

ctfshow-Misc入门

原创

[H3rmesk1t](#) 于 2021-07-29 03:36:00 发布 1159 收藏 10

分类专栏: [Misc](#) 文章标签: [Misc](#) [ctfshow](#)

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/LYJ20010728/article/details/119193793>

版权



[Misc](#) 专栏收录该内容

10 篇文章 1 订阅

订阅专栏

ctfshow-Misc入门

写在前面

图片篇(基础操作)

[misc1](#)

[misc2](#)

[misc3](#)

[misc4](#)

图片篇(信息附加)

[misc5](#)

[misc6](#)

[misc7](#)

[misc8](#)

[misc9](#)

zsteg (补充)

[misc10](#)

[misc11](#)

[misc12](#)

[misc13](#)

[misc14](#)

[misc15](#)

[misc16](#)

[misc17](#)

[misc18](#)

[misc19](#)

[misc20](#)

[misc21](#)

misc22

misc23

misc41

图片篇(文件结构)

misc24

misc25

misc26

misc27

misc28

misc29

misc30

misc31

misc32

misc33

misc34

misc35

misc36

misc37

misc38

misc39

misc40

misc42

misc43

misc44

misc45

misc46

misc47

misc48

misc49

图片篇(颜色通道)

misc50

写在前面

后续提取图片中的flag均为脚本提取，部分flag提取出错需要人工再次核验哈~，flag提取演示

图片篇(基础操作)

misc1

flag在下载的图片上

ctfshow{22f1fb91fc4169f1c9411ce632a0ed8d}

<https://blog.csdn.net/LYJ20010728>

```
Cmder
C:\Users\95235
λ python
Python 3.8.8 (default, Apr 13 2021, 15:08:03) [MSC v.1916 64 bit (AMD64)] :: Anaconda, Inc. on win32

Warning:
This Python interpreter is in a conda environment, but the environment has
not been activated. Libraries may fail to load. To activate this environment
please see https://conda.io/activation

Type "help", "copyright", "credits" or "license" for more information.
>>> import pytesseract
>>> from PIL import Image
>>> img = Image.open(r'C:\Users\95235\Downloads\misc1\misc1.png')
>>> text = pytesseract.image_to_string(img)
>>> print(text)
ctfshow{22f1fb91fc4169f1c9411ce632a0ed8d}
^
>>> quit()
```

<https://blog.csdn.net/LYJ20010728>

misc2

将后缀名改为 `.png` 即可在图片上看到flag

```
Cmder
C:\Users\95235
λ python
Python 3.8.8 (default, Apr 13 2021, 15:08:03) [MSC v.1916 64 bit (AMD64)] :: Anaconda, Inc. on win32

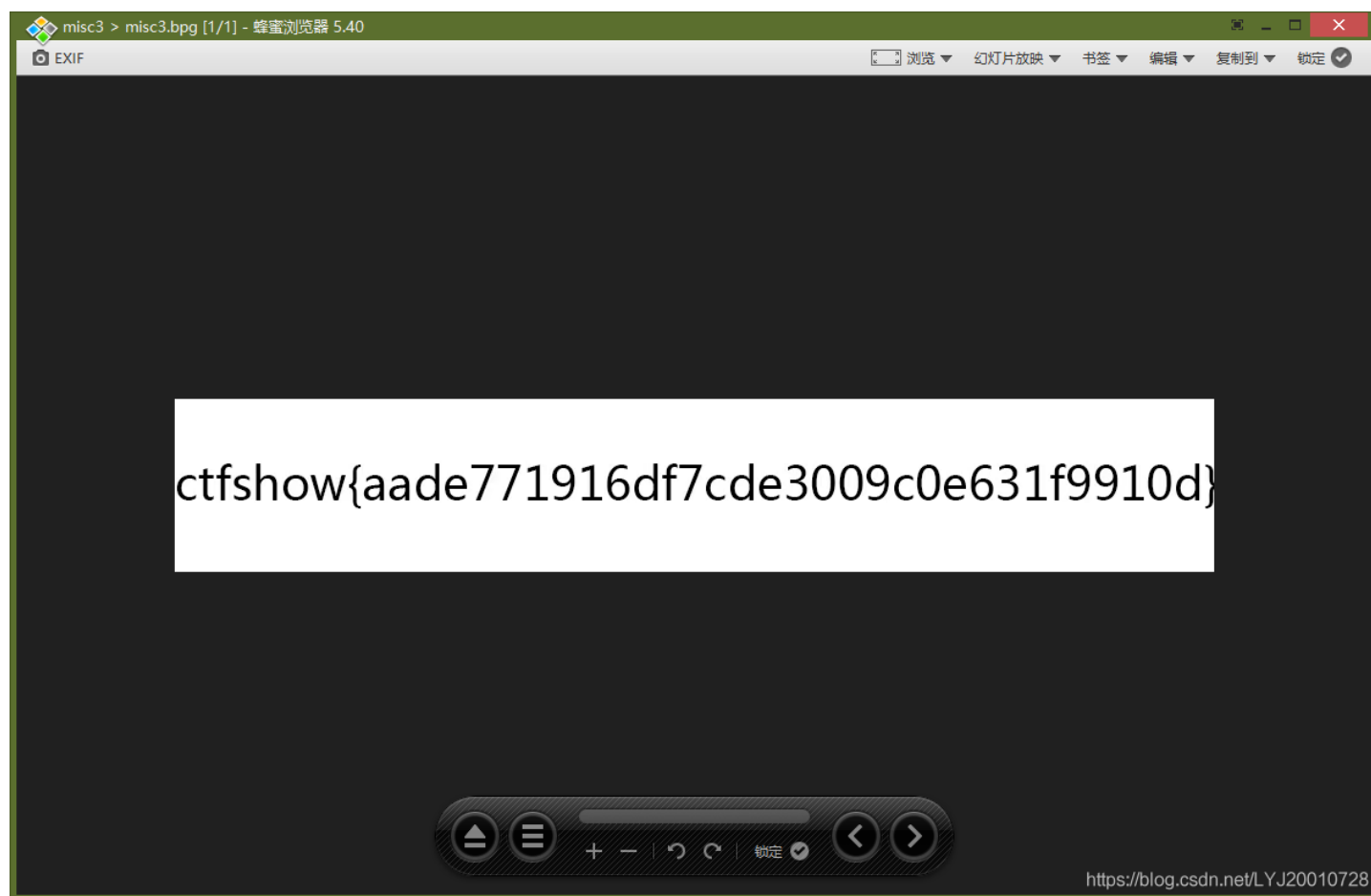
Warning:
This Python interpreter is in a conda environment, but the environment has
not been activated. Libraries may fail to load. To activate this environment
please see https://conda.io/activation

Type "help", "copyright", "credits" or "license" for more information.
>>> import pytesseract
>>> from PIL import Image
>>> img = Image.open(r'C:\Users\95235\Downloads\misc2\misc2.png')
>>> text = pytesseract.image_to_string(img)
>>> print(text)
ctfshow{6f66202f21ad22a2a19520cdd3f69e7b}
^
>>> quit()
```

<https://blog.csdn.net/LYJ20010728>

misc3

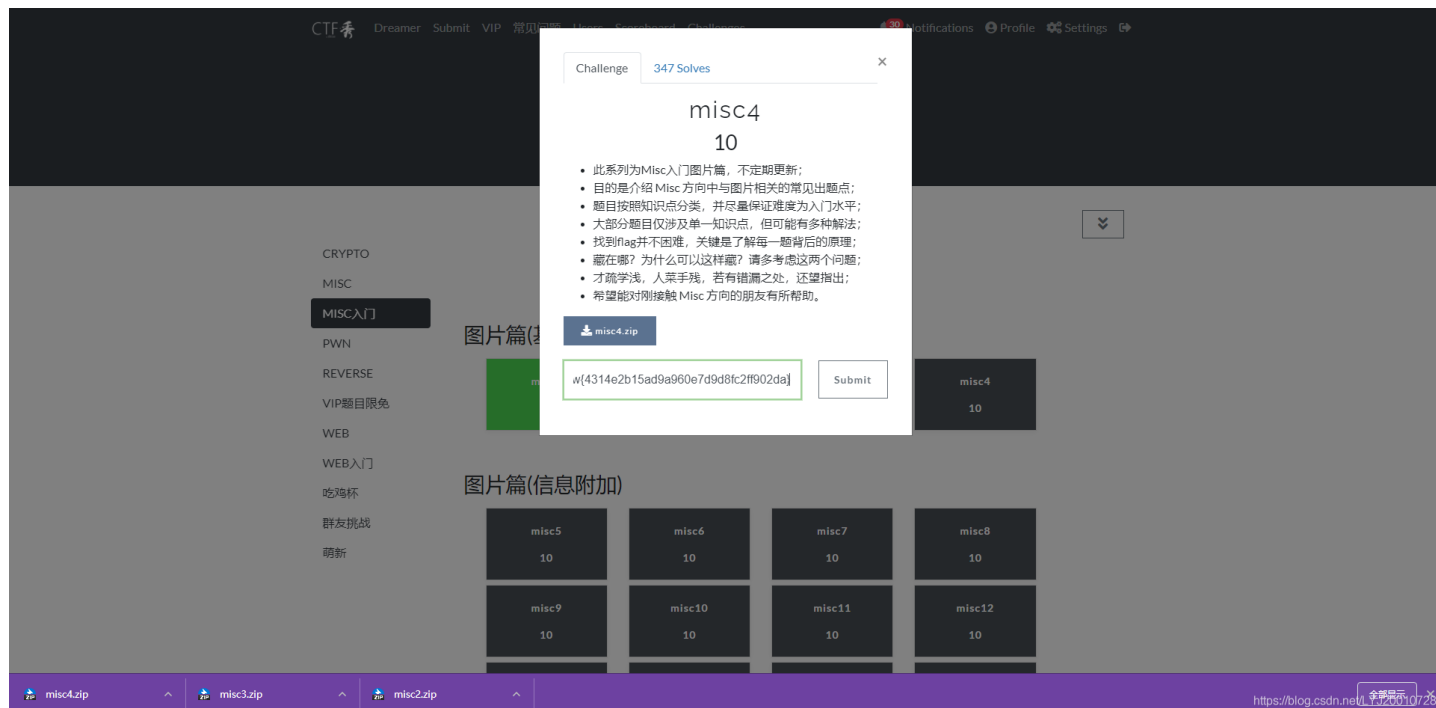
推荐一款图片浏览器 [Honeyview](#)，直接可以查看bpg格式的图片



misc4

用 HxD 依次查看文件头，将后缀名依次改为 [.png](#)、[.jpg](#)、[.bmp](#)、[.gif](#)、[.tif](#)、[.webp](#)，将内容拼接起来即可得到flag

名称	修改日期	类型	大小
1.png	2021/2/4 17:25	PNG 文件	6 KB
2.jpg	2021/2/4 17:25	JPG 文件	19 KB
3.bmp	2021/2/4 17:26	BMP 文件	396 KB
4.gif	2021/2/4 17:27	GIF 文件	2 KB
5.tif	2021/2/4 17:28	TIF 文件	418 KB
6.webp	2021/3/25 0:49	Image (webp) File	1 KB



图片篇(信息附加)

misc5

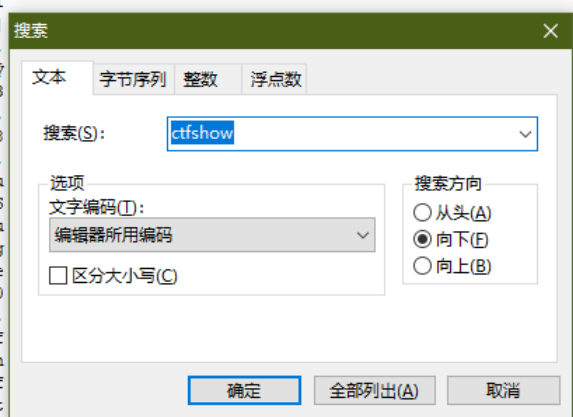
用 **HxD** 打开，拖到尾部即可发现flag

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	对应文本
00000D30	55	39	40	58	D7	5D	32	3D	7F	79	BE	3D	9D	AC	AC	D2	U9@X]2=.y%=-.-0
00000D40	9D	40	EB	09	84	D0	19	E9	8C	A1	B9	59	FC	D2	42	F3	.@e.,.D.e@i;^YüÖBó
00000D50	E9	A0	47	30	04	DE	43	3A	91	48	A3	D0	95	06	BD	D3	é G0.ÉC: 'H&D*.éÓ
00000D60	D2	D5	C1	6F	C1	FC	58	DD	B4	2C	5C	FF	92	EF	C7	E1	ÔÔÁoÁúXÝ',\y' iÇá
00000D70	AE	67	A5	6B	20	16	02	21	74	4A	36	BD	7B	CD	BA	62	0g¥k ...!tJ6s{Í'ó
00000D80	00	FB	F5	52	D8	FC	E4	7A	DD	A9	A9	E5	15	BF	52	18	.úóR0üázY@0á.¿R.
00000D90	4C	03	84	A9	45	7B	E1	A9	AC	88	99	45	A1	AB	94	9D	L.,@E{á@-™Ej;«".
00000DA0	00	00	9A	2B	94	1A	68	4A	69	02	80	B6	70	85	10	00	..š+ ".hJl.€Pm...
00000DB0	68	2E	2D	FA	FF	8A	BB	15	9E	0A	E1	0B	83	00	6D	E1	h.-úýŠ».ž.á.f.má
00000DC0	0A	21	00	F0	46	F3	70	7D	92	9B	5C	A4	C2	15	41	80	..!ôFóp)' >\kÁ.A€
00000DD0	B6	12	08	01	00	00	22	E5	96	51	00	00	80	48	09	84	Ÿ....."á-Q..€H..
00000DE0	00	00	00	91	12	08	01	00	00	22	25	10	02	00	00	44"%.D
00000DF0	4A	20	04	00	00	88	94	40	08	00	00	10	29	81	10	00	J ...^"@.....)
00000E00	00	20	52	02	21	00	00	40	A4	04	42	00	00	80	48	09	. R.!..@k.B..€H.
00000E10	84	00	00	91	12	08	01	00	00	22	25	10	02	00	00	00"%.D
00000E20	44	4A	20	04	00	00	88	94	40	08	00	00	10	29	81	10	DJ ...^"@.....)
00000E30	00	00	20	52	02	21	00	00	40	A4	04	42	00	00	80	48	. R.!..@k.B..€H.
00000E40	09	84	00	00	91	12	08	01	00	00	22	25	10	02	00	00"%.D
00000E50	00	44	4A	20	04	00	00	88	94	40	08	00	00	10	29	81	.DJ ...^"@.....)
00000E60	10	00	00	20	52	02	21	00	00	40	A4	04	42	00	00	80	. R.!..@k.B..€H.
00000E70	48	09	84	00	00	91	12	08	01	00	00	22	25	10	02	00	H....."%.D
00000E80	00	00	44	4A	20	04	00	00	88	94	40	08	00	00	10	29	..DJ ...^"@.....)
00000E90	81	10	00	00	20	52	02	21	00	00	40	A4	04	42	00	00 R.!..@k.B..
00000EA0	80	48	09	84	00	00	91	12	08	01	00	00	22	25	10	00	€H....."%.D
00000EB0	02	00	00	44	4A	20	04	00	00	88	94	40	08	00	00	10	...DJ ...^"@.....)
00000EC0	29	81	10	00	00	20	52	02	21	00	00	40	A4	04	42	00).... R.!..@k.B..
00000ED0	00	80	48	09	84	00	00	91	12	08	01	00	00	22	25	10	.€H....."%.D
00000EE0	10	02	00	00	44	4A	20	04	00	00	88	94	40	08	00	00	...DJ ...^"@.....)
00000EF0	10	29	81	10	00	00	20	52	02	21	00	00	40	A4	04	42	.).... R.!..@k.B..
00000F00	00	00	80	48	09	84	00	00	91	12	08	01	00	00	22	25	..€H....."%.D
00000F10	25	10	02	00	00	44	4A	20	04	00	00	88	94	40	08	00	%....DJ ...^"@.....)
00000F20	33	3E	20	BA	99	89	97	04	00	00	00	00	49	45	4E	44	3> °™%-.....IEND
00000F30	AE	42	60	82	63	74	66	73	68	6F	77	7B	32	61	34	37	@B`,ctfshow{2a47
00000F40	36	62	34	30	31	31	38	30	35	66	31	61	38	65	34	62	6b4011805f1a8e4b
00000F50	39	30	36	63	38	66	38	34	30	38	33	65	7D	90	6c	8f	84083e}

