**Lab 15: Patching EXEs with Ollydbg**

**Course Name:** Malware Analysis and Reverse Engineering (IAM302)

**Student Name:** Nguyễn Trần Vinh – SE160258

**Instructor Name:** Mai Hoàng Đỉnh

**Lab Due Date:** 11/3/2023

**Purpose**

* To practice disassembling and modifying binaries.

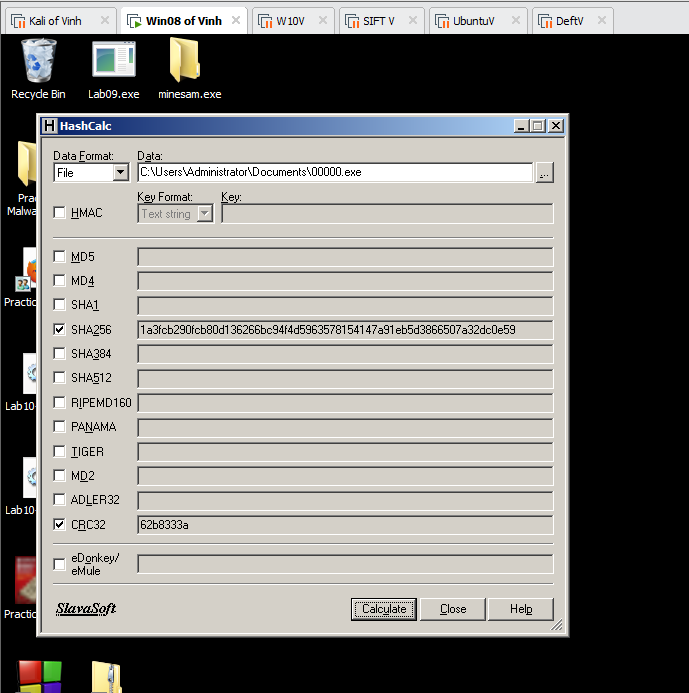
**What You Need**

* A Windows machine, real or virtual. I used a Windows Server 2008 virtual machine.
* You need several files to examine. They are all in the Documents folder of the VM your instructor handed out. If you don't have that, download them with these links:
* exe
* 3EXEs.zip
* easy.zip
* 256exes.zip

