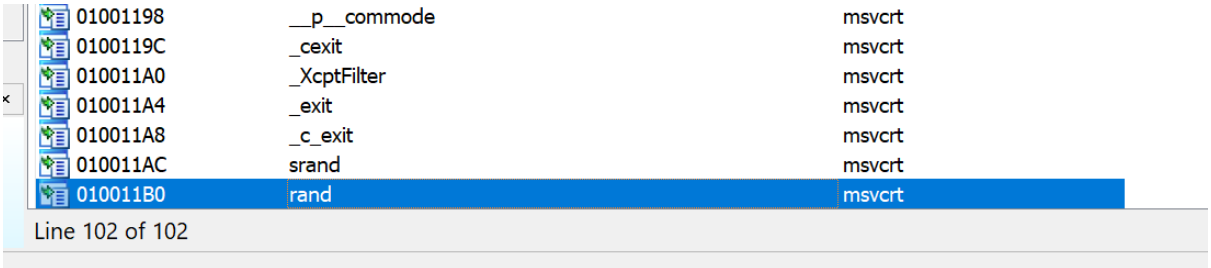
Reverse Engineering Lab 5
Minesweeper

Radu Dilirici, 510

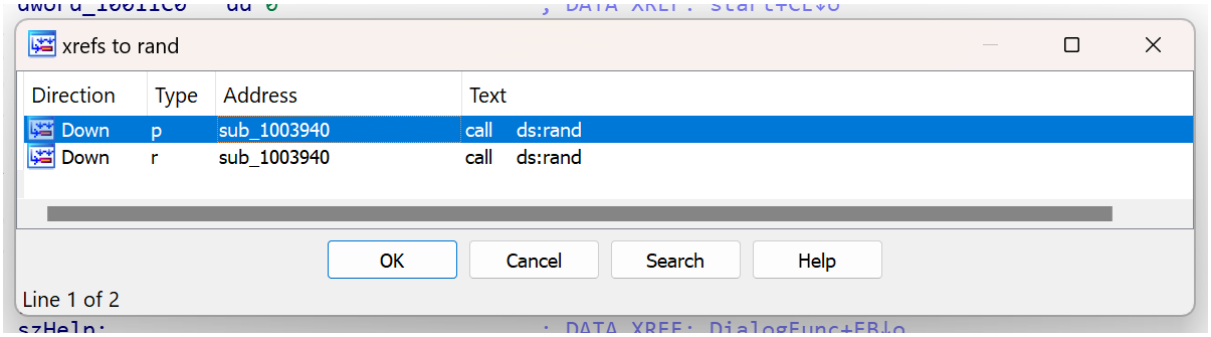
1. Identificarea Bombelor

Initial am presupus ca jocul se initializeaza la apasarea primei casute, astfel incat sa nu poti apasa prima oara pe o bomba. De aceea, am analizat in x32dbg (varianta 32 bits a lui x64dbg) ce se executa la apasarea primei casute, insa nu am avut succes. Se pare ca jocul este initializat de la bun inceput, iar daca cumva jucatorul apasa din prima pe o bomba, programul o muta in alta parte.

Pentru ca generarea campului ar trebui sa se intample intr-un mod aleator (alta presupunere) am cautat in sectiunea de imports din IDA o functie de random si am gasit **rand**.

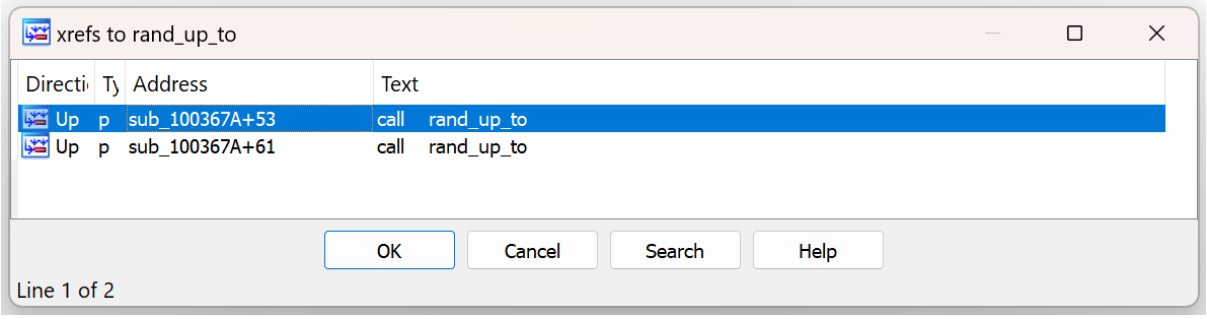


Apoi m-am uitat in ce locuri este folosita functia **rand**. Aceasta avea doua referinte, iar ambele in aceeasi functie.



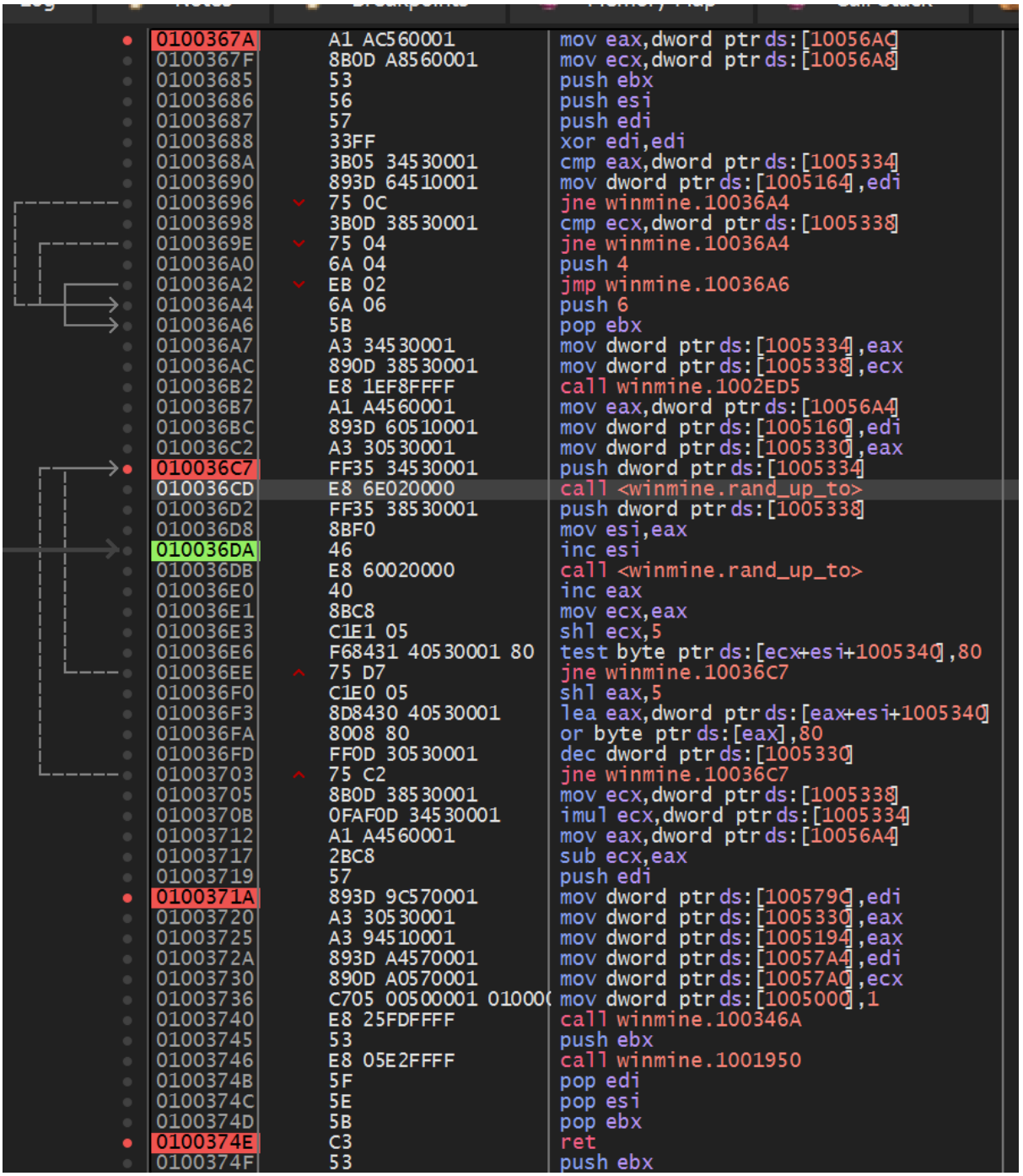

```
1 int __stdcall sub_1003940(int a1)
2 {
3   return rand() % a1;
4 }
```

