**LAB 8**

**AIM:**

To learn debugging using various tools: IDA pro, x64dbg, olly dbg and windbg.

**SOFTWARE REQUIRED:**

IDA Freeware, x64DBG, and WinDBG.

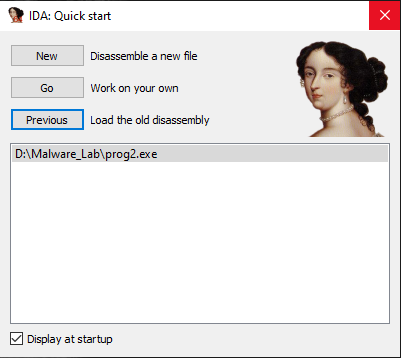
**INTRODUCTION:**

In this practical lab we will use various tools such as IDA Freeware, x64DBG, and WinDBG to Debug EXE or Executable files.

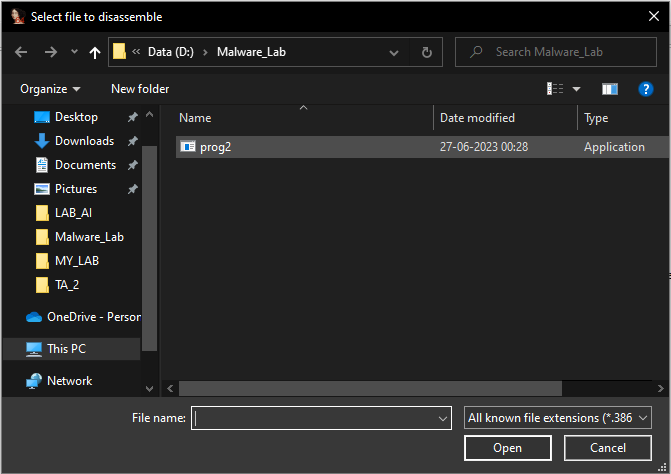
All the tools that are mentioned above are free and open source tools expect for IDA which also has a paid version known as IDA Pro. We will use these tools to Debug an EXE or Executable file. WinDBG is a Microsoft propritory tool but the other two tools can be used in other operating systems as well.

**STEPS TO DEBUG IN IDA FREEWARE:**

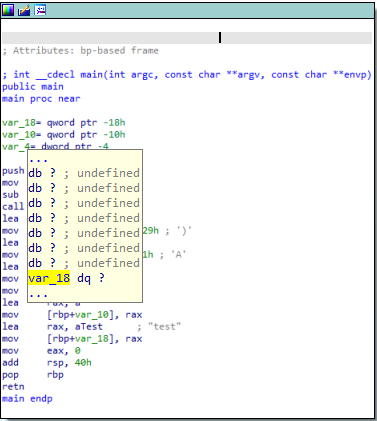
1. Download and install IDA Freeware and Open it.



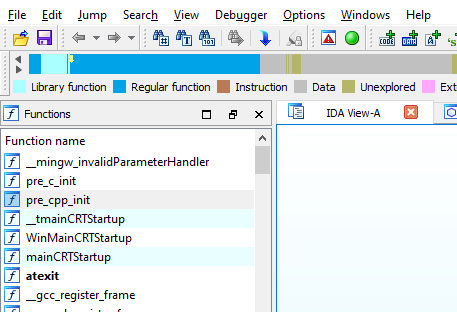
1. Once the above screen appears, select the New option to start a new project.



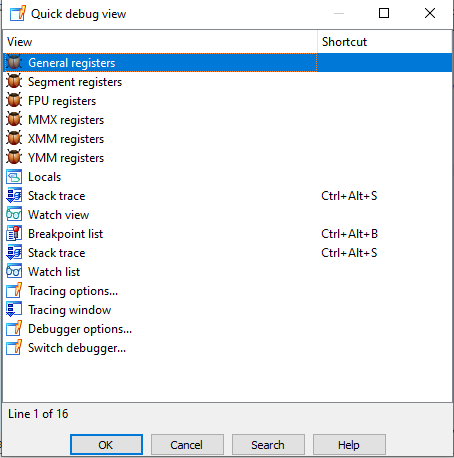
1. Select the file you want to upload which in this case is the prog2 file and click on Open to load the given file into IDA.



