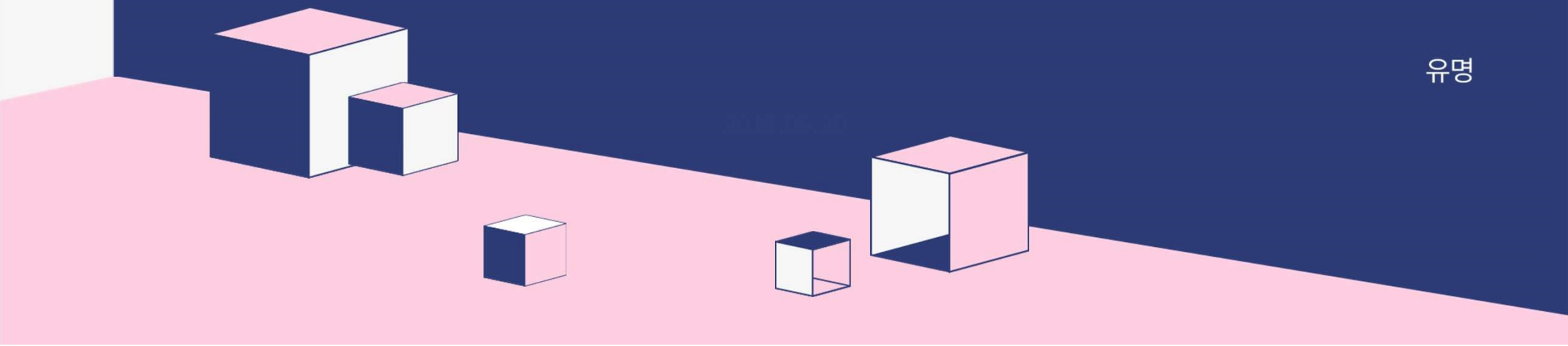
피카츄 배구 핵



유명

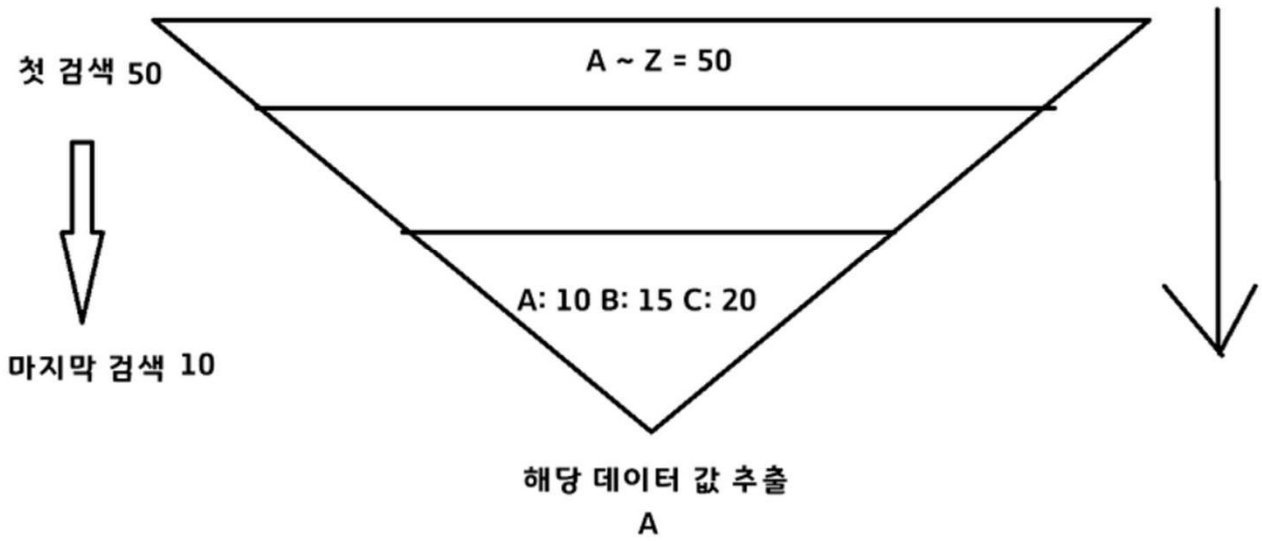
사용한것

치트엔진

메모리 에디트 툴 및 헥스 에디터 프로그램이다. 오픈소스이며강력한 헥스에디팅/메모리에디팅 툴로, 다른 프로그램에 비해 스캔 속도가 매우 빠른 편이다.레지스터까지 변경할 수 있다.

치트엔진 검색 원리

내가 변경하려는 값 A의 값이 50이라고 해보자. 하지만 데이터상 주소형태로 표시되어 있기 때문에 어떤 주소가 A를 의미하는지 모른다.
그래서 검색을 통해 50의 값을 가진 모든 데이터를 찾고 A값의 변경을 통해서 처음에 검색된 값들을 하나씩 소거해 주는 것이다.



