# CTFshow-Misc(部分wp)

# 原创

i\_kei ● 于 2021-01-31 22:19:30 发布 ● 2470 ☆ 收藏 11
 分类专栏: CTFshow 文章标签: <u>信息安全 加密解密 zip base64 密码学</u>
 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u>版权协议,转载请附上原文出处链接和本声明。
 本文链接: <u>https://blog.csdn.net/i\_kei/article/details/113465825</u>

### 版权



#### CTFshow 专栏收录该内容

9篇文章7订阅

订阅专栏

因为太菜了,所以更新比较慢,会慢慢边复现边写wp,flag打码是想让看我博客的小伙伴们能够自己独立复现一遍而不是照抄 flag,有错误的地方还请师傅们不吝指教

#### 目录

杂项签到 misc2 miscx misc50 misc30 stega1 misc3

misc40 misc30

红包题第一弹

## 杂项签到

用ZipCenOp.jar可以解zip压缩包伪加密

```
—(root@kali)-[~/tools/misc]
—# java -jar ZipCenOp.jar r download.zip
```



用010将图中09改为00也可以达到同样效果

启动 💿	dos	nlo	ad.	zipŧ	E 🗃												
▼ 编辑;	句: -	十六进	曲制(	H) "	jž	行脑	本	- 12	回行権	莫板:	ZIF	Tenp	late	e. bt	- D		
	0	1	2	3	4	5	6	7	8	9	A	B	Ç	D	Ē	F	0123456789ABCDEF
00F0h:	C2	EB	C1	CB	2F	<b>A</b> 0	00	20	00	00	00	00	00	01	00	18	ÂĕÁË/
0100h:	00	0B	08	D4	7C	C7	D2	D5	01	0B	08	D4	7C	C7	D2	D5	ô çòõô çòõ
0110h:	01	13	9E	05	74	C7	D2	D5	01	75	70	15	00	01	40	2A	ž.tÇÒÕ.up@*
0120h:	E9	CC	E5	BF	98	E8	AE	B0	E5	AF	86	E7	A0	81	E4	BA	élå;~è®°å tç .ã°
0130h:	86	2F	50	4B	01	02	1F	00	14	00	00	00	08	00	87	B8	†/PK‡,
0140h:	38	50	30	64	D7	04	28	00	00	00	26	00	00	00	13	00	8P0d×.(&
0150h:	45	00	00	00	00	00	00	00	20	00	00	00	42	00	00	00	EB
0160h:	CD	FC	BC	C7	C3	DC	C2	EB	C1	CB	2F	66	6C	61	67	2E	íü¼ÇÃÜÂĕÁË∕flag.
0170h:	74	78	74	A0	00	20	00	00	00	00	00	01	00	18	00	A9	txt©
0180h:	EF	70	8B	C7	D2	D5	01	<b>A</b> 9	EF	70	8B	C7	D2	D5	01	A4	ĭp<ÇÒÕ.©ĭp<ÇÒÕ.¤
0190h:	6D	3D	7B	C7	D2	D5	01	75	70	1D	00	01	93	92	6F	2B	m={ÇÒÕ.up"'o+
01A0h:	E5	BF	98	E8	AE	B0	E5	AF	86	E7	A0	81	E4	BA	86	2F	å;~è®°å⁻tç .ä°t/
01B0h:	66	6C	61	67	2E	74	78	74	50	4B	05	06	00	00	00	00	flag.txtPK
01C0h:	02	00	02	00	FC	00	00	00	BC	00	00	00	00	00			u¥

#### misc2

新建一个虚拟机,然后添加一个软盘,设置成如图所示



然后开启虚拟机即可看到flag

fla g{ctfshow}	
	https://blog.csdn.net/i_kei

miscx



打开misc1.zip,解压出没加密的misc.png



打开misc.png,没发现什么,难道压缩包密码就是2020



试一下果然是,太良心了(不像牛年大吉藏在图片文件头那么狗) 打开word,发现一串音乐符号加密

# 文本加密为音乐符号

אינט אינט אינע אינע אינע אינע אינע אינע אינע אינע
加密 解密 □使用密码
U2FsdGVkX1/eK2855m8HM4cTq8Fquqtm6QDbcUu4F1yQpA==
https://blog.csdn.net/i_kei

