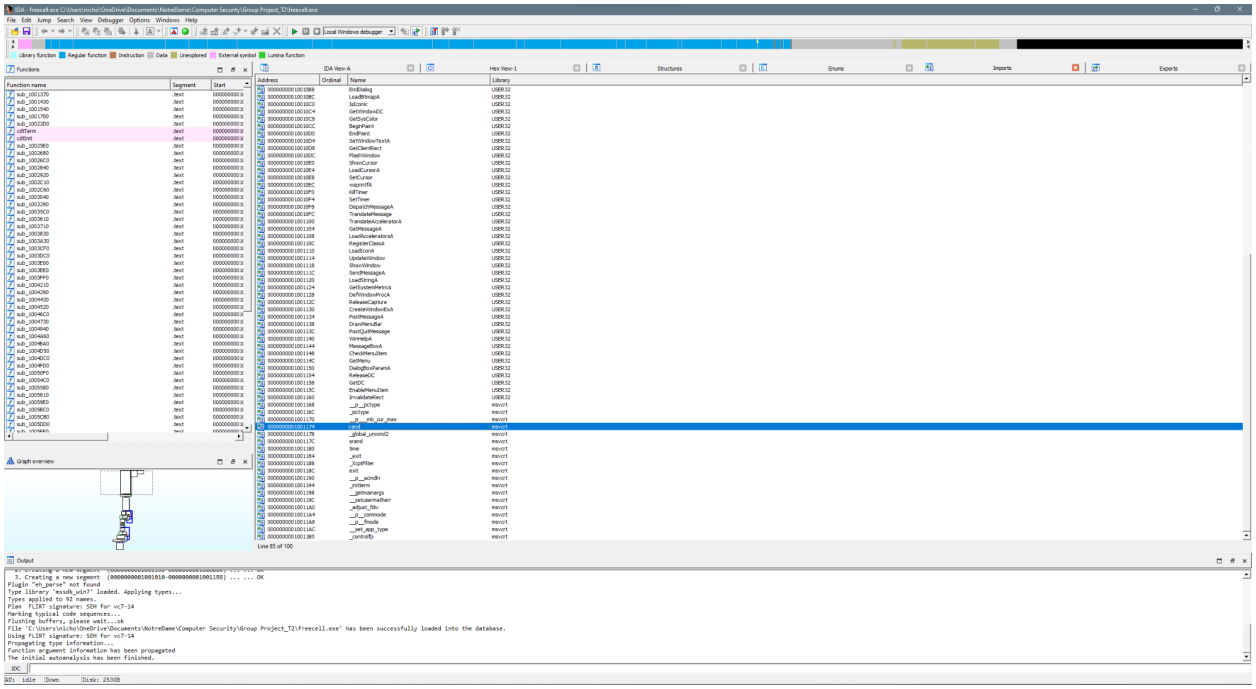
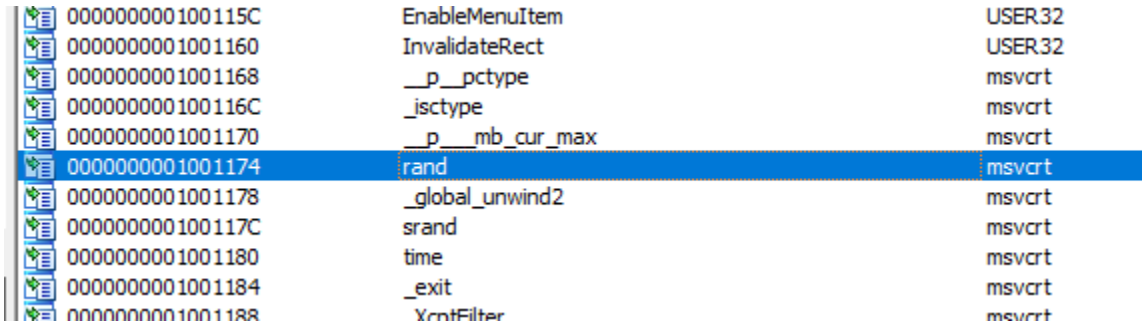
Part 1: Find the cards.

This document shares how our group found the cards in memory:

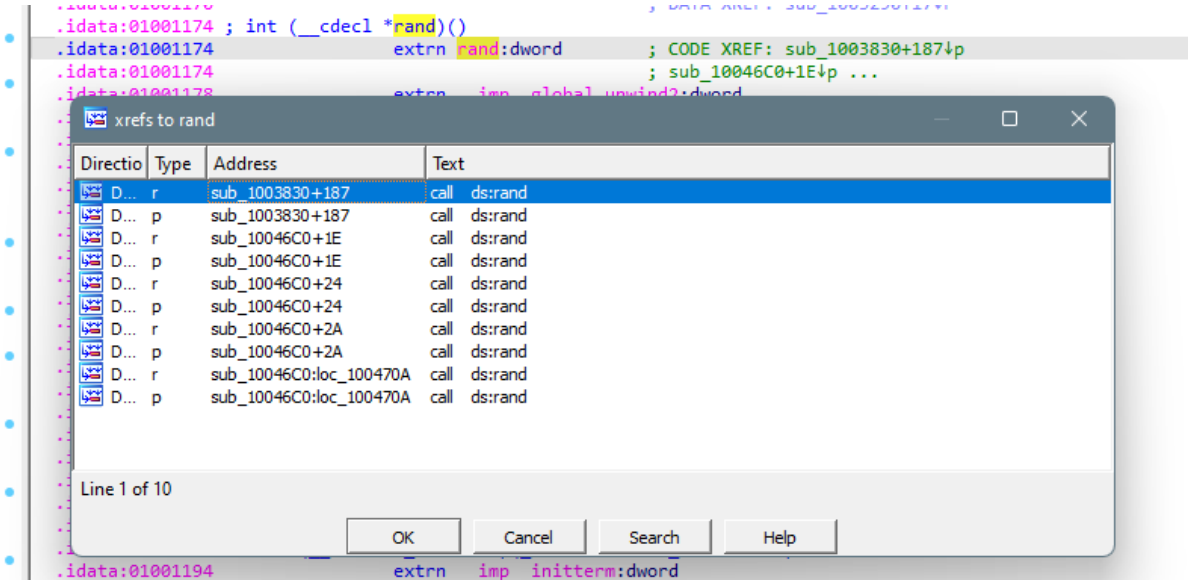
1. **Locate the rand function in IDA**
    a. As each game randomly places all the cards, it makes sense that the cards would be generated near a rand function



