实验吧安全杂项WP(三）

原创

Neil-Yale 于 2017-03-20 21:30:46 发布 5244 收藏 2

文章标签： c语言 安全 百度 压缩 CTF

本文链接：https://blog.csdn.net/yalecaltech/article/details/64158016

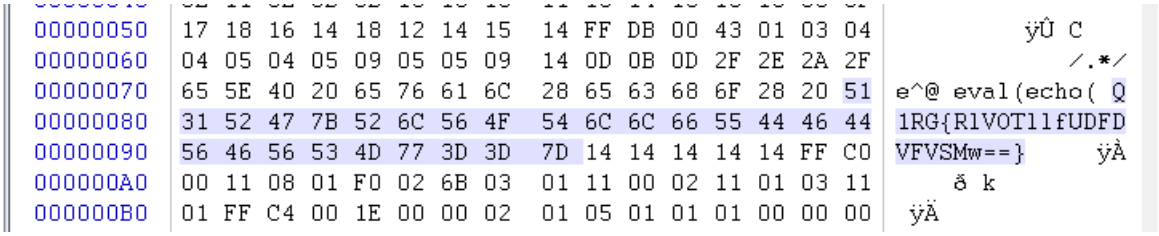
1.有趣的文件（http://www.shiyanbar.com/ctf/1861）
最前面的8位是地址，不用管，后面的应该是文件头，百度afbc 1c27

看样子应该是.7z的压缩文件，不过给出的acsii里面没有37 7a，这就是缺少的，需要我们补上
，补上后发现什么文件也不是，问题出在哪里呢？
百度后发现每两位应该交换一下

这个任务太繁重了，本来还想这放在winhex里面手工的，这里直接python吧

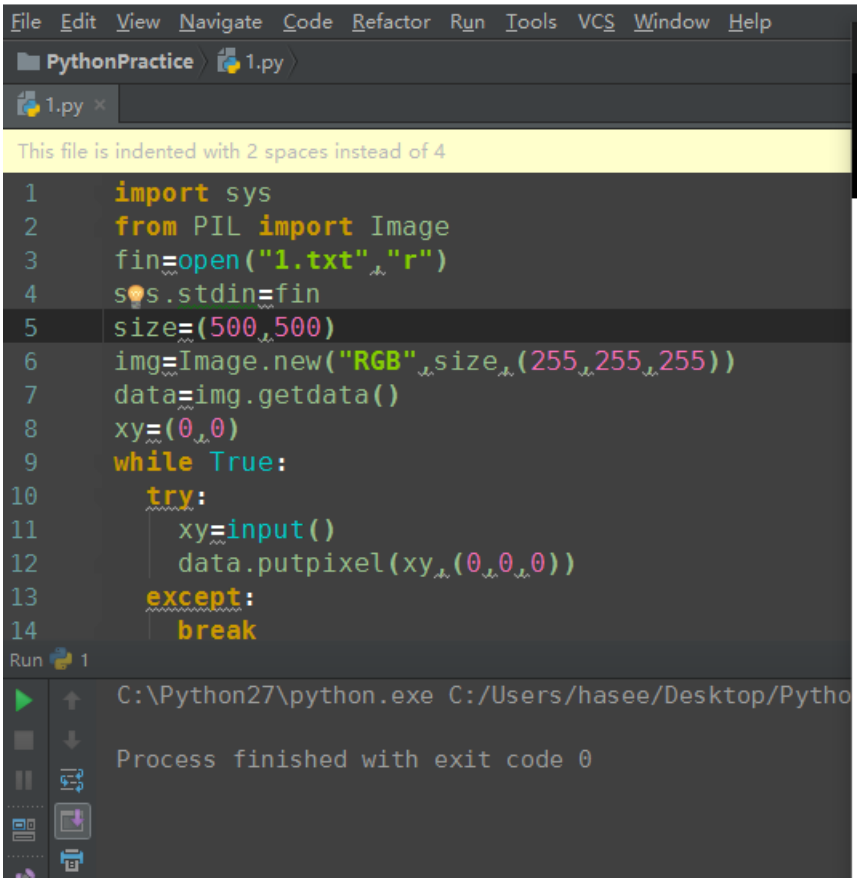
```
def revStr(s):
news=””
for i in xrange(0,len(s),4):
news+=s[i+2:i+4]
news+=s[i:i+2]
return news
```

def foo():
f=open(‘funfile’)
s=”377a”
for line in f:
s+=revStr(line.strip()[8:].replace(‘ ‘,”))
fsave=open(‘fun.7z’,’wb’)
fsave.write(s.decode(‘hex’))
fsave.close()
pass
if **name** == ‘**main**‘:
foo()
print ‘finished’
自动生成fun.7z压缩文件，解压后是一张阿狸的图片，拖进winhex看看，发现疑似flag的base64加密过的



