9.1: Patching an EXE

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

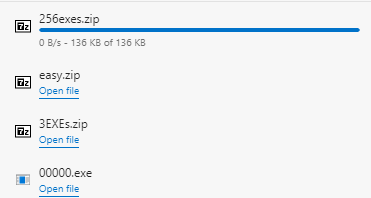
that, download them with these links:

00000.exe

3EXEs.zip

easy.zip

256exes.zip



Getting the EXE

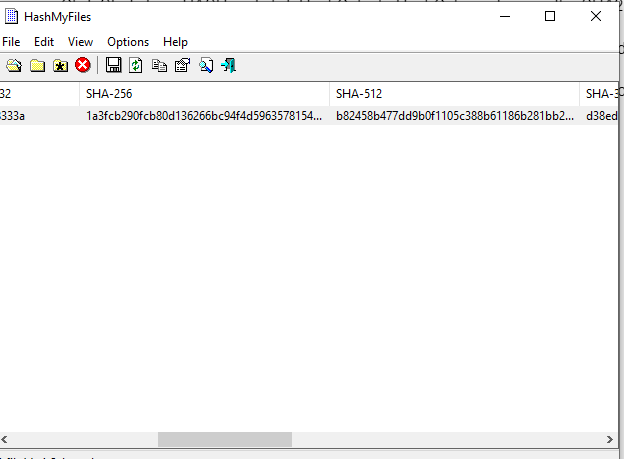
In the Documents folder of the VM handed out by your instructor, find the 00000.exe file.

Checking the Hash

Click Start. Type HASH and click HashCalc. In HashCalc, make sure the SHA256 box is checked, as shown below.

Click Start, Documents. Drag the 00000.exe file from the Documents folder and drop it onto the HashCalc box.

HashCalc calculates the SHA256 hash of the file. It should match the value shown below.



Running the EXE

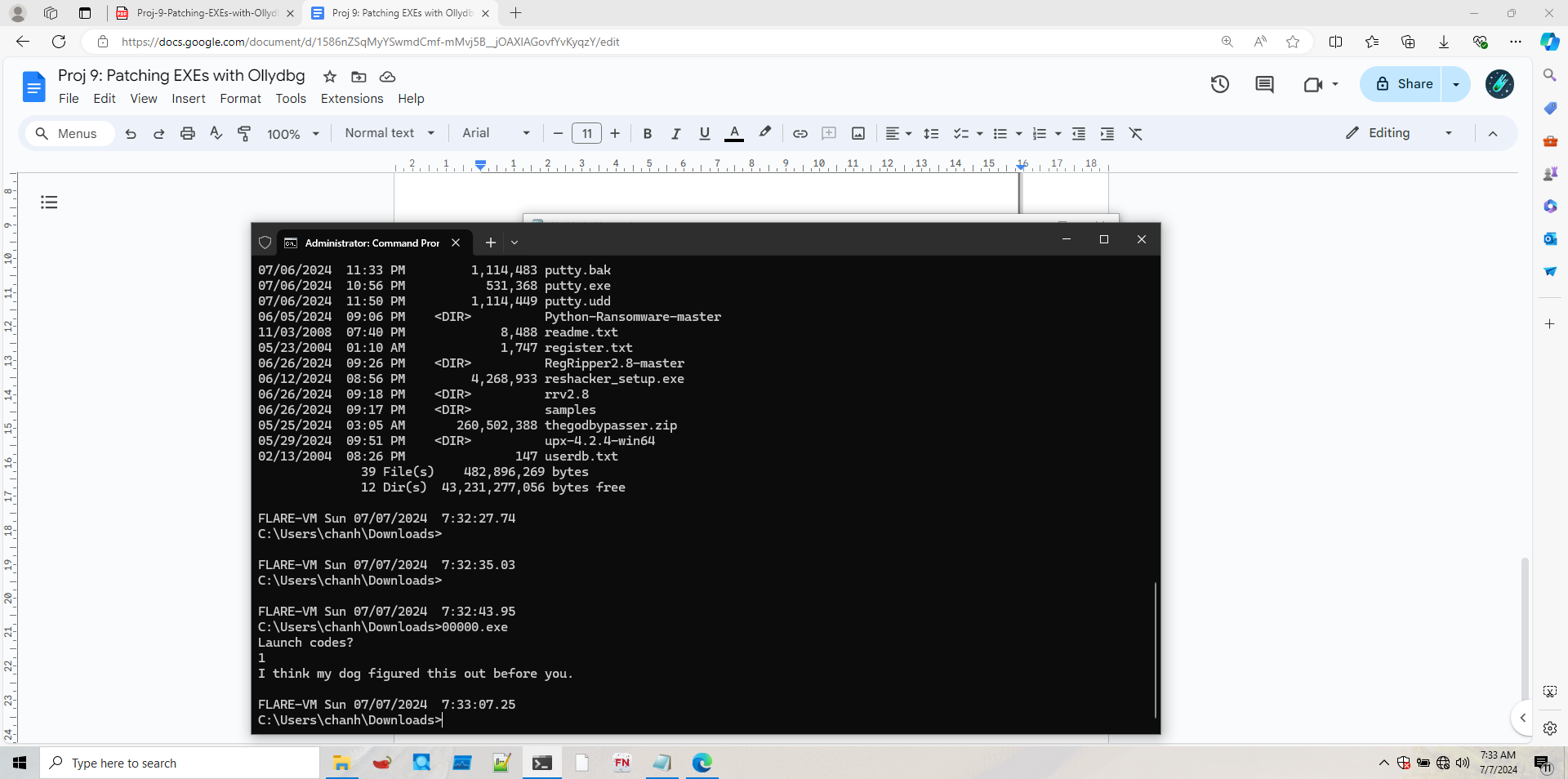
Click the black square icon at the lower left of your desktop to open a Command Prompt.

