

# 实验吧隐写术部分writeup (1)

原创

[saltyfishy](#) 于 2017-09-10 19:07:27 发布 1145 收藏 1

文章标签: [ctf](#)

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/saltyfish\\_yuch/article/details/77923988](https://blog.csdn.net/saltyfish_yuch/article/details/77923988)

版权

题目: Spamcarver

Spamcarver 分值: 30

来源: PicoCTF 2013 难度: 难 参与人数: 704人 Get Flag: 181人 答题人数: 195人 解题通过率: 93%

开盖有惊喜  
格式: flag(xxx)

解题链接: <http://ctf5.shiyabar.com/stega/spamcarver/spamcarver.jpg> 通过

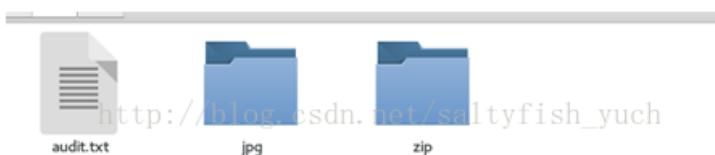
提交

下载得到图片直接丢进kali里binwalk, 发现压缩文件尾

```
root@kali:~# cd Desktop
root@kali:~/Desktop# binwalk gai.jpg
DECIMAL      HEXADECEMAL  DESCRIPTION
-----
0            0x0          JPEG image data, JFIF standard 1.01
64001       0xFA01       End of Zip archive

root@kali:~/Desktop# foremost -i gai.jpg -o gai
Processing: gai.jpg
|foundat=
|UT
*
ot@kali:~/Desktop#
```

于是foremost打开zip即为flag



题目: NAVSAT

NAVSAT 分值: 10

来源: PicoCTF 2013 难度: 易 参与人数: 402人 Get Flag: 178人 答题人数: 187人 解题通过率: 95%

继续补补又三年  
格式: flag(box)

解题链接: <http://ctf5.shiyanshi.com/stega/navsat/recovery.zip> 通过 saltyfish\_yuch

提交

压缩包下载, 无法解压, 于是丢进winhex发现key, 这里因为压缩包里还有一张地图, 根据key还以为要在地图找信息, 没想到就是flag

offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
0	3F	3F	03	04	0A	00	00	00	00	00	22	79	8E	42	76	7D	2E	EF	1B	00	00	00	1B	00	00	00	0F	00	1C	00	4D	61	77
32	67	37	2D	42	57	2F	48	65	79	2E	74	78	74	55	54	09	00	03	D0	FE	4A	51	0B	FF	6A	51	75	78	0B	00	01	04	
64	8F	03	00	04	8F	03	00	00	00	4B	65	78	1A	29	8E	65	78	74	20	73	74	4E	70	20	54	61	75	20	42	69	64	0	
96	61	6E	69	0A	50	4B	03	04	14	00	00	00	08	00	27	B6	47	32	1B	A6	C3	9C	E4	52	04	00	0C	36	05	00	14	00	
128	1C	00	4D	61	67	37	2D	42	57	2F	43	68	61	72	74	2D	31	35	2E	70	64	66	55	54	09	00	03	BA	76	08	42	AF	
160	FE	6A	51	75	78	0B	00	01	04	8F	03	00	00	04	8E	65	00	00	9C	97	4D	94	25	51	D3	24	5A	B6	ED	1B	B6	BA	
192	6C	2B	B6	6D	74	97	A8	5A	6C	2B	B6	6D	74	97	A8	5A	33	75	FD	8C	98	89	71	D7	9C	83	56	A8	CC	71	10	8E	
224	22	77	44	8C	78	9E	8E	8C	D8	64	8A	A2	E2	F4	0C	0C	20	30	6C	44	4C	44	0E	6E	D6	44	7C	7C	30	8C	B2	66	
256	F6	16	A6	94	44	EC	FF	44	CA	30	8C	E2	56	B6	A6	66	CE	44	8C	E2	B6	46	A6	66	A2	66	26	0E	A6	66	30	02	
288	02	30	2E	AE	CE	66	46	76	30	9E	1B	C9	49	72	0E	4B	4C	48	1A	DC	A7	1A	6F	47	78	2C	9E	B4	B1	82	7B	AA	
320	54	78	34	5C	68	C7	10	78	EA	9D	32	1E	E4	19	AE	AD	E5	40	3F	39	E3	12	D6	A5	31	34	45	34	CA	28	D3	5D	

