

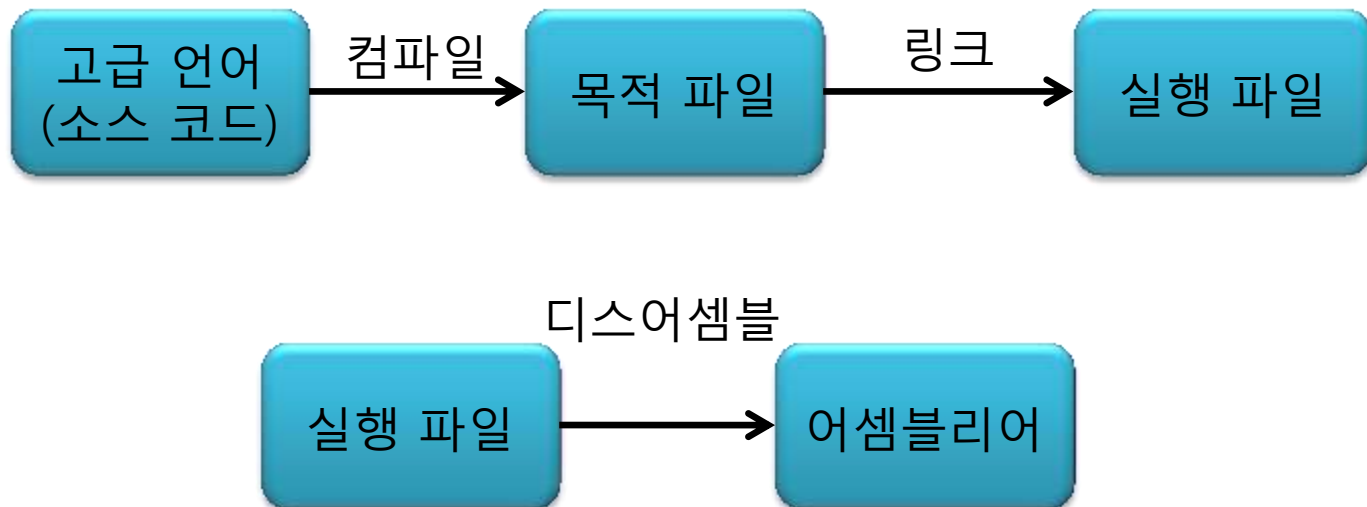
보안실습 3-1

Reverse Engineering (리버스 엔지니어링)

완성된 제품을 분석하여 제품의 기본적인 설계 개념과 적용 기술을 파악하고 재현하는 것.

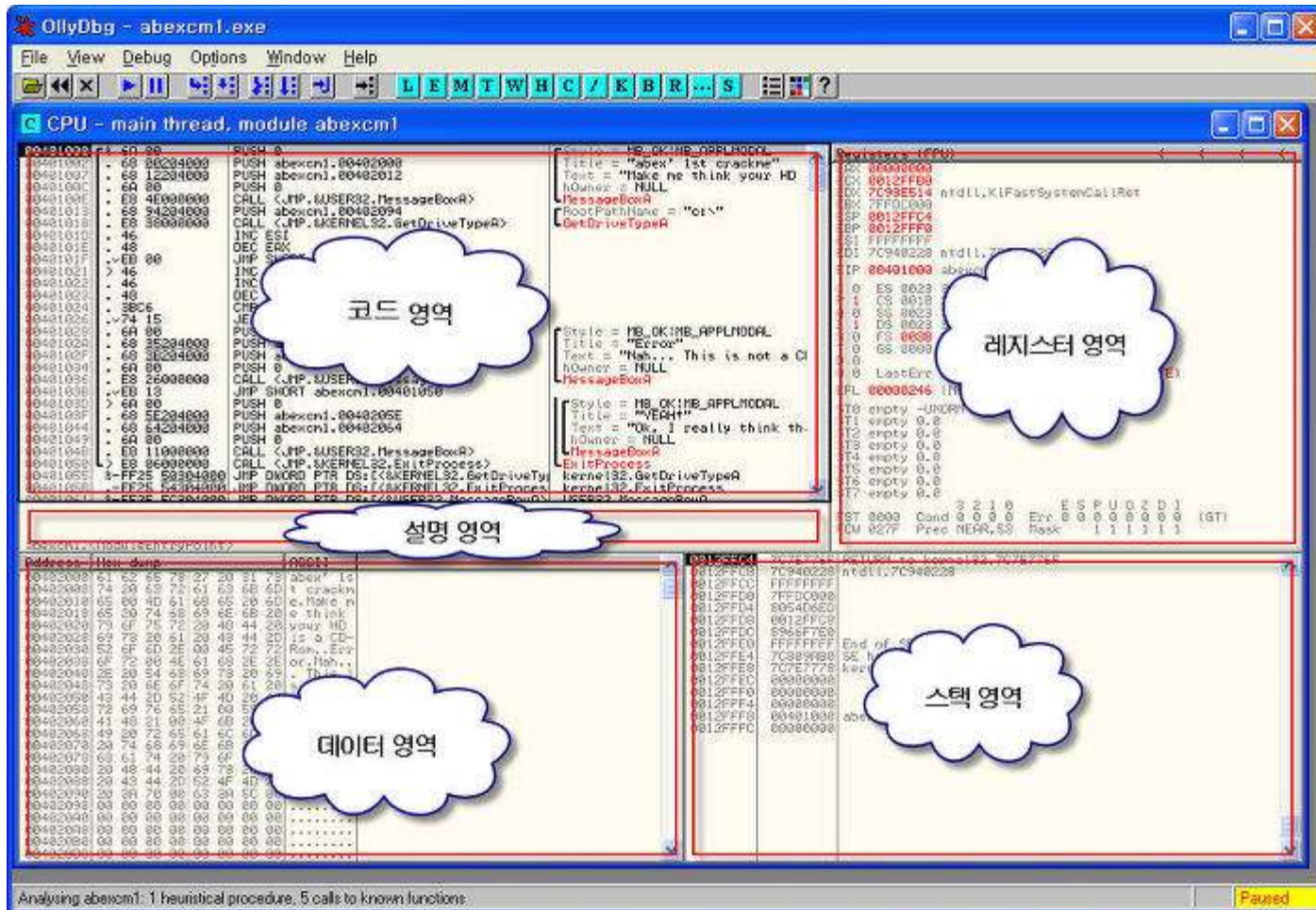
실행 파일을 수정하거나 프로그램의 동작을 변경할 수 있고, 또 유사한 동작의 복제 프로그램이나 보다 기능이 향상된 프로그램도 개발할 수 있다. 소프트웨어에 대한 역공학 자체는 위법 행위가 아니지만, 대부분의 제품이 이의 **금지를 명문화**하고 있어 이러한 수법으로 개발한 제품은 **지적 재산을 침해**할 위험성이 있다.