Execute these commands:

cd \users\administrator\documents

00000.exe

It asks for a "Launch code". Enter 1. Your code is wrong, and it insults you, as shown below



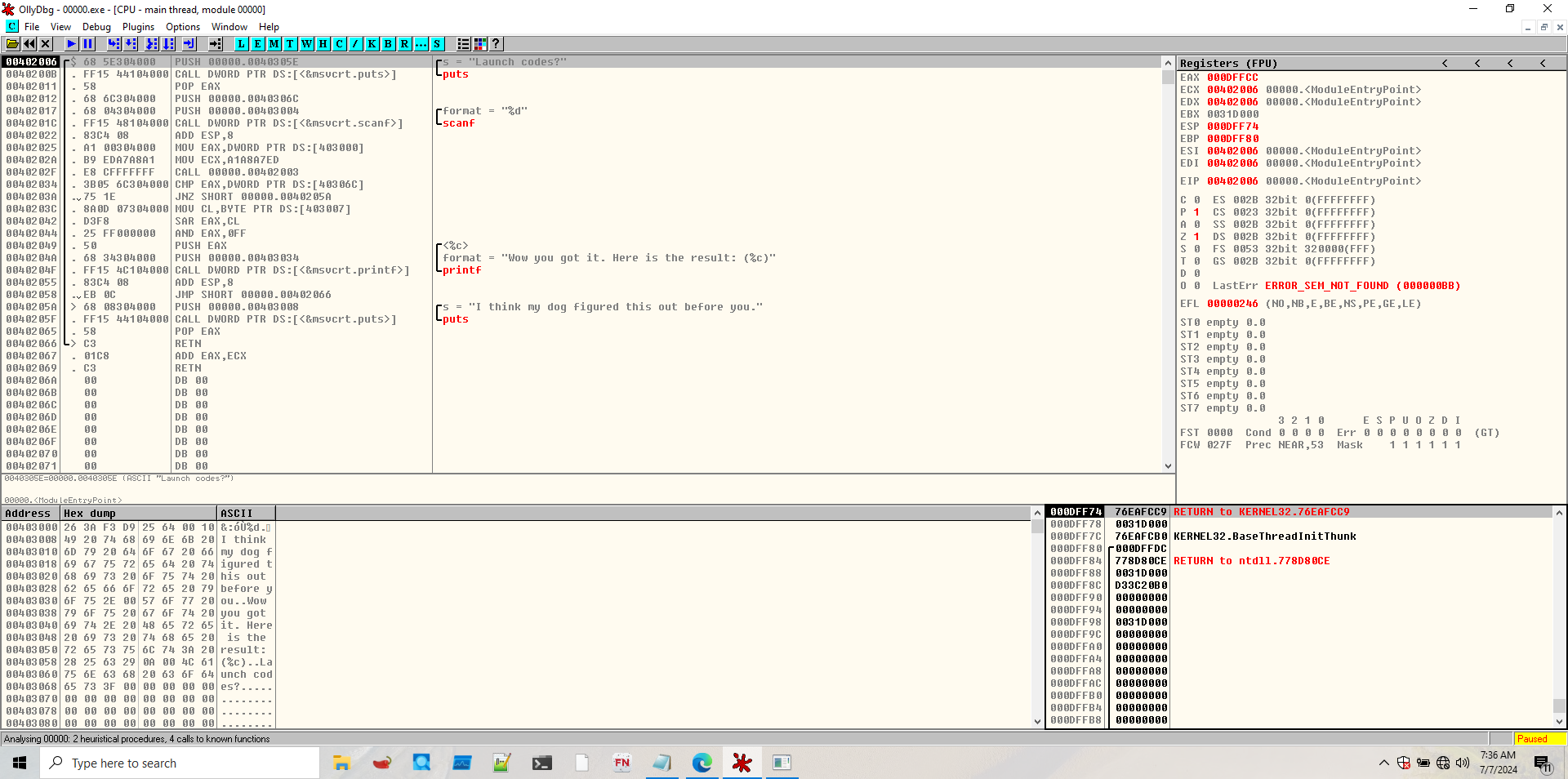
Examining the EXE with Ollydbg

Open the file in OllyDbg, as shown below.

Look at the rightmost section, and you can easily see what the program does; it prints out "Launch codes?", reads in a decimal

number (%d), and then chooses to print either a winning message with a result, or an insult.

