

全网最详细攻防世界MISC新手区题

原创

yatkm 于 2020-11-01 21:45:30 发布 733 收藏 5

分类专栏: [ctf_misc](#) 文章标签: [信息安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/Yshshsj/article/details/109433565>

版权



[ctf_misc](#) 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

全网最详细攻防世界MISC新手区题

1. this_is_flag
2. pdf
3. give_you_flag
4. 坚持60s
5. gif
6. 掀桌子
7. 如来十三掌
8. stegano
9. SimpleRAR
10. base64stego
11. ext3
12. 功夫再高也怕菜刀

1. this_is_flag

this_is_flag

👍 69 最佳Writeup由王兆敏提供

难度系数: ★★ 2.0

题目来源: 暂无

题目描述: Most flags are in the form flag{xxx}, for example flag{th1s_!s_a_d4m0_4la9}

题目场景: 暂无

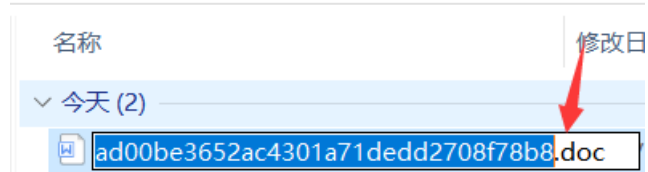
题目附件: 暂无

<https://blog.csdn.net/Yshshsj>

由一眼看出法得到令人心动不已的flag。

2. pdf

根据题目意思flag就在图片的后面，把文件后缀改成doc（也可以右键图片，在图片层级选项设置为至于底层），就可以获得flag啦啦啦啦



3. give_you_flag

下载后发现是一张gif图，第50帧是二维码（我是用stegsolve一帧帧看的）。



奈何ps如此高深（我太菜了，还不会ps。。），没有办法只好打开电脑的画图工具来把这二维码缺失的三个定位符补上。不禁感叹学信息安全还得学画画，唉。。。

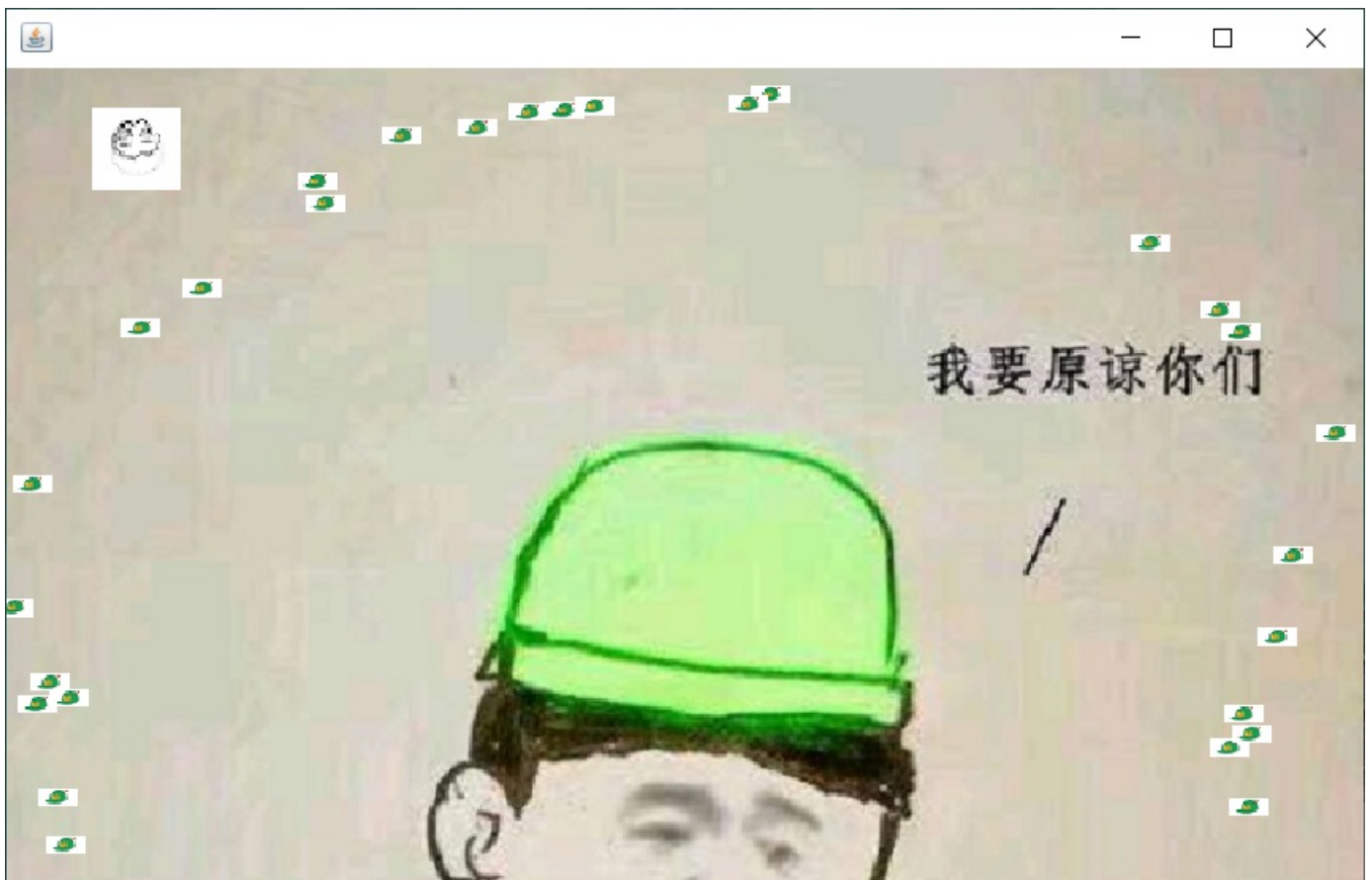


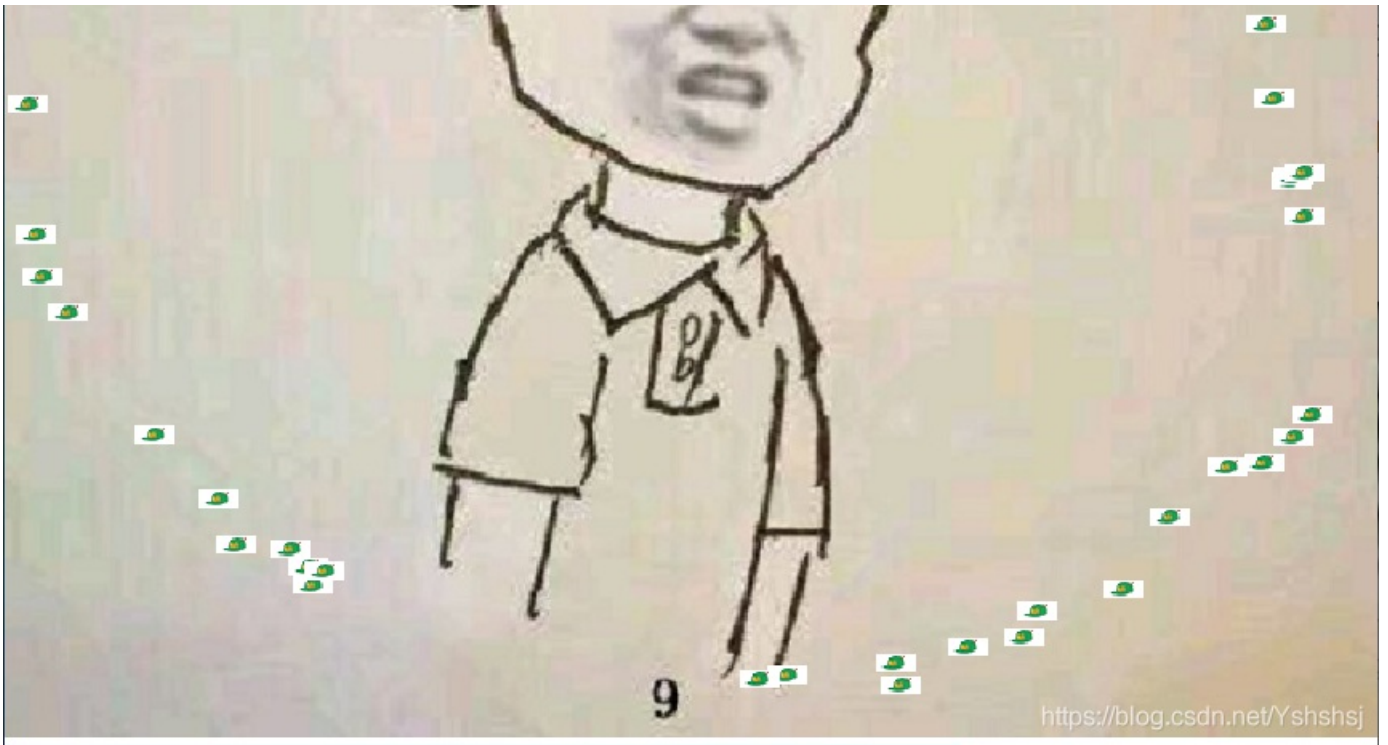
扫码赢大奖啦~~

4. 坚持60s

jd-gui github下载:<https://github.com/java-decompiler/jd-gui/releases/tag/v1.6.6>

头顶上的青青草原，哈哈哈。看到这是一个java游戏，用jd-gui打开





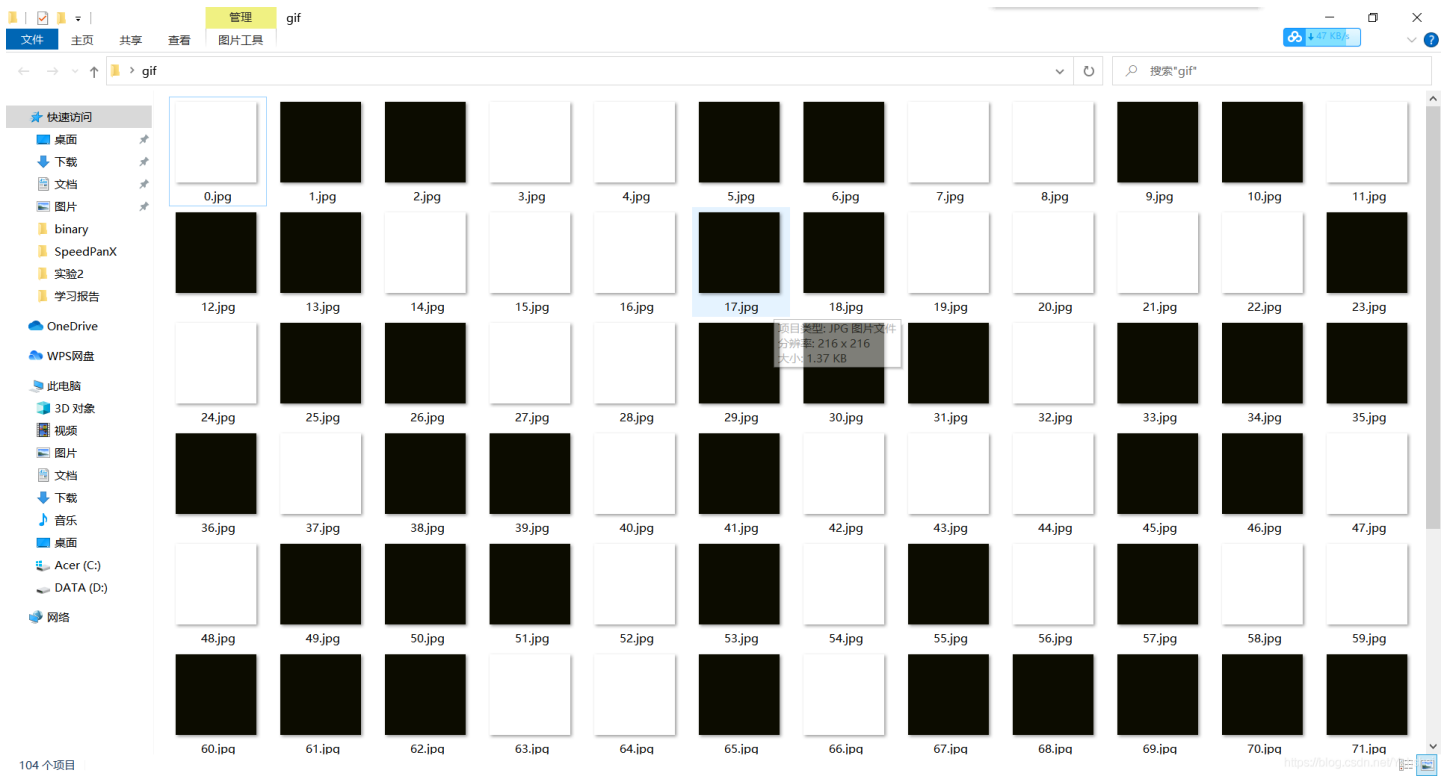
查看了一下源代码可以发现flag（当然也可以使用搜索功能搜索flag）