Din “traducerea” functiei in pseudocod putem observa ca aceasta returneaza un numar aleator mai mic decat argumentul dat (aici a1). Am cautat mai departe unde este folosita aceasta functie, pe care am numit-o **rand_up_to**.




```
1  int sub_100367A()
2  {
3    signed int v0; // ebx
4    int v1; // esi
5    int v2; // eax
6    signed int v4; // [esp-4h] [ebp-10h]
7
8    dword_1005164 = 0;
9    if ( dword_10056AC != dword_1005334 || uValue != dword_1005338 )
10     v4 = 6;
11   else
12     v4 = 4;
13   v0 = v4;
14   dword_1005334 = dword_10056AC;
15   dword_1005338 = uValue;
16   sub_1002ED5();
17   dword_1005160 = 0;
18   dword_1005330 = dword_10056A4;
19   do
20   {
21     do
22     {
23       v1 = rand_up_to(dword_1005334) + 1;
24       v2 = rand_up_to(dword_1005338) + 1;
25     }
26     while ( byte_1005340[32 * v2 + v1] < 0 );
27     byte_1005340[32 * v2 + v1] |= 0x80u;
28     --dword_1005330;
29   }
30   while ( dword_1005330 );
31   dword_100579C = 0;
32   dword_1005330 = dword_10056A4;
33   dword_1005194 = dword_10056A4;
34   dword_10057A4 = 0;
35   dword_10057A0 = dword_1005334 * dword_1005338 - dword_10056A4;
36   dword_1005000 = 1;
37   sub_100346A(0);
38   return sub_1001950(v0);
39 }
```

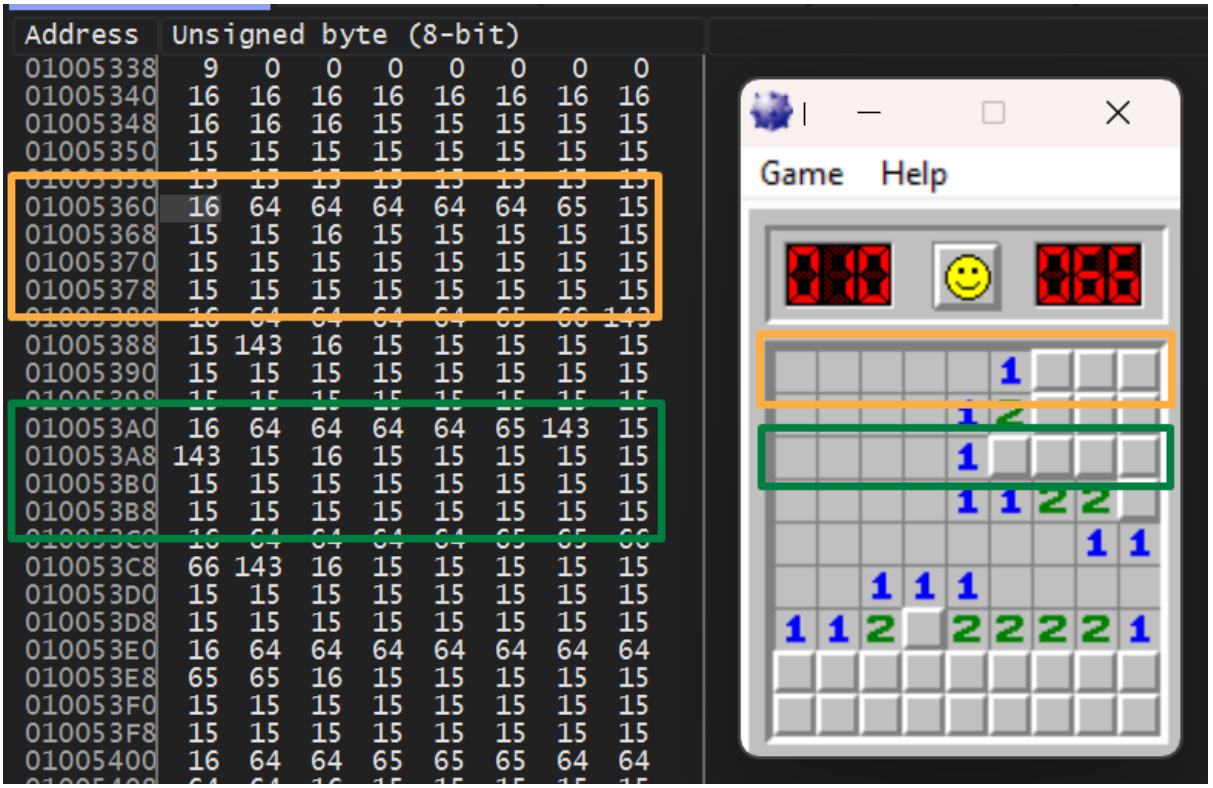
Se pare ca si aceasta este folosita intr-un singur loc. Pentru ca initial nu am stiut ce rol are aceasta functie am decis sa rulez Minesweeper in x32dbg si sa pun Breakpoints in cateva locuri din codul de mai sus, mai exact la inceputul si sfarsitul functiei si la inceputul si sfarsitul **while**-ului mare.



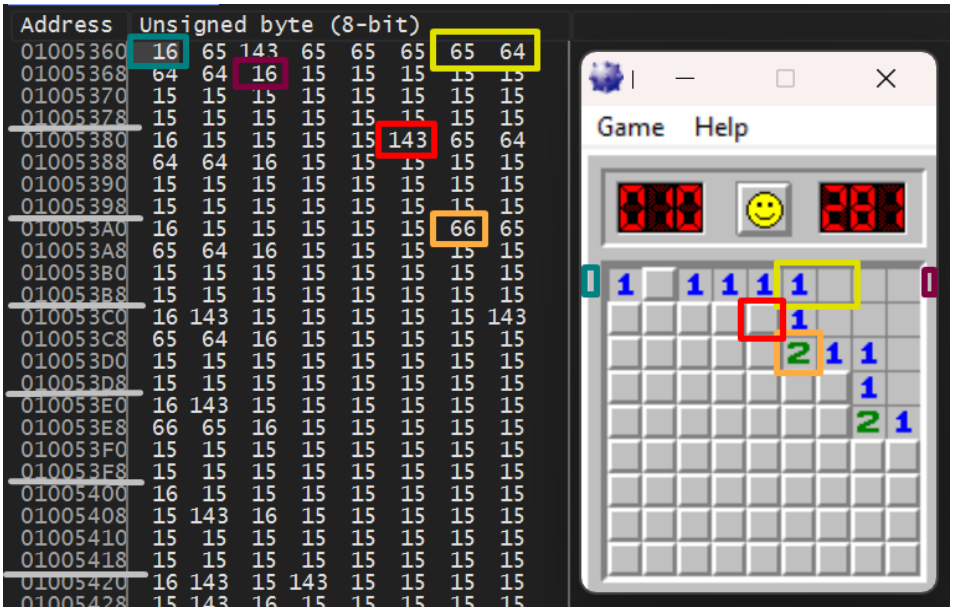
Cand programul a ajuns la inceputul while-ului am mutat EIP dupa acesta. Aceasta actiune a rezultat intr-un camp gol in joc. De asemenea, resetarea nivelului prin apasarea fetei zambitoare rezulta in redeclansarea acestor breakpointuri. De aici am ajuns la concluzia ca acea parte este esentiala la initializarea casutelor.

