# CTF\_论剑场 misc杂项 WriteUp(持续更新)

# 

3 篇文章 1 订阅 订阅专栏

CTF 专栏收录该内容

签到题 头像 0和1的故事 Snake 这个人真的很高 你能找到flag吗 向日葵 安慰的话语 画图 flag在不在这里 Blind 火眼金睛 被截获的电报 怀疑人生 500txt c2un easyzip findme 小明的文件 二维码 春节三重礼 之后的再做了之后更新

签到题

# 읍 签到

作者: admin | 已解决: 358 | 一血: admin

签个到吧 flag{abcdABCD1234}

### 提交这里的flag即可

# 头像

53	C4	62	05	D7	8A	9A	15	8C	08	9F	32	C6	79	C9	F9	SÄb.׊š.Œ.Ÿ2ÆyÉù
16	EE	1F	66	6C	61	67	7в	62	47	78	76	64	6D	56	30	.î.flag{bGxvdmV0
61	47	56	6E	61	58	4A	73	7D	00	0в	F9	98	7A	73	0D	aGVnaXJs}ù~zs.
в7	Α9	5C	AE	DF	11	E.3	8F	Α9	45	E.5	23	E6	14	63	DC	·©∖®ß.ã.©Eå#æ.cÜ

### 下载图片用010打开找到flag的字符串

### 用base64转换

加密/解密	散列/哈希	BASE64	图片/BASE64转换		
明文:					BASE64:
llovethegirl				BASE64编码 >	bGxvdmV0aGVnaXJs

### 题目中说要用md5加密后 提交

	ass. novernegin		unicode <u>sinex</u>
S	alt:		HEX
н	ash:		
_	力 <b>D</b> 和 图	<b>E</b>	
_			

于是加密后再提交......

0和1的故事

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	46	6C	61	67	5F	69	73	5F	6E	6F	74	5F	68	65	72	65	<pre>Flag_is_not_here</pre>
00000016	0D	0A	09	20	20	09	20	09	20	09	09	20	09	20	09	20	
00000032	09	09	20	20	09	20	20	09	09	09	20	20	20	09	09	09	
00000048	20	09	20	09	20	09	09	09	09	20	20	20	20	09	09	09	
00000064	20	09	09	09	09	09	09	20	20	20	20	20	20				

解压之后用winhex打开

发现一堆09200920

<pre>&gt;&gt;&gt; str1 = '092020092009200900920092009092020090920200909092020090909202009090920092009 2009090909</pre>	
>>>	~

之后把09替换成1 20替换成0 在hex一下就好了 提交的就是十六进制数(我之前还以为这个十六进制数还要怎么转一下所以一直处在懵逼状态)

# Snake



开始游戏要先注册

실 账号管理		—	×
登录 注册 重置			
账号:	aaa		
Sec. 1			
2510);			
问题:	你所读的中学是?	-	
		_	
答案:	ааа		

注册
https://blog.osdn.nai/qq_41995976

🙆 账号管理	– 🗆 X
登录 注册 重盟	
账号:	aaa
72534.	
<u>сти-</u> у.	
	<b>啓</b> 己
	<u> </u>
	https://blog.csdn.net/qq_41995976

登录后发现是一个贪吃蛇游戏并且题干里说要攒够500分就可获得flag

🔮 Snake Game	– 🗆 X
<u>~~</u>	Account ID:12 用户名:aaa 最高分:0 局数:0
	Game 分数:0 长度:3
	角色1 ▼ 食物1 ▼
	开始游戏
	$\begin{array}{c} \uparrow \\ \hline \\$
	SHIFI 加速 重新开始
https://blog.	osdn.net/gc_41995976

一开始思路是逆向工程 然后找flag 但是根据经验( 并且电脑里正好有CE 就使用CE来改分数了

	🐔 Cheat Engine 6	5.7						— 🗆	$\times$
_	文件(E) 编辑(E)	表单 D3D Ja	va 帮助( <u>H</u> )						
	烈 📂 🔲 —			000	02FE8-javaw.	exe			ŝ
	结里:22								STINGTO
	地址	当前值	先前值	^	新的扫描	再次扫描		撤销扫描	设置
	268C56A0	5	5						
	268C56C8	5	5			但:			
	268C56D8	5	5		Hex [5				
П	268C56F0	5	5		扫描 光刑 報	缅拗值	~	Not	
	268EB2A8	5	5			S WORK LEL			
	268EB2B8	5	5		数值类型 4	字节	~		
	2690D608	5	5		内存扫描选	项			
	2690D618	5	5		<i>∓</i> #4	00000	0000000000		_
	2690FF40	5	5						灵
	2F441678	5	5		停止	7ffff	fffffffffff		
	2F4417F0	5	5		☑ 可写		■ 可执行		
	2F441810	5	5		三 写时拷贝				
	2F441870	5	5			●对齐			
	76BF29550	5	5		⊻ 快速扫描		数		
	<		>	× 🗙	□扫描时暂	停游戏			
	查看内存				0			手动添加	地址
	激活描述		地址		类型	数值			
	无描述		76BF29550		4 字节	5			~
			改变数 请输入 500	(信 、新的数	值:				
							E	<u>O</u> K	取消
	高级选项					https:	//blog.esdn.r	iet/gg_4196	加注释



但是发现改了分数之后的flag为乱码……于是又搞了一会儿发现是长度的问题……

于是把长度和分数一起修改:

			******	
激活	描述	地址	类型	数值
	分数	76D084E60	4 字节	500
	长度	76D0A7F24	4 字节	503



成功获得了flag

这个人真的很高

		_	_	_		_			_	_			_		_	_	
C:E820h:	91	66	C9	66	27	C0	BF	17	90	в3	FE	FF	B1	DE	1E	FE	`fEf'A¿³þÿ±Þ.þ
C:E830h:	98	E5	07	F8	7f	4A	42	01	D7	D7	FD	4E	93	00	00	00	~å.ø.JB.××ýN™ <mark></mark>
C:E840h:	00									0D	0A	0D	0A	0D	$\mathbf{A}0$	0D	
C:E850h:	0A	0D	0A	0D	0A	0D	$\mathbf{A0}$	0D	0A	0D	0A	0D	0A	0D	0A	0D	
C:E860h:	0A	0D	0A	0D	0A	0D	0A	0D	0A	0D	0A	0D	0A	0D	0A	0D	
C:E870h:	0A	0D	0A	0D	0A	61	61	62	49	31	31	75	73	31	31	74	aabI11us11t
C:E880h:	73	31	79	79	30	7D											s1yy0}

