IA-32 CPU & Register

리버싱 = Reverse Engineering

IA-32 register

> **Intel Architecture 32 bit register**

- Intel사에서 32bit 아키텍쳐에서 사용하는 레지스터를 말한다.

- 레지스터란 프로세서 안에 존재하는 저장 장치로, 메모리나 기억 장치보다 빠르게 동작한다.
  그렇기 때문에 프로세서가 명령을 실행할 때에는 직접 메모리등을 조작하지 않고 메모리에서 레지스터로 읽어온 데이터로 조작하는 경우가 많다.

- 32bit 레지스터들은 앞에 E가 붙는 것이 특징이다. *E 는 Extended의 약자이다.*

범용 레지스터

- 기본적으로는 어떻게 사용해도 문제는 없다.
  그러나 각 레지스터는 통상적인 용도가 있기 때문에 함부로 사용하지는 않는다.

Name	Full Name	Use
EAX	Extended Accumulator Register	연산 결과를 저장한다.
ECX	Extended Counter Register	루프 숫자 등의 카운트를 저장한다.
EDX	Extended Data Register	연산에 사용하는 데이터를 저장한다.
EBX	Extended Base Register	주소의 기본 값을 저장한다. *간접번지 지정시 사용된다. ex : [EBP+val_8]*
ESI	Extended Source Index Register	복사 혹은 비교를 하는데 사용되는 Source 문자열을 나타낸다.
EDI	Extended Destination Index Register	복사 혹은 비교를 하는데 사용되는 Destination 문자열을 나타낸다.

이 6개의 범용 레지스터중 EAX, ECX, EDX, EBX 레지스터의 하위 16bit 는 각각 AX, CX, DX, BX _(16bit 아키텍쳐에서 쓰던 범용 레지스터)_ 라고 하며 그 안에서도 상위 8bit는 AH, CH, DH, BH 레지스터, 하위 8bit는 AL, CL, DL, BL 레지스터라고 한다.

EAX 구조

```
|              EAX              |
|               |      AX       |
|               |  AH  |  AL    |
```

- 나머지 레지스터들도 같은 구조를 가진다.

포인터 레지스터 || 특수 레지스터

문서마다 표기한 이름이 다르다.

- 각각 전용 용도가 있다.
- 프로그램을 실행하는 데 매우 중요한 역할을 하는 레지스터

Name	Full Name	Use
ESP	Extended Stack Pointer	현재 스택의 최상단 주소를 가리킨다.
EBP	Extended Base Pointer	Frame Pointer라고도 불리며 stack frame을 사용할 경우 현재 실행중 함수의 stack frame의 바닥을 가리킨다.
EIP	Extended Instruction Pointer	다음에 실행할 어셈블리 명령주소를 가리킨다.
EFL	Eflags Register	연산의 결과 및 시스템 제어를 위한 정보가 각각 배정되어 있다.

여기서 Eflags Register에 대해 좀 더 자세히 알아보자.

- Eflags 에는 17개의 플래그가 저장된다.
- 각각의 플래그들은 어셈블리 명령어들을 수행할 때 조건을 판별하는 중요한 역할을 한다.

Name	Full Name	Use
CF	Carry Flag	연산 명령으로 자리올림이나 부호변경이 발생할 때 설정(1)된다.
ZF	Zero Flag	연산 결과가 0이 되는경우 설정(1)된다. 아닐 때는 해제(0)된다.
SF	Sign Flag	연산 결과가 음수가 될 때 설정(1)된다. 양수일때는 해제된다.

OF	Overflow Flag	부호피 연산자가 부호 있는 정수라는 가정하에 "연산결과값"이 "결과값이 들어갈 피 연산자의 범위"를 벗어났을 때 설정된다.

세그먼트 레지스터

- 세그먼트의 주소를 참조하는 데 사용하는 레지스터이다.
- 세그먼트란 메모리를 관리하기 위해 데이터의 종류에 따라 영역을 구분하여 저장하는 곳이다.

Name	Full Name	Use
CS	Code Segment Register	코드 세그먼트의 주소를 저장한다. Instruction Pointer 레지스터가 가진 offset값과 합쳐서 실행을위한 명령어 주소를 참조하게 된다.
DS	Data Segment Register	데이터 세그먼트의 주소를 저장한다. AX,CX,DX,SI,DI레지스터와 합쳐서 데이터 영역의 주소를 참조하게된다
SS	Stack Segment Register	스택 세그먼트의 주소를 저장한다. SP , BP 레지스터와 합쳐서 스택영역의 주소를 참조하게 된다
ES	Extra Segment Register	보조 세그먼트의 주소를 저장한다. *일반적으로는 문자열 관련 처리를 수행하는데 사용된다.*
FS	F Segment Register	기억 장소 요구사항을 처리하기 위해 80386 아키텍쳐에서 추가로 도입된 세그먼트 레지스터이다.
GS	G Segment Register	기억 장소 요구사항을 처리하기 위해 80386 아키텍쳐에서 추가로 도입된 세그먼트 레지스터이다.