EDDI
Electronic Design
Development Institute

# 에디로봇아카데미
## 임베디드 마스터 Lv2 과정

제 1기

2021. 10. 8

김태훈

# CONTENTS

EDDI
Electronic Design
Development Institute

```c
#include <stdio.h>

int mult(int num1, int num2);

int main(void)
{
    int num = 3, num2 = 2;
    int res;

    res = mult(num, num2);
    printf("res = %d\n", res);

    return 0;
}

int mult(int num1, int num2)
{
    return num1 * num2;
}
```

# CONTENTS

EDDI
Electronic Design Development Institute

```
Dump of assembler code for function main:
=> 0x0000555555555149 <+0>:     endbr64
   0x000055555555514d <+4>:     push   %rbp
   0x000055555555514e <+5>:     mov    %rsp,%rbp
   0x0000555555555151 <+8>:     sub    $0x10,%rsp
   0x0000555555555155 <+12>:    movl   $0x3,-0xc(%rbp)
   0x000055555555515c <+19>:    movl   $0x2,-0x8(%rbp)
   0x0000555555555163 <+26>:    mov    -0x8(%rbp),%edx
   0x0000555555555166 <+29>:    mov    -0xc(%rbp),%eax
   0x0000555555555169 <+32>:    mov    %edx,%esi
   0x000055555555516b <+34>:    mov    %eax,%edi
   0x000055555555516d <+36>:    callq  0x555555555192 <mult>
   0x0000555555555172 <+41>:    mov    %eax,-0x4(%rbp)
   0x0000555555555175 <+44>:    mov    -0x4(%rbp),%eax
   0x0000555555555178 <+47>:    mov    %eax,%esi
   0x000055555555517a <+49>:    lea    0xe83(%rip),%rdi        # 0x555555556004
   0x0000555555555181 <+56>:    mov    $0x0,%eax
   0x0000555555555186 <+61>:    callq  0x555555555050 <printf@plt>
   0x000055555555518b <+66>:    mov    $0x0,%eax
   0x0000555555555190 <+71>:    leaveq
   0x0000555555555191 <+72>:    retq
End of assembler dump.
```

# CONTENTS

EDDI
Electronic Design
Development Institute

## STEP 1

```
=> 0x0000555555555149 <+0>:    endbr64
```

**In the MEMORY**

| address | data | |
|---|---|---|
| 0x7fffffffdda8 | 0xf7de90b3(trash) | <- rsp |
| 0x0 | cannot access | <- rbp |

**In the register**

| name | data |
|---|---|
| rsp | 0x7fffffffdda8 |
| rbp | 0x0 |
| rip | 0x55555555514d |

# CONTENTS

EDDI
Electronic Design
Development Institute

## STEP2

```
=> 0x000055555555514d <+4>:    push   %rbp
```

push

```
1) rsp = rsp-8
2) *rsp = rbp
```

**In the MEMORY**

| address | data | |
|---|---|---|
| | | |
| 0x7fffffffdda8 | 0xf7de90b3(trash) | |
| 0x7fffffffdda0 | 0x0 | <- rsp |
| | | |
| 0x0 | cannot access | <- rbp |

**In the register**

| name | data |
|---|---|
| rsp | 0x7fffffffdda0 |
| rbp | 0x0 |
| rip | 0x55555555514e |

# CONTENTS

EDDI
Electronic Design
Development Institute

## STEP3

```
=> 0x000055555555514e <+5>:    mov    %rsp,%rbp
```

```
rbp = rsp
```

**In the MEMORY**

| address | data | |
|---|---|---|
| | | |
| 0x7fffffffdda8 | 0xf7de90b3(trash) | |
| 0x7fffffffdda0 | 0x0 | <- rsp, rbp |
| | | |
| 0x0 | cannot access | |

**In the register**

| name | data |
|---|---|
| rsp | 0x7fffffffdda0 |
| rbp | 0x7fffffffdda0 |
| rip | 0x555555555151 |

# CONTENTS

EDDI
Electronic Design
Development Institute

## STEP4

```
=> 0x0000555555555151 <+8>:    sub    $0x10,%rsp
```

```
rsp = rsp - 10
```

**In the MEMORY**

| address | data | |
|---|---|---|
| | | |
| 0x7fffffffdda8 | 0xf7de90b3(trash) | |
| 0x7fffffffdda0 | 0x0 | <- rbp |
| | | |
| 0x7fffffffdd90 | ? | <- rsp |
| | | |
| 0x0 | cannot access | |