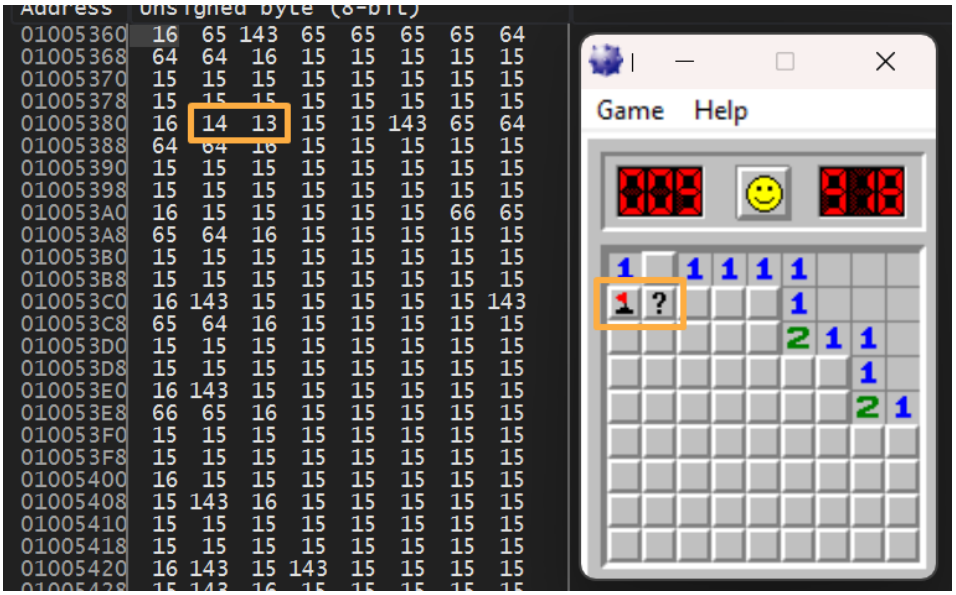
Dupa mai multe investigatii am observat ca acea lista care se modifica in interiorul **while**-ului este de fapt matricea de joc. Aceasta are 32 de coloane, motiv pentru care v1 se inmulteste cu 32. Deci acea instructiune se poate interpreta ca m[v1][v2].

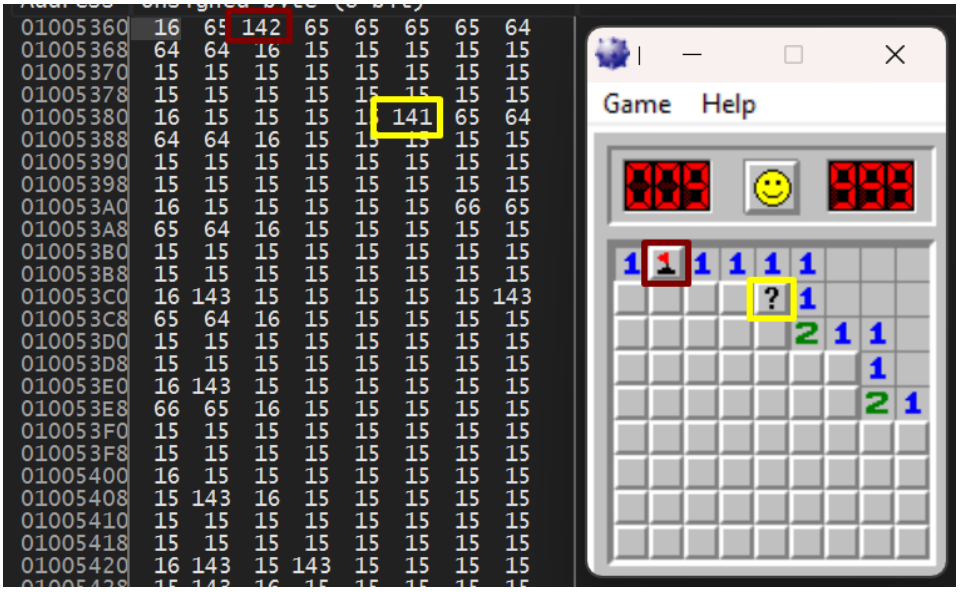
Mai jos se poate observa interpretarea acestei matrice. Aici am ales vizualizarea datelor ca unsigned byte, deoarece mi s-a parut cea mai usor de urmarit. Fiecare rand din matrice incepe si se termina cu valoarea 16, iar intre aceste doua pozitii exista diverse valori, dar cele mai predominante sunt 15 si 64. De asemenea, de la finalul unul rand (unde exista valoarea 16) pana la inceperea urmatorului rand toate valorile sunt tot 15 (fill pana la 32 de elemente pe rand).



In urmatoarele poze am corelat datele din memorie cu casutele din joc.







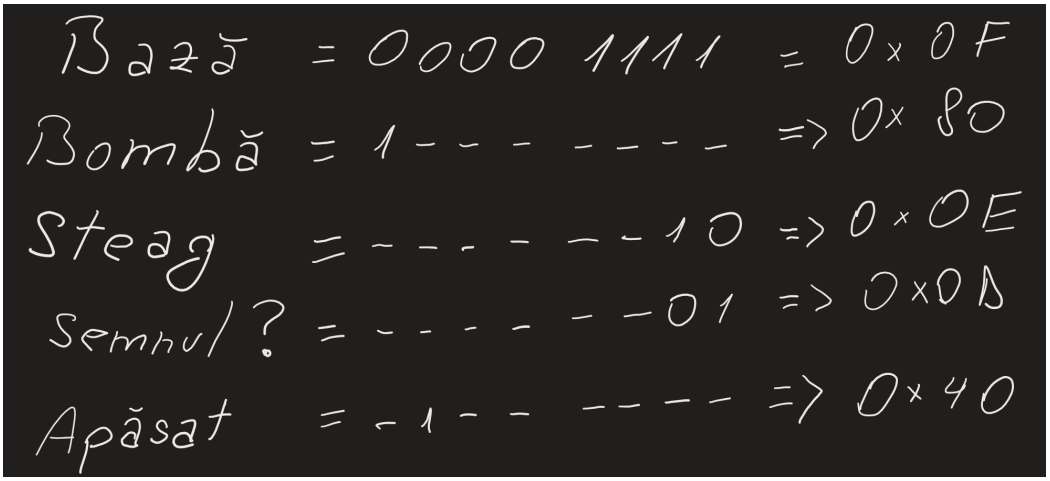
De aici am ajuns la urmatoarele concluzii:

- 15 = casuta neapasata
- 14 = casuta neapasata cu stegulet
- 13 = casuta neapasata cu semnul intrebarii

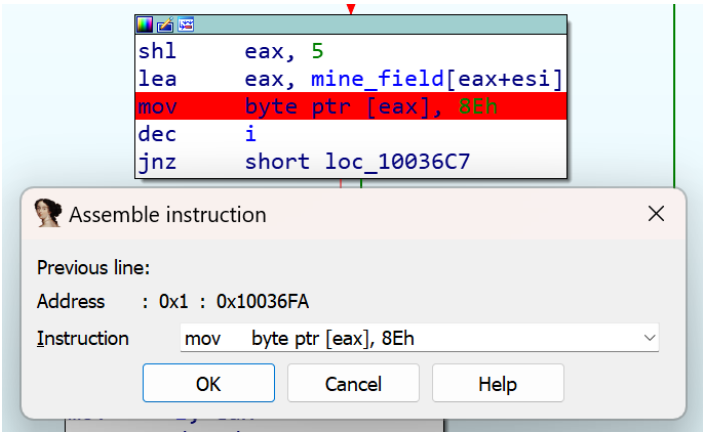
- 64 = casuta apasata cu 0 bombe in vecinatate
- 65 = casuta apasata cu o bomba in vecinatate
- etc… (64 + numarul de bombe din vecinatate)