Rabbit解密,密钥为2020,解出misc2的压缩包密码

在线Ra	bbit算》	去加密解	密丁县
The second second			

2020			
Rabbit加密	Rabbit解密	清空输入框	复制结果文本
welcome_to_	payhelp		

#### 解出hint.txt

	hint.txt	-	记事本
--	----------	---	-----

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

VmpKMFUxTXhXWGxVV0dob1RUSjRVVII3V2t0aFJscDBZMGhLYTAxWGVIaFZiRkpUWWtaYVZWSnJXbFpOVjJoeVZYcEdZVkpzVG5KVWJHaHB Wa1ZWZDFkV1ZtRmtNRFZYVjJ4c2FWSIVWbFJVVnpWdVRXeFZIV1ZHVGxSaVZrWTBXVIJPYzFWR1pFZFRiVGxYWW01Q1dGcEdXbE5UUjBZMIV XMTBWMWRGU2xkV1ZtUXdVekpGZUZOWWJHaFRSVFZWV1d0YVMxTXhjRVZUYTFwc1ZteHdlRlp0ZERCV01VcFlaRE53V0Zac2NIWIdSekZMV W1zeFdWSnNTbWxXUjNodIZtMXdUMkI5Vm5OaVNGWnBVbXh3YzFac1VrZFNiRIY0WVVkMFZXSIZXbmxWYIRWUFZsWlpIbEZyWkZSaVJrcFFW V3hGYkUwd1VXeE5NRkVsTTBRJTNE

 $\times$ 

|--|

url解码会好看一	·些							
Unicode编码	UTF-8编码	URL编码/解码	Unix时间戳	Ascii/Native编码互转	Hex编码/解码	Html编码/解码		
welcome_to_2020 flag is coming the key is hello 20	20!7							
					utf-8	▼UrlEncode编码	UrlDecode解码 清空 https://blog.csdn.n	结果 et/i_kei

压缩包密码时hello 2020!

解压得到flag.txt

☐ flag.txt - 记事本 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H) flag{gC 0 0u}

## misc50

将图片foremost分离出压缩包和另一张图片 用zsteg一把梭得到base64编码字符串



解码得KEY{Lazy\_Man},提交不对,可能是后面需要用到得密钥



GEZDGNBVGYFA====

base32解密得到flag.zip压缩包密码为123456

得到thienc.txt,将其转换成16进制文本 附上大佬脚本: https://blog.csdn.net/weixin\_45940434/article/details/104292369

```
import re
def read_file(filepath):
   with open(filepath) as fp:
        content=fp.read();
number = read_file('thienc.txt')
result = []
result.append(re.findall(r'.{2}', number))
result = result[0]
strings =''
for i in result:
   strings += z
b= strings.split('0x')
strings=''
for i in b:
   strings +=i
with open('result.txt', 'w') as f:
   f.write(strings)
```

