```
Quick analysis of the game data file
September 21, 2016
                                                         Fuck knows what prompted me to write this article.
 It's no secret that many games use custom binary formats to store many files in their primary or compressed form. Naturally, during loading of any game,
                                             everything necessary from these binaries is read and unloaded into RAM.
 But what if the file of an unknown format is so much that neither TOC nor formatted signatures can be found in it either at the beginning or at the end?
                                                                              It's very simple.
 Any encrypted or compressed file undergoes preliminary decryption / decompression in RAM. This happens due to calls of a certain number of functions
 in the executable file or game script itself, but we will not reverse the executable file. It will be enough to analyze the binary format in a particular case.
                                           Take the demo version of X - Beyond The Frontier, released back in 1999.
                                                             Dropnem my favorite hex-editor file 01.DAT
                             | 🗠 🎮 | 🐰 🖺 | 🗙 | 🔑 | 🏲 🙌 🖂 🙀 | 🧇 🔿
                       | 00000010 | 33 32 33 33 CC E8 33 70 33 32 32 32 32 32 32 32 33 | 3233Mu3p32222222 | | 行き運動制
                       000000000 33 22 3B 33 73 33 73 30 32 11 33 31 22 32 30 22 3";353502 31"20"
                       0000000B0 32 CC F7 33 2C 33 33 32 36 32 32 32 32 32 32 33 2M43,33262222223
                       000000C0 33 33 33 33 33 33 32 31 30 37 36 35 34 3B 3A 33333332107654;:
                       8800000E0 36 37 37 33 33 32 4E 32 31 30 33 37 22 36 21 12 677332N21037"6! 嬢地(駅)
                       000000F0 02 72 35 20 62 52 34 11 42 27 01 B2 A2 92 3B 10 r5 bR4 B' Iğ'; 奥孙⊶録
                       00000100 71 82 F2 26 61 E2 C3 17 00 51 41 B1 3A 39 25 24 | q,т&авГ QA±:9%$ |
                       00000120 70 77 76 75 74 7B 7A 79 60 67 66 65 64 6B 6A 69 pwvut{zy`gfedkji
                       88888158 A9 91 98 97 96 95 94 9B 9A 99 81 88 87 86 85 84 © h---">ь"" ⊞‡‡...,
                       88 88 89 F1 F0 F7 F6 F5 F4 FB FA F9 E1 E0 E7 E6 <16сстрчцхфыъщбазж
                       88888 178 | E5 E4 E8 EA E9 D2 D1 D8 D7 D6 D5 D4 D8 DA D9 C2 | едлю́ТСРЧЦХФЫБЩВ
                       80000180 С1 С0 С7 С6 С5 С4 СВ СА С9 СС F7 33 2С 32 33 30 БАЗЖЕДЛКИМч3,230 營業報費2分計
                       88888148 31 38 37 36 35 34 38 39 39 38 CC F7 33 86 22 33 187654:・98Mu3±**3 (竹藤原葉)
                      File Properties
                                                                                                                          Size: 12,778,337 bytes | SPARSE UNCHANGED OVERWRITE
                   You can immediately notice that there are duplicate bytes in the file, such as 32h and less common 33h.
                 Practice shows that game developers are not particularly
                    bothered with encryption, so we have before us with a
         probability of 80% a bit XOR operation, which is quite common
                                        in various game formats and not only.
                               Let's check, select all the bytes with Ctrl + A and go to the Edit menu and then select
                                                                       Operation -> Bitwise ...
                   FlexHEX - [01.DAT]
                                                                                                                                                _ _
                    <u>File Stream Edit Search Navigate View Tools Window Help</u>
                    01.DAT
                                                                3233Ми3р32222222
                              33 32 33 33 CC E8 33 70 33 32 32 32 32 32 32 32 32
                                                                22222222222222
                                                                222222222МиЗр222
                                                                222222222222222
                              222222222222Mu
                                                                3";3s3s02 31"20"
                              32 CC F7 33 2C 33 33 32 36 32 32 32 32 32 32 33
                                                                2M43,33262222223
                       000000000 33 33 33 33 33 33 33 32 31 30 37 36 35 34 3B 3A
                                                               333333332107654;:
                       88888888 39 38 CC F7 33 86 23 33 31 32 38 38 31 37 38 36
                                                                98M43‡#312001706
                                                                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';
                       00000100
                       88888118 2B 2A 29 16 15 14 1B 1A 19 07 06 05 04 0B 0A 09 98888120 70 77 76 75 74 7B 7A 79 60 67 66 65 64 6B 6A 69
