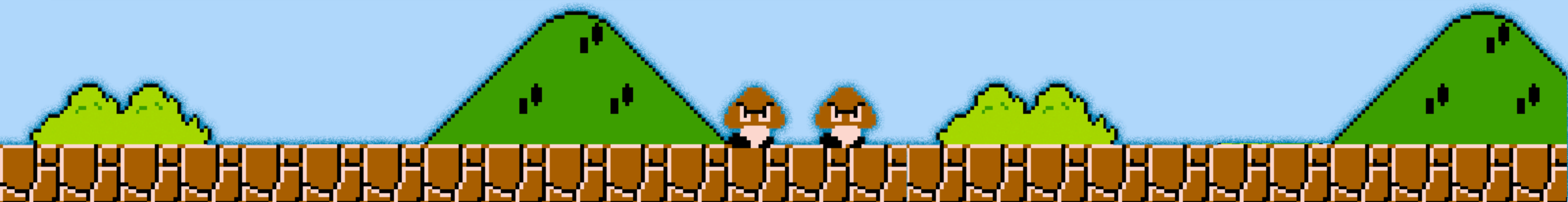
GAME HACKING

by Ross Simpson



About Me:

I'm a Ruby on Rails developer at Platform45 - we make web and iOS applications and games: http://www.platform45.com

Have been hacking games, off and on, since 2005.

Twitter: @hypn
Email: ross@hypn.za.net
Website: http://www.hypn.za.net

Not Covered:

- Latest games - I want to avoid lawsuits and "history repeats itself" (methods shown work for the latest games, eg: DotA 2)
- FPS (aim) Bots - typically require DirectX/OpenGL programming knowledge (and I have none)
- Android games - I'm an iPhone user, sorry!

DISCLAIMER:

The “Terms of Service” / “Terms and Conditions” of most games prevent you from decompiling or modifying game files, or intercepting and manipulating data traffic.

Hack creators have been sued for making hacks (under “copyright infringement”).

You might get banned from your favourite game.

ZaCon 4 - Game Hacking

1. Console Games

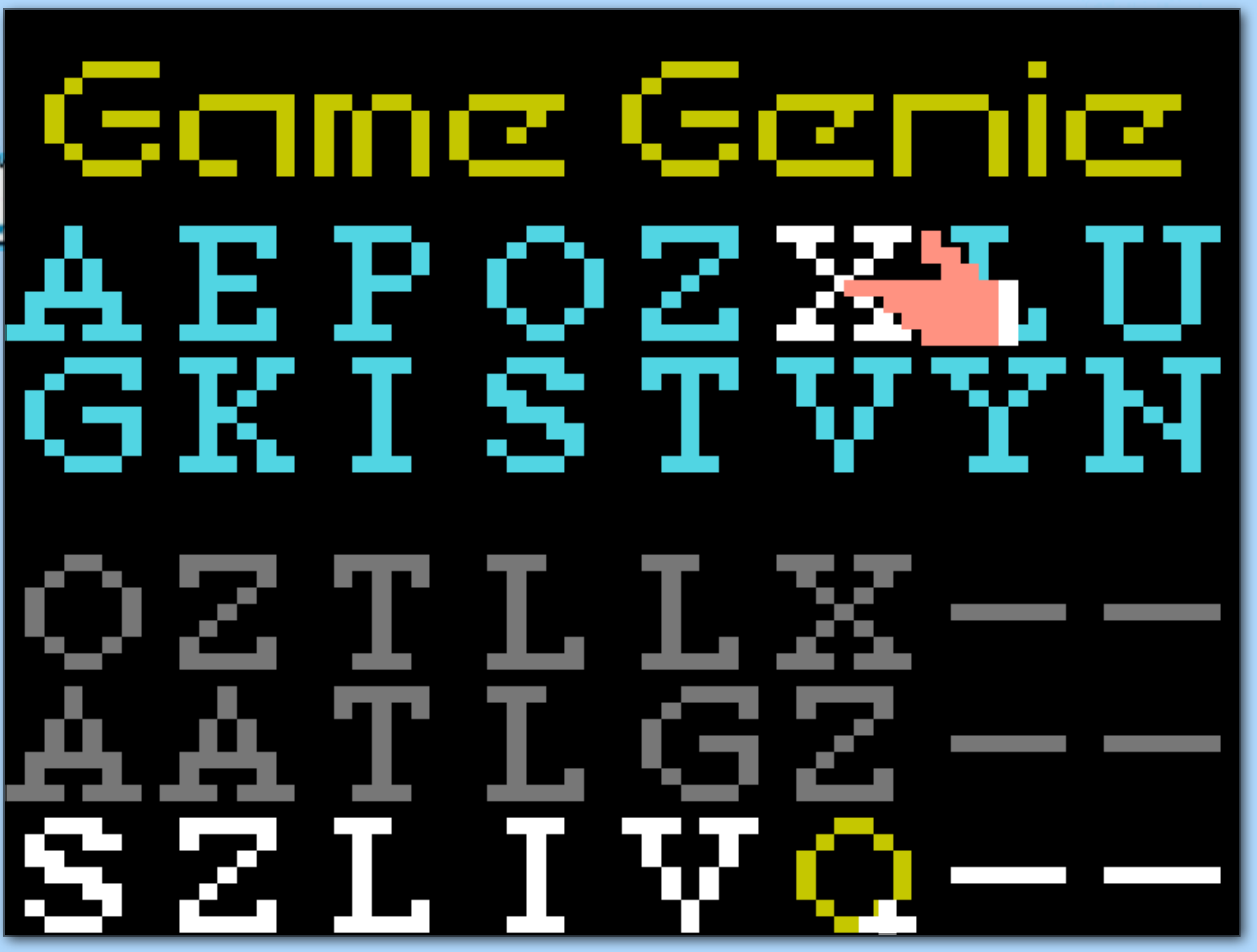
   1.1. Game Genie and others

GAME HACKING

Game Genie

Inserted in to the NES before game cartridges.

GAME HACKING



OZTLLX

AATLGZ

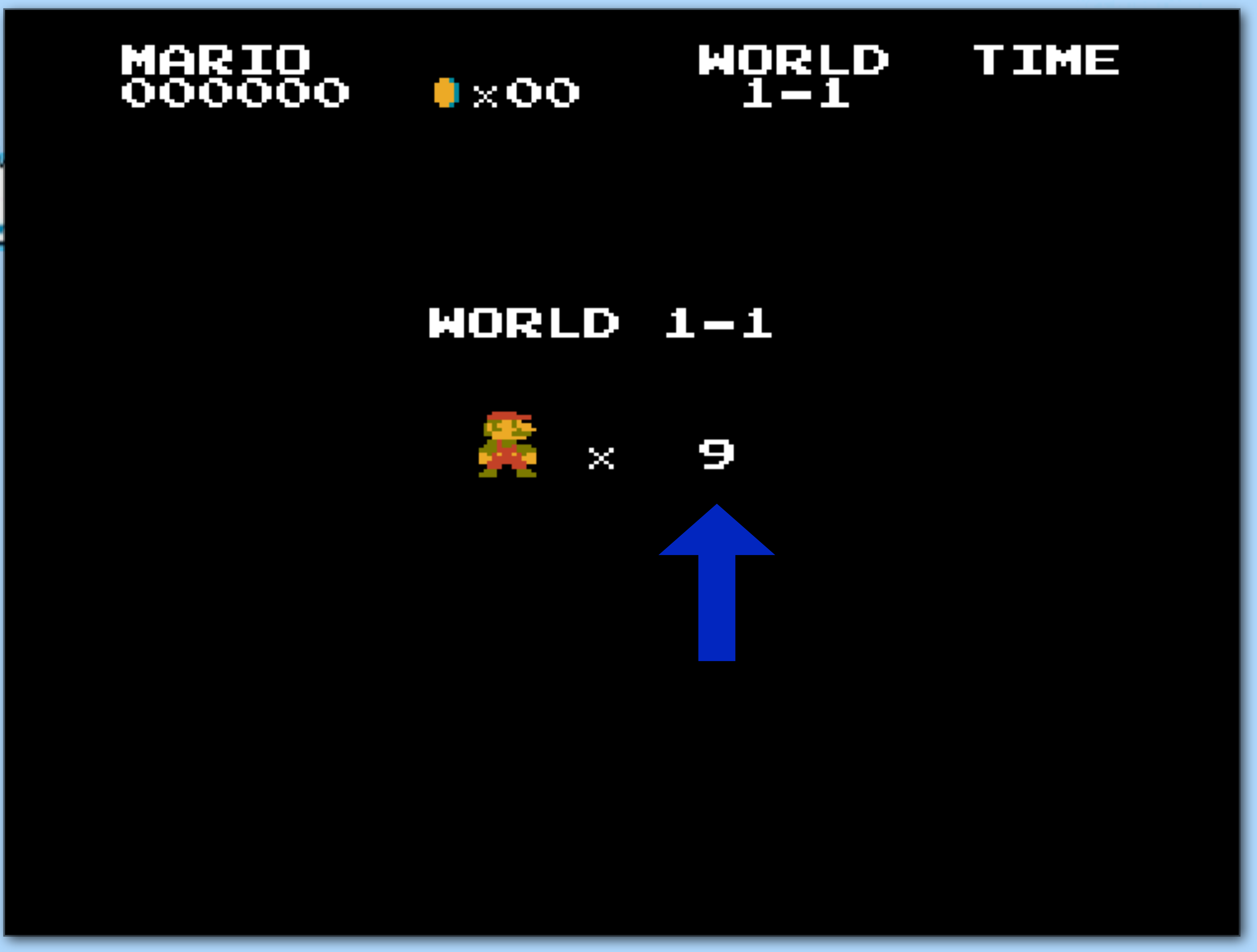
SZLIVO

Game Genie

Inserted in to the NES before game cartridges.

User is prompted to enter codes, which ultimately overwrote game logic:

GAME HACKING


MARIO
000000
×00
WORLD
1-1
TIME

WORLD 1-1

× 9

Game Genie

Inserted in to the NES before game cartridges.

User is prompted to enter codes, which ultimately overwrote game logic:

infinite lives

GAME HACKING

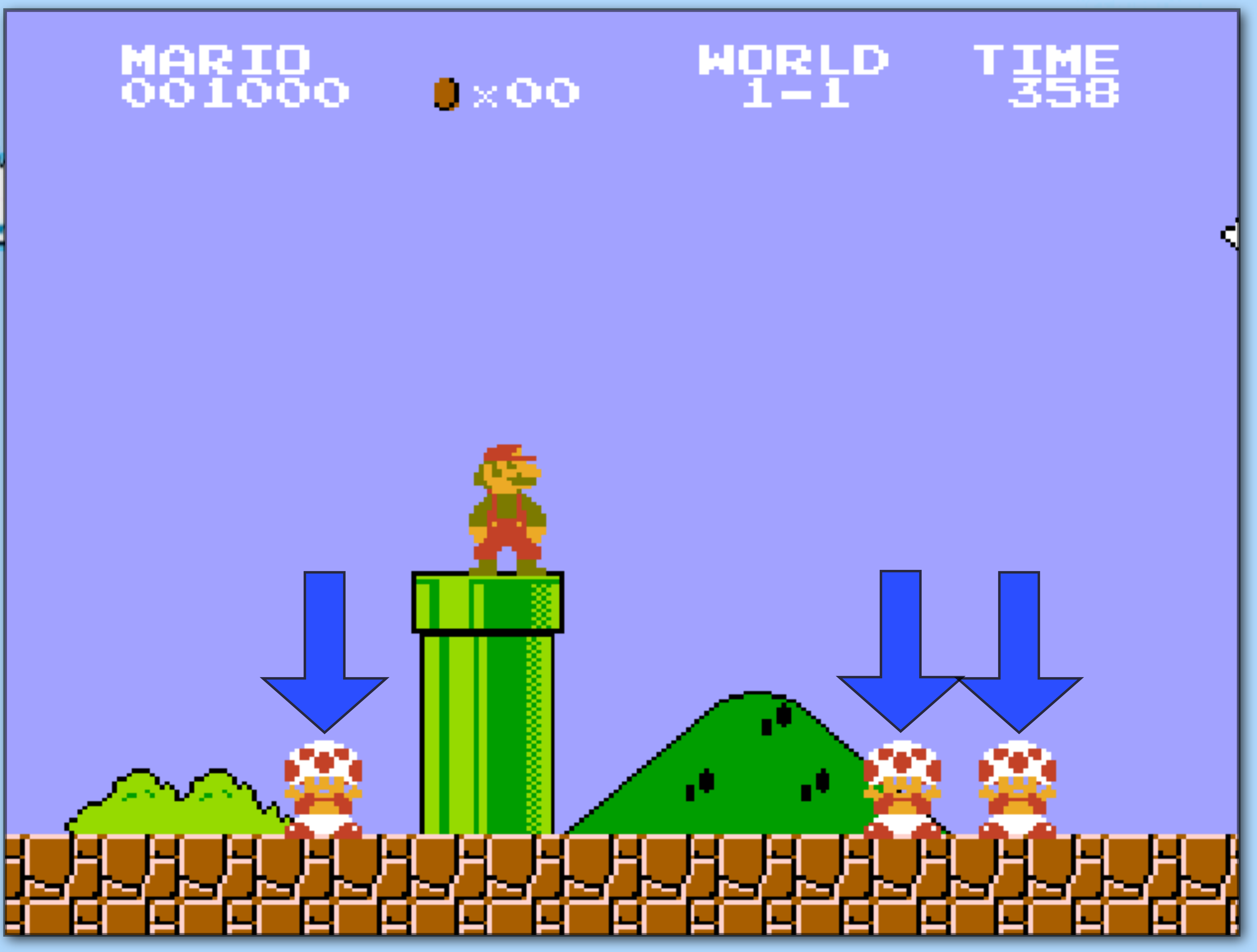
Game Genie

Inserted in to the NES before game cartridges.

User is prompted to enter codes, which ultimately overwrote game logic:

- infinite lives
- super powers

GAME HACKING



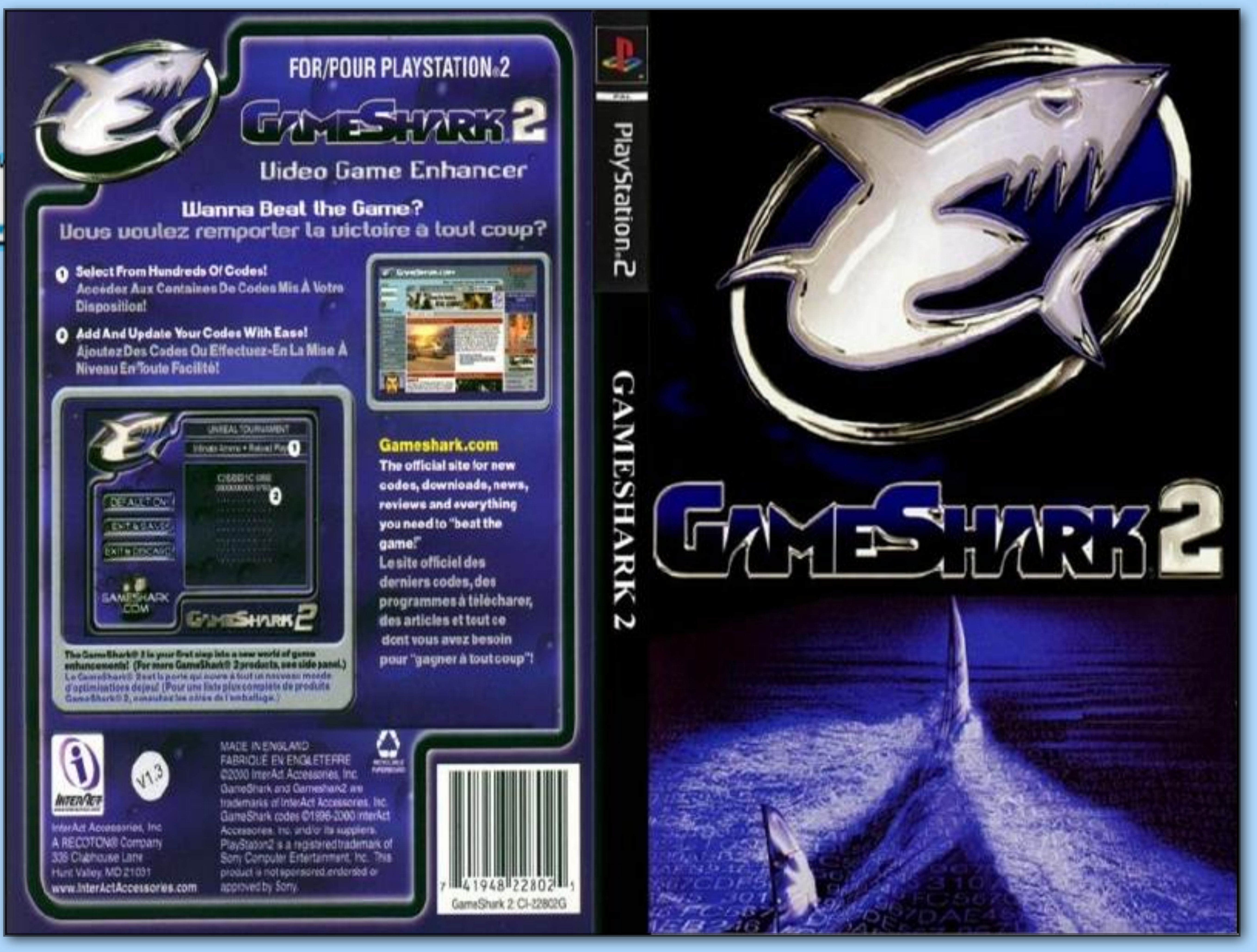
Game Genie

Inserted in to the NES before game cartridges.

User is prompted to enter codes, which ultimately overwrote game logic:

- infinite lives
- super powers
- kill Toad!
  (change the game)

GAME HACKING


FOR/POUR PLAYSTATION 2
GAMESHARK 2
Video Game Enhancer
Wanna Beat the Game?
Vous voulez remporter la victoire à tout coup?
Select From Hundreds Of Codes!
Add And Update Your Codes With Ease!
Gameshark.com
The official site for new codes, downloads, news, reviews and everything you need to "beat the game!"
PlayStation 2
GAMESHARK 2
GAMESHARK 2

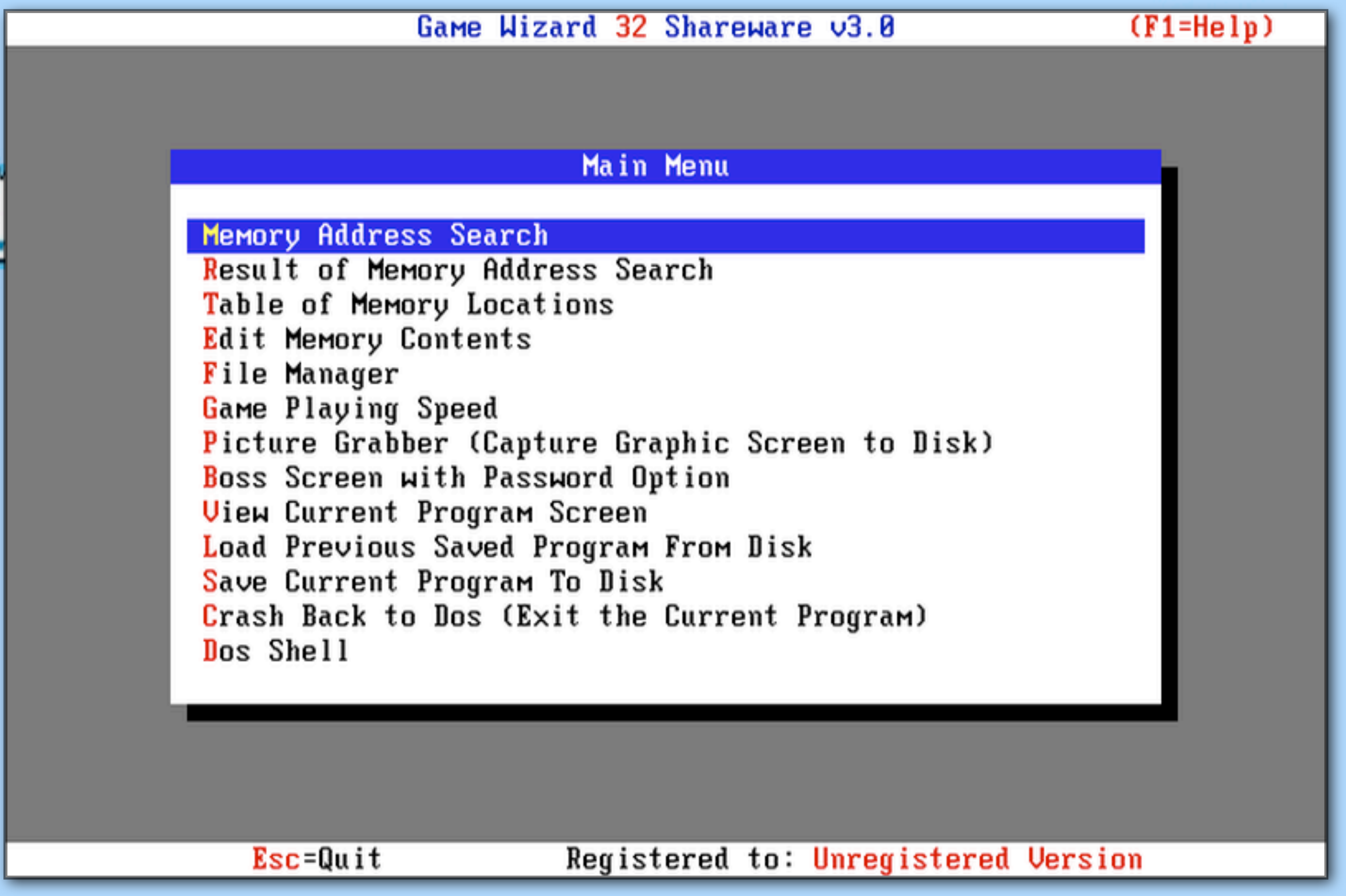
Game Genie is available for mutliple consoles.

Many similar devices and systems have been created, such as the GameShark.

ZaCon 4 - Game Hacking

1. Console Games
2. DOS Games
    - 2.1. Memory Scanning

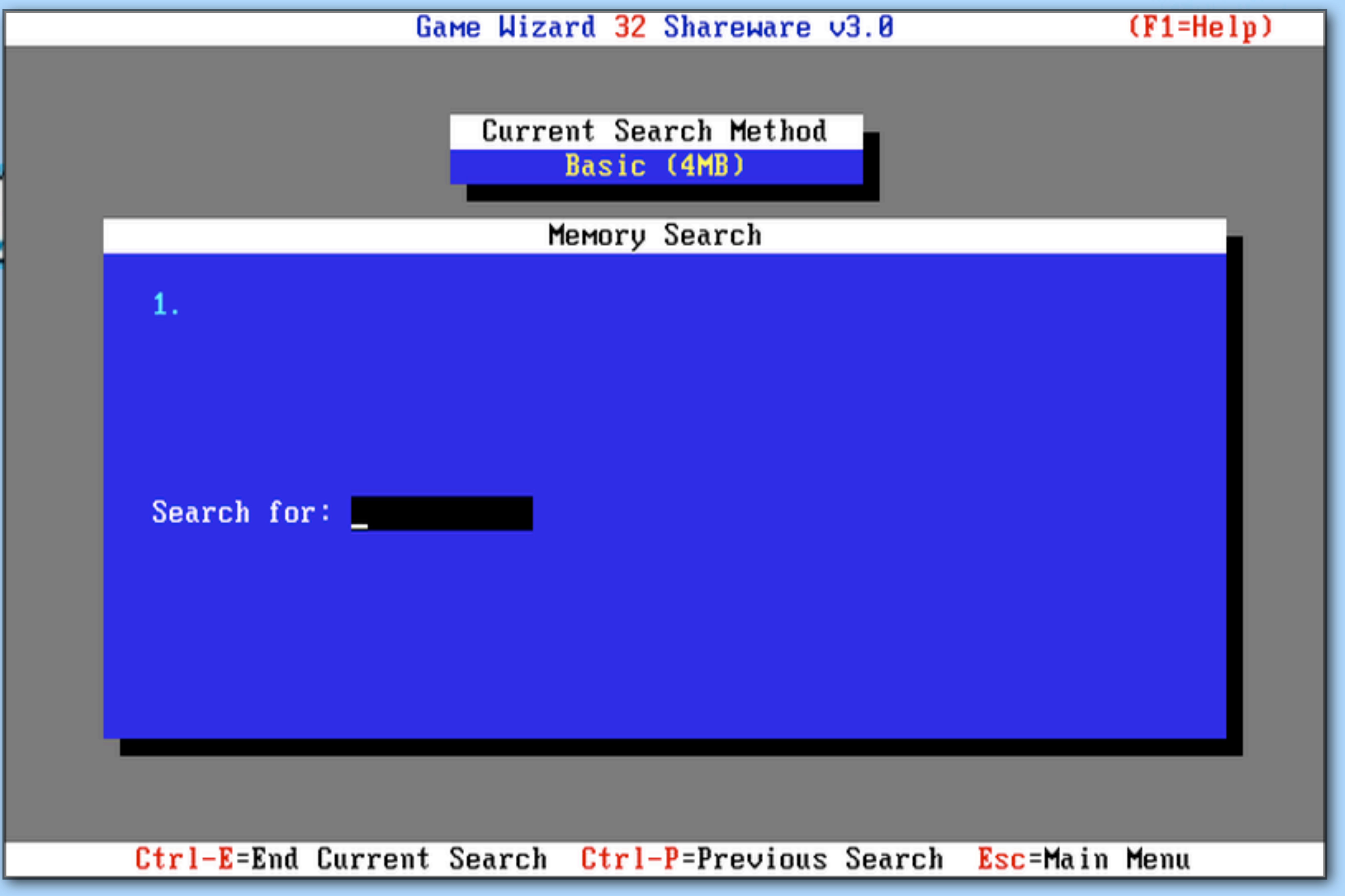
GAME HACKING



```
Game Wizard 32 Shareware v3.0                    (F1=Help)

                       Main Menu

 Memory Address Search
 Result of Memory Address Search
 Table of Memory Locations
 Edit Memory Contents
 File Manager
 Game Playing Speed
 Picture Grabber (Capture Graphic Screen to Disk)
 Boss Screen with Password Option
 View Current Program Screen
 Load Previous Saved Program From Disk
 Save Current Program To Disk
 Crash Back to Dos (Exit the Current Program)
 Dos Shell

Esc=Quit            Registered to: Unregistered Version
```

Game Wizard 32 is a DOS memory scanner

GAME HACKING

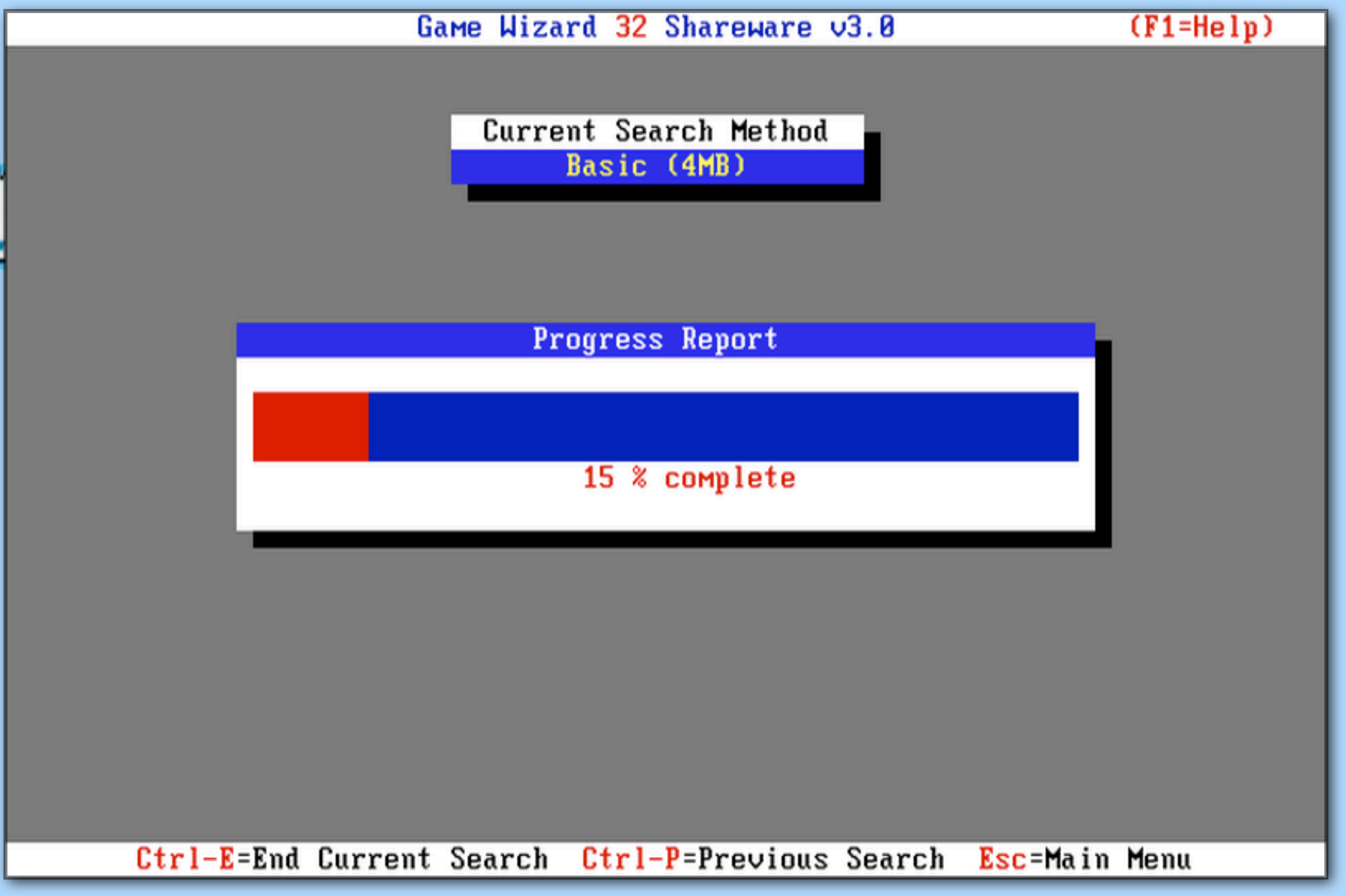


```
Game Wizard 32 Shareware v3.0                    (F1=Help)

              Current Search Method
                   Basic (4MB)

                  Memory Search

  1.



  Search for: _



Ctrl-E=End Current Search  Ctrl-P=Previous Search  Esc=Main Menu
```

Game Wizard 32 is a DOS memory scanner

Search for a value (eg: health, ammo, money) in game

GAME HACKING



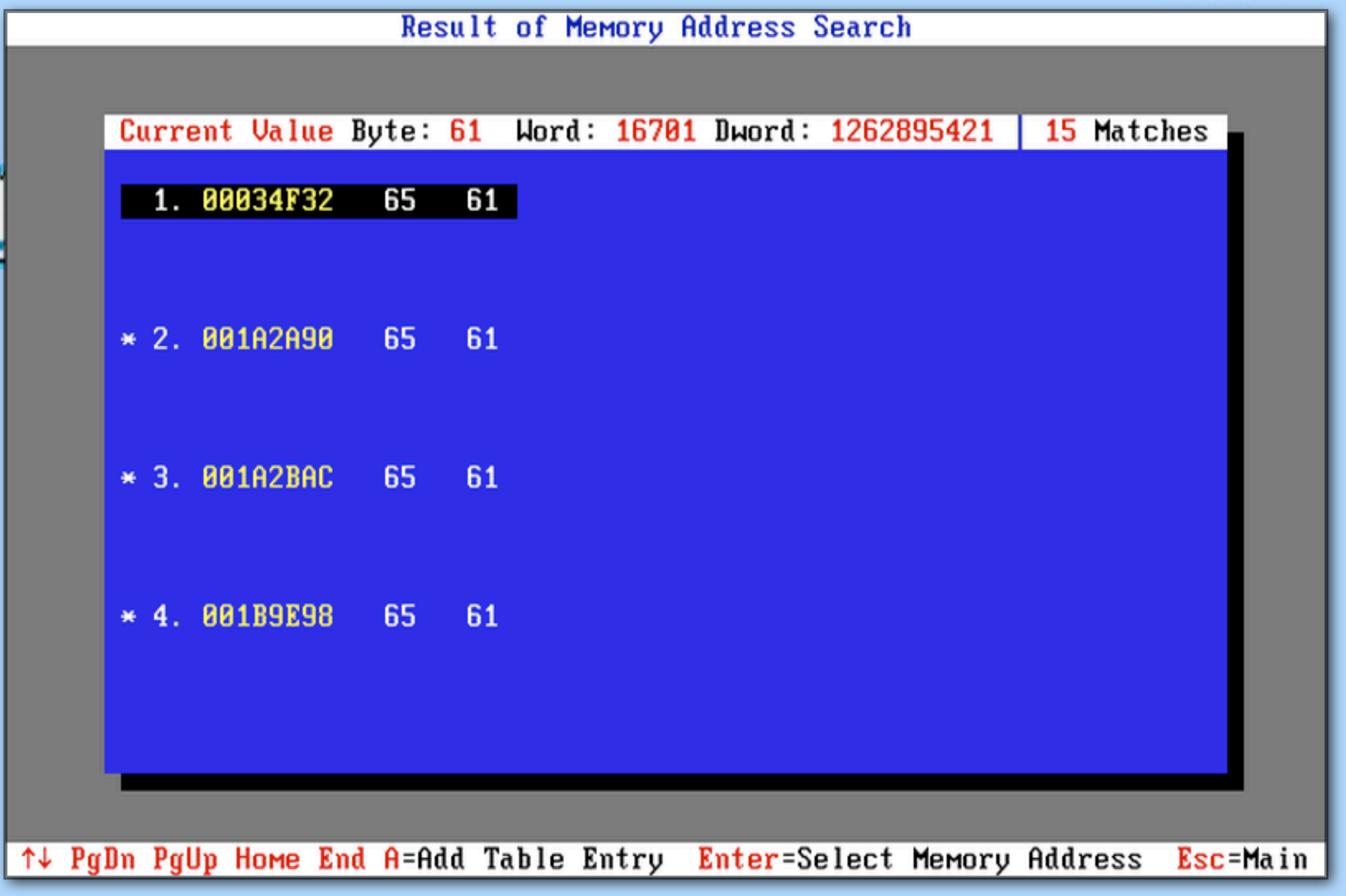
```
Game Wizard 32 Shareware v3.0                    (F1=Help)

              Current Search Method
                   Basic (4MB)

                  Progress Report

                   15 % complete

 Ctrl-E=End Current Search  Ctrl-P=Previous Search  Esc=Main Menu
```

Game Wizard 32 is a DOS memory scanner

Search for a value (eg: health, ammo, money) in game

Keep searching for the value, as is it changes

GAME HACKING



```
                    Result of Memory Address Search

 Current Value Byte: 61  Word: 16701 Dword: 1262895421 | 15 Matches

   1. 00034F32   65   61

 * 2. 001A2A90   65   61

 * 3. 001A2BAC   65   61

 * 4. 001B9E98   65   61

↑↓ PgDn PgUp Home End A=Add Table Entry  Enter=Select Memory Address  Esc=Main
```

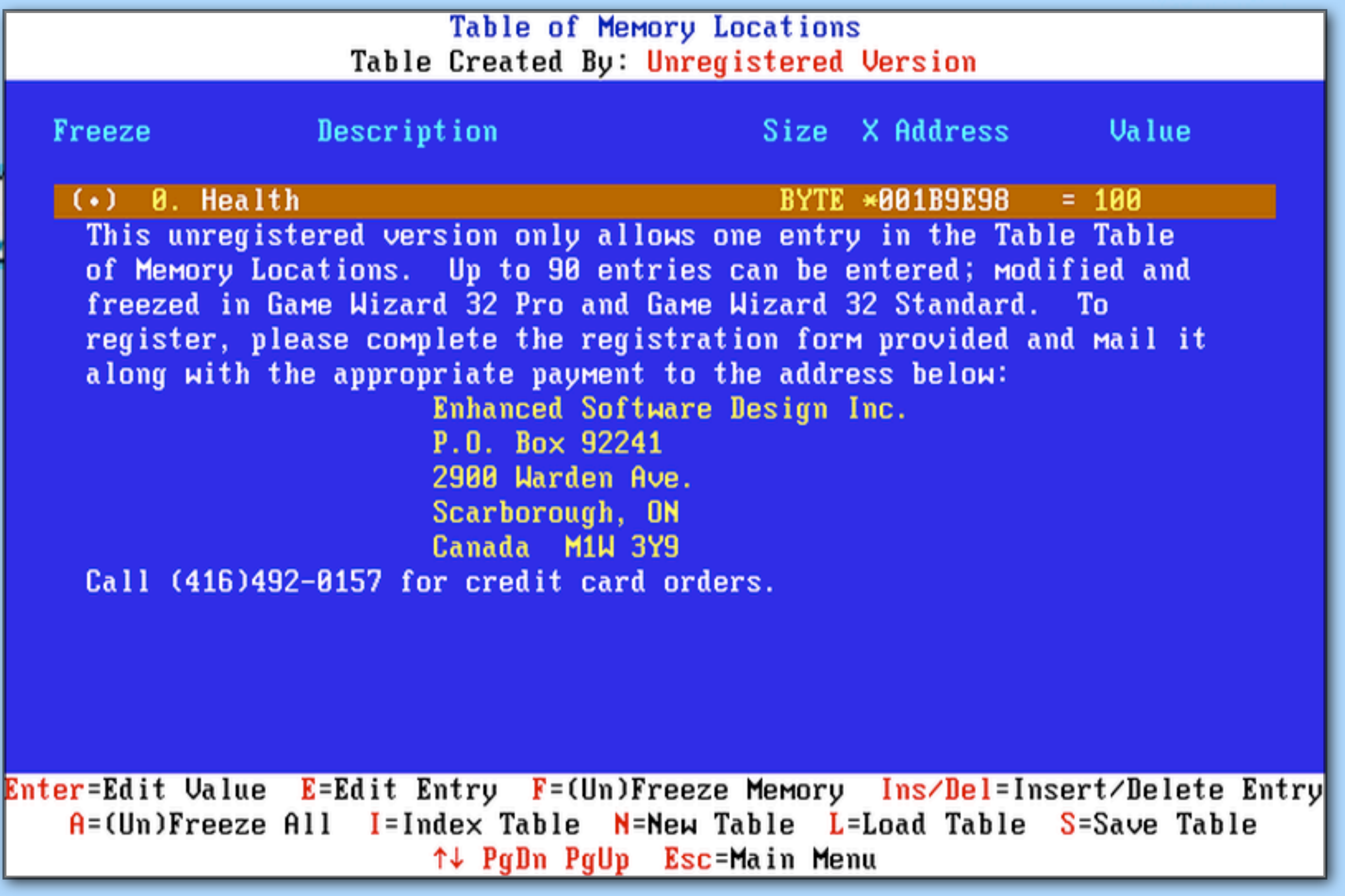
Game Wizard 32 is a DOS memory scanner

Search for a value (eg: health, ammo, money) in game

Keep searching for the value, as is it changes

Find the correct memory address (trial and error)

GAME HACKING



```
                    Table of Memory Locations
           Table Created By: Unregistered Version

  Freeze          Description             Size  X Address     Value

 (•)  0. Health                           BYTE *001B9E98    = 100
   This unregistered version only allows one entry in the Table Table
   of Memory Locations.  Up to 90 entries can be entered; modified and
   freezed in Game Wizard 32 Pro and Game Wizard 32 Standard.  To
   register, please complete the registration form provided and mail it
   along with the appropriate payment to the address below:
                      Enhanced Software Design Inc.
                      P.O. Box 92241
                      2900 Warden Ave.
                      Scarborough, ON
                      Canada  M1W 3Y9
   Call (416)492-0157 for credit card orders.

Enter=Edit Value  E=Edit Entry  F=(Un)Freeze Memory  Ins/Del=Insert/Delete Entry
    A=(Un)Freeze All  I=Index Table  N=New Table  L=Load Table  S=Save Table
                        ↑↓ PgDn PgUp  Esc=Main Menu
```

Game Wizard 32 is a DOS memory scanner

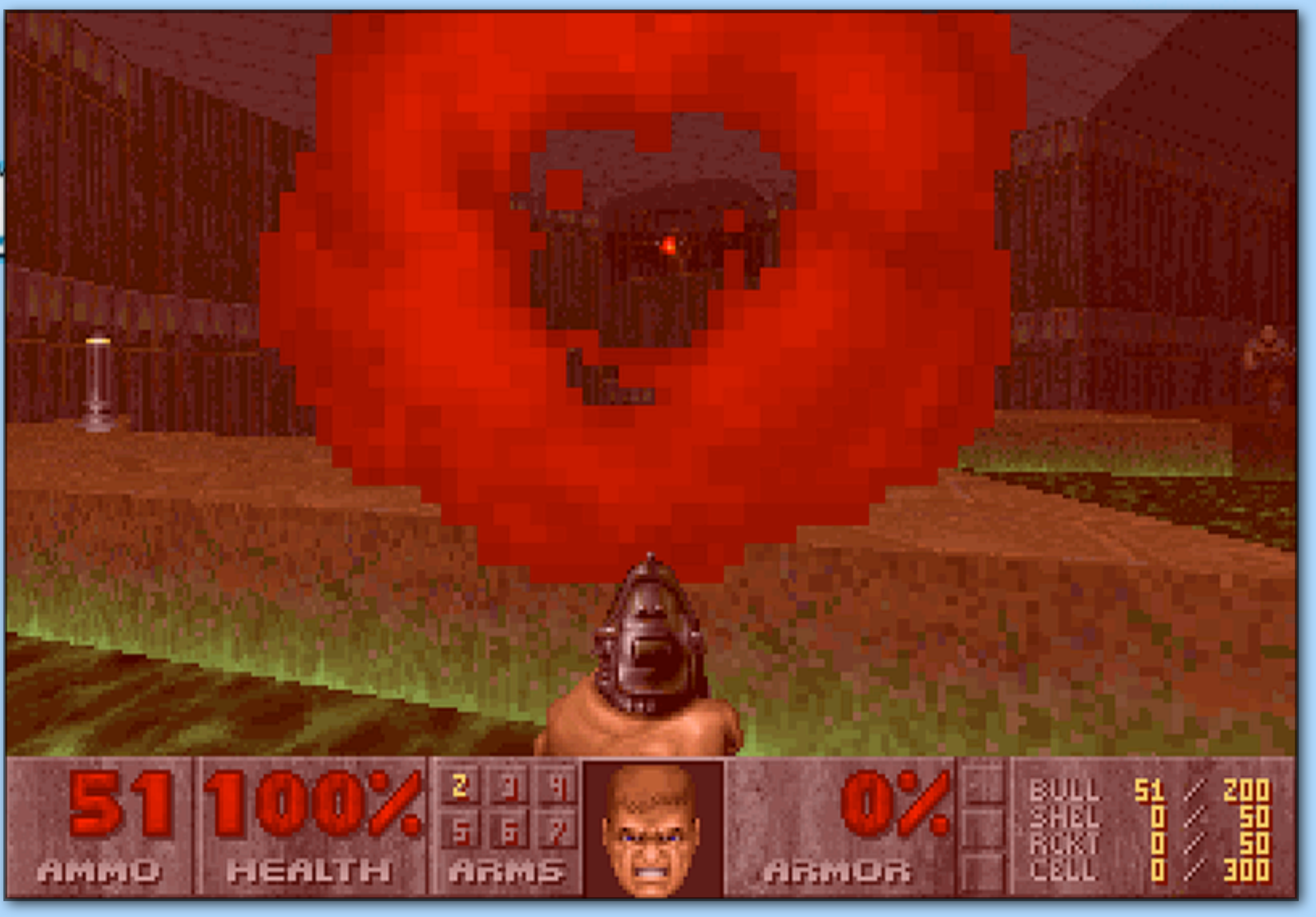
Search for a value (eg: health, ammo, money) in game

Keep searching for the value, as is it changes

Find the correct memory address (trial and error)

Enter a new value, and "freeze" it if desired

GAME HACKING



Game Wizard 32 is a DOS memory scanner

Search for a value (eg: health, ammo, money) in game

Keep searching for the value, as is it changes

Find the correct memory address (trial and error)

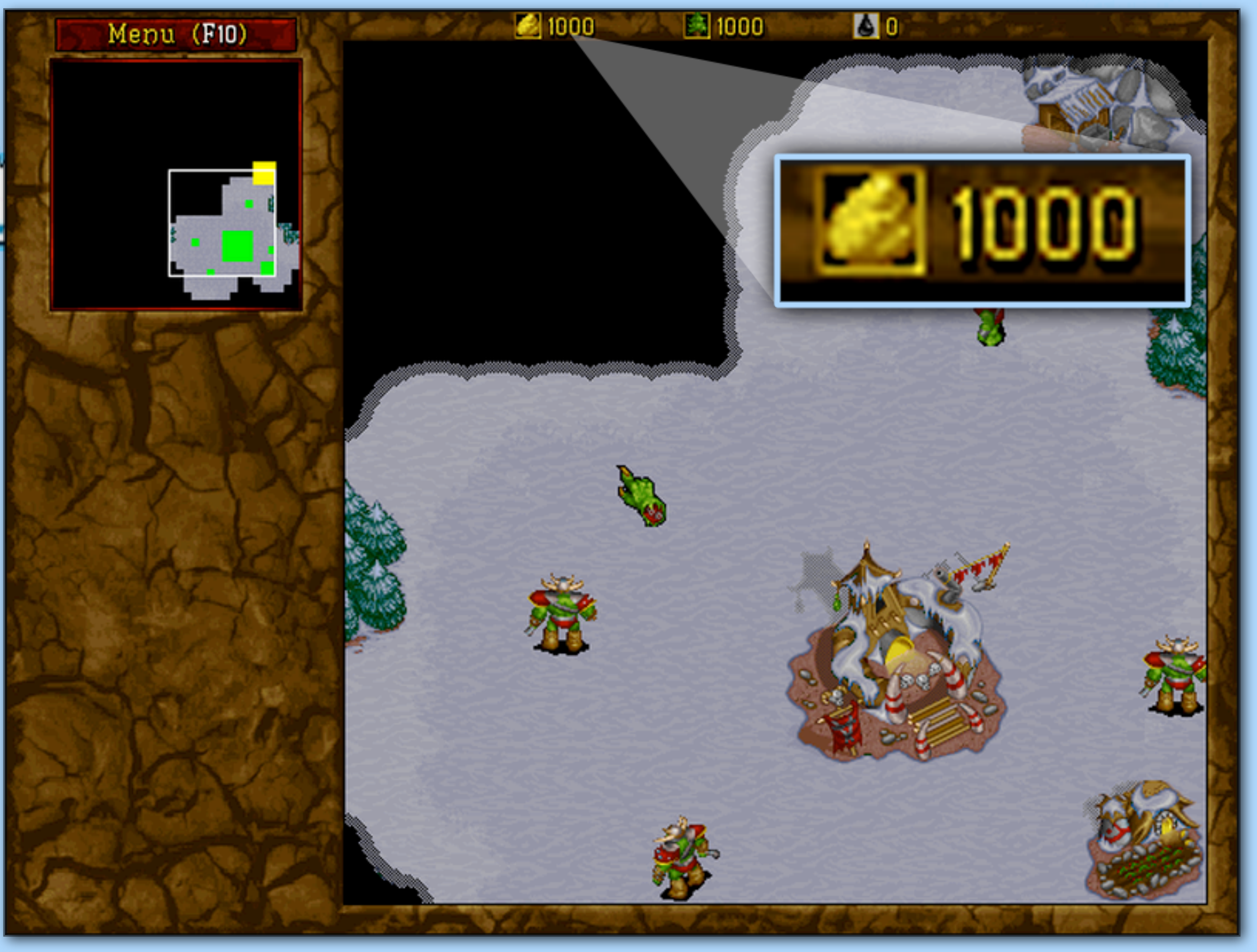
Enter a new value, and "freeze" it if desired

God mode!

