Lab 11: Using OllyDbg to Analyze Lab09-01.exe

Course Name: Malware Analysis and Reverse Engineering (IAM302)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 22/2/2023

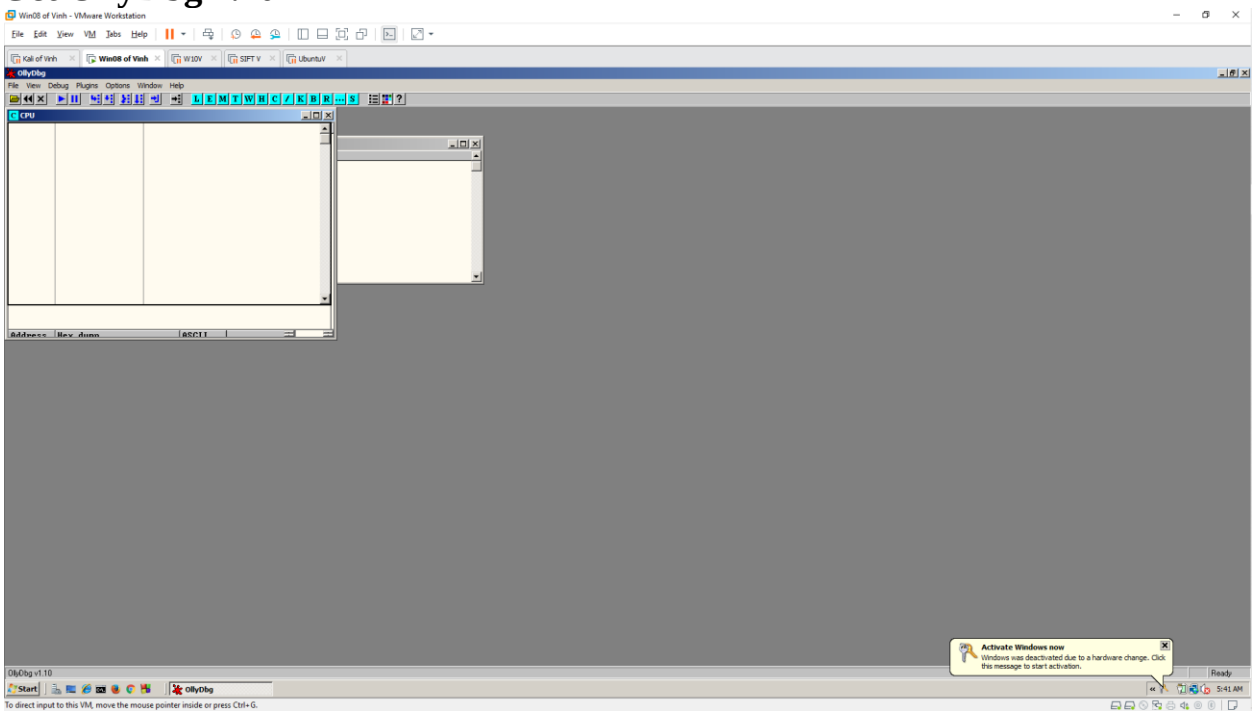
What You Need

- A Windows machine, real or virtual. I tried this on Windows 7, 10, and Server 2008 and it works on them all.

