

11: Using OllyDbg to Analyze Lab09-01.exe (Part 1) (15 pts.)

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.

Summary

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

Get OllyDbg 1.10 here:

<http://www.ollydbg.de/download.htm>

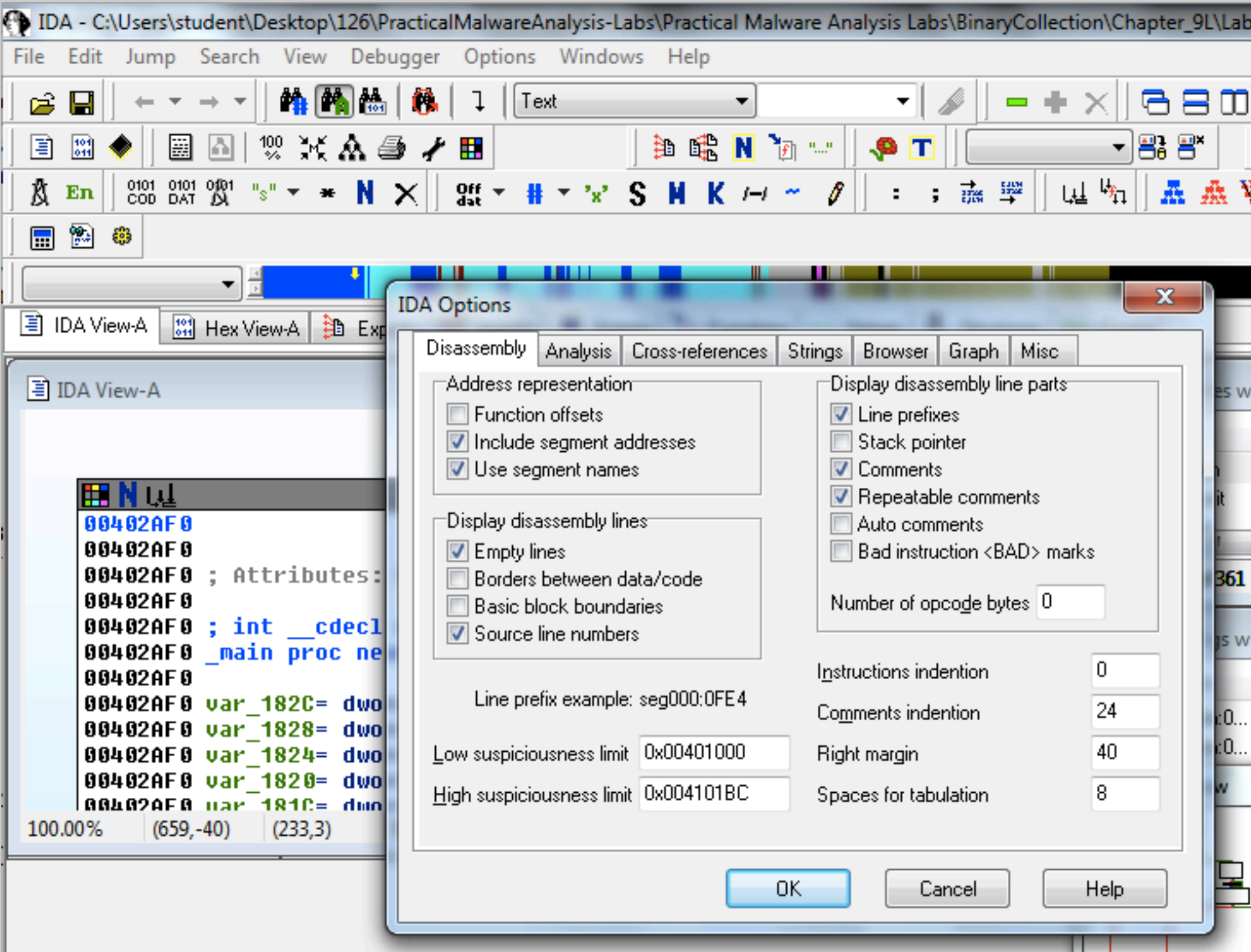
Don't waste your time on OllyDbg 2.00 or 2.01. They are both broken.

Finding the Main Entry Point

Open the Lab09-01.exe file in IDA Pro.

