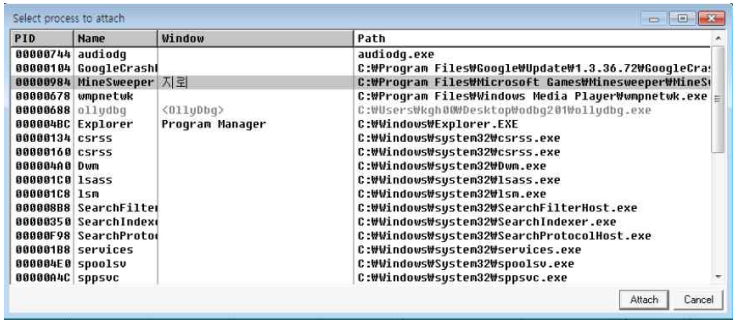
Minesweeper Reversing

김건희

Minesweeper 시간 설정 변경

File -> Attach

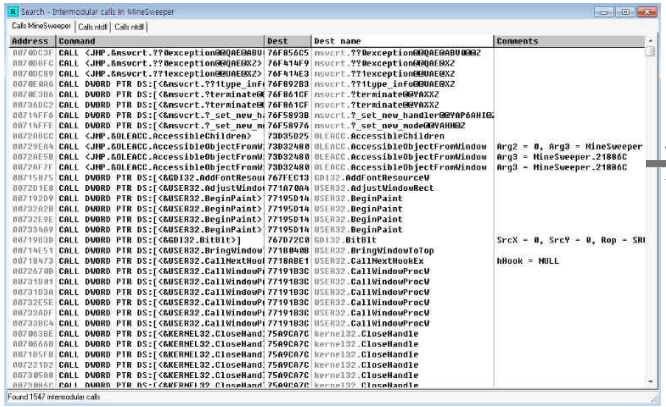
Attach를 통해 실행 중인 프로세스를
디버거에 올려준다.



Select module -> minesweeper

Minesweeper 시간 설정 변경

Search for -> All intermodular calls

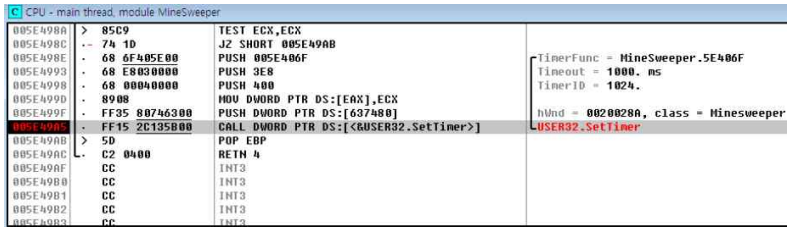


가정 : SetTimer() 함수가 시간을 설정한다.

```
00714905 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
```

```
00714905 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




