

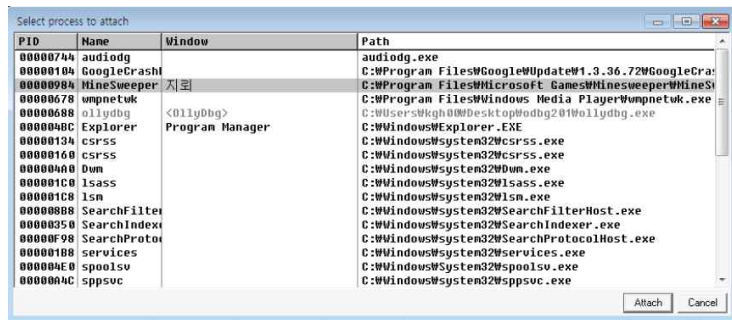
---

# Minesweeper Reversing

# Minesweeper 시간 설정 변경

File -> Attach

Attach를 통해 실행 중인 프로세스를 디버거에 올려준다.



Select module -> minesweeper

[illegible]

007149A5	CALL	DWORD	PTR	DS:[<USER32.SetTimer>]	771952EF	USER32.SetTimer
007178F2	CALL	DWORD	PTR	DS:[<USER32.SetTimer>]	771952EF	USER32.SetTimer
007261B2	CALL	DWORD	PTR	DS:[<USER32.SetTimer>]	771952EF	USER32.SetTimer

007149A5	CALL	DWORD	PTR	DS:[<USER32.SetTimer>]	771952EF	USER32.SetTimer
007178F2	CALL	DWORD	PTR	DS:[<USER32.SetTimer>]	771952EF	USER32.SetTimer
007261B2	CALL	DWORD	PTR	DS:[<USER32.SetTimer>]	771952EF	USER32.SetTimer

# Minesweeper 시간 설정 변경

CPU - main thread, module Minesweeper		
005E498A	> 85C9	TEST ECX,ECX
005E498C	-- 74 1D	JZ SHORT 005E49AB
005E498E	- 68 6F405E00	PUSH 005E406F
005E4993	- 68 E8030000	PUSH 3E8
005E4998	- 68 00040000	PUSH 400
005E499D	- 8908	MOV DWORD PTR DS:[EAX],ECX
005E499F	- FF35 80746300	PUSH DWORD PTR DS:[637480]
005E49A5	- FF15 2C135800	CALL DWORD PTR DS:[<USER32.SetTimer>]
005E49AB	> 5D	POP EBP
005E49AC	- C2 0400	RETN 4
005E49AF	CC	INT3
005E49B0	CC	INT3
005E49B1	CC	INT3
005E49B2	CC	INT3
005E49B3	CC	INT3



- 68 6F405E00	PUSH 005E406F	TimerFunc = Minesweeper.5E406F
- 68 E8030000	PUSH 3E8	Timeout = 1000. ms
- 68 00040000	PUSH 400	TimerID = 1024.
- 8908	MOV DWORD PTR DS:[EAX],ECX	
- FF35 80746300	PUSH DWORD PTR DS:[637480]	hWnd = 00200280, class = Minesweeper
- FF15 2C135800	CALL DWORD PTR DS:[<USER32.SetTimer>]	USER32.SetTimer

C++

```
UINT_PTR SetTimer(
    HWND      hWnd,
    UINT_PTR  nIDEvent,
    UINT      uElapse,
    TIMERPROC lpTimerFunc
);
```

PUSH 3E8(16진수) = 1000(10진수)

Timeout = 1000. ms // 1.000초

# Minesweeper 시간 설정 변경

```

· 68 6F405E00 | PUSH 005E406F
· 68 E8030000 | PUSH 3E8
· 68 00040000 | PUSH 400
· 8908 | MOV DWORD PTR DS:[EAX],ECX
FF35 80746300 | PUSH DWORD PTR DS:[637400]
FF15 2C135B00 | CALL DWORD PTR DS:[<&USER32.SetTimer>]