首先下载图片后用editor 010打开发现最后有一串字符串尝试补全提交之后没有成功

### **失败!** 姿势不正确.

## CHALLENGES

●类型: misc ▼

×

flag{aabl11us11ts1yy0}

Submit

## 然后题干中说的 这个人很高 可能是要修改图片的高度

struct PNG_CHUNK chunk[0]	IHDR (Critical, Pu	8h	19h	Fg:	Bg:
uint32 length	13	8h	4h	Fg:	Bg:
<ul> <li>union CTYPE type</li> </ul>	IHDR	Ch	4h	Fg: 📃	Bg:
uint32 ctype	49484452h	Ch	4h	Fg: 📃	Bg:
> char cname[4]	IHDR	Ch	4h	Fg: 📃	Bg:
struct PNG_CHUNK_IHDR ihdr	499 x 800 (x8)	10h	Dh	Fg:	Bg:
uint32 width	499	10h	4h	Fg:	Bg:
uint32 height	800	14h	4h	Fg:	Bg:
ubyte bits	8	18h	1h	Fg:	Bg:
enum PNG_COLOR_SPAC	AlphaTrueColor (6)	19h	1h	Fg:	Bg:
enum PNG_COMPR_MET	Deflate (0)	1Ah	1h	Fg:	Bg:

# 于是修改后打开图片发现另外一串字符串



于是又花了好久去想如何去组合试了一会儿发现可能是栅栏密码 但是!!但是!!出来的最接近的组合是这样的



https://blog.csdn.net/qq\_41995976

这几个提交了都不对于是自己按照英语的词义改了位置修改了文本于是提交成功了(这谁受得住?) .....



# 你能找到flag吗

level1根据提示 暴力破解

```
作者: third | 已解决: 7 | 一血: answer42
```

```
youcatflag.zip 小明喜欢用自己的手机号来加密zip,我们通过社工只查到了他手机号的前三位为199,你能解开这个压缩包吗?(手机号为伪造手机号,请不要试图拨打
或社工)
```



C BACK	步骤 4 / 4: 破解密码.Go	NEXT
Ziperello ver. 2.1	版权所有 (C) 2008 FDRLab	https://blog.esdmnet/qc_41995976

### 破解获得密码

) y	oucatflag.zip						- 当前目录	登道找(支持包内查找)	a
×	名称	<ul> <li>大小</li> </ul>	压缩后大小	类型	安全	修改时间	CRC32	压缩算法	
^	(上层目录)								
	🚔 level2.zip *	6.34 KB	6.35 KB	好压 ZIP 压缩文件		2019-04-28 19:56:56	886E308A	ZipCrypto Store	
	Readme.txt *	1 KB	1 KB	文本文档		2019-04-15 22:19:50	3D112FF4	ZipCrypto Deflate	
								₩ ₹ -	
1 #							<b>23</b> 中国压缩3	<b>45好压</b> <sup>软件知名品牌</sup>	1
le	vel2.zip						▼ 当前目	录查找(支持包内查找)	
c	名称	◆ 大小	压缩后大小	类型	安全	修改时间	CRC32	压缩算法	I
^	<mark></mark> (上层目录) ■ level3.zip * 副 Readme.txt *	5.90 KB 1 KB	5.91 KB 1 KB	好压 ZIP 压缩文件 文本文档		2019-04-28 19:56:56 2019-04-15 22:19:50	509A6868 3D112FF4	ZipCrypto Store ZipCrypto Deflate	

level2的压缩包和第一个压缩包 有相同的文件 CRC32值 一样 可以用明文攻击

🔏 ARC	HPR 4.	54 - 10	%			_	-	$\times$		
文件(F)	恢复(	R) 帮	助(H)							
	. Ø		<b>帰</b> 停止	الم الم الم	🥸	(?) ≢88h		<b>同</b> 退出		
				Jacob Claurel	双山关空	:				
IC: Juse	rs (Admir	listrator	pesktop	yeveiz, zip	明义			~		
范围	长度	字典	明文	自动保存	选项 冨	颕				
一明文说	硕一									
明文文	[件路径	:								
C:\Use	ers\Admi	inistrato	r \Desktop	Readme.zip	📄 •	开始于 <mark>:</mark>	9424	<b>N</b>		
	密钥	9932	21cca	密钥	5381d998	密钥	002ba68	3 着		
	- 	- :# #1 <del>.&gt;,</del>	44/2 450	ੀ ਨੇ ਸਹ ਅੰਤ	÷-14-					
1768	+使用_	一进刺又	.I+1F/09	1又 219 相余	XI <del>I</del>					
─状态窗										
2019/5	/17 19:1	11:07 - /	ARCHPR 4	1.54 build 45	已启动	10.10.1	<u>*−1+7 TT</u>	~		
2019/5	/1/ 19:1 /17 19:1	12:34 - ) 12:34 - E	以住℃№ 明文攻击	isers (Adminis 已开始	trator (Deskt	top (evel 2. zi	2日11升。			
								$\sim$		
当前口令	<b>}:</b>	n/a			平均速度:	n/a				
品用时间	]: += `++	8s		10040/1070	剩余时间:	3m	52s			
明义坝世	证住进	:17, 撜	系留钥 (	13348/12/64	+1) %					
				10	ust//interer	esetrone	t/crcr_2tt	995978		
ARCHPR V	ersion 4	1.54 (c)	1997-201	2 ElcomSoft (	.o. Ltd.	rooranni o	a olol - 1 i	555515		

level3是伪加密 解开之后有个图片 修改宽度就可以得到flag了

uint32 iength	13	80	40	rg:	Bg:
union CTYPE type	IHDR	Ch	4h	Fg: 📃	Bg:
struct PNG_CHUNK_IHDR ihdr	640 x 400 (x8)	10h	Dh	Fg:	Bg:
uint32 width	640	10h	4h	Fg:	Bg:
uint32 height	600	14h	4h	Fg:	Bg:
ubyte bits	8	18h	1h	Fg:	Bg:
	True Color (2)	105	16	Ea.	Det