                              50 57 56 55 54 5B 5A 59 40 47 46 45 44 4B 4A 49
                              B0 B7 B6 B5 B4 BB BA B9 A1 A0 A7 A6 A5 A4 AB AA
A9 91 90 97  96 95 94 9B  9A 99 81 80  87 86 85 84
                       00000140
                                                                ·¶μґ»εΝΫ §¦Ґ¤«€
                                                                            랰떶뭅릺성Wb∭
                                                                            醋暢腫運來
                                                                )` h--•″>љ™Ր<mark>T</mark>≢‡...,,
                       00000150
                              8B 8A 89 F1 F0 F7 F6 F5 F4 FB FA F9 E1 E0 E7 E6
                                                                            निद्रसंक्वित्तरहा
                              E5 E4 EB EA E9 D2 D1 D0 D7 D6 D5 D4 DB DA D9 C2
                                                                едлки́ТСРЧЦХФЫЬЩВ
                                                                            bb링탑홋퓕뀽싙
                       88888188 C1 C8 C7 C6 C5 C4 CB CA C9 CC F7 33 2C 32 33 38
                                                               БАЗЖЕДЛКИМЧЗ,230
                                                                            상<del>욪쓃</del>풇챙24(개)
                       2222222233333332
                      File Properties
                        Stream
                   Perform a bitwise (logical) operation
                                                                                                                       Selected: 12,778,337 bytes ][ SPARSE UNCHANGED OVERWRITE
   In the window that appears, select XOR from the Operation list, and select Hex Bytes as the second operand in the second list.
                   In the bottom field, we enter 32 as a test of what we get in the output. This will be our second operand.
                                                        Bitwise Operation
                                                                                XOR (Exclusive OR)
                                                          Operation:
                                                          Second Operand:
                                                                                Hex Bytes
                                                                                    Cancel
                                                                              Conquered ...
                   FlexHEX - [01.DAT]
                                                                                                                                                _ _
                   <u>File Stream Edit Search Navigate View Tools Window Help</u>
                   01.DAT
                       00 00 00 00 00 00 00 00 00 00 00 00
                       000000000 01 10 09 01 41 01 41 02 00 23 01 03 10 00 02 10
                       000000B0 00 FE C5 01 1E 01 01 00 04 00 00 00 00 00 00 01
                       000000C0 01 01 01 01 01 01 01 00 03 02 05 04 07 06 09 08
                                                                            āāā â$∜[
                       00000000 0B 0A FE C5 01 B4 11 01 03 00 02 02 03 05 02 04
                                                                            [없됐đ Ādj
                       000000E0 04 05 05 01 01 00 7C 00 03 02 01 05 10 04 13 20
                       8888886 38 48 87 12 58 68 86 23 78 15 33 88 98 88 89 22 88 P #p 3Hg
                       00000100 43 B0 C0 14 53 D0 F1 25 32 63 73 83 08 0B 17 16 C°A SPC%2csf
                                                                            学っまの経動
                       00000110 19 18 1B 24 27 26 29 28 2B 35 34 37 36 39 38 3B $\$'&)(+547698;
                       00000120 42 45 44 47 46 49 48 4B 52 55 54 57 56 59 58 5B BEDGFIHKRUTWUYX[
                       00000150 | 9B A3 A2 A5 A4 A7 A6 A9 A8 AB B3 B2 B5 B4 B7 B6 | >JÿҐ×ަ⊚Ё«iIμґ·¶
                       88888178 D7 D6 D9 D8 DB E8 E3 E2 E5 E4 E7 E6 E9 E8 EB F8 ЧЦЩШЫАГВЕДЗЖИ́ИЛР 👯 БЪБЪБЪБЪ
                       88888188 F3 F2 F5 F4 F7 F6 F9 F8 FB FE C5 01 1E 00 01 02 УТХФЧЦЩШЫЮЕ
                                                                            त तत्तत्तत्तत्त
                       त्रत्वत
                       88888148 83 82 85 84 87 86 89 88 88 84 FF C5 81 R4 18 81
                      File Properties
                        Stream
                                                                                                                             Selected: 16 bytes | SPARSE MODIFIED OVERWRITE
        Hmm. Nothing interesting though. It reminds me of something. YES! This is very similar to the header of the jpg images.
                   <u>File Stream Edit Search Navigate View Tools Window Help</u>
                    01.DAT File2
                   88888889 FF D8 FF E9 90 10 4A 46 49 46 99 01 91 01 00 48 яШяа JFIF
