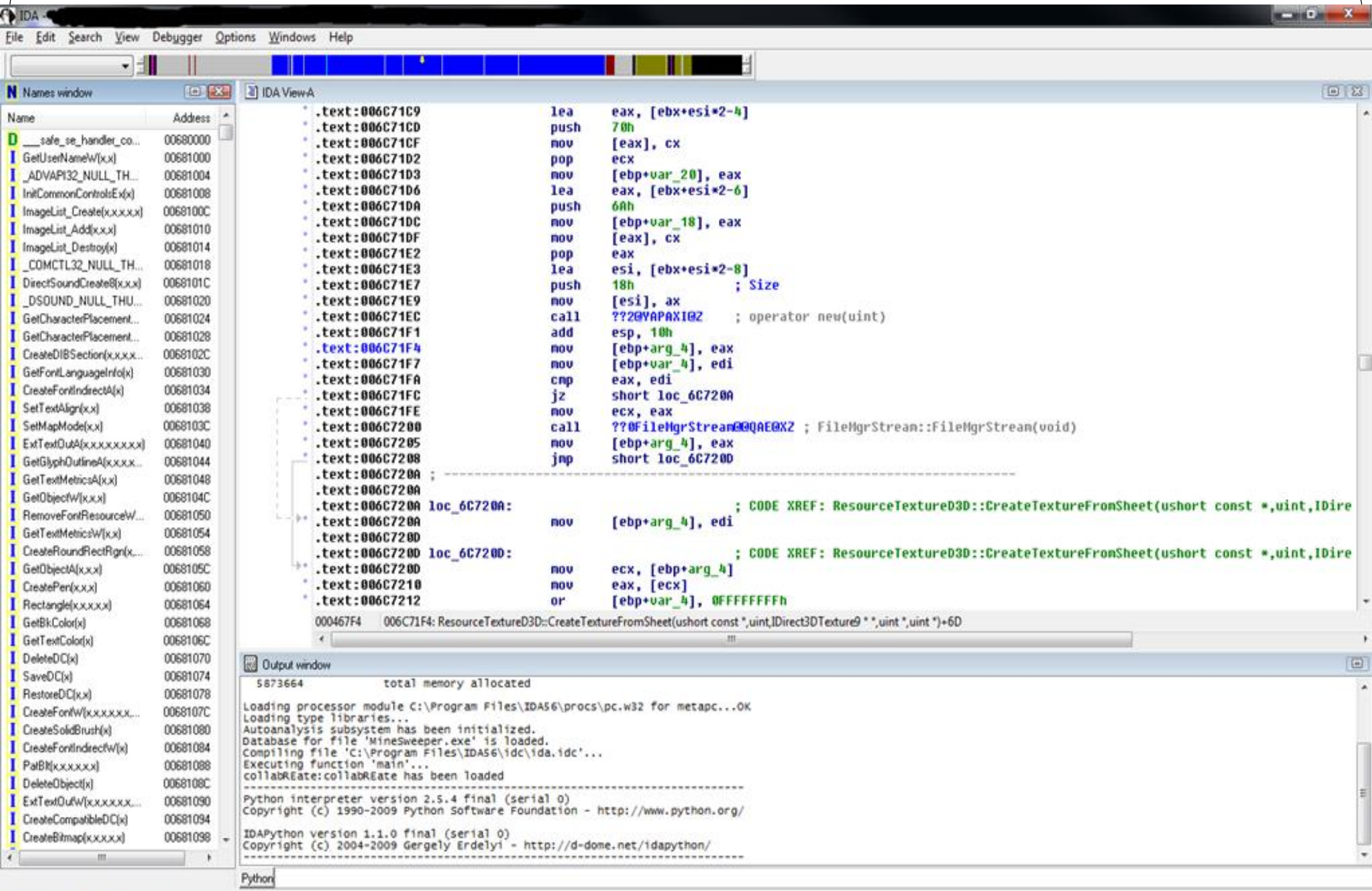
Looking Into the Eye of the Bits

By Assaf Nativ

Memory Analysis SyScan'11

Who am I?


IDA -
File Edit Search View Debugger Options Windows Help
Names window
Name
Address
___safe_se_handler_co... 00680000
GetUserNameW(x,x) 00681000
_ADVAPI32_NULL_TH... 00681004
InitCommonControlsEx(x) 00681008
ImageList_Create(x,x,x,x,x) 0068100C
ImageList_Add(x,x,x) 00681010
ImageList_Destroy(x) 00681014
_COMCTL32_NULL_TH... 00681018
DirectSoundCreate8(x,x,x) 0068101C
_DSOUND_NULL_THU... 00681020
GetCharacterPlacement... 00681024
GetCharacterPlacement... 00681028
CreateDIBSection(x,x,x,x... 0068102C
GetFontLanguageInfo(x) 00681030
CreateFontIndirectA(x) 00681034
SetTextAlign(x,x) 00681038
SetMapMode(x,x) 0068103C
ExtTextOutA(x,x,x,x,x,x,x,x) 00681040
GetGlyphOutlineA(x,x,x,x... 00681044
GetTextMetricsA(x,x) 00681048
GetObjectW(x,x,x) 0068104C
RemoveFontResourceW... 00681050
GetTextMetricsW(x,x) 00681054
CreateRoundRectRgn(x,... 00681058
GetObjectA(x,x,x) 0068105C
CreatePen(x,x,x) 00681060
Rectangle(x,x,x,x,x) 00681064
GetBkColor(x) 00681068
GetTextColor(x) 0068106C
DeleteDC(x) 00681070
SaveDC(x) 00681074
RestoreDC(x,x) 00681078
CreateFontW(x,x,x,x,x,x,... 0068107C
CreateSolidBrush(x) 00681080
CreateFontIndirectW(x) 00681084
PatBlt(x,x,x,x,x,x) 00681088
DeleteObject(x) 00681088
ExtTextOutW(x,x,x,x,x,x,... 00681090
CreateCompatibleDC(x) 00681094
CreateBitmap(x,x,x,x,x) 00681098
IDA View-A
.text:006C71C9 lea eax, [ebx+esi*2-4]
.text:006C71CD push 70h
.text:006C71CF mov [eax], cx
.text:006C71D2 pop ecx
.text:006C71D3 mov [ebp+var_20], eax
.text:006C71D6 lea eax, [ebx+esi*2-6]
.text:006C71DA push 6Ah
.text:006C71DC mov [ebp+var_18], eax
.text:006C71DF mov [eax], cx
.text:006C71E2 pop eax
.text:006C71E3 lea esi, [ebx+esi*2-8]
.text:006C71E7 push 18h ; Size
.text:006C71E9 mov [esi], ax
.text:006C71EC call ??2@YAPAXI@Z ; operator new(uint)
.text:006C71F1 add esp, 10h
.text:006C71F4 mov [ebp+arg_4], eax
.text:006C71F7 mov [ebp+var_4], edi
.text:006C71FA cmp eax, edi
.text:006C71FC jz short loc_6C720A
.text:006C71FE mov ecx, eax
.text:006C7200 call ??0FileMgrStream@@QAE@XZ ; FileMgrStream::FileMgrStream(void)
.text:006C7205 mov [ebp+arg_4], eax
.text:006C7208 jmp short loc_6C720D
.text:006C720A ; ---
.text:006C720A
.text:006C720A loc_6C720A: ; CODE XREF: ResourceTextureD3D::CreateTextureFromSheet(ushort const *,uint,IDire
.text:006C720A mov [ebp+arg_4], edi
.text:006C720D
.text:006C720D loc_6C720D: ; CODE XREF: ResourceTextureD3D::CreateTextureFromSheet(ushort const *,uint,IDire
.text:006C720D mov ecx, [ebp+arg_4]
.text:006C7210 mov eax, [ecx]
.text:006C7212 or [ebp+var_4], 0FFFFFFFFh
000467F4 006C71F4: ResourceTextureD3D::CreateTextureFromSheet(ushort const *,uint,IDirect3DTexture9 * *,uint *,uint *)+6D
Output window
5873664 total memory allocated
Loading processor module C:\Program Files\IDA56\procs\pc.w32 for metapc...OK
Loading type libraries...
Autoanalysis subsystem has been initialized.
Database for file 'MineSweeper.exe' is loaded.
Compiling file 'C:\Program Files\IDA56\idc\ida.idc'...
Executing function 'main'...
collabREate:collabREate has been loaded
Python interpreter version 2.5.4 final (serial 0)
Copyright (c) 1990-2009 Python Software Foundation - http://www.python.org/
IDAPython version 1.1.0 final (serial 0)
Copyright (c) 2004-2009 Gergely Erdelyi - http://d-dome.net/idapython/
Python
AU: idle
Down
Disk: 32GB


ECK-02.PCB
20051219
Ver2.0
AT89C4051-24SI
BLUE
YELLOW
RED
Normal
DECT


MT BOX
00C1DCD447
www.mt-box.org
SAMSUNG
SAMSUNG
NOKIA
NOKIA
NOKIA
NOKIA


sentrigo™


McAfee®
Proven Security™


intel
inside
®

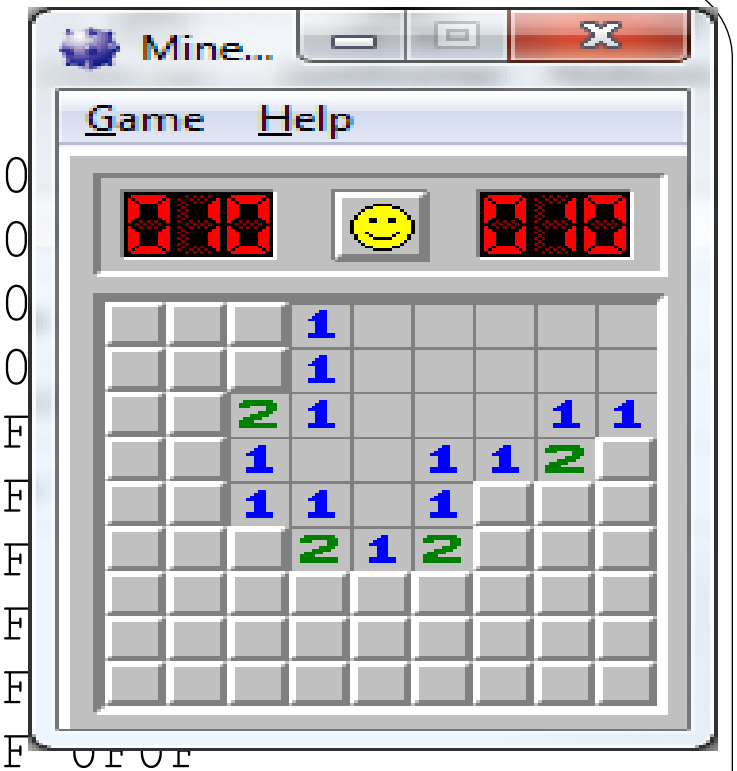
Wandering in memory land

```
000  0000 0000 0000 0000 - 0000 0000 0000 0000
010  0000 0000 0000 0000 - 0000 0000 0000 0000
020  0000 0000 0000 0000 - 0000 0000 0000 0000
030  0A00 0000 0900 0000 - 0900 0000 0000 0000
040  1010 1010 1010 1010 - 1010 100F 0F0F 0F0F
050  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
060  100F 0F0F 4140 4040 - 4040 100F 0F0F 0F0F
070  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
080  100F 0F8F 4140 4040 - 4040 100F 0F0F 0F0F
090  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
0A0  100F 8F42 4140 4040 - 4141 100F 0F0F 0F0F
0B0  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
0C0  108F 0F41 4040 4141 - 428F 100F 0F0F 0F0F
0D0  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
0E0  100F 0F41 4140 418F - 0F0F 100F 0F0F 0F0F
0F0  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
100  100F 0F8F 4241 420F - 0F0F 100F 0F0F 0F0F
110  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
120  100F 0F0F 0F8F 0F0F - 0F0F 100F 0F0F 0F0F
130  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
140  100F 0F0F 0F0F 8F0F - 0F0F 100F 0F0F 0F0F
```

A hint...

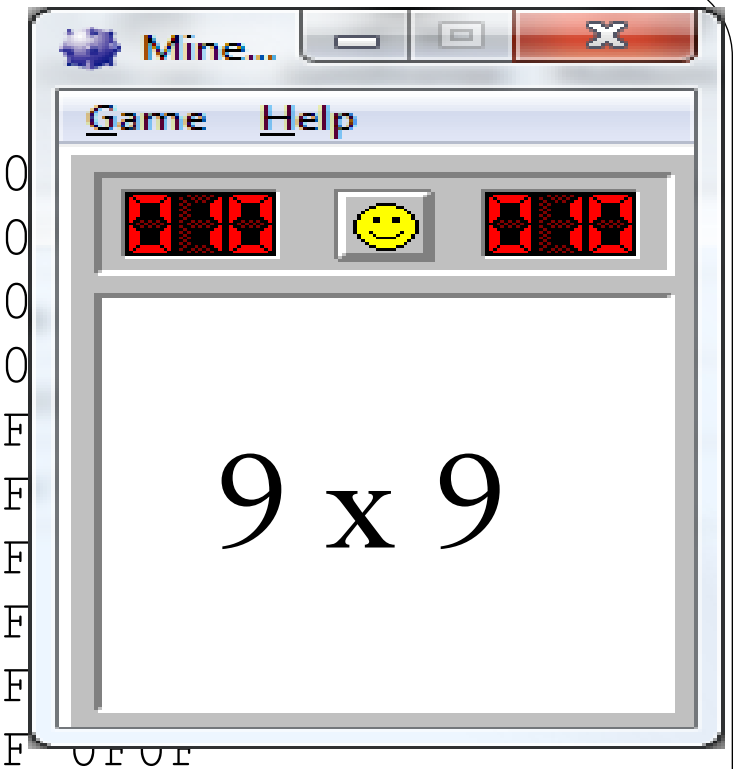
Memory land

```
000  0000 0000 0000 0000 - 0000 0000 0000
010  0000 0000 0000 0000 - 0000 0000 0000
020  0000 0000 0000 0000 - 0000 0000 0000
030  0A00 0000 0900 0000 - 0900 0000 0000
040  1010 1010 1010 1010 - 1010 100F 0F0F
050  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F
060  100F 0F0F 4140 4040 - 4040 100F 0F0F
070  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F
080  100F 0F8F 4140 4040 - 4040 100F 0F0F
090  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F
0A0  100F 8F42 4140 4040 - 4141 100F 0F0F 0F0F
0B0  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
0C0  108F 0F41 4040 4141 - 428F 100F 0F0F 0F0F
0D0  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
0E0  100F 0F41 4140 418F - 0F0F 100F 0F0F 0F0F
0F0  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
100  100F 0F8F 4241 420F - 0F0F 100F 0F0F 0F0F
110  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
120  100F 0F0F 0F8F 0F0F - 0F0F 100F 0F0F 0F0F
130  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
140  100F 0F0F 0F0F 8F0F - 0F0F 100F 0F0F 0F0F
```



Memory land

```
000  0000 0000 0000 0000 - 0000 0000 0000
010  0000 0000 0000 0000 - 0000 0000 0000
020  0000 0000 0000 0000 - 0000 0000 0000
030  0A00 0000 0900 0000 - 0900 0000 0000
040  1010 1010 1010 1010 - 1010 100F 0F0F
050  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F
060  100F 0F0F 4140 4040 - 4040 100F 0F0F
070  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F
080  100F 0F8F 4140 4040 - 4040 100F 0F0F
090  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F
0A0  100F 8F42 4140 4040 - 4141 100F 0F0F 0F0F
0B0  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
0C0  108F 0F41 4040 4141 - 428F 100F 0F0F 0F0F
0D0  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
0E0  100F 0F41 4140 418F - 0F0F 100F 0F0F 0F0F
0F0  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
100  100F 0F8F 4241 420F - 0F0F 100F 0F0F 0F0F
110  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
120  100F 0F0F 0F8F 0F0F - 0F0F 100F 0F0F 0F0F
130  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
140  100F 0F0F 0F0F 8F0F - 0F0F 100F 0F0F 0F0F
```

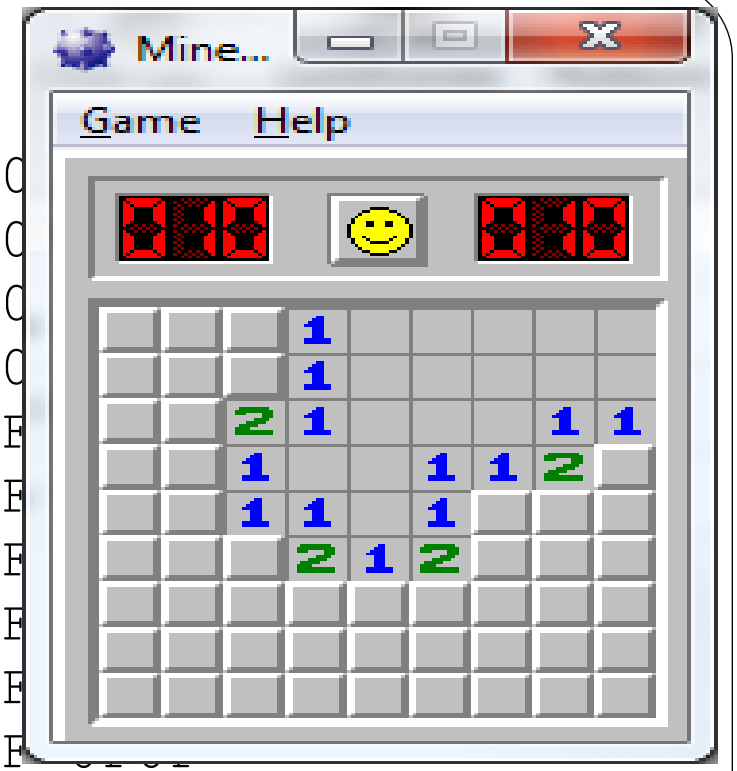


Memory land

```
000  0000 0000 0000 0000 - 0000 0000 0000
010  0000 0000 0000 0000 - 0000 0000 0000
020  0000 0000 0000 0000 - 0000 0000 0000
030  0A00 0000 0900 0000 - 0900 0000 0000
040  1010 1010 1010 1010 - 1010 100F 0F0F
050  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F
060  100F 0F0F 4140 4040 - 4040 100F 0F0F
070  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F
080  100F 0F8F 4140 4040 - 4040 100F 0F0F
090  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
0A0  100F 8F42 4140 4040 - 4141 100F 0F0F 0F0F
0B0  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
0C0  108F 0F41 4040 4141 - 428F 100F 0F0F 0F0F
0D0  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
0E0  100F 0F41 4140 418F - 0F0F 100F 0F0F 0F0F
0F0  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
100  100F 0F8F 4241 420F - 0F0F 100F 0F0F 0F0F
110  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
120  100F 0F0F 0F8F 0F0F - 0F0F 100F 0F0F 0F0F
130  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
140  100F 0F0F 0F0F 8F0F - 0F0F 100F 0F0F 0F0F
```

