Methodology

There are two ways to analyse a piece of program: statically and dynamically. Static analysis means we can open the program in a disassembler and/or decompiler. Popular options are `Ghidra` and `IDA`. In this project, I used `Ghidra` for static analysis because it is free and provides a decompiler. `IDA` has a free version but it does not include a decompiler.

TODO: Add a screenshot of Ghidra interface

In dynamic analysis, we run the program and pause it at the beginning. Then we proceed step by step which allows us to see the status of stack, memory, registers and instructions. This is also known as called *debugging*. Common softwares include `x64dbg`, `OllyDbg` and `WinDbg`. I used `x64dbg` and `OllyDbg` interchangeably in this project.

TODO: screenshot of x64dbg

To debug a dll, we cannot run it directly. A dll (or library in general) is just a collection of functions. There is no `main` function as the entry point. In order to debug a function in a library, we need to write a program which loads the library and call the function. In this project, such program is created, in fact several were written to fulfill different needs when debugging.