|  |  |  |
| --- | --- | --- |
| Week | Malware Analysis Tools and Techniques | Duration |
| 7 | OLLYDBG Practical | 120 mins |

**Lesson Objectives**

The objective of this practical is to familiarise the students of how to use OllyDBG to reverse-engineer a PE.

# Lab 01 [120 mins]

In this lab, you will try to reverse engineer the file: Q1.exe.

You can download the file <https://goo.gl/TnLhPj>

**Instructions**

Run the program and note the message box that the program displays. It seems that the program’s evaluation period has expired.



You need to reverse-engineer the program so that you can bypass the evaluation period check.

**Question 1**

What does the function located at address 0x401073 perform? How many parameters do the function accepts?

**Question 2**

What is the return value when this function finishes executing? What is the desired value?

**Question 3**

When will the jump taken at address 0x40107B?

Make the necessary changes for the jump to take place and run the program.

You should see the following screen.



**Question 4**

What does the function located at address 0x4010A9 perform?

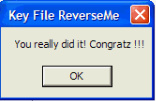
**Question 5**

When is the jump located at 0x4010B0 taken?

Make the necessary changes for the jump to take place.

**Question 6**

Make all necessary changes so that you are able to see the following message box.



**Question 7**

Patch the file so that you can always display the “You really did it!” box every time you run the PE.

\*\*\* END \*\*\*