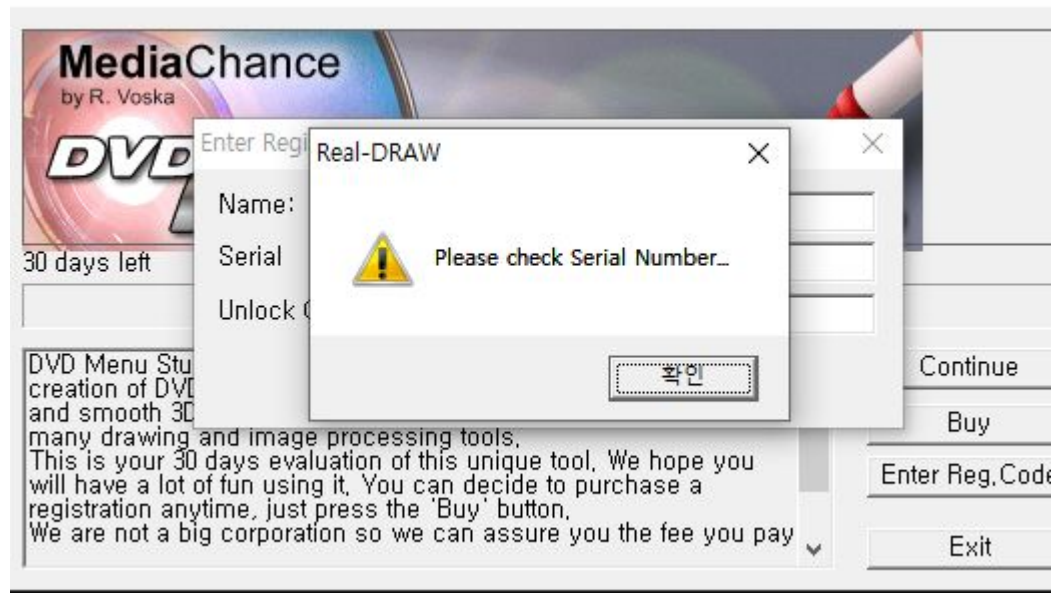
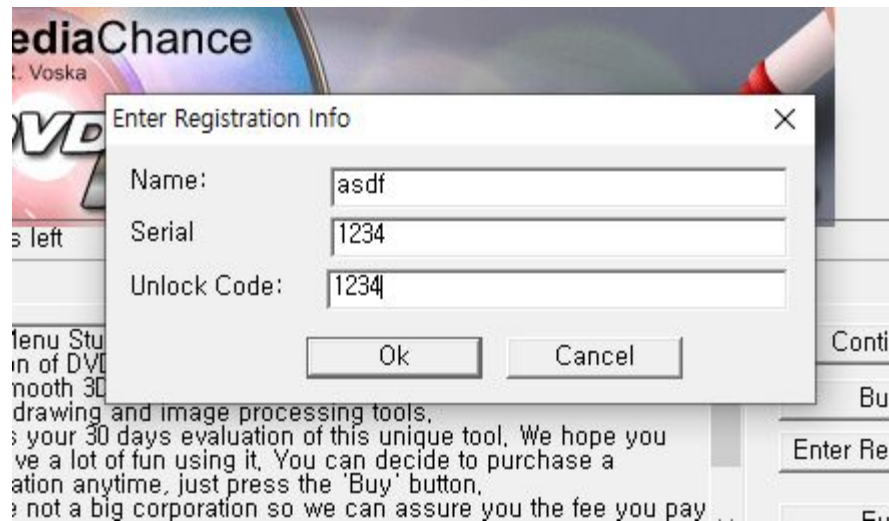


프로그램 시작시 나타나는 화면이다.
30일 남았다는 메시지가 나오고,
등록하라는 화면과 함께 **Name**,
Serial, **Unlock Code**를 입력하라고
나오고, 시리얼 번호를 잘못 입력시
오류 메시지가 뜬다.



시리얼 코드를 잘못 입력하면, 해당 오류메시지가 뜬다. 문자열을 검색해 해당 영역으로 이동한다.



아까 검색한 문자열에 **bp**를 걸고
필드를 모두 채우고 실행한다.

