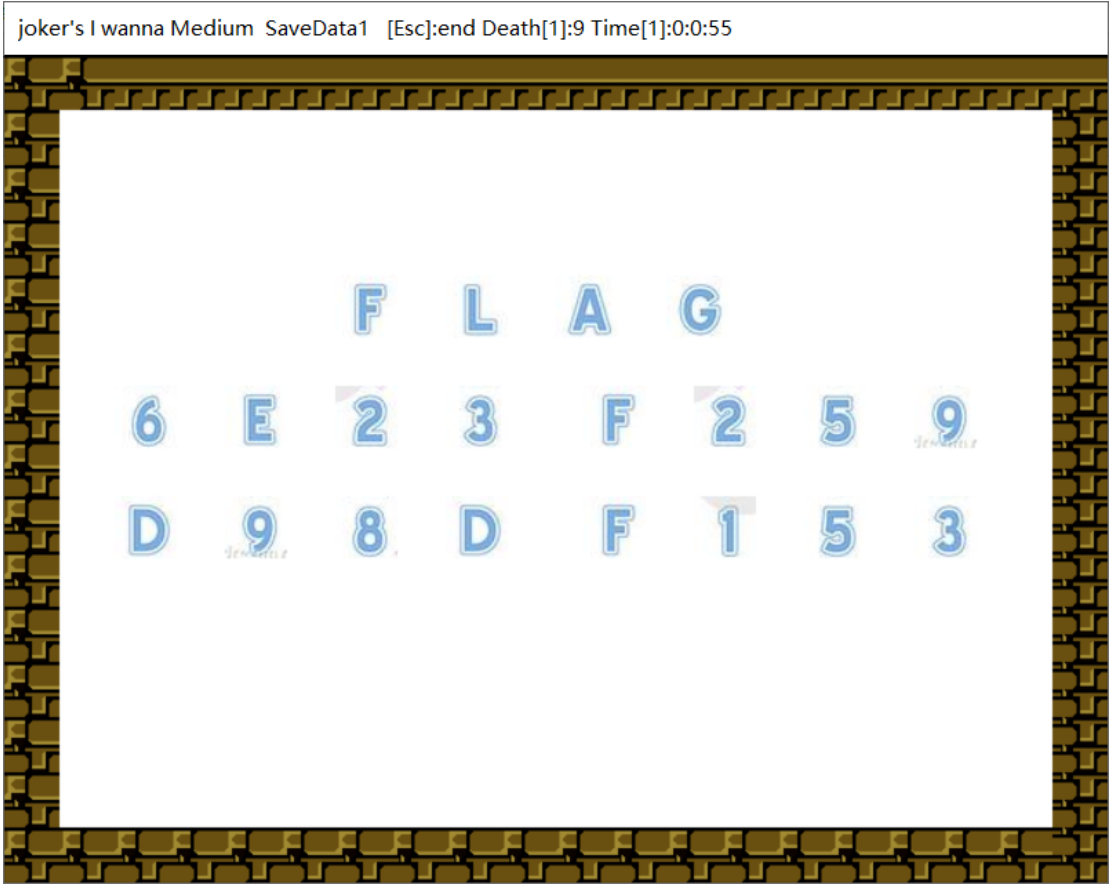
听说游戏通关就有flag
题目来源：第七季极客大挑战

game_1.zip

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	..	A	..	C									
:	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 关的时候可以得到 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

jpg

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>Ñîĩ".æ*ĂŽ<ø.
EA 03 A8 35 12 39 F0 8E 6C A2 9E 1D 66 E2 BB 87	ê."5.9ðŽlčž.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.\$....yĐ.(.¥.©
78 DC 59 69 DA 8F 64 6E E6 7B A3 57 31 EE 8D DC	xÜYiÚ.dnæ{fWlî.Û
CB 62 45 62 89 EE 5B DC B6 73 01 E3 FF D9 66 67	ĚbEb%î[ÜŦs.ăÿÛfg
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

栏数: ☒ 只列举完整匹配的

密文框:

fg2ivyo}l{2s3_o@aw__rcl@

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_rlg iy}{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

A terminal window titled "终端" (Terminal) with standard macOS window controls. The terminal displays a large block of green text, which appears to be a base64-encoded string. Below this, there is a line of text: "Path=game". This is followed by a "DeletionDate=2016-06-27T12:27:37" and a "key{" line. A blue arrow points to the "key{" line. Below it, the key value is displayed: "key{feb81d3834e2423c9903f4755464060b}". The terminal then shows some more text, including "game.trashinfo" and "game.trashinfo.0L1PJY". At the bottom, the prompt "/桌面#" is visible, followed by a red prompt character and a tilde "~".