题目: In Hex, No One Can Hear You Complain

In Hex, No One Can Hear You Complain 分值: 10

来源: PicoCTF 2013 难度: 易 参与人数: 346人 Get Flag: 216人 答题人数: 221人 解题通过率: 98%

修改试试看?  
格式: flag(box)

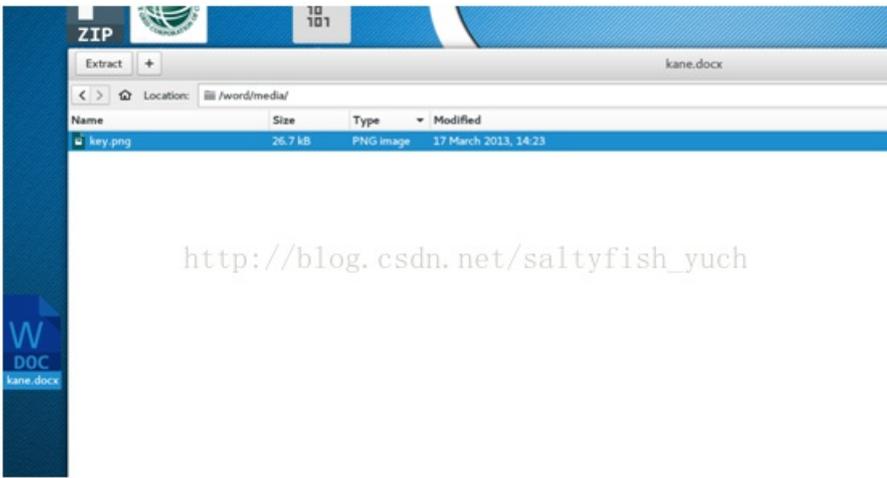
解题链接: <http://ctf5.shiyanshi.com/stega/in-hex/kane.docx> 通过 saltyfish\_yuch

