클라이언트 해킹 – 크랙(CRACK)

정보보호학개론

이병천 교수님

제출일 : **15.06.11**

정보보호학과

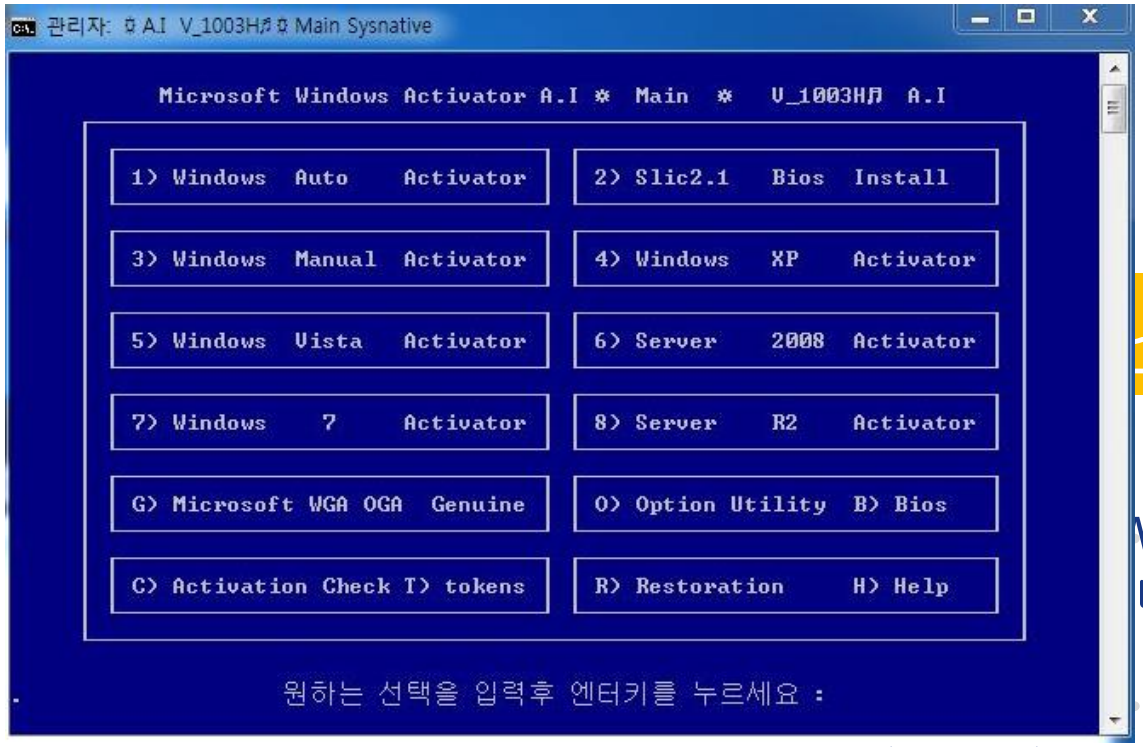
91514672 김수운

91514684 김예진

클라이언트 해킹이란?

- 사용자에 의해 설치된 실행 파일에 대한 크랙, 메모리 변조, 파일 변조 등을 하는 공격이다.

- 클라이언트 해킹을 위해서는 리버스 엔지니어링을 기반으로 분석을 진행한다.
  - 리버스 엔지니어링 – 장치 또는 시스템의 기술적인 원리를 구조분석을 통해 발견하는 과정.



산?

vare 프로그램을
변경하는 작업을

- EX) Windows 정품 인증 크랙 프로그램
  - 제품 번호 인증을 우회하거나 제품 번호를 계산하는 알고리즘을 무력화하여 Shareware를 Freeware로 변경시킨다.

그에 따른 피해는?

- 정당한 사용료를 지불하고 사용해야 할 게임, 또는 프로그
  - 개발자의

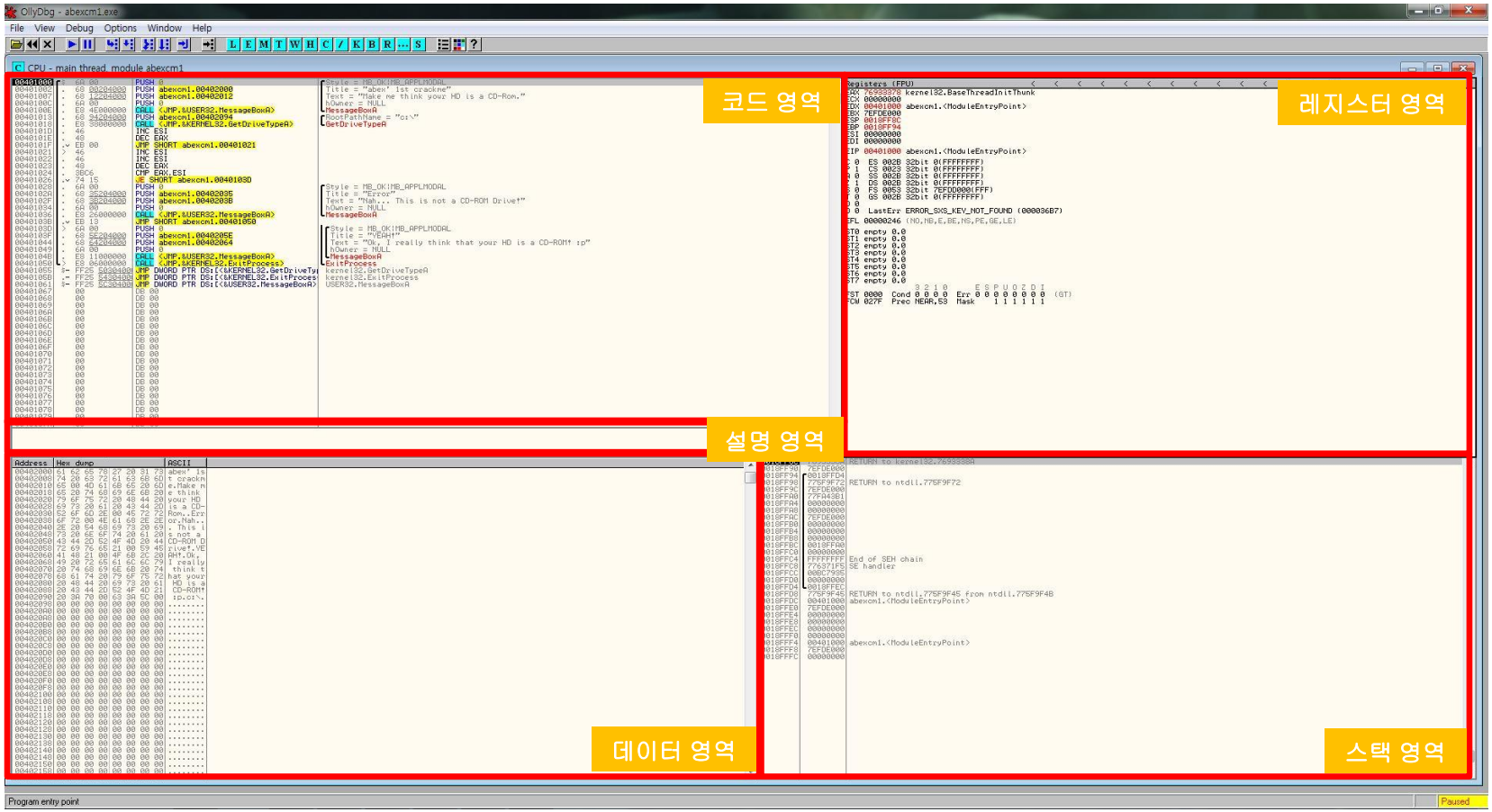
ollydbg

- Ollydbg는 freeware이며, 악성코드 분석, 취약점을 찾기 위해 많이 사용하는 디버거이다.

Abex의 Crack Me! #1

- Abex의 Crack Me 첫번째 문제.
- 프로그램이 하드드라이브를 CD-ROM으로 인식하도록 만들어야 한다.

