i春秋 MISC 神秘的文件

原创

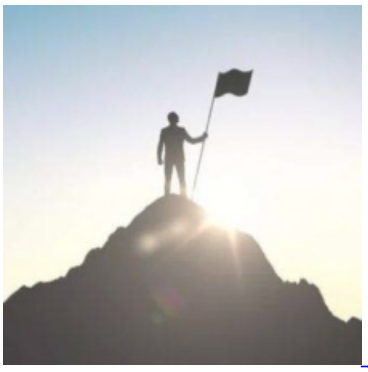
A_dmins 于 2019-06-21 15:51:18 发布 946 收藏 6

分类专栏： CTF题 一天一道CTF i春秋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/qq_42967398/article/details/93196765

版权



CTF题 同时被 3 个专栏收录

115 篇文章 11 订阅

订阅专栏

一天一道CTF

52 篇文章 5 订阅

订阅专栏

i春秋CTF

21 篇文章 1 订阅

订阅专栏

i春秋 MISC 神秘的文件

一天一道CTF题目，能多不能少

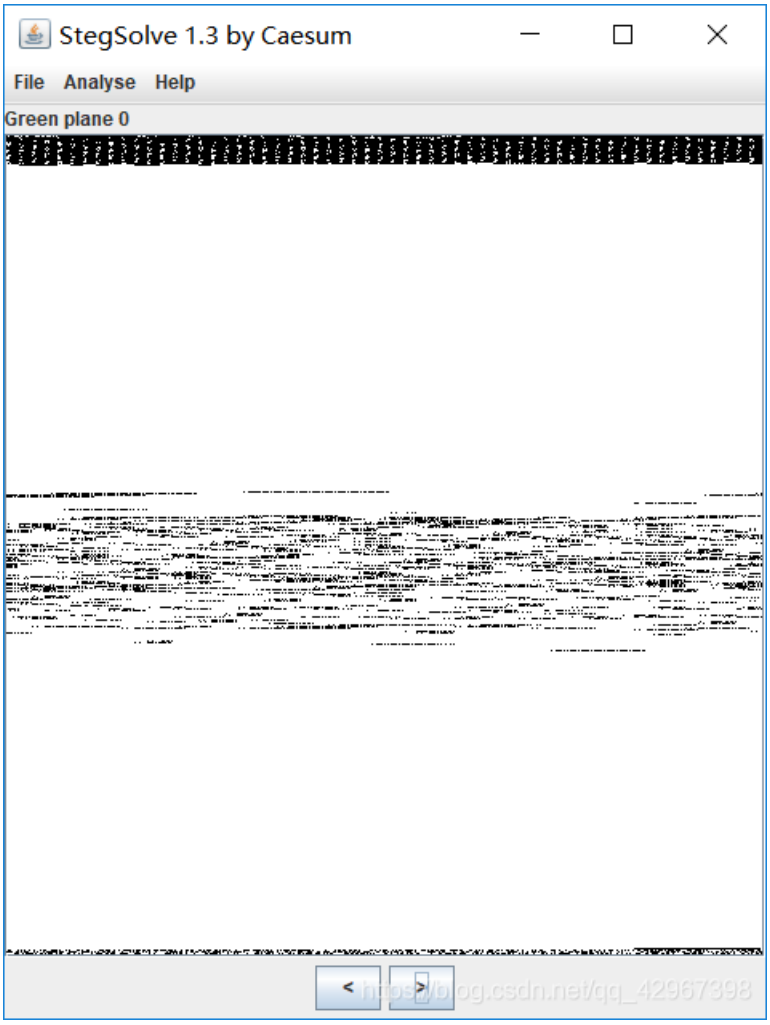
下载文件，没有后缀名，拖到winhex中查看，得知是一个PNG图片：

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	‰PNG IHDR
00000016	00	00	01	D8	00	00	01	FF	08	02	00	00	00	7B	12	5B	Ø ÿ { [
00000032	40	00	01	00	00	49	44	41	54	78	9C	EC	FD	7D	90	64	@ IDATxœìý} d
00000048	D7	95	1F	88	FD	EE	B9	F7	DD	7C	F9	32	2B	2B	2B	BB	×• ˆýî¹÷Ý|ù2+++»
00000064	BA	BA	FA	03	CD	46	03	04	C1	2F	0C	87	C3	01	39	9C	ººú ÍF Á/ ‡Ã 9œ
00000080	0F	51	DC	99	D9	91	76	A5	5D	D9	5A	AD	3E	66	27	76	QÜ™Ù'v¥]ÙZ->f'v
00000096	D7	92	2C	2B	BC	8E	75	84	77	D7	1F	11	FE	C3	B1	AB	×',+¼Žu„w× þÃ±«
