ISA do IA-32 *(parte 1)*

Teste 3

Nº	**Nome**	**Turma/Grupo/Nº:**
		Total de horas dedicadas a PI+AC na semana anterior **:**

Nota: Apresente sempre o raciocínio ou os cálculos que efectuar; o não cumprimento desta regra equivale à não resolução do exercício.

1. Considere o seguinte o seguinte programa em C (listagem incompleta) que foi editado num ficheiro e posteriormente compilado para executar num PC (com CPU IA32):

```
void test3 (int *xp, int *yp)
{
      int x,y;
      corpo_da_função
}

void main ()
{
      int x = 5;
      int y = 2;
      test3 (&x, &y);
      printf ("x=%d , y=%d /n", x, y);
}
```

Considere ainda a seguinte listagem obtida durante o desenvolvimento desse programa:

```
00401060 <_test3>:
  401060:   55                      push   %ebp
  401061:   89 e5                   mov    %esp,%ebp
  401063:   53                      push   %ebx
  401064:   8b 4d 08                mov    0x8(%ebp),%ecx
  401067:   8b 5d 0c                mov    0xc(%ebp),%ebx
  40106a:   8b 11                   mov    (%ecx),%edx
  40106c:   8b 03                   mov    (%ebx),%eax
  40106e:   8d 04 80                lea    (%eax,%eax,4),%eax
  401071:   c1 e0 05                shl    $0x5,%eax
  401074:   83 c0 40                add    $0x40,%eax
  401077:   89 01                   mov    %eax,(%ecx)
  401079:   8d 54 d2 07             lea    0x7(%edx,%edx,8),%edx
  40107d:   89 13                   mov    %edx,(%ebx)
  40107f:   5b                      pop    %ebx
  401080:   5d                      pop    %ebp
  401081:   c3                      ret
```

Sabe-se que, no `main`, no fim da execução da instrução que invoca a função `test3` (e correspondente à instrução de `call` do IA32), os registos do CPU continham os seguintes valores:

%eax: 0x5	*%ebx*: 0x2c00	*%ebp*: 0x40fc98
%ecx: 0x2c	*%esi*: 0x8008	*%esp*: 0x40fc84
%edx: 0xffffff80	*%edi*: 0x12	*%eip*: 0x401060

a) **(A)** **Indique, justificando**, como se obteve a listagem com o código da função em *assembly* (i.e., que utilitários do Unix é que se teriam usado e como).

b) **(A/R)** Quando o processador tiver concluído a execução da 1ª instrução do corpo da função (procure-a, pensando!), **indique, justificando**, a lista de registos e de todas as células de memória que foram modificadas (i.e., onde um novo valor foi escrito), desde que se analisou o conteúdo dos registos.

c) **(A/R)** Sabendo que a instrução em `0x401064` coloca no registo `%ecx` o apontador para a variável `x`, **indique, justificando**, o valor do operando origem (*source*) na instrução de `mov` que começa no endereço `0x401079`.
Sugestão: Veja 1º que valor vai ser colocado no registo `%edx` logo em `0x40106a` e depois como esse valor é usado...

d) **(R)** Complete a questão da alínea **b)**: **indique, apresentando os cálculos**, os novos valores que deverão estar nesses locais (se foi modificado mais que uma vez, indique apenas o último valor).

e) **(R/B)** Recupere o código do corpo da função em C (resolução no verso desta folha).

Nº	**Nome**	**Turma/Grupo/Nº:**