Crack Me #1 - ollydbg 분석



Crack Me #1 – ollydbg 분석

```
00401000  $  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
00401002  .  68 00204000    PUSH abexcm1.00402000                    Title = "abex' 1st crackme"
00401007  .  68 12204000    PUSH abexcm1.00402012                    Text = "Make me think your HD is a CD-Rom."
0040100C  .  6A 00          PUSH 0                                   hOwner = NULL
0040100E  .  E8 4E000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
00401013  .  68 94204000    PUSH abexcm1.00402094                    RootPathName = "c:\"
00401018  .  E8 38000000    CALL <JMP.&KERNEL32.GetDriveTypeA>       GetDriveTypeA
0040101D  .  46             INC ESI
0040101E  .  48             DEC EAX
0040101F  .v EB 00          JMP SHORT abexcm1.00401021
00401021  >  46             INC ESI
00401022  .  46             INC ESI
00401023  .  48             DEC EAX
00401024  .  3BC6           CMP EAX,ESI
00401026   v 74 15          JE SHORT abexcm1.0040103D
00401028  .  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
0040102A  .  68 35204000    PUSH abexcm1.00402035                    Title = "Error"
0040102F  .  68 3B204000    PUSH abexcm1.0040203B                    Text = "Nah... This is not a CD-ROM Drive!"
00401034  .  6A 00          PUSH 0                                   hOwner = NULL
00401036  .  E8 26000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
0040103B  .v EB 13          JMP SHORT abexcm1.00401050
0040103D  >  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
0040103F  .  68 5E204000    PUSH abexcm1.0040205E                    Title = "YEAH!"
00401044  .  68 64204000    PUSH abexcm1.00402064                    Text = "Ok, I really think that your HD is a CD-ROM! :p"
00401049  .  6A 00          PUSH 0                                   hOwner = NULL
0040104B  .  E8 11000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
00401050  >  E8 06000000    CALL <JMP.&KERNEL32.ExitProcess>         ExitProcess
00401055  $- FF25 5030400   JMP DWORD PTR DS:[<&KERNEL32.GetDriveTy  kernel32.GetDriveTypeA
0040105B  .- FF25 5430400   JMP DWORD PTR DS:[<&KERNEL32.ExitProces  kernel32.ExitProcess
00401061  $- FF25 5C30400   JMP DWORD PTR DS:[<&USER32.MessageBoxA>  USER32.MessageBoxA
00401067     00             DB 00
00401068     00             DB 00
00401069     00             DB 00
0040106A     00             DB 00
0040106B     00             DB 00
```

Crack Me #1 – ollydbg 분석

```
00401000  $   6A 00          PUSH 0                                  Style = MB_OK|MB_APPLMODAL
00401002  .   68 00204000    PUSH abexcm1.00402000                   Title = "abex' 1st crackme"
00401007  .   68 12204000    PUSH abexcm1.00402012                   Text = "Make me think your HD is a CD-Rom."
0040100C  .   6A 00          PUSH 0                                  hOwner = NULL
0040100F  .   E8 4F000000    CALL <JMP.&USER32.MessageBoxA>          MessageBoxA
00401013  .   68 94204000    PUSH abexcm1.00402094                   RootPathName = "c:\"
00401018  .   E8 38000000    CALL <JMP.&KERNEL32.GetDriveTypeA>      GetDriveTypeA
0040101D  .   46             INC ESI
0040102A  .   68 35204000    PUSH abexcm1.00402035                   Title = "Error"
0040102F  .   68 3B204000    PUSH abexcm1.0040203B                   Text = "Nah... This is not a CD-ROM Drive!"
00401034  .   6A 00          PUSH 0                                  hOwner = NULL
00401036  .   E8 26000000    CALL <JMP.&USER32.MessageBoxA>          MessageBoxA
0040103B  .v  EB 13          JMP SHORT abexcm1.00401050
0040103D  >   6A 00          PUSH 0                                  Style = MB_OK|MB_APPLMODAL
0040103F  .   68 5E204000    PUSH abexcm1.0040205E                   Title = "YEAH!"
00401044  .   68 64204000    PUSH abexcm1.00402064                   Text = "Ok, I really think that your HD is a CD-ROM! :p"
00401049  .   6A 00          PUSH 0                                  hOwner = NULL
0040104B  .   E8 11000000    CALL <JMP.&USER32.MessageBoxA>          MessageBoxA
00401050  >   E8 06000000    CALL <JMP.&KERNEL32.ExitProcess>        ExitProcess
00401055  $-  FF25 5030400   JMP DWORD PTR DS:[<&KERNEL32.GetDriveTy  kernel32.GetDriveTypeA
0040105B  .-  FF25 5430400   JMP DWORD PTR DS:[<&KERNEL32.ExitProces  kernel32.ExitProcess
00401061  $-  FF25 5C30400   JMP DWORD PTR DS:[<&USER32.MessageBoxA>  USER32.MessageBoxA
00401067      00             DB 00
00401068      00             DB 00
00401069      00             DB 00
0040106A      00             DB 00
0040106B      00             DB 00
```

00401013에서 **00402094**를 **PUSH**로 스택에 올리고있다.
주석을 보아 **00402094**는 **C**를 의미함을 알 수 있다.

Crack Me #1 – ollydbg 분석

```
00401000  $  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
00401002  .  68 00204000    PUSH abexcm1.00402000                    Title = "abex' 1st crackme"
00401007  .  68 12204000    PUSH abexcm1.00402012
0040100C  .  6A 00          PUSH 0
0040100E  .  E8 4E000000    CALL <JMP.&USER32.MessageBoxA>
00401013  .  68 94204000    PUSH abexcm1.00402094
00401018  .  E8 38000000    CALL <JMP.&KERNEL32.GetDriveTy
0040101D  .  46             INC ESI
0040101E  .  48             DEC EAX
0040101F  .v EB 00          JMP SHORT abexcm1.00401021
00401021  >  46             INC ESI
00401022  .  46             INC ESI
00401023  .  48             DEC EAX
00401024  .  3BC6           CMP EAX,ESI
00401026  .v 74 15          JE SHORT abexcm1.0040103D
00401028  .  6A 00          PUSH 0
0040102A  .  68 35204000    PUSH abexcm1.00402035
0040102F  .  68 3B204000    PUSH abexcm1.0040203B
00401034  .  6A 00          PUSH 0
00401050  >  E8 06000000    CALL <JMP.&KERNEL32.ExitProcess>         ExitProcess
00401055  $- FF25 5030400   JMP DWORD PTR DS:[<&KERNEL32.GetDriveTy  kernel32.GetDriveTypeA
0040105B  .- FF25 5430400   JMP DWORD PTR DS:[<&KERNEL32.ExitProces  kernel32.ExitProcess
00401061  $- FF25 5C30400   JMP DWORD PTR DS:[<&USER32.MessageBoxA>  USER32.MessageBoxA
00401067     00             DB 00
00401068     00             DB 00
00401069     00             DB 00
0040106A     00             DB 00
0040106B     00             DB 00
```

Value	Meaning
0	The drive type cannot be determined.
1	The root directory does not exist.
DRIVE_REMOVABLE	The drive can be removed from the drive.
DRIVE_FIXED	The disk cannot be removed from the drive.
DRIVE_REMOTE	The drive is a remote (network) drive.
DRIVE_CDROM	The drive is a CD-ROM drive.
DRIVE_RAMDISK	The drive is a RAM disk.

GetDriveTypeA함수는 디스크의 루트 패스를 전달하면 **0,1** 등의 값을 리턴한다. 이 값을 통해 드라이브를 체크 할 수 있다.

Crack Me #1 – ollydbg 분석

```
00401000  $   6A 00          PUSH 0                                  Style = MB_OK|MB_APPLMODAL
00401002  .   68 00204000    PUSH abexcm1.00402000                   Title = "abex' 1st crackme"
00401007  .   68 12204000    PUSH abexcm1.00402012                   Text = "Make me think your HD is a CD-Rom."
0040100C  .   6A 00          PUSH 0                                  hOwner = NULL
0040100E  .   E8 4E000000    CALL <JMP.&USER32.MessageBoxA>          MessageBoxA
00401013  .   68 94204000    PUSH abexcm1.00402094                   RootPathName = "c:\"
00401018  .   E8 38000000    CALL <JMP.&KERNEL32.GetDriveTypeA>      GetDriveTypeA
0040101D  .   46             INC ESI
0040101E  .   48             DEC EAX
0040101F  .v  EB 00          JMP SHORT abexcm1.00401021
00401021  >   46             INC ESI
00401022  .   46             INC ESI
00401023  .   48             DEC EAX
00401024  .   3BC6           CMP EAX,ESI
00401026  .v  74 15          JE SHORT abexcm1.0040103D
00401028  .   6A 00          PUSH 0                                  Style = MB_OK|MB_APPLMODAL
0040102A  .   68 35204000    PUSH abexcm1.00402035                   Title = "Error"
0040102F  .   68 3B204000    PUSH abexcm1.0040203B                   Text = "Nah... This is not a CD-ROM Drive!"
00401061  $-  FF25 5C30400   JMP DWORD PTR DS:[<&USER32.MessageBoxA>  USER32.MessageBoxA
00401067      00             DB 00
00401068      00             DB 00
00401069      00             DB 00
0040106A      00             DB 00
0040106B      00             DB 00
```