get flag:

```
key{feb81d3834e2423c9903f4755464060b}
```

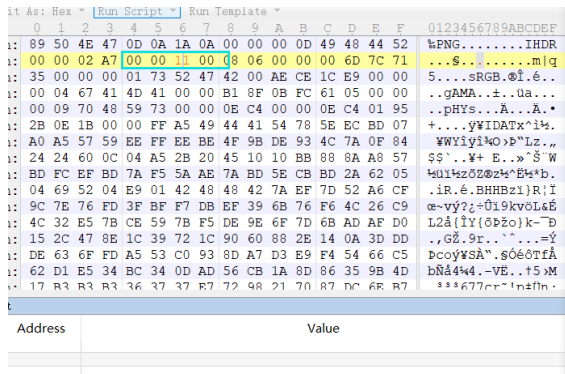
16、隐写 3

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



get flag:

flag{He1l0_d4_bal}

17、做个游戏(08067CTF)

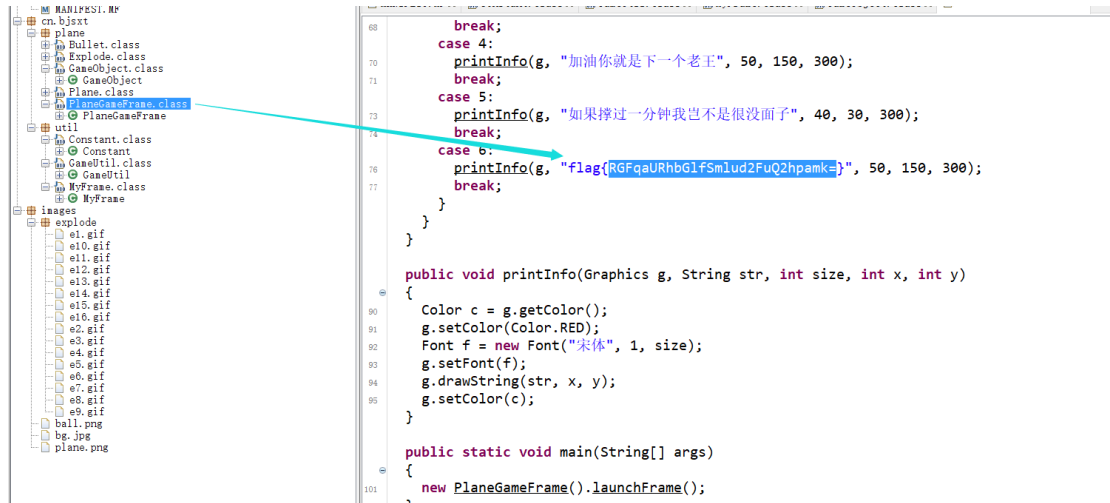
做个游戏(o8o67CTF)

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



RGFqaURhbG1fSm1ud2FuQ2hpamk=

加密

解密

☐ 解密结果以16进制显示

DajiDali_JinwanChiji

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, 为了不为难你, 大佬特地让我悄悄地把前七位告诉你

1391040**

Goodluck!!

作者@NewBee

wifi.cap

根据 tips 密码为手机号, 现在知道密码前 7 位, 后四位可通过爆破得到, 利用 Linux 下的 **crunch** 工具辅助爆破。

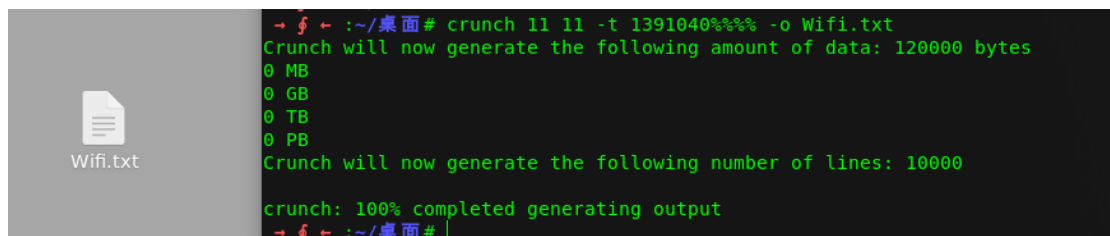
PS: Crunch 是一种创建密码字典工具, 该字典通常用于暴力破解。使用 **Crunch** 工具生成的密码可以发送到终端、文件或另一个程序。

```
crunch [minimum length] [maximum length] [character set] [options]
```

crunch 命令常用的选项如下所示。

-o: 用于指定输出字典文件的位置。 -b: 指定写入文件最大的字节数。该大小可以指定 KB、MB 或 GB, 但是必须与 -o START 选项一起使用。 -t: 设置使用的特殊格式。 -l: 该选项用于当 -t 选项指定 @、% 或 ^ 时, 用来识别占位符的一些字符。

生成 Wifi.txt 字典



PS: 命令解析

```
crunch 11 11 -t 1391040%% -o Wifi.txt
```

最小 11 最大 11

-t	指定模式
@	插入小写字母
,	插入大写字母
%	插入数字
^	插入特殊符号

利用 Linux 下 Wifi 破解工具 aircrack-ng 破解 wifi.cap 密码

```

终端

[00:00:03] 7688/9999 keys tested (2247.11 k/s)

Time left: 1 second                                76.89%

KEY FOUND! [ 13910407686 ]

Master Key      : C4 60 FE 8B 14 7D 58 00 91 D7 0A 9C 3C DE 44 69
                  0B E1 CD 81 07 F8 28 DB EA 76 1E ED 81 A3 FF FD

Transient Key   : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 1C E7 D0 96 DE 87 93 56 88 1D 08 C8 B9 AA B3 B0
→ $ ← :~/桌面# aircrack-ng -w Wifi.txt wifi.cap