                    00000020 07 07 07 09 09 08 0A 0C 14 0D 0C 0B 0B 0C 19 12
                                                                         ₹ [<del>ಡ</del>ಿಎಂಡಿಬ್ದುಗ
                   00000030 13 0F 14 1D 1A 1F 1E 1D 1A 1C 1C 20 24 2E 27 20
                                                                         ÷εΰΕ⊐Ϊ "լ
                                                            ",# (7),01444
                          22 2C 23 1C 1C 28 37 29 2C 30 31 34 34 34 1F 27
                    00000050 39 3D 38 32 3C 2E 33 34 32 FF DB 00 43 01 09 09 9=82<.342яЫ С
                                                                        濄捌佣ÛŃß
                    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
                   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
                   000000E0 05 04 04 00 00 01 7D 01 02 03 00 04 11 05 12 21
                   000000F0 31 41 06 13 51 61 07 22 71 14 32 81 91 A1 08 23 1A Qa "q 2f`ў #
                    00000100 42 B1 C1 15 52 D1 F0 24 33 62 72 82 09 0A 16 17 B±6 RCp$3br,
                   00000110 18 19 1A 25 26 27 28 29 2A 34 35 36 37 38 39 3A
                   00000120 43 44 45 46 47 48 49 4A 53 54 55 56 57 58 59 5A CDEFGHIJSTUUWXYZ
                   00000130 63 64 65 66 67 68 69 6A 73 74 75 76 77 78 79 7A cdefghijstuvwxyz
                          83 84 85 86 87 88 89 8A 92 93 94 95 96 97 98 99 r,,...+*#%h'``"*--"
                   00000150 9A A2 A3 A4 A5 A6 A7 A8 A9 AA B2 B3 B4 B5 B6 B7 AĞJ¤Ґ¦§Ё©€ІІҐµ¶•
                   98999169 B8 B9 BA C2 C3 C4 C5 C6 C7 C8 C9 CA D2 D3 D4 D5 ENEBTДЕЖЗИЙКТУФХ водавать
                    00000170 D6 D7 D8 D9 DA E1 E2 E3 E4 E5 E6 E7 E8 E9 EA F1 ЦЧШЩЬбВГДЕЖЗИЙКС
                                                                        त्वत्वत्वत्वत्वत्वः
                    00000180 F2 F3 F4 F5 F6 F7 F8 F9 FA FF C4 00 1F 01 00 03 ТуфхцчищъяД
                   व वववव
                    88888148 82 83 84 85 86 87 88 89 84 88 FF CA 88 85 11 88
                      File Properties
                                                                                                                             Selected: 16 bytes | SPARSE MODIFIED OVERWRITE
So this is really XOR and this time we will have 33 as the second operand.
Press Ctrl + Z to undo the previous operation and re- XOR with the new operand.
We get the following at the output:
                   😆 FlexHEX
                                                                                                                                                - □ ×
                   <u>File Stream Edit Search Navigate View Tools Window Help</u>
                    00000010 00 01 00 00 FF DB 00 43 00 01 01 01 01 01 01 01
                                                                            Ā To絲森āāā
                       स्टब्स्टब्स्
                       स्वत्यत्वत्यत्वत्य
                       00000050 01 01 01 01 01 01 01 01 FF DB 00 43 01 01 01
                                                                            āāāā !ÛŃā
                       रत्वत्वत्वत्वत्
                       रत्वत्वत्वत्वत्
                       स्टब्स्टब्स्टब्स्
                       aaaaaaaa
                       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
                       000000D0 OA 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
                       888888989 31 41 86 13 51 61 87 22 71 14 32 81 91 A1 88 23 | 1A Qa "q 2f`ў # | 稼慑∂赈
                       00000100 42 B1 C1 15 52 D1 F0 24 33 62 72 82 09 0A 16 17 B±6 RCp$3br,
                       00000110 18 19 1A 25 26 27 28 29 2A 34 35 36 37 38 39 3A
                       00000120 | 43 44 45 46 47 48 49 4A 53 54 55 56 57 58 59 5A | CDEFGHIJSTUVWXYZ | II: 原動語 基金
                       99999159 | 94 A2 A3 A4 A5 A6 A7 A8 A9 AA B2 B3 B4 B5 B6 B7 | "AĞJ»Ґ¦ŞЁ©€ІІ́ѓµ¶-
                       98688178 D6 D7 D8 D9 DA E1 E2 E3 E4 E5 E6 E7 E8 E9 EA F1 ЦЧШЦЬ6ВГдежзийкс "БЪБЪБЪБЪ
                       880000180 F2 F3 F4 F5 F6 F7 F8 F9 FA FF C4 00 1F 01 00 03 ТУФХЦЧШЦЬЯД
                                                                            ъъъ笠 Äğ`
                                                                      त्र वत्रवत्र
स्थलकेर
                       88888148 82 83 84 85 86 87 88 89 84 88 FF C4 88 R5 11 88
                      File Properties
                        Stream
                                                                                                                           Size: 12,778,337 bytes ][ SPARSE MODIFIED OVERWRITE
                                                Scroll down the file to make sure it is completely decrypted.
                   🔁 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
                       00C2F9F0 30 30 30 3B 32 30 30 30 3B 20 77 77 77 2E 54 48 000;2000; www.TH
                       00C2FA20 | 53 4F 55 4E 44 3B 0D 0A 39 31 36 3B 20 33 30 30 | SOUND; 916; 300 | 体制 = 臓炎
                       00C2FA30 30 3B 31 30 30 30 3B 20 46 4F 52 43 45 20 46 45 0;1000; FORCE FE