INC ESI → ESI레지스터 값 1증가 DEC EAX → EAX레지스터 값 1감소
CMP EAX,ESI → EAX, ESI레지스터 값을 비교 후 플래그 레지스터 세팅
JE → (Jump If Equal) 비교 값이 같을 경우 지정 주소로 분기

Crack Me #1 – ollydbg 분석

00401028~00401036은 실패 했을 시에 **MessageBoxA**함수를 이용하여 에러 메시지를 띄우고, **0040103B**에서 **00401050**으로 분기하여 프로그램을 종료한다.

```
00401000  $  6A 00          PUSH 0                                  Style = MB_OK|MB_APPLMODAL
00401002  .  68 00204000    PUSH abexcm1.00402000                   Title = "abex' 1st crackme"
00401024  .  3BC6           CMP EAX,ESI
00401026  .v 74 15          JE SHORT abexcm1.0040103D
00401028  .  6A 00          PUSH 0                                  Style = MB_OK|MB_APPLMODAL
0040102A  .  68 35204000    PUSH abexcm1.00402035                   Title = "Error"
0040102F  .  68 3B204000    PUSH abexcm1.0040203B                   Text = "Nah... This is not a CD-ROM Drive!"
00401034  .  6A 00          PUSH 0                                  hOwner = NULL
00401036  .  E8 26000000    CALL <JMP.&USER32.MessageBoxA>          MessageBoxA
0040103B  .v EB 13          JMP SHORT abexcm1.00401050
0040103D  >  6A 00          PUSH 0                                  Style = MB_OK|MB_APPLMODAL
0040103F  .  68 5E204000    PUSH abexcm1.0040205E                   Title = "YEAH!"
00401044  .  68 64204000    PUSH abexcm1.00402064                   Text = "Ok, I really think that your HD is a CD-ROM! :p"
00401049  .  6A 00          PUSH 0                                  hOwner = NULL
0040104B  .  E8 11000000    CALL <JMP.&USER32.MessageBoxA>          MessageBoxA
00401050  >  E8 06000000    CALL <JMP.&KERNEL32.ExitProcess>        ExitProcess
00401055  $- FF25 5030400   JMP DWORD PTR DS:[<&KERNEL32.GetDriveTy  kernel32.GetDriveTypeA
0040105B  .- FF25 5430400   JMP DWORD PTR DS:[<&KERNEL32.ExitProces  kernel32.ExitProcess
00401061  $- FF25 5C30400   JMP DWORD PTR DS:[<&USER32.MessageBoxA>  USER32.MessageBoxA
00401067     00             DB 00
00401068     00             DB 00
00401069     00             DB 00
0040106A     00             DB 00
0040106B     00             DB 00
```

Crack Me #1 – ollydbg 분석

```
00401000  $   6A 00          PUSH 0                                  Style = MB_OK|MB_APPLMODAL
00401002  .   68 00204000    PUSH abexcm1.00402000                   Title = "abex' 1st crackme"
00401007  .   68 12204000    PUSH abexcm1.00402012                   Text = "Make me think your HD is a CD-Rom."
0040100C  .   6A 00          PUSH 0                                  hOwner = NULL
0040100E  .   E8 4E000000    CALL <JMP.&USER32.MessageBoxA>          MessageBoxA
00401013  .   68 94204000    PUSH abexcm1.00402094                   RootPathName = "c:\"
00401018  .   E8 38000000    CALL <JMP.&KERNEL32.GetDriveTypeA>      GetDriveTypeA
0040101D  .   46             INC ESI
0040101E  .   48             DEC EAX
0040101F  .v  EB 00          JMP SHORT abexcm1.00401021
00401034  .   6A 00          PUSH 0                                  hOwner = NULL
00401036  .   E8 26000000    CALL <JMP.&USER32.MessageBoxA>          MessageBoxA
0040103B  .v  EB 13          JMP SHORT abexcm1.00401050
0040103D  >   6A 00          PUSH 0                                  Style = MB_OK|MB_APPLMODAL
0040103F  .   68 5E204000    PUSH abexcm1.0040205E                   Title = "YEAH!"
00401044  .   68 64204000    PUSH abexcm1.00402064                   Text = "Ok, I really think that your HD is a CD-ROM! :p"
00401049  .   6A 00          PUSH 0                                  hOwner = NULL
0040104B  .   E8 11000000    CALL <JMP.&USER32.MessageBoxA>          MessageBoxA
00401050  >   E8 06000000    CALL <JMP.&KERNEL32.ExitProcess>        ExitProcess
00401055  $-  FF25 5030400   JMP DWORD PTR DS:[<&KERNEL32.GetDriveTy  kernel32.GetDriveTypeA
0040105B  .-  FF25 5430400   JMP DWORD PTR DS:[<&KERNEL32.ExitProces  kernel32.ExitProcess
00401061  $-  FF25 5C30400   JMP DWORD PTR DS:[<&USER32.MessageBoxA>  USER32.MessageBoxA
00401067      00             DB 00
00401068      00             DB 00
00401069      00             DB 00
0040106A      00             DB 00
0040106B      00             DB 00
```

0040103D~0040104B는 성공 했을 시에 **MessageBoxA**함수를 이용하여 성공 메시지를 띄우고, **00401050**에서 프로그램을 종료한다.

Crack Me #1 – ollydbg 크랙킹

```
00401018  .  E8 38000000   CALL <JMP.&KERNEL32.GetDriveTypeA>      GetDriveTypeA
0040101D  .  46            INC ESI
0040101E  .  48            DEC EAX
0040101F  .v EB 00         JMP SHORT abexcm1.00401021
00401021  >  46            INC ESI
00401022  .  46            INC ESI
00401023  .  48            DEC EAX
00401024  .  3BC6          CMP EAX,ESI
00401026  .v 74 15         JE SHORT abexcm1.0040103D
00401028  .  6A 00         PUSH 0                                  Style = MB_OK|MB_APPLMODAL
0040102A  .  68 35204000   PUSH abexcm1.00402035                   Title = "Error"
0040102F  .  68 3B204000   PUSH abexcm1.0040203B                   Text = "Nah... This is not a CD-ROM Drive!"
00401034  .  6A 00         PUSH 0                                  hOwner = NULL
00401036  .  E8 26000000   CALL <JMP.&USER32.MessageBoxA>          MessageBoxA
0040103B  .v EB 13         JMP SHORT abexcm1.00401050
0040103D  >  6A 00         PUSH 0                                  Style = MB_OK|MB_APPLMODAL
0040103F  .  68 5E204000   PUSH abexcm1.0040205E                   Title = "YEAH!"
00401044  .  68 64204000   PUSH abexcm1.00402064                   Text = "Ok, I really think that your HD is a CD-ROM! :p"
00401049  .  6A 00         PUSH 0                                  hOwner = NULL
0040104B  .  E8 11000000   CALL <JMP.&USER32.MessageBoxA>          MessageBoxA
00401050  >  E8 06000000   CALL <JMP.&KERNEL32.ExitProcess>        ExitProcess
00401055  $- FF25 5030                                             DriveTypeA
0040105B  .- FF25 5430                                             tProcess
0040103D=abexcm1.00401
```

Assemble at 00401026

JMP SHORT 0040103D

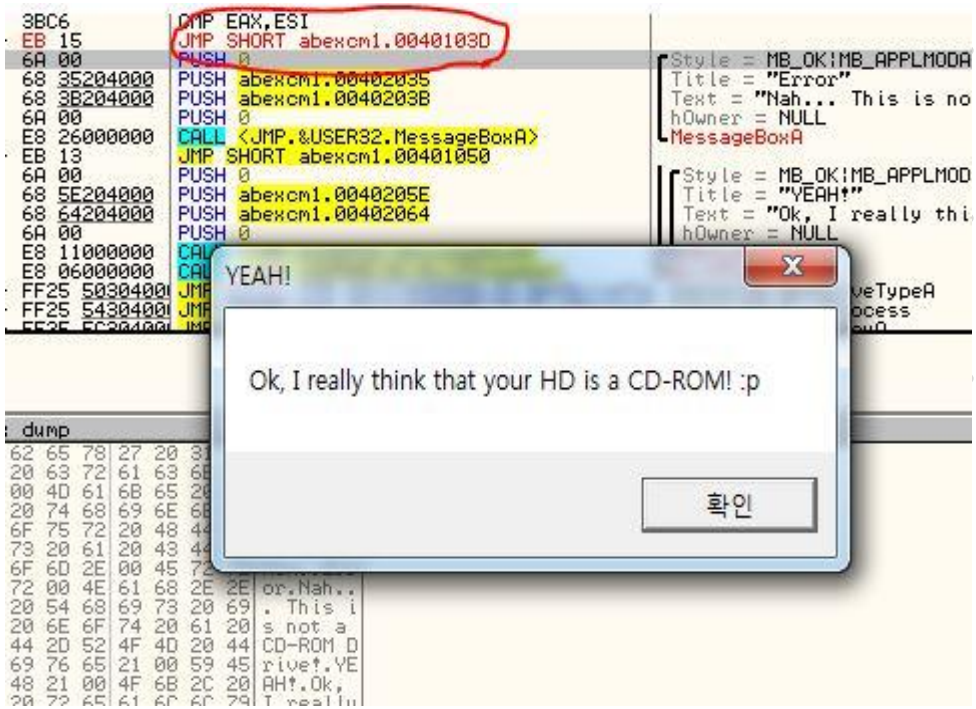
☑ Fill with NOP's

Assemble | Cancel

Address	Hex dump
00402000	61 62 65 78
00402008	74 20 63 72
00402010	65 00 4D 61

GetDriveTypeA함수가 끝나는 지점인 **00401026**에서 바로 성공메시지를 출력시키는 주소로 분기되도록 수정한다.