- 143 = bomba
- 142 = bomba cu stegulet
- 141 = bomba cu semnul intrebarii

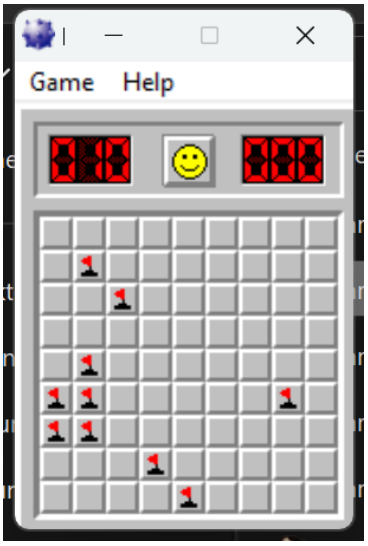
Ba chiar mai mult, aceste date au mai mult sens daca le gandim ca **flags** in binar sau hexadecimal. Fiecare casuta e reprezentata de cate un byte astfel:



In functia de generare a campului se executa operatia **OR** cu **0x80** pe matrice. Acum ne putem da seama ca asta inseamna de fapt adaugarea unei bombe pe acea pozitie. Pentru a avea stegulete pe toate bombele, am schimbat in IDA instructiunea de **OR** cu setarea in memorie a valorii **0x8E** (casuta de baza + bomba + steag = **1000 1110**).

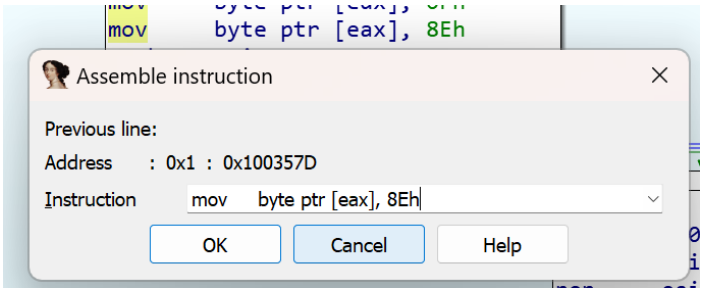


Succes!



Exista insa si cazul in care apasam din prima pe o bomba, iar programul o repozitioneaza. Am gasit codul care seteaza noua bomba, insa modificarea acestuia la fel ca in cazul precedent nu a dus la acelasi rezultat. Casuta avea setata valoarea corecta (0x8E) si nu se putea apasa (casutele cu stegulet nu pot fi apasate), insa steguletul nu era si afisat.

Instructiunea este la adresa **0x100357D**.



2. Semnul intrebarii pe casutele goale

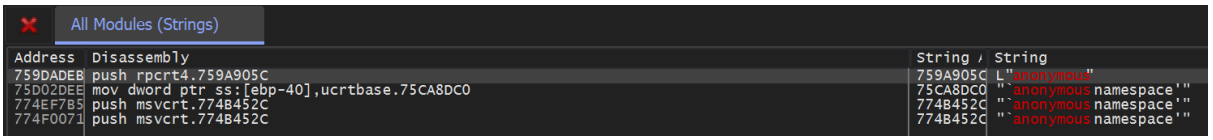
Cautand prin locurile in care se foloseste matricea am gasit portiunea de initializare acesteia cu valoarea 15 (**0x0F**). Am inlocuit aceasta valoare cu 13 (**0x0D**), iar rezultatul a fost ca toate celelalte patratele aveau semnul intrebarii pe ele.

Urmatoul pas era sa adaug 1 (sau sa setez valoarea **0x0E**) pe casutele adiacente bombelor. Acest lucru l-as fi facut la setarea bombelor, insa nu am reusit sa fac acest lucru.

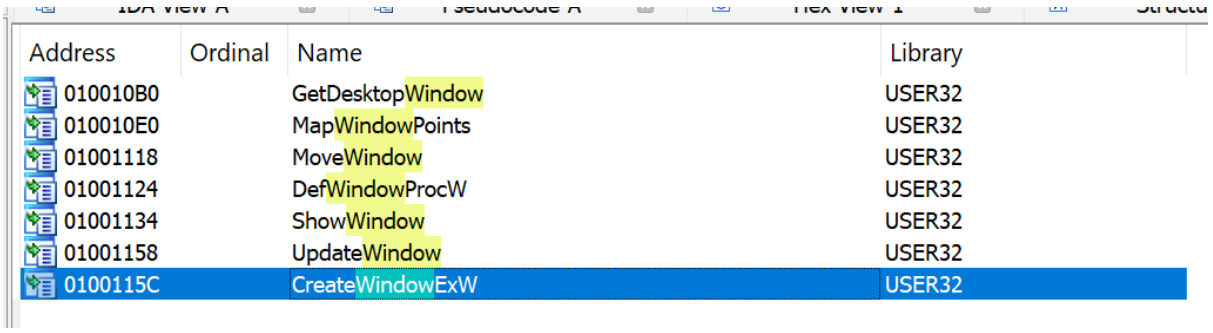
3. Highscores

In mod inplicit, scorurile sunt de 999 secunde de catre “*Anonymous*”. Am incercat mai multe metode de a gasi ori cand se completeaza aceste valori, ori unde sunt stocate valorile initiale.

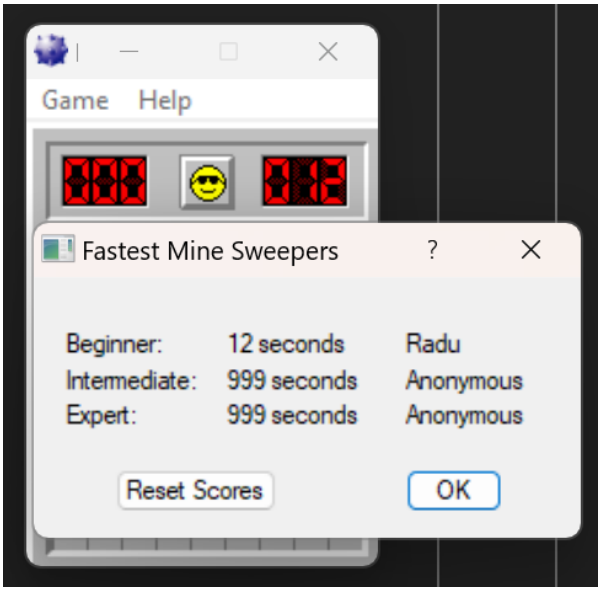
Am cautat dupa stringul “*Anonymous*”:

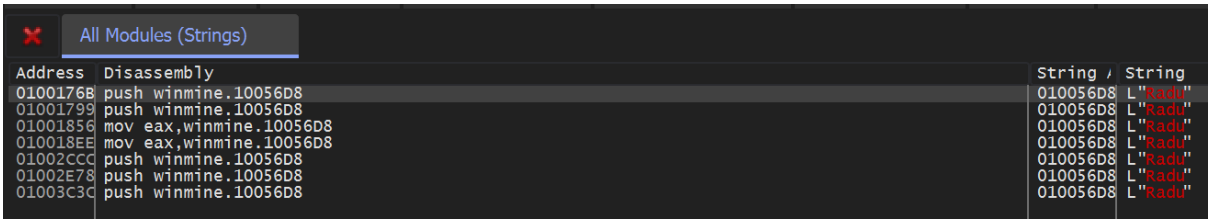


Am cautat cand se creaza o noua fereastra, incercand sa gasesc pop up-ul in care utilizatorul isi trece numele:

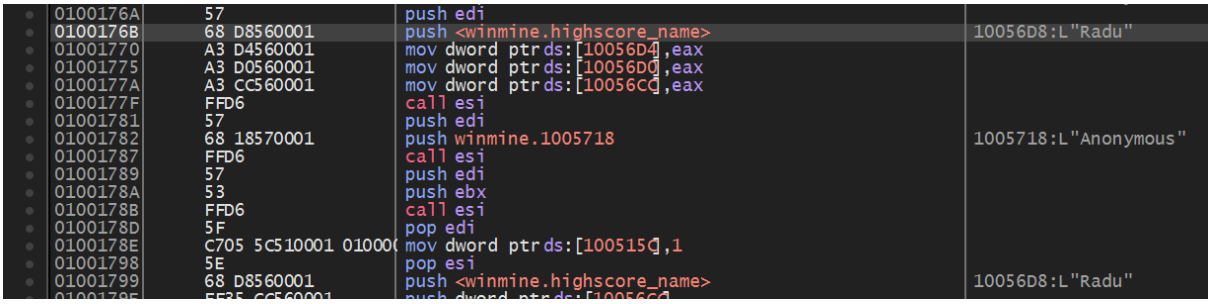


Insa nu am gasit informatii utile. Am terminat jocul si mi-am completat numele. Apoi am cautat referinte catre numele meu in x32dbg.





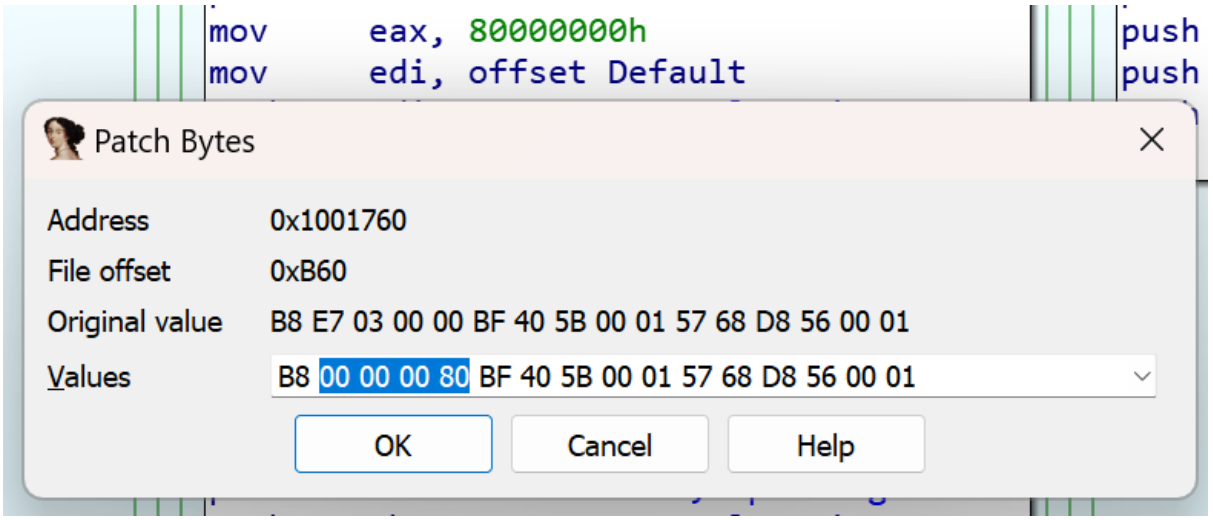
Am gasit un loc interesant in care se foloseste acest string si am analizat functia in IDA.

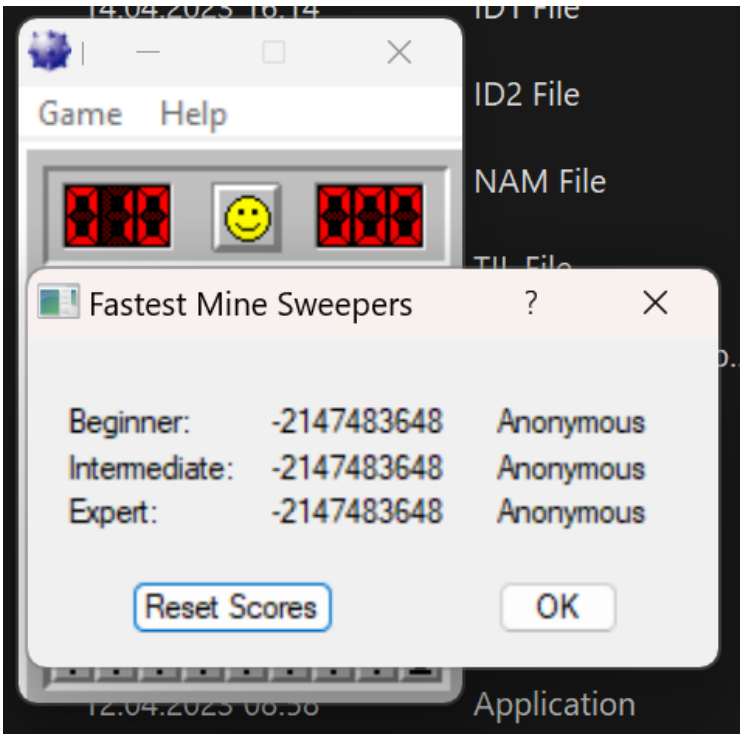



```
*(_DWORD *)&dword_10056D0 = 999;
*(_DWORD *)&dword_10056CC = 999;
lstrcpyW(&ReturnedString, &Default);
lstrcpyW(&word_1005718, &Default);
lstrcpyW(&word_1005758, &Default);
dword_100515C = 1;
goto LABEL_11;
}
```

Aici se initializeaza datele din **Highscores** (se poate observa si valoarea 999 de mai sus).

Pentru a modifica valoarea scorurilor initiale am facut un patch in IDA. Am setat valoarea de la **0x3E7** (999) la **0x80000000** (cea mai mica valoare posibila).