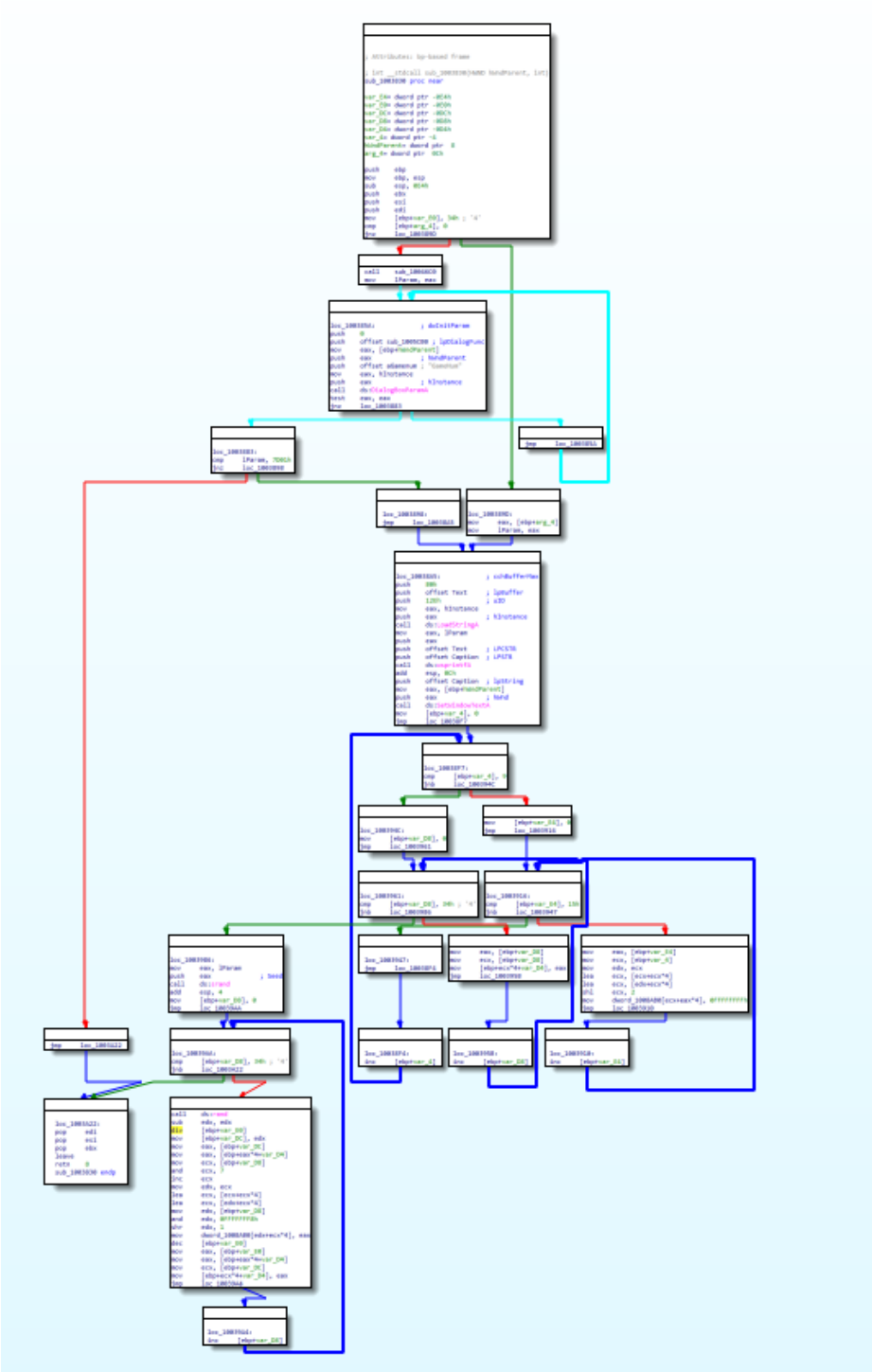
=>



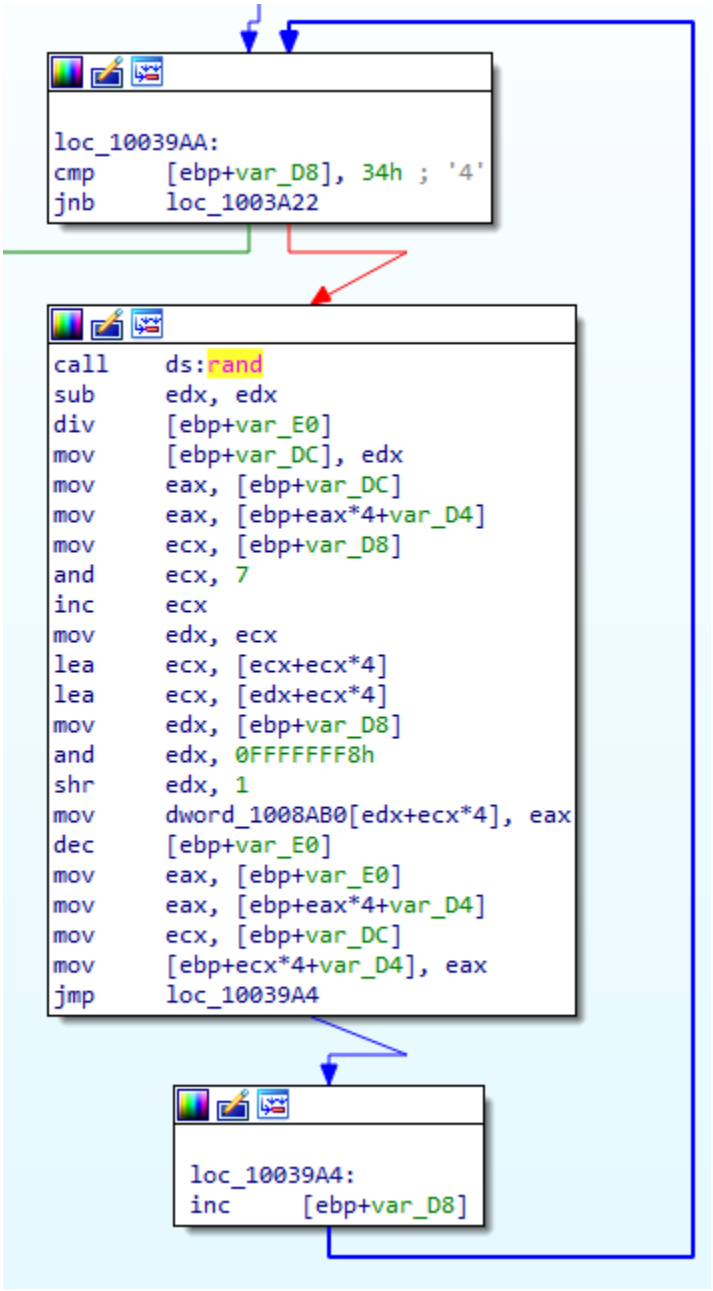
2. Find where rand is called using xrefs