                       00C2FA50 30 30 3B 31 30 30 3B 20 33 44 20 43 4F 43 4B 00;1000; 3D COCK
                       00C2FA60 50 49 54 3B 0D 0A 39 32 31 3B 20 35 30 30 3B 35 PIT; 921; 500;5
                       00C2FA70 30 30 3B 20 4D 4F 52 45 20 49 4E 46 4F 3B 0D 0A 00; MORE INFO;
                       88C2FA88 39 32 31 38 28 31 35 38 38 38 32 35 38 38 38 28 921; 1588;2588;
                       00C2FA90 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;
                       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 3B | ILD; 918; 4000;
                       00C2FB00 3B 20 31 30 30 30 3B 31 35 30 30 3B 20 58 2D 42 ; 1000;1500; X-B
                       00C2FB10 | 65 79 6F 6E 64 20 74 68 65 20 46 72 6F 6E 74 69 | eyond the Fronti
                       00C2FB20 | 65 72 3B 0D 0A 39 32 31 3B 20 35 30 30 3B 35 30 | er; 921; 500;50 |
                       88C2FB38 38 38 28 4D 4F 52 45 28 49 4E 46 4F 3B 8D 8A 39 8; MORE INFO; 9
                       00C2FB40 32 31 3B 20 31 35 30 30 3B 32 35 30 30 3B 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;
                      🖫 🖬 File Propertie
                                                                                                                           Size: 12,778,337 bytes ][ SPARSE MODIFIED OVERWRITE
Everything is ok, but there is problem number two, how do you determine the file boundaries?
Next to the above file is 01.CAT, which, judging by its name, is a specific header and TOC, and due to its small size it is quite
suitable for storing data about the file table of names and offsets.
And it is also encrypted, but using a different algorithm. I will not go into the details of the search, I can only add that the decryption
code is executed after calling standard functions for working with files, namely in this place:
                                                          Decryption loop in x.exe.
Brief essence of the algorithm:
     1. We take the first byte;
     2. Take the decryption key = DBh;
     3. Xor it with the first byte;
     4. Increase (we get DCh);
     5. Xorim the second byte with the increased value;
     6. Increase again (we get DDh );
     7. We repeat from the first step, moving on to the next pair of bytes.
On Delphi, you would get something like this loop code:
 Where:
     1. DataFile: File of byte;
     2. IncXor, readbuf1, writebuf1, writebuf2, readbuf2, i, count, offset, Fsize: integer;
     3. IncXor has an initial value of $ DB;
After decryption, the file looks like this:
                   🔁 FlexHEX - [01.CAT]
                    <u>File Stream Edit Search Navigate View Tools Window Help</u>
                    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
                   00000030 36 36 0A 74 65 78 2F 74 72 75 65 2F 31 30 32 2E 66 tex/true/102.
                                                                                       灣跳鄉藍
                   00000040 | 6A 70 67 20 33 32 31 34 0A 74 65 78 2F 74 72 75 | jpg 3214 tex/tru
                   00000050 | 65 2F 31 30 33 2E 6A 70 67 20 33 30 38 38 0A 74 | e/103.jpg 3088 t
                                                                                       田小瀬が棚
                   00000060 65 78 2F 74 72 75 65 2F 31 30 34 2E 6A 70 67 20 ex/true/104.jpg
                                                                                       碳重 中澤
                    00000070 32 39 39 36 0A 74 65 78 2F 74 72 75 65 2F 31 30 2996 tex/true/10
                    00000080 | 35 2E 6A 70 67 20 32 39 30 38 0A 74 65 78 2F 74 | 5.jpg 2908 tex/t
                                                                                       灣空歌館
                    00000090 72 75 65 2F 31 30 36 2E 6A 70 67 20 32 38 31 36 | rue/106.jpg 2816
                    00000000 0A 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 | g 2718 tex/true/
                    000000C0 31 30 38 2E 6A 70 67 20 32 37 31 33 0A 74 65 78 108.jpg 2713 tex
                    00000000 | 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.
                    000000F0 | 6A 70 67 20 32 35 36 37 0A 74 65 78 2F 74 72 75 | jpg 2567 tex/tru |
                    00000100 | 65 2F 31 31 31 2E 6A 70 67 20 34 30 33 37 0A 74 | e/111.jpg 4037 t | 田 港外郷
                    00000110 | 65 78 2F 74 72 75 65 2F 31 31 32 2E 6A 70 67 20 | ex/true/112.jpg
                    00000120 34 30 33 38 0A 74 65 78 2F 74 72 75 65 2F 31 31 4038 tex/true/11
                    00000130 │ 33 2E 6A 70 67 20 33 39 36 38 0A 74 65 78 2F 74 │ 3.jpg 3968 tex/t │ □ 灪無郷館
                    00000140 72 75 65 2F 31 31 34 2E 6A 70 67 20 33 37 39 35 | rue/114.jpg 3795 | 翻□ 激源
                    00000150 0A 74 65 78 2F 74 72 75 65 2F 31 31 35 2E 6A 70 tex/true/115.jp 球糖品中心港
                   00000160 67 20 33 37 37 33 0A 74 65 78 2F 74 72 75 65 2F g 3773 tex/true/ 画家職論
                   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 → 激練研究
                       -- 🚾 File Properties
```