misc6

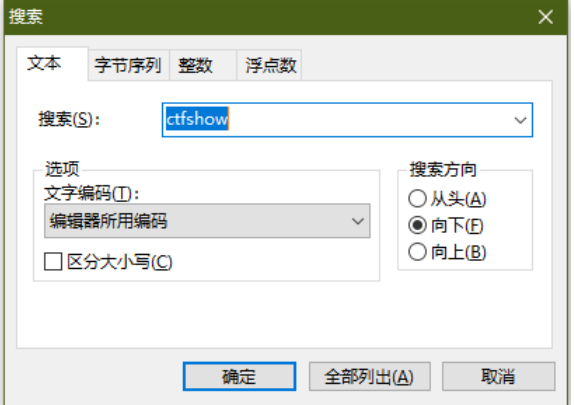
用 HxD 打开，搜索关键词 **ctfshow** 即可发现flag

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	对应文本
00000560	FE	72	32	49	29	0E	46	26	2E	4D	07	1F	26	9A	EE	A0	px2I).F&.M..&š1
00000570	C4	D5	63	43	99	ED	32	DF	63	C1	6F	B5	12	BA	EB	AA	ÀÖcC™i2BcÁoµ.°é*
00000580	B6	D5	53	43	2B	60	0D	63	1A	00	6B	5A	04	35	AD	68	ŸÖSC+`.c..kZ.5.h
00000590	FA	2D	6A	92	49	29	03	30	70	AB	CA	7E	65	78	F5	33	ú-j'I).0p«Ê-exô3
000005A0	2A	D1	B6	CC	86	B1	A2	C7	0F	6F	B5	F6	81	BD	DF	41	*ŃŸİ+±oÇ.ouó.¼&A
000005B0	9F	E6	29	DF	45	59	15	3A	9B	9B	BA	B7	44	89	23	83	Ÿæ)æEY.:>>°D#f
000005C0	B8	7B	9B	0E	44	49	25	35	A8	E9	BD	3B	1A	DF	5B	1F	,{.DI%5"é%:.&[.
000005D0	16	9A	6D	D8	2A	F5	2B	AD	AD	77	A6	D0	D6	B2	AD	EC	.šm0*ô+..w DÓ°.i
000005E0	68	77	A4	C6	D7	5F	E8	FF	00	E0	D5	94	92	49	4C	5D	hwæE×_èý.àÓ''IL]
000005F0	5D	6E	73	5E	6E	67	39	84	96	38	89	2D	24	6D	3B	7F]ns^æ+9,,-8%-šm;.:
00000600	77	DA	54	92	49	25	29	24	92	49	4A	49	24	92	53	FF	wÚ'I(š)š'IJİš'Sý
00000610	D9	FF	ED	0D	F2	50	68	6F	74	6F	73	68	6F	70	20	33	Ûyi.òPhotoshop 3
00000620	2E	30	00	38	42	49	4D	04	25	00	00	00	00	00	10	00	.0.8BIM.š.....
00000630	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	388
00000640	42	49	4D	04	3A	00	00	00	00	00	D7	00	00	00	10	00	BIM.1.....*
00000650	00	00	01	00	00	00	00	00	0B	70	72	69	6E	74	4F	75printOu
00000660	74	70	75	74	00	00	05	00	00	00	00	00	50	73	74	53	tput.....PstS
00000670	62	6F	6F	6C	01	00	00	00	00	49	6E	74	65	65	6E	75	bool.....Inteenu
00000680	6D	00	00	00	00	49	6E	74	65	00	00	00	00	49	6D	67	m....Inte....Img
00000690	20	00	00	00	0F	63	74	66	73	68	6F	77	7B	64	35	65	...ctfshow}{d5e
000006A0	39	33	37	61	65	66	62	30	39	31	64	33	38	65	37	30	937aefb091d38e70
000006B0	64	39	32	37	62	38	30	65	31	65	32	65	61	7D	00	01	d927b80e1e2ea}..
000006C0	00	00	00	00	0F	70	72	69	6E	74	50	72	6F	6F	66	66printProof
000006D0	53	65	74	75	70	4F	62	6A	63	00	00	00	05	68	21	68	SetupObjc....h!h
000006E0	37	8B	BE	7F	6E	00	00	00	00	0A	70	72	6F	6F	66	66	7<%..n.....proof
000006F0	53	65	74	75	70	00	00	00	01	00	00	00	00	42	6C	74	Setup.....Blt
00000700	6E	65	6E	75	6D	00	00	00	0C	62	75	69	6C	74	69	6E	nenum....builtin
00000710	50	72	6F	6F	66	00	00	00	09	70	72	6F	6F	66	43	4D	Proof....proofCM
00000720	59	4B	00	38	42	49	4D	04	3B	00	00	00	00	02	2D	00	YK.8BIM.;.....-
00000730	00	00	10	00	00	00	01	00	00	00	00	00	12	70	72	69pri
00000740	6E	74	4F	75	74	70	75	74	4F	70	74	69	6F	6E	73	00	ntOutputOptions.
00000750	00	00	17	00	00	00	00	43	70	74	6E	62	6F	6F	6C	00Cptnbool.
00000760	00	00	00	00	43	6C	62	72	62	6F	6F	6C	00	00	00	00Clbrbool....
00000770	00	52	67	73	4D	62	6F	6F	6C	00	00	00	00	43	72	00	.RgsMbool.....Cr
00000780	6E	43	62	6F	6F	6C	00	00	00	00	00	43	6E	74	43	62	nCbool.....CntCb
00000790	6F	6F	6C	00	00	00	00	00	4C	62	6C	73	62	6F	6F	6C	ool.....Lblsbool
000007A0	00	00	00	00	00	4E	67	74	76	62	6F	6F	6C	00	00	00Ngtvbool...
000007B0	00	00	45	6D	6C	44	62	6F	6F	6C	00	00	00	00	00	49	..Em1Dbool.....I



用 HxD 打开，搜索关键词 `ctfshow` 即可发现flag

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	对应文本
00007D20	55	D8	AB	B1	57	62	AE	C5	5D	8A	BB	15	76	2A	EC	55	U0«±Wb@Á]Š».v*iU
00007D30	D8	AB	B1	57	62	AE	C5	5D	8A	BB	15	76	2A	EC	55	D8	0«±Wb@Á]Š».v*iU0
00007D40	AB	B1	57	62	AE	C5	5D	8A	BB	15	76	2A	EC	55	D8	AB	«±Wb@Á]Š».v*iU0«
00007D50	B1	57	62	AE	C5	5D	8A	BB	15	76	2A	EC	55	D8	AB	B1	±Wb@Á]Š».v*iU0«±
00007D60	57	62	AE	C5	5D	8A	BB	15	76	2A	EC	55	D8	AB	B1	57	Wb@Á]Š».v*iU0«±W
00007D70	62	AE	C5	5D	8A	BF	FF	D1	FB	F9	8A	BB	15	76	2A	EC	b@Á]ŠçÿŃùš».v*i
00007D80	55	D8	AB	B1	57	62	AE	C5	5D	8A	BB	15	76	2A	EC	55	U0«±Wb@Á]Š».v*iU
00007D90	D8	AB	B1	57	62	AE	C5	5D	8A	BB	15	76	2A	EC	55	D8	0«±Wb@Á]Š».v*iU0
00007DA0	AB	B1	57	62	AE	C5	5D	8A	BB	15	76	2A	EC	55	D8	AB	«±Wb@Á]Š».v*iU0«
00007DB0	B1	57	62	AE	C5	5D	8A	BB	15	76	2A	EC	55	D8	AB	B1	±Wb@Á]Š».v*iU0«±
00007DC0	57	62	AE	C5	5D	8A	BB	15	76	2A	EC	55	D8	AB	B1	57	Wb@Á]Š».v*iU0«±W
00007DD0	62	AE	C5	5D	8A	BB	15	76	2A	EC	55	D8	AB	B1	57	62	b@Á]Š».v*iU0«±Wb
00007DE0	AE	C5	5D	8A	BB	15	76	2A	EC	55	D8	AB	B1	57	62	AE	@Á]Š».v*iU0«±Wb@
00007DF0	C5	5D	8A	BB	15	76	2A	EC	55	D8	AB	B1	57	62	AE	C5	Á]Š».v*iU0«±Wb@Á
00007E00	5D	8A	BB	15	76	2A	EC	55	D8	AB	B1	57	62	AE	C5	5D]Š».v*iU0«±Wb@Á]
00007E10	8A	BB	15	76	2A	EC	55	D8	AB	B1	57	62	AE	C5	5D	8A	Š».v*iU0«±Wb@Á]Š
00007E20	BB	15	76	2A	EC	55	D8	AB	B1	57	62	AE	C5	5D	8A	BB	».v*iU0«±Wb@Á]Š»
00007E30	15	76	2A	EC	55	D8	AB	B1	57	62	AE	C5	5D	8A	BB	15	.v*iU0«±Wb@Á]Š.
00007E40	76	2A	EC	55	D8	AB	B1	57	62	AE	C5	5D	8A	BF	63	74	v*iU0«±Wb@Á]Šç[
00007E50	66	73	68	6F	77	7B	63	35	65	37	37	63	39	63	32	38	fshow{c5e77c9c28
00007E60	39	32	37	35	65	33	66	33	30	37	33	36	32	65	31	65	9275e3f3073c62e1e
00007E70	64	38	36	62	62	37	7D	76	2A	EC	55	D8	AB	B1	57	62	d86bb7)v*iU0«±Wb
00007E80	AE	C5	5D	8A	BF	FF	D5	FB	F9	8A	BB	15	76	2A	EC	55	@Á]ŠçÿŃùš».v*iU
00007E90	D8	AB	B1	57	62	AE	C5	5D	8A	BB	15	76	2A	EC	55	D8	0«±Wb@Á]Š».v*iU0
00007EA0	AB	B1	57	62	AE	C5	5D	8A	BB	15	76	2A	EC	55	D8	AB	«±Wb@Á]Š».v*iU0«
00007EB0	B1	57	62	AE	C5	5D	8A	BB	15	76	2A	EC	55	D8	AB	B1	±Wb@Á]Š».v*iU0«±
00007EC0	57	62	AE	C5	5D	8A	BB	15	76	2A	EC	55	D8	AB	B1	57	Wb@Á]Š».v*iU0«±W
00007ED0	62	AE	C5	5D	8A	BB	15	76	2A	EC	55	D8	AB	B1	57	62	b@Á]Š».v*iU0«±Wb
00007EE0	AE	C5	5D	8A	BB	15	76	2A	EC	55	D8	AB	B1	57	62	AE	@Á]Š».v*iU0«±Wb@
00007EF0	C5	5D	8A	BB	15	76	2A	EC	55	D8	AB	B1	57	62	AE	C5	Á]Š».v*iU0«±Wb@Á
00007F00	5D	8A	BB	15	76	2A	EC	55	D8	AB	B1	57	62	AE	C5	5D]Š».v*iU0«±Wb@Á]
00007F10	8A	BB	15	76	2A	EC	55	D8	AB	B1	57	62	AE	C5	5D	8A	Š».v*iU0«±Wb@Á]Š
00007F20	BB	15	76	2A	EC	55	D8	AB	B1	57	62	AE	C5	5D	8A	BB	».v*iU0«±Wb@Á]Š»
00007F30	15	76	2A	EC	55	D8	AB	B1	57	62	AE	C5	5D	8A	BB	15	.v*iU0«±Wb@Á]Š.
00007F40	76	2A	EC	55	D8	AB	B1	57	62	AE	C5	5D	8A	BB	15	76	v*iU0«±Wb@Á]Š».v
00007F50	2A	EC	55	D8	AB	B1	57	62	AE	C5	5D	8A	BF	FF	D6	FB	*iU0«±Wb@Á]ŠçÿŃù
00007F60	F9	8A	BB	15	76	2A	EC	55	D8	AB	B1	57	62	AE	C5	5D	ùš».v*iU0«±Wb@Á]
00007F70	8A	BB	15	76	2A	EC	55	D8	AB	B1	57	62	AE	C5	5D	8A	Š».v*iU0«±Wb@Á]Š



<https://blog.csdn.net/LYJ20010728>

binwalk 查看图片发现隐藏图片，利用 foremost 提取出来

```
(kali@kali)-[~/Desktop]
└─$ binwalk misc8.png
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 900 x 150, 8-bit/color RGBA, non-interlaced
91	0x5B	Zlib compressed data, compressed
3892	0xF34	PNG image, 900 x 150, 8-bit/color RGB, non-interlaced
3954	0xF72	Zlib compressed data, default compression

```
(kali@kali)-[~/Desktop]
└─$ foremost misc8.png
Processing: misc8.png
|*|

(kali@kali)-[~/Desktop]
└─$
```

<https://blog.csdn.net/LYJ20010728>

```
Cmder
C:\Users\95235
λ pytho
Python 3.8.8 (default, Apr 13 2021, 15:08:03) [MSC v.1916 64 bit (AMD64)] :: Anaconda, Inc. on win32

Warning:
This Python interpreter is in a conda environment, but the environment has
not been activated. Libraries may fail to load. To activate this environment
please see https://conda.io/activation

Type "help", "copyright", "credits" or "license" for more information.
>>> import pytesseract
>>> from PIL import Image
>>> img = Image.open(r'C:\Users\95235\Downloads\misc8\00000007.png')
>>> text = pytesseract.image_to_string(img)
>>> print(text)
ctfshow{1df0a9a3f709a2605803664b55783687}
>>> quit()
```

<https://blog.csdn.net/LYJ20010728>

misc9

用 `zsteg` 查看图片，发现flag

```
(kali@kali)-[~/Desktop]
└─$ zsteg misc9.png
meta XML:com.adobe.xmp.. text: "<?xpacket begin=\\\" id=\\\"W5M0MpCehiHzreSzNTczkc9d\\\"?> <x:xmpmeta xmlns:x=\\\"adobe:ns:meta/\\\" x:
org/1999/02/22-rdf-syntax-ns#\\\"> <rdf:Description rdf:about=\\\" xmlns:xmp=\\\"http://ns.adobe.com/xap/1.0/\\\" xmlns:dc=\\\"http://p
be.com/xap/1.0/mm/\\\" xmlns:stEvt=\\\"http://ns.adobe.com/xap/1.0/sType/ResourceEvent#\\\" xmp:CreatorTool=\\\"Adobe Photoshop CC 2019
tadataDate=\\\"2021-02-24T17:32:07+08:00\\\" dc:format=\\\"image/png\\\" photoshop:ColorMode=\\\"3\\\" photoshop:ICCPProfile=\\\"sRGB IEC61966
0ec0-4640-87cb-795628d37d8d\\\" xmpMM:OriginalDocumentID=\\\"xmp.did:f9094e65-0ec0-4640-87cb-795628d37d8d\\\"> <xmpMM:History> <rdf:S
when=\\\"2021-02-24T17:22:36+08:00\\\" stEvt:softwareAgent=\\\"Adobe Photoshop CC 2019 (Windows)\\\"/> </rdf:Seq> </xmpMM:History> </rd
00000000: 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d |<?xpacket begin=
00000010: 22 feff 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 ||. id="W5M0MpCe|
00000020: 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 |hiHzreSzNTczkc9d|
00000030: 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 |"?> <x:xmpmeta x|
00000040: 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 |mlns:x="adobe:ns|
00000050: 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d |:meta/" x:xmptk=|
00000060: 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 |"Adobe XMP Core|
00000070: 35 2e 36 2d 63 31 34 35 20 37 39 2e 31 36 33 34 |5.6-c145 79.1634|
00000080: 39 39 2c 20 32 30 31 38 2f 30 38 2f 31 33 2d 31 |99, 2018/08/13-1|
00000090: 36 3a 34 30 3a 32 32 20 20 20 20 20 20 20 22 |6:40:22 "|
000000a0: 3e 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 |> <rdf:RDF xmlns|
000000b0: 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 |:rdf="http://www|
000000c0: 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f |.w3.org/1999/02/|
000000d0: 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 |22-rdf-syntax-ns|
000000e0: 23 22 3e 20 3c 72 64 66 3a 44 65 73 63 72 69 70 |#> <rdf:Descrip|
000000f0: 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 |tion rdf:about=|
meta Warning .. text: "ctfshow{5c5e819508a3ab1fd823f11e83e93c75}"
```

<https://blog.csdn.net/LYJ20010728>

zsteg (补充)

zsteg安装方法 (补充)

更换RubyGems的源

```
gem sources --remove https://rubygems.org/  
gem sources --add https://gems.ruby-china.com/  
gem sources -l  
安装zsteg  
git clone https://hub.fastgit.org/zed-0xff/zsteg.git  
cd zsteg  
gem install zsteg
```

zsteg的使用方法 (常见)

查看帮助

```
zsteg -h
```

查看LSB信息

```
zsteg pcat.png
```

检测zlib

-b的位数是从1开始的

```
zsteg zlib.bmp -b 1 -o xy -v
```

显示细节

```
zsteg pcat.png -v
```

尝试所有已知的组合

```
zsteg pcat.png -a
```

导出内容

```
zsteg -E "b1,bgr,lsb,xy" pcat.png > p.exe
```

更多的使用方法可以查看README.md

misc10

用 `binwalk` 查看图片，分离图片，查看数据块即可发现flag，需要注意的是zlib是PNG IDAT的可选压缩格式

```
(kali@kali)-[~/Desktop]
└─$ binwalk misc10.png

DECIMAL      HEXADECIMAL     DESCRIPTION
-----
0            0x0             PNG image, 900 x 150, 8-bit/color RGB, non-interlaced
1382        0x566          Zlib compressed data, default compression
4325        0x10E5         Zlib compressed data, default compression

(kali@kali)-[~/Desktop]
└─$ binwalk -e misc10.png

DECIMAL      HEXADECIMAL     DESCRIPTION
-----
0            0x0             PNG image, 900 x 150, 8-bit/color RGB, non-interlaced
1382        0x566          Zlib compressed data, default compression
4325        0x10E5         Zlib compressed data, default compression

(kali@kali)-[~/Desktop]
└─$ ls
ctf  dirsearch  misc10.png  _misc10.png.extracted  starting_point_H3rmesk1t.ovpn  volatility  vulhub