🥦 010 编辑	器 6.0永乐汉化版	ž - D:\	Download	s\ctfs	how	-mis	c\we	elcor	me2	000	0250	01\fla	ag∖≇	版建3	(本)	て档.	txt*				<u></u>	_		×
文件(F) 编辑	i(E) 搜索(S) 社	见图(V)	格式(O)	脚本	(I)	模板	(L)	工具	L(T)	窗[	J(W)	) 켞	s助(H	H)										
- 🕑 -	8 8 9 9	2	% 🗈 🔒	5		P	ÅB	p.	•	3	A	2	Hex	5	¶.		0100 0001		2	*		2	0	
工作区		5	×新建文	本文者	<b>1.</b> t:	xt*																		$\longleftrightarrow \psi$
≥ 打开的文件	ŧ		* 编辑	为: 1	六	井制(	(H) '	jž	行胜	本	* ž	运行相	莫板	Ŧ										^
D:\\fla	ag\新建文本文档	.txt*		Q	1	2	3	4	5	6	7	8	9	A	B	Ç	Ď	Ę	Ę	012	3456	7891	ABCDEF	
🥑 收藏夹文件	=		0000h:	37	7A	BC	AF	27	1C	00	04	4B	BE	4D	1B	00	F3	14	00	7 z3	C'	.K34	Mó	
2 最近的文件	=		0010h:	00	00	00	00	72	00	00	00	00	00	00	00	4D	48	4A	27		.r		MHJ'	
D:\\ft	oi\flag.zip		0020h:	AO	C5	72	61	E1	99	AB	4D	99	27	89	78	8C	D0	2B	AA	.A1	'à♫	Mm '	SXCED+*	
D:\ \w	elcome png		0030h:	1E	FO	7D	6D	39	F5	C5	53	23	EB	CC	52	63	8B	24	3E	.0)	m9őA	S#ë	IRc(\$>	
D:\ \w	elcome2 zin	- 1	0040h:	DF	DA	B2	96	81	F3	11	7B	B2	FE	F1	9A	22	34	EA	E5	BU	0.	{ 2 þ1	is"4êa	
D.1	ercomez.zip		0050h:	FE	FC	73	C1	1A	8F	AD	F7	3A	5B	75	10	CB	B2	CA	82	pus	A	÷:[]	1.E <sup>2</sup> E,	
D:\\d	ownioad.zip		0060h:	D5	FF	4A	B9	50	<b>A</b> 8	92	31	00	C7	21	7E	E7	47	62	D6	OY	1-B .	1.Ç	!∼çGb0	
C:\User	s\\ZIP lemplat	e.bt	0070h:	F4	81	55	CB	98	DF	E5	90	5E	79	2D	77	73	43	19	08	0.t	JE~Bá	loe^Y	-wsC	
D:\Dow	nloads\DS_Stor	e	0080h:	EO	23	64	6C	D4	C7	66	C7	53	61	42	B1	3F	20	8D	33	à#c	lloçf	ÇSal	8±? .3	
D:\\al	bout_fw.png		, 0090h:	4C	EB	28	11	72	2B	C8	DB	53	94	04	43	A9	05	C2	FD	Lë	(.r+E	US"	.CO.Aý	
◎ 文件  2	资源管理器		00A0h:	F5	AF	31	2C	51	C8	18	19	05	A9	5B	66	95	DD	17	E3	0 1	,QE.	0	[f•Y.ā	
<b>U</b> 2011	24 000 10 12 00		00B0h:	E2	33	D9	22	CE	5A	47	OF	DO	F2	2F	4C	4E	D3	91	50	ast	J"IZG	.Đo,	/LNO'P	
检查		8	x 00C0h:	11	EF	CA	79	AS	4E	E1	47	82	23	5C	E9	2B	AO	79	51	.11	y Na	G, #	le+.yQ	
类型	伯		00DOh:	4F	9E	D7	AD	45	B7	CE	65	AS	EE	E1	C6	EE	42	92	FB	02>	-E · I	eSia	AEIB'U	
带符号的字节	-43		00E0h:	5C	BB	CA	D6	49	FF	92	El	72	AB	46	35	10	7C	40	FF	\»E	OIY'	ar«	E5.109	
无符号的字节	213		00F0h:	01	F2	3E	D3	DC	44	88	C3	A2	DB	88	86	E9	4F	OD	2E	.02	OUD	A¢U	teo	
签名短	-43		0100h:	90	15	D3	C2	12	04	BB	B1	94	30	9E	B9	1D	15	3D	78	0e.0	A »	±"0:	21=X	
无符号的短	65493	_	0110h:	5A	CD	5D	DB	55	9A	20	90	EB	5B	6E	43	3D	60	80	42	ZI	UUS	ϑ [1	nC= '€B	
符号的整数	-1186267179		0120h:	C7	71	11	B4	47	2A	DO	6A	B9	0B	79	72	95	7A	38	5A	Çq.	G*Đ	]1.	yr•z8Z	
大符号的整数 然早的 lat64	3108/0011/	7	0130h:	57	4A	E9	7F	BE	87	8E	AO	6D	60	C4	33	59	63	A0	AO	WJé	4.¥‡Z	.m`/	A3Yc .	
无符号的 Int	357210251911	7	0140h:	11	FO	DE	65	A2	1A	62	25	B3	4A	3F	CI	43	07	03	20	.01	e¢.b	2 3 J	?AC	
浮法	-0.0001935953		0150h:	59	F6	D3	63	F9	87	FO	A3	DE	2C	96	96	4E	A1	A2	F1	Yö	cu‡ð	£Þ,	N;¢ñ	
	27502466040	~	0160h:	CD	A1	2A	70	53	69	64	4A	87	6C	AA	OD	A2	AD	B2	EF	I;'	pSid	J\$1	· ¢-21	lee w
2 目初 🔝	受量 🖪 书签	1.4	0170h:	A6	7C	D9	56	56	BB	B5	25	39	11	3F	A3	AA	40	8C	74	1444	VVV»	89.	?£40@Et	