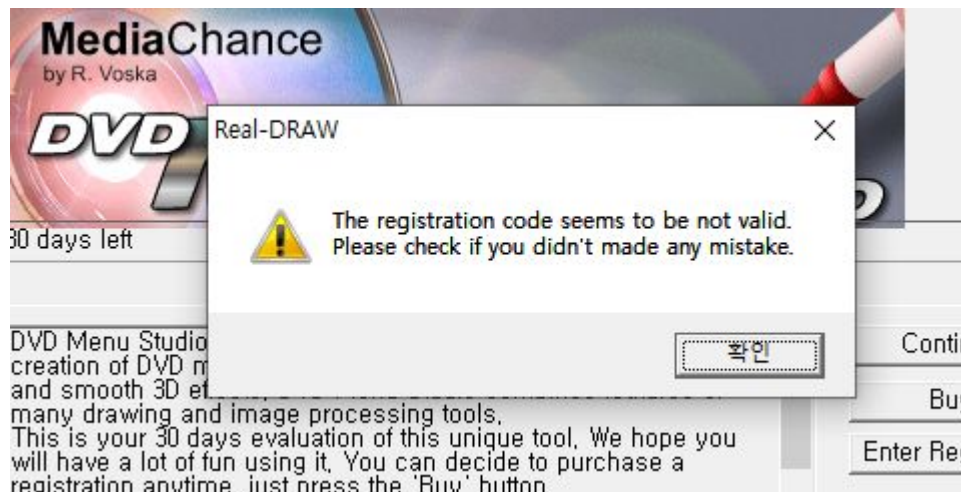
그러면 해당 영역에서 멈추게된다.

첫번째 문자열은 **name** 필드를
채우지 않았을 경우 나오는 메시지
같고, 두번째는 시리얼 번호를
틀렸을 경우 나오는 메시지다.

| | | | |
|----------|---------------|--------------------------------|--|
| 00522368 | > 1BC0 | SBB EAX, EAX | |
| 0052236A | > 83D8 FF | SBB EAX, -1 | |
| 0052236C | > 85C0 | TEST EAX, EAX | |
| 00522371 | > 75 10 | JNZ SHORT DVDMenuS.00522383 | |
| 00522373 | . 50 | PUSH EAX | [Arg3 Arg2 Arg1 = 00648878 ASCII "Please enter your name" DVDMenuS.005B5F4C |
| 00522374 | . 50 | PUSH EAX | |
| 00522375 | . 68 78886400 | PUSH DVDMenuS.00648878 | |
| 0052237A | . E8 CD3B0900 | CALL DVDMenuS.005B5F4C | |
| 0052237F | . 5F | POP EDI | |
| 00522380 | . 5E | POP ESI | |
| 00522381 | . 5B | POP EBX | |
| 00522382 | . C3 | RETN | |
| 00522383 | > 8B43 60 | MOV EAX, DWORD PTR DS:[EBX+60] | |
| 00522386 | . 6A 00 | PUSH 0 | [Arg3 = 00000000 Arg2 = 00000000 Arg1 = 00648858 ASCII "Please check Serial Number..." DVDMenuS.005B5F4C |
| 0052238B | . 8378 F8 08 | CMP DWORD PTR DS:[EAX-8], 8 | |
| 0052238C | > 7D 10 | JGE SHORT DVDMenuS.0052239E | |
| 0052238E | . 6A 00 | PUSH 0 | |
| 00522390 | . 68 58886400 | PUSH DVDMenuS.00648858 | |
| 00522395 | . E8 B23B0900 | CALL DVDMenuS.005B5F4C | |
| 0052239A | . 5F | POP EDI | |
| 0052239B | . 5E | POP ESI | |
| 0052239C | . 5B | POP EBX | |
| 0052239D | . C3 | RETN | |

| | | | |
|----------|---------------|-------------------------------|---|
| 00522381 | . 5E | POP EBX | |
| 00522382 | . C3 | RETN | |
| 00522383 | > 8B43 60 | MOV EAX,DWORD PTR DS:[EBX+60] | |
| 00522386 | . 6A 00 | PUSH 0 | |
| 0052238E | . 8378 F8 08 | CMPL DWORD PTR DS:[EAX-8],8 | Arg3 = 00000000 |
| 0052239C | . 7D 10 | JGE SHORT DVDMenuS.0052239E | |
| 0052239E | . 6A 00 | PUSH 0 | Arg2 = 00000000 |
| 00522398 | . 68 58886400 | PUSH DVDMenuS.00648858 | Arg1 = 00648858 ASCII "Please check Serial Number..." |
| 00522395 | . E8 B23B0900 | CALL DVDMenuS.005B5F4C | DVDMenuS.005B5F4C |
| 0052239A | . 5F | POP EDI | |
| 00522398 | . 5E | POP ESI | |
| 0052239C | . 5B | POP EBX | |
| 0052239D | . C3 | RETN | |
| 0052239E | \ 8BFB | MOVB EBX,EBX | |

두번째 문자열은 입력한 시리얼 코드의 길이를 비교한다. 8 미만이면 해당 오류를 출력한다. 즉, 시리얼 코드의 길이는 8이상이어야 된다.