```
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                  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 = 0020028A, class = Minesweeper
·  FF15 2C135B00  CALL DWORD PTR DS:[<&USER32.SetTimer>]  USER32.SetTimer
```

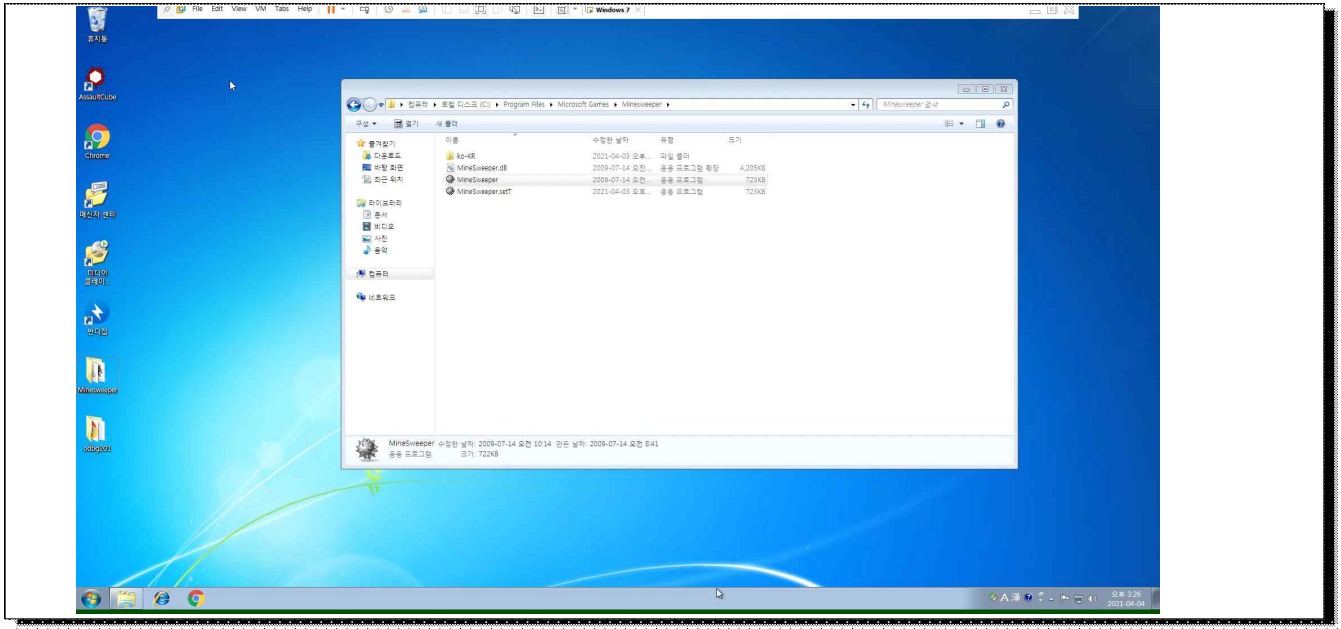
Timeout = 1000. ms // 1.000초

