Assignment 9

1. Briefly describe the concept of “Stack Frame”.

A stack frame is basically the collection of everything that a function needs when it gets called. This includes temporary variables, saved copies of modified registers, argument requirements, and the return address for when the function is done executing.

1. Briefly describe the concept of a “Calling Convention”.

A calling convention can be looked at as instructions for how to receive arguments for a function call or command execution. Calling conventions also contain directions for how to return a result after the function has completed execution.

1. Why do the book examples always start functions with “push ebp” and “mov ebp, esp”?

Because ebp is used as a way to keep trace backwards up the stack since it is a pointer the ebp for the previous frame. By pushing ebp then moving esp to it you create basically, a trail of steps to trace backwards up the stack.

1. What is the x64 equivalent to “push ebp” and “mov ebp, esp”?

Push rbp and mov rbp, rsp

1. What are the differences between “Microsoft x64” calling convention and “System V AMD64 ABI calling convention”?

There are many differences between these 2 calling convention types like what registers they use and that they are made for different operating systems. In coding, however, the main difference is that in Microsoft calling convention a shadow space is provided while in AMD64 ABI it must be declared by the programmer.

1. Upon entry to myfunction, what does the stack look like when using Microsoft x64 calling convention?

The stack has the return address, the shadow space, and then the last parameter in ascending order.

1. Upon entry to myfunction what does the stack look like when using stdcall convention?

The parameters are pushed onto the stack from right to left. EAX, ECX, and EDX are used in the function.