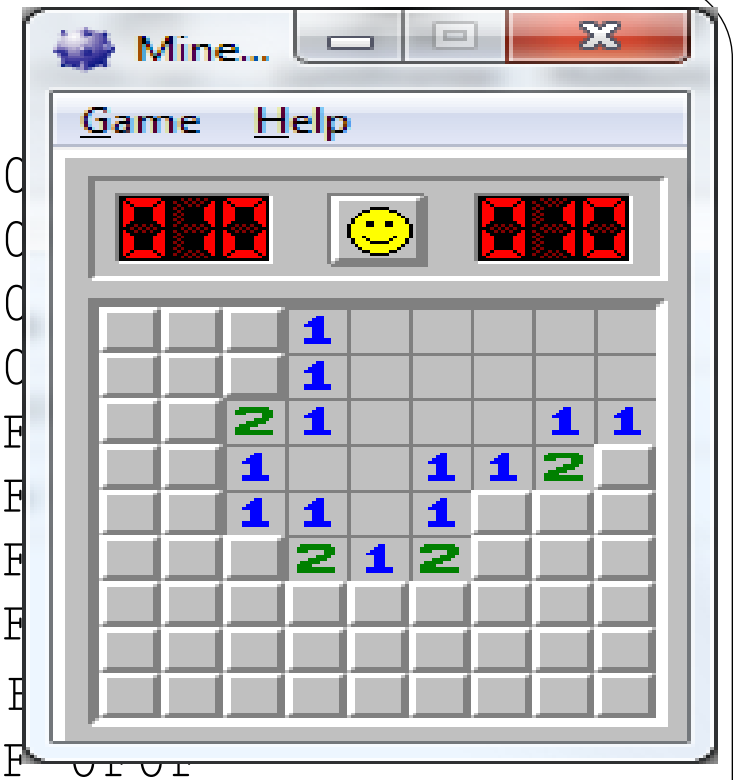
Memory land

```
000  0000 0000 0000 0000 - 0000 0000 0000
010  0000 0000 0000 0000 - 0000 0000 0000
020  0000 0000 0000 0000 - 0000 0000 0000
030  0A00 0000 0900 0000 - 0900 0000 0000
040  1010 1010 1010 1010 - 1010 100F 0F0F
050  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F
060  100F 0F0F 4140 4040 - 4040 100F 0F0F
070  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F
080  100F 0F8F 4140 4040 - 4040 100F 0F0F
090  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F
0A0  100F 8F42 4140 4040 - 4141 100F 0F0F 0F0F
0B0  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
0C0  108F 0F41 4040 4141 - 428F 100F 0F0F 0F0F
0D0  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
0E0  100F 0F41 4140 418F - 0F0F 100F 0F0F 0F0F
0F0  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
100  100F 0F8F 4241 420F - 0F0F 100F 0F0F 0F0F
110  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
120  100F 0F0F 0F8F 0F0F - 0F0F 100F 0F0F 0F0F
130  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
140  100F 0F0F 0F0F 8F0F - 0F0F 100F 0F0F 0F0F
```



Memory land

```
000  0000 0000 0000 0000 - 0000 0000 0000
010  0000 0000 0000 0000 - 0000 0000 0000
020  0000 0000 0000 0000 - 0000 0000 0000
030  0A00 0000 0900 0000 - 0900 0000 0000
040  1010 1010 1010 1010 - 1010 100F 0F0F
050  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F
060  100F 0F0F 4140 4040 - 4040 100F 0F0F
070  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F
080  100F 0F8F 4140 4040 - 4040 100F 0F0F
090  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F
0A0  100F 8F42 4140 4040 - 4141 100F 0F0F 0F0F
0B0  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
0C0  108F 0F41 4040 4141 - 428F 100F 0F0F 0F0F
0D0  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
0E0  100F 0F41 4140 418F - 0F0F 100F 0F0F 0F0F
0F0  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
100  100F 0F8F 4241 420F - 0F0F 100F 0F0F 0F0F
110  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
120  100F 0F0F 0F8F 0F0F - 0F0F 100F 0F0F 0F0F
130  0F0F 0F0F 0F0F 0F0F - 0F0F 0F0F 0F0F 0F0F
140  100F 0F0F 0F0F 8F0F - 0F0F 100F 0F0F 0F0F
```



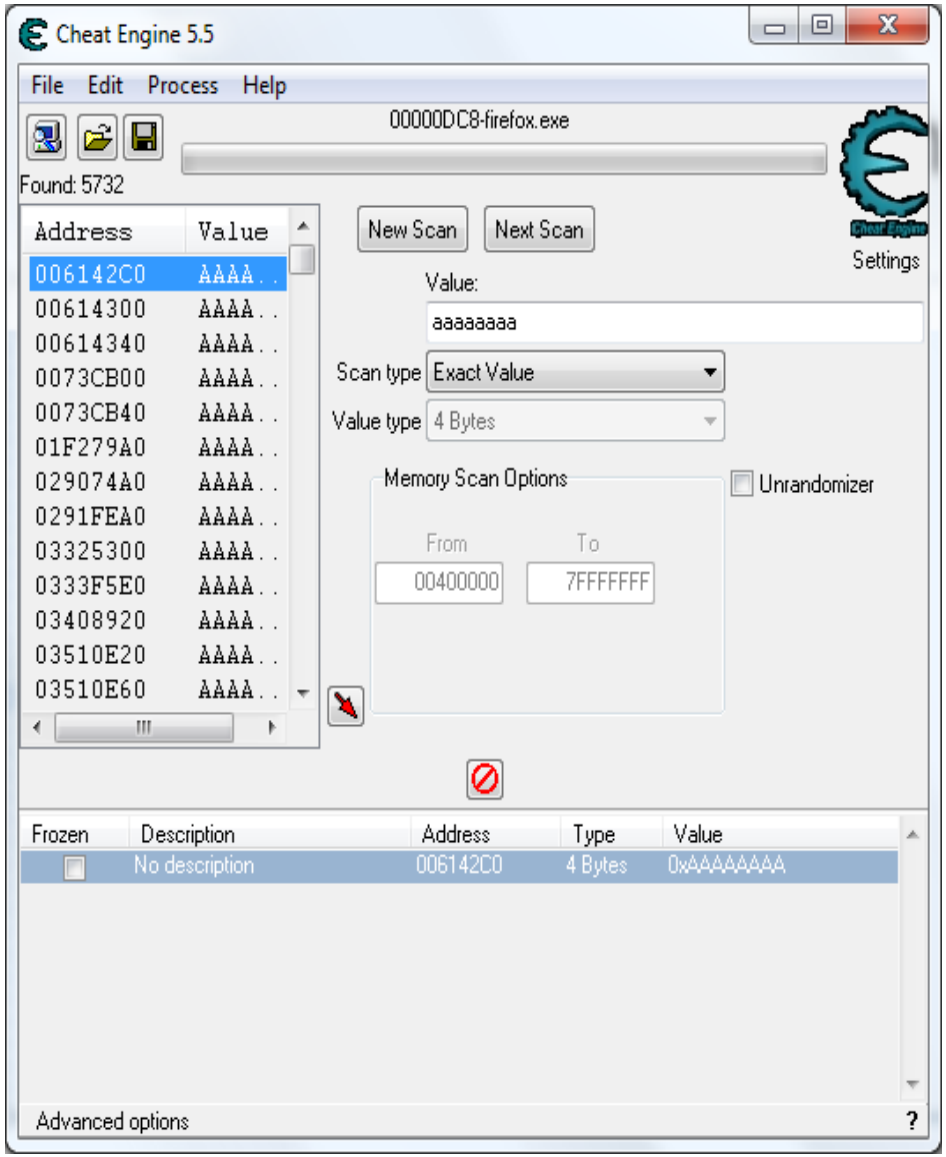
Definition of Memory Software Analysis

Recovering internal implementation by reading the memory of a running process.

Without disassembling machine code.

Memory analysis in practice

- Games cheating



Memory analysis in practice

- Games cheating
- Analysis of crash dumps

Memory analysis in practice

- Games cheating
- Analysis of crash dumps
- SRE
  - Examine memory
  - Not everyone can do SRE, while everyone knows C++

Memory analysis in practice

- Games cheating
- Analysis of crash dumps
- SRE
  - Examine memory
  - Not everyone can do SRE, while everyone knows C++
  - Avoiding conflicts with the law

Memory analysis in practice

- Games cheating
- Analysis of crash dumps
- SRE
  - Examine memory
  - Not everyone can do SRE, while everyone knows C++
  - Avoiding conflicts with the law
- Exploit developing
- Debugging
- Security & Monitoring

We use it to figure out internal implementations of Data Bases

MS SQL Server - User Info

```
          0         4         8         C
 0        1         0         0  50F3C38  ............8<..
10        1   5993988         4  59939F0  .....9.......9..
20        3         0         0  5993998  ............9..
30       14   5993A18        1A         0  .....:..........
40        0         0         0         0  ................
50        0   59939D0        14  59939B8  .....9.......9..
60        C  11D9D4AA  11D9D4AA         0  ................
70   170101    180070   50F2001  50F3FF0  ....p.... ...?..
```

5993988: sa (unicode)

MS SQL Server - User Info

```
          0          4          8          C
 0        1          0          0   50F3C38   ............8<..
10        1    5993988          4   59939F0   .....9.......9..
20        3          0          0   5993998   ............9..
30       14    5993A18         1A         0   .....:..........
40        0          0          0         0   ................
50        0    59939D0         14   59939B8   .....9.......9..
60        C   11D9D4AA   11D9D4AA         0   ................
70   170101     180070    50F2001   50F3FF0   ....p.... ...?..
```

5993988: sa (unicode)
59939B8: master (unicode)

MS SQL Server - User Info

```
          0          4          8          c
 0        1          0          0   50F3C38   ............8<..
10        1    5993988          4   59939F0   .....9.......9..
20        3          0          0   5993998   ............9..
30       14    5993A18         1A         0   .....:..........
40        0          0          0         0   ................
50        0    59939D0         14   59939B8   .....9.......9..
60        C   11D9D4AA   11D9D4AA         0   ................
70   170101     180070    50F2001   50F3FF0   ....p.... ...?..
```

5993988: sa (unicode)
59939B8: master (unicode)
5993998: myPa55word (unicode)

MS Response

From our investigation it appears that to locate any of the authentication information administrator level privileges are required. This tends to fall under Rule 6 of the 10 Immutable Laws of Security (http://www.microsoft.com/technet/archive/community/columns/security/essays/10imlaws.mspx) where basically you have to trust your administrators.

The Web Response

SC MAGAZINE
FOR IT SECURITY PROFESSIONALS

Microsoft disputes password-stealing SQL Server bug

Angela Moscaritolo September 02, 2009

PRINT EMAIL REPRINT PERMISSIONS FONT SIZE: A | A | A

For more than a year, Microsoft has been sitting on a purported SQL Server vulnerability that could enable a malicious insider to obtain users' passwords, claims database security vendor Sentrigo.

The software giant, however, said that the issue is not a security flaw.

The potential bug, which Sentrigo notified Microsoft about last September, involves SQL Server keeping passwords unencrypted in its database memory, Slavik Markovich, CTO at Sentrigo, told SCMagazineUS.com on Tuesday. The issue affects SQL Server 2000, 2005 and 2008, running on Windows operating systems.

RELATED ARTICL
- Mass SQL inj scaling up
- New mass SQ infects 56,000
- Microsoft warn vulnerability
- Thousands of SQL attack
- Microsoft reco to address SQ
- Microsoft goe massive SQL
- Researchers of SQL attacks

Passwordizer

- Pass-what?
- How does it work
- Current status

How does it work?

```
session = ...
INFO_OFFSETS = \
    [0xe0, 0x18, 0x1d4, 0x**, 0x**]  # MSSQL build #$%^
info = mint.resolveOffsetsList(session, INFO_OFFSETS)[-1]
username = mint.readDword(info + 0x28)
username_len, username = \
        ((username >> 16), username & 0xffff)
print 'User name:', mint.readString(info + username,
\                                   isUnicode=True)
password = mint.readDword(info + 0x2c)
password_len, password = \
        ((username >> 16), username & 0xffff)
print 'Password:', mint.readString(info + password,
\                                   isUnicode=True)
```

Let's take a trip to memory land

What are we expected to find in the memory realm?

- Pointers
- Data
- Text
- Time stamp
- Complete Random
- Code

It depends on how we look at it.

```
00  6C29 760A 6C29 760A - 0100 0000 0000 0000    l)v.l)v.........
10  0100 0000 387B C603 - 387B C603 0000 0000    ....8{..8{......
20  0000 0000 0000 0000 - 4C7B C603 4C7B C603    ........L{..L{..
30  0000 0000 0000 0000 - 0000 0000 607B C603    ............`{..
40  607B C603 0000 0000 - 0000 0000 0000 0000    `{..............
50  747B C603 747B C603 - 0000 0000 0000 0000    t{..t{..........
60  0000 0000 887B C603 - 887B C603 0000 0000    .....{...{......
70  0000 0000 0000 0000 - 9C7B C603 9C7B C603    .........{...{..
80  0000 0000 0000 0000 - 0000 0000 B07B C603    ............{..
90  B07B C603 0000 0000 - 0000 0000 0000 0000    .{..............
A0  C47B C603 C47B C603 - 0000 0000 0000 0000    .{...{..........
B0  0000 0000 D87B C603 - D87B C603 0000 0000    .....{...{......
C0  0000 0000 0000 0000 - EC7B C603 EC7B C603    .........{...{..
D0  0000 0000 0000 0000 - 0000 0000 007C C603    .............|..
E0  007C C603 0000 0000 - 0000 0000 0000 0000    .|..............
F0  147C C603 147C C603 - 0000 0000 0000 0000    .|...|..........
```

Reading memory

```
 0  A76296C  A76296C        1        0  l)v.l)v.........
10        1  3C67B38  3C67B38        0  ....8{..8{......
20        0        0  3C67B4C  3C67B4C  ........L{..L{..
30        0        0        0  3C67B60  ............`{..
40  3C67B60        0        0        0  `{..............
50  3C67B74  3C67B74        0        0  t{..t{..........
60        0  3C67B88  3C67B88        0  .....{...{......
70        0        0  3C67B9C  3C67B9C  .........{...{..
80        0        0        0  3C67BB0  ............{..
90  3C67BB0        0        0        0  .{..............
a0  3C67BC4  3C67BC4        0        0  .{...{..........
b0        0  3C67BD8  3C67BD8        0  .....{...{......
c0        0        0  3C67BEC  3C67BEC  .........{...{..
d0        0        0        0  3C67C00  ............|..
e0  3C67C00        0        0        0  .|..............
f0  3C67C14  3C67C14        0        0  .|...|..........
```

Reading memory

0	A76296C	A76296C	1	0	1
14	3C67B38	3C67B38	0	0	0
28	3C67B4C	3C67B4C	0	0	0
3c	3C67B60	3C67B60	0	0	0
50	3C67B74	3C67B74	0	0	0
64	3C67B88	3C67B88	0	0	0
78	3C67B9C	3C67B9C	0	0	0
8c	3C67BB0	3C67BB0	0	0	0
a0	3C67BC4	3C67BC4	0	0	0
b4	3C67BD8	3C67BD8	0	0	0
c8	3C67BEC	3C67BEC	0	0	0
dc	3C67C00	3C67C00	0	0	0
f0	3C67C14	3C67C14	0	0	0

Reading memory

	Next	Prev	Num items	2 * Dont Know	
0	A76296C	A76296C	1	0	1
14	3C67B38	3C67B38	0	0	0
28	3C67B4C	3C67B4C	0	0	0
3c	3C67B60	3C67B60	0	0	0
50	3C67B74	3C67B74	0	0	0
64	3C67B88	3C67B88	0	0	0
78	3C67B9C	3C67B9C	0	0	0
8c	3C67BB0	3C67BB0	0	0	0
a0	3C67BC4	3C67BC4	0	0	0
b4	3C67BD8	3C67BD8	0	0	0
c8	3C67BEC	3C67BEC	0	0	0
dc	3C67C00	3C67C00	0	0	0
f0	3C67C14	3C67C14	0	0	0

Data types (Session data)

```
  0    8B4354        0  37EA374  37EA374  TC......t.~.t.~.
 10         1        0  59E8258        0  ........X.......
 20         0        0       33        0  ........3.......
 30         0 4FE0EEB5 4745091B 5B8DEA9A  .......O..EG...[
 40 7C6F9AD9  2E2A970         2       33  ..o|p.......3...
 50       3EA        0         0        0  ................
 60         1        0         0        1  ................
 70         0        0        E6        0  ................
 80    F01E71     9D8B F8717C2F        8  q......./|q.....
 90    F0B145     9D8B   F0B145     9D8B  E.......E.......
 a0    EC8606     9D8B         2        0  ................
 b0 F8717C2F        8        39        0  /|q.....9.......
 c0       3D5        0         0        0  ................
 d0         0        0         0        0  ................
 e0         0        0         0        0  ................
 f0        39        0         0        0  9...............
100       3D5        0         F        0  ................
110        4E        0        4E        0  N.......N.......
120        4E        0         0        0  N...............
130    11DA8F        0         0        0  ................
140         0        0 F8717C2F        8  ......../|q.....
150    5B8ED6        0         0        0  ..[.............
```

Data types: Data

```
  0    8B4354        0  37EA374  37EA374  TC.....t.~.t.~.
 10         1        0  59E8258        0  ........X.......
 20         0        0       33        0  ........3.......
 30         0 4FE0EEB5 4745091B 5B8DEA9A  .......O..EG...[
 40 7C6F9AD9  2E2A970        2       33  ..o|p.......3...
 50       3EA        0        0        0  ................
 60         1        0        0        1  ................
 70         0        0       E6        0  ................
 80    F01E71     9D8B F8717C2F        8  q......./|q.....
 90    F0B145     9D8B   F0B145     9D8B  E.......E.......
 a0    EC8606     9D8B        2        0  ................
 b0 F8717C2F        8       39        0  /|q.....9.......
 c0       3D5        0        0        0  ................
 d0         0        0        0        0  ................
 e0         0        0        0        0  ................
 f0        39        0        0        0  9...............
100       3D5        0        F        0  ................
110        4E        0       4E        0  N.......N.......
120        4E        0        0        0  N...............
130    11DA8F        0        0        0  ................
140         0        0 F8717C2F        8  ......../|q.....
150    5B8ED6        0        0        0  ..[.............
```

Data types: Pointers

```
  0    8B4354        0  37EA374  37EA374  TC.....t.~.t.~.
 10         1        0  59E8258        0  ........X.......
 20         0        0       33        0  ........3.......
 30         0 4FE0EEB5 4745091B 5B8DEA9A  .......O..EG...[
 40 7C6F9AD9  2E2A970          2       33  ..o|p.......3...
 50       3EA        0        0        0  ................
 60         1        0        0        1  ................
 70         0        0       E6        0  ................
 80    F01E71     9D8B F8717C2F        8  q......./|q.....
 90    F0B145     9D8B   F0B145     9D8B  E.......E.......
 a0    EC8606     9D8B        2        0  ................
 b0 F8717C2F        8       39        0  /|q.....9.......
 c0       3D5        0        0        0  ................
 d0         0        0        0        0  ................
 e0         0        0        0        0  ................
 f0        39        0        0        0  9...............
100       3D5        0        F        0  ................
110        4E        0       4E        0  N.......N.......
120        4E        0        0        0  N...............
130    11DA8F        0        0        0  ................
140         0        0 F8717C2F        8  ......../|q.....
150    5B8ED6        0        0        0  ..[.............
```

Where does this memory belong

- Data section
- Code section
- Stack
- Heap
- OS

Data types: Time stamp

0	8B4354	0	37EA374	37EA374	TC.....t.~.t.~.
10	1	0	59E8258	0	........X.....
20	0	0	33	0	........3.....
30	0	4FE0EEB5	4745091B	5B8DEA9A	.......O..EG...[
40	7C6F9AD9	2E2A970	2	33	..o|p.......3...
50	3EA	0	0	0	....
60	1	0	0	1	....
70	0	0	E6	0	....
80	**F01E71**	**9D8B**	F8717C2F	8	q......./|q.....
90	**F0B145**	**9D8B**	**F0B145**	**9D8B**	E.......E.....
a0	**EC8606**	**9D8B**	2	0	....
b0	F8717C2F	8	39	0	/|q.....9.....
c0	3D5	0	0	0	....
d0	0	0	0	0	....
e0	0	0	0	0	....
f0	39	0	0	0	9...............
100	3D5	0	F	0	....
110	4E	0	4E	0	N.......N.....
120	4E	0	0	0	N...............
130	11DA8F	0	0	0	....
140	0	0	F8717C2F	8	......../|q.....
150	5B8ED6	0	0	0	..[.............