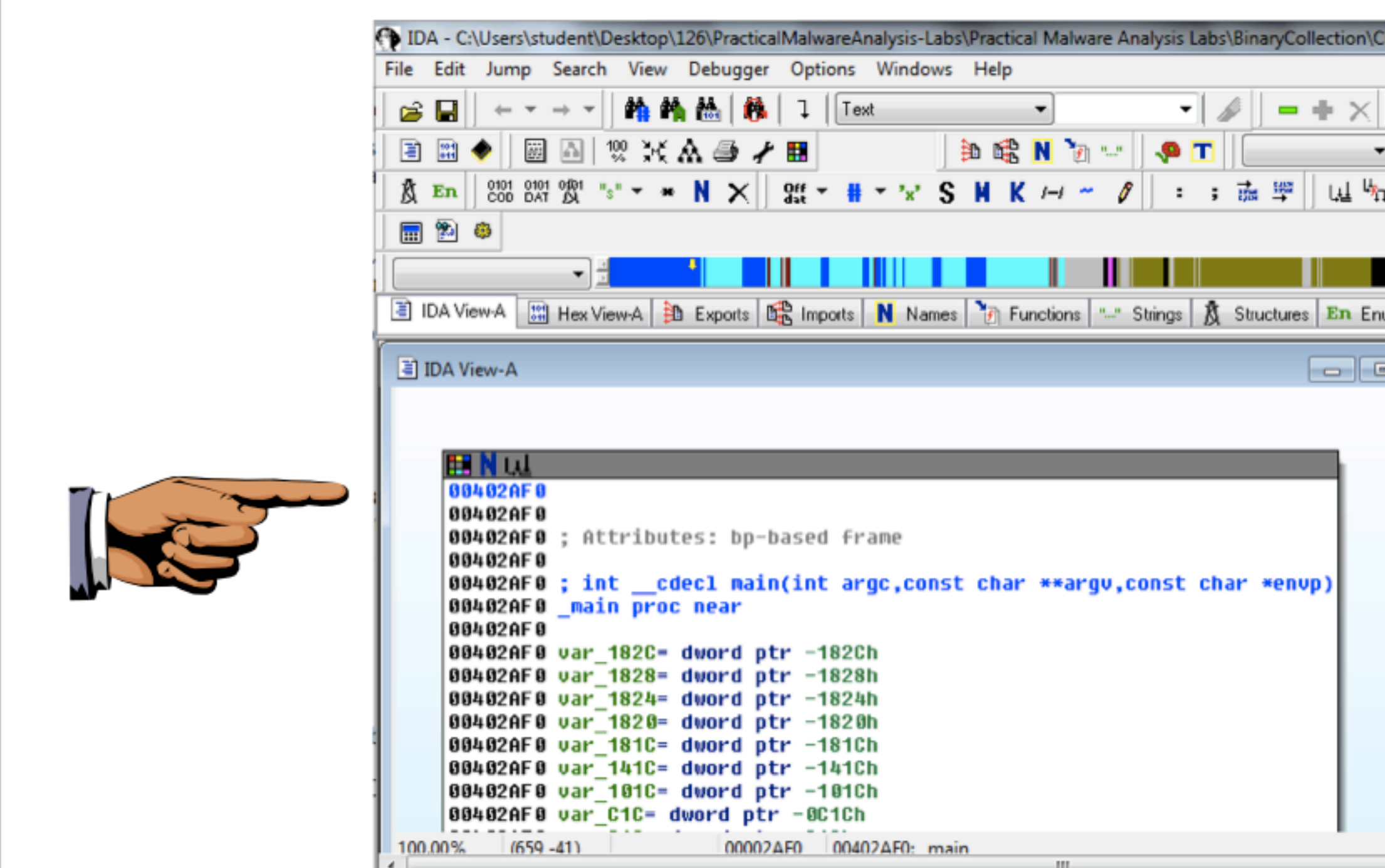
Click **Options, General**. Check "**Line Prefixes**", as shown below.

Click **OK**.



Click **Windows, "Reset Desktop"**.

IDA Pro shows that main starts at 0x402AF0, as shown below:



Saving the Screen Image

Make sure you can see the **0x402AF0** address, as shown above.

On your keyboard, press the PrntScrn key.

Click **Start**, type in **PAINT**, and open Paint.

Press **Ctrl+V** to paste in the image of your desktop.

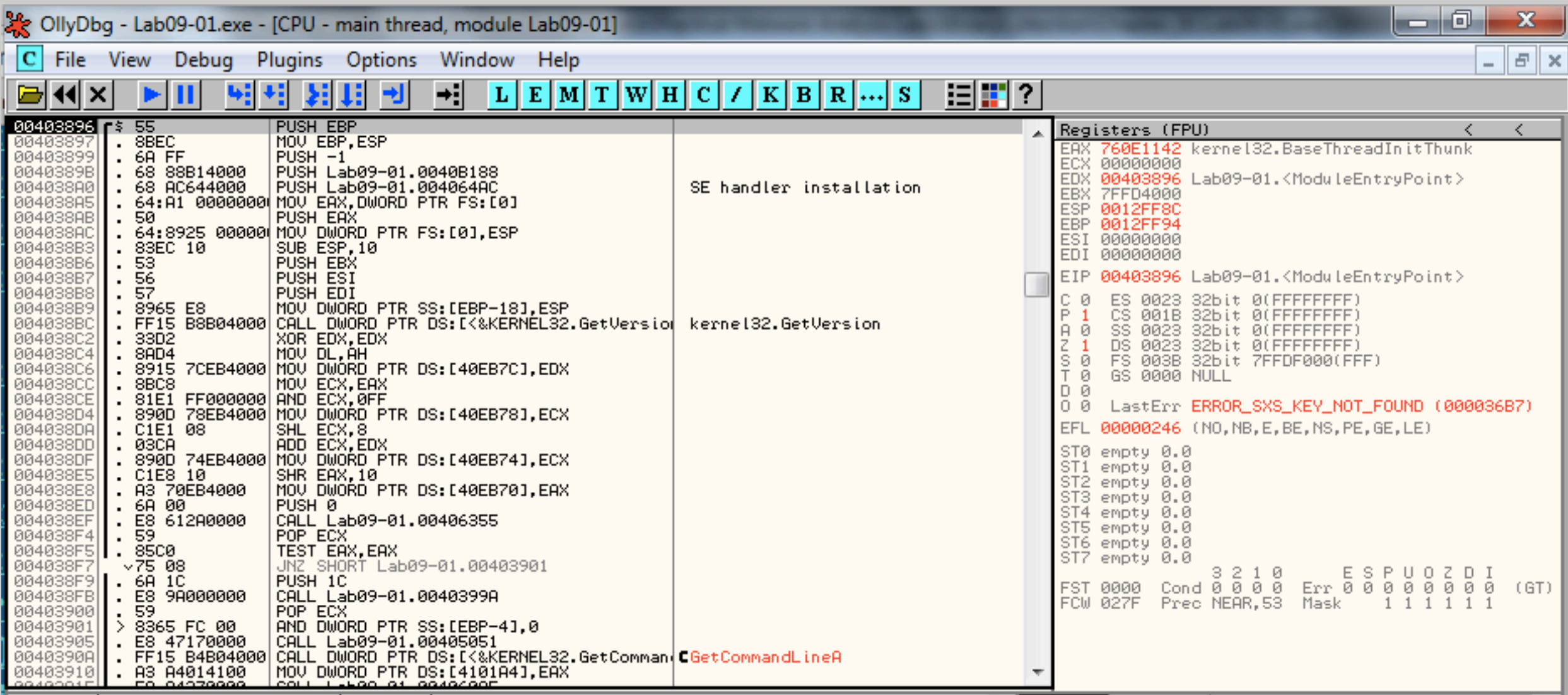
YOU MUST SUBMIT WHOLE-DESKTOP IMAGES TO GET FULL CREDIT.