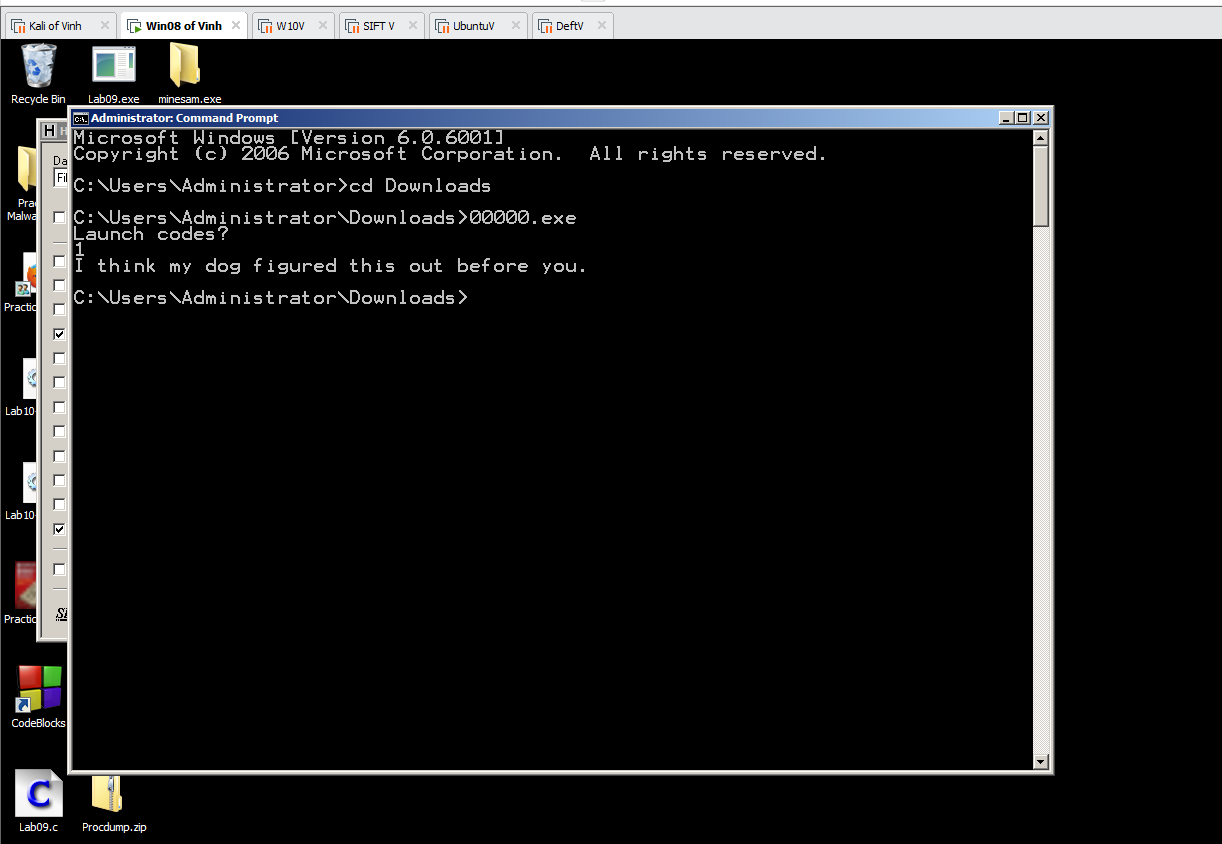
**9.1: Patching an EXE (15 pts)**

**Getting the EXE**

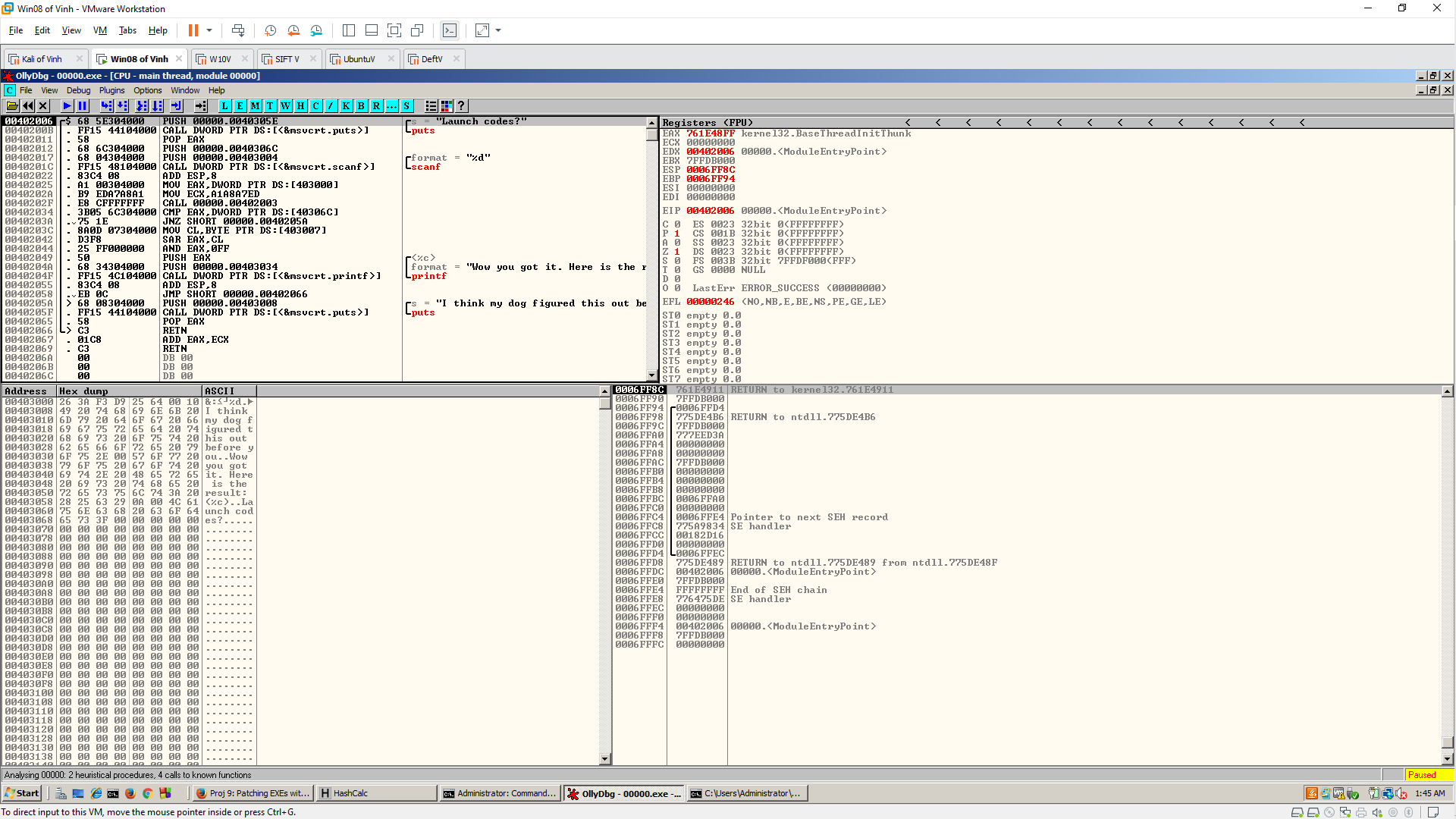
**Checking the Hash**

****

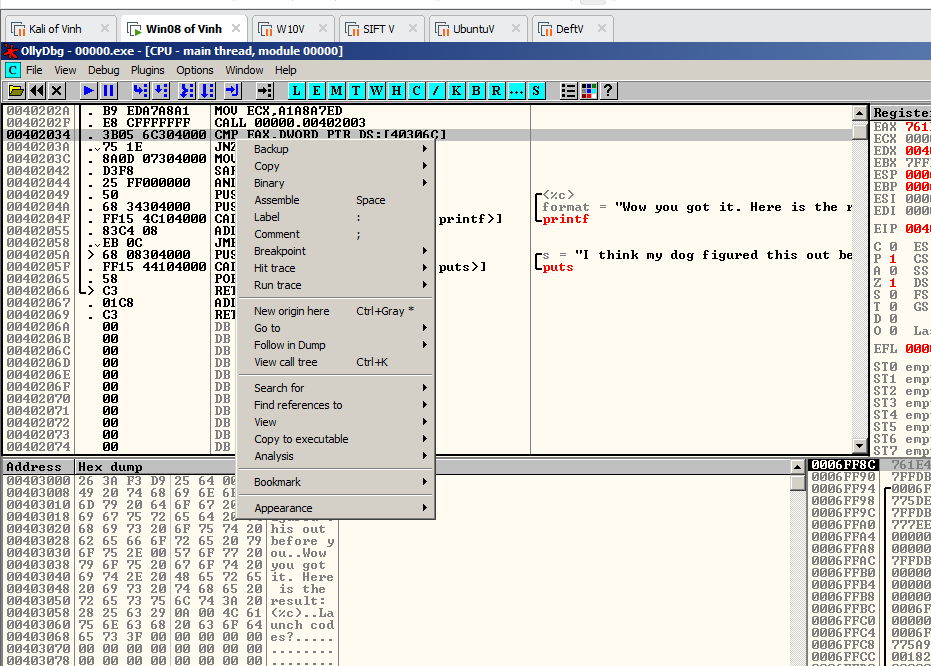
**Running the EXE**

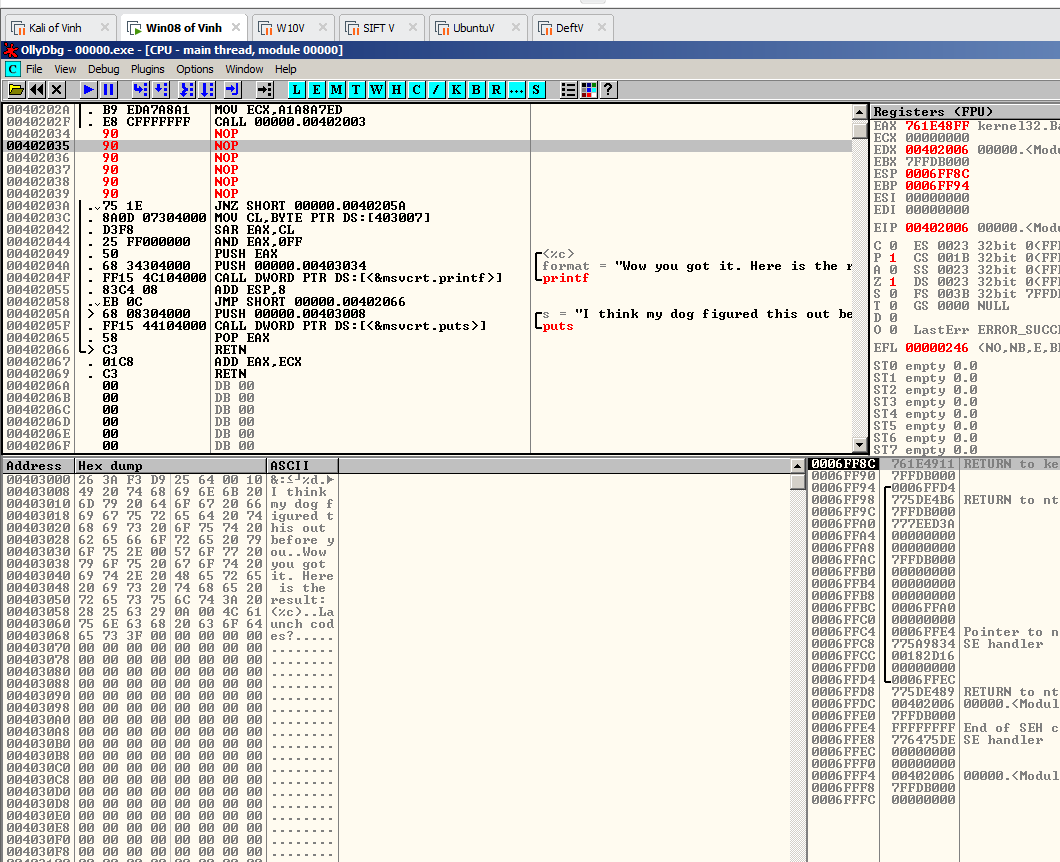
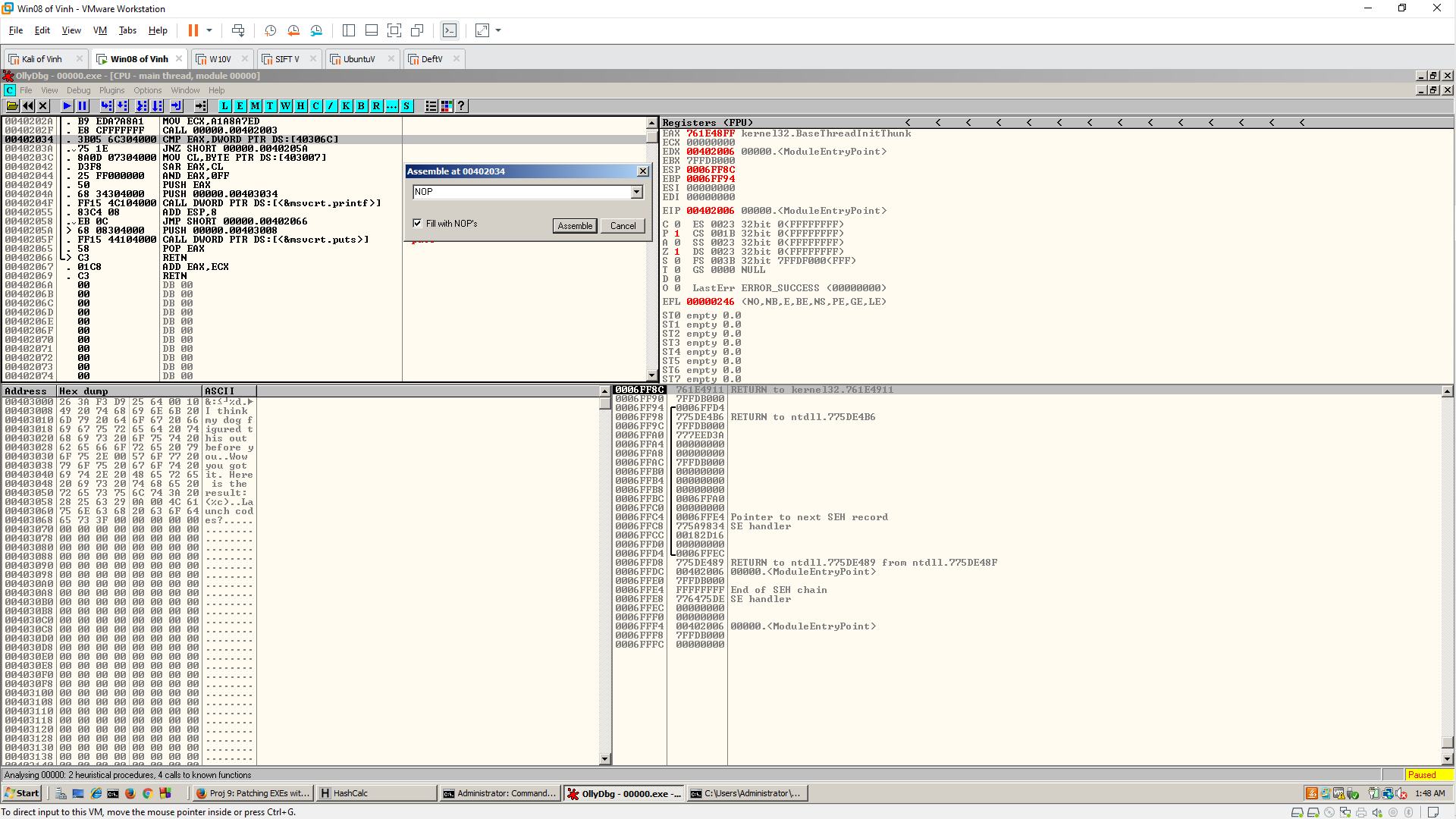
****