3. **Clicking on the first entry above we are brought to the following code**



… which contains the following loop:



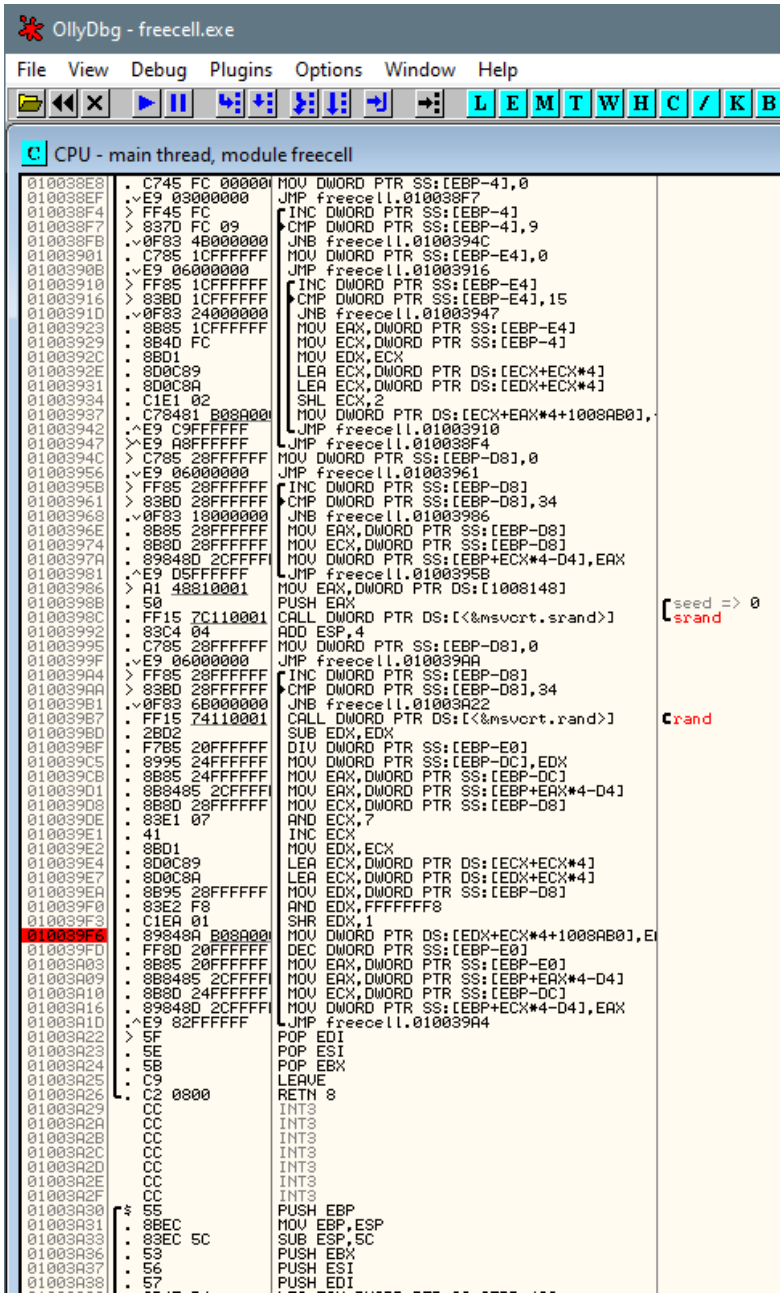
… notice this loop continues “34h” times which is 52 in decimal. Also, it calls the rand function at the top. This seems like a place where cards are being generated.

4. **Specifically, after analyzing the code it appears the card is being placed into dword_1008AB0. This instruction occurs at 010039F6:**

```
mov     dword_1008AB0[edx+ecx*4], eax
```

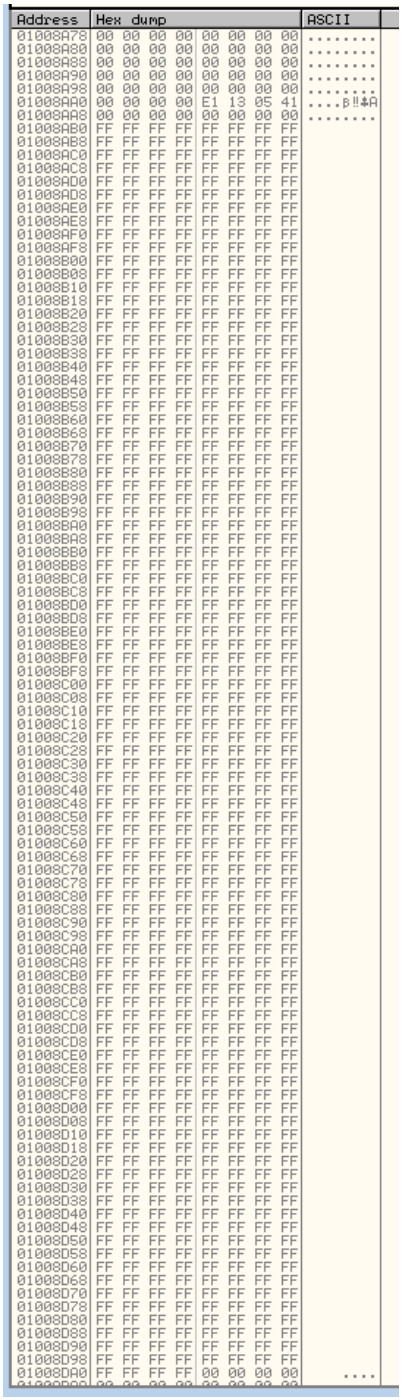
```
100.00% (2,1688) (365,934) 000039F6 00000000010039F6: sub_1003830+1C6 (Synchronized with Hex View-1)
```

5. **Moving to OllyDbg we go to that instruction and set a breakpoint**



… as we expect it occurs near the call to rand.