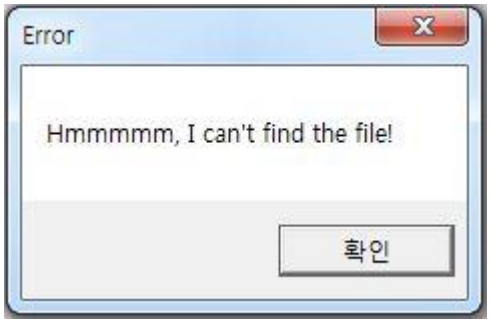
Crack Me #1 – ollydbg 크랙킹



0040103D로 분기되도록 수정된 것을 확인 할 수 있고, 실행 결과 성공 메시지가 출력된 것을 확인 했다.

- 크랙킹 성공!

Abex의 Crack Me! #3



- Abex의 Crack Me 세번째 문제.
- 프로그램이 keyfile을 인식하도록 만들어야 한다.

Crack Me #3 – ollydbg 분석

```
00401000  $  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
00401002  .  68 00204000    PUSH abexcm3.00402000                    Title = "abex' 3rd crackme"
00401007  .  68 12204000    PUSH abexcm3.00402012                    Text = "Click OK to check for the keyfile."
0040100C  .  6A 00          PUSH 0                                   hOwner = NULL
0040100E  .  E8 8C000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
00401013  .  6A 00          PUSH 0                                   hTemplateFile = NULL
00401015  .  68 80000000    PUSH 80                                  Attributes = NORMAL
0040101A  .  6A 03          PUSH 3                                   Mode = OPEN_EXISTING
0040101C  .  6A 00          PUSH 0                                   pSecurity = NULL
```

00401000부터 0040100C까지 PUSH를 이용하여 MessageBoxA 함수에 필요한 값을 스택에 올리고 있다.

```
00401041  .  E8 4D000000    CALL <JMP.&KERNEL32.GetFileSize>         GetFileSize
00401046  .  83F8 12        CMP EAX,12
00401049  .v 75 15          JNZ SHORT abexcm3.00401060
0040104B  .  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
0040104D  .  68 35204000    PUSH abexcm3.00402035                    Title = "Well done!"
00401052  .  68 40204000    PUSH abexcm3.00402040                    Text = "Yep, keyfile found!"
00401057  .  6A 00          PUSH 0                                   hOwner = NULL
00401059  .  E8 41000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
0040105E  .v EB 28          JMP SHORT abexcm3.00401088
00401060  >  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
00401062  .  68 79204000    PUSH abexcm3.00402079                    Title = "Error"
00401067  .  68 7F204000    PUSH abexcm3.0040207F                    Text = "The found file is not a valid keyfile!"
0040106C  .  6A 00          PUSH 0                                   hOwner = NULL
0040106E  .  E8 2C000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
00401073  .v EB 13          JMP SHORT abexcm3.00401088
00401075  >  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
00401077  .  68 54204000    PUSH abexcm3.00402054                    Title = "Error"
0040107C  .  68 5A204000    PUSH abexcm3.0040205A                    Text = "Hmmmm, I can't find the file!"
00401081  .  6A 00          PUSH 0                                   hOwner = NULL
00401083  .  E8 17000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
00401088  >  E8 0C000000    CALL <JMP.&KERNEL32.ExitProcess>         ExitProcess
0040108D  $- FF25 5430400   JMP DWORD PTR DS:[<&KERNEL32.CreateFile  kernel32.CreateFileA
00401093  $- FF25 5830400   JMP DWORD PTR DS:[<&KERNEL32.GetFileSiz  kernel32.GetFileSize
00401099  .- FF25 5C30400   JMP DWORD PTR DS:[<&KERNEL32.ExitProces  kernel32.ExitProcess
0040109F  $- FF25 6430400   JMP DWORD PTR DS:[<&USER32.MessageBoxA>  USER32.MessageBoxA
004010A5     00             DB 00
004010A6     00             DB 00
004010A7     00             DB 00
004010A8     00             DB 00
```

Crack Me #3 – ollydbg 분석

```
00401000  $  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
00401002  .  68 00204000    PUSH abexcm3.00402000                    Title = "abex' 3rd crackme"
00401007  .  68 12204000    PUSH abexcm3.00402012                    Text = "Click OK to check for the keyfile."
0040100C  .  6A 00          PUSH 0                                   hOwner = NULL
0040100E  .  E8 8C000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
00401013  .  6A 00          PUSH 0                                   hTemplateFile = NULL
00401015  .  68 80000000    PUSH 80                                  Attributes = NORMAL
0040101A  .  6A 03          PUSH 3                                   Mode = OPEN_EXISTING
0040101C  .  6A 00          PUSH 0                                   pSecurity = NULL
0040101E  .  6A 00          PUSH 0                                   ShareMode = 0
00401020  .  68 00000080    PUSH 80000000                            Access = GENERIC_READ
00401025  .  68 B8204000    PUSH abexcm3.004020B8                    FileName = "abex.key"
0040102A  .  E8 5E000000    CALL <JMP.&KERNEL32.CreateFileA>         CreateFileA
0040102F  .  A3 CA204000    MOV DWORD PTR DS:[4020CA],EAX
00401034  .  83F8 FF        CMP EAX,-1
00401037  .v 74 3C          JE SHORT abexcm3.00401075
00401039  .  6A 00          PUSH 0                                   pFileSizeHigh = NULL
0040103B  .  FF35 CA204000  PUSH DWORD PTR DS:[4020CA]               hFile = NULL
00401041  .  E8 4D000000    CALL <JMP.&KERNEL32.GetFileSize>         GetFileSize
00401046  .  83F8 12        CMP EAX,12
00401067  .  68 7F204000    PUSH abexcm3.0040207F                    Text = "The found file is not a valid keyfile!"
0040106C  .  6A 00          PUSH 0                                   hOwner = NULL
0040106E  .  E8 2C000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
00401073  .v EB 13          JMP SHORT abexcm3.00401088
00401075  >  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
00401077  .  68 54204000    PUSH abexcm3.00402054                    Title = "Error"
0040107C  .  68 5A204000    PUSH abexcm3.0040205A                    Text = "Hmmmm, I can't find the file!"
00401081  .  6A 00          PUSH 0                                   hOwner = NULL
00401083  .  E8 17000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
00401088  >  E8 0C000000    CALL <JMP.&KERNEL32.ExitProcess>         ExitProcess
0040108D  $- FF25 5430400   JMP DWORD PTR DS:[<&KERNEL32.CreateFile  kernel32.CreateFileA
00401093  $- FF25 5830400   JMP DWORD PTR DS:[<&KERNEL32.GetFileSiz  kernel32.GetFileSize
00401099  .- FF25 5C30400   JMP DWORD PTR DS:[<&KERNEL32.ExitProces  kernel32.ExitProcess
0040109F  $- FF25 6430400   JMP DWORD PTR DS:[<&USER32.MessageBoxA>  USER32.MessageBoxA
004010A5     00             DB 00
004010A6     00             DB 00
004010A7     00             DB 00
004010A8     00             DB 00
```

CreateFileA 함수는 매개변수로 쓰는 파일이 있다면 파일의 핸들 값을 가져오고, 없다면 오류 값을 리턴한다.