(kali@kali)-[~/Desktop]
└─$ cd _misc10.png.extracted

(kali@kali)-[~/Desktop/_misc10.png.extracted]
└─$ ls
10E5  10E5.zlib  566  566.zlib

(kali@kali)-[~/Desktop/_misc10.png.extracted]
└─$ cat 10E5
ctfshow{353252424ac69cb64f643768851ac790}

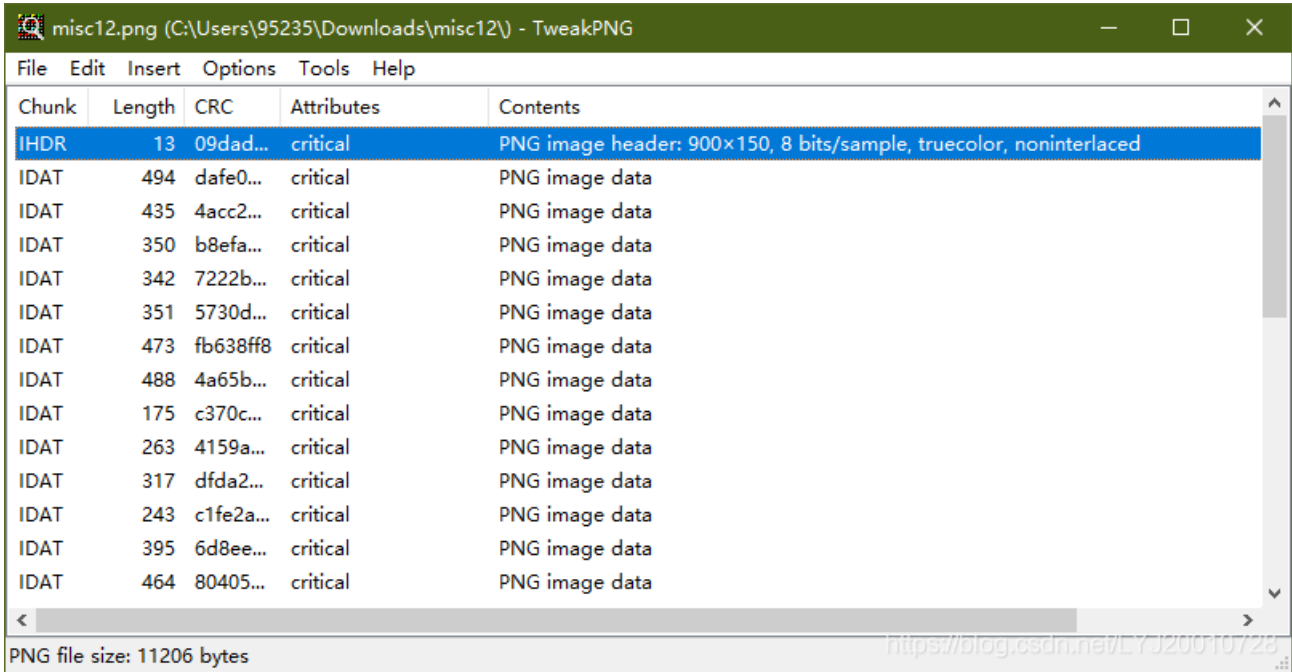
(kali@kali)-[~/Desktop/_misc10.png.extracted]
└─$
```

<https://blog.csdn.net/LYJ20010728>

misc11

binwalk 查看发现两个IDAT数据块，尝试删去第一个数据块，查看图片发现flag

测试后发现需要删掉前8个IDAT块



misc13

HxD 查看发现图片尾部存在可疑数据，观察发现 { 前面那一串字符从第一位开始每隔一位选取一个字符，连起来就是ctfshow，编写脚本提取flag

```
s="631A74B96685738668AA6F4B77B07B216114655336A5655433346578612534DD38EF66AB35103195381F628237BA6545347C3254647E373A64E465F136FA66F5341E3107321D665438F1333239E9616C7D"
flag=""
for i in range(0,len(s),4):
    flag += s[i]
    flag += s[i+1]
print(flag)
```

misc14

binwalk 查看图片，发现JPEG图片，foremost 和 binwalk 无法成功提取，用 HxD 打开搜索文件头手动提取

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 对应文本
000007E0 00 00 01 00 06 00 00 01 1A 00 05 00 00 00 01 00 .....
000007F0 00 01 96 01 1B 00 05 00 00 00 01 00 00 01 9E 01 ..-.....ž.
00000800 28 00 03 00 00 00 01 00 02 00 00 02 01 00 04 00 (.
00000810 00 00 01 00 00 01 A6 02 02 00 04 00 00 00 01 00 .....!.....
00000820 00 04 D5 00 00 00 00 00 00 00 00 48 00 00 00 01 00 ..Ö.....H....
00000830 00 00 48 00 00 00 01 FF D8 FF E0 00 10 4A 46 49 ..H....ÿøÿà..JFIF
00000840 46 00 01 01 01 00 78 00 78 00 00 FF DB 00 43 00 ¼.....x.x..ÿÜ.C.
00000850 02 01 01 02 01 01 02 02 02 02 02 02 02 03 05 .....
00000860 03 03 03 03 03 06 04 04 03 05 07 06 07 07 06 .....
00000870 07 07 08 09 0B 09 08 08 0A 08 07 07 0A 0D 0A 0A .....
00000880 0B 0C 0C 0C 0C 07 09 0E 0F 0D 0C 0E 0B 0C 0C 0C .....
00000890 FF DB 00 43 01 02 02 02 03 03 03 06 03 03 06 0C ÿÜ.C.....
000008A0 08 07 08 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C .....
000008B0 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C .....
000008C0 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C .....
000008D0 0C 0C 0C 0C 0C FF C0 00 11 08 00 18 01 9C 03 01 .....ÿÀ.....œ..
000008E0 22 00 02 11 01 03 11 01 FF C4 00 1F 00 00 01 05 ".
000008F0 01 01 01 01 01 01 00 00 00 00 00 00 00 00 01 02 .....
00000900 03 04 05 06 07 08 09 0A 0B FF C4 00 B5 10 00 02 .....ÿÀ.µ...
00000910 01 03 03 02 04 03 05 05 04 04 00 00 01 7D 01 02 .....}..
00000920 03 00 04 11 05 12 21 31 41 06 13 51 61 07 22 71 .....!1A..Qa."q
00000930 14 32 81 91 A1 08 23 42 B1 C1 15 52 D1 F0 24 33 .2..'.#B±Ä.RÑø93
00000940 62 72 82 09 0A 16 17 18 19 1A 25 26 27 28 29 2A br,.....%&'()*
00000950 34 35 36 37 38 39 3A 43 44 45 46 47 48 49 4A 53 456789:CDEFGHIJS
00000960 54 55 56 57 58 59 5A 63 64 65 66 67 68 69 6A 73 TUVWXYZcdefghijs
00000970 74 75 76 77 78 79 7A 83 84 85 86 87 88 89 8A 92 tuvwxzfy.....+*%&'
00000980 93 94 95 96 97 98 99 9A A2 A3 A4 A5 A6 A7 A8 A9 ""*---"mšcεm¥;§"©
00000990 AA B2 B3 B4 B5 B6 B7 B8 B9 BA C2 C3 C4 C5 C6 C7 *~'µ¶·¸°ÁÂÃÄÅÇ
000009A0 C8 C9 CA D2 D3 D4 D5 D6 D7 D8 D9 DA E1 E2 E3 E4 ÈÉÊËÖÓÔÕ×ØÙÚáäää
000009B0 E5 E6 E7 E8 E9 EA F1 F2 F3 F4 F5 F6 F7 F8 F9 FA åæçèéêñòóôõö÷øùú
000009C0 FF C4 00 1F 01 00 03 01 01 01 01 01 01 01 01 01 ÿÀ.....
000009D0 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0A .....
000009E0 0B FF C4 00 B5 11 00 02 01 02 04 04 03 04 07 05 ..ÿÀ.µ.....
000009F0 04 04 00 01 02 77 00 01 02 03 11 04 05 21 31 06 .....w.....!l.
00000A00 12 41 51 07 61 71 13 22 32 81 08 14 42 91 A1 B1 .AQ.aq."2...B'±
00000A10 C1 09 23 33 52 F0 15 62 72 D1 0A 16 24 34 E1 25 Ä.#3Rø.brÑ..$4á&
00000A20 F1 17 18 19 1A 26 27 28 29 2A 35 36 37 38 39 3A ñ....&'()*56789:
00000A30 43 44 45 46 47 48 49 4A 53 54 55 56 57 58 59 5A CDEFGHIJSTUVWXYZ
```

<https://blog.csdn.net/LYJ20010728>

```
C:\Users\95235
λ python
Python 3.8.8 (default, Apr 13 2021, 15:08:03) [MSC v.1916 64 bit (AMD64)] :: Anaconda, Inc. on win32

Warning:
This Python interpreter is in a conda environment, but the environment has
not been activated. Libraries may fail to load. To activate this environment
please see https://conda.io/activation

Type "help", "copyright", "credits" or "license" for more information.
>>> import pytesseract
>>> from PIL import Image
>>> img = Image.open(r'C:\Users\95235\Downloads\misc14\misc.jpg')
>>> text = pytesseract.image_to_string(img)
>>> print(text)
ctfshow{ce528f767fc465b8787cdb936363e6943
q
>>> |
```

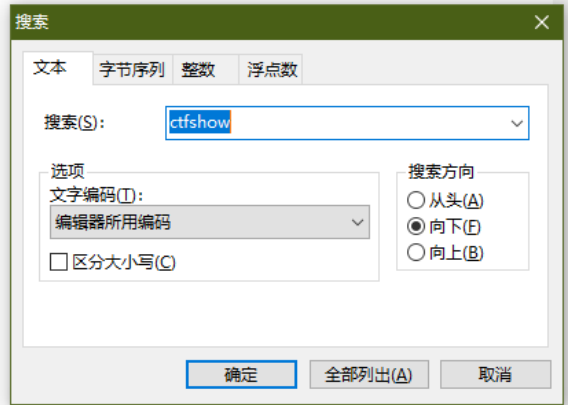
misc15

用 HxD 打开搜索关键词 `ctfshow` 即可发现flag

```

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 对应文本
00000000 42 4D 4E 09 01 00 00 00 00 00 67 01 00 00 28 00 BMN.....g...(.
00000010 00 00 84 03 00 00 96 00 00 00 01 00 04 00 00 00 .....-.....
00000020 00 00 D8 08 01 00 74 12 00 00 74 12 00 00 00 00 ..0...t...t....
00000030 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 80 .....e...e..e
00000040 00 00 00 80 80 00 80 00 00 80 00 00 80 00 80 80 ...ee.e...e.e.ee
00000050 00 00 80 80 80 00 C0 C0 C0 00 00 00 FF 00 00 FF ..eee.AAA...y..y
00000060 00 00 00 FF FF 00 FF 00 00 00 FF 00 FF 00 FF FF ...yy.y...y.y.yy
00000070 00 00 FF FF FF 00 74 78 6F 3D 2B 29 0B 62 4D 34 ..yy.y.txo=+).bM4
00000080 44 53 79 69 24 3B 55 37 28 46 54 2D 45 75 66 75 DSyi$;U7(FT-Eufu
00000090 56 6D 52 74 38 63 2F 71 35 4C 52 51 73 64 43 4E VmRt8c/q5LRQsdCN
000000A0 56 68 69 21 4F 3F 49 6A 29 09 2C 49 48 38 75 3E Vhi!O?Ij).,IH8u>
000000B0 25 31 4D 68 7D 43 0B 76 73 31 76 74 2C 70 28 71 %lMh)C.vslvt,p(q
000000C0 4A 4B 4E 0D 0D 49 2F 5E 25 68 3A 76 2D 62 7D 3E JKN..I/^#h:v-b)>
000000D0 49 59 74 6A 21 71 61 33 09 65 63 74 66 73 68 6E IYtj!qa3.ectfsho
000000E0 77 7B 66 62 65 37 62 62 36 35 37 33 39 37 65 36 [fibe7bb657397e6
000000F0 65 30 61 36 61 64 65 61 33 65 34 30 32 36 35 34 e0a6adea3e402654
00000100 32 35 7D 50 5B 20 50 42 78 4D 31 0D 4B 44 46 67 25]P[ PBxMl.KDFg
00000110 62 3C 62 57 50 46 39 31 39 6B 7B 5C 69 30 3C 31 b<bWPF919k{\i0<l
00000120 62 61 7B 63 09 63 77 71 49 5A 5F 59 6B 2E 67 5F ba(c.cwqIZ_Yk.g_
00000130 45 3C 49 68 5A 49 57 7A 6E 43 5A 6D 3E 29 59 38 E<IhZIWznCZm>)Y8
00000140 4D 7C 63 0C 59 2E 41 25 68 6A 26 6A 3E 2C 59 63 M|c.Y.A#hj&j>,Yc
00000150 5F 2A 79 78 4B 76 52 67 7C 23 25 22 4C 54 2F 48 *_yxKvRg|#%"LT/H
00000160 47 0A 66 47 7B 3D 39 FF FF FF FF FF FF FF FF G.fG(=9yyyyyyyyyy
00000170 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyy
00000180 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyy
00000190 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyy
000001A0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyy
000001B0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyy
000001C0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyy
000001D0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyy
000001E0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyy
000001F0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyy
00000200 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyy
00000210 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyy
00000220 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyy
00000230 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyy
00000240 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyy
00000250 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF yyyyyyyyyyyyyyyy

```



<https://blog.csdn.net/LYJ20010728>

misc16

binwalk 查看图片，发现额外数据，用 binwalk -e 提取出来，查看提取出来的文件发现flag

```

(kali@kali)-[~/Desktop]
└─$ binwalk misc16.png
DECIMAL      HEXADECEMIAL  DESCRIPTION
-----
0             0x0           PNG image, 900 x 150, 8-bit/color RGB, non-interlaced
41           0x29         Zlib compressed data, best compression
3540        0xDD4       LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: -1 bytes

(kali@kali)-[~/Desktop]
└─$ foremost misc16.png
Processing: misc16.png
|*|

(kali@kali)-[~/Desktop]
└─$ binwalk -e misc16.png
DECIMAL      HEXADECEMIAL  DESCRIPTION
-----
0             0x0           PNG image, 900 x 150, 8-bit/color RGB, non-interlaced
41           0x29         Zlib compressed data, best compression
3540        0xDD4       LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: -1 bytes

(kali@kali)-[~/Desktop]
└─$ ls
ctf_dirsearch  misc16.png  _misc16.png.extracted  starting_point_H3rmesk1t.ovpn  volatility  vulhub

(kali@kali)-[~/Desktop]
└─$ cd _misc16.png.extracted

(kali@kali)-[~/Desktop/_misc16.png.extracted]
└─$ ls
29 29.zlib DD4 DD4.7z

(kali@kali)-[~/Desktop/_misc16.png.extracted]
└─$ cat DD4
ctfshow{a7e32f131c011290a62476ae77190b52}

(kali@kali)-[~/Desktop/_misc16.png.extracted]
└─$

```

<https://blog.csdn.net/LYJ20010728>

misc17

binwalk 提取出来的东西解不出，尝试 zsteg，根据提示提取信息得到PNG图片，查看图片发现flag

```

kali@kali: ~/Desktop/_fl...
kali@kali:~/Desktop/_flag.extracted
File Actions Edit View Help
kali@kali:~/Desktop
└─$ zsteg misc17.png
[?] 3544 bytes of extra data after zlib stream
extradata:
00000000: e1 1f 30 53 86 4f c5 a4 1b f5 e6 e5 c7 46 0a 92 |...05.0.....F...
00000010: 9b ee 72 e7 c9 9e b9 a7 74 de 92 4d ad 61 5b 58 |..r....t..M.a[X
00000020: f2 98 65 77 2b d2 d3 85 32 fc 08 83 86 1f 0f 1e |..ew*...2.....
00000030: cb ab ac 9c 4b ca 02 2b e2 ce e4 ae 6b 1a 2c c6 |...K.....
00000040: 7b c8 9a 77 31 2f 9e 67 0b 49 3e 53 fe 17 a5 50 |!..w!/g..>5...P
00000050: 20 e5 1d 8c d5 49 e5 25 a5 31 cb 8b c5 3b 09 |....INR.T1...;
00000060: a2 a6 fe 5b da 4f 9e 78 9c 5d 46 d6 e2 6b 6b 2a |...[.0.x.]f..kk*
00000070: f2 62 0c ba 7b 19 a0 27 f3 84 77 99 02 77 05 79 |.0..p...w..w.y
00000080: 5b 44 d7 79 03 54 11 a1 f3 84 24 56 7e ff 55 d1 |[0.y.T...T4w..U
00000090: c6 39 90 c8 21 7f 26 39 44 58 78 c3 ed 37 4a 7c |.9...!.89DXx..7J|
000000a0: 50 24 e8 79 7b 4b 9c fa 2a 2c bb e8 b9 fb 40 2c |P$.y{K..*.,....D,
000000b0: 50 05 21 4c 2b 29 65 b4 60 1c 27 0b 4c 16 bf f1 |P..l;}e..'.L...
000000c0: 77 c0 55 04 3e 25 0e 18 1e 58 ab 0f 13 11 f2 3f |w.U.%...X....?
000000d0: cf a0 32 b1 f5 a8 1b 99 a7 4b 46 89 cf 85 89 50 |..2.....KF....P
000000e0: 88 20 8f 4f fd e2 97 55 68 73 b4 96 ba dd 25 a3 |..0...Uhs....X.
000000f0: 83 72 3f 99 77 9e 0a 08 50 4f 11 8f 87 65 c0 29 |.r?.w....PO...e.)
kali@kali:~/Desktop
└─$ zsteg -E "extradata:0" misc17.png > flag
kali@kali:~/Desktop
└─$ file flag
flag: data
kali@kali:~/Desktop
└─$ bimg -e flag
DECIMAL      HEXADECEIMAL  DESCRIPTION
-----
497          0x1f1         bzip2 compressed data, block size = 900k
kali@kali:~/Desktop
└─$ ls
ctf 006.bz2 006.bz2.extracted dirsearch flag _flag.extracted flag.txt misc17.png misc17.png.extracted starting_point_H4rneskit.ovpn volatility vulhub
kali@kali:~/Desktop
└─$ cd _flag.extracted
kali@kali:~/Desktop/_flag.extracted
└─$ ls
1f1
kali@kali:~/Desktop/_flag.extracted
└─$ cat 1f1
PNG