Data types: Random

```
  0    8B4354          0  37EA374  37EA374  TC......t.~.t.~.
 10         1          0  59E8258        0  ........X.......
 20         0          0       33        0  ........3.......
 30         0 4FE0EEB5 4745091B 5B8DEA9A  ........O..EG...[
 40 7C6F9AD9   2E2A970          2       33  ..o|p.......3...
 50       3EA          0        0        0  ................
 60         1          0        0        1  ................
 70         0          0       E6        0  ................
 80    F01E71       9D8B F8717C2F        8  q......./|q.....
 90    F0B145       9D8B   F0B145     9D8B  E.......E.......
 a0    EC8606       9D8B        2        0  ................
 b0 F8717C2F          8       39        0  /|q.....9.......
 c0       3D5          0        0        0  ................
 d0         0          0        0        0  ................
 e0         0          0        0        0  ................
 f0        39          0        0        0  9...............
100       3D5          0        F        0  ................
110        4E          0       4E        0  N.......N.......
120        4E          0        0        0  N...............
130    11DA8F          0        0        0  ................
140         0          0 F8717C2F        8  ......../|q.....
150    5B8ED6          0        0        0  ..[.............
```

Data types: Code

```
00  6884 2478 026A 3368 - 6824 7802 6878 2478   h.$x.j3hh$x.hx$x
10  026A 01E8 85E6 B600 - 83C4 1433 C0C3 9090   .j.........3....
20  9090 908B FF55 8BEC - 81EC 0401 0000 A124   .....U.........$
30  4032 0233 C589 45FC - 833D 8CC7 6D02 0056   @2.3..E..=..m..V
40  8B75 0C74 0983 3D90 - C76D 0200 7513 32C0   .u.t..=..m..u.2.
50  5E8B 4DFC 33CD E8C9 - 14C5 FF8B E55D C210   ^.M.3........]..
60  0068 0001 0000 8D85 - FCFE FFFF 6A00 50E8   .h.........j.P.
70  4534 C5FF 8B45 1083 - C40C 3DFE 0000 0072   E4...E....=....r
80  05B8 FE00 0000 5350 - 8D8D FCFE FFFF 5651   ......SP......VQ
90  E8E8 16C5 FF8B 7514 - 83C4 0C83 FE02 766B   ......u.......vk
A0  8A5D 088A C3F6 D856 - 8D95 FCFE FFFF 52B9   .].....V......R.
B0  6840 3202 1BC0 83C0 - 2350 E8CA 68D0 0085   h@2.....#P..h...
C0  C074 4884 DB74 228B - 0D8C C76D 025B C744   .tH..t".....m.[.D
D0  B1F4 0000 0000 B001 - 5E8B 4DFC 33CD E841   ........^.M.3..A
E0  14C5 FF8B E55D C210 - 008B 1590 C76D 025B   .....].......m.[
F0  C744 B2F4 0000 0000 - B001 5E8B 4DFC 33CD   .D........^.M.3.
```

Data types: Code

```
00   6884 2478 026A 3368 - 6824 7802 6878 2478   h.$x.j3hh$x.hx$x
10   026A 01E8 85E6 B600 - 83C4 1433 C0C3 9090   .j.........3....
20   9090 908B FF55 8BEC - 81EC 0401 0000 A124   .....U.........$
30   4032 0233 C589 45FC - 833D 8CC7 6D02 0056   @2.3..E..=..m..V
40   8B75 0C74 0983 3D90 - C76D 0200 7513 32C0   .u.t..=..m..u.2.
50   5E8B 4DFC 33CD E8C9 - 14C5 FF8B E55D C210   ^.M.3........]..
60   0068 0001 0000 8D85 - FCFE FFFF 6A00 50E8   .h.........j.P.
70   4534 C5FF 8B45 1083 - C40C 3DFE 0000 0072   E4...E....=....r
80   05B8 FE00 0000 5350 - 8D8D FCFE FFFF 5651   ......SP......VQ
90   E8E8 16C5 FF8B 7514 - 83C4 0C83 FE02 766B   ......u.......vk
A0   8A5D 088A C3F6 D856 - 8D95 FCFE FFFF 52B9   .].....V......R.
B0   6840 3202 1BC0 83C0 - 2350 E8CA 68D0 0085   h@2.....#P..h...
C0   C074 4884 DB74 228B - 0D8C C76D 025B C744   .tH..t".....m.[.D
D0   B1F4 0000 0000 B001 - 5E8B 4DFC 33CD E841   ........^.M.3..A
E0   14C5 FF8B E55D C210 - 008B 1590 C76D 025B   .....].......m.[
F0   C744 B2F4 0000 0000 - B001 5E8B 4DFC 33CD   .D........^.M.3.
```

Data types: Virtual table

	0	4	8	c
00	1BF767C	1BF7674	1051866	10518B9
10	1C0F93D	1C0F960	1C00B78	145AA92
20	1C0F9C7	145AC1F	90909090	55FF8B90
30	5653EC8B	8BF98B57	20A83847	6A80875
40	AC39850F	8B660046	458B0C55	205D8B08
50	3314758B	104D39C9	3C578966	950F178B

Data types: Virtual table

	0	4	8	c
00	1BF767C	1BF7674	1051866	10518B9
10	1C0F93D	1C0F960	1C00B78	145AA92
20	1C0F9C7	145AC1F	90909090	55FF8B90
30	5653EC8B	8BF98B57	20A83847	6A80875
40	AC39850F	8B660046	458B0C55	205D8B08
50	3314758B	104D39C9	3C578966	950F178B

Buffers limits

- Magic constants
  - Oracle: 0xBA5EBA11, 0xEEE
  - DB2: 0xDB2CAFEx
- Parsing the heap
  - MSDN or Linux source code

The Environment

API needed

- Read memory
- Search
  - Differential search
- Recursive search
- Wandering around

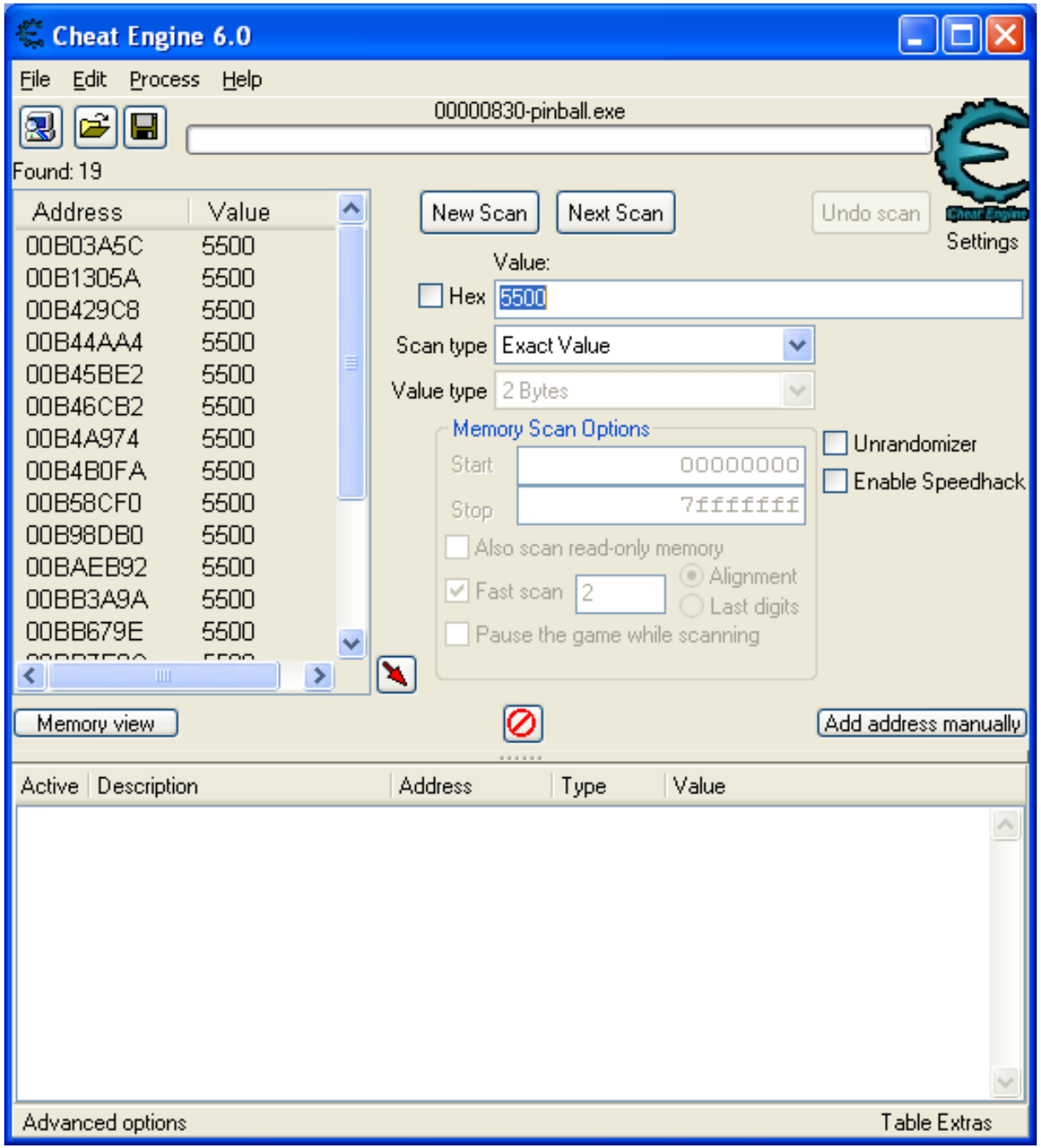
Tools for the task

- Remote process memory reader
  - Python is just the best
    - PyDbg
    - Mint
  - The Cheat Engine
  - Any other debugger

Differential search

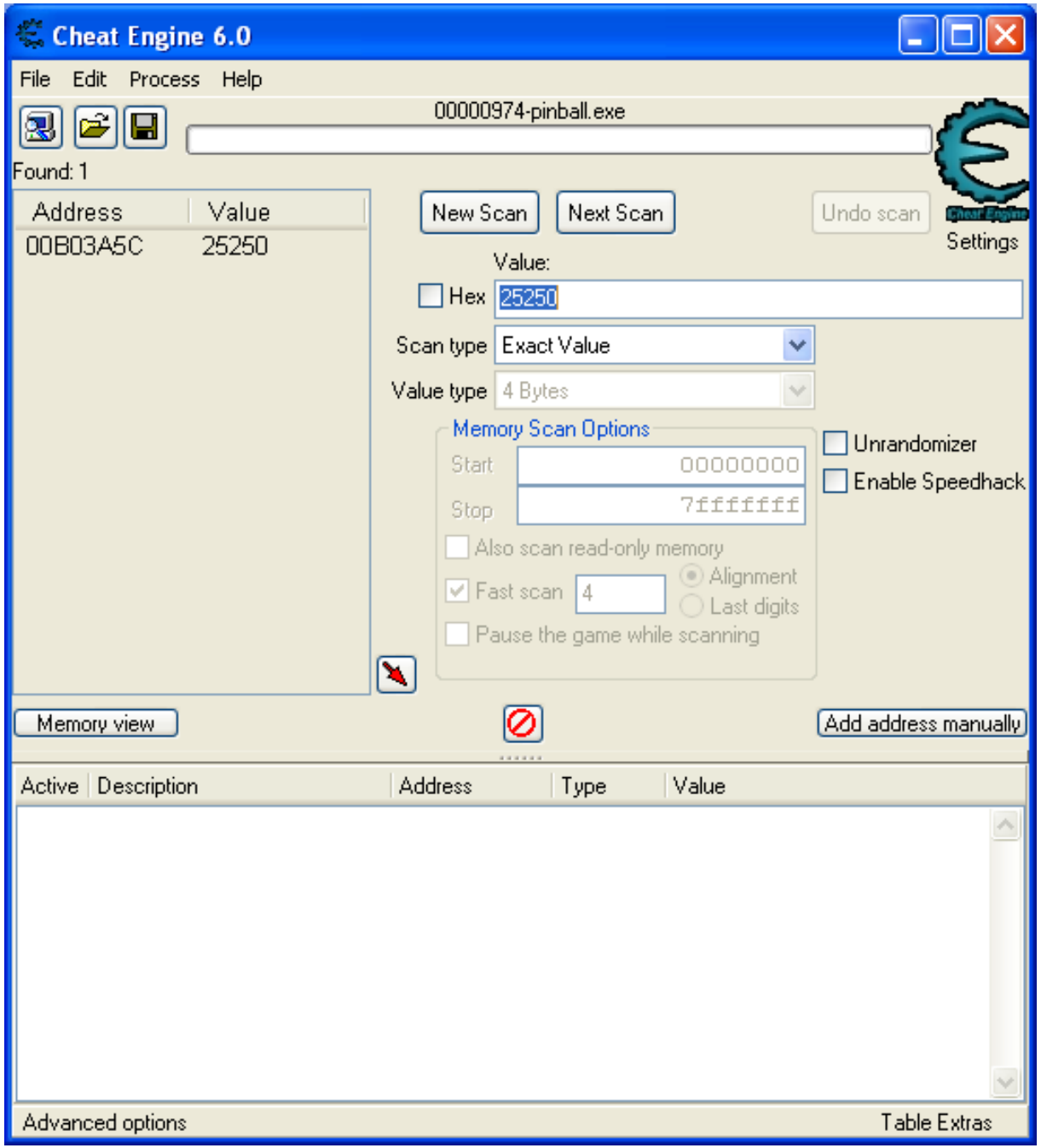
Differential search

Differential search



Differential search

Differential search



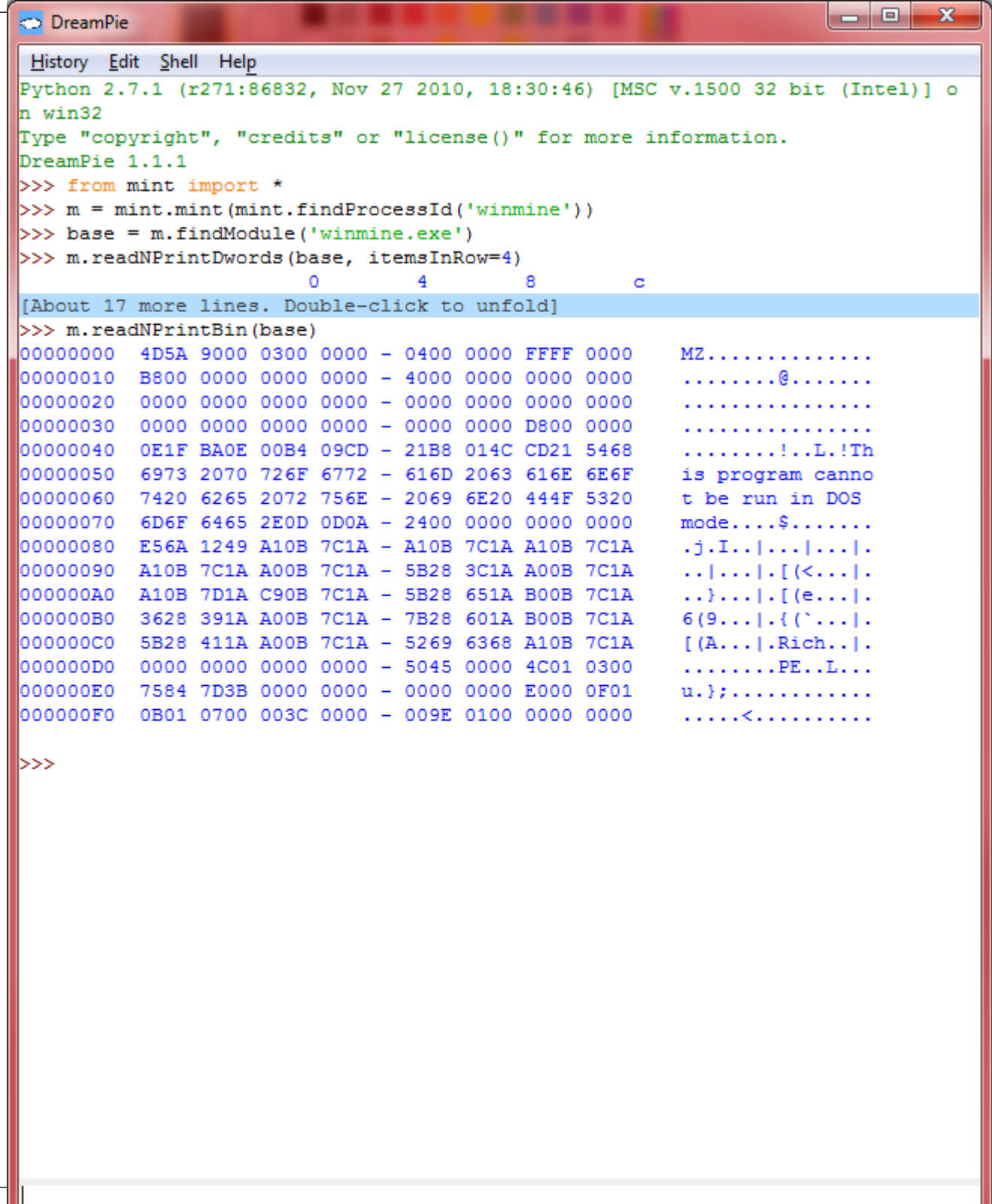
Differential search (The fun part)

