unknownproject Быстрый анализ игрового датафайла сентября 21, 2016 Хуй знает, что меня побудило на написание этой статьи. Ни для кого не секрет, что во многих играх используются кастомные бинарные форматы для хранения множества файлов в первичном или сжатом виде.Естественно, что во время загрузки любой игры из этих бинарных файлов происходит считывание и выгрузка в оперативную память всего необходимого. Но как быть, если файл неизвестного формата настолько, что в нем нельзя найти ни ТОС, ни форматные сигнатуры ни в начале, ни в конце? А очень просто. Любой зашифрованный или сжатый файл проходит предварительную расшифровку/разжатие в оперативной памяти. Это происходит благодаря вызовам определенного числа функций в самом исполняемом файле или игровом скрипте, но мы не будет реверсить исполняемый файл.Достаточно будет анализа бинарного формата в конкретном случае. <u>Возьмем демоверсию игры "X - Beyond The Frontier", вышедшей в свет в далеком 1999 году.</u> Дропнем в мой любимый hex-редактор файл **01.DAT** 0000000A0 33 22 3B 33 73 33 73 30 32 11 33 31 22 32 30 22 3":353502 31"20" 000000B0 32 CC F7 33 2C 33 33 32 36 32 32 32 32 32 33 2M43,33262222223 000000D0 39 38 CC F7 33 86 23 33 31 32 30 30 31 37 30 36 98M43##312001706 0000000E0 36 37 37 33 33 32 4E 32 31 30 33 37 22 36 21 12 677332N21037"6! 000000F0 02 72 35 20 62 52 34 11 42 27 01 B2 A2 92 3B 10 r5 bR4 B' Iğ'; 00000110 28 2A 29 16 15 14 18 1A 19 07 06 05 04 08 0A 09 +*) 00000120 70 77 76 75 74 78 7A 79 60 67 66 65 64 68 6A 69 pwvut{zy`gfedkji 888898138 | 50 57 56 55 54 58 5A 59 40 47 46 45 44 48 4A 49 | PWUUT[ZY@ĞFEDKJI | 坐資際職績 80000140 B0 B7 B6 B5 B4 BB BA B9 A1 A0 A7 A6 A5 A4 AB AA ° ¶μτ'»εΝΫ §¦Γ≭«ε ଅଞ୍≘∄∦Ђ∭ 88880150 A9 91 98 97 96 95 94 9B 9A 99 81 86 87 86 85 84 ◎ h---">₼" Тま‡..., 酵腸血液 99990160 8B 8A 89 F1 F0 F7 F6 F5 F4 FB FA F9 E1 E0 E7 E6 «Масрчихомыщемаж въбыть в 888888178 E5 E4 EB EA E9 D2 D1 D0 D7 D6 D5 D4 DB DA D9 C2 | едлкиТСРЧЦХФЫЪЩВ БЪТЕТЕТЬ 99999189 С1 С9 С7 С6 С5 С4 СВ СА С9 СС F7 33 2C 32 33 39 БАЗЖЕДЛКИМЧЗ.239 營業報酬2/40/1/2 88889148 | 31 38 37 <mark>36</mark> 35 34 38 34 39 38 CC F7 33 86 22 33 | 187654··98Mu3±"3 | File Properties Size: 12,778,337 bytes][SPARSE UNCHANGED OVERWRIT Сразу же можно заметить, что в файле есть повторяющиеся байты, такие как **32h** и менее встречающиеся **33h**. Практика показывает, что игровые разработчики не особо запариваются с шифрованием, поэтому перед нами с вероятностью 80% битовая операция XOR, которая встречается довольно часто в различных игровых форматах и не только.