```

<https://blog.csdn.net/LYJ20010728>

```

Cmder
C:\Users\95235
λ python
Python 3.8.8 (default, Apr 13 2021, 15:08:03) [MSC v.1916 64 bit (AMD64)] :: Anaconda, Inc. on win32

Warning:
This Python interpreter is in a conda environment, but the environment has
not been activated. Libraries may fail to load. To activate this environment
please see https://conda.io/activation

Type "help", "copyright", "credits" or "license" for more information.
>>> import pytesseract
>>> from PIL import Image
>>> img = Image.open(r'C:\Users\95235\Downloads\misc17\flag.png')
>>> text = pytesseract.image_to_string(img)
>>> print(text)
ctfshow{0fe61fc42e8bbe55b9257d251749ae45}
Q
>>> quit()

```

<https://blog.csdn.net/LYJ20010728>

misc18

用 **exiftool** 查看图片，flag在标题、作者、照相机和镜头型号里

```

(kali@kali)-[~/Desktop]
└─$ exiftool misc18.jpg
ExifTool Version Number      : 12.16
File Name                    : misc18.jpg
Directory                   : .
File Size                    : 21 KiB
File Modification Date/Time  : 2021:03:13 11:44:41-05:00
File Access Date/Time       : 2021:07:28 14:54:22-04:00
File Inode Change Date/Time  : 2021:07:28 14:54:21-04:00
File Permissions             : rw-----
File Type                    : JPEG
File Type Extension         : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit              : inches
X Resolution                 : 120
Y Resolution                 : 120
Exif Byte Order              : Big-endian (Motorola, MM)
Camera Model Name            : 28ac17e5f0
Artist                       : 5d60c208f7
XP Title                     : ctfshow{32}
XP Author                    : 5d60c208f7
Padding                      : (Binary data 2072 bytes, use -b option to extract)
About                        : uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b
Title                        : ctfshow{32}
Description                  : ctfshow{32}
Creator                      : 5d60c208f7
Warning                      : [minor] Fixed incorrect URI for xmlns:MicrosoftPhoto
Lens Model                   : 2d4cf5a839}
Image Width                  : 900
Image Height                 : 150
Encoding Process             : Baseline DCT, Huffman coding
Bits Per Sample              : 8
Color Components              : 3
Y Cb Cr Sub Sampling        : YCbCr4:2:0 (2 2)
Image Size                   : 900x150
Megapixels                   : 0.135

```

<https://blog.csdn.net/LYJ20010728>

misc19

用 `exiftool` 查看图片，flag在主机上的文档名里

```

(kali@kali)-[~/Desktop]
└─$ exiftool misc19.tif
ExifTool Version Number      : 12.16
File Name                    : misc19.tif
Directory                   : .
File Size                    : 26 KiB
File Modification Date/Time  : 2021:03:24 23:12:27-04:00
File Access Date/Time       : 2021:07:28 14:57:41-04:00
File Inode Change Date/Time  : 2021:07:28 14:57:41-04:00
File Permissions             : rw-----
File Type                    : TIFF
File Type Extension         : tif
MIME Type                    : image/tiff
Exif Byte Order              : Little-endian (Intel, II)
Subfile Type                 : Full-resolution image
Image Width                  : 900
Image Height                 : 150
Bits Per Sample              : 8 8 8
Compression                  : LZW
Photometric Interpretation   : RGB
Document Name                : ctfshow{dfdcf08038cd446a5}
Strip Offsets                : 21688 25422
Orientation                  : Horizontal (normal)
Samples Per Pixel            : 3
Rows Per Strip               : 97
Strip Byte Counts            : 3733 749
X Resolution                 : 72
Y Resolution                 : 72
Planar Configuration        : Chunky
Resolution Unit              : inches
Software                     : Adobe Photoshop CC 2019 (Windows)
Modify Date                  : 2021:03:25 10:35:18
Host Computer                : eb50782f8d3605d}
Predictor                    : Horizontal differencing
XMP Toolkit                  : Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22
Creator Tool                  : Adobe Photoshop CC 2019 (Windows)
Create Date                  : 2021:03:13 11:03:03+08:00
Metadata Date                : 2021:03:25 10:35:18+08:00
Format                       : image/tiff
Color Mode                   : RGB
ICC Profile Name              : sRGB IEC61966-2.1
Instance ID                  : xmp.iid:ae9ae05b-7497-6e4b-8083-763920ef3505
Document ID                  : adobe:docid:photoshop:c214f24b-b22e-c14d-a0f5-91da2f09bb14
Original Document ID         : xmp.did:ff921484-29ad-7544-a030-38f38d997aa5
History Action                : created, converted, saved
History Instance ID          : xmp.iid:ff921484-29ad-7544-a030-38f38d997aa5, xmp.iid:ae9ae05b-7497-6e4b-8083-763920ef3505
History When                  : 2021:03:13 11:03:03+08:00, 2021:03:25 10:35:18+08:00
History Software Agent        : Adobe Photoshop CC 2019 (Windows), Adobe Photoshop CC 2019 (Windows)
History Parameters            : from image/png to image/tiff
History Changed               : /

```

<https://blog.csdn.net/LYJ20010728>

misc20

用 `exiftool` 查看图片，flag在评论里


```
(kali@kali)-[~/Desktop]
└─$ exiftool misc20.jpg
ExifTool Version Number      : 12.16
File Name                    : misc20.jpg
Directory                   : .
File Size                    : 14 KiB
File Modification Date/Time  : 2021:03:24 04:32:48-04:00
File Access Date/Time       : 2021:07:28 14:59:31-04:00
File Inode Change Date/Time  : 2021:07:28 14:59:31-04:00
File Permissions             : rw-----
File Type                    : JPEG
File Type Extension         : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit              : inches
X Resolution                 : 120
Y Resolution                 : 120
Exif Byte Order              : Big-endian (Motorola, MM)
Comment                      : 这图片也太难看了。来自：西替曼抚秀大括号西九七九六四必一谈易西曼抚零六易一第七九西二一第第谈第五九三易四二大括号
Image Width                  : 900
Image Height                 : 150
Encoding Process             : Baseline DCT, Huffman coding
Bits Per Sample              : 8
Color Components             : 3
Y Cb Cr Sub Sampling        : YCbCr4:2:0 (2 2)
Image Size                   : 900x150
Megapixels                   : 0.135
```

<https://blog.csdn.net/LYJ20010728>

misc21

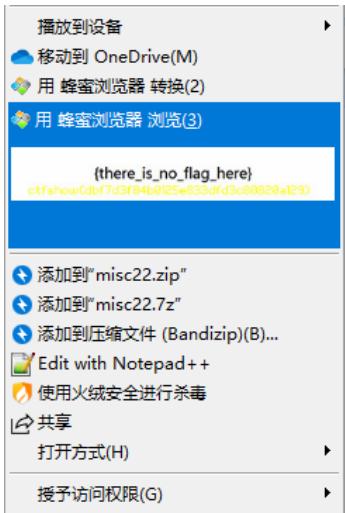
用 `exiftool` 查看图片，将序列号 `686578285826597329` 转字符得到 `hex(X&Ys)`，分别将 `X/Y Resolution` 和 `X/Y Position` 转成 `hex`，然后拼接起来，flag为 `ctfshow{e8a221498d5c073b4084eb51b1a1686d}`

```
(kali@kali)-[~/Desktop]
└─$ exiftool misc21.jpg
ExifTool Version Number      : 12.16
File Name                    : misc21.jpg
Directory                   : .
File Size                    : 14 KiB
File Modification Date/Time  : 2021:03:24 12:37:58-04:00
File Access Date/Time       : 2021:07:28 15:00:57-04:00
File Inode Change Date/Time  : 2021:07:28 15:00:57-04:00
File Permissions             : rw-----
File Type                    : JPEG
File Type Extension         : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit              : inches
Exif Byte Order              : Big-endian (Motorola, MM)
X Resolution                 : 3902939465
Y Resolution                 : 2371618619
Page Name                    : https://ctf.show/
X Position                   : 1082452817
Y Position                   : 2980145261
Target Printer               : ctfshow{}
Exif Version                 : 0232
Components Configuration    : Y, Cb, Cr, -
Security Classification      : Top Secret
Flashpix Version            : 0100
Color Space                  : Uncalibrated
Serial Number                : 686578285826597329
Image Width                  : 900
Image Height                 : 150
Encoding Process             : Baseline DCT, Huffman coding
Bits Per Sample              : 8
Color Components             : 3
Y Cb Cr Sub Sampling        : YCbCr4:2:0 (2 2)
Image Size                   : 900x150
Megapixels                   : 0.135
```

<https://blog.csdn.net/LYJ20010728>

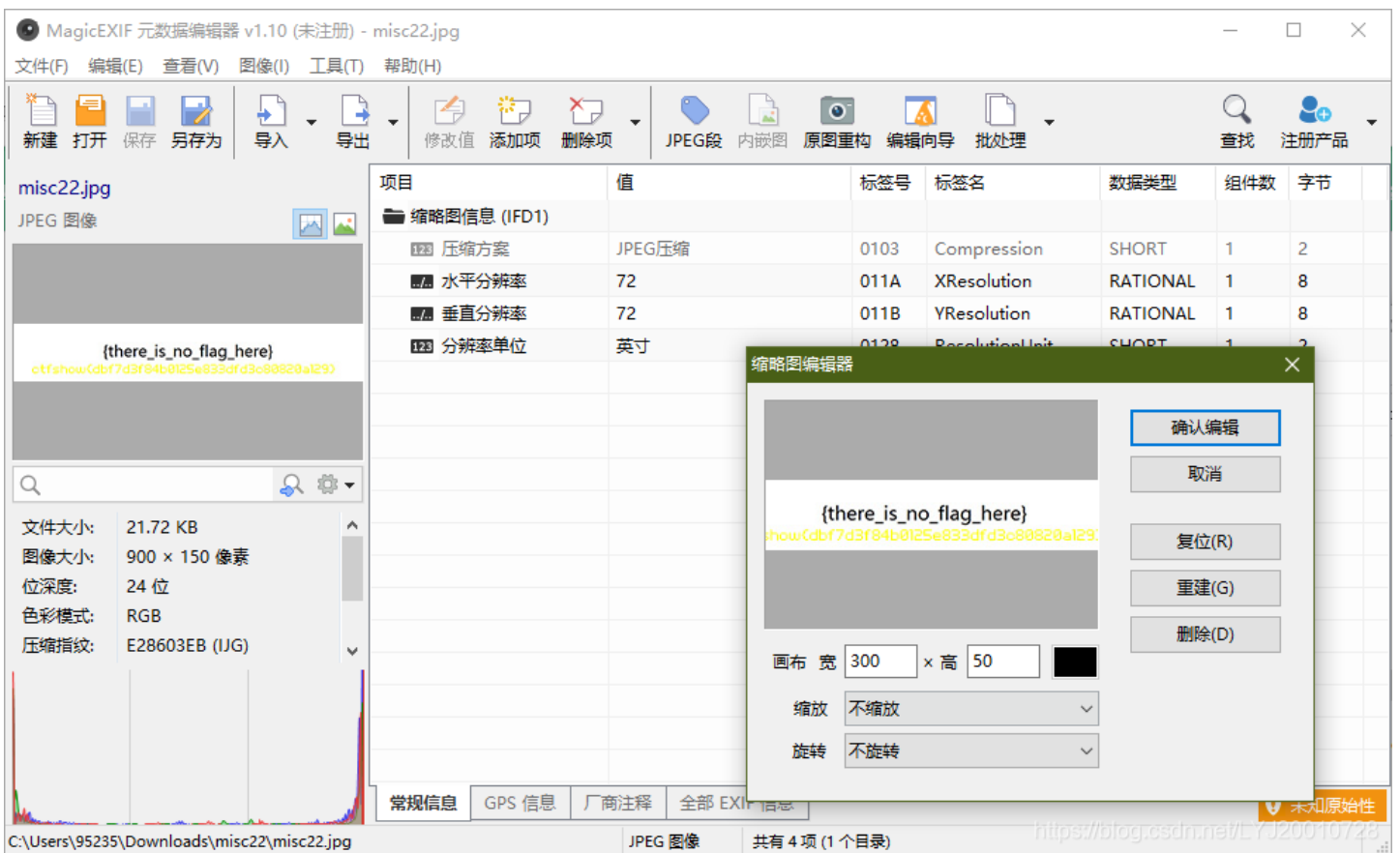
misc22

直接查看图片没有发现什么，但是用 `Honeyview` 浏览缩略图时发现数据



<https://blog.csdn.net/LYJ20010728>

利用 **MagicEXIF** 查看图片，flag为 `ctfshow{dbf7d3f84b0125e833dfd3c80820a129}`



<https://blog.csdn.net/LYJ20010728>

misc23

用 **exiftool** 看一下发现有好几个历史时间，**History Action** 中有提示

```

kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali) [~/Desktop]
└─┬─ exiftool misc23.psd
  ├── ExifTool Version Number : 12.16
  ├── File Name : misc23.psd
  ├── Directory :
  ├── File Size : 64 KiB
  ├── File Modification Date/Time : 2021:03:25 04:33:07-04:00
  ├── File Access Date/Time : 2021:07:28 15:19:46-04:00
  ├── File Inode Change Date/Time : 2021:07:28 15:19:46-04:00
  ├── File Permissions : rw-
  ├── File Type : PSD
  ├── File Type Extension : psd
  ├── MIME Type : application/vnd.adobe.photoshop
  ├── Num Channels : 3
  ├── Image Height : 150
  ├── Image Width : 900
  ├── Bit Depth : 8
  ├── IPTC Digest : 00000000000000000000000000000000
  ├── XMP Toolkit : Image::ExifTool 11.98
  ├── Format : application/vnd.adobe.photoshop
  ├── Color Mode : RGB
  ├── Text Layer Name : {there is no flag here}
  ├── Text Layer Text : {there is no flag here}
  ├── Create Date : 2021:03:25 15:45:24+08:00
  ├── Creator Tool : Adobe Photoshop CC 2019 (Windows)
  ├── Metadata Date : 2021:03:25 16:02:50+08:00
  ├── Modify Date : 2021:03:25 16:02:50+08:00
  ├── Document ID : xmp.did:49520599-6932-e144-8fab-dfd5873be5bc
  ├── History Action : cfshow1; UnixTimestamp, DECToHEX, getflag
  ├── History Instance ID : xmp.iid:1, xmp.iid:2, xmp.iid:3, xmp.iid:4
  ├── History Software Agent : Adobe Photoshop CC 2019 (Windows), Adobe Photoshop CC 2019 (Windows), Adobe Photoshop CC 2019 (Windows)
  ├── History When : 1997:09:22 02:17:02+08:00, 2055:07:15 12:14:46+08:00, 2038:05:05 16:50:45+08:00, 1984:08:03 16:41:46+08:00
  ├── History Changed : /
  ├── Instance ID : xmp.iid:066304e-08bd-0246-815c-0c8c684a0c81
  ├── Original Document ID : xmp.did:49520599-6932-e144-8fab-dfd5873be5bc
  ├── X Resolution : 72
  ├── Displayed Units X : inches
  ├── Y Resolution : 72
  ├── Displayed Units Y : inches
  ├── Print Style : Centered
  ├── Print Position : 0 0
  ├── Print Scale : 1
  ├── Global Angle : 90
  ├── Global Altitude : 30
  ├── URL List :
  ├── Slices Group Name :
  ├── Num Slices : 1
  ├── Pixel Aspect Ratio : 1
  ├── Photoshop Thumbnail : (Binary data 1155 bytes, use -b option to extract)
  ├── Has Real Merged Data : Yes
  └── Writer Name : Adobe Photoshop

```

<https://blog.csdn.net/LYJ20010728>

将给出的四个时间的戳转换出来，分别hex后拼在一起，转换地址

现在的Unix时间戳(Unix timestamp)是:

Unix时间戳 (Unix timestamp) 秒

时间 (年/月/日 时:分:秒) 秒

时间 年 月 日 时 分 秒 秒

<https://blog.csdn.net/LYJ20010728>

misc41

提示中的 F001 是突破点， HxD 查看图片发现有大量 F001 组成了某种形状


```
C:\Users\95235\Desktop
λ python exp.py
宽为: bytearray(b'\x00\x00\x03\x84')
高为: bytearray(b'\x00\x00\x00\xfa')

C:\Users\95235\Desktop
λ
```