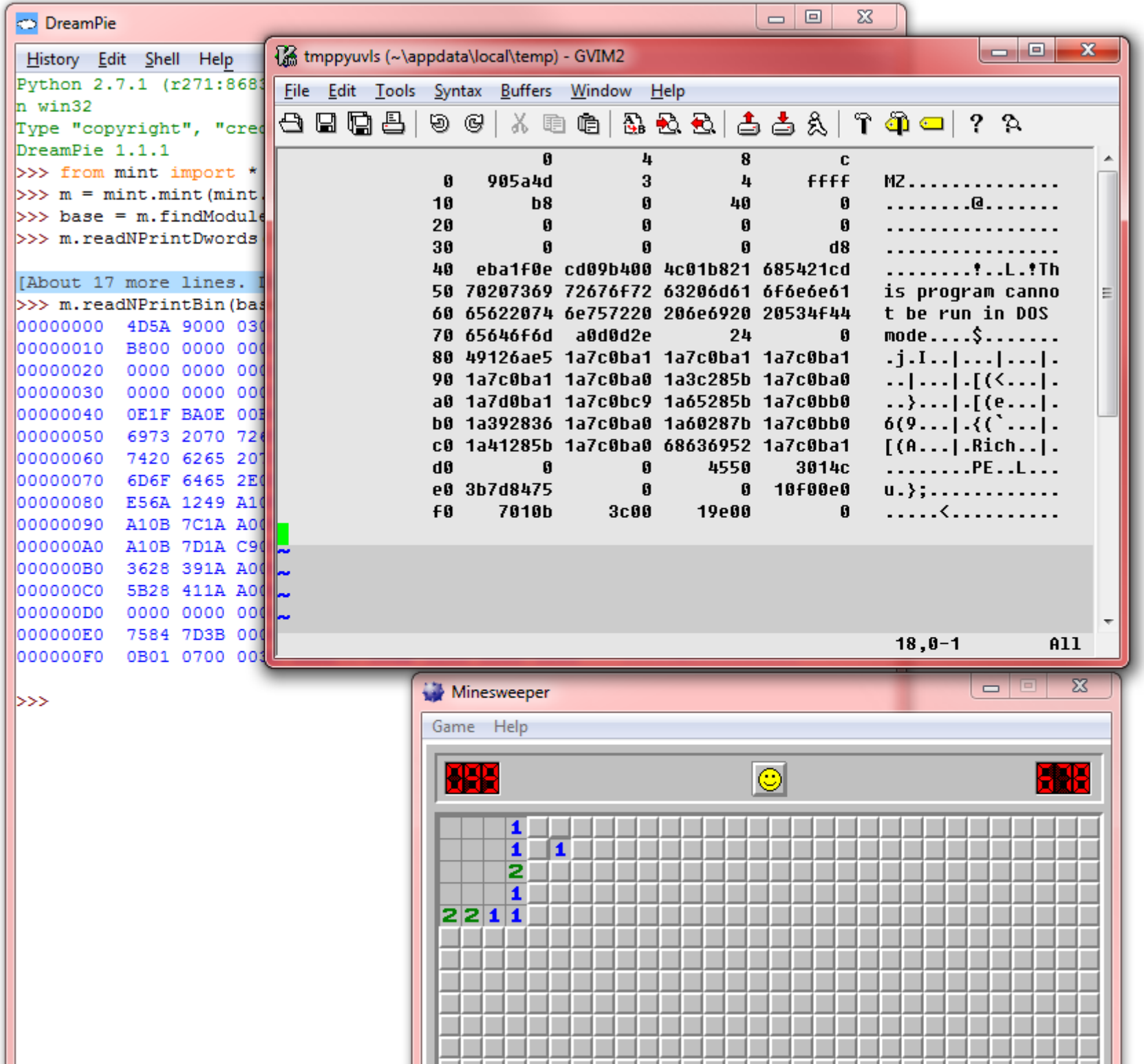
Python

DreamPie

History Edit Shell Help

```
Python 2.7.1 (r271:86832, Nov 27 2010, 18:30:46) [MSC v.1500 32 bit (Intel)] o
n win32
Type "copyright", "credits" or "license()" for more information.
DreamPie 1.1.1
>>> from mint import *
>>> m = mint.mint(mint.findProcessId('winmine'))
>>> base = m.findModule('winmine.exe')
>>> m.readNPrintDwords(base, itemsInRow=4)
                      0        4        8        c
               0   905a4d        3        4     ffff   MZ..............
              10       b8        0       40        0   ........@.......
              20        0        0        0        0   ................
              30        0        0        0       d8   ................
              40  eba1f0e cd09b400 4c01b821 685421cd   ........!..L.!Th
              50 70207369 72676f72 63206d61 6f6e6e61   is program canno
              60 65622074 6e757220 206e6920 20534f44   t be run in DOS
              70 65646f6d  a0d0d2e       24        0   mode....$.......
              80 49126ae5 1a7c0ba1 1a7c0ba1 1a7c0ba1   .j.I..|...|...|.
              90 1a7c0ba1 1a7c0ba0 1a3c285b 1a7c0ba0   ..|...|.[(<...|.
              a0 1a7d0ba1 1a7c0bc9 1a65285b 1a7c0bb0   ..}...|.[(e...|.
              b0 1a392836 1a7c0ba0 1a60287b 1a7c0bb0   6(9...|.{(`...|.
              c0 1a41285b 1a7c0ba0 68636952 1a7c0ba1   [(A...|.Rich..|.
              d0        0        0     4550     3014c   ........PE..L...
              e0 3b7d8475        0        0  10f00e0   u.};............
              f0    7010b     3c00    19e00        0   .....<..........

>>> m.readNPrintBin(base)
00000000  4D5A 9000 0300 0000 - 0400 0000 FFFF 0000    MZ..............
00000010  B800 0000 0000 0000 - 4000 0000 0000 0000    ........@.......
00000020  0000 0000 0000 0000 - 0000 0000 0000 0000    ................
00000030  0000 0000 0000 0000 - 0000 0000 D800 0000    ................
00000040  0E1F BA0E 00B4 09CD - 21B8 014C CD21 5468    ........!..L.!Th
00000050  6973 2070 726F 6772 - 616D 2063 616E 6E6F    is program canno
00000060  7420 6265 2072 756E - 2069 6E20 444F 5320    t be run in DOS
00000070  6D6F 6465 2E0D 0D0A - 2400 0000 0000 0000    mode....$.......
00000080  E56A 1249 A10B 7C1A - A10B 7C1A A10B 7C1A    .j.I..|...|...|.
00000090  A10B 7C1A A00B 7C1A - 5B28 3C1A A00B 7C1A    ..|...|.[(<...|.
000000A0  A10B 7D1A C90B 7C1A - 5B28 651A B00B 7C1A    ..}...|.[(e...|.
000000B0  3628 391A A00B 7C1A - 7B28 601A B00B 7C1A    6(9...|.{(`...|.
000000C0  5B28 411A A00B 7C1A - 5269 6368 A10B 7C1A    [(A...|.Rich..|.
000000D0  0000 0000 0000 0000 - 5045 0000 4C01 0300    ........PE..L...
000000E0  7584 7D3B 0000 0000 - 0000 0000 E000 0F01    u.};............
000000F0  0B01 0700 003C 0000 - 009E 0100 0000 0000    .....<..........

>>>
```


DreamPie
History Edit Shell Help
Python 2.7.1 (r271:86832, Nov 27 2010, 18:30:46) [MSC v.1500 32 bit (Intel)] o
n win32
Type "copyright", "credits" or "license()" for more information.
DreamPie 1.1.1
>>> from mint import *
>>> m = mint.mint(mint.findProcessId('winmine'))
>>> base = m.findModule('winmine.exe')
>>> m.readNPrintDwords(base, itemsInRow=4)
0 4 8 c
[About 17 more lines. Double-click to unfold]
>>> m.readNPrintBin(base)
00000000 4D5A 9000 0300 0000 - 0400 0000 FFFF 0000 MZ..............
00000010 B800 0000 0000 0000 - 4000 0000 0000 0000 ....@.......
00000020 0000 0000 0000 0000 - 0000 0000 0000 0000 ....
00000030 0000 0000 0000 0000 - 0000 0000 D800 0000 ....
00000040 0E1F BA0E 00B4 09CD - 21B8 014C CD21 5468 ....!..L.!Th
00000050 6973 2070 726F 6772 - 616D 2063 616E 6E6F is program canno
00000060 7420 6265 2072 756E - 2069 6E20 444F 5320 t be run in DOS
00000070 6D6F 6465 2E0D 0D0A - 2400 0000 0000 0000 mode....$.......
00000080 E56A 1249 A10B 7C1A - A10B 7C1A A10B 7C1A .j.I..|...|...|.
00000090 A10B 7C1A A00B 7C1A - 5B28 3C1A A00B 7C1A ..|...|.[(<...|.
000000A0 A10B 7D1A C90B 7C1A - 5B28 651A B00B 7C1A ..}...|.[(e...|.
000000B0 3628 391A A00B 7C1A - 7B28 601A B00B 7C1A 6(9...|.{(`...|.
000000C0 5B28 411A A00B 7C1A - 5269 6368 A10B 7C1A [(A...|.Rich..|.
000000D0 0000 0000 0000 0000 - 5045 0000 4C01 0300 ........PE..L...
000000E0 7584 7D3B 0000 0000 - 0000 0000 E000 0F01 u.};............
000000F0 0B01 0700 003C 0000 - 009E 0100 0000 0000 .....<..........
>>>

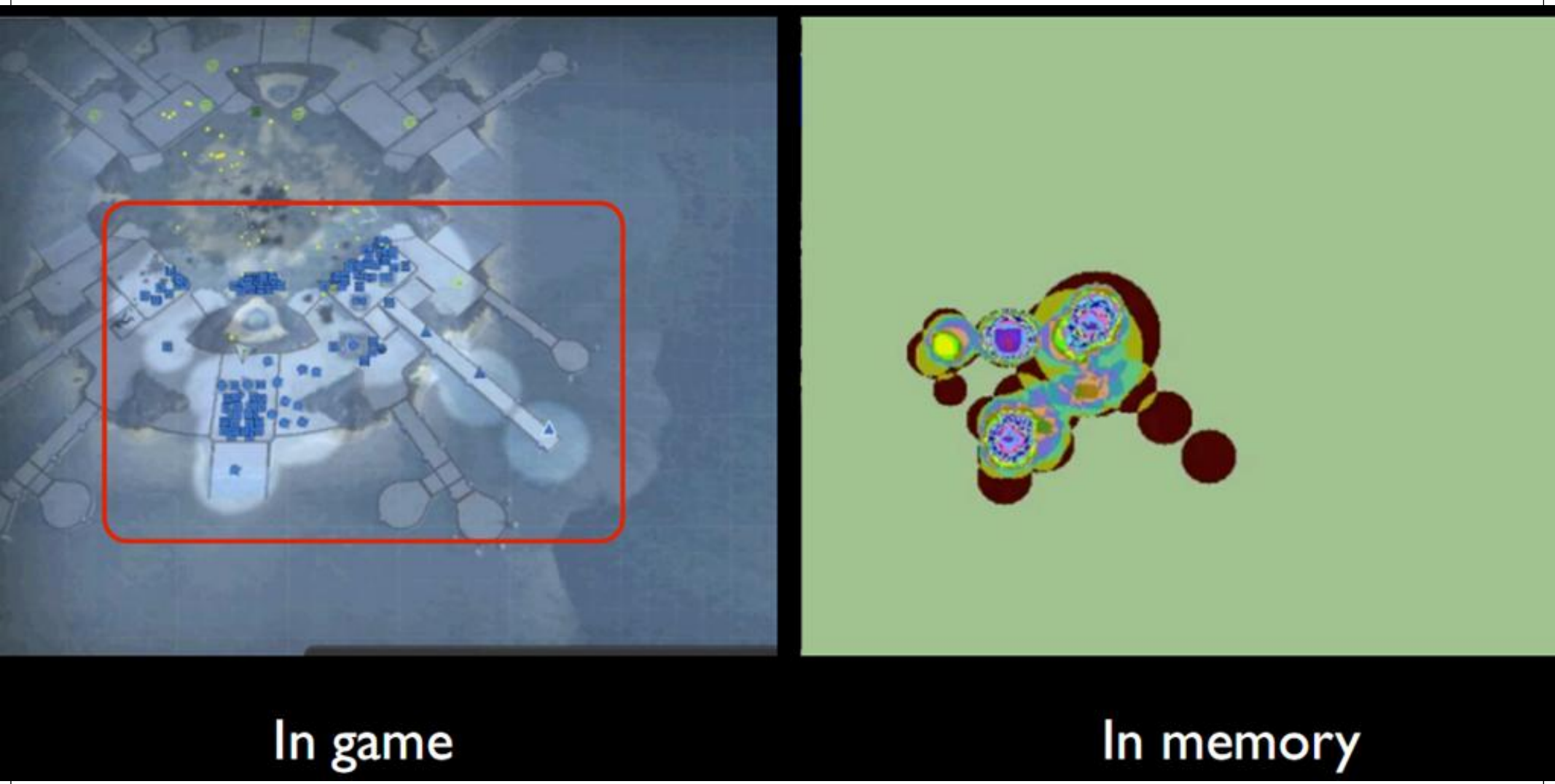

DreamPie
History Edit Shell Help
Python 2.7.1 (r271:868
n win32
Type "copyright", "cred
DreamPie 1.1.1
>>> from mint import *
>>> m = mint.mint(mint.
>>> base = m.findModule
>>> m.readNPrintDwords
[About 17 more lines. I
>>> m.readNPrintBin(bas
00000000 4D5A 9000 03
00000010 B800 0000 00
00000020 0000 0000 00
00000030 0000 0000 00
00000040 0E1F BA0E 00
00000050 6973 2070 72
00000060 7420 6265 20
00000070 6D6F 6465 2E
00000080 E56A 1249 A1
00000090 A10B 7C1A A0
000000A0 A10B 7D1A C9
000000B0 3628 391A A0
000000C0 5B28 411A A0
000000D0 0000 0000 00
000000E0 7584 7D3B 00
000000F0 0B01 0700 00
>>>
tmppyuvls (~\appdata\local\temp) - GVIM2
File Edit Tools Syntax Buffers Window Help
0 4 8 c
0 905a4d 3 4 ffff MZ..............
10 b8 0 40 0 ....@.......
20 0 0 0 0 ....
30 0 0 0 d8 ....
40 eba1f0e cd09b400 4c01b821 685421cd ....!..L.!Th
50 70207369 72676f72 63206d61 6f6e6e61 is program canno
60 65622074 6e757220 206e6920 20534f44 t be run in DOS
70 65646f6d a0d0d2e 24 0 mode....$.......
80 49126ae5 1a7c0ba1 1a7c0ba1 1a7c0ba1 .j.I..|...|...|.
90 1a7c0ba1 1a7c0ba0 1a3c285b 1a7c0ba0 ..|...|.[(<...|.
a0 1a7d0ba1 1a7c0bc9 1a65285b 1a7c0bb0 ..}...|.[(e...|.
b0 1a392836 1a7c0ba0 1a60287b 1a7c0bb0 6(9...|.{(`...|.
c0 1a41285b 1a7c0ba0 68636952 1a7c0ba1 [(A...|.Rich..|.
d0 0 0 4550 3014c .....PE..L...
e0 3b7d8475 0 0 10f00e0 u.};.....
f0 7010b 3c00 19e00 0 .....<.....
18,0-1 All
Minesweeper
Game Help

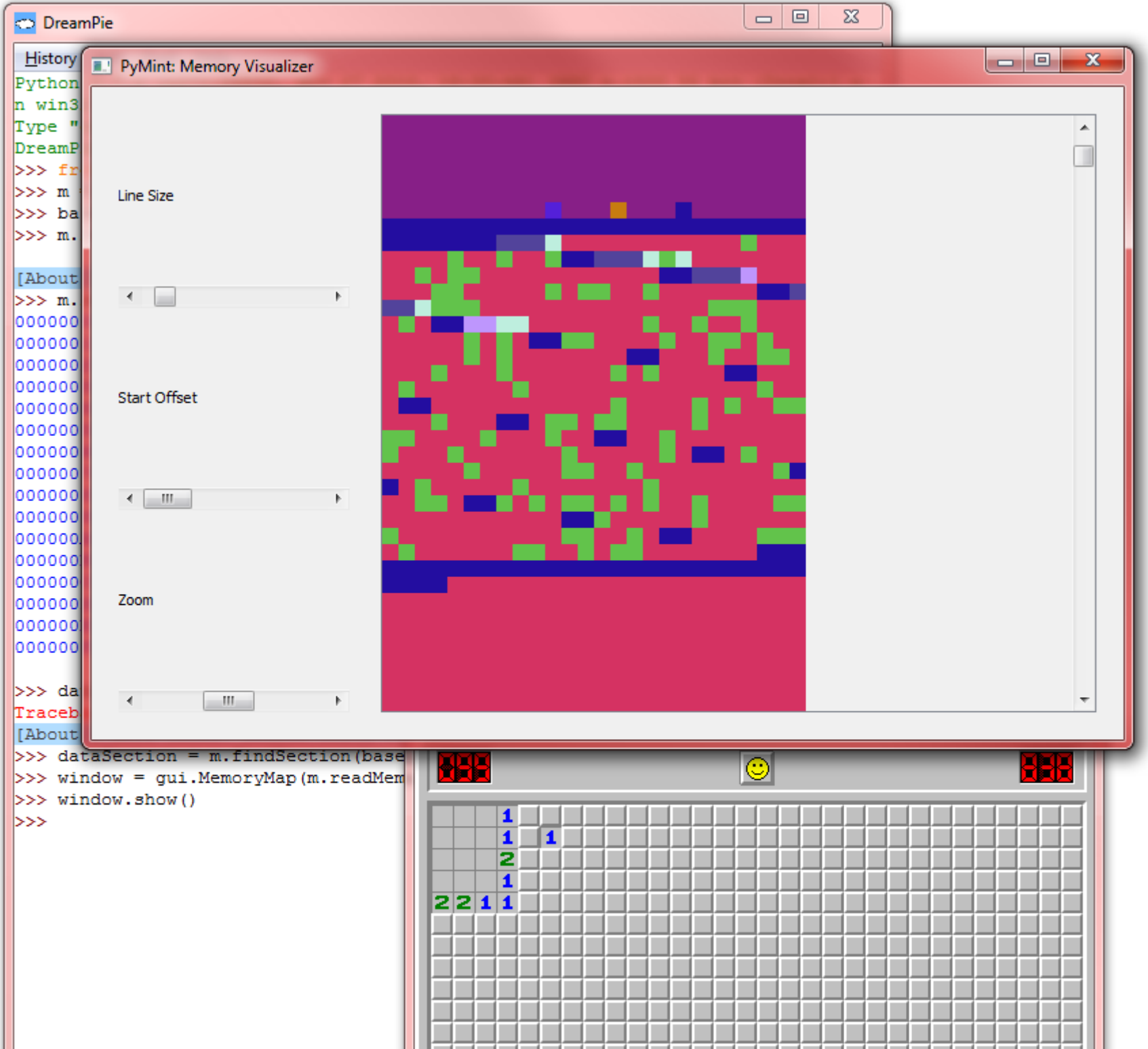
Recursive Search

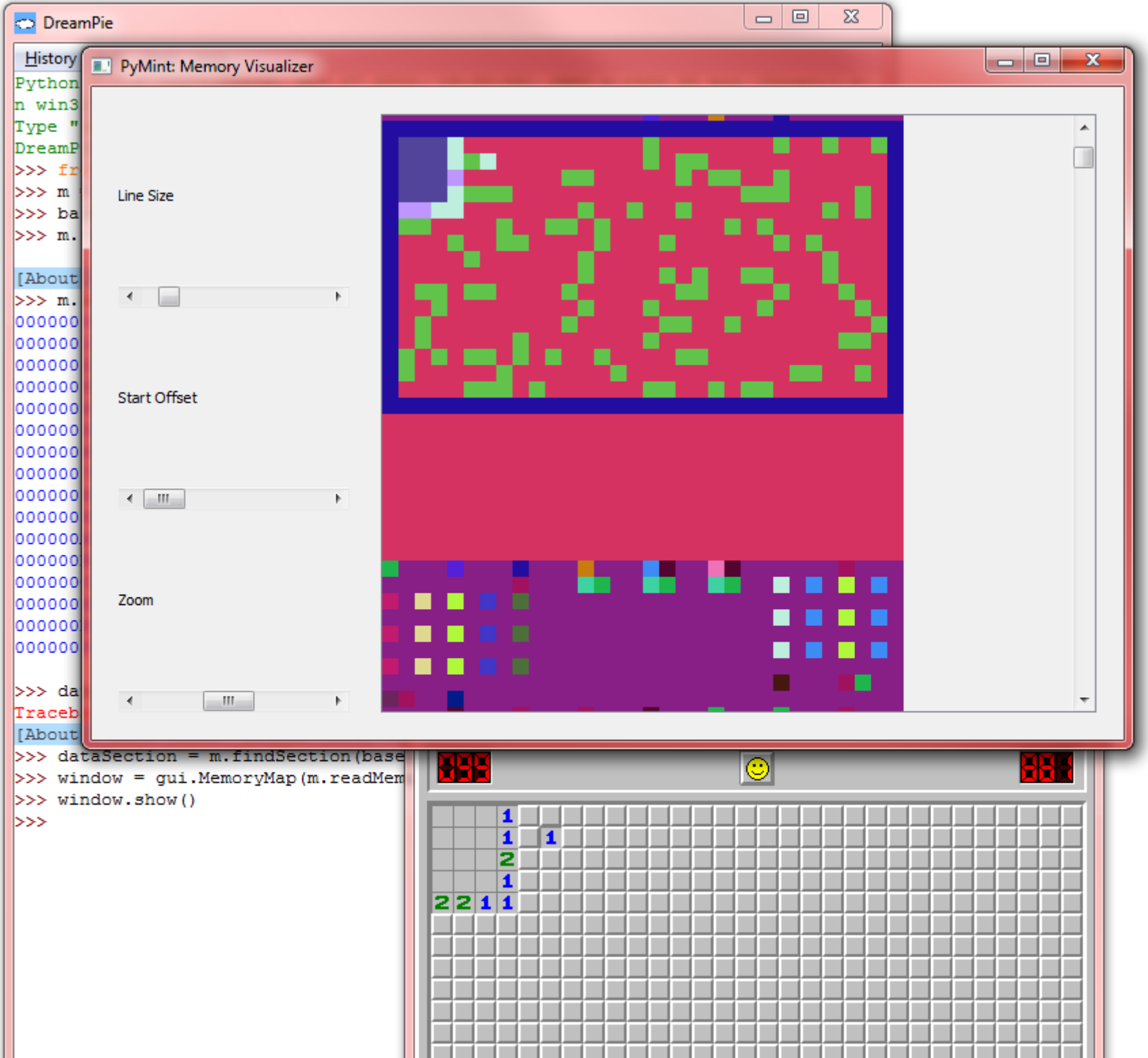
```
>>> for route in m.recursiveFind(0x54e5e58, session, 0x200, 3):
        m.printRecursiveFindResult(route)


0x54e5e0c ['0x1a0', '0x8', '0x98', '0xf4'] 89022040
0x54e5e0c ['0x1a0', '0xb0', '0xf4'] 89022040
0x54e5e0c ['0x1a4', '0x98', '0xf4'] 89022040
0x54e5e0c ['0x1d4', '0x44', '0x8c', '0x2c'] 89022040
0x54e5e0c ['0x1d4', '0x44', '0x90', '0x2c'] 89022040
0x54e5e0c ['0x1d4', '0x44', '0xb4', '0x2c'] 89022040
0x54e5e0c ['0x1d4', '0x10c', '0x8c', '0x2c'] 89022040
0x54e5e0c ['0x1d4', '0x10c', '0x90', '0x2c'] 89022040
0x54e5e0c ['0x1d4', '0x10c', '0xb4', '0x2c'] 89022040


>>>
```