1.점수 메모리 주소 찾기


(PAUSED!)
게임(G) 설정(C) 윈도우(W) 도움(H) 디버그(D)
1
0
치트 엔진 6.6
파일(F) 편집(E) 표 D3D 도움말(H)
찾음: 7,249
주소 값 이전 값 First
000984B8 631232 1 1
000984D0 0 1 1
00098568 478481652 1 1
00098580 624168 1 1
00098738 625768 1 1
00098748 625952 1 1
00098A84 1 1 1
00098B34 1 1 1
00098B70 8096 1 1
00098C20 4294966064 1 1
00098CA8 624480 1 1
00098D14 0 1 1
00098D58 1 1 1
00098E38 627552 1 1
00098E80 1048591 1 1
00099060 0 1 1
00099264 515 1 1
새로운 검색
다음 검색
검색 되돌리기
설정
값:
16진수
1
검색 유형 정확한 값
값 유형 4 바이트
Compare to first scan
Lua formula
제외
비임의추출기
스피드 핵 활성화
메모리 검색 선택사항
All
시작 0000000000000000
중지 00007fffffffffff
쓰기 가능
실행 가능
CopyOnWrite
Active memory only
빠른 검색 4
정렬
마지막 숫자
검색 하는동안 게임을 중지하기
메모리 보기
수동으로 주소 추가하기
활성회 설명 주소 유형 값
고급 선택 사항
기타 표

1.점수 메모리 주소 찾기

치트 엔진 6.6
파일(F) 편집(E) 표 D3D 도움말(H)
찾음: 19
주소
값
이전 값
First
0009FDC8 0 2 1
0031B150 2 2 1
023F6DB4 2 2 1
023F6DB8 2 2 1
034B06C8 2 2 1
034B06E0 2 2 1
05070050 1 2 1
05070058 1 2 1
05070060 1 2 1
0507006C 1 2 1
05070074 1 2 1
05070088 1 2 1
05070090 1 2 1
05070098 1 2 1
050700A4 1 2 1
050700AC 1 2 1
050700B4 1 2 1
새로운 검색
다음 검색
검색 되돌리기
값:
16진수
2
검색 유형
정확한 값
값 유형
4 바이트
Compare to first scan
Lua formula
제외
비임의추출기
스피드 핵 활성화
메모리 검색 선택사항
All
시작
0000000000000000
중지
00007fffffffffff
쓰기 가능
실행 가능
CopyOnWrite
Active memory only
빠른 검색
4
정렬
마지막 숫자
검색 하는동안 게임을 중지하기
메모리 보기
수동으로 주소 추가하기
활성화 설명
주소
유형
값
고급 선택 사항
기타 표
설정
게임(G) 설정(C) 윈도우(W) 도움(H) 디버그(D)
(PAUSED!)
2
0

1.점수 메모리 주소 찾기


게임(G) 설정(C) 윈도우(W) 도움(H) 디버그(D)
3
0
Ready?
치트 엔진 6.6
파일(F) 편집(E) 표 D3D 도움말(H)
찾음:1
주소 값 이전 값 First
02560A24 3 3 1
새로운 검색
다음 검색
검색 되돌리기
값:
16진수
3
검색 유형 정확한 값
값 유형 4 바이트
Compare to first scan
Lua formula
제외
비임의추출기
스피드 핵 활성화
메모리 검색 선택사항
All
시작 0000000000000000
중지 00007fffffffffff
쓰기 가능
실행 가능
CopyOnWrite
Active memory only
빠른 검색 4
정렬
마지막 숫자
검색 하는동안 게임을 중지하기
메모리 보기
수동으로 주소 추가하기
활성회 설명 주소 유형 값
고급 선택 사항
기타 표

범용 레지스터

EAX : 사칙연산 등 산술 연산에 자동으로 사용되며, 함수의 반환 값을 처리할 때도 사용됩니다.
EBX : 간접 번지 지정에 사용됩니다. 산수, 변수를 저장합니다.
ECX : 반복(Loop)에서 반복 Count 역할을 수행합니다.
EDX : EAX를 보조하는 역할을 합니다. 예를 들어 나누기를 진행할 경우 몫은 EAX에 나머지는 EDX에 저장됩니다.