6. **When we run Freecell with this breakpoint you will notice that a large area of memory is free:**



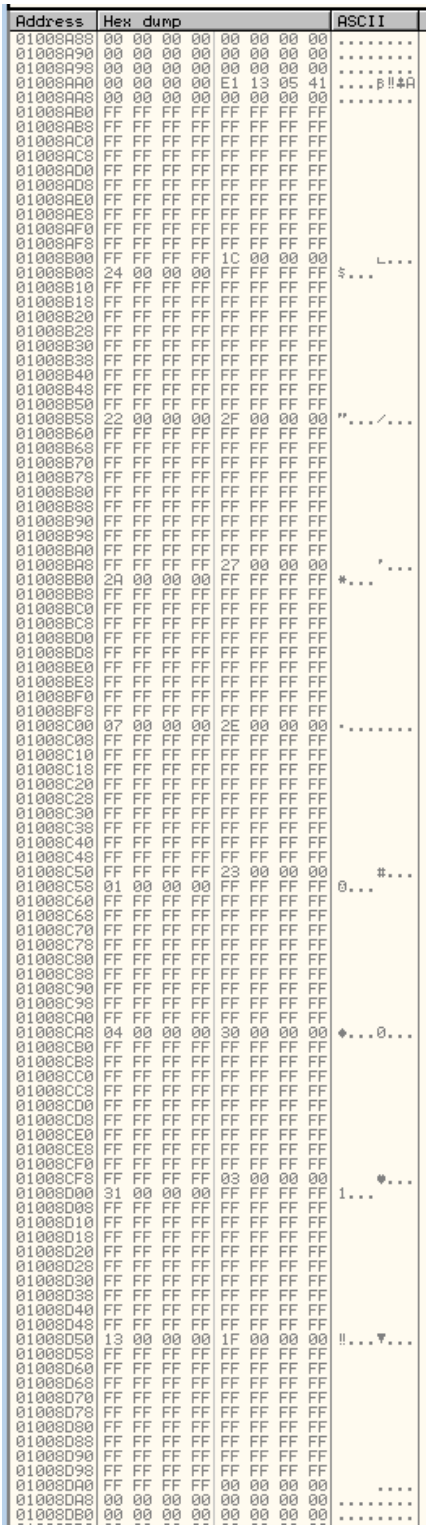
Address	Hex dump	ASCII
01008A78	00 00 00 00 00 00 00 00	....
01008A80	00 00 00 00 00 00 00 00	....
01008A88	00 00 00 00 00 00 00 00	....
01008A90	00 00 00 00 00 00 00 00	....
01008A98	00 00 00 00 00 00 00 00	....
01008AA0	00 00 00 00 E1 13 05 41	....ß‼♣A
01008AA8	00 00 00 00 00 00 00 00	....
01008AB0	FF FF FF FF FF FF FF FF	
01008AB8	FF FF FF FF FF FF FF FF	
01008AC0	FF FF FF FF FF FF FF FF	
01008AC8	FF FF FF FF FF FF FF FF	
01008AD0	FF FF FF FF FF FF FF FF	
01008AD8	FF FF FF FF FF FF FF FF	
01008AE0	FF FF FF FF FF FF FF FF	
01008AE8	FF FF FF FF FF FF FF FF	
01008AF0	FF FF FF FF FF FF FF FF	
01008AF8	FF FF FF FF FF FF FF FF	
01008B00	FF FF FF FF FF FF FF FF	
01008B08	FF FF FF FF FF FF FF FF	
01008B10	FF FF FF FF FF FF FF FF	
01008B18	FF FF FF FF FF FF FF FF	
01008B20	FF FF FF FF FF FF FF FF	
01008B28	FF FF FF FF FF FF FF FF	
01008B30	FF FF FF FF FF FF FF FF	
01008B38	FF FF FF FF FF FF FF FF	
01008B40	FF FF FF FF FF FF FF FF	
01008B48	FF FF FF FF FF FF FF FF	
01008B50	FF FF FF FF FF FF FF FF	
01008B58	FF FF FF FF FF FF FF FF	
01008B60	FF FF FF FF FF FF FF FF	
01008B68	FF FF FF FF FF FF FF FF	
01008B70	FF FF FF FF FF FF FF FF	
01008B78	FF FF FF FF FF FF FF FF	
01008B80	FF FF FF FF FF FF FF FF	
01008B88	FF FF FF FF FF FF FF FF	
01008B90	FF FF FF FF FF FF FF FF	
01008B98	FF FF FF FF FF FF FF FF	
01008BA0	FF FF FF FF FF FF FF FF	
01008BA8	FF FF FF FF FF FF FF FF	
01008BB0	FF FF FF FF FF FF FF FF	
01008BB8	FF FF FF FF FF FF FF FF	
01008BC0	FF FF FF FF FF FF FF FF	
01008BC8	FF FF FF FF FF FF FF FF	
01008BD0	FF FF FF FF FF FF FF FF	
01008BD8	FF FF FF FF FF FF FF FF	
01008BE0	FF FF FF FF FF FF FF FF	
01008BE8	FF FF FF FF FF FF FF FF	
01008BF0	FF FF FF FF FF FF FF FF	
01008BF8	FF FF FF FF FF FF FF FF	
01008C00	FF FF FF FF FF FF FF FF	
01008C08	FF FF FF FF FF FF FF FF	
01008C10	FF FF FF FF FF FF FF FF	
01008C18	FF FF FF FF FF FF FF FF	
01008C20	FF FF FF FF FF FF FF FF	
01008C28	FF FF FF FF FF FF FF FF	
01008C30	FF FF FF FF FF FF FF FF	
01008C38	FF FF FF FF FF FF FF FF	
01008C40	FF FF FF FF FF FF FF FF	
01008C48	FF FF FF FF FF FF FF FF	
01008C50	FF FF FF FF FF FF FF FF	
01008C58	FF FF FF FF FF FF FF FF	
01008C60	FF FF FF FF FF FF FF FF	
01008C68	FF FF FF FF FF FF FF FF	
01008C70	FF FF FF FF FF FF FF FF	
01008C78	FF FF FF FF FF FF FF FF	
01008C80	FF FF FF FF FF FF FF FF	
01008C88	FF FF FF FF FF FF FF FF	
01008C90	FF FF FF FF FF FF FF FF	
01008C98	FF FF FF FF FF FF FF FF	
01008CA0	FF FF FF FF FF FF FF FF	
01008CA8	FF FF FF FF FF FF FF FF	
01008CB0	FF FF FF FF FF FF FF FF	
01008CB8	FF FF FF FF FF FF FF FF	
01008CC0	FF FF FF FF FF FF FF FF	
01008CC8	FF FF FF FF FF FF FF FF	
01008CD0	FF FF FF FF FF FF FF FF	
01008CD8	FF FF FF FF FF FF FF FF	
01008CE0	FF FF FF FF FF FF FF FF	
01008CE8	FF FF FF FF FF FF FF FF	
01008CF0	FF FF FF FF FF FF FF FF	
01008CF8	FF FF FF FF FF FF FF FF	
01008D00	FF FF FF FF FF FF FF FF	
01008D08	FF FF FF FF FF FF FF FF	
01008D10	FF FF FF FF FF FF FF FF	
01008D18	FF FF FF FF FF FF FF FF	
01008D20	FF FF FF FF FF FF FF FF	
01008D28	FF FF FF FF FF FF FF FF	
01008D30	FF FF FF FF FF FF FF FF	
01008D38	FF FF FF FF FF FF FF FF	
01008D40	FF FF FF FF FF FF FF FF	
01008D48	FF FF FF FF FF FF FF FF	
01008D50	FF FF FF FF FF FF FF FF	
01008D58	FF FF FF FF FF FF FF FF	
01008D60	FF FF FF FF FF FF FF FF	
01008D68	FF FF FF FF FF FF FF FF	
01008D70	FF FF FF FF FF FF FF FF	
01008D78	FF FF FF FF FF FF FF FF	
01008D80	FF FF FF FF FF FF FF FF	
01008D88	FF FF FF FF FF FF FF FF	
01008D90	FF FF FF FF FF FF FF FF	
01008D98	FF FF FF FF FF FF FF FF	
01008DA0	FF FF FF FF 00 00 00 00	....