A screenshot of a Java decompiler window. The window title is "PlaneGameFrame.class - Java Decompiler". The left sidebar shows a project tree with "PlaneGameFrame.class" selected. The main area shows the source code for the class. A red circle highlights a line of code: `println(g, "flag{R6fqaURhbc1f5mLud2FuQ2hpamk-}", 50, 150, 300);`. A red arrow points from the text "查看了一下源代码可以发现flag" to this line of code. The code is as follows:

```
43     this.bae = new Explode(this.p.x, this.p.y);
44     }
45     this.bao.draw(g);
46     }
47     }
49     if (!this.p.isLive()) {
50     println(g, "兄弟就死了的嘛", 50, 150, 200);
51     int period = (int)((this.endTime.getTime() - this.startTime.getTime()) / 1000L);
52     println(g, "你的持久度才" + period + "秒", 50, 150, 250);
53     switch (period / 10) {
54     case 0:
55     println(g, "真·头顶一片青青草原", 50, 150, 300);
56     break;
57     case 1:
58     println(g, "这东西你也要抢着带?", 50, 150, 300);
59     break;
60     case 2:
61     println(g, "如果梦想有颜色,那一定是原谅色", 40, 30, 300);
62     break;
63     case 3:
64     println(g, "哟,炊事班长呵兄弟", 50, 150, 300);
65     break;
66     case 4:
67     println(g, "加油你就是下一个老王", 50, 150, 300);
68     break;
69     case 5:
70     println(g, "如果撑过一分钟我岂不是很有面子", 40, 30, 300);
71     break;
72     case 6:
73     println(g, "flag{R6fqaURhbc1f5mLud2FuQ2hpamk-}", 50, 150, 300);
74     break;
75     }
76     }
77     }
78     }
79     }
80     }
81     }
82     }
83     }