1. Once the file gets loaded, there would be various options available in the menu bar that would be visible at the top left corner of the screen, in those options, select the Debugger option.



1. When you select the Debugger option, a drop down menu will appear, from that menu select Quick Debug View and the below screen would appear.



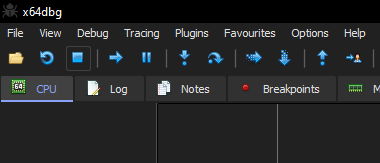
1. From the above window you can select various options to view various debugging options, amongst them, select General Registers and click OK.



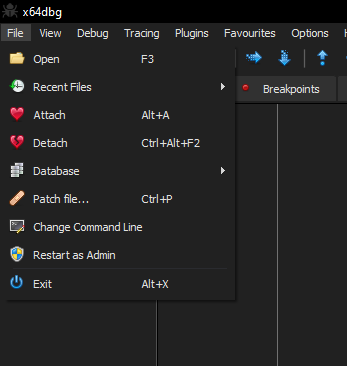
**Conclusion:** This way you can debug an executable file in various ways using IDA.

**STEPS TO DEBUG IN x64DBG**:

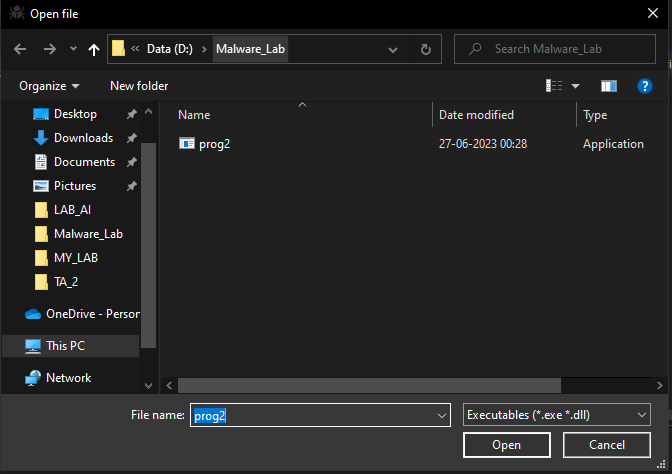
1. Download and Install x64DBG and open it.



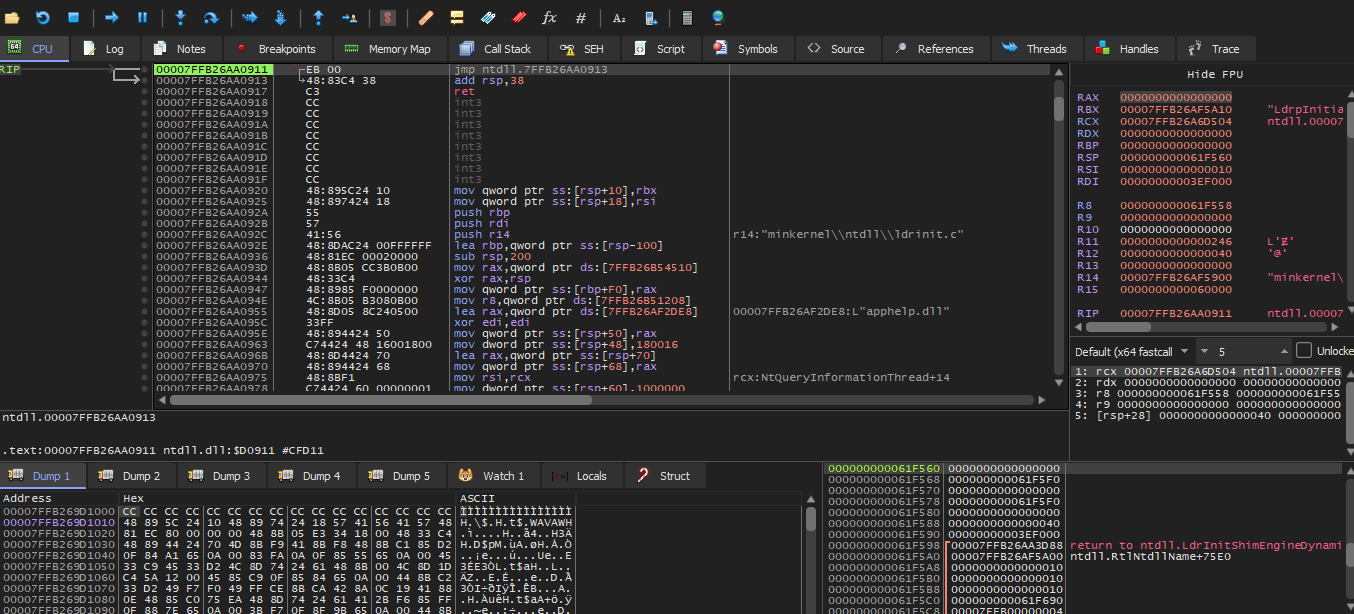
1. Once the above screen appears, select File and click on Open, or press F3.