Проверим.Выделим все байты с помощью **Ctrl+A** и обратимся к меню **Edit**, а затем выберем **Operation -> Bitwise...** <u>File Stream Edit Search Navigate View Tools Window Help</u>

3233МиЗр32222222

00000010 33 32 33 33 CC E8 33 70 33 32 32 32 32 32 32 32

<u>File Stream Edit Search Navigate View Tools Window Help</u>

01.DAT File2

99999919 99 48 99 99 FF DB 99 43 99 98 96 96 97 96 95 98 00000020 07 07 07 09 09 08 0A 0C 14 0D 0C 0B 0B 0C 19 12

00000030 13 0F 14 1D 1A 1F 1E 1D 1A 1C 1C 20 24 2E 27 20

000000000 09 0C 0B 0C 18 0D 0D 18 32 21 1C 21 32 32 32 32

000000000 00 11 08 04 00 02 FC 03 01 22 00 02 11 01 03 11 990000B0 01 FF C4 00 1F 00 00 01 05 01 01 01 01 01 01 00 9Д 000000C0 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09

00000010 00 01 00 00 FF DB 00 43 00 01 01 01 01 01 01 01

00000050 01 01 01 01 01 01 01 01 FF DB 00 43 01 01 01

000000000 00 11 08 00 40 00 40 03 01 22 00 02 11 01 03 11

000000B0 01 FF C4 00 1F 00 00 01 05 01 01 01 01 01 01 00

000000C0 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09

именно в этом месте:

88888888 FF D8 FF E8 88 18 4A 46 49 46 88 81 81 81 88 48 RMRa JFIF

00000040 22 2C 23 1C 1C 28 37 29 2C 30 31 34 34 34 1F 27 ",# (7),01444 00000050 39 3D 38 32 3C 2E 33 34 32 FF DB 00 43 01 09 09 9=82<.3429Ы C

22222222222222 00000050 32 32 32 32 32 32 32 32 32 CC E8 33 70 32 32 32 22222222222222 222222222222222 222222222222222 33 22 3B 33 73 33 73 30 32 11 33 31 22 32 30 22 3";3s3s02 31"20<mark>"</mark> 32 CC F7 33 2C 33 33 32 36 32 32 32 32 32 32 32 33 2M43,33262222223 33333332107654;: 33 33 33 33 33 33 33 32 31 30 37 36 35 34 3B 3A 39 38 CC F7 33 86 23 33 31 32 30 30 31 37 30 36 98M43**‡#**312001706 類 類 類 列 ○ ● 類 36 37 37 33 33 32 4E 32 31 30 33 37 22 36 21 12 677332N21037"6 * 02 72 35 20 62 52 34 11 42 27 01 B2 A2 92 3B 10 71 82 F2 26 61 E2 C3 17 00 51 41 B1 3A 39 25 24 r5 bR4 B' Iğ'; **腹**睑 (毒性 q,т&авГ QA±:9%\$ 2B 2A 29 16 15 14 1B 1A 19 07 06 05 04 0B 0A 09 70 77 76 75 74 78 7A 79 60 67 66 65 64 68 6A 69 50 57 56 55 54 58 5A 59 40 47 46 45 44 48 4A 49 B0 B7 B6 B5 B4 BB BA B9 A1 A0 A7 A6 A5 A4 AB AA pwvut{zy`gfedkji PWVUT[ZY@GFEDKJI A9 91 90 97 96 95 94 9B 9A 99 81 80 87 86 85 84 ົງ`ຖ−-•″>љ™ٌ<mark>`</mark>†‡‡...,, 醋锡鱼 8B 8A 89 F1 F0 F7 F6 F5 F4 FB FA F9 E1 E0 E7 E6 त्त्र∰छ्त्वत्रह кЉ‰срчцхфыъщбазж едики́ТСРЧЦХФЫЪШВ E5 E4 EB EA E9 D2 D1 D0 D7 D6 D5 D4 DB DA D9 C2 다동말단홋뀕튭슾 C1 C0 C7 C6 C5 C4 CB CA C9 CC F7 33 2C 32 33 30 File Propertie Selected: 12,778,337 bytes][SPARSE UNCHANGED OVERWRITE Perform a bitwise (logical) operation.

