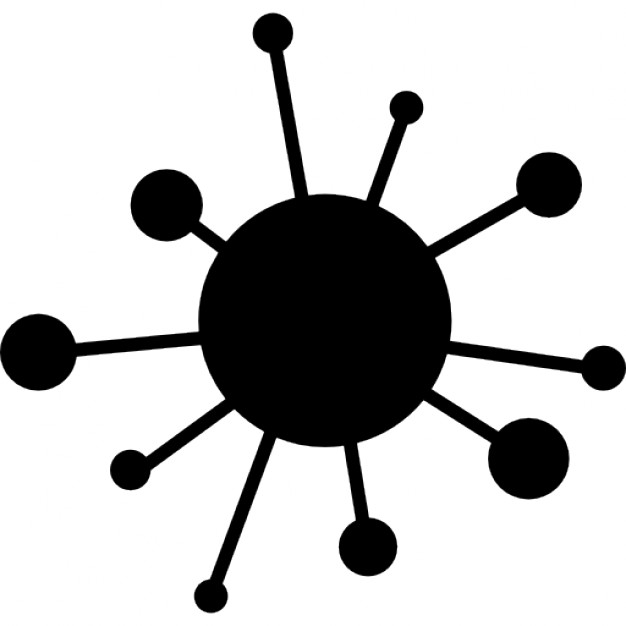
# 计算机病毒学

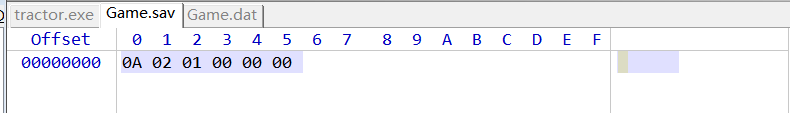
拖拉机游戏破解



学号：0x091395

姓名：uknowho

破解游戏存档



0位表示自己的牌

1位表示对方的牌

2位表示庄家

01：南为庄家

02：东为庄家

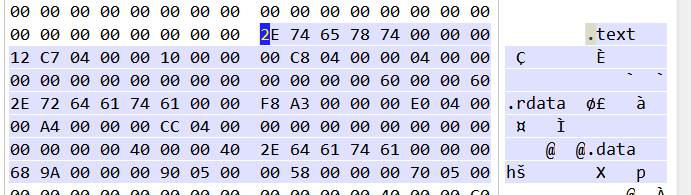
03：北为庄家

04：西为庄家



破解新开始游戏

PE文件段表：



文件想要读取.data数据区的内容初始化游戏。  
找到.data段在本文的偏移处：为00057000；

找到00057000处：

Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F

00057180 10 00 00 00 43 43 61 72 64 44 6F 63 00 00 00 00 CCardDoc

00057190 47 61 6D 65 2E 64 61 74 00 00 00 00 25 73 00 00 Game.dat %s

000571A0 44 6F 67 00 44 56 44 00 46 55 43 4B 45 4D 41 53 Dog DVD FUCKEMAS

000571B0 00 00 00 00 4B 47 42 00 5A 68 61 6E 67 20 46 65 KGB Zhang Fe

000571C0 6E 67 00 00 31 36 36 2E 31 31 31 2E 39 33 2E 38 ng 166.111.93.8

000571D0 00 00 00 00 43 4C 55 42 58 00 00 00 43 4C 55 42 CLUBX CLUB

000571E0 44 00 00 00 43 4C 55 42 55 00 00 00 44 49 41 4D D CLUBU DIAM

000571F0 4F 4E 44 58 00 00 00 00 44 49 41 4D 4F 4E 44 44 ONDX DIAMONDD

00057200 00 00 00 00 44 49 41 4D 4F 4E 44 55 00 00 00 00 DIAMONDU

00057210 48 45 41 52 54 58 00 00 48 45 41 52 54 44 00 00 HEARTX HEARTD

00057220 48 45 41 52 54 55 00 00 53 50 41 44 45 58 00 00 HEARTU SPADEX

00057230 53 50 41 44 45 44 00 00 53 50 41 44 45 55 00 00 SPADED SPADEU

00057240 4E 4F 54 52 55 4D 50 58 00 00 00 00 4E 4F 54 52 NOTRUMPX NOTR

00057250 55 4D 50 44 00 00 00 00 4E 4F 54 52 55 4D 50 55 UMPD NOTRUMPU

00057260 00 00 00 00 43 61 6E 74 20 6C 6F 61 64 20 70 6C Cant load pl

00057270 61 79 20 62 75 74 74 6F 6E 20 62 69 74 6D 61 70 ay button bitmap

00057280 00 00 00 00 43 61 6E 74 20 6C 6F 61 64 20 70 75 Cant load pu

00057290 74 20 62 75 74 74 6F 6E 20 62 69 74 6D 61 70 00 t button bitmap

000572A0 4D 69 64 69 20 65 72 72 6F 72 00 00 6A 64 66 61 Midi error jdfa

000572B0 6B 00 00 00 64 66 61 6B 64 00 00 00 25 73 00 00 k dfakd %s

000572C0 64 64 64 64 64 64 64 64 64 64 00 00 6B 64 66 00 dddddddddd kdf

000572D0 64 6A 66 00 64 64 64 64 64 64 64 64 64 64 00 00 djf dddddddddd

000572E0 64 6A 6B 66 61 73 6A 66 64 61 66 6A 66 6A 73 66 djkfasjfdafjfjsf

000572F0 61 00 00 00 47 65 74 55 70 2E 77 61 76 00 00 00 a GetUp.wav

00057300 47 65 74 44 6F 77 6E 2E 77 61 76 00 55 70 67 72 GetDown.wav Upgr

00057310 61 64 65 2E 77 61 76 00 42 65 55 70 67 72 61 64 ade.wav BeUpgrad

