图片数据恢复--i春秋网鼎杯网络安全大赛clip题目writeup

原创

tdcoming 于 2018-08-21 21:12:43 发布 2467 收藏 1

分类专栏： CTF 文章标签： ctf 数据恢复

本文链接：https://blog.csdn.net/qq_29647709/article/details/81914699

> Horse Clip-Clop
> A strange filesystem is recovered from a damaged old hard disk.

翻译一下就是：

马夹

从损坏的旧硬盘中恢复一个奇怪的文件系统。

使用winhex打开，查看的时候发现png

```
00 38 61 AD 49 78 01 01  00 04 FF FB 89 50 4E 47  .8a-Ix....ÿû‰PNG
0D 0A 1A 0A 00 00 00 0D  49 48 44 52 00 00 03 4F  ........IHDR...O
00 00 00 2F 08 00 00 00  00 1E 49 AE 01 00 00 11  .../......I®....
12 49 44 41 54 78 01 EC  D3 31 01 00 00 08 04 A1  .IDATx.ìÓ1.....¡
EF 5F FA 2C E1 08 1D 58  5F 80 05 F8 04 3E 81 4F  ï_ú,á..X_€.ø.>.O
80 4F E0 13 F8 04 2C E0  F7 D3 B5 77 16 40 72 55  €Oà.ø.,à÷Óµw.@rU
4D 1B 7E D6 25 EE B6 1B  57 DC 1D 22 38 71 45 82  M.~Ö%î¶.WÜ."8qE‚
3B 31 DC DD DD DD 25 86  43 1C 77 77 48 70 8B BB  ;1ÜÝÝÝ%†C.wwHp‹»
6D D6 92 CC EE F4 FF 4D  CD A9 7B B8 95 EE 59 EE  mÖ'ÌîôÿMÍ©{¸•îYî
52 7F 7D 92 79 F0 AE 2E  FA 3D FD CE BB 73 EF 9D  R.}'yð®.ú=ýΠ»sï.
49 E5 DB 63 3B E5 E7 34  D9 7E CA ED C0 0A A9 0D  IåÛc;åç4Ù~ÊíÀ.©.
9F 0E 6F 9D C7 DD 22 09  62 CF 0E 6D 57 50 AF DB  Ÿ.o.ÇÝ".bÏ.mWP¯Û
E1 D3 AA C4 F1 38 F0 AB  28 28 BD 76 B5 FC BE FE  áÓªÄñ8ð«((½vµü¾þ
C5 05 05 C5 FD EE 2E 4D  D9 BB 80 4D B8 5D EF AD  Å..Åýî.MÙ»€M¸]ï-
19 5D 7C EA 21 CB 6F EE  5B 5C 27 B7 E5 9E 17 FC  .]|ê!Ëoî[\'·å•.ü
28 A9 A9 DA 03 6E AE 71  43 4B AF EB D5 2A B7 FE  (©©Ú.n®qCK¯ëÕ*·þ
76 63 3F 37 AA D1 4F 12  9D 5F 81 F1 11 FC 53 D4  vc?7ªÑO..._.ñ.üSÔ
```