00000112	F0	7A	1D	0E	87	43	72	28	C2	D2	5A	B2	14	B2	64	C9	ðz ‡Cr(ÂÒZ² ²dÉ
00000128	D2	EE	78	66	56	1A	71	38	33	1C	0C	49	71	40	10	04	Òîxf V q83 Iq@
00000144	41	10	68	02	8D	EE	42	77	75	75	75	55	56	56	56	E6	A h îBwuuuUVVVæ
00000160	CB	97	F7	9D	7B	8E	FF	B8	2F	B3	AB	D1	1F	44	37	9A	Ë—÷ {Žÿ¸/³«Ñ D7š
00000176	9A	91	C8	1B	88	44	F5	CB	97	F7	DD	77	3F	CE	3D	E7	š'È ˆDõË—÷Ýw?Î=ç
00000192	77	7E	E7	5C	A3	A2	30	80	A2	29	66	F1	87	E2	F6	75	w~ç\£¢0€¢)fñ‡âöu
00000208	B3	B8	82	FB	DC	76	FC	8F	E3	BF	35	77	FE	EA	0F	4E	³¸‚ûÜvü ã¿5wþê N
00000224	79	57	9B	EF	6E	E4	FB	6C	F9	F7	F5	F5	1F	30	2E	F7	yW›ïnäûlù÷õõ 0.÷
00000240	BB	F3	11	EA	37	77	8D	E9	BD	8B	00	00	E8	5D	77	99	»ó ê7w é½‹ è]w™
00000256	63	77	E8	B1	FB	14	00	A2	85	98	F4	6F	51	00	B0	86	cwè±û ¢…˜ôoQ °†
00000272	A3	28	19	03	15	52	07	63	C0	E0	5A	42	65	C9	82	22	£(R cÀàZBeÉ‚"
00000288	A4	02	1F	41	03	4C	54	CA	6A	A0	66	D7	E9	F5	01	0F	¤ A LTÊj f×éõ