이번에는 시리얼 코드를 8글자 이상 입력하고 실행했더니 시리얼 번호가 맞지 않는다고 나온다. 해당 오류 메시지로 검색을 해본다.

| | | | |
|----------|-----------------|---|--|
| 004DC19D | > 83F8 03 | CMP EAX,3 | |
| 004DC1A0 | .v75 1E | JNZ SHORT DVDMenuS.004DC1C0 | |
| 004DC1A2 | . 8B57 1C | MOV EDX,DWORD PTR DS:[EDI+1C] | |
| 004DC1A5 | . 50 | PUSH EAX | |
| 004DC1A6 | . 52 | PUSH EDX | |
| 004DC1A7 | . FF15 B4575E00 | CALL DWORD PTR DS:[<&USER32.KillTimer>] | [TimerID hWnd KillTimer |
| 004DC1AC | . 6A 00 | PUSH 0 | Arg3 = 00000000 |
| 004DC1AF | . 6A 00 | PUSH 0 | Arg2 = 00000000 |
| 004DC1B1 | . 68 5C666400 | PUSH DVDMenuS.0064665C | Arg1 = 0064665C ASCII "The registration |
| 004DC1B6 | . E8 919D0000 | CALL DVDMenuS.005B5F4C | DVDMenuS.005B5F4C |
| 004DC1BB | .vE9 B7000000 | JMP DVDMenuS.004DC277 | |
| 004DC1C0 | > 83F8 04 | CMP EAX,4 | |
| 004DC1C3 | .v75 1E | JNZ SHORT DVDMenuS.004DC1E3 | |
| 004DC1C5 | . 50 | PUSH EAX | [TimerID hWnd KillTimer |
| 004DC1C6 | . 8B47 1C | MOV EAX,DWORD PTR DS:[EDI+1C] | Arg3 = 00000000 |
| 004DC1C9 | . 50 | PUSH EAX | Arg2 = 00000000 |
| 004DC1CA | . FF15 B4575E00 | CALL DWORD PTR DS:[<&USER32.KillTimer>] | Arg1 = 0064665C ASCII "Thank you for you |
| 004DC1D0 | . 6A 00 | PUSH 0 | DVDMenuS.005B5F4C |
| 004DC1D2 | . 6A 00 | PUSH 0 | |
| 004DC1D4 | . 68 FC656400 | PUSH DVDMenuS.006465FC | |
| 004DC1D9 | . E8 6E9D0000 | CALL DVDMenuS.005B5F4C | |
| 004DC1DE | .vE9 94000000 | JMP DVDMenuS.004DC277 | |
| 004DC1E3 | > 83F8 05 | CMP EAX,5 | |
| 004DC1E6 | .v75 15 | JNZ SHORT DVDMenuS.004DC1FD | |
| 004DC1E8 | . 8B4F 1C | MOV ECX,DWORD PTR DS:[EDI+1C] | [TimerID |
| 004DC1EB | . 50 | PUSH EAX | |

해당 부분에서 멈추게 된다. 두개의 메시지가 보이고, 위에는 시간과 관련된 함수가 보인다.

밑에 두 메시지는 등록 성공/실패시 보이는 메시지다.