Bitwise Operation X Operation: XOR (Exclusive OR) Second Operand: Hex Bytes

В появившемся окне из списка **Operation** выбираем **XOR,** а в качестве второго операнда во втором списке

выбираем Hex Bytes.

В нижнее поле введем 32 в качестве проверки того, что мы получим на выходе. Это и будет нашим вторым

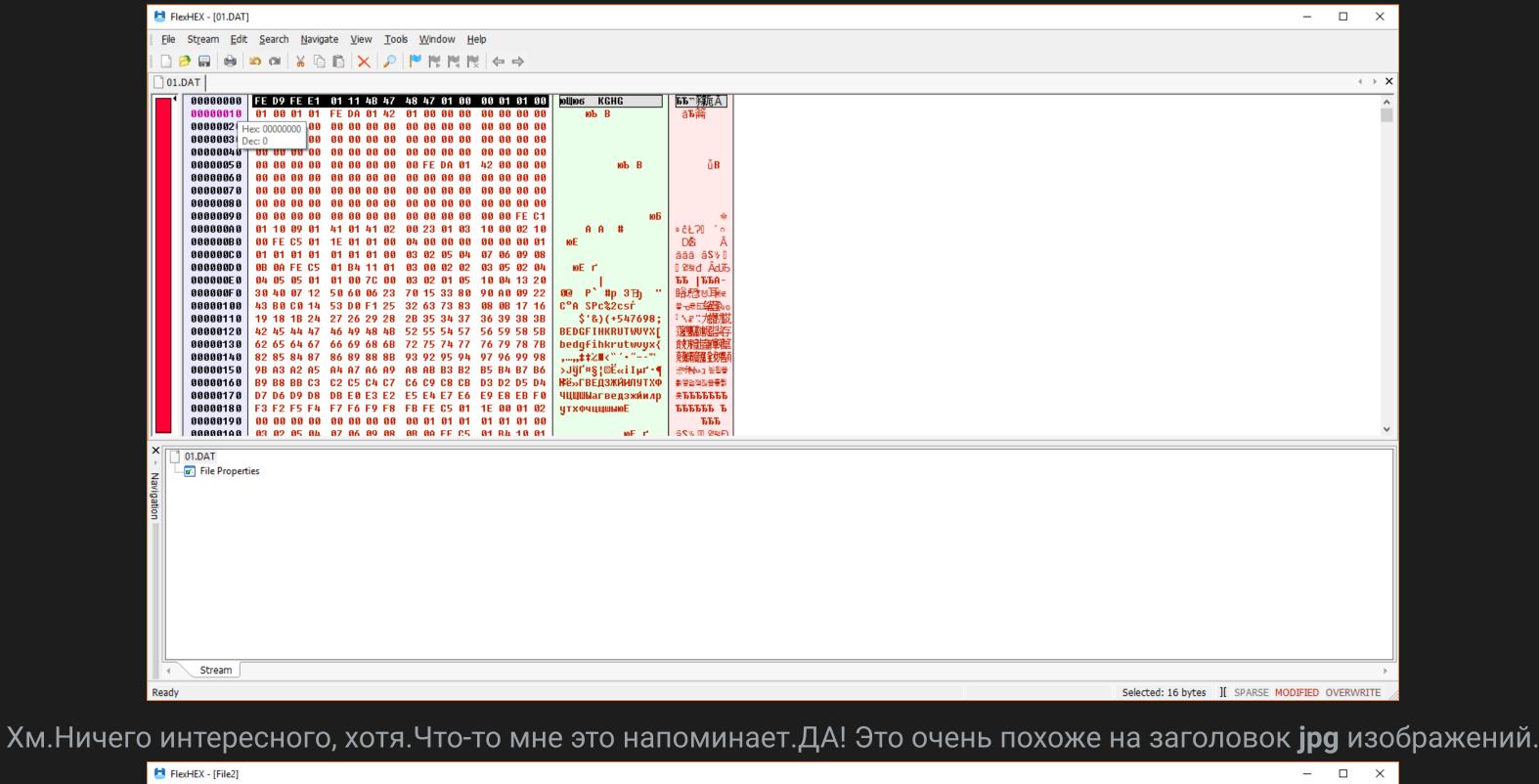
операндом.