```
68 6F405E00     PUSH 005E406F                  TimerFunc = MineSweeper.5E406F
68 88130000     PUSH 1388
68 00040000     PUSH 400                       TimerID = 1024.
8908           MOV DWORD PTR DS:[EAX],ECX
FF35 80746300  PUSH DWORD PTR DS:[637480]     hWnd = 0020028A, class = Minesweeper
FF15 2C135B00  CALL DWORD PTR DS:[<&USER32.SetTimer>]
```

PUSH 1388(16진수) = 5000(10진수)

Timeout = 5000. ms // 5.000초

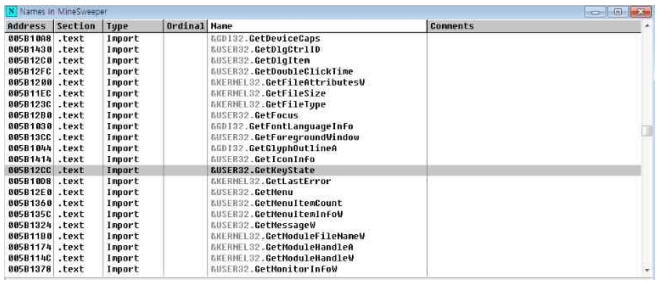
Minesweeper 시간 설정 변경



Minesweeper 맵핵

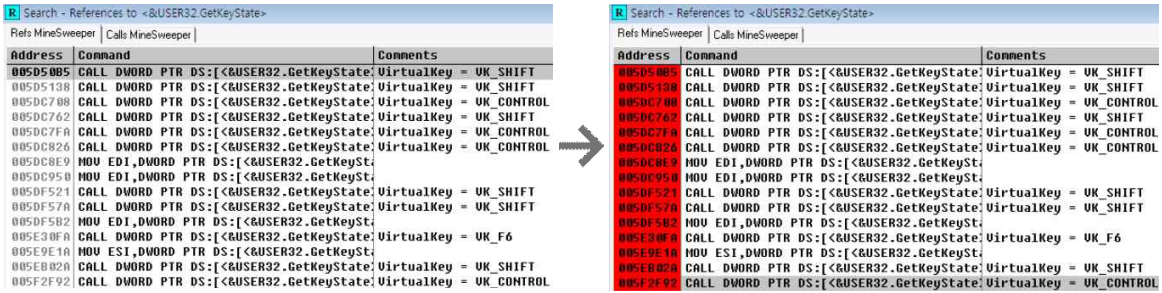
1. 타일을 클릭했을 때 SetTimer() 함수가 호출된다. (예정)
2. 지뢰를 눌렀을 때 GetDlgItem() 함수가 호출된다. (예정)
3. 타일을 눌렀을 때 GetKeyState() 함수가 호출된다. (o)

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



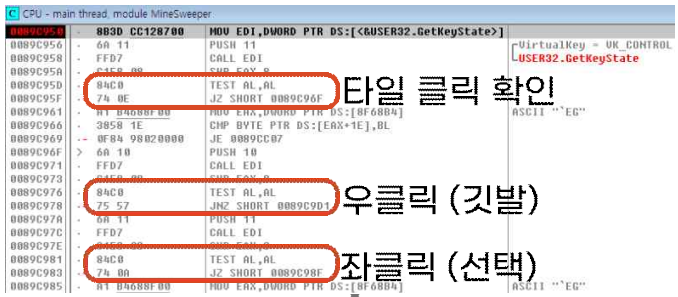
Minesweeper 맵핵

Names -> Find references

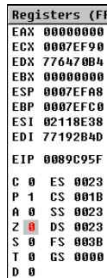


타일을 눌렀을때 반응하는 GetKeyState()함수 찾기

Minesweeper 맵핵



CMP/TEST - 비교문
JNE/JE/JZ - 점프문



점프문에서 ZF값을 0으로 바꾸어 분기문의 역할을 확인

Minesweeper 맵핵

Code

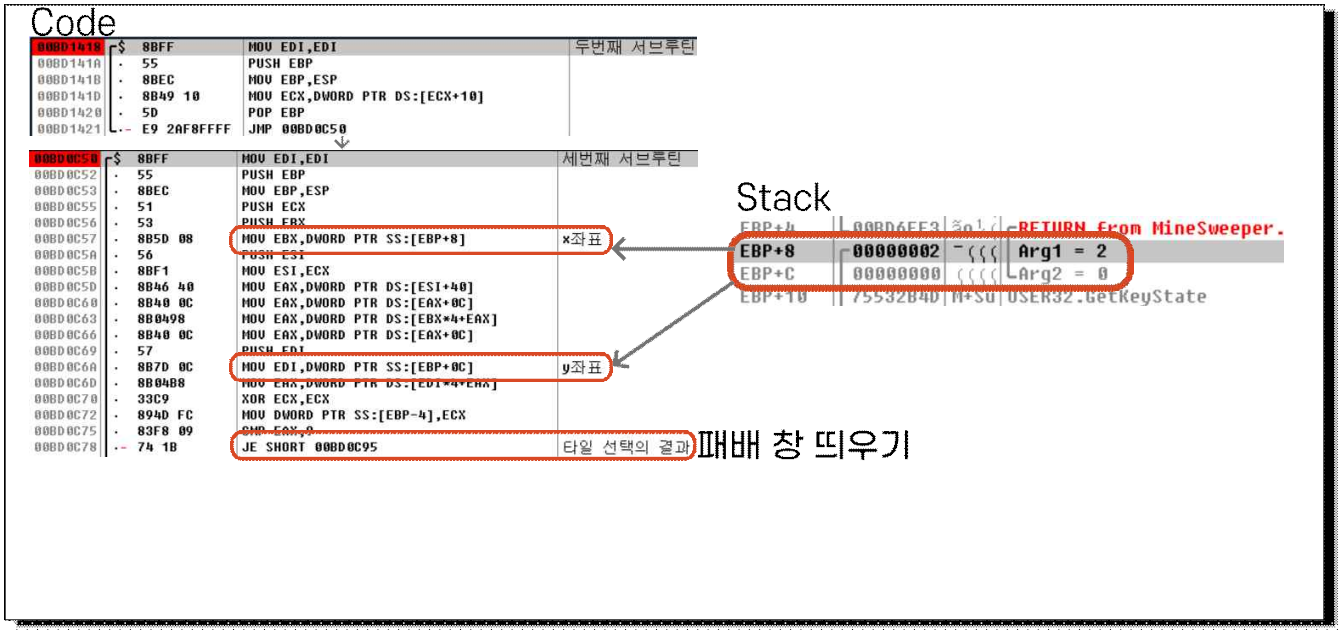
```
CPU - main thread, module MineSweeper
00BDC9A1  .  8B56 1C        MOV EDX,DWORD PTR DS:[ESI+1C]
00BDC9A4  .  8B40 0C        MOV EAX,DWORD PTR DS:[EAX+0C]
00BDC9A7  .  833C90 0A      CMP DWORD PTR DS:[EDX*4+EAX],0A
00BDC9AB  .- 0F84 B1000000  JE 00BDCA62
00BDC9B1  .  385E 48        CMP BYTE PTR DS:[ESI+48],BL
00BDC9B4  .- 0F84 4D020000  JE 00BDCC07
00BDC9BA  .  385D 0B        CMP BYTE PTR SS:[EBP+0B],BL
00BDC9BD  .- 0F85 44020000  JNE 00BDCC07
00BDC9C3  > 56              PUSH ESI                          Arg1
00BDC9C4  .  E8 EEA5FFFF    CALL 00BD6FB7                     MineSweeper.00BD6FB7