**In the register**

| name | data |
|---|---|
| rsp | 0x7fffffffdd90 |
| rbp | 0x7fffffffdda0 |
| rip | 0x555555555155 |

# CONTENTS

EDDI
Electronic Design
Development Institute

## STEP5

```
=> 0x0000555555555155 <+12>:    movl   $0x3,-0xc(%rbp)
=> 0x000055555555515c <+19>:    movl   $0x2,-0x8(%rbp)
```

```
*(rbp-0xc) = 3
*(rbp-0x8) = 2
```

movl은 32bit 연산이라 4개만 jump
movl = move double WORD (대문자 WORD는 2 byte, 소문자 WORD는 register의 크기, cpu가 한번에 연산할 수 있는 크기)

**In the MEMORY**

| address | data | |
|---|---|---|
| 0x7fffffffdda8 | 0xf7de90b3(trash) | |
| 0x7fffffffdda0 | 0x0 | <- rbp |
| 0x7fffffffdd9c | | |
| 0x7fffffffdd98 | 0x2 | |
| 0x7fffffffdd94 | 0x3 | |
| 0x7fffffffdd90 | ? | <- rsp |
| | | |
| 0x0 | cannot access | |

**In the register**

| name | data |
|---|---|
| rsp | 0x7fffffffdd90 |
| rbp | 0x7fffffffdda0 |
| rip | 0x555555555163 |

# CONTENTS

EDDI
Electronic Design
Development Institute

## STEP5

```
=> 0x0000555555555163 <+26>:    mov    -0x8(%rbp),%edx
=> 0x0000555555555166 <+29>:    mov    -0xc(%rbp),%eax
```

```
edx = *(rbp-0x8)
eax = *(rbp-0xc)
```

**In the MEMORY**

| address | data | |
|---|---|---|
| | | |
| 0x7fffffffdda8 | 0xf7de90b3(trash) | |
| 0x7fffffffdda0 | 0x0 | <- rbp |
| 0x7fffffffdd9c | | |
| 0x7fffffffdd98 | 0x2 | |
| 0x7fffffffdd94 | 0x3 | |
| 0x7fffffffdd90 | ? | <- rsp |
| | | |
| 0x0 | cannot access | |

**In the register**

| name | data |
|---|---|
| rsp | 0x7fffffffdd90 |
| rbp | 0x7fffffffdda0 |
| rip | 0x555555555169 |
| rax | 3 |
| rdx | 2 |

# CONTENTS

EDDI
Electronic Design
Development Institute

## STEP6

```
=> 0x0000555555555169 <+32>: mov    %edx,%esi
=> 0x000055555555516b <+34>: mov    %eax,%edi
```

```
esi = edx
edi = eax
```

**In the MEMORY**

| address | data | |
|---|---|---|
| | | |
| 0x7fffffffdda8 | 0xf7de90b3(trash) | |
| 0x7fffffffdda0 | 0x0 | <- rbp |
| 0x7fffffffdd9c | | |
| 0x7fffffffdd98 | 0x2 | |
| 0x7fffffffdd94 | 0x3 | |
| 0x7fffffffdd90 | ? | <- rsp |
| | | |
| 0x0 | cannot access | |

**In the register**

| name | data |
|---|---|
| rsp | 0x7fffffffdd90 |
| rbp | 0x7fffffffdda0 |
| rip | 0x55555555516d |
| rax | 3 |
| rdx | 2 |
| rdi | 3 |
| rsi | 2 |

# CONTENTS

EDDI
Electronic Design
Development Institute

```
=> 0x000055555555516d <+36>: callq  0x555555555192 <mult>
```

```
rsp = rsp-0x8
*rsp = (next address of instruction)(0x000055555555172)
 rip = 0x555555555192
```