Crack Me #3 – ollydbg 분석

```
00401000  $  6A 00          PUSH 0                                  Style = MB_OK|MB_APPLMODAL
00401002  .  68 00204000    PUSH abexcm3.00402000                   Title = "abex' 3rd crackme"
00401007  .  68 12204000    PUSH abexcm3.00402012                   Text = "Click OK to check for the keyfile."
0040100C  .  6A 00          PUSH 0                                  hOwner = NULL
0040100F  .  E8 8C000000    CALL <JMP.&USER32.MessageBoxA>          MessageBoxA
00401013  .  6A 00          PUSH 0                                  hTemplateFile = NULL
00401015  .  68 80000000    PUSH 80                                 Attributes = NORMAL
0040101A  .  6A 03          PUSH 3                                  Mode = OPEN_EXISTING
0040101C  .  6A 00          PUSH 0                                  pSecurity = NULL
0040101E  .  6A 00          PUSH 0                                  ShareMode = 0
00401020  .  68 00000080    PUSH 80000000                           Access = GENERIC_READ
00401025  .  68 B9204000    PUSH abexcm3.004020B9                   FileName = "abex.l2c"
0040102A  .  E8 5E000000    CALL <JMP.&KERNEL32.CreateFileA>        CreateFileA
0040102F  .  A3 CA204000    MOV DWORD PTR DS:[4020CA],EAX
00401034  .  83F8 FF        CMP EAX,-1
00401037  .v 74 3C          JE SHORT abexcm3.00401075
00401039  .  6A 00          PUSH 0                                  pFileSizeHigh = NULL
0040103B  .  FF35 CA204000  PUSH DWORD PTR DS:[4020CA]              hFile = NULL
00401041  .  E8 4D000000    CALL <JMP.&KERNEL32.GetFileSize>        GetFileSize
00401046  .  83F8 12        CMP EAX,12
00401067  .  68 7F204000    PUSH abexcm3.0040207F                   Text = "The found file is not a valid keyfile!"
0040106C  .  6A 00          PUSH 0                                  hOwner = NULL
0040106E  .  E8 2C000000    CALL <JMP.&USER32.MessageBoxA>          MessageBoxA
00401073  .v EB 13          JMP SHORT abexcm3.00401088
00401075  >  6A 00          PUSH 0                                  Style = MB_OK|MB_APPLMODAL
00401077  .  68 54204000    PUSH abexcm3.00402054                   Title = "Error"
0040107C  .  68 5A204000    PUSH abexcm3.0040205A                   Text = "Hmmmm, I can't find the file!"
00401081  .  6A 00          PUSH 0                                  hOwner = NULL
00401083  .  E8 17000000    CALL <JMP.&USER32.MessageBoxA>          MessageBoxA
00401088  >  E8 0C000000    CALL <JMP.&KERNEL32.ExitProcess>        ExitProcess
0040108D  $- FF25 5430400   JMP DWORD PTR DS:[<&KERNEL32.CreateFile  kernel32.CreateFileA
00401093  $- FF25 5830400   JMP DWORD PTR DS:[<&KERNEL32.GetFileSiz  kernel32.GetFileSize
00401099  .- FF25 5C30400   JMP DWORD PTR DS:[<&KERNEL32.ExitProces  kernel32.ExitProcess
0040109F  $- FF25 6430400   JMP DWORD PTR DS:[<&USER32.MessageBoxA>  USER32.MessageBoxA
004010A5     00             DB 00
004010A6     00             DB 00
004010A7     00             DB 00
004010A8     00             DB 00
```

0040101A에서 파일이 존재하는지 확인한다.
00401025에서 파일 이름이 **'abex.l2c'**인 **keyfile**을 요구한다.

Crack Me #3 – ollydbg 분석

```
00401000  $  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
00401002  .  68 00204000    PUSH abexcm3.00402000                    Title = "abex' 3rd crackme"
00401007  .  68 12204000    PUSH abexcm3.00402012                    Text = "Click OK to check for the keyfile."
0040100C  .  6A 00          PUSH 0                                   hOwner = NULL
0040100E  .  E8 8C000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
00401013  .  6A 00          PUSH 0                                   hTemplateFile = NULL
00401015  .  68 80000000    PUSH 80                                  Attributes = NORMAL
0040101A  .  6A 03          PUSH 3                                   Mode = OPEN_EXISTING
0040101C  .  6A 00          PUSH 0                                   pSecurity = NULL
0040101E  .  6A 00          PUSH 0                                   ShareMode = 0
00401020  .  68 00000080    PUSH 80000000                            Access = GENERIC_READ
00401025  .  68 B9204000    PUSH abexcm3.004020B9                    FileName = "abex.l2c"
0040102F  .  A3 CA204000    MOV DWORD PTR DS:[4020CA],EAX
00401034  .  83F8 FF        CMP EAX,-1
00401037  .v 74 3C          JE SHORT abexcm3.00401075
0040103B  .  FF35 CA204000  PUSH DWORD PTR DS:[4020CA]               hFile = NULL
00401041  .  E8 4D000000    CALL <JMP.&KERNEL32.GetFileSize>         GetFileSize
00401046  .  83F8 12        CMP EAX,12
0040106E  .  E8 2C000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
00401073  .v EB 13          JMP SHORT abexcm3.00401088
00401075  >  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
00401077  .  68 54204000    PUSH abexcm3.00402054                    Title = "Error"
0040107C  .  68 5A204000    PUSH abexcm3.0040205A                    Text = "Hmmmm, I can't find the file!"
00401081  .  6A 00          PUSH 0                                   hOwner = NULL
00401083  .  E8 17000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
00401088  >  E8 0C000000    CALL <JMP.&KERNEL32.ExitProcess>         ExitProcess
0040108D  $- FF25 5430400   JMP DWORD PTR DS:[<&KERNEL32.CreateFile  kernel32.CreateFileA
00401093  $- FF25 5830400   JMP DWORD PTR DS:[<&KERNEL32.GetFileSiz  kernel32.GetFileSize
00401099  .- FF25 5C30400   JMP DWORD PTR DS:[<&KERNEL32.ExitProces  kernel32.ExitProcess
0040109F  $- FF25 6430400   JMP DWORD PTR DS:[<&USER32.MessageBoxA>  USER32.MessageBoxA
004010A5     00             DB 00
004010A6     00             DB 00
004010A7     00             DB 00
004010A8     00             DB 00
```

0040102F에서 **4020CA**에 담긴 값을 **EAX**레지스터로 읽어온다.
00401034에서 **EAX**의 값과 **-1**을 비교후에 플래그 레지스터를 세팅한다.
00401037에서 값이 같다면 **00401075**로 분기.

Crack Me #3 – ollydbg 분석

```
00401000  $  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
00401002  .  68 00204000    PUSH abexcm3.00402000                    Title = "abex' 3rd crackme"
00401007  .  68 12204000    PUSH abexcm3.00402012                    Text = "Click OK to check for the keyfile."
0040100C  .  6A 00          PUSH 0                                   hOwner = NULL
0040100E  .  E8 8C000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
00401013  .  6A 00          PUSH 0                                   hTemplateFile = NULL
00401015  .  68 80000000    PUSH 80                                  Attributes = NORMAL
0040101A  .  6A 03          PUSH 3                                   Mode = OPEN_EXISTING
0040101C  .  6A 00          PUSH 0                                   pSecurity = NULL
0040101E  .  6A 00          PUSH 0                                   ShareMode = 0
00401020  .  68 00000080    PUSH 80000000                            Access = GENERIC_READ
00401025  .  68 B9204000    PUSH abexcm3.004020B9                    FileName = "abex.l2c"
0040102A  .  E8 5E000000    CALL <JMP.&KERNEL32.CreateFileA>         CreateFileA
0040102F  .  A3 CA204000    MOV DWORD PTR DS:[4020CA],EAX
00401034  .  83F8 FF        CMP EAX,-1
00401037  .v 74 3C          JE SHORT abexcm3.00401075
00401039  .  6A 00          PUSH 0                                   pFileSizeHigh = NULL
0040103B  .  FF35 CA204000  PUSH DWORD PTR DS:[4020CA]               hFile = NULL
00401041  .  E8 4D000000    CALL <JMP.&KERNEL32.GetFileSize>         GetFileSize
00401046  .  83F8 12        CMP EAX,12
00401049  .v 75 15          JNZ SHORT abexcm3.00401060
0040104B  .  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
0040104D  .  68 35204000    PUSH abexcm3.00402035                    Title = "Well done!"
00401052  .  68 40204000    PUSH abexcm3.00402040                    Text = "Yep, keyfile found!"
00401073  .v EB 13          JMP SHORT abexcm3.00401088
00401075  >  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
00401077  .  68 54204000    PUSH abexcm3.00402054                    Title = "Error"
0040107C  .  68 5A204000    PUSH abexcm3.0040205A                    Text = "Hmmmm, I can't find the file!"
00401081  .  6A 00          PUSH 0                                   hOwner = NULL
00401083  .  E8 17000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
00401088  >  E8 0C000000    CALL <JMP.&KERNEL32.ExitProcess>         ExitProcess
0040108D  $- FF25 5430400   JMP DWORD PTR DS:[<&KERNEL32.CreateFile  kernel32.CreateFileA
00401093  $- FF25 5830400   JMP DWORD PTR DS:[<&KERNEL32.GetFileSiz  kernel32.GetFileSize
00401099  .- FF25 5C30400   JMP DWORD PTR DS:[<&KERNEL32.ExitProces  kernel32.ExitProcess
0040109F  $- FF25 6430400   JMP DWORD PTR DS:[<&USER32.MessageBoxA>  USER32.MessageBoxA
004010A5     00             DB 00
004010A6     00             DB 00
004010A7     00             DB 00
004010A8     00             DB 00
```

GetFileSize 함수는 4020CA에 담긴파일의 크기를 리턴해준다.

