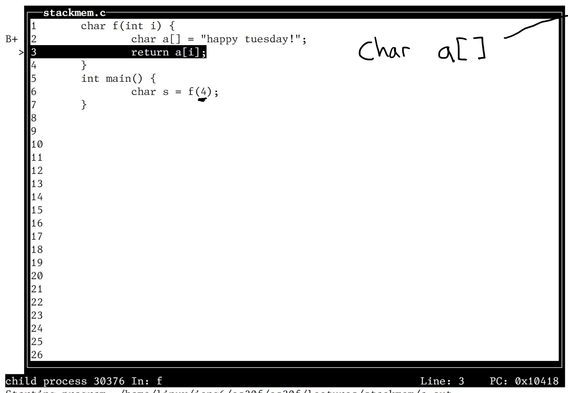
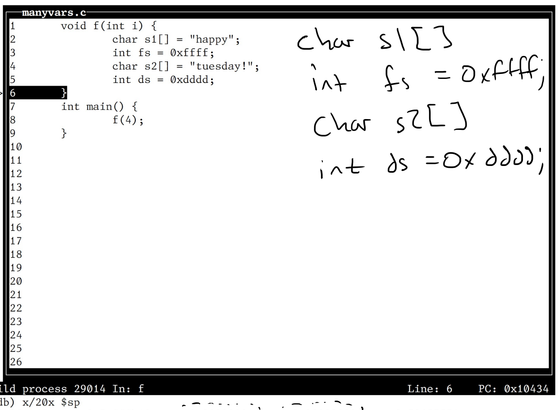
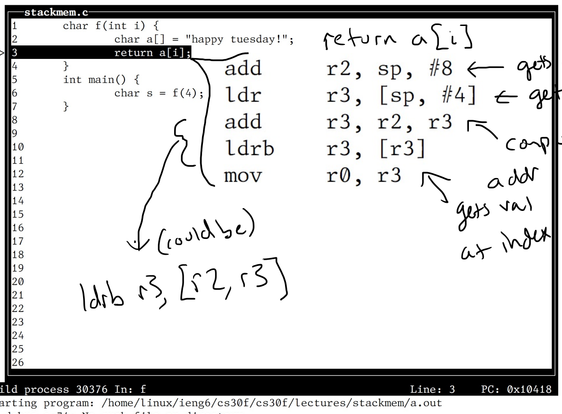

stackmem.c
1 char f(int i) {
2 char a[] = "happy tuesday!";
3 return a[i];
4 }
5 int main() {
6 char s = f(4);
7 }
Char a[]
stack-allocated array
child process 30376 In: f Line: 3 PC: 0x10418
Starting program: /home/linux/ieng6/cs30f/cs30f/lectures/stackmem/a.out
dl-debug.c:74: No such file or directory.
dl-debug.c:74: No such file or directory.
dl-debug.c:74: No such file or directory.
examine → x/20x $sp
address
20 words
hex
Breakpoint 1, f (i=4) at stackmem.c:2
(gdb) s
(gdb) x/20x $sp
0x7efffae0: 0x00000000 0x00000004 0x70706168 0x75742079
0x7efffaf0: 0x61647365 0x00002179 0x00000000 0x7efffb0c
0x7efffb00: 0x00000000 0x00000000 0x00000000 0x76e90294
0x7efffb10: 0x76fb5000 0x7efffc64 0x00000001 0x0001043c
0x7efffb20: 0x76fb9318 0x76fb9000 0x00000000 0x00000000
(gdb)
4
p p a h
u t y
a d s e
\0 ! y
0
fp


twostrs.c
1 void f(int i) {
2 char s1[] = "happy";
3 char s2[] = "tuesday!";
4 }
5 int main() {
6 f(4);
7 }
char s1[]
char s2[]
child process 30044 In: f Line: 4 PC: 0x10424
(gdb) s
(gdb) s
(gdb) x/40x $sp
0x7efffae0: 0x00000000 0x00000004 0x000103b0 0x73657574
0x7efffaf0: 0x21796164 0x00010400 0x70706168 0x00010079
0x7efffb00: 0x00000000 0x7efffb0c 0x00000000 0x76e90294
0x7efffb10: 0x76fb5000 0x7efffc64 0x00000001 0x00010438
0x7efffb20: 0x76fb9318 0x76fb9000 0x00000000 0x00000000
0x7efffb30: 0x000102c0 0x00000000 0x00000000 0x00000000
0x7efffb40: 0x76fff000 0x00000000 0xcc42e7a2 0xc4541ee2
0x7efffb50: 0x00000000 0x00000000 0x00000000 0x00000000
0x7efffb60: 0x00000000 0x00000000 0x00000000 0x00000000
0x7efffb70: 0x00000000 0x00000000 0x00000000 0x00000000
(gdb)
Should we get/expect this layout on all C impls/arch?
A: Yes B: No
4
s e u t
! y a d
\0
P P a h
\0 y


manyvars.c
1 void f(int i) {
2 char s1[] = "happy";
3 int fs = 0xffff;
4 char s2[] = "tuesday!";
5 int ds = 0xdddd;
6 }
7 int main() {
8 f(4);
9 }
char s1[]
int fs = 0xffff;
Char s2[]
int ds = 0xdddd;
child process 29014 In: f Line: 6 PC: 0x10434
(gdb) x/20x $sp
0x7efffad8: 0x7efffb10 0x00000004 0x00000000 0x73657574
0x7efffae8: 0x21796164 0x00010400 0x70706168 0x00010079
0x7efffaf8: 0x0000dddd 0x0000ffff 0x00000000 0x7efffb0c
0x7efffb08: 0x00000000 0x76e90294 0x76fb5000 0x7efffc64
0x7efffb18: 0x00000001 0x00010450 0x76fb9318 0x76fb9000
(gdb)
Which order do we get
4 s2 s1 ds fs
4 s1 s2 fs ds
4 ds s2 fs s1
A B C
4
s e u t
! y a d
\0
P P a h
\0 y
d d d d
f f f f


stackmem.c
1 char f(int i) {
2 char a[] = "happy tuesday!";
3 return a[i];
4 }
5 int main() {
6 char s = f(4);
7 }
return a[i]
add r2, sp, #8 ← gets array addr
ldr r3, [sp, #4] ← gets index
add r3, r2, r3 ← computes addr w/index
ldrb r3, [r3]
mov r0, r3 ← gets val at index
(could be)
ldrb r3, [r2, r3]
r2
r3
0x.... ae8
0x.... aec
0x79 'y'
child process 30376 In: f Line: 3 PC: 0x10418
Starting program: /home/linux/ieng6/cs30f/cs30f/lectures/stackmem/a.out
dl-debug.c:74: No such file or directory.
dl-debug.c:74: No such file or directory.
dl-debug.c:74: No such file or directory.
Breakpoint 1, f (i=4) at stackmem.c:2
(gdb) s
(gdb) x/20x $sp
sp+8
sp+12
0x7efffae0: 0x00000000 0x00000004 0x70706168 0x75742079
0x7efffaf0: 0x61647365 0x00002179 0x00000000 0x7efffb0c
0x7efffb00: 0x00000000 0x00000000 0x00000000 0x76e90294
0x7efffb10: 0x76fb5000 0x7efffc64 0x00000001 0x0001043c
0x7efffb20: 0x76fb9318 0x76fb9000 0x00000000 0x00000000
(gdb)