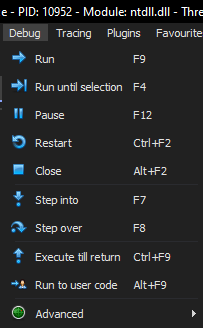
1. Once you click on Open, select the file you want to open. Select the file you want to open and Click on open.



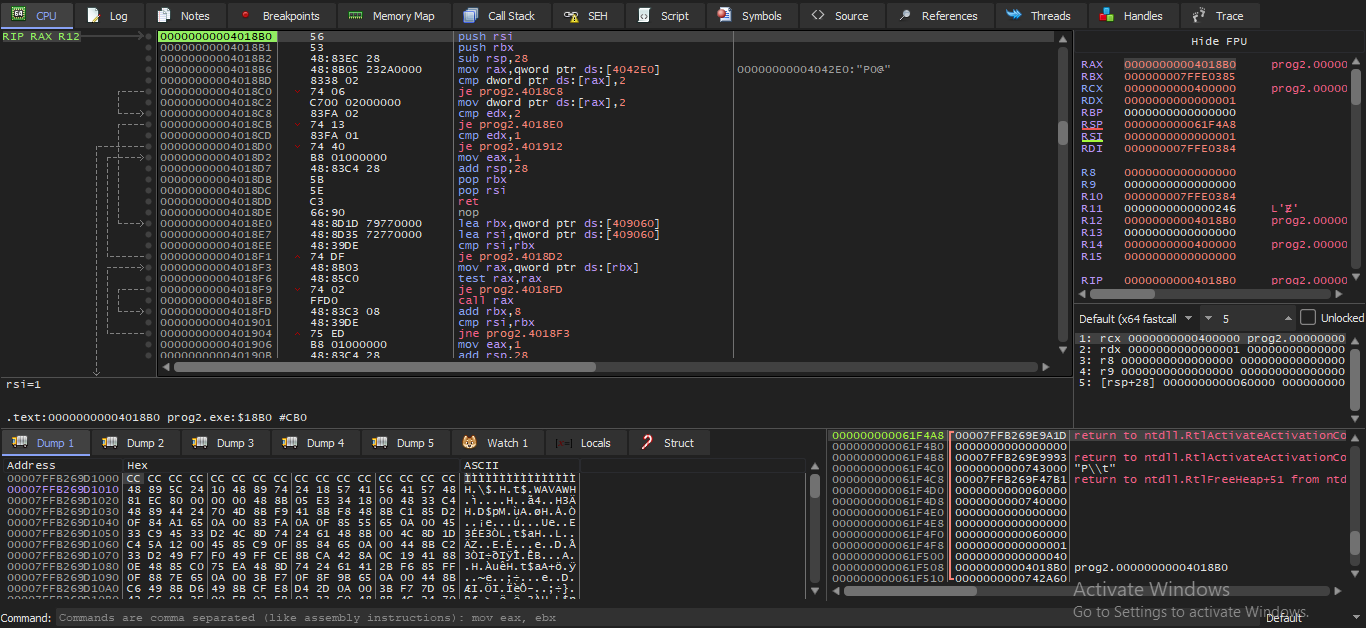
1. Once the file opens the below screen will be available