… as we hit run to execute one loop, the memory begins to fill in:

After 1 loop:

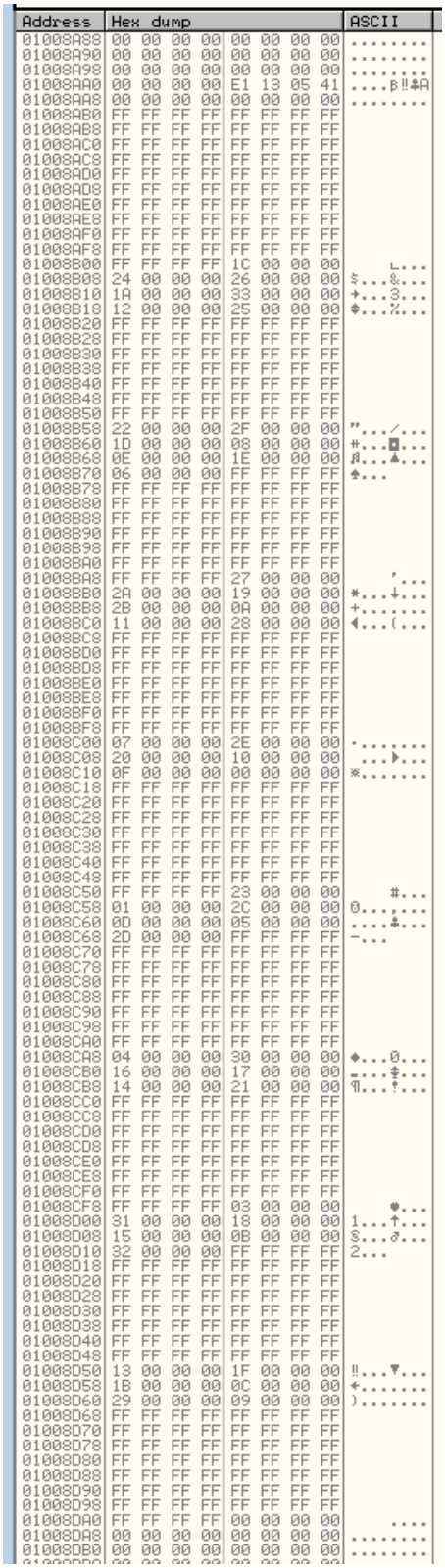
Address	Hex dump	ASCII
01008A88	00 00 00 00 00 00 00 00	....
01008A90	00 00 00 00 00 00 00 00	....
01008A98	00 00 00 00 00 00 00 00	....
01008AA0	00 00 00 00 E1 13 05 41	....ß‼♣A
01008AA8	00 00 00 00 00 00 00 00	....
01008AB0	FF FF FF FF FF FF FF FF	
01008AB8	FF FF FF FF FF FF FF FF	
01008AC0	FF FF FF FF FF FF FF FF	
01008AC8	FF FF FF FF FF FF FF FF	
01008AD0	FF FF FF FF FF FF FF FF	
01008AD8	FF FF FF FF FF FF FF FF	
01008AE0	FF FF FF FF FF FF FF FF	
01008AE8	FF FF FF FF FF FF FF FF	
01008AF0	FF FF FF FF FF FF FF FF	
01008AF8	FF FF FF FF FF FF FF FF	
01008B00	FF FF FF FF 1C 00 00 00	└...
01008B08	FF FF FF FF FF FF FF FF	
01008B10	FF FF FF FF FF FF FF FF	
01008B18	FF FF FF FF FF FF FF FF	
01008B20	FF FF FF FF FF FF FF FF	
01008B28	FF FF FF FF FF FF FF FF	
01008B30	FF FF FF FF FF FF FF FF	
01008B38	FF FF FF FF FF FF FF FF	
01008B40	FF FF FF FF FF FF FF FF	
01008B48	FF FF FF FF FF FF FF FF	
01008B50	FF FF FF FF FF FF FF FF	
01008B58	FF FF FF FF FF FF FF FF	
01008B60	FF FF FF FF FF FF FF FF	
01008B68	FF FF FF FF FF FF FF FF	
01008B70	FF FF FF FF FF FF FF FF	
01008B78	FF FF FF FF FF FF FF FF	
01008B80	FF FF FF FF FF FF FF FF	
01008B88	FF FF FF FF FF FF FF FF	
01008B90	FF FF FF FF FF FF FF FF	
01008B98	FF FF FF FF FF FF FF FF	
01008BA0	FF FF FF FF FF FF FF FF	
01008BA8	FF FF FF FF FF FF FF FF	
01008BB0	FF FF FF FF FF FF FF FF	
01008BB8	FF FF FF FF FF FF FF FF	
01008BC0	FF FF FF FF FF FF FF FF	
01008BC8	FF FF FF FF FF FF FF FF	
01008BD0	FF FF FF FF FF FF FF FF	
01008BD8	FF FF FF FF FF FF FF FF	
01008BE0	FF FF FF FF FF FF FF FF	
01008BE8	FF FF FF FF FF FF FF FF	
01008BF0	FF FF FF FF FF FF FF FF	
01008BF8	FF FF FF FF FF FF FF FF	
01008C00	FF FF FF FF FF FF FF FF	
01008C08	FF FF FF FF FF FF FF FF	
01008C10	FF FF FF FF FF FF FF FF	
01008C18	FF FF FF FF FF FF FF FF	
01008C20	FF FF FF FF FF FF FF FF	
01008C28	FF FF FF FF FF FF FF FF	
01008C30	FF FF FF FF FF FF FF FF	
01008C38	FF FF FF FF FF FF FF FF	
01008C40	FF FF FF FF FF FF FF FF	
01008C48	FF FF FF FF FF FF FF FF	
01008C50	FF FF FF FF FF FF FF FF	
01008C58	FF FF FF FF FF FF FF FF	
01008C60	FF FF FF FF FF FF FF FF	
01008C68	FF FF FF FF FF FF FF FF	
01008C70	FF FF FF FF FF FF FF FF	
01008C78	FF FF FF FF FF FF FF FF	
01008C80	FF FF FF FF FF FF FF FF	
01008C88	FF FF FF FF FF FF FF FF	
01008C90	FF FF FF FF FF FF FF FF	
01008C98	FF FF FF FF FF FF FF FF	
01008CA0	FF FF FF FF FF FF FF FF	
01008CA8	FF FF FF FF FF FF FF FF	
01008CB0	FF FF FF FF FF FF FF FF	
01008CB8	FF FF FF FF FF FF FF FF	
01008CC0	FF FF FF FF FF FF FF FF	
01008CC8	FF FF FF FF FF FF FF FF	
01008CD0	FF FF FF FF FF FF FF FF	
01008CD8	FF FF FF FF FF FF FF FF	
01008CE0	FF FF FF FF FF FF FF FF	
01008CE8	FF FF FF FF FF FF FF FF	
01008CF0	FF FF FF FF FF FF FF FF	
01008CF8	FF FF FF FF FF FF FF FF	
01008D00	FF FF FF FF FF FF FF FF	
01008D08	FF FF FF FF FF FF FF FF	
01008D10	FF FF FF FF FF FF FF FF	
01008D18	FF FF FF FF FF FF FF FF	
01008D20	FF FF FF FF FF FF FF FF	
01008D28	FF FF FF FF FF FF FF FF	
01008D30	FF FF FF FF FF FF FF FF	
01008D38	FF FF FF FF FF FF FF FF	
01008D40	FF FF FF FF FF FF FF FF	
01008D48	FF FF FF FF FF FF FF FF	
01008D50	FF FF FF FF FF FF FF FF	
01008D58	FF FF FF FF FF FF FF FF	
01008D60	FF FF FF FF FF FF FF FF	
01008D68	FF FF FF FF FF FF FF FF	
01008D70	FF FF FF FF FF FF FF FF	
01008D78	FF FF FF FF FF FF FF FF	
01008D80	FF FF FF FF FF FF FF FF	
01008D88	FF FF FF FF FF FF FF FF	
01008D90	FF FF FF FF FF FF FF FF	
01008D98	FF FF FF FF FF FF FF FF	
01008DA0	FF FF FF FF 00 00 00 00	....
01008DA8	00 00 00 00 00 00 00 00	....
01008DB0	00 00 00 00 00 00 00 00	....