```

get flag:

```
flag{13910407686}
```

19、Linux2

Linux2

100

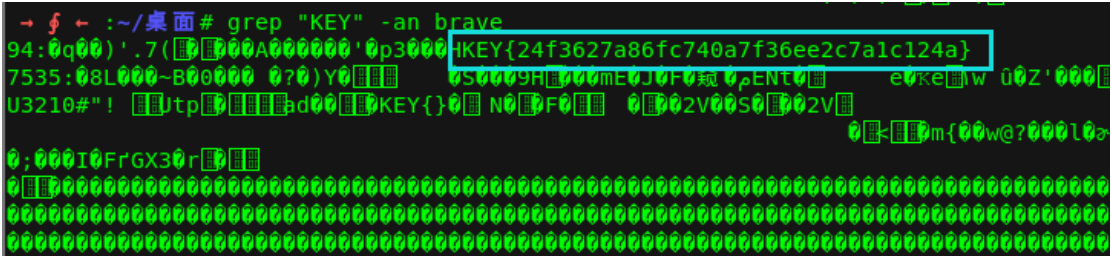
给你点提示吧: key的格式是KEY{}

题目地址: 链接: <http://pan.baidu.com/s/1skJ6t7R> 密码: s7jy

根据提示，使用 Linux 下 grep 搜索关键字 KEY 得到 flag

```
→ $ ← ~/桌面# grep "KEY" -an brave
```

PS: a 代表二进制问价、n 代表字符串出现的位置



get flag:

```
KEY{24f3627a86fc740a7f36ee2c7a1c124a}
```

20、账号被盗了

账号被盗了
100

<http://123.206.87.240:9001/>

修改 cookie 得到新的 Url

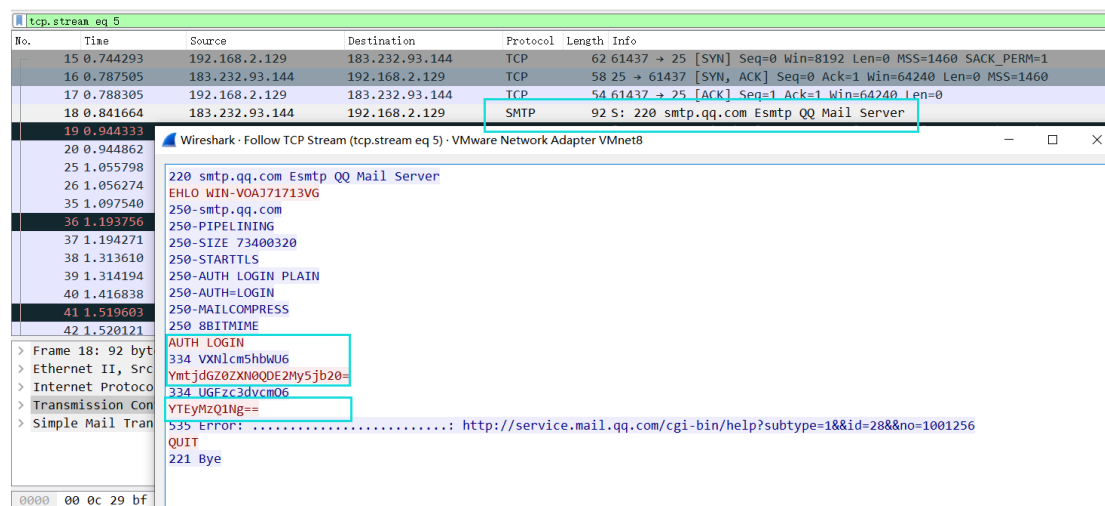


Login 游戏界面



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

bktftest@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

★ KEY值所在处 (1)

草稿箱 (1)

1.7折飞青岛 价格堪比高铁票 立即出发>>

flag{182100518+725593795416}

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

属性	值
说明	
标题	出题人已经跑路了
主题	出题人已经跑路了
分级	☆☆☆☆☆
标记	
备注	TVNEUzQ1NkFTRDEyM3p6
来源	
作者	
拍摄日期	
程序名称	
获取日期	
版权	
图像	
图像 ID	
分辨率	3016 x 4032
宽度	3016 像素