84     }
85     }
86     }
87     }
88     }
89     }
90     public void println(Graphics g, String str, int size, int x, int y) {
91     Color c = g.getColor();
92     g.setColor(Color.RED);
93     Font f = new Font("宋体", 1, size);
94     g.setFont(f);
95     g.drawString(str, x, y);
96     g.setColor(c);
97     }
98     }
99     }
100    public static void main(String[] args) {
```

5. gif

刚开始的时候看着这些黑白块，联想到了摩斯密码，但是好像不太可行。于是盲猜黑白块代表的是黑为1、白为0的二进制。



011001100110110001100001011001110111101101000110011101010100111001011110110011101101001010001100111101

二进制在线转字符串: http://www.txttool.com/WenBen_BinaryStr.asp

二进制转字符串的结果就是梦寐以求的flag啦。

输入二进制文本:

011001100110110001100001011001110111101101000110011101010100111001011110110011101101001010001100111101

转换后的文本:

flag{FuN_gIF}

6. 掀桌子

掀桌子 WP 建议

👍 90 最佳Writeup由 [flag{not_here}](#) · [渣渣禹](#)提供

难度系数: ★★★★★ 4.0

题目来源: DDCTF2018

题目描述: 菜狗截获了一份报文如下c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e9f3e4e3e8eaf9eaf3e2e4e6f2, 生气地掀翻了桌子(°_°)

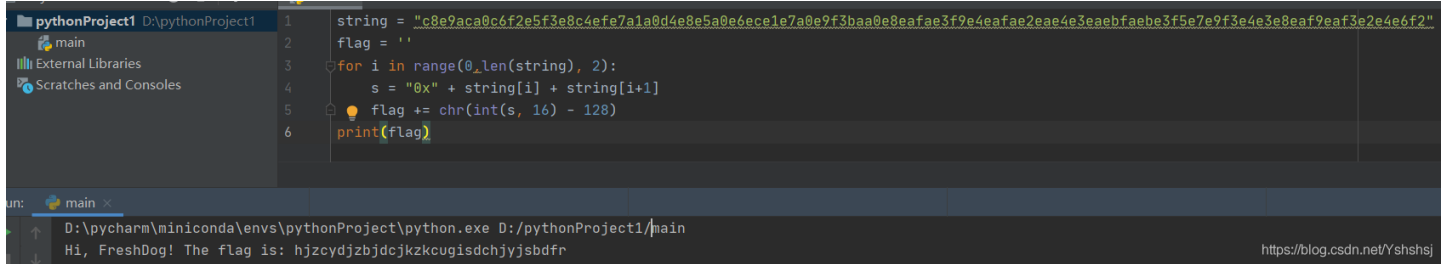
题目场景: 暂无

题目附件: 暂无

<https://blog.csdn.net/Yshshsj>


```
string = "c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eae3fae3f5e7e9f3e4e3e8eaf9eaf3e2e4e6f2"
flag = ''
for i in range(0,len(string), 2):
    s = "0x" + string[i] + string[i+1]
    flag += chr(int(s, 16) - 128)
print(flag)
```