根据脚本计算出来的值修改宽高，保存后即可看到flag

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	对应文本
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG.....IHDR
00000010	00	00	03	84	00	00	00	FA	b8	02	00	00	00	76	EC	1Eú]....vi.
00000020	40	00	00	20	F9	49	44	41	54	78	DA	ED	DD	D9	95	E4	@.. ùIDATxÚíÛ•ã
00000030	36	B6	05	50	59	23	43	CA	0A	F9	20	1B	64	82	3C	90	6¶.PY#CÈ.ù .d,<.
00000040	05	65	41	39	50	06	C8	00	19	A0	FF	FA	CF	87	D5	5C	.eA9P.È.. ýúÏ+õ\

```
C:\Users\95235\Desktop
λ python
Python 3.8.8 (default, Apr 13 2021, 15:08:03) [MSC v.1916 64 bit (AMD64)] :: Anaconda, Inc. on win32

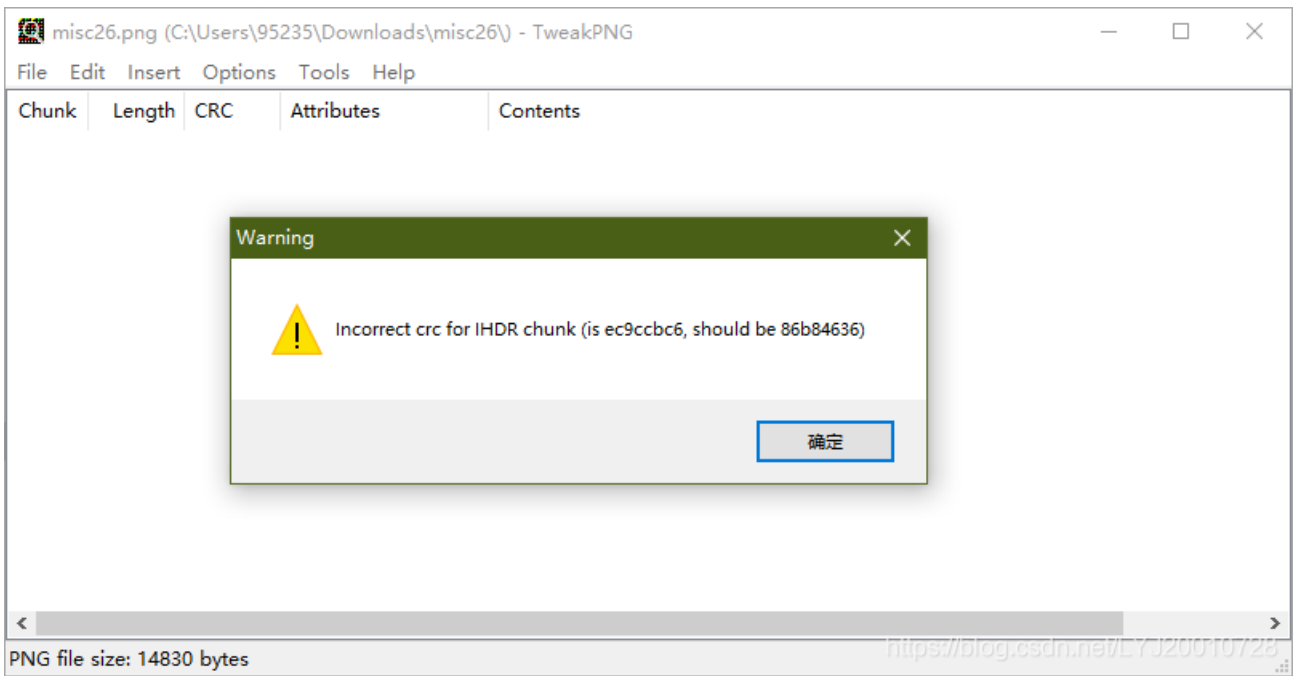
Warning:
This Python interpreter is in a conda environment, but the environment has
not been activated. Libraries may fail to load. To activate this environment
please see https://conda.io/activation

Type "help", "copyright", "credits" or "license" for more information.
>>> import pytesseract
>>> from PIL import Image
>>> img = Image.open(r'C:\Users\95235\Downloads\misc25\misc25.png')
>>> text = pytesseract.image_to_string(img)
>>> print(text)
{there_is_no_flag_here}

ctfshow{494f611fccc5842dd597f460874ce38f57}
9
>>> |
```

misc26

用 TweakPNG 查看图片发现图片的CRC值不对，和上一题一样用脚本跑一下看看



```
C:\Users\95235\Desktop
λpython exp.py
宽为: bytearray(b'\x00\x00\x03\x84')
高为: bytearray(b'\x00\x00\x02^')
```

```
C:\Users\95235\Desktop
λ |
```

cmd.exe

Search

根据脚本计算出来的值修改宽高，保存后即可看到flag

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	对应文本	
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG.....IHDR	
00000010	00	00	03	84	00	00	02	5E	08	06	00	00	00	00	EC	9C	CBiœË
00000020	C6	00	00	39	B5	49	44	41	54	78	DA	ED	DD	C1	B1	EA	Ë..9µIDATxÜiÝÃ±ê	
00000030	4C	62	36	60	A5	40	0A	2C	9C	00	19	B8	48	81	2A	47	Lb6`¥@.,œ...H.*G	
00000040	C0	C6	01	B0	F2	9E	8D	03	38	55	13	01	11	B8	8A	B5	ÀË.°òž...8U...Šµ	
00000050	77	6C	1C	00	01	78	C3	CA	FB	CF	A3	99	CB	8C	BE	BE	wl...xÃËûi±™ËË%¼	
00000060	2D	E8	6E	75	0B	01	CF	5B	F5	D4	FF	7B	BE	7B	38	3A	-ènu..Ï[ôÛÿ{%(8:	

```

C:\Users\95235\Desktop
λ python
Python 3.8.8 (default, Apr 13 2021, 15:08:03) [MSC v.1916 64 bit (AMD64)] :: Anaconda, Inc. on win32

Warning:
This Python interpreter is in a conda environment, but the environment has
not been activated. Libraries may fail to load. To activate this environment
please see https://conda.io/activation

Type "help", "copyright", "credits" or "license" for more information.
>>> import pytesseract
>>> from PIL import Image
>>> img = Image.open(r'C:\Users\95235\Downloads\misc26\misc26.png')
>>> text = pytesseract.image_to_string(img)
>>> print(text)
{there_is_no_flag_here}

ctfshow{94aef1
+True height(hex) of this picture+
087a7ccf2e28e742efd704c}
0
>>> print(img.size)
(900, 606)
>>> print(hex(606))
0x25e
>>> |

```

misc27

根据提示，猜测依旧是修改图片高度，将高度改高后即可发现flag

010 Editor - C:\Users\95235\Downloads\misc27\misc27.jpg

File Edit Search View Format Scripts Templates Debug Tools Window Help

Lenna.bmp Startup misc27.jpg x

Workspace

Hex	ASCII
0000h: FF D8 FF EE 00 0E 41 64 6F 62 65 00 64 40 00 00	ÿøÿï..Adobe.d@..
0010h: 00 01 FF DB 00 84 00 02 02 02 02 02 02 02 02	..ÿU.....
0020h: 02 03 02 02 02 03 04 03 02 02 03 04 05 04 04
0030h: 04 04 05 06 05 05 05 05 05 05 06 06 07 07 08
0040h: 07 06 09 09 0A 0A 09 09 0C 0C 0C 0C 0C 0C 0C
0050h: 0C 0C 0C 0C 0C 0C 0C 01 03 03 03 05 04 05 09
0060h: 06 09 0D 0A 09 0A 0D 0F 0E 0E 0E 0E 0F 0F 0C
0070h: 0C 0C 0C 0F 0F 0C 0C 0C 0C 0C 0C 0F 0C 0C 0C
0080h: 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0090h: 0C 0C 0C 0C 0C 0C 0C 0C FF C0 00 11 08 00 96 03ÿÄ...-
00A0h: 84 03 01 11 00 02 11 01 03 11 01 FF DD 00 04 00ÿÝ...
00B0h: 71 FF C4 01 A2 00 00 00 07 01 01 01 01 01 00	qÿÄ.C.....
00C0h: 00 00 00 00 00 00 04 05 03 02 06 01 00 07 08
00D0h: 0A 0B 01 00 02 02 03 01 01 01 01 01 00 00 00
00E0h: 00 00 00 01 00 02 03 04 05 06 07 08 09 0A 0B
00F0h: 00 02 01 03 03 02 04 02 06 07 03 04 02 06 02s
0100h: 01 02 03 11 04 00 05 21 12 31 41 51 06 13 61!.1A0..a"

Template Results - JPG.bt

Name	Value	Start	Size	Color	Comment
struct DQT dqt		12h	86h	Fg: Bg: [red]	
struct SOF0 sof0		98h	13h	Fg: Bg: [red]	
enum M_ID marker	M_SOF0 (FFC0h)	98h	2h	Fg: Bg: [red]	
WORD szSection	17	9Ah	2h	Fg: Bg: [red]	
ubyte precision	8	9Ch	1h	Fg: Bg: [red]	
WORD Y_image	150	9Dh	2h	Fg: Bg: [red]	
WORD X_image	900	9Fh	2h	Fg: Bg: [red]	
ubyte nr_comp	3	A1h	1h	Fg: Bg: [red]	
struct COMPS comp[3]		A2h	9h	Fg: Bg: [red]	
struct DRI dri		ABh	6h	Fg: Bg: [red]	

Inspector

Type	Value
Binary	00000000
Signed Byte	0
Unsigned Byte	0
Signed Short	-27136
Unsigned Short	38400
Signed Int	-2080139776
Unsigned Int	2214827520
Signed Int64	4786189215438336
Unsigned Int64	4786189215438336

Selected: 2 bytes (Range: 157 [9Dh] to 158 [9Eh]) Start: 157 [9Dh] Sel: 2 [2h] Size: 33,217 Hex ANSI Lit W OVR

Cmder

C:\Users\95235\Desktop

λ pytho

Python 3.8.8 (default, Apr 13 2021, 15:08:03) [MSC v.1916 64 bit (AMD64)] :: Anaconda, Inc. on win32

Warning:
This Python interpreter is in a conda environment, but the environment has not been activated. Libraries may fail to load. To activate this environment please see https://conda.io/activation

Type "help", "copyright", "credits" or "license" for more information.

```
>>> import pytesseract
>>> from PIL import Image
>>> img = Image.open(r'C:\Users\95235\Downloads\misc27\misc27.jpg')
>>> text = pytesseract.image_to_string(img)
>>> print(text)
{there_is_no_flag_here}
```

ctfshow{5cc4f19eb01705b99bf41492430a1a114}

```
>>> print(img.size)
(900, 250)
```

<https://blog.csdn.net/LYJ20010728>

misc28

根据提示，猜测依旧是修改图片高度，将高度改高后即可发现flag，但是需要注意从预览图中能看到flag，但是直接打开看不到，可以使用图片编辑器或者Stegsolve打开

010 Editor - C:\Users\95235\Downloads\misc28\misc28.gif

File Edit Search View Format Scripts Templates Debug Tools Window Help

Lenna.bmp Startup misc27.jpg misc28.gif x

Workspace

Hex	ASCII
0000h: 47 49 46 38 39 61 84 03 96 00 C4 00 00 00 00 00	GIF89a...-A....

Hex editor view showing memory dump and analysis tools.

Template Results - GIF.bt ↻

Name	Value	Start	Size	Color	Comment
struct DATA Data		6Dh	14C8h	Fg: Bg:	
struct GRAPHICCONTROLE...		6Dh	8h	Fg: Bg:	
struct IMAGEDESCRIPTOR I...		75h	Ah	Fg: Bg:	
UBYTE ImageSeperator	44	75h	1h	Fg: Bg:	
ushort ImageLeftPosition	0	76h	2h	Fg: Bg:	
ushort ImageTopPosition	0	78h	2h	Fg: Bg:	
ushort ImageWidth	900	7Ah	2h	Fg: Bg:	
ushort ImageHeight	150	7Ch	2h	Fg: Bg:	
struct IMAGEDESCRIPTO...		7Eh	1h	Fg: Bg:	
struct IMAGEDATA ImageD		7Fh	14B6h	Fg: Bg:	

Inspector

Type	Value
Binary	10010110
Signed Byte	-106
Unsigned Byte	150
Signed Short	150
Unsigned Short	150
Signed Int	83886230
Unsigned Int	83886230
Signed Int64	-82054518726522305...
Unsigned Int64	10241292201057321...

Selected: 2 bytes (Range: 124 [7Ch] to 125 [7Dh]) Start: 124 [7Ch] Sel: 2 [2h] Size: 3,430 Hex ANS I LT W OVR

```

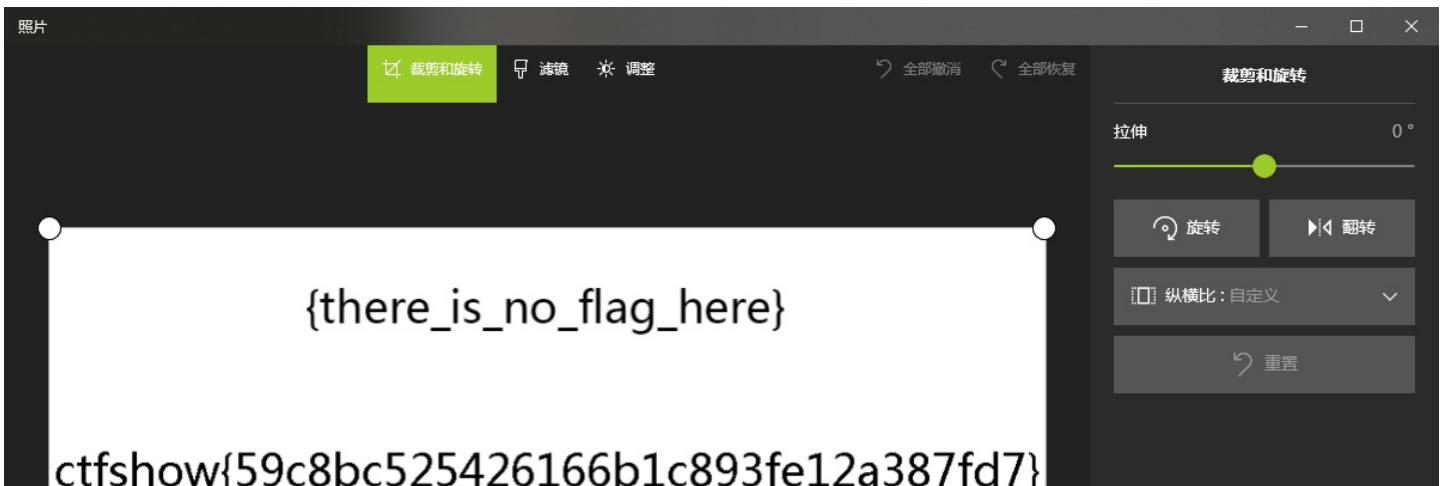
C:\Users\95235\Desktop
λ python
Python 3.8.8 (default, Apr 13 2021, 15:08:03) [MSC v.1916 64 bit (AMD64)] :: Anaconda, Inc. on win32

Warning:
This Python interpreter is in a conda environment, but the environment has
not been activated. Libraries may fail to load. To activate this environment
please see https://conda.io/activation

Type "help", "copyright", "credits" or "license" for more information.
>>> import pytesseract
>>> from PIL import Image
>>> img = Image.open(r'C:\Users\95235\Downloads\misc28\misc28.gif')
>>> text = pytesseract.image_to_string(img)
>>> print(text)
{there_is_no_flag_here}

ctfshow{59c8bc525426166b1c893fe12a387fd7}
λ
>>> print(img.size)
(900, 250)
>>> quit()

C:\Users\95235\Desktop
λ
  
```



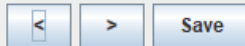
misc29

GIF有很多帧，将每一帧的高度都改高后，用 [Stegsolve](#) 查看，在第八帧即可发现flag

Frame : 8 of 10

{there_is_no_flag_here}

ctfshow{03ce5be6d60a4b3c7465ab9410801440}



<https://blog.csdn.net/LYJ20010728>

misc30

根据提示修改BMP图片宽度即可发现flag

010 Editor - C:\Users\95235\Downloads\misc30\misc30.bmp*

File Edit Search View Format Scripts Templates Debug Tools Window Help

Lenna.bmp Startup misc27.jpg misc28.gif misc29.gif misc30.bmp* x

Workspace

File	Path
Open Files	
Lenna.bmp	C:\Users...ictures\
misc27.jpg	C:\User...misc27\
misc28.gif	C:\User...misc28\
misc29.gif	C:\User...misc29\
misc30.bmp*	C:\User...misc30\
Favorite Files	
Recent Files	
Bookmarked Files	

Inspector

Type	Value
Binary	10110110
Signed Byte	-74
Unsigned Byte	182
Signed Short	950
Unsigned Short	950
Signed Int	950
Unsigned Int	950
Signed Int64	644245095350
Unsigned Int64	644245095350

Template Results - BMP.bt

Name	Value	Start	Size	Color	Comment
struct BITMAPINFOHEADER b...		Eh	28h	Fg: Bg:	
DWORD biSize	40	Eh	4h	Fg: Bg:	
LONG biWidth	950	12h	4h	Fg: Bg:	
LONG biHeight	150	16h	4h	Fg: Bg:	
WORD biPlanes	1	1Ah	2h	Fg: Bg:	
WORD biBitCount	24	1Ch	2h	Fg: Bg:	
DWORD biCompression	0	1Eh	4h	Fg: Bg:	
DWORD biSizeImage	427802	22h	4h	Fg: Bg:	
LONG biXPelsPerMeter	2834	26h	4h	Fg: Bg:	
LONG biYPelsPerMeter	2834	2Ah	4h	Fg: Bg:	