4DC1A0부분에서 분기를 결정한다.EAX 값과 비교해 3과 같으면

| | | | |
|----------|-----------------|---|---------|
| 004DC02E | . 8BC8 | MOV ECX,EAX | |
| 004DC030 | . E8 50A00D00 | CALL DVDMenuS.005B6085 | LDVDM |
| 004DC035 | . 8D4D EC | LEA ECX,DWORD PTR SS:[EBP-14] | |
| 004DC038 | . C745 FC FFFF | MOV DWORD PTR SS:[EBP-4],-1 | |
| 004DC03F | . E8 27DD0C00 | CALL DVDMenuS.005A9D6B | |
| 004DC044 | . E9 2E020000 | JMP DVDMenuS.004DC277 | |
| 004DC049 | > 83F8 02 | CMP EAX,2 | |
| 004DC04C | . 0F85 4B010000 | JNZ DVDMenuS.004DC19D | |
| 004DC052 | . 8B57 1C | MOV EDX,DWORD PTR DS:[EDI+1C] | |
| 004DC055 | . 50 | PUSH EAX | Timer |
| 004DC056 | . 52 | PUSH EDX | hWnd |
| 004DC057 | . FF15 B4575E00 | CALL DWORD PTR DS:[<&USER32.KillTimer>] | KillTim |
| 004DC05D | . E8 E7590E00 | CALL DVDMenuS.005C1A49 | |
| 004DC062 | . 8B70 04 | MOV ESI,DWORD PTR DS:[EAX+4] | |
| 004DC065 | . 6A 00 | PUSH 0 | rArg1 |

4DC1A0 함수는 해당 영역에서
분기되는걸 알 수 있다.

| | | | |
|----------|-----------------|---|--------------|
| 004DBDEB | . 68 F4010000 | PUSH 1F4 | Timeout = 50 |
| 004DBDF0 | . 6A 02 | PUSH 2 | TimerID = 2 |
| 004DBDF2 | . 52 | PUSH EDX | hWnd |
| 004DBDF3 | . FF15 B8575E00 | CALL DWORD PTR DS:[<&USER32.SetTimer>] | SetTimer |
| 004DBDF9 | . E9 79040000 | JMP DVDMenuS.004DC277 | |
| 004DBDFE | > 83F8 07 | CMP EAX,7 | |
| 004DBE01 | . 0F85 42020000 | JNZ DVDMenuS.004DC049 | |
| 004DBE07 | . 50 | PUSH EAX | TimerID |
| 004DBE08 | . 8B47 1C | MOV EAX,DWORD PTR DS:[EDI+1C] | |
| 004DBE0B | . 50 | PUSH EAX | hWnd |
| 004DBE0C | . FF15 B4575E00 | CALL DWORD PTR DS:[<&USER32.KillTimer>] | KillTimer |
| 004DBE12 | . E8 325C0E00 | CALL DVDMenuS.005C1A49 | |
| 004DBE17 | . 8B40 04 | MOV EAX,DWORD PTR DS:[EAX+4] | |
| 004DBE1A | . 8D4D EC | LEA ECX,DWORD PTR SS:[EBP-14] | |

또 40C04C는 40BE01 부분에서
분기하는걸 알 수 있다.

이렇게 분기문을 쭉 따라가다 보면
최초로 시작되는 부분을 찾을 수 있다.

| | | | |
|----------|--------------------|---|---------|
| 004DBD80 | . 55 | PUSH EBP | |
| 004DBD81 | . 8BEC | MOV EBP,ESP | |
| 004DBD83 | . 6A FF | PUSH -1 | SE hand |
| 004DBD85 | . 68 17B85D00 | PUSH DVDMenuS.005DB817 | |
| 004DBD8A | . 64:A1 00000000 | MOV EAX,DWORD PTR FS:[0] | |
| 004DBD90 | . 50 | PUSH EAX | |
| 004DBD91 | . 64:8925 00000000 | MOV DWORD PTR FS:[0],ESP | |
| 004DBD98 | . 81EC 68010000 | SUB ESP,168 | |
| 004DBD9E | . 8B45 08 | MOV EAX,DWORD PTR SS:[EBP+8] | |
| 004DBDA1 | . 53 | PUSH EBX | |
| 004DBDA2 | . 56 | PUSH ESI | |
| 004DBDA3 | . 57 | PUSH EDI | |
| 004DBDA4 | . 83F8 01 | CMP EAX,1 | |
| 004DBDA7 | . 8BF9 | MOV EDI,ECX | |
| 004DBDA9 | . 75 53 | JNZ SHORT DVDMenuS.004DBDFE | |
| 004DBDAB | . 50 | PUSH EAX | TimerID |
| 004DBDAC | . 8B47 1C | MOV EAX,DWORD PTR DS:[EDI+1C] | |
| 004DBDAF | . 50 | PUSH EAX | hWnd |
| 004DBDB0 | . FF15 B4575E00 | CALL DWORD PTR DS:[<&USER32.KillTimer>] | KillTim |
| 004DBDB6 | . E8 8E5C0E00 | CALL DVDMenuS.005C1A49 | |

4DBD9E에서 EAX 값을 설정하고, 그
뒤로 어떤 값과 비교해 분기를
결정한다.