인덱스 레지스터

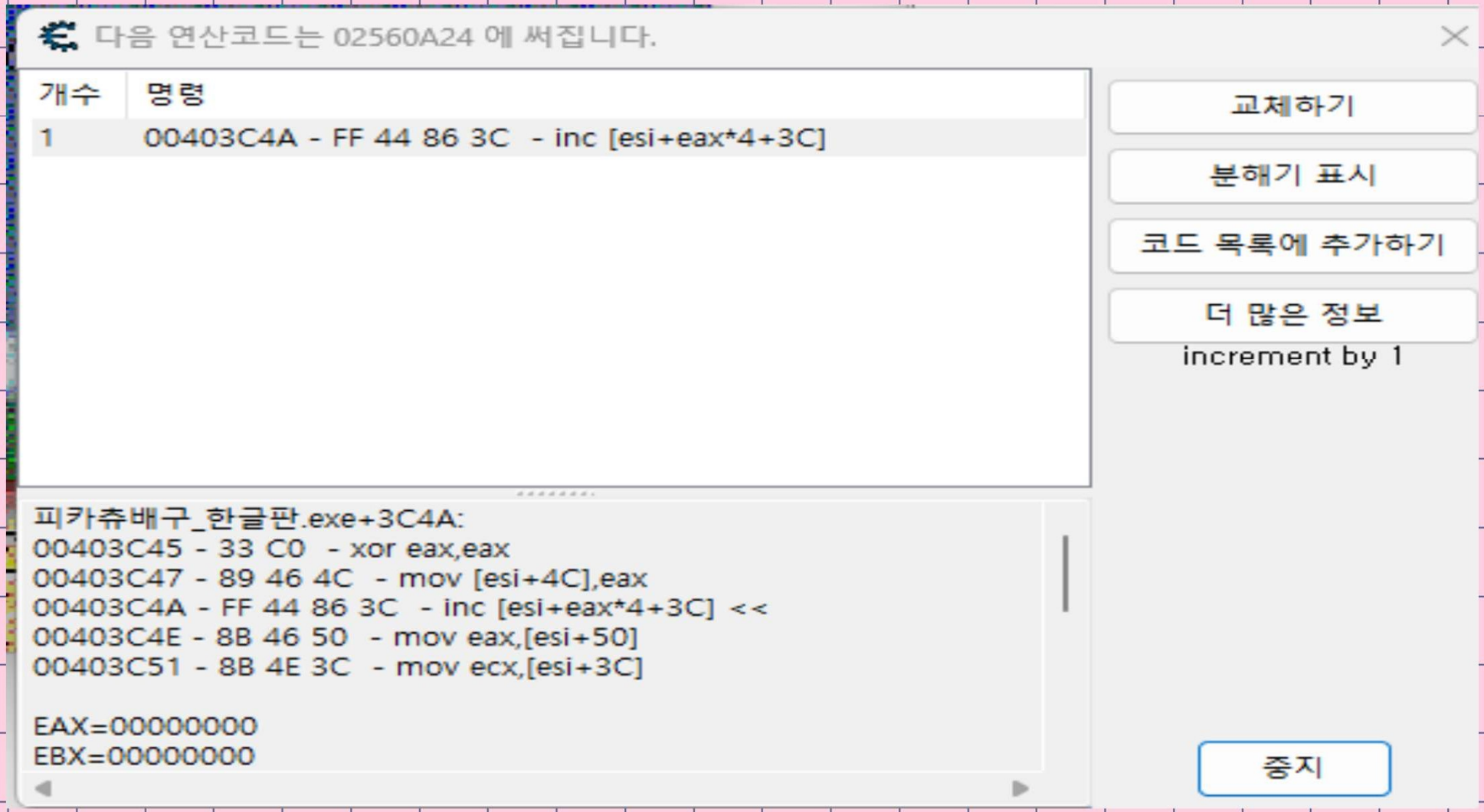
ESI : 복사나 비교를 할 경우 출발지 주소를 저장하는 레지스터입니다.
EDI : 복사나 비교를 할 경우 목적지 주소를 저장하는 레지스터입니다.