用脚本跑一下，flag 就出来啦~~



7. 如来十三掌

夜哆悉諳多苦奢陀奢諦冥神哆盧穆幡三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀諳怖奢智侄諸若奢數菩奢集遠俱老竟寫明奢若梵等盧幡豆蒙密離怯婆幡礙他哆提哆多鉢以南哆心曰姪罰蒙訥神。舍切真怯勝訥得俱沙罰娑是怯遠得訥數罰輸哆遠薩得槃漫夢盧幡亦醯訥娑幡瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿幡沙蘇輸奢恐豆侄得罰提哆伽諳沙楞鉢三死怯摩大蘇者數一遮

<https://blog.csdn.net/Yshshsj>

看到这些可以联系到与佛论禅编码

在开头加上 '佛曰：' 然后 参悟佛所言的真意'

与佛论禅

MzkuM3gvMUAwnzuwn3cgozMlMTuvqzAenJchMUAeqzWenzEmLJW9

听佛说宇宙的真谛

参悟佛所言的真意

普度众生

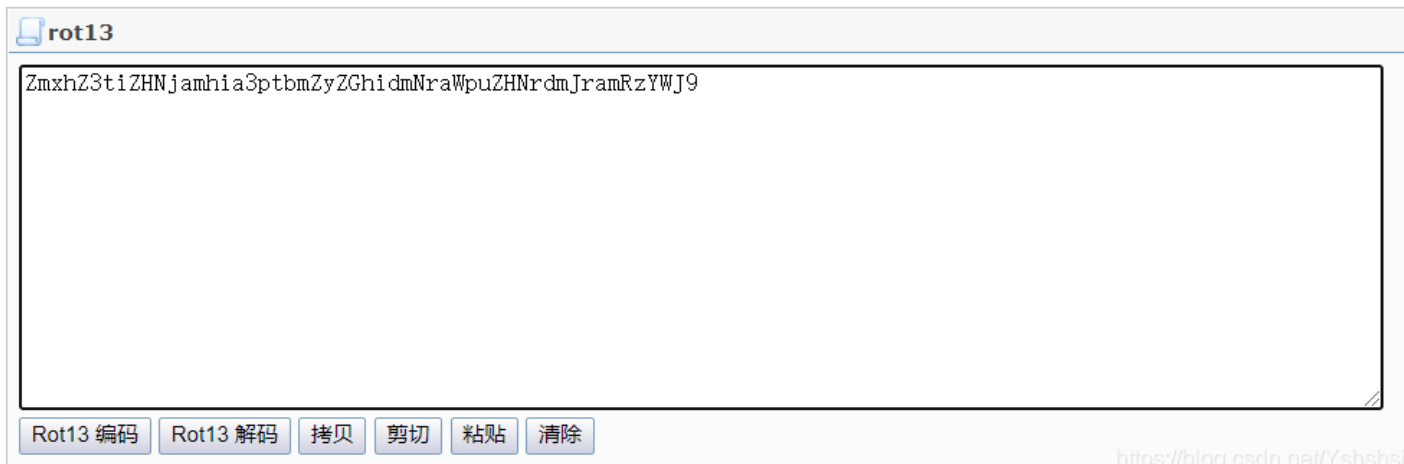
悠然，随心，随性，随缘

佛曰：夜哆悉諳多苦奢陀奢諦冥神哆盧穆幡三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀諳怖奢智侄諸若奢數菩奢集遠俱老竟寫明奢若梵等盧幡豆蒙密離怯婆幡礙他哆提哆多鉢以南哆心曰姪罰蒙訥神。舍切真怯勝訥得俱沙罰娑是怯遠得訥數罰輸哆遠薩得槃漫夢盧幡亦醯訥娑幡瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿幡沙蘇輸奢恐豆侄得罰提哆伽諳沙楞鉢三死怯摩大蘇者數一遮

<https://blog.csdn.net/Yshshsj>

得到一串编码后，突然想起题目是在暗示rot13加密方式（敲着base64的手突然就停了下来）

rot13解密网址: <http://www.mxcz.net/tools/rot13.aspx>



解密完后发现 还是一串编码, 再次使用rot13解密, 发现不行, 于是转用base64 (突然觉得base64又香了不少), 没错就是它, 它又来了。

请输入要进行 Base64 编码或解码的字符

ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9

编码 (Encode)

解码 (Decode)

↑ 交换

(编码快捷键: **Ctrl** + **Enter**)

Base64 编码或解码的结果:

编/解码后自动全选

flag{bdscjhbkmnfrdhbvckijndskvbkjdsab}

<https://blog.csdn.net/Yshshsj>

8. stegano

用火狐打开刚才下载pdf文件, 控制台输入

```
document.documentElement.textContent
```

然后回车查看



发现一串特殊的编码：

BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA AB BBBB BA AAAB AB BBBB AAAAA AB BBBB BAAA ABAA AAABB BB AAABB AAAAA AAAAA AAAAB BBA AAABB

看到有空格隔开，于是猜测摩斯密码‘A’代替‘.’，‘B’代替‘—’
只能一个个打（老工具人了），解密后得到flag。（ps：填flag的时候要注意格式喔）

摩斯密码转换网址：<http://moersima.00cha.net/>

输入摩尔斯电码，点击“解密”，即可将摩尔斯电码翻译成可识别的字符。



解密

congratulations,flag:1nv151bl3m3554g3

推荐：中文摩斯密码翻译>>

<https://blog.csdn.net/yshshj>

9. SimpleRAR

把下载的文件解压后，发现只有一个flag.txt(很显然是假的)，用 winhex 打开发现有一个 png 文件。

rar对png的文件类型编码是74，就在flag.txt文件结束，这里是7A，所以要把圈圈里的7A改过来喔，保存再次解压。

WinHex - [18c5326aada0499eafbe03ad8a52e40c.rar]