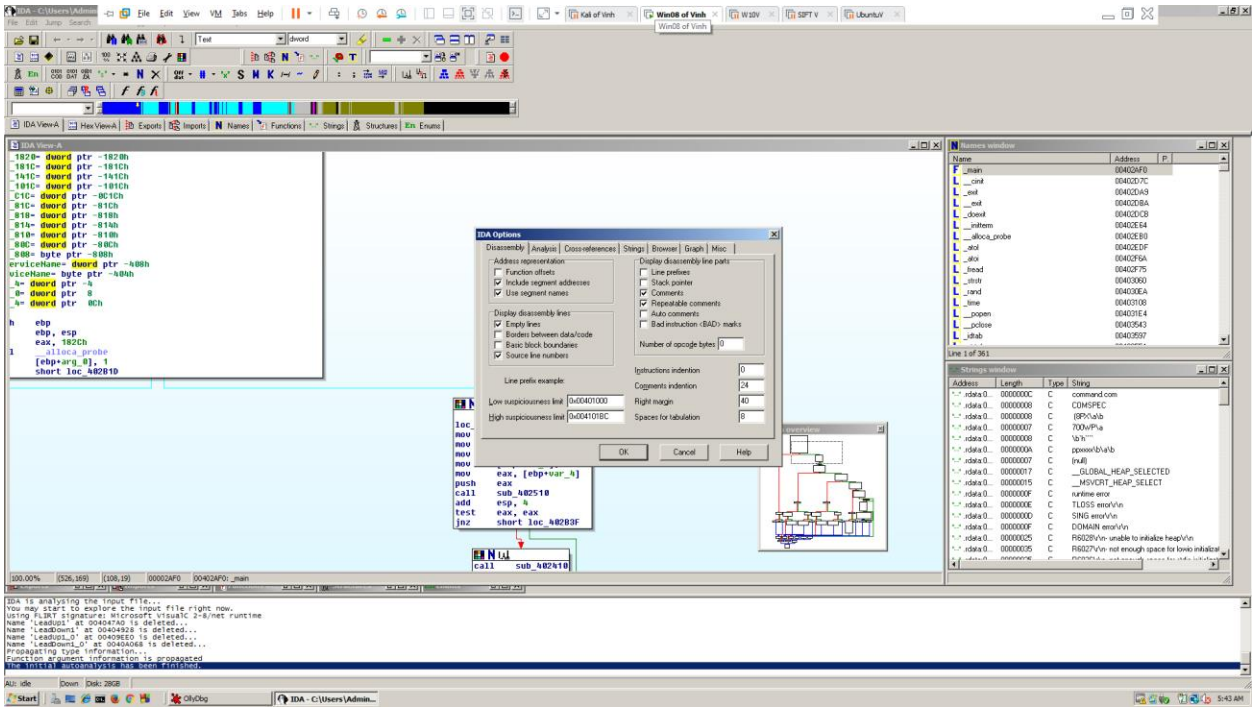
Purpose

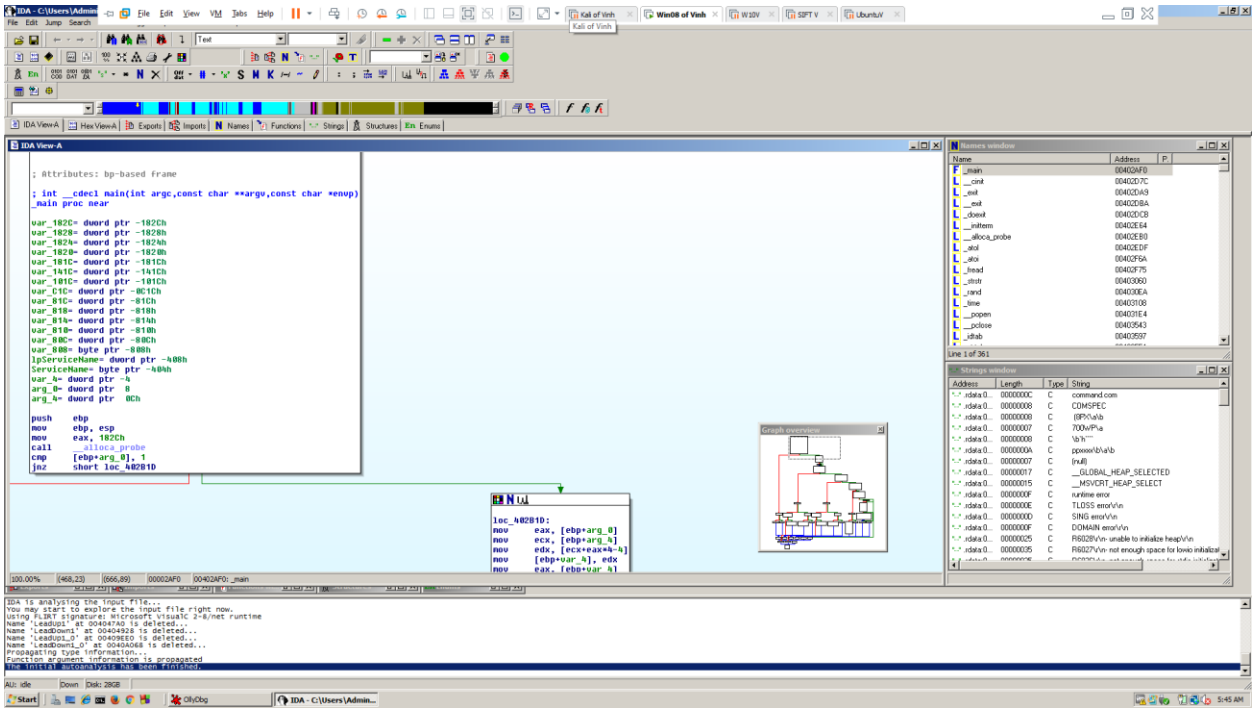
- This is just the beginning of Lab09-01, performing the first run-through. This analysis shows that if the code is executed as it is, it checks for a certain registry key, and if that key is absent, it deletes itself