Crack Me #3 – ollydbg 분석

00401046에서 **EAX**의 값과 **12**와 비교하여 플래그 레지스터를 세팅한다. **JNZ(Jump If Not Zero)**는 플래그 레지스터가 **0**이 아니거나 값이 같지 않을경우 지정주소로 분기한다.

```
00401000  $  6A 00          PUSH 0                                  Style = MB_OK|MB_APPLMODAL
00401002  .  68 00204000    PUSH abexcm3.00402000                   Title = "abex' 3rd crackme"
00401007  .  68 12204000    PUSH abexcm3.00402012                   Text = "Click OK to check for the keyfile."
0040100C  .  6A 00          PUSH 0                                  hOwner = NULL
0040100E  .  E8 8C000000    CALL <JMP.&USER32.MessageBoxA>          MessageBoxA
00401013  .  6A 00          PUSH 0                                  hTemplateFile = NULL
0040103B  .  FF35 CA204000  PUSH DWORD PTR DS:[4020CA]              hFile = NULL
00401041  .  E8 4D000000    CALL <JMP.&KERNEL32.GetFileSize>        GetFileSize
00401046  .  83F8 12        CMP EAX,12
00401049  .v 75 15          JNZ SHORT abexcm3.00401060
0040104B  .  6A 00          PUSH 0                                  Style = MB_OK|MB_APPLMODAL
0040104D  .  68 35204000    PUSH abexcm3.00402035                   Title = "Well done!"
00401052  .  68 40204000    PUSH abexcm3.00402040                   Text = "Yep, keyfile found!"
00401057  .  6A 00          PUSH 0                                  hOwner = NULL
00401059  .  E8 41000000    CALL <JMP.&USER32.MessageBoxA>          MessageBoxA
0040105E  .v EB 28          JMP SHORT abexcm3.00401088
00401060  >  6A 00          PUSH 0                                  Style = MB_OK|MB_APPLMODAL
00401062  .  68 79204000    PUSH abexcm3.00402079                   Title = "Error"
00401067  .  68 7F204000    PUSH abexcm3.0040207F                   Text = "The found file is not a valid keyfile!"
0040106C  .  6A 00          PUSH 0                                  hOwner = NULL
0040106E  .  E8 2C000000    CALL <JMP.&USER32.MessageBoxA>          MessageBoxA
00401073  .v EB 13          JMP SHORT abexcm3.00401088
00401075  >  6A 00          PUSH 0                                  Style = MB_OK|MB_APPLMODAL
00401077  .  68 54204000    PUSH abexcm3.00402054                   Title = "Error"
0040107C  .  68 5A204000    PUSH abexcm3.0040205A                   Text = "Hmmmmm, I can't find the file!"
00401081  .  6A 00          PUSH 0                                  hOwner = NULL
00401083  .  E8 17000000    CALL <JMP.&USER32.MessageBoxA>          MessageBoxA
00401088  >  E8 0C000000    CALL <JMP.&KERNEL32.ExitProcess>        ExitProcess
0040108D  $- FF25 5430400   JMP DWORD PTR DS:[<&KERNEL32.CreateFile  kernel32.CreateFileA
00401093  $- FF25 5830400   JMP DWORD PTR DS:[<&KERNEL32.GetFileSiz  kernel32.GetFileSize
00401099  .- FF25 5C30400   JMP DWORD PTR DS:[<&KERNEL32.ExitProces  kernel32.ExitProcess
0040109F  $- FF25 6430400   JMP DWORD PTR DS:[<&USER32.MessageBoxA>  USER32.MessageBoxA
004010A5     00             DB 00
004010A6     00             DB 00
004010A7     00             DB 00
004010A8     00             DB 00
```

Crack Me #3 – ollydbg 분석

```
00401000  $  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
00401002  .  68 00204000    PUSH abexcm3.00402000                    Title = "abex' 3rd crackme"
00401007  .  68 12204000    PUSH abexcm3.00402012                    Text = "Click OK to check for the keyfile."
0040100C  .  6A 00          PUSH 0                                   hOwner = NULL
0040100E  .  E8 8C000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
00401013  .  6A 00          PUSH 0                                   hTemplateFile = NULL
00401015  .  68 80000000    PUSH 80                                  Attributes = NORMAL
0040101A  .  6A 03          PUSH 3                                   Mode = OPEN_EXISTING
0040101C  .  6A 00          PUSH 0                                   pSecurity = NULL
```

0040104B~00401059는 성공했을 시 **MessageBoxA**함수로 성공 메시지를 띄운다.

```
00401041  .  E8 4D000000    CALL <JMP.&KERNEL32.GetFileSize>         GetFileSize
00401046  .  83F8 12        CMP EAX,12
00401049  .v 75 15          JNZ SHORT abexcm3.00401060
0040104B  .  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
0040104D  .  68 35204000    PUSH abexcm3.00402035                    Title = "Well done!"
00401052  .  68 40204000    PUSH abexcm3.00402040                    Text = "Yep, keyfile found!"
00401057  .  6A 00          PUSH 0                                   hOwner = NULL
00401059  .  E8 41000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
0040105E  .v EB 28          JMP SHORT abexcm3.00401088
00401060  >  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
00401062  .  68 79204000    PUSH abexcm3.00402079                    Title = "Error"
00401067  .  68 7F204000    PUSH abexcm3.0040207F                    Text = "The found file is not a valid keyfile!"
0040106C  .  6A 00          PUSH 0                                   hOwner = NULL
0040106E  .  E8 2C000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
00401073  .v EB 13          JMP SHORT abexcm3.00401088
00401075  >  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
00401077  .  68 54204000    PUSH abexcm3.00402054                    Title = "Error"
0040107C  .  68 5A204000    PUSH abexcm3.0040205A                    Text = "Hmmmm, I can't find the file!"
00401081  .  6A 00          PUSH 0                                   hOwner = NULL
00401083  .  E8 17000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
00401088  >  E8 0C000000    CALL <JMP.&KERNEL32.ExitProcess>         ExitProcess
0040108D  $- FF25 5430400   JMP DWORD PTR DS:[<&KERNEL32.CreateFile  kernel32.CreateFileA
00401093  $- FF25 5830400   JMP DWORD PTR DS:[<&KERNEL32.GetFileSiz  kernel32.GetFileSize
00401099  .- FF25 5C30400   JMP DWORD PTR DS:[<&KERNEL32.ExitProces  kernel32.ExitProcess
0040109F  $- FF25 6430400   JMP DWORD PTR DS:[<&USER32.MessageBoxA>  USER32.MessageBoxA
004010A5     00             DB 00
004010A6     00             DB 00
004010A7     00             DB 00
004010A8     00             DB 00
```

Crack Me #3 – ollydbg 분석

```
00401000  $  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
00401002  .  68 00204000    PUSH abexcm3.00402000                    Title = "abex' 3rd crackme"
00401007  .  68 12204000    PUSH abexcm3.00402012                    Text = "Click OK to check for the keyfile."
0040100C  .  6A 00          PUSH 0                                   hOwner = NULL
0040100E  .  E8 8C000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
00401013  .  6A 00          PUSH 0                                   hTemplateFile = NULL
00401015  .  68 80000000    PUSH 80                                  Attributes = NORMAL
0040101A  .  6A 03          PUSH 3                                   Mode = OPEN_EXISTING
0040101C  .  6A 00          PUSH 0                                   pSecurity = NULL
```