ZaCon 4 - Game Hacking

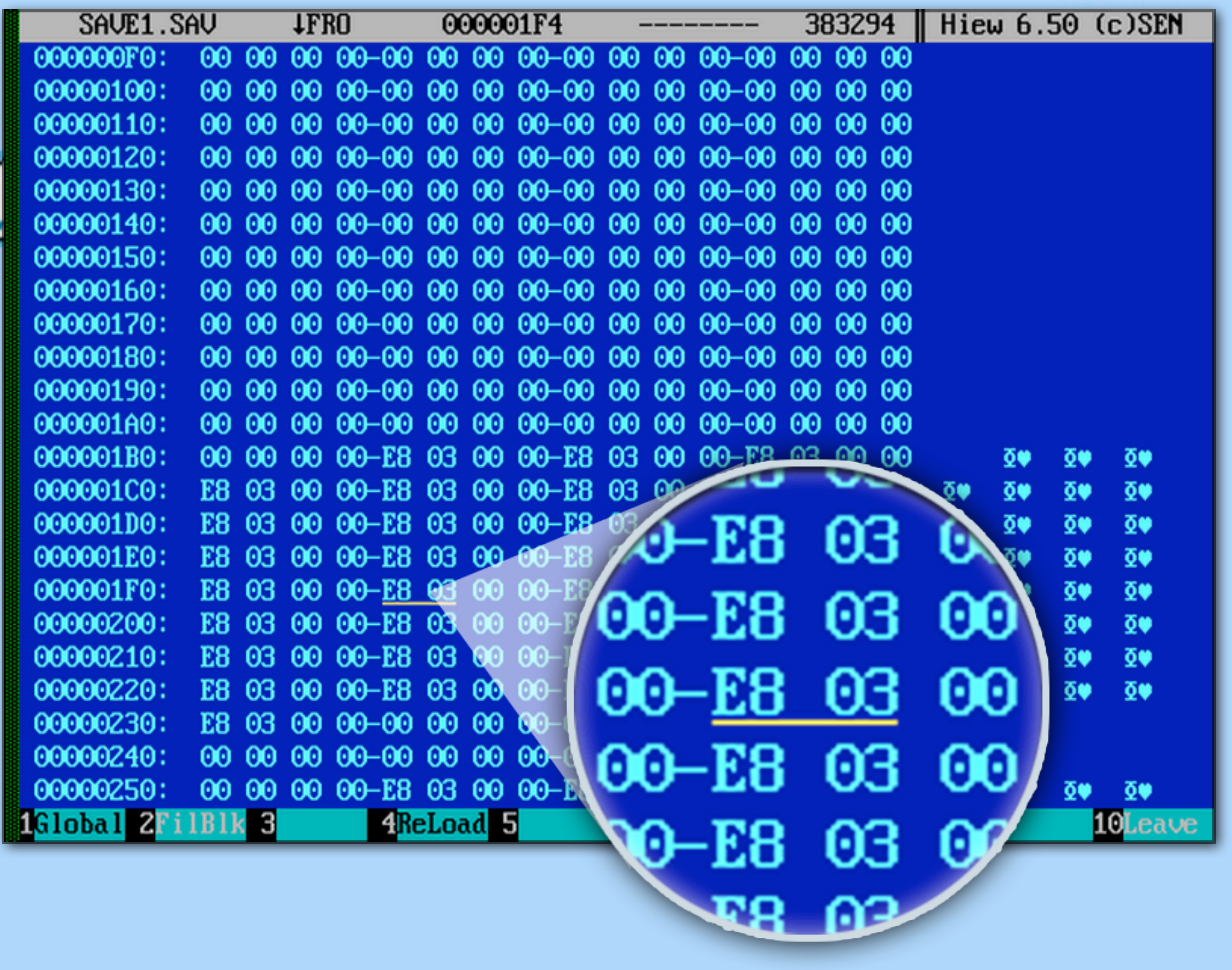
1. Console Games
2. DOS Games
   2.1. Memory Scanning
   2.2. Hex Editing save games

GAME HACKING



Take note of the value (eg: health, ammo, money) in game to be changed, and create a save game

GAME HACKING



```
 SAVE1.SAV      ↓FRO        000001F4     ---------     383294 ║ Hiew 6.50 (c)SEN
000000F0:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000100:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000110:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000120:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000130:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000140:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000150:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000160:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000170:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000180:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000190:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
000001A0:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
000001B0:  00 00 00 00-E8 03 00 00-E8 03 00 00-E8 03 00 00          Φ♥  Φ♥  Φ♥
000001C0:  E8 03 00 00-E8 03 00 00-E8 03 00                     Φ♥  Φ♥  Φ♥  Φ♥
000001D0:  E8 03 00 00-E8 03 00 00-E8 03                            Φ♥  Φ♥  Φ♥
000001E0:  E8 03 00 00-E8 03 00 00-E8                               Φ♥  Φ♥  Φ♥
000001F0:  E8 03 00 00-E8 03 00 00-E8                                   Φ♥  Φ♥
00000200:  E8 03 00 00-E8 03 00 00-E                                    Φ♥  Φ♥
00000210:  E8 03 00 00-E8 03 00 00-                                     Φ♥  Φ♥
00000220:  E8 03 00 00-E8 03 00 00-                                     Φ♥  Φ♥
00000230:  E8 03 00 00-00 00 00 00-
00000240:  00 00 00 00-00 00 00 00-
00000250:  00 00 00 00-E8 03 00 00-E                                    Φ♥  Φ♥
1Global 2FilBlk 3       4ReLoad 5                              10Leave
```

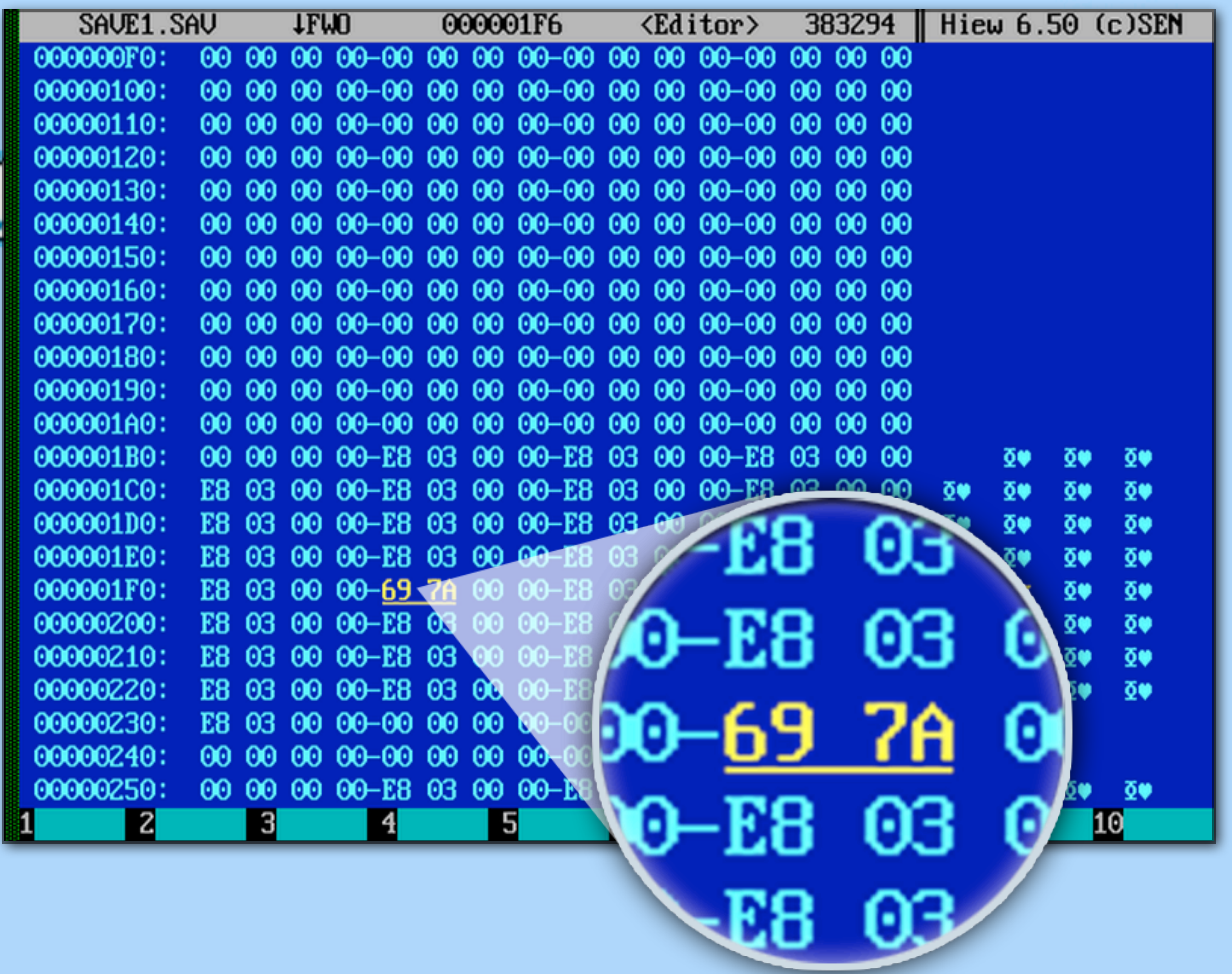
```
0-E8 03 0
00-E8 03 00
00-E8 03 00
00-E8 03 00
0-E8 03 0
E8 03
```

Take note of the value (eg: health, ammo, money) in game to be changed, and create a save game

Open the save game and find the hex value of the amount (bytes might be switched)

1000 = 03E8 in hex

GAME HACKING



```
 SAVE1.SAV      ↓FWO       000001F6     <Editor>   383294 ║ Hiew 6.50 (c)SEN
000000F0:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000100:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000110:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000120:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000130:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000140:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000150:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000160:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000170:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000180:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000190:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
000001A0:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
000001B0:  00 00 00 00-E8 03 00 00-E8 03 00 00-E8 03 00 00        Φ♥  Φ♥  Φ♥
000001C0:  E8 03 00 00-E8 03 00 00-E8 03 00 00-E8 03 00 00    Φ♥  Φ♥  Φ♥  Φ♥
000001D0:  E8 03 00 00-E8 03 00 00-E8 03 00                       Φ♥  Φ♥  Φ♥
000001E0:  E8 03 00 00-E8 03 00 00-E8 03                          Φ♥  Φ♥  Φ♥
000001F0:  E8 03 00 00-69 7A 00 00-E8 03                              Φ♥  Φ♥
00000200:  E8 03 00 00-E8 03 00 00-E8                                 Φ♥  Φ♥
00000210:  E8 03 00 00-E8 03 00 00-E8                                 Φ♥  Φ♥
00000220:  E8 03 00 00-E8 03 00 00-E8                                 Φ♥  Φ♥
00000230:  E8 03 00 00-00 00 00 00-00
00000240:  00 00 00 00-00 00 00 00-00
00000250:  00 00 00 00-E8 03 00 00-E8                                 Φ♥  Φ♥
1       2       3       4       5                                  10
```

Take note of the value (eg: health, ammo, money) in game to be changed, and create a save game

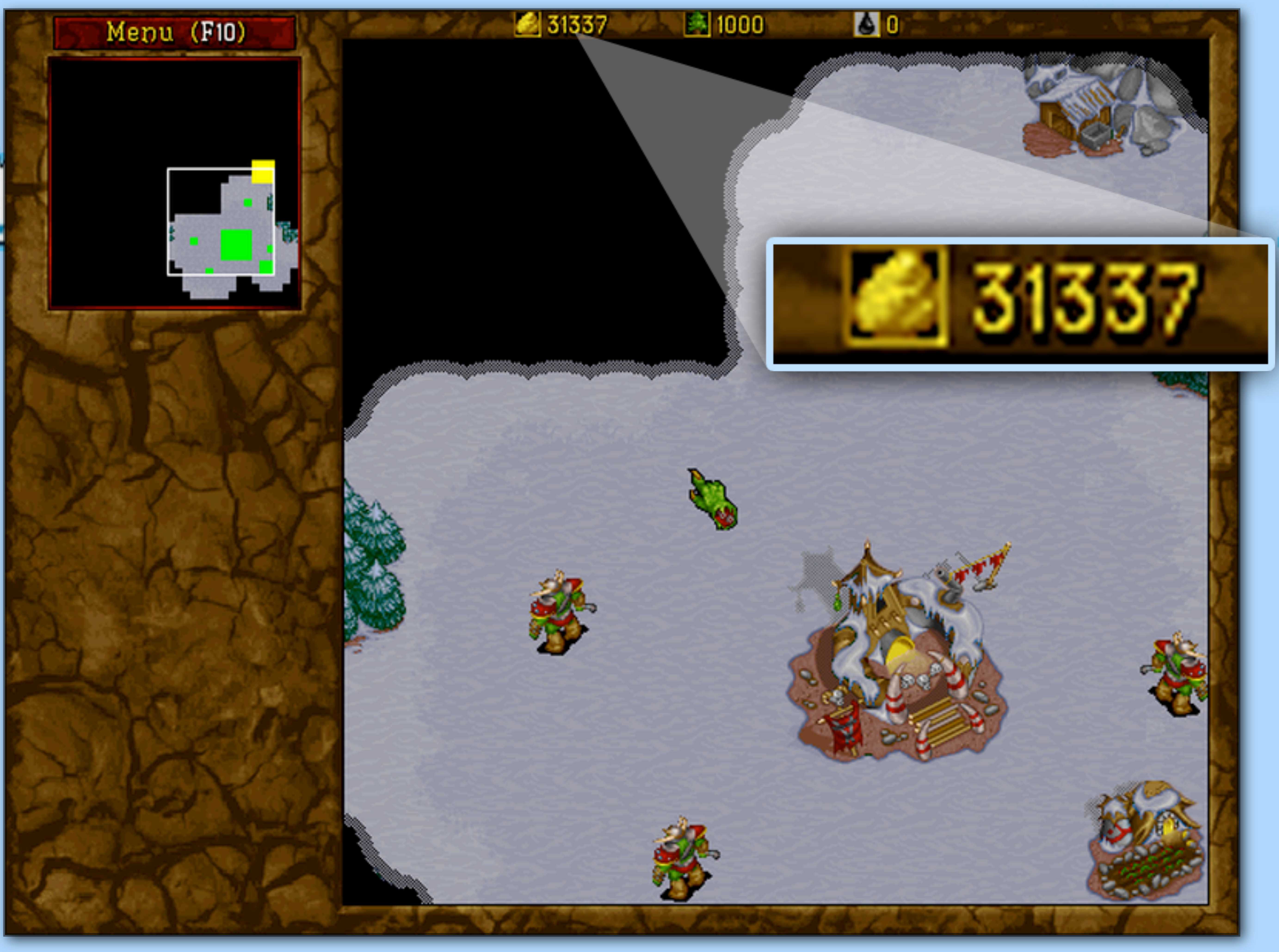
Open the save game and find the hex value of the amount (bytes might be switched)

1000 = 03E8 in hex

Overwrite with the new value (trial and error)

31337 = 7A69 in hex

GAME HACKING



Take note of the value (eg: health, ammo, money) in game to be changed, and create a save game

Open the save game and find the hex value of the amount (bytes might be switched)

1000 = 03E8 in hex

Overwrite with the new value (trial and error)

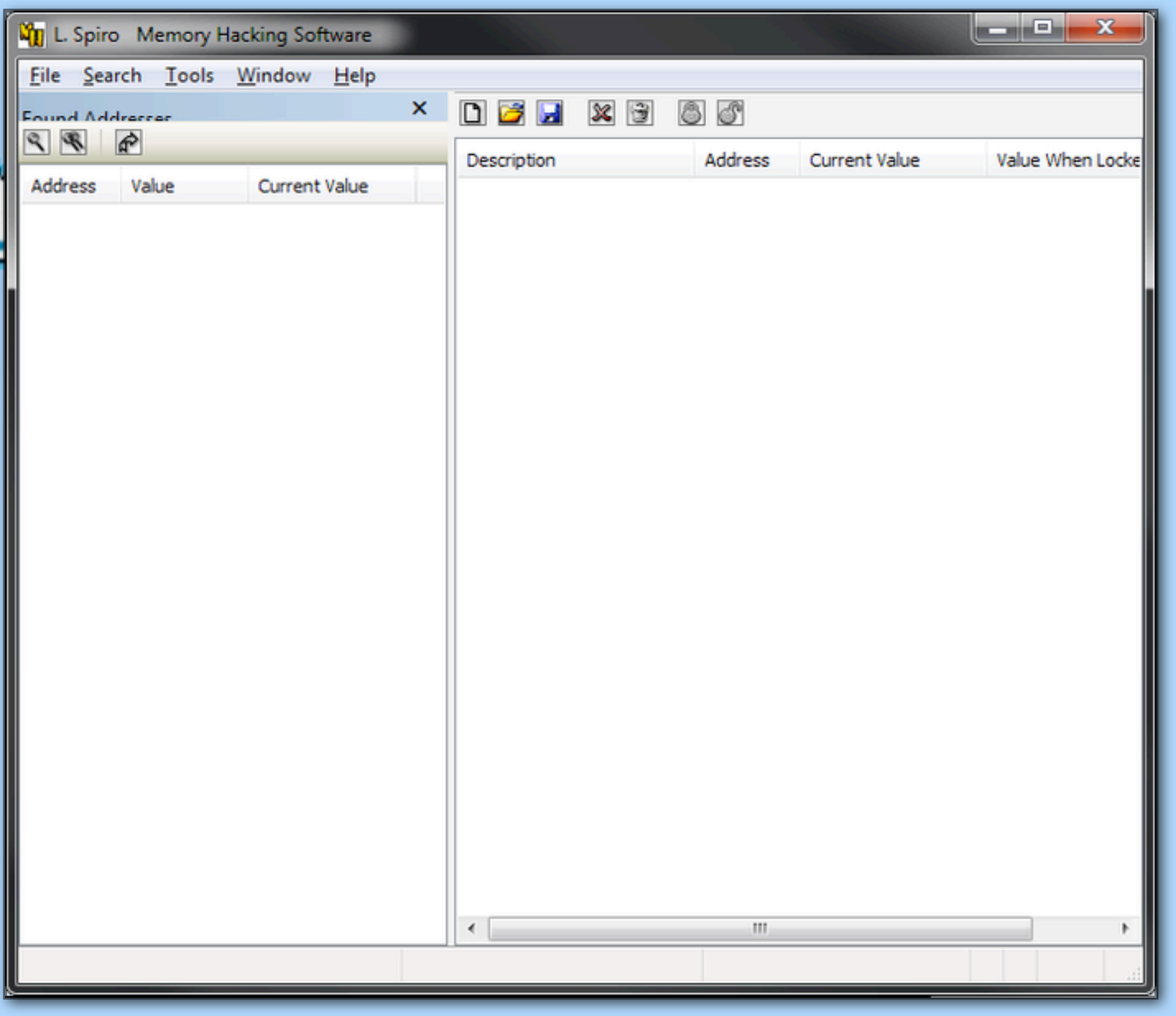
31337 = 7A69 in hex

Profit!

ZaCon 4 - Game Hacking

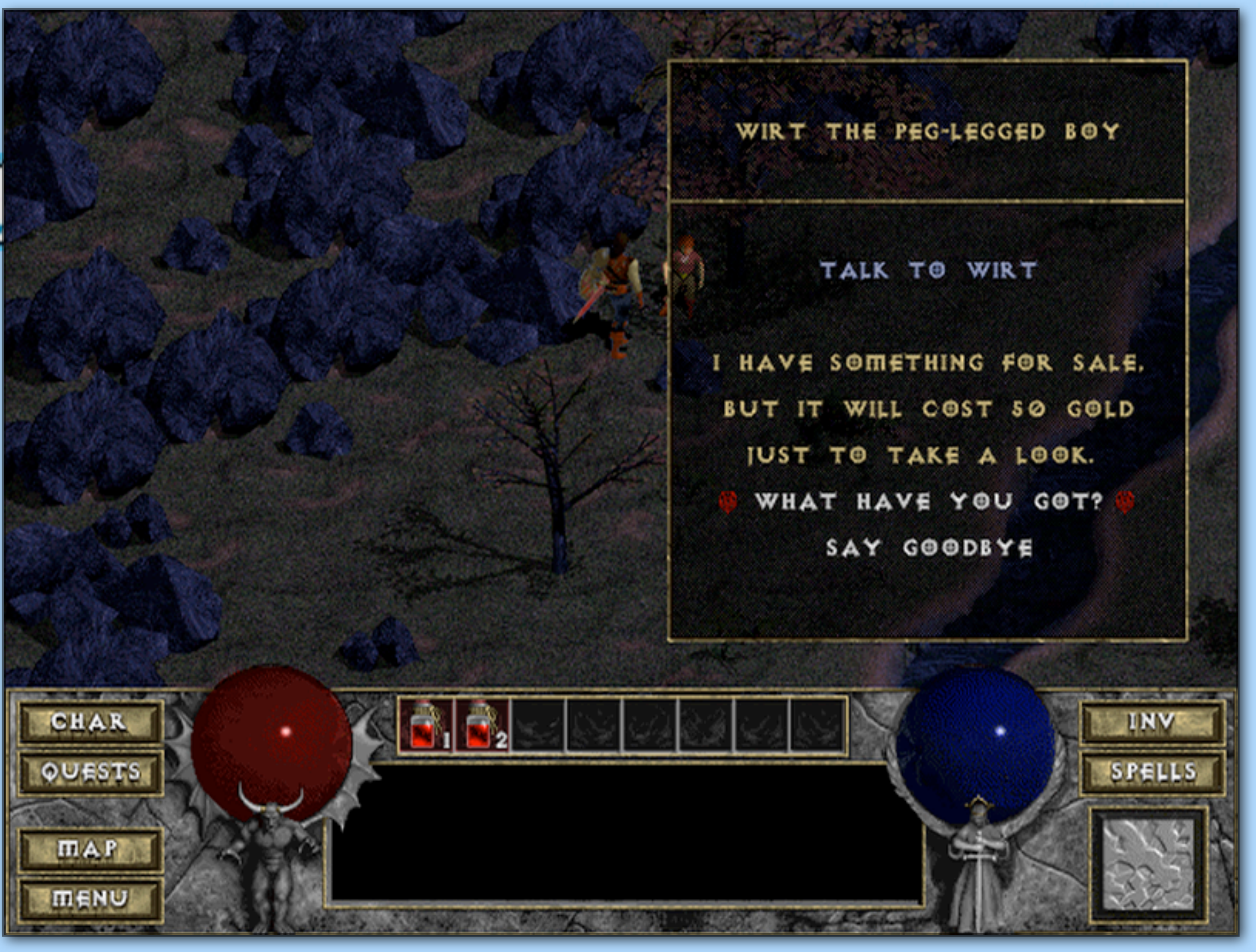
1. Console Games
2. DOS Games
3. Windows Games
    - 3.1. Diablo I & Memory Scanning

GAME HACKING



MHS ("Memory Hacking Software") is a great Windows memory scanner

GAME HACKING



WIRT THE PEG-LEGGED BOY

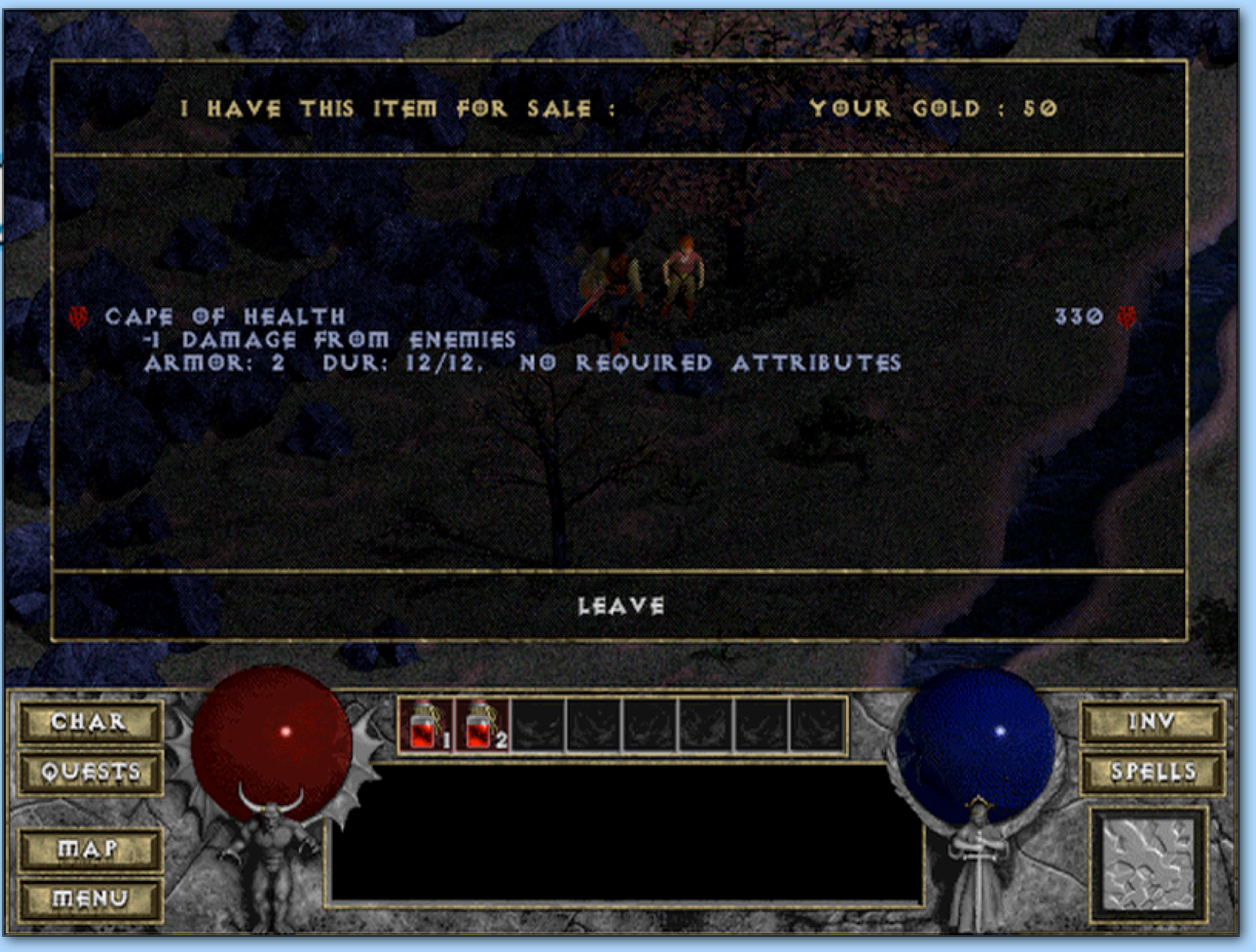
TALK TO WIRT

I HAVE SOMETHING FOR SALE,
BUT IT WILL COST 50 GOLD
JUST TO TAKE A LOOK.
WHAT HAVE YOU GOT?
SAY GOODBYE

MHS ("Memory Hacking Software") is a great Windows memory scanner

Some game mechanics are available to the game client even if not shown

GAME HACKING



I HAVE THIS ITEM FOR SALE :

YOUR GOLD : 50

CAPE OF HEALTH 330
-1 DAMAGE FROM ENEMIES
ARMOR: 2 DUR: 12/12, NO REQUIRED ATTRIBUTES

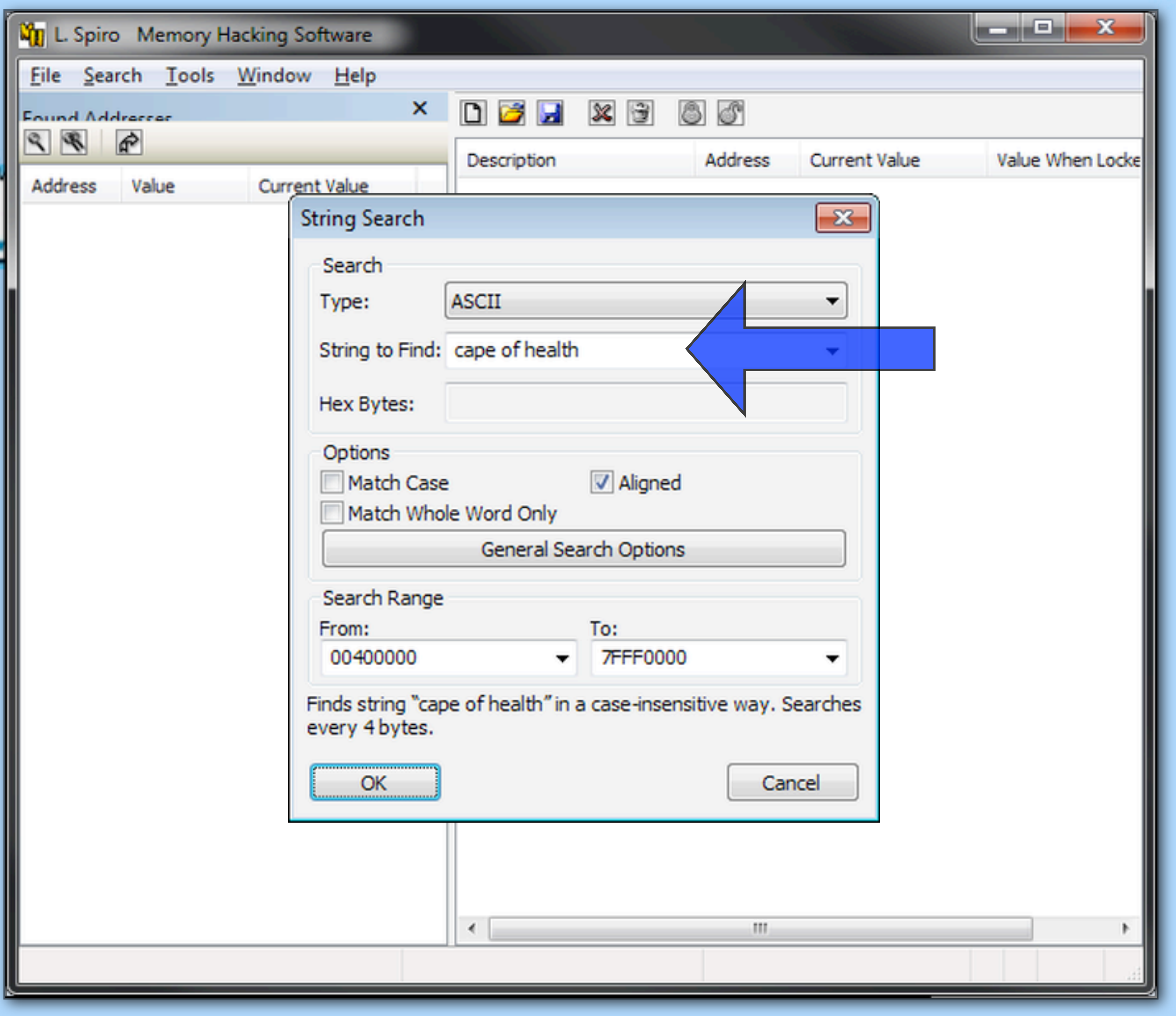
LEAVE

MHS ("Memory Hacking Software") is a great Windows memory scanner

Some game mechanics are available to the game client even if not shown

Eg: Wirt's "Cape of Health" in Diablo 1

GAME HACKING


L. Spiro Memory Hacking Software
File Search Tools Window Help
Found Addresses
Address Value Current Value
Description Address Current Value Value When Locke
String Search
OK
Cancel

Search

Type: ASCII

String to Find: cape of health

Hex Bytes:

Options

□ Match Case ☑ Aligned

□ Match Whole Word Only

General Search Options

Search Range

From: 00400000 To: 7FFF0000

Finds string "cape of health" in a case-insensitive way. Searches every 4 bytes.

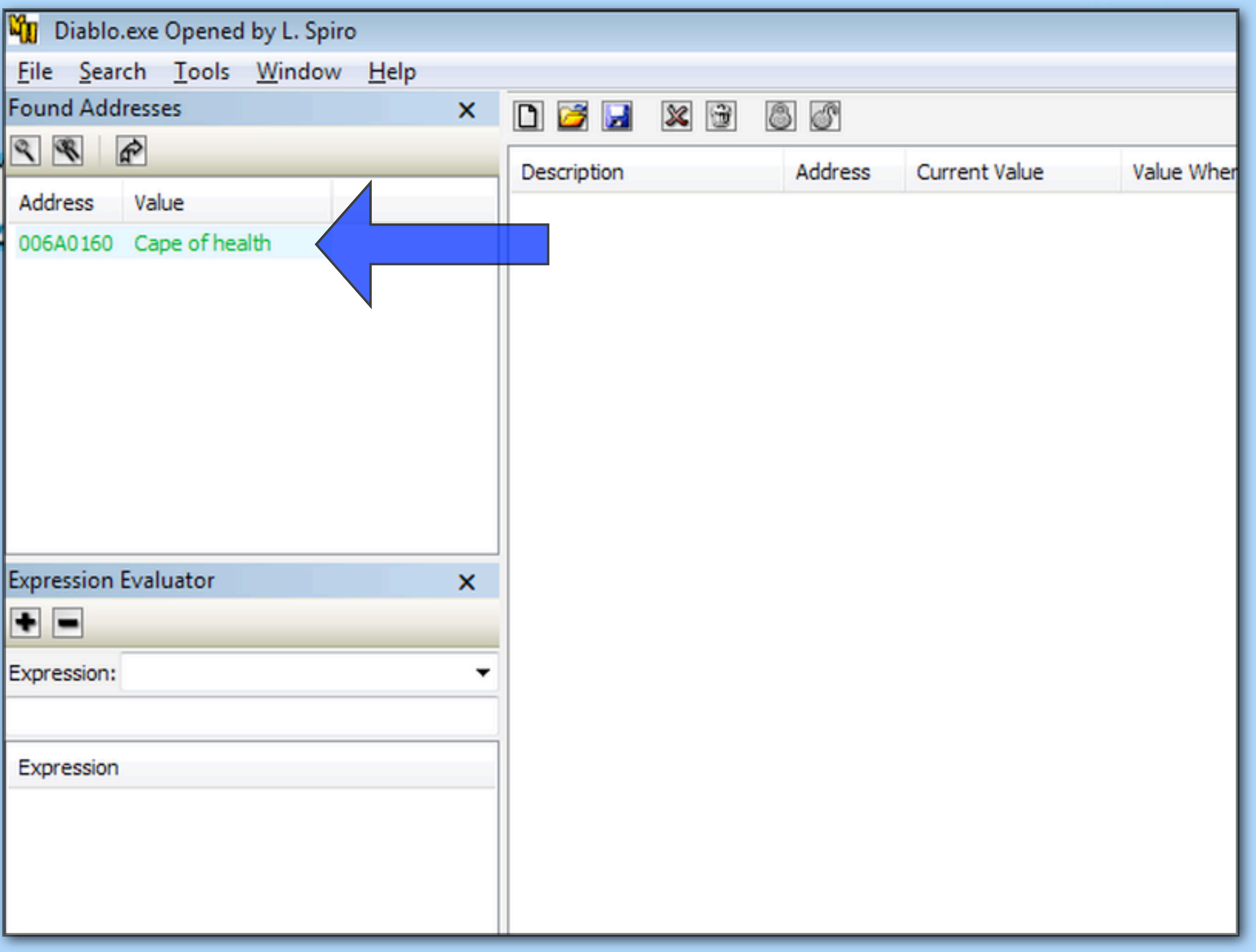
MHS ("Memory Hacking Software") is a great Windows memory scanner

Some game mechanics are available to the game client even if not shown

Eg: Wirt's "Cape of Health" in Diablo 1

Doing a "string" search for it in MHS...