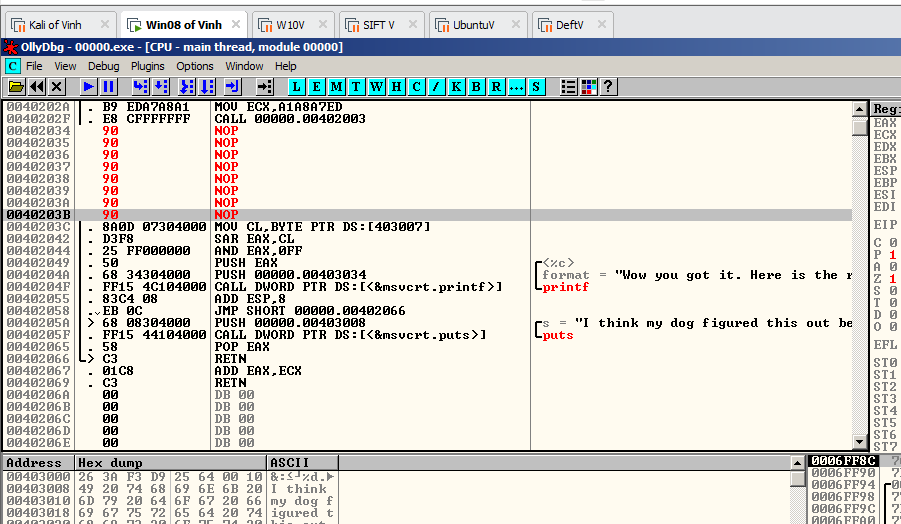
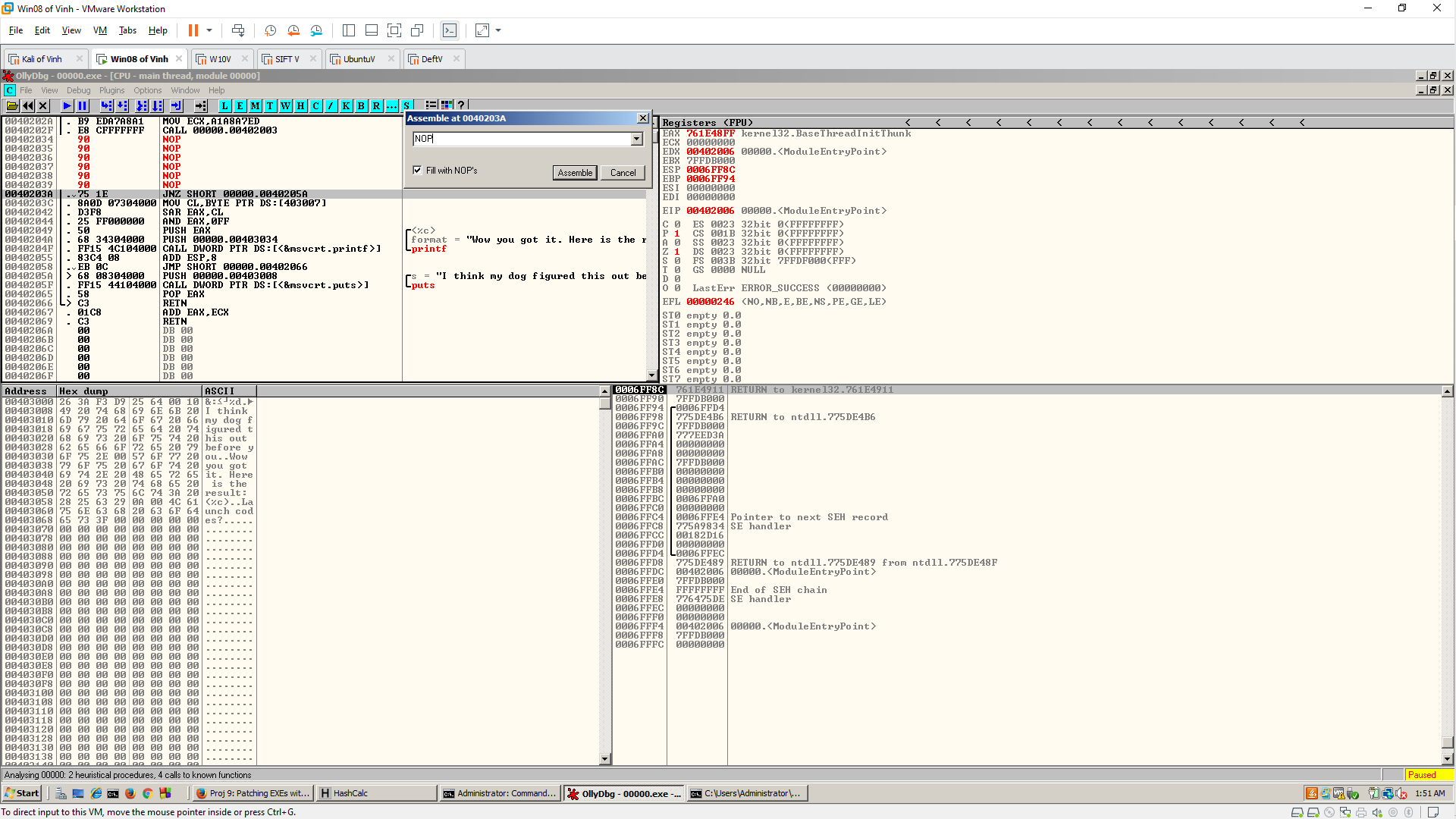
**Examining the EXE with Ollydbg**