00401060~0040106E는 파일의 크기가 맞지 않을 때 **MessageBox A** 함수로 오류 메시지를 출력해준다.

```
00401041  .  E8 4D000000    CALL <JMP.&KERNEL32.GetFileSize>         GetFileSize
00401046  .  83F8 12        CMP EAX,12
00401049  .v 75 15          JNZ SHORT abexcm3.00401060
0040104B  .  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
0040104D  .  68 35204000    PUSH abexcm3.00402035                    Title = "Well done!"
00401052  .  68 40204000    PUSH abexcm3.00402040                    Text = "Yep, keyfile found!"
00401057  .  6A 00          PUSH 0                                   hOwner = NULL
00401059  .  E8 41000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
0040105E  .v EB 28          JMP SHORT abexcm3.00401088
00401060  >  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
00401062  .  68 79204000    PUSH abexcm3.00402079                    Title = "Error"
00401067  .  68 7F204000    PUSH abexcm3.0040207F                    Text = "The found file is not a valid keyfile!"
0040106C  .  6A 00          PUSH 0                                   hOwner = NULL
0040106E  .  E8 2C000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
00401073  .v EB 13          JMP SHORT abexcm3.00401088
00401075  >  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
00401077  .  68 54204000    PUSH abexcm3.00402054                    Title = "Error"
0040107C  .  68 5A204000    PUSH abexcm3.0040205A                    Text = "Hmmmmm, I can't find the file!"
00401081  .  6A 00          PUSH 0                                   hOwner = NULL
00401083  .  E8 17000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
00401088  >  E8 0C000000    CALL <JMP.&KERNEL32.ExitProcess>         ExitProcess
0040108D  $- FF25 5430400   JMP DWORD PTR DS:[<&KERNEL32.CreateFile  kernel32.CreateFileA
00401093  $- FF25 5830400   JMP DWORD PTR DS:[<&KERNEL32.GetFileSiz  kernel32.GetFileSize
00401099  .- FF25 5C30400   JMP DWORD PTR DS:[<&KERNEL32.ExitProces  kernel32.ExitProcess
0040109F  $- FF25 6430400   JMP DWORD PTR DS:[<&USER32.MessageBoxA>  USER32.MessageBoxA
004010A5     00             DB 00
004010A6     00             DB 00
004010A7     00             DB 00
004010A8     00             DB 00
```

Crack Me #3 – ollydbg 분석

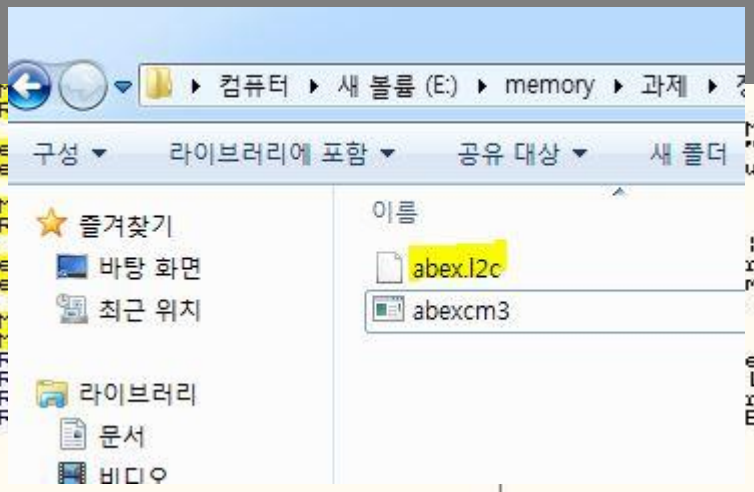
```
00401000  $  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
00401002  .  68 00204000    PUSH abexcm3.00402000                    Title = "abex' 3rd crackme"
00401007  .  68 12204000    PUSH abexcm3.00402012                    Text = "Click OK to check for the keyfile."
0040100C  .  6A 00          PUSH 0                                   hOwner = NULL
0040100E  .  E8 8C000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
00401013  .  6A 00          PUSH 0                                   hTemplateFile = NULL
00401015  .  68 80000000    PUSH 80                                  Attributes = NORMAL
0040101A  .  6A 03          PUSH 3                                   Mode = OPEN_EXISTING
0040101C  .  6A 00          PUSH 0                                   pSecurity = NULL
00401041  .  E8 4D000000    CALL <JMP.&KERNEL32.GetFileSize>         GetFileSize
00401046  .  83F8 12        CMP EAX,12
00401049  .v 75 15          JNZ SHORT abexcm3.00401060
0040104B  .  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
0040104D  .  68 35204000    PUSH abexcm3.00402035                    Title = "Well done!"
00401052  .  68 40204000    PUSH abexcm3.00402040                    Text = "Yep, keyfile found!"
00401057  .  6A 00          PUSH 0                                   hOwner = NULL
00401059  .  E8 41000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
0040105E  .v EB 28          JMP SHORT abexcm3.00401088
00401060  >  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
00401062  .  68 79204000    PUSH abexcm3.00402079                    Title = "Error"
00401067  .  68 7F204000    PUSH abexcm3.0040207F                    Text = "The found file is not a valid keyfile!"
0040106C  .  6A 00          PUSH 0                                   hOwner = NULL
0040106E  .  E8 2C000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
00401073  .v EB 13          JMP SHORT abexcm3.00401088
00401075  >  6A 00          PUSH 0                                   Style = MB_OK|MB_APPLMODAL
00401077  .  68 54204000    PUSH abexcm3.00402054                    Title = "Error"
0040107C  .  68 5A204000    PUSH abexcm3.0040205A                    Text = "Hmmmm, I can't find the file!"
00401081  .  6A 00          PUSH 0                                   hOwner = NULL
00401083  .  E8 17000000    CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
00401088  >  E8 0C000000    CALL <JMP.&KERNEL32.ExitProcess>         ExitProcess
0040108D  $- FF25 5430400   JMP DWORD PTR DS:[<&KERNEL32.CreateFile  kernel32.CreateFileA
00401093  $- FF25 5830400   JMP DWORD PTR DS:[<&KERNEL32.GetFileSiz  kernel32.GetFileSize
00401099  .- FF25 5C30400   JMP DWORD PTR DS:[<&KERNEL32.ExitProces  kernel32.ExitProcess
0040109F  $- FF25 6430400   JMP DWORD PTR DS:[<&USER32.MessageBoxA>  USER32.MessageBoxA
004010A5     00             DB 00
004010A6     00             DB 00
004010A7     00             DB 00
004010A8     00             DB 00
```

00401075~00401083은 매개변수가 되는 파일을 찾지 못했을 때 **MessageBox A** 함수로 오류 메시지를 출력해준다.

Crack Me #3 – ollydbg 크랙킹

```
00401000  $  6A 00          PUSH 0                          Style = MB_OK|MB_APPLMODAL
00401002  .  68 00204000    PUSH abexcm3.00402000           Title = "abex' 3rd crackme"
00401007  .  68 12204000    PUSH abexcm3.00402012           Text = "Click OK to check for the keyfile."
0040100C  .  6A 00          PUSH 0                          hOwner = NULL
0040100E  .  E8 8C000000    CALL <JMP.&USER32.MessageBoxA>  MessageBoxA
00401013  .  6A 00          PUSH 0                          hTemplateFile = NULL
00401015  .  68 80000000    PUSH 80                         Attributes = NORMAL
0040101A  .  6A 03          PUSH 3                          Mode = OPEN_EXISTING
0040101C  .  6A 00          PUSH 0                          pSecurity = NULL
0040101E  .  6A 00          PUSH 0                          ShareMode = 0
00401020  .  68 00000080    PUSH 80000000                   Access = GENERIC_READ
00401025  .  68 B9204000    PUSH abexcm3.004020B9           FileName = "abex.l2c"
0040102A  .  E8 5E000000    CALL <JMP.&KERNEL32.CreateFileA> CreateFileA
0040102F  .  A3 CA204000    MOV DWORD PTR DS:[4020CA],EAX
00401034  .  83F8 FF        CMP EAX,-1
00401037  .v 74 3C          JE SHORT abexcm3.00401075
00401059  .  E8 41000000    CALL <JM
0040105E  .v EB 28          JMP SHOR
00401060  >  6A 00          PUSH 0                          MB_APPLMODAL
00401062  .  68 79204000    PUSH abe                        "
00401067  .  68 7F204000    PUSH abe                        und file is not a valid keyfile!"
0040106C  .  6A 00          PUSH 0
0040106E  .  E8 2C000000    CALL <JM
00401073  .v EB 13          JMP SHOR
00401075  >  6A 00          PUSH 0                          |MB_APPLMODAL
00401077  .  68 54204000    PUSH abe                        r"
0040107C  .  68 5A204000    PUSH abe                        m, I can't find the file!"
00401081  .  6A 00          PUSH 0
00401083  .  E8 17000000    CALL <JM
00401088  >  E8 0C000000    CALL <JM
0040108D  $- FF25 5430400   JMP DWOR                        eFileA
00401093  $- FF25 5830400   JMP DWOR                        leSize
00401099  .- FF25 5C30400   JMP DWOR                        rocess
0040109F  $- FF25 6430400   JMP DWOR                        BoxA
004010A5     00             DB 00
004010A6     00             DB 00
004010A7     00             DB 00
004010A8     00             DB 00
```

Keyfile이 될 **'abex.l2c'** 라는 이름의 파일을 생성해준다.