# 

# 向日葵

图片最后有个RAR的文件

00033632	1E	E1	B6	64	3C	E0	9E	73	FD	6B	<b>B</b> 8	FF	00	97	F9	3E	á¶d<àžsýk,ÿ −ù>
00033648	82	В9	FD	6F	FE	42	12	7F	D7	25	FE	B5	93	Α9	26	D5	,¹ýoþB ×%þµ"©&Õ
00033664	CD	62	67	4C	8B	6F	FD	9D	0A	82	40	56	72	01	E7	97	ĺbgL <oý ,@vr="" td="" ç−<=""></oý>
00033680	35	AB	E2	66	1A	6A	Α6	98	55	E4	58	63	0D	23	<b>A</b> 0	E4	5«ấf j¦~UäXc # ä
00033696	BB	72	46	ЗD	<b>B</b> 3	FA	56	5C	5F	F2	12	D3	FF	00	EΒ	9A	»rF=³úV\_ò Óÿ ëš
00033712	D6	F7	89	FF	00	E4	61	BC	FF	00	AE	87	F9	54	C6	2A	Ö÷‱ÿ äa∿ÿ ®‡ùTÆ*
00033728	53	<b>B</b> 3	FE	B5	2D	E8	9B	F4	3C	DE	DE	D1	2E	E1	63	20	S³þµ-è>ô<ÞÞÑ.ác
00033744	05	83	64	0C	E0	8A	CF	BE	D3	C5	99	57	59	33	<b>B</b> 8	FD	fd àŠÏ¾ÓÅ™WY3,ý
00033760	D3	D6	BA	5B	9F	F8	FB	93	FD	FA	E7	<b>B</b> 5	AF	F8	FE	lF	ÓÖ°[Ÿøû"ýú絯øþ
00033776	EE	8A	ED	<b>A</b> 5	29	7B	4B	5F	42	22	4B	69	2C	86	01	92	îŠí¥){K_B"Ki,† ′
00033792	49	07	B1	<b>A</b> 2	9B	65	FE	A0	FF	00	BD	45	39	45	5C	47	I ±¢>eþ ÿ ≒E9E∖G
00033808	FF	D9	52	61	72	21	1A	07	01	00	33	92	B5	E5	0A	01	ÿÙRar! 3′µå
00033824	05	06	00	05	01	01	80	80	00	8E	DO	B5	F7	23	02	03	€€ ŽĐµ÷#
00033840	0B	87	01	04	C2	01	20	C2	04	30	1C	80	03	00	07	36	‡ Â Â 0 € 6
00033856	36	36	2E	74	78	74	0A	03	02	17	1B	89	15	E5	98	D4	66.txt % å~Ô
00033872	01	C5	1B	84	26	54	74	23	F6	70	34	BE	04	E2	6D	2E	Ă "&Tt#öp4¾ âm.
00033888	C7	78	D4	25	0D	32	53	39	5E	D3	22	35	22	Α6	82	82	ÇxÔ% 2S9^Ó"5"¦,,
00033904	2B	A0	86	A0	BA	2A	2A	3C	0D	E0	2D	6B	46	FE	7F	90	+ † °**< à-kFþ
00033920	51	E3	59	47	8C	CC	F7	2C	F8	FA	FC	A3	D9	EC	CE	31	QãYGŒÌ÷,øúü£ÙìÎl
00033936	55	D4	3C	5C	17	F2	ЗF	5B	47	0C	EE	53	32	7C	6C	BE	UÔ<∖ ò?[G 1S2 1¾
00033952	Β4	52	89	E2	85	0F	94	B8	54	C4	B6	F7	EC	4F	C2	50	′R‰â… ″,TĶ÷ìOÂP
00033968	64	FF	B8	0D	45	52	6B	4A	C0	F1	97	80	<b>E1</b>	24	57	9E	dÿ, ERkJÀñ—€á\$Wž
00033984	EA	F4	<b>A</b> 1	96	4A	2C	D0	81	73	C3	00	D2	46	DF	BF	AB	êô;−J,Đ sà ÒFß¿≪
00034000	FC	3C	87	6B	51	35	Α4	80	1D	77	56	51	03	05	04	00	ü<‡kQ5¤€ wVQ
																	.csdn.net/qq_4199597

一开始是用foremost跑了一边发现没出来 然后就自己粘贴复制把rar提出来了

文件(F)	编辑(E)	格式(O)	查看(V)	帮助(H)	
在一个。 (2, 5)	a[5][5]	的二维数	效组中有	下列几个	·元素
(5, 1) (2, 4) (2, 5)					
(3,5) (3,2)					
(1, 4) (5, 1)					
(2, 2) (2, 5) (4, 5)					
(2, 1) (1, 2)					
(4,5)	8/1/				
囲之ゴ1≀ 	ag走什么	HE C.CS			

得到一个txt

看到是一个5x5的数组就想到了波利比奥斯方阵密码 但是试了一下发现并不对

ſ.,	1	2	3	4	5
1	a	b	с	d	е
2	f	g	h	i	j
3	k	1	m	m	Ο
4	р	q	r	s	t
5	u	v	w	х	у

得到 juijoldugjtfbty 凯撒遍历解密得到 ithinkctfiseasy

这题给的提示是真的少

# 安慰的话语

先把科加斯的图片拉去binwalk跑一边 得到一个压缩包

压缩包的txt里有段佛曰……

佛曰: 能那栗俱曰皤大夜呐漫侄依佛梵遮等諳顛老訶老諳者耨梵婆真輸故般豆輸俱明皤涅諳得缽跋無俱提至朋缽上實遮侄遮皤心菩呐老皤夷 梵諦爍南咒怯心究呐明缽神罰故諳輸勝俱蘇一哆摩恐哆喝哆切切諳阿死哆若有摩缽真若夢姪侄離蒙哆倒是侄薩曰怯耶豆般利皤都若夜俱耨逝 訶諳無侄悉涅皤波諳耶諳婆罰彌倒諳摩缽智梵闍怯波罰遠地若侄迦梵闍實殿侄依喝梵寫槃醯特三除竟呐滅諳究漫諳一等冥耶侄世地缽提吉羅 皤除罰遮咒薩薩梵盡

像是前几年很流行的佛曰加密来着(那时候好多论坛和群里都玩这个来着?)

http://www.keyfc.net/bbs/tools/tudoucode.aspx 解密地址

得到一串

e58e8be7bca9e58c85e5af86e7a081e4b8ba7061737331323321212121

一开始没啥思路 试了很久 最后发现 把他们加上%然后urldecode解码就好了

%e5%8e%8b%e7%bc%a9%e5%8c%85%e5%a<del>f</del>%86%e7%a0%81%e4%b8%ba%70%61%73%73%31%32%33%21%21%21%2

得到压缩包密码为 pass123!!!! 然后另外一个压缩包输入密码进去之后 会有一堆压缩包

最后到一个虚空.zip的压缩包 是一个伪加密

里边有个txt是base64 转码后得到一个urldecode 再转得到

> 公正公正公正友善公正公正*屏蔽的关键字*公正法治法治诚信*屏蔽的关键字*自由友善公正公正敬业公正法治公正爱国法治自由平等友善敬业公 正友善敬业公正公正平等友善敬业公正爱国公正友善敬业法治富强公正平等法治友善法治

# 去试了一下flag{

社会主义核心价值观:富强、	民主、文明、	和谐;自由、	平等、公	证、法治;	爱国、敬业、	诚信、友善	
flag{							
					编码		
	_						
公正公正公正诚信文明公正	民主会正法治	法治诚们民主					

发现前面内容和解码得到的一样 所以猜测这两个被屏蔽的就是民主了

填进去再转码就得到flag了

画图

首先把flag.bmp放在winhex 发现下边有好多类似于 0 0 255 255 255这样的数值 猜测是 坐标和RGB的值 我们把这个数值复制一下放到一个txt里