GAME HACKING



Diablo.exe Opened by L. Spiro

Address	Value
006A0160	Cape of health

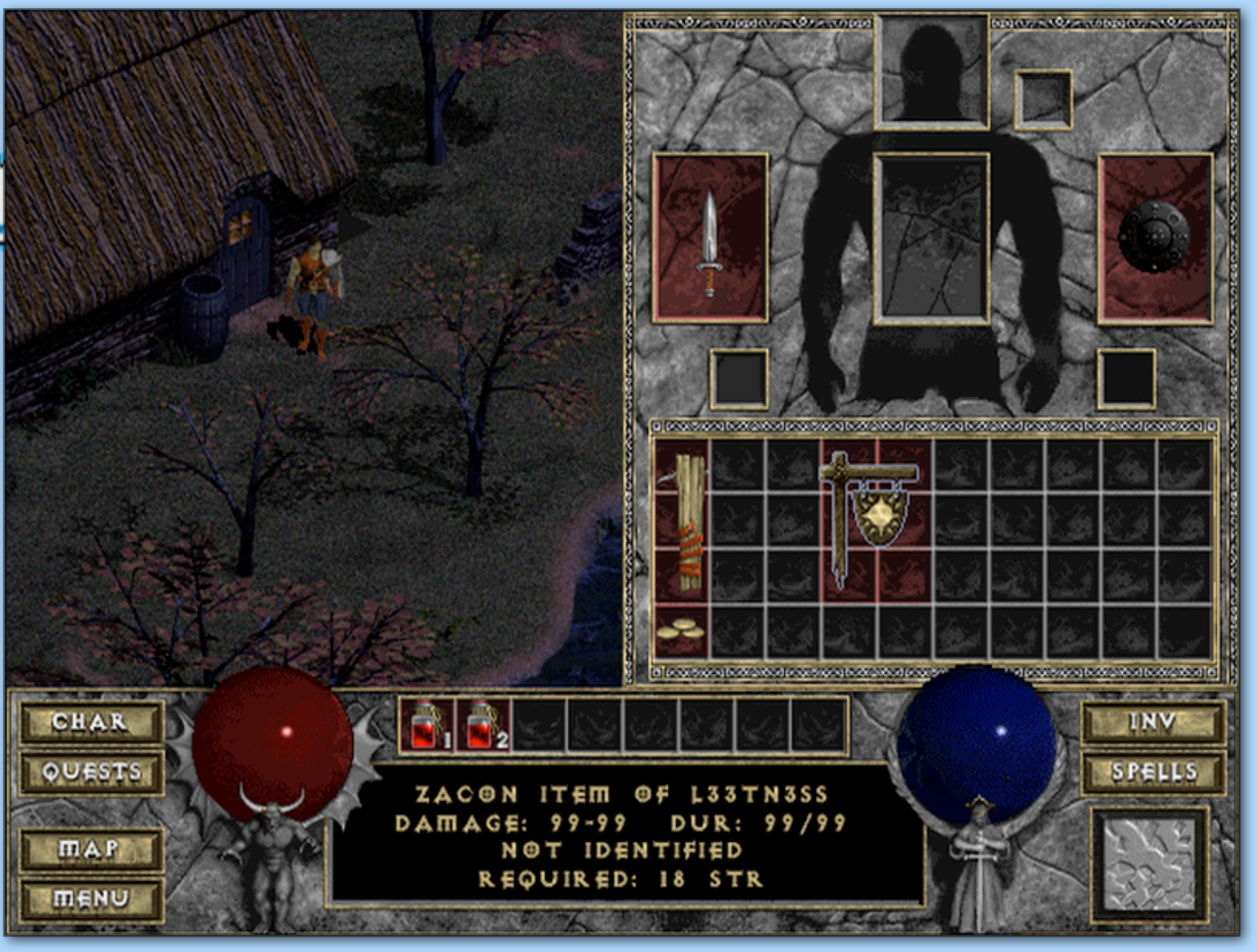
MHS ("Memory Hacking Software") is a great Windows memory scanner

Some game mechanics are available to the game client even if not shown

Eg: Wirt's "Cape of Health" in Diablo 1

Doing a "string" search for it in MHS... finds the address, which can be read in the future.

GAME HACKING



ZACON ITEM OF L33TN3SS
DAMAGE: 99-99 DUR: 99/99
NOT IDENTIFIED
REQUIRED: 18 STR

Diablo I had no multiplayer "state" checking

Game clients dictated the stats of their character to each other (peer to peer, via Battle.Net)

Character stats could be changed

Items could be exported, imported and modified

Custom items could be created (eg: "Zacon Item of L33tn3ss")

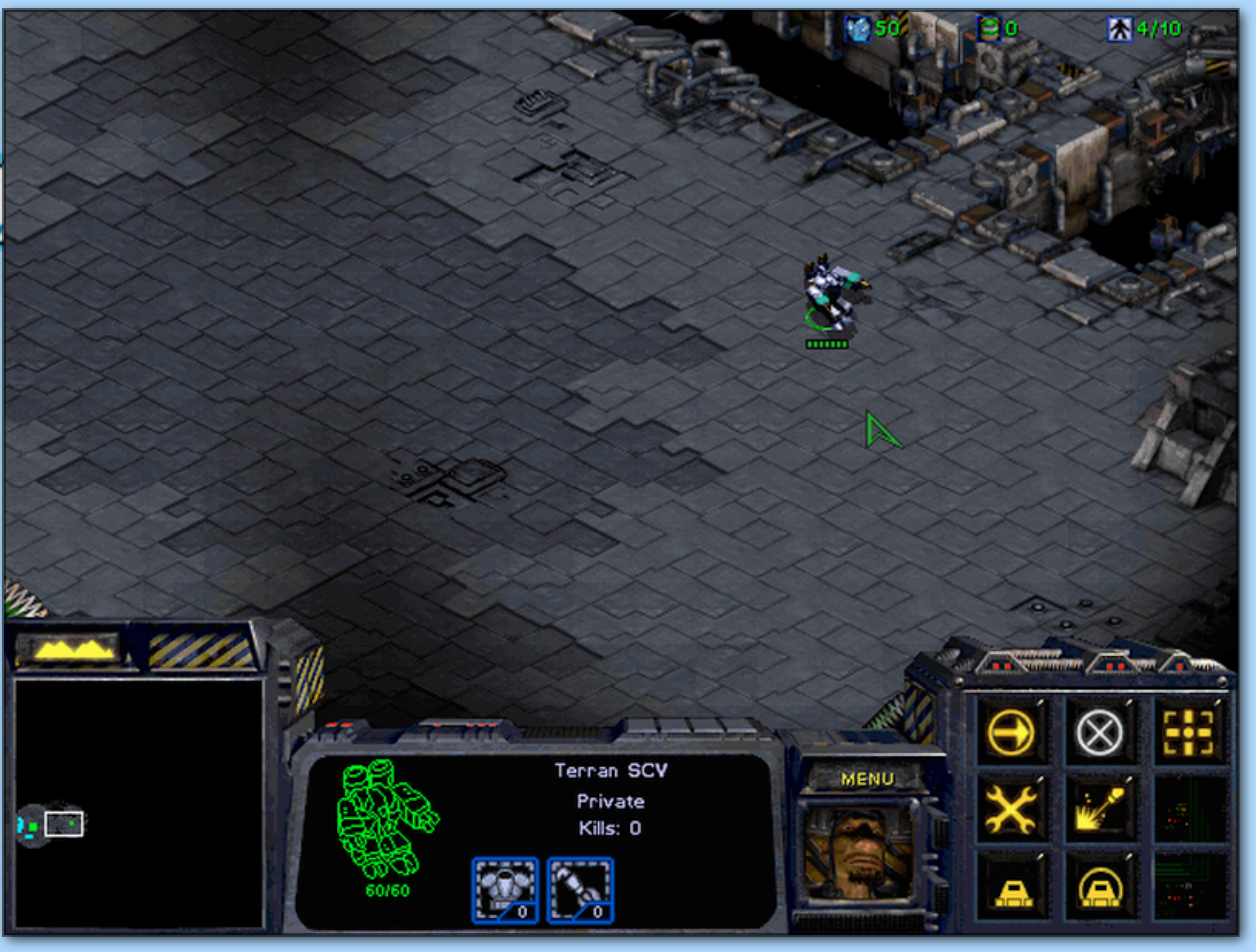
ZaCon 4 - Game Hacking

1. Console Games
2. DOS Games
3. Windows Games

   3.1. Diablo I & Memory Scanning

   3.2. StarCraft I map hack with OllyDbg (debugger)

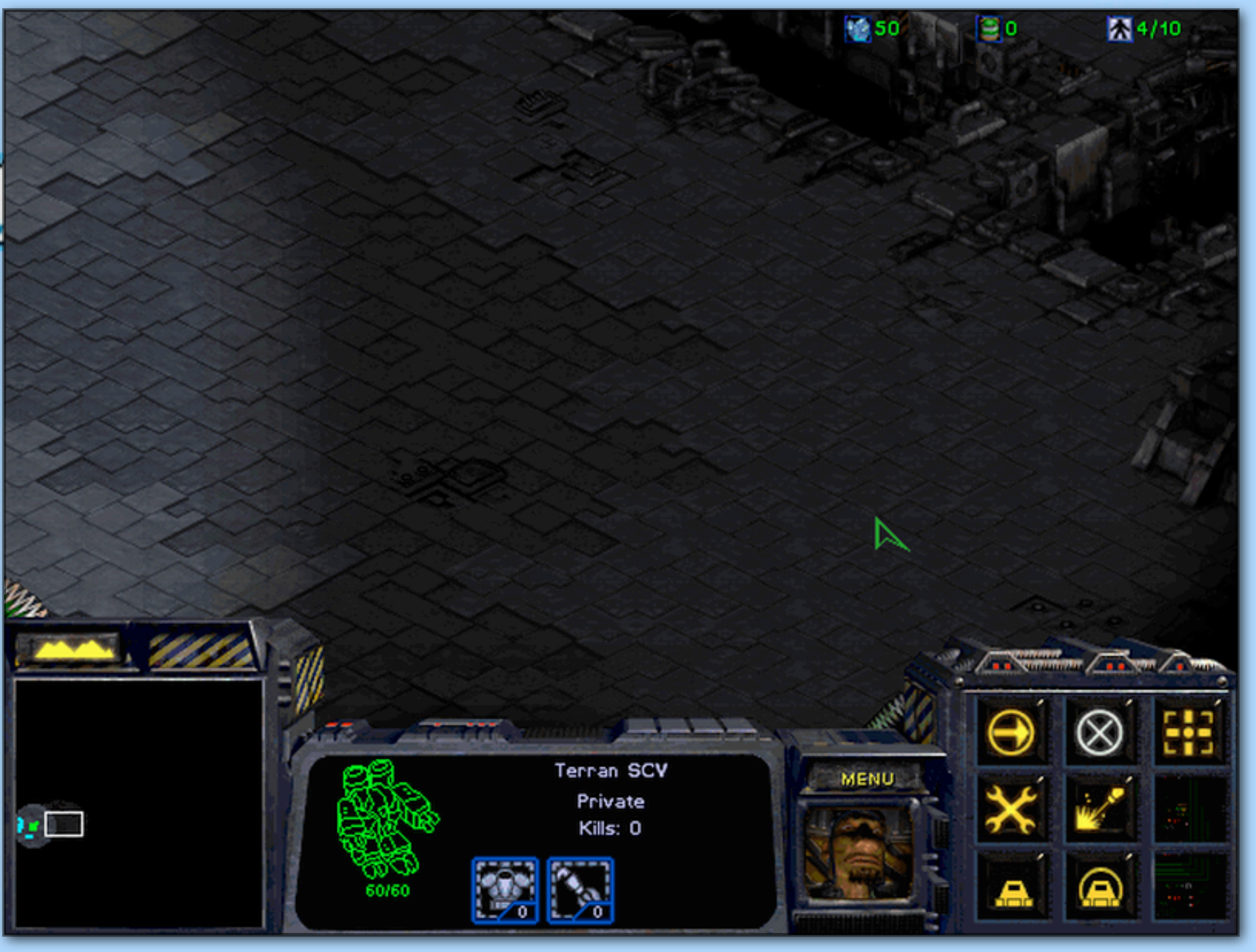
GAME HACKING



Making of a StarCraft map hack:

1. explore a new area, and search for “unknown” data

GAME HACKING

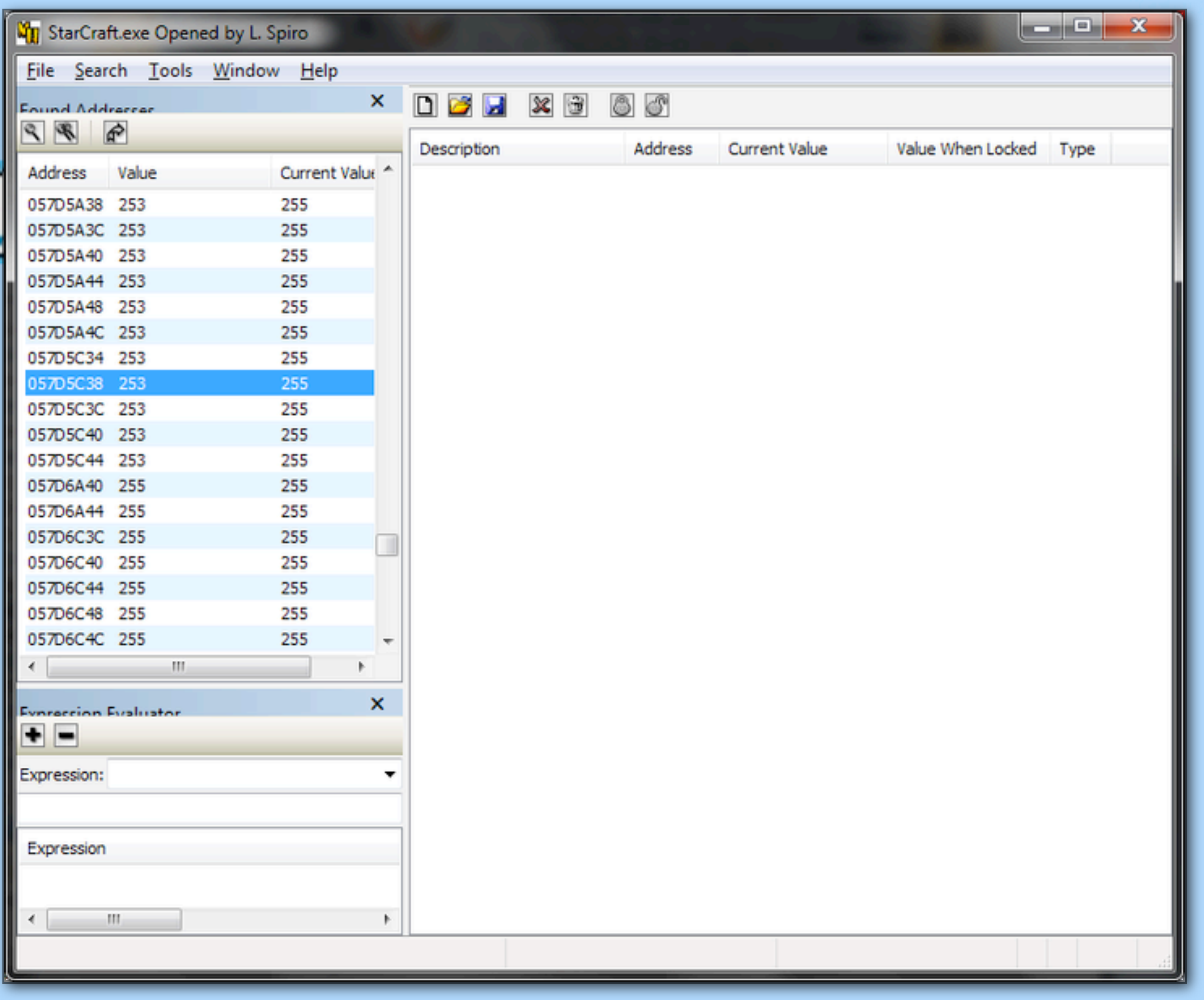


Making of a StarCraft map hack:

1. explore a new area, and search for "unknown" data

2. leave the area, and search again

GAME HACKING



Address	Value	Current Value
057D5A38	253	255
057D5A3C	253	255
057D5A40	253	255
057D5A44	253	255
057D5A48	253	255
057D5A4C	253	255
057D5C34	253	255
057D5C38	253	255
057D5C3C	253	255
057D5C40	253	255
057D5C44	253	255
057D6A40	255	255
057D6A44	255	255
057D6C3C	255	255
057D6C40	255	255
057D6C44	255	255
057D6C48	255	255
057D6C4C	255	255

Making of a StarCraft map hack:

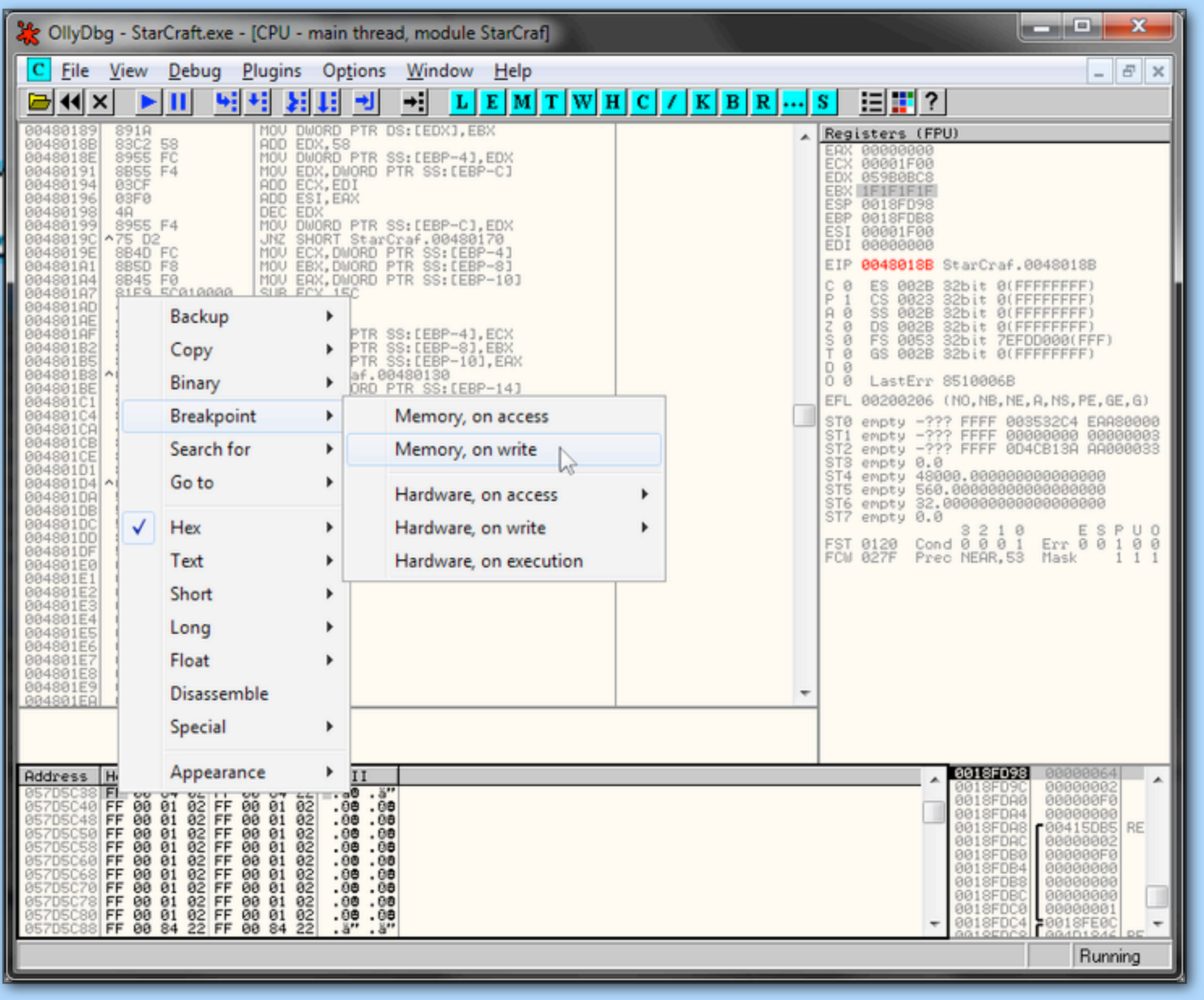
1. explore a new area, and search for “unknown” data

2. leave the area, and search again

3. repeat until “suspicious” results are found (lots of addresses changing between two values, in order)

4. copy one of these addresses

GAME HACKING



```
00480189   891A         MOV DWORD PTR DS:[EDX],EBX
0048018B   83C2 58      ADD EDX,58
0048018E   8955 FC      MOV DWORD PTR SS:[EBP-4],EDX
00480191   8B55 F4      MOV EDX,DWORD PTR SS:[EBP-C]
00480194   03CF         ADD ECX,EDI
00480196   03F0         ADD ESI,EAX
00480198   4A           DEC EDX
00480199   8955 F4      MOV DWORD PTR SS:[EBP-C],EDX
0048019C  ^75 D2        JNZ SHORT StarCraf.00480170
0048019E   8B4D FC      MOV ECX,DWORD PTR SS:[EBP-4]
004801A1   8B5D F8      MOV EBX,DWORD PTR SS:[EBP-8]
004801A4   8B45 F0      MOV EAX,DWORD PTR SS:[EBP-10]
004801A7   81E9 5C010000 SUB ECX,15C
004801AD
004801AE
004801AF                PTR SS:[EBP-4],ECX
004801B2                PTR SS:[EBP-8],EBX
004801B5                PTR SS:[EBP-10],EAX
004801B8  ^             af.00480130
004801BE                ORD PTR SS:[EBP-14]
004801C1
004801C4
004801CA
004801CB
004801CE
004801D1
004801D4  ^
004801DA
004801DB
004801DC
004801DD
004801DF
004801E0
004801E1
004801E2
004801E3
004801E4
004801E5
004801E6
004801E7
004801E8
004801E9
004801EA
```

```
Registers (FPU)
EAX 00000000
ECX 00001F00
EDX 059B0BC8
EBX 1F1F1F1F
ESP 0018FD98
EBP 0018FDB8
ESI 00001F00
EDI 00000000

EIP 0048018B StarCraf.0048018B

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 0  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 7EFDD000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr 8510006B

EFL 00200206 (NO,NB,NE,A,NS,PE,GE,G)

ST0 empty -??? FFFF 003532C4 EAA80000
ST1 empty -??? FFFF 00000000 00000003
ST2 empty -??? FFFF 0D4CB13A AA000033
ST3 empty 0.0
ST4 empty 48000.000000000000000
ST5 empty 560.00000000000000000
ST6 empty 32.000000000000000000
ST7 empty 0.0
               3 2 1 0      E S P U O
FST 0120  Cond 0 0 0 1  Err 0 0 1 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1
```

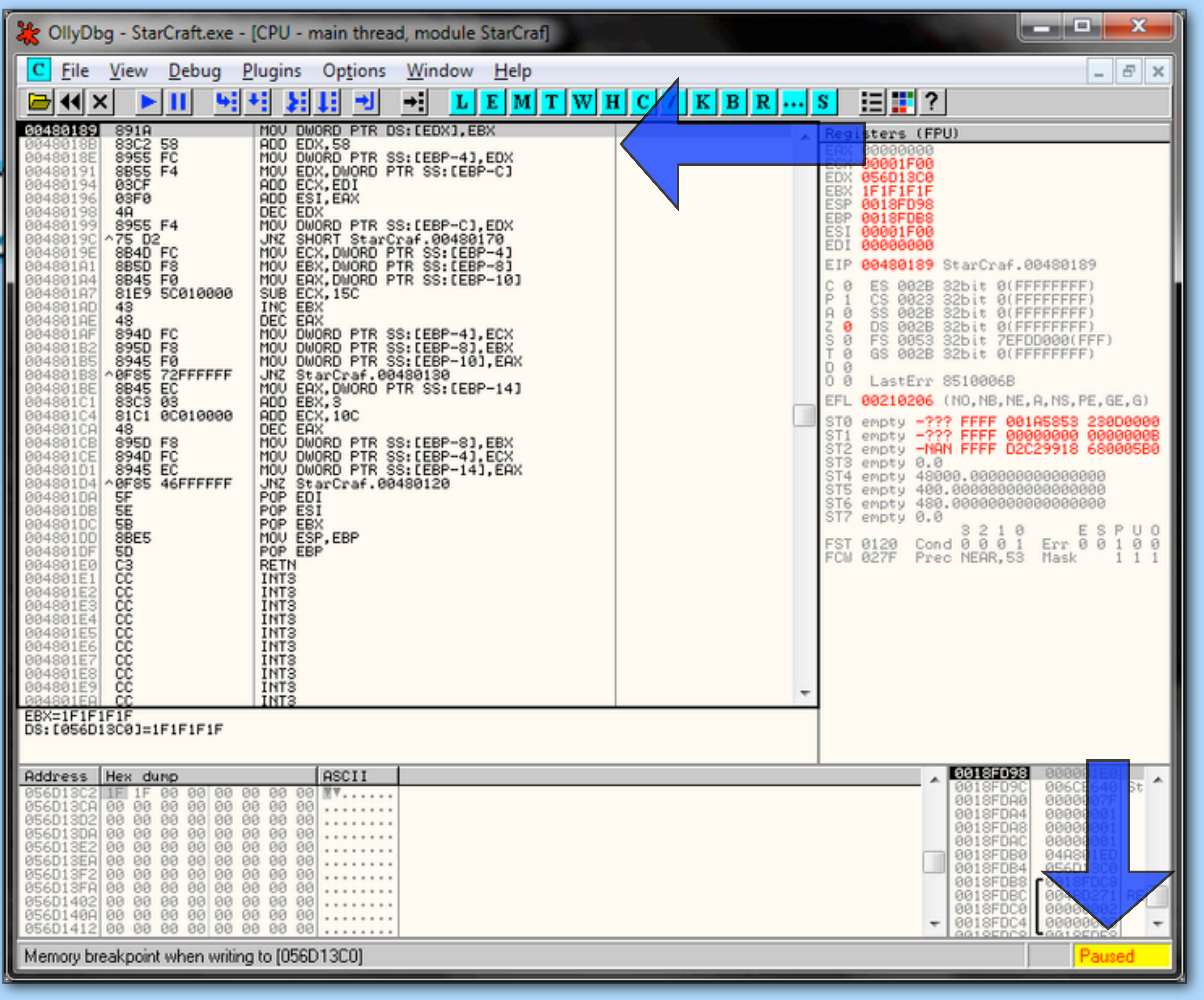
```
Address  He                        II
057D5C38 FF 00 84 22 FF 00 84 22   .ä" .ä"
057D5C40 FF 00 01 02 FF 00 01 02   .00 .00
057D5C48 FF 00 01 02 FF 00 01 02   .00 .00
057D5C50 FF 00 01 02 FF 00 01 02   .00 .00
057D5C58 FF 00 01 02 FF 00 01 02   .00 .00
057D5C60 FF 00 01 02 FF 00 01 02   .00 .00
057D5C68 FF 00 01 02 FF 00 01 02   .00 .00
057D5C70 FF 00 01 02 FF 00 01 02   .00 .00
057D5C78 FF 00 01 02 FF 00 01 02   .00 .00
057D5C80 FF 00 01 02 FF 00 01 02   .00 .00
057D5C88 FF 00 84 22 FF 00 84 22   .ä" .ä"
```

```
0018FD98  00000064
0018FD9C  00000002
0018FDA0  000000F0
0018FDA4  00000000
0018FDA8 [00415DB5  RE
0018FDAC  00000002
0018FDB0  000000F0
0018FDB4  00000000
0018FDB8  00000000
0018FDBC  00000000
0018FDC0  00000001
0018FDC4 [0018FE0C
```

Making of a StarCraft map hack:

5. attach OllyDbg to the game, and put a breakpoint on the memory address

GAME HACKING


OllyDbg - StarCraft.exe - [CPU - main thread, module StarCraf]
C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S
?
Registers (FPU)
Paused

```
00480189   891A            MOV DWORD PTR DS:[EDX],EBX
0048018B   83C2 58         ADD EDX,58
0048018E   8955 FC         MOV DWORD PTR SS:[EBP-4],EDX
00480191   8B55 F4         MOV EDX,DWORD PTR SS:[EBP-C]
00480194   03CF            ADD ECX,EDI
00480196   03F0            ADD ESI,EAX
00480198   4A              DEC EDX
00480199   8955 F4         MOV DWORD PTR SS:[EBP-C],EDX
0048019C  ^75 D2           JNZ SHORT StarCraf.00480170
0048019E   8B4D FC         MOV ECX,DWORD PTR SS:[EBP-4]
004801A1   8B5D F8         MOV EBX,DWORD PTR SS:[EBP-8]
004801A4   8B45 F0         MOV EAX,DWORD PTR SS:[EBP-10]
004801A7   81E9 5C010000   SUB ECX,15C
004801AD   43              INC EBX
004801AE   48              DEC EAX
004801AF   894D FC         MOV DWORD PTR SS:[EBP-4],ECX
004801B2   895D F8         MOV DWORD PTR SS:[EBP-8],EBX
004801B5   8945 F0         MOV DWORD PTR SS:[EBP-10],EAX
004801B8  ^0F85 72FFFFFF   JNZ StarCraf.00480130
004801BE   8B45 EC         MOV EAX,DWORD PTR SS:[EBP-14]
004801C1   83C3 03         ADD EBX,3
004801C4   81C1 0C010000   ADD ECX,10C
004801CA   48              DEC EAX
004801CB   895D F8         MOV DWORD PTR SS:[EBP-8],EBX
004801CE   894D FC         MOV DWORD PTR SS:[EBP-4],ECX
004801D1   8945 EC         MOV DWORD PTR SS:[EBP-14],EAX
004801D4  ^0F85 46FFFFFF   JNZ StarCraf.00480120
004801DA   5F              POP EDI
004801DB   5E              POP ESI
004801DC   5B              POP EBX
004801DD   8BE5            MOV ESP,EBP
004801DF   5D              POP EBP
004801E0   C3              RETN
004801E1   CC              INT3
004801E2   CC              INT3
004801E3   CC              INT3
004801E4   CC              INT3
004801E5   CC              INT3
004801E6   CC              INT3
004801E7   CC              INT3
004801E8   CC              INT3
004801E9   CC              INT3
004801EA   CC              INT3
EBX=1F1F1F1F
DS:[056D13C0]=1F1F1F1F
```

```
Registers (FPU)
EAX 00000000
ECX 00001F00
EDX 056D13C0
EBX 1F1F1F1F
ESP 0018FD98
EBP 0018FDB8
ESI 00001F00
EDI 00000000

EIP 00480189 StarCraf.00480189

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 0  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 7EFDD000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr 8510006B

EFL 00210206 (NO,NB,NE,A,NS,PE,GE,G)

ST0 empty -??? FFFF 001A5853 230D0000
ST1 empty -??? FFFF 00000000 0000000B
ST2 empty -NAN FFFF D2C29918 680005B0
ST3 empty 0.0
ST4 empty 48000.0000000000000000
ST5 empty 400.00000000000000000
ST6 empty 480.00000000000000000
ST7 empty 0.0
               3 2 1 0      E S P U O
FST 0120  Cond 0 0 0 1  Err 0 0 1 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1
```

```
Address   Hex dump                  ASCII
056D13C2  1F 1F 00 00 00 00 00 00   ▼▼......
056D13CA  00 00 00 00 00 00 00 00   ........
056D13D2  00 00 00 00 00 00 00 00   ........
056D13DA  00 00 00 00 00 00 00 00   ........
056D13E2  00 00 00 00 00 00 00 00   ........
056D13EA  00 00 00 00 00 00 00 00   ........
056D13F2  00 00 00 00 00 00 00 00   ........
056D13FA  00 00 00 00 00 00 00 00   ........
056D1402  00 00 00 00 00 00 00 00   ........
056D140A  00 00 00 00 00 00 00 00   ........
056D1412  00 00 00 00 00 00 00 00   ........
```

```
0018FD98
0018FD9C
0018FDA0
0018FDA4
0018FDA8
0018FDAC
0018FDB0
0018FDB4
0018FDB8
0018FDBC
0018FDC0
0018FDC4
```

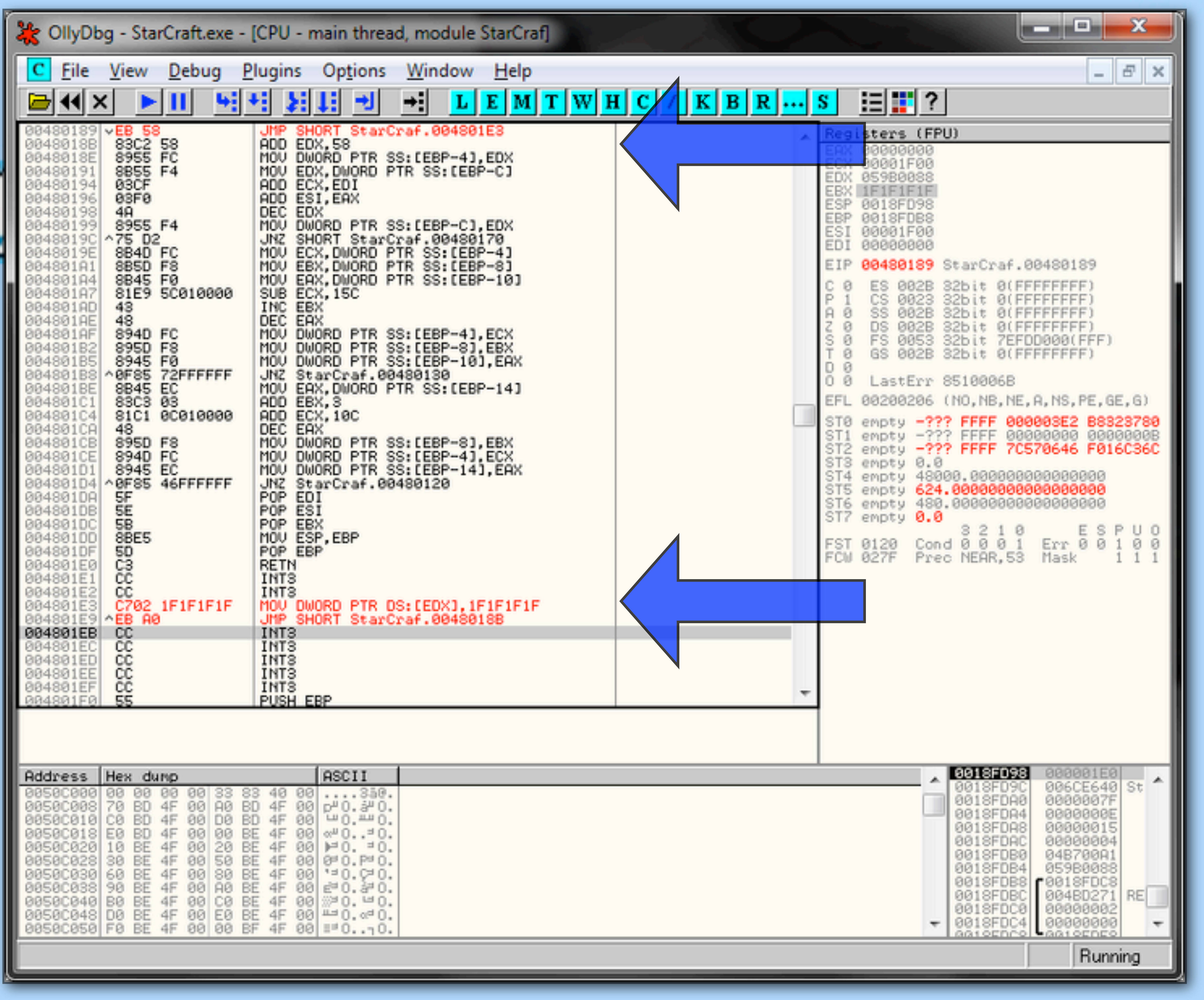
Memory breakpoint when writing to [056D13C0]

Making of a StarCraft map hack:

5. attach OllyDbg to the game, and put a breakpoint on the memory address

6. wait for the game to pause (map being redrawn)

GAME HACKING


OllyDbg - StarCraft.exe - [CPU - main thread, module StarCraf]
C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S ?

```
00480189 ˅EB 58          JMP SHORT StarCraf.004801E3
0048018B  83C2 58        ADD EDX,58
0048018E  8955 FC        MOV DWORD PTR SS:[EBP-4],EDX
00480191  8B55 F4        MOV EDX,DWORD PTR SS:[EBP-C]
00480194  03CF           ADD ECX,EDI
00480196  03F0           ADD ESI,EAX
00480198  4A             DEC EDX
00480199  8955 F4        MOV DWORD PTR SS:[EBP-C],EDX
0048019C ^75 D2          JNZ SHORT StarCraf.00480170
0048019E  8B4D FC        MOV ECX,DWORD PTR SS:[EBP-4]
004801A1  8B5D F8        MOV EBX,DWORD PTR SS:[EBP-8]
004801A4  8B45 F0        MOV EAX,DWORD PTR SS:[EBP-10]
004801A7  81E9 5C010000  SUB ECX,15C
004801AD  43             INC EBX
004801AE  48             DEC EAX
004801AF  894D FC        MOV DWORD PTR SS:[EBP-4],ECX
004801B2  895D F8        MOV DWORD PTR SS:[EBP-8],EBX
004801B5  8945 F0        MOV DWORD PTR SS:[EBP-10],EAX
004801B8 ^0F85 72FFFFFF  JNZ StarCraf.00480130
004801BE  8B45 EC        MOV EAX,DWORD PTR SS:[EBP-14]
004801C1  83C3 03        ADD EBX,3
004801C4  81C1 0C010000  ADD ECX,10C
004801CA  48             DEC EAX
004801CB  895D F8        MOV DWORD PTR SS:[EBP-8],EBX
004801CE  894D FC        MOV DWORD PTR SS:[EBP-4],ECX
004801D1  8945 EC        MOV DWORD PTR SS:[EBP-14],EAX
004801D4 ^0F85 46FFFFFF  JNZ StarCraf.00480120
004801DA  5F             POP EDI
004801DB  5E             POP ESI
004801DC  5B             POP EBX
004801DD  8BE5           MOV ESP,EBP
004801DF  5D             POP EBP
004801E0  C3             RETN
004801E1  CC             INT3
004801E2  CC             INT3
004801E3  C702 1F1F1F1F  MOV DWORD PTR DS:[EDX],1F1F1F1F
004801E9 ^EB A0          JMP SHORT StarCraf.0048018B
004801EB  CC             INT3
004801EC  CC             INT3
004801ED  CC             INT3
004801EE  CC             INT3
004801EF  CC             INT3
004801F0  55             PUSH EBP
```

```
Registers (FPU)
EAX 00000000
ECX 00001F00
EDX 059B0088
EBX 1F1F1F1F
ESP 0018FD98
EBP 0018FDB8
ESI 00001F00
EDI 00000000

EIP 00480189 StarCraf.00480189

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 0  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 7EFDD000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr 8510006B

EFL 00200206 (NO,NB,NE,A,NS,PE,GE,G)

ST0 empty -??? FFFF 000003E2 B8323780
ST1 empty -??? FFFF 00000000 0000000B
ST2 empty -??? FFFF 7C570646 F016C36C
ST3 empty 0.0
ST4 empty 48000.000000000000000
ST5 empty 624.00000000000000000
ST6 empty 480.00000000000000000
ST7 empty 0.0
               3 2 1 0      E S P U O
FST 0120  Cond 0 0 0 1  Err 0 0 1 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1
```

```
Address   Hex dump                 ASCII
0050C000  00 00 00 00 33 83 40 00  ....3â@.
0050C008  70 BD 4F 00 A0 BD 4F 00  p╜O.á╜O.
0050C010  C0 BD 4F 00 D0 BD 4F 00  └╜O.╨╜O.
0050C018  E0 BD 4F 00 00 BE 4F 00  α╜O..╛O.
0050C020  10 BE 4F 00 20 BE 4F 00  ►╛O. ╛O.
0050C028  30 BE 4F 00 50 BE 4F 00  0╛O.P╛O.
0050C030  60 BE 4F 00 80 BE 4F 00  `╛O.Ç╛O.
0050C038  90 BE 4F 00 A0 BE 4F 00  É╛O.á╛O.
0050C040  B0 BE 4F 00 C0 BE 4F 00  ░╛O.└╛O.
0050C048  D0 BE 4F 00 E0 BE 4F 00  ╨╛O.α╛O.
0050C050  F0 BE 4F 00 00 BF 4F 00  ≡╛O..┐O.
```

```
0018FD98  000001E0
0018FD9C  006CE640  St
0018FDA0  0000007F
0018FDA4  0000000E
0018FDA8  00000015
0018FDAC  00000004
0018FDB0  04B700A1
0018FDB4  059B0088
0018FDB8  0018FDC8
0018FDBC  004BD271  RE
0018FDC0  00000002
0018FDC4  00000000
```

Running

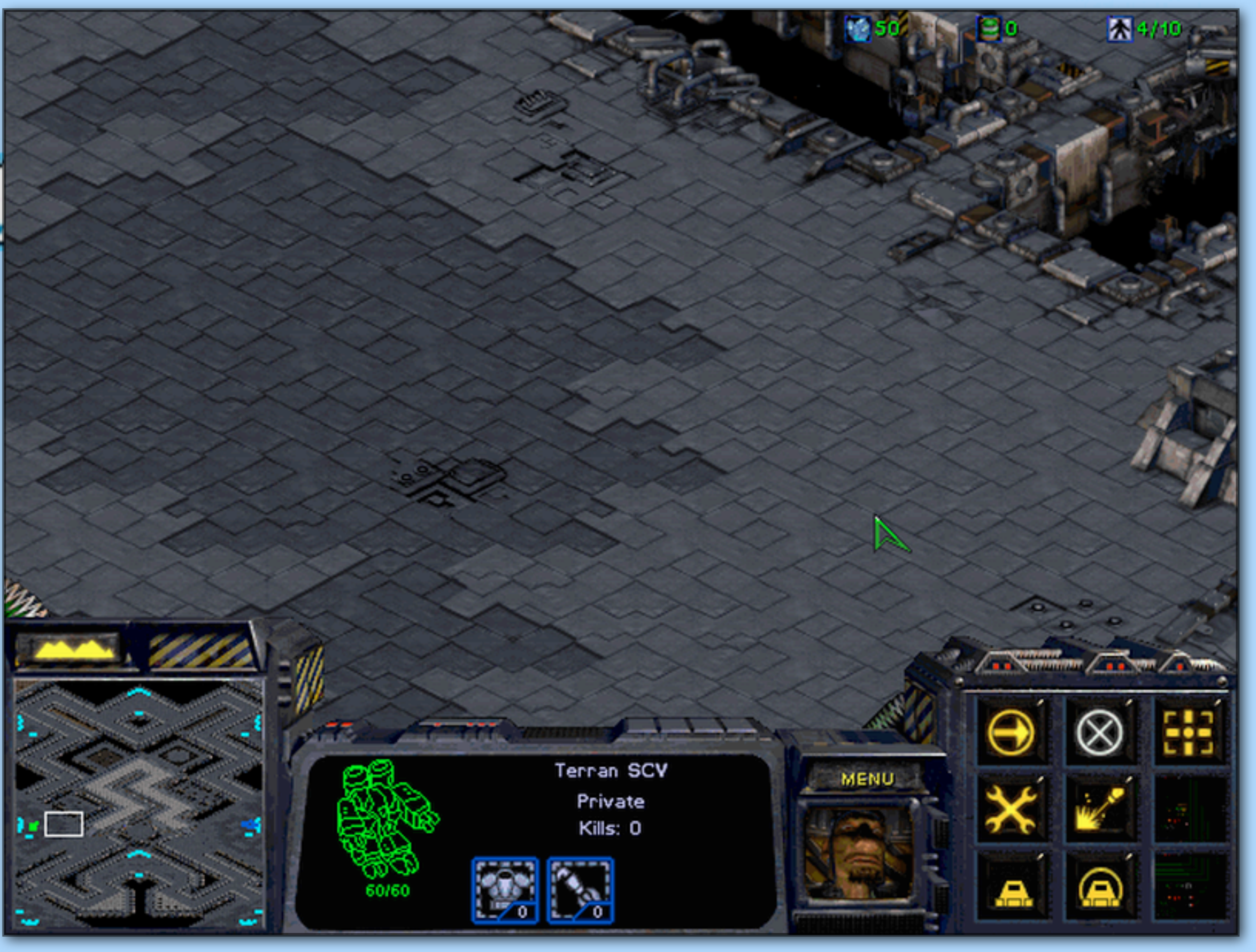
Making of a StarCraft map hack:

5. attach OllyDbg to the game, and put a breakpoint on the memory address

6. wait for the game to pause (map being redrawn)

7. modify the code to always set the “shown” value (jump to code cave if necessary)

GAME HACKING



Making of a StarCraft map hack:

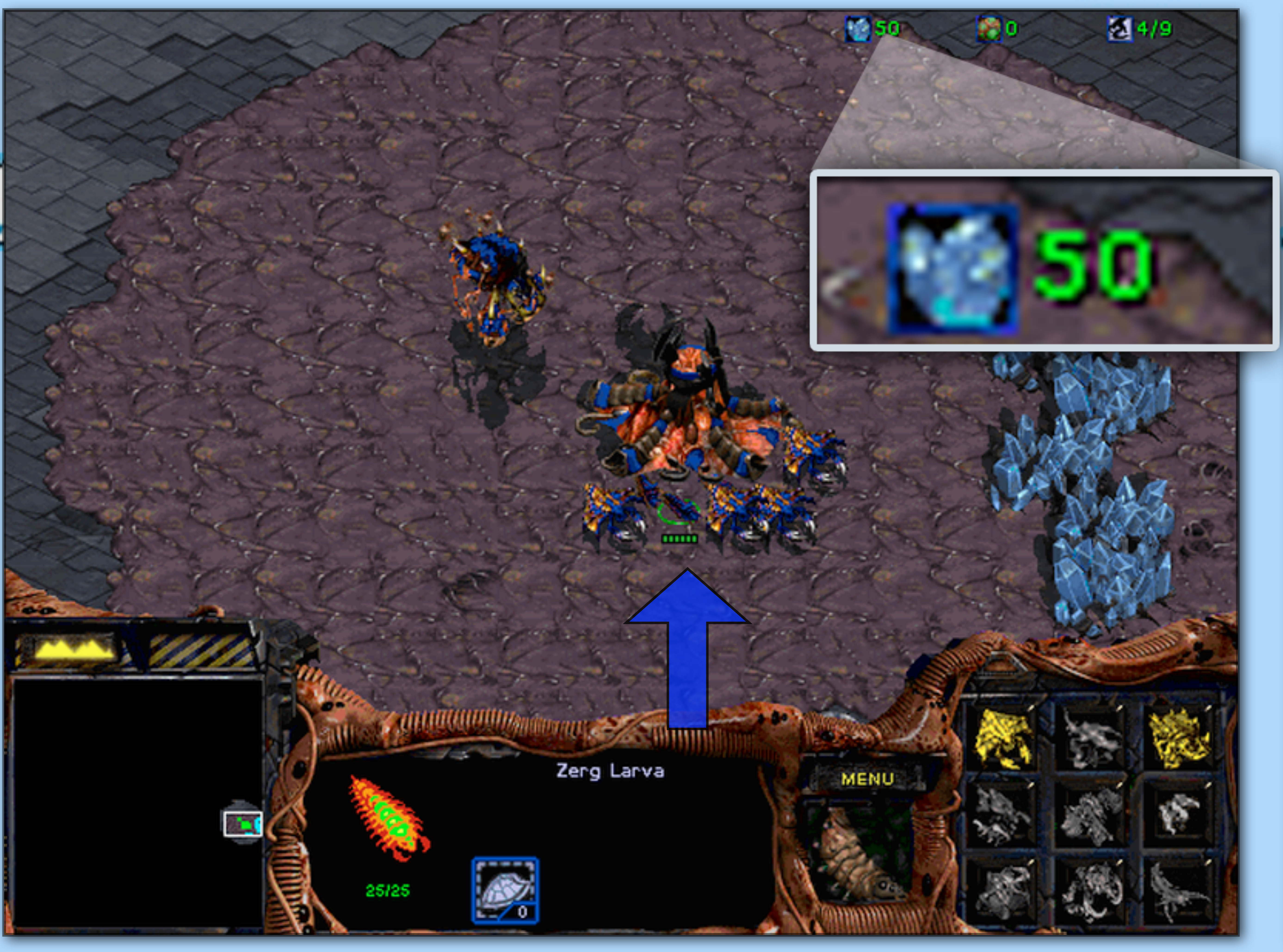
5. attach OllyDbg to the game, and put a breakpoint on the memory address

6. wait for the game to pause (map being redrawn)

7. modify the code to always set the "shown" value (jump to code cave if necessary)

Map hack!
(in multiplayer)

GAME HACKING

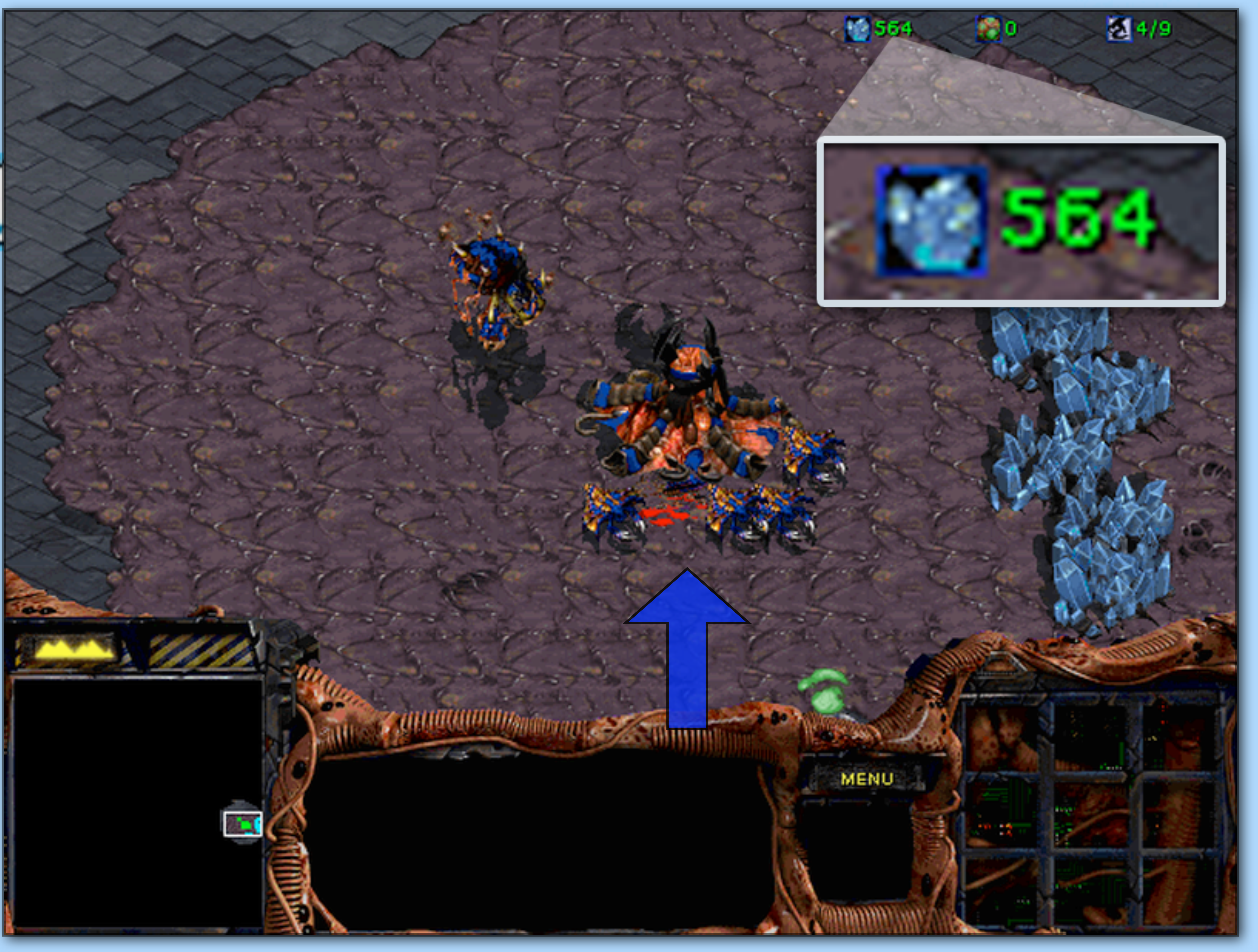


Unlike Diablo 1, StarCraft has "state" checking, so values couldn't just be modified...

... (flawed) game logic has to be exploited

> "The *Zerg Mineral Hack works by sending a command that tells a larva to morph into an invalid unit, which is worth 564 minerals. Then, the morphing auto-cancels (it's a feature of the hack, not the exploit) and the player receives 514 extra minerals.*" - Zynastor

GAME HACKING

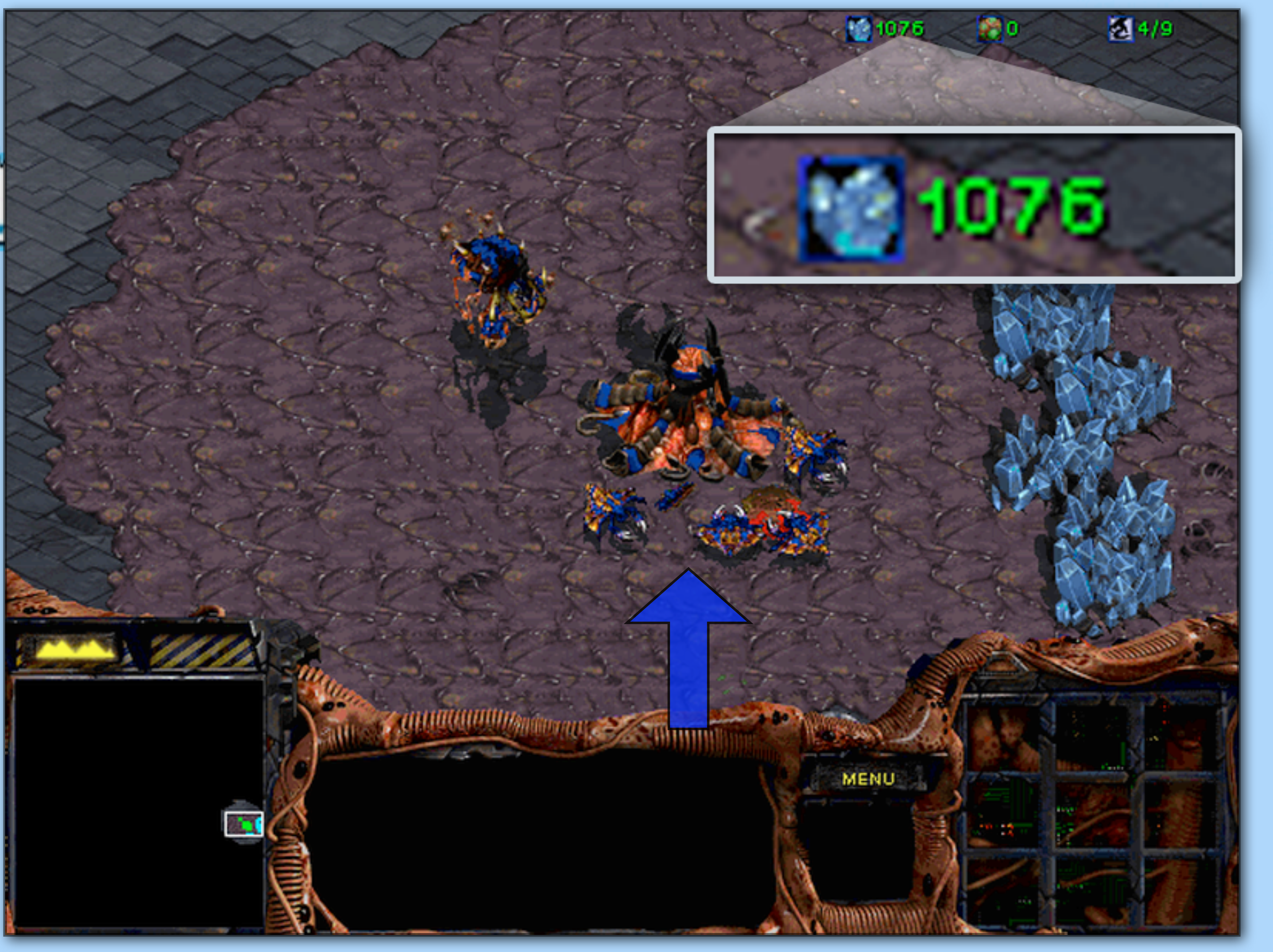


Unlike Diablo 1, StarCraft has "state" checking, so values couldn't just be modified...

... (flawed) game logic has to be exploited

"The *Zerg Mineral Hack works by sending a command that tells a larva to morph into an invalid unit, which is worth 564 minerals. Then, the morphing auto-cancels (it's a feature of the hack, not the exploit) and the player receives 514 extra minerals.*" - Zynastor

GAME HACKING

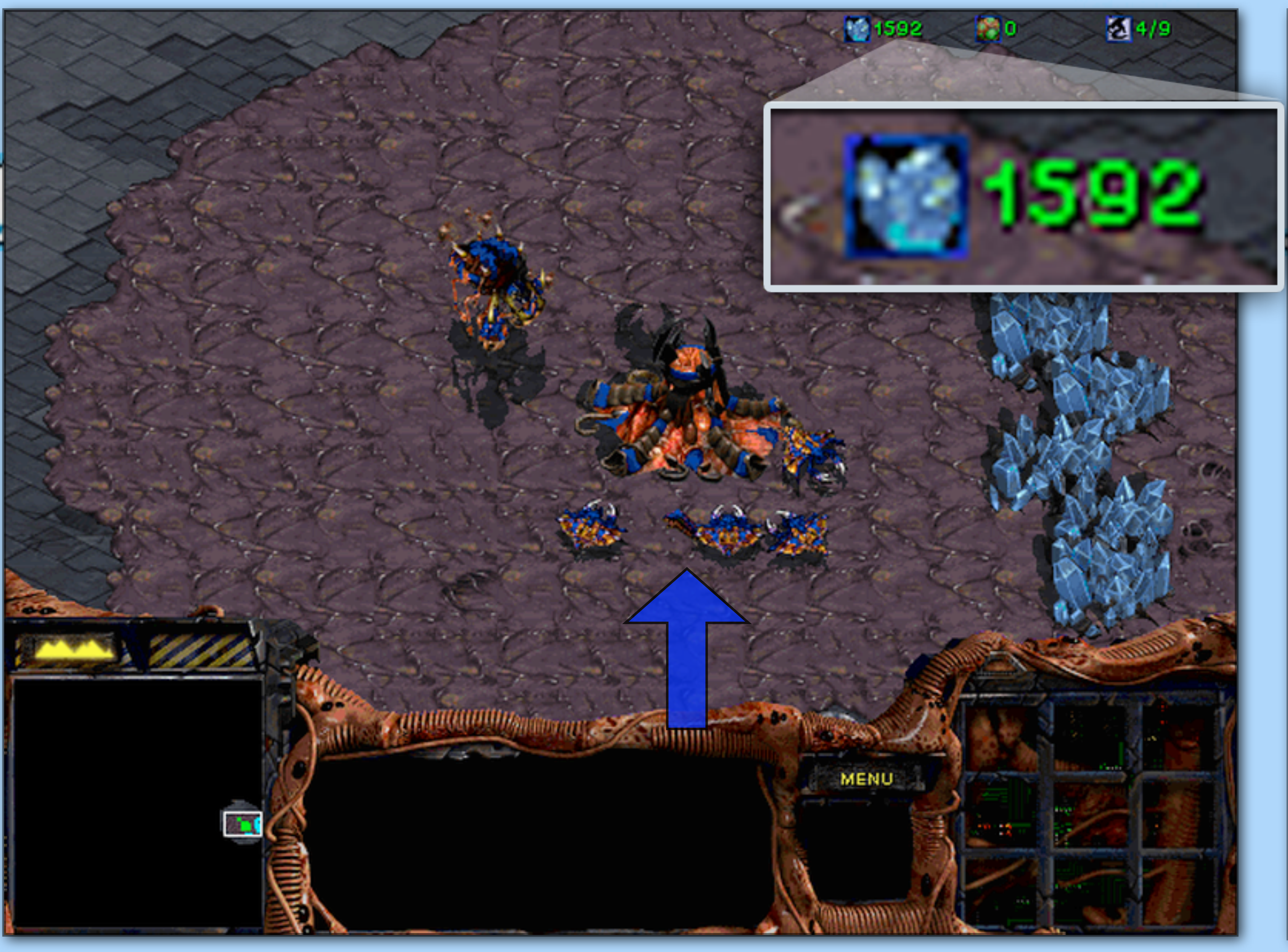


Unlike Diablo 1, StarCraft has "state" checking, so values couldn't just be modified...

... (flawed) game logic has to be exploited

"The *Zerg Mineral Hack works by sending a command that tells a larva to morph into an invalid unit, which is worth 564 minerals. Then, the morphing auto-cancels (it's a feature of the hack, not the exploit) and the player receives 514 extra minerals.*" - Zynastor

GAME HACKING



Unlike Diablo 1, StarCraft has "state" checking, so values couldn't just be modified...

... (flawed) game logic has to be exploited

"The Zerg Mineral Hack works by sending a command that tells a larva to morph into an invalid unit, which is worth 564 minerals. Then, the morphing auto-cancels (it's a feature of the hack, not the exploit) and the player receives 514 extra minerals." - Zynastor

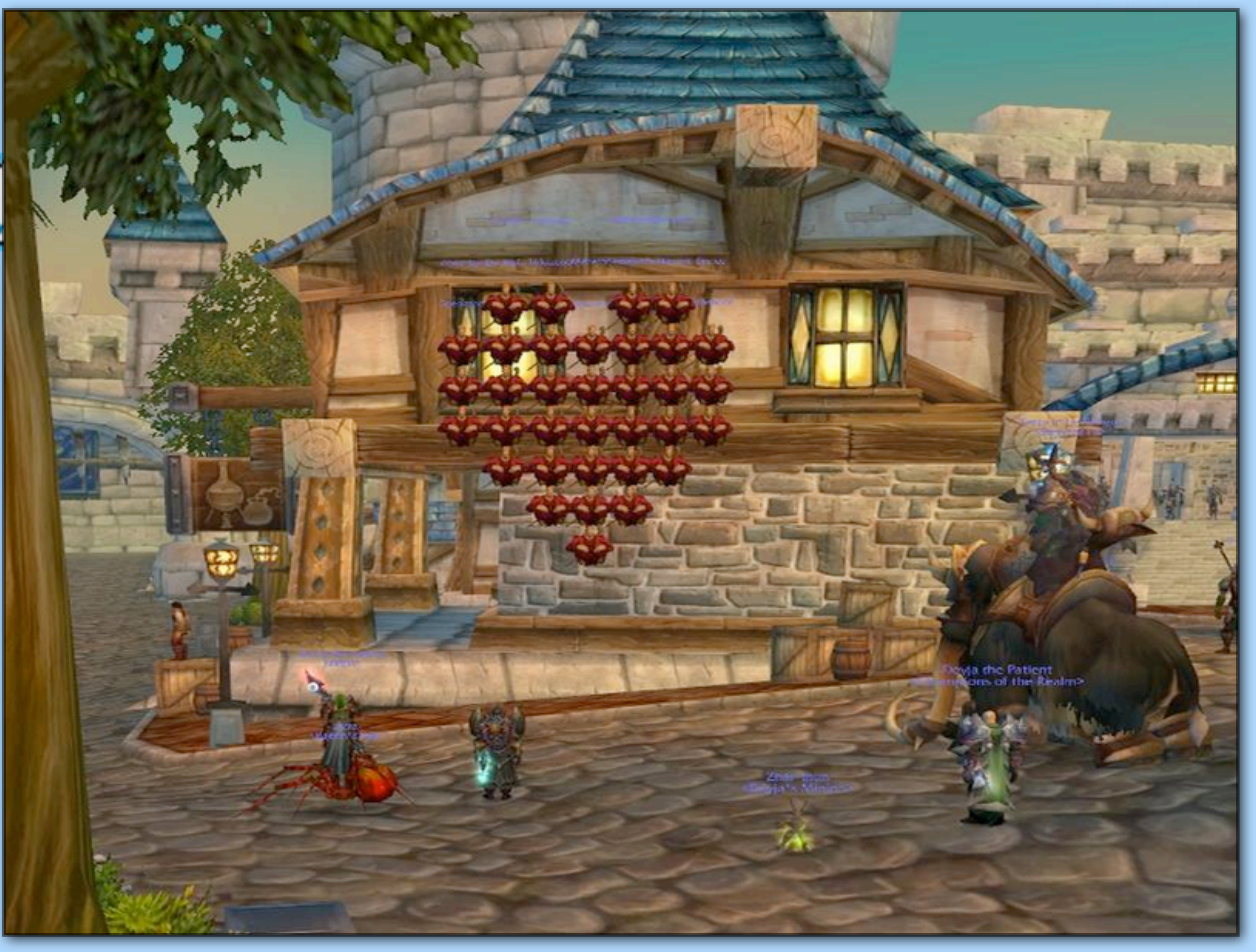
1600 minerals, seconds in to the game, and counting!

ZaCon 4 - Game Hacking

1. Console Games
2. DOS Games
3. Windows Games

    3.3. World of Warcraft & more memory hacks

GAME HACKING

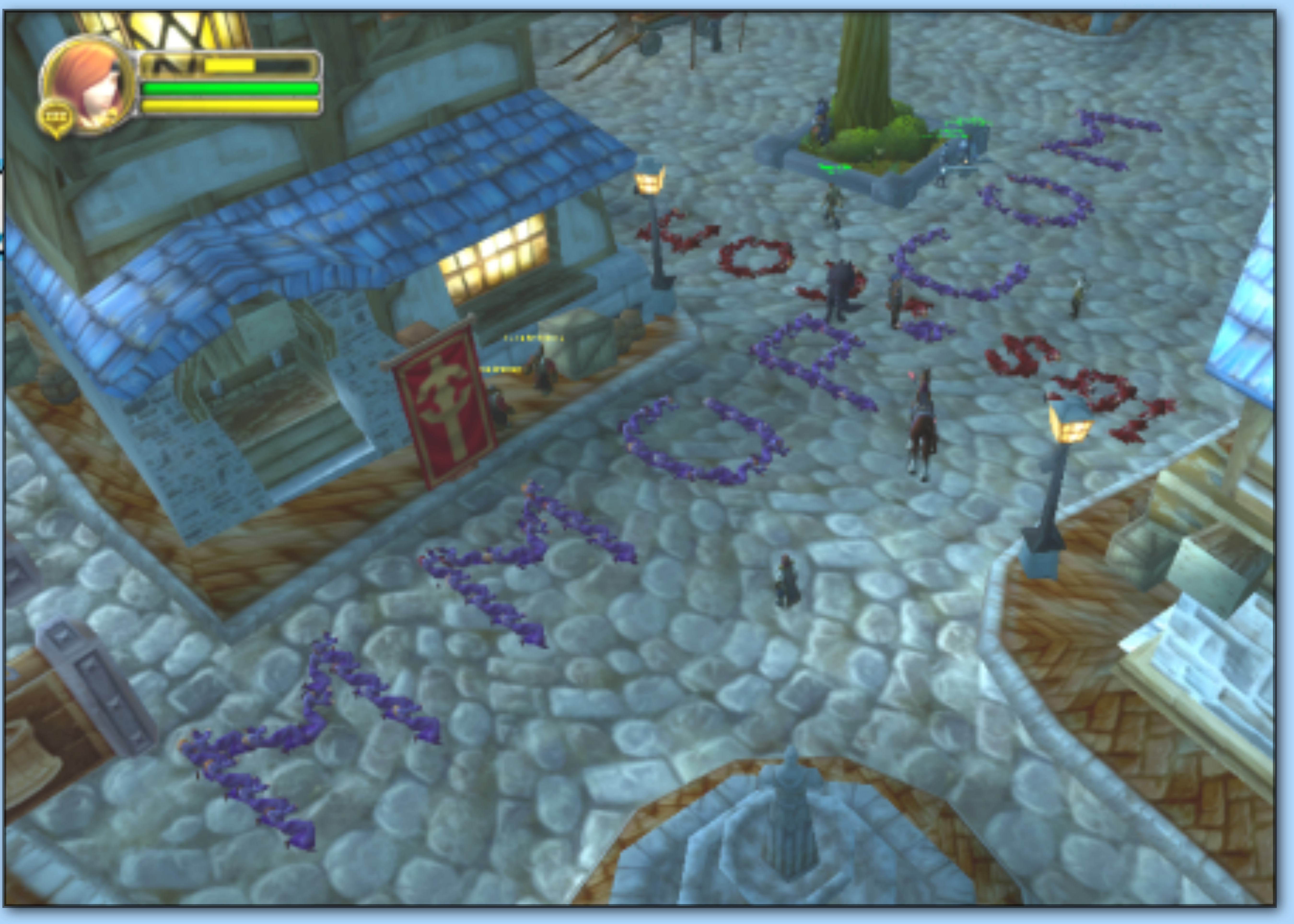


"Memory Hacking" is often thought to be simple, limiting, and "lame"

Many hacks can be achieved by changing, or freezing, memory values:

Teleporting, flying, no-clipping, speed hacks, etc

GAME HACKING



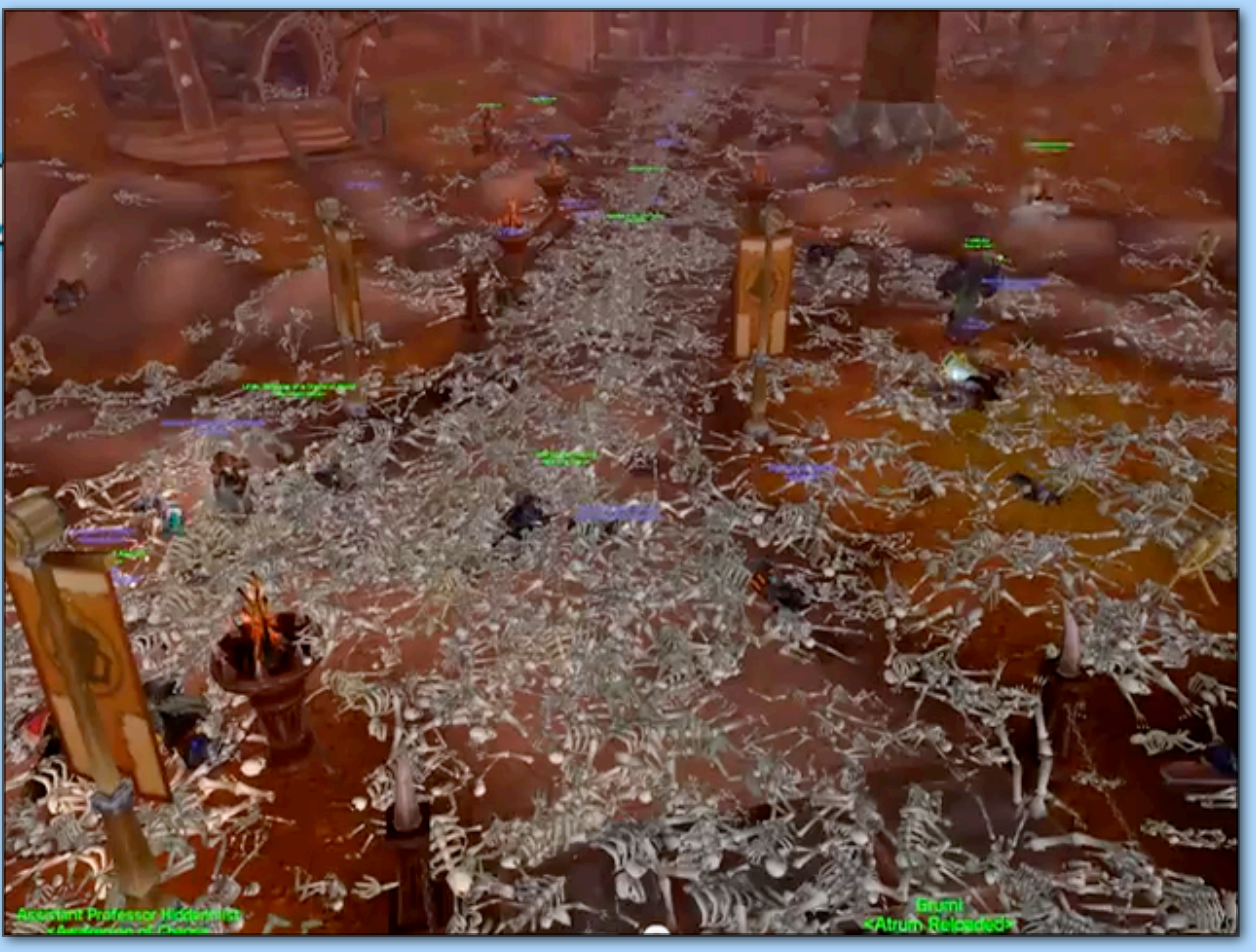
"Memory Hacking" is often thought to be simple, limiting, and "lame"

Many hacks can be achieved by changing, or freezing, memory values:

Teleporting, flying, no-clipping, speed hacks, etc

Spammers make use of them

GAME HACKING



“Memory Hacking” is often thought to be simple, limiting, and “lame”

Many hacks can be achieved by changing, or freezing, memory values:

Teleporting, flying, no-clipping, speed hacks, etc

Spammers make use of them

Sometimes “restricted” Spell IDs are found, and used, by non-GameMasters, resulting in mass (in-game) death

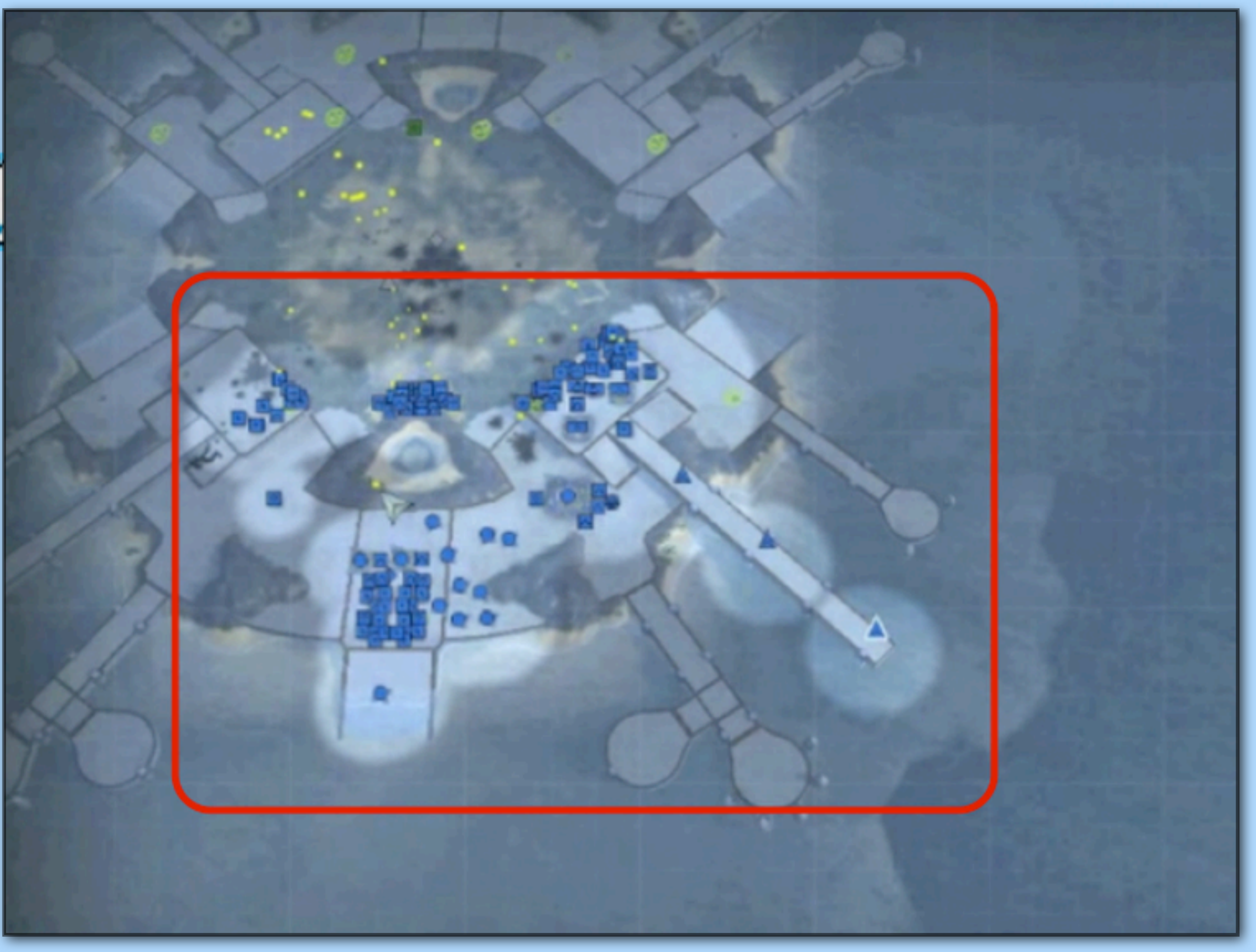
ZaCon 4 - Game Hacking

1. Console Games
2. DOS Games
3. Windows Games

   3.3. World of Warcraft & more memory hacks

   3.4. Kartograph

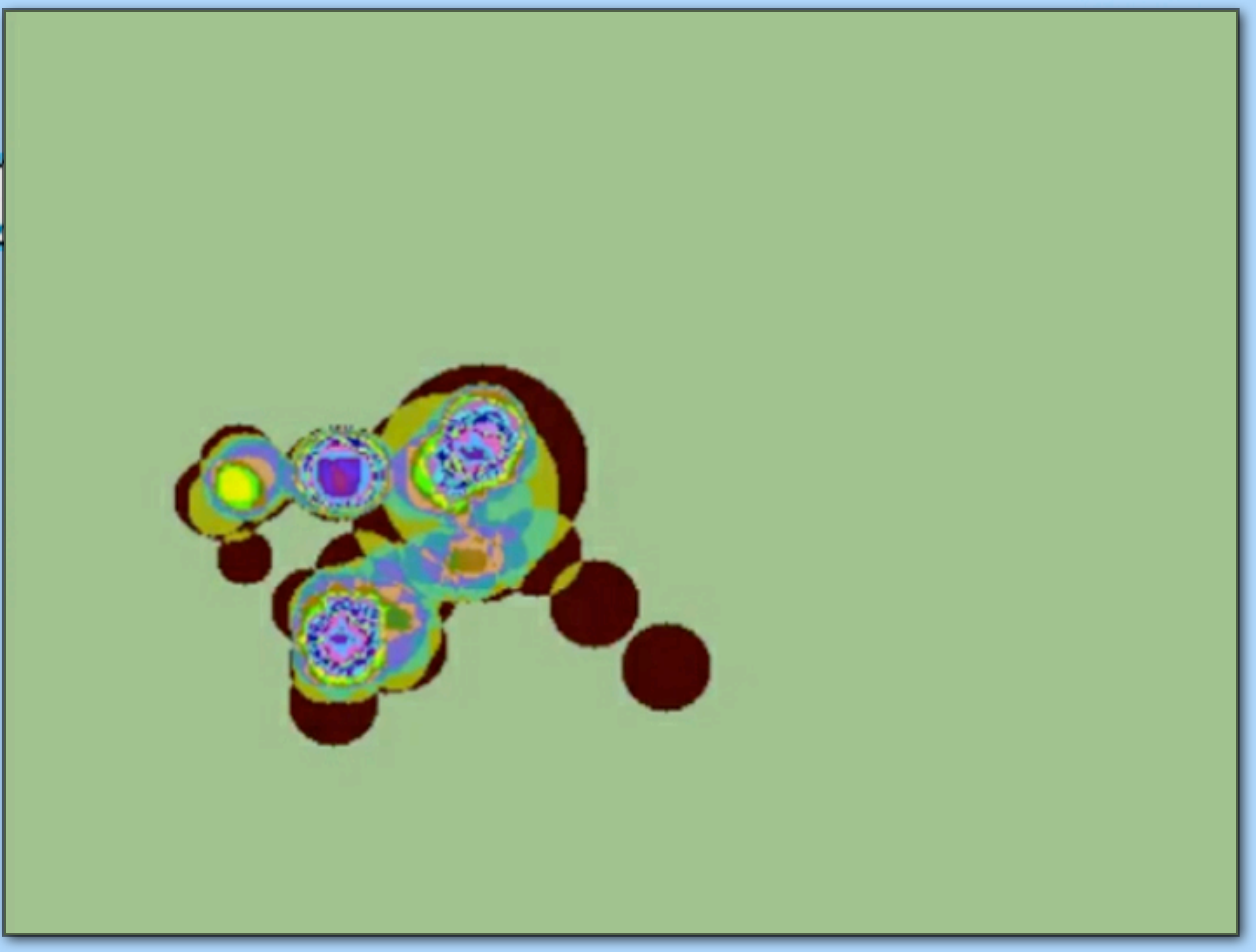
GAME HACKING



“Kartograph”, shown at Defcon 18, takes an interesting approach to game hacks:

Game memory is monitored

GAME HACKING



“Kartograph”, shown at Defcon 18, takes an interesting approach to game hacks:

Game memory is monitored, and shown as a “heat map”, making identifying data, and making (especially map) hacks, much quicker and easier

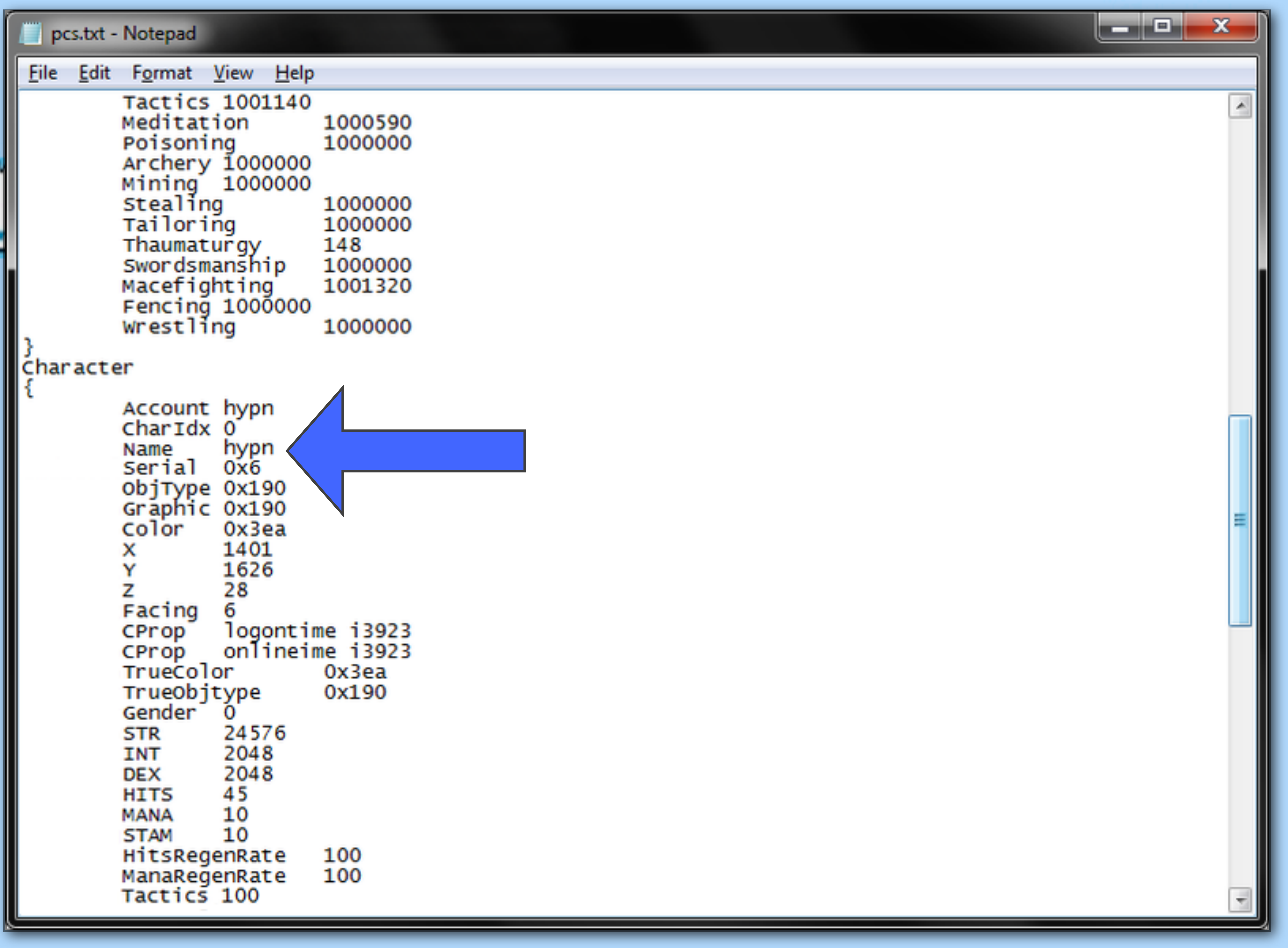
I can’t do them enough justice in these slides, visit http://elie.im/talks/kartograph to learn more about it!