解压密码是刚刚的KEY{Lazy\_Man},得到secenc.txt

文本是base64和base32循环加密

附上Cheyenne大佬的代码,我自己改了一丢丢

```
# @Author: Cheyenne
import base64
import re
f = open('secenc.txt').read().encode('utf-8')
while True:
    if re.match('^[2-7A-Z=]+$', f.decode('utf-8')):
        f = base64.b32decode(f)
    elif re.match('^[0-9a-zA-Z+/=]+$', f.decode('utf-8')):
        f = base64.b64decode(f)
    else:
        print(f.decode('utf-8'))
        break
with open('result.txt', 'w', encoding='utf-8') as file:
    file.write(str(f,encoding='utf-8'))
print("Decryption complete!")
```

#### 🥘 result.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
?
. 1 1 1 1 1 ? 1?!!. ?!!!! 1!? ? 1 ?!! !!! ?
!?!!. ?
11.?
<u>1.?</u>
IIIII I?.?I?III IIII. II. IIIII II.?
?!.?! !!!!. ?!? !!.? ?.?!. ? !.!.! .!. ?!?
<u>  .?        ?.? . ?      .?  ?  . ??.?  .?</u>
?
117.7 1.711 1.1.1 .7
! ?!!.? ? .?!.? !.?
1.?
?!? !? !?!!? ? ?!? <sup>\$2,7DIOG.CSQL</sup> ? <sup>HEI/I_KE</sup>

```
一步步解就好
```

	11.0224
+++++ +++++ [->++ +++++ +++<] >++.+ +++++ .<+++ [-><];	≻ ≜
+++ +++.<	
++++[ ->+++ +<]>+ +++.< +++++ +[-> <]>.< +++[- >++	+<
]>+++ ++.++	
+++++<+++ ++++[ ->< ]> <++++ +++	[-
>++++ {] 💦 🔪	
>++++ +++++ +++~~ <++++ [->++ ++<]> +++	↔.
<+++ +++[-	
><1><++ ++[-> ++++< 1>,+++,<+ ++[-><1 >	
<+ +++[-	1
Text to Ook! Text to short Ook! Ook! to Text	2.004
Text to Brainfuck Brainfuck to Text	ot/i k

++++ +++<]	A
++++ +++++ +++	<++++ [->++ ++<]> +++++ .
+++ +++[-	
<]> <++ ++[-> ++++< ]>.	.++ ++.<+ ++[-><] >
.<+ +++[- 🔪	
++++ <]>++	-> <]> <++
++++ [->++	
++++ <]>++ ++.++ ++ <b>\</b> ++ .+++ ++	++. <++++ +++++ [->
<]>	·
<u> &lt;+++ +++++ +[-&gt;+ ++++A +++&lt;] &gt;++</u>	+++ +++++ ++. < //
Text to Ook! Text to short ok!	Ook! to Text
Taxt to Brainfueld Brainfueld to Tax	<ul> <li>Notificial and a set of the first of the set</li> </ul>