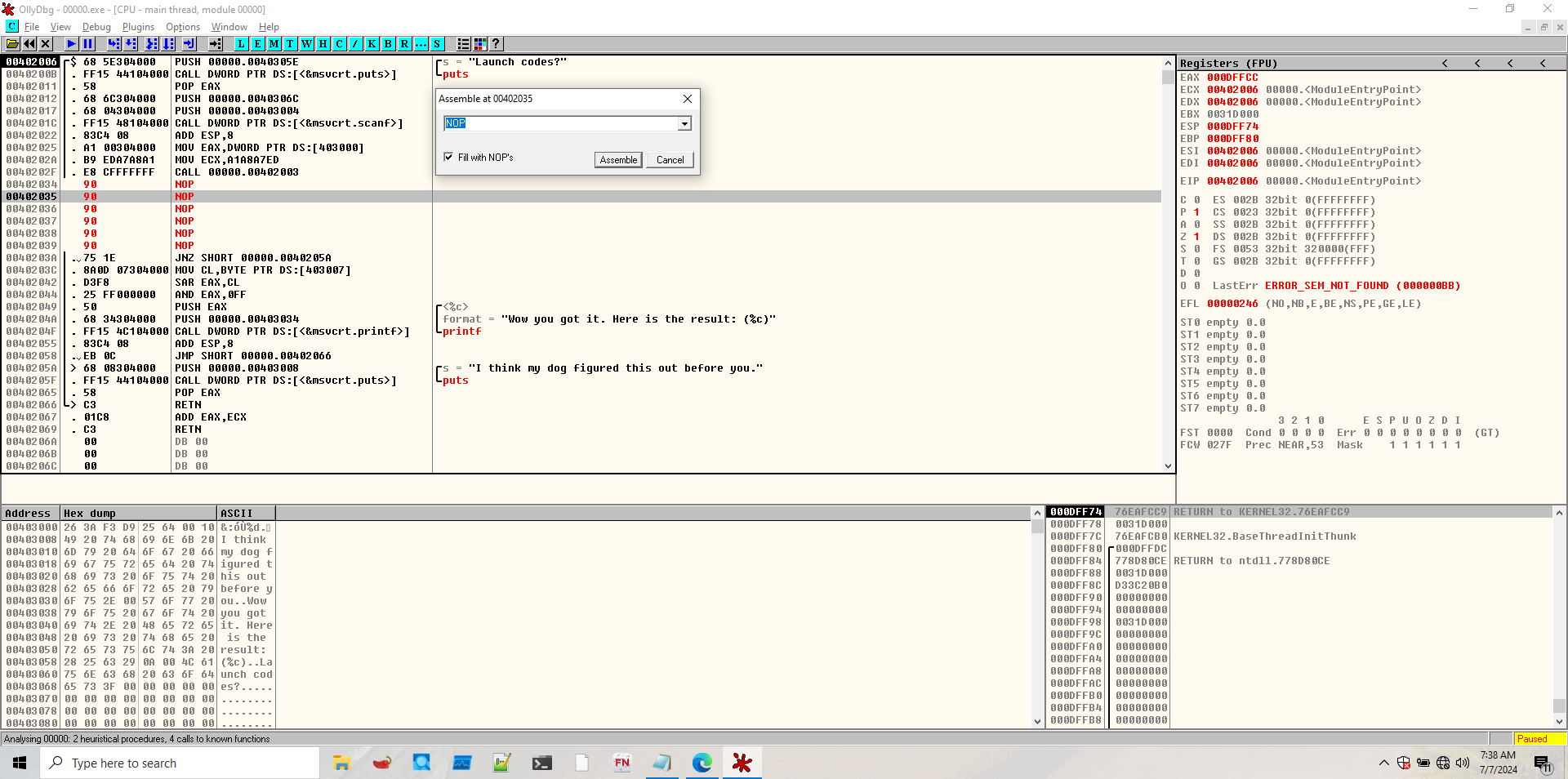
The choice is performed by two instructions: CMP (Compare) and JNZ (Jump if Not Zero), outlined in green in the image below.