****

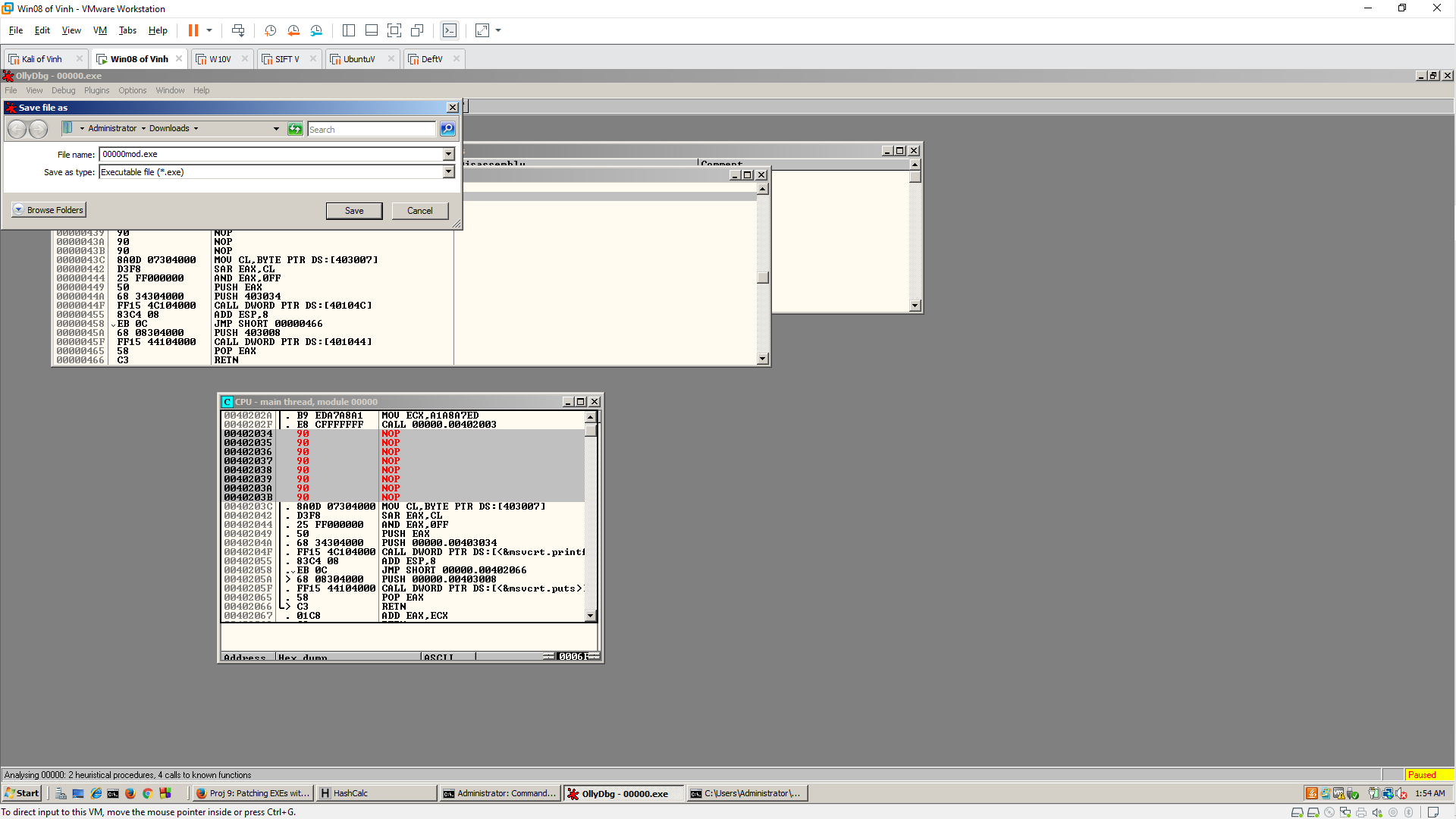
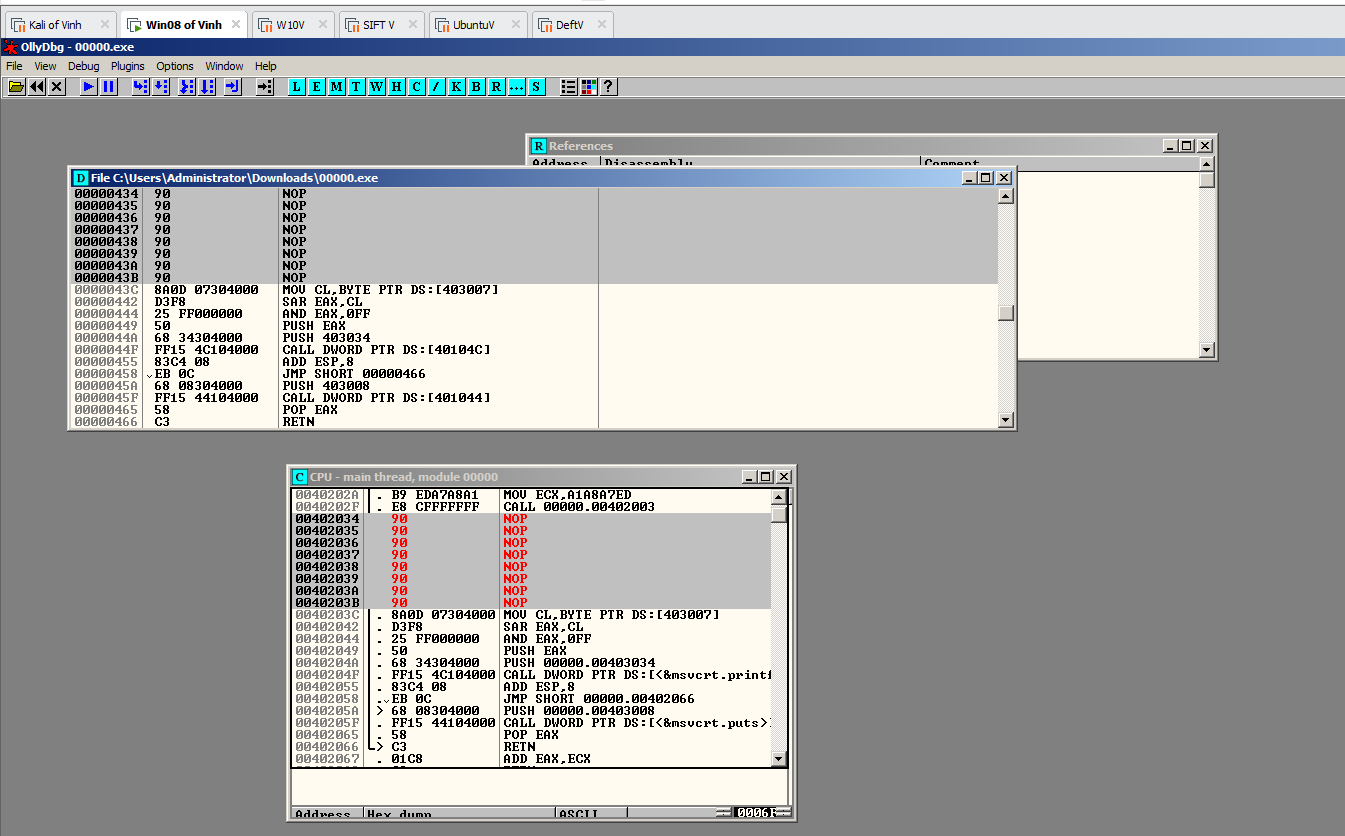
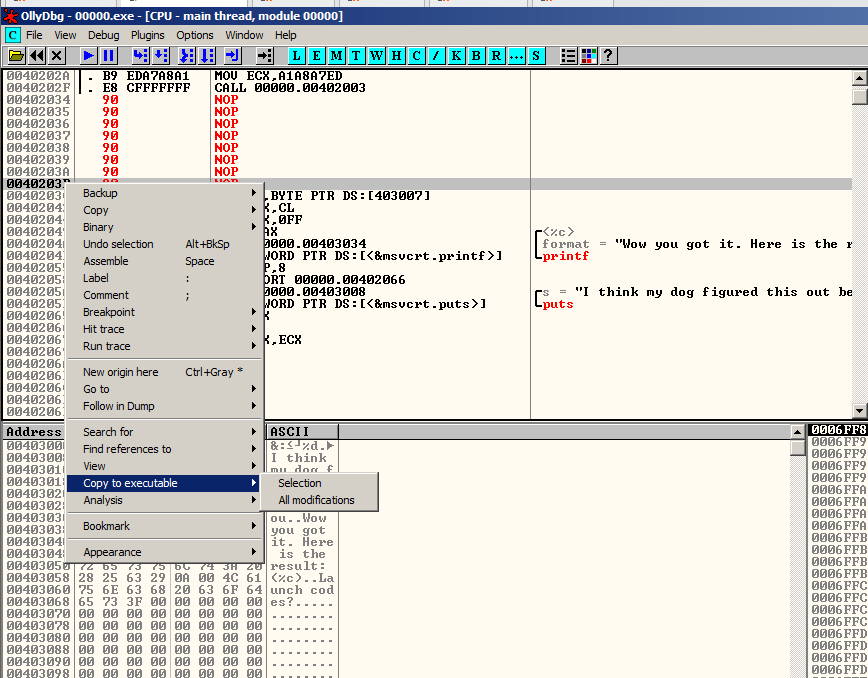
**Modifying the EXE**