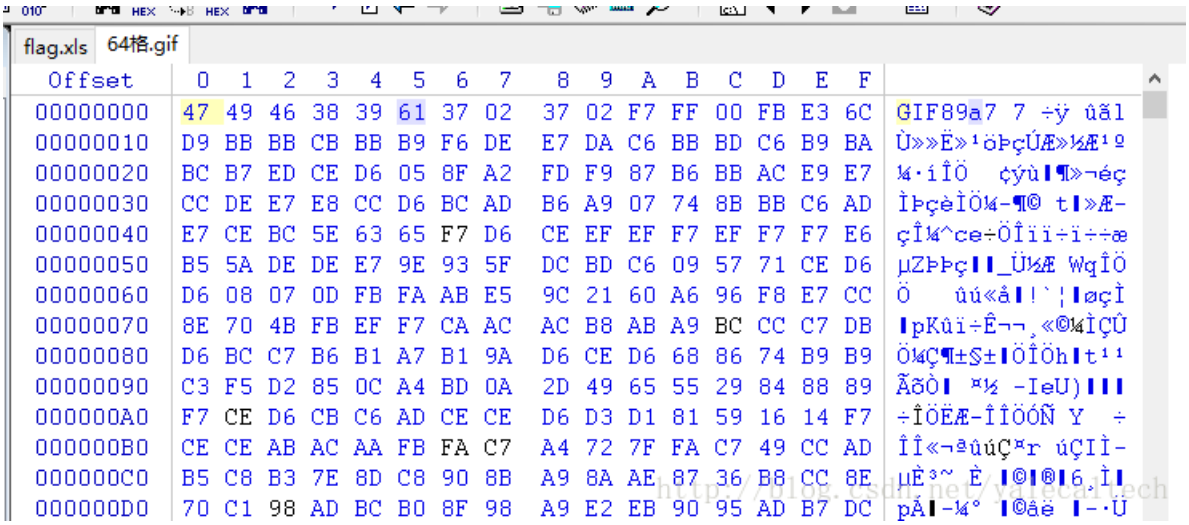
复制后base64解码就行了

2.Paint&Scan(http://www.shiyanbar.com/ctf/1860)
只给出了坐标，肯定是要求作图的咯
先把数据保存下来，然后跑python
(很多大神用Matlab,但是体积太大；有用matplotlib库的，但是安装麻烦）

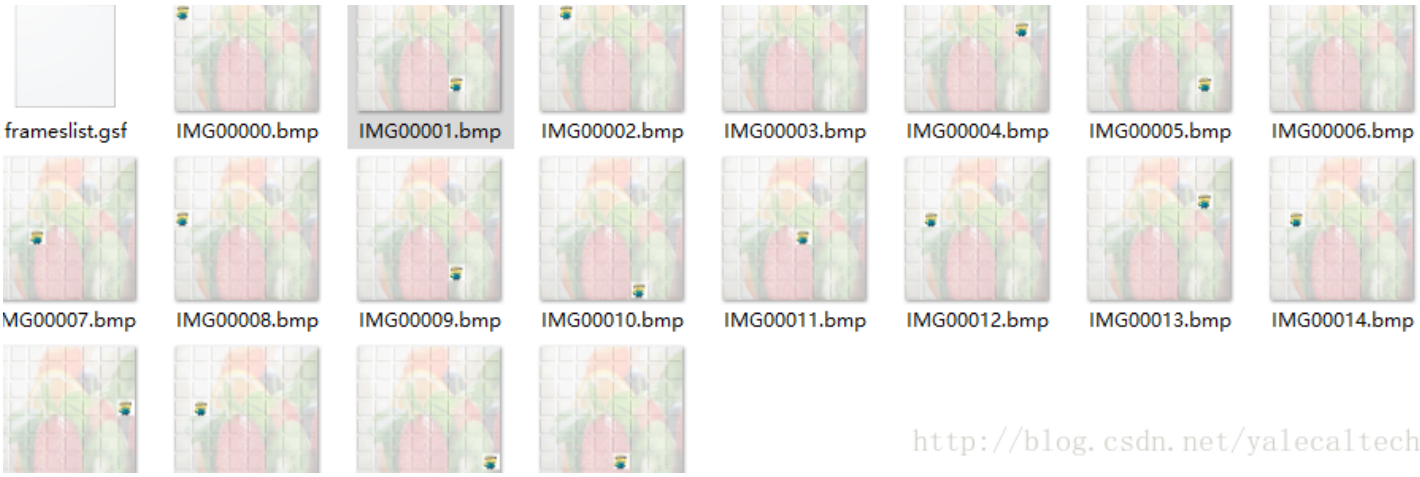


扫描就得到结果了

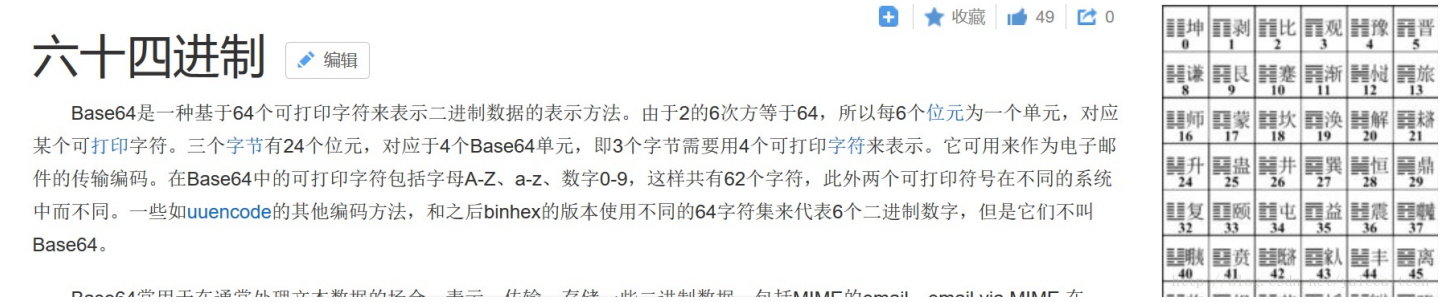
3.64格（http://www.shiyanbar.com/ctf/1857）
下载来的文件解压后是gif，打不开，直接仍winhex
发现少文件头
补上



保存后打开，发现是动图，使用gifsplitter分离得到十九张图片



题目提示64格，图片刚好也是64格
64联想到64进制？base64?
百度64进制
右边这幅图好像有点感觉



对应这维尼所在的格子求得18个数字
16，53，17。。。。。。。
再将数字对应百度百科下的表解得字母

2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8

13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

得到Q1RGe2FiY19kZWZfZ30

base64解码之

得到CTF{abc_def_g}