[출처] 두산동아, TTA 한국정보통신기술협회



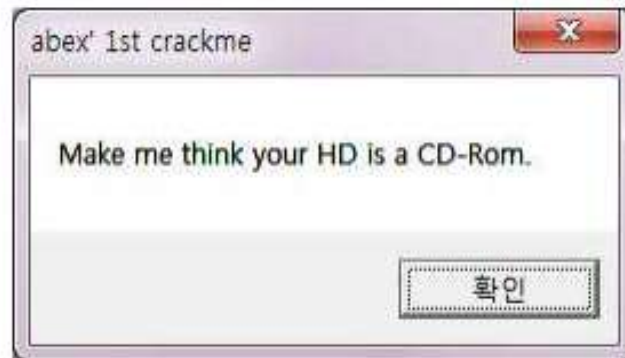
보안실습 3-1

Ollydbg 설명

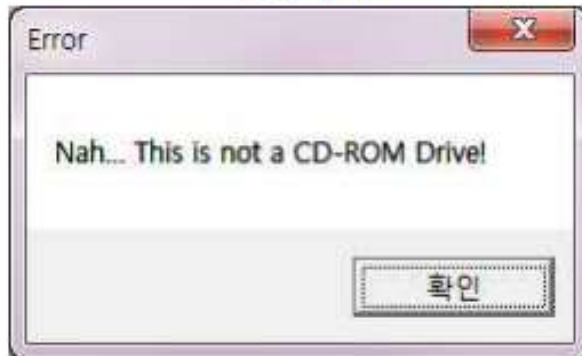


보안실습 3-1

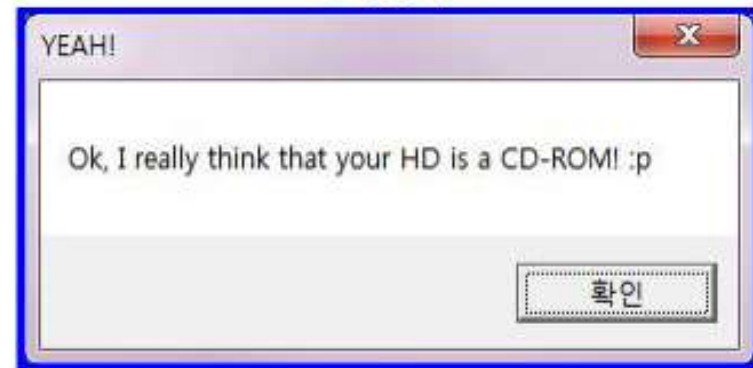
실습 프로그램 흐름



①실패시



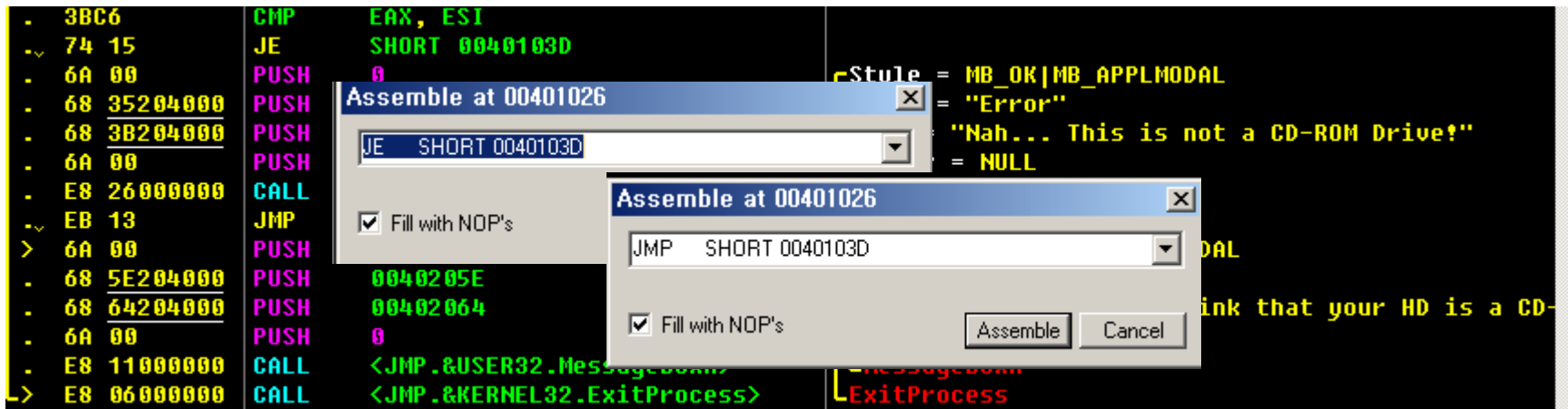
②성공시



보안실습 3-1

Solution 1

1. File -> Open-> 실습파일 선택
2. 00401024 JE SHORT abexcm_1.0040103D -> JMP SHORT 0040103D
3. 분기문(JE)를 무조건분기문(JMP)로 수정



```
- 3BC6      CMP     EAX, ESI
~ 74 15      JE      SHORT 0040103D
- 6A 00      PUSH    0
- 68 35204000 PUSH    0
- 68 3B204000 PUSH    0
- 6A 00      PUSH    0
- E8 26000000 CALL    00401000
~ EB 13      JMP     0040103D
> 6A 00      PUSH    0
- 68 5E204000 PUSH    0040205E
- 68 64204000 PUSH    00402064
- 6A 00      PUSH    0
- E8 11000000 CALL    <JMP.&USER32.MessageBox>
L> E8 06000000 CALL    <JMP.&KERNEL32.ExitProcess>
```

Assemble at 00401026

JE SHORT 0040103D

☒ Fill with NOP's

Assemble at 00401026

JMP SHORT 0040103D

☒ Fill with NOP's

Assemble Cancel

※ JE = Jump if Equal