```

```

TimerFunc = MineSweeper.5E406F
Timeout = 1000. ms
TimerID = 1024.
hWnd = 0020028A, class = Minesweeper
USER32.SetTimer

```

Timeout = 1000. ms // 1.000초



```

68 6F405E00 | PUSH 005E406F
68 08130000 | PUSH 1388
68 00040000 | PUSH 400
8908 | MOV DWORD PTR DS:[EAX],ECX
FF35 80746300 | PUSH DWORD PTR DS:[637400]
FF15 2C135B00 | CALL DWORD PTR DS:[<&USER32.SetTimer>]

```

```

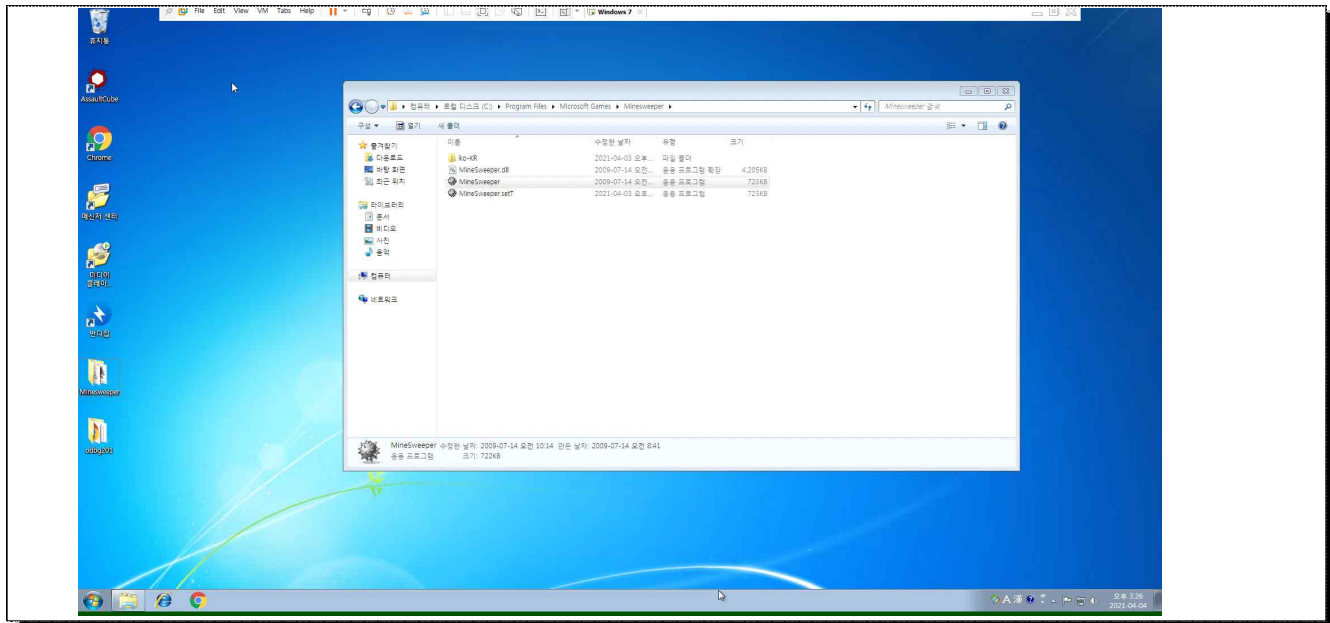
TimerFunc = MineSweeper.5E406F
TimerID = 1024.
hWnd = 0020028A, class = Minesweeper

```

PUSH 1388(16진수) = 5000(10진수)