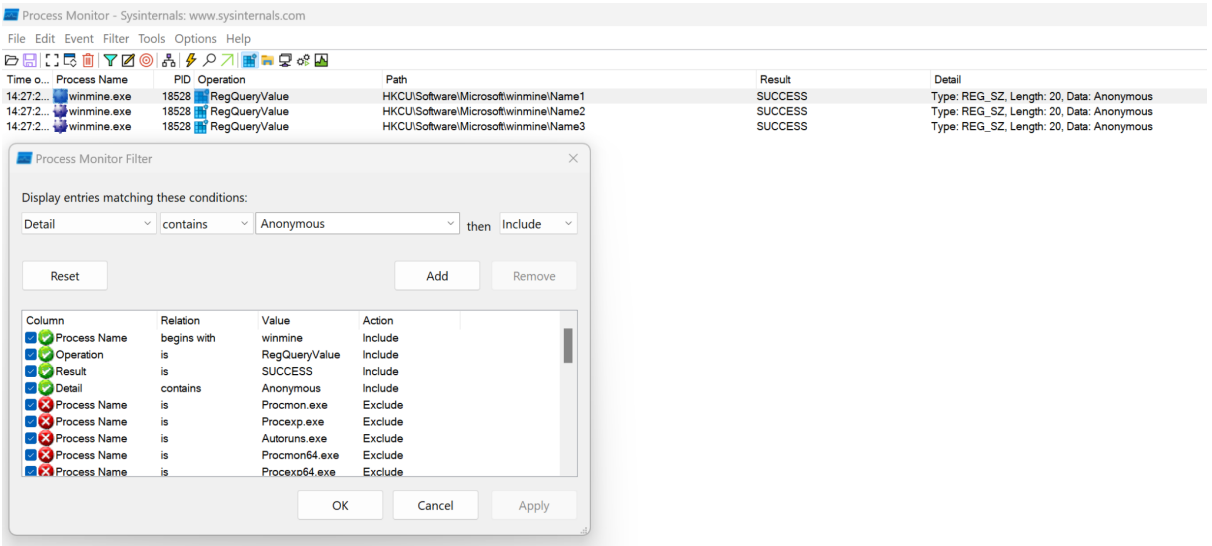




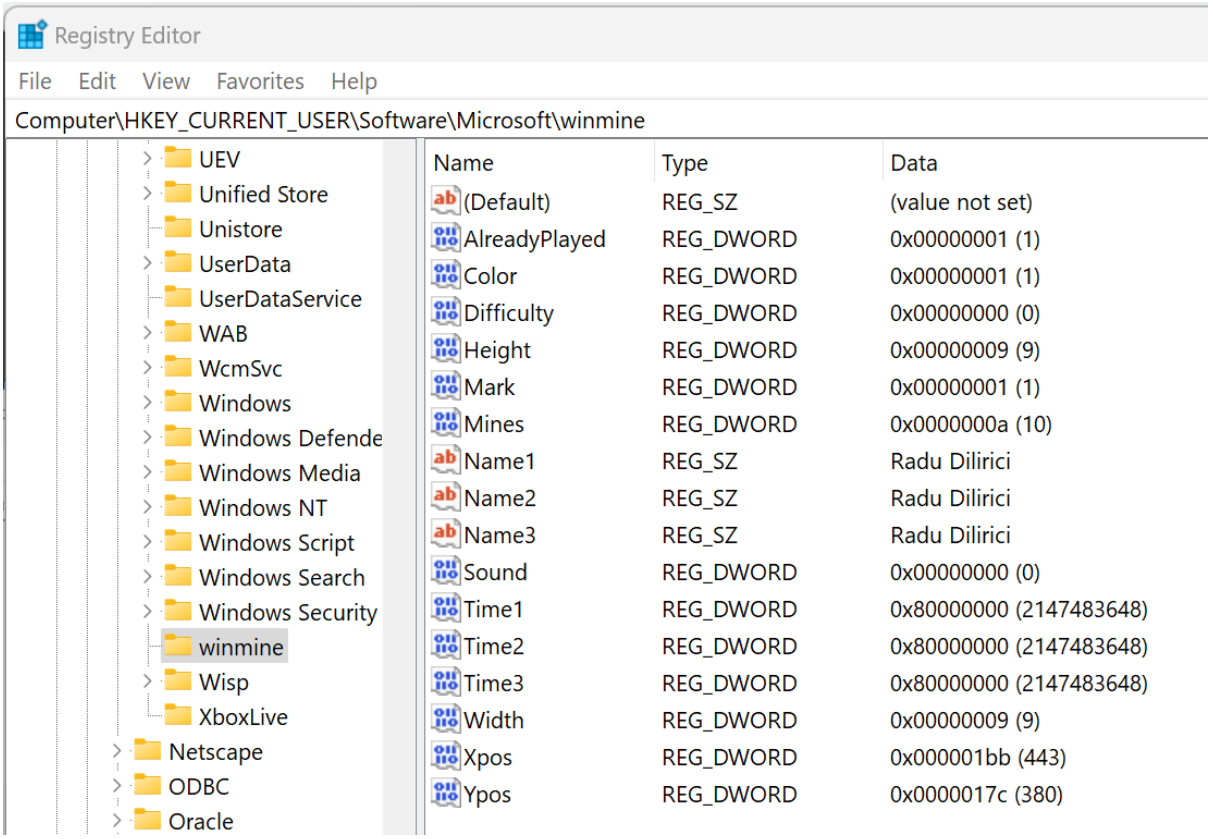
Din pacate, la repornirea jocului scorurile sunt aduse la valoarea 0 daca sunt negative. Probabil putem modifica acest comportament, dar nu am incercat acest lucru.

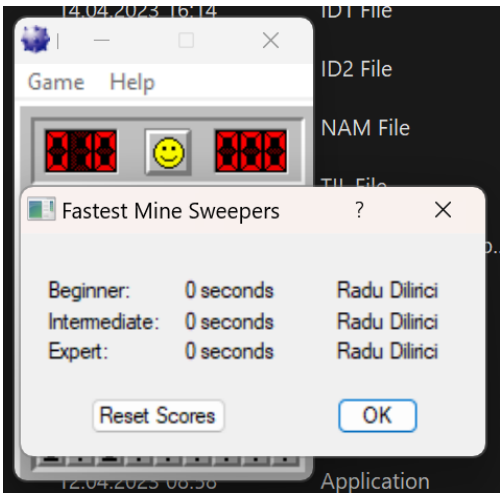
Cat despre nume, nu am gasit in program valoarea default a acestuia. Am gasit intr-un blog cum aceste date ar fi stocate in registrii: https://www.unknowncheats.me/forum/general-programming-and-reversing/18330-reversing-minesweeper-hidden-options.html. Asa ca am urmat aceasta idee.

Intr-adevar, dupa analizarea programului cu **Process Monitor**, am putut observa ce registrii sunt folositi pentru a stoca datele respective.



Apoi am intrat in **Registry Editor** si am modificat valorile (Name1, Name2 si Name3) din acel loc.



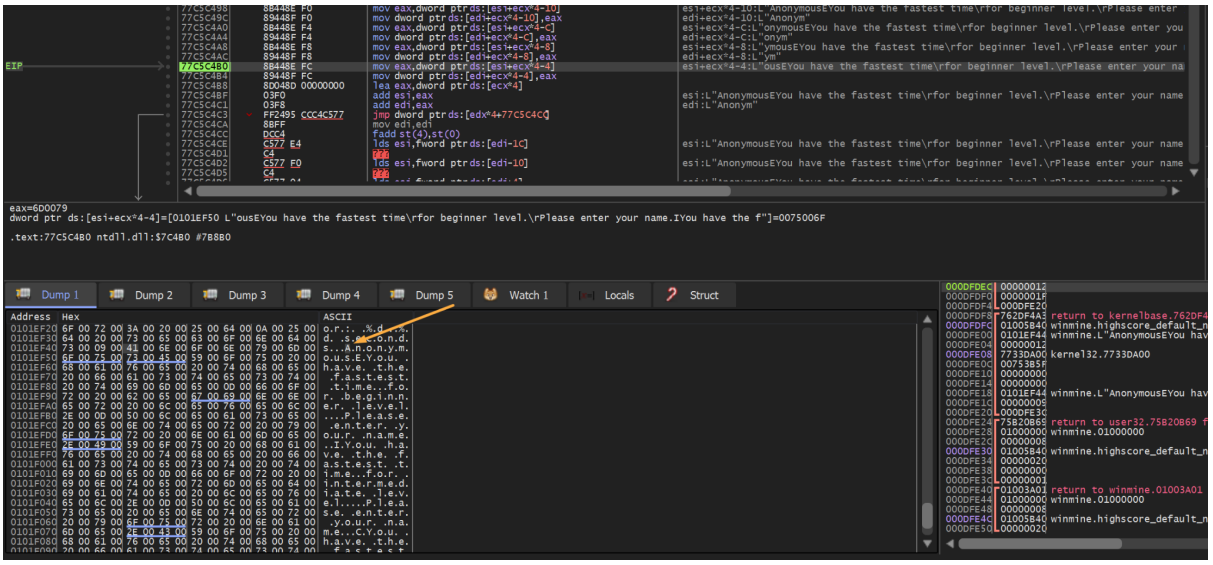


Acest lucru insa modifica datele doar temporar. La resetarea scorurilor, acestea vor avea din nou numele “*Anonymous*”.