X Cancel

Поксорили...

Help

OK



00000120 43 44 45 46 47 48 49 4A 53 54 55 56 57 58 59 5A CDEFGHIJSTUUWXYZ 膝鞭血試験的 8888138 | 63 64 65 66 67 68 69 69 73 74 75 76 77 78 79 78 | cdefahijstuuwxuz | 披珠洋源 00000140 83 84 85 86 87 88 89 8A 92 93 94 95 96 97 98 99 f,,...‡\$#≈\h'""*--00000150 | 9A A2 A3 A4 A5 A6 A7 A8 A9 AA B2 B3 B4 B5 B6 B7 | AğJ≍Ґ¦ŞЁ©€ІІҐµ¶• 88888168 В8 В9 ВА С2 С3 С4 С5 С6 С7 С8 С9 СА D2 D3 D4 D5 ЁЙ€ВГДЁЖЗИЙКТУФХ 98989179 D6 D7 D8 D9 DA E1 E2 E3 E4 E5 E6 E7 E8 E9 EA F1 ЦЧШБ6ВГДЕЖЗИЙКС ... БЪБЪБЪБЪ

್ತ [ఊഒൗ&ಬುರ್

." احتا06÷

)協)(RÚN3

2 ! !2222 ക്യോഘ ച ഉത്

```
00000000 0A 0B FF C4 00 B5 10 00 02 01 03 03 02 04 03 05
                      000000E0 05 04 04 00 00 01 7D 01 02 03 00 04 11 05 12 21
                      666666F6 31 41 66 13 51 61 97 22 71 14 32 81 91 A1 68 23 1A 0a "g 2f 'ğ # 練傷。脲「
                     00000100 42 B1 C1 15 52 D1 F0 24 33 62 72 82 09 0A 16 17 B±6 RCp$3br,
                                                                                AVE OF ES
                      00000110 | 18 19 1A 25 26 27 28 29 2A 34 35 36 37 38 39 3A | %&'()*456789: | 💵 +×英柳銈
                     00000180 F2 F3 F4 F5 F6 F7 F8 F9 FA FF C4 00 1F 01 00 03 ТуфхцчшцьяД
                                                                                ъъъ笠 Äğ`
                     88888148 82 83 84 85 86 87 88 89 84 88 FF C4 88 R5 11 88
                                                                                ಇ ಕೊಳ್ಳ
                        File Properties
                          Stream
                                                                                                                                          Selected: 16 bytes | SPARSE MODIFIED OVERWRITE
Значит это действительно XOR и на этот раз вторым операндом у нас будет 33.
Жмем Ctrl+Z для отмены предыдущей операции и выполняем XOR повторно с новым операндом.
Получаем на выходе следующее:
                     FlexHEX
                                                                                                                                                               _ _
                     <u>F</u>ile St<u>r</u>eam <u>E</u>dit <u>S</u>earch <u>N</u>avigate <u>V</u>iew <u>T</u>ools <u>W</u>indow <u>H</u>elp
                     01.DAT
                                                                                    <mark>1515</mark>∞滯騰 Ā
Ā 154稱āāā
                         00000000 FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01 яшяа JFIF
```