00BD6FB7  ┌$ 8BFF          MOV EDI,EDI                       첫 서브루틴
00BD6FB9  .  55             PUSH EBP
00BD6FBA  .  8BEC           MOV EBP,ESP
00BD6FBC  .  A1 B468C300    MOV EAX,DWORD PTR DS:[0C368B4]
00BD6FC1  .  53             PUSH EBX
00BD6FC2  .  56             PUSH ESI
00BD6FC3  .  8B75 08        MOV ESI,DWORD PTR SS:[EBP+8]
00BD6FC6  .  57             PUSH EDI
00BD6FC7  .  C680 C5000000  MOV BYTE PTR DS:[EAX+0C5],1
00BD6FCE  .  FF76 1C        PUSH DWORD PTR DS:[ESI+1C]        Arg2
00BD6FD1  .  8BF9           MOV EDI,ECX
00BD6FD3  .  FF76 18        PUSH DWORD PTR DS:[ESI+18]        Arg1
00BD6FD6  .  8B0D B468C300  MOV ECX,DWORD PTR DS:[0C368B4]
00BD6FDC  .  32DB           XOR BL,BL
00BD6FDE  .  E8 35A4FFFF    CALL 00BD1418                     MineSweeper.00BD1418

00BD1418  ┌$ 8BFF          MOV EDI,EDI                       두번째 서브루틴
00BD141A  .  55             PUSH EBP
00BD141B  .  8BEC           MOV EBP,ESP
00BD141D  .  8B49 10        MOV ECX,DWORD PTR DS:[ECX+10]
00BD1420  .  5D             POP EBP
00BD1421  L.- E9 2AF8FFFF   JMP 00BD0C50
```

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

Stack

```
0019EC40  00BD6FE3  ão½  RETURN from MineSweeper.00BD1418 to MineSweeper.00BD6FE3
0019EC44  00000002  ☺    Arg1 = 2
0019EC48  00000000  ♥    Arg2 = 0
0019EC4C  75532B4D  M+Su  USER32.GetKeyState
```

Minesweeper 맵핵



Minesweeper 맵핵

Code

