

## Latihan Soal 9 2023

### 1. Array

Diberikan kode assembly berikut:

```
local_array:
    pushl %ebp
    movl %esp, %ebp
    subl $32, %esp
    movl $0x1, 0xffffffff0(%ebp)
    movl $0x3, 0xffffffff4(%ebp)
    movl $0x5, 0xffffffff8(%ebp)
    movb $0x69, 0xffffffffeb(%ebp)
    movb $0x66, 0xffffffffec(%ebp)
    movb $0x69, 0xffffffffed(%ebp)
    movb $0x74, 0xffffffffee(%ebp)
    movb $0x62, 0xffffffffef(%ebp)
    movl -8(%ebp), %eax
    andl 8(%ebp), %eax
    movl %eax, -4(%ebp)
    leal -21(%ebp), %edx
    movl -4(%ebp), %eax
    addl %edx, %eax
    movzbl (%eax), %eax
    movsbl %al, %eax
    movl %ebp, %esp
    popl %ebp
    ret
```

Apabila diketahui bahwa huruf 'a' merupakan karakter ASCII ke 97 dan 'b' merupakan karakter ASCII ke 98, dan seterusnya. **Lengkapilah** kode bahasa C berikut berdasarkan kode assembly di atas:

```
int local_array(int i)
{
    int A[3] = { 1, 3, 5 };
    char B[5] = { i, f, i, t, b };

    int idx = ____; A[2] & i

    return B[idx];
}
```

Jika argumen i dalam fungsi local\_array diberi nilai 15, nilai apa yang akan

dikembalikan oleh fungsi local\_array tersebut? B[5] = A[0] = 1

## 2. Struktur Data

Diberikan struktur data sebagai berikut pada mesin IA32:

union = ambil yg paling besar

```

struct s1 {
    char a[3]; 3 -> 4
    union u1 b; 4
    int c; 4
};
12 bytes

struct s2 {
    struct s1 *d; 4
    char e; 1 -> 4
    int f[4]; 16
    struct s2 *g; 4
};
28 bytes

union u1 {
    struct s1 *h;
    struct s2 *i;
    char j;
};
4 bytes

```

Lengkapilah kode C yang kosong pada pasangan kode assembly – bahasa C di bawah ini

|  |  |
|--|--|
| <pre> proc1:     movl 0 -&gt; *d     pushl %ebp     movl 4 -&gt; e     movl %esp, %ebp     movl 8(%ebp), %eax f[0]     movl 12(%eax), %eax f[1]     movl %ebp, %esp     popl %ebp     ret </pre>   | <pre> int proc1(struct s2 *x) {     return x-&gt; f[1] ; }      eax = *x     eax = *(x + 12) </pre>  |
| <pre> proc2:     pushl %ebp     movl %esp, %ebp     movl 8(%ebp), %eax *x     movl 4(%eax), %eax b.i     movl 20(%eax), %eax b.i -&gt; f[3]     movl %ebp, %esp     popl %ebp     ret </pre>   | <pre> int proc2(struct s1 *x) {     return x-&gt; ; }      x -&gt; b.i -&gt; f[3]      eax = *x     eax = *(x + 4) # dia udh ngakses u1 b     eax = *(x + 4 + 20) </pre>       |
| <pre> proc3:     pushl %ebp     movl %esp, %ebp     movl 8(%ebp), %eax *x     movl (%eax), %eax x-&gt; h     movsbl 4(%eax), %eax x-&gt; h -&gt; b.j     movl %ebp, %esp     popl %ebp     ret </pre>  | <pre> char proc3(union u1 *x) {     return x-&gt; ; }      x -&gt; h -&gt; b.j      eax = *(x + 4) </pre>  |
| <pre> proc4:     pushl %ebp     movl %esp, %ebp     movl 8(%ebp), %eax *x     movl (%eax), %eax x-&gt; i     movl 24(%eax), %eax x-&gt; i -&gt; g     movl (%eax), %eax x-&gt; i -&gt; g -&gt; d     movsbl 1(%eax), %eax x-&gt; i -&gt; g -&gt; d -&gt; a[1]     movl %ebp, %esp     popl %ebp     ret </pre> | <pre> char proc4(union u1 *x) {     Return x-&gt; ; }      x -&gt; i -&gt; g -&gt; d -&gt; a[1]      eax = *x     eax = *(x + 24) # akses s2 *i     eax = *(x + 24 + 1) </pre> |

3. Diberikan kode C rekursif berikut:

```
int silly(int n, int *p)
{
    int val, val2;
    if (n > 0)
        val2 = silly(n << 1, &val);
    else
        val = val2 = 0;
    *p = val + val2 + n;
}
```

dengan hasil assembly sebagai berikut

```
silly:
    pushl %ebp
    movl %esp,%ebp
    subl $20,%esp
    pushl %ebx
    movl 8(%ebp),%ebx
    testl %ebx,%ebx
    jle .L3
    addl $-8,%esp
    leal -4(%ebp),%eax
    pushl %eax
    leal (%ebx,%ebx),%eax
    pushl %eax
    call silly
    jmp .L4
.p2align 4,,7
.L3:
    xorl %eax,%eax
    movl %eax,-4(%ebp)
.L4:
    movl -4(%ebp),%edx
    addl %eax,%edx
    movl 12(%ebp),%eax
    addl %edx,%ebx
    movl %ebx,(%eax)
    movl -24(%ebp),%ebx
    movl %edx,%eax
    movl %ebp,%esp
    popl %ebp
    ret
```

- a. Apakah variabel val disimpan pada stack? Jika iya, pada byte offset berapakah (relatif terhadap %ebp) variabel tersebut disimpan? Mengapa perlu disimpan pada stack?  
ya, pada %ebp-4, krn butuh pass pointer buat recursive call
- b. Apakah variabel val2 disimpan pada stack? Jika iya, pada byte offset berapakah (relatif terhadap %ebp) variabel tersebut disimpan? Mengapa perlu disimpan pada stack?  
tidak
- c. Apakah ada nilai yang disimpan (jika ada) pada posisi -24(%ebp)? Jika ada yang disimpan, mengapa nilai tersebut perlu disimpan?  
ya, nilai %ebx krn callee save register
- d. Apakah ada nilai yang disimpan (jika ada) pada posisi -8(%ebp)? Jika ada yang disimpan, mengapa nilai tersebut perlu disimpan?  
tidak