WinHex interface showing a hex dump of a file named '18c5326aada0499eafbe03ad8a52e40c...' with a metadata sidebar on the left. A red circle highlights the hex value '7A' at offset 00000050, and a red arrow points to the ASCII string 'secret.png' at offset 00000080.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ASCII
00000000	52	61	72	21	1A	07	00	CF	90	73	00	00	0D	00	00	00	Rar!...İ.s.....
00000010	00	00	00	00	D5	56	74	20	90	2D	00	10	00	00	00	10ÖVt.-.....
00000020	00	00	00	02	C7	88	67	36	6D	BB	4E	4B	1D	30	08	00	...Çİg6m»NK.O..
00000030	20	00	00	00	66	6C	61	67	2E	74	78	74	00	B0	57	00	...flag.txt.°W.
00000040	43	66	6C	61	67	20	69	73	20	6E	6F	74	20	68	65	72	Cflag is not her
00000050	65	A8	30	7A	00	90	2F	00	3A	15	00	00	42	16	00	00	e`<Z ./:....B...
00000060	02	BC	E9	8	2F	6E	84	4F	4B	1D	33	0A	00	20	00	00	.4éI/nİOK.3... .
00000070	00	73	65	6	72	65	74	2E	70	6E	67	00	F0	40	AB	18	secret.png.đ@«.
00000080	11	C1	11	55	08	D1	55	80	0D	99	C4	90	87	93	22	10	Á.U.ÑUI.İ.İ.İ."
00000090	4C	58	DA	18	B1	A4	58	16	33	83	08	F4	3A	18	42	0B	LXÚ.±*X.3I.ò:.B.
000000A0	04	05	85	96	21	AB	1A	43	08	66	EC	61	0F	A0	10	21	..İ!«.C.fia. .!
000000B0	AB	3D	02	80	B0	10	90	C5	8D	A1	1E	84	42	50	43	29	«=.I°.Á.i.İB°C)
000000C0	08	10	DA	0F	23	99	CC	F3	9D	C4	85	86	67	73	39	DE	..Ú.#İİó.Äİİgs9b
000000D0	47	63	91	DE	C4	77	ED	A8	DC	46	F4	C5	54	CD	55	6A	Gc'PÁwi ÜFóÁTÍUj

用winhex打开png文件后发现其实是gif文件。

WinHex - [secret.png]

WinHex interface showing a hex dump of a file named 'secret.png'. A red arrow points to the hex value 'FF' at offset 00000010, which corresponds to the ASCII string 'y' in the XMP metadata.

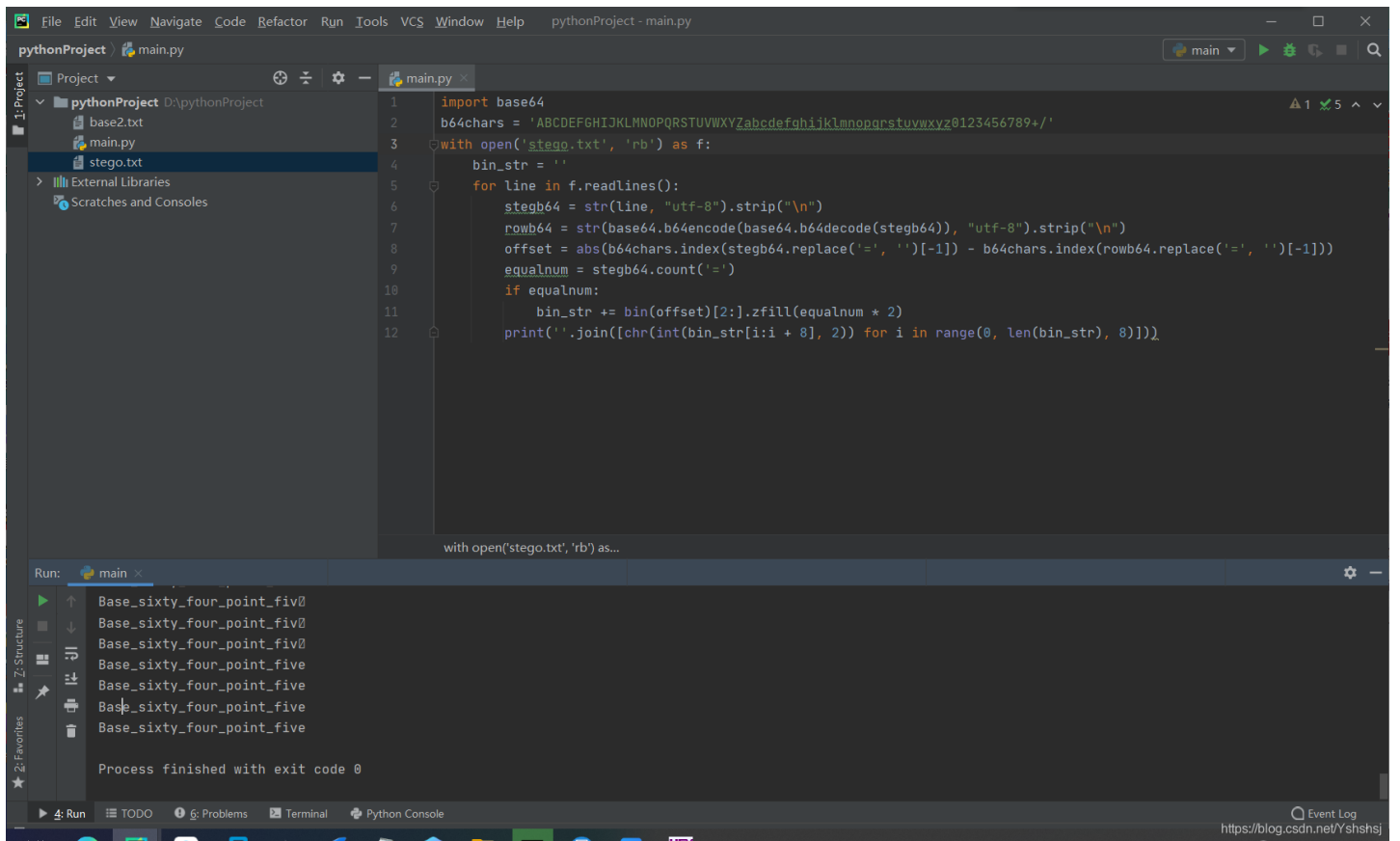
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ASCII
00000000	47	49	46	38	39	61	18	01	18	01	91	02	00	FE	FF	FF	IF89a....'..pyy
00000010	FF	FF	FF	FF	FF	FF	00	00	00	21	FF	0B	58	4D	50	20	yyyyyy...!y.XMP
00000020	44	61	74	61	58	4D	50	3C	3F	78	70	61	63	6B	60	74	DataXMP<?xpacket
00000030	20	62	65	67	69	6E	3D	22	EF	BB	BF	22	20	6F	64	3D	begin="i»¿" id=
00000040	22	57	35	4D	30	4D	70	43	65	68	69	48	7A	72	65	53	"W5MOMpCehiHzreS
00000050	7A	4E	54	63	7A	6B	63	39	64	22	3F	3E	20	3C	78	3A	zNTczkc9d"?> <x:
00000060	78	6D	70	6D	65	74	61	20	78	6D	6C	6E	73	3A	78	3D	xmpmeta xmlns:x=
00000070	22	61	64	6F	62	65	3A	6E	73	3A	6D	65	74	61	2F	22	"adobe:ns:meta/"
00000080	20	78	3A	78	6D	70	74	6B	3D	22	41	64	6F	62	65	20	x:xmptk="Adobe
00000090	58	4D	50	20	43	6F	72	65	20	35	2E	33	2D	63	30	31	XMP Core 5.3-c01
000000A0	31	20	36	36	2E	31	34	35	36	36	31	2C	20	32	30	31	1 66.145661, 201