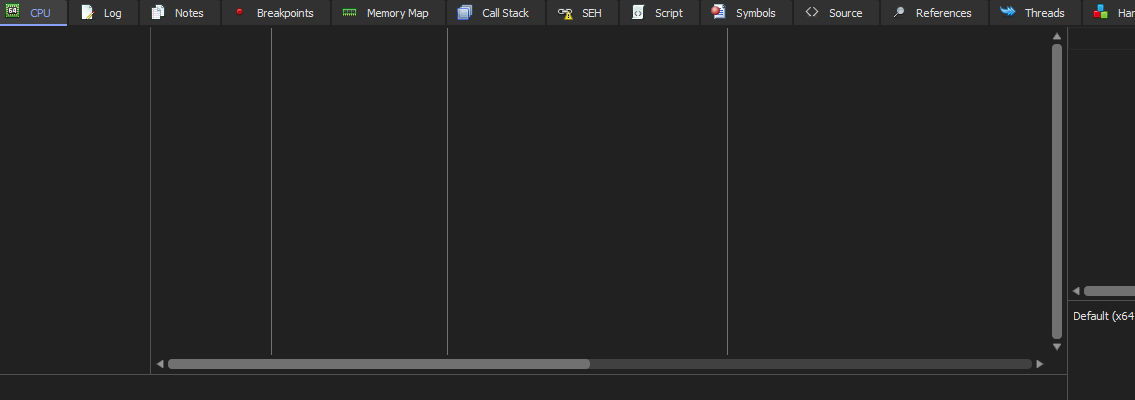
1. Once the file has loaded, then we can debug the file. From the no. of options available select Debug or F9.



1. Click on Run and the file will get Debugged.



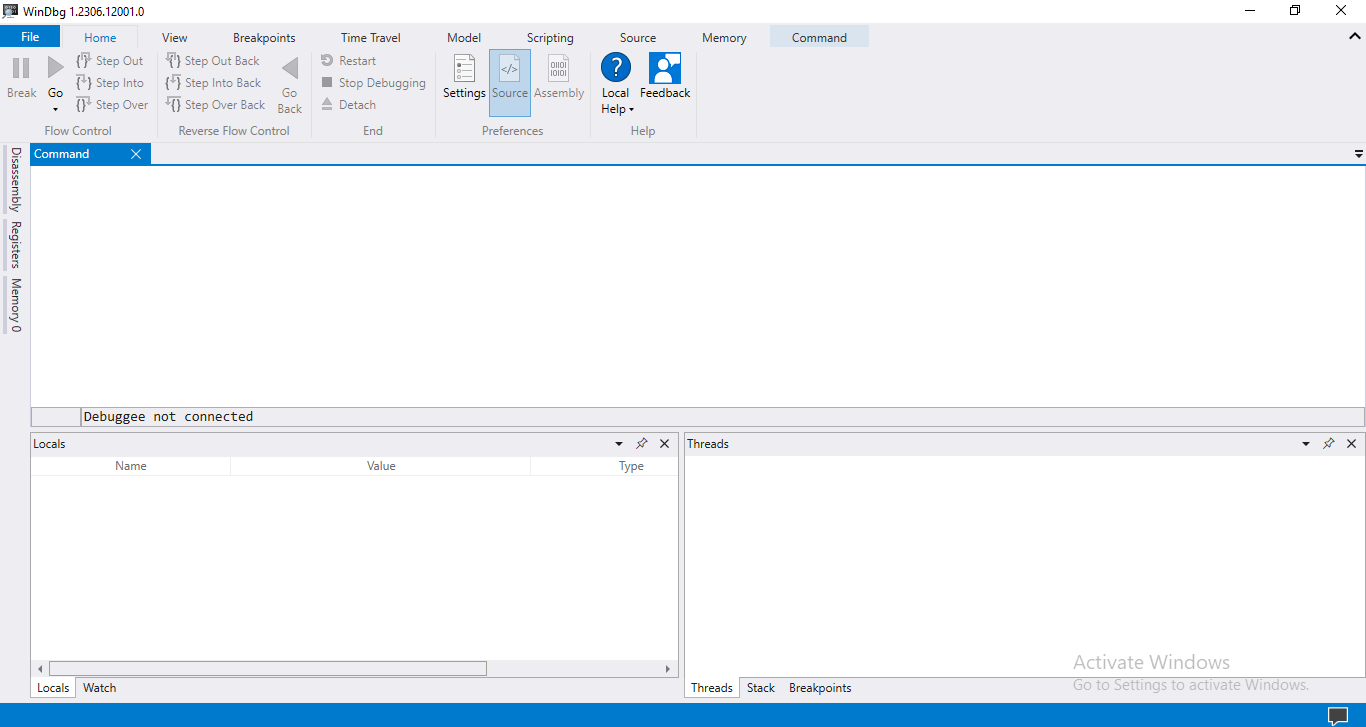
1. Now that the file has been Debugged you can see the details and when you are done with it click on Close in Debug menu or press Alt + F12 and all the operations will close.