000000E0 05 04 04 00 00 01 7D 01 02 03 00 04 11 05 12 21 8888888F8 31 41 86 13 51 61 87 22 71 14 32 81 91 A1 88 23 1A Qa "q 2f`ў # 稼働J駅T 00000100 42 B1 C1 15 52 D1 F0 24 33 62 72 82 09 0A 16 17 B±6 RCp\$3br, 88888118 | 18 19 1A 25 26 27 28 29 2A 34 35 36 37 38 39 3A | %&'()*456789: 00000130 63 64 65 66 67 68 69 6A 73 74 75 76 77 78 79 7A cdefghijstuvwxyz 00000140 83 84 85 86 87 88 89 8A 92 93 94 95 96 97 98 99 fy....‡‡≣⊘h'""•-- ™ 00000170 D6 D7 D8 D9 DA E1 E2 E3 E4 E5 E6 E7 E8 E9 EA F1 ЦЧШЦЬбВГДЕЖЗИЙКС Tadadad_{ee} 88000180 F2 F3 F4 F5 F6 F7 F8 F9 FA FF C4 00 1F 01 00 03 ТУФХЦЧШЦЬЯД न ननन

स्टब्स्टब्स्टब्स्

त्रत्रत्रत्रत्रत

स्टब्स्टब्स्टब्स्

स्टब्स्टब्स्टब्स्

स्टब्स्टब्स्टब्स्

बबबबबबब

aaaaaaa≅

@tÃđ°

lÄ Āaāā Ā 3√ई

```
File Properties
                   Пролистаем файл в самый низ, чтобы убедиться в том, что он полностью расшифрован.
                   <u>File Stream Edit Search Navigate View Tools Window Help</u>
                   00C2F9F0 30 30 30 3B 32 30 30 30 3B 20 77 77 77 2E 54 48 000;2000; www.TH ~央冷・腱車
                      80C2FA88 51 2E 64 65 3B 8D 8A 39 31 36 3B 20 31 30 30 30 Q.de; 916; 1800 1颗性令
                      00C2FA10 3B 31 30 30 30 3B 20 53 55 52 52 4F 55 4E 44 20 ;1000; SURROUND
                      00C2FA20 | 53 4F 55 4E 44 3B 0D 0A 39 31 36 3B 20 33 30 30 | SOUND; 916; 300 |
                      00C2FA60 50 49 54 3B 0D 0A 39 32 31 3B 20 35 30 30 3B 35 PIT; 921; 500;5 整形
                      00C2FA70 30 30 38 20 4D 4F 52 45 20 49 4E 46 4F 38 0D 0A 00; MORE INFO;
                      00C2FA80 39 32 31 3B 20 31 35 30 30 3B 32 35 30 30 3B 20 921; 1500;2500;
                      80C2FA98 77 77 77 2E 65 67 6F 73 6F 66 74 2E 64 65 3B 0D www.egosoft.de;
                      00C2FAA0 0A 39 31 38 3B 20 33 30 30 3B 37 30 30 3B 20 20 918; 300;700;
                      00C2FAB0 54 52 41 44 45 38 0D 0A 39 31 38 3B 20 31 35 30 TRADE; 918; 150 湯田=版公
                      80C2FAC0 | 30 3B 37 30 30 3B 20 46 49 47 48 54 3B 0D 0A 39 | 0;700; FIGHT; 9 | 鬼)處理
                      00C2FAD0 31 38 38 20 32 38 30 30 38 37 30 30 38 20 42 55 18; 2800;700; BU
                      00C2FAE0 49 4C 44 3B 0D 0A 39 31 38 3B 20 34 30 30 30 3B ILD; 918; 4000; 
00C2FAF0 37 30 30 3B 20 54 48 49 4E 4B 3B 0D 0A 39 31 39 700; THINK; 919 X無嫌業性
                      80C2FB00 3B 20 31 30 30 30 3B 31 35 30 30 3B 20 58 2D 42 ; 1000;1500; X-B | ※← √地
                      88C2FB18 65 79 6F 6E 64 20 74 68 65 20 46 72 6F 6E 74 69 eyond the Fronti 祥揚桴牆縣
                      00C2FB20 | 65 72 3B 0D 0A 39 32 31 3B 20 35 30 30 3B 35 30 | er; 921; 500;50 |
                      88C2FB38 38 38 20 4D 4F 52 45 28 49 4E 46 4F 3B 8D 8A 39 8; MORE INFO; 9 興和义臣
                             32 31 38 20 31 35 30 30 38 32 35 30 30 38 20 77 21; 1500;2500; w
                      00C2FB50 77 77 2E 65 67 6F 73 6F 66 74 2E 64 65 3B 0D 0A ww.egosoft.de;
                      00C2FB70
                     File Properties
                                                                                                                        Size: 12,778,337 bytes | SPARSE MODIFIED OVERWRITE
Все ок.Но возникла проблема номер два.Как определить границы файлов?
Рядом с вышеописанным файлом лежит 01.САТ, который, судя по его названию, представляет из себя
специфичный заголовок и ТОС, а из-за своего малого размера вполне подходит для хранения данных о
файловой таблице имен и смещений.
И он тоже зашифрован, но уже по другому алгоритму.В детали поиска я вдаваться не буду, могу только
дополнить, что код расшифровки выполняется после вызова стандартных функций для работы с файлами, а
```

```
Краткая суть алгоритма:
    . Берем первый байт ;
     Берем ключ расшифровки = DBh ;
     Ксорим его с первым байтом ;
     Увеличиваем (получаем DCh);
```