修改了后缀后，按照题目意思把图层给分离出来（用的是ps，还特地下载了个ps学了一下），再用stegsolve查看



把二维码拼起来，然后再把定位符补上就扫描就可以获取flag啦（都快把我整图吐了。。）





```
pythonProject - main.py
pythonProject D:\pythonProject
  base2.txt
  main.py
  stego.txt
  External Libraries
  Scratches and Consoles

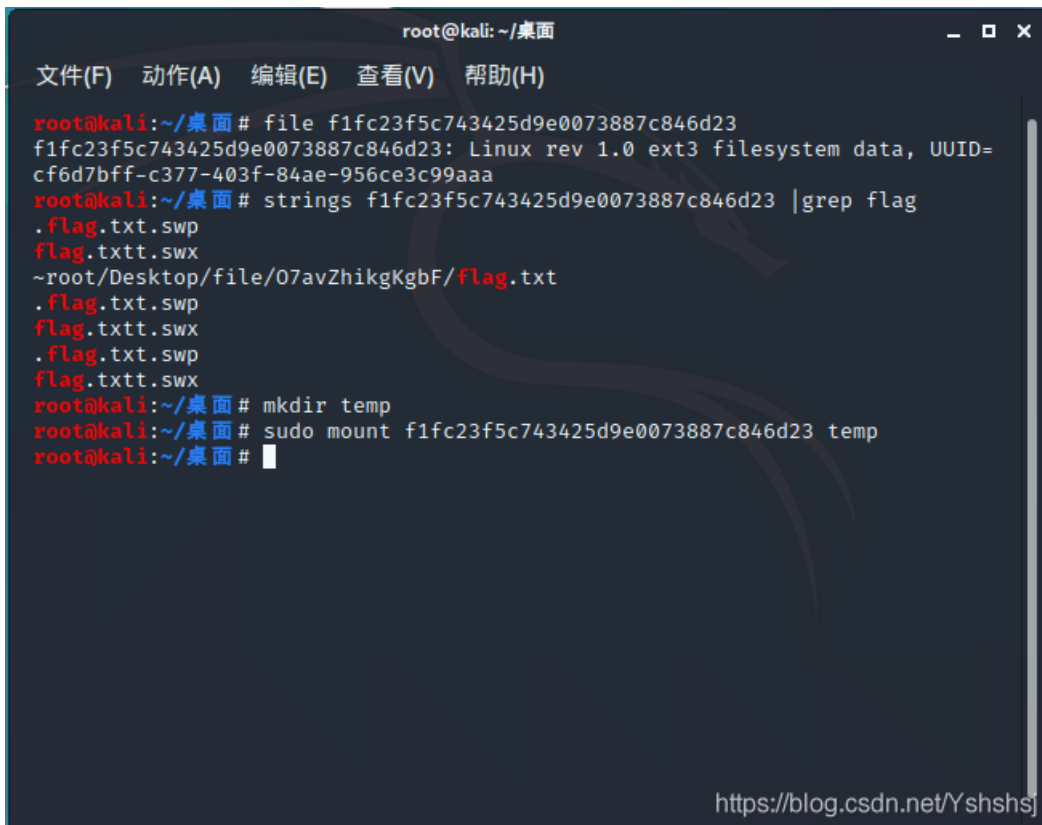
1 import base64
2 b64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
3 with open('stego.txt', 'rb') as f:
4     bin_str = ''
5     for line in f.readlines():
6         stegb64 = str(line, "utf-8").strip("\n")
7         rowb64 = str(base64.b64encode(base64.b64decode(stegb64)), "utf-8").strip("\n")
8         offset = abs(b64chars.index(stegb64.replace('=', ''))[-1]) - b64chars.index(rowb64.replace('=', ''))[-1])
9         equalnum = stegb64.count('=')
10        if equalnum:
11            bin_str += bin(offset)[2:].zfill(equalnum * 2)
12        print(''.join([chr(int(bin_str[i:i + 8], 2)) for i in range(0, len(bin_str), 8)]])

Run: main
Base_sixty_four_point_fiv
Base_sixty_four_point_fiv
Base_sixty_four_point_fiv
Base_sixty_four_point_fiv
Base_sixty_four_point_fiv
Base_sixty_four_point_fiv
Base_sixty_four_point_fiv
Base_sixty_four_point_fiv
Process finished with exit code 0
```