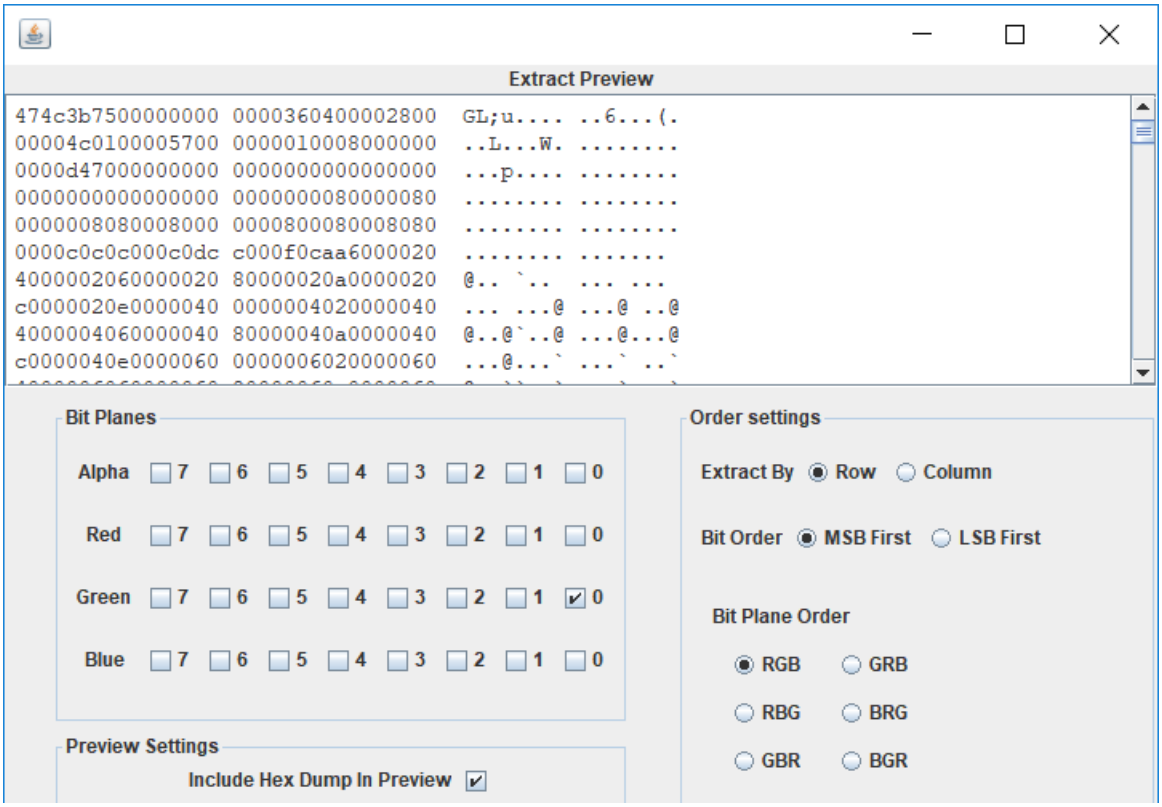
```
00000320  64 5A 55 02 E7 8B 15 EB  56 41 6D 4B 85 81 57 18  dZU ç‹ ëVAmK… W
00000336  05 8C 00 64 00 12 98 28  A4 02 00 86 60 48 0C D8  Œ d  ˜(¤  †`H Ø
00000352  22 02 30 70 80 01 DC E2  5D 15 D6 34 AF 71 F7 10  " 0p€ Üâ] Ö4¯q÷
00000368  DF D1 57 E9 C5 C4 2C 7F  FB C3 F2 FB 5F 64 F9 29  ßÑWéÅÄ, ûÃòû_dù)
00000384  10 03 27 A0 19 4B E6 E8  9B AF 5E 7E FD F5 37 47    ' Kæè›¯^~ýõ7G
00000400  A3 E1 4F FF D4 27 3F F2  EC 07 2D CC 9C EB B6 73  £áOÿÔ'?òì -Ìœë¶s
00000416  06 26 72 B0 CE 9A 3B 66  34 E1 CE 25 F8 FE 8B 03   &r°Îš;f4áÎ%øþ‹
00000432  EE 5C 63 C7 67 95 DE 75  F1 EE DB 70 9F DB 74 F1  î\cÇg•ÞuñîÛpŸÛtñ
00000448  F9 FD 96 C5 F7 AB FF C1  CF BD BB CD E6 3E 2F F5  ùý–Å÷«ÿÁϽ»Íæ>/õ
00000464  68 45 8F 7D BE 97 F6 DC  5D 1E 70 FF 3D 3B FC 9E  hE }¾—öÜ] pÿ=;üž
00000480  F7 3F 5A FF EB 5D 9F 78  C0 8E 45 F7 B9 7E FB FE  ÷?Zÿë]ŸxÀŽE÷¹~ûþ
00000496  D4 04 02 04 50 08 A0 2A  C6 90 02 06 D4 DC 67 33  Ô   P  *Æ   ÔÜg3
00000512  27 50 89 0C 8E 11 92 41  20 D1 0A 43 2B 4C 27 F5  'P‰ Ž ’A Ñ C+L'õ
00000528  FC 48 4D 20 17 15 C2 D1  44 98 EE C9 33 61 7A C8  üHM  ÂÑD˜îÉ3azÈ
00000544  B5 16 BD 9E 97 BA 9E 8C  EA C9 51 D1 6D 19 0E F3  µ ½ž—ºžŒêÉQÑm  ó
00000560  C9 61 E0 79 DE ED 14 FD  B5 4E B7 1B 19 55 10 CA  Éaàyßí ýµN·  U Ê