**In the MEMORY**

| address | data | |
|---|---|---|
| 0x7fffffffdda8 | 0xf7de90b3(trash) | |
| 0x7fffffffdda0 | 0x0 | <- rbp |
| 0x7fffffffdd9c | | |
| 0x7fffffffdd98 | 0x2 | |
| 0x7fffffffdd94 | 0x3 | |
| 0x7fffffffdd90 | ? | |
| 0x7fffffffdd88 | 0x555555555172 | <- rsp |
| | | |
| 0x0 | cannot access | |

**In the register**

| name | data |
|---|---|
| rsp | 0x7fffffffdd90 |
| rbp | 0x7fffffffdda0 |
| rip | 0x555555555192 |
| rax | 3 |
| rdx | 2 |
| rdi | 3 |
| rsi | 2 |

# CONTENTS

EDDI
Electronic Design
Development Institute

```
=> 0x0000555555555192 <+0>:  endbr64
```

```
dummy
```

**In the MEMORY**

| address | data | |
|---|---|---|
| | | |
| 0x7fffffffdda8 | 0xf7de90b3(trash) | |
| 0x7fffffffdda0 | 0x0 | <- rbp |
| 0x7fffffffdd9c | | |
| 0x7fffffffdd98 | 0x2 | |
| 0x7fffffffdd94 | 0x3 | |
| 0x7fffffffdd90 | ? | |
| 0x7fffffffdd88 | 0x555555555172 | <- rsp |
| | | |
| 0x0 | cannot access | |

**In the register**

| name | data |
|---|---|
| rsp | 0x7fffffffdd88 |
| rbp | 0x7fffffffdda0 |
| rip | 0x555555555196 |
| rax | 3 |
| rdx | 2 |
| rdi | 3 |
| rsi | 2 |

# CONTENTS

EDDI
Electronic Design
Development Institute

```
=> 0x0000555555555196 <+4>:  push   %rbp
```

```
rsp = rsp-0x8
*rsp = rbp
```

**In the MEMORY**

| address | data | |
|---|---|---|
| | | |
| 0x7fffffffdda8 | 0xf7de90b3(trash) | |
| 0x7fffffffdda0 | 0x0 | <- rbp |
| 0x7fffffffdd9c | | |
| 0x7fffffffdd98 | 0x2 | |
| 0x7fffffffdd94 | 0x3 | |
| 0x7fffffffdd90 | ? | |
| 0x7fffffffdd88 | 0x555555555172 | |
| 0x7fffffffdd80 | 0x7fffffffdda0 | <- rsp |
| | | |
| 0x0 | cannot access | |

**In the register**

| name | data |
|---|---|
| rsp | 0x7fffffffdd80 |
| rbp | 0x7fffffffdda0 |
| rip | 0x555555555197 |
| rax | 3 |
| rdx | 2 |
| rdi | 3 |
| rsi | 2 |

# CONTENTS

EDDI
Electronic Design
Development Institute

```
=> 0x0000555555555197 <+5>:  mov    %rsp,%rbp
```

```
rbp = rsp
```

**In the MEMORY**

| address | data | |
|---|---|---|
| | | |
| 0x7fffffffdda8 | 0xf7de90b3(trash) | |
| 0x7fffffffdda0 | 0x0 | |
| 0x7fffffffdd9c | | |
| 0x7fffffffdd98 | 0x2 | |
| 0x7fffffffdd94 | 0x3 | |
| 0x7fffffffdd90 | ? | |
| 0x7fffffffdd88 | 0x555555555172 | |
| 0x7fffffffdd80 | 0x7fffffffdda0 | <- rsp, rbp |
| | | |
| 0x0 | cannot access | |

**In the register**

| name | data |
|---|---|
| rsp | 0x7fffffffdd80 |
| rbp | 0x7fffffffdd80 |
| rip | 0x55555555519a |
| rax | 3 |
| rdx | 2 |
| rdi | 3 |
| rsi | 2 |

# CONTENTS

EDDI
Electronic Design Development Institute

```
=> 0x000055555555519a <+8>:  mov    %edi,-0x4(%rbp)
=> 0x000055555555519d <+11>: mov    %esi,-0x8(%rbp)
```

```
*(rbp-4) = edi
*(rbp-8) = esi
```