提交

直接丢进winhex, 在末尾发现png

offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
26848	0E	5C	0B	02	51	97	29	ED	FA	B7	C9	97	15	8F	05	6A	AC	A4	35	4A	D4	61	6A	B1	28	83	2C	CC	A5	5A	9D	4F	
26880	20	CA	48	42	24	1D	FA	8C	00	AD	26	64	37	C1	2D	AB	F3	4A	2E	1A	4D	FD	52	16	45	5A	1B	87	79	94	59	F5	
26912	8B	D1	09	4A	A3	A3	AD	C9	80	8E	DE	FE	62	CA	52	42	59	3A	0A	5C	62	D9	0C	8D	07	B4	DE	F7	2A	32	A6	0	
26944	41	5B	79	70	58	72	2B	50	04	79	0C	66	3C	75	63	99	EC	CA	FB	A3	52	90	79	AF	11	E5	14	FD	E3	BF	99	F7	
26976	0C	52	72	13	02	D9	11	71	68	38	92	91	A4	46	95	72	2B	01	72	89	42	E6	3C	76	11	09	EF	4C	A6	FB	A5	DE	
27008	93	0E	78	8A	25	07	45	E7	E5	B9	00	58	01	F5	A8	D9	1E	1F	76	FF	07	6E	DA	51	82	C6	1D	59	34	0D	69	4F	
27040	A4	B3	6A	B4	DE	13	97	AF	87	33	D9	55	F2	8F	31	1C	B8	5F	BF	12	45	56	1B	73	49	0A	6C	ED	AC	60	7C	04	
27072	59	59	2E	02	79	00	46	D5	8F	08	F9	39	2C	7B	9A	03	61	FC	4B	EE	0B	FB	18	F8	98	3D	C5	BF	22	EA	A9	8B	
27104	29	25	A4	C1	82	05	3C	58	0E	5C	DC	D0	5E	71	C4	8E	8E	CA	E6	82	0A	1A	1A	3D	10	63	FF	13	31	F6	3F		
27136	17	E3	08	70	10	5F	94	6D	91	7B	24	AF	37	4D	78	90	85	7C	0D	35	82	89	D9	53	44	36	A3	3C	08	4D	BF		
27168	0D	5A	27	4E	B6	09	64	D7	90	31	24	FD	22	92	48	5A	8C	4D	D3	E2	18	B4	75	EF	3B	17	E8	DE	1D	36	P9	F1	
27200	4E	75	1E	1E	A7	59	3A	77	CF	56	28	4D	77	7B	27	35	5D	5D	A6	FC	E8	35	CB	C7	74	96	14	7B	AD	1E	AE	89	
27232	8C	71	7D	3E	2F	BD	A0	05	2F	27	5A	7F	D1	90	3F	50	4B	01	02	14	03	14	03	00	00	00	00	AA	91	71	42	3F	
27264	7D	7C	FF	33	1F	01	00	00	08	03	00	00	13	00	00	00	00	00	00	00	00	00	00	20	80	A4	81	00	00	00	58	43	
27296	4F	4E	74	65	4E	74	5F	54	79	70	45	73	5D	2E	78	6D	6C	50	4B	01	02	14	03	14	03	00	00	08	00	AA	91	71	
27328	42	E8	D0	01	23	D9	00	00	00	3D	02	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	5F	
27360	72	65	6C	73	2F	2E	72	65	6C	73	50	4B	01	02	14	03	14	03	00	00	08	00	AA	91	71	42	81	56	51	DC	DA	00	
27392	00	00	64	01	00	00	10	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	
27424	2F	41	70	70	2E	78	4D	6C	50	4B	01	02	14	03	14	03	00	00	00	00	AA	91	71	42	09	54	C9	AC	1A	01	00	00	
27456	F8	01	00	00	01	00	00	00	00	00	00	00	00	00	00	20	80	A4	81	5A	03	00	00	64	4F	63	50	72	6F	70	73	2F	63
27488	4F	72	65	2E	78	6D	6C	50	4B	01	02	14	03	14	03	00	00	00	00	AA	91	71	42	3F	15	B9	44	80	01	00	00	AF	
27520	0C	00	00	1C	00	00	00	00	00	00	00	00	00	20	80	A4	81	A3	04	00	00	73	4F	72	44	2F	5F	72	65	6C	73	2F	
27552	44	4F	63	75	6D	65	4E	74	2E	78	4D	6C	2E	72	65	6C	73	50	4B	01	02	14	03	14	03	00	00	08	00	AA	91	71	
27584	42	E8	D0	01	23	D9	00	00	00	3D	02	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
27616	4F	72	65	2F	4D	6F	63	75	6D	65	4E	74	2E	78	6D	6C	50	4B	01	02	14	03	14	03	00	00	08	00	AA	91	71	42	
27648	03	83	E3	21	D9	00	00	00	53	02	00	00	12	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	77	4F
27680	72	48	2F	66	4F	4E	74	54	61	62	6C	65	2E	78	6D	6C	50	4B	01	02	14	03	14	03	00	00	08	00	E7	72	71	42	
27712	42	3D	B0	35	2C	5A	00	00	5E	68	00	00	12	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	77	6F
27744	72	44	2F	6D	65	64	49	61	2F	6B	65	79	2E	70	6E	67	50	4B	01	02	14	03	14	03	00	00	08	00	AA	91	71	42	
27776	8E	83	3D	4B	42	02	00	00	07	08	00	00	0F	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	77	6F
27808	72	44	2F	73	74	79	6C	65	73	2E	78	6D	6C	50	4B	05	06	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
27840	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

直接在kali中打开, 打开图片即为flag



题目：越光宝盒

越光宝盒 分值：10

来源：墨流云 难度：易 参与人数：603人 Get Flag：206人 答题人数：215人 解题通过率：96%

corrupt png

解题链接：<http://ctf5.shiyanbar.com/stega/corrupt/timgK.png> 通过

提交

[http://blog.csdn.net/saltyfish\\_yuch](http://blog.csdn.net/saltyfish_yuch)