Timeout = 5000. ms // 5.000초

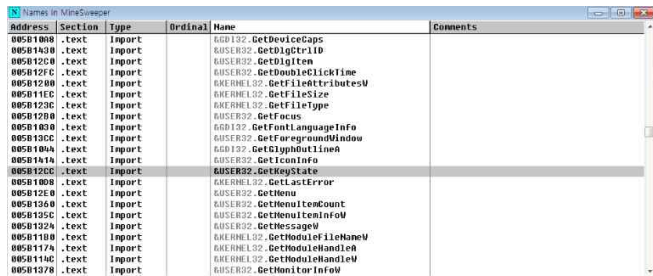
# Minesweeper 시간 설정 변경



# Minesweeper 맵핵

1. 타일을 클릭했을 때 SetTimer() 함수가 호출된다. (예정)
2. 지뢰를 눌렀을 때 GetDlgItem() 함수가 호출된다. (예정)
3. 타일을 눌렀을 때 GetKeyState() 함수가 호출된다. (o)

Search for -> Names (프로그램에서 사용하는 함수와 문자열을 보여줌)



Address	Section	Type	Ordinal	Name	Comments
005B1088	.text	Import		GDI32.GetDeviceCaps	
005B1430	.text	Import		USER32.GetDlgItem110	
005B12C0	.text	Import		USER32.GetDlgItem	
005B12F0	.text	Import		USER32.GetDoubleClickTime	
005B1280	.text	Import		KERNEL32.GetFileAttributesW	
005B11E0	.text	Import		KERNEL32.GetFileSize	
005B1230	.text	Import		KERNEL32.GetFileType	
005B1290	.text	Import		USER32.GetFocus	
005B1820	.text	Import		GDI32.GetFontLanguageInfo	
005B13C0	.text	Import		USER32.GetForegroundWindow	
005B104A	.text	Import		GDI32.GetGlyphOutlineA	
005B141A	.text	Import		USER32.GetIconInfo	
005B12C8	.text	Import		USER32.GetKeyState	
005B1008	.text	Import		KERNEL32.GetLastError	
005B12E0	.text	Import		USER32.GetMenu	
005B1360	.text	Import		USER32.GetMenuItemCount	
005B1350	.text	Import		USER32.GetMenuItemInfoW	
005B132A	.text	Import		USER32.GetMessageW	
005B1180	.text	Import		KERNEL32.GetModuleFileNameW	
005B117A	.text	Import		KERNEL32.GetModuleHandleA	
005B114E	.text	Import		KERNEL32.GetModuleHandleW	
005B1370	.text	Import		USER32.GetMonitorInfoW	

# Minesweeper 맵핵

Names -> Find references

R Search - References to <&USER32.GetKeyState>		
Refs MineSweeper   Calls MineSweeper		
Address	Command	Comments
005D50B5	CALL DWORD PTR DS:[<&USER32.GetKeyState>	VirtualKey = VK_SHIFT
005D5138	CALL DWORD PTR DS:[<&USER32.GetKeyState>	VirtualKey = VK_SHIFT
005D5C08	CALL DWORD PTR DS:[<&USER32.GetKeyState>	VirtualKey = VK_CONTROL
005D5C76	CALL DWORD PTR DS:[<&USER32.GetKeyState>	VirtualKey = VK_SHIFT
005D5C7F	CALL DWORD PTR DS:[<&USER32.GetKeyState>	VirtualKey = VK_CONTROL
005D5C82	CALL DWORD PTR DS:[<&USER32.GetKeyState>	VirtualKey = VK_CONTROL
005D5C89	MOV EDI,DWORD PTR DS:[<&USER32.GetKeySt	
005D5C95	MOV EDI,DWORD PTR DS:[<&USER32.GetKeySt	
005D5F21	CALL DWORD PTR DS:[<&USER32.GetKeyState>	VirtualKey = VK_SHIFT
005D5F57	CALL DWORD PTR DS:[<&USER32.GetKeyState>	VirtualKey = VK_SHIFT
005D5F5B	MOV EDI,DWORD PTR DS:[<&USER32.GetKeySt	
005E30FA	CALL DWORD PTR DS:[<&USER32.GetKeyState>	VirtualKey = VK_F6
005E9E1A	MOV ESI,DWORD PTR DS:[<&USER32.GetKeySt	
005EB02A	CALL DWORD PTR DS:[<&USER32.GetKeyState>	VirtualKey = VK_SHIFT
005F2F92	CALL DWORD PTR DS:[<&USER32.GetKeyState>	VirtualKey = VK_CONTROL