ZaCon 4 - Game Hacking

1. Console Games
2. DOS Games
3. Windows Games

   3.5. Ultima Online "POL" server exploitation with W32Dasm

GAME HACKING



```
        Tactics 1001140
        Meditation      1000590
        Poisoning       1000000
        Archery 1000000
        Mining  1000000
        Stealing        1000000
        Tailoring       1000000
        Thaumaturgy     148
        Swordsmanship   1000000
        Macefighting    1001320
        Fencing 1000000
        Wrestling       1000000
}
Character
{
        Account hypn
        CharIdx 0
        Name    hypn
        Serial  0x6
        ObjType 0x190
        Graphic 0x190
        Color   0x3ea
        X       1401
        Y       1626
        Z       28
        Facing  6
        CProp   logontime i3923
        CProp   onlineime i3923
        TrueColor       0x3ea
        TrueObjtype     0x190
        Gender  0
        STR     24576
        INT     2048
        DEX     2048
        HITS    45
        MANA    10
        STAM    10
        HitsRegenRate   100
        ManaRegenRate   100
        Tactics 100
```

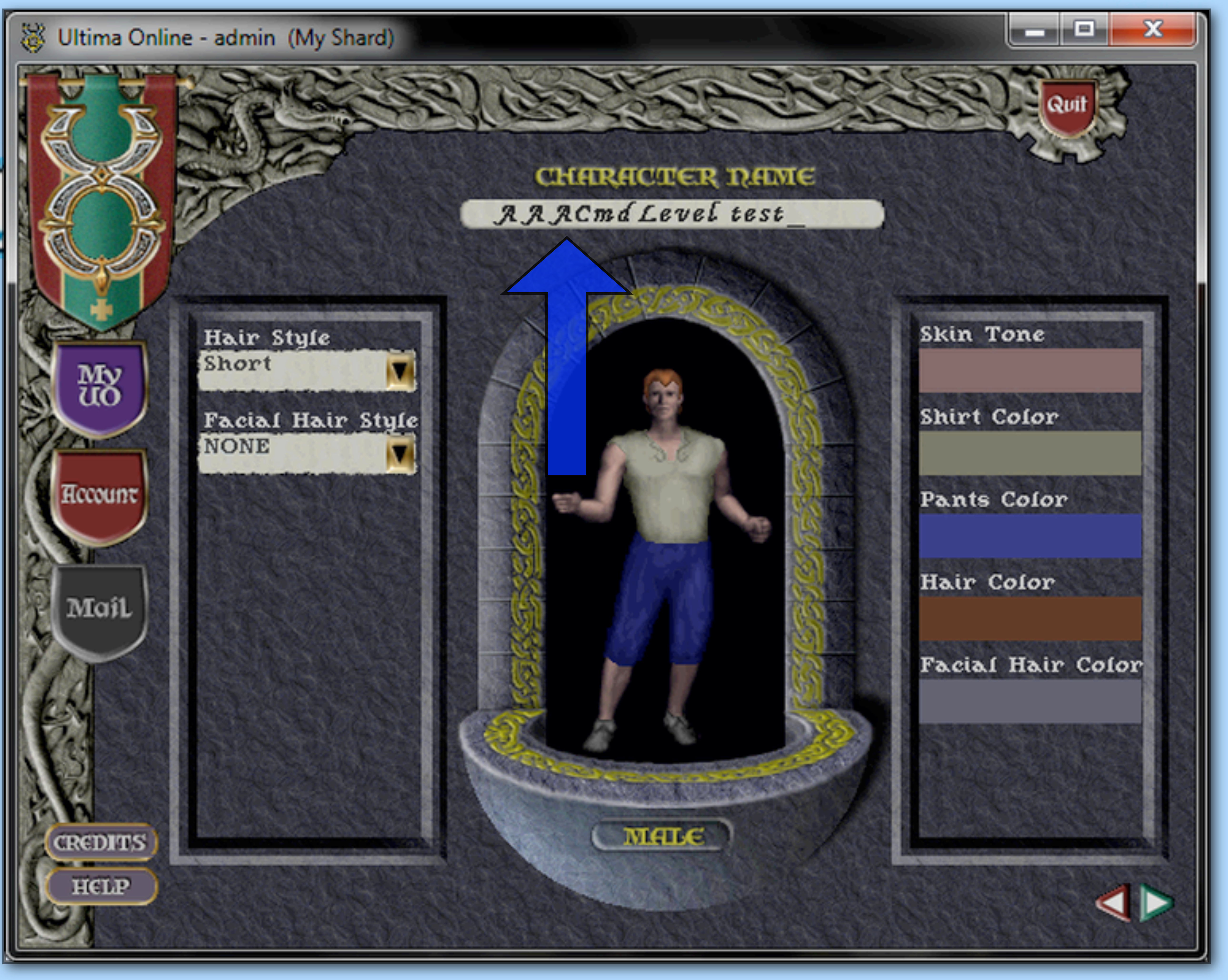
“POL”, an Ultima Online server emulator, stores it’s data in key-value based text files.

An advisory was mailed out, suggesting that if someone where to insert a “newline” character additional properties could be inserted.

Luckily this was deemed impossible ;)

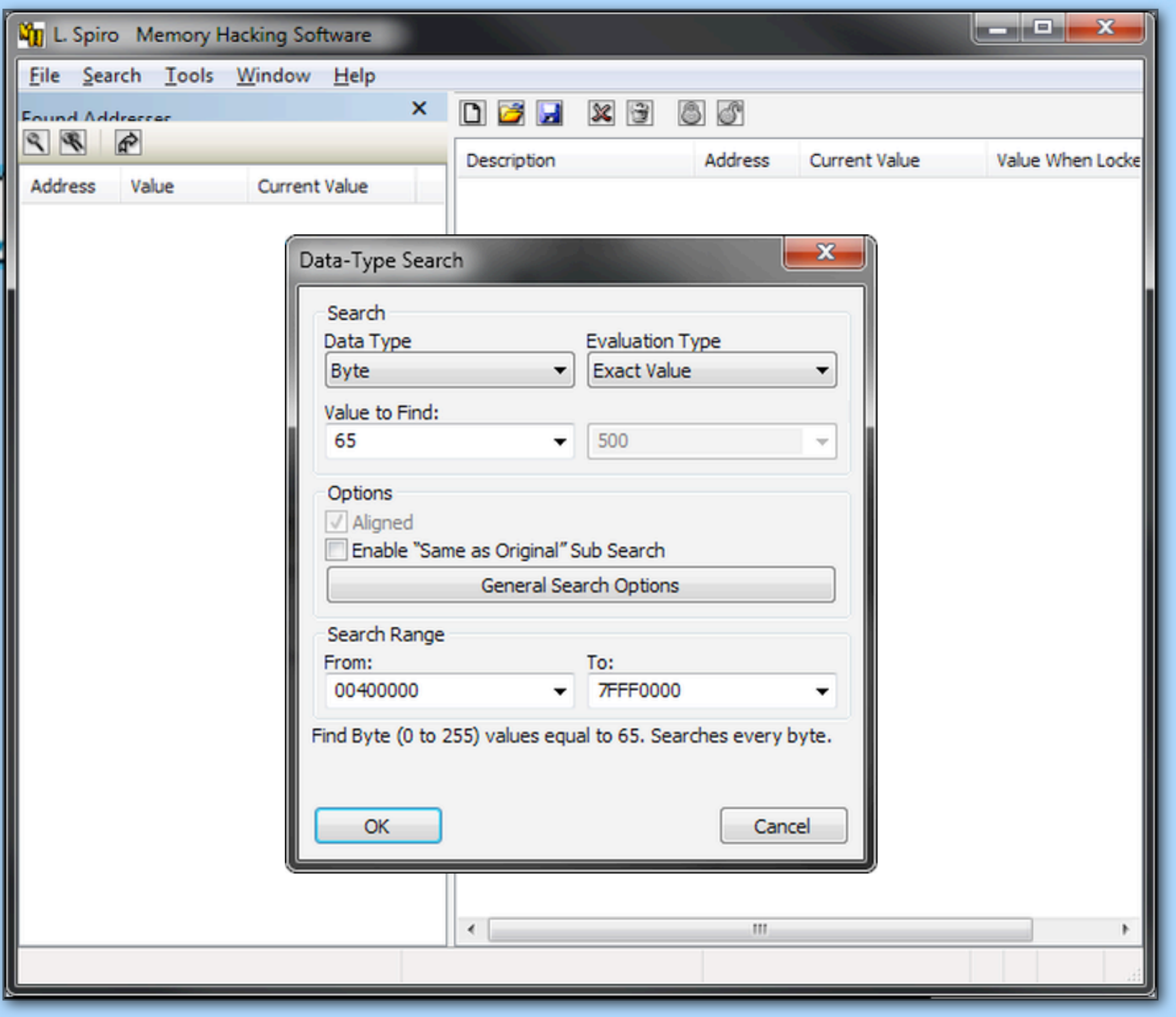
So I set out to do it…

GAME HACKING



Game clients often restrict input, but we can put in “markers” (the third “A” in this case)

GAME HACKING


L. Spiro Memory Hacking Software
File Search Tools Window Help
Found Addresses
Address Value Current Value
Description Address Current Value Value When Locke
Data-Type Search

Search

Data Type: Byte

Evaluation Type: Exact Value

Value to Find: 65

500

Options

☑ Aligned

□ Enable "Same as Original" Sub Search

Search Range

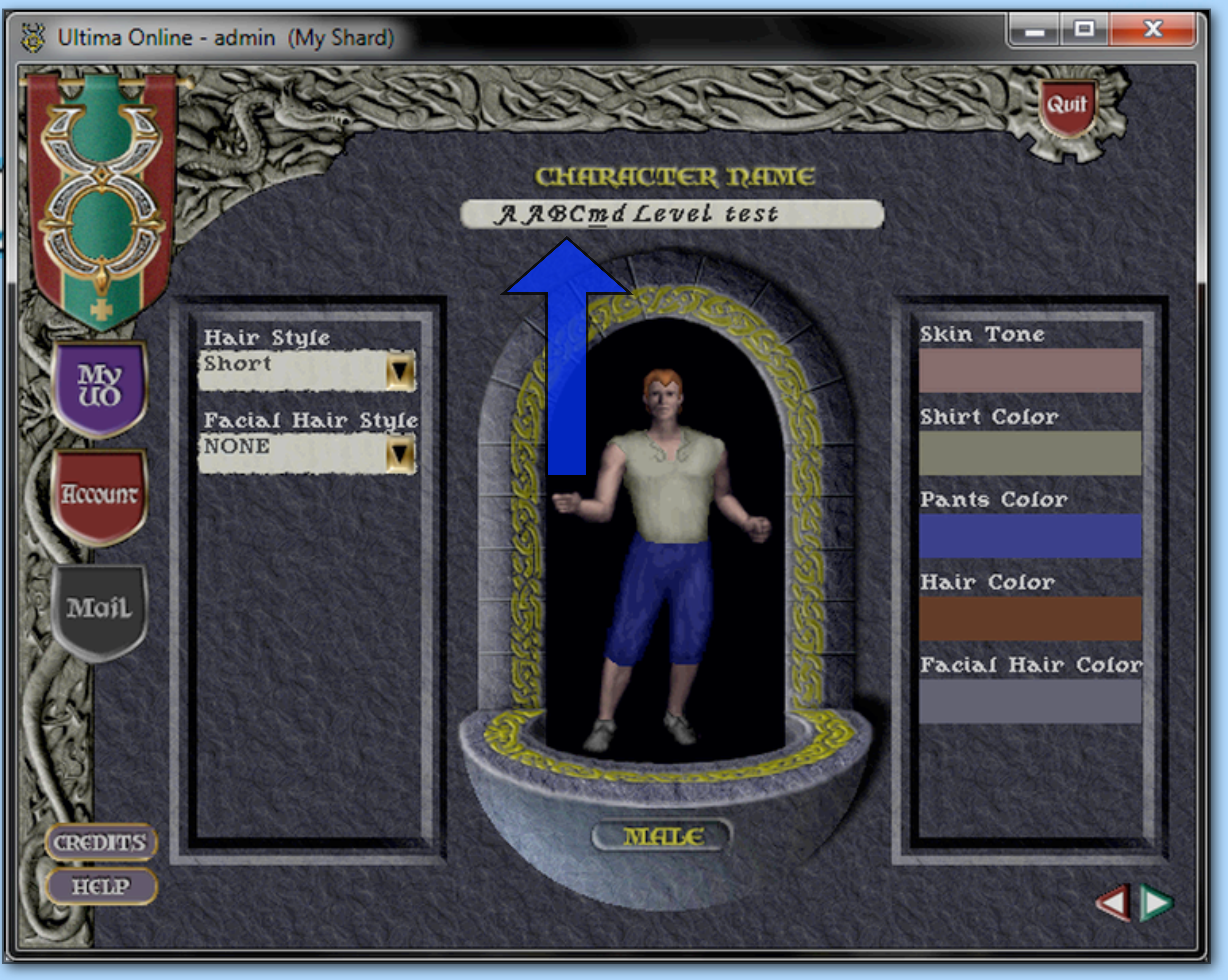
From: 00400000

To: 7FFF0000

Find Byte (0 to 255) values equal to 65. Searches every byte.

Game clients often restrict input, but we can put in “markers” (the third “A” in this case), and then search for it’s hex value in memory...

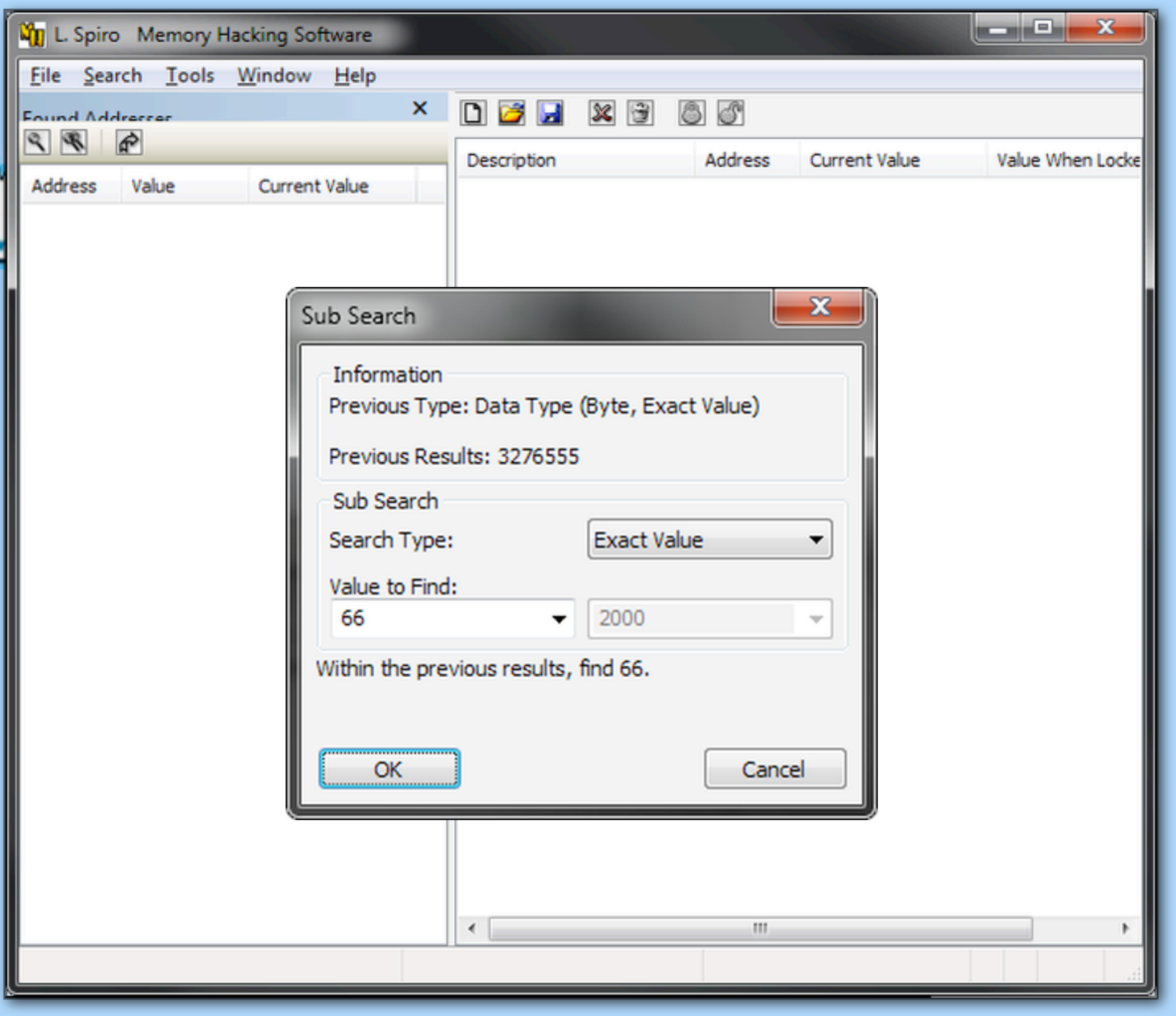
GAME HACKING



Game clients often restrict input, but we can put in “markers” (the third “A” in this case), and then search for it’s hex value in memory...

(changing it,

GAME HACKING



Information

Previous Type: Data Type (Byte, Exact Value)

Previous Results: 3276555

Sub Search

Search Type: Exact Value

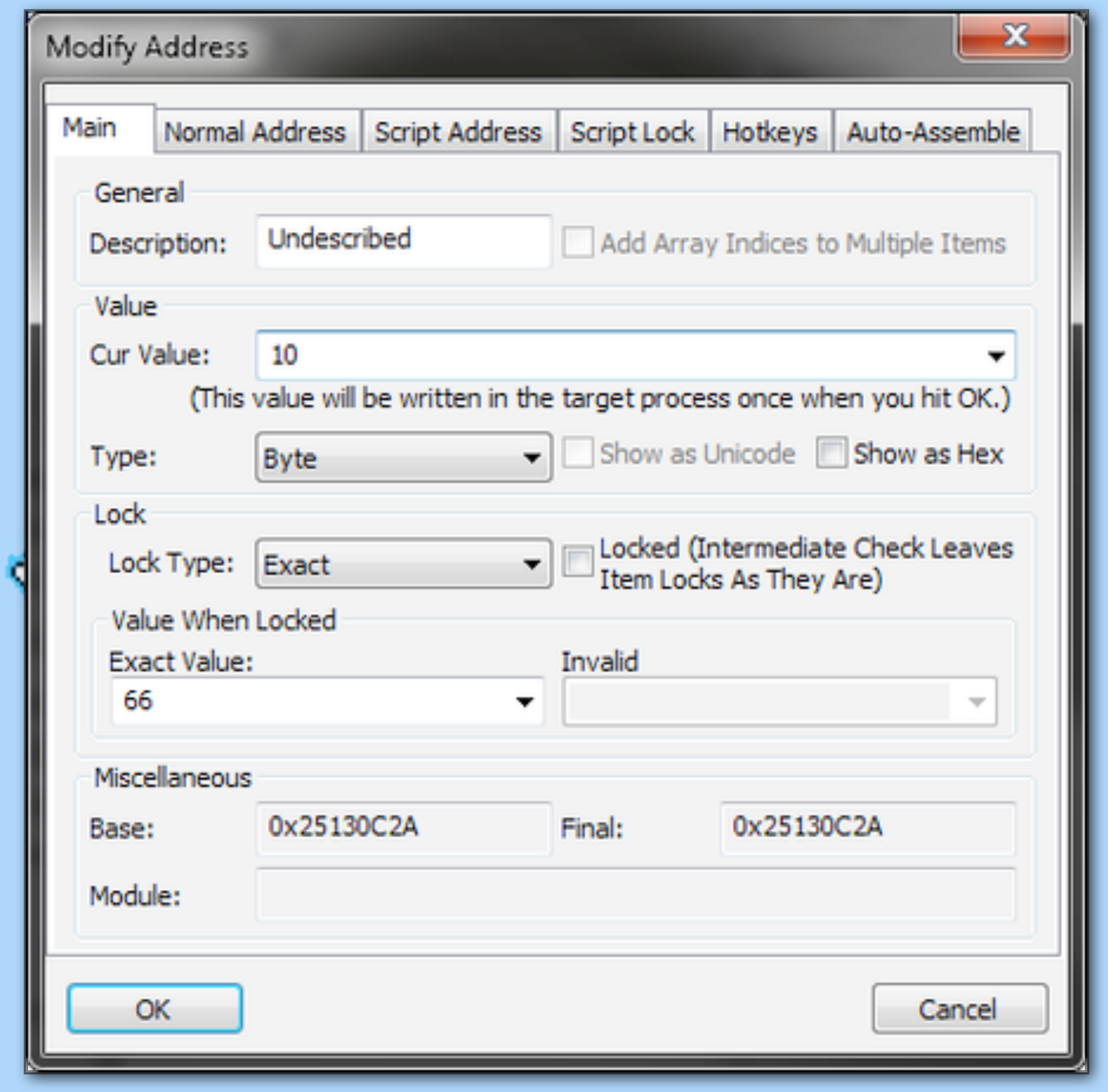
Value to Find: 66 2000

Within the previous results, find 66.

Game clients often restrict input, but we can put in “markers” (the third “A” in this case), and then search for it’s hex value in memory...

(changing it, and searching for it’s new value, until we find it)

GAME HACKING



Modify Address

General

Description: Undescribed

□ Add Array Indices to Multiple Items

Value

Cur Value: 10

(This value will be written in the target process once when you hit OK.)

Type: Byte □ Show as Unicode □ Show as Hex

Lock

Lock Type: Exact □ Locked (Intermediate Check Leaves Item Locks As They Are)

Value When Locked

Exact Value: 66

Invalid

Miscellaneous

Base: 0x25130C2A Final: 0x25130C2A

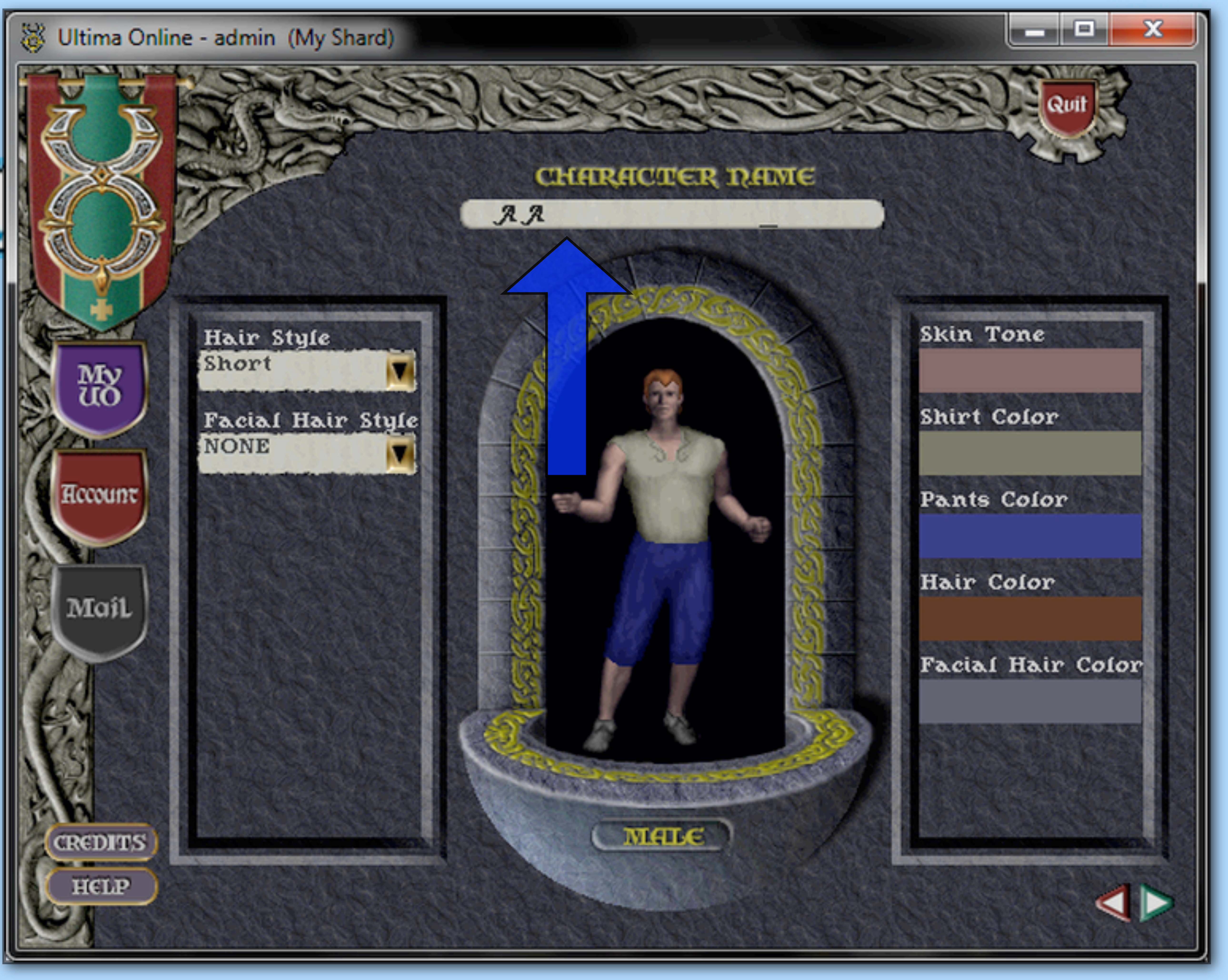
Module:

Game clients often restrict input, but we can put in "markers" (the third "A" in this case), and then search for it's hex value in memory...

(changing it, and searching for it's new value, until we find it)

... and then replacing it with something like, like a newline

GAME HACKING



Ultima Online - admin (My Shard)

Hair Style: Short

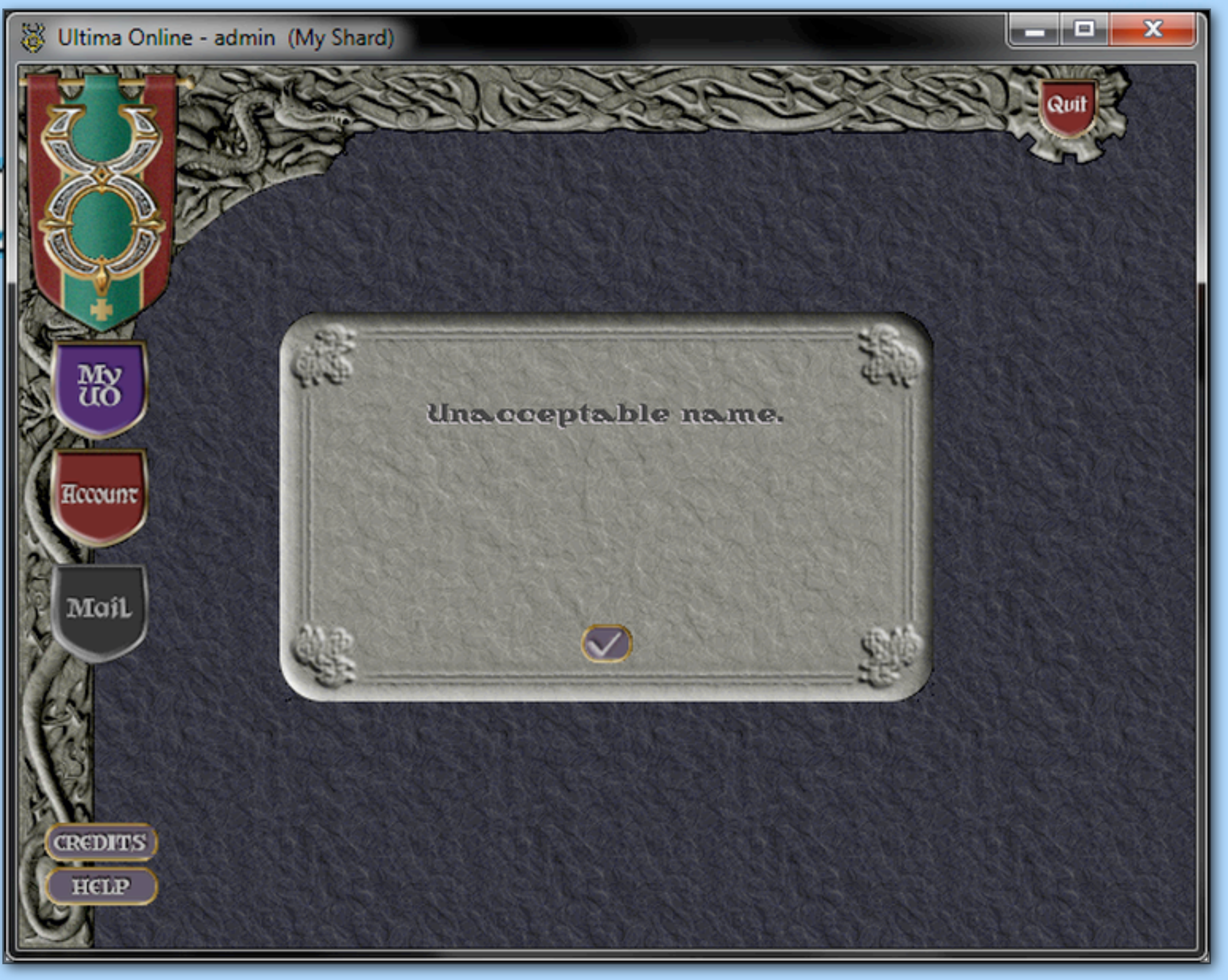
Facial Hair Style: NONE

Game clients often restrict input, but we can put in "markers" (the third "A" in this case), and then search for it's hex value in memory...

(changing it, and searching for it's new value, until we find it)

... and then replacing it with something like, like a newline

GAME HACKING



Ultima Online - admin (My Shard)

Unacceptable name.

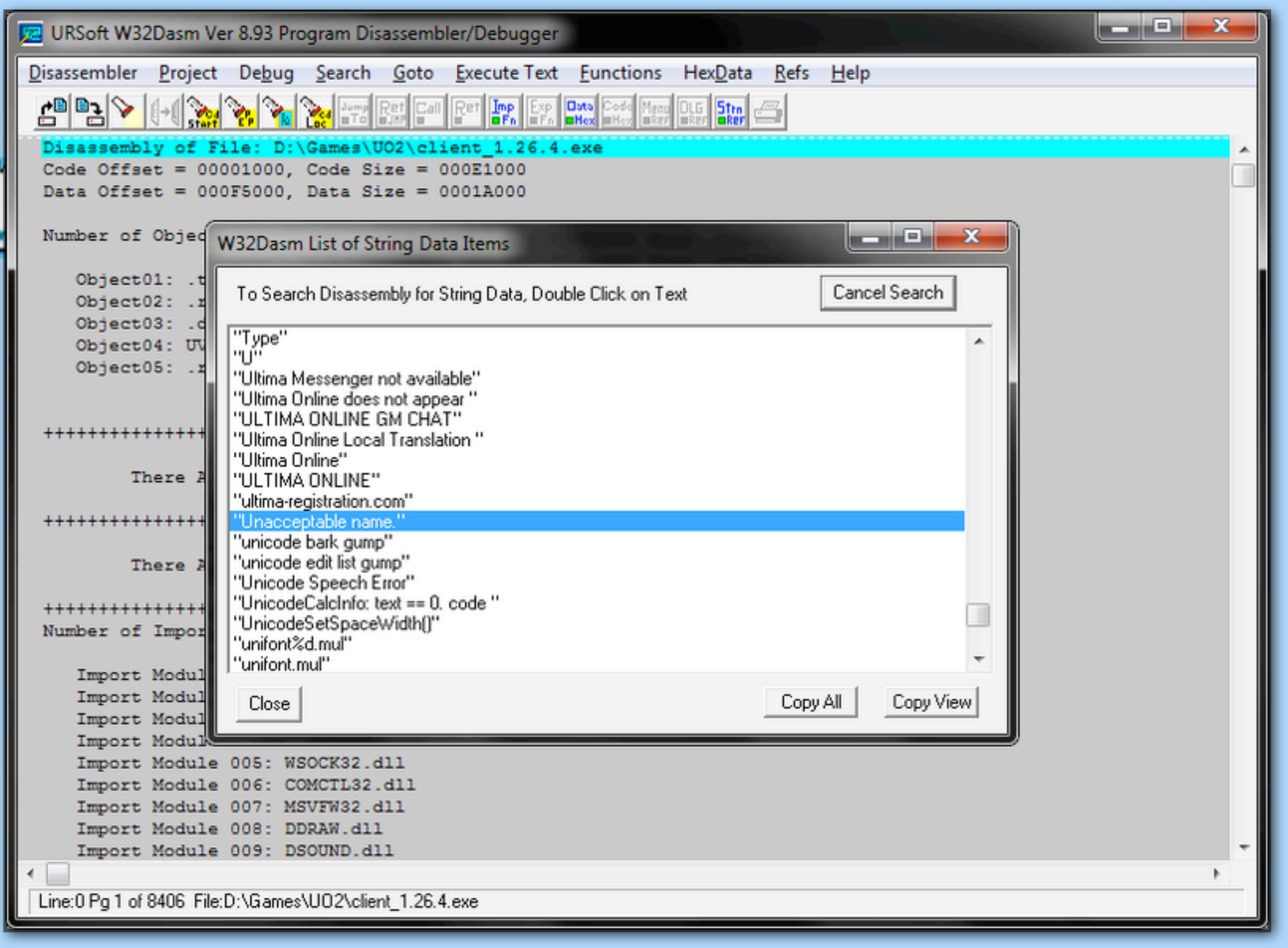
Game clients often restrict input, but we can put in "markers" (the third "A" in this case), and then search for it's hex value in memory...

(changing it, and searching for it's new value, until we find it)

... and then replacing it with something like, like a newline (or something else more malicious?)

Game clients don't always like us doing that... BUT...

GAME HACKING


URSoft W32Dasm Ver 8.93 Program Disassembler/Debugger
Disassembler Project Debug Search Goto Execute Text Functions HexData Refs Help
W32Dasm List of String Data Items
Cancel Search
Close
Copy All
Copy View

```
Disassembly of File: D:\Games\UO2\client_1.26.4.exe
Code Offset = 00001000, Code Size = 000E1000
Data Offset = 000F5000, Data Size = 0001A000

Number of Objec

   Object01: .t
   Object02: .r
   Object03: .d
   Object04: UV
   Object05: .r

+++++++++++++++

        There A

+++++++++++++++

        There A

+++++++++++++++
Number of Impor

   Import Modul
   Import Modul
   Import Modul
   Import Modul
   Import Module 005: WSOCK32.dll
   Import Module 006: COMCTL32.dll
   Import Module 007: MSVFW32.dll
   Import Module 008: DDRAW.dll
   Import Module 009: DSOUND.dll
```

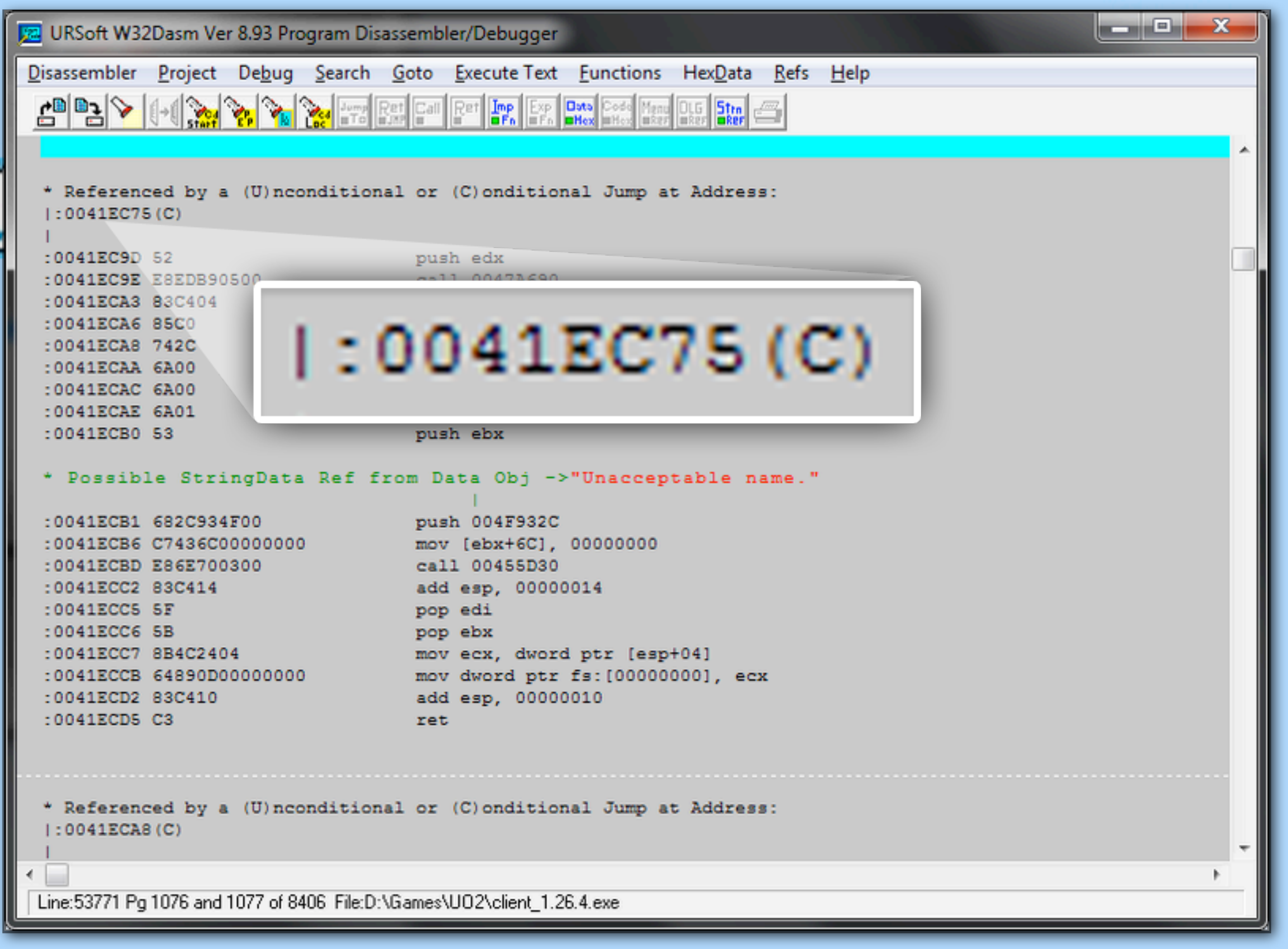
To Search Disassembly for String Data, Double Click on Text

```
"Type"
"U"
"Ultima Messenger not available"
"Ultima Online does not appear "
"ULTIMA ONLINE GM CHAT"
"Ultima Online Local Translation "
"Ultima Online"
"ULTIMA ONLINE"
"ultima-registration.com"
"Unacceptable name."
"unicode bark gump"
"unicode edit list gump"
"Unicode Speech Error"
"UnicodeCalcInfo: text == 0. code "
"UnicodeSetSpaceWidth()"
"unifont%d.mul"
"unifont.mul"
```

Line:0 Pg 1 of 8406 File:D:\Games\UO2\client_1.26.4.exe

W32Dasm (aka WinDasm) is a decompiler which can find text strings in an application

GAME HACKING

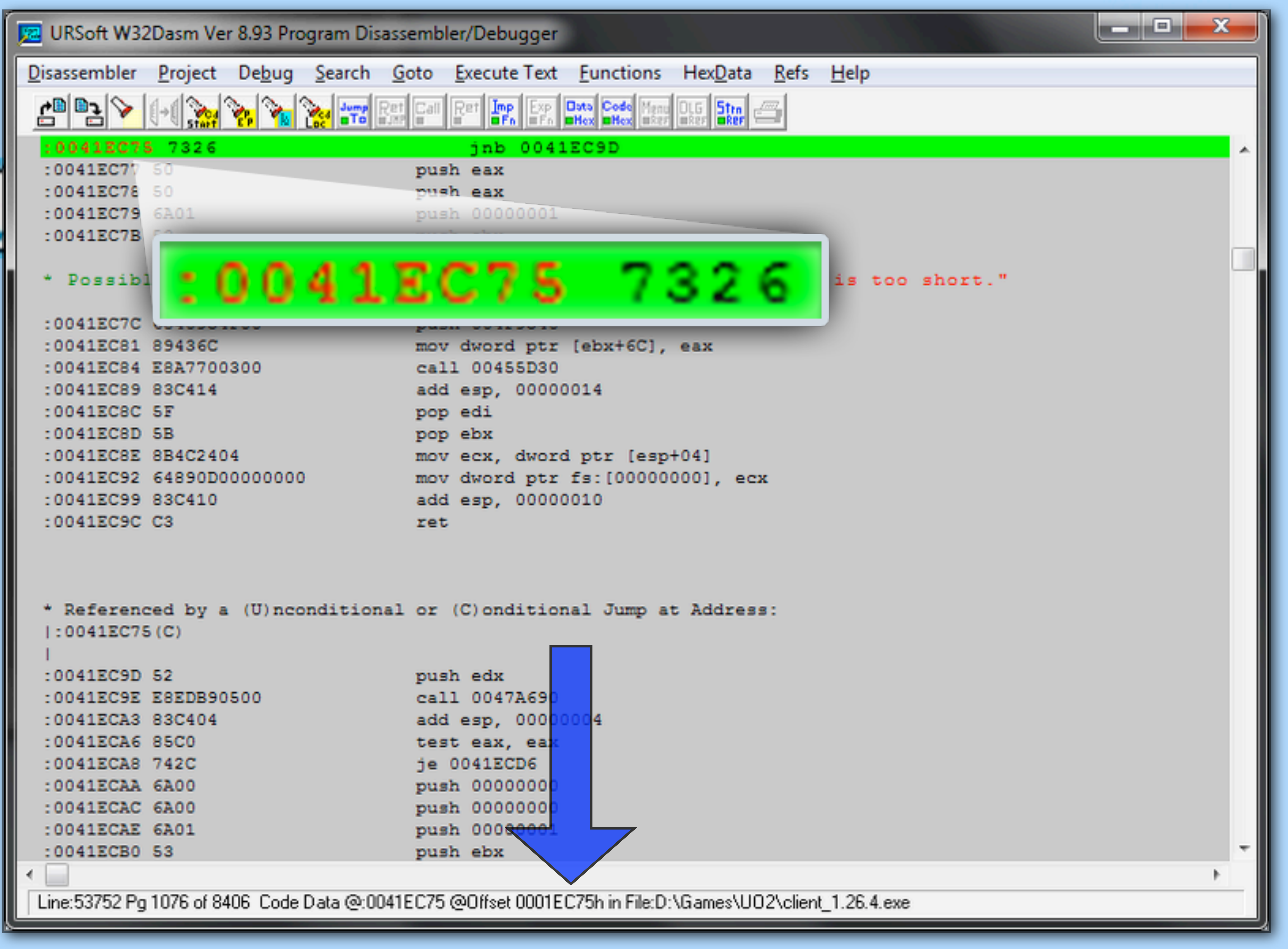

URSoft W32Dasm Ver 8.93 Program Disassembler/Debugger
Disassembler Project Debug Search Goto Execute Text Functions HexData Refs Help
|:0041EC75(C)
Line:53771 Pg 1076 and 1077 of 8406 File:D:\Games\UO2\client_1.26.4.exe

```
* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:0041EC75(C)
|
:0041EC9D 52                      push edx
:0041EC9E E8EDB90500              call 0047A690
:0041ECA3 83C404
:0041ECA6 85C0
:0041ECA8 742C
:0041ECAA 6A00
:0041ECAC 6A00
:0041ECAE 6A01
:0041ECB0 53                      push ebx

* Possible StringData Ref from Data Obj ->"Unacceptable name."
                                  |
:0041ECB1 682C934F00              push 004F932C
:0041ECB6 C7436C00000000          mov [ebx+6C], 00000000
:0041ECBD E86E700300              call 00455D30
:0041ECC2 83C414                  add esp, 00000014
:0041ECC5 5F                      pop edi
:0041ECC6 5B                      pop ebx
:0041ECC7 8B4C2404                mov ecx, dword ptr [esp+04]
:0041ECCB 64890D00000000          mov dword ptr fs:[00000000], ecx
:0041ECD2 83C410                  add esp, 00000010
:0041ECD5 C3                      ret

* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:0041ECA8(C)
|
```