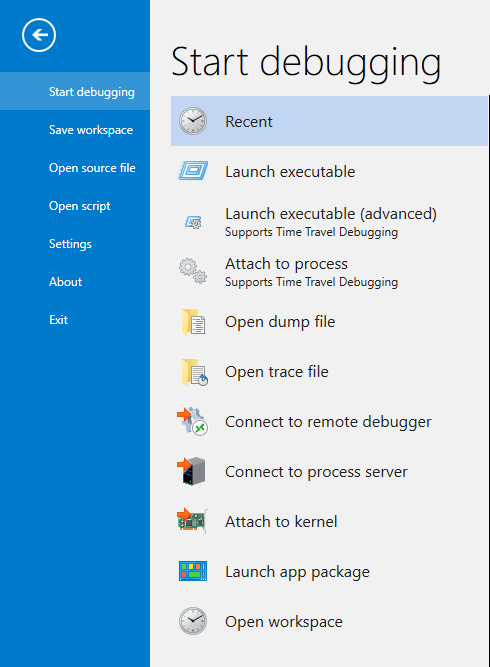
**Conclusion:** This is how you Debug a file in x64.

**STEPS TO DEBUG IN WINDBG:**

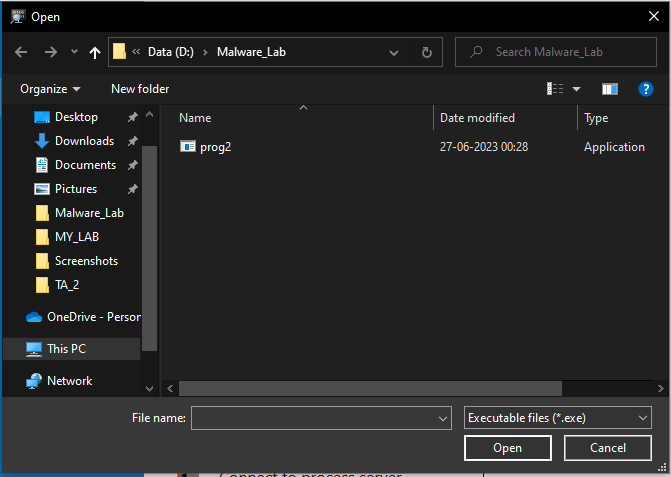
1. Download and Install WinDBG and open it.



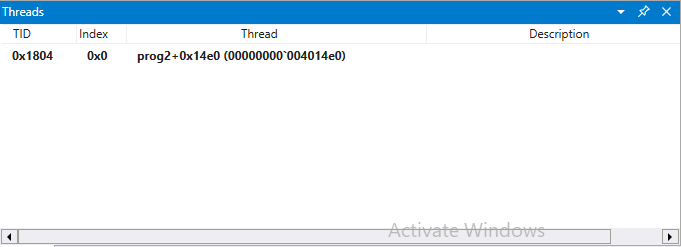
1. Select on File option and a list of options will be available. From those options click on Launch Executables.