R Search - References to <&USER32.GetKeyState>		
Refs MineSweeper   Calls MineSweeper		
Address	Command	Comments
005D50B5	CALL DWORD PTR DS:[<&USER32.GetKeyState>	VirtualKey = VK_SHIFT
005D5138	CALL DWORD PTR DS:[<&USER32.GetKeyState>	VirtualKey = VK_SHIFT
005D5C08	CALL DWORD PTR DS:[<&USER32.GetKeyState>	VirtualKey = VK_CONTROL
005D5C76	CALL DWORD PTR DS:[<&USER32.GetKeyState>	VirtualKey = VK_SHIFT
005D5C7F	CALL DWORD PTR DS:[<&USER32.GetKeyState>	VirtualKey = VK_CONTROL
005D5C82	CALL DWORD PTR DS:[<&USER32.GetKeyState>	VirtualKey = VK_CONTROL
005D5C89	MOV EDI,DWORD PTR DS:[<&USER32.GetKeySt	
005D5C95	MOV EDI,DWORD PTR DS:[<&USER32.GetKeySt	
005D5F21	CALL DWORD PTR DS:[<&USER32.GetKeyState>	VirtualKey = VK_SHIFT
005D5F57	CALL DWORD PTR DS:[<&USER32.GetKeyState>	VirtualKey = VK_SHIFT
005D5F5B	MOV EDI,DWORD PTR DS:[<&USER32.GetKeySt	
005E30FA	CALL DWORD PTR DS:[<&USER32.GetKeyState>	VirtualKey = VK_F6
005E9E1A	MOV ESI,DWORD PTR DS:[<&USER32.GetKeySt	
005EB02A	CALL DWORD PTR DS:[<&USER32.GetKeyState>	VirtualKey = VK_SHIFT
005F2F92	CALL DWORD PTR DS:[<&USER32.GetKeyState>	VirtualKey = VK_CONTROL

타일을 눌렀을때 반응하는 GetKeyState()함수 찾기



# Minesweeper 맵핵

```

CPU - main thread, module Minesweeper
0089C954 8B3D CC128700 MOV EDI,DWORD PTR DS:[<USER32.GetKeyState>]
0089C956 6A 11 PUSH 11
0089C958 FFD7 CALL EDI
0089C95A 545B 00 SHR EAX,B
0089C95D 84C0 TEST AL,AL
0089C95F 74 0E JZ SHORT 0089C96F
0089C961 81 0A688F00 MOV EAX,DWORD PTR DS:[8F6884]
0089C966 3B5B 1E CMP BYTE PTR DS:[EAX+1E],BL
0089C969 74 0E JZ SHORT 0089C977
0089C96F 6A 10 PUSH 10
0089C971 FFD7 CALL EDI
0089C973 545B 00 SHR EAX,B
0089C976 84C0 TEST AL,AL
0089C978 75 57 JNZ SHORT 0089C9D1
0089C97A 6A 11 PUSH 11
0089C97C FFD7 CALL EDI
0089C97E 545B 00 SHR EAX,B
0089C981 84C0 TEST AL,AL
0089C983 74 0A JZ SHORT 0089C98F
0089C985 81 0A688F00 MOV EAX,DWORD PTR DS:[8F6884]

```

타일 클릭 확인

우클릭 (깃발)

좌클릭 (선택)

CMP/TEST - 비교문  
JNE/JE/JZ - 점프문

Registers (F)	
EAX	00000000
ECX	0007EF90
EDX	776470B4
EBX	00000000
ESP	0007EFA8
EBP	0007EFC0
ESI	02118E38
EDI	77192B40
EIP	0089C95F
C 0	ES 0023
P 1	CS 001B
A 0	SS 0023
Z 0	DS 0023
S 0	FS 003B
T 0	GS 0000
D 0	