Save the image with a filename of **"Proj 11a from YOUR NAME"**.

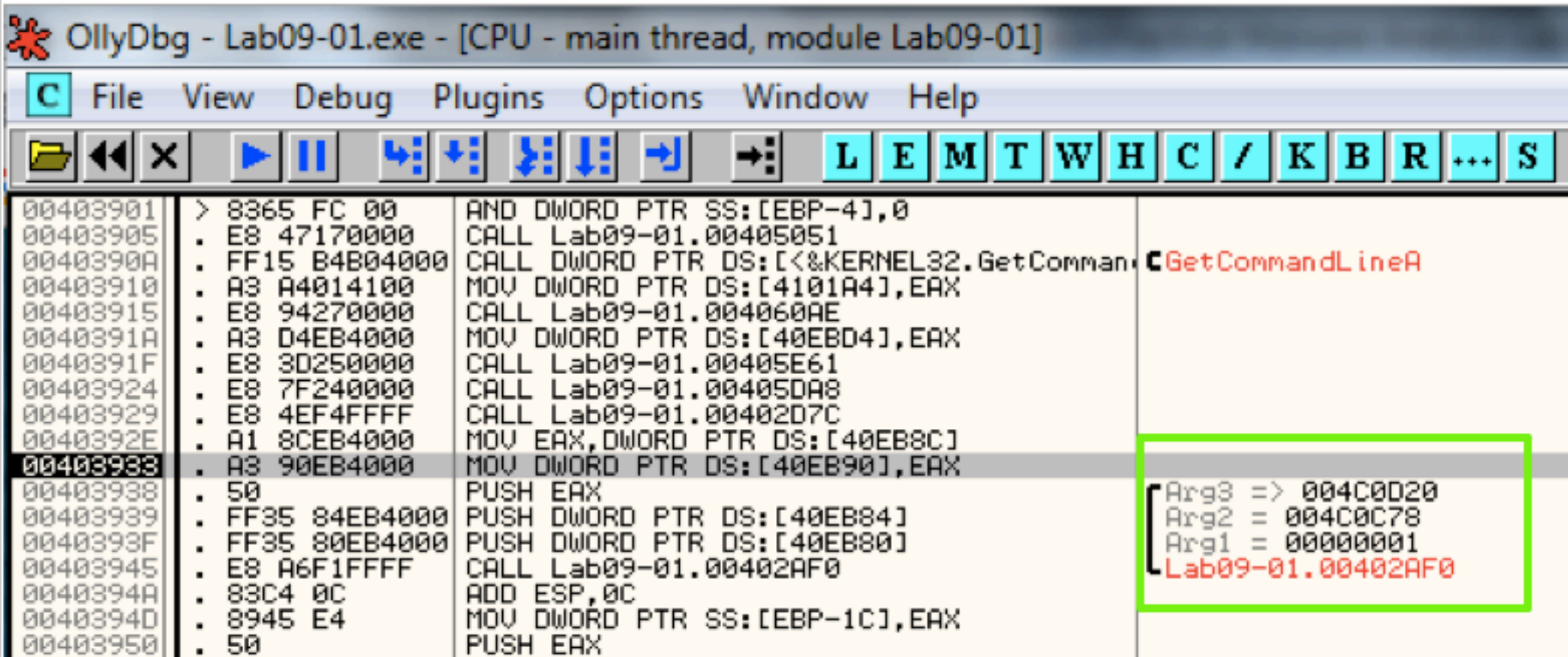
Using OllyDbg to Walk Through Quickly

Open Lab09-01.exe in OllyDbg.