Modifying the EXE

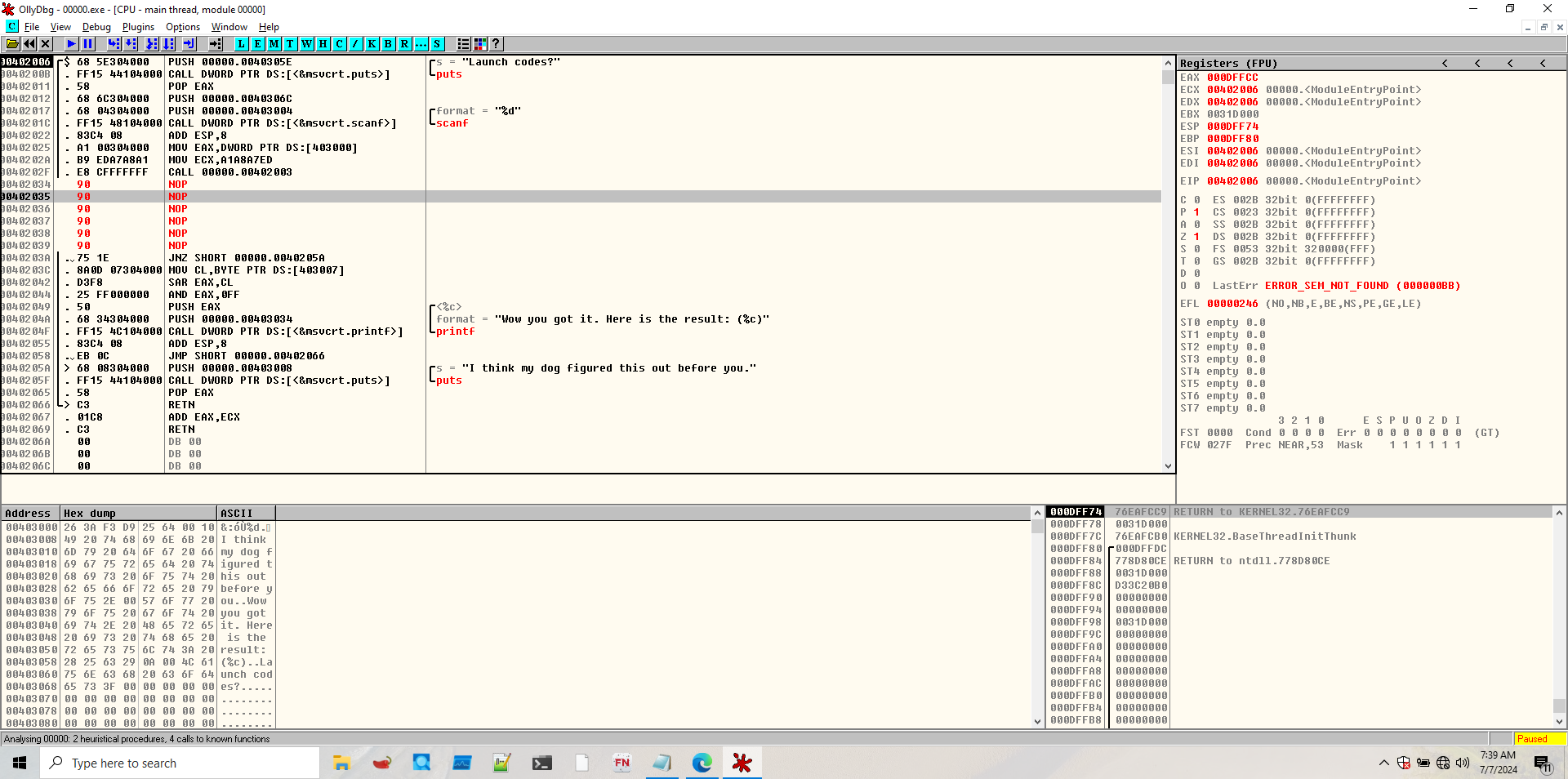
Right-click the CMP instruction and click Assemble, as shown below