## 得到flag

flag{We	Thow! }
Text to Ook!	Text to short Ook! Ook! to Text

misc30

4 星空	jpg 属性	ŧ	:
常规	安全	详细信息 以前的	版本
属性		值	^
标题	9		
主题 分级		$\stackrel{_{\scriptscriptstyle \wedge}}{_{\scriptscriptstyle \wedge}} \stackrel{_{\scriptscriptstyle \wedge}}{_{\scriptscriptstyle \sim}} \stackrel{_{\scriptscriptstyle \sim}}{_{\scriptscriptstyle \sim}} \stackrel{_{\scriptscriptstyle \sim}}}{_{\scriptscriptstyle \sim}} \stackrel{_{\scriptscriptstyle \sim}}{_{\scriptscriptstyle \sim}} \stackrel{_{\scriptscriptstyle \sim}}}{_{\scriptscriptstyle \sim}} \stackrel{_{\scriptscriptstyle \sim}}}{_{\scriptscriptstyle \sim}} \stackrel{_{\scriptscriptstyle \sim}}{_{\scriptscriptstyle \sim}} \stackrel{_{\scriptscriptstyle \sim}}}{_{\scriptscriptstyle \sim}} \stackrel{_{\scriptscriptstyle \sim}}{_{\scriptscriptstyle \sim}} \stackrel{_{\scriptscriptstyle \sim}}}{_{\scriptscriptstyle \sim}} \stackrel{_{\scriptscriptstyle \sim}}}{_{\scriptscriptstyle \sim}} \stackrel{_{\scriptscriptstyle \sim}}}$	
标记 备注		little stars	https://blog.csdn.net/i_k

再次解压,密码为little stars,解压出一个doc文档 此地无银三百两,全选后将文字颜色设置为黑,发现另一个压缩包密码Hello friend!

解压出一张二维码,扫描得flag



stega1

#### 使用JPHS工具打开,点Seek,密码为空。

JPHS for WIndows - Freeware version BETA te	st rev 0.5	_	
Exit Open jpeg Hide Seek Save jpeg Help About	Save jpeg as	Pass phrase	Options
Input jpeg Director D: \Downloads\ctfshow-misc\f Filename flag.jpg Filesi: 40 Kb WidtH030 pixel He A Enter the pass phrase and confirmation	iaht655 nivel		×
F D Filename	Cancel		
Filesiz Kb This jpeg file has not been modified			
			n.net/i_kei

保存为flag.txt,打开即为flag

🥘 flag										
文件(F)	文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)									
flag{3c	8.				.30fb}					

misc3

# misc3

# 1

密文: zse4rfvsdf 6yjmko0

提示1: 解密后两个字符,小写提示2: 看看自己下面

提交flag{明文}

https://blog.csdn.net/i\_kei

看自己下面可还行

按照提示依次连接键盘字母数字即可



## misc40

#### 有三个文件未加密, 依次查看

🗎 misc40.zip - WinRAR						
文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N)	帮助(H)					
添加         解压到         訓試         血弧         資源	直找 向		日描病毒	注释	自解压格式	
🗈 🖀 misc40.zip - ZIP 压缩文件, 解包大小为	2,182,113 字节					
名称	大小	压缩后大小	类型		修改时间	CRC32
III A second se second second sec			本地磁盘			
■ 一张普通的二维码.png	27,425	24,965	PNG 文件		2020/1/3 17:00	11DA4892
conversion.txt	30	26	文本文档		2020/1/3 16:49	42D89310
svega.wav *	1,823,640	931,797	WAV 文件		2020/1/3 16:44	AC6DF267
svega.mp3	331,018	328,725	MP3 文件		2020/1/3 16:42	F3DFE349

#### 首先打开txt文件

☐ conversion.txt - 记事本 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H) 110001010100011101 1110001010100011101