| | | | |
|----------|-----------------|---|----------|
| 004DC1B1 | . 68 5C666400 | PUSH 0 | |
| 004DC1B6 | . E8 919D0D00 | CALL DVDMenuS.0064665C | Arg1 |
| 004DC1B8 | . vE9 B7000000 | CALL DVDMenuS.005B5F4C | DVDMenuS |
| 004DC1C0 | > 83F8 04 | JMP DVDMenuS.004DC277 | |
| 004DC1C3 | . v75 1E | CMP EAX,4 | |
| 004DC1C5 | . 50 | JNZ SHORT DVDMenuS.004DC1E3 | Time |
| 004DC1C6 | . 8B47 1C | PUSH EAX | hWnd |
| 004DC1C9 | . 50 | MOV EAX,DWORD PTR DS:[EDI+1C] | Kill |
| 004DC1CA | . FF15 B4575E00 | PUSH EAX | Arg3 |
| 004DC1D0 | . 6A 00 | CALL DWORD PTR DS:[<&USER32.KillTimer>] | Arg2 |
| 004DC1D2 | . 6A 00 | PUSH 0 | DVDMenuS |
| 004DC1D4 | . 68 FC656400 | PUSH 0 | |
| 004DC1D9 | . E8 6E9D0D00 | PUSH DVDMenuS.0064665C | |
| 004DC1DE | . vE9 94000000 | CALL DVDMenuS.005B5F4C | |
| | | JMP DVDMenuS.004DC277 | |

결국에 메시지를 출력하기 전에 EAX, 4 와 비교하고, 같아야지만 성공 메시지가 출력된다. 즉, EAX는 4여야 한다.

다시 코드를 살펴보면

EBP+8부분에는 3이 들어있다. 해당 주소에 값을 변경하고, 패치하려 했지만, 그 순간에만 적용되고, 다시 실행하면, 똑같이 3이 들어온다.

| | | | |
|----------|------------------|-------------------------------|------|
| 004DBD90 | . 50 | PUSH EAX | |
| 004DBD91 | . 64:8925 000000 | MOV DWORD PTR FS:[0],ESP | |
| 004DBD98 | . 81EC 68010000 | SUB ESP,168 | |
| 004DBD9E | . 8B45 08 | MOV EAX,DWORD PTR SS:[EBP+8] | |
| 004DBDA1 | . 53 | PUSH EBX | |
| 004DBDA2 | . 56 | PUSH ESI | |
| 004DBDA3 | . 57 | PUSH EDI | |
| 004DBDA4 | . 83F8 01 | CMP EAX,1 | |
| 004DBDA7 | . 8BF9 | MOV EDI,ECX | |
| 004DBDA9 | . v75 53 | JNZ SHORT DVDMenuS.004DBDFE | Time |
| 004DBDAB | . 50 | PUSH EAX | hWnd |
| 004DBDAC | . 8B47 1C | MOV EAX,DWORD PTR DS:[EDI+1C] | |
| 004DBDAF | . 50 | PUSH EAX | |

왜냐하면 ASLR 보호기법이 적용돼 매 실행마다 주소가 바뀌기 때문이다. 그래서 패치를 해주어야된다. MOV EAX, 4를 해주면 되는데, 이렇게 할 경우 명령 크기가 5바이트가 돼 주소값 자체가 바뀌게 된다. 왜냐하면 기존 명령이 3바이트이기 때문이다. 이 때 필요한게 인라인 패치다.

| | | |
|------------------------------|------------------|--------|
| 004DBE4D | . v0F85 54010000 | JNZ DX |
| 004DBE53 | . 6A 00 | PUSH 0 |
| Stack SS:[0019EE70]=00000003 | | |
| EAX=0019EED4 | | |