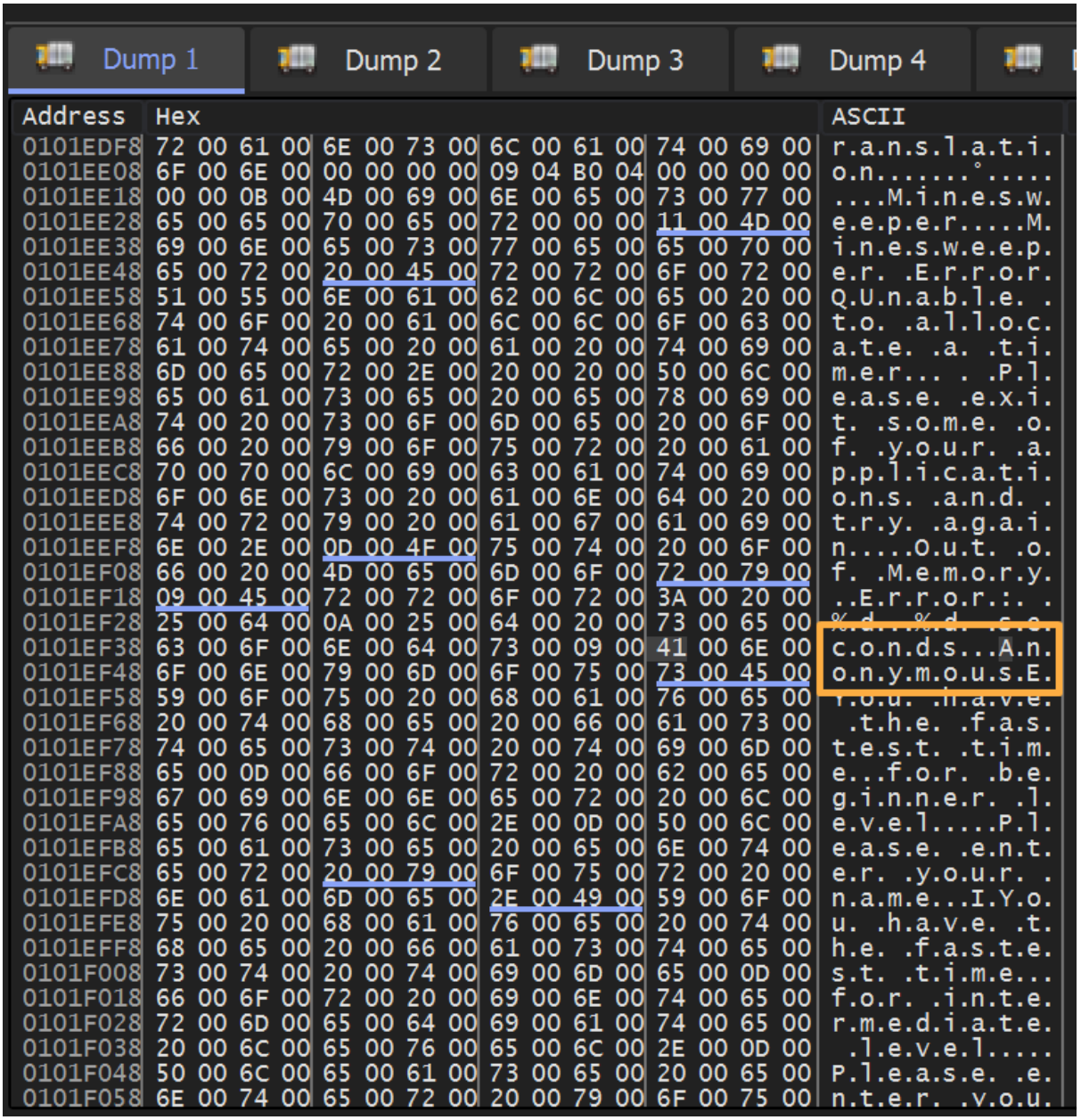
Cred ca am gasit functia in care initializeaza aceste valori, insa nu am stiut cum sa o modific astfel incat sa contina stringul dorit.

```
1int __stdcall initialize_default_highscore_name(__int16 a1, LPWSTR lpBuffer, int cchBufferMax)
2{
3  int result; // eax
4
5  result = LoadStringW(hModule, (unsigned __int16)a1, lpBuffer, cchBufferMax);
6  if ( !result )
7    result = sub_1003950(1001);
8  return result;
9}
```

Pare ca numele “*Anonymous*” sunt luate din memoria programului, dar din nou, nu am reusit sa gasesc locul in care aceasta memorie este initializata. Problema principala a fost alocarea dinamica a acestei memorii. Informatia nu se regaseste mereu la aceeasi adresa.

