Latihan Soal 9 2023

1. **Array**

   Diberikan kode assembly berikut:

```
local_array:
      pushl %ebp
      movl  %esp, %ebp
      subl  $32, %esp
      movl  $0x1, 0xfffffff0(%ebp)
      movl  $0x3, 0xfffffff4(%ebp)
      movl  $0x5, 0xfffffff8(%ebp)
      movb  $0x69, 0xffffffeb(%ebp)
      movb  $0x66, 0xffffffec(%ebp)
      movb  $0x69, 0xffffffed(%ebp)
      movb  $0x74, 0xffffffee(%ebp)
      movb  $0x62, 0xffffffef(%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:

```
_char_ 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? Idx= 5 & 15 (0101 & 1111)___nilai yg tersimpan pada B[5], yaitu -16(%ebp) , yaitu LSB dari nilai A[0]___

2. **Struktur Data**

Diberikan struktur data sebagai berikut pada mesin IA32:

```
struct s1 {
  char a[3];
  union u1 b;
  int c;
};
```

```
struct s2 {
  struct s1 *d;
  char e;
  int f[4];
  struct s2 *g;
};
```

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

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

proc1:
pushl %ebp
movl %esp,%ebp
movl 8(%ebp),%eax
movl 12(%eax),%eax
movl %ebp,%esp
popl %ebp
ret
	int proc1(struct s2 *x)
	{
	return x->_____ ;
	}
	Jawab: return x->f[1];

proc2:
pushl %ebp
movl %esp,%ebp
movl 8(%ebp),%eax
movl 4(%eax),%eax
movl 20(%eax),%eax
movl %ebp,%esp
popl %ebp
ret
	int proc2(struct s1 *x)
	{
	return x->_____ ;
	}
	Jawab: return x->b.i->f[3];

proc3:
pushl %ebp
movl %esp,%ebp
movl 8(%ebp),%eax
movl (%eax),%eax
movsbl 4(%eax),%eax
movl %ebp,%esp
popl %ebp
ret
	char proc3(union u1 *x)
	{
	return x->_____ ;
	}
	Jawab: return x->h->b.j;

proc4:
pushl %ebp
movl %esp,%ebp
movl 8(%ebp),%eax
movl (%eax),%eax
movl 24(%eax),%eax
movl (%eax),%eax
movsbl 1(%eax),%eax
	char proc4(union u1 *x)
	{
	return x->_____ ;
	}
	Jawab: x->i->g->d->a[1];

movl %ebp,%esp popl %ebp ret	

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?
   jawab: yes, -4, Need to pass pointer to it to 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?
   jawab: no

c. Apakah ada nilai yang disimpan (jika ada) pada posisi -24(%ebp)? Jika ada yang disimpan, mengapa nilai tersebut perlu disimpan?
   jawab: the value of %ebx is saved here, because %ebx is a %callee-save register.

d. Apakah ada nilai yang disimpan (jika ada) pada posisi -8(%ebp)? Jika ada yang disimpan, mengapa nilai tersebut perlu disimpan?
   jawab: nothing is stored here