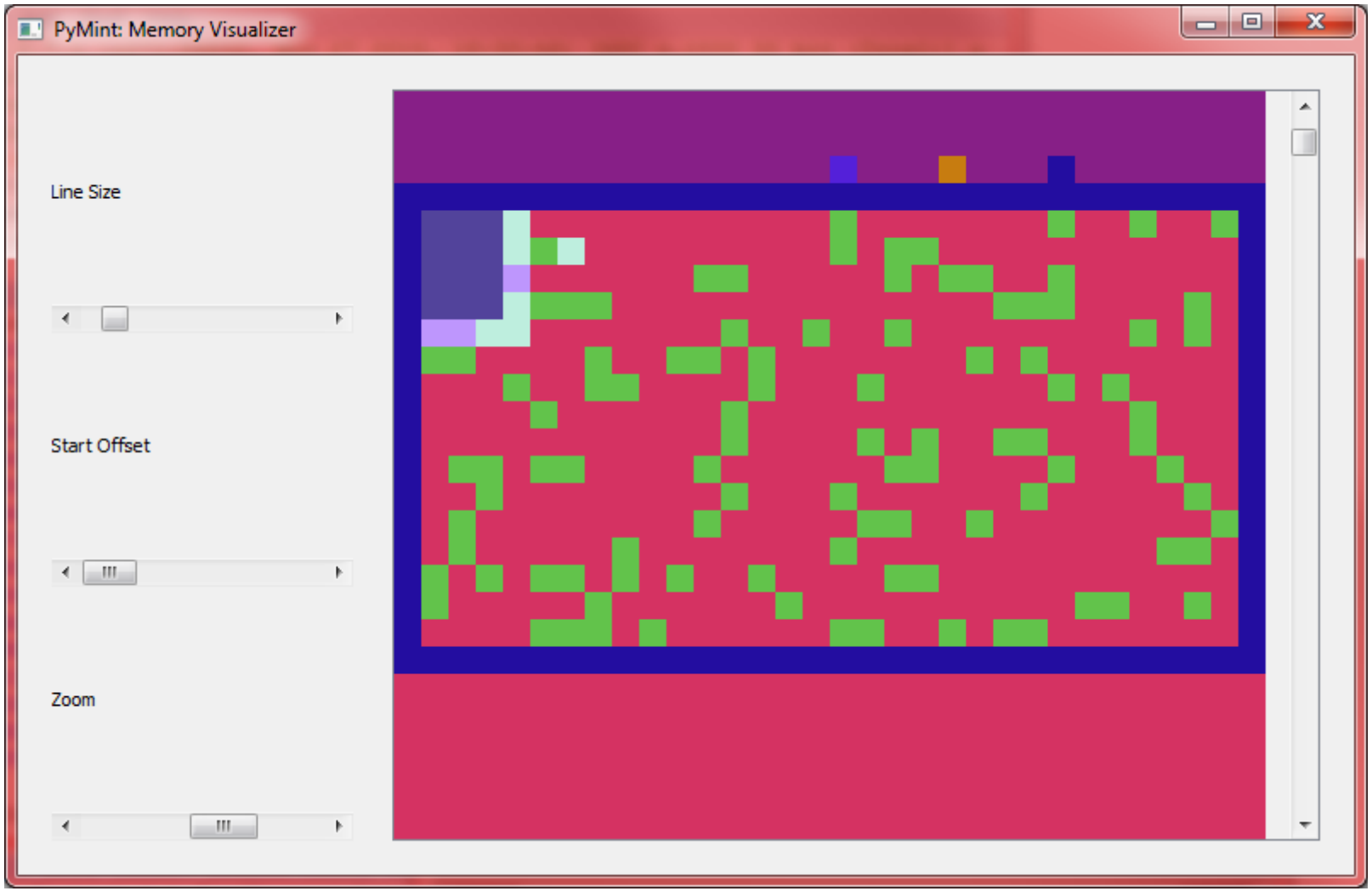
Data display: Graphical

Credit goes to Kartograph (DefCon2010)



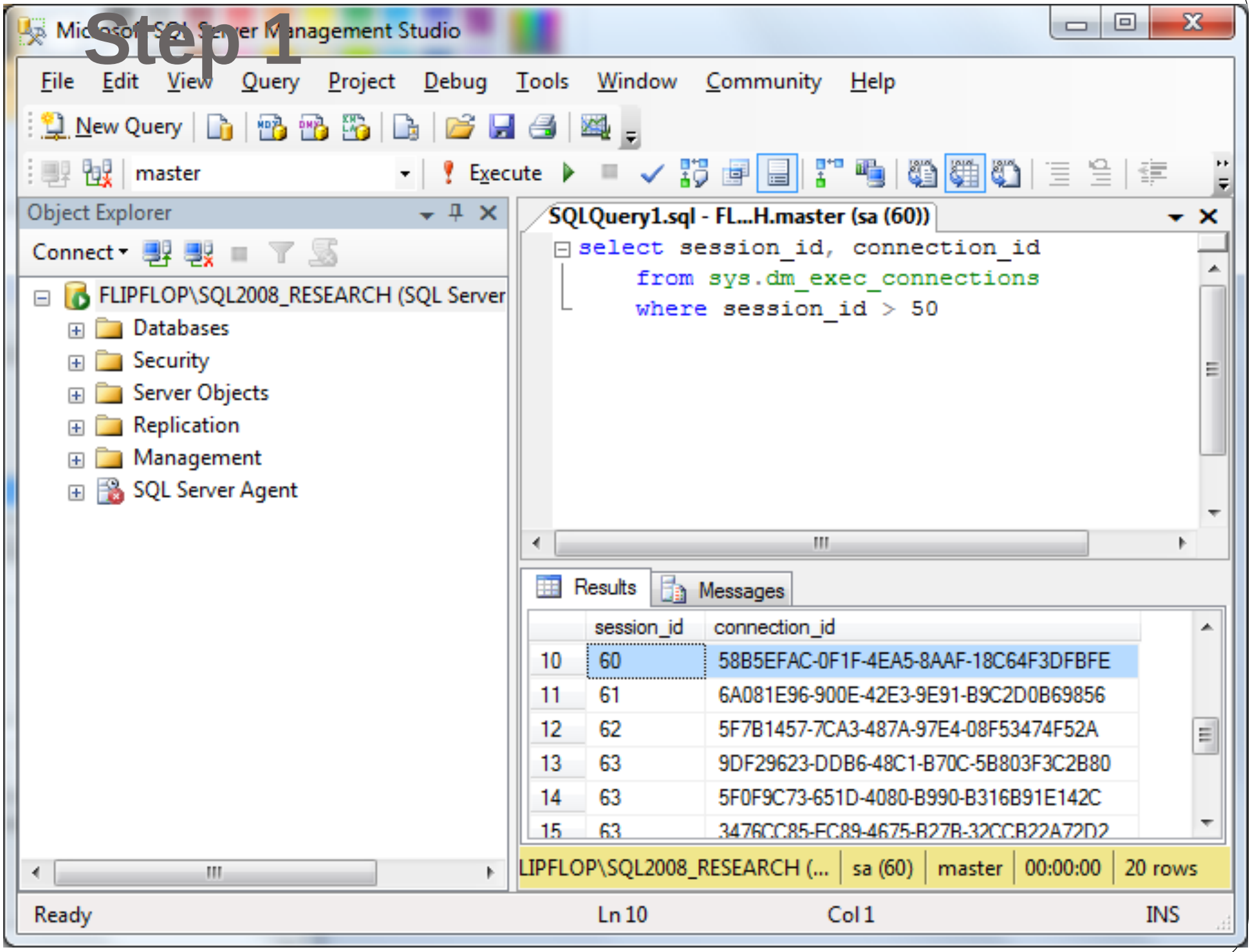

DreamPie
History
Python
n win3
Type "
DreamP
>>> fr
>>> m
>>> ba
>>> m.
[About
>>> m.
000000
000000
000000
000000
000000
000000
000000
000000
000000
000000
000000
000000
000000
000000
>>> da
Traceb
[About
>>> dataSection = m.findSection(base
>>> window = gui.MemoryMap(m.readMem
>>> window.show()
>>>
PyMint: Memory Visualizer
Line Size
Start Offset
Zoom


DreamPie
History
Python
n win3
Type "
DreamP
>>> fr
>>> m
>>> ba
>>> m.
[About
>>> m.
000000
000000
000000
000000
000000
000000
000000
000000
000000
000000
000000
000000
000000
000000
>>> da
Traceb
[About
>>> dataSection = m.findSection(base
>>> window = gui.MemoryMap(m.readMem
>>> window.show()
>>>
PyMint: Memory Visualizer
Line Size
Start Offset
Zoom

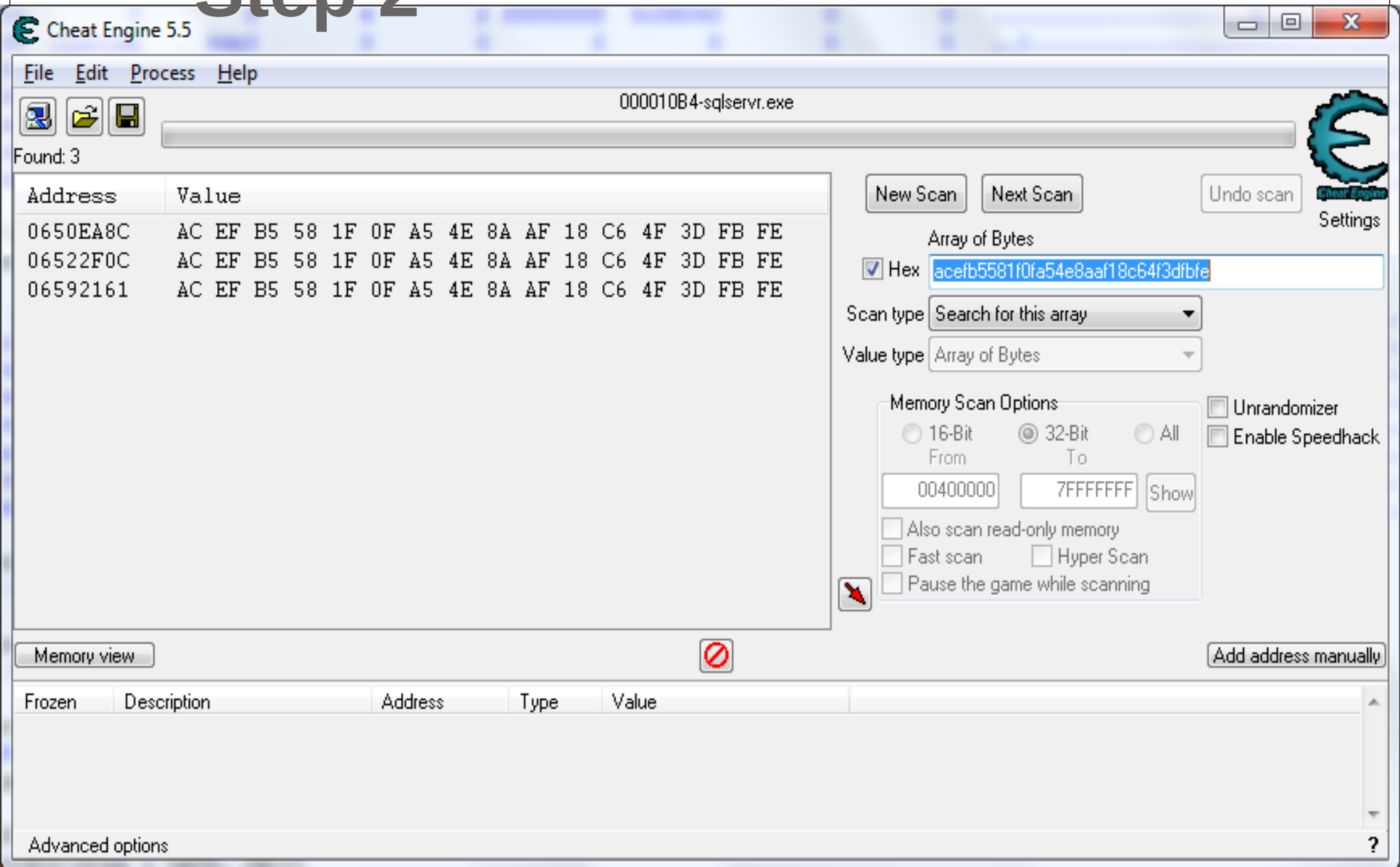

PyMint: Memory Visualizer
Line Size
Start Offset
Zoom

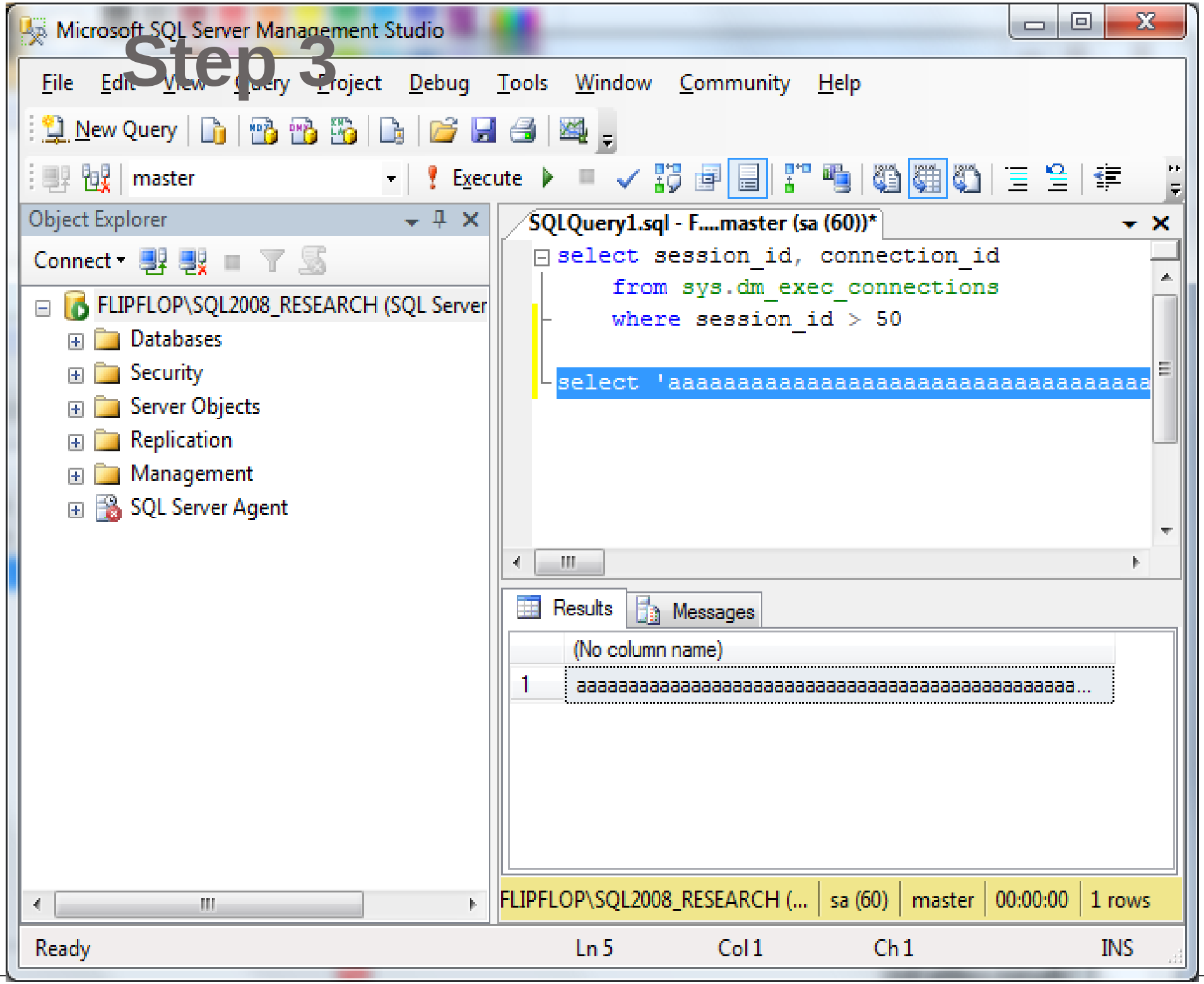
Example

Searching for sessions table (MSSQL), in ten easy steps

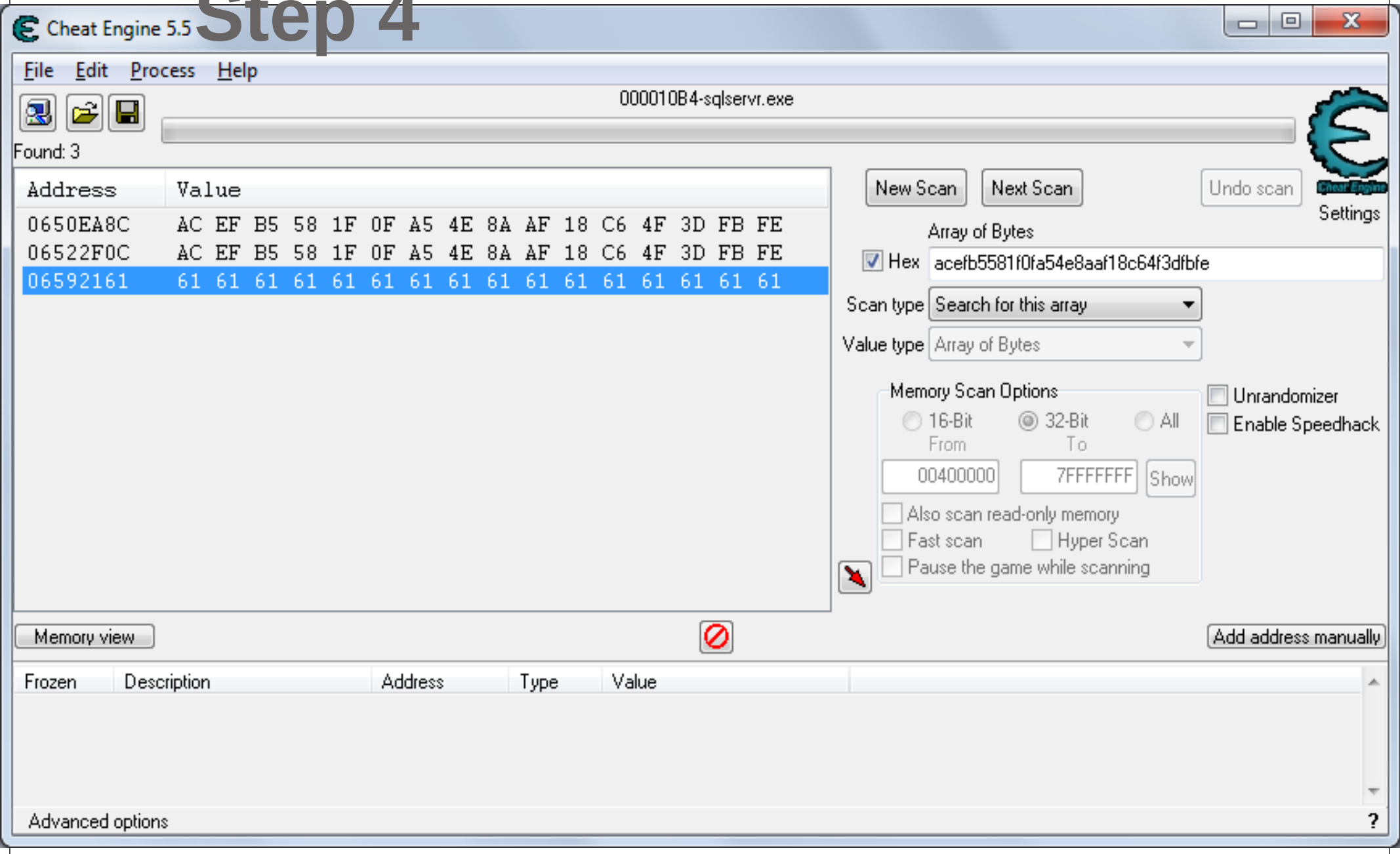

Step 1
Microsoft SQL Server Management Studio
File Edit View Query Project Debug Tools Window Community Help
New Query
master
Execute
Object Explorer
Connect
FLIPFLOP\SQL2008_RESEARCH (SQL Server
Databases
Security
Server Objects
Replication
Management
SQL Server Agent
SQLQuery1.sql - FL...H.master (sa (60))
select session_id, connection_id
from sys.dm_exec_connections
where session_id > 50
Results
Messages
session_id
connection_id
10 60 58B5EFAC-0F1F-4EA5-8AAF-18C64F3DFBFE
11 61 6A081E96-900E-42E3-9E91-B9C2D0B69856
12 62 5F7B1457-7CA3-487A-97E4-08F53474F52A
13 63 9DF29623-DDB6-48C1-B70C-5B803F3C2B80
14 63 5F0F9C73-651D-4080-B990-B316B91E142C
15 63 3476CC85-EC89-4675-B27B-32CCB22A72D2
LIPFLOP\SQL2008_RESEARCH (...
sa (60)
master
00:00:00
20 rows
Ready
Ln 10
Col 1
INS