****

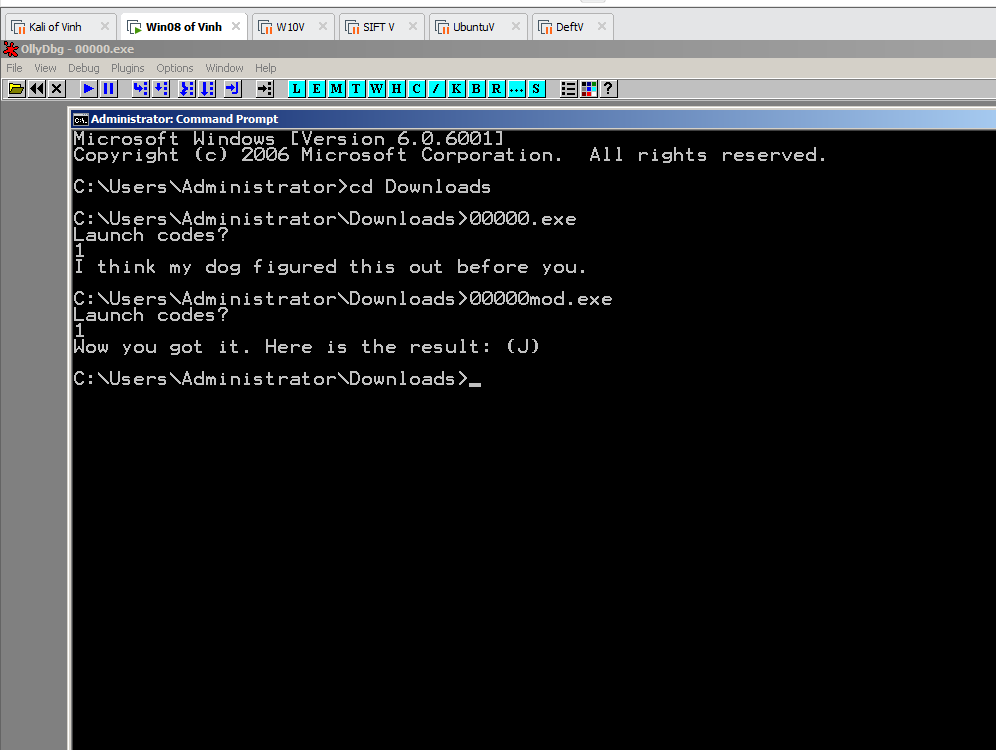
****

****

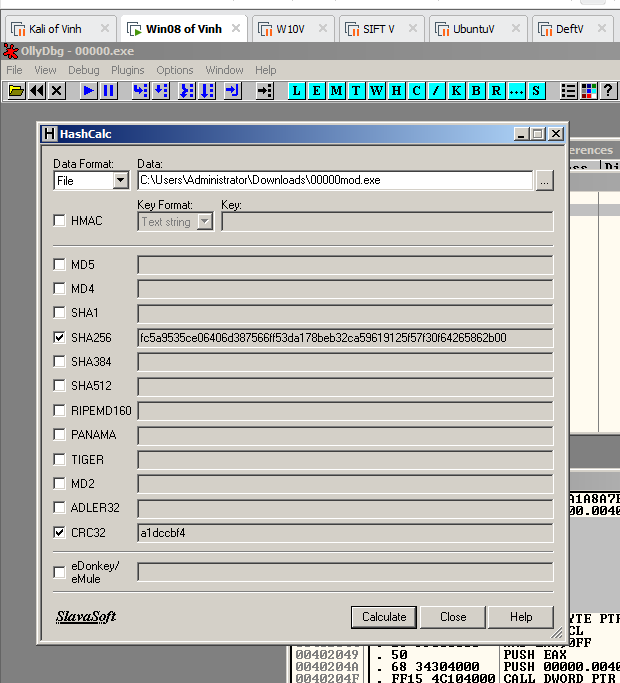
**Saving the Modified File**

****

**Running the Modified File**

****

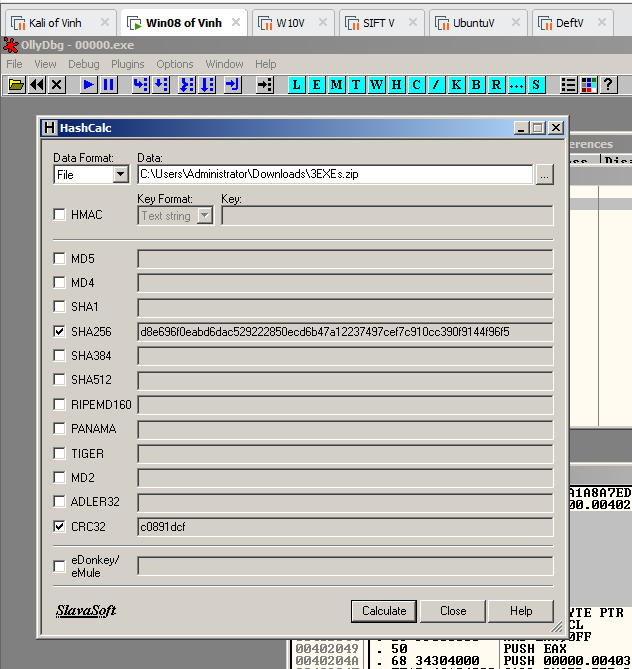
**Checking the Hash**

****

**9.2: Patching Three EXEs**

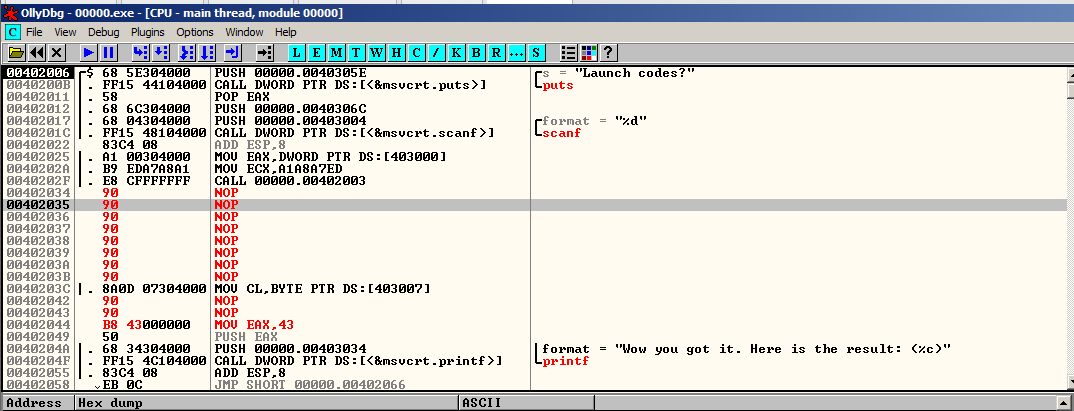
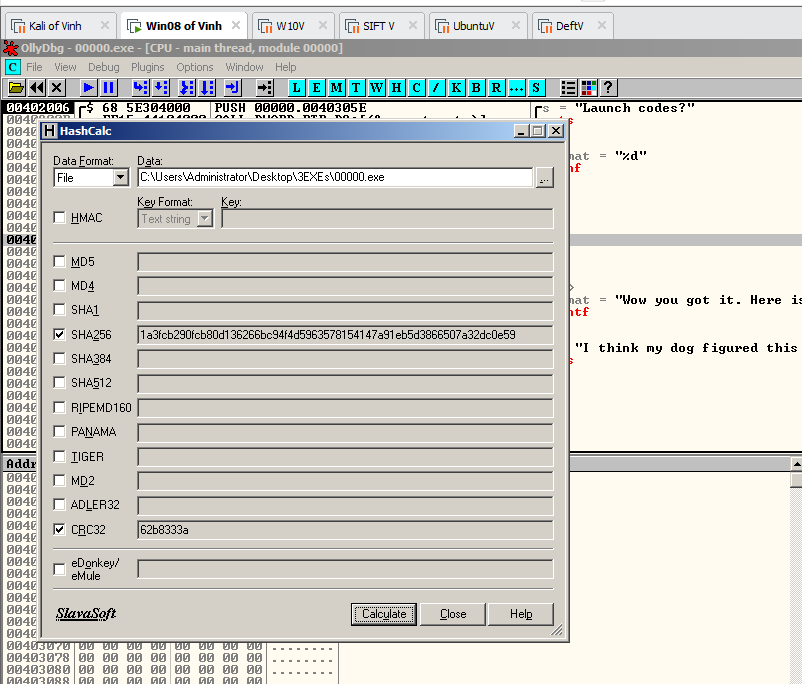
**Getting the EXEs**