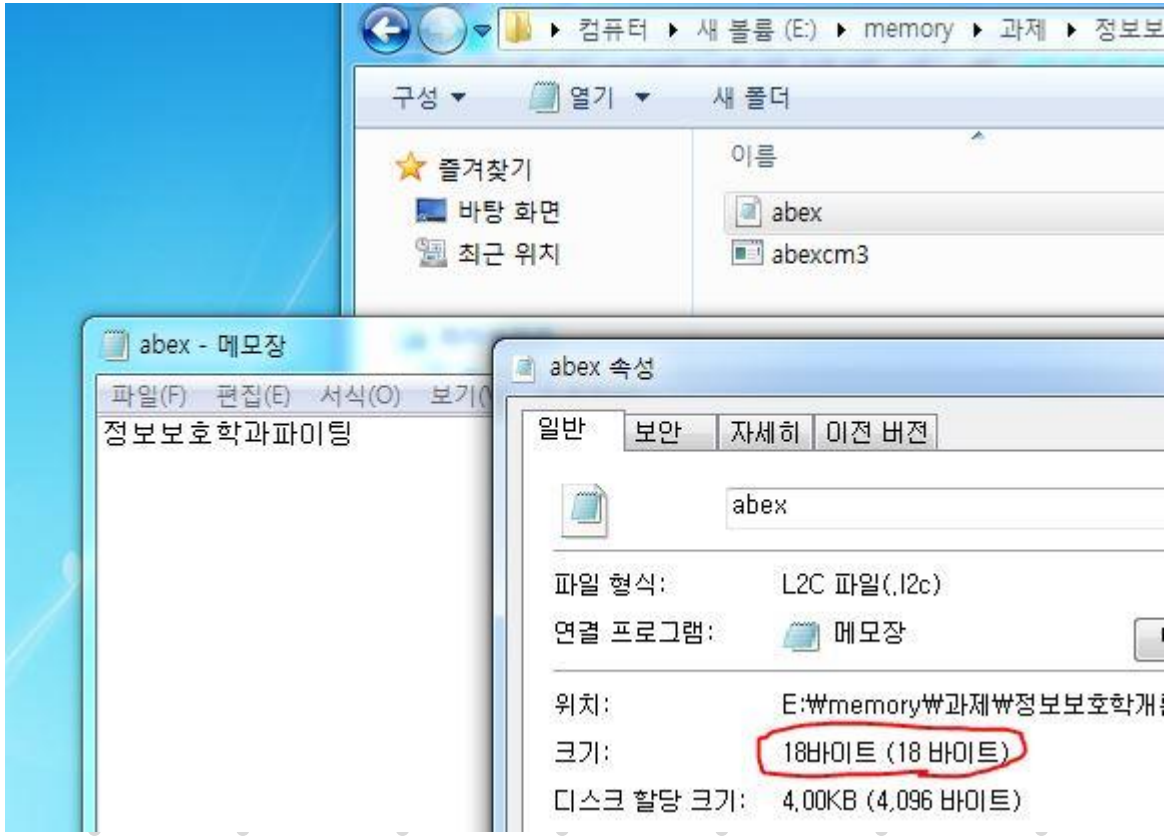


Crack Me #3 – ollydbg 크랙킹

```
00401000  $  6A 00          PUSH 0                                  Style = MB_OK|MB_APPLMODAL
00401002  .  68 00204000    PUSH abexcm3.00402000                   Title = "abex' 3rd crackme"
00401007  .  68 12204000    PUSH abexcm3.00402012                   Text = "Click OK to check for the keyfile."
0040100C  .  6A 00          PUSH 0                                  hOwner = NULL
0040100E  .  E8 8C000000    CALL <JMP.&USER32.MessageBoxA>          MessageBoxA
00401013  .  6A 00          PUSH 0                                  hTemplateFile = NULL
00401015  .  68 80000000    PUSH 80                                 Attributes = NORMAL
0040101A  .  6A 03          PUSH 3                                  Mode = OPEN_EXISTING
0040101C  .  6A 00          PUSH 0                                  pSecurity = NULL
0040101E  .  6A 00          PUSH 0                                  ShareMode = 0
00401020  .  68 00000080    PUSH 80000000                           Access = GENERIC_READ
00401025  .  68 B9204000    PUSH abexcm3.004020B9                   FileName = "abex.l2c"
00401020  .  E8 5E000000    CALL <JMP.&KERNEL32.CreateFileA>        CreateFileA
0040102F  .  A3 CA204000    MOV DWORD PTR DS:[4020CA],EAX
00401034  .  83F8 FF        CMP EAX,-1
00401037  .v 74 3C          JE SHORT abexcm3.00401075
00401039  .  6A 00          PUSH 0                                  pFileSizeHigh = NULL
0040103B  .  FF35 CA204000  PUSH DWORD PTR DS:[4020CA]              hFile = NULL
00401041  .  E8 4D000000    CALL <JMP.&KERNEL32.GetFileSize>        GetFileSize
00401046  .  83F8 12        CMP EAX,12
00401049  .v 75 15          JNZ SHORT abexcm3.00401060
0040104B  .  6A 00          PUSH 0                                  Style = MB_OK|MB_APPLMODAL
0040104D  .  68 35204000    PUSH abexcm3.00402035                   Title = "Well done!"
00401052  .  68 40204000    PUSH abexcm3.00402040                   Text = "Yep, keyfile found!"
0040107C  .  68 5A204000    PUSH abexcm3.0040205A                   Text = "Hmmmm, I can't find the file!"
00401081  .  6A 00          PUSH 0                                  hOwner = NULL
00401083  .  E8 17000000    CALL <JMP.&USER32.MessageBoxA>          MessageBoxA
00401088  >  E8 0C000000    CALL <JMP.&KERNEL32.ExitProcess>        ExitProcess
0040108D  $- FF25 5430400   JMP DWORD PTR DS:[<&KERNEL32.CreateFile  kernel32.CreateFileA
00401093  $- FF25 5830400   JMP DWORD PTR DS:[<&KERNEL32.GetFileSiz  kernel32.GetFileSize
00401099  .- FF25 5C30400   JMP DWORD PTR DS:[<&KERNEL32.ExitProces  kernel32.ExitProcess
0040109F  $- FF25 6430400   JMP DWORD PTR DS:[<&USER32.MessageBoxA>  USER32.MessageBoxA
004010A5     00             DB 00
004010A6     00             DB 00
004010A7     00             DB 00
004010A8     00             DB 00
```

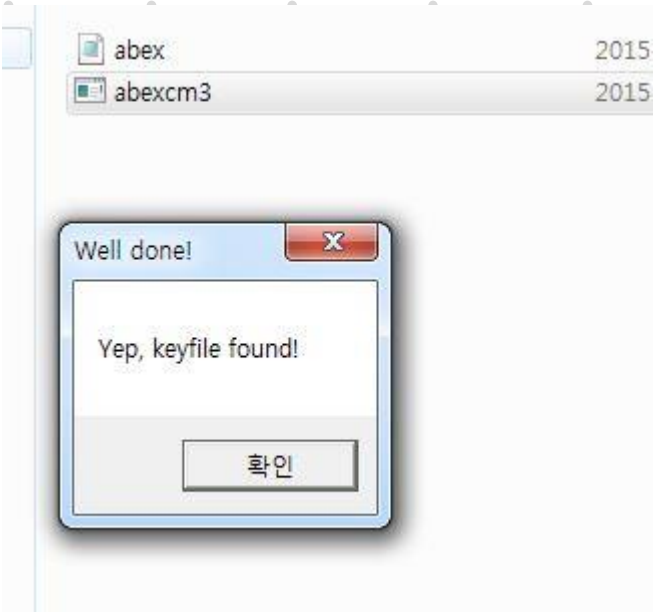
여기서, **12**는 **16**진수로 표기된 값으로, **10**진수로 바꾸면 **18**이다.

Crack Me #3 – ollydbg 크랙킹



'abex.l2c 파일의 크기를 18byte로 맞춰준다.

Crack Me #3 – ollydbg 크랙킹



실행 시에 성공 메시지가 출력 되는 것을 확인 할 수 있다.

-크랙킹 성공!

Abex의 Crack Me 실습을 통해서

- 디버깅 프로그램인 ollydbg를 통한 프로그램 분석 방법을 배울 수 있었다.
- 프로그램 알고리즘을 분석, 무력화하여 크랙킹을 직접 해볼 수 있었다.

Q&A!

감사합니다!