将图片下载下来直接丢进虚拟机显示文件残缺

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~# cd Desktop
root@kali:~/Desktop# file timgK.png
timgK.png: data
root@kali:~/Desktop#
_1.rar.extracted
http://blog.csdn.net/saltyfish_yuch
```

用winhex打开图片判断为文件头残缺，于是百度png文件头

## PNG的文件结构

对于一个PNG文件来说，其文件头总是由位固定的字节来描述的：

十进制数	137 80 78 71 13 10 26 10
十六进制数	89 50 4E 47 0D 0A 1A 0A

[http://blog.csdn.net/saltyfish\\_yuch](http://blog.csdn.net/saltyfish_yuch)

将正确的文件头写入

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F	ANSI ASCII
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	00	00	01	DD	00	00	01	2C	08	02	00	00	00	09	91	FE	%PNG IHDR Ÿ ,`p
00000020	85	00	00	00	09	70	48	59	73	00	00	0B	13	00	00	0B	13	01	00	9A	9C	18	00	00	00	20	63	48	52	4D	00	00	... pHYs Šœ , cHRM
00000040	7A	25	00	00	80	83	00	00	F9	FF	00	00	80	E9	00	00	75	30	00	00	EA	60	00	00	3A	98	00	00	17	6F	92	5F	z% €f ùÿ €é u0 é` :~ o'_
00000060	C5	46	00	01	20	3F	49	44	41	54	78	DA	EC	FD	69	8C	5C	59	76	26	08	9E	BB	BC	D5	76	33	DF	DD	E9	4E	D2	ÃF ?ILATxúÿiG\Yv& Z»%Óv3BýéNÖ
00000080	C9	E0	12	64	EC	91	91	A9	54	6E	92	52	29	69	32	55	92	5A	B5	09	55	25	34	66	A9	5F	8D	41	0F	30	03	0C	Èà `dì`'eTn'R)i2U'Zp U%4f€_ A 0
000000A0	06	98	6E	60	A6	67	06	E8	59	7A	06	EA	FA	31	5D	98	99	42	77	55	03	3D	9B	AA	A0	91	52	4A	49	A5	DC	33	~n`!α èÿz éúì\~BwU =>* `RJIYÜ3

保存，打开即为flag

题目：Dark Star

Dark Star 分值：20

来源：PicoCTF 2013

难度：中

参与人数：488人

Get Flag：132人

答题人数：149人

解题通过率：89%

Sure are a lot of stars out there... but there's a lot of empty space for things to hide in, too.

解题链接：<http://ctf5.shiyanbar.com/stega/dark-star/darkstar.img> **通过**

提交

[http://blog.csdn.net/saltyfish\\_yuch](http://blog.csdn.net/saltyfish_yuch)

文件下载之后发现无法打开，于是丢入虚拟机binwalk一下发现图片

```
root@kali:~/Desktop# binwalk darkstar.img
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
146752      0x300400    PNG image, 192 x 56, 8-bit/color RGBA, non-interlaced
146809      0x300439    Zlib compressed data, default compression
1719616     0x480400    JPEG image data, JFIF standard 1.01
1721664     0x480C00    JPEG image data, JFIF standard 1.01
1729856     0x482C00    JPEG image data, JFIF standard 1.01
1730238     0x482D7E    Copyright string: "Copyright (c) 1998 Hewlett-Packard Company"
1738048     0x484C00    JPEG image data, JFIF standard 1.01
1738346     0x484D2A    Copyright string: "Copyright 1999 Adobe Systems Incorporated"
1740040     0x4853C8    JPEG image data, JFIF standard 1.02
1743332     0x4860A4    Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"<rdf:Description rdf:about="" xmlns:tiff="http://ns.adobe.com/tiff/1.0/" xmlns:xif="http://www.xif.com/1.0/">

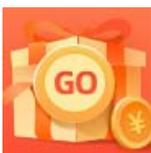
```

于是分离出图片

```
root@kali:~/Desktop# foremost darkstar.img -o darkstar
Processing: darkstar.img
|*| http://blog.csdn.net/saltyfish_yuch
```

分离出的图片即可找到flag

持续施工中。。。



[创作打卡挑战赛](#) >  
[赢取流量/现金/CSDN周边激励大奖](#)