자주 사용되는 명령어

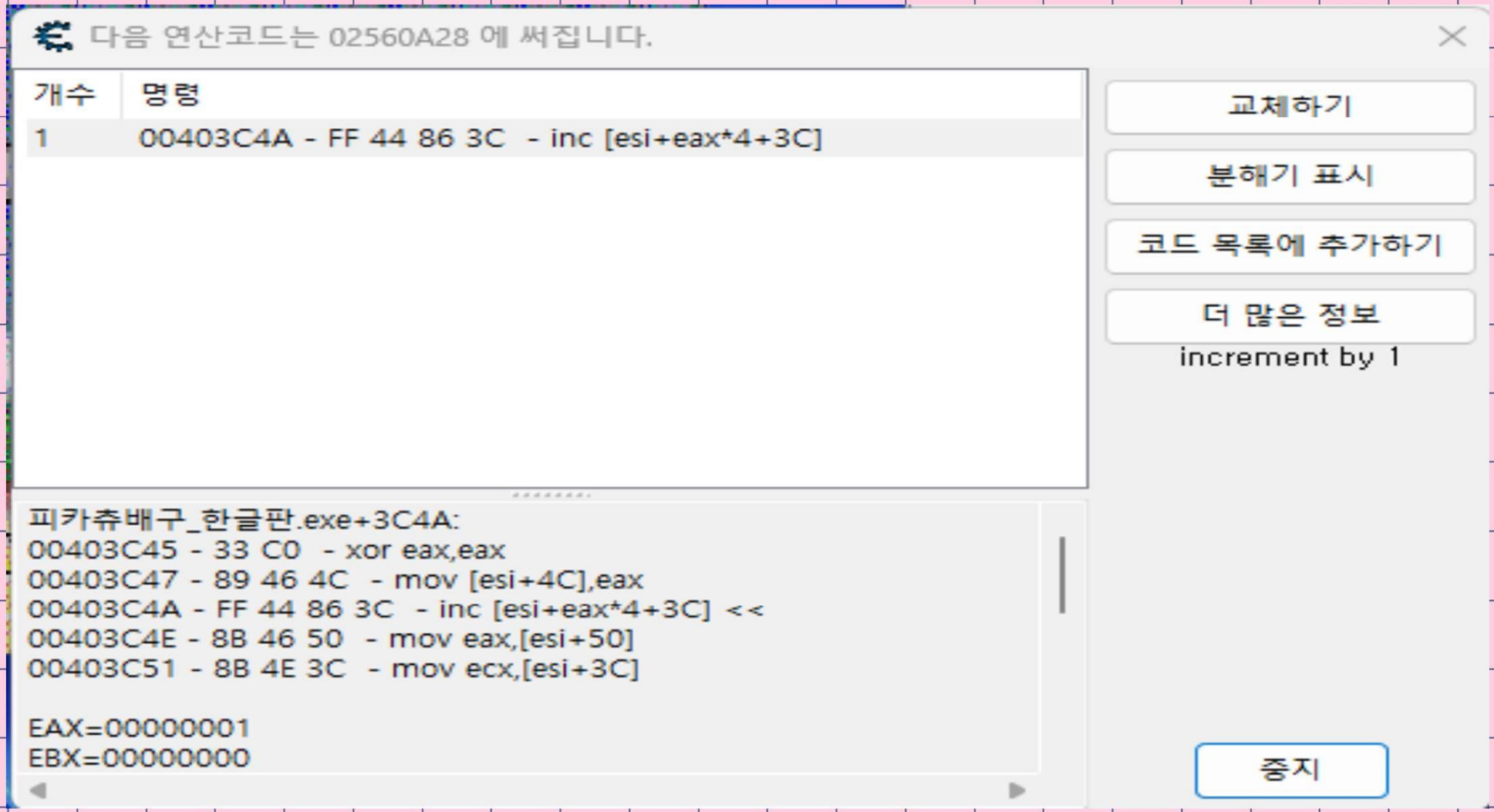
명령어	예제	설명	분류
push	push eax	eax의 값을 스택에 저장	스택 조작
pop	pop eax	스택 가장 상위에 있는 값을 꺼내서 eax에 저장	스택 조작
mov	mov eax, ebx	메모리나 레지스터의 값을 옮길때 사용	데이터 이동
inc	lnc eax	eax의 값을 1증가시킨다 (++)	데이터 조작
dec	dec eax	eax의 값을 1감소시킨다 (--)	데이터 조작
add	add eax, ebx	레지스터나 메모리의 값을 덧셈할때 쓰인다.	논리, 연산
sub	sub eax, ebx	레지스터나 메모리의 값을 뺄셈할때 쓰인다.	논리, 연산
call	call proc	프로시저를 호출한다.	프로시저
ret	ret	호출했던 바로 다음 지점으로 이동	프로시저
cmp	cmp eax, ebx	레지스터와 레지스터의 값을 비교	비교
jmp	jmp proc	특정한 곳으로 분기	분기
int	int S0x80	OS에 할당된 인터럽트 영역을 system call	인터럽트
nop	nop	아무 동작도 하지 않는다. (No Operation)	

2.피카츄 배구의 점수 득점원리

2.피카츄 배구의 점수 득점원리(왼쪽 플레이어)



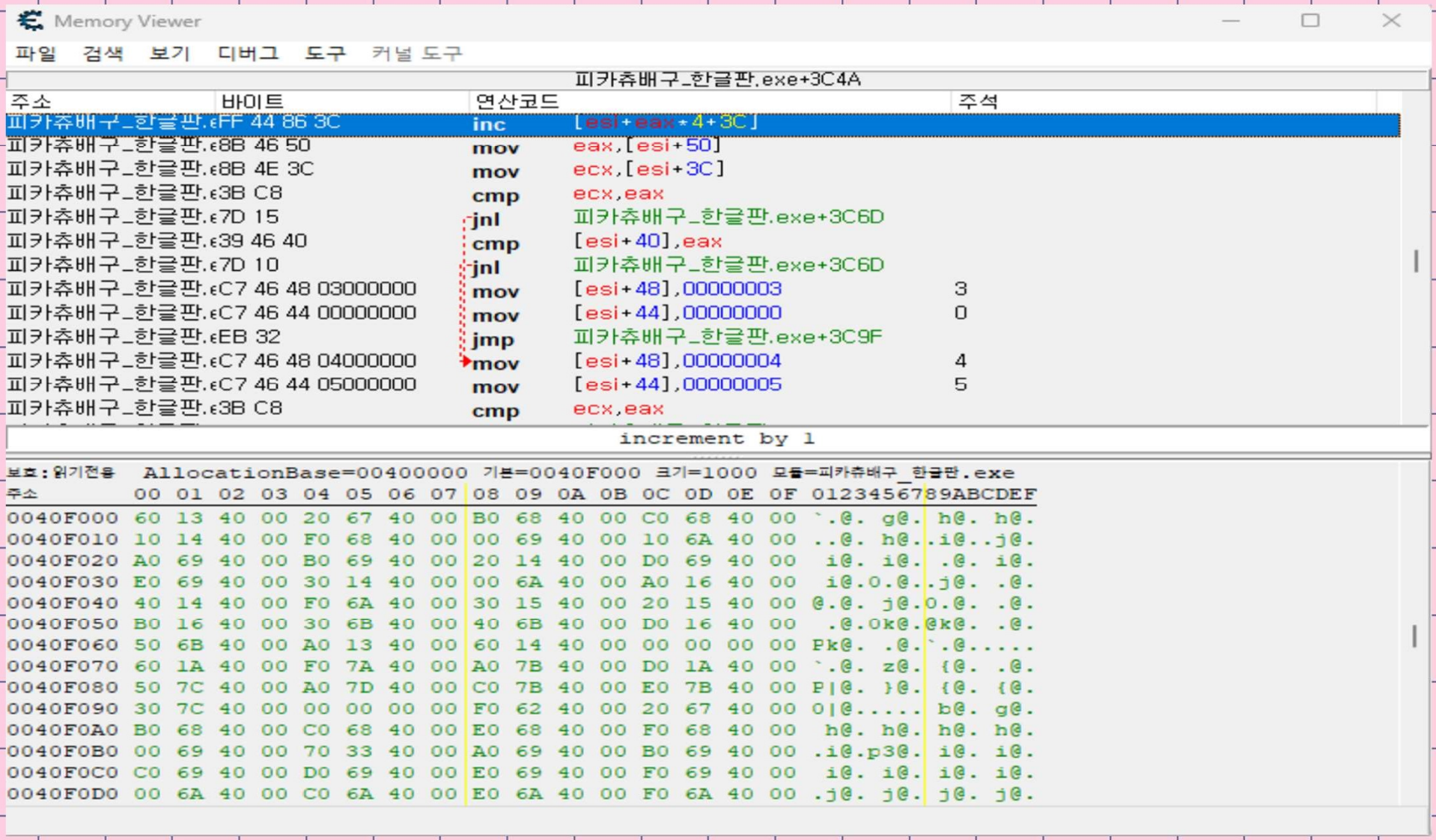
2.피카츄 배구의 점수 득점원리(오른쪽 플레이어)



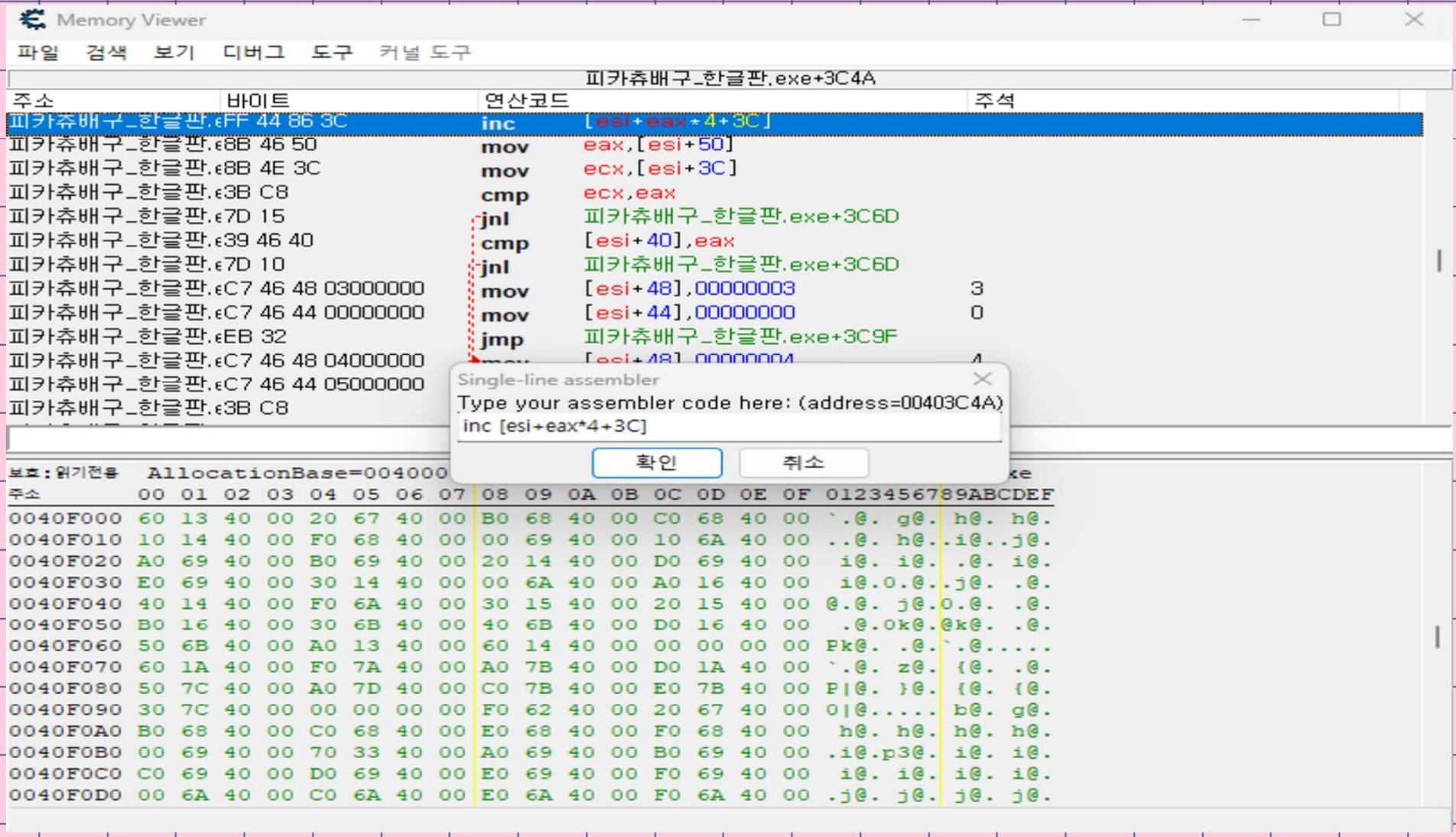
2.피카츄배구 득점원리 정리

오른쪽 플래이어가 득점을 하면 eax가 1이되어 1X4가되어 4를 추가 한다. 왼쪽 플레이어가 득점하면 0X4가되어 0을 추가한다 그래서 오른쪽 플레이어의 주소가 왼쪽 플레이어의 주소값의 4를 더한 값이 된다.