W32Dasm (aka WinDasm) is a decompiler which can find text strings in an application, and show us the code around them

In this case there's a "Conditional" jump from 0041EC75

GAME HACKING


URSoft W32Dasm Ver 8.93 Program Disassembler/Debugger
Disassembler Project Debug Search Goto Execute Text Functions HexData Refs Help
:0041EC75 7326

```
:0041EC75 7326                    jnb 0041EC9D
:0041EC77 50                   push eax
:0041EC78 50                   push eax
:0041EC79 6A01                 push 00000001
:0041EC7B

* Possibl                                            is too short."

:0041EC7C
:0041EC81 89436C               mov dword ptr [ebx+6C], eax
:0041EC84 E8A7700300           call 00455D30
:0041EC89 83C414               add esp, 00000014
:0041EC8C 5F                   pop edi
:0041EC8D 5B                   pop ebx
:0041EC8E 8B4C2404             mov ecx, dword ptr [esp+04]
:0041EC92 64890D00000000       mov dword ptr fs:[00000000], ecx
:0041EC99 83C410               add esp, 00000010
:0041EC9C C3                   ret



* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:0041EC75(C)
|
:0041EC9D 52                   push edx
:0041EC9E E8EDB90500           call 0047A690
:0041ECA3 83C404               add esp, 00000004
:0041ECA6 85C0                 test eax, eax
:0041ECA8 742C                 je 0041ECD6
:0041ECAA 6A00                 push 00000000
:0041ECAC 6A00                 push 00000000
:0041ECAE 6A01                 push 00000001
:0041ECB0 53                   push ebx
```

Line:53752 Pg 1076 of 8406 Code Data @:0041EC75 @Offset 0001EC75h in File:D:\Games\UO2\client_1.26.4.exe

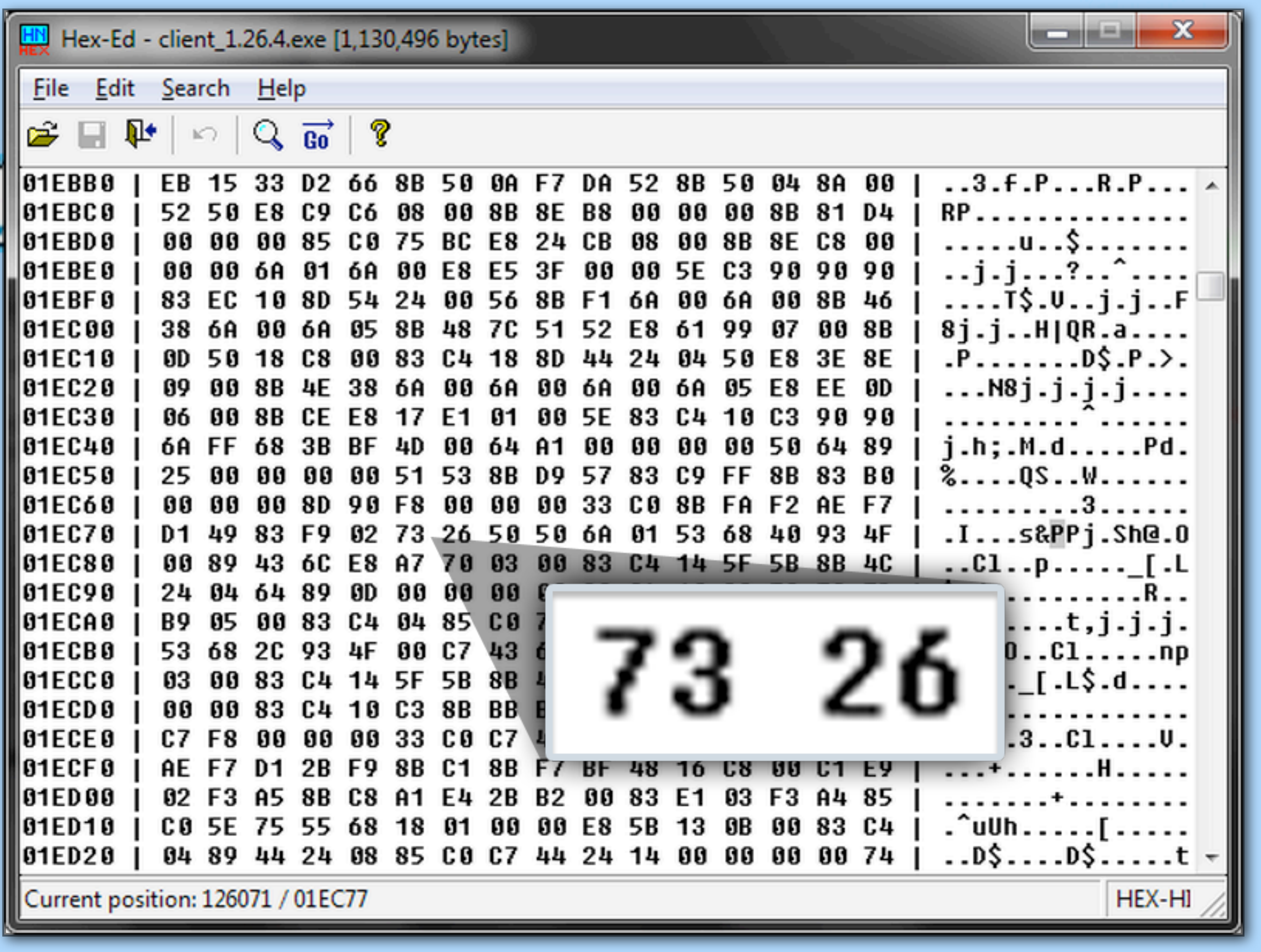
W32Dasm (aka WinDasm) is a decompiler which can find text strings in an application, and show us the code around them

In this case there's a "Conditional" jump from 0041EC75

Which performs some kind of checking, and then jumps to the code with the string in, if the condition is met.

We can make note of the offset (0001EC75)...

GAME HACKING



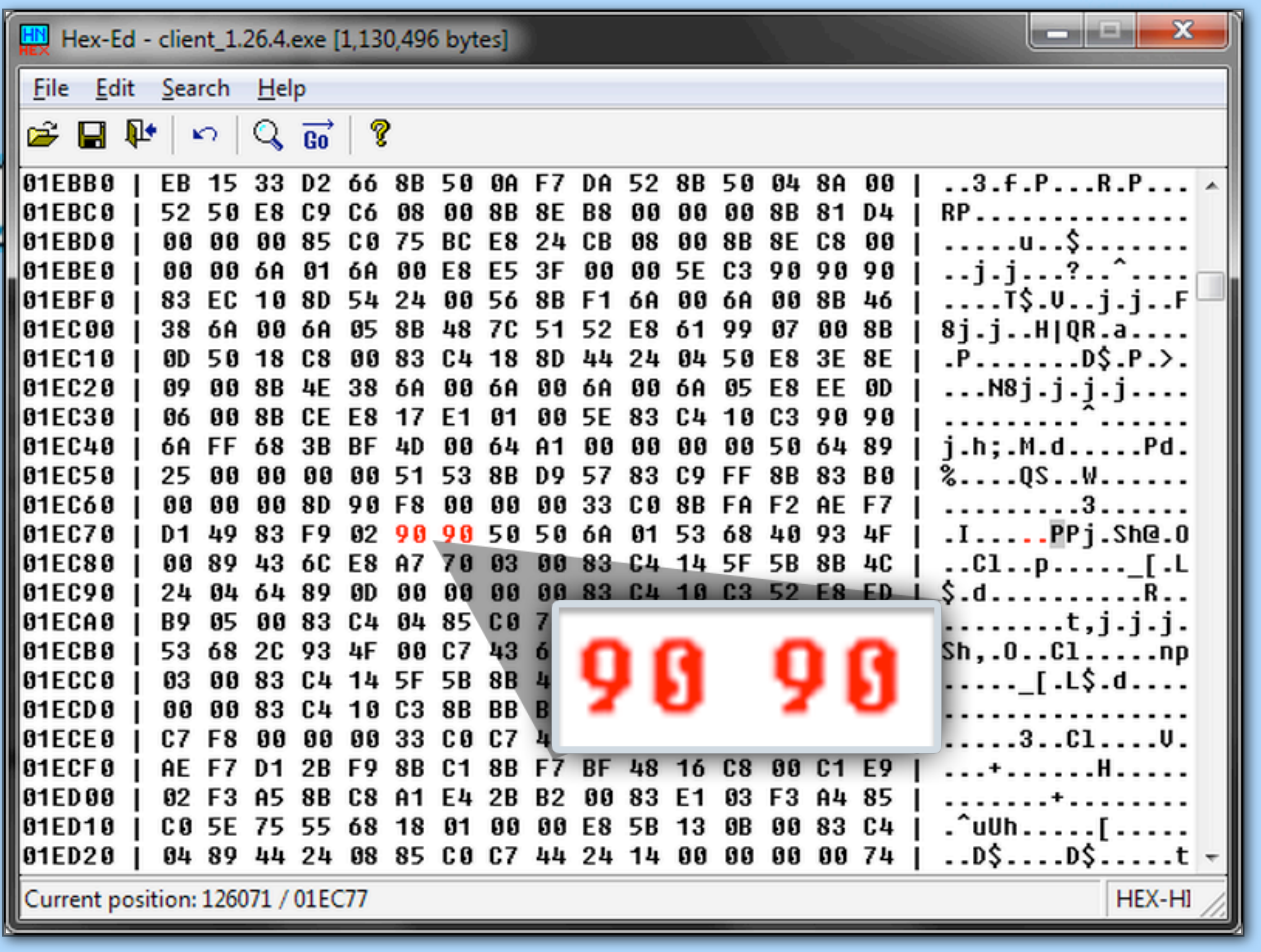
```
01EBB0 | EB 15 33 D2 66 8B 50 0A F7 DA 52 8B 50 04 8A 00 | ..3.f.P...R.P...
01EBC0 | 52 50 E8 C9 C6 08 00 8B 8E B8 00 00 00 8B 81 D4 | RP..............
01EBD0 | 00 00 00 85 C0 75 BC E8 24 CB 08 00 8B 8E C8 00 | .....u..$.......
01EBE0 | 00 00 6A 01 6A 00 E8 E5 3F 00 00 5E C3 90 90 90 | ..j.j...?..^....
01EBF0 | 83 EC 10 8D 54 24 00 56 8B F1 6A 00 6A 00 8B 46 | ....T$.V..j.j..F
01EC00 | 38 6A 00 6A 05 8B 48 7C 51 52 E8 61 99 07 00 8B | 8j.j..H|QR.a....
01EC10 | 0D 50 18 C8 00 83 C4 18 8D 44 24 04 50 E8 3E 8E | .P.......D$.P.>.
01EC20 | 09 00 8B 4E 38 6A 00 6A 00 6A 00 6A 05 E8 EE 0D | ...N8j.j.j.j....
01EC30 | 06 00 8B CE E8 17 E1 01 00 5E 83 C4 10 C3 90 90 | .........^......
01EC40 | 6A FF 68 3B BF 4D 00 64 A1 00 00 00 00 50 64 89 | j.h;.M.d.....Pd.
01EC50 | 25 00 00 00 00 51 53 8B D9 57 83 C9 FF 8B 83 B0 | %....QS..W......
01EC60 | 00 00 00 8D 90 F8 00 00 00 33 C0 8B FA F2 AE F7 | .........3......
01EC70 | D1 49 83 F9 02 73 26 50 50 6A 01 53 68 40 93 4F | .I...s&PPj.Sh@.O
01EC80 | 00 89 43 6C E8 A7 70 03 00 83 C4 14 5F 5B 8B 4C | ..Cl..p....._[.L
01EC90 | 24 04 64 89 0D 00 00 00                              .........R..
01ECA0 | B9 05 00 83 C4 04 85 C0                              ....t,j.j.j.
01ECB0 | 53 68 2C 93 4F 00 C7 43                              O..Cl.....np
01ECC0 | 03 00 83 C4 14 5F 5B 8B                              ._[.L$.d....
01ECD0 | 00 00 83 C4 10 C3 8B BB                              ............
01ECE0 | C7 F8 00 00 00 33 C0 C7                              .3..Cl....V.
01ECF0 | AE F7 D1 2B F9 8B C1 8B F7 BF 48 16 C8 00 C1 E9 | ...+......H.....
01ED00 | 02 F3 A5 8B C8 A1 E4 2B B2 00 83 E1 03 F3 A4 85 | .......+........
01ED10 | C0 5E 75 55 68 18 01 00 00 E8 5B 13 0B 00 83 C4 | .^uUh....[......
01ED20 | 04 89 44 24 08 85 C0 C7 44 24 14 00 00 00 00 74 | ..D$....D$.....t
```

Current position: 126071 / 01EC77

... and open the file, going to that location, in a hexeditor

Where we see the same hex codes

GAME HACKING



```
01EBB0 | EB 15 33 D2 66 8B 50 0A F7 DA 52 8B 50 04 8A 00 | ..3.f.P...R.P...
01EBC0 | 52 50 E8 C9 C6 08 00 8B 8E B8 00 00 00 8B 81 D4 | RP..............
01EBD0 | 00 00 00 85 C0 75 BC E8 24 CB 08 00 8B 8E C8 00 | .....u..$.......
01EBE0 | 00 00 6A 01 6A 00 E8 E5 3F 00 00 5E C3 90 90 90 | ..j.j...?..^....
01EBF0 | 83 EC 10 8D 54 24 00 56 8B F1 6A 00 6A 00 8B 46 | ....T$.V..j.j..F
01EC00 | 38 6A 00 6A 05 8B 48 7C 51 52 E8 61 99 07 00 8B | 8j.j..H|QR.a....
01EC10 | 0D 50 18 C8 00 83 C4 18 8D 44 24 04 50 E8 3E 8E | .P.......D$.P.>.
01EC20 | 09 00 8B 4E 38 6A 00 6A 00 6A 00 6A 05 E8 EE 0D | ...N8j.j.j.j....
01EC30 | 06 00 8B CE E8 17 E1 01 00 5E 83 C4 10 C3 90 90 | .........^......
01EC40 | 6A FF 68 3B BF 4D 00 64 A1 00 00 00 00 50 64 89 | j.h;.M.d.....Pd.
01EC50 | 25 00 00 00 00 51 53 8B D9 57 83 C9 FF 8B 83 B0 | %....QS..W......
01EC60 | 00 00 00 8D 90 F8 00 00 00 33 C0 8B FA F2 AE F7 | .........3......
01EC70 | D1 49 83 F9 02 90 90 50 50 6A 01 53 68 40 93 4F | .I.....PPj.Sh@.O
01EC80 | 00 89 43 6C E8 A7 70 03 00 83 C4 14 5F 5B 8B 4C | ..Cl..p....._[.L
01EC90 | 24 04 64 89 0D 00 00 00 00 83 C4 10 C3 52 E8 ED | $.d..........R..
01ECA0 | B9 05 00 83 C4 04 85 C0 7                         .........t,j.j.j.
01ECB0 | 53 68 2C 93 4F 00 C7 43 6                         Sh,.O..Cl.....np
01ECC0 | 03 00 83 C4 14 5F 5B 8B 4                         ....._[.L$.d....
01ECD0 | 00 00 83 C4 10 C3 8B BB B                         ................
01ECE0 | C7 F8 00 00 00 33 C0 C7 4                         .....3..Cl....V.
01ECF0 | AE F7 D1 2B F9 8B C1 8B F7 BF 48 16 C8 00 C1 E9 | ...+.......H.....
01ED00 | 02 F3 A5 8B C8 A1 E4 2B B2 00 83 E1 03 F3 A4 85 | .......+........
01ED10 | C0 5E 75 55 68 18 01 00 00 E8 5B 13 0B 00 83 C4 | .^uUh.....[.....
01ED20 | 04 89 44 24 08 85 C0 C7 44 24 14 00 00 00 00 74 | ..D$....D$.....t
```

90 90

Current position: 126071 / 01EC77

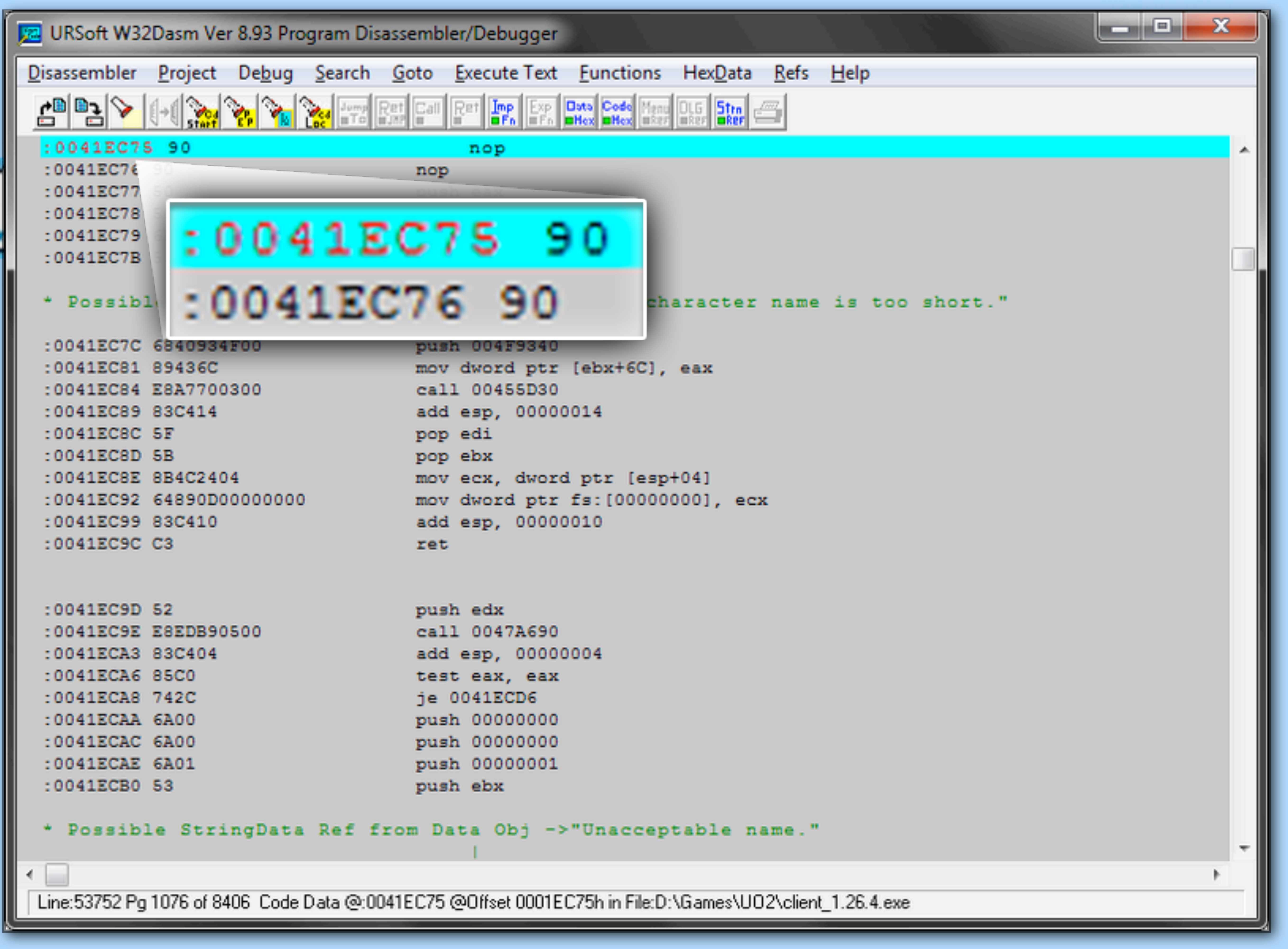
HEX-HI

... and open the file, going to that location, in a hexeditor

Where we see the same hex codes

Changing them to “90”s...

GAME HACKING


URSoft W32Dasm Ver 8.93 Program Disassembler/Debugger
Disassembler Project Debug Search Goto Execute Text Functions HexData Refs Help

```
:0041EC75 90                         nop
:0041EC76                       nop
:0041EC77
:0041EC78
:0041EC79
:0041EC7B

* Possibl                                     character name is too short."

:0041EC7C 6840934F00            push 004F9340
:0041EC81 89436C                mov dword ptr [ebx+6C], eax
:0041EC84 E8A7700300            call 00455D30
:0041EC89 83C414                add esp, 00000014
:0041EC8C 5F                    pop edi
:0041EC8D 5B                    pop ebx
:0041EC8E 8B4C2404              mov ecx, dword ptr [esp+04]
:0041EC92 64890D00000000        mov dword ptr fs:[00000000], ecx
:0041EC99 83C410                add esp, 00000010
:0041EC9C C3                    ret


:0041EC9D 52                    push edx
:0041EC9E E8EDB90500            call 0047A690
:0041ECA3 83C404                add esp, 00000004
:0041ECA6 85C0                  test eax, eax
:0041ECA8 742C                  je 0041ECD6
:0041ECAA 6A00                  push 00000000
:0041ECAC 6A00                  push 00000000
:0041ECAE 6A01                  push 00000001
:0041ECB0 53                    push ebx

* Possible StringData Ref from Data Obj ->"Unacceptable name."
```

```
:0041EC75 90
:0041EC76 90
```

Line:53752 Pg 1076 of 8406 Code Data @:0041EC75 @Offset 0001EC75h in File:D:\Games\UO2\client_1.26.4.exe

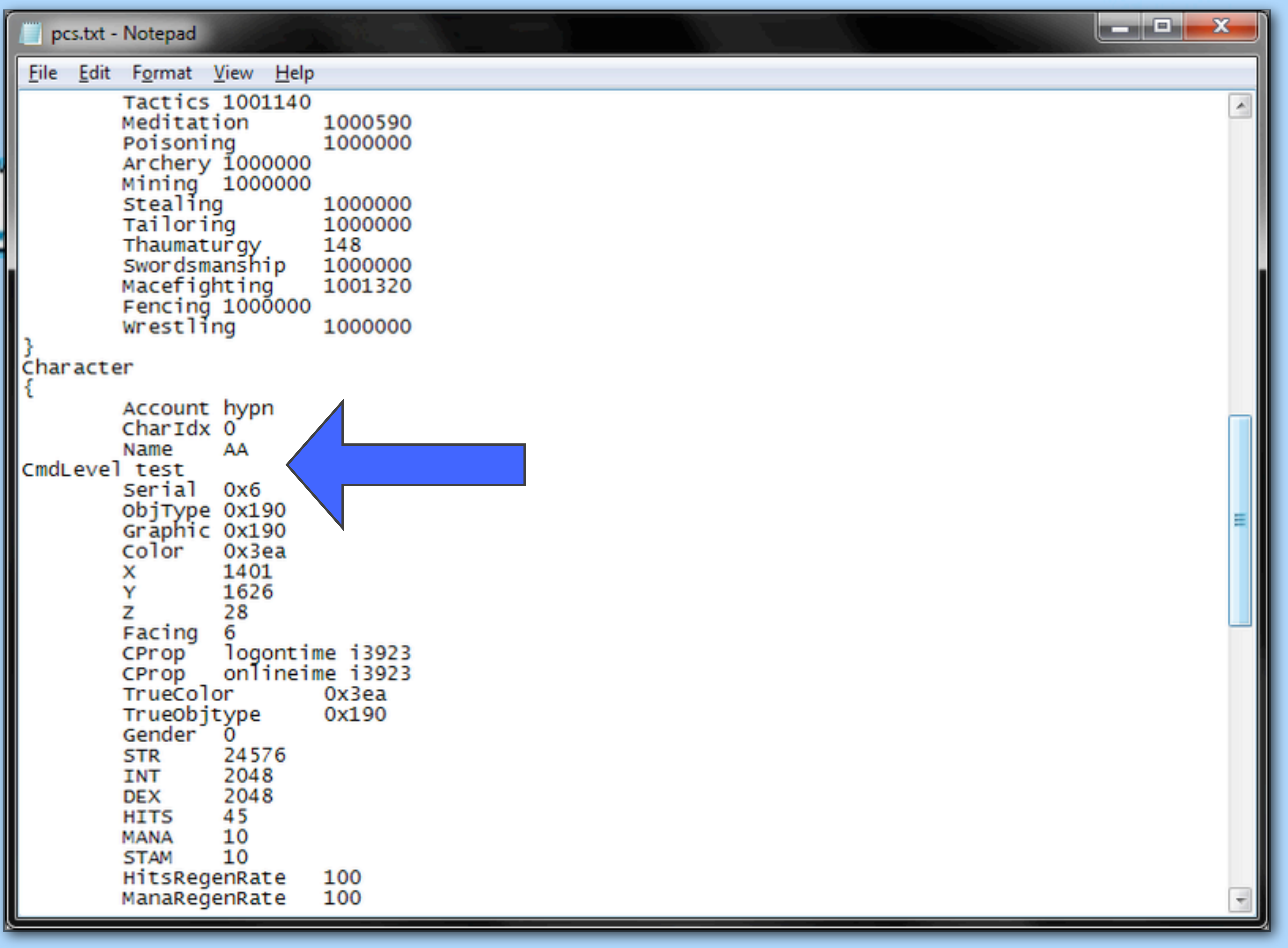
... and open the file, going to that location, in a hexeditor

Where we see the same hex codes

Changing them to “90”s... “nop”s them out

“nop”s basically mean “do nothing” (“No Operation”) - in this case, never error on invalid characters

GAME HACKING



```
        Tactics 1001140
        Meditation      1000590
        Poisoning       1000000
        Archery 1000000
        Mining  1000000
        Stealing        1000000
        Tailoring       1000000
        Thaumaturgy     148
        Swordsmanship   1000000
        Macefighting    1001320
        Fencing 1000000
        Wrestling       1000000
}
Character
{
        Account hypn
        CharIdx 0
        Name    AA
CmdLevel test
        Serial  0x6
        ObjType 0x190
        Graphic 0x190
        Color   0x3ea
        X       1401
        Y       1626
        Z       28
        Facing  6
        CProp   logontime i3923
        CProp   onlineime i3923
        TrueColor       0x3ea
        TrueObjtype     0x190
        Gender  0
        STR     24576
        INT     2048
        DEX     2048
        HITS    45
        MANA    10
        STAM    10
        HitsRegenRate   100
        ManaRegenRate   100
```

The "CmdLevel test" payload after our marker would give your character GameMaster powers.

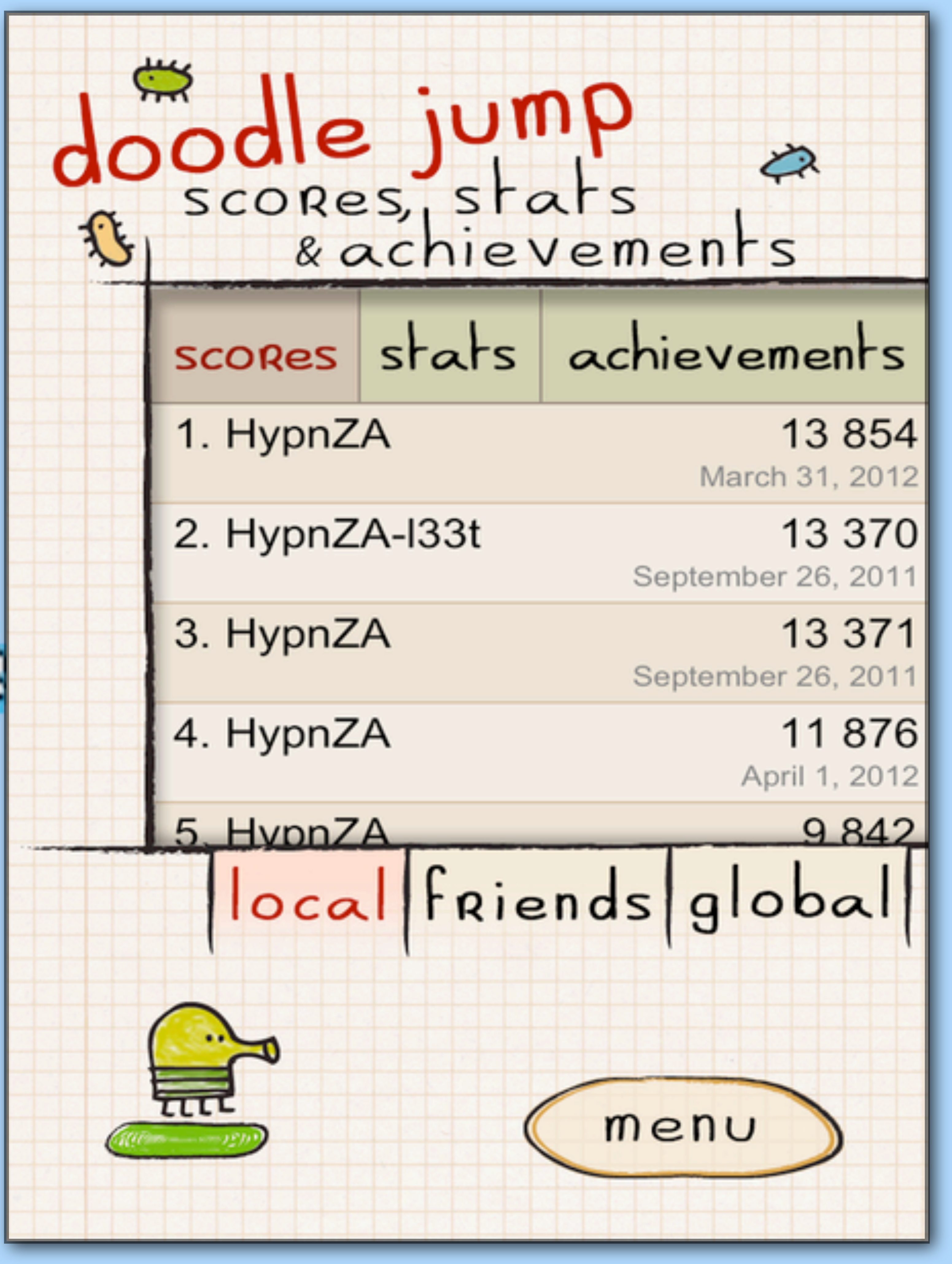
This has been fixed in more recent POL versions - for character names, but theoretically every text input (such as naming pets) may still be vulnerable

ZaCon 4 - Game Hacking

1. Console Games
2. DOS Games
3. Windows Games
4. iPhone / iPad Games

    4.1. Non-Jailbroken hacks - modifying “plist” and other config files

GAME HACKING



doodle jump
scores, stats & achievements

1. HypnZA 13 854
March 31, 2012

2. HypnZA-l33t 13 370
September 26, 2011

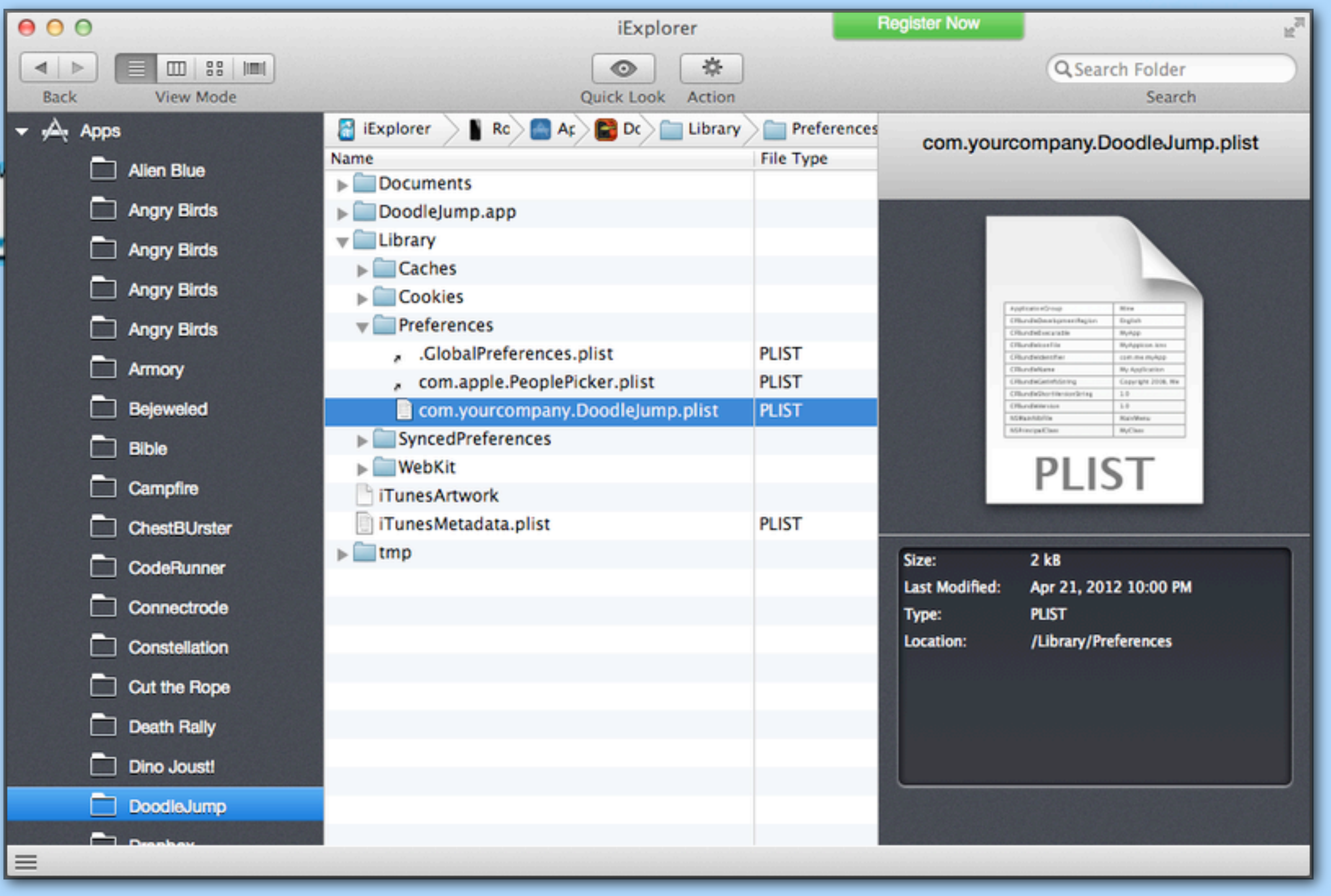
3. HypnZA 13 371
September 26, 2011

4. HypnZA 11 876
April 1, 2012

5. HypnZA 9 842

iPhone games can be hacked, to some degree, without jailbreaking

GAME HACKING



Name	File Type
▶ Documents	
▶ DoodleJump.app	
▼ Library	
▶ Caches	
▶ Cookies	
▼ Preferences	
.GlobalPreferences.plist	PLIST
com.apple.PeoplePicker.plist	PLIST
com.yourcompany.DoodleJump.plist	PLIST
▶ SyncedPreferences	
▶ WebKit	
iTunesArtwork	
iTunesMetadata.plist	PLIST
▶ tmp	

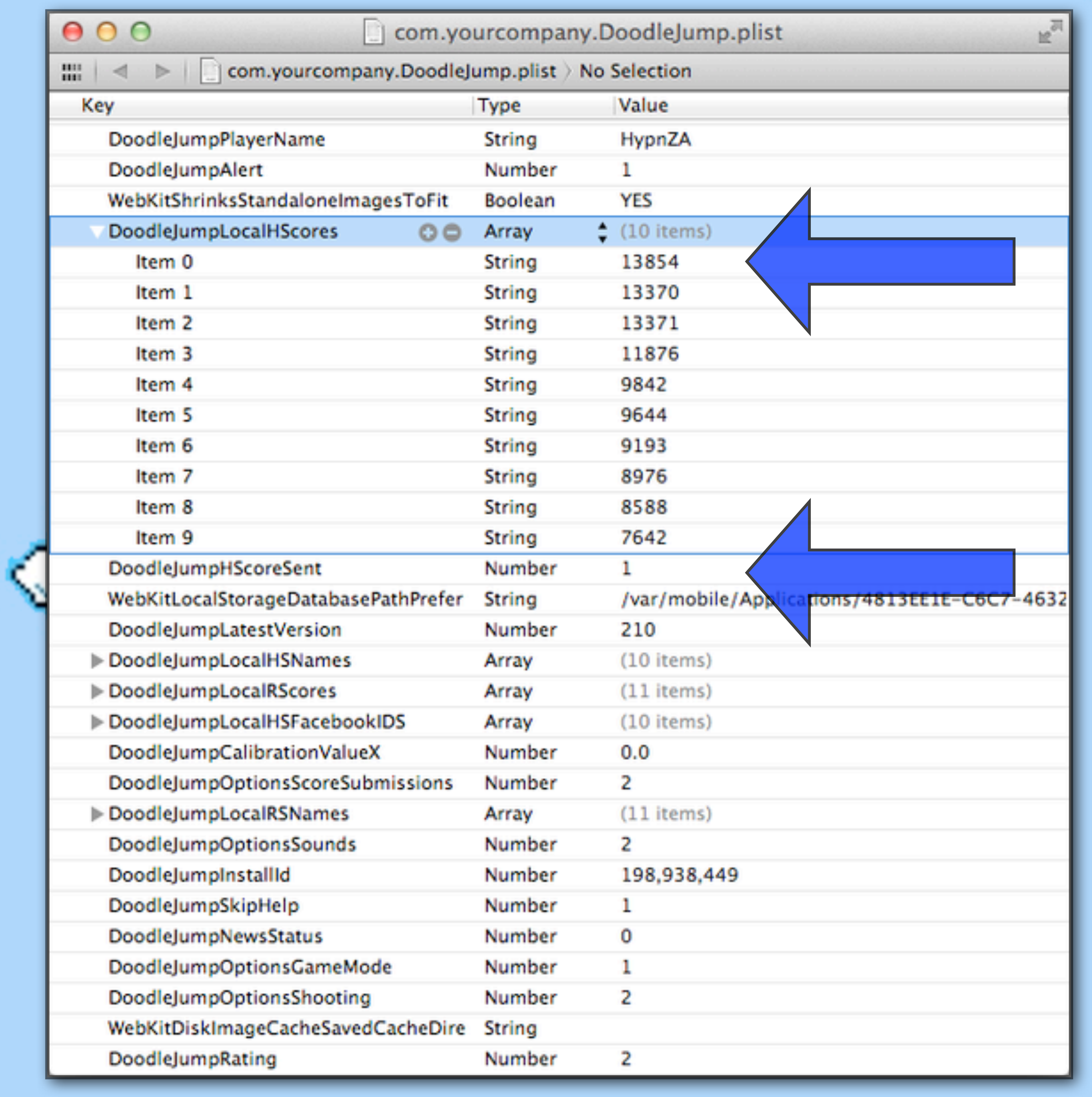
com.yourcompany.DoodleJump.plist

Size: 2 kB
Last Modified: Apr 21, 2012 10:00 PM
Type: PLIST
Location: /Library/Preferences

iPhone games can be hacked, to some degree, without jailbreaking

Using a program like "iExplorer" game files can be accessed

GAME HACKING



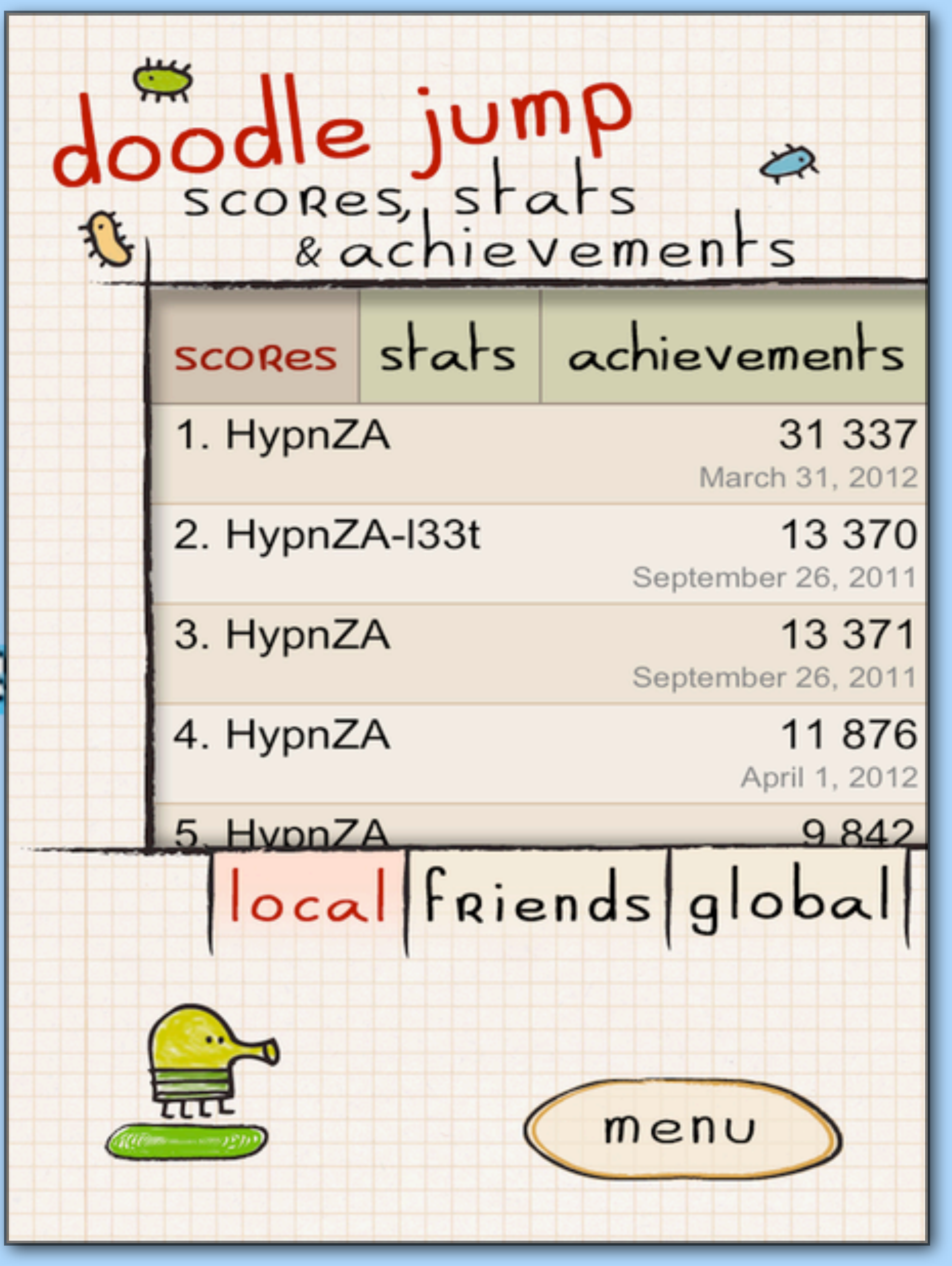
com.yourcompany.DoodleJump.plist
com.yourcompany.DoodleJump.plist 〉 No Selection