■ 画图.txt - 记事本	– 🗆 X	
↓ 文件(F) 編辑(E) 格式(O) 查看(V) 報助(H) 0 0 255 255 255		
0 3 255 255 255		H
0 4 255 255 255 0 5 255 255 255		1
0 10 255 255 255		
0 11 255 255 255 0 12 255 255		
0 13 255 255 255 0 14 255 255 255		P
0 17 255 255 255		
0 18 255 255 255 20 19 255 255 255		
0 20 255 255 255 0 21 255 255		
0 22 255 255 255 0 23 255 255 255		
0 24 255 255 255 255 255 255 255 255 255		
0 26 255 255 255		
0 27 200 200 200 0 28 255 255 255		
0 29 255 255 255 0 30 255 255 255		
0 31 255 255 255 0 32 255 255 255		
0 33 255 255 255 0 34 255 255		
0 35 255 255 255		
0 37 255 255 255		
0 38 255 255 255 255		
10 40 255 255 255 0 41 255 255 255		
0 42 255 255 255 0 43 255 255 255		
0 44 255 255 255 0 45 255 255		7.61

然后可以利用python来画图 代码:

```
from PIL import Image
x = 173 #x坐标 通过对txt里的行数进行整数分解
y = 173 #y坐标 x*y = 行数
im = Image.new("RGB",(x,y))#创建图片
file = open('画图.txt') #打开rbg值文件
#通过一个个rgb点生成图片
for i in range(0,30000):
    line = file.readline()#获取一行
    rgb = line.split(" ")#分离rgb
    try:
        im.putpixel((int(rgb[0]),int(rgb[1])),(int(rgb[2]),int(rgb[3]),int(rgb[4])))#rgb转化为像素
except:
        im.show()
        break
```

代码是直接拿这个博主的代码改的 https://www.cnblogs.com/webFuckeeeer/p/4536776.html

flag {painterYOur}

得到flag

flag在不在这里

首先一个rar的压缩包 暴力跑一边就发现了密码

A 🙈	RPR 1.53 - 0%		_	
	Advanced RAR P	assword	Recovery	
	🖹 🦬 🧖	٢		
	」井 1条仔 开始! 1号止 家四日成功恢复1	基准	帮助  天士	返出
G:	Advanced RAR P	assword Reco	very统计:	^
范	总计密码	385		
-3	总计时间	4s 443ms		
불	平均速度(密码/秒)	86		
G	该文件密码	666		6
	16进制密码	36 36 36		6
			✔ 确定	
一状态	の間口			1
\ct:	f\ctf工具\压缩包破解\rar\			^
2019 2019 2019	9/5/21 21:02:19 - 开始字英顺解 9/5/21 21:02:23 - 密码已成功恢复! 9/5/21 21:02:23 - 666、是该文件的	的有效密码~		~
当前海巴西部	密码: 666 时间: 4s 硕解处理中,已处理 385 密码	平均速度: 剩余时间:	86 p/s 46m 38s	
	(	0%		-
ARPR	version 1.53 (c) 2000-2005 ElcomS	Soft Co. Ltd.		

所以就在这里边找 最后找着找着发现改一下高度就行了

	union of the type	INDIC	
1	struct PNG CHUNK IHDR ihdr	518 x 1000 (x8)	10
	uint32 width	518	10
	uint32 height	1000	14
	ubyte bits	8	18
	enum PNG COLOR SPAC	TrueColor (2)	19

(一开始改的比较小还没看到来着之后想着下边没有出现黑色就又试着改大了一点)

flag(e53a0a2978c28872a4505bdb51db0	16dc) log.csdn.nai/qq_4199597

Blind

下过来图片里边有个压缩包分离之后发现两张图片一样题目是Blind猜测是盲水印加密 于是用脚本decode即可

python2 decode.py --original blind.png --image blind\_blind.png --result result.png



# 结果

github地址: https://github.com/linyacool/blind-watermark https://github.com/chishaxie/BlindWaterMark 两种加密方式不同 解不出来用另外一个试试

# 火眼金睛

拿到的题目到手是一个压缩包 题干中给的提示有tips:five-digit 于是猜测是5位数字

	字符类型: 固定	定字符集	[	4
字付集 ▼ 数字 (0 - 9) □ 小写字母 (a - z) □ 大写字母 (A - Z)	□ 特殊符号(!@) □ 空格 □ 所有印刷字符	最小密码长度 = 最大密码长度 =	5 <b>•</b>	<b></b>
	1- 200 -			



暴力破解后得到密码

^	(上层目	目录)										
	💼 flag.pr	ng *			280.71 KB	279.87 KB	看图王 PNG 图片		2018-12-06 11:20:10	0AD401E5	ZipCrypto Deflate	
	readm	e.txt *			1 KB	1 KB	文本文档		2018-12-06 13:21:1	A5C515EC	ZipCrypto Deflate	
											- ₹ ₹ -	
1		Δ										
	8	٩.								2	345灯止 🖆	
	删除	密码	自解压	工具箱						中国压缩	软件知名品牌 📕	
	Crack.zip									- 当前	目录查找(支持包内查找)	Q 高級
×	名称				大小	压缩后大小	类型	安.	修改时间	CRC32	◆ 压缩算法	路径
^	、(上屋	]目录)										
	💼 flag.z	tip *			280.75 KB	280.76 KB	好压 ZIP 压缩文件		2018-12-06 13:27:26	5 EABEC170	ZipCrypto Store	
4	📄 readr	me.txt *			1 KB	1 KB	文本文档		2018-12-06 13:21:	A5C515EC	ZipCrypto Deflate	

下一个压缩包内有和已经破解出来的压缩包一样的文件 于是又用到明文破解了

但是这里可能会出个问题 把之前的Readme.txt压缩之后开始明文攻击的时候可能会出现这里的提示



这里尝试了好久也找了许多资料发现是压缩算法的问题我这个压缩的算法和作者压缩的算法不一样

🔒 压缩3	く作								×
4	231	<b>1</b> 5	纾压	• •	<b>国</b> 压	缩影	<b>と件知</b> ■ 180=#	名品	牌
受抑	क्रम्य	文件	笡法	RTIA	注释	кащі ]	ni (axaen o	¥9.0021	.90)
- 压缩	算法	AIT .		HUIHU	171+				
压缩	方法(M):	Deflate	:64	$\sim$	线程个数	(T):	7 ~	(8 CPV)	
字典力	大小(D):	64 KB		$\sim$	文件类型	过滤:			
单词	大小(₩):	32		$\sim$	◉开倉	∃(¥)	○关闭(	N)	
固实力	大小(S):			$\sim$	ŝ	扁辑过	滤列表(E)		
П	近乘内方。	997 <b>10</b>							
压细) 解压)	∬需内存: 新需内存:	227 MB 2 MB			J	玉缩方	式配置(A)		
切换至	轻巧模式		ā	角定(O)	e//alo.a.	取消((		帮助(H)	978

所以没办法破解 于是换了个算法 再次尝试

口令已成功恢复!		×
Advanced Ard	hive Password Recovery 统计信息:	
总计口令	n/a	
总计时间	9s 14ms	
平均速度(口令/秒)	n/a	
这个文件的口令	Kkdlong!	- Ca
十六进制口令	4b 6b 64 6c 6f 6e 67 21	<u></u>
保存…	✔ 确定	