00000576  0C 0C 89 51 00 1A 15 50  03 63 00 18 36 62 1D 11    ‰Q   P c  6b
00000592  A8 69 A8 1A 81 2A 0C 41  A1 C6 18 75 B7 5F 87 CC  ¨i¨  * A¡Æ u·_‡Ì
00000608  BB 3B FF BE 73 26 BD 2E  DD EE 8D C7 BE D9 7F CF  »;ÿ¾s&½.Ýî Ç¾Ù Ï
00000624  AA BE E7 3E FD 7E EA 7F  BC EB FA 7E F5 3F AE A7  ª¾ç>ý~ê ¼ëú~õ?®§
00000640  DC 51 0F 01 22 2A 96 00  45 46 64 00 88 1A 98 CC  ÜQ  "*– EFd ˆ ˜Ì
00000656  DB 3A D4 CC 6C 5D D6 72  19 A0 0A 35 64 CC F7 94  Û:ÔÌl]Ör   5dÌ÷”
00000672  B7 F7 6C 7F 2A EF AD FD  F7 DF AE 1F 57 2F 3C 9A  ·÷l *ï-ý÷ß® W/<š
00000688  BE F6 DE 1F FD 00 69 F5  50 32 FA 91 35 C7 7B 5E  ¾öÞ ý iõP2ú‘5Ç{^
00000704  BF BB C2 47 90 86 0F B5  7A BF A7 D4 BE BB 3C A0  ¿»ÂG † µz¿§Ô¾»<
00000720  FE BB BF 7A 6F F5 9B E3  D7 9B 7F 34 9A 27 00 02  þ»¿zoõ›ã×› 4š'
00000736  8C 21 C0 28 45 11 43 8D  0C 27 86 A8 8A 81 B1 44  Œ!À(E C  '†¨Š ±D
00000752  10 26 11 80 51 1D CD C7  7B B1 1A D7 61 1C AA 49  & €Q ÍÇ{± ×a ªI
00000768  CD 65 E0 52 10 7D DE 6D  15 9D 6E B7 E3 B3 96 8F  ÍeàR }Þm  n·ã³–
00000784  75 D8 19 1E 0D 6F B5 3C  85 C9 61 B5 37 5F 5D 29  uØ   oµ<…Éaµ7_])
00000800  BC D4 19 19 CB 06 21 03  59 EB 8B 8E EF 44 E3 60  ¼Ô  Ë ! Yë‹ŽïDã`
00000816  BC AA 37 B0 4A 30 12 0D  19 20 6A 64 22 32 49 68  ¼ª7°J0    jd"2Ih
```