After 15 more loops:



Address	Hex dump	ASCII
01008A88	00 00 00 00 00 00 00 00	....
01008A90	00 00 00 00 00 00 00 00	....
01008A98	00 00 00 00 00 00 00 00	....
01008AA0	00 00 00 00 E1 13 05 41	....ß‼♣A
01008AA8	00 00 00 00 00 00 00 00	....
01008AB0	FF FF FF FF FF FF FF FF	
01008AB8	FF FF FF FF FF FF FF FF	
01008AC0	FF FF FF FF FF FF FF FF	
01008AC8	FF FF FF FF FF FF FF FF	
01008AD0	FF FF FF FF FF FF FF FF	
01008AD8	FF FF FF FF FF FF FF FF	
01008AE0	FF FF FF FF FF FF FF FF	
01008AE8	FF FF FF FF FF FF FF FF	
01008AF0	FF FF FF FF FF FF FF FF	
01008AF8	FF FF FF FF FF FF FF FF	
01008B00	FF FF FF FF 1C 00 00 00	␣...
01008B08	24 00 00 00 FF FF FF FF	$...
01008B10	FF FF FF FF FF FF FF FF	
01008B18	FF FF FF FF FF FF FF FF	
01008B20	FF FF FF FF FF FF FF FF	
01008B28	FF FF FF FF FF FF FF FF	
01008B30	FF FF FF FF FF FF FF FF	
01008B38	FF FF FF FF FF FF FF FF	
01008B40	FF FF FF FF FF FF FF FF	
01008B48	FF FF FF FF FF FF FF FF	
01008B50	FF FF FF FF FF FF FF FF	
01008B58	22 00 00 00 2F 00 00 00	".../...
01008B60	FF FF FF FF FF FF FF FF	
01008B68	FF FF FF FF FF FF FF FF	
01008B70	FF FF FF FF FF FF FF FF	
01008B78	FF FF FF FF FF FF FF FF	
01008B80	FF FF FF FF FF FF FF FF	
01008B88	FF FF FF FF FF FF FF FF	
01008B90	FF FF FF FF FF FF FF FF	
01008B98	FF FF FF FF FF FF FF FF	
01008BA0	FF FF FF FF FF FF FF FF	
01008BA8	FF FF FF FF 27 00 00 00	'...
01008BB0	2A 00 00 00 FF FF FF FF	*...
01008BB8	FF FF FF FF FF FF FF FF	
01008BC0	FF FF FF FF FF FF FF FF	
01008BC8	FF FF FF FF FF FF FF FF	
01008BD0	FF FF FF FF FF FF FF FF	
01008BD8	FF FF FF FF FF FF FF FF	
01008BE0	FF FF FF FF FF FF FF FF	
01008BE8	FF FF FF FF FF FF FF FF	
01008BF0	FF FF FF FF FF FF FF FF	
01008BF8	FF FF FF FF FF FF FF FF	
01008C00	07 00 00 00 2E 00 00 00	•.......
01008C08	FF FF FF FF FF FF FF FF	
01008C10	FF FF FF FF FF FF FF FF	
01008C18	FF FF FF FF FF FF FF FF	
01008C20	FF FF FF FF FF FF FF FF	
01008C28	FF FF FF FF FF FF FF FF	
01008C30	FF FF FF FF FF FF FF FF	
01008C38	FF FF FF FF FF FF FF FF	
01008C40	FF FF FF FF FF FF FF FF	
01008C48	FF FF FF FF FF FF FF FF	
01008C50	FF FF FF FF 23 00 00 00	#...
01008C58	01 00 00 00 FF FF FF FF	☺...
01008C60	FF FF FF FF FF FF FF FF	
01008C68	FF FF FF FF FF FF FF FF	
01008C70	FF FF FF FF FF FF FF FF	
01008C78	FF FF FF FF FF FF FF FF	
01008C80	FF FF FF FF FF FF FF FF	
01008C88	FF FF FF FF FF FF FF FF	
01008C90	FF FF FF FF FF FF FF FF	
01008C98	FF FF FF FF FF FF FF FF	
01008CA0	FF FF FF FF FF FF FF FF	
01008CA8	04 00 00 00 30 00 00 00	♦...0...
01008CB0	FF FF FF FF FF FF FF FF	
01008CB8	FF FF FF FF FF FF FF FF	
01008CC0	FF FF FF FF FF FF FF FF	
01008CC8	FF FF FF FF FF FF FF FF	
01008CD0	FF FF FF FF FF FF FF FF	
01008CD8	FF FF FF FF FF FF FF FF	
01008CE0	FF FF FF FF FF FF FF FF	
01008CE8	FF FF FF FF FF FF FF FF	
01008CF0	FF FF FF FF FF FF FF FF	
01008CF8	FF FF FF FF 03 00 00 00	♥...
01008D00	31 00 00 00 FF FF FF FF	1...
01008D08	FF FF FF FF FF FF FF FF	
01008D10	FF FF FF FF FF FF FF FF	
01008D18	FF FF FF FF FF FF FF FF	
01008D20	FF FF FF FF FF FF FF FF	
01008D28	FF FF FF FF FF FF FF FF	
01008D30	FF FF FF FF FF FF FF FF	
01008D38	FF FF FF FF FF FF FF FF	
01008D40	FF FF FF FF FF FF FF FF	
01008D48	FF FF FF FF FF FF FF FF	
01008D50	13 00 00 00 1F 00 00 00	‼...▼...
01008D58	FF FF FF FF FF FF FF FF	
01008D60	FF FF FF FF FF FF FF FF	
01008D68	FF FF FF FF FF FF FF FF	
01008D70	FF FF FF FF FF FF FF FF	
01008D78	FF FF FF FF FF FF FF FF	
01008D80	FF FF FF FF FF FF FF FF	
01008D88	FF FF FF FF FF FF FF FF	
01008D90	FF FF FF FF FF FF FF FF	
01008D98	FF FF FF FF FF FF FF FF	
01008DA0	FF FF FF FF 00 00 00 00	....
01008DA8	00 00 00 00 00 00 00 00	....
01008DB0	00 00 00 00 00 00 00 00	....