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...n.....EOö
8A 00 00 00 09 70 48 59 73 00 00 12 74 00 00 12	\$....pHys...t...
74 01 DE 66 1F 78 00 00 0A 4D 69 43 43 50 50 68	t.bf.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.VBöö±-l.."#-.
C8 10 59 A2 10 92 00 61 84 10 12 40 C5 85 88 0A	E.Yc.'..a...@A...'
56 14 15 11 9C 48 55 C4 82 D5 0A 48 9D 88 E2 A0	V...æHUA,ö.H.^ä
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	}ziíîûxûkçœüÿÏ
0F 80 11 12 26 91 E6 A2 6A 00 39 52 85 3C 3A D8	.e...s'æ±j.9R...<:ø
1F 8F 4F 48 C4 C9 BD 80 02 15 48 E0 04 20 10 E6	..OHAEæ...Hä...æ
CB C2 67 05 C5 00 00 F0 03 79 78 7E 74 B0 3F FC	EÄg.Ä...ö.yx~t°?u
01 AF 6F 00 02 00 70 D5 2E 24 12 C7 E1 FF 83 BA	.°o...pö.\$..Çáýf°
50 26 57 00 20 91 00 F0 22 12 E7 0B 01 90 52 00	P&W 'à" c...R

BU

BUGKU{a1e5aSA}

get flag:

```
BUGKU{a1e5a5A}
```

22、爆照(08067CTF)

爆照(o8o67CTF)
100

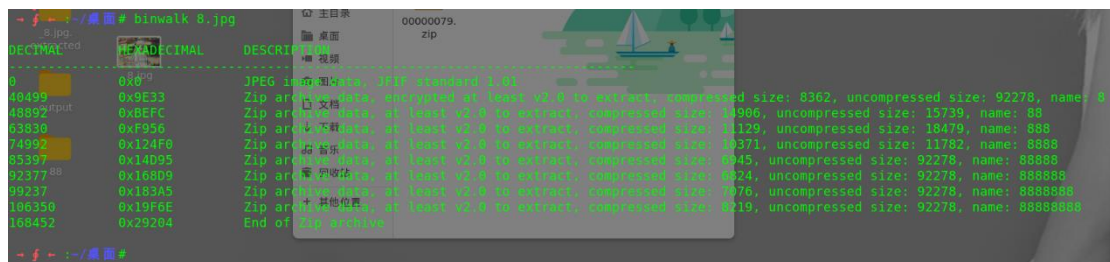
flag格式 flag{xxx_xxx_xxx}

8.jpg

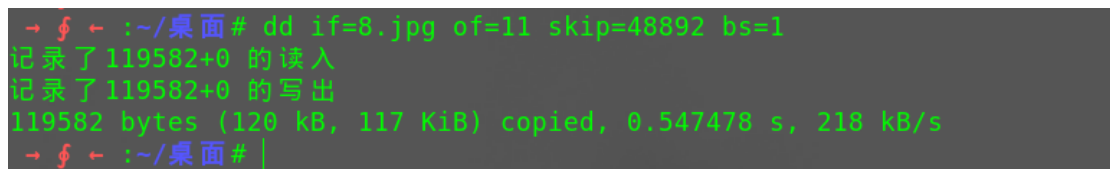
Flag

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



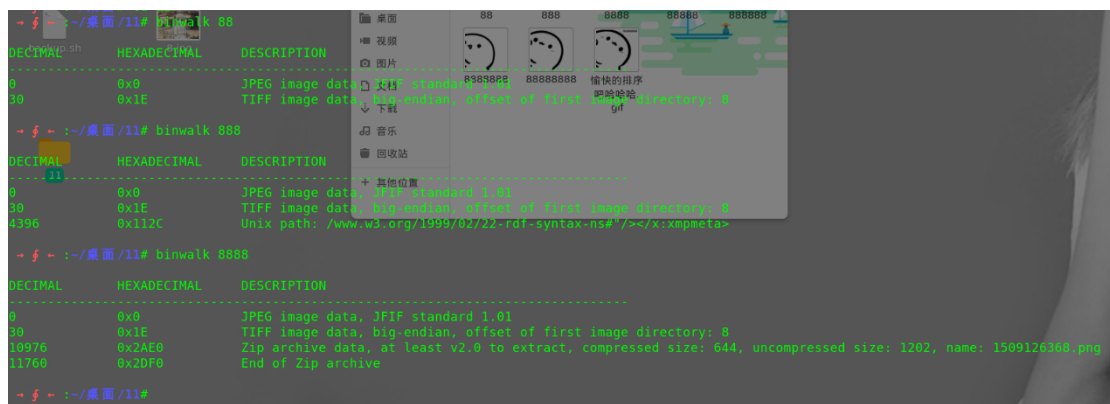
```
dd if=8.jpg of=11 skip=48892 bs=1
```