Ксорим второй байт с увеличенным значением ;

Повторяем с первого шага, переходя к следующей паре байт.

Снова увеличиваем (получаем **DDh**);

На делфи получился бы примерно такой код цикла:

```
Где:
   1. DataFile: File of byte;
   2. IncXor,readbuf1,writebuf1,writebuf2,readbuf2,i,count,offset,Fsize:integer;
      Переменной IncXor присвоено начальное значение = $DB;
После расшифровки файл выглядит следующим образом:
               FlexHEX - [01.CAT]
                                                                                                                          <u>File Stream Edit Search Navigate View Tools Window Help</u>
                       01.CAT
                | 00000000 | 30 31 2E 64 61 74 0A 74 65 78 2F 74 72 75 65 2F | 01.dat tex/true/ | 1 探晰論語
                00000010 31 30 30 2E 6A 70 67 20 33 36 30 35 0A 74 65 78 100.jpg 3605 tex
                00000020 | 2F 74 72 75 65 2F 31 30 31 2E 6A 70 67 20 33 34 | /true/101.jpg 34 | 瑞融 激初
```

碳重 章

玻璃小灘駅

00000030 | 36 36 0A 74 65 78 2F 74 72 75 65 2F 31 30 32 2E | 66 tex/true/102. | 00000040 | 6A 70 67 20 33 32 31 34 0A 74 65 78 2F 74 72 75 | jpg 3214 tex/tru |

00000060 | 65 78 2F 74 72 75 65 2F 31 30 34 2E 6A 70 67 20 | ex/true/104.jpg

00000080 35 2E 6A 70 67 20 32 39 30 38 0A 74 65 78 2F 74 5.jpg 2908 tex/t

000000000 OA 74 65 78 2F 74 72 75 65 2F 31 30 37 2E 6A 70 tex/true/107.jp 000000B0 | 67 20 32 37 31 38 0A 74 65 78 2F 74 72 75 65 2F | q 2718 tex/true/ 000000C0 31 30 38 2E 6A 70 67 20 32 37 31 33 0A 74 65 78 108.jpg 2713 tex | 000000D0 | 2F 74 72 75 65 2F 31 30 39 2E 6A 70 67 20 32 36 | /true/109.jpg 26 |

000000E0 38 36 0A 74 65 78 2F 74 72 75 65 2F 31 31 30 2E 86 tex/true/110.