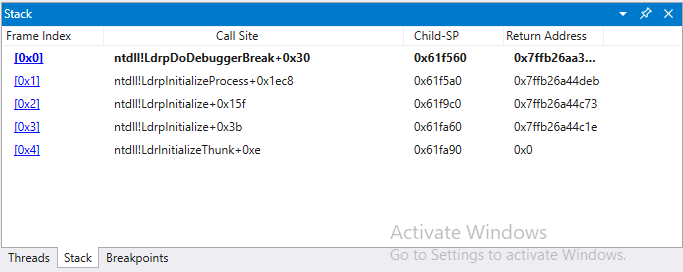


1. Once you click on Launch Executables, select the file you want to open and Click on Open.

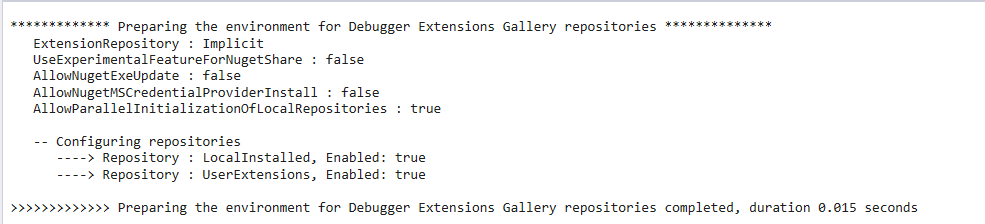


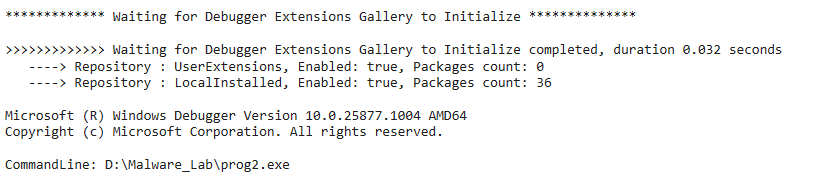
1. Once you open the file you will be able to see the Threads and Stacks in the file.

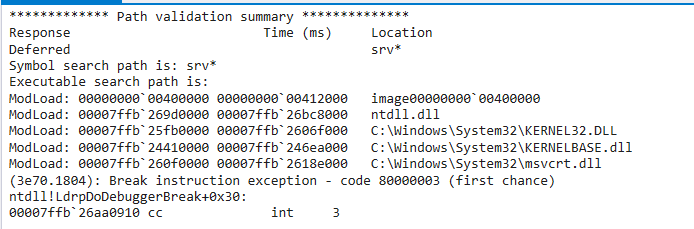




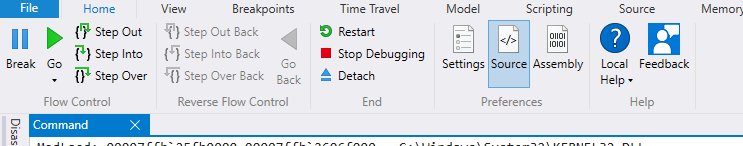
1. Now from the number of options available in the tool, select Debug. Once you select Debug the following would occur.



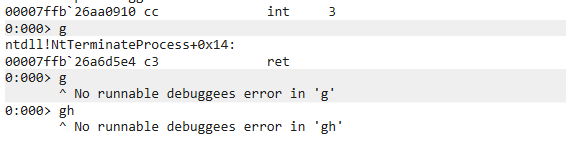




1. This will show you various details and further option to debug the file in real time to look for more errors and malicious codes by clicking on GO option.



1. Once you click on Go it will show you 2 different types of exceptions if available. Those errors are Handled and Unhandled Exceptions.



**Conclusion:** In this way we can use various tools to Debug files and look for any errors that might be available in the executable