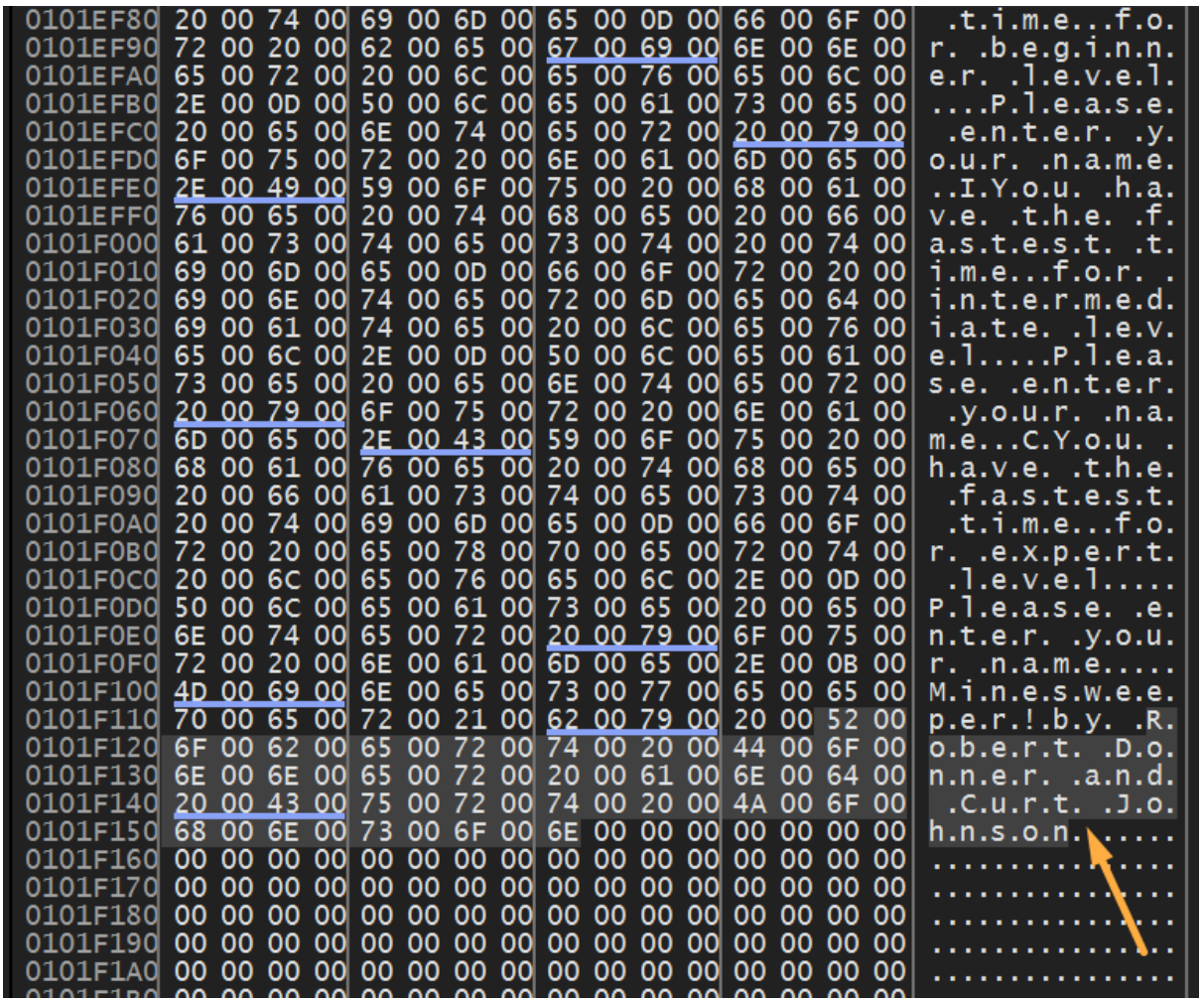


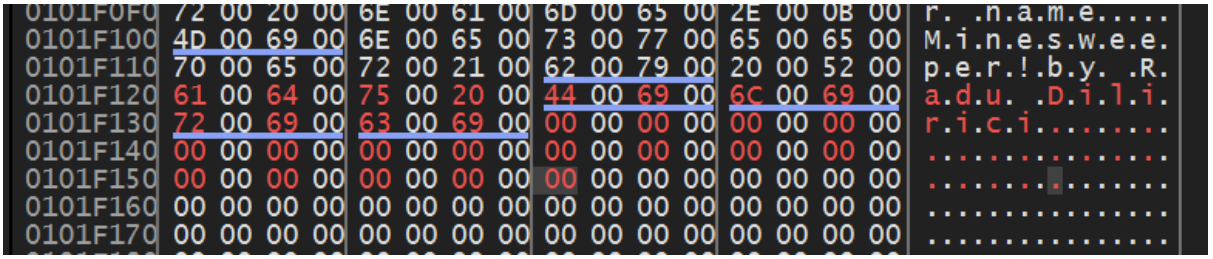
Pe langa cuvantul “*Anonymous*” subliniat mai jos (de la acea adresa este luat) se mai observa si alte texte ale programului, precum “*Unable to allocate a timer. Please exit some of your applications and try again.*”. Nu am reusit sa gasesc referinte la aceste texte, nici in ce locuri apar in joc.



4. Creator

Am gasit numele celor doi autori in acelasi loc din memoria programuli. Am schimbat memoria astfel incat sa reprezinte numele meu, iar astfel a ajuns sa fie afisat in pagina de **About**.


0101EF80 20 00 74 00 69 00 6D 00 65 00 0D 00 66 00 6F 00 .t.i.m.e...f.o.
0101EF90 72 00 20 00 62 00 65 00 67 00 69 00 6E 00 6E 00 r. .b.e.g.i.n.n.
0101EFA0 65 00 72 00 20 00 6C 00 65 00 76 00 65 00 6C 00 e.r. .l.e.v.e.l.
0101EFB0 2E 00 0D 00 50 00 6C 00 65 00 61 00 73 00 65 00 ....P.l.e.a.s.e.
0101EFC0 20 00 65 00 6E 00 74 00 65 00 72 00 20 00 79 00 .e.n.t.e.r. .y.
0101EFD0 6F 00 75 00 72 00 20 00 6E 00 61 00 6D 00 65 00 o.u.r. .n.a.m.e.
0101EFE0 2E 00 49 00 59 00 6F 00 75 00 20 00 68 00 61 00 ..I.Y.o.u. .h.a.
0101EFF0 76 00 65 00 20 00 74 00 68 00 65 00 20 00 66 00 v.e. .t.h.e. .f.
0101F000 61 00 73 00 74 00 65 00 73 00 74 00 20 00 74 00 a.s.t.e.s.t. .t.
0101F010 69 00 6D 00 65 00 0D 00 66 00 6F 00 72 00 20 00 i.m.e...f.o.r. .
0101F020 69 00 6E 00 74 00 65 00 72 00 6D 00 65 00 64 00 i.n.t.e.r.m.e.d.
0101F030 69 00 61 00 74 00 65 00 20 00 6C 00 65 00 76 00 i.a.t.e. .l.e.v.
0101F040 65 00 6C 00 2E 00 0D 00 50 00 6C 00 65 00 61 00 e.l.....P.l.e.a.
0101F050 73 00 65 00 20 00 65 00 6E 00 74 00 65 00 72 00 s.e. .e.n.t.e.r.
0101F060 20 00 79 00 6F 00 75 00 72 00 20 00 6E 00 61 00 .y.o.u.r. .n.a.
0101F070 6D 00 65 00 2E 00 43 00 59 00 6F 00 75 00 20 00 m.e...C.Y.o.u. .
0101F080 68 00 61 00 76 00 65 00 20 00 74 00 68 00 65 00 h.a.v.e. .t.h.e.
0101F090 20 00 66 00 61 00 73 00 74 00 65 00 73 00 74 00 .f.a.s.t.e.s.t.
0101F0A0 20 00 74 00 69 00 6D 00 65 00 0D 00 66 00 6F 00 .t.i.m.e...f.o.
0101F0B0 72 00 20 00 65 00 78 00 70 00 65 00 72 00 74 00 r. .e.x.p.e.r.t.
0101F0C0 20 00 6C 00 65 00 76 00 65 00 6C 00 2E 00 0D 00 .l.e.v.e.l.....
0101F0D0 50 00 6C 00 65 00 61 00 73 00 65 00 20 00 65 00 P.l.e.a.s.e. .e.
0101F0E0 6E 00 74 00 65 00 72 00 20 00 79 00 6F 00 75 00 n.t.e.r. .y.o.u.
0101F0F0 72 00 20 00 6E 00 61 00 6D 00 65 00 2E 00 0B 00 r. .n.a.m.e.....
0101F100 4D 00 69 00 6E 00 65 00 73 00 77 00 65 00 65 00 M.i.n.e.s.w.e.e.
0101F110 70 00 65 00 72 00 21 00 62 00 79 00 20 00 52 00 p.e.r.!.b.y. .R.
0101F120 6F 00 62 00 65 00 72 00 74 00 20 00 44 00 6F 00 o.b.e.r.t. .D.o.
0101F130 6E 00 6E 00 65 00 72 00 20 00 61 00 6E 00 64 00 n.n.e.r. .a.n.d.
0101F140 20 00 43 00 75 00 72 00 74 00 20 00 4A 00 6F 00 .C.u.r.t. .J.o.
0101F150 68 00 6E 00 73 00 6F 00 6E 00 00 00 00 00 00 00 h.n.s.o.n.......
0101F160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0101F170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0101F180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0101F190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0101F1A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....


0101F0F0 72 00 20 00 6E 00 61 00 6D 00 65 00 2E 00 0B 00 r. .n.a.m.e.....
0101F100 4D 00 69 00 6E 00 65 00 73 00 77 00 65 00 65 00 M.i.n.e.s.w.e.e.
0101F110 70 00 65 00 72 00 21 00 62 00 79 00 20 00 52 00 p.e.r.!.b.y. .R.
0101F120 61 00 64 00 75 00 20 00 44 00 69 00 6C 00 69 00 a.d.u. .D.i.l.i.
0101F130 72 00 69 00 63 00 69 00 00 00 00 00 00 00 00 00 r.i.c.i.........
0101F140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0101F150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0101F160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0101F170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....

A se ignora iconita neagra din poza, pe care am stricat-o pe parcursul modificarii programului. In executabilul trimis, iconita este cea originala.

Acesta metoda m-a ajutat in a-mi scrie numele in aceasta pagina, insa este o modificare temporara. La repornirea jocului, numele originale sunt din nou folosite.

Pasii prezentati sunt doar care au adus rezultate. Am incercat mai multe abordari fara a progresa in rezolvarea cerintelor.