보안실습 3-1

Solution 2

1. File -> Open-> 실습파일 선택
2. CMP EAX, ESI 수행시 레지스터 값 변경
3. 실행

The screenshot displays a debugger window with assembly code on the left and a register list on the right. Two 'Modify EAX' dialog boxes are overlaid on the assembly code.

Assembly Code (Left):

```
PUSH 00402000
PUSH 00402012
PUSH 0
CALL <JMP.&USER32.Mes
PUSH 00402094
CALL <JMP.&KERNEL32.G
INC ESI
DEC EAX
JMP SHORT 00401021
INC ESI
INC ESI
DEC EAX
CMP EAX, ESI
JE SHORT 0040103D
```

Register List (Right):

```
EAX 00000001
ECX 76F838AA ntdll.76F838AA
EDX 0088D6B8
EBX 7EFDE000
ESP 0018FF8C
EBP 0018FF94
ESI 00000003
EDI 00000000
EIP 00401024 abexcm1.00401024
C 0 ES 002B 32bit 0(FFFFFFFF)
P 0 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 0 DS 002B 32bit 0(FFFFFFFF)
```

Modify EAX Dialog (Left):

- Hexadecimal: 00000001
- Signed: 1
- Unsigned: 1
- Char: \x00 \x00 \x00 \x00

Modify EAX Dialog (Right):

- Hexadecimal: 00000003
- Signed: 3
- Unsigned: 3
- Char: \x00 \x00 \x00 \x03