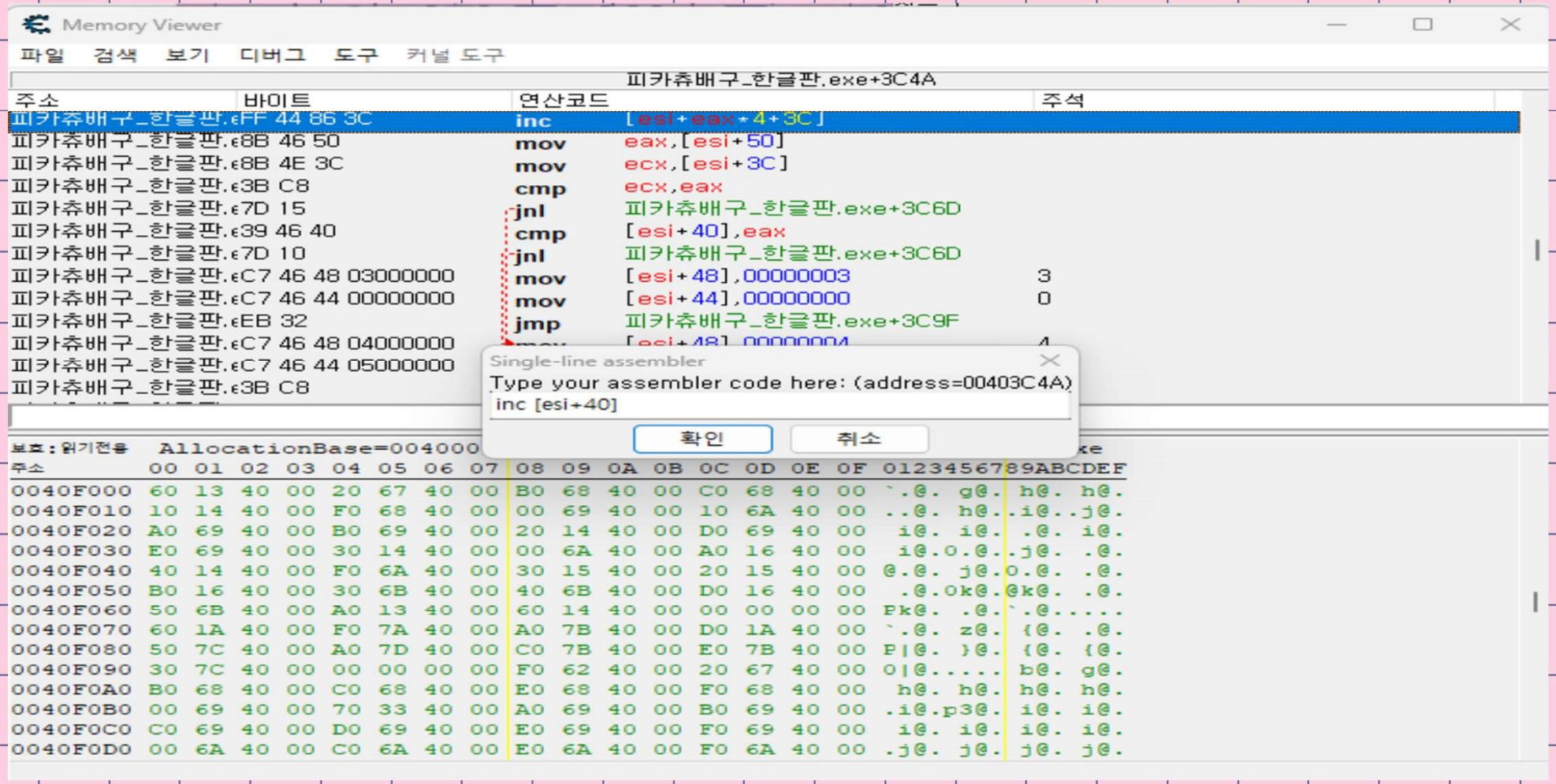
3.나만 득점하도록 조작


Memory Viewer
파일 검색 보기 디버그 도구 커널 도구
피카츄배구_한글판.exe+3C4A
주소 바이트 연산코드 주석
피카츄배구_한글판.exe+3C4A FF 44 86 3C inc [esi+eax*4+3C]
피카츄배구_한글판.exe+3C4E 8B 46 50 mov eax,[esi+50]
피카츄배구_한글판.exe+3C51 8B 4E 3C mov ecx,[esi+3C]
피카츄배구_한글판.exe+3C54 3B C8 cmp ecx,eax
피카츄배구_한글판.exe+3C56 7D 15 jnl 피카츄배구_한글판.exe+3C6D
피카츄배구_한글판.exe+3C58 39 46 40 cmp [esi+40],eax
피카츄배구_한글판.exe+3C5B 7D 10 jnl 피카츄배구_한글판.exe+3C6D
피카츄배구_한글판.exe+3C5D C7 46 48 03000000 mov [esi+48],00000003 3
피카츄배구_한글판.exe+3C64 C7 46 44 00000000 mov [esi+44],00000000 0
피카츄배구_한글판.exe+3C6B EB 32 jmp 피카츄배구_한글판.exe+3C9F
피카츄배구_한글판.exe+3C6D C7 46 48 04000000 mov [esi+48],00000004 4
피카츄배구_한글판.exe+3C74 C7 46 44 05000000 mov [esi+44],00000005 5
피카츄배구_한글판.exe+3C7B 3B C8 cmp ecx,eax
increment by 1
보호:읽기전용 AllocationBase=00400000 기본=0040F000 크기=1000 모듈=피카츄배구_한글판.exe
주소 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 0123456789ABCDEF
0040F000 60 13 40 00 20 67 40 00 B0 68 40 00 C0 68 40 00 `.@. g@. h@. h@.
0040F010 10 14 40 00 F0 68 40 00 00 69 40 00 10 6A 40 00 ..@. h@..i@..j@.
0040F020 A0 69 40 00 B0 69 40 00 20 14 40 00 D0 69 40 00 i@. i@. .@. i@.
0040F030 E0 69 40 00 30 14 40 00 00 6A 40 00 A0 16 40 00 i@.0.@..j@. .@.
0040F040 40 14 40 00 F0 6A 40 00 30 15 40 00 20 15 40 00 @.@. j@.0.@. .@.
0040F050 B0 16 40 00 30 6B 40 00 40 6B 40 00 D0 16 40 00 .@.0k@.@k@. .@.
0040F060 50 6B 40 00 A0 13 40 00 60 14 40 00 00 00 00 00 Pk@. .@.`.@.....
0040F070 60 1A 40 00 F0 7A 40 00 A0 7B 40 00 D0 1A 40 00 `.@. z@. {@. .@.
0040F080 50 7C 40 00 A0 7D 40 00 C0 7B 40 00 E0 7B 40 00 P|@. }@. {@. {@.
0040F090 30 7C 40 00 00 00 00 00 F0 62 40 00 20 67 40 00 0|@..... b@. g@.
0040F0A0 B0 68 40 00 C0 68 40 00 E0 68 40 00 F0 68 40 00 h@. h@. h@. h@.
0040F0B0 00 69 40 00 70 33 40 00 A0 69 40 00 B0 69 40 00 .i@.p3@. i@. i@.
0040F0C0 C0 69 40 00 D0 69 40 00 E0 69 40 00 F0 69 40 00 i@. i@. i@. i@.
0040F0D0 00 6A 40 00 C0 6A 40 00 E0 6A 40 00 F0 6A 40 00 .j@. j@. j@. j@.