Get OllyDbg 1.10

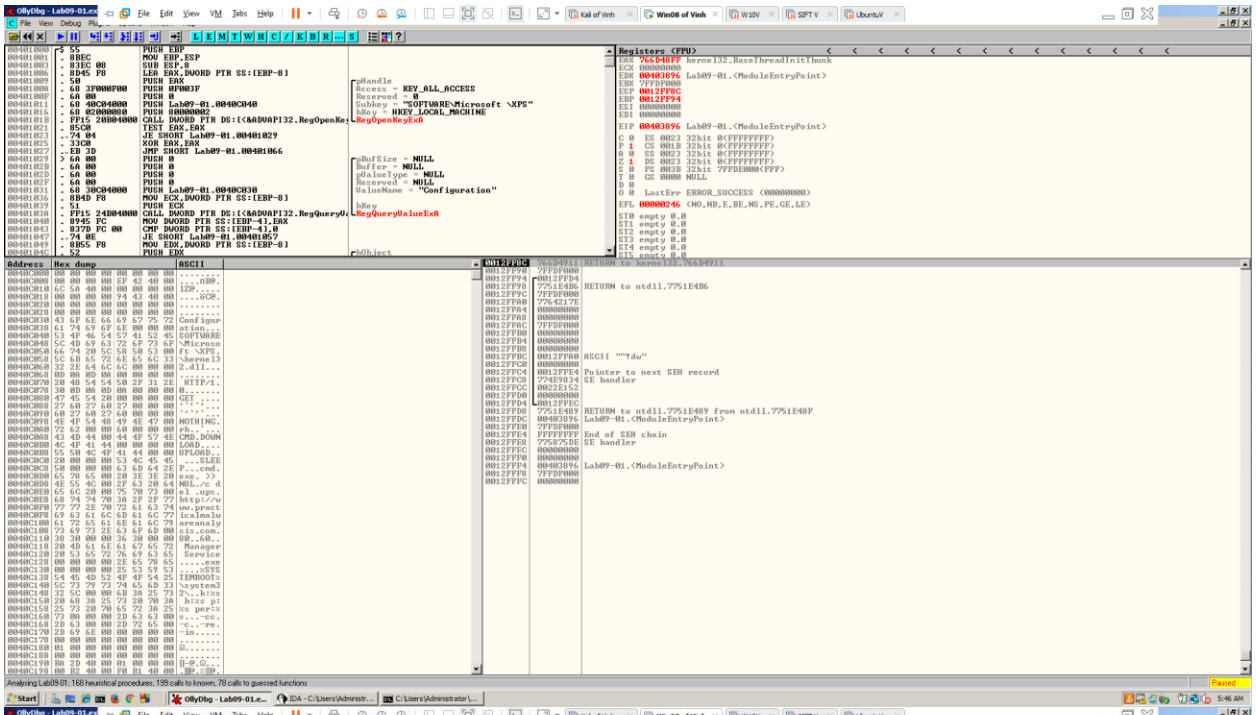


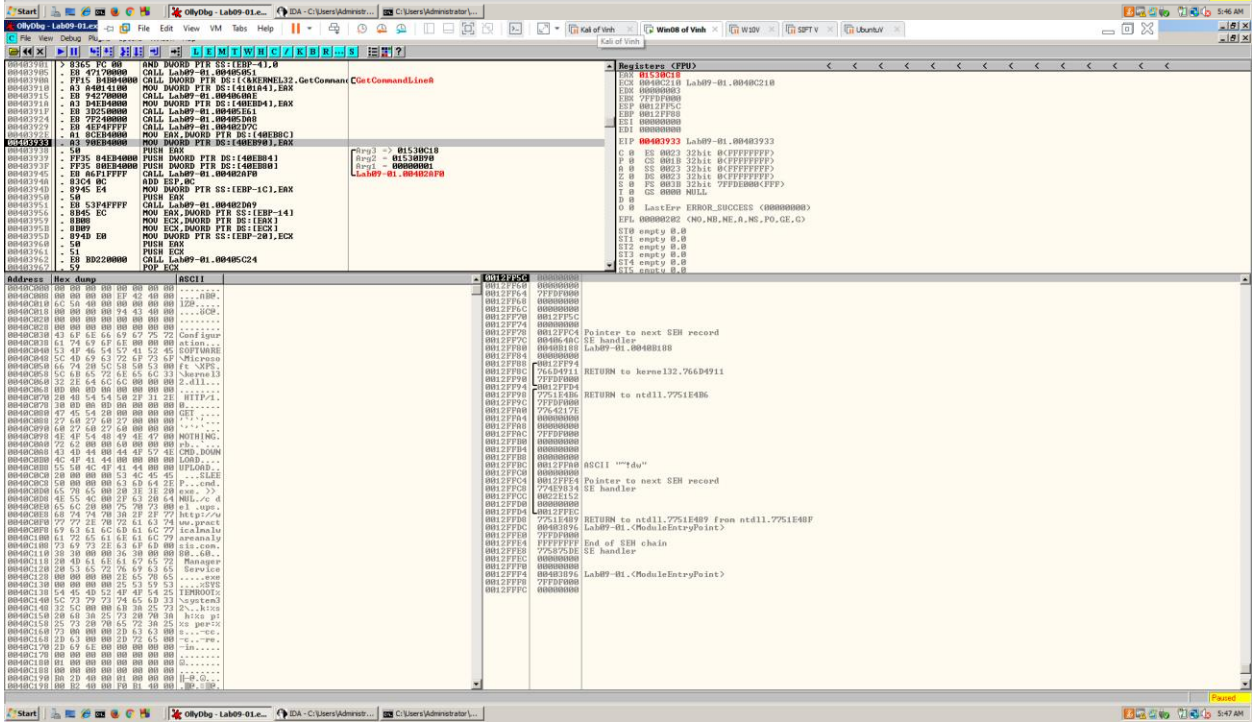
Finding the Main Entry Point





Using OllyDbg to Walk Through Quickly


OllyDbg - Lab09-01.ex
Registers (FPU)
Analysing Lab09-01: 168 heuristical procedures, 155 calls to known, 78 calls to guessed functions
Paused
5:46 AM


OllyDbg - Lab09-01.ex
Registers (FPU)
Paused
5:47 AM