점프문에서 ZF값을 0으로 바꾸어  
분기문의 역할을 확인

```

0089C954 8B3D CC128700 MOV EDI,DWORD PTR DS:[<USER32.GetKeyState>]
0089C956 6A 11 PUSH 11
0089C958 FFD7 CALL EDI
0089C95A 545B 00 SHR EAX,B
0089C95D 84C0 TEST AL,AL
0089C95F 74 0E JZ SHORT 0089C96F

```

# Minesweeper 맵핵

## Code

CPU - main thread, module MineSweeper

000DC9A1	8056 1C	MOV EDX,DWORD PTR DS:[ESI+1C]	
000DC9A4	8B40 0C	MOV EAX,DWORD PTR DS:[EAX+0C]	
000DC9A7	833C90 0A	CMPI DWORD PTR DS:[EDX+4+EAX],0A	
000DC9AB	0F84 B1000000	JE 000DCA62	
000DC9B1	385E 48	CMPI BYTE PTR DS:[ESI+48],BL	
000DC9B4	0F84 40020000	JE 000DCC07	
000DC9BA	385D 00	CMPI BYTE PTR SS:[EBP+00],BL	
000DC9BD	0F85 44020000	JNE 000DCC07	
000DC9C3	> 56	PUSH ESI	
000DC9C9	E8 EA5FFFFF	CALL 000D6FB7	Arg1 MineSweeper.000D6FB7

000D6FB7	\$ 8BFF	MOV EDI,EDI	첫 서브루틴
000D6FB9	55	PUSH EBP	
000D6FBA	8BEC	MOV EBP,ESP	
000D6FBC	A1 B468C300	MOV EAX,DWORD PTR DS:[0C368B4]	
000D6FC1	53	PUSH EBX	
000D6FC2	56	PUSH ESI	
000D6FC3	8B75 08	MOV ESI,DWORD PTR SS:[EBP+8]	
000D6FC6	57	PUSH EDI	
000D6FC7	C600 C5000000	MOV BYTE PTR DS:[EAX+0C5],1	
000D6FCE	FF76 1C	PUSH DWORD PTR DS:[ESI+1C]	Arg2
000D6FD1	8BF9	MOV EDI,ECX	Arg1
000D6FD3	FF76 18	PUSH DWORD PTR DS:[ESI+18]	
000D6FD6	8B00 B468C300	MOV ECX,DWORD PTR DS:[0C368B4]	
000D6FDC	320B	XOR BL,BL	
000D6FDE	E8 35A4FFFF	CALL 000D1418	MineSweeper.000D1418

000D1418	\$ 8BFF	MOV EDI,EDI	두번째 서브루틴
000D141A	55	PUSH EBP	
000D141B	8BEC	MOV EBP,ESP	
000D141D	8B49 10	MOV ECX,DWORD PTR DS:[ECX+10]	
000D1420	5D	POP EBP	
000D1421	E9 2AF8FFFF	JMP 000D0C50	

	0	1	2	3	4	5	6	7	8
0									
1									
2									
3									
4									
5									
6									
7									
8									

## Stack

0019EC40	000D6FE3	CALL 000D6FE3	RETURN from MineSweeper.000D1418 to MineSweeper.000D6FE3
0019EC44	00000002	Arg1 = 2	
0019EC48	00000000	Arg2 = 0	
0019EC4C	75532B40	USER32.GetKeyState	

# Minesweeper 맵핵

## Code

```

000D1419 8BFF MOV EDI,EDI          두번째 서브루틴
000D141A 55   PUSH EBP
000D141B 8BEC MOV EBP,ESP
000D141D 8B49 10 MOV ECX,DWORD PTR DS:[ECX+10]
000D1420 5D   POP EBP
000D1421 E9 2AF8FFFF JMP 000D0C50