#### 2>4>8>10

#### 根据提示将字符串由二进制依次转到10进制,这里我们直接转,得到202013

Base Cor	nverter(进制	訓转换)		
From	To 10			
-				
110001010	100011101			202013 ttps://blog.csdn.net/i_kei
用010打开图片,	发现一段brainfuck,	复制出来		
Ŏ 1 2 6780h: BB 1C F5 6700h: 42 60 82	3 4 5 6 7 8 81 B7 F0 C6 00 00	9 A B C D E I 0 00 00 49 45 4E 44 A		
67A0h: E4 A3 A9 67B0h: 2F 2A A1 67C0h: 2B 2B 2B	3F 20 7E A9 DF A E4 3F A3 E0 2A 2 2B 2B 2B 2B 2B 5B 3	9 A5 A9 DF 20 20 20 2 F 20 20 0D 0A 0D 0A 2 E 3E 2B 2B 2B 3E 2B 2B 2 E 3E 2B 2B 3E 2B 2B 2	F 䣩? ~©ß©¥©ß / B /*;ä?£à*/+ B +++++++[>>++>+++	
67D0h: 2B 3E 2B 67E0h: 2B 3E 2B 67F0h: 2B 2B 2B 6800h: 2B 2B 2B	2B         2B         2B         2B         2B         2B         3           2B         3B         3B <td>E 2B 2B</td> <td>B +&gt;+++++&gt;++++&gt;++++ B +&gt;++++++&gt;++++&gt;++++</td> <td></td>	E 2B	B +>+++++>++++>++++ B +>++++++>++++>++++	
6810h: 2B 2B 2B 6820h: 2B 2B 2B 6830h: 2B 2B 2B 6840h: 2B 3E 2B	2B         2B         2B         2B         2B         2B         2I         2I           2B         2B         2B         2B         2B         2B         2B         2I         2I </td <td>B 3E 2B 2B 2B 2B 2B 2B 2 B 2B 2B 2B 3E 2B 2B 2 B 2B 2B 2B 2B 2B 2B 2B 2 B 2B 2B 2B 2B 2B 2B 2B 2 B 2B 2B 2B 2B 2B 2B 2B 2</td> <td>B ++++++++&gt;+++++ B ++++++++++&gt;+++ B ++++++++++</td> <td></td>	B 3E 2B 2B 2B 2B 2B 2B 2 B 2B 2B 2B 3E 2B 2B 2 B 2B 2B 2B 2B 2B 2B 2B 2 B 2B 2B 2B 2B 2B 2B 2B 2 B 2B 2B 2B 2B 2B 2B 2B 2	B ++++++++>+++++ B ++++++++++>+++ B ++++++++++	
6850h: 2B 2B 2B 6860h: 2B 2B 2B 6870h: 2B 3E 2B 6880h: 2B 2B 2B	2B         2B         2B         2B         2B         3           2B         2B <td>E 2B 2B 2B 2B 2B 2B 2B 2B 2 B 2B 2B 2B 3E 2B 2B 2B 2</td> <td>B ++++++&gt;++++++ B ++++++++++++++++++++++</td> <td></td>	E 2B 2B 2B 2B 2B 2B 2B 2B 2 B 2B 2B 2B 3E 2B 2B 2B 2	B ++++++>++++++ B ++++++++++++++++++++++	
6890h: 2B 2B 2B 68A0h: 2B 2B 2B 68B0h: 2B 2B 2B 68C0h: 2B 2B 2B	2B         2B         2B         2B         2B         2B         2I           2B         2B         2B         2B         2B         2B         2B         2I         2I           2B         2B         2B         2B         2B         2B         2B         2I         2I           2B         2B         2B         2B         2B         2B         2B         2I         2I           2B         2B         2B         2B         2B         2B         2B         2I         2I	B 2B 2B 2B 2B 2B 2B 2B 2B 2 B 3E 2B 2B 2B 2B 2B 2B 2 B 2B 2B 2B 2B 2B 2B 2B 2 C 3C	B ++++++++>++++++++++++++++++++++++++++	
68D0h: 3C 3C 3C	3C 3C 3C 3C 3C 2C	D 5D 3E 3E 3E 3E 3E 3	E <<<<<]>>>>>	

#### brainfuck解密



#### 核心价值观编码

社会主义核心价值观: 富强、民主、文明、和谐; 自由、平等、公正、法治; 爱国、敬业、诚信、友善

123456			
	编码	解码	<i>n</i>
和谐民主和谐文明和谐和谐自由和谐平等和谐公正			

https://blog.csdn.net/i kei

#### 使用MP3Stego解密

D:\Tools\Misc\MP3Stego\_1\_1\_18\MP3Stego>Decode.exe -X -P 123456 svega.mp3 MP3StegoEncoder 1.1.17 See README file for copyright info Input file = 'svega.mp3' output file = 'svega.mp3.pcm' Will attempt to extract hidden information. Output: svega.mp3.txt the bit stream file svega.mp3 is a BINARY file HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=3, js=0, c=0, o=0, e=0 alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1 mode=single-ch, sblim=32, jsbd=32, ch=1 [Frame 791]Avg slots/frame = 417.434; b/smp = 2.90; br = 127.839 kbps Decoding of "svega.mp3" is finished The decoded PCM output file name is "svega.mp3.pcm" https://blog.csdn.net/i\_kei

得到svega.mp3.txt,打开得到hint

wega.mp3.txt - 记事本
 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
 hint: 静默之眼
 对了~另一个音乐的密码是abc123哦
 你马上就成功了!