In the Assemble box, enter NOP

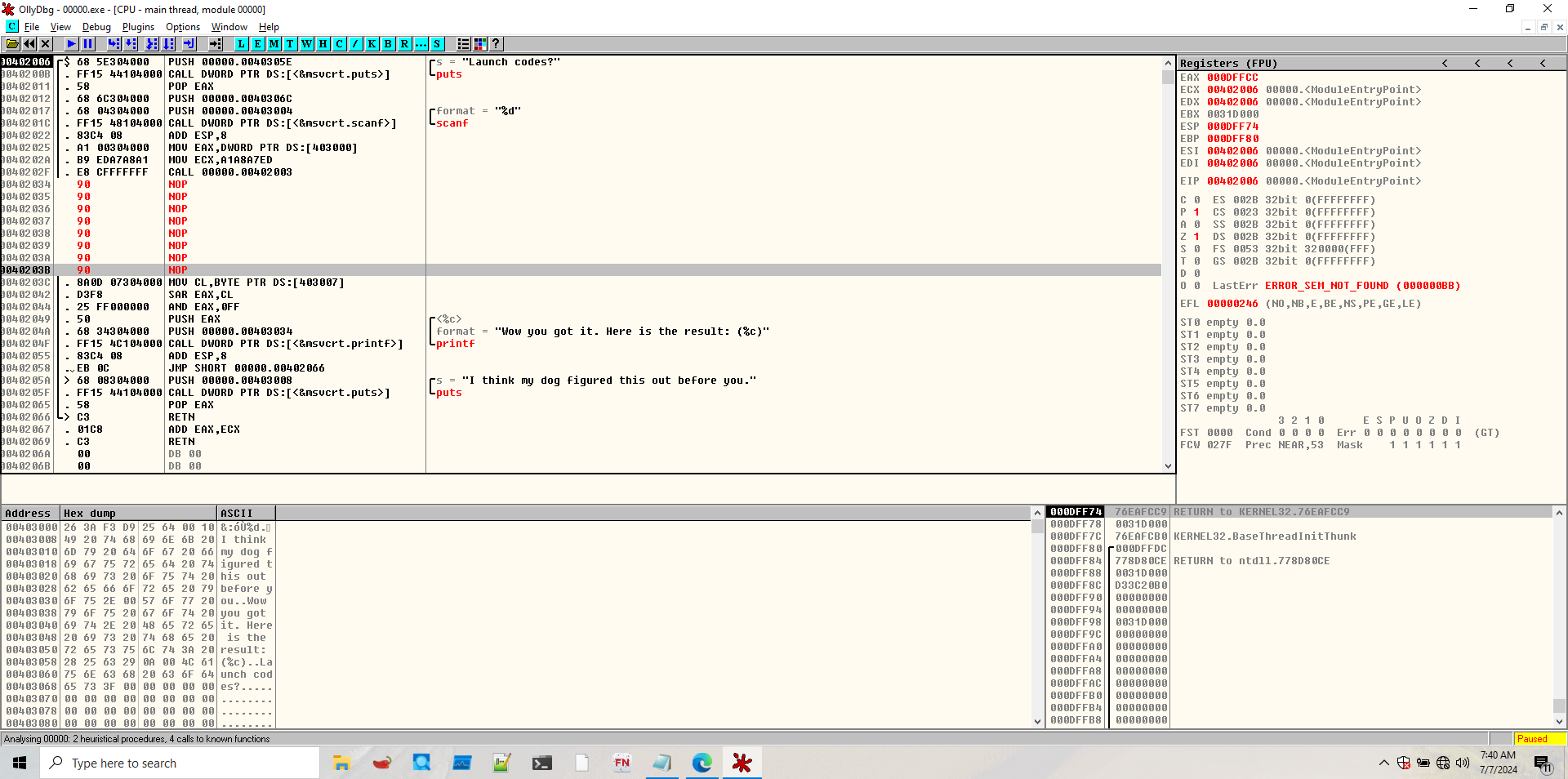


Click the Assemble button. Click the Cancel button

The CMP instruction is replaced by a series of NOPs, as shown below

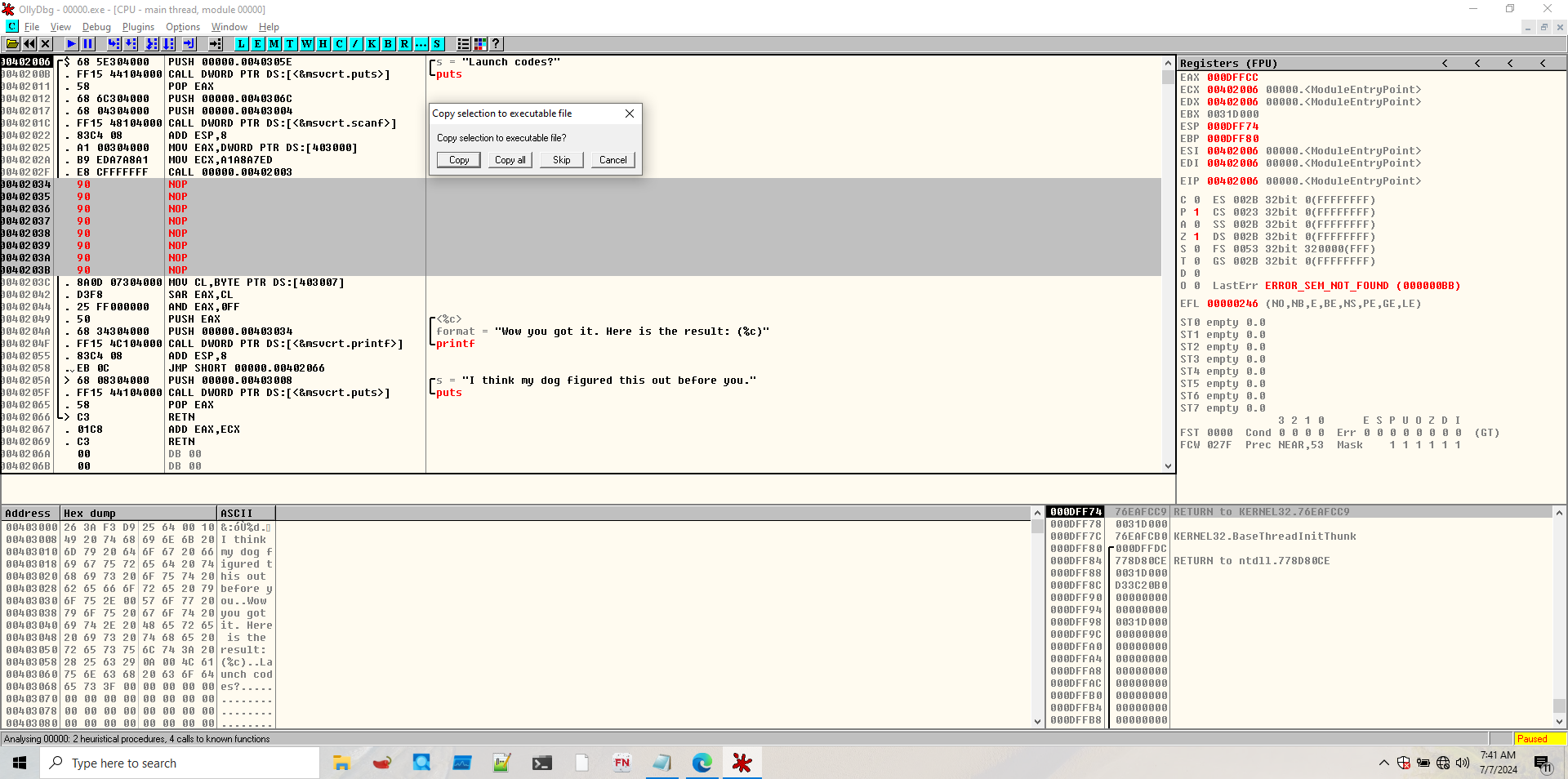


Repeat the process to replace the JNZ instruction with NOPs also, as shown below



Saving the Modified File

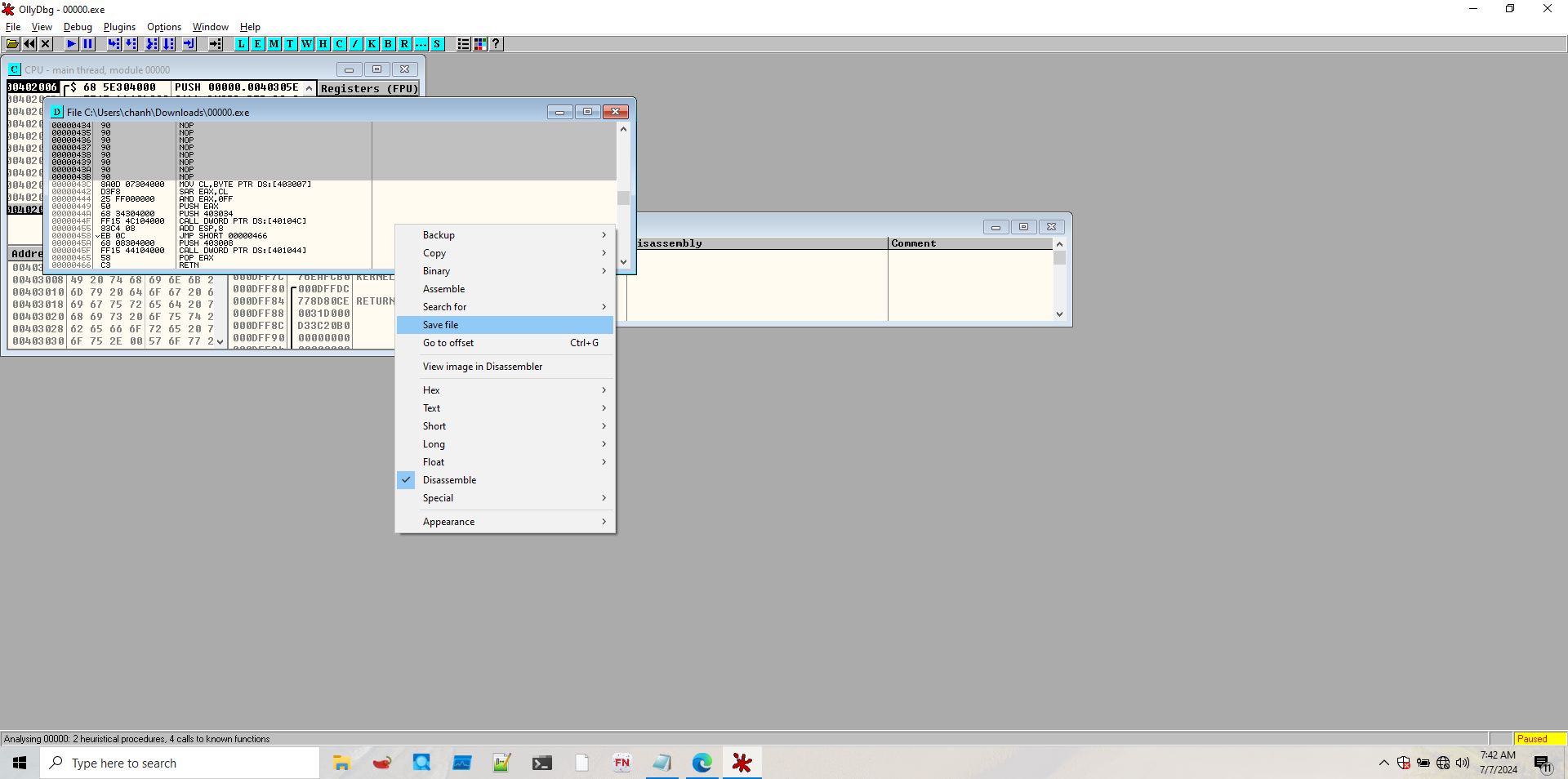
In OllyDbg, in the top left pane, right-click and click "Copy to executable", "All modifications", as shown below



A "Copy selection to executable file?" box pops up. Click the "Copy all" button.

A "File" box appears, as shown below.

Right-click in it and click "Save file".



A "Save file as" box appears. Change the filename to 00000mod.exe, as shown below, and click Save.



