Operating Systems (234123) - Spring 2015
Home Assignment 1 - Dry

Due date:	Sunday, 17.4.2015, 12:30
Teaching assistant in charge:	Arie Tal

Question 1

In class we have seen the sequence:

```
pushl %ebp
movl %esp, %ebp
```

(a) Please explain when and where this sequence is used and why.

(b) Assume we are not setting `%ebp` to `%esp` (nor storing the value of `%esp` at the entry to a callee to any other register or memory) , could you suggest another way for a callee to access its parameters and local variables?

(c) What would be the advantages/disadvantages of the approach you suggested in (b) compared to using `%ebp` for that purpose?

Question 2

(a) What is the purpose of privilege rings?

(b) In what way can code in CPL 3 access instructions that require CPL 0?

Question 3

(a) Why does the `int` instruction save the `%ss` and `%esp` registers? Where are they being saved?

(b) What is the purpose of the Task State Segment (TSS, see slides from Tutorial 4), and how is it being used when accessing the kernel via a system call?

(c) When does the TSS get modified and why?

Question 4

(a) What will the following code do, exactly?

```
int main(int argc, char *argv[])
{
   while(fork() > 0);
}
```

(b) What is the maximum number of child processes that each process in the above code could have?