得到几张图片



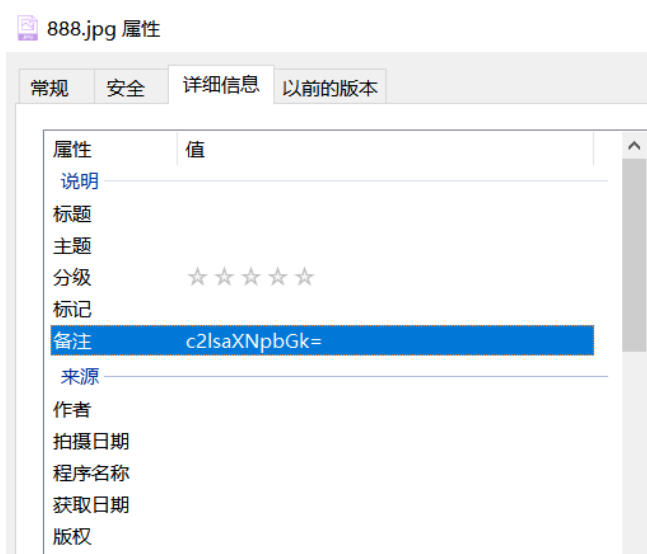
binwalk 分析这几张图片，发现前三张存在被修改的记录



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



c2lsaXNpbGk=

☐ 解密结果以16进制显示

silisili

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)

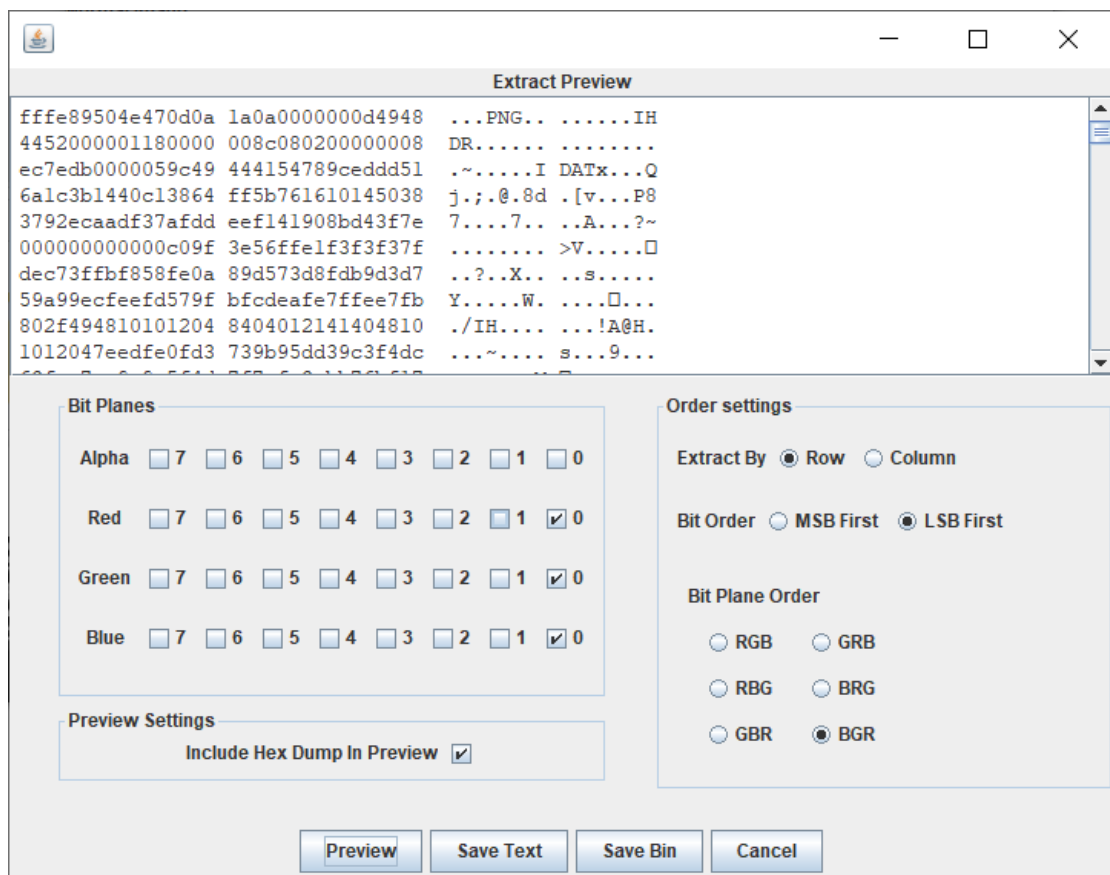
猫片(安恒)