Step 2


Cheat Engine 5.5
File Edit Process Help
000010B4-sqlservr.exe
Found: 3
Address Value
0650EA8C AC EF B5 58 1F 0F A5 4E 8A AF 18 C6 4F 3D FB FE
06522F0C AC EF B5 58 1F 0F A5 4E 8A AF 18 C6 4F 3D FB FE
06592161 AC EF B5 58 1F 0F A5 4E 8A AF 18 C6 4F 3D FB FE
New Scan
Next Scan
Undo scan
Settings
Array of Bytes
Hex
acefb5581f0fa54e8aaf18c64f3dfbfe
Scan type
Search for this array
Value type
Array of Bytes
Memory Scan Options
16-Bit
32-Bit
All
From
To
00400000
7FFFFFFF
Show
Also scan read-only memory
Fast scan
Hyper Scan
Pause the game while scanning
Unrandomizer
Enable Speedhack
Memory view
Add address manually
Frozen
Description
Address
Type
Value
Advanced options


Step 3
Microsoft SQL Server Management Studio
File Edit View Query Project Debug Tools Window Community Help
New Query
master
Execute
Object Explorer
Connect
FLIPFLOP\SQL2008_RESEARCH (SQL Server
Databases
Security
Server Objects
Replication
Management
SQL Server Agent
SQLQuery1.sql - F....master (sa (60))*
select session_id, connection_id
from sys.dm_exec_connections
where session_id > 50
select 'aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Results
Messages
(No column name)
1
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa...
FLIPFLOP\SQL2008_RESEARCH (...
sa (60)
master
00:00:00
1 rows
Ready
Ln 5
Col 1
Ch 1
INS

Step 4


Cheat Engine 5.5
File Edit Process Help
000010B4-sqlservr.exe
Found: 3
Address Value
0650EA8C AC EF B5 58 1F 0F A5 4E 8A AF 18 C6 4F 3D FB FE
06522F0C AC EF B5 58 1F 0F A5 4E 8A AF 18 C6 4F 3D FB FE
06592161 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61
New Scan
Next Scan
Undo scan
Settings
Array of Bytes
Hex
acefb5581f0fa54e8aaf18c64f3dfbfe
Scan type
Search for this array
Value type
Array of Bytes
Memory Scan Options
16-Bit
32-Bit
All
From
To
00400000
7FFFFFFF
Show
Also scan read-only memory
Fast scan
Hyper Scan
Pause the game while scanning
Unrandomizer
Enable Speedhack
Memory view
Add address manually
Frozen
Description
Address
Type
Value
Advanced options

Step 5

```
>>> m.readNPrintDwords(0x06522F0C - 0x80, itemsInRow=4)
                    0        4        8        c
                0        0 ffffffff ffffffff        0   ................
               10        0        0        0        0   ................
               20        0 ffffffff ffffffff        0   ................
               30        0        0        0        0   ................
               40        0        0        0        0   ................
               50        0        0        0        0   ................
               60        0        0        0        0   ................
               70        0        1   d00308       3c   ............<...
               80 58b5efac 4ea50f1f c618af8a fefb3d4f   ...X...N....O=..
               90       16   79c5c0        0        0   ......y.........
               a0        0   557e8c0     1000  11ca6e9   ......W.........
               b0   f38c34        0   f370c5        0   4........p......
               c0        0        0        0        0   ................
               d0  65907a8        c        c     1000   ..Y.............
               e0        0        0        4 c6e9f07b   ............{...
               f0  1cb16ee b6ede372        1 b20de741   ....r.......A...


>>>
```

Step 6

```
>>> m.readNPrintDwords(0x0650EA8C - 0x80, itemsInRow=4)
                0        4        8        c
 0              0        0        0        2   ................
10              1  6624d78  66a41dc        0   ....xMb..Aj.....
20              3  5d65990        1        0   .....Y..........
30              0        0        0  6628040   ............@.b.
40           1000    40140  5b0d6d0  11c4354   ....@.......TC..
50        650e128  37ea404  37ea404        1   (.P...~...~.....
60              0  6590258        0        0   ....X.Y.........
70              0       3c        0        0   ....<...........
80     58b5efac 4ea50f1f c618af8a fefb3d4f   ...X...N....O=..
90      6522f08        0        0        0   ./R.............
a0              0        0        0        1   ................
b0              0        0        1        0   ................
c0              0       e6        0  160118b   ..............`.
d0           9da3 b20ef8b5        3  163f699   ..............c.
e0           9da3  163f699     9da3  15dbd77   ......c.....w.].
f0           9da3        2        0 b20ef8b5   ................

>>>
```

Step 7

```
>>> m.readNPrintDwords(0x0650EA8C - 0x80, itemsInRow=4)
                   0        4        8        c
                0  0        0        0        2  ................
               10  0        1  6624d78  66a41dc0  ....xMb..Aj.....
               20  0        3  5d65990        1  .....Y..........
               30  0        0        0  [illegible]  ............@.b.
               40  0     1000    40140  5b0d6d0  11c4354  ....@.......TC..
               50  0  650e128  37ea404  37ea404        1  (.P...~...~.....
               60  0        0  6590258        0        0  ....X.Y.........
               70  0        0       3c        0        0  ....<...........
               80  0 58b5efac 4ea50f1f c618af8a fefb3d4f  ...X...N....O=..
               90  0  6522f08        0        0        0  ./R.............
               a0  0        0        0        0        1  ................
               b0  0        0        0        1        0  ................
               c0  0        0       e6        0  160118b  ..............`.
               d0  0     9da3 b20ef8b5        3  163f699  ..............c.
               e0  0     9da3  163f699     9da3  15dbd77  ......c.....w.].
               f0  0     9da3        2        0 b20ef8b5  ................

>>>
```

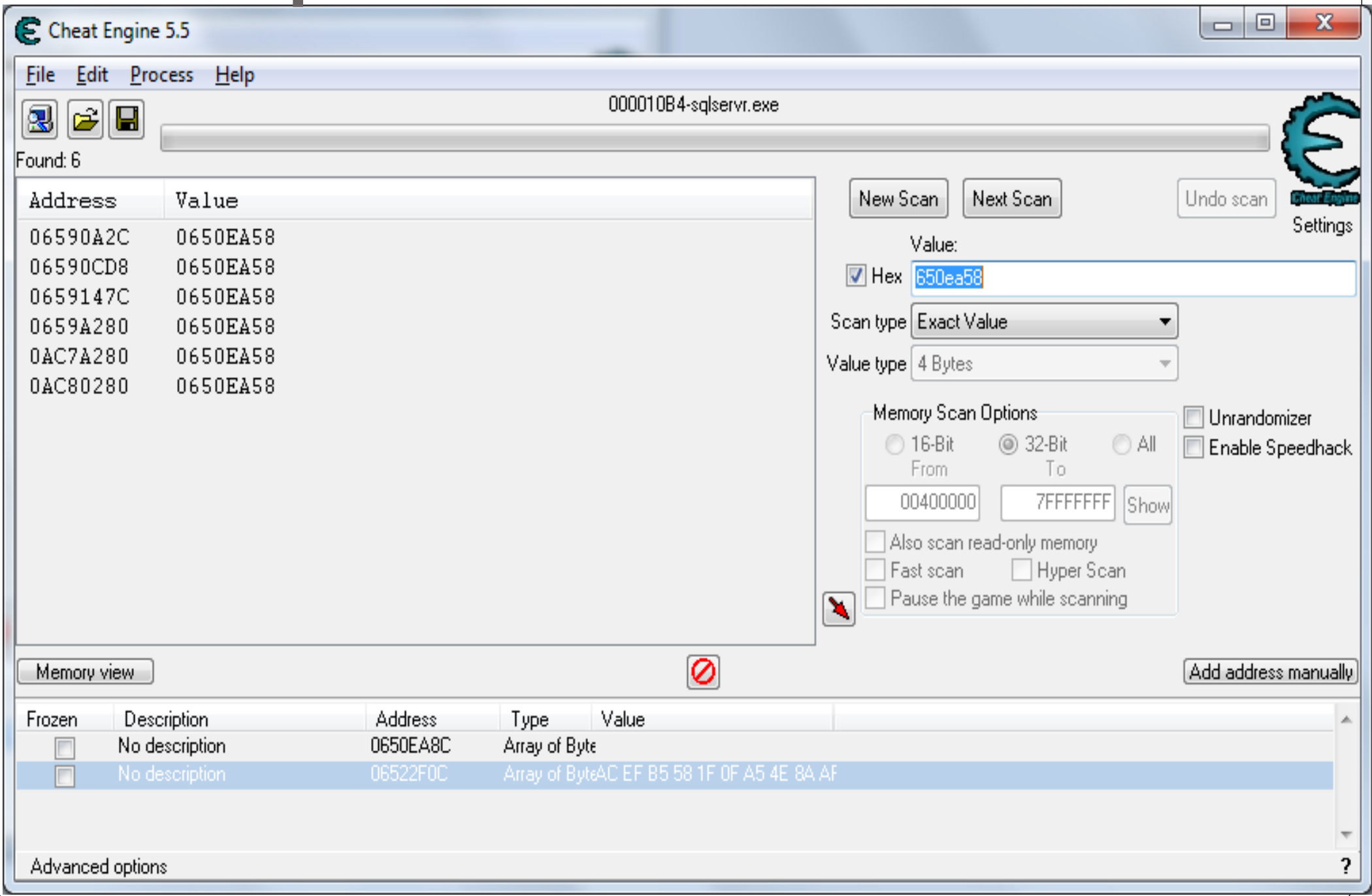
Step 8

```
>>> m.readNPrintDwords(0x11c4354, itemsInRow=4)
                   0        4        8        c
               0  11c72a7  11c7150  15cbbbc  15cc1c4   .r..Pq....\...\.
              10  15cbbbc  15cbbbc  15cc1cc  15cc1d6   ..\...\...\...\.
              20  15cbbbc  15cbbbc  15cbbbc  15cbbbc   ..\...\...\...\.
              30  15cbbbc  15cbbbc 90909090 55ff8b90   ..\...\........U
              40 8d51ec8b ca831041 c10ff0ff 840f4a10   ..Q.A........J..
              50     40bb c35de58b 90909090 55ff8b90   .@....]........U
              60 ff6aec8b a89b7868   a16402 50000000   ..j.hx...d.....P
              70 4024a151 c53302c3 f4458d50     a364   Q.$@..3.P.E.d...
              80 558b0000 f0558908   fc45c7 85000000   ...U..U..E......
              90 8b3774d2 c8831c41 c7028901 fffffc45   .t7.A.......E...
              a0 8366ffff  f011a41 891a41b7 d2331c51   ..f.A....A..Q.3.
              b0 18413b66 8bc2940f f44d8bc2    d8964   f;A.......M.d...
              c0 59000000 c25de58b d2330004 9090cdeb   ...Y..]...3.....
              d0 8b909090 ec8b55ff 560c458b 8b57f08b   .....U...E.V..W.
              e0 e681087d ffffe000 e8ce8b50 ffffff6d   }.......P...m...
              f0 850fc085    20448 1a46b70f  1f88366   ....H.....F.f...

>>>
```

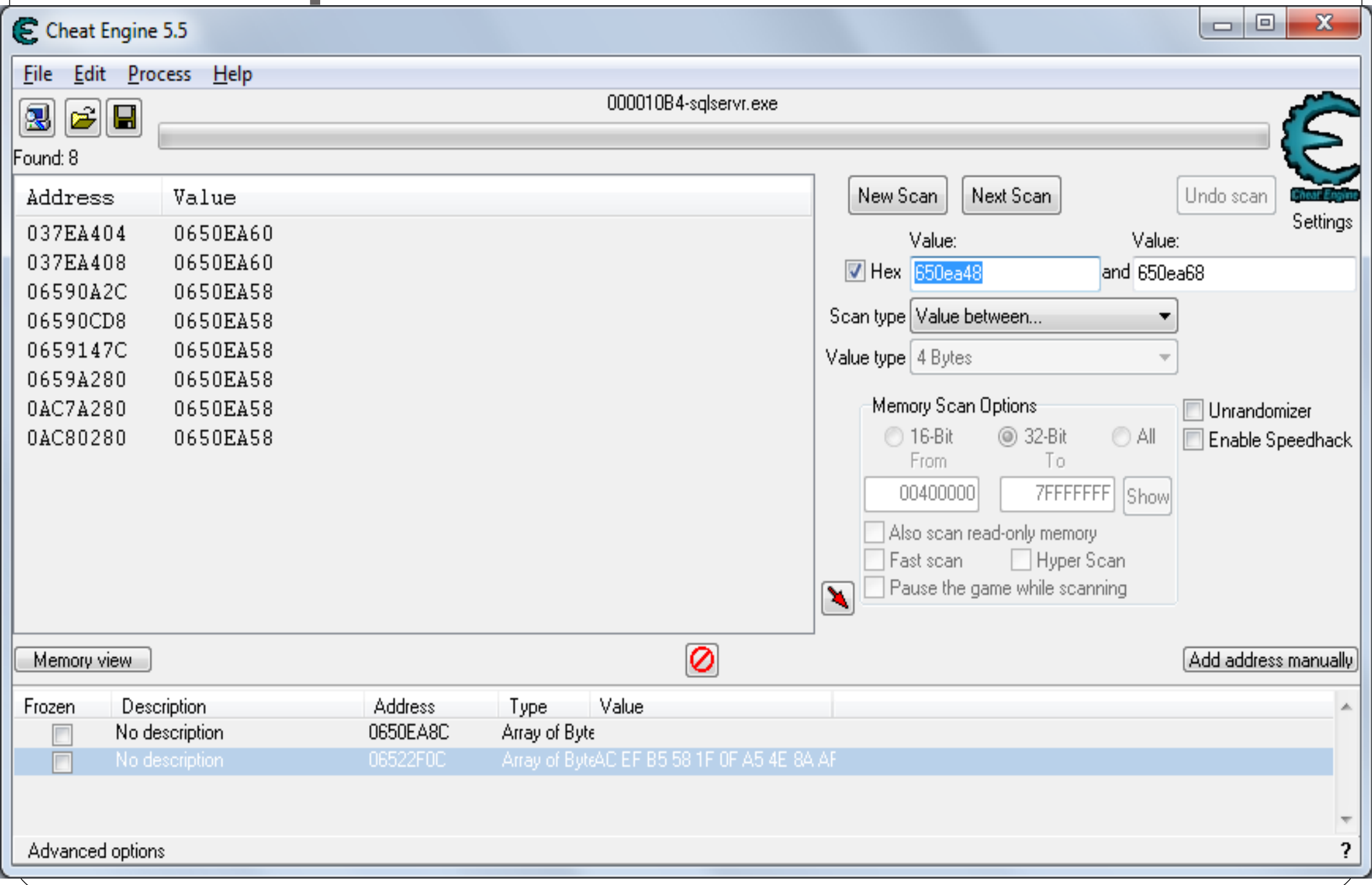
Step 9

```
>>> hex(0x0650EA8C - 0x34)
'0x650ea58'
>>>
```

Step A


Cheat Engine 5.5
File Edit Process Help
000010B4-sqlservr.exe
Found: 6
Address Value
06590A2C 0650EA58
06590CD8 0650EA58
0659147C 0650EA58
0659A280 0650EA58
0AC7A280 0650EA58
0AC80280 0650EA58
New Scan
Next Scan
Undo scan
Settings
Value:
Hex
650ea58
Scan type
Exact Value
Value type
4 Bytes
Memory Scan Options
16-Bit
32-Bit
All
From
To
00400000
7FFFFFFF
Show
Also scan read-only memory
Fast scan
Hyper Scan
Pause the game while scanning
Unrandomizer
Enable Speedhack
Memory view
Add address manually
Frozen
Description
Address
Type
Value
No description
0650EA8C
Array of Byte
No description
06522F0C
Array of ByteAC EF B5 58 1F 0F A5 4E 8A AF
Advanced options

Step B


Cheat Engine 5.5
File Edit Process Help
000010B4-sqlservr.exe
Found: 8
Address Value
037EA404 0650EA60
037EA408 0650EA60
06590A2C 0650EA58
06590CD8 0650EA58
0659147C 0650EA58
0659A280 0650EA58
0AC7A280 0650EA58
0AC80280 0650EA58
New Scan
Next Scan
Undo scan
Settings
Value:
Hex
650ea48
and
Value:
650ea68
Scan type
Value between...
Value type
4 Bytes
Memory Scan Options
16-Bit
32-Bit
All
From
To
00400000
7FFFFFFF
Show
Also scan read-only memory
Fast scan
Hyper Scan
Pause the game while scanning
Unrandomizer
Enable Speedhack
Memory view
Add address manually
Frozen
Description
Address
Type
Value
No description
0650EA8C
Array of Byte
No description
06522F0C
Array of ByteAC EF B5 58 1F 0F A5 4E 8A AF
Advanced options

