Yi-Rou (Monica) Hung u22561154

6.2) For this problem we have a contradiction or more of a paradox.

Firstly, in case 1, D(CV) returns TRUE that means that CV has a virus, then the program moves to the next part. If CV does not exhibit virus-like behavior, how can D know that the CV is a virus?

In Case 2 D(CV) returns FALSE (not a virus), D(CV) claims that the CV doesn't have a virus, then program will execute the 'infect-executable' part, which means that it shows virus-like behavior and infect the programs. This shows that D is wrong, because it is contradicting itself and telling us that CV is a virus. Thus, D cannot correctly determine whether CV is a virus or not.

6.3) The metamorphic code added some extra instructions to the original code so that the code functionality remains identical to the original one. The 'push ecx' and 'pop ecx', 'swap eax' and 'swap ebx' and 'nop' will have no impact. The purpose of metamorphic code is to evade signature-based detection. So by having these no-op instructions, it is harder for the anti-virus detection by pattern-matching to pick it up because it does not change the outcome of the original program. So therefore, the virus can appear different each time it is examined by the antivirus software, even though it behaves the same.