00000DC0 47 20 0E 70 0F 38 CE 7B 8C 7B F1 52 07 48 B0 63

99999DD9 19 70 0F EF 0E 55 B9 07 23 6E 4A AE 06 57 39 25

00000DE0 87 6E 78 80 9C 9F D7 F3 FC 05 78 58 9C 44 F1 35 65 56 6F 56 F4 4B 64 B4 B6 BD 5F 46 ED D1 6A D5

999996E99 AD EA D1 A5 1A 30 50 82 B2 4B AE ED FE 8B B2 E8

00000E20 01 01 00 00 01 00 01 00 00 FF DB 00 43 00 01 01

File Properties

B4 B2 B1 FF D9 FF D8 FF E0 00 10 4A 46 49 46 00

00000050 | 65 2F 31 30 33 2E 6A 70 67 20 33 30 38 38 0A 74 | e/103.jpg 3088 t | 田中澤州郷

00000070 32 39 39 36 0A 74 65 78 2F 74 72 75 65 2F 31 30 2996 tex/true/10 次統論

00000090 72 75 65 2F 31 30 36 2E 6A 70 67 20 32 38 31 36 | rue/106.jpg 2816 | 翻車 灘岬

00000100 | 65 2F 31 31 31 2E 6A 70 67 20 34 30 33 37 0A 74 | e/111.jpg 4037 t | 田 灣沙娜 00000110 65 78 2F 74 72 75 65 2F 31 31 32 2E 6A 70 67 20 ex/true/112.jpg | 碳酸計 灪 00000120 34 30 33 38 0A 74 65 78 2F 74 72 75 65 2F 31 31 4038 tex/true/11 /部版語中 - 00000130 | 33 2E 6A 70 67 20 33 39 36 38 0A 74 65 78 2F 74 | 3.jpg 3968 tex/t | □ ※抽締館 00000140 72 75 65 2F 31 31 34 2E 6A 70 67 20 33 37 39 35 rue/114.jpg 3795 電力 薄減 00000150 | 0A 74 65 78 2F 74 72 75 65 2F 31 31 35 2E 6A 70 | tex/true/115.jp | 珊瑚山 灣 00000160 67 20 33 37 37 33 0A 74 65 78 2F 74 72 75 65 2F q 3773 tex/true/ 原際環境部 のののの17の 31 31 36 2F 6A 7の 67 2の 33 37 32 35 のA 74 65 78 116 ing 3725 tex □ 1 激動動脈状

```
× 01.CAT
                  --- 🚾 File Properties
                    Stream
                                                                                               Size: 25,421 bytes | SPARSE READ-ONLY OVERWRITE
   Первые шесть байт - внутреннее имя.Вполне вероятно, что таким образом проверяется валидность.Седьмой
                                                 байт - символ завершения строки.
     Далее отчетливо видны имена файлов с полными путями и их размеры, представленными в виде строк.
В завершении отмечу, что файлы в 01.DAT слеплены, а значит смещение нужно высчитывать от размера предыдущего.
                                                                                                        - 🗆 X
    <u>File Stream Edit Search Navigate View Tools Window Help</u>
           01.DAT
       88888878 4A CE ED 38 F2 A4 ED CB D9 5D 34 CC E9 65 18 51
       000000080 7E D2 6F 9F 99 35 CA 97 2D AD 16 D3 5D 5F 35 D5
       808880098 EE B4 E8 CF 46 F1 CF 8D EE 3C 4C 6D ED 3C B8 D2
       8888888888 38 40 88 66 88 90 03 9F 29 23 25 8F DE 7D DB 77
       00000DB0 16 62 58 E4 28 DA AA 10 79 E0 C0 42 0E 37 31 1D
                                                              感 あるよう
```

27. 萬華遊風服

鸂唎漥圆

БΥ 騰湯

ե եենե

व्यवव्यव्यव्य *व*दवदवदवद *व्यव्यव्यव्यव्य व्यव्यव्यव्यव* **釉**aaaaaa *व्यवववववव व्यव्यव्यव्यव व्यव्यव्यव्य* ā 🕍 🊟 '' ∟″đ≋ά dā ππ π¢

G р 80{Њ{cR H°c

‡nхЂыџЧуь хХыDс5 eVoVoKdr¶S_FHCjX

Stream Selected: 3,605 bytes][SPARSE UNCHANGED OVERWRITE На этом мутная хуйня закончилась.