COS330 PRACTICAL 5

By Dylan Kapnias (u18108467)

Question 6

6.2) D will not be able to correctly determine if CV is a virus or not due to CV itself only propagating after it has internally checked whether D will register it as a virus. If D determines that CV is a virus, main-program just carries on to it's next action, however if D does not determine CV as a virus, the CV will propagate itself, thus D is not working as intended.

6.3) The metamorphic version of the code will produce the same effect as the original code due to lines 2,3,5,6 performing redundant actions i.e., pushing ecx to the stack and then popping the stack back into ecx, such that ecx never changed and swapping eax and ebx twice, such that the registers retain their original values. The only effect it has, is in further obfuscating the original virus execution such that signature-based virus detection software will have a harder time in registering that the code is in fact a virus.