用脚本跑一下，也很轻松得到flag了（前几天的比赛中也遇到了这样的隐写题（base64加密了49次。。））

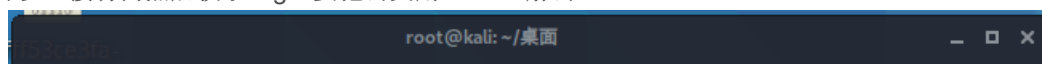
11. ext3

把下载好的文件，拷贝一份到kali中，挂载到系统上。mount命令用于加载文件系统到指定的加载点。此命令的最常用于挂载cdrom，使我们可以访问cdrom中的数据。

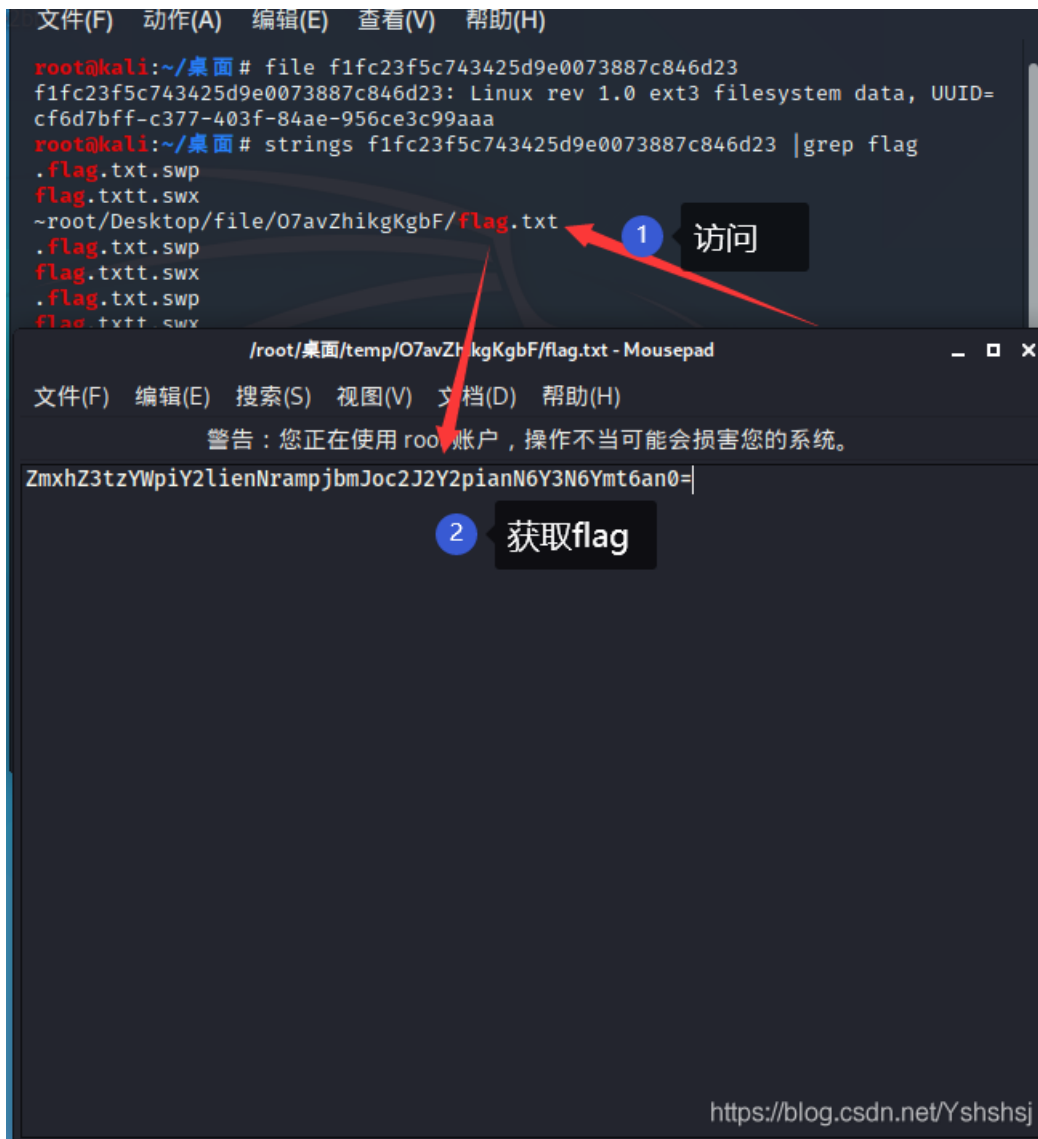


```
root@kali: ~/桌面
文件(F) 动作(A) 编辑(E) 查看(V) 帮助(H)
root@kali:~/桌面# file f1fc23f5c743425d9e0073887c846d23
f1fc23f5c743425d9e0073887c846d23: Linux rev 1.0 ext3 filesystem data, UUID=
cf6d7bff-c377-403f-84ae-956ce3c99aaa
root@kali:~/桌面# strings f1fc23f5c743425d9e0073887c846d23 |grep flag
.flag.txt.swp
flag.txtt.swx
~root/Desktop/file/07avZhikKgbF/flag.txt
.flag.txt.swp
flag.txtt.swx
.flag.txt.swp
flag.txtt.swx
root@kali:~/桌面# mkdir temp
root@kali:~/桌面# sudo mount f1fc23f5c743425d9e0073887c846d23 temp
root@kali:~/桌面#
```

执行完命令后，可以直接访问然后获取flag（要把密文用base64解密）



```
root@kali:~/桌面
```



ZmxhZ3tzYWpiY2lienNrampjbmJoc2J2Y2pianN6Y3N6Ymt6an0=

编码 (Encode)

解码 (Decode)

↕ 交换

(编码快捷键: **Ctrl** + **Enter**)

Base64 编码或解码的结果:

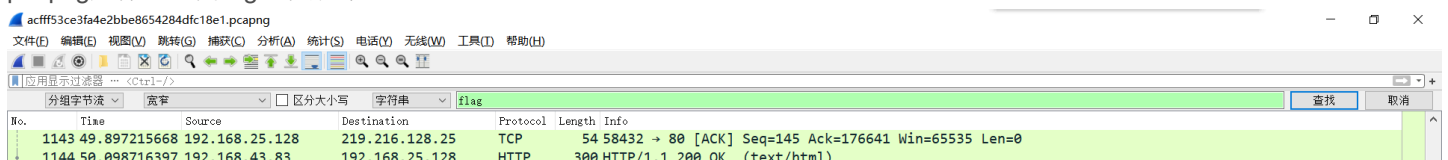
flag{sajbcibzskjjcnbhsbvcjbjszcszbkzj}

<https://blog.csdn.net/Yshshsj>

啊，终于又写完一题，看到每一个flag呼之欲出，就会不禁的开心。

12. 功夫再高也怕菜刀

下载附件，用foremost进行pcapng文件的分离，得到一个zip，打开zip，得到一份加密的flag.txt文件。然后用wireshark打开pcapng文件，查找flag.txt关键字，




```

4FE6959FC53E6F770E96AFB5FCB6E67D366DC3A689B6D2D236C8BA9000DB89705BF798CE679C1F96043FF3CE3EA5BA7191FC158B70E4F98643BB0409D9
71F3B7FCB2B58F03855C7CDB41039FEEA83A72FDFB3FF7DF0F0066AC83D2D3FEBEA4FF00D0C578F8896CBC53FBD53767DF0089D775CDFCEDEEE192B
FA36BE69DAFE5F0E96BDD690465CEF8326FE08C7DA197A20E365B47D831C00DE9DF201CE3DCB677866DADB71291FF2C61E8B02FABBF188638DD83CEE
AD297FD5A7FD7F37F4AC8B8E92F00D7E8FE46BC5AD276BFCFEFF7B57F87CE4FAA87BD865771E9ADB2D251FD36DBE156693E6C9BA90E580C21D9866FF
009F780F1B467A4926E00FF176E0B3118731C7CD8D876128A738B780F2646FFA6B2678C1E49E30480356FEEDCFF00D7D27F37ACAD47A5FF00FB07F23
5E3577A7AB7F85FF001F7775B37756B452F6B0DAB827BC9C75F5F651DB6D39FEE56FB526F0EE1CB30D9F28018C00E3F751F57B8931F002D1B191E99E3
2319C999F681B7A90C6156C60609D073276E31F2E7B8183F2F37EE7EFD0CFD7383F9C758F77D65FF00AF78FF00F408EBC6C4DD4ADE4F5F4EDBD97BBA2E
9A7F2A3E830EB45E89F7DD41EBD5FC7AF7F7BAC9B59E658327293B9CF2E1BEF7FB5FF02EBF8D15763FF571F00B8BF0A08A2B86DFE1FFC05797F93FBFE
FE9E65DA5FF81BFF002F5FE96BFFD9 HTTP/1.1 200 OK
Date: Fri, 08 Dec 2017 11:42:07 GMT
Server: Apache/2.4.23 (win64) PHP/5.6.25
X-Powered-By: PHP/5.6.25
Content-Length: 7
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

->|1|<-POST /upload/1.php HTTP/1.1
User-Agent: Java/1.8.0_151
Host: 192.168.43.83
Accept: text/html, image/gif, image/jpeg, *, q=.2, */*; q=.2
Connection: keep-alive
Content-type: application/x-www-form-urlencoded
Content-Length: 723

aa=@eval.
(base64_decode($_POST[action]));&action=QG1uaV9zZXQoImRpc3BsYXl1fXZjY3JzIiwiaW1MCiIp0BzZXRfdGltZV9saw1pdCgwKtAc2V0X2h2ljx3
F1b3Rlc19ydW50aw1lKDAp02VjaG8oIi0%2BFCIP0zskRD1iYXNlnjRfZGVjb2RlKCRfUE9TVFsiejEiXSk7JY9YQg9wZw5kaIoJEQp02lmKCRGPT10VUXMKX
tly2hvkCJFulJPUjovLyBQYXR0IE5vdCBG63VuZCBPciB0byBQZXJtaXZaw9uISiP031bHNLeyRNPu5VTEw7JEW9TlVMTdt3aGlzSgkTj1AcmVhZGRpcigk
RikpeyRQPSRELiIvIi4kTjSkV01AZGf0ZSgiWS1tLWQgSDppOnMileBmaWxlbnRpbWUoJFApKtTAJEU9c3Vic3RyKGJhc2VfY29udmVydChAZmlsZXBlcm1zKC
RQKSwxMcw4KSwtnck7JFI9Ilx0Ii4kVC4iXHQiLkBmaWxlcl2l6ZSgkUCkuIlx0Ii4kRS4iCiI7awYoQGLzX2RpcigkUckpJE0uPSROLiIvIi4kUjtlbnNlICRM
Lj0kTi4kUjtlZWNobyAKTS4kTDTAY2xvc2VkaXIoJEYp0307ZWNobygifiDwtIik7ZGllKkck7z1=RDpcd2FtCY0XHd3d1x1cGxvYWRcHTTP/1.1 200 OK
Date: Fri, 08 Dec 2017 11:42:11 GMT
Server: Apache/2.4.23 (win64) PHP/5.6.25
X-Powered-By: PHP/5.6.25

```

分组 1144, 53 客户端 分组, 2 服务器 分组, 3 turn(s). 点击选择.

整个对话 (206 kB) 显示和保存数据为 ASCII 流 7

保存为jpg格式，可以得到图片，即是flag.txt的密钥，打开flag.txt即可获得flag。



flag.txt - 记事本

文件(E) 编辑(E) 格式(O) 查看(V) 帮助(H)

flag{3OpWdJ-JP6FzK-koCMAK-VkfWBq-75Un2z}

<https://blog.csdn.net/Yshshs>