| | | | |
|----------|-----------------|---|-----------------------------|
| 004DC1C8 | > 83F8 04 | CMP EAX,4 | |
| 004DC1C9 | .v75 1E | JNZ SHORT DVDMenuS.004DC1E3 | |
| 004DC1C5 | . 50 | PUSH EAX | TimerID |
| 004DC1C6 | . 8B47 1C | MOV EAX,DWORD PTR DS:[EDI+1C] | |
| 004DC1C9 | . 50 | PUSH EAX | hWnd |
| 004DC1CA | . FF15 B4575E00 | CALL DWORD PTR DS:[<&USER32.KillTimer>] | KillTimer |
| 004DC1D0 | . 6A 00 | PUSH 0 | Arg3 = 00000000 |
| 004DC1D2 | . 6A 00 | PUSH 0 | Arg2 = 00000000 |
| 004DC1D4 | . 68 FC656400 | PUSH DVDMenuS.006465FC | Arg1 = 006465FC ASCII "Thar |
| 004DC1D9 | . E8 6E9D0000 | CALL DVDMenuS.005B5F4C | DVDMenuS.005B5F4C |
| 004DC1DE | .vE9 94000000 | JMP DVDMenuS.004DC277 | |
| 004DC1E3 | > 83F8 05 | CMP EAX,5 | |
| 004DC1E6 | .v75 15 | JNZ SHORT DVDMenuS.004DC1FD | |
| 004DC1E8 | . 8B4F 1C | MOV ECX,DWORD PTR DS:[EDI+1C] | |
| 004DC1EB | . 50 | PUSH EAX | TimerID |

궁금해서 MOV EAX, 4로 패치해봤다. 그런데 등록 성공 메시지가 무한으로 나왔다. 왜 무한으로 바졌는지 해당 프로그램을 분석해봤다. 패치한 주소는 이전과 다를거 없이 바뀐게 없다. 하지만 하나씩 트레이싱 해봤는데, 주소만 안바뀌었지 명령 실행하는 우선순위가 바뀌어 하나씩 땡겨져서 실행되는것 같다.

CALL해야하는 부분에서 계속 jmp가 되면서 해당 명령과 다른 동작을 진행했다.

| | | | |
|----------|------------------|---|--------------|
| 004DBD91 | . 64:8925 000000 | MOV DWORD PTR FS:[0],ESP | |
| 004DBD98 | . 81EC 68010000 | SUB ESP,168 | |
| 004DBD9E | . B8 04000000 | MOV EAX,4 | |
| 004DBDA3 | . 57 | PUSH EDI | |
| 004DBDA4 | . 83F8 01 | CMP EAX,1 | |
| 004DBDA7 | . 8BF9 | MOV EDI,ECX | |
| 004DBDA9 | .v75 53 | JNZ SHORT DVDMenuS.004DBDFE | |
| 004DBDAB | . 50 | PUSH EAX | TimerID => 4 |
| 004DBDAC | . 8B47 1C | MOV EAX,DWORD PTR DS:[EDI+1C] | |
| 004DBDAF | . 50 | PUSH EAX | hWnd |
| 004DBDB0 | . FF15 B4575E00 | CALL DWORD PTR DS:[<&USER32.KillTimer>] | KillTimer |
| 004DBDB6 | . E8 8E5C0E00 | CALL DVDMenuS.005C1A49 | |
| 004DBDB8 | . 8B40 04 | MOV EAX,DWORD PTR DS:[EAX+4] | |

다음과 같이 해당 CALL 명령 다음에 JMP가 동작하는데, 해당 명령에서 jmp가 진행돼 원래 있던 곳으로 갔다.

| | | |
|----------|------------------|-------------------------------|
| 0040B08H | . 64:H1 00000000 | MOV EHX,DWORD PTR FS:[0] |
| 0040BD90 | . 50 | PUSH EAX |
| 0040BD91 | . 64:8925 000000 | MOV DWORD PTR FS:[0],ESP |
| 0040BD98 | . 81EC 68010000 | SUB ESP,168 |
| 0040BD9E | 8B45 08 | MOV EAX,DWORD PTR SS:[EBP+8] |
| 0040BDA1 | 53 | PUSH EBX |
| 0040BDA2 | 56 | PUSH ESI |
| 0040BDA3 | . 57 | PUSH EDI |
| 0040BDA4 | . 83F8 01 | CMP EAX,1 |
| 0040BDA7 | . 8BF9 | MOV EDI,ECX |
| 0040BDA9 | . 75 53 | JNZ SHORT DVDMenuS.0040BDFE |
| 0040BDAB | . 50 | PUSH EAX |
| 0040BDBF | 8B47 1C | MOV ECX,DWORD PTR DS:[EDI+1C] |

그래서 3바이트 명령으로 바꿔줘야한다. 그중 한가지 방법이 떠올랐다. **MOV AX, 4**를 쓰면 3바이트가 되고, 인라인 패치를 굳이 안해도 정상적으로 패치되었다.

이번에는 또 다른 인라인 패치를 통해 코드를 패치해볼 것이다.