得到压缩包密码abc123,解压得svega.wav

根据提示静默之眼,就是使用SilentEye解密,Sound quality为high,type为AES128,Key为202013 点decode得到flag

😫 Decode mess	age: D:/Downloa	ds/ctfshow-misc/misc40/sve	ega.wav	?	$\times$
	Options	Media's encodir	ng format :	WAVE	• 0
	Sound quality:	99.2188% high		Adva	nced
Deco	ded message	JI			
	naý(	n)			
Fype AES128	Key ******	***	***	· Internet int	- Izzarta
CharSet: UTF8	Encryp	ted data 🗹 Compressed dat	🕹 Cancel	De De	code

# misc30

使用zipcenop解开zip伪加密

```
└──(root⊡kali)-[~/tools/misc]
└─# java -jar zipcenop.jar r aihe.zip
```

#### 解压得aihe.mp3 使用foremost分离出一张图片



很明显劫脚下肯定还隐藏着东西,需要恢复正确得宽高 查看图片属性,看到高度为371,宽度为895,分别将其由10进制转为16进制:0173、037f

#### 🛋 00000000.jpg 属性

属性		值		^
说明	]			
标题				
主题				
分级		$\stackrel{\star}{\leftrightarrow} \stackrel{\star}{\leftrightarrow} \stackrel{\star}{\leftrightarrow}$	$\Rightarrow$ $\Rightarrow$	
标记				
备注				
来源	Į			
作者				
拍摄	日期			
程序	名称			
获取	日期			
版权				
图傷				
图像	ID			
分辨	*	895 x 37	1	
宽度		895 像素		
高度		371 像素		
水平	分辨率	96 dpi		
垂直	分辨率	96 dpi		
位深	度	24		
THE				*
	性和个人	人信息		

 $\times$ 

#### 用010打开图片, ctrl+f搜索0173

	0	1	Ž	3	4	5	6	7	8	9	Α	В	С	D	Е	F	0123456789ABCDEF
0000h:	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	60	<mark>ÿØ</mark> ÿàJFIF`
0010h:	00	60	00	00	FF	DB	00	43	00	08	06	06	07	06	05	08	ÿÛ.C
0020h:	07	07	07	09	09	08	0A	0C	14	0D	0C	0B	0B	0C	19	12	
0030h:	13	0F	14	1D	1A	1F	1E	1D	1A	1C	1C	20	24	2E	27	20	\$.'
0040h:	22	2C	23	1C	1C	28	37	29	2C	30	31	34	34	34	1 F	27	",#(7),01444.'
0050h:	39	ЗD	38	32	3C	2E	33	34	32	FF	DB	00	43	01	09	09	9=82<.342 <mark>ÿÛ.C</mark>
0060h:	09	0C	0B	0C	18	0D	0D	18	32	21	1C	21	32	32	32	32	
0070h:	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	222222222222222222222222222222222222222
0080h:	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	222222222222222222222222222222222222222
0090h:	32	32	32	32	32	32	32	32	32	32	32	32	32	32	FF	C2	222 <u>22</u> 2222222222 <mark>ÿÂ</mark>
00A0h:	00	11	08	01	73	03	7F	03	01	22	00	02	11	01	03	11	<mark></mark> .S <mark></mark> ."
00B0h:	01	FF	C4	00	1B	00	01	00	02	03	01	01	00	00	00	00	<mark>.</mark> ÿÄ
00C0h:	00	00	00	00	00	00	00	01	02	03	04	05	06	07	FF	C4	<u></u> <mark>ÿA</mark>
00D0h:	00	19	01	01	01	01	01	01	01	00	00	00	00	00	00	00	
00E0h:	00	00	00	00	01	02	03	04	05	FF	DA	00	0C	03	01	00	ÿÚ
00F0h:	02	10	03	10	00	00	01	F7	E0	00	00	00	00	00	00	00	ֈ
0100h:	00	00	00	00	00	00	00	00	00	00	00	00	08	9C	39	A0	<mark></mark>
0110h:	28	0A	D9	48	B9	15	26	AC	6D	0A	A5	A5	01	41	01	51	<mark>(.ÜH¹.&amp;¬m.¥¥.A.C</mark>
0120h:	8F	2A	02	80	00	00	00	00	00	00	00	00	00	00	00	00	<mark>.*.€</mark>
0130h:	00	00	00	00	00	00	00	00	00	00	00	08	90	00	00	00	og.csan.net/i_kei.
0140h•	00	00	00	00	29	8F	35	23	20	AA	F3	3A	95	8R	8A	23	) 5# ªó••‹\$#