破解成功 得到张图片



首先在winHex查看 最后有组base64

<b>.</b>	12	LA	00	00	00	00	00	00	10	00	- 1	<b>1</b> 1	21	21	21	2.7	
<b>1:</b>	91	91	FF	BC	$\mathbf{FC}$	$\mathbf{F}\mathbf{D}$	F7	FF	03	15	26	E2	A3	в3	52	9в	``ÿ¼üý÷ÿ&⣰R>
	6B	00	00	00	00									0D	0A	0D	L TEMPOD
<b>1:</b>	0A	5A	6D	78	68	5A	33	74	55	61	44	46	7A	58	7A	46	. ZmxhZ3tUaDFzXzF
<b>1:</b>	7A	58	32	5A	68	61	32	56	6D	4D	57	46	6E	66	51	ЗD	zX2Zha2VmMWFnfQ=
	3D																=

解出来是flag{Th1s\_1s\_fakef1ag}这是个假flag先尝试一下能不能提交……



						-9-
/	struct PNG_CHUNK chunk[0]	IHDR (Critical, Pu	8h	19h	Fg:	Bg:
	uint32 length	13	8h	4h	Fg:	Bg:
	> union CTYPE type	IHDR	Ch	4h	Fg: 📃	Bg:
	struct PNG_CHUNK_IHDR ihdr	500 x 800 (x8)	10h	Dh	Fg:	Bg:
	uint32 width	500	10h	4h	Fg:	Bg:
	uint32 height	800	14h	4h	Fg:	Bg:
	ubyte bits	8	18h	1h	Fg:	Bg:
	enum PNG_COLOR_SPAC	AlphaTrueColor (6)	19h	1h	Fg:	Bg:
		B (1 + (B))		- 1	-	



# 出来混 迟早要还的

flag{40 https://diog.cs/493d}1995976

得到flag~

被截获的电报



/ 4 / 71 144 15 4

## 摩斯密码在线加密解密工具

01 1010	1 00	11111	10 1101	001 0	0 1010	101			
Space:				S	hort:	0		Long:	1
加密	解密								
AC	ĴΩ								

得到flag

# 怀疑人生

下过来一共三题

第一题跑一边字典 密码为password 里边文本先转base64 在urldecode XHU2Nlx1NmNcdTYxXHU2N1x1N2JcdTY4XHU2MVx1NjNcdTZiXHU2NVx1Nzl= 得到: flag{hacker

先跑一边 short ook!

https://www.splitbrain.org/services/ook 得到 3oD54e 再跑一边base58(这谁想得到??) http://ctf.ssleye.com/base58w.html 得到 misc

第三题不能直接用手机扫出来 这里用这个网站扫可以扫出来 https://online-barcode-reader.inliteresearch.com/

得到12580} 三个一起提交就行了

# 500txt

一开始没什么思路 还以为是要转码什么的 想了半天没啥思路 就想着是不是里边藏了什么关键字 就自己写了个脚本查

```
for i in range(1,501):
  with open(str(i)+'.txt',"r") as f:
    str1 = f.read()
    if 'key{' in str1:
        print(i)
```

试了flag、ctf、key之后 再到txt里看了一下 就找到flag了

# c2un

下载过来是一个doc文件 打开出现这样的页面

😡 C@n	U.docx		$\odot \times$	+							
9 - C	⊽ 开始	插入	页面布局	引用	审阅 视	图章节	安全	开发工具	特色应用		
ఝ雅黑 3 <i>I</i> ⊻-	· -= ∴ · ײ ×₂	- A⁺ A - a≵	A <sup>-</sup>	ý - ∷ _ =	- ≟ - ≞ ≞ = ■	≟ Å* ≝ ≛≣ *	원 ≒-4 ☆-⊞-	AaBbC	cDd AaBb	AaBb() 标题 2	AaBbC( 



https://blog.csdn.net/qq\_41995976

### 于是放到winhex看一眼

C@nU.docx																			
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	1		ANSI ASCII	^
00000000	50	4B	03	04	14	00	00	00	08	00	87	4E	E2	40	D4	в	FK	‡Nâ@Ô¶	
00000016	FF	DA	61	01	00	00	98	05	00	00	13	00	00	00	5B	4	ÿÚa	~ [C	
00000032	6F	6E	74	65	6E	74	5F	54	79	70	65	73	5D	2E	78	6		_Types].xm	
00000048	6C	B5	94	4B	4F	C3	30	10	84	EF	48	FC	87	C8	57	94	lµ″KO	ÃO "ïHü‡ÈW"	
00000064	B8	70	40	08	35	ED	81	C7	11	7A	28	12	57	E3	6C	5A	,p@ 5	í Ç z( WãlZ	
00000080	0B	BF	E4	DD	96	F6	DF	B3	49	1F	07	54	35	0D	85	4B	¿äÝ-	öß I T5K	
00000006	74	61	20	50	on	26	Þ¢	07	50	0.5	80	ъo	1.2	1.2	07	τo	84-6	កត+និតនាពិ 🗛	

**B** •

flag 不在这里哦

#### PK字样 应该是个压缩包 改后缀名打开

•	C@nU.zip\_rels			
×	名称	大小	压缩后大小	类型
	(上层目录)			
	🚔 flag.zip	10.26 KB	10.18 KB	好压 ZIP 压缩文件
	🔮 .rels	1 KB	1 KB	XML 文档

### 在里边的一个文件夹里找到flag.zip

这个压缩包是有密码的 里边有给出提示弱口令 于是就拿去字典跑一下 得到密码是password



打开me}.txt 发现是一堆十六进制字符 先拿到去转换一下 看到了PNG的文件头 所以放到WinHex变成图片

16进制到文本字符串的转换,在线实时转换 16进制到文本字符串的转换,在线实时转换(支持中文转换)
加密或解密字符串长度不可以超过10M
E4FA7E97D6F7D667DF8A0D689DC74FD2CF5FA588FBDE2989FA0A11F7CFD00C029492BA668BB64C374976AA77A87D237F3D5B650294F57CC66F54E374EA7E93D7D82F 5BAA8E9F7FAFD31BF4E433FEFD20280E392564CD176C986E92ED54EF50EA56FE6AB3DAC3A9EAE92CDEA9D6E9C51337CC51CEBF881AEFBFD313F50433FF5EA02808392 564CD176C986E92ED54EF50EA56FE6AB6DA1529EA898CDE74DADE7D53C5F31D33A7EA0EB7E7FCCCFD4D02FB0C600E070A41553B45DB261FABD0AA77447D367F3E13 652354F51CF66B2A8E9EC9AED2BE65BC78B9A7EA91F1FF36335F4CBAC3400381069C5146D976C98EE52ED54EF50FA66BEDA46AAE629EAD94CAEB4369AF08BA65CDFF7 F6DE8F0FF8BD1AF7A22600600C69C5146D976C987EAFC229DDD1F4D97CB82D54CAB314B3C95C696D34E1174DB9BEEFEDBD1F1FED7B35E8454D00C024D28A29DA31 D933FD5E8553BAA3E9B3F9701BA99AA7A86733B9D2DA68C22F9A727DDFDB7B3F5ED4345EC35DD404000C23AD98A24D936DD3EF5538A53B9A3E9B0FB791AA798A7 A36932BA08D26FCA229D7F703BDF7FBE37CB2867BA53506008723AD98A27D939DD32F5535753BA0BE9C6FB791AA798A7A36932BAD8D26FCA229D7F703BDF7FBE37CB2867BA53506008723AD98A27D939DD32 F55B5454D1C449FCD87D848D53C453D9BC995D646137EC594EBF8B1AE7BC5413E59635DD404000C23AD98A27D939DD3EF5538A51BE6CF4759FF7187F53DFC50553B4
16)世期任字符     字符转16进制     清空结果     8       ◆PNG     □□□
IHDRocccccccccccccccccccccccccccccccccccc