100

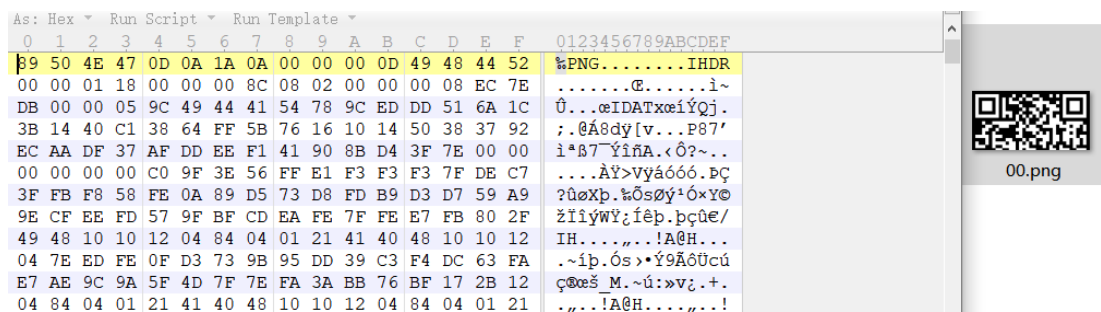
hint:LSB BGR NTFS

png

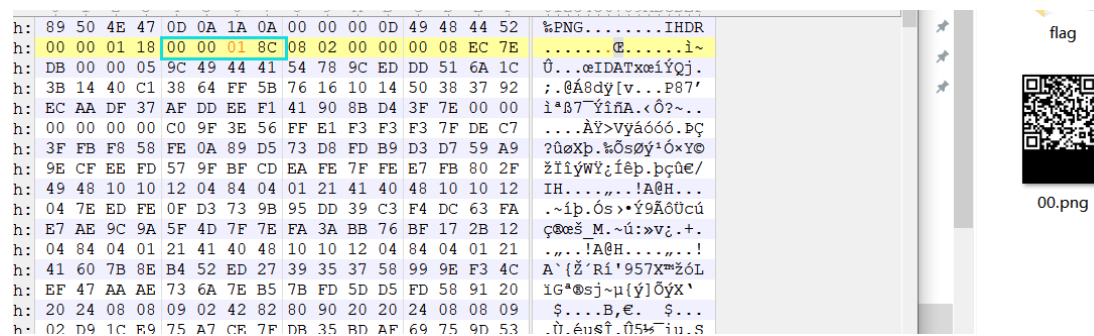
根据提示 LSB 隐写得到新的二维码



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



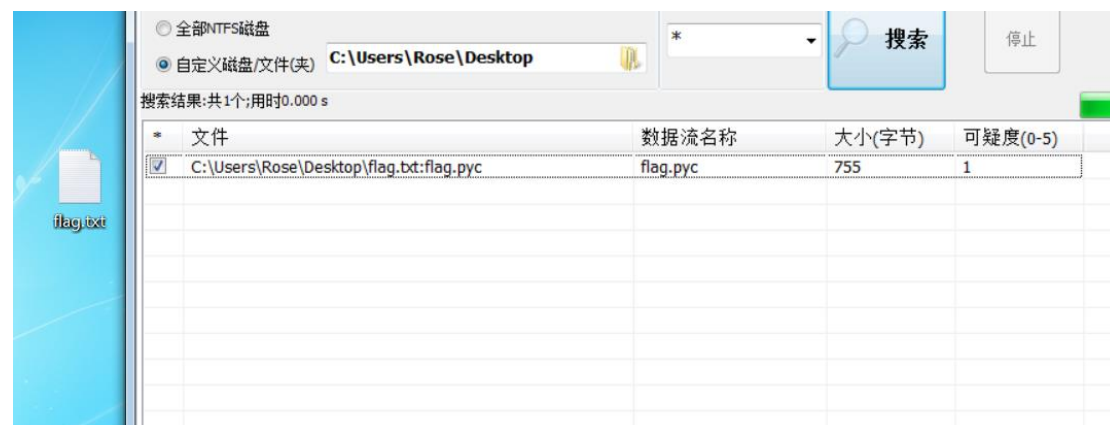
扫描二维码得到云盘连接: <https://pan.baidu.com/s/1pLT2J4f>



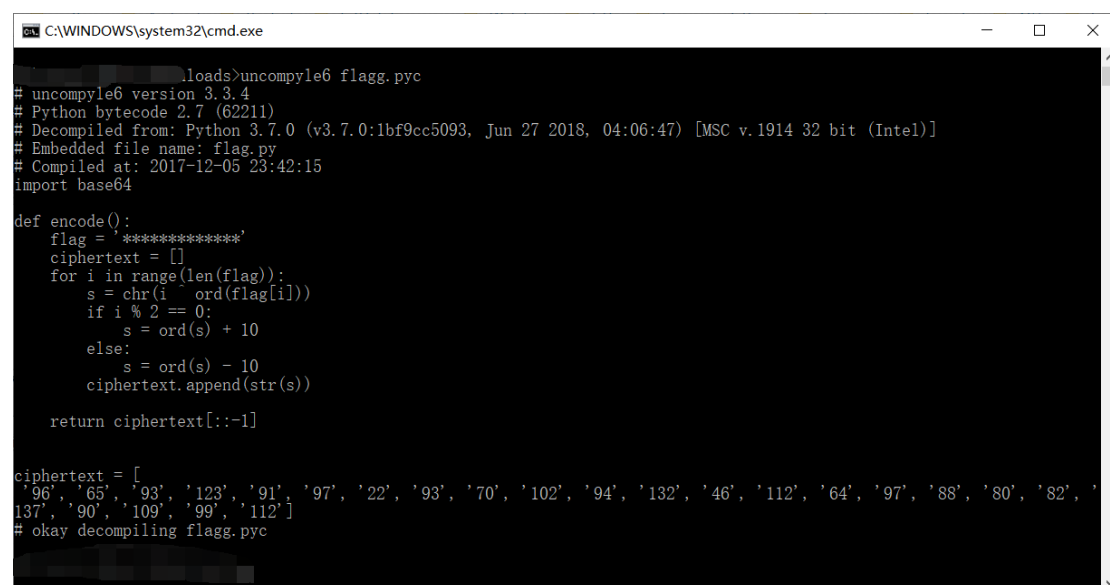
链接下载得到 flag.rar 压缩包，使用 WinRAR 解压，得到 flag.txt，发现并不是 flag，依据题目提示还有一个提示 NTFS 没有用到，于是利用工具 ntfsstreameditor 进行提取，得到一个 pyc 文件，将 pyc 反编译回去，得到一个 python 的 flag 加密函数。