Edited template variable. Start: 18 [12h] Sel: 4 [4h] Size: 427,802 Hex ANSI LIT W OVR

Cmder

```

λ python
Python 3.8.8 (default, Apr 13 2021, 15:08:03) [MSC v.1916 64 bit (AMD64)] :: Anaconda, Inc. on win32

Warning:
This Python interpreter is in a conda environment, but the environment has
not been activated. Libraries may fail to load. To activate this environment
please see https://conda.io/activation

Type "help", "copyright", "credits" or "license" for more information.
>>> import pytesseract
>>> from PIL import Image
>>> img = Image.open(r'C:\Users\95235\Downloads\misc30\misc30.bmp')
>>> text = pytesseract.image_to_string(img)
>>> print(text)
ctfshow{6db8536da312f6aeb42da2f45b5f213c}
>>> quit()

```

<https://blog.csdn.net/LYJ20010728>

misc31

根据题给描述，计算正确宽度

```

C:\Users\95235\Desktop
λ python
Python 3.8.8 (default, Apr 13 2021, 15:08:03) [MSC v.1916 64 bit (AMD64)] :: Anaconda, Inc. on win32

Warning:
This Python interpreter is in a conda environment, but the environment has
not been activated. Libraries may fail to load. To activate this environment
please see https://conda.io/activation

Type "help", "copyright", "credits" or "license" for more information.
>>> s = (487253-53)/3
>>> s /= 150
>>> print(s)
1082.6666666666667
>>>

```

010 Editor - C:\Users\95235\Downloads\misc31\misc31.bmp

File Edit Search View Format Scripts Templates Debug Tools Window Help

misc31.bmp x

Address	Hex	ASCII
0000h	42 4D 58 6F 07 00 00 00 00 00 36 00 00 00 28 00	BMXo.....6...(.-..... ..".o.....yyyyyyyyyy
0010h	00 00 84 03 00 00 96 00 00 00 01 00 18 00 00 00
0020h	00 00 22 6F 07 00 12 0B 00 00 12 0B 00 00 00 00
0030h	00 00 00 00 00 00 FF FF FF FF FF FF FF FF
0040h	FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0050h	FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0060h	FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0070h	FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0080h	FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0090h	FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00A0h	FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00B0h	FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00C0h	FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00D0h	FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00E0h	FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00F0h	FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0100h	FF FF FF FF FF FF FF FF FF FF FF FF FF FF

Template Results - BMP.bt

Name	Value	Start	Size	Color	Comment
struct BITMAPINFOHEADER b...		Eh	28h	Fg: Bg:	
DWORD biSize	40	Eh	4h	Fg: Bg:	
LONG biWidth	1082	12h	4h	Fg: Bg:	
LONG biHeight	150	16h	4h	Fg: Bg:	
WORD biPlanes	1	1Ah	2h	Fg: Bg:	
WORD biBitCount	24	1Ch	2h	Fg: Bg:	
DWORD biCompression	0	1Eh	4h	Fg: Bg:	
DWORD biSizeImage	487202	22h	4h	Fg: Bg:	
LONG biXPelsPerMeter	2834	26h	4h	Fg: Bg:	
LONG biYPelsPerMeter	2834	2Ah	4h	Fg: Bg:	

Inspector

Type	Value
Binary	10000100
Signed Byte	-124
Unsigned Byte	132
Signed Short	900
Unsigned Short	900
Signed Int	900
Unsigned Int	900
Signed Int64	644245095300
Unsigned Int64	644245095300

Selected: 4 bytes (Range: 18 [12h] to 21 [15h]) Start: 18 [12h] Sel: 4 [4h] Size: 487,256 Hex ANS I LT W OVR

```

C:\Users\95235\Desktop
λ python
Python 3.8.8 (default, Apr 13 2021, 15:08:03) [MSC v.1916 64 bit (AMD64)] :: Anaconda, Inc. on win32

Warning:
This Python interpreter is in a conda environment, but the environment has
not been activated. Libraries may fail to load. To activate this environment
please see https://conda.io/activation

Type "help", "copyright", "credits" or "license" for more information.
>>> import pytesseract
>>> from PIL import Image
>>> img = Image.open(r'C:\Users\95235\Downloads\misc31\misc31.bmp')
>>> text = pytesseract.image_to_string(img)
>>> print(text)
ctfshow{fb09dcc9005fe3feeefb73646b55efd5}
q
>>> print(img.size)
(1082, 150)
>>> quit()

```

<https://blog.csdn.net/LYJ20010728>

misc32

根据题给描述，计算出正确的高宽

```
import zlib
import struct

# 同时爆破宽度和高度
filename = "misc32.png"
with open(filename, 'rb') as f:
    all_b = f.read()
    data = bytearray(all_b[12:29])
    n = 4095
    for w in range(n):
        width = bytearray(struct.pack('>i', w))
        for h in range(n):
            height = bytearray(struct.pack('>i', h))
            for x in range(4):
                data[x+4] = width[x]
                data[x+8] = height[x]
            crc32result = zlib.crc32(data)
            # 替换成图片的crc
            if crc32result == 0xE14A4C0B:
                print("宽为: ", end = '')
                print(width, end = ' ')
                print(int.from_bytes(width, byteorder='big'))
                print("高为: ", end = '')
                print(height, end = ' ')
                print(int.from_bytes(height, byteorder='big'))
```

```
C:\Users\95235\Desktop
λ python exp.py
宽为: bytearray(b'\x00\x00\x04\x14')
高为: bytearray(b'\x00\x00\x00\x96')

C:\Users\95235\Desktop
λ |
```



修改宽高保存后即可看到flag

010 Editor - C:\Users\95235\Downloads\misc32\misc32.png

misc32.png x

Name	Value	Start	Size	Color	Comment
union CType type	IHDR	Ch	4h	Fg: Bg:	
struct PNG_CHUNK_IHDR ihdr	900 x 150 (x8)	10h	Dh	Fg: Bg:	
uint32 width	1044	10h	4h	Fg: Bg:	
uint32 height	150	14h	4h	Fg: Bg:	
ubyte bits	8	18h	1h	Fg: Bg:	
enum PNG_COLOR_SPAC...	TrueColor (2)	19h	1h	Fg: Bg:	
enum PNG_COMPR_MET...	Deflate (0)	1Ah	1h	Fg: Bg:	
enum PNG_FILTER METH...	AdaptiveFiltering (0)	1Bh	1h	Fg: Bg:	
enum PNG_INTERLACE_...	NoInterlace (0)	1Ch	1h	Fg: Bg:	
uint32 crc	F14A4C0Bh	1Dh	4h	Fg: Bg:	

Inspector

Type	Value
Binary	00000000
Signed Byte	0
Unsigned Byte	0
Signed Short	0
Unsigned Short	0
Signed Int	-2080178176
Unsigned Int	2214789120
Signed Int64	-76381049658055720...
Unsigned Int64	10808639107903979...

Selected: 4 bytes (Range: 16 [10h] to 19 [13h]) Start: 16 [10h] Sel: 4 [4h] Size: 2,872 Hex ANSI LHT W OVR

Cmder

```
C:\Users\95235\Desktop
λ python
Python 3.8.8 (default, Apr 13 2021, 15:08:03) [MSC v.1916 64 bit (AMD64)] :: Anaconda, Inc. on win32

Warning:
This Python interpreter is in a conda environment, but the environment has
not been activated. Libraries may fail to load. To activate this environment
please see https://conda.io/activation

Type "help", "copyright", "credits" or "license" for more information.
>>> import pytesseract
>>> from PIL import Image
>>> img = Image.open(r'C:\Users\95235\Downloads\misc32\misc32.png')
>>> print(text)
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
NameError: name 'text' is not defined
>>> text = pytesseract.image_to_string(img)
>>> print(text)
ctfshow{685082227bcf70d17d1b39a5c1195aa9}
0
>>> quit()

C:\Users\95235\Desktop
λ
```

cmd.exe

misc33

根据题给描述，计算出正确的高宽

```
C:\Users\95235\Desktop
λ python exp.py
宽为: bytearray(b'\x00\x00\x03\xd2')
高为: bytearray(b'\x00\x00\x00\xe')

C:\Users\95235\Desktop
λ |
```

修改宽高保存后即可看到flag

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	对应文本
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG.....IHDR
00000010	00	00	03	D2	00	00	00	8E	08	02	00	00	00	52	55	A7	...ò...ž]....RUS
00000020	98	00	00	00	09	70	48	59	73	00	00	0B	13	00	00	0B	~....pHYs.....
00000030	13	01	00	9A	9C	18	00	00	0A	B3	49	44	41	54	78	DA	...šœ....³IDATxÚ
00000040	ED	DD	DB	9A	A2	48	16	80	51	DF	FF	A5	99	DB	9E	FE	íÝÛšçH.€Q8ÿ¥™Ùžp
00000050	66	52	89	7D	44	D7	BA	EC	CE	CA	42	08	22	7E	11	A9	fR%)D×°iîĒB."~.©
00000060	D7	05	00	00	14	7B	D9	05	00	00	20	BB	01	00	40	76	*....{Û... »..@v

```
C:\Users\95235\Desktop
λ python
Python 3.8.8 (default, Apr 13 2021, 15:08:03) [MSC v.1916 64 bit (AMD64)] :: Anaconda, Inc. on win32

Warning:
This Python interpreter is in a conda environment, but the environment has
not been activated. Libraries may fail to load. To activate this environment
please see https://conda.io/activation

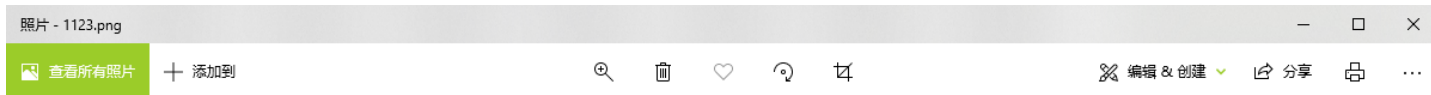
Type "help", "copyright", "credits" or "license" for more information.
>>> import pytesseract
>>> from PIL import Image
>>> img = Image.open(r'C:\Users\95235\Downloads\misc33\misc33.png')
>>> text = pytesseract.image_to_string(img)
>>> print(text)
ctfshow{03070a10ec3a3282bale352f4e07b0a9}
q
>>> quit()
```

<https://blog.csdn.net/LYJ20010728>

misc34

利用脚本把生成的所有图片都保存下来了，观察哪个是正常的

```
import zlib
import struct
filename = r"C:\Users\95235\Downloads\misc34\misc34.png"
with open(filename, 'rb') as f:
    all_b = f.read()
    #w = all_b[16:20]
    #h = all_b[20:24]
    for i in range(901,1200):
        name = str(i) + ".png"
        f1 = open(r"C:\Users\95235\Downloads\misc34\\" + name, "wb")
        im = all_b[:16]+struct.pack('>i',i)+all_b[20:]
        f1.write(im)
        f1.close()
```

< ctfshow{03e102077e3e5de9dd9c04aba16ef014} >

<https://blog.csdn.net/LYJ20010428>

misc35

先把图片基础的高度调高一点（高度在600，宽度在993-1000这个范围内都可以得到flag），才能看到flag

```
import zlib
import struct
filename = r"C:\Users\95235\Downloads\misc35\misc35.jpg"
with open(filename, 'rb') as f:
    all_b = f.read()
    #w = all_b[159:161]
    #h = all_b[157:159]
    for i in range(901,1200):
        name = str(i) + ".jpg"
        f1 = open(r"C:\Users\95235\Downloads\misc35\\" + name, "wb")
        im = all_b[:159]+struct.pack('>h',i)+all_b[161:]
        f1.write(im)
        f1.close()
```

```
C:\Users\95235\Desktop
λ python
Python 3.8.8 (default, Apr 13 2021, 15:08:03) [MSC v.1916 64 bit (AMD64)] :: Anaconda, Inc. on win32

Warning:
This Python interpreter is in a conda environment, but the environment has
not been activated. Libraries may fail to load. To activate this environment
please see https://conda.io/activation

Type "help", "copyright", "credits" or "license" for more information.
>>> import pytesseract
>>> from PIL import Image
>>> img = Image.open(r'C:\Users\95235\Downloads\misc35\997.jpg')
>>> text = pytesseract.image_to_string(img)
>>> print(text)
ctfshow{ca35201ca9ed607e5a68f44ef5 7 3fbc3}
q
>>> quit
Use quit() or Ctrl-Z plus Return to exit
>>> quit()

C:\Users\95235\Desktop
λ
C:\Users\95235\Desktop
λ
```

misc36

和上一题一样先把图片基础的高度调高一点，脚本爆破即可，用照片编辑器查看gif文件

```
import zlib
import struct
filename = r"C:\Users\95235\Downloads\misc36\misc36.gif"
with open(filename, 'rb') as f:
    all_b = f.read()
    for i in range(920,951):
        name = str(i) + ".gif"
        f1 = open(r"C:\Users\95235\Downloads\misc36\\" + name, "wb")
        im = all_b[:38]+struct.pack('>h',i)[::-1]+all_b[40:]
        f1.write(im)
        f1.close()
```

010 Editor - C:\Users\95235\Downloads\misc36\misc36.gif*

File Edit Search View Format Scripts Templates Debug Tools Window Help

misc35.jpg misc36.gif* x

Workspace

File	Path
Open Files	
misc35.jpg	C:\User...misc35\
misc36.gif*	C:\User...misc36\
Favorite Files	
Recent Files	
misc32.png	C:\User...misc32\
misc31.bmp	C:\User...misc31\
misc30.bmp	C:\User...misc30\
misc29.gif	C:\User...misc29\
misc28.gif	C:\User...misc28\
misc27.jpg	C:\User...misc27\
Lenna.bmp	C:\Users...ictures\
Bookmarked Files	
Workspace	
Explorer	

```

0020h: 00 2C 00 00 00 00 84 03 2C 01 00 02 FF 8C 8F A9 .....yE.
0030h: CB ED 0F A3 9C B4 DA 8B B3 DE BC FB 0F 86 E2 48 Èi.Èæ`Uç³P%Ù.îâH
0040h: 96 E6 89 A6 EA CA B6 EE 0B C7 F2 4C D7 F6 8D E7 -æ;|éÊñi.ÇòL×ò.ç
0050h: FA CE F7 FE 0F 0C 0A 87 C4 A2 F1 88 4C 2A 97 CC úÏ=p...†Açñ`L*-I
0060h: A6 F3 09 8D 4A A7 D4 AA F5 8A CD 6A B7 DC AE F7 |ó..Jš0°6šÍj·U@±
0070h: 0B 0E 8B C7 E4 B2 F9 8C 4E AB D7 EC B6 FB 0D 8F ..çÇ²ùENα×iñü..
0080h: CB E7 F4 BA FD 8E CF EB F7 FC BE FF 0F 18 28 38 Èçð°ÿZİè=ú%ÿy..(8
0090h: 48 58 68 78 88 98 A8 B8 C8 D8 E8 F8 08 19 29 39 HXhx`~`Èøèø..)9
00A0h: 49 59 69 79 89 99 A9 B9 C9 D9 E9 F9 09 1A 2A 3A IYiy%™@¹ÉÜéú..*:
00B0h: 4A 5A 6A 7A 8A 9A AA BA CA DA EA FA 0A 1B 2B 3B JZjzšš°èÜéú..+;
00C0h: 4B 5B 6B 7B 8B 9B AB BB CB DB EB FB 0B 1C 2C 3C K{k{ç}«»ÉÜéú..,<
00D0h: 4C 5C 6C 7C 8C 9C AC BC CC DC EC FC 0C 1D 2D 3D L\l|Èæ-¼İÜiü..=-
00E0h: 4D 5D 6D 7D 8D 9D AD BD CD DD ED FD 0D 1E 2E 3E M]m}...-¼İYÿy..>
00F0h: 4E 5E 6E 7E 8E 9E AE BE CE DE EE FE 0E 1F 2F 3F N^n~žž@%İbİp../?
0100h: 4F 5F 6F 7F 8F 9F AF BF CF DF EF FF 0F 30 A0 C0 O_o..ÿ;İBİÿ.0 Å
0110h: 81 04 0B 1A 3C 88 30 A1 C2 85 0C 1B 3A 7C 08 31 ...<0jÅ...:|.1
0120h: A2 C4 89 14 2B 5A BC 88 31 A3 C6 8D FF 1C 3B 7A cÅ%.+Z%¹fE.ÿ.:z

```

Template Results - GIF.bt

Name	Value	Start	Size	Color	Comment
> struct GRAPHICCONTROLE...		19h	8h	Fg: Bg:	
▼ struct IMAGEDESCRIPTOR I...		21h	Ah	Fg: Bg:	
UByte ImageSeperator	44	21h	1h	Fg: Bg:	
ushort ImageLeftPosition	0	22h	2h	Fg: Bg:	
ushort ImageTopPosition	0	24h	2h	Fg: Bg:	
ushort ImageWidth	900	26h	2h	Fg: Bg:	
ushort ImageHeight	300	28h	2h	Fg: Bg:	
> struct IMAGEDESCRIPTO...		2Ah	1h	Fg: Bg:	
> struct IMAGEDATA ImageD...		2Bh	AA6h	Fg: Bg:	
> struct TRAILER Trailer		AD1h	1h	Fg: Bg:	

Inspector

Type	Value
Binary	00101100
Signed Byte	44
Unsigned Byte	44
Signed Short	300
Unsigned Short	300
Signed Int	33554732
Unsigned Int	33554732
Signed Int64	-62286047327520027...
Unsigned Int64	12218139340957548...