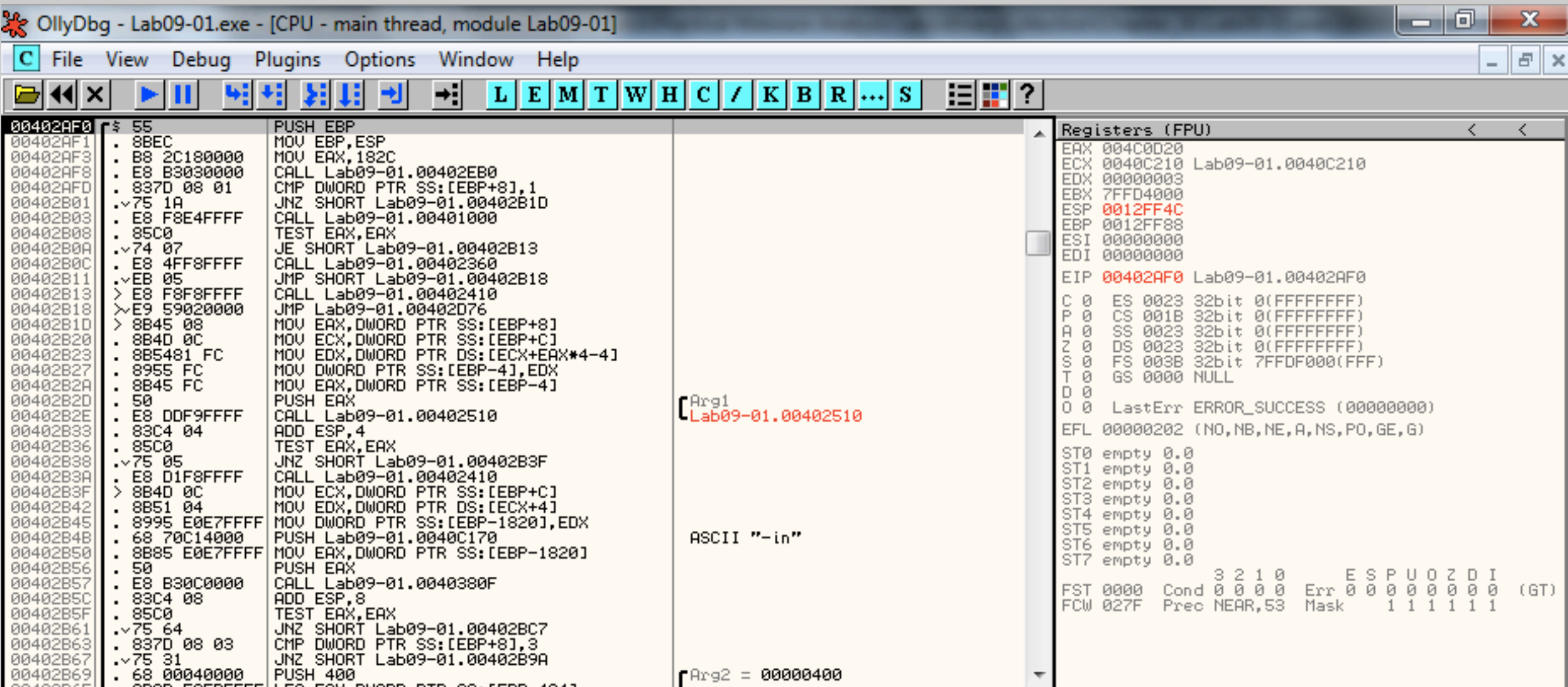
You start at a preamble, which comes before the entry point you saw in IDA Pro, as shown below.



Press F8 forty times, to step over until address 0x403933. In the upper left pane of OllyDbg, scroll down a few lines to show the code that sets the arguments and calls main, as highlighted below.

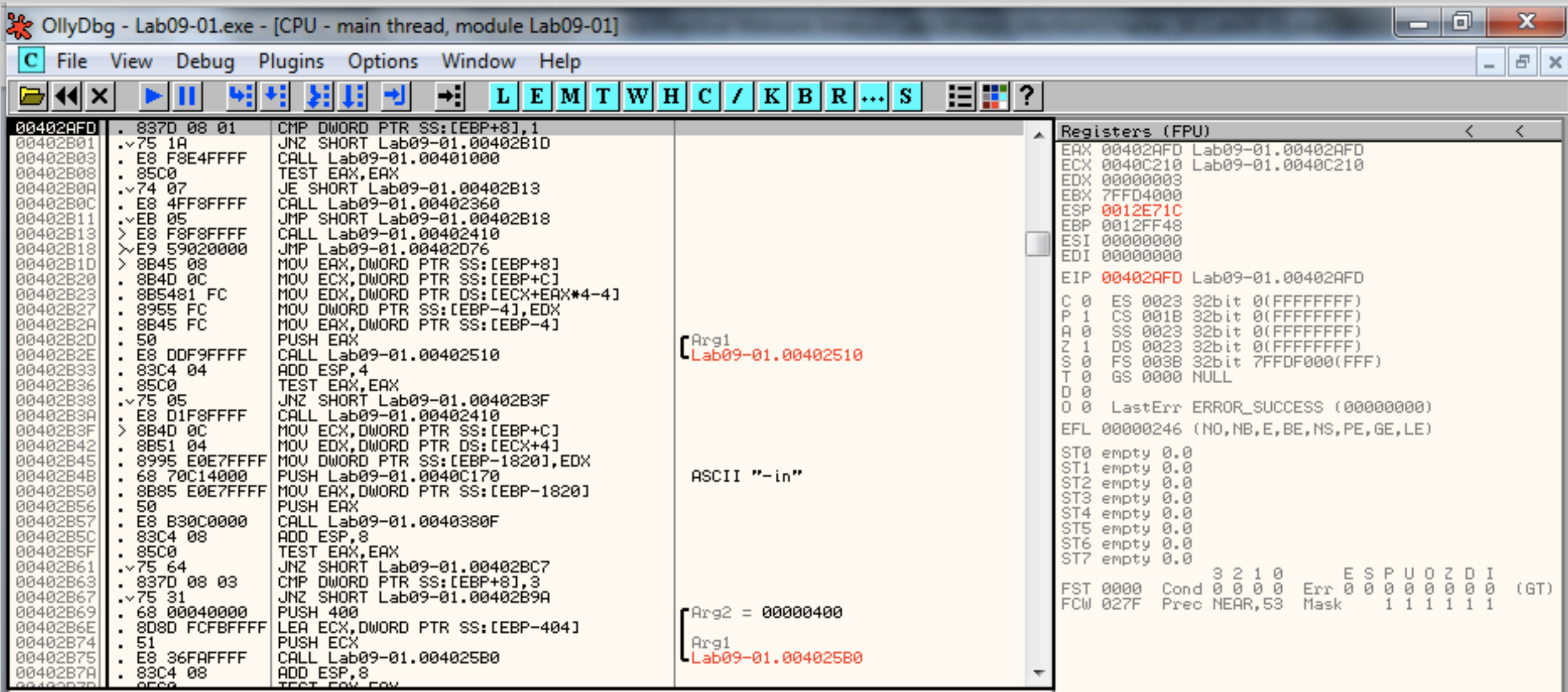


Press F7 five times to load parameters and call main from 0x403945, showing a new section of code starting at 0x402AF0, as shown below.



Press F7 twenty-one times to call a short subroutine and get to 0x402AFD, as shown below.

This CMP operation is testing to see if the number of command-line arguments is 1.



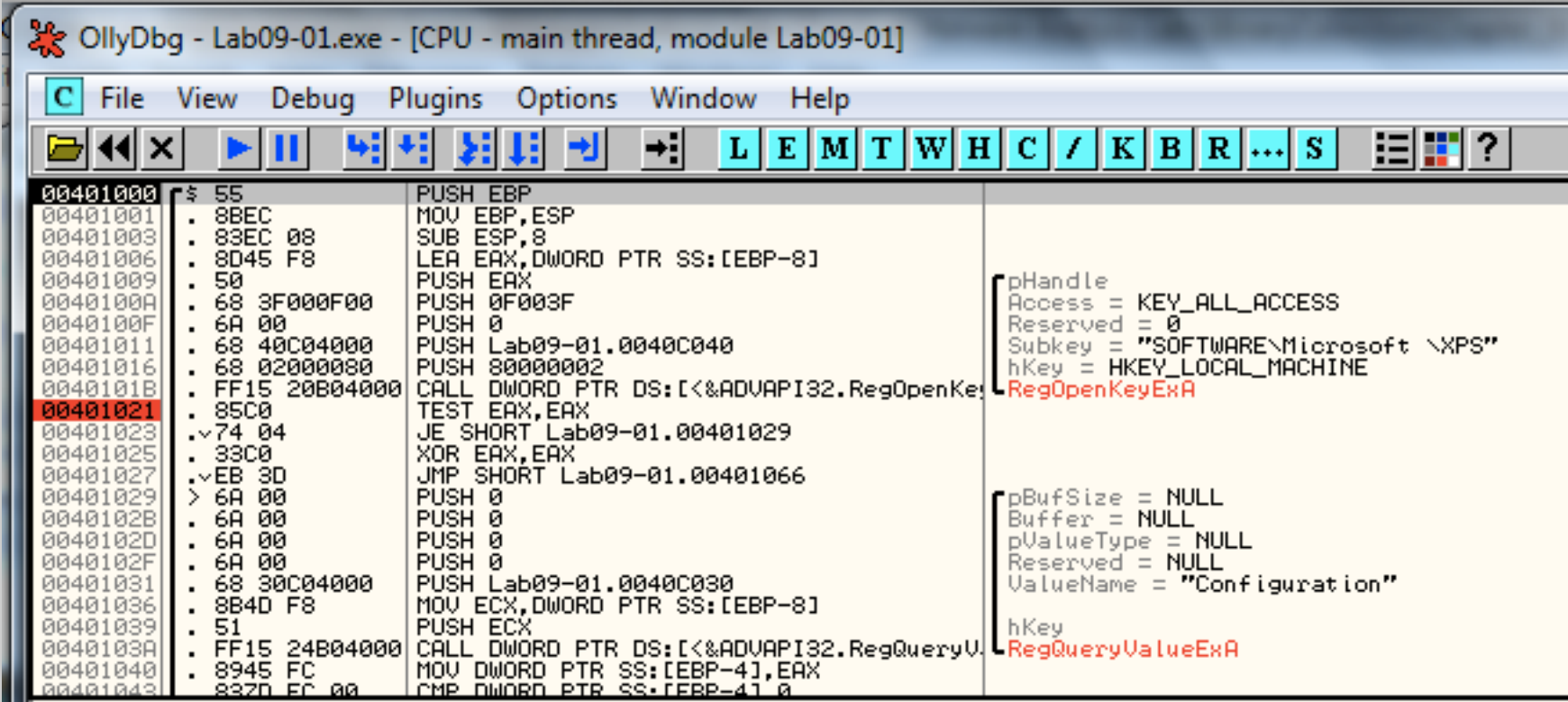
Press F7 three times to pass the test and jump to 0x00401000, as shown below.

Now we are in the routine starting at 0x401000.

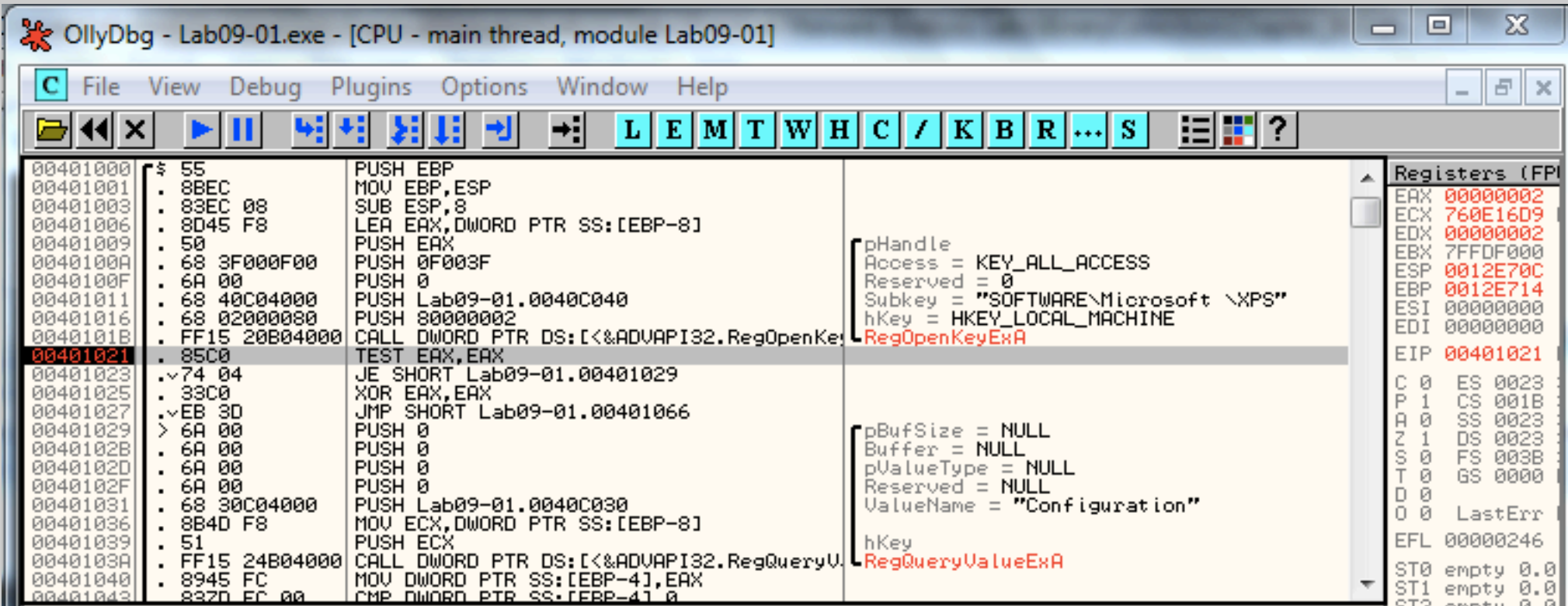
It calls RegOpenKeyExA at 0x40101B.

Left-click the line starting with 0x401021 and press F2 to put a breakpoint there. That address turns red, as shown below.

Left-click the line starting with 0x401000. Press F9 to run to the breakpoint.



Look at the upper right to see the registers. EAX now contains 2, as shown below.



This is a "non-zero error code", as explained here:

[http://msdn.microsoft.com/en-us/library/windows/desktop/ms724897\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724897(v=vs.85).aspx)

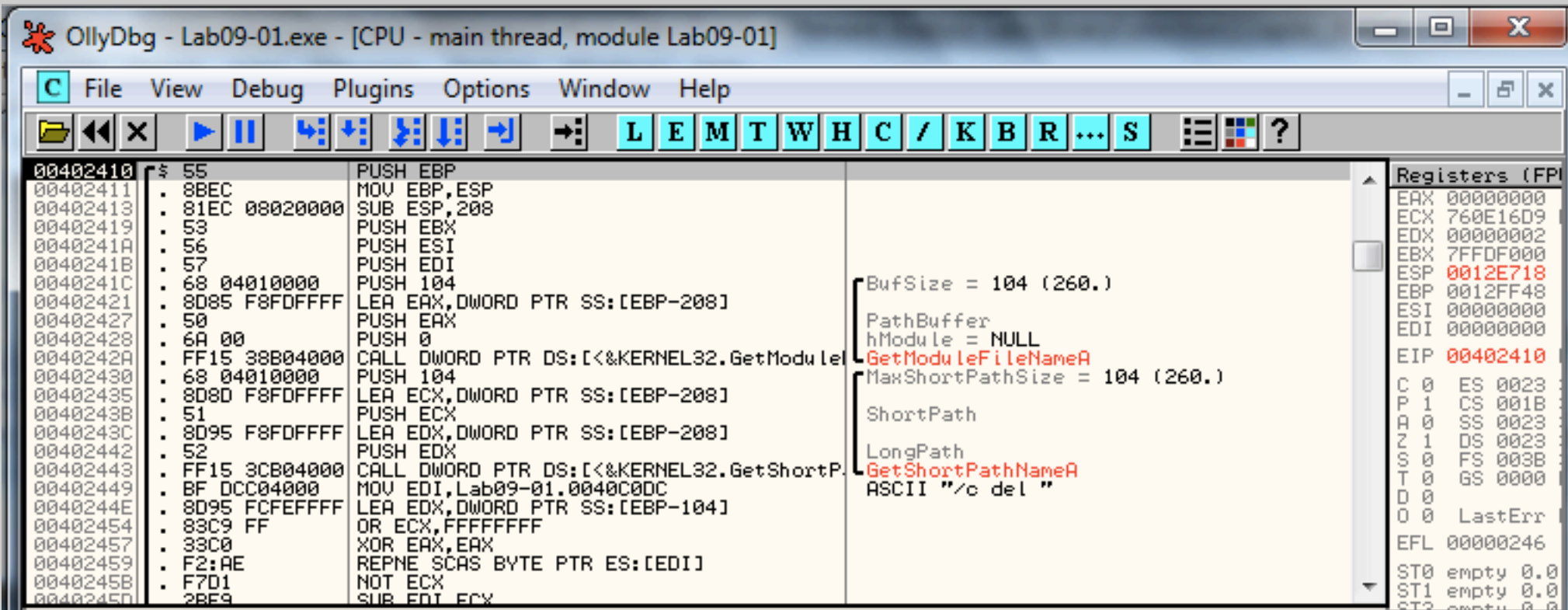
That means the test failed--it did not find the registry key it was looking for.

Press F7 three times to get to location 0x401027.

Press F7 to execute the JMP.

Press F7 three times to step through the subroutine and get to 0x402B08.

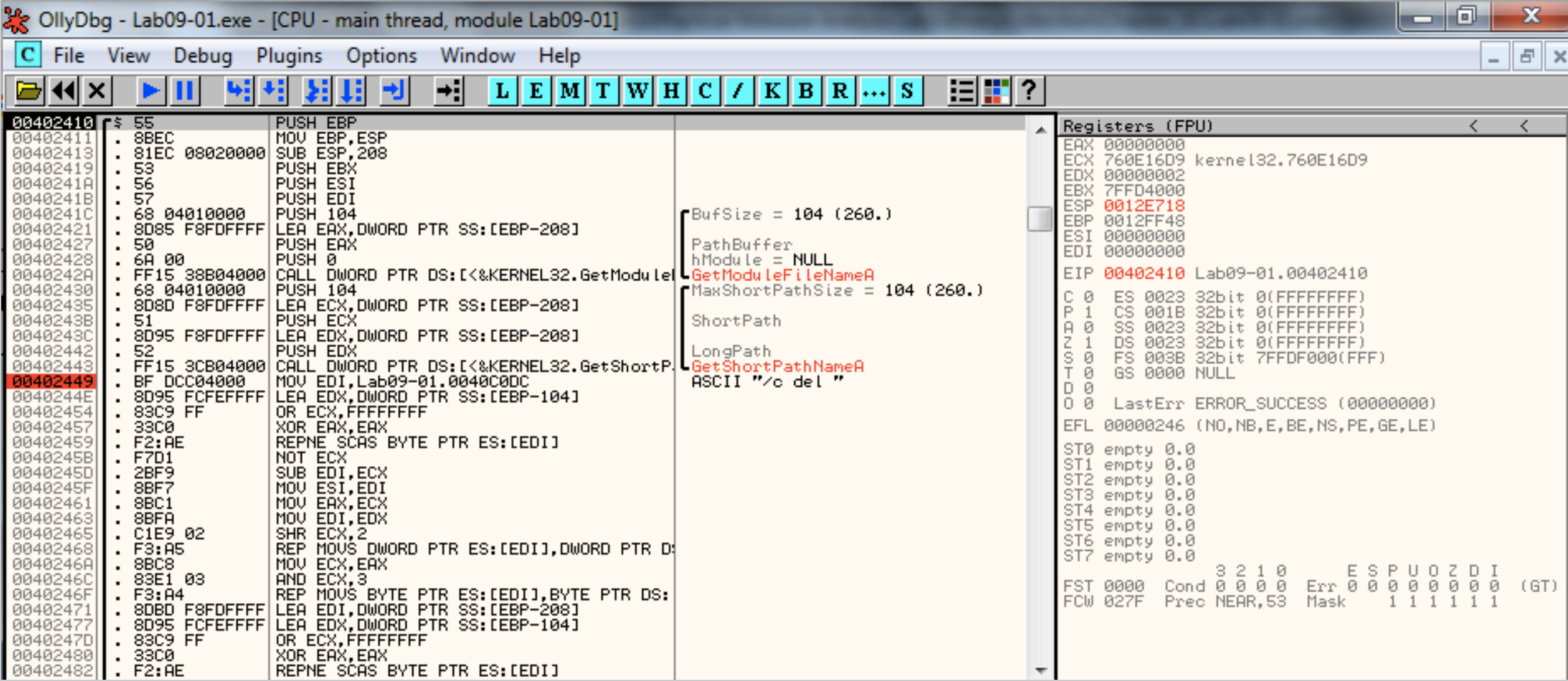
Press F7 three times to get to location 0x402410, as shown below:



This function uses GetModuleFilename to get the path to the current executable and builds the ASCII string

/c del path-to-executable >> NUL

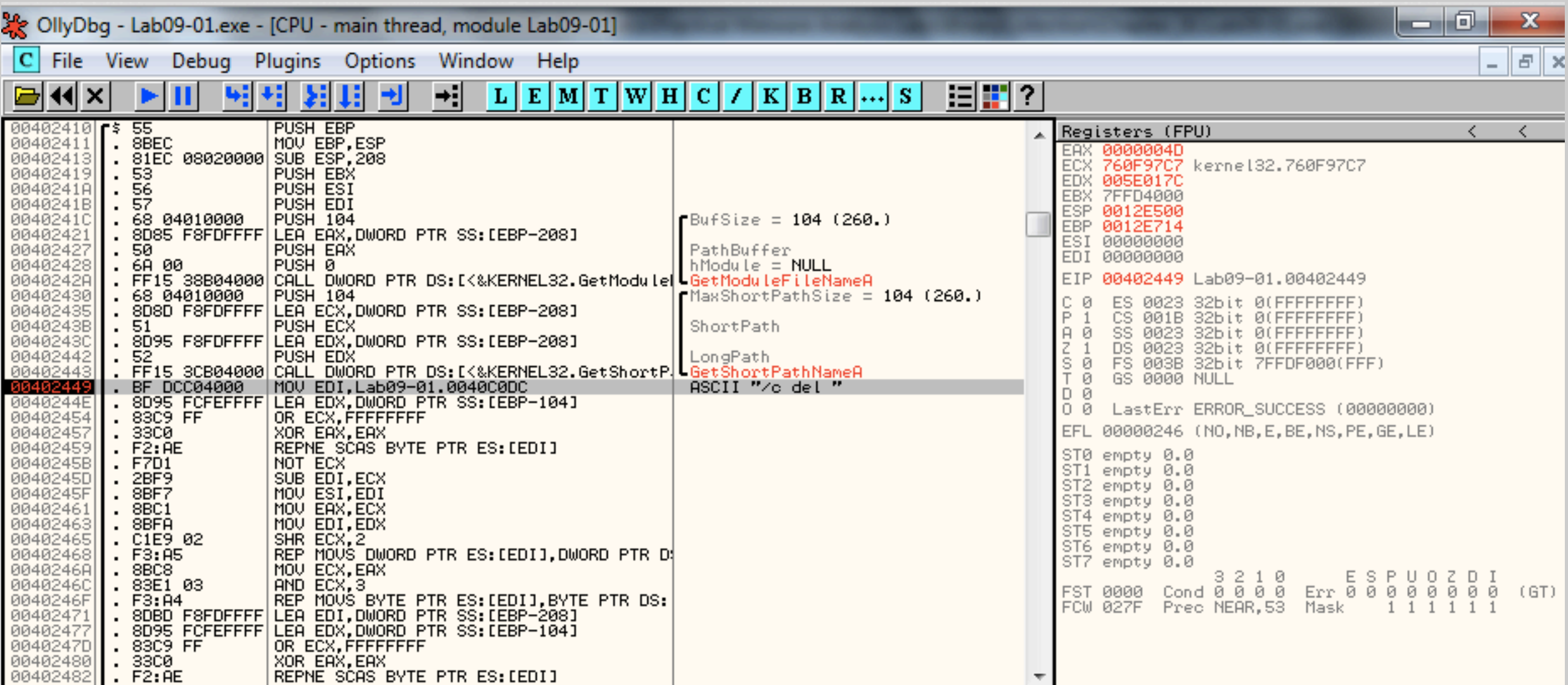
To see that, place a breakpoint just after GetShortPathNameA, so its address turns red, as shown below.