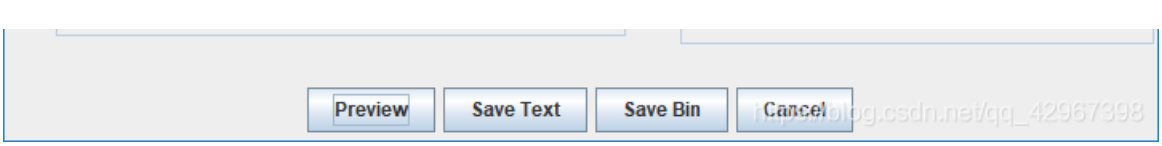
更改后缀名，得到一张so beautiful的图片：

查看了属性，什么都没有
binwalk了，什么都没有
直到Stegsolve，有所发现：



这个有点东西啊，直接Analyse一下，Data Extrect查看：





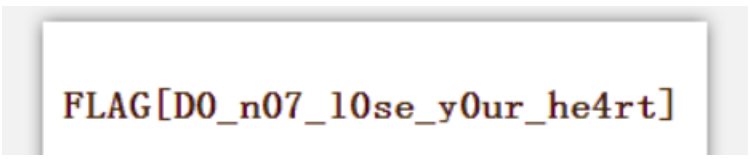
这都是些啥啊，不过这里面肯定有点东西的，
先save Bin下来，根据题目又知道文件损坏，那肯定是叫我们修复文件
不过目前我们还不知道是什么文件，只能靠自己去猜测了
把save下来的文件放到winhex下查看文件尾，不过没看出啥来，不过不是平常常见文件的文件尾（常见文件头，文章文件尾后面有描述）：

```
029920  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
029936  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
029952  FF FF FF FF FF FF FF FF  FF FF 00 00 00 00 00 00  ÿÿÿÿÿÿÿÿÿÿ
029968  00 00 00 01 9E AD BA 70  BA F2 CF C4 6D 82 89 31      ž-ºpºòÏÄm‚‰1
029984  08 BB 27 28 CA 2E F0 C1  4B A8 44 02 FE FA 4C 97   »'(Ê.ðÁK¨D þúL—
030000  E5 A3 A9 82 E2 92 38 27  9A B8 CB 26 DF 59 F1 BB  å£©‚â’8'š¸Ë&ßYñ»
030016  CE F2 DB 1B 56 CC 4A 28  47 8C 2B FD 7B 22 19 0C  ÎòÛ VÌJ(GŒ+ý{"
030032  A3 AE 80 8E 0E 0A B2 4F  7A 9A BB F4 13 64 C5 82  £®€Ž  ²Ozš»ô dÅ‚
030048  D4 17 F2 A1 BC BC 71 CC  32 25 26 1E 65 46 C6 FE  Ô ò¡¼¼qÌ2%& eFÆþ
030064  0D 3E F2 71 B0 BF 81 DB  14 7D CE 22 13 2B BD 7F   >òq°¿ Û }Î" +½
030080  F3 40 F2 2C E9 2D 66 95  D9 94 F8 D0 59 46 9C DA  ó@ò,é-f•Ù”øÐYFœÚ
030096  FB 0C 8E 0F 0F B7 E1 53  7B F2 0B DD 7D E2 C5 D7  û Ž  ·áS{ò Ý}âÅ×
030112  2C A1 8D 4F E2 48 AB F3  74 D3 3F BC C2 61 E9 76  ,¡ OâH«ótÓ?¼Âaév
030128  48 97 53 BC B5 80 F6 11  A4 BB 6B 8E 61 93 7E 11  H—S¼µ€ö ¤»kŽa“~
030144  1F AC 4D E6 B2                                     ¬Mæ²
```