```
00BD0C50  /$  8BFF          MOV EDI,EDI                          세번째 서브루틴
00BD0C52  |.  55            PUSH EBP
00BD0C53  |.  8BEC          MOV EBP,ESP
00BD0C55  |.  51            PUSH ECX
00BD0C56  |.  53            PUSH EBX
00BD0C57  |.  8B5D 08       MOV EBX,DWORD PTR SS:[EBP+8]         x좌표
00BD0C5A  |.  56            PUSH ESI
00BD0C5B  |.  8BF1          MOV ESI,ECX
00BD0C5D  |.  8B46 40       MOV EAX,DWORD PTR DS:[ESI+40]
00BD0C60  |.  8B40 0C       MOV EAX,DWORD PTR DS:[EAX+0C]
00BD0C63  |.  8B0498        MOV EAX,DWORD PTR DS:[EBX*4+EAX]
00BD0C66  |.  8B40 0C       MOV EAX,DWORD PTR DS:[EAX+0C]
00BD0C69  |.  57            PUSH EDI
00BD0C6A  |.  8B7D 0C       MOV EDI,DWORD PTR SS:[EBP+0C]        y좌표
00BD0C6D  |.  8B0488        MOV EAX,DWORD PTR DS:[EDI*4+EAX]
00BD0C70  |.  33C9          XOR ECX,ECX
00BD0C72  |.  894D FC       MOV DWORD PTR SS:[EBP-4],ECX
00BD0C75  |.  83F8 09       CMP EAX,9
00BD0C78  |.- 74 1B         JE SHORT 00BD0C95                    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  |.  3848 18       CMP BYTE PTR DS:[EAX+18],CL
00730C87  |.- 74 5C         JE SHORT 00730CE5
00730C89  |.  51            PUSH ECX                             Arg3
00730C8A  |.  51            PUSH ECX                             Arg2
00730C8B  |.  51            PUSH ECX                             Arg1
00730C8C  |.  E8 58F90000   CALL 007405E9                        MineSweeper.007405E9
00730C91  |.  33C9          XOR ECX,ECX
00730C93  |.- EB 50         JMP SHORT 00730CE5
00730C95  |>  394E 18       CMP DWORD PTR DS:[ESI+18],ECX
00730C98  |.  75 20         JNE SHORT 00730CBA
00730C9A  |.  57            PUSH EDI                             Arg2
00730C9B  |.  53            PUSH EBX                             Arg1
```

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 D4 5C 5B 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

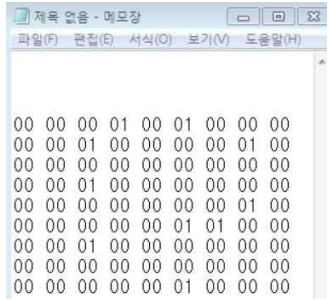
Code

```
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 90FDFFFF     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
00730CBA    8B46 44         MOV EAX,DWORD PTR DS:[ESI+44]
00730CBD    8B40 0C         MOV EAX,DWORD PTR DS:[EAX+0C]
00730CC0    8B0498          MOV EAX,DWORD PTR DS:[EBX*4+EAX]
00730CC3    8B40 0C         MOV EAX,DWORD PTR DS:[EAX+0C]
00730CC6    380C07          CMP BYTE PTR DS:[EAX+EDI],CL
00730CC9    74 05           JE SHORT 00730CD0
```

```
C 0  ES 0023
P 1  CS 001B
A 0  SS 0023
Z 1  DS 0023
S 0  FS 003B
T 0  GS 0000
```

Minesweeper 맵핵

```
CMP DWORD PTR DS:[ESI+18],ECX - 비교와 점프 구문 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] - 지뢰 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 - 지뢰 확인 결과 저장
INC EBX - X 좌표 처리
INC EDX - 지뢰 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 00F9DD83 - Y 좌표와 관련된 반복문을 위한 점프
POP EDI - 레지스터 값 복구
POP EBX
POP ECX
POP EDX
POP EAX
JMP 00F40CBA - 원래 로직 복귀
```



End