**In the MEMORY**

| address | data | |
|---|---|---|
| | | |
| 0x7fffffffdda8 | 0xf7de90b3(trash) | |
| 0x7fffffffdda0 | 0x0 | |
| 0x7fffffffdd9c | | |
| 0x7fffffffdd98 | 0x2 | |
| 0x7fffffffdd94 | 0x3 | |
| 0x7fffffffdd90 | ? | |
| 0x7fffffffdd88 | 0x555555555172 | |
| 0x7fffffffdd80 | 0x7fffffffdda0 | <- rsp, rbp |
| 0x7fffffffdd7c | 3 | |
| 0x7fffffffdd78 | 2 | |
| | | |
| 0x0 | cannot access | |

**In the register**

| name | data |
|---|---|
| rsp | 0x7fffffffdd80 |
| rbp | 0x7fffffffdd80 |
| rip | 0x5555555551a0 |
| rax | 3 |
| rdx | 2 |
| rdi | 3 |
| rsi | 2 |

# CONTENTS

EDDI
Electronic Design
Development Institute

```
=> 0x00005555555551a0 <+14>: mov    -0x4(%rbp),%eax
```

```
*eax = *(rbp-4)
```

**In the MEMORY**

| address | data | |
|---|---|---|
| | | |
| 0x7fffffffdda8 | 0xf7de90b3(trash) | |
| 0x7fffffffdda0 | 0x0 | |
| 0x7fffffffdd9c | | |
| 0x7fffffffdd98 | 0x2 | |
| 0x7fffffffdd94 | 0x3 | |
| 0x7fffffffdd90 | ? | |
| 0x7fffffffdd88 | 0x555555555172 | |
| 0x7fffffffdd80 | 0x7fffffffdda0 | <- rsp, rbp |
| 0x7fffffffdd7c | 3 | |
| 0x7fffffffdd78 | 2 | |
| | | |
| 0x0 | cannot access | |

**In the register**

| name | data |
|---|---|
| rsp | 0x7fffffffdd80 |
| rbp | 0x7fffffffdd80 |
| rip | 0x5555555551a3 |
| rax | 3 |
| rdx | 2 |
| rdi | 3 |
| rsi | 2 |

# CONTENTS

EDDI
Electronic Design
Development Institute

```
=> 0x00005555555551a3 <+17>: imul   -0x8(%rbp),%eax
```

```
*eax = (*eax) * (*(rbp-8))
```

**In the MEMORY**

| address | data | |
|---|---|---|
| | | |
| 0x7fffffffdda8 | 0xf7de90b3(trash) | |
| 0x7fffffffdda0 | 0x0 | |
| 0x7fffffffdd9c | | |
| 0x7fffffffdd98 | 0x2 | |
| 0x7fffffffdd94 | 0x3 | |
| 0x7fffffffdd90 | ? | |
| 0x7fffffffdd88 | 0x555555555172 | |
| 0x7fffffffdd80 | 0x7fffffffdda0 | <- rsp, rbp |
| 0x7fffffffdd7c | 3 | |
| 0x7fffffffdd78 | 2 | |
| | | |
| 0x0 | cannot access | |

**In the register**

| name | data |
|---|---|
| rsp | 0x7fffffffdd80 |
| rbp | 0x7fffffffdd80 |
| rip | 0x5555555551a7 |
| rax | 6 |
| rdx | 2 |
| rdi | 3 |
| rsi | 2 |

# CONTENTS

EDDI
Electronic Design
Development Institute

```
=> 0x00005555555551a7 <+21>: pop    %rbp
```

```
rbp = *rsp
rsp = rsp + 8
```

**In the MEMORY**

| address | data | |
|---|---|---|
| | | |
| 0x7fffffffdda8 | 0xf7de90b3(trash) | |
| 0x7fffffffdda0 | 0x0 | <- rbp |
| 0x7fffffffdd9c | | |
| 0x7fffffffdd98 | 0x2 | |
| 0x7fffffffdd94 | 0x3 | |
| 0x7fffffffdd90 | ? | |
| 0x7fffffffdd88 | 0x555555555172 | <- rsp |
| 0x7fffffffdd80 | 0x7fffffffdda0 | |
| 0x7fffffffdd7c | 3 | |
| 0x7fffffffdd78 | 2 | |
| | | |
| 0x0 | cannot access | |

**In the register**

| name | data |
|---|---|
| rsp | 0x7fffffffdd88 |
| rbp | 0x7fffffffdda0 |
| rip | 0x5555555551a8 |
| rax | 6 |
| rdx | 2 |
| rdi | 3 |