Selected: 2 bytes (Range: 40 [28h] to 41 [29h]) Start: 40 [28h] Sel: 2 [2h] Size: 2,770 Hex ANSI LIT W OVR

裁剪和旋转 滤镜 调整 全部撤销 全部恢复

ctfshow{1ebf739f832906d60f57436b8179166f}

<https://blog.csdn.net/LYJ20010728>

misc37

用 Stegsolve 查看, flag 在 8、14、21、31、34 帧中, 拼接起来即可

Frame : 9 of 45

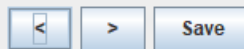
ctfshow{



<https://blog.csdn.net/LYJ20010728>

Frame : 14 of 45

2056782c



<https://blog.csdn.net/LYJ20010728>

Frame : 21 of 45

d57b1326



<https://blog.csdn.net/LYJ20010728>

Frame : 31 of 45

1dcbbe3d



<https://blog.csdn.net/LYJ20010728>

Frame : 34 of 45

6eecda17}



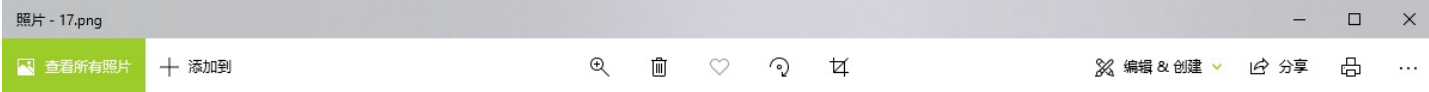
<https://blog.csdn.net/LYJ20010728>

misc38

题目所给的是png图片，可以使用APNG Disassembler来把每一帧分离出来，9、17、36、40 帧中藏有flag

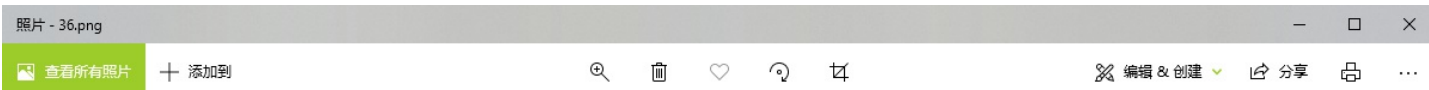
ctfshow{48

<https://blog.csdn.net/LYJ20010101>



b722b570c6

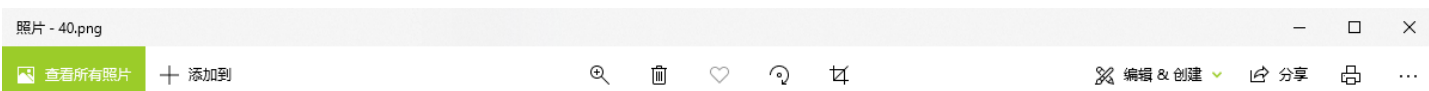
<https://blog.csdn.net/LYJ20010101>

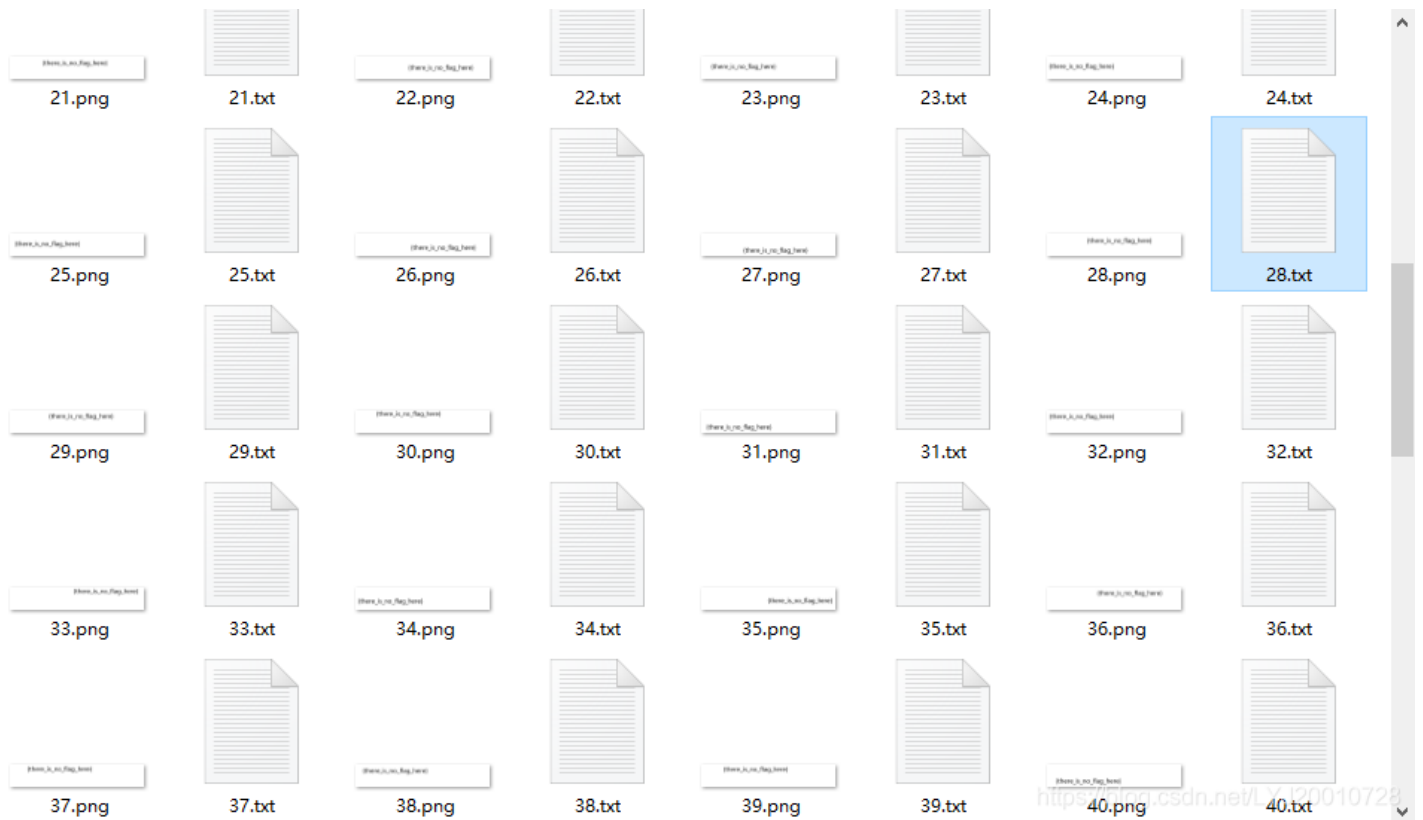


03ef58cc0b



<https://blog.csdn.net/LYJ20010101>





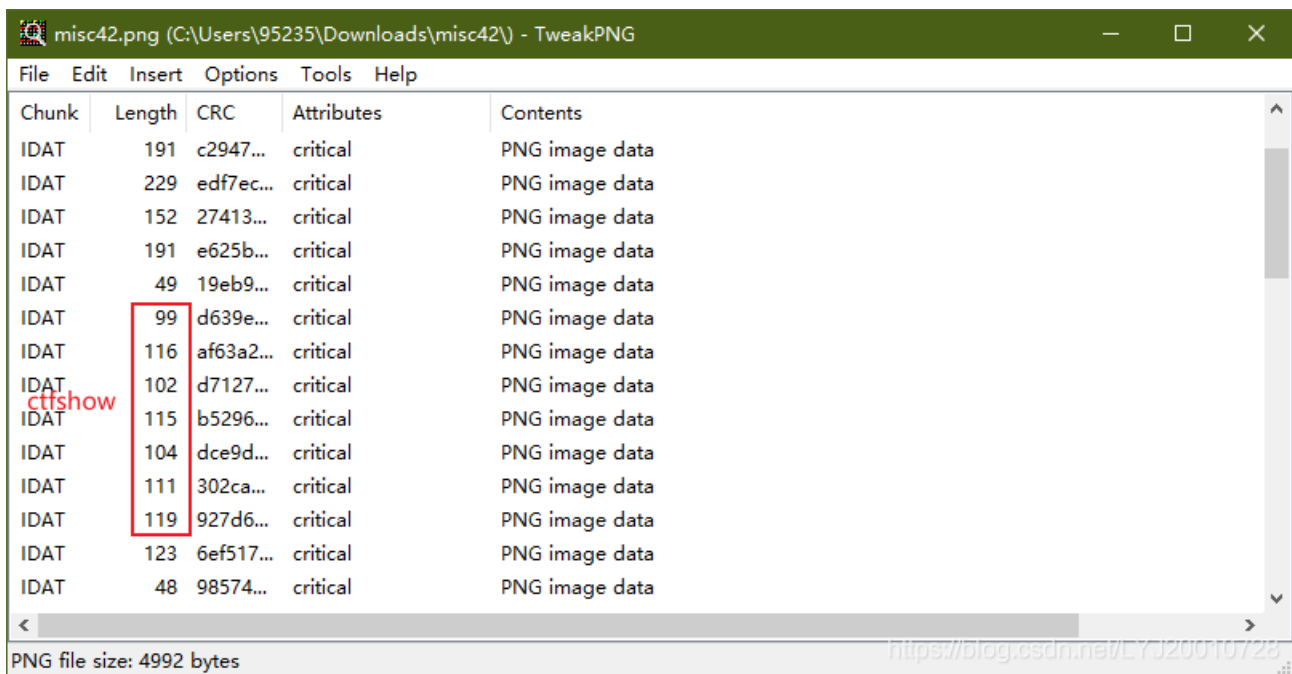
```
C:\Users\95235\Downloads\misc40
λ python
Python 3.8.8 (default, Apr 13 2021, 15:08:03) [MSC v.1916 64 bit (AMD64)] :: Anaconda, Inc. on win32

Warning:
This Python interpreter is in a conda environment, but the environment has
not been activated. Libraries may fail to load. To activate this environment
please see https://conda.io/activation

Type "help", "copyright", "credits" or "license" for more information.
>>> flag = ""
>>> for i in range(28,69):
...     f = open(r'C:\Users\95235\Downloads\misc40\' + str(i) + '.txt')
...     s = f.read()
...     flag += chr(int(s.split("/")[0][6:]))
...
>>> print(flag)
ctfshow{95ca0297dff0f6b1bdaca394a6fcb95b}
>>>
```

misc42

根据提示，用 `tweakpng` 打开图片，发现IDAT块的长度很可疑，有一部分IDAT块的长度转换为字符是 `ctfshow`，将后面的接着转换成字符即可得到flag



misc43

根据题给描述，先用tweakpng打开分析一下图片，发现报了一堆错，使用 `pngdebugger` 分析，发现所有IDAT块的crc32值都是错误的


```
C:\Tools\Tools_with_CTF\png-debugger\Debug (master -> origin)
λ .\PNGDebugger.exe C:\Users\95235\Downloads\misc43\misc43.png
--
file-path=C:\Users\95235\Downloads\misc43\misc43.png
file-size=4560 bytes

0x00000000  png-signature=0x89504E470D0A1A0A
0x00000008  chunk-length=0x00000000 (13)
0x0000000C  chunk-type='IHDR'
0x0000001D  crc-code=0x90DAD161
>> (CRC CHECK)  crc-computed=0x90DAD161 => CRC OK!

0x00000021  chunk-length=0x00000180 (384)
0x00000025  chunk-type='IDAT'
0x000000A9  crc-code=0xE59387E5
>> (CRC CHECK)  crc-computed=0x8385F691 => CRC FAILED

0x000001AD  chunk-length=0x00000180 (384)
0x000001B1  chunk-type='IDAT'
0x00000335  crc-code=0x93A62E63
>> (CRC CHECK)  crc-computed=0x42434298 => CRC FAILED

0x00000339  chunk-length=0x00000180 (384)
0x0000033D  chunk-type='IDAT'
0x000004C1  crc-code=0x74667368
>> (CRC CHECK)  crc-computed=0x4462C3A1 => CRC FAILED

0x000004C5  chunk-length=0x00000180 (384)
0x000004C9  chunk-type='IDAT'
0x0000064D  crc-code=0x6F777B36
>> (CRC CHECK)  crc-computed=0x397611E1 => CRC FAILED

0x00000651  chunk-length=0x00000180 (384)
0x00000655  chunk-type='IDAT'
0x000007D9  crc-code=0x65623235
>> (CRC CHECK)  crc-computed=0x4F82AFA2 => CRC FAILED

0x000007DD  chunk-length=0x00000180 (384)
0x000007E1  chunk-type='IDAT'
0x00000965  crc-code=0x38396666
>> (CRC CHECK)  crc-computed=0xDEFED27F => CRC FAILED

0x00000969  chunk-length=0x00000180 (384)
0x0000096D  chunk-type='IDAT'
0x00000AF1  crc-code=0x66663565
>> (CRC CHECK)  crc-computed=0x04F13EC2 => CRC FAILED

0x00000AF5  chunk-length=0x00000180 (384)
0x00000AF9  chunk-type='IDAT'
0x00000C7D  crc-code=0x33398666
>> (CRC CHECK)  crc-computed=0x665B7BEF => CRC FAILED
```

将错误的IDAT块的 `crc-code` 提取出来，拼接起来转字符串即可得到flag

```
C:\Users\95235\Downloads\misc40
λ python
Python 3.8.8 (default, Apr 13 2021, 15:08:03) [MSC v.1916 64 bit (AMD64)] :: Anaconda, Inc. on win32

Warning:
This Python interpreter is in a conda environment, but the environment has
not been activated. Libraries may fail to load. To activate this environment
please see https://conda.io/activation

Type "help", "copyright", "credits" or "license" for more information.
>>> import binascii
>>> def hex_to_str(s):
...     hex = s.encode('utf-8')
...     str_bin = bin
binascii bin(
...     str_bin = binascii.unhexlify(hex)
...     return str_bin.decode('utf-8')
...
>>> s = 'E59387E593A62E63746673686F777B366562323538396666666663565333930666536623837353034646263303839327D'
>>> hex_to_str(s)
'哇哦.ctfshow{6eb2589ffff5e390fe6b87504dbc0892}'
>>>
```

```
import binascii
def hex_to_str(s):
    hex = s.encode('utf-8')
    str_bin = bin
    str_bin = binascii.unhexlify(hex)
    return str_bin.decode('utf-8')

s = 'E59387E593A62E63746673686F777B366562323538396666666663565333930666536623837353034646263303839327D'
hex_to_str(s)
```

misc44

根据提示，用 **PNGDebugger** 打开，把信息导入到txt文件中

```
Cmder
C:\Users\95235\Downloads\misc40
λ C:\Tools\Tools_with_CTF\png-debugger\Debug\PNGDebugger.exe C:\Users\95235\Downloads\misc44\misc44.png > message .txt
```

利用脚本把 **CRC OK** 的替换成1， **CRC FAILED** 替换成0，注意先把前十行的内容删去，再把最后四行删去

```
C:\Users\95235\Desktop
λpython exp.py
1111111111111111101100011011101000110011001110011011010000110111101110111101111011000110110001100110000101
1001100011001100110010011000100110011000111001001101100011001100110000001110000110011001100011001100100011
0110001100110011001000110011001100010110001001100101001101110011100000110011011001100011011000111001011001011111
01
344
ÿÿctfshow{cc1af32bf96308fc1263231be783f69e}
C:\Users\95235\Desktop
λ
```

misc45

根据题给描述，猜测是文件转换，测试后发现转成 **.bmp** 格式后，用 **binwalk** 提取即可，看大师傅的blog发现考察点是 **png和bmp像素点的读取方式**

```
(kali@kali) [~/Desktop]
└─$ binwalk misc45.bmp
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PC bitmap, Windows 3.x format,, 900 x 150 x 24
65536	0x10000	gzip compressed data, has original file name: "flag.png", from Unix, last modified: 2021-03-29 15:44:52

```
(kali@kali) [~/Desktop]
└─$ binwalk -e misc45.bmp
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PC bitmap, Windows 3.x format,, 900 x 150 x 24
65536	0x10000	gzip compressed data, has original file name: "flag.png", from Unix, last modified: 2021-03-29 15:44:52

```
(kali@kali) [~/Desktop]
└─$ cd _misc45.bmp.extracted

(kali@kali) [~/Desktop/_misc45.bmp.extracted]
└─$ ls
flag.png
```

<https://blog.csdn.net/LYJ20010728>

```
C:\Users\95235\Desktop
λ python
Python 3.8.8 (default, Apr 13 2021, 15:08:03) [MSC v.1916 64 bit (AMD64)] :: Anaconda, Inc. on win32

Warning:
This Python interpreter is in a conda environment, but the environment has
not been activated. Libraries may fail to load. To activate this environment
please see https://conda.io/activation

Type "help", "copyright", "credits" or "license" for more information.
>>> import pytesseract
>>> from PIL import Image
>>> img = Image.open(r'C:\Users\95235\Downloads\misc45\flag.png')
>>> text = pytesseract.image_to_string(img)
>>> print(text)
ctfshow{057a722a5587979c34966c2436283e70}
>>>
```

misc46

根据题给描述，搜索后猜测应该是画图之类的，先提取出GIF的详细信息

```
identify misc46.gif > message.txt
```

```
(kali@kali) [~/Desktop]
└─$ identify misc46.gif > message.txt

(kali@kali) [~/Desktop]
└─$ gedit message.txt
```