Key	Type	Value
DoodleJumpPlayerName	String	HypnZA
DoodleJumpAlert	Number	1
WebKitShrinksStandaloneImagesToFit	Boolean	YES
▼ DoodleJumpLocalHScores	Array	(10 items)
Item 0	String	13854
Item 1	String	13370
Item 2	String	13371
Item 3	String	11876
Item 4	String	9842
Item 5	String	9644
Item 6	String	9193
Item 7	String	8976
Item 8	String	8588
Item 9	String	7642
DoodleJumpHScoreSent	Number	1
WebKitLocalStorageDatabasePathPrefer	String	/var/mobile/Applications/4813EE1E-C6C7-4632
DoodleJumpLatestVersion	Number	210
▶ DoodleJumpLocalHSNames	Array	(10 items)
▶ DoodleJumpLocalRScores	Array	(11 items)
▶ DoodleJumpLocalHSFacebookIDS	Array	(10 items)
DoodleJumpCalibrationValueX	Number	0.0
DoodleJumpOptionsScoreSubmissions	Number	2
▶ DoodleJumpLocalRSNames	Array	(11 items)
DoodleJumpOptionsSounds	Number	2
DoodleJumpInstallId	Number	198,938,449
DoodleJumpSkipHelp	Number	1
DoodleJumpNewsStatus	Number	0
DoodleJumpOptionsGameMode	Number	1
DoodleJumpOptionsShooting	Number	2
WebKitDiskImageCacheSavedCacheDire	String	
DoodleJumpRating	Number	2

iPhone games can be hacked, to some degree, without jailbreaking

Using a program like "iExplorer" game files can be accessed, and changed (eg: changing a high-score, and setting scores as not have been sent yet)

GAME HACKING



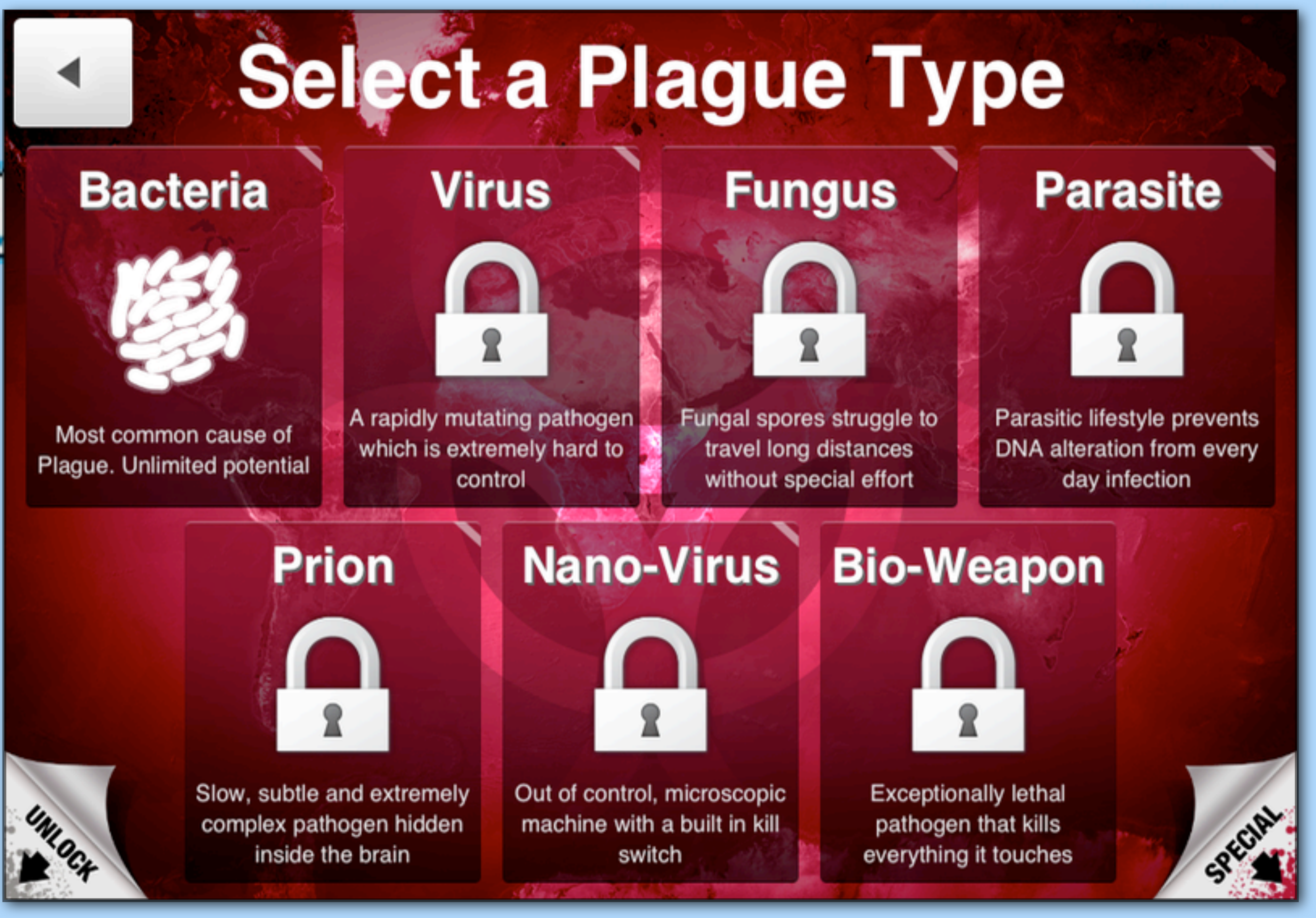
1. HypnZA	31 337	March 31, 2012
2. HypnZA-l33t	13 370	September 26, 2011
3. HypnZA	13 371	September 26, 2011
4. HypnZA	11 876	April 1, 2012
5. HypnZA	9 842	

iPhone games can be hacked, to some degree, without jailbreaking

Using a program like "iExplorer" game files can be accessed, and changed (eg: changing a high-score, and setting scores as not have been sent yet)

The next time the game is run, the scores are updated!

GAME HACKING



Select a Plague Type

Bacteria

Most common cause of Plague. Unlimited potential

Virus

A rapidly mutating pathogen which is extremely hard to control

Fungus

Fungal spores struggle to travel long distances without special effort

Parasite

Parasitic lifestyle prevents DNA alteration from every day infection

Prion

Slow, subtle and extremely complex pathogen hidden inside the brain

Nano-Virus

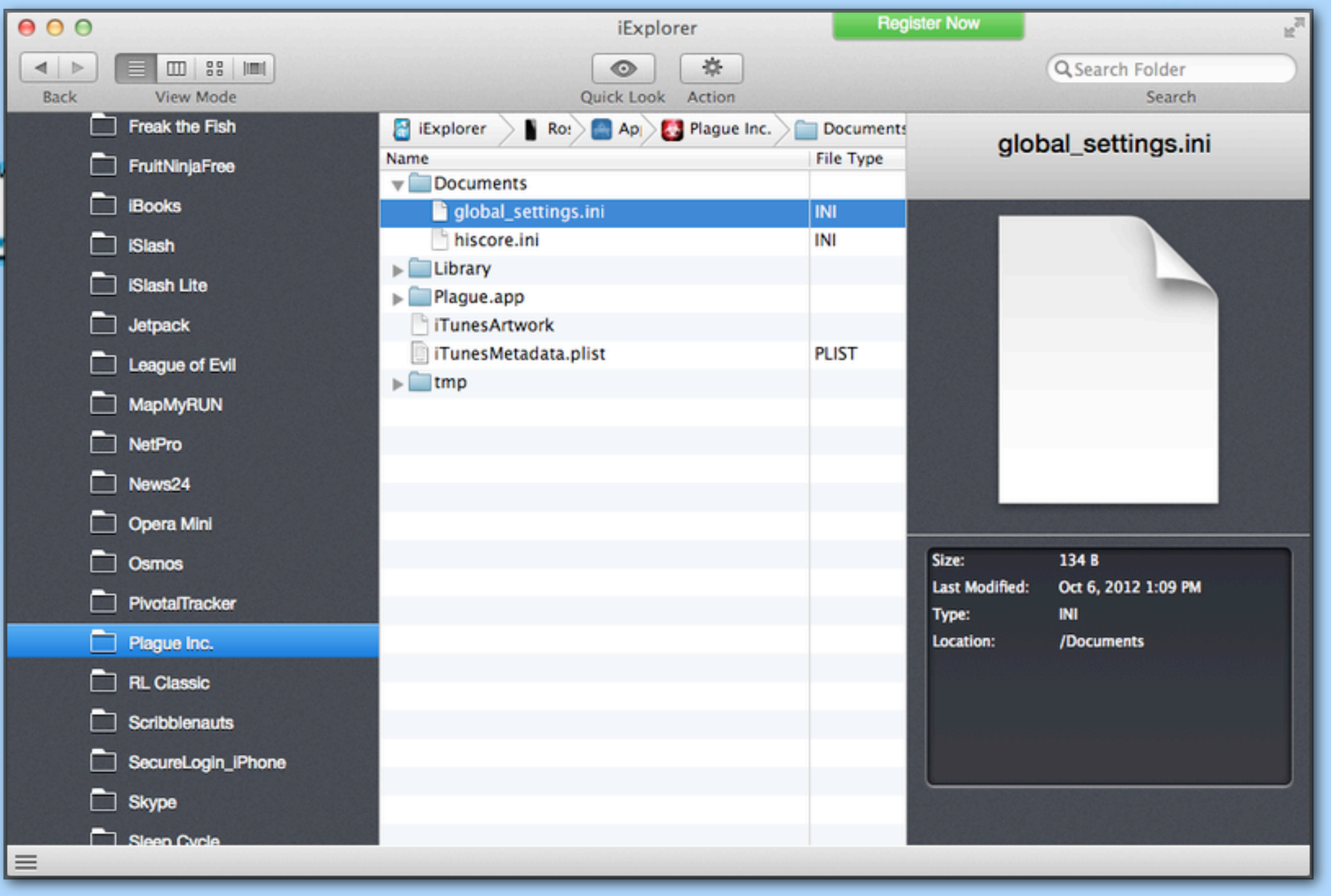
Out of control, microscopic machine with a built in kill switch

Bio-Weapon

Exceptionally lethal pathogen that kills everything it touches

Some games “lock” content until certain levels or scores are reached (or payments have been made)

GAME HACKING



Name	File Type
Documents	
global_settings.ini	INI
hiscore.ini	INI
Library	
Plague.app	
iTunesArtwork	
iTunesMetadata.plist	PLIST
tmp	

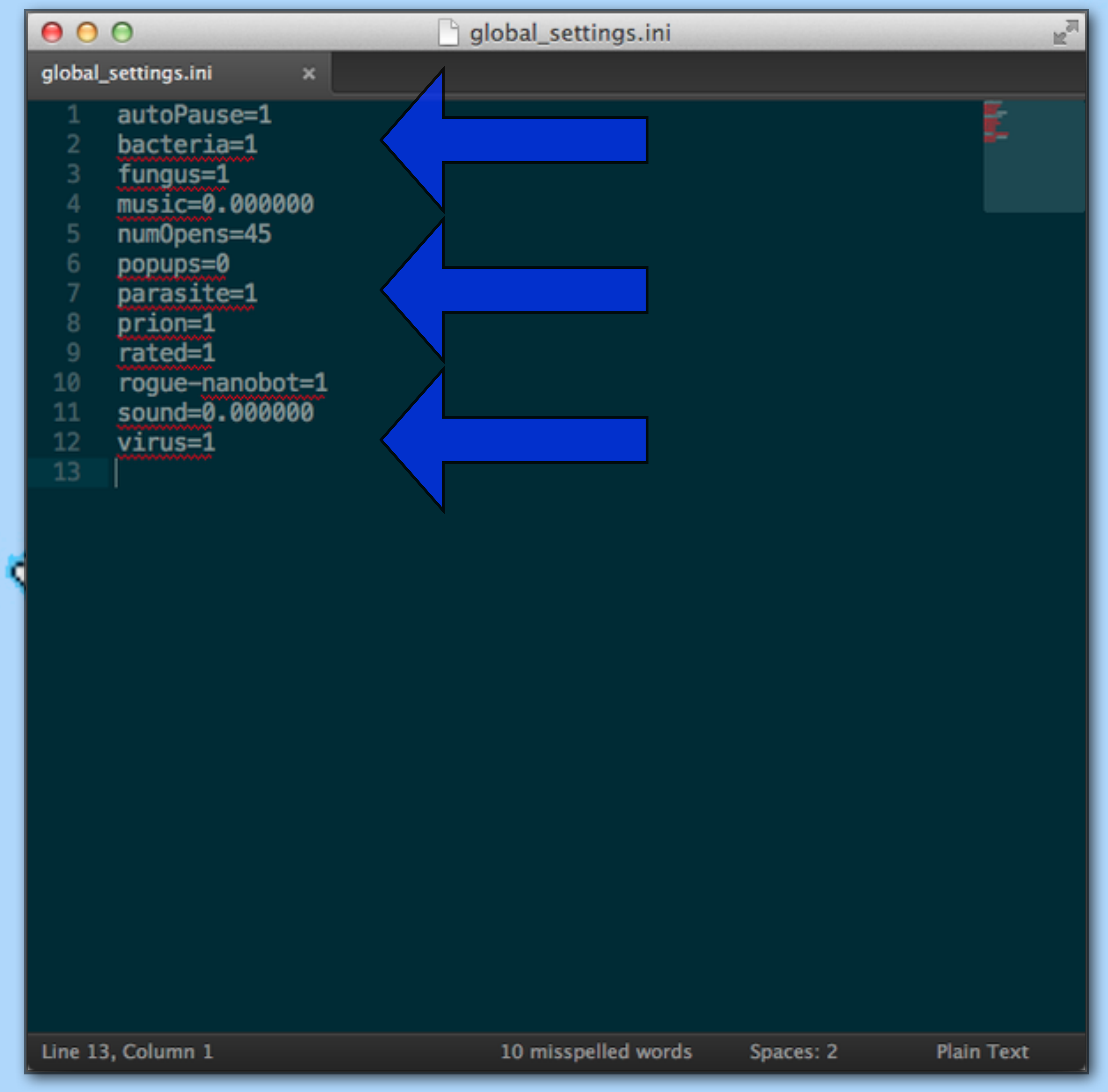
global_settings.ini

Size: 134 B
Last Modified: Oct 6, 2012 1:09 PM
Type: INI
Location: /Documents

Some games "lock" content until certain levels or scores are reached (or payments have been made)

Often these "locks" are controlled in config files (look out for "ini", "plist" and "sqlite" files!)

GAME HACKING



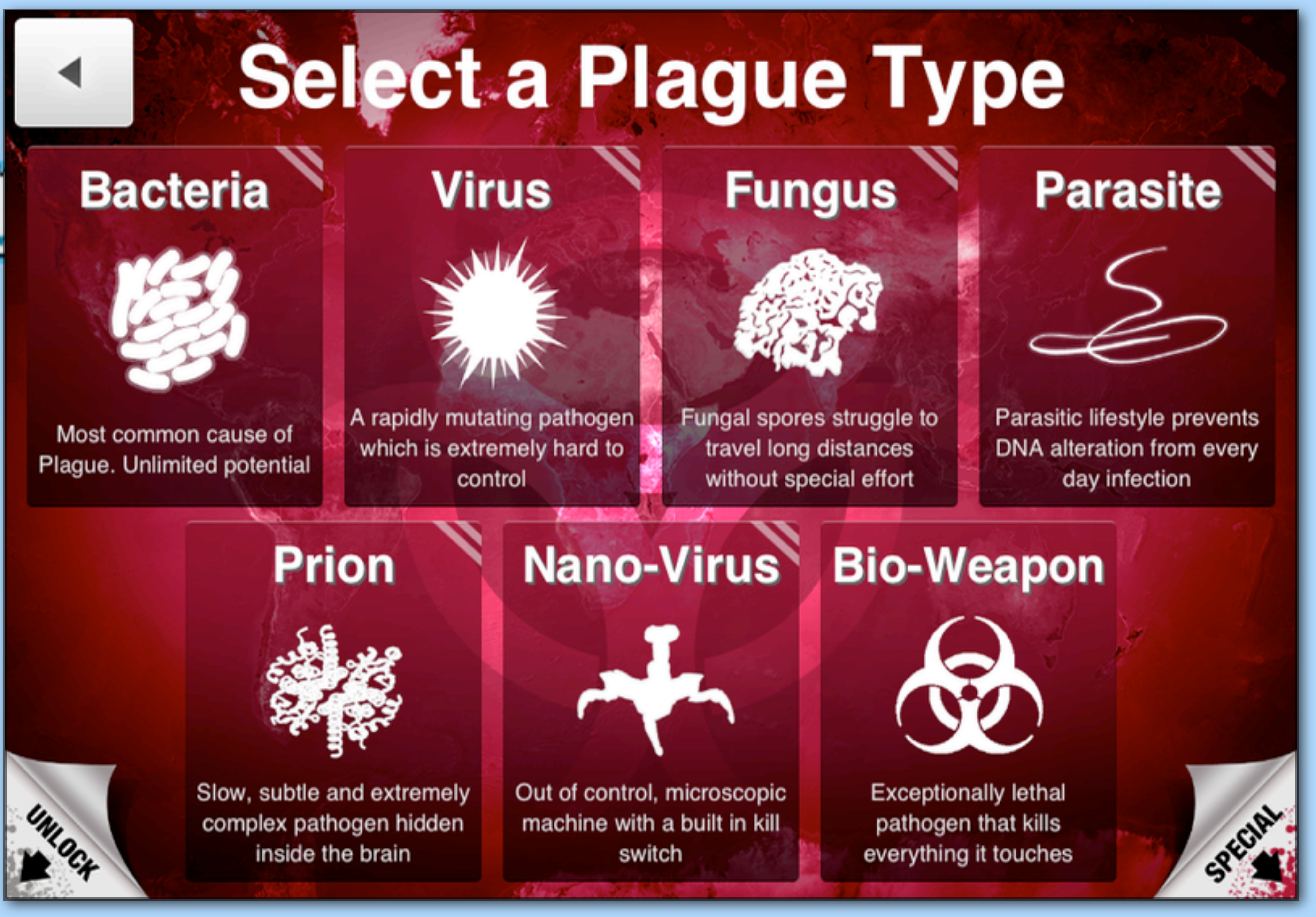
```
autoPause=1
bacteria=1
fungus=1
music=0.000000
numOpens=45
popups=0
parasite=1
prion=1
rated=1
rogue-nanobot=1
sound=0.000000
virus=1

```

Some games “lock” content until certain levels or scores are reached (or payments have been made)

Often these “locks” are controlled in config files (look out for “ini”, “plist” and “sqlite” files!)

Changing “0” values to “1”s often does the trick

GAME HACKING



Select a Plague Type

Bacteria

Most common cause of Plague. Unlimited potential

Virus

A rapidly mutating pathogen which is extremely hard to control

Fungus

Fungal spores struggle to travel long distances without special effort

Parasite

Parasitic lifestyle prevents DNA alteration from every day infection

Prion

Slow, subtle and extremely complex pathogen hidden inside the brain

Nano-Virus

Out of control, microscopic machine with a built in kill switch

Bio-Weapon

Exceptionally lethal pathogen that kills everything it touches

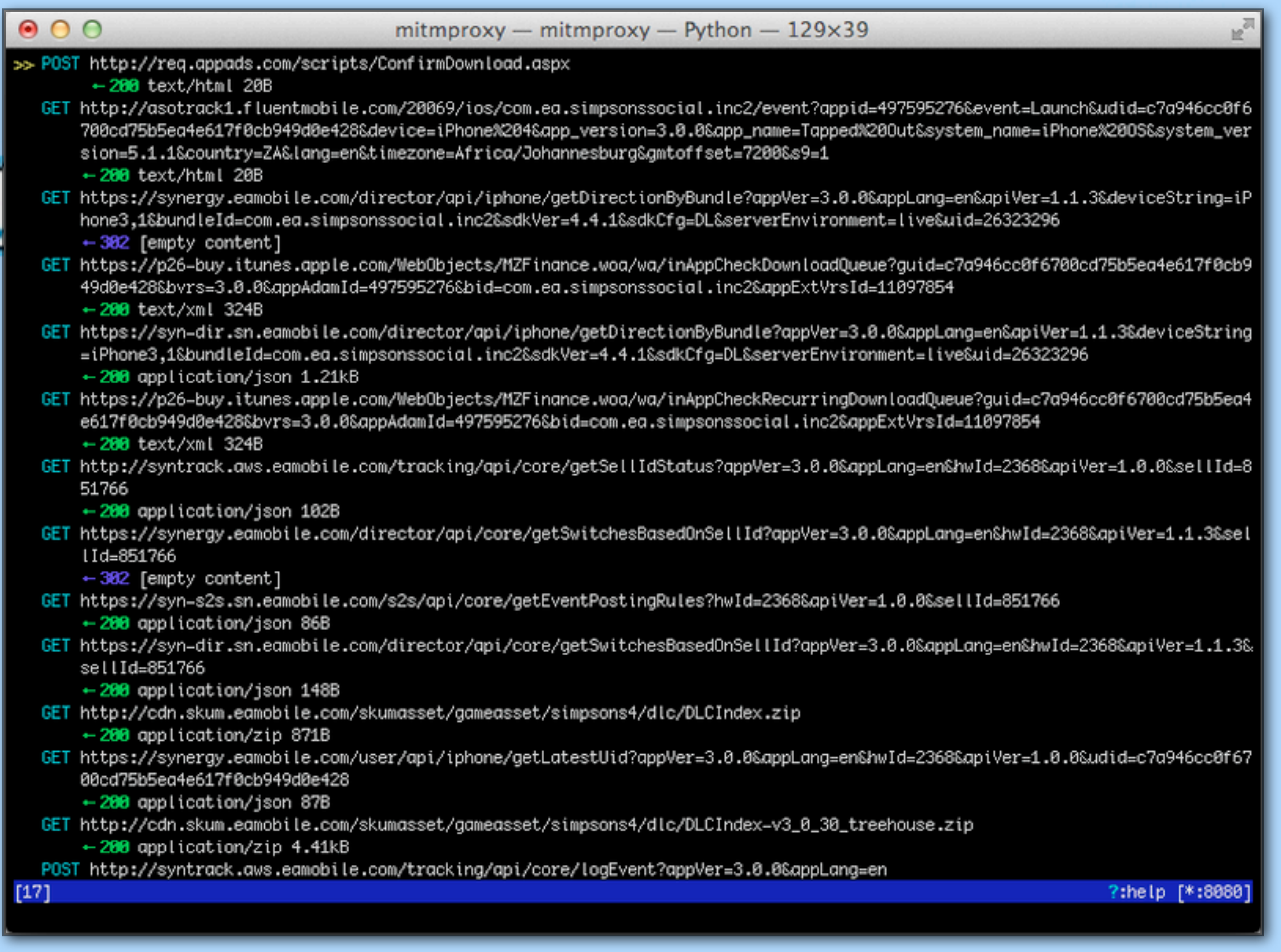
Some games "lock" content until certain levels or scores are reached (or payments have been made)

Often these "locks" are controlled in config files (look out for "ini", "plist" and "sqlite" files!)

Changing "0" values to "1"s often does the trick

Unlocked!

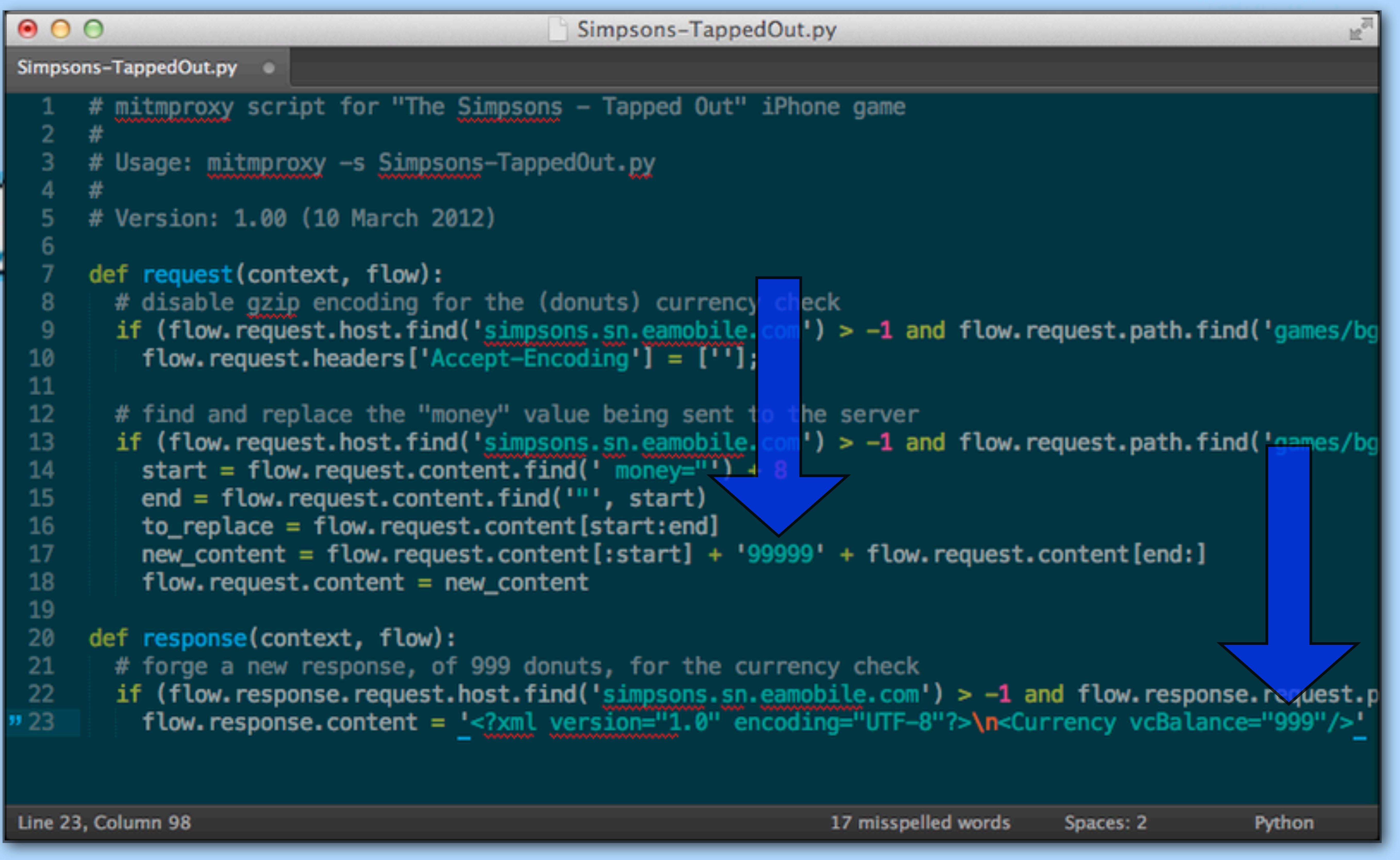
GAME HACKING



```
>> POST http://req.appads.com/scripts/ConfirmDownload.aspx
        ←200 text/html 20B
   GET http://asotrack1.fluentmobile.com/20069/ios/com.ea.simpsonssocial.inc2/event?appid=497595276&event=Launch&udid=c7a946cc0f6
       700cd75b5ea4e617f0cb949d0e428&device=iPhone%204&app_version=3.0.0&app_name=Tapped%20Out&system_name=iPhone%20OS&system_ver
       sion=5.1.1&country=ZA&lang=en&timezone=Africa/Johannesburg&gmtoffset=7200&s9=1
       ←200 text/html 20B
   GET https://synergy.eamobile.com/director/api/iphone/getDirectionByBundle?appVer=3.0.0&appLang=en&apiVer=1.1.3&deviceString=iP
       hone3,1&bundleId=com.ea.simpsonssocial.inc2&sdkVer=4.4.1&sdkCfg=DL&serverEnvironment=live&uid=26323296
       ←302 [empty content]
   GET https://p26-buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/inAppCheckDownloadQueue?guid=c7a946cc0f6700cd75b5ea4e617f0cb9
       49d0e428&bvrs=3.0.0&appAdamId=497595276&bid=com.ea.simpsonssocial.inc2&appExtVrsId=11097854
       ←200 text/xml 324B
   GET https://syn-dir.sn.eamobile.com/director/api/iphone/getDirectionByBundle?appVer=3.0.0&appLang=en&apiVer=1.1.3&deviceString
       =iPhone3,1&bundleId=com.ea.simpsonssocial.inc2&sdkVer=4.4.1&sdkCfg=DL&serverEnvironment=live&uid=26323296
       ←200 application/json 1.21kB
   GET https://p26-buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/inAppCheckRecurringDownloadQueue?guid=c7a946cc0f6700cd75b5ea4
       e617f0cb949d0e428&bvrs=3.0.0&appAdamId=497595276&bid=com.ea.simpsonssocial.inc2&appExtVrsId=11097854
       ←200 text/xml 324B
   GET http://syntrack.aws.eamobile.com/tracking/api/core/getSellIdStatus?appVer=3.0.0&appLang=en&hwId=2368&apiVer=1.0.0&sellId=8
       51766
       ←200 application/json 102B
   GET https://synergy.eamobile.com/director/api/core/getSwitchesBasedOnSellId?appVer=3.0.0&appLang=en&hwId=2368&apiVer=1.1.3&sel
       lId=851766
       ←302 [empty content]
   GET https://syn-s2s.sn.eamobile.com/s2s/api/core/getEventPostingRules?hwId=2368&apiVer=1.0.0&sellId=851766
       ←200 application/json 86B
   GET https://syn-dir.sn.eamobile.com/director/api/core/getSwitchesBasedOnSellId?appVer=3.0.0&appLang=en&hwId=2368&apiVer=1.1.3&
       sellId=851766
       ←200 application/json 148B
   GET http://cdn.skum.eamobile.com/skumasset/gameasset/simpsons4/dlc/DLCIndex.zip
       ←200 application/zip 871B
   GET https://synergy.eamobile.com/user/api/iphone/getLatestUid?appVer=3.0.0&appLang=en&hwId=2368&apiVer=1.0.0&udid=c7a946cc0f67
       00cd75b5ea4e617f0cb949d0e428
       ←200 application/json 87B
   GET http://cdn.skum.eamobile.com/skumasset/gameasset/simpsons4/dlc/DLCIndex-v3_0_30_treehouse.zip
       ←200 application/zip 4.41kB
   POST http://syntrack.aws.eamobile.com/tracking/api/core/logEvent?appVer=3.0.0&appLang=en
[17]                                                                                                          ?:help [*:8080]
```

Tools like Burp Suite, and mitmproxy, can be used to intercept game traffic

GAME HACKING



```
# mitmproxy script for "The Simpsons - Tapped Out" iPhone game
#
# Usage: mitmproxy -s Simpsons-TappedOut.py
#
# Version: 1.00 (10 March 2012)

def request(context, flow):
  # disable gzip encoding for the (donuts) currency check
  if (flow.request.host.find('simpsons.sn.eamobile.com') > -1 and flow.request.path.find('games/bg
    flow.request.headers['Accept-Encoding'] = [''];

  # find and replace the "money" value being sent to the server
  if (flow.request.host.find('simpsons.sn.eamobile.com') > -1 and flow.request.path.find('games/bg
    start = flow.request.content.find(' money="') + 8
    end = flow.request.content.find('"', start)
    to_replace = flow.request.content[start:end]
    new_content = flow.request.content[:start] + '99999' + flow.request.content[end:]
    flow.request.content = new_content

def response(context, flow):
  # forge a new response, of 999 donuts, for the currency check
  if (flow.response.request.host.find('simpsons.sn.eamobile.com') > -1 and flow.response.request.p
    flow.response.content = '<?xml version="1.0" encoding="UTF-8"?>\n<Currency vcBalance="999"/>'
```

Tools like Burp Suite, and mitmproxy, can be used to intercept game traffic

And re-write values, such as XP, gold, scores, or “premium” (paid-for) credits

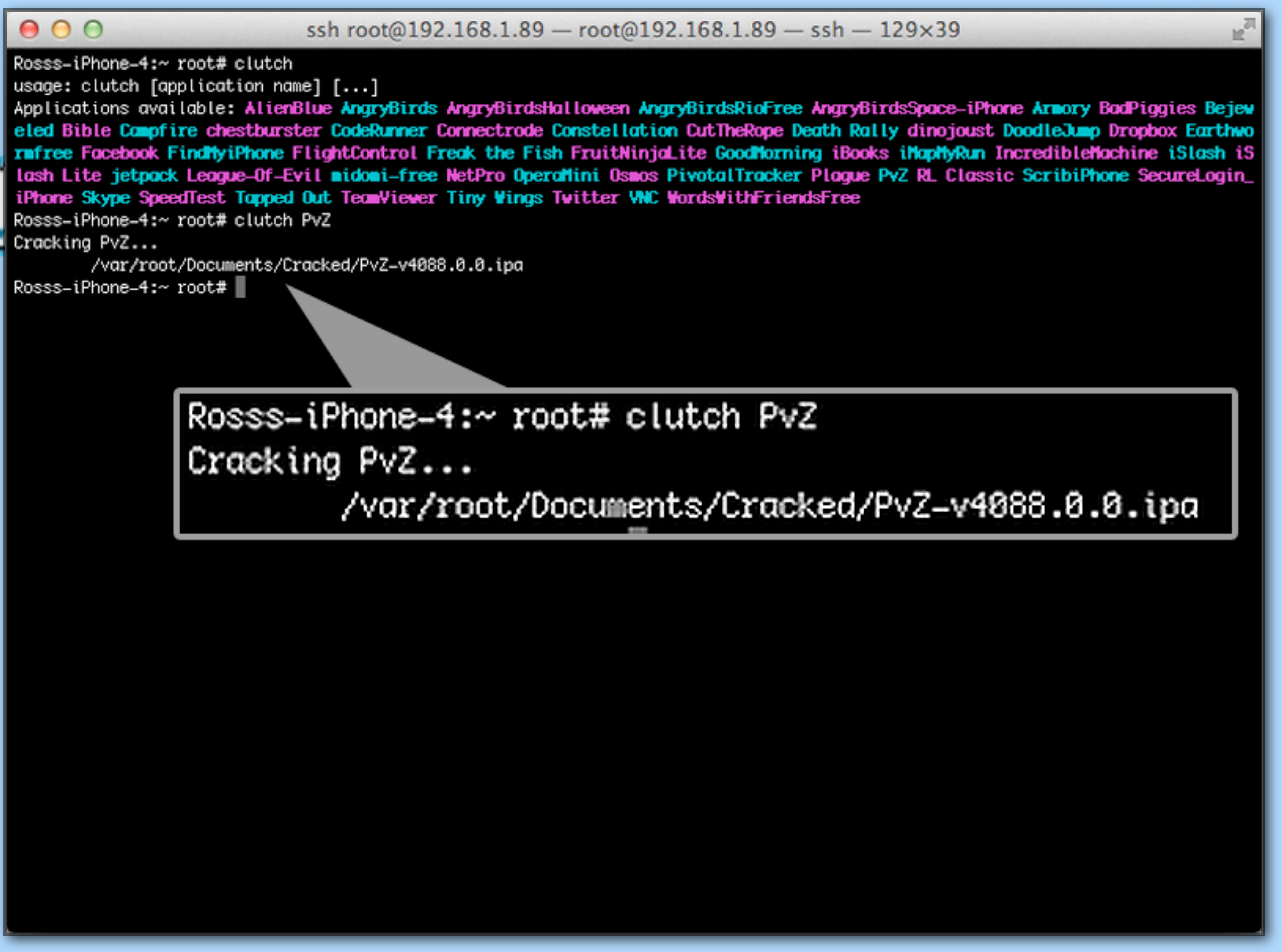
mitmproxy lets you write scripts to do this automatically

ZaCon 4 - Game Hacking

1. Console Games
2. DOS Games
3. Windows Games
4. iPhone / iPad Games

    4.2. Jailbroken hacks - decompiling with IDA Pro

GAME HACKING



```
Rosss-iPhone-4:~ root# clutch
usage: clutch [application name] [...]
Applications available: AlienBlue AngryBirds AngryBirdsHalloween AngryBirdsRioFree AngryBirdsSpace-iPhone Armory BadPiggies Bejew
eled Bible Campfire chestburster CodeRunner Connectrode Constellation CutTheRope Death Rally dinojoust DoodleJump Dropbox Earthwo
rmfree Facebook FindMyiPhone FlightControl Freak the Fish FruitNinjaLite GoodMorning iBooks iMapMyRun IncredibleMachine iSlash iS
lash Lite jetpack League-Of-Evil midomi-free NetPro OperaMini Osmos PivotalTracker Plague PvZ RL Classic ScribiPhone SecureLogin_
iPhone Skype SpeedTest Tapped Out TeamViewer Tiny Wings Twitter VNC WordsWithFriendsFree
Rosss-iPhone-4:~ root# clutch PvZ
Cracking PvZ...
        /var/root/Documents/Cracked/PvZ-v4088.0.0.ipa
Rosss-iPhone-4:~ root#
```

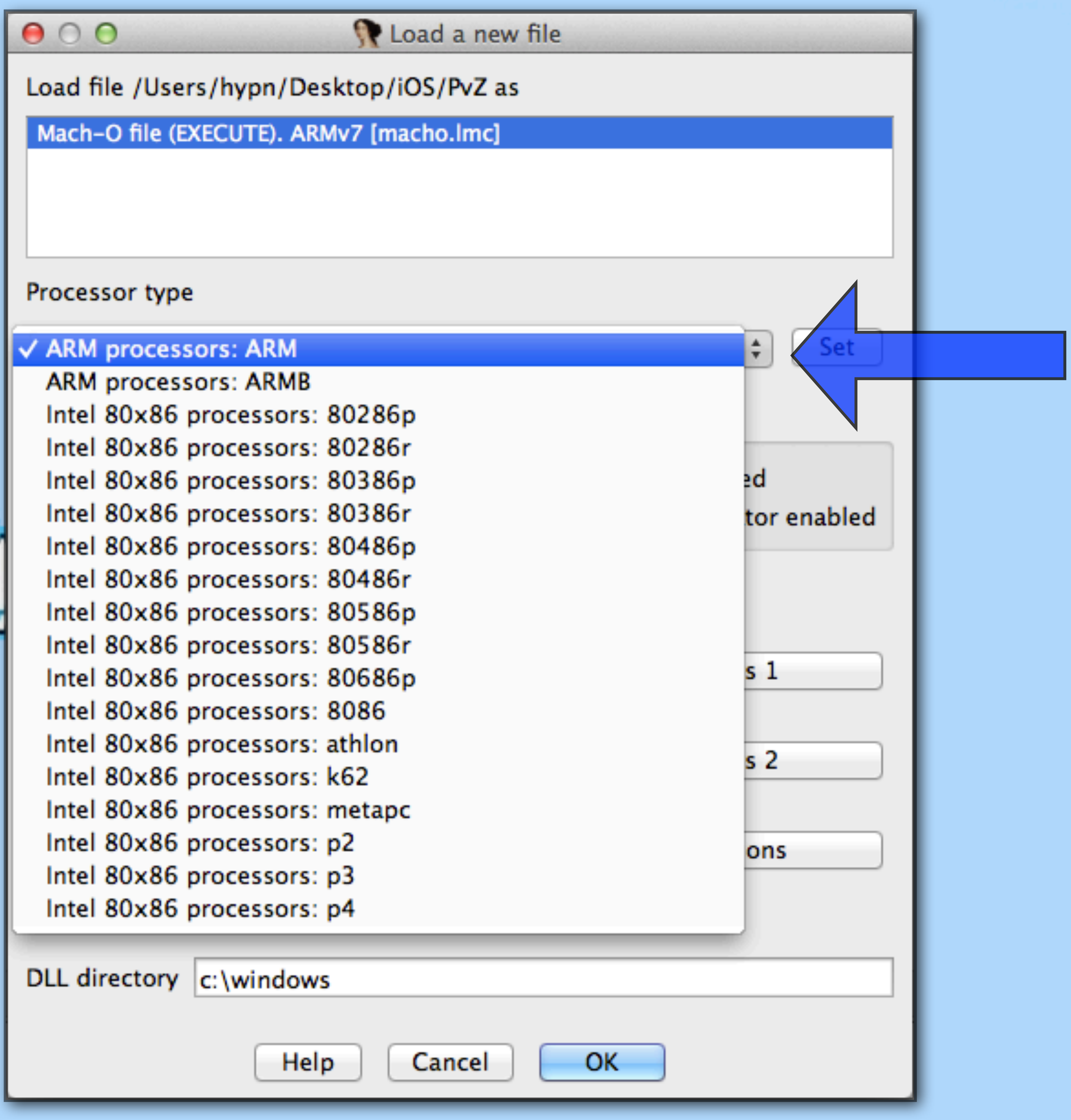
Rosss-iPhone-4:~ root# clutch PvZ
Cracking PvZ...
/var/root/Documents/Cracked/PvZ-v4088.0.0.ipa

iOS games are encrypted when downloaded from the App Store

Calculating offsets, using “gdb” to dump memory, and trial and error byte switching can decrypt apps... OR...