**Checking the Hash**

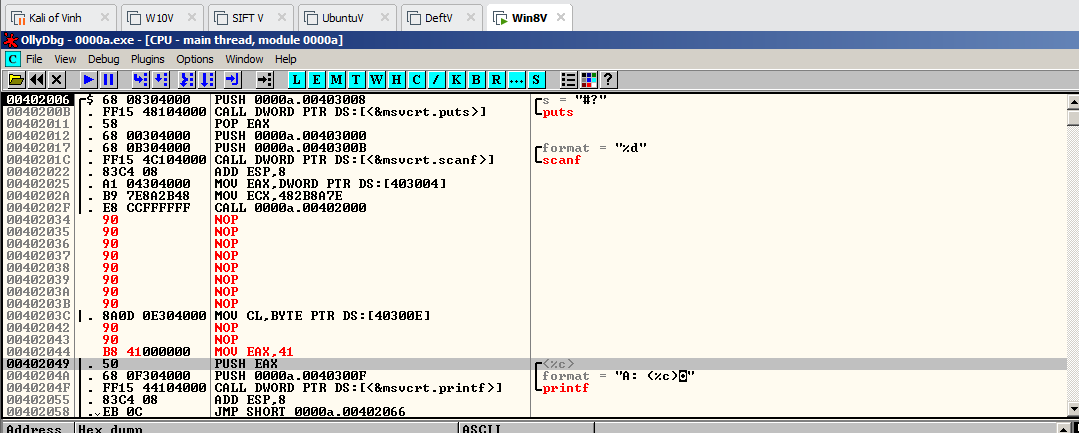
****

**Patch the Files**

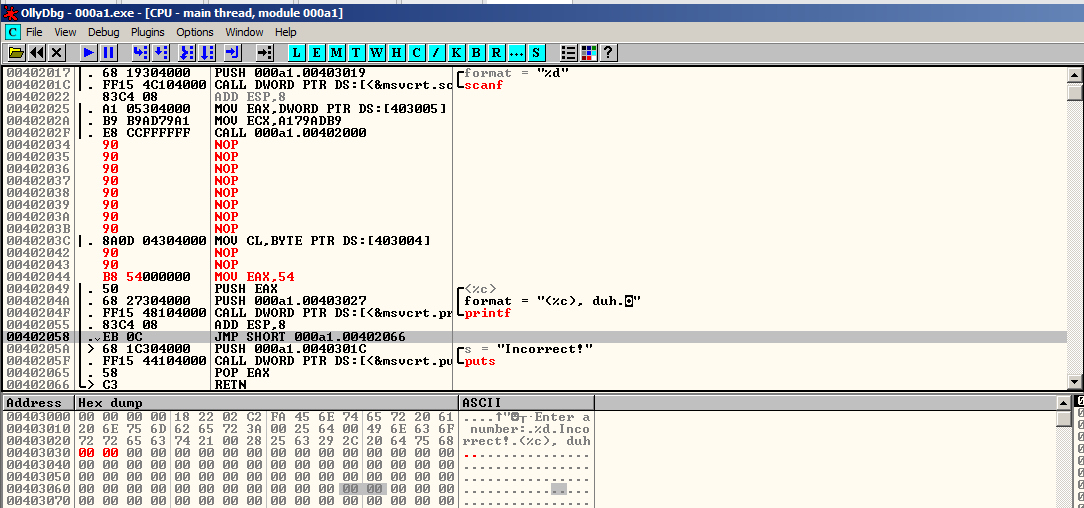
**00000.exe**

****

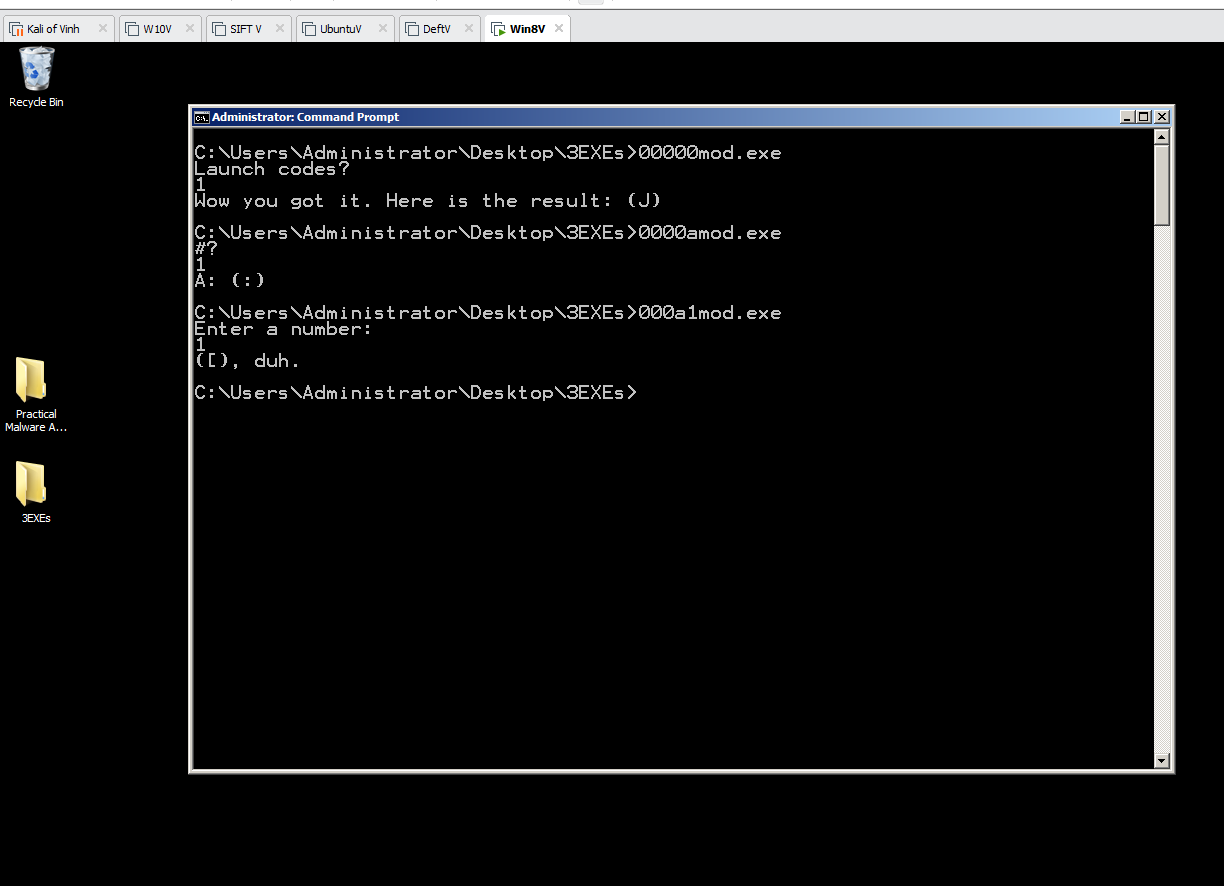
