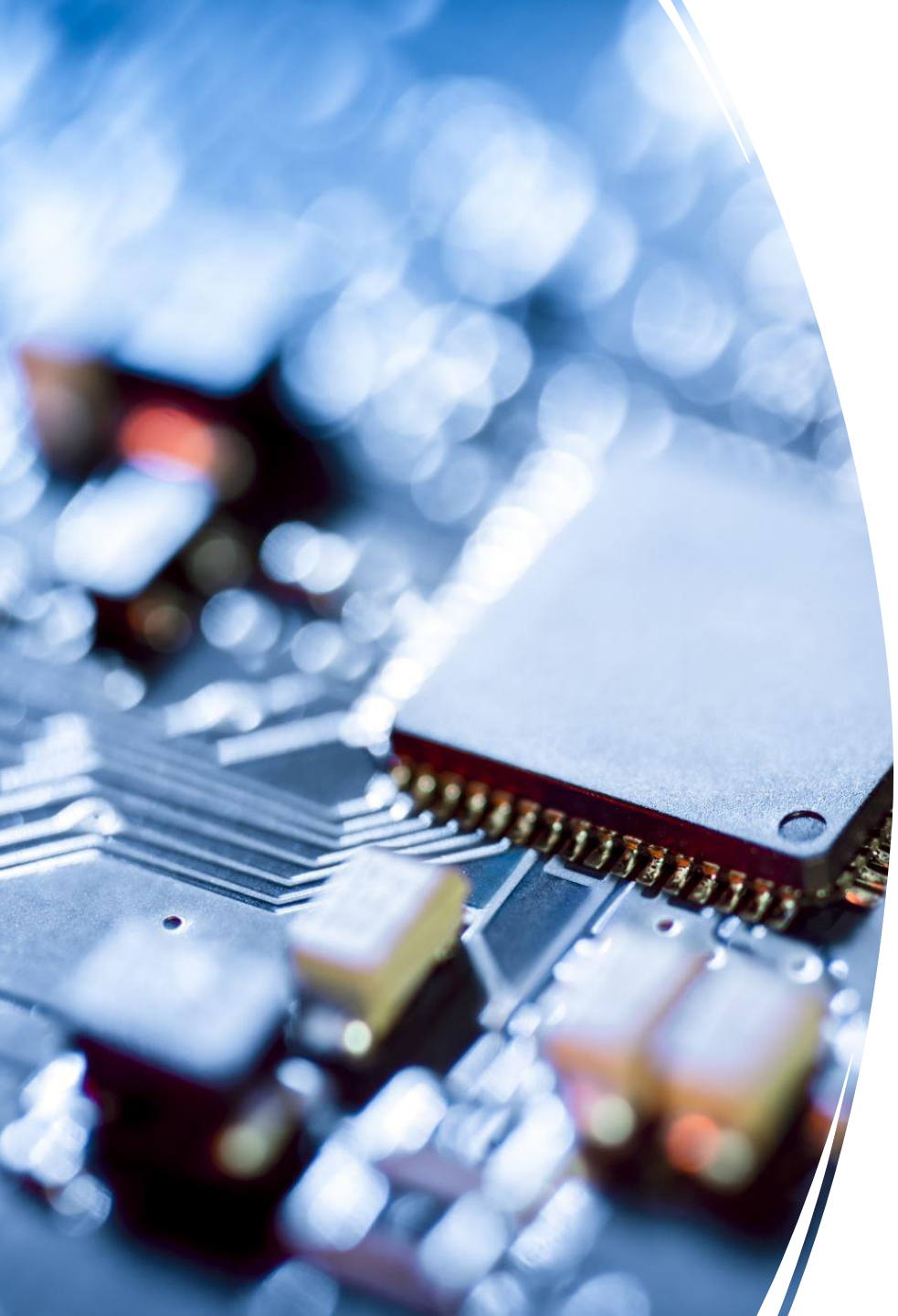


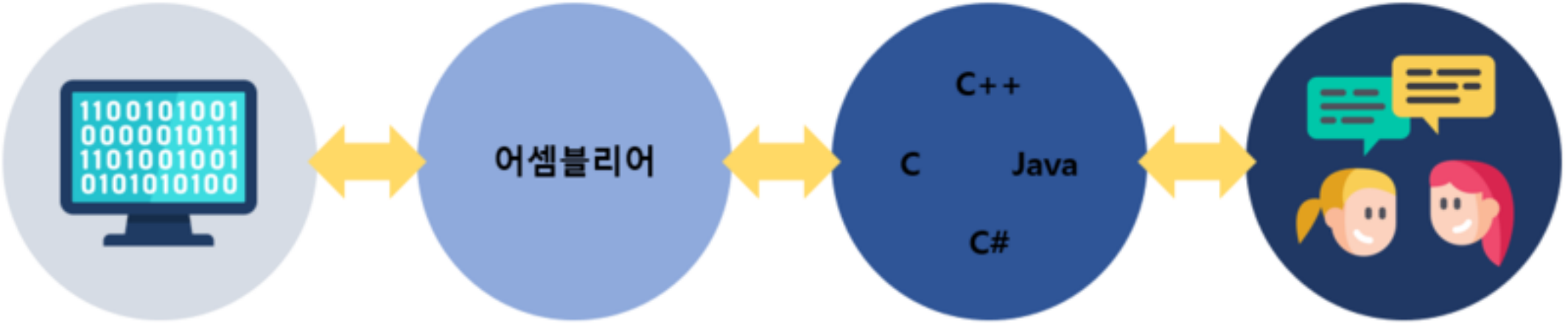
Assembly

92113528 김민기

목차

- 어셈블리어란?
- Intel & AT&T
- 레지스터
- 명령어
- 예제

어셈블리어란?