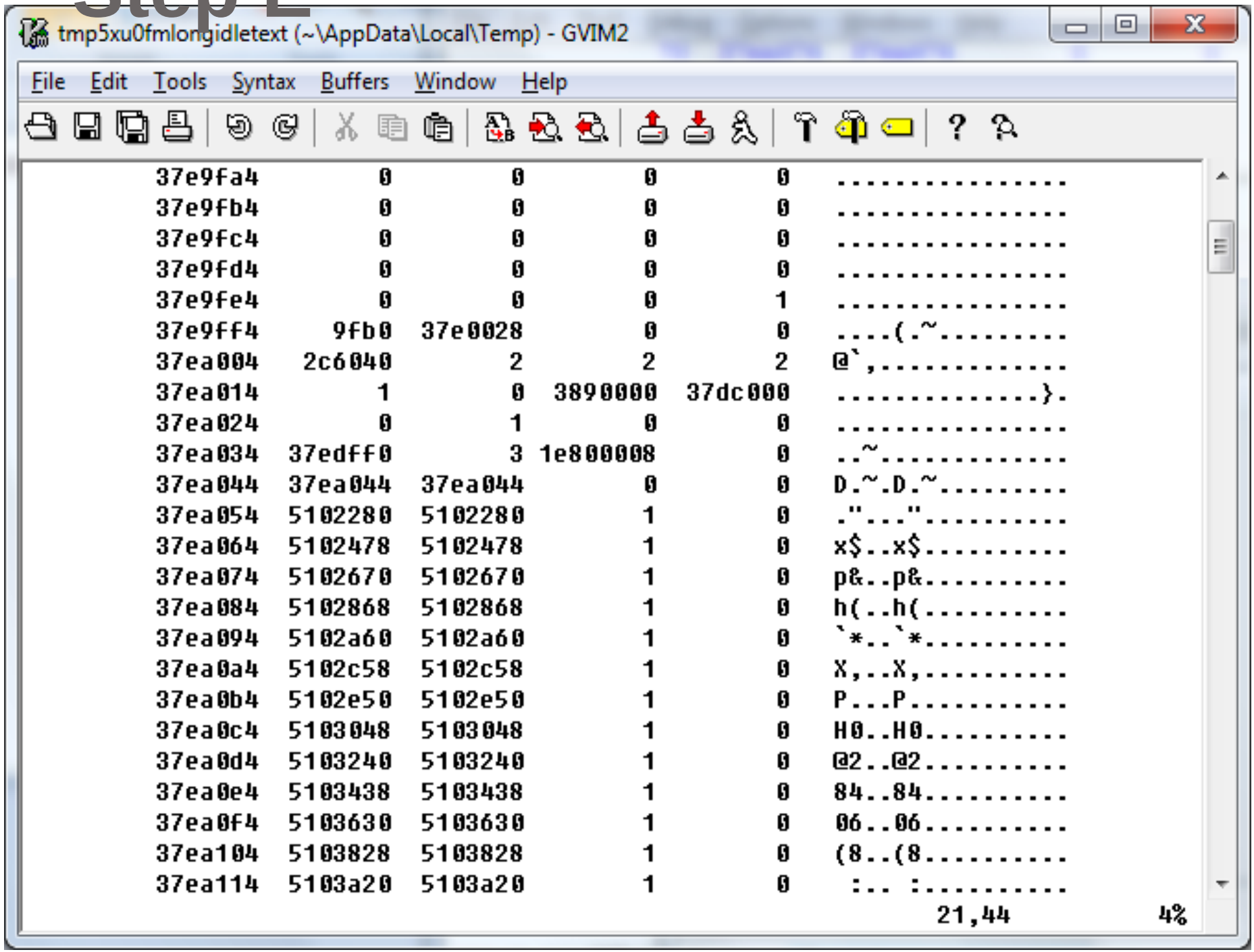
Step C

```
>>> m.readNPrintDwords(0x037EA404, itemsInRow=4)
                    0         4         8         c
                0  650ea60  650ea60         1         0   `.P.`.P.........
               10  58b0a60  650ec58         2         0   `...X.P.........
               20  650ee50  650ee50         1         0   P.P.P.P.........
               30  650fa20  650f048         4         0    .P.H.P.........
               40  650fc18  650f630         3         0   ..P.0.P.........
               50  37ea454  37ea454         0         0   T.~.T.~.........
               60  37ea464  37ea464         0         0   d.~.d.~.........
               70  37ea474  37ea474         0         0   t.~.t.~.........
               80  37ea484  37ea484         0         0   ..~...~.........
               90  37ea494  37ea494         0         0   ..~...~.........
               a0  37ea4a4  37ea4a4         0         0   ..~...~.........
               b0  37ea4b4  37ea4b4         0         0   ..~...~.........
               c0  37ea4c4  37ea4c4         0         0   ..~...~.........
               d0  37ea4d4  37ea4d4         0         0   ..~...~.........
               e0  37ea4e4  37ea4e4         0         0   ..~...~.........
               f0  37ea4f4  37ea4f4         0         0   ..~...~.........


>>>
```

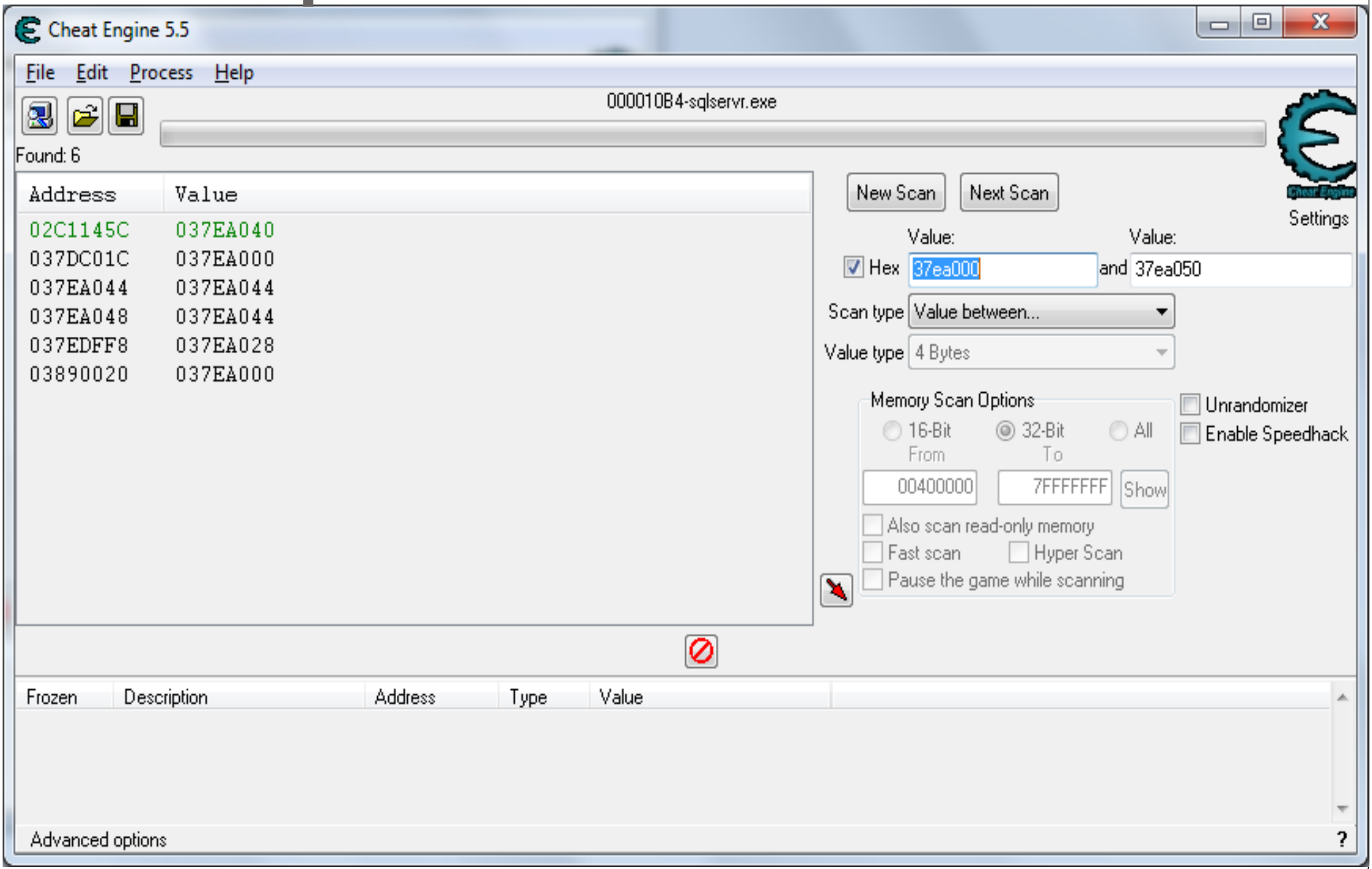
Step D

	0	4	8	c	
00	650ea60	650ea60	1	0	`.P.`.P.....
10	58b0a60	650ec58	2	0	`...X.P.....
20	650ee50	650ee50	1	0	P.P.P.P.....
30	650fa20	650f048	4	0	.P.H.P.....
40	650fc18	650f630	3	0	..P.0.P.....
50	37ea454	37ea454	0	0	T.~.T.~.....
60	37ea464	37ea464	0	0	d.~.d.~.....
70	37ea474	37ea474	0	0	t.~.t.~.....
80	37ea484	37ea484	0	0	..~...~.....
90	37ea494	37ea494	0	0	..~...~.....
a0	37ea4a4	37ea4a4	0	0	..~...~.....
b0	37ea4b4	37ea4b4	0	0	..~...~.....
c0	37ea4c4	37ea4c4	0	0	..~...~.....
d0	37ea4d4	37ea4d4	0	0	..~...~.....
e0	37ea4e4	37ea4e4	0	0	..~...~.....
f0	37ea4f4	37ea4f4	0	0	..~...~.....

Step E


tmp5xu0fmlongidletext (~\AppData\Local\Temp) - GVIM2
File Edit Tools Syntax Buffers Window Help
37e9fa4 0 0 0 0 ....
37e9fb4 0 0 0 0 ....
37e9fc4 0 0 0 0 ....
37e9fd4 0 0 0 0 ....
37e9fe4 0 0 0 1 ....
37e9ff4 9fb0 37e0028 0 0 ....(.~.....
37ea004 2c6040 2 2 2 @`,.....
37ea014 1 0 3890000 37dc000 ....}.
37ea024 0 1 0 0 ....
37ea034 37edff0 3 1e800008 0 ..~.....
37ea044 37ea044 37ea044 0 0 D.~.D.~.....
37ea054 5102280 5102280 1 0 ."..."....
37ea064 5102478 5102478 1 0 x$..x$....
37ea074 5102670 5102670 1 0 p&..p&....
37ea084 5102868 5102868 1 0 h(..h(....
37ea094 5102a60 5102a60 1 0 `*..`*....
37ea0a4 5102c58 5102c58 1 0 X,..X,....
37ea0b4 5102e50 5102e50 1 0 P...P.....
37ea0c4 5103048 5103048 1 0 H0..H0....
37ea0d4 5103240 5103240 1 0 @2..@2....
37ea0e4 5103438 5103438 1 0 84..84....
37ea0f4 5103630 5103630 1 0 06..06....
37ea104 5103828 5103828 1 0 (8..(8....
37ea114 5103a20 5103a20 1 0 :.. :....
21,44 4%

Step F

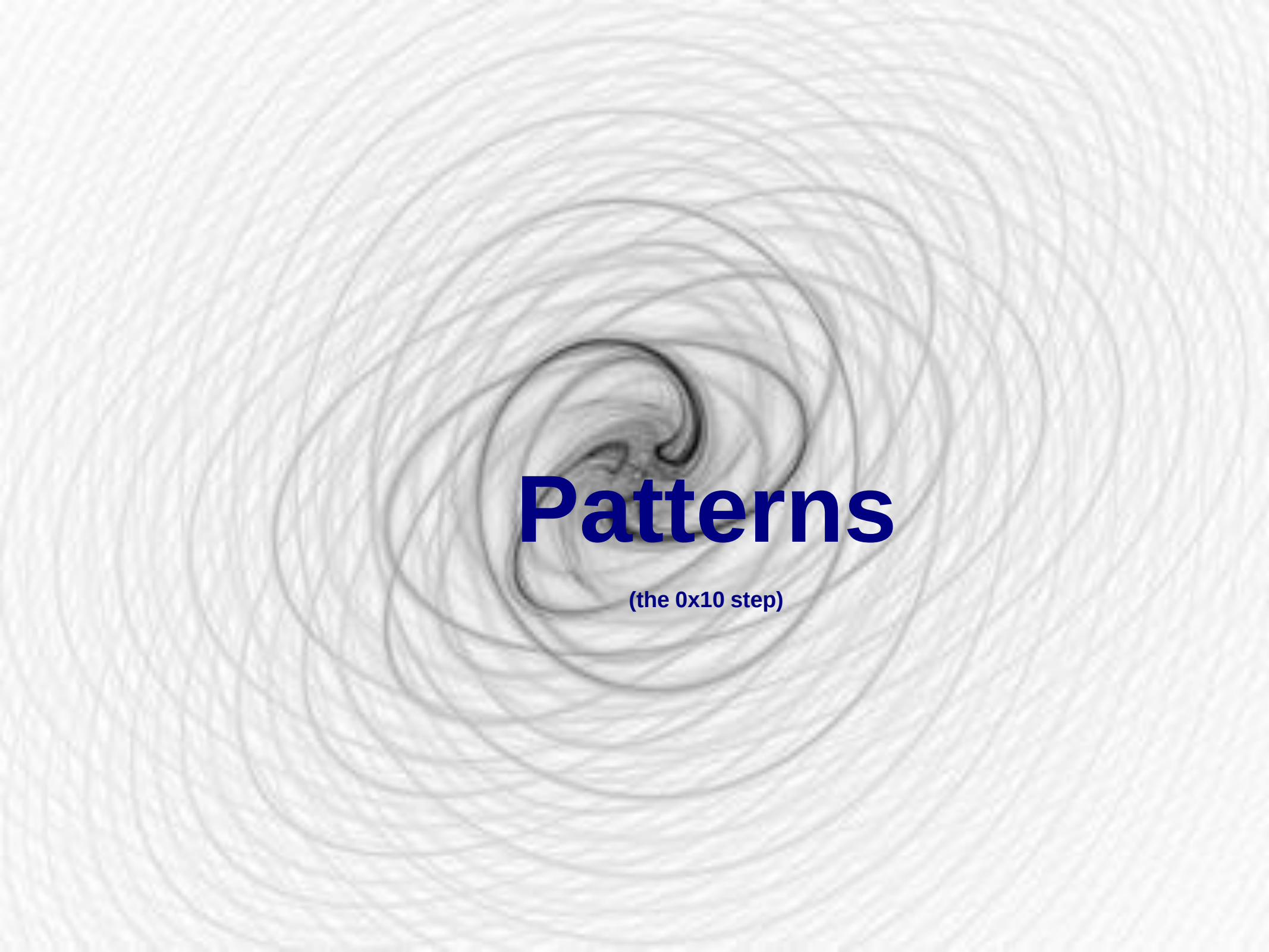

Cheat Engine 5.5
File Edit Process Help
000010B4-sqlservr.exe
Found: 6
Address Value
02C1145C 037EA040
037DC01C 037EA000
037EA044 037EA044
037EA048 037EA044
037EDFF8 037EA028
03890020 037EA000
New Scan
Next Scan
Settings
Value:
Hex
37ea000
and
Value:
37ea050
Scan type
Value between...
Value type
4 Bytes
Memory Scan Options
16-Bit
32-Bit
All
From
To
00400000
7FFFFFFF
Show
Also scan read-only memory
Fast scan
Hyper Scan
Pause the game while scanning
Unrandomizer
Enable Speedhack
Frozen
Description
Address
Type
Value
Advanced options

What did we get?

- A pointer to a table set in a global address (In the data section)
- All currently connected sessions
- A struct with information about every session, such as session id, user name, password...

Version proofed

- Everything is lost with each new update
  - Is it?
  - Hardly ever, because when they add something to a class / struct they add it to the end of it.
  - They hardly ever change the basic stuff
  - It just doesn't happen


Patterns
(the 0x10 step)

Automating Update Proof

- Lets say that there are changes in memory structures
  - The patterns survive
  - x86 vs AMD64 vs IA64 vs all the others

Candy

- Python environment to define memory patterns
  - Patterns of shape
    - **Name**
    - **Range**
    - **Data type**
    - **Extra check function**

Range

One of three:

1. End range *0x10*
2. (start, end) *(0x10, 0x20)*
3. (start, end, step) *(0x10, 0x20, 4)*

Data Types

- NUMBER (const value / range / enum, size)
- BUFFER (const value / anything goes, size)
- STRING (Nullterm, is_unicode, isPrintable, const value)
- TIME_STAMP(datetime)
- POINTER
- POINTER_TO_STRUCT
- STRUCT
- ARRAY

Shape example

```
SHAPE(
    "name",
    (0x10, 0x20),
    STRING(“SyScan") )
```

Example of pattern

```
          0         4         8         c
 0 205DB800 209E2800         3         0    ..] .(. ........
10         0         0 200B57C0   C52CA0    .........W. .,..
20   C52D15    45F189         0        3E   .-....E.....>...
30        33         0         1        41  3...........A...
40         B         0        41        41  ........A...A...
50     2E000    C60BFD         0    45E57C  ............|.E.
60         0         0         0    737350  ............Pss.
70         0         0         0         0  ................
80         0         0         0         0  ................
90         0  20606920  20606920  207EC8C0  .... i`  i` ..~
a0  209D2840  206068A4  206068A4  20606900  @(. .h` .h` .i`
b0        20      F2F0         1         0    ............
c0         2        21         0  209E2000  ....!....... .
d0  209E2000  209E2000    4BC8E4         0  . . . . ..K.....
e0         0         0         0        41  ............A...
f0         0         0         0         0  ................
```

Example of pattern

```
Pattern =
   [
     SHAPE("pssSlotsTable", 0x10000,
POINTER_TO_STRUCT(
        [
           SHAPE("next", 0, POINTER()),
           SHAPE("prev", 0, POINTER()),
           SHAPE("name", (0x40, 0x100), STRING("Pss"))
        ]
   ]

# Shape is (Name, Place, Data type, Extra check function)
```

Search on Windows 32bit

```
>>> pattern = [\
        SHAPE('pssSlotsTable', 0x10000, POINTER_TO_STRUCT( STRUCT([
                SHAPE('next', 0, POINTER()),
                SHAPE('prev', 0, POINTER()),
                SHAPE('name', (0x40,0x100), STRING(fixedValue='Pss', isPrintable=False))]))))]
>>> for i in search(pattern, RESOURCE):
        print i


pssSlotsTable: @2002f578 (offset: 00000258) value=553807872
next:   @21027000 (offset: 00000000) value=553631744
prev:   @21027004 (offset: 00000004) value=558133248
name:   @2102706c (offset: 0000006c) value='Pss'

>>>
```

How about Solaris SPARC 64bit?

```
>>> pattern = [\
...     SHAPE('pssSlotsTable', 0x10000, POINTER_TO_STRUCT( STRUCT([
...             SHAPE('next', 0, POINTER()),
...             SHAPE('prev', 0, POINTER()),
...             SHAPE('name', (0x40,0x100), STRING(fixedValue='Pss', i
>>> for i in search(pattern, RESOURCE):
...     print i
...

pssSlotsTable:  @1000001ed30 (offset: 00000430) value=1099538436096L
next:   @10001991000 (offset: 00000000) value=1099538253824L
prev:   @10001991008 (offset: 00000008) value=1099544035328L
name:   @10001991d0 (offset: 000000d0) value='Pss'

>>>
```

Example of complicated pattern

```
          0        4        8        c
 0        0        0        0        0   ................
10        0        1        0 20256090   ............`%
20 20255890       1FF 20A1E000 20ADF000   .X% ....... ...
30 20A1C000 20A1D000 204E8800        0   ... ... ..N ....
40        0        0        0        0   ................
50        0 204A6800 204A6960 204A6A10   .....hJ `iJ .jJ
60 204A6CB0 204A6E00 204A6ED0 204A6F70   .lJ .nJ .nJ poJ
70 204A7000 204A70C0 204A71E0 204A7230   .pJ .pJ .qJ 0rJ
```