### 打开图片 发现是一片空白 试了好久 发现放到stegsolve里有反应





结合之前压缩包里的文件名 猜测flag可能为flag{seeme} 提交之后成功了……

# easyzip



打开encrypt文件 发现zip的压缩包是用时间戳加密的



### 查一下现在的时间戳大概是155xxxxxx

👔 Ziperello				_	
ziperello	) vord recovery to	ol	帮助	关于	退出
	字符类型: 固定的	字符集			
「字符集 ▼ 数字 (0 - 9) □ 小写字母 (a - z) □ 大写字母 (A - Z) □	│ 特殊符号 (!@) │ 空格 │ 所有印刷字符	最小密码长度 =     1       最大密码长度 =     10	■ L L L L L M M M L M M L M M L M M L M M L M M L M M L M M L M M L M M L M M M M M M M M M M M M M		
	步骤 3				
<ol> <li>选择字符集类型:固定或自</li> </ol>	自设。				
定义可能存在于密码中的字符	F集。				
3. 设置最小及最大密码长度。					
4. 输入起始密码(非必需)					
		步骤 3 / 4: 暴力破解设定	1.0		NEXT 💓
Ziperello ver. 2.1	版权所有 (C) 2008	FDRLab	nups://ble	терезентнөмер	e <u>-</u> 471995976

### 爆破一下 就可以出来了

👔 Ziperello				_	
ziperello zip passwo	ord recovery too	bl	帮助	关于	退出
	当前密码长度 当前密码 当前速度	10 信息 ×	また。 生备就绪,请点击[开始] 主意:搜索进度条(%)及 前的密码效验长度相关。	<b>步骤 4</b> 按钮 剩余时间字段显 破解 AES 算法加	記示的信息与当 嘧的密码可能
逝去时间: 00:00:06	15%	金内: 1552529384     通定	。 刘秋(昭		
18:28:30: 密码 <b>: <sup>*</sup>155252938</b> 4	↓".时间:6s				
		步骤 4 / 4: 破解密码.Go			
Ziperello ver. 2.1	版权所有 (C) 2008 F	DRLab	hitps://blog	<del>.eschinet/cj</del>	E4H995976

# findme

压缩包里有个flag.vmdk文件 去搜了一下好像要用虚拟机安装虚拟盘什么的 感觉太麻烦了就用winhex看了一下看到里面有zip文件头就去用foremost-master跑了一下 还真跑出来一个压缩包

← → ▼ 12 \= ▼ ■ 00006072.zp							白前日		
◆ 名称	大小	压缩后大小	类型	安全	修改时间	CRC32	压缩算	注释	
(上层目录)								据悉解压密码是43开头的手机。	弓
indme.jpg *	686.91 KB	671.36 KB	看图王 JPG 图		2017-08-04 20:13:35	DB5CEF9F	ZipCr		

旁边有提示是13位开头的手机号



拿软件爆破一下是一张图片

规安全	详细信息 以前的版本	
		_
属性	值	^
说明 ———		
标题		
主题		
分级	$\Rightarrow \Rightarrow $	
标记		
备注	flag{3df136a74f51b7767ba0172713b06	1
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	3840 x 2160	
宽度	3840 像素	
高度	2160 像素	
水平分辨率	96 dpi	
垂直分辨率	96 dpi	
位深度	24	~
删除属性和个人		

(上层目录)				
1.txt *	1 KB	1 KB	文本文档	201
2.txt *	1 KB	1 KB	文本文档	201
3.txt *	1 KB	1 KB	文本文档	201
100 小明的文件.pdf *	21.50 KB	16.11 KB	看图王	201
歴中「11×14(0チロ)				

下载过来的压缩包有四个文件 其中三个txt 只有六个字节 跑了一遍弱口令 和伪加密 发现都不能 那应该就是要crc32碰撞了

小明的文件

c 🔤 选择C:\Windows\System32\cmd.exe —	×
alternative: 4Dimre (OK)	
alternative: 6Y2cB4 (OK)	
alternative: D55UOm (OK)	
alternative: E5tdTt (OK)	
alternative: NRDIvD (OK)	
alternative: P10kVQ (OK)	
alternative: Q1qZMH (OK)	
alternative: Vi98fw (OK)	
alternative: Vuvdgc (OK)	
alternative: X/Dibe (OK)	
Talternative (marging DK)	
alternative: crc32K)	
alternative iDr/gi (OK)	
alternative. indig (ok)	
alternative: wfKOFk (OK)	
alternative: zI s9u (OK)	
G:\学校需要的文件\ctf\ctf工具\CRC32碰撞\crc32-master>python3 crc32.py reverse 0x6A037F6B	
4 bytes: {0x97, 0xf7, 0x0a, 0x34}	
verification checksum: 0x6a037f6b (OK)	
alternative to the form	
alternative bbits_ (UK)	
alternative	
alternative, Surun (OK)	
alternative. SloClr (OK)	
alternative: 4FPDi (OK)	
alternative: bthYpu (OK)	
alternative: chf4jx (OK)	e
alternative: kbp₩fP (OK)	
sitemeting: 1s2Ells (02)	



### G:\学校需要的文件\ctf\ctf工具\CRC32碰撞\crc32-master>

https://blog.csdn.net/qq\_41995976

都跑一边找出有规律的字符串得到 easy\_crc32\_6bits 成功解压文件 打开pdf 发现一个二维码



扫描后发现是个假的flag 放进winhex、010editor、一系列操作都没结果后 于是我就开始了一波神奇的操作了!