1100101001
0000010111
1101001001
0101010100
어셈블리어
C++
C
Java
C#

Intel & AT&T

Opcode	Operand1	Operand2
ADD	EAX	EBX

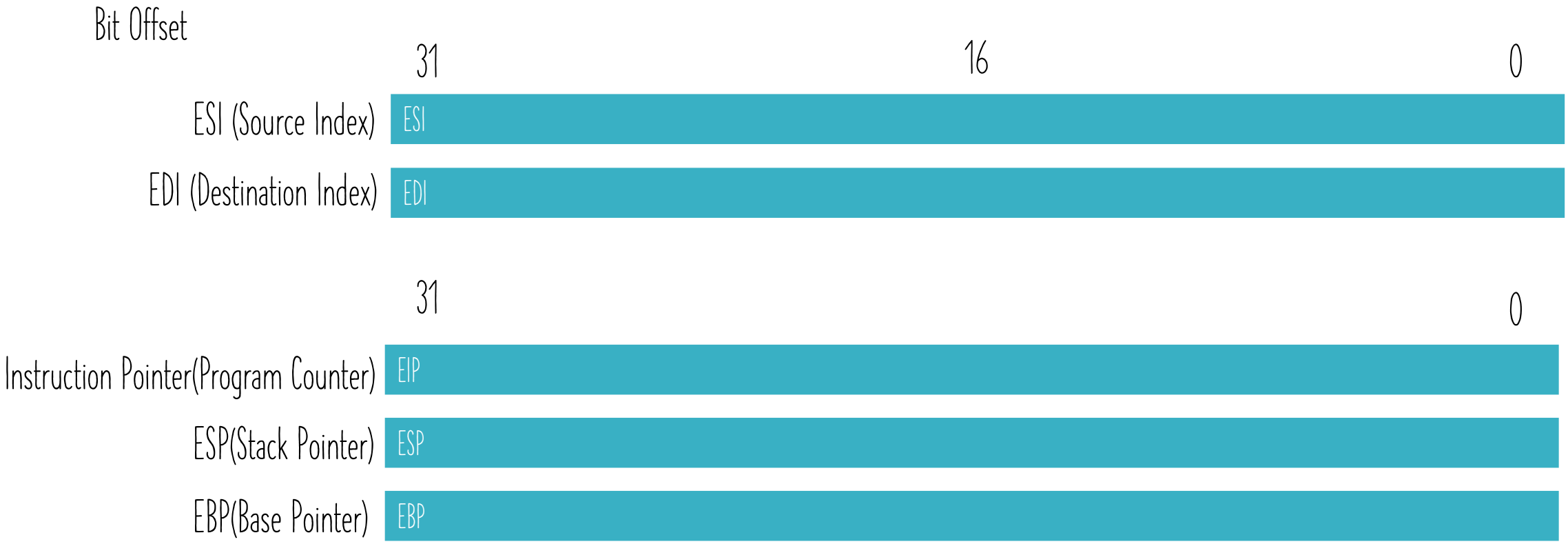
Intel	AT&T
1, 2, 3, 4, 5	$1, $2, $3, $4, $5

Intel	AT&T
EAX, EBX, EBP	%EAX, %EBX, %EBP

register


Bit Offset
31
16
8
0
EAX
AH
AL
(AX)
EBX
BH
BL
(BX)
ECX
CH
CL
(CX)
EDX
DH
DL
(DX)

register


Bit Offset
31
16
0
ESI (Source Index)
ESI
EDI (Destination Index)
EDI
31
0
Instruction Pointer(Program Counter)
EIP
ESP(Stack Pointer)
ESP
EBP(Base Pointer)
EBP

Command

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	inc 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 $0x80	OS에 할당된 인터럽트 영역을 system call	인터럽트
nop	nop	아무 동작도 하지 않는다. (No Operation)	

예제

```c
#include<stdio.h>
int main(){
    int a=1;
    int b=2;
    int c = a + b;

    printf("%d", c);
}
```

예제

```
push        ebp
mov         ebp,esp
sub         esp,0E4h
push        ebx
push        esi
push        edi
lea         edi,[ebp+FFFFFF1Ch]
mov         ecx,39h
mov         eax,0CCCCCCCCh
rep stos    dword ptr es:[edi]
mov         ecx,9AC003h
call        009A1316
mov         dword ptr [ebp-8],1
mov         dword ptr [ebp-14h],2
mov         eax,dword ptr [ebp-8]
add         eax,dword ptr [ebp-14h]
mov         dword ptr [ebp-20h],eax
```

```
mov         eax,dword ptr [ebp-20h]
push        eax
push        9A7D08h
call        009A10CD
add         esp,8
xor         eax,eax
pop         edi
pop         esi
pop         ebx
add         esp,0E4h
cmp         ebp,esp
call        009A123F
mov         esp,ebp
pop         ebp
ret
```