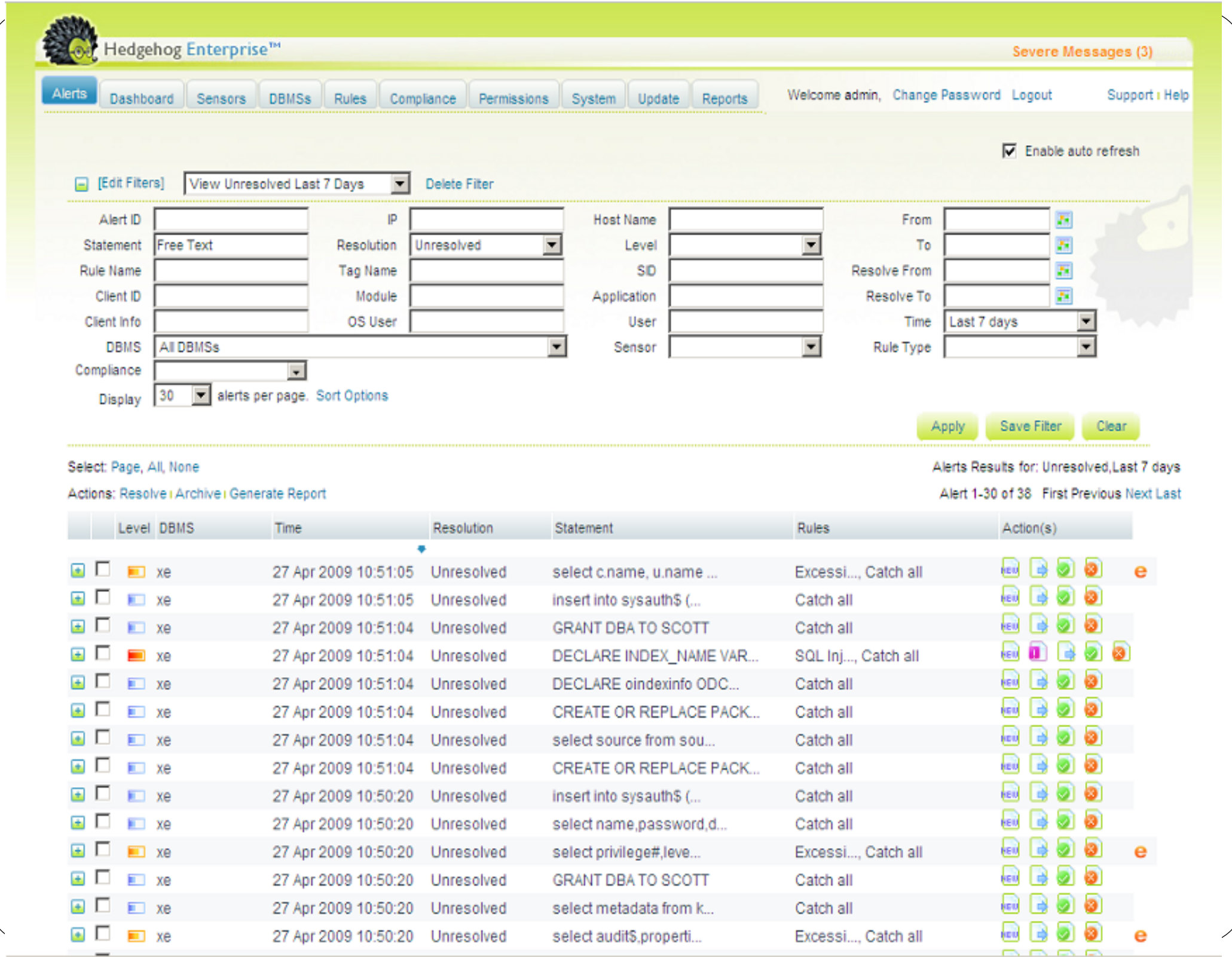
Pattern #2

```
Pattern = [
    SHAPE("cache", (0, 0x10000), STRUCT([
        SHAPE("table_size", 0, NUMBER((0x100, 0x100000))),
        SHAPE("table1",     0, POINTER()),
        SHAPE("table2",     0, POINTER(),
              extraCheck = lambda context:
                 context.table2 ==
                 context.table1 +
                 ((context.table_size + 1) * PSIZE))])))]

# Shape is (Name, Place, Data type, Extra check function)
```

The Real World

The Hedgehog connection

Database activity monitoring


Hedgehog Enterprise™
Severe Messages (3)
Alerts
Dashboard
Sensors
DBMSs
Rules
Compliance
Permissions
System
Update
Reports
Welcome admin, Change Password Logout
Support | Help
Enable auto refresh
[Edit Filters]
View Unresolved Last 7 Days
Delete Filter
Alert ID
IP
Host Name
From
Statement
Free Text
Resolution
Unresolved
Level
To
Rule Name
Tag Name
SID
Resolve From
Client ID
Module
Application
Resolve To
Client Info
OS User
User
Time
Last 7 days
DBMS
All DBMSs
Sensor
Rule Type
Compliance
Display
30
alerts per page.
Sort Options
Apply
Save Filter
Clear
Select: Page, All, None
Alerts Results for: Unresolved,Last 7 days
Actions: Resolve | Archive | Generate Report
Alert 1-30 of 38 First Previous Next Last
Level
DBMS
Time
Resolution
Statement
Rules
Action(s)
xe 27 Apr 2009 10:51:05 Unresolved select c.name, u.name ... Excessi..., Catch all
xe 27 Apr 2009 10:51:05 Unresolved insert into sysauth$ (... Catch all
xe 27 Apr 2009 10:51:04 Unresolved GRANT DBA TO SCOTT Catch all
xe 27 Apr 2009 10:51:04 Unresolved DECLARE INDEX_NAME VAR... SQL Inj..., Catch all
xe 27 Apr 2009 10:51:04 Unresolved DECLARE oindexinfo ODC... Catch all
xe 27 Apr 2009 10:51:04 Unresolved CREATE OR REPLACE PACK... Catch all
xe 27 Apr 2009 10:51:04 Unresolved select source from sou... Catch all
xe 27 Apr 2009 10:51:04 Unresolved CREATE OR REPLACE PACK... Catch all
xe 27 Apr 2009 10:50:20 Unresolved insert into sysauth$ (... Catch all
xe 27 Apr 2009 10:50:20 Unresolved select name,password,d... Catch all
xe 27 Apr 2009 10:50:20 Unresolved select privilege#,leve... Excessi..., Catch all
xe 27 Apr 2009 10:50:20 Unresolved GRANT DBA TO SCOTT Catch all
xe 27 Apr 2009 10:50:20 Unresolved select metadata from k... Catch all
xe 27 Apr 2009 10:50:20 Unresolved select audit$,properti... Excessi..., Catch all

Alert 32859000 (B) Details 25 Apr 2011 20:33:48

Sensor:	qa3-win2003.sentr...	Instance	qa3-win2003\SQL20...
Session ID:	54	Level	LOW
User:	sa	Application:	Microsoft SQL Server Management ...
Executing User:	sa	IP:	192.168.254.170
OS User:		Host Name:	STDIO
Action:		Terminal:	
CMD Type:	SELECT	Module:	
Log on time:	25 Apr 2011 20:33:48	Context Info:	

Statement:

```
SELECT dtb.collation_name AS [Collation], dtb.name AS [DatabaseName2]
FROM master.sys.databases AS dtb WHERE (dtb.name=@_msparam_0)
```

Rules: all

Accessed Objects:

Schema	Name	Type
master.DBO	DBPROP	TABLE
master.sys	sysdbreg	TABLE

Inflow SQL:

```
(@_msparam_0 nvarchar(4000))SELECT dtb.collation_name AS [Collation], dtb.name
AS [DatabaseName2] FROM master.sys.databases AS dtb WHERE
(dtb.name=@_msparam_0)
```

Inflow Objects:

Schema	Name	Type
master.sys	sysdbreg	TABLE
master.DBO	DBPROP	TABLE

Resolution: Unresolved

What's next?

- Open sourcing everything
  - http://code.google.com/p/pymint/
  - http://code.google.com/p/pycandy/
  - http://nativassaf.blogspot.com/2011/03/looking-into-eye-of-bits.html
- Add regex to mint
- Web Servers Monitoring
- Anti-Virus
- Flash debugger
- Drink some coffee...

FIN

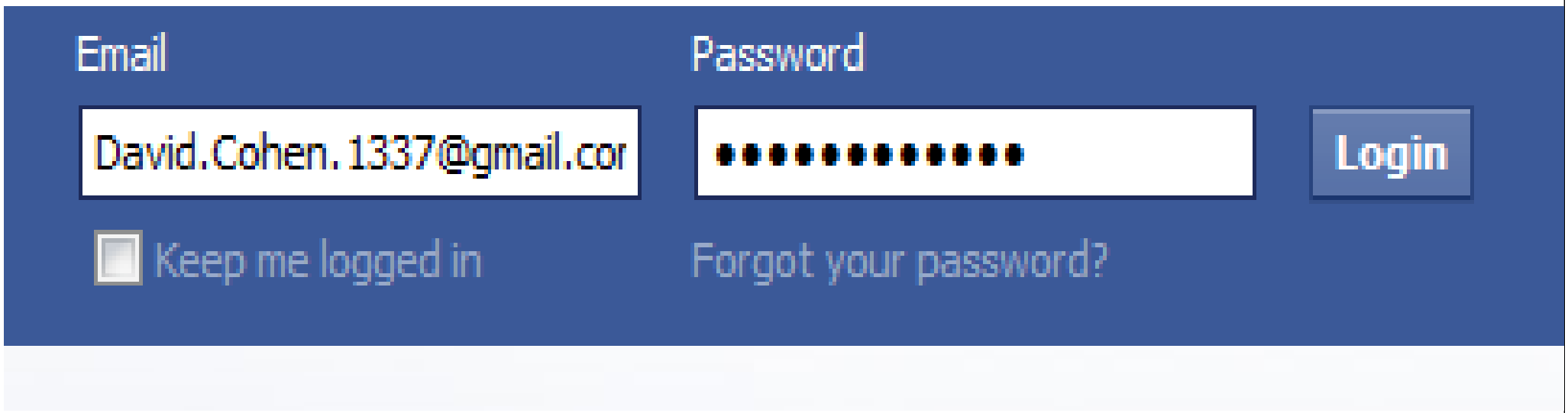
Questions?

Nativ.Assaf@gmail.com

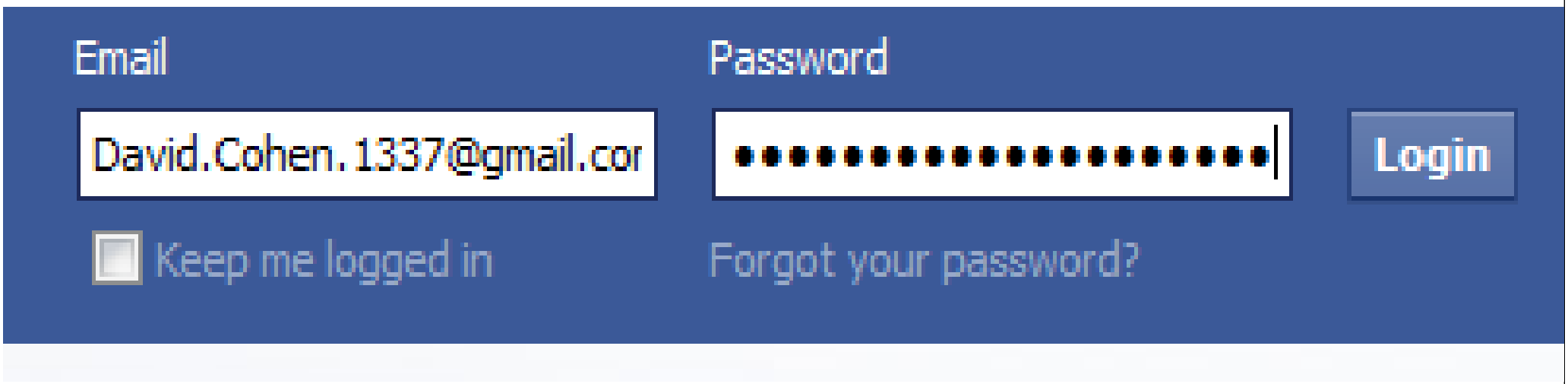
http://tinyurl.com/assafnativ

http://tinyurl.com/nativassaf

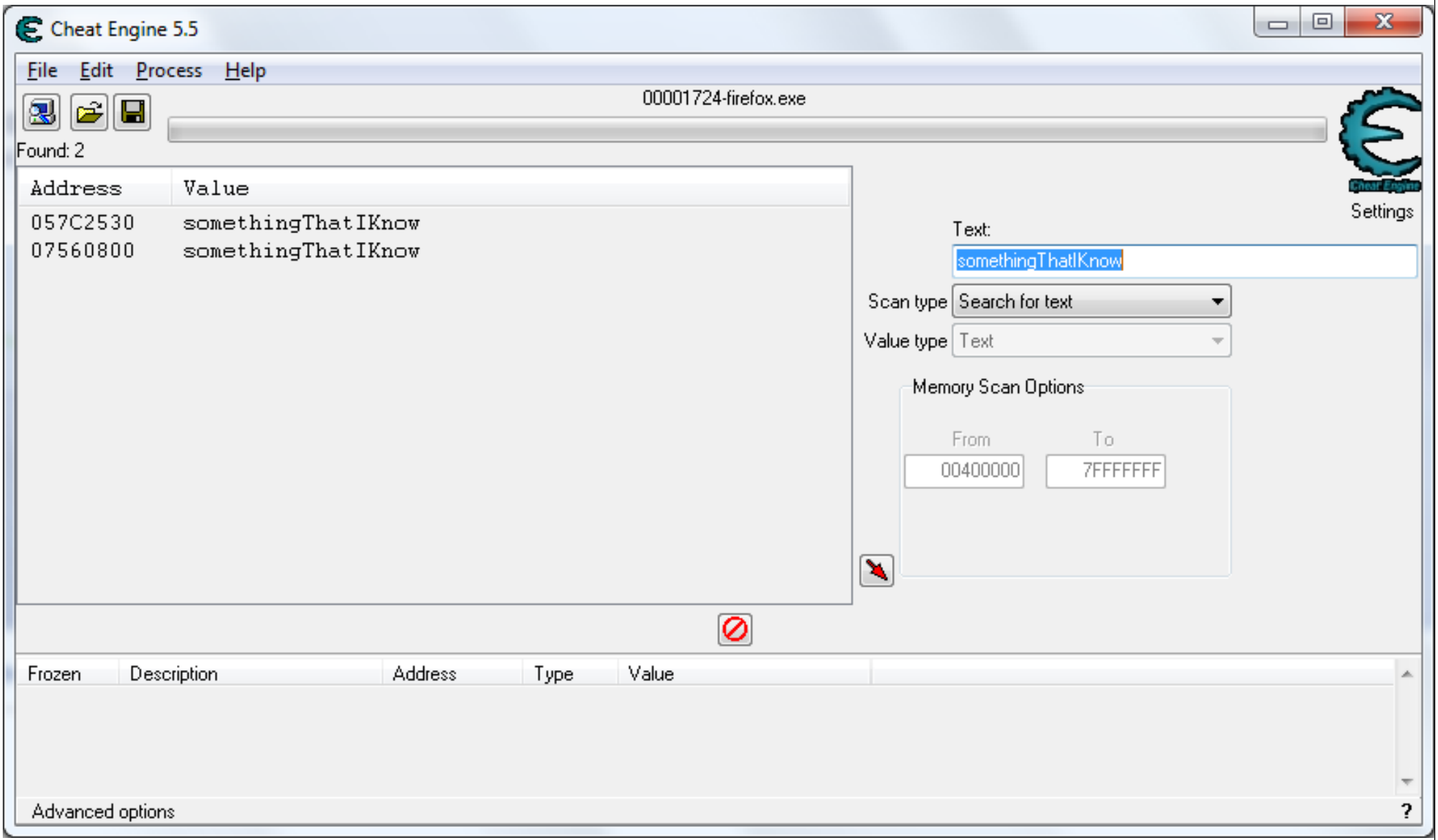
A trick to uncover asterisks passwords



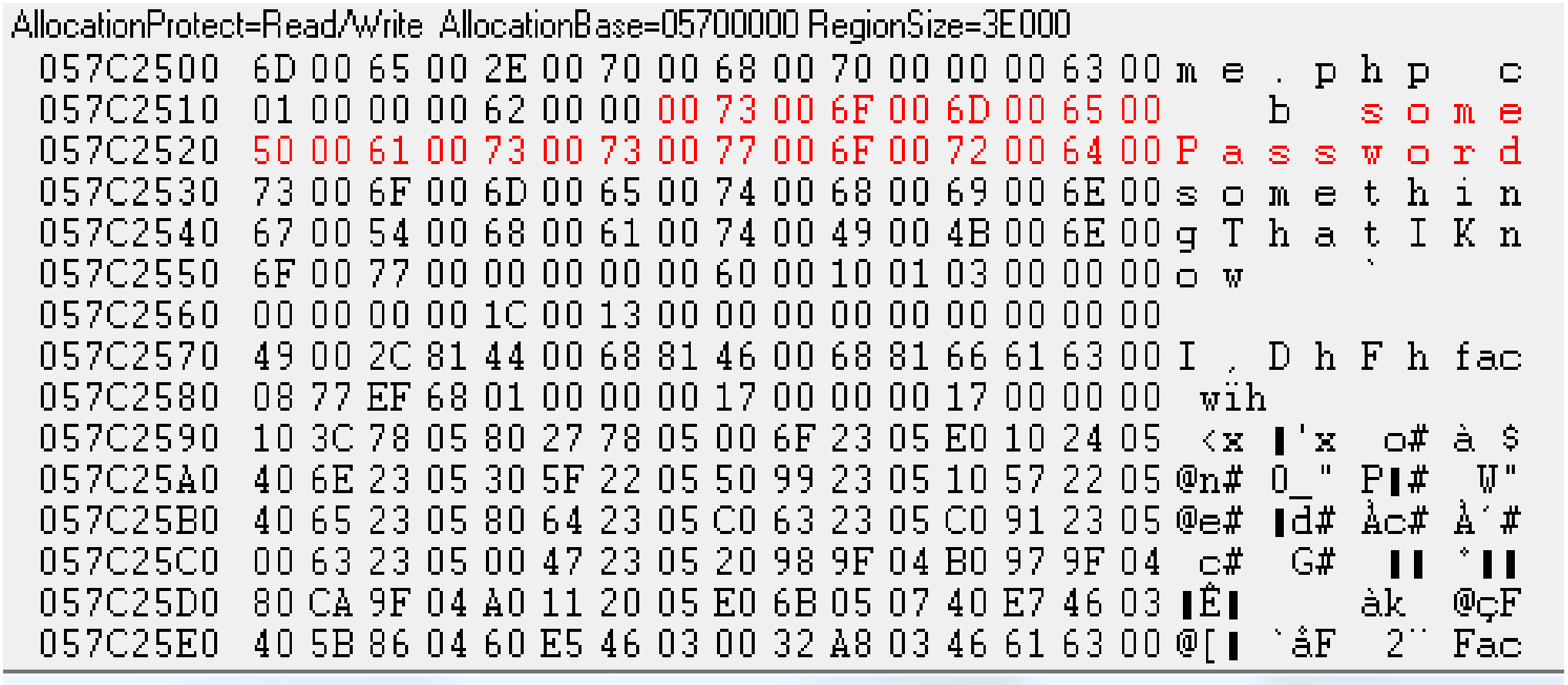
Step 2


Email
Password
David.Cohen.1337@gmail.cor
Login
Keep me logged in
Forgot your password?

Step 3


Cheat Engine 5.5
File Edit Process Help
00001724-firefox.exe
Found: 2
Address Value
057C2530 somethingThatIKnow
07560800 somethingThatIKnow
Settings
Text:
somethingThatIKnow
Scan type Search for text
Value type Text
Memory Scan Options
From
To
00400000
7FFFFFFF
Frozen Description Address Type Value
Advanced options

Step 4


AllocationProtect=Read/Write AllocationBase=05700000 RegionSize=3E000
057C2500 6D 00 65 00 2E 00 70 00 68 00 70 00 00 00 63 00 m e . p h p c
057C2510 01 00 00 00 62 00 00 00 73 00 6F 00 6D 00 65 00 b s o m e
057C2520 50 00 61 00 73 00 73 00 77 00 6F 00 72 00 64 00 P a s s w o r d
057C2530 73 00 6F 00 6D 00 65 00 74 00 68 00 69 00 6E 00 s o m e t h i n
057C2540 67 00 54 00 68 00 61 00 74 00 49 00 4B 00 6E 00 g T h a t I K n
057C2550 6F 00 77 00 00 00 00 00 60 00 10 01 03 00 00 00 o w `
057C2560 00 00 00 00 1C 00 13 00 00 00 00 00 00 00 00 00
057C2570 49 00 2C 81 44 00 68 81 46 00 68 81 66 61 63 00 I , D h F h fac
057C2580 08 77 EF 68 01 00 00 00 17 00 00 00 17 00 00 00 wïh
057C2590 10 3C 78 05 80 27 78 05 00 6F 23 05 E0 10 24 05 <x 'x o# à $
057C25A0 40 6E 23 05 30 5F 22 05 50 99 23 05 10 57 22 05 @n# 0_" P# W"
057C25B0 40 65 23 05 80 64 23 05 C0 63 23 05 C0 91 23 05 @e# d# Àc# À'#
057C25C0 00 63 23 05 00 47 23 05 20 98 9F 04 B0 97 9F 04 c# G# ° °
057C25D0 80 CA 9F 04 A0 11 20 05 E0 6B 05 07 40 E7 46 03 Ê à k @çF
057C25E0 40 5B 86 04 60 E5 46 03 00 32 A8 03 46 61 63 00 @[`åF 2¨ Fac

10x

Nativ.Assaf@gmail.com
http://tinyurl.com/assafnativ
http://tinyurl.com/nativassaf