	☑ 小明的:	文件.pdf 🕹		1	1 → 1		8
1							
2	输出格式:	docx	▼ <u>设置</u>	🗹 🌾 提取图片中	的文字		
	输出目录:	PDF相同目录	▼ 保存到P	DF相同的目录		开始转换	070

首先 我先 把他转成了DOCX





然后改成ZIP

← → ▼ 🛃 ≔ ▼ 📙 小明的文件.zip\word\media					
◆ 名称	大小	压缩后大小	类型	安	修改明
(上层目录)					
mimage1.png	11.40 KB	11.17 KB	看图王		2019
image2.jpeg	16.84 KB	13.94 KB	看图王		2019

打开居然找到了两张图片 其中一张是PDF本来就有了 另外一张是这个



用PS修复了一番加了三个点点之后就得到了这个二维码 扫出来就是答案了



注意!!!上边的转成doc做法是在扯蛋!! 后边我发现直接把PDF拉去foremost-master跑一边分离就好了!!

函 > 新加卷(G:) > 学校需要的文件 > ctf > ctf工具 > 图片隐写分离 > foremost-master > outfile > jpg



二维码

<u>т</u>	0		_	/■ 压缩包密码.txt - 记事本		_		×
e	( <b>1</b>			 文件(F) 編辑(E) 格式(O) 查看(V) 帮助(H)				
删除	密码	自解压	工具箱		gAAArIAAACtCAIAAADDBAuwAAAAAXN	SROIA	rs4c6	QAAA ^
- 49/77				AKnQUIBAACxjwv8YQUAAAAjcEhZcwAADsMAAA/DAcdvc zCwnKOWUO3ogwOdWr1QUOo3oV9gR/PWHAKCRBOBAyAIA	qGQAAAZ/SUKBVHhe7d1NcujIFIXRXh( ATGOBABCy/AAATWOAAbCy/AAFTWAAAbCy	cLYjZ wC∆⊬∆	зхрух Ц≬∩Ма	Yqql CACB
	ə (I).zıp\匙日			kAQAQsgAACFkAAIQsAABCFgAAIQsAgIAFAEDIAgAgZAE	EAELIAAAhZAACELAAAQhYAACELAICQI	BQBAy	AIAIG	QBAB
×	◆ 名称			CyAAAIWQAAhCwAAEIWAAAhCwCAkAUAQMgCACBkAQAQsg	gAACFkAAIQsAABCFgAAIQsAgJAFAED	IAgAg	ZAEAE	LIAA
Pro CC ^	(上层目录)			ANZAACELAAAQNYAACELAICQBQBAyAIAIGQBABCyAAAI	VQAAHCWAAEIWAAAHCWCAKAUAQMgCACI	BRAQA	QsgAA	CFkA
	💼 wenjian.rar			AIUSAADOF GAAIUSAGJAF ADDIAGAGAAAADDIIAAAADAAAA AARIWAAAACwCAxAHAOMgCACBxAQAQqaAACFxAAIQqgN	/s6/rP7PaVc	DUYAA	AIWQA	Ancw
	📄 压缩包密码.tx	:		+CXkwVwpoz1JzKx28Jten/fLtP55fad81W/8fM539/Ac	caPss7je9ueT9SWe/hsEB7wXWQBnail	P1znQ	fDV₩w	jO3D
				0M2Ifrbj0yneZdv2Go/SY7v+4N/w4B0CL00WwJnGkXp/	/xG4T9tFM7488n/jZti1apvVhdpe7+			-
				+1fzoY3+fRVZQG8F1kAZxom70G8KRczgnfDdr4238298	Se1Z3Xbdoh30H9N			
				+5Ue2L4ILWAKI2ISOAYQIFSA7KgYWphGK3nmXIDXUI+2 +5I8+nc+I5dbCsI1w7x6H/I+sYmPD164w5sF6z8n58DI	2/109+epApI9U2222bHa/A Lk&Vunczn26PI0c/ONOTmk20694d34	71 P		
				+vVSNp/OtqO+W9ugXVzOm2Vdvzsdzwf5Mbg78n9CFsDL	_kgVwpiKHm/F8MV0vo/z40UAThe3x7	∦x/fQ	uNpi	
6)				+bXBheYHpmPhrfUVs8Xdxv9Mj4NPC6ZAGcqU3f8r/ud	X5PB9s0Xabv5dJ/Zmrv5n1b2C7vtV3I	K8vUV	xjqY1	Pmde
				90V+YFyo21314v1HexvAG9HFsCJD1M0Q/urD				
_				+U6yefj79stfxDQL21qFhz2a8rVdjFP9PG/3DzcmW7MJ	l/a/5sj7Wx6qW8gCeHOyAM5zHKJ1rk)	83+98	Aft	
				+uSyesHXUU+dUZeZyrXbyu3yoF96IARW53phvZtAHL+j	]rteDI/l/erxkan Ju726f+LfW0.uk9T/iLu70C9LFickm	5 mm 4 m	Ph6/m	0rmB
				elCzot9ri66anmw17HZVt	UNISOCCITEIR SXROL ( JEANGAGEL KAD	JIIII 142	NDO/ W	aypp
				+07T6T6vLR08R0DTL01vZPsjiHT3568vC7wMWQAAhCwA	AAEIWAAAhCwCAkAUAOMgCACBkAQAQs	e AACF	kAAIQ	sAAB
				CFgAAIQsAgJAFAEDIAgAgZAG8oXx98vaNxev3KT/9EuF	P2zcfL1yAX/RuR81XJ7fi4TV0DfCxZ	ĂG9oy	II	
				+shtZAPwfsgDe0D4L+tkPJvajLKhkAfxqsgD01Iftogz	zjcm05u1663L62LNjvUP/H30/7cd+jI	Ha/Xt	iHfz	
				+uzZX306hrgY8kCONH6JwGLPnb319uIXib0zt0s00w5c	q11wKffr+B			
				+z1Dv3jbs1wMeSbfAitnicD2M/oof13S8Knq3sj3X8Pz	zq+ftVrs/Ec+EiyAM/Uh2IR53flBnE			
				+Sp77/d6fH1agrU4+tYYmN7uVcDfCx74Kd7ppuV5pcfu	nuoemgnqx/S/DvgUDU+ vatoFt9baj91 bafz1wT/POwWt5f1dOf	ຂະວັນດ	BoCib	Onfh
				bZ3HGcGR2V/Wrv+Vv5sFT1aWEtid1IHfi/v6ZaP5T10	ofCxZAB	owany	DIGID	opio
				+szvUnjHwgZAF8mO2zgtXygcMDu08UgF9NFsCHGbLg				
				+bAvi1ÜBIÄvgd/vhbxmA30IWAAAhCwCAkAUAQMgCACBk	kAQAQsgAACFkAAIQsAABCFgAAIQsAg	JAFAE	DIAgA	gZAE
				AELIAAAhZAACELAAAQhYAACELAICQBQBAyAIAIGQBABC	CyAAAIWQAAhCwAAEIWAAAhCwCAkAUA(	QMgCA	CBkAQ	AQsg
				AAUTKAAIUSAADUT GAAIUSAGJATAEDI AGAGZAEAELI AAP	ANZAACELAAAQNYAACELAICQEQEAyAII	AIGQB	ABCyA	ADO/
				v zbr uzy 112 crung gAAAAEIF IKSUUMU				995976