A jailbroken app called “clutch” can be used to decrypt them quickly and easily

GAME HACKING



Load a new file

Load file /Users/hypn/Desktop/iOS/PvZ as

Mach-O file (EXECUTE). ARMv7 [macho.lmc]

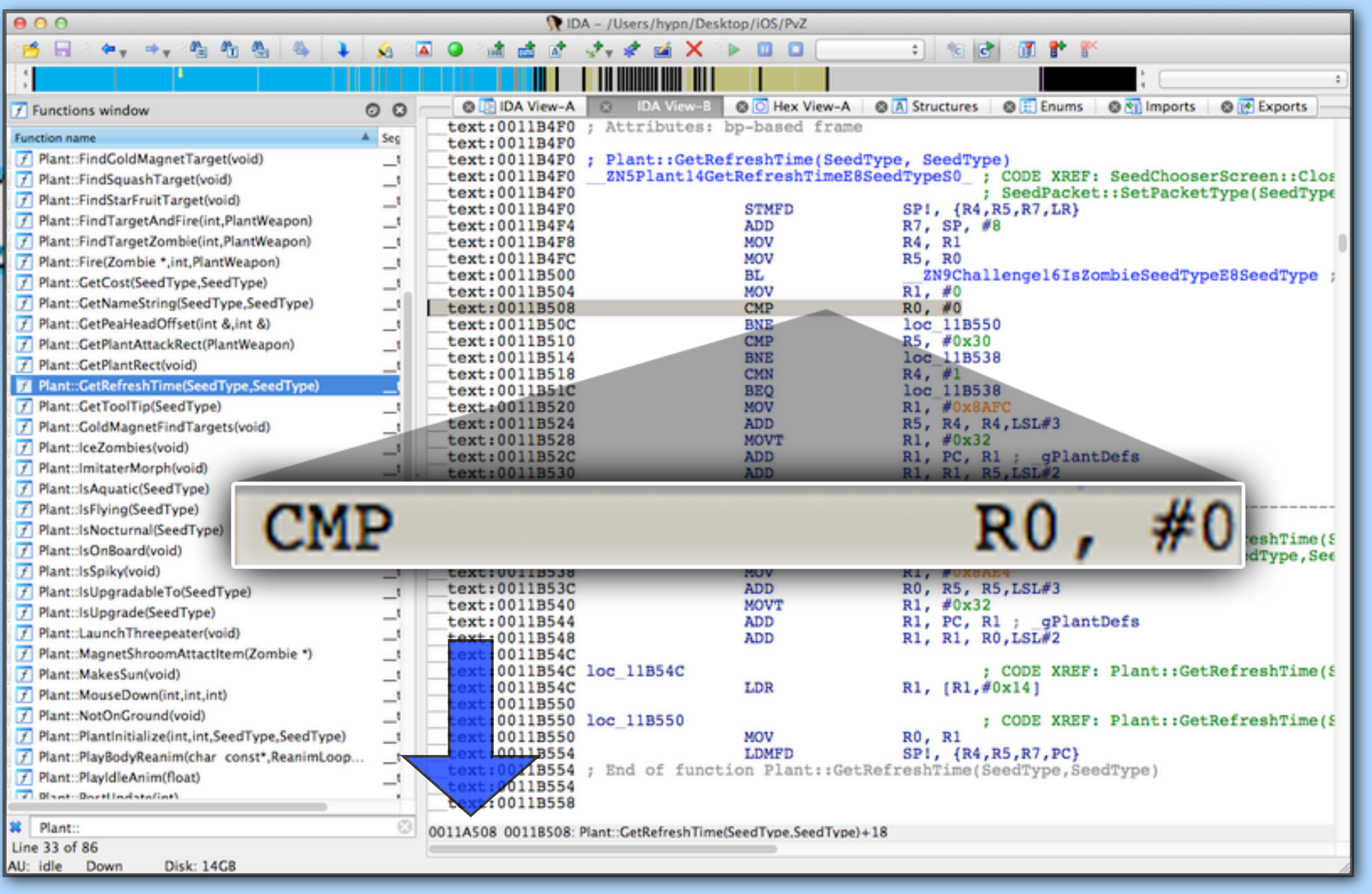
Processor type

✓ ARM processors: ARM
ARM processors: ARMB
Intel 80x86 processors: 80286p
Intel 80x86 processors: 80286r
Intel 80x86 processors: 80386p
Intel 80x86 processors: 80386r
Intel 80x86 processors: 80486p
Intel 80x86 processors: 80486r
Intel 80x86 processors: 80586p
Intel 80x86 processors: 80586r
Intel 80x86 processors: 80686p
Intel 80x86 processors: 8086
Intel 80x86 processors: athlon
Intel 80x86 processors: k62
Intel 80x86 processors: metapc
Intel 80x86 processors: p2
Intel 80x86 processors: p3
Intel 80x86 processors: p4

DLL directory: c:\windows

Decrypted iOS apps can be opened in "IDA Pro" - be sure to set the "Processor type" to "ARM" though!

GAME HACKING



```
Plant::FindGoldMagnetTarget(void)
Plant::FindSquashTarget(void)
Plant::FindStarFruitTarget(void)
Plant::FindTargetAndFire(int,PlantWeapon)
Plant::FindTargetZombie(int,PlantWeapon)
Plant::Fire(Zombie *,int,PlantWeapon)
Plant::GetCost(SeedType,SeedType)
Plant::GetNameString(SeedType,SeedType)
Plant::GetPeaHeadOffset(int &,int &)
Plant::GetPlantAttackRect(PlantWeapon)
Plant::GetPlantRect(void)
Plant::GetRefreshTime(SeedType,SeedType)
Plant::GetToolTip(SeedType)
Plant::GoldMagnetFindTargets(void)
Plant::IceZombies(void)
Plant::ImitaterMorph(void)
Plant::IsAquatic(SeedType)
Plant::IsFlying(SeedType)
Plant::IsNocturnal(SeedType)
Plant::IsOnBoard(void)
Plant::IsSpiky(void)
Plant::IsUpgradableTo(SeedType)
Plant::IsUpgrade(SeedType)
Plant::LaunchThreepeater(void)
Plant::MagnetShroomAttactItem(Zombie *)
Plant::MakesSun(void)
Plant::MouseDown(int,int,int)
Plant::NotOnGround(void)
Plant::PlantInitialize(int,int,SeedType,SeedType)
Plant::PlayBodyReanim(char  const*,ReanimLoop...
Plant::PlayIdleAnim(float)
Plant::PostUpdate(int)

Plant::
Line 33 of 86
AU:  idle     Down        Disk: 14GB
```

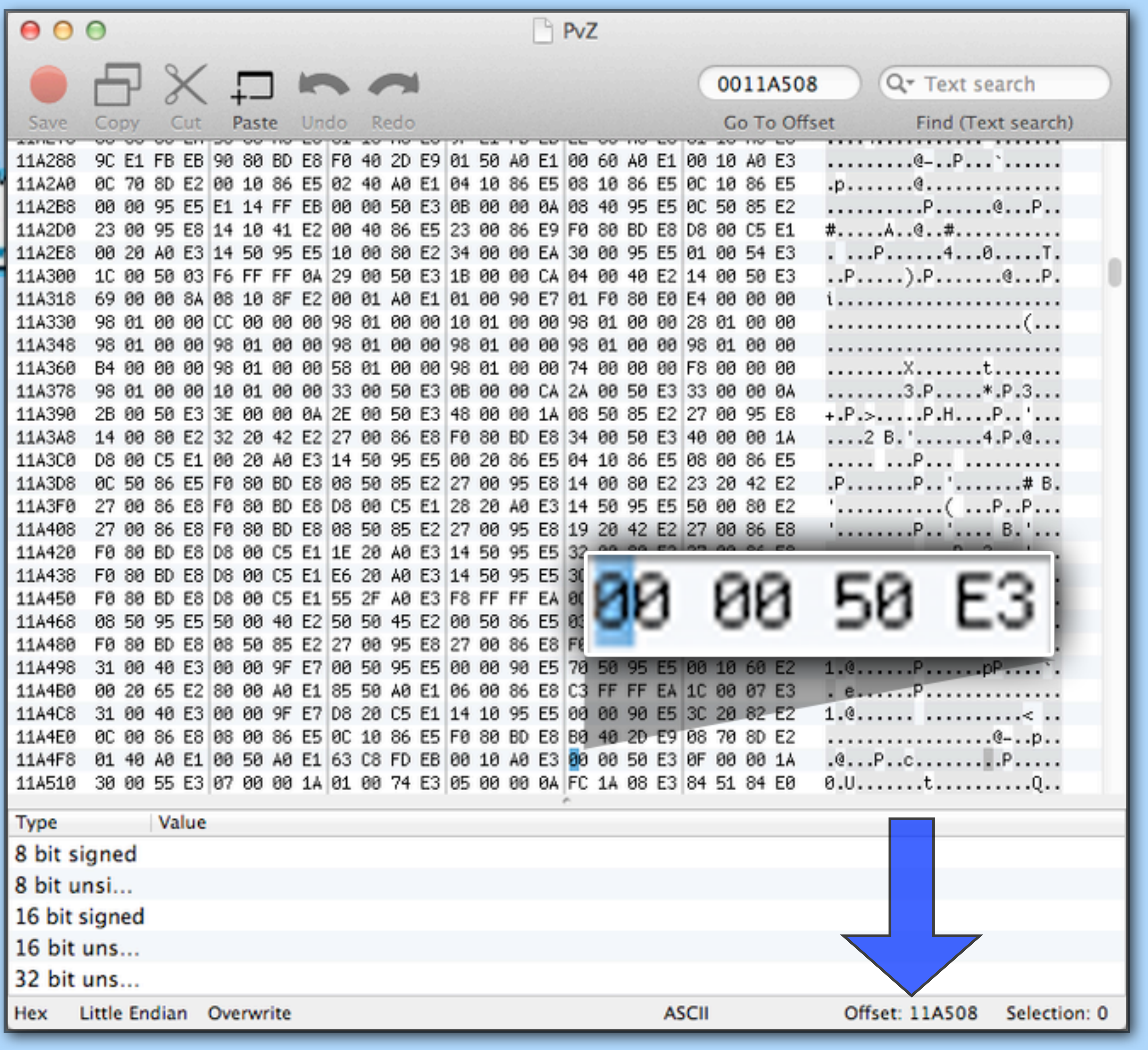
```
text:0011B4F0 ; Attributes: bp-based frame
text:0011B4F0
text:0011B4F0 ; Plant::GetRefreshTime(SeedType, SeedType)
text:0011B4F0 __ZN5Plant14GetRefreshTimeE8SeedTypeS0_ ; CODE XREF: SeedChooserScreen::Clos
text:0011B4F0                                         ; SeedPacket::SetPacketType(SeedType
text:0011B4F0                 STMFD           SP!, {R4,R5,R7,LR}
text:0011B4F4                 ADD             R7, SP, #8
text:0011B4F8                 MOV             R4, R1
text:0011B4FC                 MOV             R5, R0
text:0011B500                 BL              __ZN9Challenge16IsZombieSeedTypeE8SeedType ;
text:0011B504                 MOV             R1, #0
text:0011B508                 CMP             R0, #0
text:0011B50C                 BNE             loc_11B550
text:0011B510                 CMP             R5, #0x30
text:0011B514                 BNE             loc_11B538
text:0011B518                 CMN             R4, #1
text:0011B51C                 BEQ             loc_11B538
text:0011B520                 MOV             R1, #0x8AFC
text:0011B524                 ADD             R5, R4, R4,LSL#3
text:0011B528                 MOVT            R1, #0x32
text:0011B52C                 ADD             R1, PC, R1 ; _gPlantDefs
text:0011B530                 ADD             R1, R1, R5,LSL#2

CMP                                          R0, #0

text:0011B538                 MOV             R1, #0x8AE4
text:0011B53C                 ADD             R0, R5, R5,LSL#3
text:0011B540                 MOVT            R1, #0x32
text:0011B544                 ADD             R1, PC, R1 ; _gPlantDefs
text:0011B548                 ADD             R1, R1, R0,LSL#2
text:0011B54C
text:0011B54C loc_11B54C                              ; CODE XREF: Plant::GetRefreshTime(S
text:0011B54C                 LDR             R1, [R1,#0x14]
text:0011B550
text:0011B550 loc_11B550                              ; CODE XREF: Plant::GetRefreshTime(S
text:0011B550                 MOV             R0, R1
text:0011B554                 LDMFD           SP!, {R4,R5,R7,PC}
text:0011B554 ; End of function Plant::GetRefreshTime(SeedType,SeedType)
text:0011B554
text:0011B558

0011A508 0011B508: Plant::GetRefreshTime(SeedType,SeedType)+18
```

Decrypted iOS apps can be opened in “IDA Pro” - be sure to set the “Processor type” to “ARM” though!

Analysis will run, displaying function names on the left, allowing you to view their actions

Un-wanted commands can be found, their offsets noted (0011A508)

GAME HACKING



```
11A288  9C E1 FB EB 90 80 BD E8 F0 40 2D E9 01 50 A0 E1 00 60 A0 E1 00 10 A0 E3   .........@-..P...`......
11A2A0  0C 70 8D E2 00 10 86 E5 02 40 A0 E1 04 10 86 E5 08 10 86 E5 0C 10 86 E5   .p.......@..............
11A2B8  00 00 95 E5 E1 14 FF EB 00 00 50 E3 0B 00 00 0A 08 40 95 E5 0C 50 85 E2   ..........P......@...P..
11A2D0  23 00 95 E8 14 10 41 E2 00 40 86 E5 23 00 86 E9 F0 80 BD E8 D8 00 C5 E1   #.....A..@..#...........
11A2E8  00 20 A0 E3 14 50 95 E5 10 00 80 E2 34 00 00 EA 30 00 95 E5 01 00 54 E3   . ...P......4...0.....T.
11A300  1C 00 50 03 F6 FF FF 0A 29 00 50 E3 1B 00 00 CA 04 00 40 E2 14 00 50 E3   ..P.....).P.......@...P.
11A318  69 00 00 8A 08 10 8F E2 00 01 A0 E1 01 00 90 E7 01 F0 80 E0 E4 00 00 00   i.......................
11A330  98 01 00 00 CC 00 00 00 98 01 00 00 10 01 00 00 98 01 00 00 28 01 00 00   ....................(...
11A348  98 01 00 00 98 01 00 00 98 01 00 00 98 01 00 00 98 01 00 00 98 01 00 00   ........................
11A360  B4 00 00 00 98 01 00 00 58 01 00 00 98 01 00 00 74 00 00 00 F8 00 00 00   ........X.......t.......
11A378  98 01 00 00 10 01 00 00 33 00 50 E3 0B 00 00 CA 2A 00 50 E3 33 00 00 0A   ........3.P.....*.P.3...
11A390  2B 00 50 E3 3E 00 00 0A 2E 00 50 E3 48 00 00 1A 08 50 85 E2 27 00 95 E8   +.P.>.....P.H....P..'...
11A3A8  14 00 80 E2 32 20 42 E2 27 00 86 E8 F0 80 BD E8 34 00 50 E3 40 00 00 1A   ....2 B.'.......4.P.@...
11A3C0  D8 00 C5 E1 00 20 A0 E3 14 50 95 E5 00 20 86 E5 04 10 86 E5 08 00 86 E5   ..... ...P... ..........
11A3D8  0C 50 86 E5 F0 80 BD E8 08 50 85 E2 27 00 95 E8 14 00 80 E2 23 20 42 E2   .P.......P..'.......# B.
11A3F0  27 00 86 E8 F0 80 BD E8 D8 00 C5 E1 28 20 A0 E3 14 50 95 E5 50 00 80 E2   '...........( ...P..P...
11A408  27 00 86 E8 F0 80 BD E8 08 50 85 E2 27 00 95 E8 19 20 42 E2 27 00 86 E8   '........P..'.... B.'...
11A420  F0 80 BD E8 D8 00 C5 E1 1E 20 A0 E3 14 50 95 E5 32
11A438  F0 80 BD E8 D8 00 C5 E1 E6 20 A0 E3 14 50 95 E5 30
11A450  F0 80 BD E8 D8 00 C5 E1 55 2F A0 E3 F8 FF FF EA
11A468  08 50 95 E5 50 00 40 E2 50 50 45 E2 00 50 86 E5
11A480  F0 80 BD E8 08 50 85 E2 27 00 95 E8 27 00 86 E8
11A498  31 00 40 E3 00 00 9F E7 00 50 95 E5 00 00 90 E5 70 50 95 E5 00 10 60 E2   1.@......P......pP....`.
11A4B0  00 20 65 E2 80 00 A0 E1 85 50 A0 E1 06 00 86 E8 C3 FF FF EA 1C 00 07 E3   . e......P..............
11A4C8  31 00 40 E3 00 00 9F E7 D8 20 C5 E1 14 10 95 E5 00 00 90 E5 3C 20 82 E2   1.@...... ..........< ..
11A4E0  0C 00 86 E8 08 00 86 E5 0C 10 86 E5 F0 80 BD E8 B0 40 2D E9 08 70 8D E2   ..................@-..p..
11A4F8  01 40 A0 E1 00 50 A0 E1 63 C8 FD EB 00 10 A0 E3 00 00 50 E3 0F 00 00 1A   .@...P..c........P.....
11A510  30 00 55 E3 07 00 00 1A 01 00 74 E3 05 00 00 0A FC 1A 08 E3 84 51 84 E0   0.U.......t..........Q..
```

00 00 50 E3

Type	Value
8 bit signed	
8 bit unsi...	
16 bit signed	
16 bit uns...	
32 bit uns...	

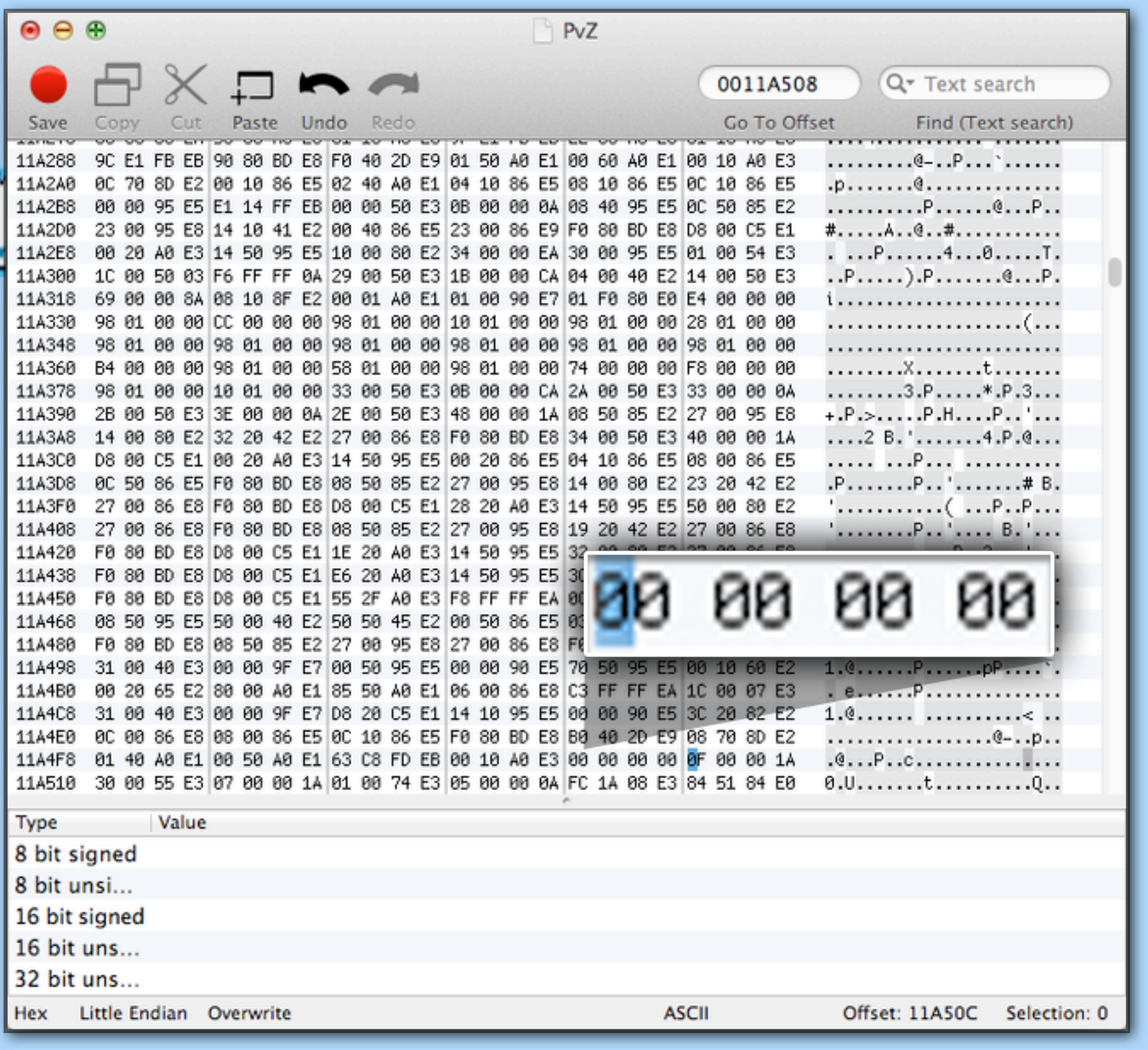
Hex Little Endian Overwrite ASCII Offset: 11A508 Selection: 0

Decrypted iOS apps can be opened in “IDA Pro” - be sure to set the “Processor type” to “ARM” though!

Analysis will run, displaying function names on the left, allowing you to view their actions

Un-wanted commands can be found, their offsets noted (0011A508), the application file opened in a hex editor

GAME HACKING



```
11A288  9C E1 FB EB 90 80 BD E8 F0 40 2D E9 01 50 A0 E1 00 60 A0 E1 00 10 A0 E3   .........@-..P...`......
11A2A0  0C 70 8D E2 00 10 86 E5 02 40 A0 E1 04 10 86 E5 08 10 86 E5 0C 10 86 E5   .p.......@..............
11A2B8  00 00 95 E5 E1 14 FF EB 00 00 50 E3 0B 00 00 0A 08 40 95 E5 0C 50 85 E2   ..........P.......@...P..
11A2D0  23 00 95 E8 14 10 41 E2 00 40 86 E5 23 00 86 E9 F0 80 BD E8 D8 00 C5 E1   #.....A..@..#...........
11A2E8  00 20 A0 E3 14 50 95 E5 10 00 80 E2 34 00 00 EA 30 00 95 E5 01 00 54 E3   . ...P......4...0.....T.
11A300  1C 00 50 03 F6 FF FF 0A 29 00 50 E3 1B 00 00 CA 04 00 40 E2 14 00 50 E3   ..P.....).P.......@...P.
11A318  69 00 00 8A 08 10 8F E2 00 01 A0 E1 01 00 90 E7 01 F0 80 E0 E4 00 00 00   i.......................
11A330  98 01 00 00 CC 00 00 00 98 01 00 00 10 01 00 00 98 01 00 00 28 01 00 00   ....................(...
11A348  98 01 00 00 98 01 00 00 98 01 00 00 98 01 00 00 98 01 00 00 98 01 00 00   ........................
11A360  B4 00 00 00 98 01 00 00 58 01 00 00 98 01 00 00 74 00 00 00 F8 00 00 00   ........X.......t.......
11A378  98 01 00 00 10 01 00 00 33 00 50 E3 0B 00 00 CA 2A 00 50 E3 33 00 00 0A   ........3.P.....*.P.3...
11A390  2B 00 50 E3 3E 00 00 0A 2E 00 50 E3 48 00 00 1A 08 50 85 E2 27 00 95 E8   +.P.>.....P.H....P..'...
11A3A8  14 00 80 E2 32 20 42 E2 27 00 86 E8 F0 80 BD E8 34 00 50 E3 40 00 00 1A   ....2 B.'.......4.P.@...
11A3C0  D8 00 C5 E1 00 20 A0 E3 14 50 95 E5 00 20 86 E5 04 10 86 E5 08 00 86 E5   ..... ...P... ..........
11A3D8  0C 50 86 E5 F0 80 BD E8 08 50 85 E2 27 00 95 E8 14 00 80 E2 23 20 42 E2   .P.......P..'.......# B.
11A3F0  27 00 86 E8 F0 80 BD E8 D8 00 C5 E1 28 20 A0 E3 14 50 95 E5 50 00 80 E2   '...........( ...P..P...
11A408  27 00 86 E8 F0 80 BD E8 08 50 85 E2 27 00 95 E8 19 20 42 E2 27 00 86 E8   '........P..'.... B.'...
11A420  F0 80 BD E8 D8 00 C5 E1 1E 20 A0 E3 14 50 95 E5 32
11A438  F0 80 BD E8 D8 00 C5 E1 E6 20 A0 E3 14 50 95 E5 30
11A450  F0 80 BD E8 D8 00 C5 E1 55 2F A0 E3 F8 FF FF EA 00
11A468  08 50 95 E5 50 00 40 E2 50 50 45 E2 00 50 86 E5 03
11A480  F0 80 BD E8 08 50 85 E2 27 00 95 E8 27 00 86 E8 F0
11A498  31 00 40 E3 00 00 9F E7 00 50 95 E5 00 00 90 E5 70 50 95 E5 00 10 60 E2   1.@.......P......pP....`.
11A4B0  00 20 65 E2 80 00 A0 E1 85 50 A0 E1 06 00 86 E8 C3 FF FF EA 1C 00 07 E3   . e.......P.............
11A4C8  31 00 40 E3 00 00 9F E7 D8 20 C5 E1 14 10 95 E5 00 00 90 E5 3C 20 82 E2   1.@...... ..........< ..
11A4E0  0C 00 86 E8 08 00 86 E5 0C 10 86 E5 F0 80 BD E8 B0 40 2D E9 08 70 8D E2   ..................@-..p..
11A4F8  01 40 A0 E1 00 50 A0 E1 63 C8 FD EB 00 10 A0 E3 00 00 00 00 0F 00 00 1A   .@...P..c...............
11A510  30 00 55 E3 07 00 00 1A 01 00 74 E3 05 00 00 0A FC 1A 08 E3 84 51 84 E0   0.U.......t..........Q..
```

```
00 00 00 00
```

Type	Value
8 bit signed	
8 bit unsi...	
16 bit signed	
16 bit uns...	
32 bit uns...	

Hex   Little Endian   Overwrite   ASCII   Offset: 11A50C   Selection: 0

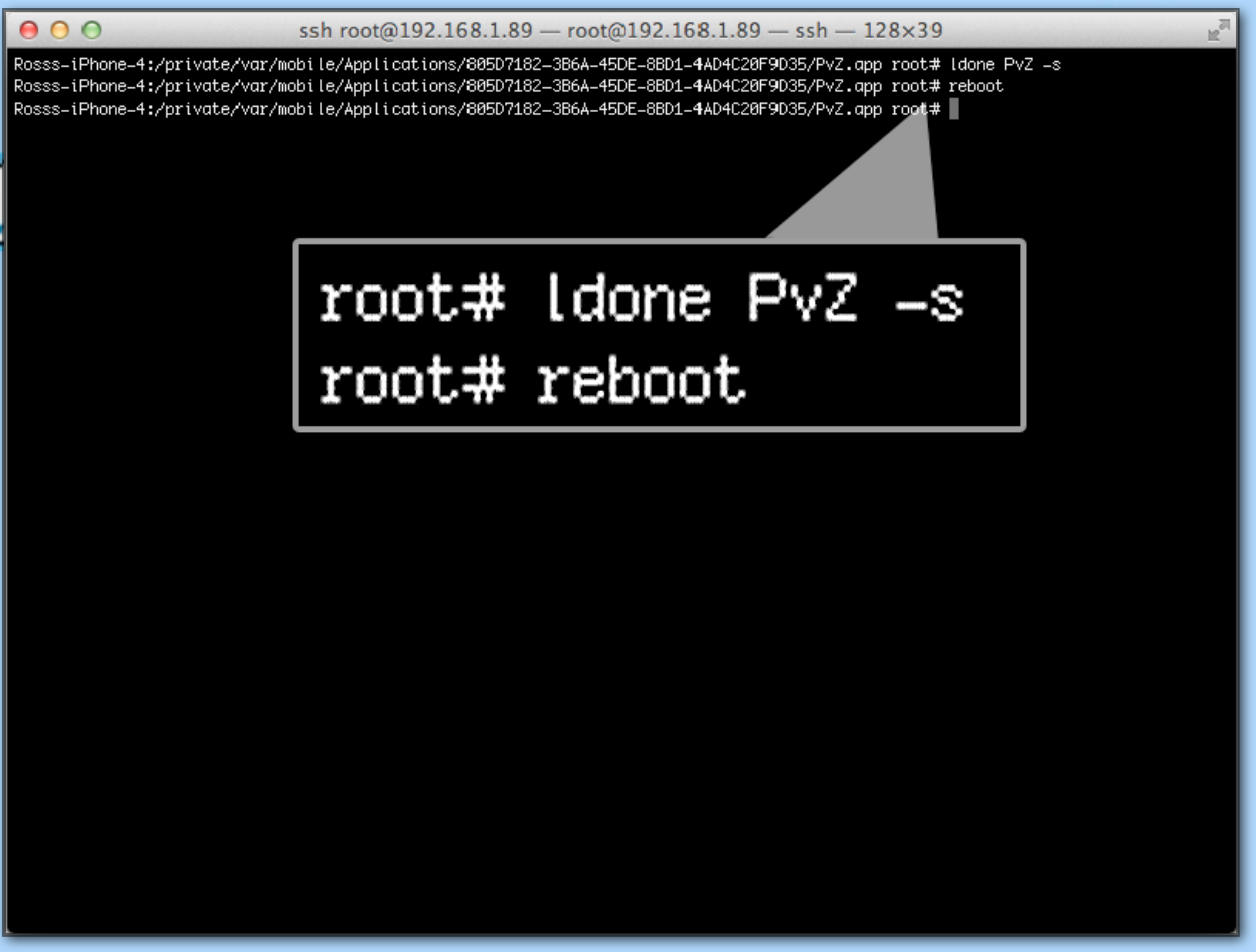
Decrypted iOS apps can be opened in “IDA Pro” - be sure to set the “Processor type” to “ARM” though!

Analysis will run, displaying function names on the left, allowing you to view their actions

Un-wanted commands can be found, their offsets noted (0011A508), the application file opened in a hex editor, and them edited out

(00’s work as NOPs in ARM)

GAME HACKING



ssh root@192.168.1.89 — root@192.168.1.89 — ssh — 128×39

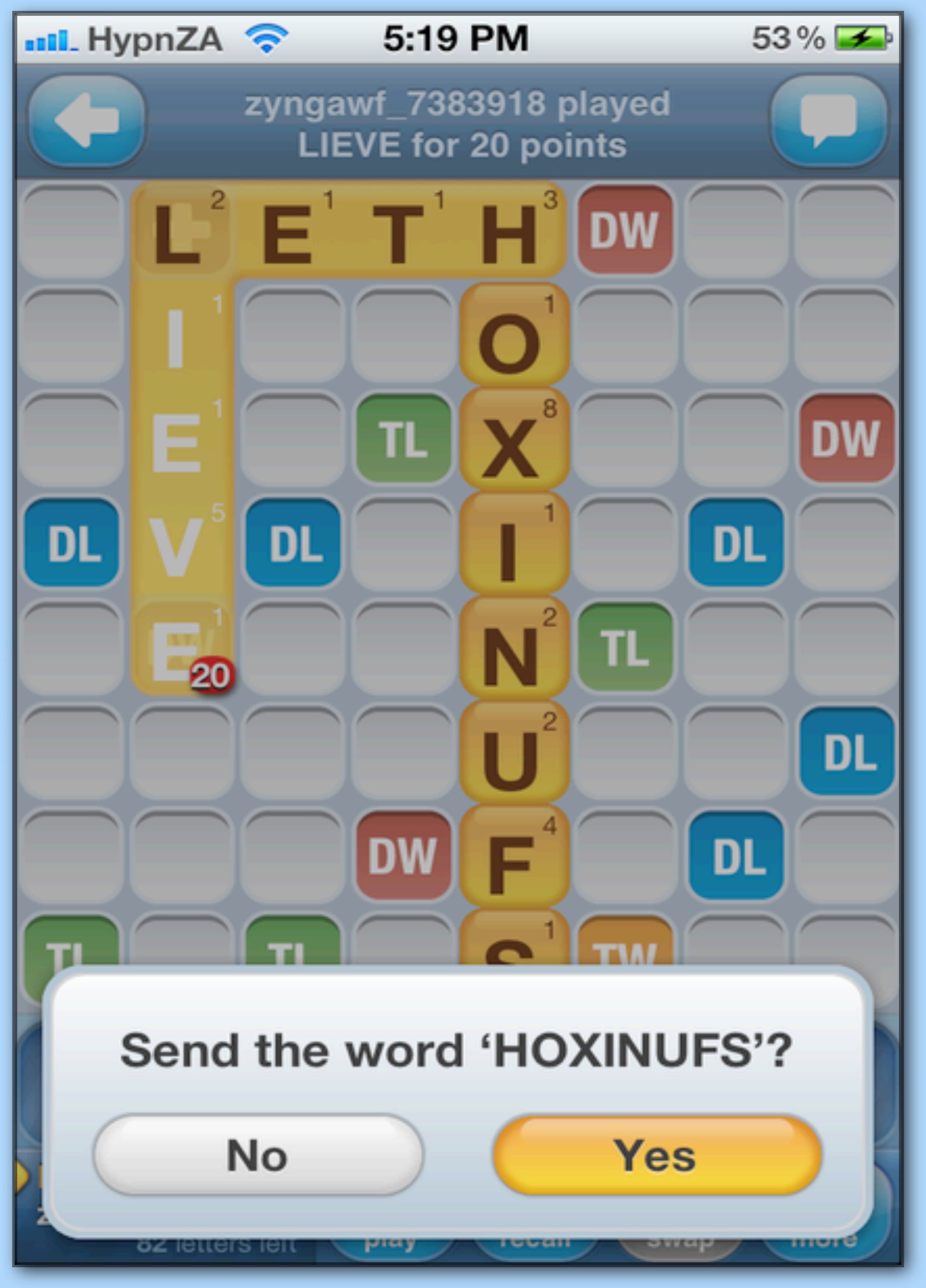
```
Rosss-iPhone-4:/private/var/mobile/Applications/805D7182-3B6A-45DE-8BD1-4AD4C20F9D35/PvZ.app root# ldone PvZ -s
Rosss-iPhone-4:/private/var/mobile/Applications/805D7182-3B6A-45DE-8BD1-4AD4C20F9D35/PvZ.app root# reboot
Rosss-iPhone-4:/private/var/mobile/Applications/805D7182-3B6A-45DE-8BD1-4AD4C20F9D35/PvZ.app root#
```

```
root# ldone PvZ -s
root# reboot
```

NOTE: after modifying an iOS application (and re-uploading it to your device), you will need to “sign” it with “ldone” (from Cydia)

Your device will probably need to be restarted before the app will run

GAME HACKING



zyngawf_7383918 played LIEVE for 20 points

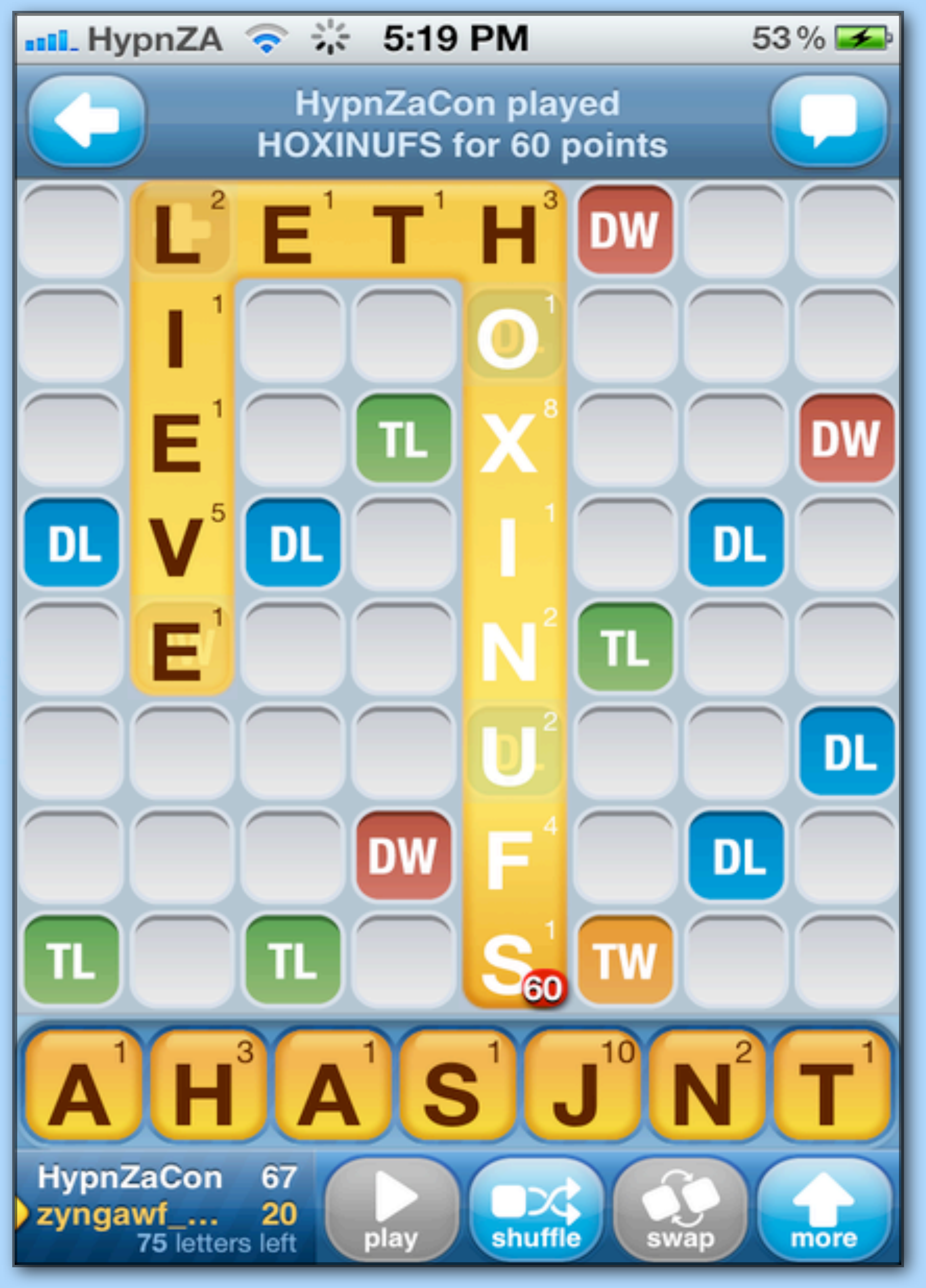
Send the word ‘HOXINUFS’?

NOTE: after modifying an iOS application (and re-uploading it to your device), you will need to “sign” it with “ldone” (from Cydia)

Your device will probably need to be restarted before the app will run

The game WordsWithFriends has a “isValidMove” method...

GAME HACKING



HypnZaCon played HOXINUFS for 60 points

NOTE: after modifying an iOS application (and re-uploading it to your device), you will need to “sign” it with “ldone” (from Cydia)

Your device will probably need to be restarted before the app will run

The game WordsWithFriends has a “isValidMove” method...

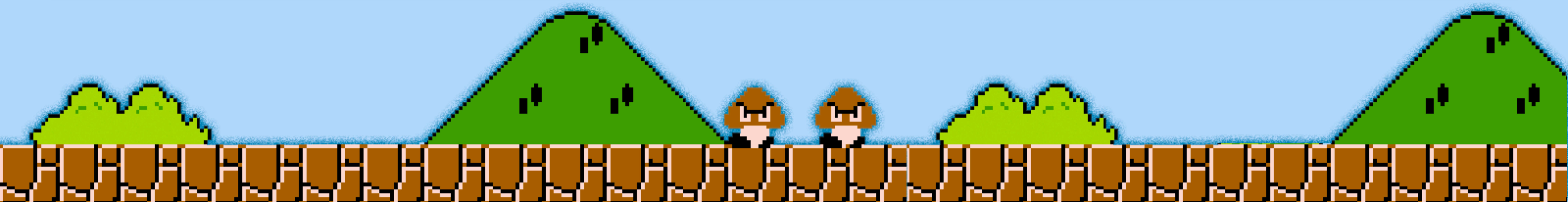
... which could be set to always return true - the server, and other clients, don’t seem to care!

Recommended Reading:

1. “Exploiting Online Games: Cheating Massively Distributed Systems” - Greg Hoglund & Gary McGraw

2. “Hacking and Securing iOS Applications” - Jonathan Zdziarski

3. Forums:
   http://www.blizzhackers.cc & http://www.mpgh.net/forum/



Real world concerns?

1. Bypass string terminators in saved games to buffer overflow and root devices? (eg: PSP - http://pspslimhacks.com/psp-6-20-save-data-exploit-released-hello-world-6-20/)
2. Send malicious (code execution?) instructions to multiplayer clients (eg: Starcraft forced map download hack)
3. Send XSS or SQL injection to “high score” severs not checking or filtering input

Thanks!

Questions?