3.나만 득점하도록 조작


Memory Viewer
파일 검색 보기 디버그 도구 커널 도구
피카츄배구_한글판.exe+3C4A
주소 바이트 연산코드 주석
피카츄배구_한글판.exe+3C4A FF 44 86 3C inc [esi+eax*4+3C]
피카츄배구_한글판.exe+3C4E 8B 46 50 mov eax,[esi+50]
피카츄배구_한글판.exe+3C51 8B 4E 3C mov ecx,[esi+3C]
피카츄배구_한글판.exe+3C54 3B C8 cmp ecx,eax
피카츄배구_한글판.exe+3C56 7D 15 jnl 피카츄배구_한글판.exe+3C6D
피카츄배구_한글판.exe+3C58 39 46 40 cmp [esi+40],eax
피카츄배구_한글판.exe+3C5B 7D 10 jnl 피카츄배구_한글판.exe+3C6D
피카츄배구_한글판.exe+3C5D C7 46 48 03000000 mov [esi+48],00000003 3
피카츄배구_한글판.exe+3C64 C7 46 44 00000000 mov [esi+44],00000000 0
피카츄배구_한글판.exe+3C6B EB 32 jmp 피카츄배구_한글판.exe+3C9F
피카츄배구_한글판.exe+3C6D C7 46 48 04000000
피카츄배구_한글판.exe+3C74 C7 46 44 05000000
피카츄배구_한글판.exe+3C7B 3B C8
Single-line assembler
Type your assembler code here: (address=00403C4A)
inc [esi+eax*4+3C]
확인
취소
보호:읽기전용 AllocationBase=004000
주소 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 0123456789ABCDEF
0040F000 60 13 40 00 20 67 40 00 B0 68 40 00 C0 68 40 00 `.@. g@. h@. h@.
0040F010 10 14 40 00 F0 68 40 00 00 69 40 00 10 6A 40 00 ..@. h@..i@..j@.
0040F020 A0 69 40 00 B0 69 40 00 20 14 40 00 D0 69 40 00 i@. i@. .@. i@.
0040F030 E0 69 40 00 30 14 40 00 00 6A 40 00 A0 16 40 00 i@.0.@..j@. .@.
0040F040 40 14 40 00 F0 6A 40 00 30 15 40 00 20 15 40 00 @.@. j@.0.@. .@.
0040F050 B0 16 40 00 30 6B 40 00 40 6B 40 00 D0 16 40 00 .@.0k@.@k@. .@.
0040F060 50 6B 40 00 A0 13 40 00 60 14 40 00 00 00 00 00 Pk@. .@.`.@.....
0040F070 60 1A 40 00 F0 7A 40 00 A0 7B 40 00 D0 1A 40 00 `.@. z@. {@. .@.
0040F080 50 7C 40 00 A0 7D 40 00 C0 7B 40 00 E0 7B 40 00 P|@. }@. {@. {@.
0040F090 30 7C 40 00 00 00 00 00 F0 62 40 00 20 67 40 00 0|@..... b@. g@.
0040F0A0 B0 68 40 00 C0 68 40 00 E0 68 40 00 F0 68 40 00 h@. h@. h@. h@.
0040F0B0 00 69 40 00 70 33 40 00 A0 69 40 00 B0 69 40 00 .i@.p3@. i@. i@.
0040F0C0 C0 69 40 00 D0 69 40 00 E0 69 40 00 F0 69 40 00 i@. i@. i@. i@.
0040F0D0 00 6A 40 00 C0 6A 40 00 E0 6A 40 00 F0 6A 40 00 .j@. j@. j@. j@.