This was the end of the murky garbage.

The first six bytes are the internal name. It is likely that this is a validation check. The seventh byte is the line terminator.

Further, the names of files with full paths and their sizes are clearly visible, presented as strings.

In conclusion, I note that the files in 01.DAT are stuck together, which means that the offset must be calculated from the size of the previous one.

Size: 25,421 bytes ][ SPARSE READ-ONLY OVERWRITE

- 🗆 X

Stream

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

00000DE0 87 6E 78 80 9C 9F D7 F3 FC 05 78 58 9C 44 F1 35 00000DF0 65 56 6F 56 F4 4B 64 B4 B6 BD 5F 46 ED D1 6A D5

00000E00 AD EA D1 A5 1A 30 50 82 B2 4B AE ED FE 8B B2 E8

00000EB0 01 01 01 FF C0 00 11 08 00 40 00 40 03 01 22 00

00000EC0 02 11 01 03 11 01 FF C4 00 1F 00 00 01 05 01 01

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

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

800000DA0 3B 4D BB 66 88 9D D3 9F 29 23 25 8F DE 7D DB 77 ;M→f■κੰΨψ)#%ΨЮ}Ы₩ | 薄驝鸌 報蚜

кСҐ ОР,ІК®нюкІ́и

त्रवत्रवत्रवत् त्रवत्रवत्रवत्

त्रवत्रवत्रवत्रत

**釉**aaaaaa

त्रत्वत्रत्वत्रत्त्वत् त्रत्वत्तत्त्वत्तत्त्

*व्यव्यव्यव्यव्य* 

ā 🕍 🏯"

∟′đ≋ά dā ъъ ъѓ

FlexHEX - [01.DAT]

01.DAT

File Properties

Stream

01.DAT