Click the line starting with 0x402410 to highlight it.

Press F9 to run to the breakpoint.

You should now be at the line ending with "ASCII "/c del ", as shown below.



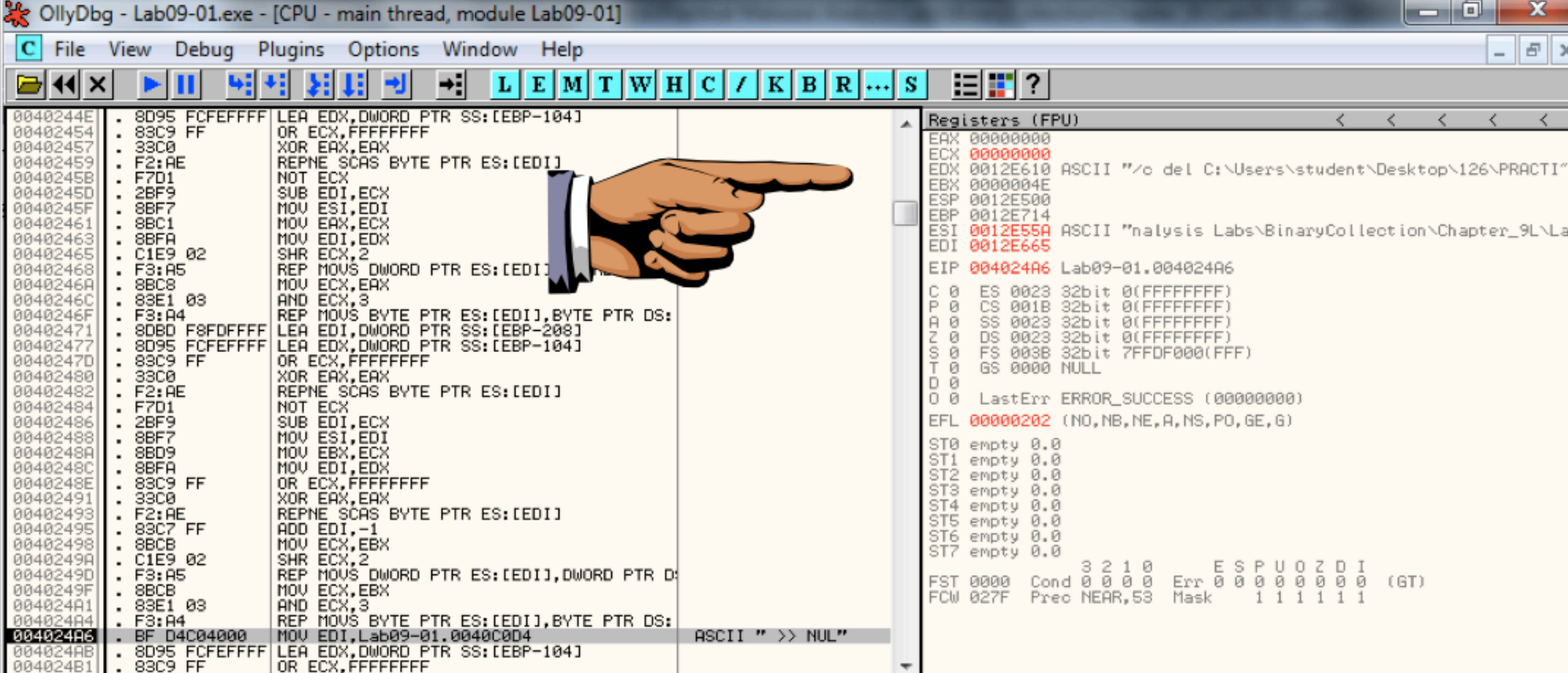
By holding F7 down or tapping it many times, you can play the code forward like a movie in slow motion.

Watch as the code slowly steps through a long path name in EDI. Then the path name flips quickly through several registers, ending up in EDX.

Stop when you see a string in EDX, starting with

ASCII "/c del C:\

as shown below:



Troubleshooting

If you press F7 too many times, EDX empties. To return to this point you must do these steps:

- From the Ollydbg menu bar, click **Debug, Restart**
- Click **Yes**
- Press **F9** to run to the breakpoint at 0x401021
- Press **F9** to run to the breakpoint at 0x402449
- Hold down or tap **F7** several dozen times to get to the desired point

Saving the Screen Image

Make sure you can see the EDX register with a value starting with ASCII `"/c del C:\` as shown above.

On your keyboard, press the PrntScrn key.

Click **Start**, type in **PAINT**, and open Paint.

Press **Ctrl+V** to paste in the image of your desktop.

YOU MUST SUBMIT WHOLE-DESKTOP IMAGES TO GET FULL CREDIT.

Save the image with a filename of **"Proj 11b from YOUR NAME"**.

Turning in Your Project

Email the images to: **cnit.126sam@gmail.com** with a subject line of **Proj 11 From Your Name**, replacing Your Name with your own first and last name. Send a Cc to yourself.

Last Modified: 3-21-16