**0000a.exe**

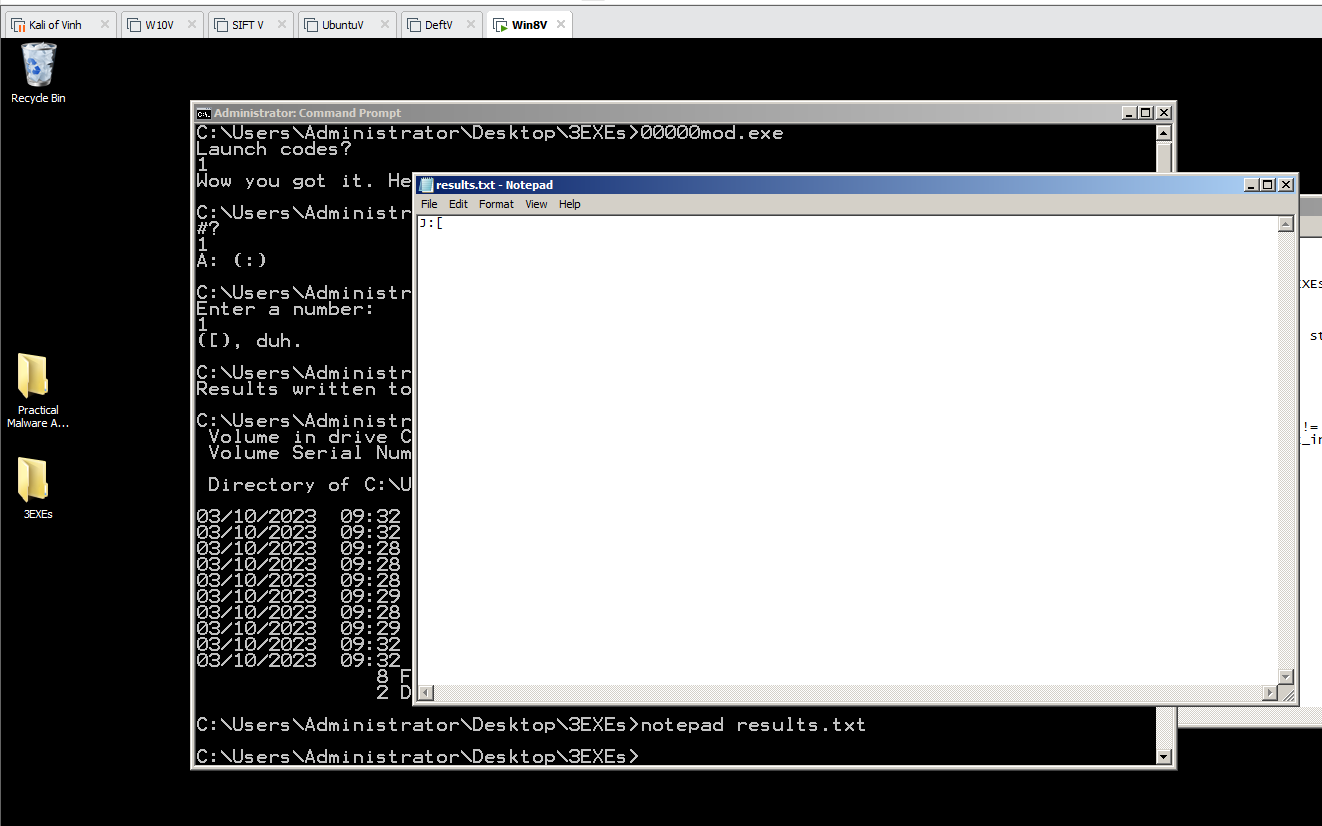
****

**000a1.exe**

****

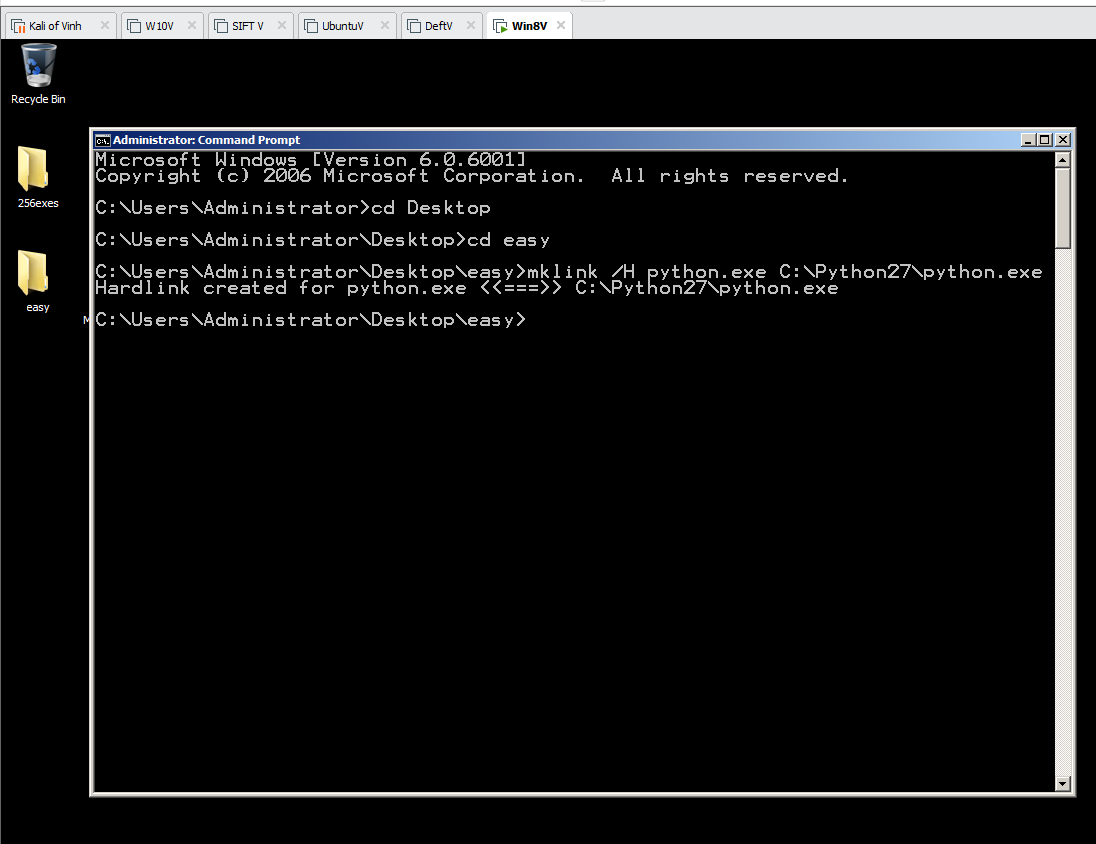
**Run file**

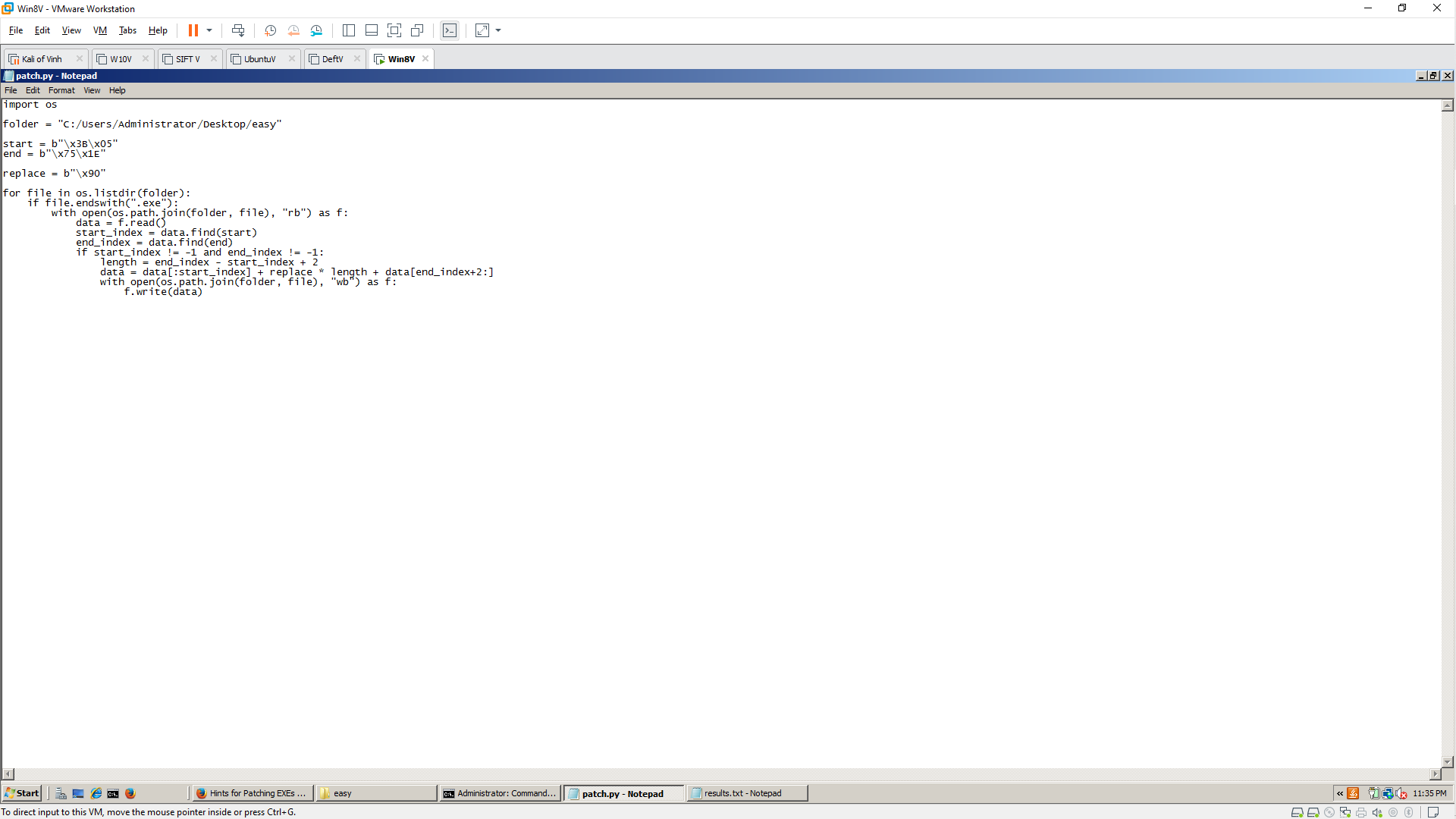