3.나만 득점하도록 조작


Memory Viewer
파일 검색 보기 디버그 도구 커널 도구
피카츄배구_한글판.exe+3C4A
주소 바이트 연산코드 주석
피카츄배구_한글판.exe+3C4A FF 44 86 3C inc [esi+eax*4+3C]
피카츄배구_한글판.exe+3C4E 8B 46 50 mov eax,[esi+50]
피카츄배구_한글판.exe+3C51 8B 4E 3C mov ecx,[esi+3C]
피카츄배구_한글판.exe+3C54 3B C8 cmp ecx,eax
피카츄배구_한글판.exe+3C56 7D 15 jnl 피카츄배구_한글판.exe+3C6D
피카츄배구_한글판.exe+3C58 39 46 40 cmp [esi+40],eax
피카츄배구_한글판.exe+3C5B 7D 10 jnl 피카츄배구_한글판.exe+3C6D
피카츄배구_한글판.exe+3C5D C7 46 48 03000000 mov [esi+48],00000003 3
피카츄배구_한글판.exe+3C64 C7 46 44 00000000 mov [esi+44],00000000 0
피카츄배구_한글판.exe+3C6B EB 32 jmp 피카츄배구_한글판.exe+3C9F
피카츄배구_한글판.exe+3C6D C7 46 48 04000000
피카츄배구_한글판.exe+3C74 C7 46 44 05000000
피카츄배구_한글판.exe+3C7B 3B C8
Single-line assembler
Type your assembler code here: (address=00403C4A)
inc [esi+40]
확인
취소
보호:읽기전용 AllocationBase=004000
주소 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 0123456789ABCDEF
0040F000 60 13 40 00 20 67 40 00 B0 68 40 00 C0 68 40 00 `.@. g@. h@. h@.
0040F010 10 14 40 00 F0 68 40 00 00 69 40 00 10 6A 40 00 ..@. h@..i@..j@.
0040F020 A0 69 40 00 B0 69 40 00 20 14 40 00 D0 69 40 00 i@. i@. .@. i@.
0040F030 E0 69 40 00 30 14 40 00 00 6A 40 00 A0 16 40 00 i@.0.@..j@. .@.
0040F040 40 14 40 00 F0 6A 40 00 30 15 40 00 20 15 40 00 @.@. j@.0.@. .@.
0040F050 B0 16 40 00 30 6B 40 00 40 6B 40 00 D0 16 40 00 .@.0k@.@k@. .@.
0040F060 50 6B 40 00 A0 13 40 00 60 14 40 00 00 00 00 00 Pk@. .@.`.@.....
0040F070 60 1A 40 00 F0 7A 40 00 A0 7B 40 00 D0 1A 40 00 `.@. z@. {@. .@.
0040F080 50 7C 40 00 A0 7D 40 00 C0 7B 40 00 E0 7B 40 00 P|@. }@. {@. {@.
0040F090 30 7C 40 00 00 00 00 00 F0 62 40 00 20 67 40 00 0|@..... b@. g@.
0040F0A0 B0 68 40 00 C0 68 40 00 E0 68 40 00 F0 68 40 00 h@. h@. h@. h@.
0040F0B0 00 69 40 00 70 33 40 00 A0 69 40 00 B0 69 40 00 .i@.p3@. i@. i@.
0040F0C0 C0 69 40 00 D0 69 40 00 E0 69 40 00 F0 69 40 00 i@. i@. i@. i@.
0040F0D0 00 6A 40 00 C0 6A 40 00 E0 6A 40 00 F0 6A 40 00 .j@. j@. j@. j@.

결과


게임(G) 설정(C) 윈도우(W) 도움(H) 디버그(D)
대결!
포켓몬스터
피카츄 배구
(C) 1997 SACHISOFT / SAWAYAKAN Programmers

THANK YOU.