然后通过搜索发现有两张这种图片。

首先提取出一张这样的图片：

开头：89504E47

结尾选择最后没有那么复杂数据的地方，也找不到文件结尾标志

```
00197350  B6 66 3C C3 EA 45 CF 33  F9 33 B6 86 4C F2 39 D1  ¶f<ÃêEI3ù3¶†Lò9Ñ
00197360  92 7C A4 50 E8 8D 66 E6  A5 9C 65 77 B8 7D 55 AA  ’|¤Pè.fæ¥œew¸}Uª
00197370  E6 C9 31 58 D9 EF 72 53  F9 77 38 32 32 A0 7E 9D  æÉ1XÙïrSùw822 ~.
00197380  C5 3C 16 BD FF 7B F7 78  5D 5A 72 F3 CE 8A 88 4F  Å<.½ÿ{÷x]ZróÎŠˆO
00197390  31 DC 12 02 96 FE EF 9C  43 57 5C 5F 26 B0 E0 83  1Ü..–þiœCW\_&°à‚
001973A0  A9 A0 BB 67 31 C3 BB 69  40 47 18 87 31 1C F0 B1  © »g1Ã»i@G.‡1.ð±
001973B0  F6 37 7B 7D 3C F5 71 C2  F3 FC A3 9F BD 0E A6 CD  ö7{}<õqÂóü£Ÿ½.¦Í
001973C0  59 6E F2 D2 66 AE 96 E7  84 8C 3F 95 6F FF AD FD  YnòÒf®–ç„Œ?•oÿ-ý
001973D0  BC 59 2A AF FE D5 6B A1  47 C7 17 77 15 99 1D B7  ¼Y*¯þÕk¡GÇ.w.™.·
001973E0  59 EA F9 5C 73 75 E0 F9  93 8F 1C 2E 2D F1 FC 3C  Yêù\suàù“...-ñü<
001973F0  FF FB EF DD CB 3D 27 3F  FB CF F0 F8 5F C6 93 AA  ÿûïÝË='?ûÏðø_Æ“ª
00197400  D2 C3 69 0C 40 E0 E9 EA  E7 B2 CE 29 A1 89 61 14  ÒÃi.@àéêç²Î)¡‰a.
00197410  8C 82 A1 06 00 B1 0D A2  2F 78 5E 63 60 18 05 A3  Œ‚¡..±.¢/x^c`..£
00197420  60 14 8C 54 00 00 04 00  00 01 78 5E 63 60 18 05  `.ŒT......x^c`..
00197430  A3 60 14 8C 54 00 00 04  00 00 01 78 5E 63 60 18  £`.ŒT......x^c`.
00197440  05 A3 60 14 8C 54 00 00  04 00 00 01 78 5E 63 60  .£`.ŒT......x^c`
00197450  18 05 A3 60 14 8C 54 00  00 04 00 00 01 78 5E 63  ..£`.ŒT......x^c
00197460  60 18 05 A3 60 14 8C 54  00 00 04 00 00 01 78 5E  `..£`.ŒT......x^
00197470  63 60 18 05 A3 60 14 8C  54 00 00 04 00 00 01 78  c`..£`.ŒT......x
```


提取出第一张图片1.png：

继续提取第二张，发现缺少头部，补全。

```
60 14 8C 54 00 00  04 00 00 01 78 5E 63 60  .£`.ŒT......x^c`
A3 60 14 8C 54 00  00 04 00 00 01 78 5E 63  ..£`.ŒT......x^c
05 A3 60 14 8C 54  00 00 04 00 00 01 78 01  `..£`.ŒT......x.
89 50 4E 47 0D 0A  1A 0A 00 00 00 0D 49 48  ..‰PNG........IH
00 00 03 4F 00 00  00 2F 08 00 00 00 00 1E  DR...O.../......
01 00 00 11 12 49  44 41 54 78 01 EC D3 31  I®.....IDATx.ìÓ1
00 08 04 A1 EF 5F  FA 2C E1 08 1D 58 5F 80  .....¡ï_ú,á..X_€
04 3E 81 4F 80 4F  E0 13 F8 04 2C E0 F7 D3  .ø.>.O€Oà.ø.,à÷Ó
16 40 72 55 4D 1B  7E D6 25 EE B6 1B 57 DC  µw.@rUM.~Ö%î¶.WÜ
38 71 45 82 3B 31  DC DD DD DD 25 86 43 1C  ."8qE‚;1ÜÝÝÝ%†C.
48 70 8B BB 6D D6  92 CC EE F4 FF 4D CD A9  wwHp‹»mÖ’ÌîôÿMÍ©
95 EE 59 EE 52 7F  7D 92 79 F0 AE 2E FA 3D  {¸•îYîR.}’yð®.ú=
BB 73 EF 9D 49 E5  DB 63 3B E5 E7 34 D9 7E  ýÎ»sï.IåÛc;åç4Ù~
C0 0A A9 0D 9F 0E  6F 9D C7 DD 22 09 62 CF  ÊíÀ.©.Ÿ.o.ÇÝ".bÏ
57 50 AF DB E1 D3  AA C4 F1 38 F0 AB 28 28  .mWP¯ÛáÓªÄñ8ð«((
B5 FC BE FE C5 05  05 C5 FD EE 2E 4D D9 BB  ½vµü¾þÅ..Åýî.MÙ»
B8 5D EF AD 19 5D  7C EA 21 CB 6F EE 5B 5C  ‡M¸]ï-.]|ê!Ëoî[\
E5 9E 17 FC 28 A9  A9 DA 03 6E AE 71 43 4B  '·å‹.ü(©©Ú.n®qCK
D5 2A B7 FE 76 63  3F 37 AA D1 4F 12 9D 5F  ¯ëÕ*·þvc?7ªÑO..‗
11 FC 53 D4 29 8B  89 EA 5F 59 26 E0 99 A6  .ñ.üSÔ)‹‰ê_Y&à™¦
6C 4E 04 97 34 BD  2B C8 6C B4 E7 93 F1 BF  Ël‹N.—4½+Èl´ç“ñ¿
42 2E 00 4C AF 75  9E 26 66 02 2E 4F DF 6F  æiB..L¯u‹&f..Oßo
```