****

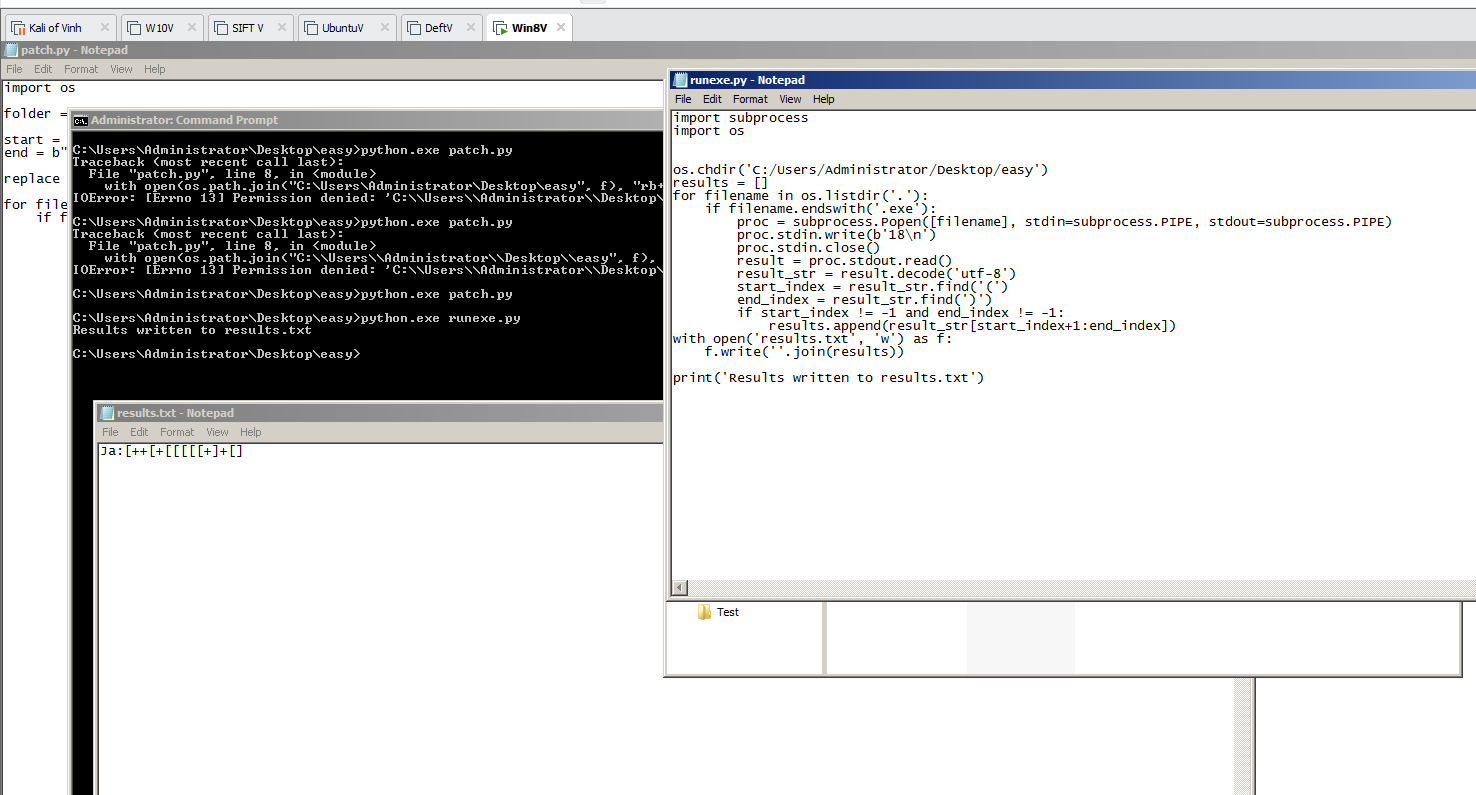
****

**9.3: Patching 19 EXEs**

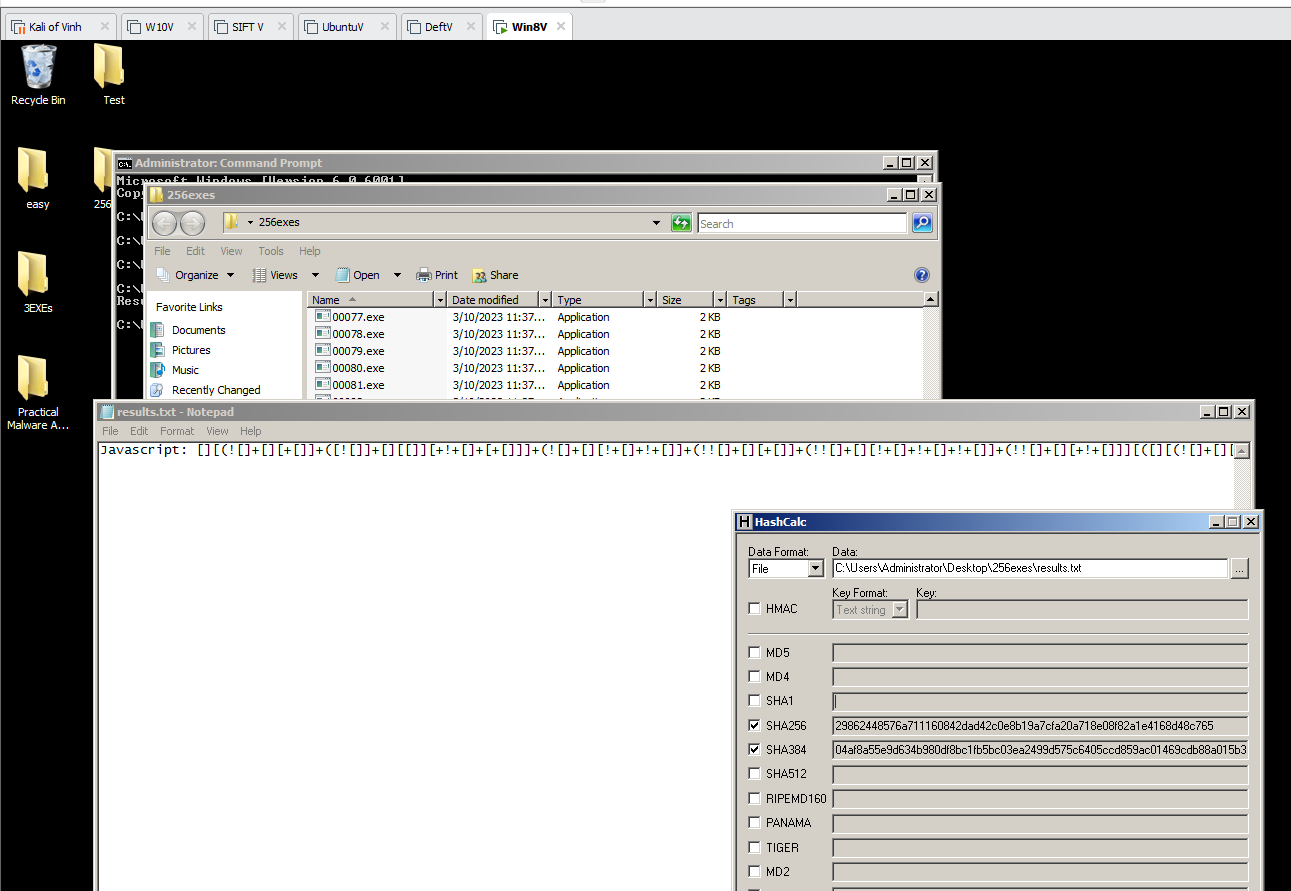
**Making Python Run on Windows**

****

****

****

**256exes**

****