해당 영역을 **MOV EAX, 4**로 패치하자니 5바이트가 돼서 그 뒤 명령을 덮어씌울 것이다. 그래서 다른 공간에 해당 부분을 복사하고, 그 영역으로 분기해서 수행한 뒤 다시 돌아오는 방법을 쓸 것이다.

| | | |
|----------|---------------|---------------------------|
| 005E47B5 | . C3 | RETN |
| 005E47B6 | . B8 F8A16300 | MOV EAX,DVDMenuS.0063A1F8 |
| 005E47B8 | .^E9 C7B9FAFF | JMP DVDMenuS.00590187 |
| 005E47C0 | 0000 | ADD BYTE PTR DS:[EAX],AL |
| 005E47C2 | 0000 | ADD BYTE PTR DS:[EAX],AL |
| 005E47C4 | 0000 | ADD BYTE PTR DS:[EAX],AL |
| 005E47C6 | 0000 | ADD BYTE PTR DS:[EAX],AL |
| 005E47C8 | 0000 | ADD BYTE PTR DS:[EAX],AL |
| 005E47CA | 0000 | ADD BYTE PTR DS:[EAX],AL |
| 005E47CC | 00 | DB 00 |
| 005E47CD | 00 | DB 00 |
| 005E47CE | 00 | DB 00 |
| 005E47CF | 00 | DB 00 |
| 005E47D0 | 00 | DB 00 |

코드 끝으로 가면 잉여 공간이 있다.
 (PE 구조는 파일 또는 메모리에서
 섹션의 시작위치는 각각 최소 기본
 단위의 배수에 해당하는 위치여야
 하므로 빈공간은 **NULL**로
 채워버리기 때문에 잉여 공간이
 있다고한다. 이 부분을 이용해
 인라인 패치를 할
 것이다.(Alignment))

이 영역으로 분기할 것이다.
 분기하기 위해 **long** 점프를
 해야한다.

어셈 코드에서 점프를 하고자 할 때
점프하고자 하는 주소를 기준으로 점프
종류가 2가지로 나뉜다.

short 점프는 주소 공간을 2 바이트만
차지하지만, 점프 명령어가 실행되는
주소와, 점프 대상 주소를 기준으로
80바이트 내로 밖에 점프하지 못한다.
그 이상 점프하고 싶으면 **long** 점프를
사용해야 한다. 하지만 이는 주소
공간을 5바이트 차지하기 때문에 잉여
공간으로 이동해 명령을 수행한 다음
다시 돌아와야한다.

| | | | |
|----------|------------------|---|-------------------------|
| 0040BD83 | . 6A FF | PUSH -1 | |
| 0040BD85 | . 68 17B85D00 | PUSH DVDMenuS.005DB817 | SE handler installation |
| 0040BD8A | . 64:A1 00000000 | MOV EAX,DWORD PTR FS:[0] | |
| 0040BD90 | . 50 | PUSH EAX | |
| 0040BD91 | . 64:8925 000000 | MOV DWORD PTR FS:[0],ESP | |
| 0040BD98 | . 81EC 68010000 | SUB ESP,168 | |
| 0040BD9E | . 8B45 08 | MOV EAX,DWORD PTR SS:[EBP+8] | |
| 0040BDA1 | . 53 | PUSH EBX | |
| 0040BDA2 | . 56 | PUSH ESI | |
| 0040BDA3 | . 57 | PUSH EDI | |
| 0040BDA4 | . 83F8 01 | CMP EAX,1 | |
| 0040BDA7 | . 8BF9 | MOV EDI,ECX | |
| 0040BDA9 | . 75 53 | JNZ SHORT DVDMenuS.004BDBFE | |
| 0040BDAE | . 50 | PUSH EAX | |
| 0040BDAF | . 8B47 1C | MOV EAX,DWORD PTR DS:[EDI+1C] | |
| 0040BDB0 | . FF15 B4575E00 | CALL DWORD PTR DVDMenuS.005DB817 | |
| 0040BDB6 | . E3 8E5C0E00 | CALL DVDMenuS.004BDBFE | |
| 0040BDB8 | . 8B40 04 | MOV EAX,DWORD PTR DS:[EDI+4] | |
| 0040BDBE | . 83B8 64010000 | CMP DWORD PTR EAX,DWORD PTR DS:[801064B8] | |
| 0040BDC5 | . 75 1F | JNZ SHORT DVDMenuS.004BDBFE | |
| 0040BDC7 | . 8BCF | MOV ECX,EDI | |
| 0040BDC9 | . E3 621C0000 | CALL DVDMenuS.004BDBFE | |
| 0040BDCD | . 8B4F 1C | MOV ECX,DWORD PTR DS:[EDI+1C] | |
| 0040BDD1 | . 6A 00 | PUSH 0 | |
| 0040BDD3 | . 68 0C800000 | PUSH 0C8 | |
| 0040BDD8 | . 6A 07 | PUSH 7 | |
| 0040BDDA | . 51 | PUSH ECX | |
| 0040BDDB | . FF15 B8575E00 | CALL DWORD PTR DVDMenuS.005DB817 | |
| 0040BDE1 | . E9 91040000 | JMP DVDMenuS.004BDBFE | |
| 0040BDE6 | . 8B57 1C | MOV EDI,DWORD PTR DS:[EDI+1C] | |
| 0040BDE9 | . 6A 00 | PUSH 0 | |
| 0040BDEB | . 68 F4010000 | PUSH 1F4 | |