### 打开密码发现是个图片的base64的值随便找个地方转换一下就好了

### http://www.vgot.net/test/image2base64.php

我用的是这个 注意要把前边的 data:xxx去掉

得到密码是asdfghjkl



然后获得一堆二维码 扫了几个发现 只有数值 0 和 1 应该组成起来是个二进制字符串 当然不可能一个个扫 之后利用两种二维码的图片大小不一样 来区分是0还是1 python脚本:

```
import os
for i in range(160):
    a = os.path.getsize(str(i) + '.png')
    if a == 443:
        print(0,end='')
    else:
        print(1,end='')
```

得到结果:

### 然后转成十六进制后再转成字符串就好了

加密或解密字符串	4长度不可以超过1	.0M
666c61677b5152	2636f646531735	5736566756c7d
16进制建立空	→25##16进4	法办注用
10/21/09/12/3/10	コー151 4支 1 0 反正伸引	海王和未
flag(C	sunl	
nag(u	ul)	

得到flag

# 春节三重礼

这是我做过最tmZZ的隐写题目了

💼 春节3	🚔 春节三重礼.zip							
×	◆ 名称	大小	压缩后大小	类型	安			
	(上层目录)							
	💼 pwd.zip *	54.66 KB	30.35 KB	好压 ZIP 压缩文件				
	■第二重大礼,zip *	107.35 KB	107.28 KB	好压 ZIP 压缩文件				

首先 一个压缩包 里边两个有密码的压缩包 没有其他提示 所以先字典跑了一边 然后又去改了一下zip伪加密 发现是**伪加密** 

pwd.zi	p里	是22	个txt
--------	----	-----	------

💼 pwd.zip 🔹											
	×	◆ 名称	大小	压缩后大小	类型	安	修改时间	CRC32	J		
	^	(上层目录)									
		0.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	64FC3E81	I		
		1.txt	68.76 KB	2.40 KB	文本文档		2019-02-08 21:14:06	AE7CFEF6	I		
		2.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	11B9F482	I		
BSS		3.txt	68.76 KB	2.40 KB	文本文档		2019-02-08 21:14:06	F5A405FC	I		
		4.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	18653CB7	I		
		5.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	99923CD2	I		
		6.txt	68.76 KB	2.40 KB	文本文档		2019-02-08 21:14:06	DA7EAE1A	I		
		1.1xt	68.76 KB	2.40 KB	文本文档		2019-02-08 21:14:06	82106E97	I		
		8.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	8BF7CDFC	I		
		9.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	DB2901B1	I		
		10.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	3AAAC194	I		
		11.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	B91EAFDD	I		
		12.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	C30DCC49	I		
		13.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	19C58668	I		
		14.txt	68.76 KB	2.40 KB	文本文档		2019-02-08 21:14:06	F6DC6A3C	I		
		15.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	A718F247	I		
		16.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	3B8D8D7B	I		
		17.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	15EB15C5	I		
		18.txt	68.76 KB	2.40 KB	文本文档		2019-02-08 21:14:06	0EE1A367	ſ		
		19.txt	68.76 KB	2.40 KB	文本文档		2019-02-08 21:14:06	F6EC1783	I		
		20.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	807ACCE7	I		
	$\checkmark$	21.txt	68.76 KB	2.39 KB	文本文档		2019-02-08 21:14:06	73BBD0B0	1 8		
							anarogioouninei/qq		4		

第二重大礼.zip里是一个加密的压缩包

×	◆ 名称										
^	(上层目录)										
	➡最后一重大礼。zip *										

### 大概就是pwd解密出来就是 第二个压缩包的密码了

然后来看txt的内容了





对比了一下前面两个txt 发现 第一个txt有公正 第二个没有 第二个有诚信 第一个却没有

大概可以猜到了是核心价值观编码http://ctf.ssleye.com/cvencode.html 找到每个txt与其他不同的部分 然后解码就行了 开始写脚本~



这里要注意一下 原文本里边本来就带有8个民主 2个 文明 1个自由 所以判断的时候 要先用replace去掉 得到内容为:



得到明文: key2:/s

然后就可以打开另外一个压缩包了







最后一个压缩包里边有个打不开的图片

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0000000	89	50	4E	47	D	A0	0A	1A	0(	00	00	0D	49	48	44	52	\$PNG
0000016	00	00	02	58	0	00	01	<b>P</b> 4	- 04	02	00	00	00	31	04	OF	Х
000032	8B	00	00	00	09	70	48	59	73	00	00	0B	13	00	00	0B	< p
1000048	13	01	00	92	90	18	00	00	00	20	63	48	52	4D	00	00	šœ

改了文件头之后在打开



然后听题干说有ntfs隐写!! 我还特地去试了半天! 发现和NTFS没有屁点关系 祝出题人买菜超级加倍

THE CONTRACT OF THE SUBS

春节三重礼.zip hint:ntfs,在最后一个压缩包里面的文件流里面flag{md5(key1+key2+key3)}

最后发现这个图片要改高度改完高度之后发现key3



key3:c0o1

注意!!!最后一位是**1**不是**I** 我转MD5的时候还试了半天!!!!

最后的最后!!还有key1没有找到!!! 于是我又又又!!!找了好久好久!!!

00111101	00	1.00	~~		~ ~	~~		~~		~~		~~	~~	~~			The second secon
00141120	48	4E	79	5E	6F	07	25	AD	01	00	6C	AD	01	00	0E	00	HNy^o %- 1-
00141136	1C	00	00	00	00	00	00	00	20	00	00	00	90	79	00	00	У
00141152	B5	DA	B6	FE	D6	D8	Β4	F3	C0	Fl	2E	7A	69	70	75	70	µÚ¶þÖØ´óÀñ.zipup
00141168	18	00	01	E4	6F	93	CD	E7	AC	AC	E4	BA	8C	E9	87	8D	äo"Íç⊣⊣ä°Œé‡
00141184	E5	Α4	<b>A</b> 7	E7	Α4	BC	2E	7A	69	70	50	4B	05	06	00	00	大ç¤4.zipPK
00141200	00	00	02	00	02	00	8D	00	00	00	$\mathbf{FD}$	26	02	00	00	00	ý&
00141216	61	32	56	35	4D	54	70	49	51	47	4E	72	4D	33	49	ЗD	a2V5MTpIQGNrM3I
00141232	40	23	24	5E	26	25	21	24	23	20	85	85	2A	26	25	00	@#\$^&%!\$#*&%
00141248	26	40	33	34	25	23	21	40	23	24	5E	26	25	21	24	23	&@34%#!@#\$^&%!\$#
00141264	20	85	85	2A	26	25	00	26	40	33	34	25	23	21	40	23	*&% &@34%#!@#
00141280	24	5E	26	25	21	24	23	20	85	85	2A	26	25	00	26	40	\$^&%!\$#*&% &@
00141296	33	34	25	23	21	64											34%#!d

base64转一下就好了得到的是key1 如果把三个key的值加一起转成md5就是flag了

之后的再做了之后更新