```

```

000D0C50 8BFF MOV EDI,EDI          세번째 서브루틴
000D0C52 55   PUSH EBP
000D0C53 8BEC MOV EBP,ESP
000D0C55 51   PUSH ECX
000D0C56 53   PUSH EBX
000D0C57 8B5D 08 MOV EBX,DWORD PTR SS:[EBP+8]  x좌표
000D0C5A 56   PUSH ESI
000D0C5B 8BF1 MOV ESI,ECX
000D0C5D 8B46 40 MOV EAX,DWORD PTR DS:[ESI+40]
000D0C60 8B40 0C MOV EAX,DWORD PTR DS:[EAX+0C]
000D0C63 8B0498 MOV EAX,DWORD PTR DS:[EBX+4+EAX]
000D0C66 8B40 0C MOV EAX,DWORD PTR DS:[EAX+0C]
000D0C69 57   PUSH EDI
000D0C6A 8B7D 0C MOV EDI,DWORD PTR SS:[EBP+0C]  y좌표
000D0C6D 8B04B8 MOV EAX,DWORD PTR DS:[EDI*4+EAX]
000D0C70 33C9 XOR ECX,ECX
000D0C72 894D FC MOV DWORD PTR SS:[EBP-4],ECX
000D0C75 83FB 09 CMP EBX,0
000D0C78 74 1B JE SHORT 000D0C95      타일 선택의 결과

```

## Stack

```

EBP+4 000D6EE3 301 0 RETURN from MineSweeper.
EBP+8 00000002 -{ Arg1 = 2
EBP+C 00000000 { Arg2 = 0
EBP+10 75532B4D M+S0 USER32.GetKeyState

```

타일 선택의 결과 패배 창 띄우기

# Minesweeper 맵핵

Code

00000C51	80FF	MOV EDI,EDI	세번째 서브루틴
00000C52	55	PUSH EBP	
00000C53	8BEC	MOV EBP,ESP	
00000C55	51	PUSH ECX	
00000C56	53	PUSH EBY	
00000C57	8B5D 08	MOV EBX,DWORD PTR SS:[EBP+8]	x좌표
00000C5A	56	PUSH ESI	
00000C5B	8BF1	MOV ESI,ECX	
00000C5D	8B46 40	MOV EAX,DWORD PTR DS:[ESI+40]	
00000C60	8B40 0C	MOV EAX,DWORD PTR DS:[EAX+0C]	
00000C63	8B0498	MOV EAX,DWORD PTR DS:[EBX*4+EAX]	
00000C66	8B40 0C	MOV EAX,DWORD PTR DS:[EAX+0C]	
00000C69	57	PUSH EDI	
00000C6A	8B7D 0C	MOV EDI,DWORD PTR SS:[EBP+0C]	y좌표
00000C6D	8B04B8	MOV EAX,DWORD PTR DS:[EDI*4+EAX]	
00000C70	33C9	XOR ECX,ECX	
00000C72	894D FC	MOV DWORD PTR SS:[EBP-4],ECX	
00000C75	83F8 09	CMP EAX,9	
00000C78	74 18	JE SHORT 000D0C95	타일 선택의 결과
00730C7A	83F8 0B	CMP EAX,0B	
00730C7D	74 16	JE SHORT 00730C95	
00730C7F	A1 B4687900	MOV EAX,DWORD PTR DS:[7968B4]	
00730C84	3B48 18	CMP BYTE PTR DS:[EAX+18],CL	
00730C87	74 5C	JE SHORT 00730CE5	
00730C89	51	PUSH ECX	
00730C8A	51	PUSH ECX	
00730C8B	51	PUSH ECX	
00730C8C	E8 58F90000	CALL 007405E9	
00730C91	33C9	XOR ECX,ECX	
00730C93	E8 50	JMP SHORT 00730CE5	
00730C95	394E 18	CMP DWORD PTR DS:[ESI+18],ECX	
00730C98	75 20	JNE SHORT 00730CBA	
00730C9A	57	PUSH EDI	
00730C9B	53	PUSH EBX	