Backup

Copy

Binary

Assemble

Label

Comment

Breakpoint

Hit trace

Run trace

New origin here

Edit

Fill with 00's

Fill with NOPs

Binary copy

해당 명령을 복사한 후 잉여 공간에 복사한다. 그리고 원래 명령을 JMP [잉여 공간 주소]로 패치한다.

| | | |
|----------|----------------|---------------------------|
| 005E47B6 | . B8 F8A16300 | MOV EAX,DVDMenuS.0063A1F8 |
| 005E47BB | . ^E9 C7B9FAFF | JMP DVDMenuS.00590187 |
| 005E47C0 | . B8 04000000 | MOV EAX,4 |
| 005E47C5 | . 53 | PUSH EBX |
| 005E47C6 | . 56 | PUSH ESI |
| 005E47C7 | . ^E9 D775EFFF | JMP DVDMenuS.004BDBA3 |
| 005E47CC | . 90 | NOP |
| 005E47CD | . 00 | DB 00 |
| 005E47CE | . 00 | DB 00 |

| | | |
|----------|------------------|-------------------------------|
| 0040BD8A | . 64:A1 00000000 | MOV EAX,DWORD PTR FS:[0] |
| 0040BD90 | . 50 | PUSH EAX |
| 0040BD91 | . 64:8925 000000 | MOV DWORD PTR FS:[0],ESP |
| 0040BD98 | . 81EC 68010000 | SUB ESP,168 |
| 0040BD9E | . ^E9 1D8A1000 | JMP DVDMenuS.005E47C0 |
| 0040BDA3 | . 57 | PUSH EDI |
| 0040BDA4 | . 83F8 01 | CMP EAX,1 |
| 0040BDA7 | . 8BF9 | MOV EDI,ECX |
| 0040BDA9 | . 75 53 | JNZ SHORT DVDMenuS.004BDBFE |
| 0040BDAE | . 50 | PUSH EAX |
| 0040BDAF | . 8B47 1C | MOV EAX,DWORD PTR DS:[EDI+1C] |

| | | | |
|----------|------------------|--------------------------|---------|
| 0040BD79 | 50 | POP EBP | |
| 0040BD7A | C2 0800 | RETN 8 | |
| 0040BD7D | 90 | NOP | |
| 0040BD7E | 90 | NOP | |
| 0040BD7F | 90 | NOP | |
| 0040BD80 | 55 | PUSH EBP | |
| 0040BD81 | 8BEC | MOV EBP,ESP | |
| 0040BD83 | 6A FF | PUSH -1 | |
| 0040BD85 | 68 17B85D00 | PUSH DVDMenuS.0050B817 | |
| 0040BD8A | 64:A1 00000000 | MOV EAX,DWORD PTR FS:[0] | SE hand |
| 0040BD90 | 50 | PUSH EAX | |
| 0040BD91 | 64:8925 00000000 | MOV DWORD PTR FS:[0],ESP | |
| 0040BD98 | 81EC 68010000 | SUB ESP,168 | |
| 0040BD9F | F9 108A1000 | IMP DVDMenuS.005F47C0 | |

패치한 후 실행하니 무한루프에 빠지게 됐다. 실행을 하면 해당 부분으로 다시 돌아오게 된다.

| Registers (FPU) | |
|-----------------|-----------------|
| EAX | 0000000C |
| ECX | 02658470 |
| EDX | 00227000 |
| EBX | 0040BD80 DVDMen |
| ESP | 0019E944 |
| ESI | 0019E944 |

원인을 분석하기 위해 하나씩 다시 분석해본다.