00057320 65 64 2E 77 61 76 00 00 27 64 66 61 00 00 00 00 ed.wav 'dfa

00057330 6B 64 66 00 25 64 00 00 6A 64 6A 00 6B 64 66 00 kdf %d jdj kdf

00057340 6A 64 66 61 6A 64 00 00 6B 64 66 61 6A 00 00 00 jdfajd kdfaj

00057350 66 75 63 6B 00 00 00 00 66 75 63 6B 00 00 00 00 fuck fuck

00057360 74 72 61 63 74 6F 72 2E 4D 49 44 00 72 72 72 00 tractor.MID rrr

00057370 72 72 00 00 64 00 00 00 64 64 64 64 64 64 64 64 rr d dddddddd

00057380 00 00 00 00 6B 64 6A 66 6B 00 00 00 64 66 6A 00 kdjfk dfj

00057390 64 6A 66 00 64 00 00 00 2C 66 00 00 64 66 00 00 djf d ,f df

000573A0 6B 64 6A 66 6B 00 00 00 64 66 6A 00 6B 64 6A 66 kdjfk dfj kdjf

000573B0 6B 00 00 00 64 66 6A 00 6B 64 6A 66 6B 00 00 00 k dfj kdjfk

000573C0 64 66 6A 00 6B 64 6A 66 6B 00 00 00 64 66 6A 00 dfj kdjfk dfj

000573D0 64 6A 61 00 64 6A 61 00 66 64 73 6A 66 73 61 64 dja dja fdsjfsad

000573E0 66 61 73 00 64 6A 66 00 64 00 00 00 2C 66 00 00 fas djf d ,f

000573F0 64 66 00 00 6B 64 6A 66 6B 00 00 00 64 66 6A 00 df kdjfk dfj

00057400 6B 64 6A 66 6B 00 00 00 64 66 6A 00 6B 64 6A 66 kdjfk dfj kdjf

00057410 6B 00 00 00 64 66 6A 00 43 43 61 72 64 56 69 65 k dfj CCardVie

00057420 77 00 00 00 45 72 72 6F 72 00 00 00 64 65 6C 65 w Error dele

00057430 74 65 20 62 6D 70 20 65 72 72 6F 72 00 00 00 00 te bmp error

00057440 45 72 72 6F 72 00 00 00 64 65 6C 65 74 65 20 62 Error delete b

00057450 6D 70 20 65 72 72 6F 72 00 00 00 00 45 72 72 6F mp error Erro

00057460 72 00 00 00 64 65 6C 65 74 65 20 62 6D 70 20 65 r delete bmp e

00057470 72 72 6F 72 00 00 00 00 45 72 72 6F 72 00 00 00 rror Error

00057480 4C 6F 61 64 20 62 69 74 6D 61 70 20 65 72 72 6F Load bitmap erro

00057490 72 20 20 61 61 61 61 61 61 61 00 00 45 72 72 6F r aaaaaaa Erro

000574A0 72 00 00 00 4C 6F 61 64 20 62 69 74 6D 61 70 20 r Load bitmap

000574B0 65 72 72 6F 72 20 20 61 61 61 61 61 61 61 00 00 error aaaaaaa

000574C0 45 72 72 6F 72 00 00 00 4C 6F 61 64 20 62 69 74 Error Load bit

000574D0 6D 61 70 20 65 72 72 6F 72 20 20 61 61 61 61 61 map error aaaaa

000574E0 61 61 00 00 45 72 72 6F 72 00 00 00 4C 6F 61 64 aa Error Load

000574F0 20 62 69 74 6D 61 70 20 65 72 72 6F 72 20 20 61 bitmap error a

00057500 61 61 61 61 61 61 00 00 4D 49 44 49 00 00 00 00 aaaaaa MIDI

00057510 B2 A5 B7 C5 4D 49 44 49 B3 F6 B4 ED 00 00 00 00 播放MIDI出错