NTFS 数据提取



pyc 反编译



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
flag
flag{
flag{Y
flag{Y@
flag{Y@e
flag{Y@e_
flag{Y@e_C
flag{Y@e_Cl
flag{Y@e_Cl3
flag{Y@e_Cl3v
flag{Y@e_Cl3ve
flag{Y@e_Cl3veR
flag{Y@e_Cl3veR_
flag{Y@e_Cl3veR_C
flag{Y@e_Cl3veR_Cl
flag{Y@e_Cl3veR_ClE
flag{Y@e_Cl3veR_ClEv
flag{Y@e_Cl3veR_ClEver
flag{Y@e_Cl3veR_ClEver!
flag{Y@e_Cl3veR_ClEver!}
>>>
```

```
# uncompiled version 3.5.4
# Python bytecode 2.7 (62211)
# Decompiled from: Python 3.7.0 (v3.7.0:1bf9cc5093, Jun 27 2018, 04:06:47) [MSC
# Embedded file name: flag.py
# Compiled at: 2017-12-08 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']
# okay decompiling flag.pyc

def decode():
    ci = ['96', '65', '93', '123', '91', '97', '22', '93', '70', '102', '94', ]
    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(s)
        flag += s
    print(flag)

decode()
```

get flag:

```
flag{Y@e_Cl3veR_ClEver!}
```

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

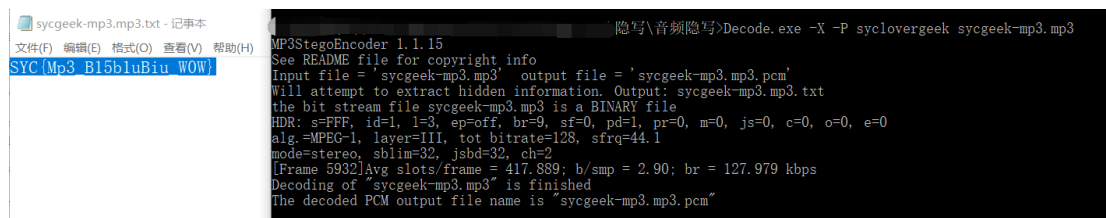
100

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
```



