

Homework 10

Problem 1

main.c	foo.c
<pre>char *p = "hello"; void print(); int main { print(); retur</pre>	<pre>#include <stdio.h> extern char *p; int n = 1000; static char *p2 = "hello moto!" void foo() { printf("%s %d", p, n); } static void foo1() { printf("%s", p2); }</pre>

Indicate the type of the following symbols, e.g. **defined global, referenced global or local**

File	Symbol	Type
main.c	p	
	print	
foo.c	p	
	n	
	p2	
	foo	
	foo1	

Problem 2

<pre>#include <stdio.h> char c = 5; int a[5]; void foo(int x) { static int y = 7; int b = x + 1; printf("%d\n", b); }</pre>

Indicate the location of the following symbols, e.g. .data, .bss, .text or stack.

Symbol	Location
c	
a	
y	
b	
foo	

Problem 3

<pre> /* file : a.c */ extern int p3(void); static int x = 1; int *xp = &x; void f2(int f) { } void p1() { f2(p3() + *xp); } </pre>	Disassembly of section .text: <pre> 00000000 <f2>: 0: 55 push %ebp 1: 89 e5 mov %esp,%ebp 3: 5d pop %ebp 4: c3 ret 00000005 <p1>: 5: 55 push %ebp 6: 89 e5 mov %esp,%ebp 8: 83 ec 08 sub \$0x8,%esp b: e8 fc ff ff ff call c <p1+0x7> 10: 8b 15 00 00 00 00 mov 0x0,%edx 16: 8b 12 mov (%edx),%edx 18: 01 d0 add %edx,%eax 1a: 83 ec 0c sub \$0xc,%esp 1d: 50 push %eax 1e: e8 fc ff ff ff call 1f <p1+0x1a> 23: 83 c4 10 add \$0x10,%esp 26: c9 leave 27: c3 ret Disassembly of section .data: 00000000 <x>: 0: 01 00 00 00 00000004 <xp>: 4: 00 00 00 00 </pre>
---	--

Question:

1. Complete the following relocation records:

RELOCATION RECORDS FOR [.text]:

OFFSET	TYPE	VALUE
0000000c	R_386_PC32	p3
_____	_____	_____
_____	_____	_____

RELOCATION RECORDS FOR [.data]:

OFFSET	TYPE	VALUE
_____	_____	_____

2. If p3 is relocated to 0x080483f3 and p1 is relocated to 0x080483d0, what will the underlined instruction be changed to after linking?

Problem 4

<pre>/* file: a.c */ #include <stdio.h> static int foobar2k = 1; int foobar1k; int main() { if (foobar2k == 1) { foobar2k = 0; foobar1k = foobar(); printf("yes%d\n", foobar1k); } if (foobar2k == 2) { printf("ok\n"); return 2; } else if (foobar1k == 2) { return 1; } else { return 0; } }</pre>	<pre>/* file: b.c */ int foobar2k; int foobar1k = 1000; int foobar() { foobar2k = foobar1k = 2; return main(); }</pre>
	Question: What's the output if we run "gcc a.c b.c && ./a.out" on a 32-bit machine?