# CONTENTS

EDDI
Electronic Design
Development Institute

```
=> 0x00005555555551a8 <+22>: retq
```

```
rip = *rsp
rsp = rsp + 8
```

**In the MEMORY**

| address | data | |
|---|---|---|
| 0x7fffffffdda8 | 0xf7de90b3(trash) | |
| 0x7fffffffdda0 | 0x0 | <- rbp |
| 0x7fffffffdd9c | | |
| 0x7fffffffdd98 | 0x2 | |
| 0x7fffffffdd94 | 0x3 | |
| 0x7fffffffdd90 | ? | <- rsp |
| 0x7fffffffdd88 | 0x555555555172 | |
| 0x7fffffffdd80 | 0x7fffffffdda0 | |
| 0x7fffffffdd7c | 3 | |
| 0x7fffffffdd78 | 2 | |
| | | |
| 0x0 | cannot access | |

**In the register**

| name | data |
|---|---|
| rsp | 0x7fffffffdd90 |
| rbp | 0x7fffffffdda0 |
| rip | 0x555555555172 |
| rax | 6 |
| rdx | 2 |
| rdi | 3 |
| rsi | 2 |

# CONTENTS

EDDI
Electronic Design
Development Institute

```
=> 0x0000555555555172 <+41>: mov    %eax,-0x4(%rbp)
```

```
*(rbp-4) = eax
```

**In the MEMORY**

| address | data | |
|---|---|---|
| 0x7fffffffdda8 | 0xf7de90b3(trash) | |
| 0x7fffffffdda0 | 0x0 | <- rbp |
| 0x7fffffffdd9c | 0x6 | |
| 0x7fffffffdd98 | 0x2 | |
| 0x7fffffffdd94 | 0x3 | |
| 0x7fffffffdd90 | ? | <- rsp |
| 0x7fffffffdd88 | 0x555555555172 | |
| 0x7fffffffdd80 | 0x7fffffffdda0 | |
| 0x7fffffffdd7c | 3 | |
| 0x7fffffffdd78 | 2 | |
| | | |
| 0x0 | cannot access | |

**In the register**

| name | data |
|---|---|
| rsp | 0x7fffffffdd90 |
| rbp | 0x7fffffffdda0 |
| rip | 0x555555555175 |
| rax | 6 |
| rdx | 2 |
| rdi | 3 |
| rsi | 2 |

# CONTENTS

EDDI
Electronic Design
Development Institute

```
=> 0x0000555555555175 <+44>: mov    -0x4(%rbp),%eax
   0x0000555555555178 <+47>: mov    %eax,%esi
```

```
eax = *(rbp-4)
esi = eax
```

**In the MEMORY**

| address | data | |
|---|---|---|
| | | |
| 0x7fffffffdda8 | 0xf7de90b3(trash) | |
| 0x7fffffffdda0 | 0x0 | <- rbp |
| 0x7fffffffdd9c | 0x6 | |
| 0x7fffffffdd98 | 0x2 | |
| 0x7fffffffdd94 | 0x3 | |
| 0x7fffffffdd90 | ? | <- rsp |
| 0x7fffffffdd88 | 0x555555555172 | |
| 0x7fffffffdd80 | 0x7fffffffdda0 | |
| 0x7fffffffdd7c | 3 | |
| 0x7fffffffdd78 | 2 | |
| | | |
| 0x0 | cannot access | |

**In the register**

| name | data |
|---|---|
| rsp | 0x7fffffffdd90 |
| rbp | 0x7fffffffdda0 |
| rip | 0x55555555517a |
| rax | 6 |
| rdx | 2 |
| rdi | 3 |

# CONTENTS

EDDI
Electronic Design
Development Institute

```
=> 0x000055555555517a <+49>: lea    0xe83(%rip),%rdi        # 0x555555556004
```

```
rdi = *(rip + e83)
```

**In the MEMORY**

| address | data | |
|---|---|---|
| 0x7fffffffdda8 | 0xf7de90b3(trash) | |
| 0x7fffffffdda0 | 0x0 | <- rbp |
| 0x7fffffffdd9c | 0x6 | |
| 0x7fffffffdd98 | 0x2 | |
| 0x7fffffffdd94 | 0x3 | |
| 0x7fffffffdd90 | ? | <- rsp |
| 0x7fffffffdd88 | 0x555555555172 | |
| 0x7fffffffdd80 | 0x7fffffffdda0 | |
| 0x7fffffffdd7c | 3 | |
| 0x7fffffffdd78 | 2 | |
| | | |
| 0x0 | cannot access | |

**In the register**

| name | data |
|---|---|
| rsp | 0x7fffffffdd90 |
| rbp | 0x7fffffffdda0 |
| rip | 0x555555555181 |
| rax | 6 |
| rdx | 2 |
| rdi | 0x555555556004 |
| rsi | 6 |

# CONTENTS

EDDI
Electronic Design
Development Institute

```
=> 0x0000555555555181 <+56>: mov    $0x0,%eax
```

```
eax = 0
```

**In the MEMORY**

| address | data | |
|---|---|---|
| 0x7fffffffdda8 | 0xf7de90b3(trash) | |
| 0x7fffffffdda0 | 0x0 | <- rbp |
| 0x7fffffffdd9c | 0x6 | |
| 0x7fffffffdd98 | 0x2 | |
| 0x7fffffffdd94 | 0x3 | |
| 0x7fffffffdd90 | ? | <- rsp |
| 0x7fffffffdd88 | 0x555555555172 | |
| 0x7fffffffdd80 | 0x7fffffffdda0 | |
| 0x7fffffffdd7c | 3 | |
| 0x7fffffffdd78 | 2 | |
| | | |
| 0x0 | cannot access | |

**In the register**

| name | data |
|---|---|
| rsp | 0x7fffffffdd90 |
| rbp | 0x7fffffffdda0 |
| rip | 0x555555555186 |
| rax | 0 |
| rdx | 2 |
| rdi | 0x555555556004 |

# CONTENTS

EDDI
Electronic Design
Development Institute

```
=> 0x0000555555555186 <+61>: callq  0x555555555050 <printf@plt>
```

```
rsp = rsp - 8
*rsp = next address of instruction (0x55555555518b)
rip  = 0x555555555050
```

**In the MEMORY**

| address | data | |
|---|---|---|
| | | |
| 0x7fffffffdda8 | 0xf7de90b3(trash) | |
| 0x7fffffffdda0 | 0x0 | <- rbp |
| 0x7fffffffdd9c | 0x6 | |
| 0x7fffffffdd98 | 0x2 | |
| 0x7fffffffdd94 | 0x3 | |
| 0x7fffffffdd90 | ? | |
| 0x7fffffffdd88 | 0x55555555518b | <- rsp |
| 0x7fffffffdd80 | 0x7fffffffdda0 | |
| 0x7fffffffdd7c | 3 | |
| 0x7fffffffdd78 | 2 | |
| | | |
| 0x0 | cannot access | |

**In the register**

| name | data |
|---|---|
| rsp | 0x7fffffffdd88 |
| rbp | 0x7fffffffdda0 |
| rip | 0x555555555050 |
| rax | 0 |
| rdx | 2 |
| rdi | 0x555555556004 |

# CONTENTS

EDDI
Electronic Design
Development Institute

```
=> 0x0000555555555190 <+71>:  leaveq
```

```
rsp = rbp
pop rbp
==============
rsp = rbp - 8
rbp = *rbp
```

**In the MEMORY**

| address | data | |
|---|---|---|
| 0x7fffffffdda8 | 0xf7de90b3(trash) | <- rsp |
| 0x7fffffffdda0 | 0x0 | |
| 0x7fffffffdd9c | 0x6 | |
| 0x7fffffffdd98 | 0x2 | |
| 0x7fffffffdd94 | 0x3 | |
| 0x7fffffffdd90 | ? | |
| 0x7fffffffdd88 | 0x55555555518b | |
| 0x7fffffffdd80 | 0x7fffffffdda0 | |
| 0x7fffffffdd7c | 3 | |
| 0x7fffffffdd78 | 2 | |
| 0x0 | cannot access | <- rbp |

**In the register**

| name | data |
|---|---|
| rsp | 0x7fffffffdd88 |
| rbp | 0x7fffffffdda0 |
| rip | 0x555555555050 |