Address	Hex	dump
01FBF588	01 00 00 00 00 00 00 40	
01FBF590	01 00 00 00 00 00 00 00	
01FBF598	00 00 00 00 61 3F 6B 60	
01FBF5A0	00 00 00 00 00 00 00 00	
01FBF5A8	10 00 00 00 00 00 00 00	
01FBF5B0	D0 F5 FB 01 40 76 14 00	
01FBF5B8	AB AB AB AB AB AB AB AB	
01FBF5C0	00 00 00 00 00 00 00 00	
01FBF5C8	15 10 04 5C 58 86 0B 18	
01FBF5D0	09 00 00 00 10 00 00 00	
01FBF5D8	10 00 00 00 20 F6 FB 01	
01FBF5E0	AB AB AB AB AB AB AB AB	
01FBF5E8	00 00 00 00 00 00 00 00	

# Minesweeper 맵핵

Code

00730C95	394E 18	CMP DWORD PTR DS:[ESI+18],ECX	
00730C98	75 20	JNE SHORT 00730CBA	
00730C9A	57	PUSH EDI	
00730C9B	53	PUSH EBX	
00730C9C	8BCE	MOV ECX,ESI	
00730C9E	E8 18F4FFFF	CALL 007300BB	
00730CA3	6A 00	PUSH 0	
00730CA5	57	PUSH EDI	
00730CA6	53	PUSH EBX	
00730CA7	6A 00	PUSH 0	
00730CA9	57	PUSH EDI	
00730CAA	53	PUSH EBX	
00730CAB	8BCE	MOV ECX,ESI	
00730CAD	E8 90F0FFFF	CALL 00730A42	
00730CB2	895E 24	MOV DWORD PTR DS:[ESI+24],EBX	
00730CB5	897E 28	MOV DWORD PTR DS:[ESI+28],EDI	
00730CB8	EB 23	JMP SHORT 00730CDD	
00730CB8	> 8B46 44	MOV EAX,DWORD PTR DS:[ESI+44]	
00730CBD	8B40 0C	MOV EAX,DWORD PTR DS:[EAX+0C]	C 0 ES 0023
00730CC0	8B0498	MOV EAX,DWORD PTR DS:[EBX+4+EAX]	P 1 CS 001B
00730CC3	8B40 0C	MOV EAX,DWORD PTR DS:[EAX+0C]	A 0 SS 0023
00730CC6	3B0C07	CMP BYTE PTR DS:[EAX+EDI],CL	Z 1 DS 0023
00730CC9	74 05	JE SHORT 00730CD8	S 0 FS 003B
			T 0 GS 0000

# Minesweeper 맵핵

```

CMP DWORD PTR DS:[ESI+18],ECX - 비교와 점프 구분 구현
JE 00F40C9A
PUSH EAX - 레지스터 값 저장
PUSH EDX
PUSH ECX
PUSH EBX
PUSH EDI
MOV EDX,0 - 레지스터 초기화
MOV ECX,0
MOV EDI,0
MOV EBX,0
MOV EAX,DWORD PTR DS:[ESI+44] - 자료 위치 비교
MOV EAX,DWORD PTR DS:[EAX+0C]
MOV EAX,DWORD PTR DS:[EBX*4+EAX]
MOV EAX,DWORD PTR DS:[EAX+EDI]
MOV BYTE PTR DS:[EDX+BA7790],CL - 자료 확인 결과 저장
INC EBX - X 좌표 처리
INC EDX - 자료 확인 결과를 저장할 위치 저장
CMP EBX,9 - X 좌표 관련된 반복문을 위한 크기 비교
JL SHORT 00F9DD8D - X 좌표와 관련된 반복문을 위한 점프
INC EDI - Y 좌표 처리
CMP EDI,9 - Y 좌표 관련된 반복문을 위한 크기 비교
JL SHORT 00F9DD88 - Y 좌표와 관련된 반복문을 위한 점프
POP EDI - 레지스터 값 복구
POP EBX
POP ECX
POP EDX
POP EAX
JMP 00F40CBA - 원래 로직 복귀

```

제목 없음 - 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

00	00	00	01	00	01	00	00	00
00	00	01	00	00	00	00	01	00
00	00	00	00	00	00	00	00	00
00	00	01	00	00	00	00	00	00
00	00	00	00	00	00	00	01	00
00	00	00	00	00	00	01	01	00
00	00	01	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00
00	00	00	00	00	01	00	00	00

---

End