get flag:

```
SYC{Mp3_B15b1uBiu_W0W}
```

26、普通的二维码

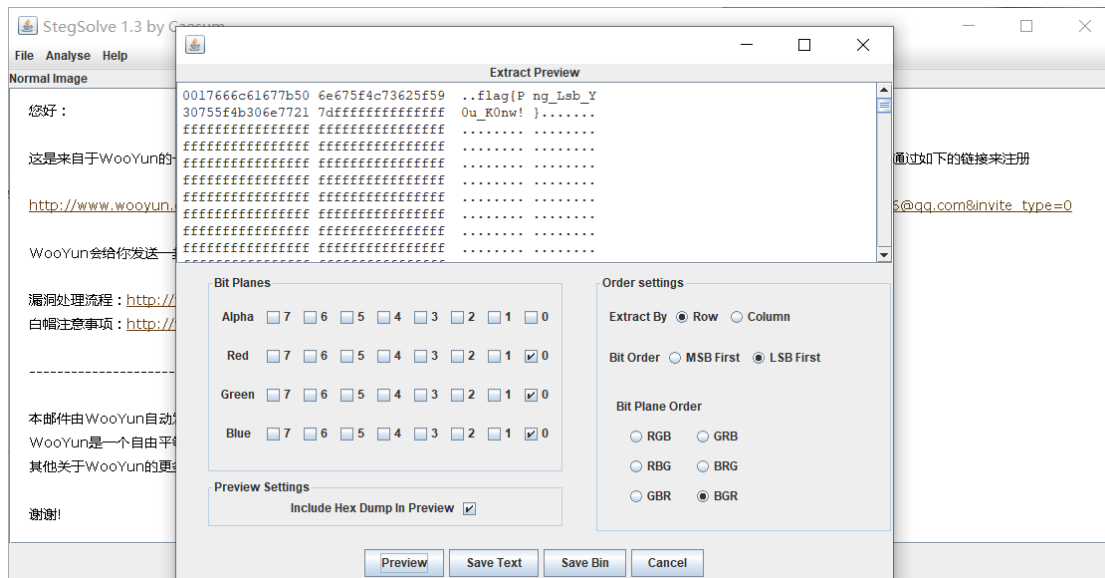
普通的二维码

100

来源：XJNU

misc80.zip

查看图片十六进制得到特殊字符串



get flag:

```
flag{Png_Lsb_YOu_K0nw!}
```

28、神秘的文件

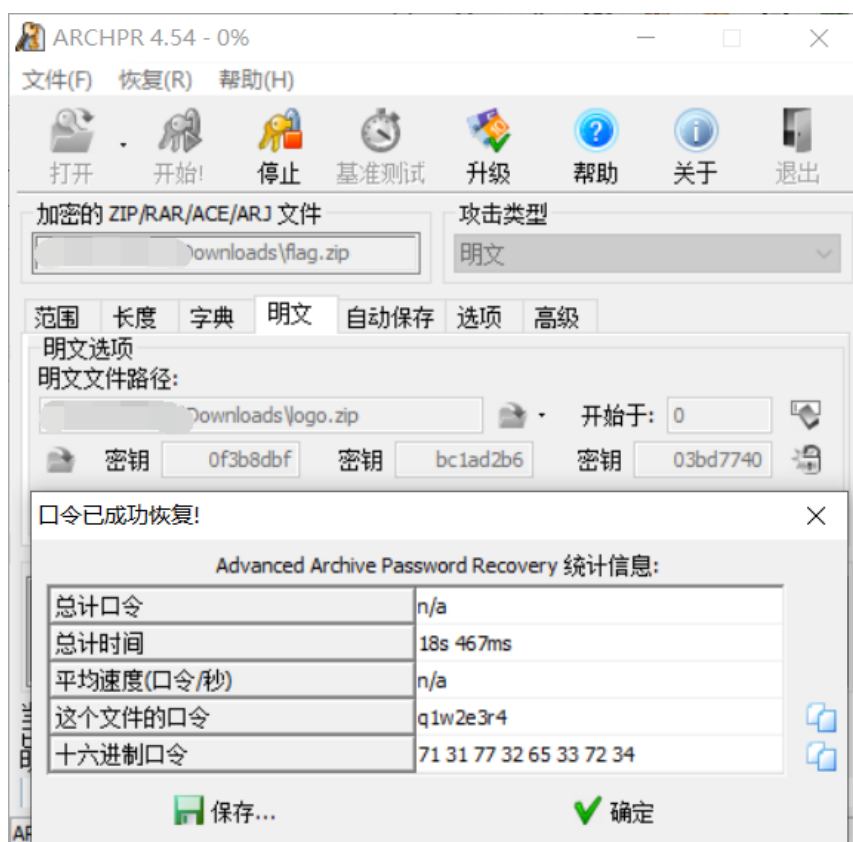
神秘的文件

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



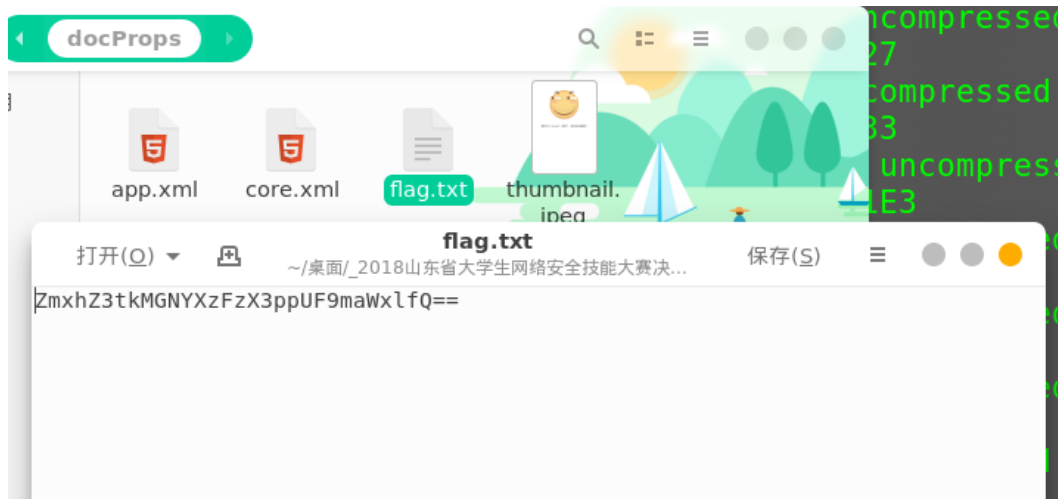
哪有什么 WriteUP，别想了，老老实实做题吧！

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
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	Zip archive data, at least v2.0 to extract, compressed size:
67	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	0x9833	Zip archive data, at least v1.0 to extract, compressed size:
gel.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		
268119	0x4181F	Zip archive data, at least v2.0 to extract, compressed size:
268650	0x41970	Zip archive data, at least v2.0 to extract, compressed size:
xml.rels		
269244	0x418BC	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	0x42680	End of Zip archive

分离文件找到 flag.txt 解码得到 flag



ZmxhZ3tkMGNYZfZ3ppUF9maWxlfQ==

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