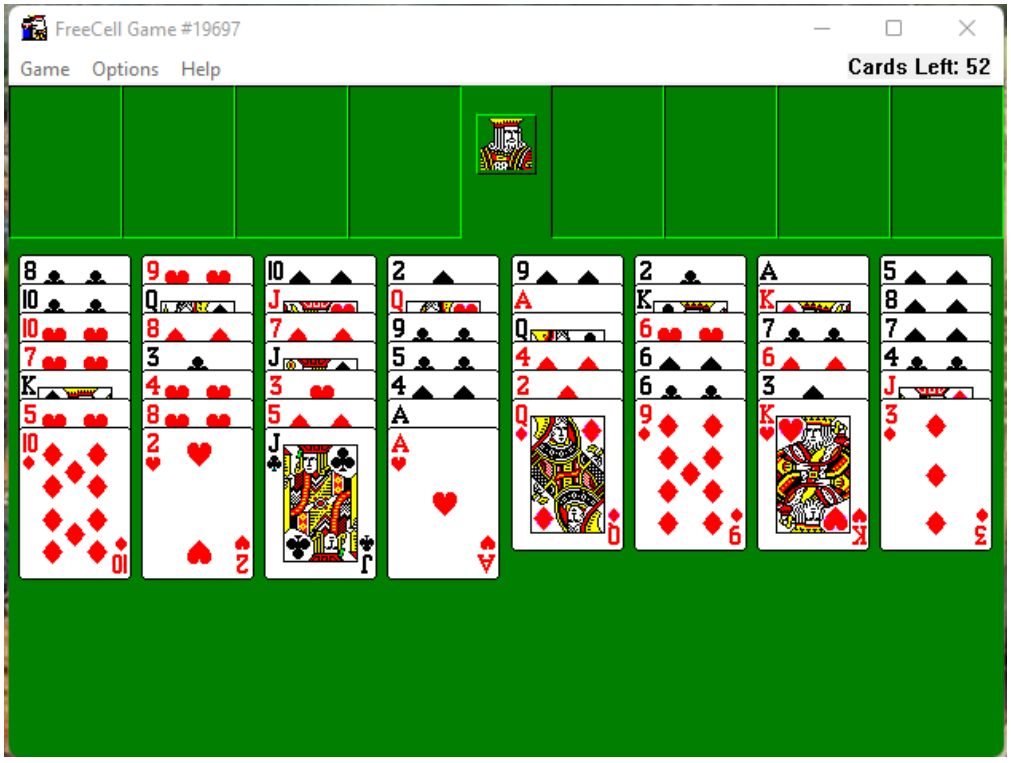
… finally after 52 loops the memory is filled with 52 hex values that represent the cards