Open	message.txt	Save
1 misc46.gif[0]	GIF 900x150 900x150+0+0 8-bit sRGB 2c 0.010u 0:00.015	
2 misc46.gif[1]	GIF 450x50 900x150+174+49 8-bit sRGB 16c 0.010u 0:00.019	
3 misc46.gif[2]	GIF 450x50 900x150+196+47 8-bit sRGB 16c 0.010u 0:00.019	
4 misc46.gif[3]	GIF 450x50 900x150+256+49 8-bit sRGB 16c 0.010u 0:00.019	
5 misc46.gif[4]	GIF 450x50 900x150+293+52 8-bit sRGB 16c 0.010u 0:00.019	
6 misc46.gif[5]	GIF 450x50 900x150+220+49 8-bit sRGB 16c 0.010u 0:00.019	
7 misc46.gif[6]	GIF 450x50 900x150+245+47 8-bit sRGB 16c 0.010u 0:00.019	

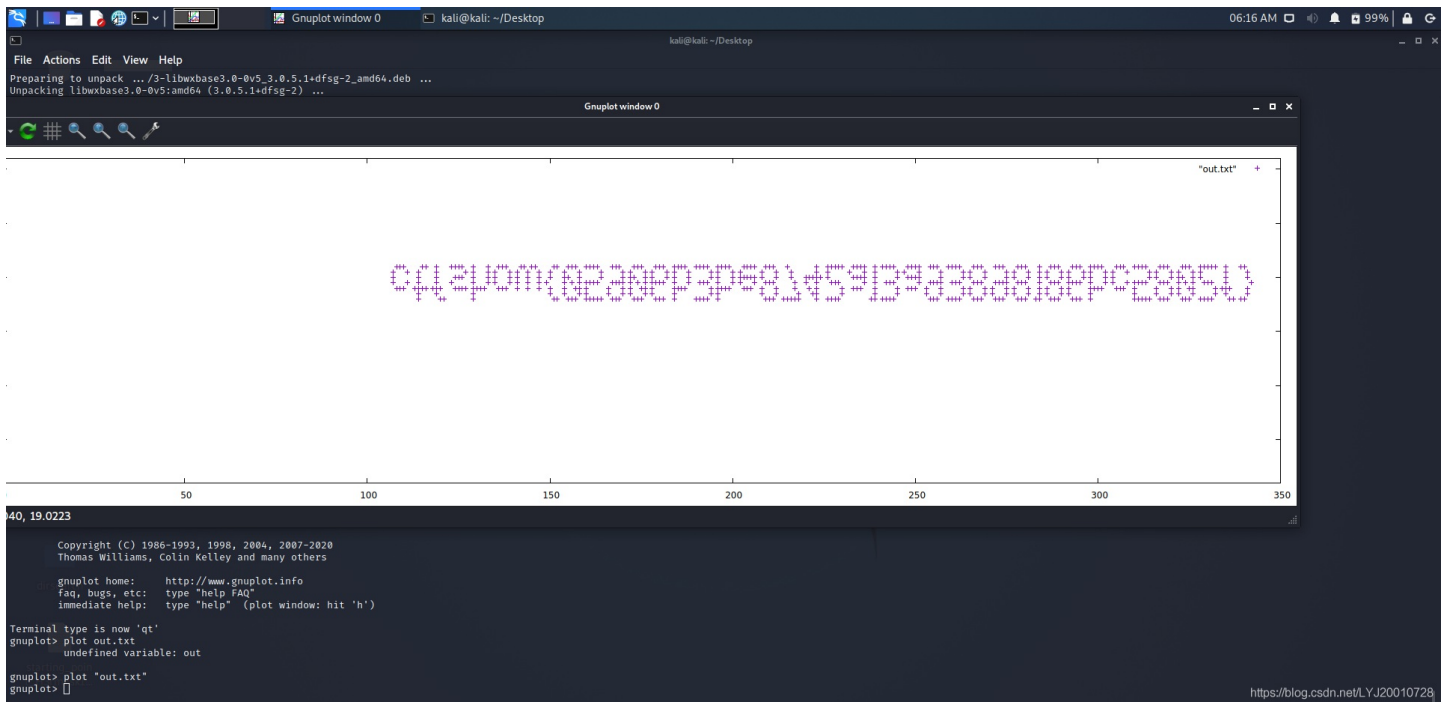
观察得到的信息，其中 0+0、174+49、196+47 这些是偏移量，用其来进行画图

坐标提取:

```
f = open(r"C:\Users\95235\Downloads\misc46\message.txt", "r")
x = f.readlines()
f.close()

f = open(r"C:\Users\95235\Downloads\misc46\out.txt", "w")
for i in x:
    f.write(i.split("+")[1])
    f.write(" ")
    f.write(i.split("+")[2][:2])
    f.write("\n")
f.close()
```

根据得到的点坐标进行绘图



<https://blog.csdn.net/LYJ20010728>

ctfshow{05905b3be8742a13a93838186bc5802f}

<https://blog.csdn.net/LYJ20010728>

测试后发现是apng格式，解题的思路是根据每一个IDAT块前面的一个fcTL块中包含的水平垂直偏移量

010 Editor - C:\Users\95235\Downloads\misc47\misc47.png

File Edit Search View Format Scripts Templates Debug Tools Window Help

misc35.jpg misc36.gif Startup misc47.png x Workspace

02C0h: 00 90 31 A3 00 00 64 CC 28 00 00 19 33 0A 00 40 ..1É..dİ(..3..@
02D0h: C6 8C 02 00 90 31 A3 00 00 64 CC 28 00 00 19 33 ÆÉ...1É..dİ(..3
02E0h: 0A 00 40 C6 8C 02 00 90 31 A3 00 00 64 CC 28 00 ..@ÆÉ...1É..dİ(.
02F0h: 00 19 33 0A 00 40 C6 8C 02 00 90 31 A3 00 00 64 ..3..@ÆÉ...1É..d
0300h: CC 28 00 00 19 33 0A 00 40 C6 8C 02 00 90 31 A3 İ(..3..@ÆÉ...1É
0310h: 00 00 64 CC 28 00 00 19 33 0A 00 40 C6 8C 02 00 ..dİ(..3..@ÆÉ..
0320h: 90 31 A3 00 00 64 CC 28 00 00 19 33 0A 00 40 C6 .1É..dİ(..3..@Æ
0330h: 8C 02 00 90 31 A3 00 00 64 CC 28 00 00 19 33 0A È...1É..dİ(..3..
0340h: 00 40 66 01 13 3E 04 29 05 E7 CD 31 00 00 00 1A .@f..>.)0çİ1...
0350h: 66 63 54 4C 00 00 00 01 00 00 01 C2 00 00 00 32 fcTL.....Ä...2
0360h: 00 00 00 B6 00 00 00 34 00 64 03 E8 00 00 0F ED ...4.d...i
0370h: FE A7 00 00 08 6C 66 64 41 5A 00 00 00 02 78 DA ps...lIdAT...xU
0380h: ED 9D DB 51 EC 3A 10 45 27 1A 02 99 28 C8 81 18 i.UQi:..E'..™(È..
0390h: 08 E1 64 40 04 44 40 02 04 40 00 04 C0 3F FF 73 .äd@.D@.@.Ä?ýs
03A0h: BB 4A 85 AA 6F DB 6E B5 A4 2D DB 9A D9 FB 8B C3 »J...ªoUñµª-ÜšUÜ«Ä
03B0h: 19 24 B9 1F CB 7A CF E5 46 51 14 45 75 E8 42 13 .\$.ÈzIãFQ.EuèB.
03C0h: 50 14 45 11 A3 14 45 51 C4 28 45 51 14 31 1A D1 P.E.É.EOÄ(EO.1.Ñ

Template Results - PNG.bt

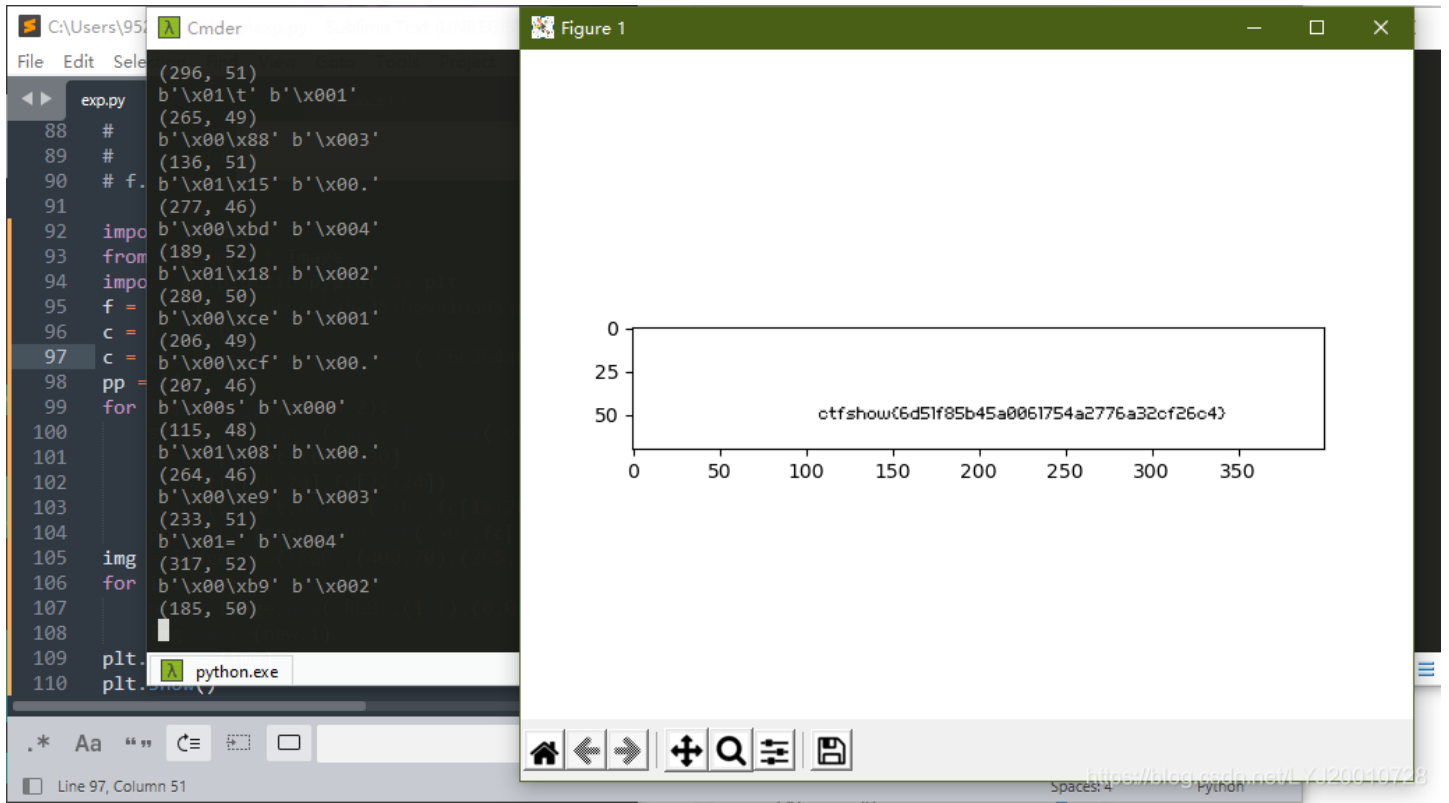
Name	Value	Start	Size	Color	Comment
struct PNG_CHUNK_FCTL fctl		354h	1Ah	Fg: Bg:	
uint32 sequence_number	1	354h	4h	Fg: Bg:	
uint32 width	450	358h	4h	Fg: Bg:	
uint32 height	50	35Ch	4h	Fg: Bg:	
uint32 x_offset	182	360h	4h	Fg: Bg:	
uint32 y_offset	52	364h	4h	Fg: Bg:	
int16 delay_num	100	368h	2h	Fg: Bg:	
int16 delay_den	1000	36Ah	2h	Fg: Bg:	
enum APNG_DISPOSE_O...	APNG_DISPOSE_O...	36Ch	1h	Fg: Bg:	
enum APNG_BLEND_OP	APNG_BLEND_OP	36Dh	1h	Fg: Bg:	

Selected: 4 bytes (Range: 864 [360h] to 867 [363h]) Start: 864 [360h] Sel: 4 [4h] Size: 1,240,626

Inspector

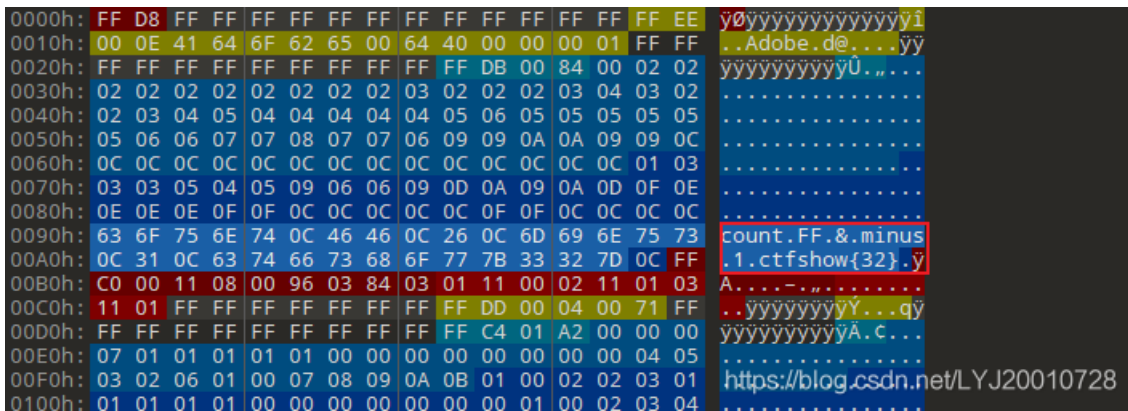
Type	Value
Binary	00000000
Signed Byte	0
Unsigned Byte	0
Signed Short	0
Unsigned Short	0
Signed Int	-1241513984
Unsigned Int	3053453312
Signed Int64	3746994893025705984
Unsigned Int64	3746994893025705984

```
import struct
from PIL import Image
import matplotlib.pyplot as plt
f = open(r'C:\Users\95235\Downloads\misc47\misc47.png', 'rb')
c = f.read()
c = c[c.index(bytes.fromhex('6663544C00000001')):]
pp = []
for i in range(1,1124,2):
    start = c.index(bytes.fromhex('6663544C0000')+struct.pack('>h',i))
    fc = c[start:start+30]
    print(fc[18:20],fc[22:24])
    print(struct.unpack('>h',fc[18:20])+struct.unpack('>h',fc[22:24]))
    pp.append(struct.unpack('>h',fc[18:20])+struct.unpack('>h',fc[22:24]))
img = Image.new('RGB', (400, 70), (255, 255, 255))
for i in pp:
    new = Image.new('RGB', (1,1), (0,0,0))
    img.paste(new,i)
plt.imshow(img)
plt.show()
```



misc48

用 010 editor 打开，发现提示 统计FF的数量再减去1、ctfshow{}中包含32个字符



因为flag长度是32位，所以只需要统计前32个段就行

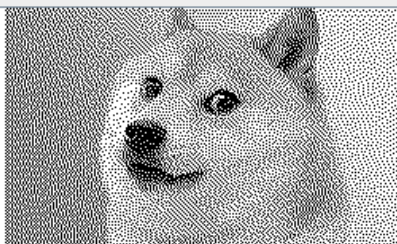
```
0 12 11 0 7 10 13 13 9 0 9 13 0 13 6 0 10 9 2 1 0 1 10 8 11 5 12 7 2 2 3 10
```

分别转换成hex即可

```
s = [0,12,11,0,7,10,13,13,9,0,9,13,0,13,6,0,10,9,2,1,0,1,10,8,11,5,12,7,2,2,3,10]
f = '0123456789abcdef'
flag = 'ctfshow{'
for i in range(len(s)):
    flag += f[s[i]]
flag += '}'
print(flag)
```


Green plane 0

wow
very flagge



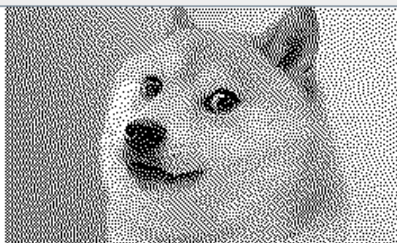
ctfshow
{844708



https://blog.csdn.net/L_YJ20010728

Red plane 1

wow
very taowwa



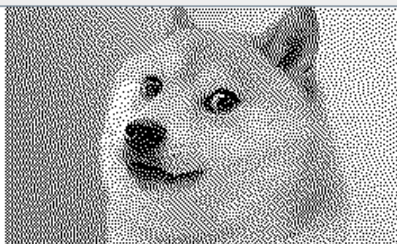
83ee1ee
c2e8864



https://blog.csdn.net/L_YJ20010728

Blue plane 2

wow
very miscce



36461bf
79111}



https://blog.csdn.net/L_YJ20010728