#### 将高度数值调高,例如和宽一样大

	0	1	2	3	4	5	6	7	Š	9	Α	В	C	D	E	F	0123456789ABCDEF
0000h:	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	60	ÿ <b>Ø</b> ÿàJFIF`
0010h:	00	60	00	00	FF	DB	00	43	00	08	06	06	07	06	05	80	<mark>.`</mark> ÿÛ.⊂
0020h:	07	07	07	09	09	80	0A	0C	14	0D	0C	0B	0B	0C	19	12	
0030h:	13	0F	14	1D	1A	1F	1E	1D	1A	1C	1C	20	24	2E	27	20	\$.*
0040h:	22	2C	23	1C	1C	28	37	29	2C	30	31	34	34	34	1F	27	",#(7),01444.'
0050h:	39	ЗD	38	32	3C	2E	33	34	32	FF	DB	00	43	01	09	09	9=82<.342 <mark>ÿÛ.C</mark>
0060h:	09	0C	0B	0C	18	0D	0D	18	32	21	1C	21	32	32	32	32	
0070h:	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	22222222 <mark>2</mark> 2222222
0080h:	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	222222222222222222222222222222222222222
0090h:	32	32	32	32	32	32	32	32	32	32	32	32	32	32	FF	C2	2222222222222222
00A0h:	00	11	08	03	7F	03	7F	03	01	22	00	02	11	01	03	11	· · · · · · · · · · · · · · · · · · ·
00B0h:	01	FF	C4	00	1B	00	01	00	02	03	01	01	00	00	00	00	.ÿÄ

00C0h:	00	00	00	00	00	00	00	01	02	03	04	05	06	07	FF	C4	ÿÄ
00D0h:	00	19	01	01	01	01	01	01	01	00	00	00	00	00	00	00	• • • • • • • • • • • • • • • • • • •
00E0h:	00	00	00	00	01	02	03	04	05	FF	DA	00	0C	03	01	00	ÿÚ
00F0h:	02	10	03	10	00	00	01	F7	E0	00	00	00	00	00	00	00	ֈ
0100h:	00	00	00	00	00	00	00	00	00	00	00	00	80	9C	39	A0	<mark></mark>
0110h:	28	0A	D9	48	B9	15	26	AC	6D	0A	A5	A5	01	41	01	51	<mark>(.ÙH¹.&amp;¬m.¥¥.A.Q</mark>
0120h:	8F	2A	02	80	00	00	00	00	00	00	00	00	00	00	00	00	<mark>.*.€</mark>
0130h:	00	00	00	00	00	00	00	00	00	00	00	08	90	00	00	00	oalasdninet/i kei
0140h ·	00	00	00	00	29	8F	35	23	20	AA	FR	3A	95	8R	88	23	<u>) 5# ªń••،Š</u> #

#### 保存后打开图片,得到隐藏的猪圈密码



#### 猪圈密码解密

#### — 猪圈密码

Pigpen Cipher

_	ш	L				٦	П	Г
Ŀ	Ŀ	Ŀ	Ð		E	Э	П	F
$\sim$	>	<		~	>	¢		:

	()÷	÷.	. 🖪	:	=	C	$\mathbf{X}$	1
*	_	٩	<ul> <li></li> </ul>	3	I	194 1	%	+

明文: welldone

https://blog.csdn.net/i\_kei

解出来well done(有空格)

红包题第一弹