在查看一下具体的内容，发现于bmp的内容有点相似，
一般的bmp图片文件头内容：

```
Offset    0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15   ANSI ASCII
00000000  42 4D AE 0A 0B 00 00 00  00 00 36 00 00 00 28 00  BM®       6   (
00000016  00 00 D8 01 00 00 FF 01  00 00 01 00 18 00 00 00    Ø   ÿ
00000032  00 00 78 0A 0B 00 74 12  00 00 74 12 00 00 00 00    x   t   t
00000048  00 00 00 00 00 00 00 09  8B 00 0B 8D 01 0D 91 01          ‹       '
00000064  0D 91 00 0B 8F 00 0A 8E  00 0C 90 04 10 94 00 0B   '      Ž      ”
00000080  91 00 0B 91 02 0E 94 07  13 99 08 14 9A 05 14 99   '   '   ”   ™   š   ™
00000096  07 16 9B 0B 1A 9F 05 12  96 04 11 95 0B 18 9C 16     ›   Ÿ   –   •   œ
00000112  23 A7 16 25 A9 0F 1E A2  0E 20 A3 16 29 AA 11 26  #§ %©   ¢   £ )ª &
00000128  A7 15 2B A9 24 3A B8 28  3E BC 1E 34 B1 1F 35 B2  § +©$:¸(>¼ 4± 5²
00000144  20 37 B1 12 2A A6 11 27  A8 0C 24 A6 09 1E A2 04   7± *¦ '¨ $¦   ¢
00000160  17 A0 08 1B A6 13 25 B2  10 20 AF 00 0E 9D 0B 19      ¦ %²  ¯
00000176  A8 09 17 A6 06 14 A3 03  11 A0 02 0F A1 01 0E A0  ¨   ¦   £       ¡
00000192  01 0D A1 02 0E A2 01 0D  A1 01 0D A1 01 0D A1 01    ¡   ¢   ¡   ¡   ¡
00000208  0D A1 00 0B A2 00 0A A1  00 07 A0 01 07 A0 01 06   ¡   ¢   ¡
00000224  9F 03 08 A1 03 08 A3 00  08 A2 00 07 A1 00 09 A3  Ÿ   ¡   £   ¢   ¡   £
00000240  02 0E A8 05 16 AD 0E 25  B7 0C 26 B6 45 60 F1 3A    ¨   -   %·  &¶E`ñ:
00000256  56 E3 01 21 A8 0C 2B B0  33 4D D7 60 7A FF 04 20  Vã !¨  +°3M×`zÿ
00000272  A3 03 22 9D 24 40 AF 4E  66 C0 52 61 A0 D3 DD FF  £  " $@¯NfÀRa ÓÝÿ
00000288  E6 F3 FF E3 F3 FF B0 C4  D5 B4 CA DC BB CE E3 BB  æóÿãóÿ°ÄÕ´ÊÜ»Îã»
00000304  CE E3 BA CD E2 BA CD E2  BA CD E2 B8 CB E0 BC CD  Îãºíâºíâºíâ¸Ëà¼Í
00000320  E2 BD CE E3 BE CF E2 BE  CF E2 BC CE DF B9 CB DC  â½Îã¾Ïâ¾Ïâ¼ÎßÊË
00000336  B5 C7 D8 B1 C5 D7 B7 CB  DD B8 CD E2 BD D1 E3 BE  µÇØ±Å×·ËÝ¸Íâ½Ñã¾
00000352  D2 E4 C2 D6 E7 C8 DC ED  CD E0 EF CC DF EE D1 E2  ÒäÂÖçÈÜíÍàïÌßîÑâ
00000368  EF D0 E1 EE CF E0 ED D0  E1 EE D4 E4 F1 D4 E4 F1  ïÐáîÏàíÐáîÔäñÔäñ
00000384  D3 E3 F0 D1 E1 EE D0 E0  ED D2 DF ED D2 DF ED D2  Óãð Ñáî Ðàí ÒßíÒßíÒ
00000400  DF ED D6 E1 EF DC E8 F4  E3 EF FB EB F5 FF F1 FB  ßíÖáïÜèôãïûëõÿñû
00000416  FF F2 FB FF F2 FB FF F1  FB FF F2 FA FF F1 FA FE  ÿòûÿòûÿñûÿòúÿñúþ
```

看我们这个有点相似，修改文件头为424D,
再继续修改后缀名，得到:



get flag：`flag{D0_n07_10se_y0ur_he4rt}`
500分的题目就到手了？？？

下面就是一些常见的文件头和文件尾，文件尾可能有点少咯！
常见的文件头：

文件类型	文件头
JPEG (jpg)	FFD8FFE1
PNG (png)	89504E47
GIF (gif)	47494638
TIFF (tif)	49492A00
Windows Bitmap (bmp)	424DC001
ZIP Archive (zip)	504B0304
RAR Archive (rar)	52617221
Adobe Photoshop (psd)	38425053
Rich Text Format (rtf)	7B5C727466
XML (xml)	3C3F786D6C
HTML (html)	68746D6C3E
Adobe Acrobat (pdf)	255044462D312E
Wave (wav)	57415645
pcap (pcap)	4D3C2B1A

常见的文件尾：
jpg 文件尾：FF D9
png 文件尾：AE 42 60 82
gif 文件尾：00 3B
zip 文件尾：50 4B