Address	Hex dump	ASCII
01008A88	00 00 00 00 00 00 00 00	....
01008A90	00 00 00 00 00 00 00 00	....
01008A98	00 00 00 00 00 00 00 00	....
01008AA0	00 00 00 00 E1 13 05 41	....ß‼♣A
01008AA8	00 00 00 00 00 00 00 00	....
01008AB0	FF FF FF FF FF FF FF FF	
01008AB8	FF FF FF FF FF FF FF FF	
01008AC0	FF FF FF FF FF FF FF FF	
01008AC8	FF FF FF FF FF FF FF FF	
01008AD0	FF FF FF FF FF FF FF FF	
01008AD8	FF FF FF FF FF FF FF FF	
01008AE0	FF FF FF FF FF FF FF FF	
01008AE8	FF FF FF FF FF FF FF FF	
01008AF0	FF FF FF FF FF FF FF FF	
01008AF8	FF FF FF FF FF FF FF FF	
01008B00	FF FF FF FF 1C 00 00 00	....∟...
01008B08	24 00 00 00 26 00 00 00	$...&...
01008B10	1A 00 00 00 33 00 00 00	→...3...
01008B18	12 00 00 00 25 00 00 00	↕...%...
01008B20	FF FF FF FF FF FF FF FF	
01008B28	FF FF FF FF FF FF FF FF	
01008B30	FF FF FF FF FF FF FF FF	
01008B38	FF FF FF FF FF FF FF FF	
01008B40	FF FF FF FF FF FF FF FF	
01008B48	FF FF FF FF FF FF FF FF	
01008B50	FF FF FF FF FF FF FF FF	
01008B58	22 00 00 00 2F 00 00 00	".../...
01008B60	1D 00 00 00 08 00 00 00	∟...◘...
01008B68	0E 00 00 00 1E 00 00 00	♫...▲...
01008B70	06 00 00 00 FF FF FF FF	♠...
01008B78	FF FF FF FF FF FF FF FF	
01008B80	FF FF FF FF FF FF FF FF	
01008B88	FF FF FF FF FF FF FF FF	
01008B90	FF FF FF FF FF FF FF FF	
01008B98	FF FF FF FF FF FF FF FF	
01008BA0	FF FF FF FF FF FF FF FF	
01008BA8	FF FF FF FF 27 00 00 00	....'...
01008BB0	2A 00 00 00 19 00 00 00	*...↓...
01008BB8	2B 00 00 00 0A 00 00 00	+.......
01008BC0	11 00 00 00 28 00 00 00	◄...(...
01008BC8	FF FF FF FF FF FF FF FF	
01008BD0	FF FF FF FF FF FF FF FF	
01008BD8	FF FF FF FF FF FF FF FF	
01008BE0	FF FF FF FF FF FF FF FF	
01008BE8	FF FF FF FF FF FF FF FF	
01008BF0	FF FF FF FF FF FF FF FF	
01008BF8	FF FF FF FF FF FF FF FF	
01008C00	07 00 00 00 2E 00 00 00	•.......
01008C08	20 00 00 00 10 00 00 00	...►...
01008C10	0F 00 00 00 00 00 00 00	☼.......
01008C18	FF FF FF FF FF FF FF FF	
01008C20	FF FF FF FF FF FF FF FF	
01008C28	FF FF FF FF FF FF FF FF	
01008C30	FF FF FF FF FF FF FF FF	
01008C38	FF FF FF FF FF FF FF FF	
01008C40	FF FF FF FF FF FF FF FF	
01008C48	FF FF FF FF FF FF FF FF	
01008C50	FF FF FF FF 23 00 00 00	....#...
01008C58	01 00 00 00 2C 00 00 00	☺...,...
01008C60	0D 00 00 00 05 00 00 00	♪...♣...
01008C68	2D 00 00 00 FF FF FF FF	-...
01008C70	FF FF FF FF FF FF FF FF	
01008C78	FF FF FF FF FF FF FF FF	
01008C80	FF FF FF FF FF FF FF FF	
01008C88	FF FF FF FF FF FF FF FF	
01008C90	FF FF FF FF FF FF FF FF	
01008C98	FF FF FF FF FF FF FF FF	
01008CA0	FF FF FF FF FF FF FF FF	
01008CA8	04 00 00 00 30 00 00 00	♦...0...
01008CB0	16 00 00 00 17 00 00 00	▬...↨...
01008CB8	14 00 00 00 21 00 00 00	¶...!...
01008CC0	FF FF FF FF FF FF FF FF	
01008CC8	FF FF FF FF FF FF FF FF	
01008CD0	FF FF FF FF FF FF FF FF	
01008CD8	FF FF FF FF FF FF FF FF	
01008CE0	FF FF FF FF FF FF FF FF	
01008CE8	FF FF FF FF FF FF FF FF	
01008CF0	FF FF FF FF FF FF FF FF	
01008CF8	FF FF FF FF 03 00 00 00	♥...
01008D00	31 00 00 00 18 00 00 00	1...↑...
01008D08	15 00 00 00 0B 00 00 00	§...♂...
01008D10	32 00 00 00 FF FF FF FF	2...
01008D18	FF FF FF FF FF FF FF FF	
01008D20	FF FF FF FF FF FF FF FF	
01008D28	FF FF FF FF FF FF FF FF	
01008D30	FF FF FF FF FF FF FF FF	
01008D38	FF FF FF FF FF FF FF FF	
01008D40	FF FF FF FF FF FF FF FF	
01008D48	FF FF FF FF FF FF FF FF	
01008D50	13 00 00 00 1F 00 00 00	‼...▼...
01008D58	1B 00 00 00 0C 00 00 00	←.......
01008D60	29 00 00 00 09 00 00 00	).......
01008D68	FF FF FF FF FF FF FF FF	
01008D70	FF FF FF FF FF FF FF FF	
01008D78	FF FF FF FF FF FF FF FF	
01008D80	FF FF FF FF FF FF FF FF	
01008D88	FF FF FF FF FF FF FF FF	
01008D90	FF FF FF FF FF FF FF FF	
01008D98	FF FF FF FF FF FF FF FF	
01008DA0	FF FF FF FF 00 00 00 00	....
01008DA8	00 00 00 00 00 00 00 00	....
01008DB0	00 00 00 00 00 00 00 00	....

7. **With this we can then make a mapping from the hex values to there corresponding card by using the cards displayed on the Freecell GUI and the cards in memory represented by hex:**

```
FF FF FF FF FF FF FF FF
FF FF FF FF 1C 00 00 00
24 00 00 00 26 00 00 00
1A 00 00 00 33 00 00 00
12 00 00 00 25 00 00 00
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
22 00 00 00 2F 00 00 00
1D 00 00 00 08 00 00 00
0E 00 00 00 1E 00 00 00
06 00 00 00 FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF 27 00 00 00
2A 00 00 00 19 00 00 00
2B 00 00 00 0A 00 00 00
11 00 00 00 28 00 00 00
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
07 00 00 00 2E 00 00 00
20 00 00 00 10 00 00 00
0F 00 00 00 00 00 00 00
02 00 00 00 FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF 23 00 00 00
01 00 00 00 2C 00 00 00
0D 00 00 00 05 00 00 00
2D 00 00 00 FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
04 00 00 00 30 00 00 00
16 00 00 00 17 00 00 00
14 00 00 00 21 00 00 00
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF 03 00 00 00
31 00 00 00 18 00 00 00
15 00 00 00 0B 00 00 00
32 00 00 00 FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF
13 00 00 00 1F 00 00 00
1B 00 00 00 0C 00 00 00
29 00 00 00 09 00 00 00
FF FF FF FF FF FF FF FF
```



8. **From this we were able to make the following mapping from hex to card. Check for yourself that the cards match. Notice that the 1st clump of cards corresponds to the 1st column of cards, the 2nd clump to the 2nd column, and so on. Also note that the last hex value in a "clump" corresponds to the top card of a column:**

	A	B	C	D	E
1	**# \ Suit**	**Clubs**	**Diamonds**	**Hearts**	**Spades**
2	**A**	00	01	02	03
3	**2**	04	05	06	07
4	**3**	08	09	0A	0B
5	**4**	0C	0D	0E	0F
6	**5**	10	11	12	13
7	**6**	14	15	16	17
8	**7**	18	19	1A	1B
9	**8**	1C	1D	1E	1F
10	**9**	20	21	22	23
11	**10**	24	25	26	27
12	**J**	28	29	2A	2B
13	**Q**	2C	2D	2E	2F
14	**K**	30	31	32	33

9. **We have successfully located the cards and we know how they are represented! Now we just need a program that can read those addresses of memory.**