和上面一样提权（也没有结尾标志）：

```
001999A0  B9 79 67 45 C4 A7 18 6E  09 01 4B FF 77 CE A1 2B  ¹ygEÄ§.n..KÿwÎ¡+
001999B0  AE 2F 13 58 F0 C1 54 D0  DD B3 98 E1 DD 34 A0 23  ®/.XðÁTÐÝ³˜áÝ4 #
001999C0  8C C3 18 0E F8 58 FB 9B  BD 3E 9E FA 38 E1 79 FE  ŒÃ..øXû›½>žú8áyþ
001999D0  D1 CF 5E 07 D3 E6 2C 37  79 69 33 57 CB 73 42 C6  ÑÏ^.Óæ,7yi3WËsBÆ
001999E0  9F CA B7 FF D6 7E DE 2C  95 57 FF EA B5 D0 A3 E3  ŸÊ·ÿÖ~Þ,•WÿêµÐ£ã
001999F0  8B BB 8A CC 8E DB 2C F5  7C AE B9 3A F0 FC C9 47  ‹»ŠÌŽÛ,õ|®¹:ðüÉG
00199A00  0E 97 96 78 7E 9E FF FD  F7 EE E5 9E 93 9F FD 67  .—–x~žÿý÷îåž“Ÿýg
00199A10  78 FC 2F E3 49 55 E9 E1  34 06 20 F0 74 F5 73 59  xü/ãIUéá4. ðtõsY
00199A20  E7 94 D0 C4 30 0A 46 C1  10 04 00 A4 D9 A1 33 78  ç”ÐÄ0.FÁ...¤Ù¡3x
00199A30  5E 63 60 18 05 A3 60 14  8C 54 00 00 04 00 00 01  ^c`..£`.ŒT......
00199A40  78 5E 63 60 18 05 A3 60  14 8C 54 00 00 04 00 00  x^c`..£`.ŒT.....
00199A50  01 78 5E 63 60 18 05 A3  60 14 8C 54 00 00 04 00  .x^c`..£`.ŒT....
00199A60  00 01 78 5E 63 60 18 05  A3 60 14 8C 54 00 00 04  ..x^c`..£`.ŒT...
00199A70  00 00 01 78 5E 63 60 18  05 A3 60 14 8C 54 00 00  ...x^c`..£`.ŒT..
00199A80  04 00 00 01 78 5E 63 60  18 05 A3 60 14 8C 54 00  ....x^c`..£`.ŒT.
00199A90  00 04 00 00 01 78 5E 63  60 18 05 A3 60 14 8C 54  .....x^c`..£`.ŒT
00199AA0  00 00 04 00 00 01 78 5E  63 60 18 05 A3 60 14 8C  ......x^c`..£`.Œ
00199AB0  54 00 00 04 00 00 01 78  5E 63 60 18 05 A3 60 14  T......x^c`..£`.
```


提取到2.png

接下来听说是分割两张图片，还原原来的flag,这个出题人的脑洞可以。