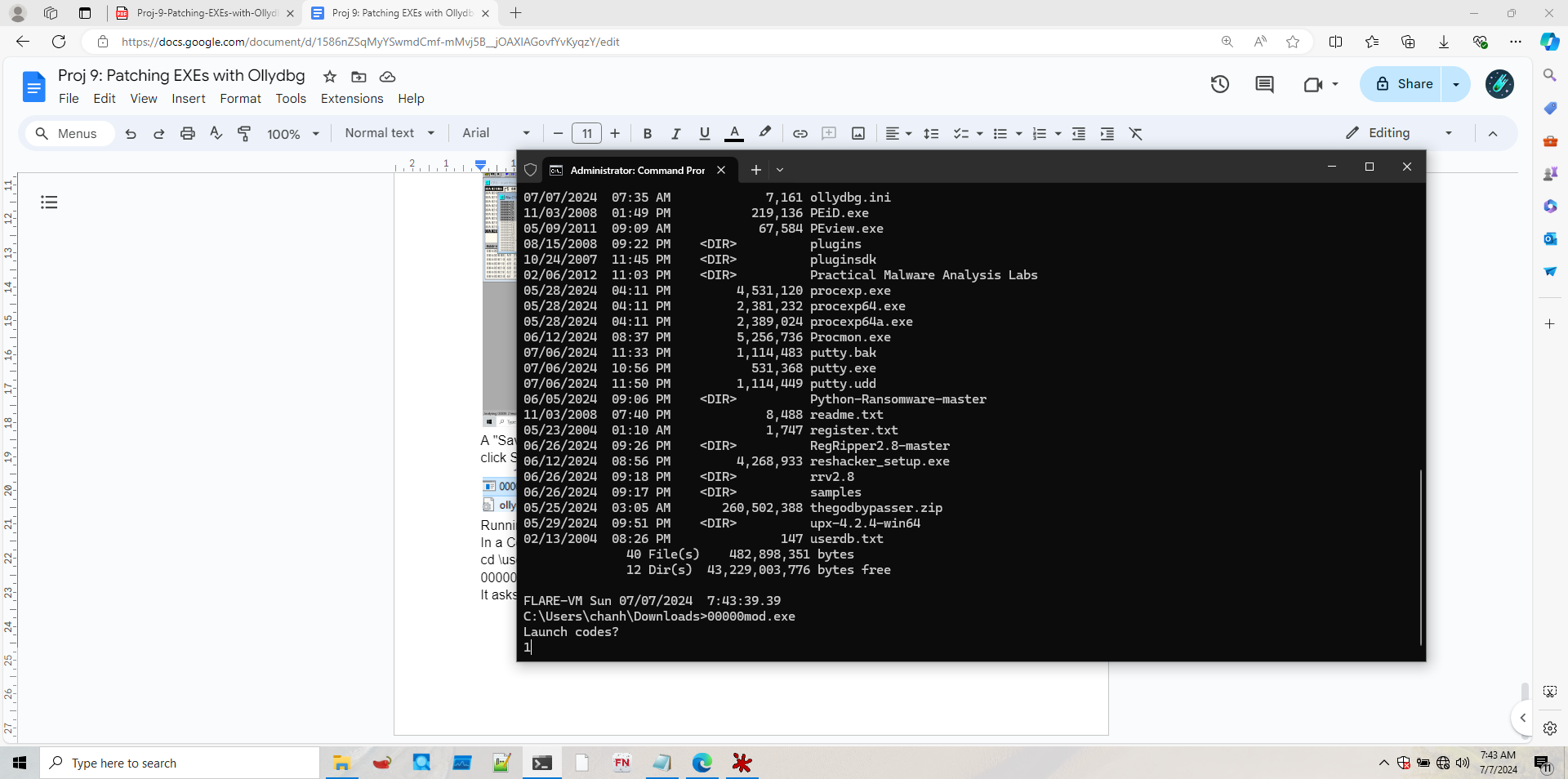
Running the Modified File

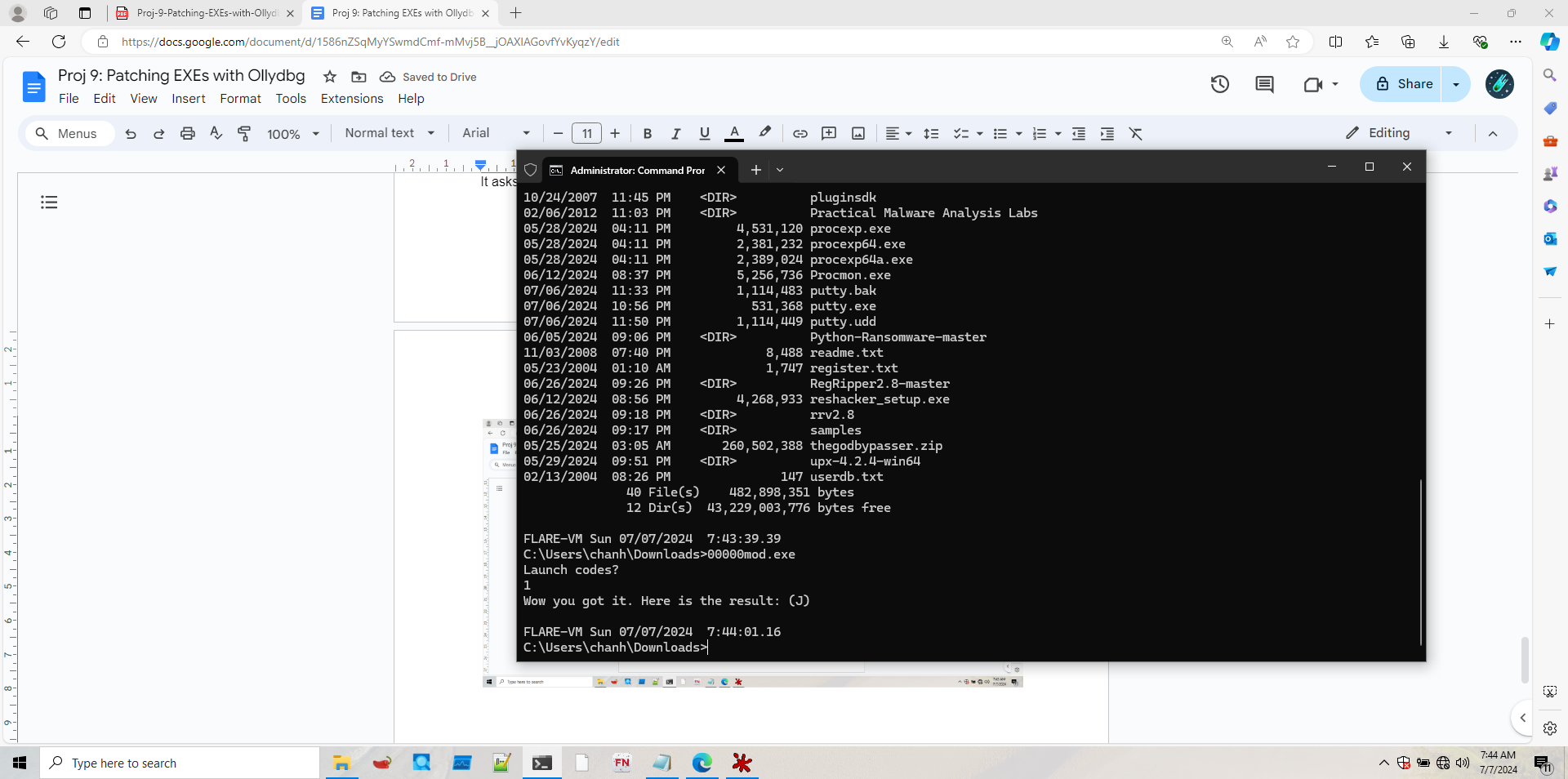
In a Command Prompt window, execute these commands:

cd \users\administrator\documents

00000mod.exe

It asks for a "Launch code". Enter 1. It accepts the code now, as shown below





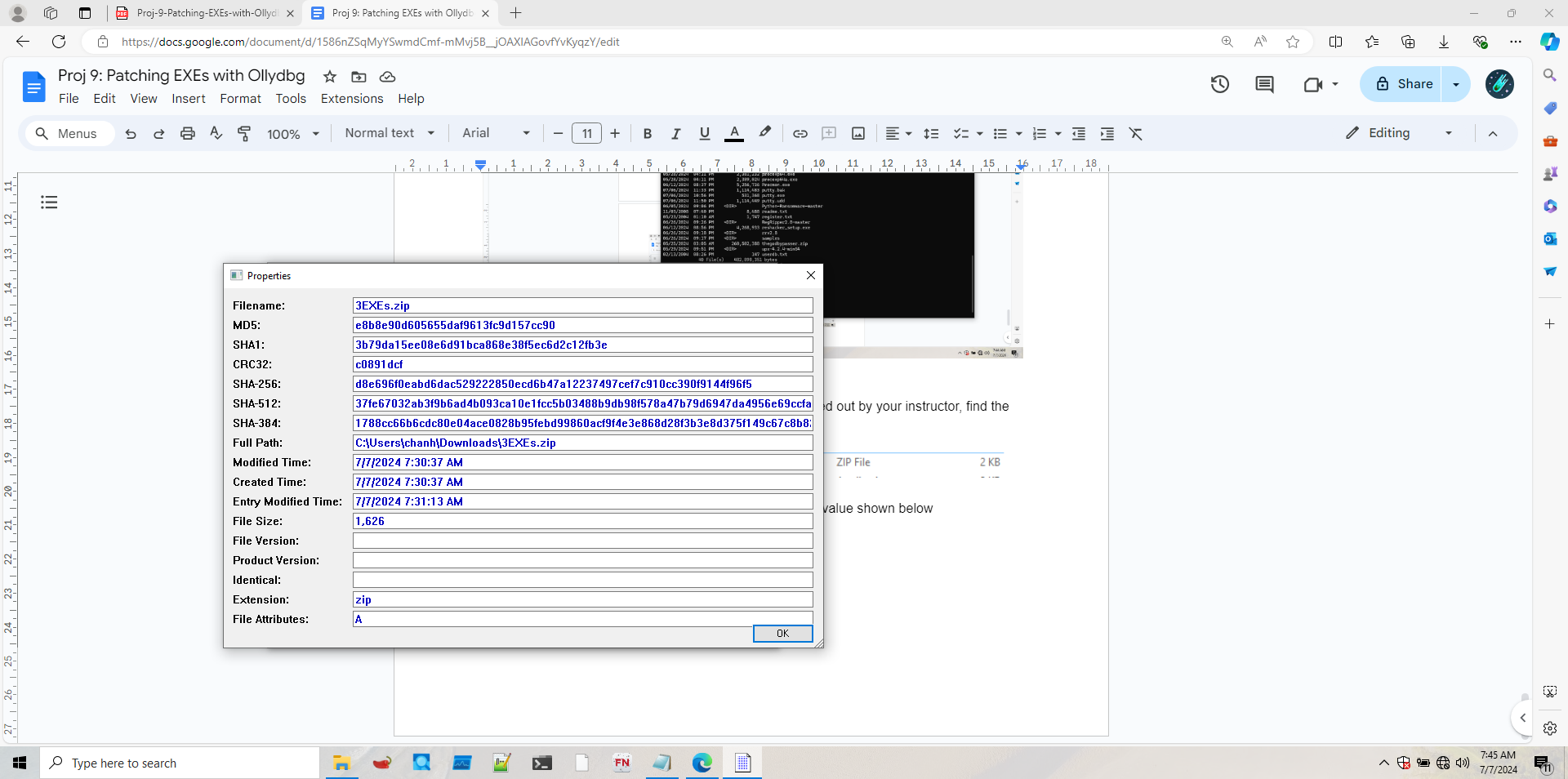
9.2: Patching Three EXEs

Getting the EXEs In the Documents folder of the VM handed out by your instructor, find the 3EXEs.zip file.



Checking the Hash

Calculate the SHA256 hash of the file. It should match the value shown below



Patch the Files

Patch all 3 files so they will accept any input.

Gather the Results

Run the three patched files. Each one returns a single character as a result. Keep the files in alphabetical order, by filename, like this:

File 00000.exe Result C

File 0000a.exe Result A

File 000a1.exe Result T

If those were the results, the answer would be CAT

The actual results are different, of course.