00057520 4D 49 44 49 00 00 00 00 B2 A5 B7 C5 4D 49 44 49 MIDI 播放MIDI

00057530 B3 F6 B4 ED 00 00 00 00 00 00 00 00 01 00 00 00 出错

00057540 02 00 00 00 03 00 00 00 10 00 00 00 43 44 65 61 CDea

00057550 6C 65 72 00 6B 64 6A 66 61 6A 64 73 66 00 00 00 ler kdjfajdsf

00057560 6B 64 61 61 61 61 00 00 6B 64 6A 66 61 6A 64 73 kdaaaa kdjfajds

00057570 66 00 00 00 6B 64 62 62 62 62 00 00 6A 64 66 00 f kdbbbb jdf

00057580 64 6A 66 61 6B 73 64 66 6A 00 00 00 6A 64 66 64 djfaksdfj jdfd

00057590 66 00 00 00 6A 66 66 6A 00 00 00 00 6B 6A 64 66 f jffj kjdf

000575A0 61 6A 66 64 00 00 00 00 64 6A 66 66 64 61 64 00 ajfd djffdad

000575B0 6A 64 66 61 6B 6A 64 66 00 00 00 00 6A 64 64 6A jdfakjdf jddj

000575C0 64 64 00 00 45 72 72 6F 72 00 00 00 4C 6F 61 64 dd Error Load

000575D0 20 42 6D 70 20 65 72 72 6F 72 00 00 6A 64 64 6A Bmp error jddj

000575E0 64 64 00 00 7C 00 00 00 7C 00 00 00 7C 00 00 00 dd | | |

000575F0 7C 00 00 00 7C 00 00 00 7C 00 00 00 7C 00 00 00 | | | |

00057600 00 00 00 00 01 E7 00 00 02 E7 00 00 03 E7 00 00 ? ? ?

00057610 43 4D 61 69 6E 46 72 61 6D 65 00 00 BE AF B8 E6 CMainFrame 警告

00057620 00 00 00 00 BD E1 CA F8 B5 B1 C7 B0 D3 CE CF B7 结束当前游戏

00057630 C2 F0 A3 BF 00 00 00 00 20 59 6F 75 20 00 00 00 吗？ You

00057640 25 73 25 64 00 00 00 00 20 57 65 73 74 20 00 00 %s%d West

00057650 25 73 25 64 00 00 00 00 20 45 61 73 74 20 00 00 %s%d East

00057660 25 73 25 64 00 00 00 00 20 4E 6F 72 74 68 20 00 %s%d North

00057670 25 73 25 64 00 00 00 00 20 55 6E 6B 6E 6F 77 20 %s%d Unknow

00057680 00 00 00 00 25 73 25 64 00 00 00 00 47 61 6D 65 %s%d Game

00057690 2E 73 61 76 00 00 00 00 25 73 00 00 47 61 6D 65 .sav %s Game

000576A0 2E 73 61 76 00 00 00 00 25 73 00 00 6B 64 6A 6B .sav %s kdjk

000576B0 66 6A 64 61 66 6A 00 00 6A 64 66 61 6B 6A 64 66 fjdafj jdfakjdf

000576C0 00 00 00 00 47 61 6D 65 2E 73 61 76 00 00 00 00 Game.sav

000576D0 25 73 00 00 4D 69 64 69 20 65 72 72 6F 72 00 00 %s Midi error

000576E0 54 72 61 63 74 6F 72 2E 68 6C 70 00 64 6A 66 00 Tractor.hlp djf

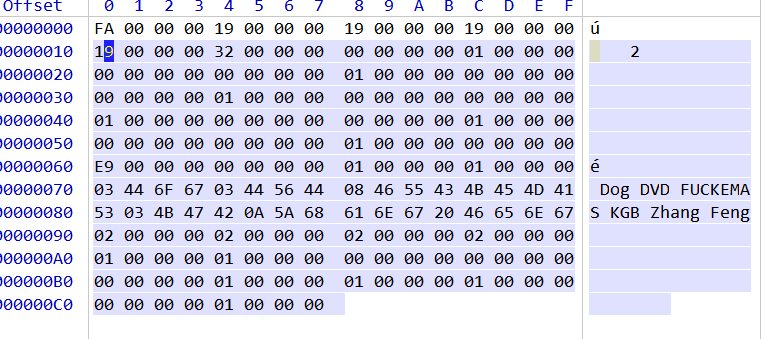
000576F0 6B 64 00 00 63 50 6C 61 79 4C 69 73 74 00 00 00 kd cPlayList

00057700 63 53 63 6F 72 65 4C 69 73 74 00 00 BE AF B8 E6 cScoreList 警告

00057710 00 00 00 00 BF AA CA BC D0 C2 D3 CE CF B7 C2 F0 开始新游戏吗

发现游戏好像读取了Game.dat文件的内容

尝试修改Game.dat内容后发现没效果



遂，失败。