Homework Assignment 2  
CSE 399 C++, Spring 2008

Name:

Due: Wednesday, Jan 30th at noon.

Assumptions: For all of these problems you may assume the following

- sizeof(int) = 4; sizeof(short) = 2; sizeof(char) = 1; all pointers require 4 bytes
- The stack starts at address 100 and grows up.
- The heap starts at address 400 and grows up.
- ??? represents an unknown/uninitialized value.

Question 1 (10 points) : Given the following declarations:

```c
char c = 'A';
char * p = &c;
char ** p2 = &p;
void * v = &p2;
```

Examine each of the following expressions. If the expression is illegal, write ILLEGAL. If the expression is legal, write its type (i.e. int ** or unsigned long\ etc):

- &p2
- p2[2]
- p + 4
- &p2[4]
- v[4]

Question 2 (5 points): There is an old C programmer’s joke which goes as follows:

Two strings walk into a bar. The first one says

    Hi I’d like a beer.A2%asd$ASDlk2;3423Ammm.234ASDfmm1ASDFLJ: #@$

The second says

You’ll have to pardon my friend, he’s not null terminated.
Explain the joke:

Question 3 (32 points): Given the following code:

```c
int x = 42; /* x is at address 100 */
int y = 13; /* y is at address 104 */
int * p; /* p is at address 108 */
int ** p2; /* p2 is at address 112 */
/* Location 1 */
p = &y;
p2 = &p;
/* Location 2 */
*p2 = &x;
**p2 = 11;
/* Location 3 */
*p = 12;
/* Location 4 */
```

Fill in the following table with the values of x, y, p, and p2 at the above indicated 4 locations:

<table>
<thead>
<tr>
<th></th>
<th>Loc 1</th>
<th>Loc 2</th>
<th>Loc 3</th>
<th>Loc 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>y</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>p</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>p2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Question 4 (13 points): Consider the following code:

```c
int * foo(int x) {
    int a[2];
    a[0] = x; a[1] = x+1;
    return a;
}
...
int * p1 = foo(2);
int * p2 = foo(3);
```

At the conclusion of this code snippet, what are the values of each of the following (2 pts each):

- p1[0]
- p1[1]
- p2[0]
- p2[1]

Explain why (5 pts):
Question 5 (35 points): Consider the following code:

```c
void * copy(int * dst, int * src, int count) {
    /* dst is at 124, src is at 128, count is at 132 */
    /* Location 2*/
    while (count) {
        count --;
        dst[count] = src[count];
    }
    /* Location 3 */
    return src + 1; /* be careful ... */
}
...
int a[3]; /* a[0] is at 100 */
ext = 2; /* b is at 112 */
ext * x; /* x is at 116 */
ext * p = malloc (2 * sizeof (*p)); /* p is at 120 */
a[0] = 9; a[1] = 22; a[2] = 112;
x = &a[1];
/* Location 1 */
x[0] = 33;
x[1] = 99;
x = copy (p, x, b);
/* Location 4 */
x[-1] = 4;
x[0] = 5;
/* Location 5*/
```

Fill in the following table indicating the values of each variable/memory location at each marked program point above. Some boxes are filled in for you.
Question 6 (5 pts): Consider the following code:

```c
int a[2];
int b;
int i;
b = 5;

for (i = 0; i <= 2; i++) {
a[i] = i;
}
printf("b is %d\n", b);
```

When the program is run, the value of b mysteriously changes from 5 to 2, even though no assignment is made to b. Explain why this occurs: