**Lab 18: Simple EXE hacking with immunity**

Task 1: Target EXE Recon

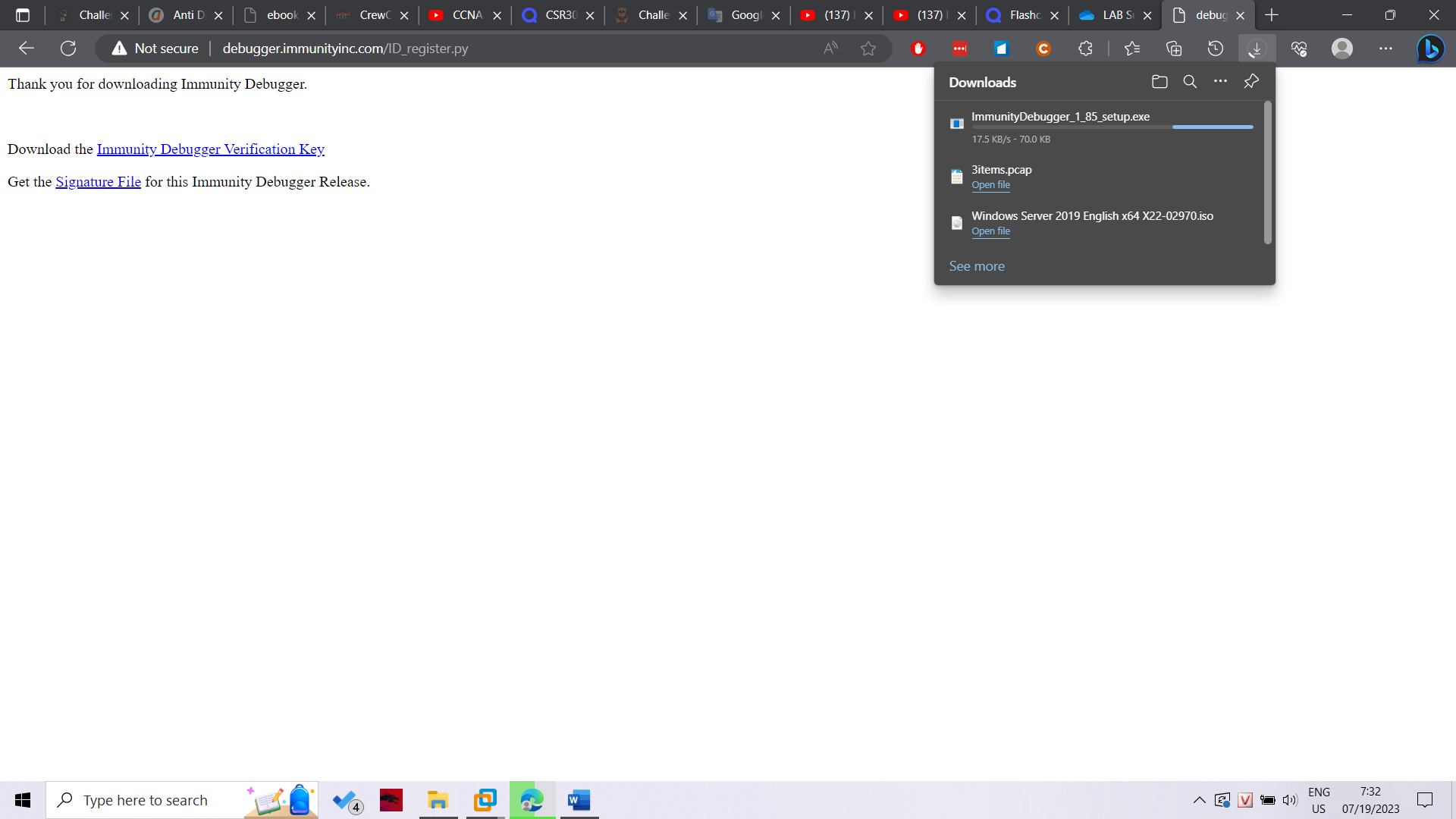
Get Immunity

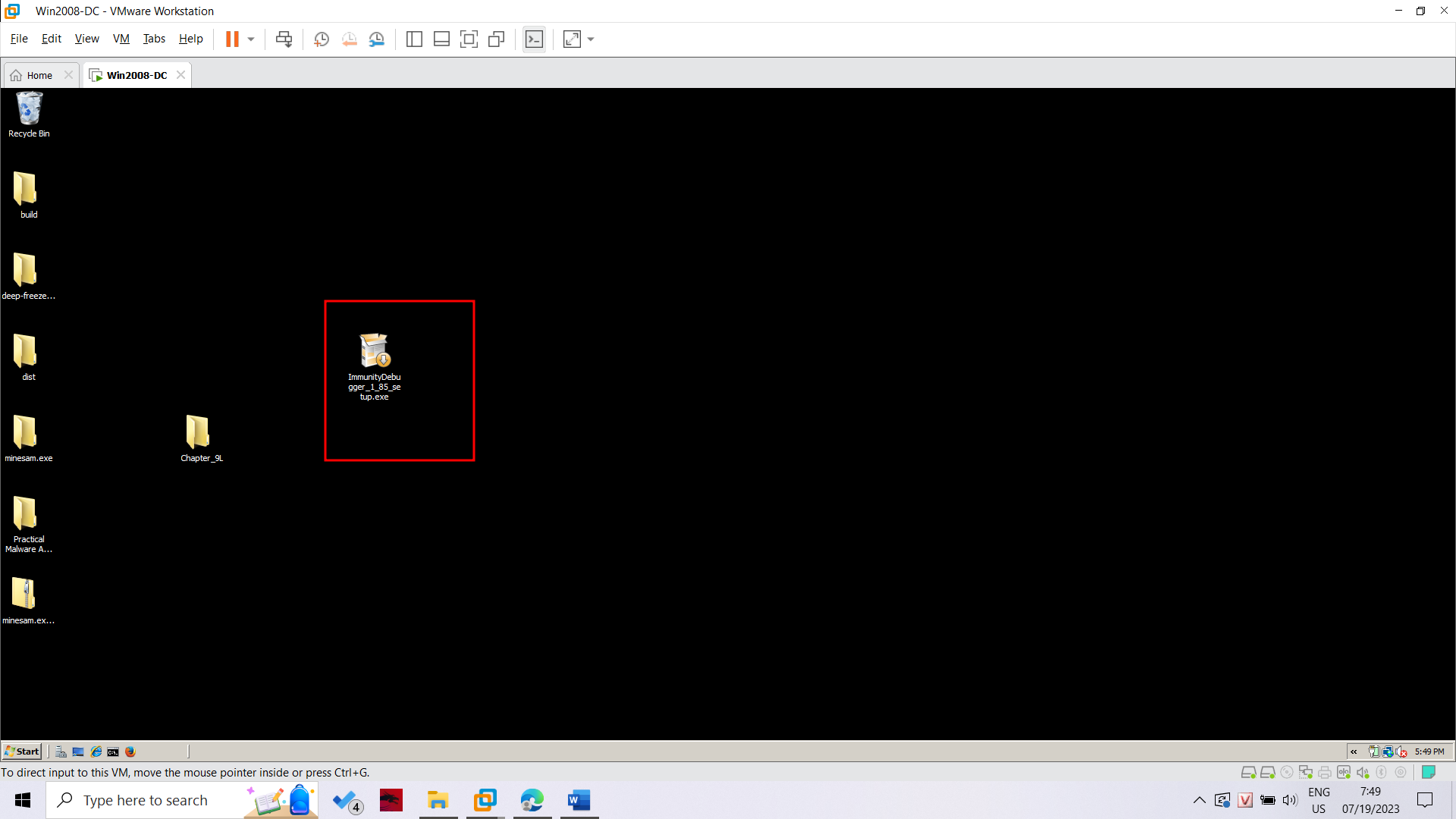
On your Windows machine, in a browser, go to

http://debugger.immunityinc.com/ID\_register.py

Fill in the form to download Immunity. Install it with the default options.

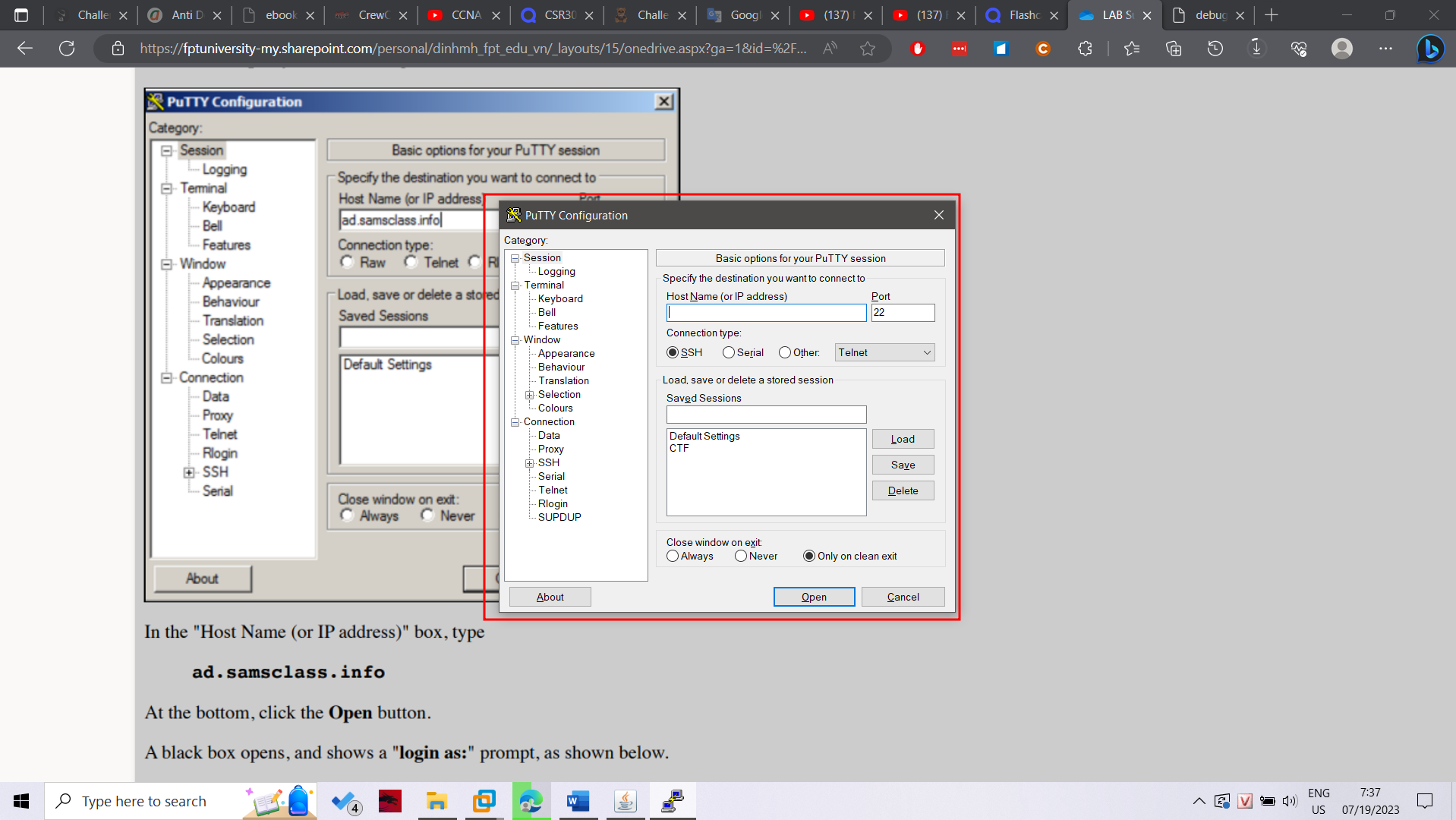


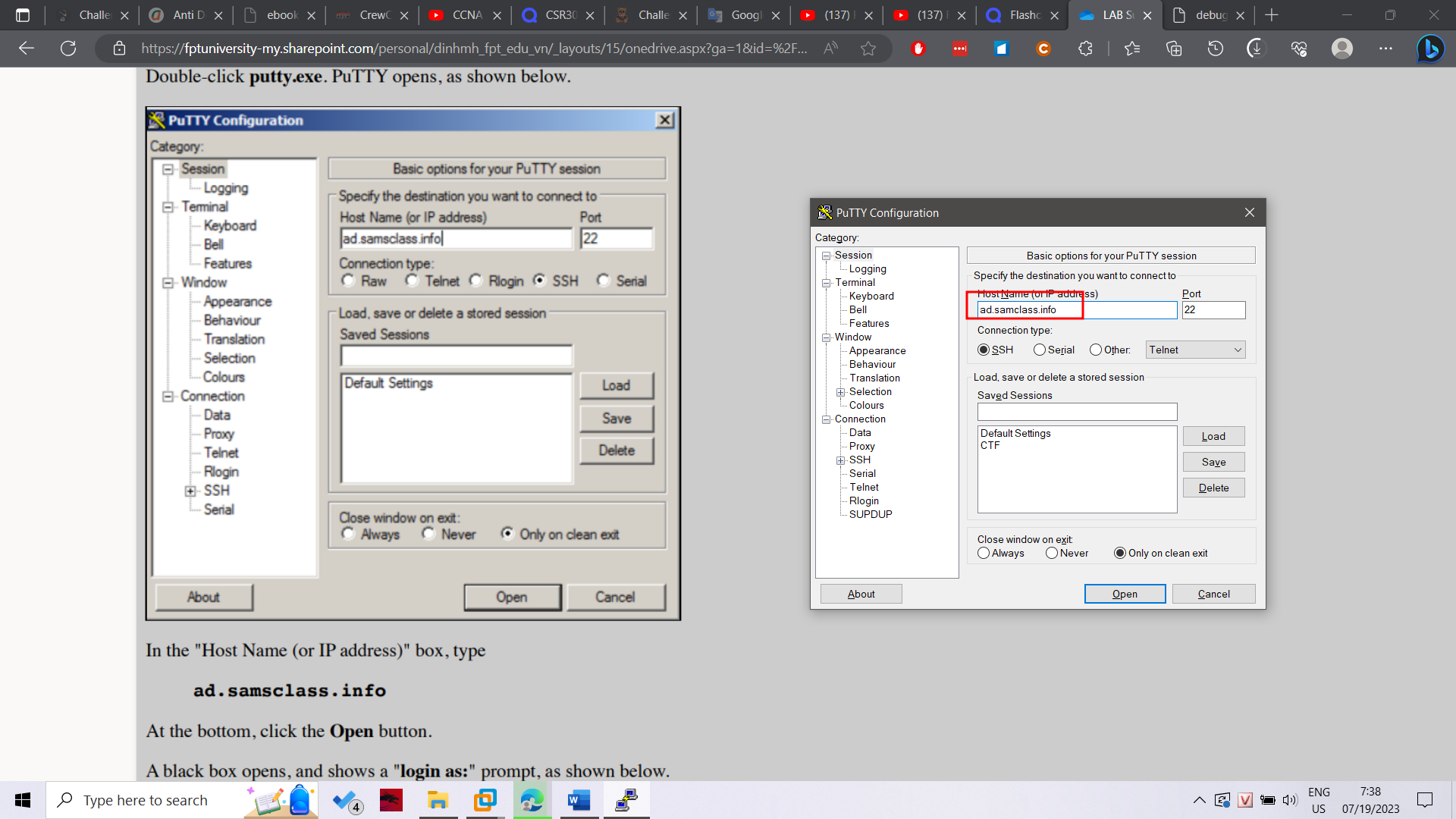


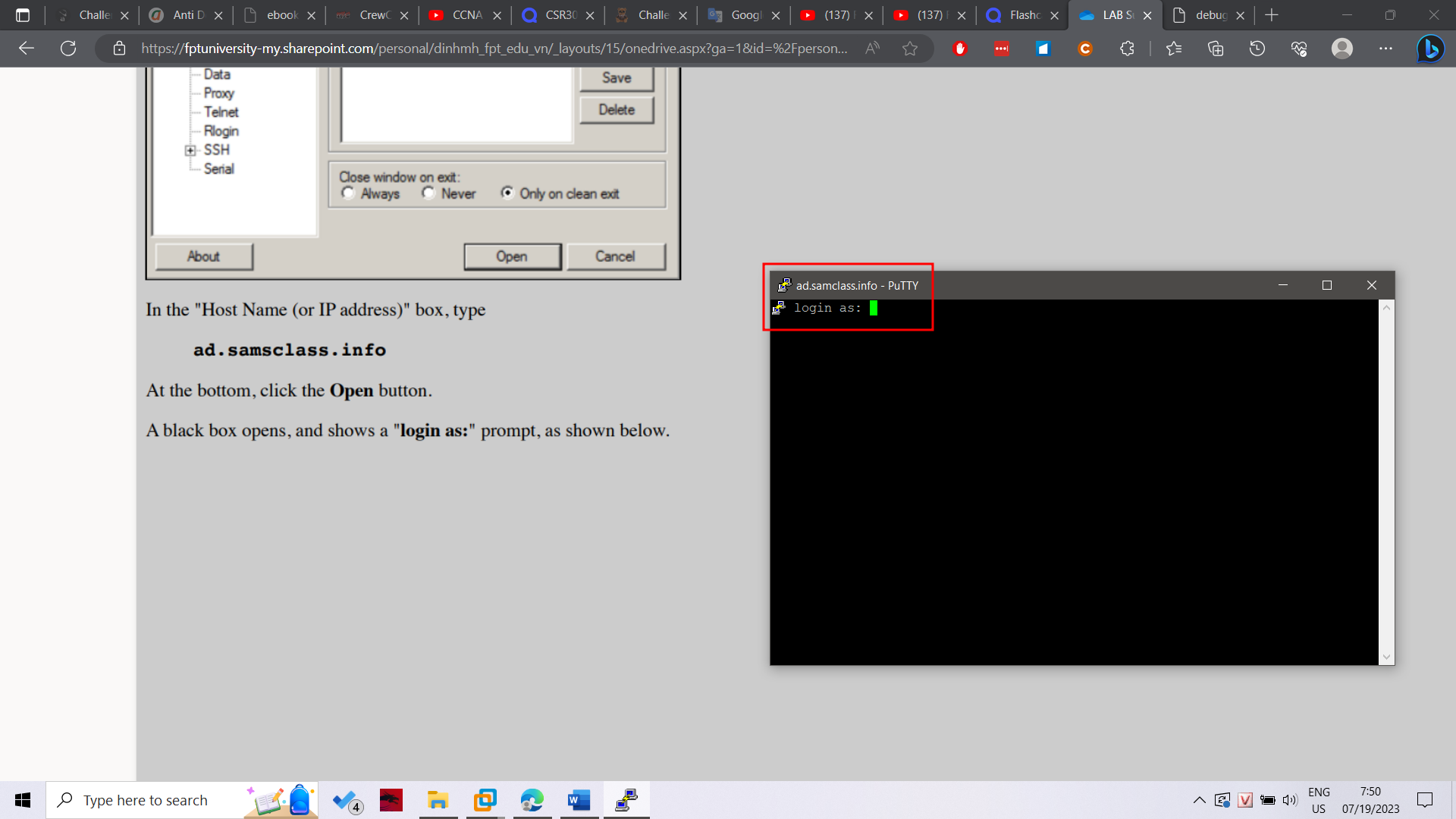


Running Putty

Double-click putty.exe. PuTTY opens, as shown below.







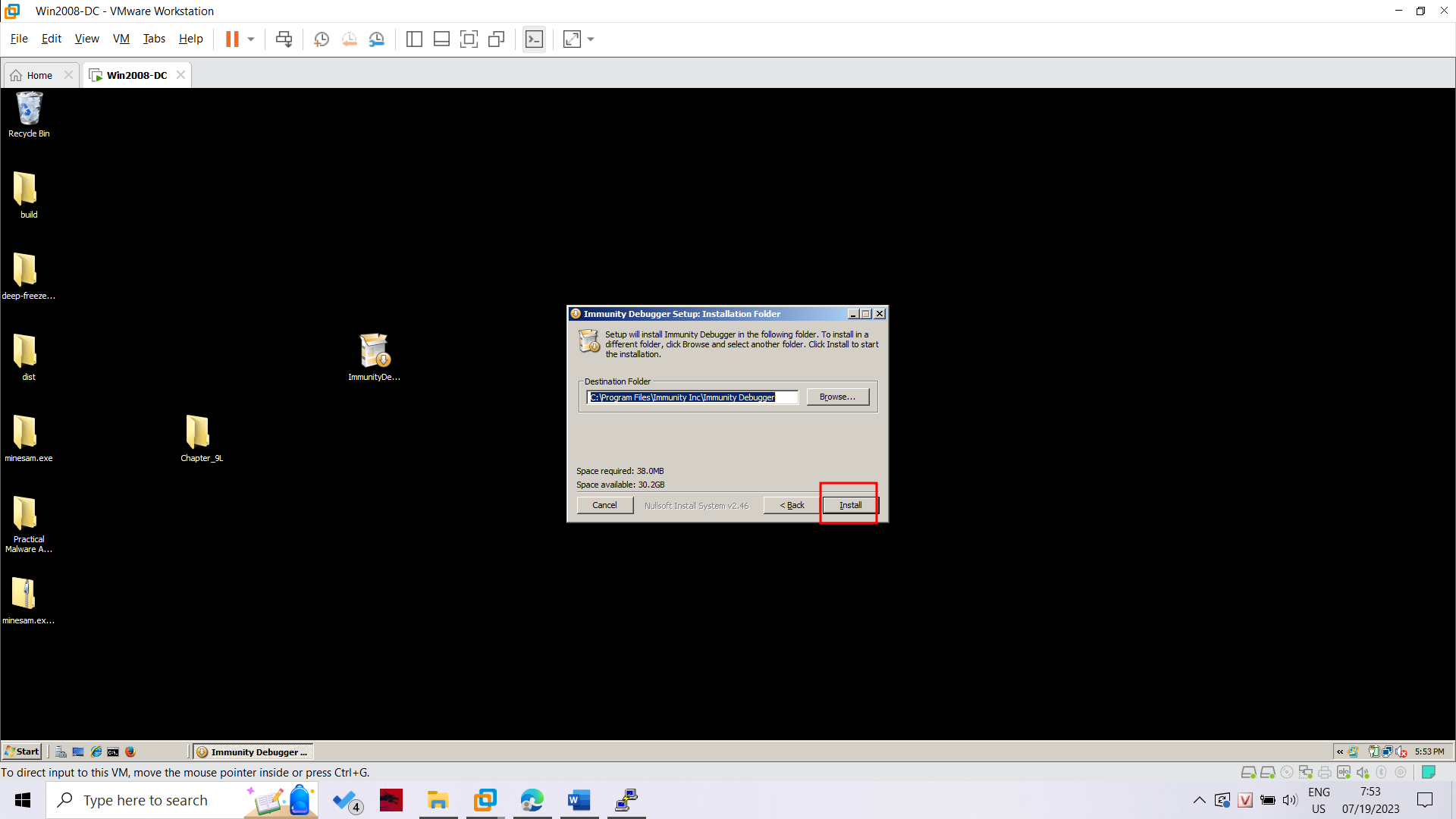
Starting the Immunity Debugger

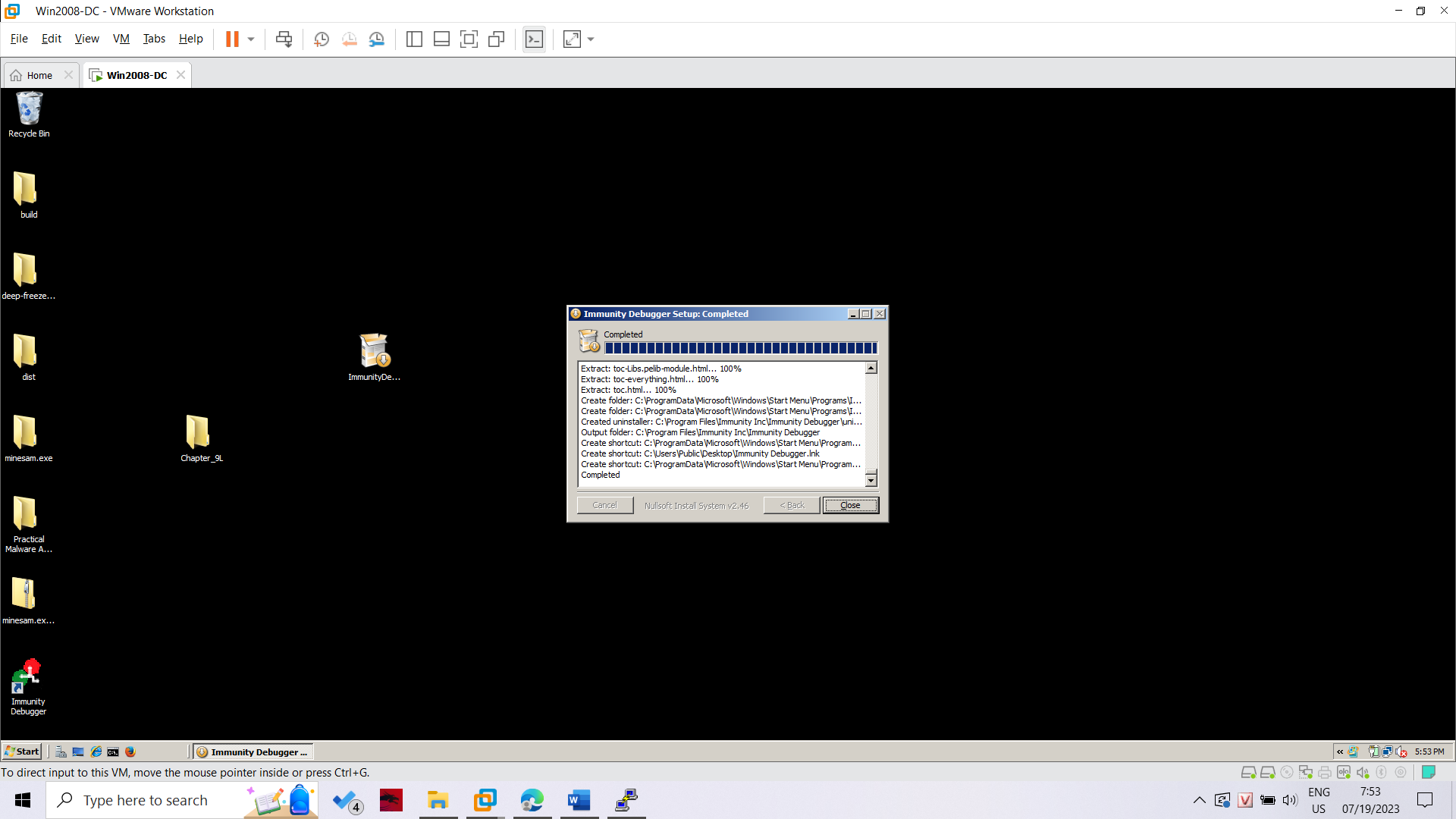
Click Start. Search for Immunity Debugger and start it.

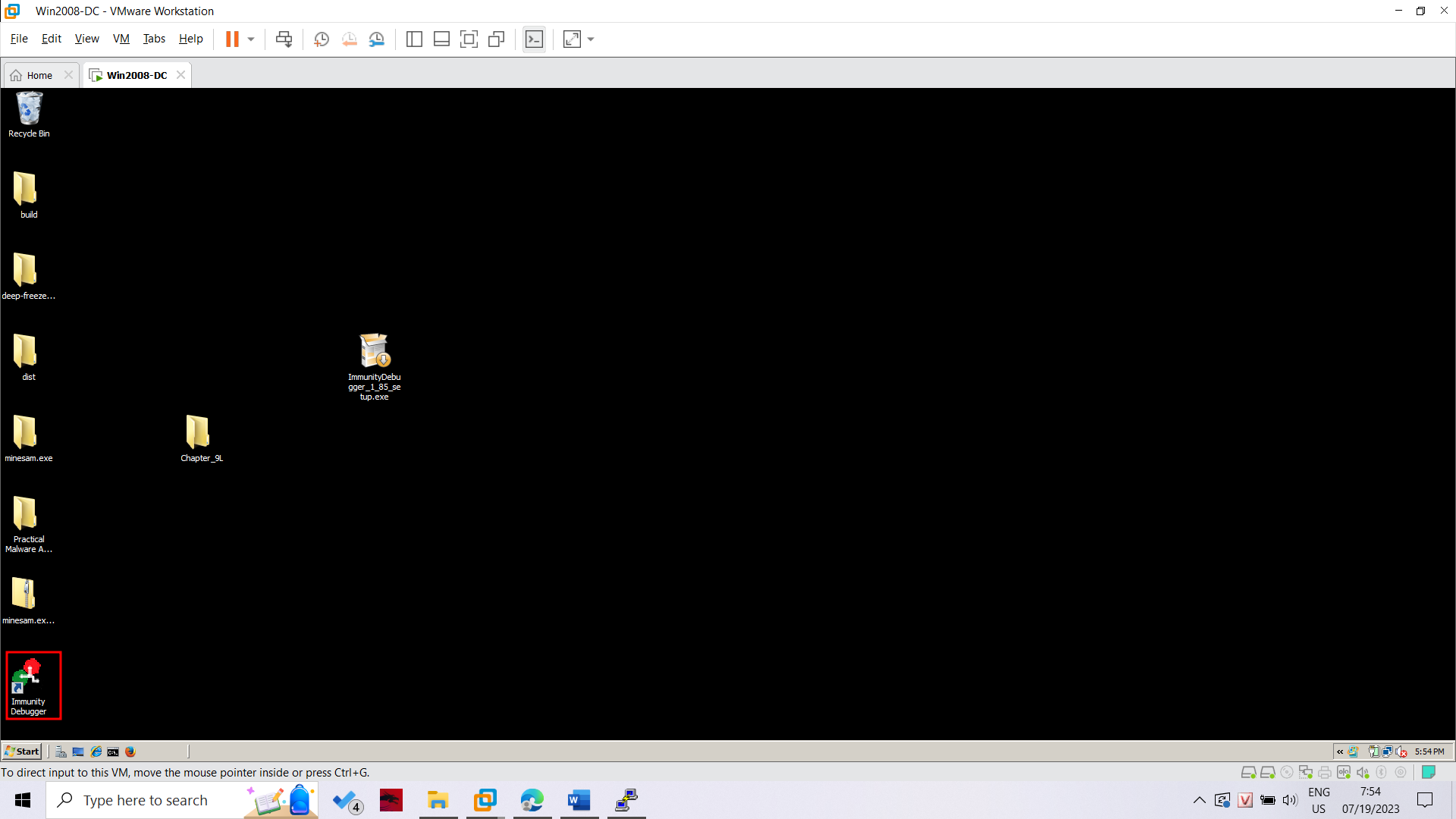
In Immunity, from the menu bar, click File, Open. Navigate to putty.exe and open it.

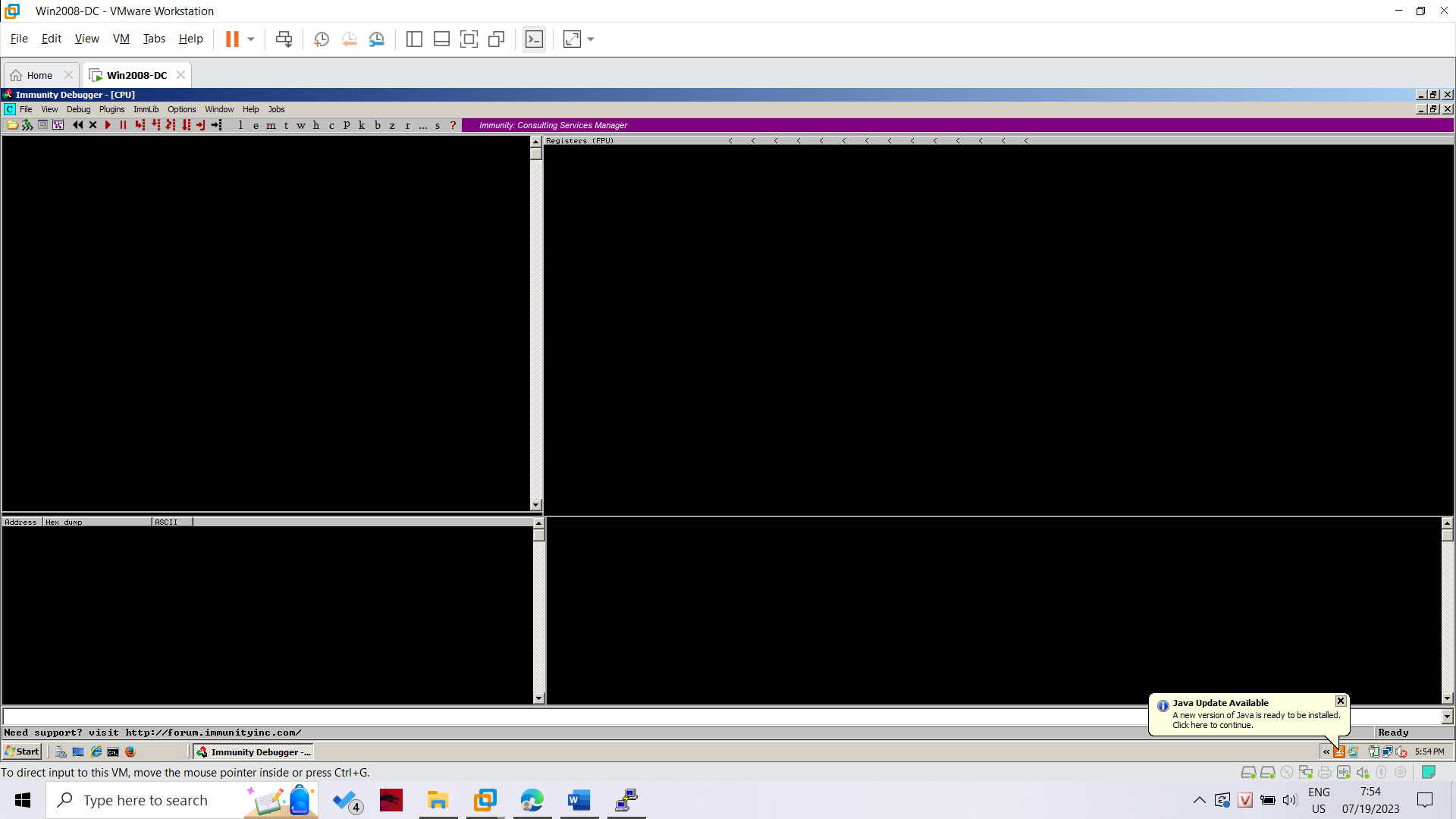
Immunity opens, as shown below. If your screen doesn't look like this, click View, CPU and maximize the CPU window

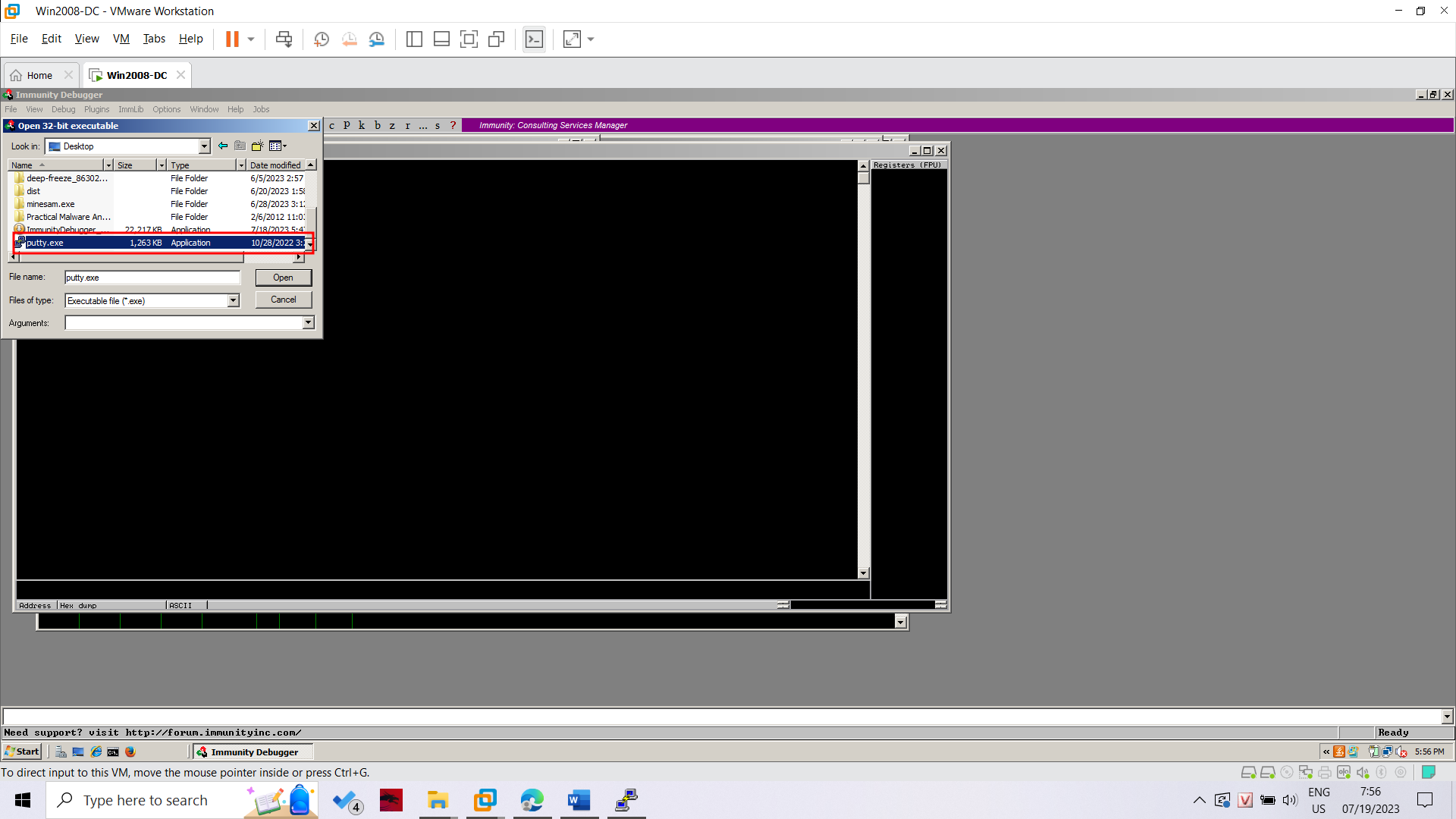


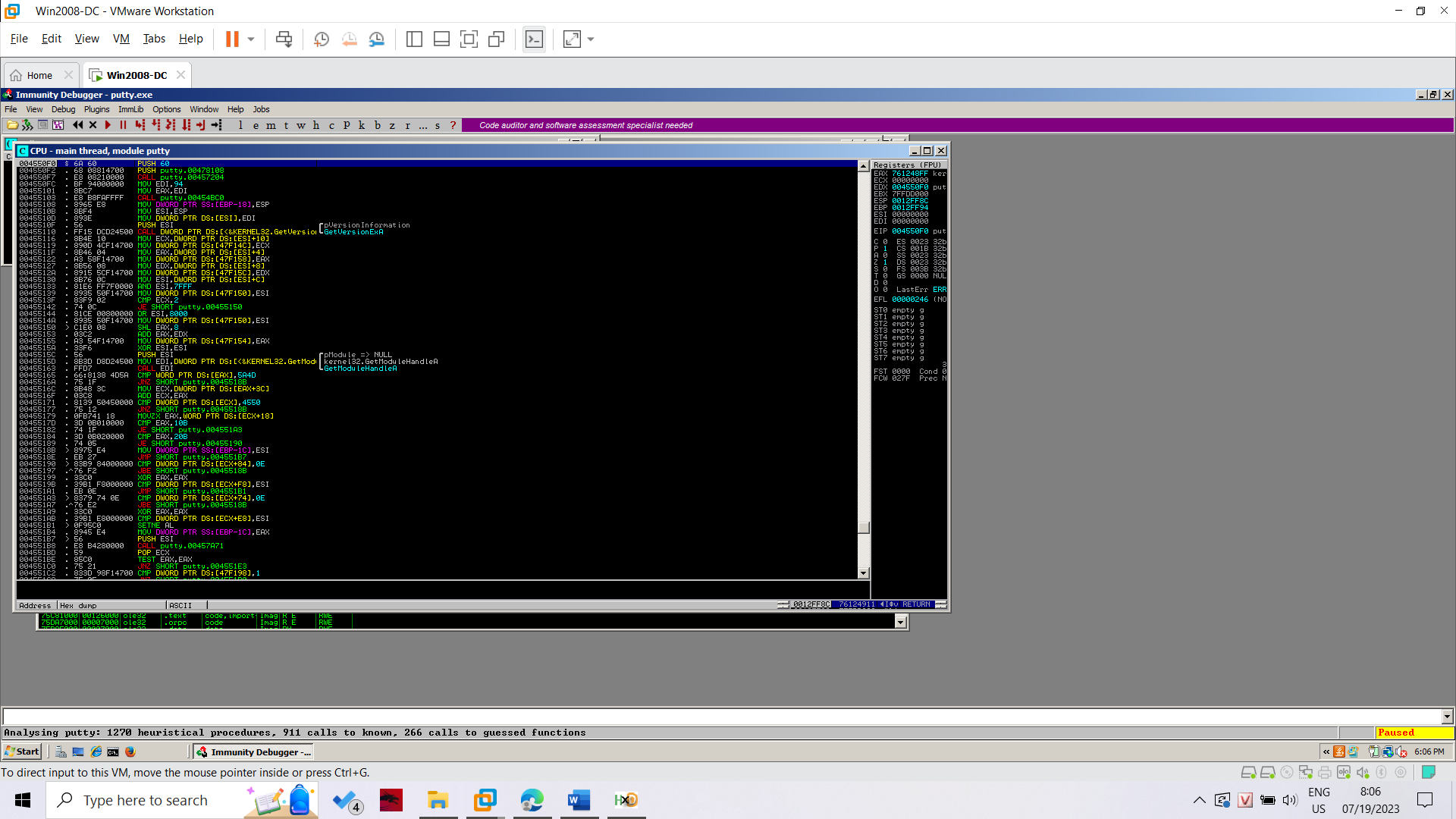










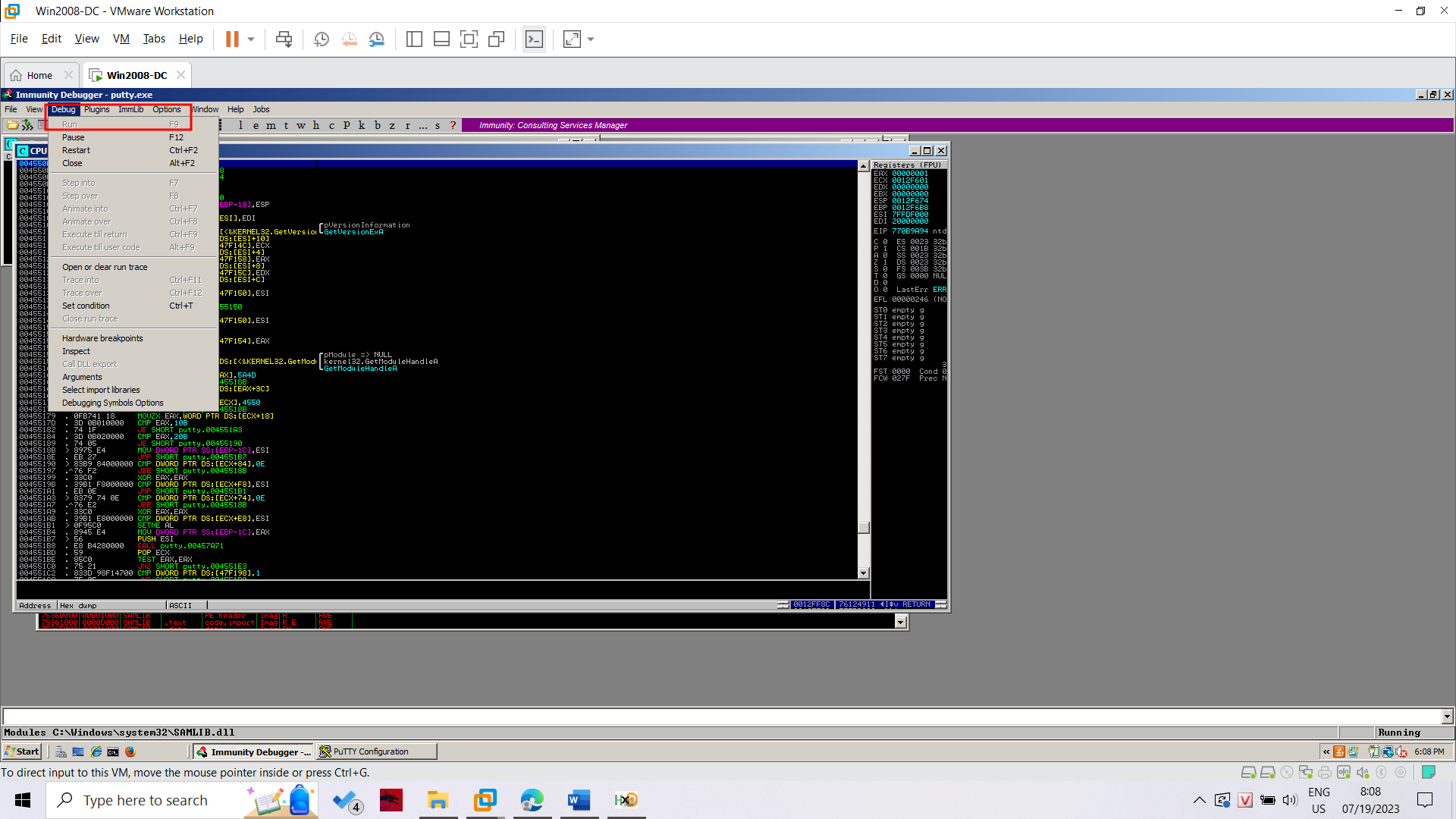
Immunity shows you a lot of data, but for now just notice the Assembly Code in the top left pane, and the Paused message in the lower right, as indicated in the figure

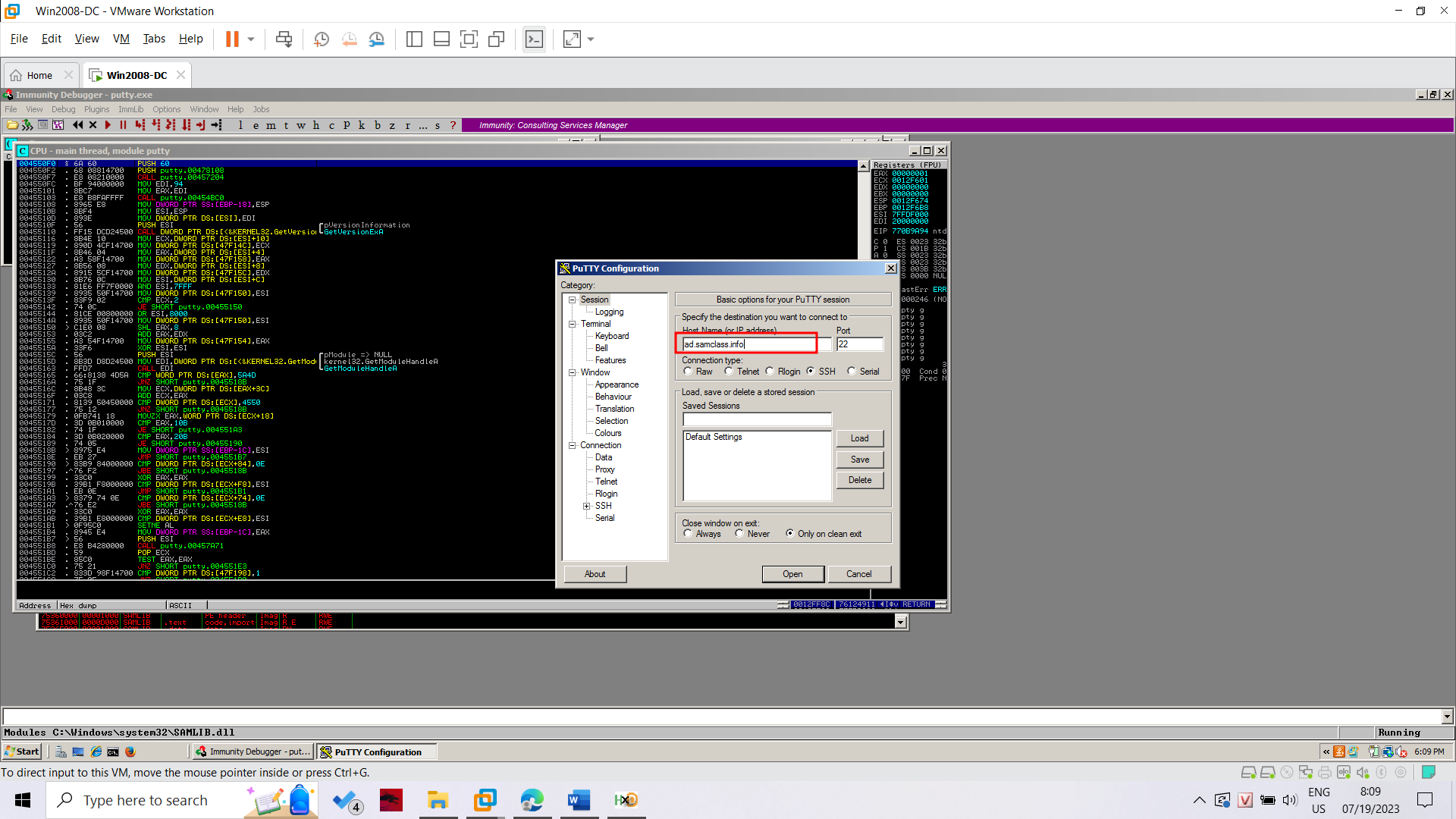
above.

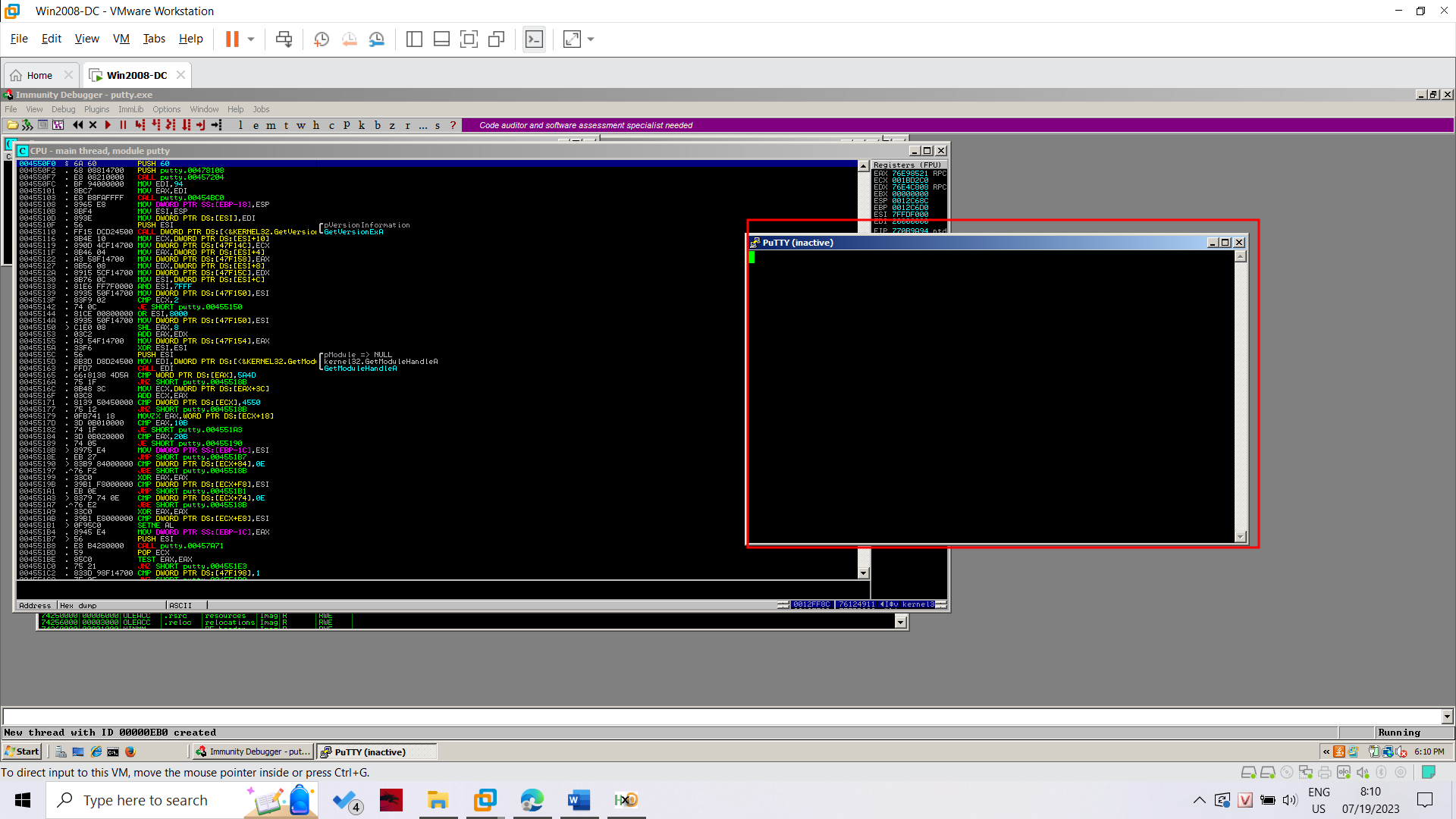
When you load a program into Immunity, it starts in a "Paused" state, with the Assembly Code window showing the first instruction.

Running Putty in Immunity

In Immunity, from the menu bar, click Debug, Run.

A Putty window opens, as shown below. 



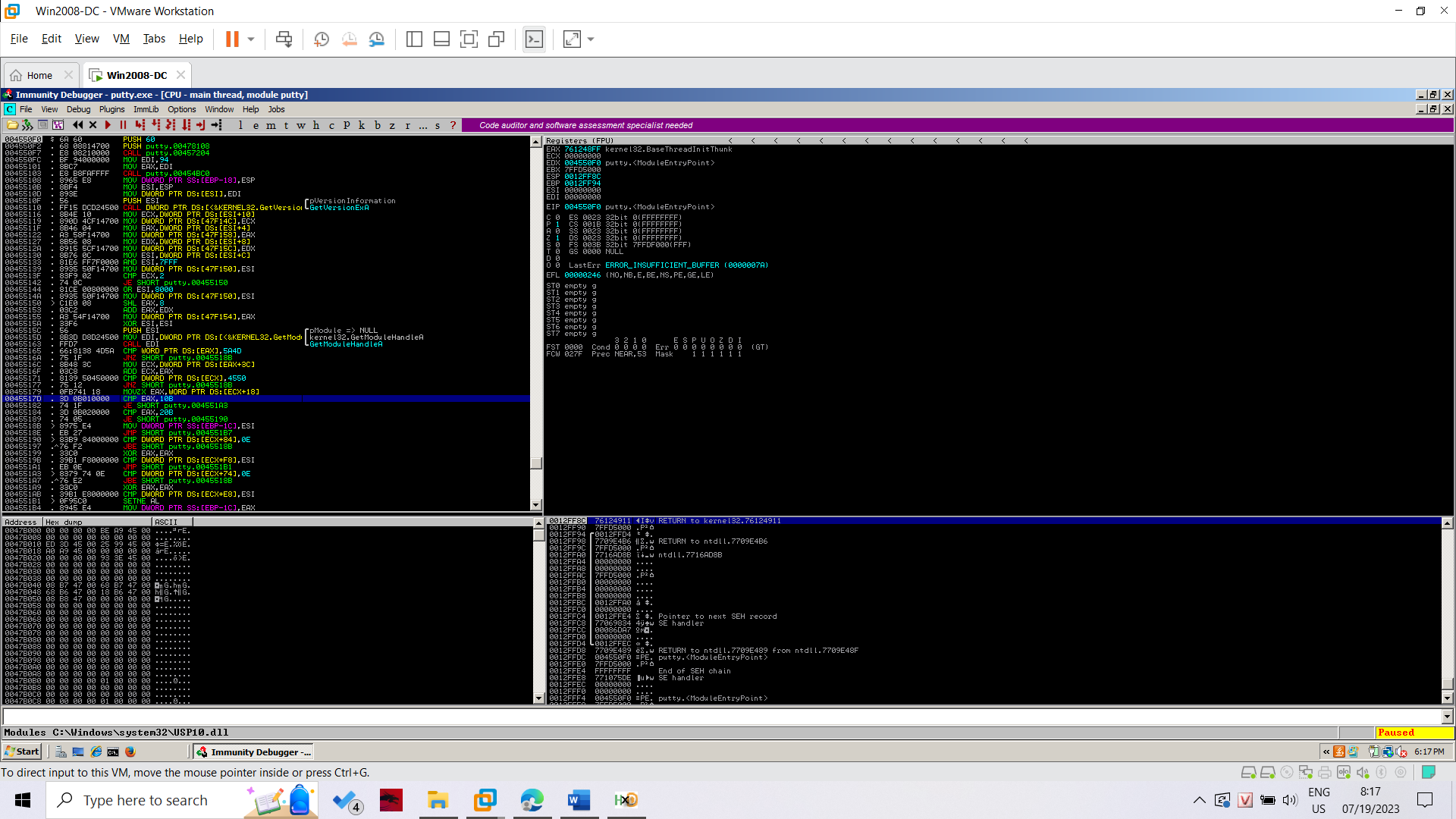


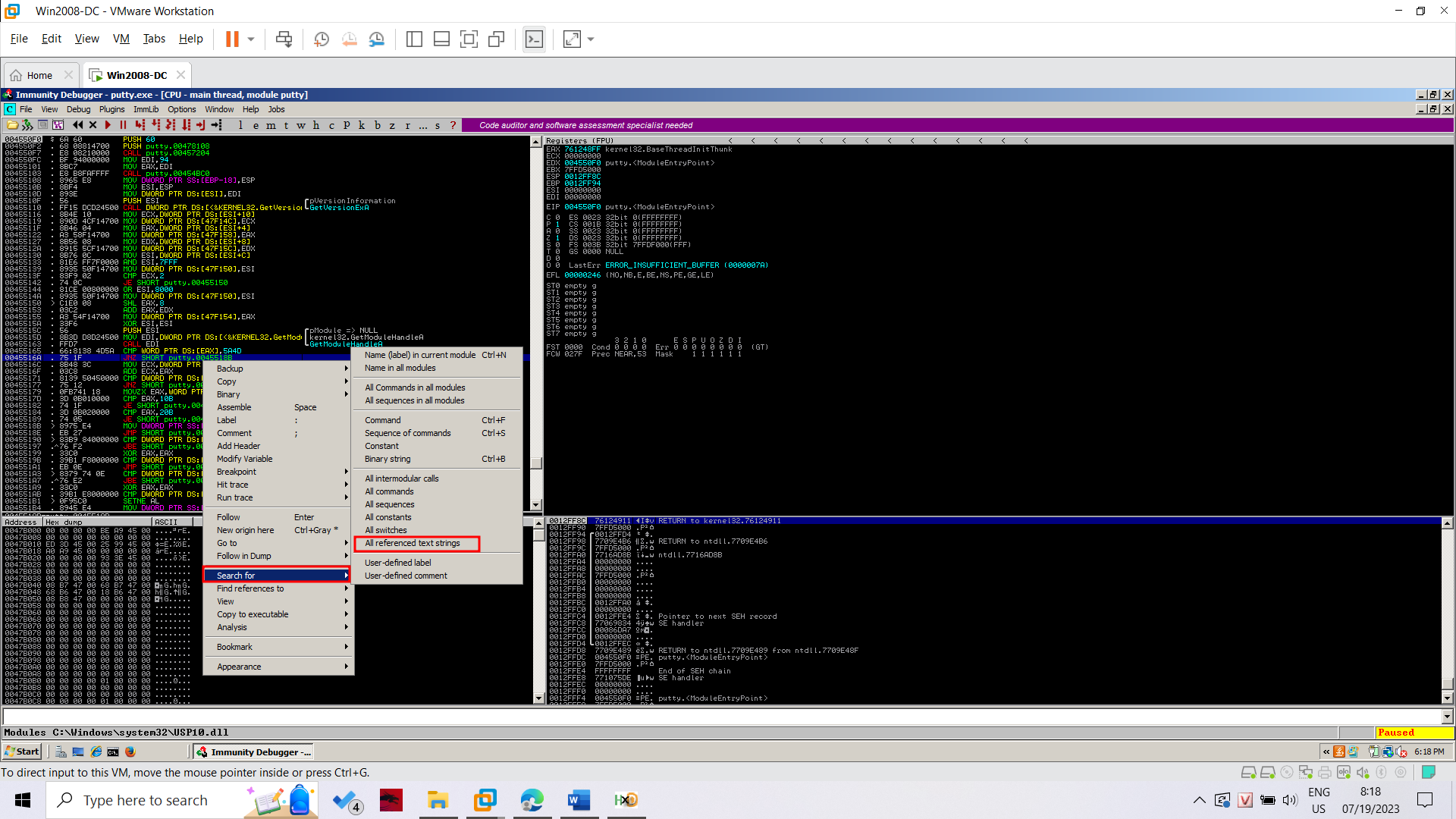
Finding the "login as" Code

Close the Putty window.

In Immunity, from the menu bar, click Debug, Restart.

In Immunity, in the "Assembly Code" pane, right-click. Point to "Search for". Click "All referenced text strings", as shown below.



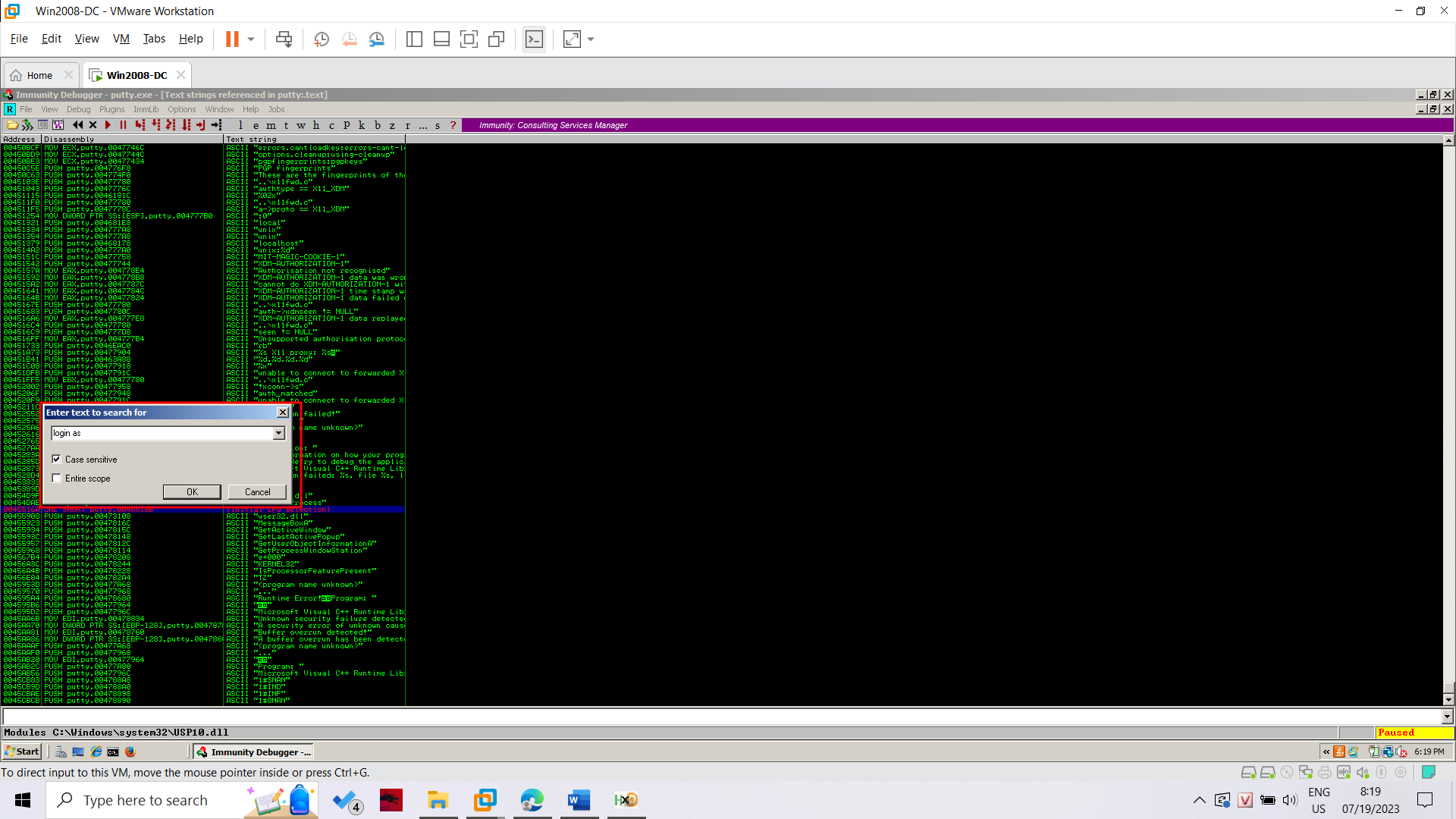


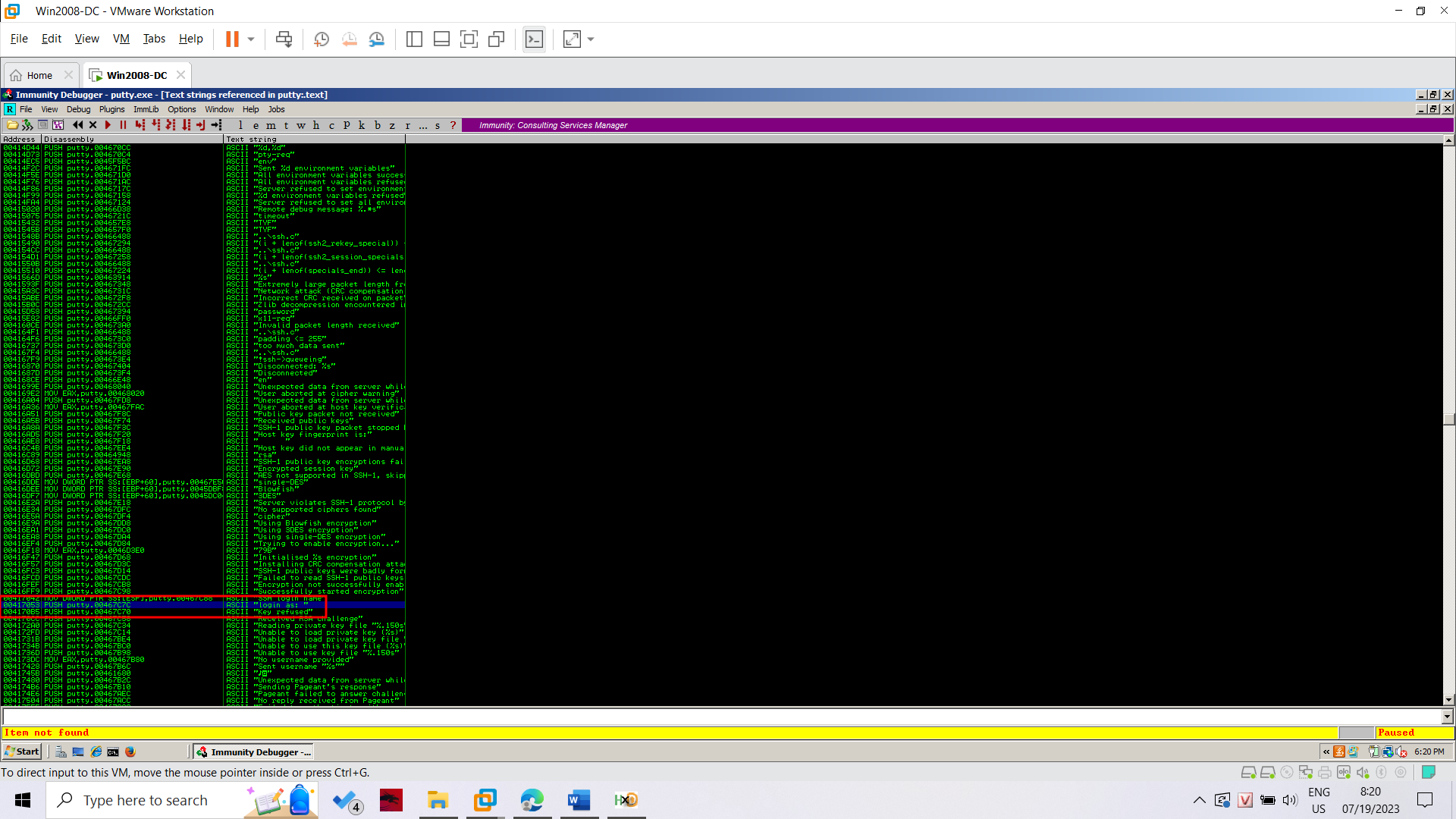
A "Text strings referenced in putty:.text" window opens, showing all the strings in the program.

Scroll to the top of the window and click on the first line, so it is highlighted.

Right-click in the window, and click "Search for text", as shown below.

Note: the search only goes down, and does not wrap, so if you begin a search near the bottom of the window it won't find "login as".

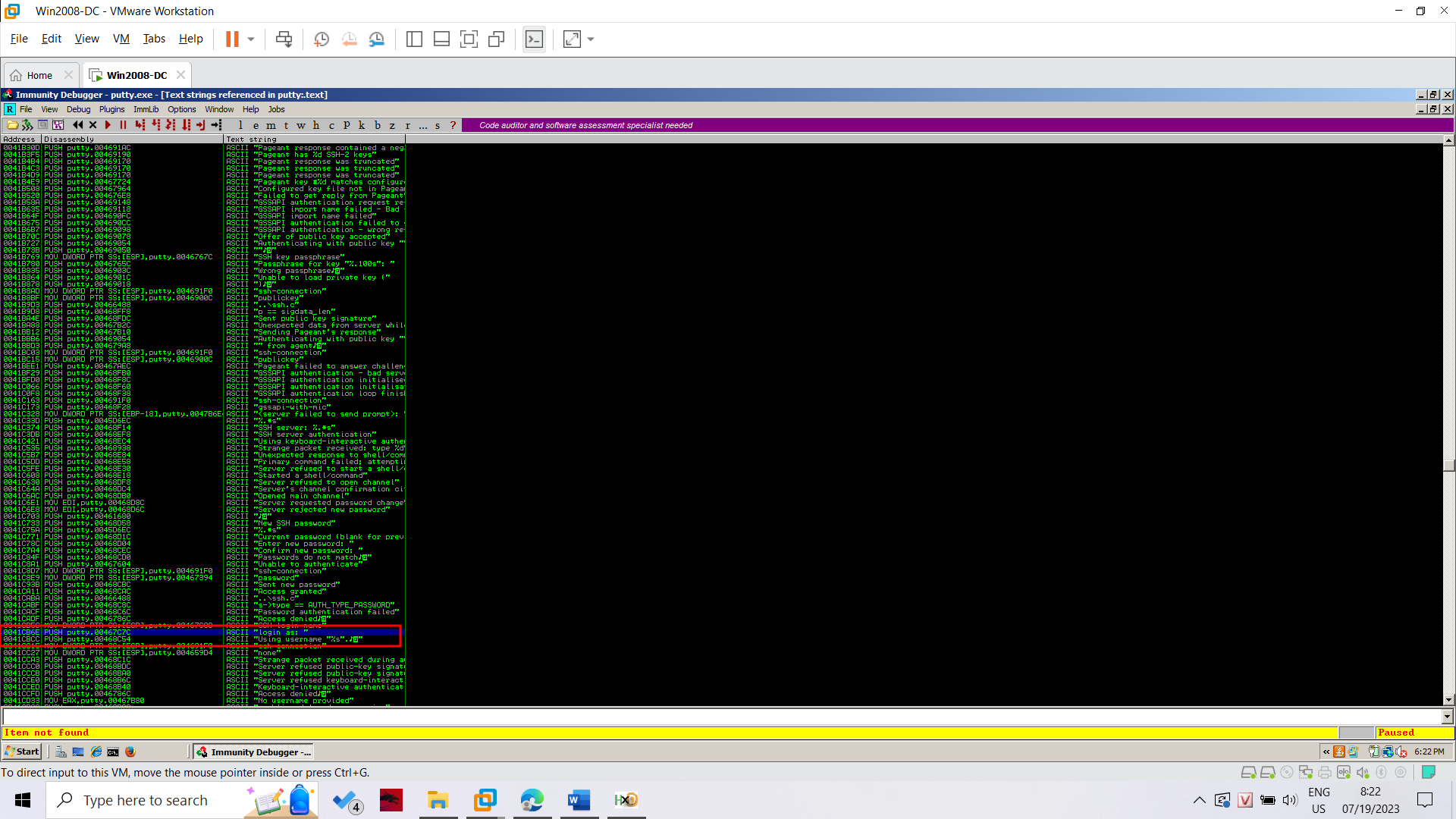


Click OK.

Immunity finds the ASCII string "login as", and the instruction that uses it, as shown below. This instruction is at address 00417053

Right-click again, and click "Search next".

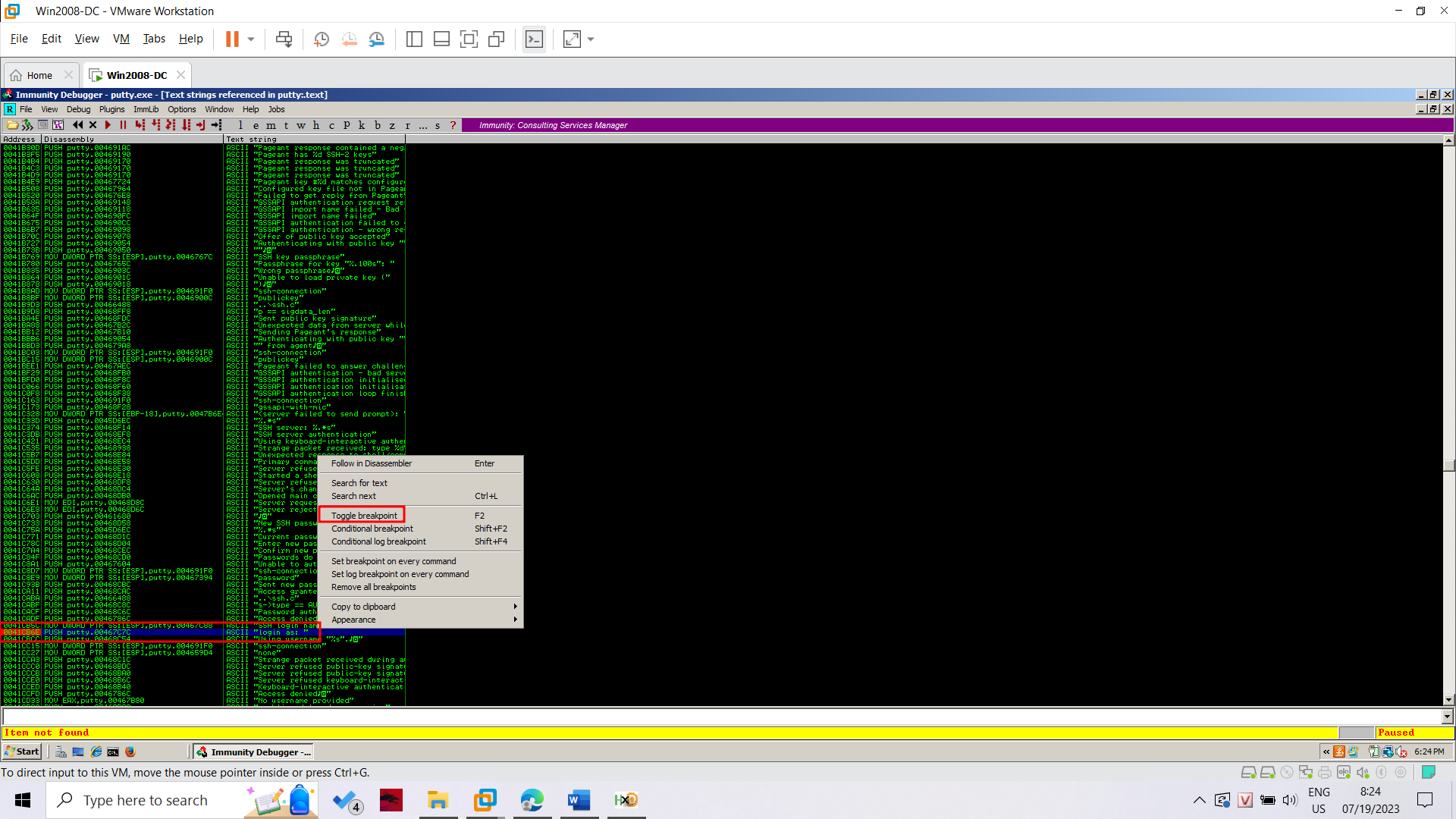
Immunity finds another line of code that uses this string, as shown below. This instruction is at address 0041CB6E.



Using Breakpoints

We'll set a breakpoint at this instruction, at address 0041CB6E.

On your keyboard, press the F2 key. Mac users, press fn+F2. The address turns red, as shown below, to indicate that there's a breakpoint here.

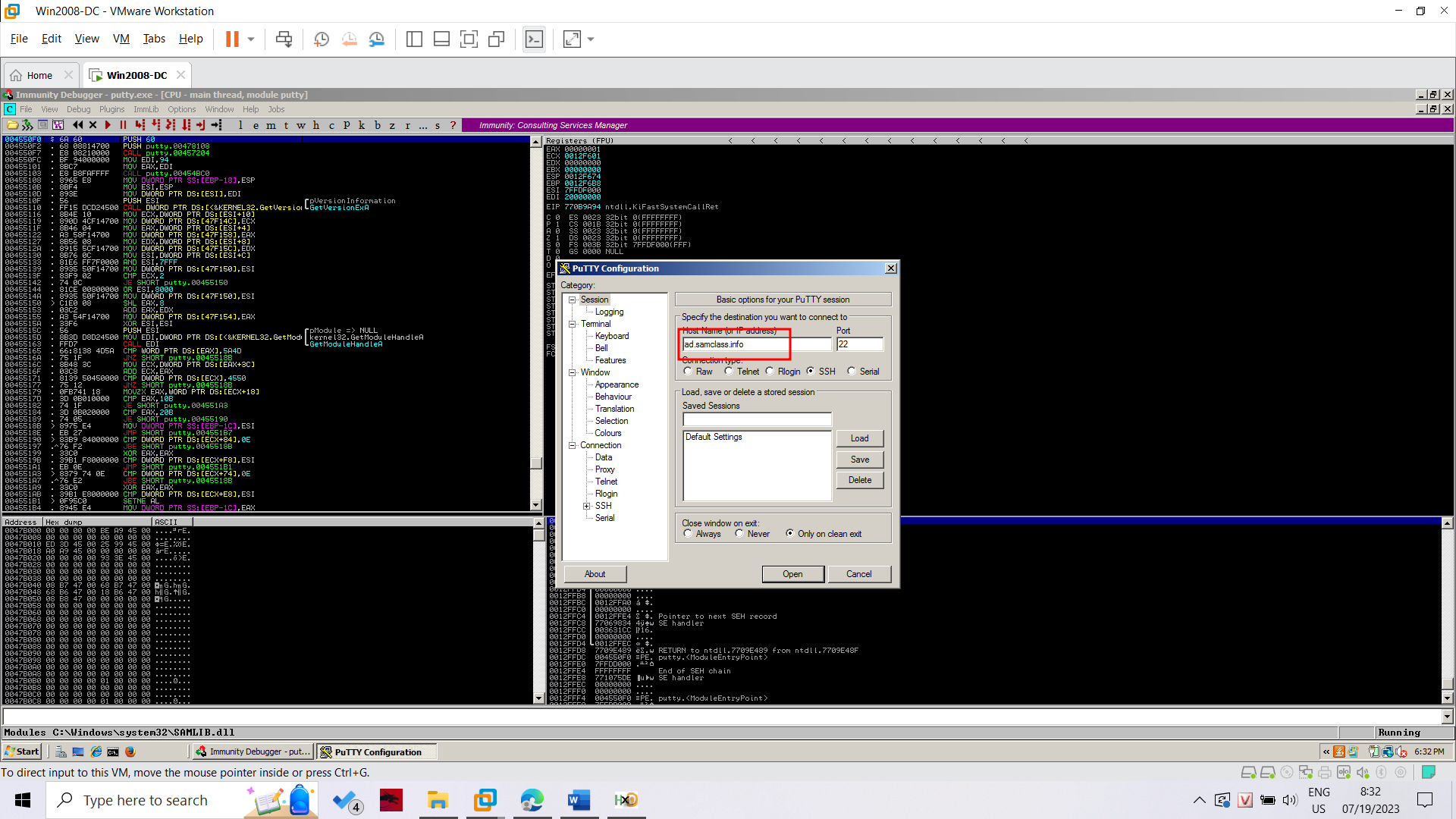


In Immunity, from the menu bar, click Debug, Restart.

A box pops up warning you that "Process 'putty' is active". Click Yes.

In Immunity, from the menu bar, click Debug, Run.

A Putty window opens, as shown below.



**Task 2: Alter the Login Message**

Removing the Breakpoint

We don't need the breakpoint any more, so we'll remove it.

In Immunity, from the menu bar, click View, Breakpoints.

A "Breakpoints" window opens, showing the breakpoint.

Right-click the breakpoint and click Remove, as shown below.

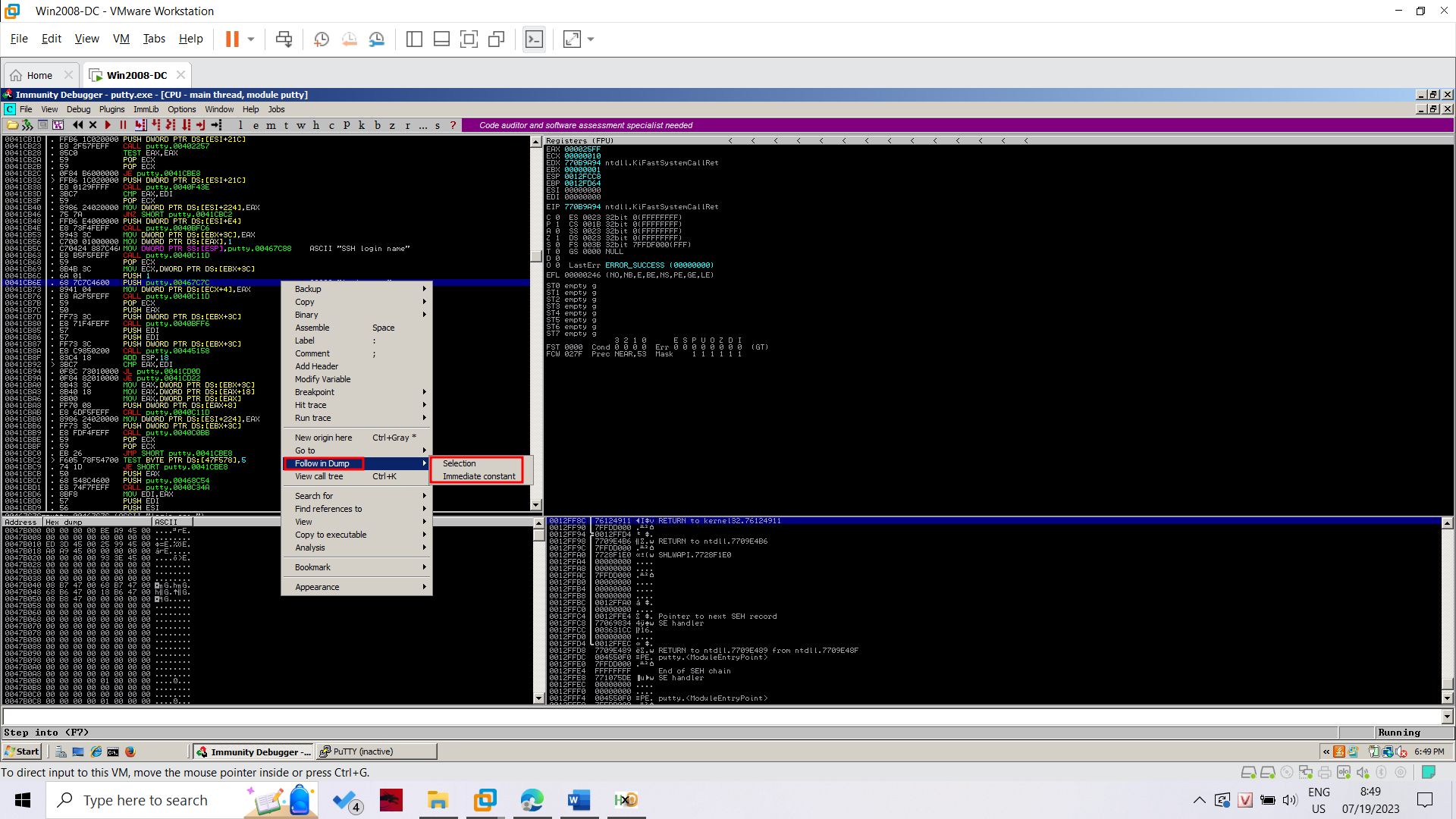


Viewing the Stored Message

In Immunity, in the CPU window, in the Assembly Code pane, right-click the intruction at address 0041CB6E and click "Follow in Dump", "Immediate constant", as

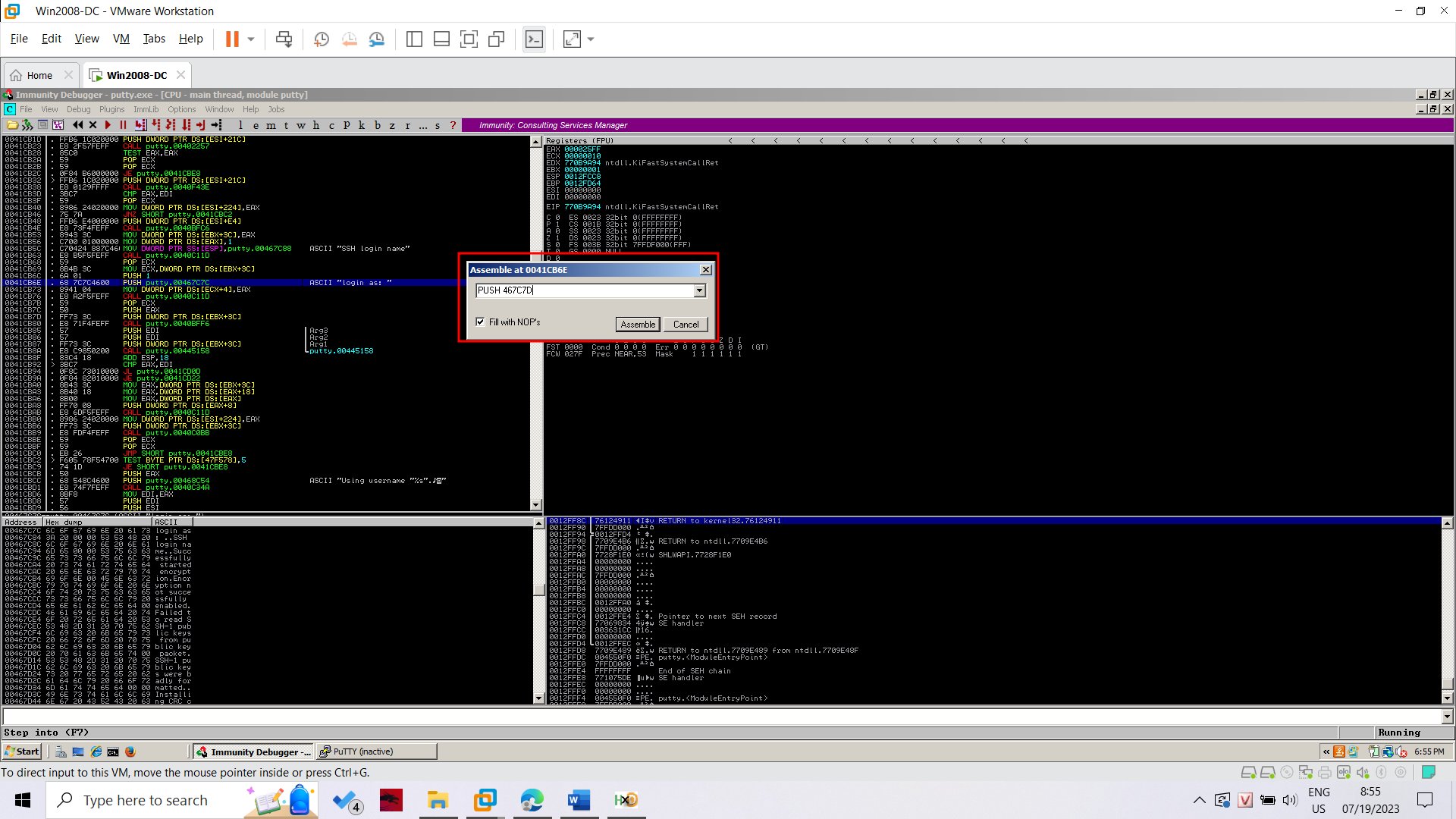
shown below.

The lower left pane shows the stored "login as" message, in hexadecimal and ASCII text



Skipping the First Letter In the Message

In Immunity, in the CPU window, in the Assembly Code pane, right-click the intruction at address 0041CB6E and click Assemble, as shown below.



An "Assemble at 0041CB6E" box appears, as shown below.

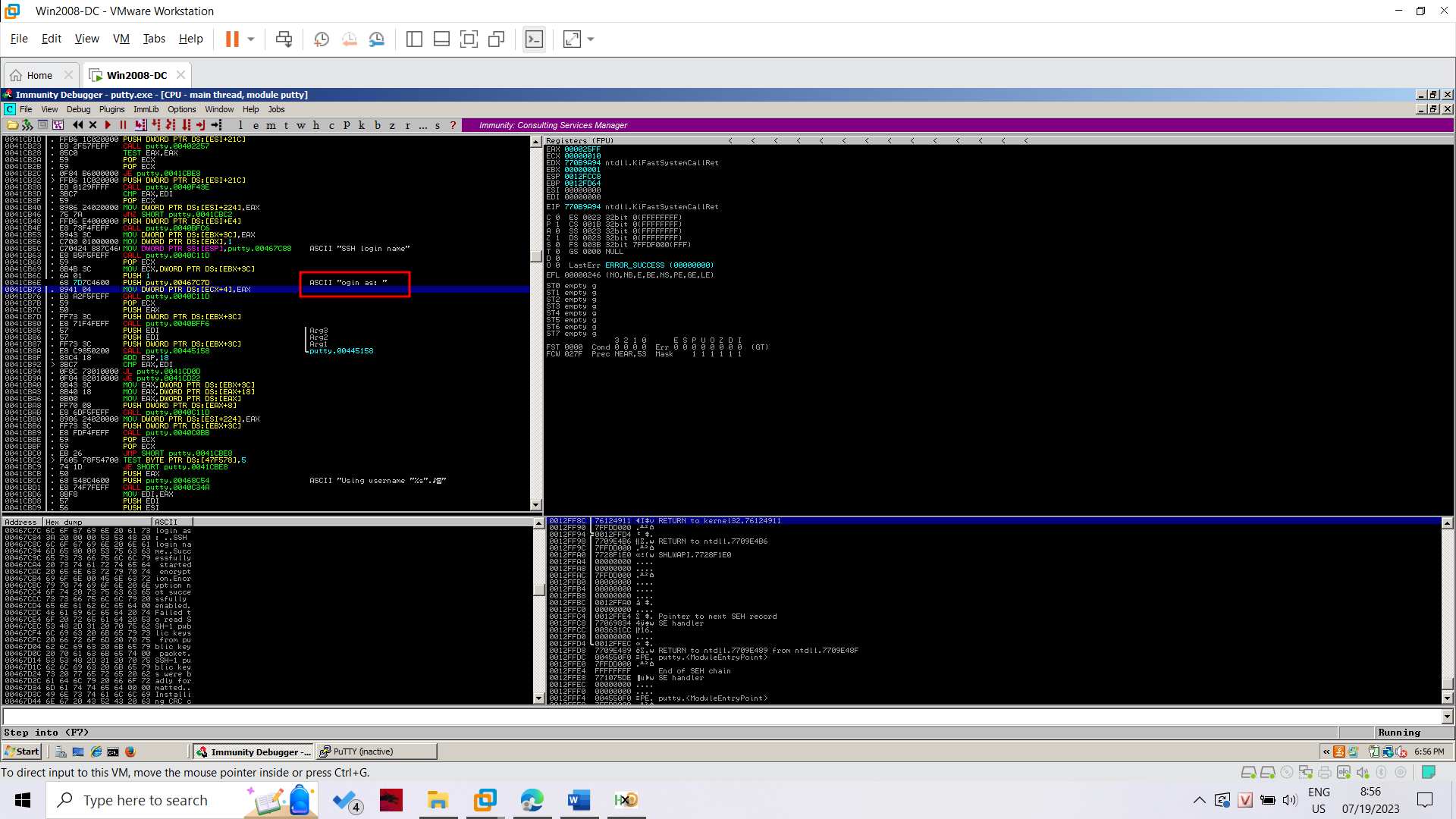
This shows the command at this location. It's a PUSH instruction, placing the address 467C7C onto the stack. That address points to the letter "l" in the ASCII string "login

as: ", as shown on the right side of the instruction line, outlined in green in the image below.

Click the Assemble button.

Click the Cancel button.

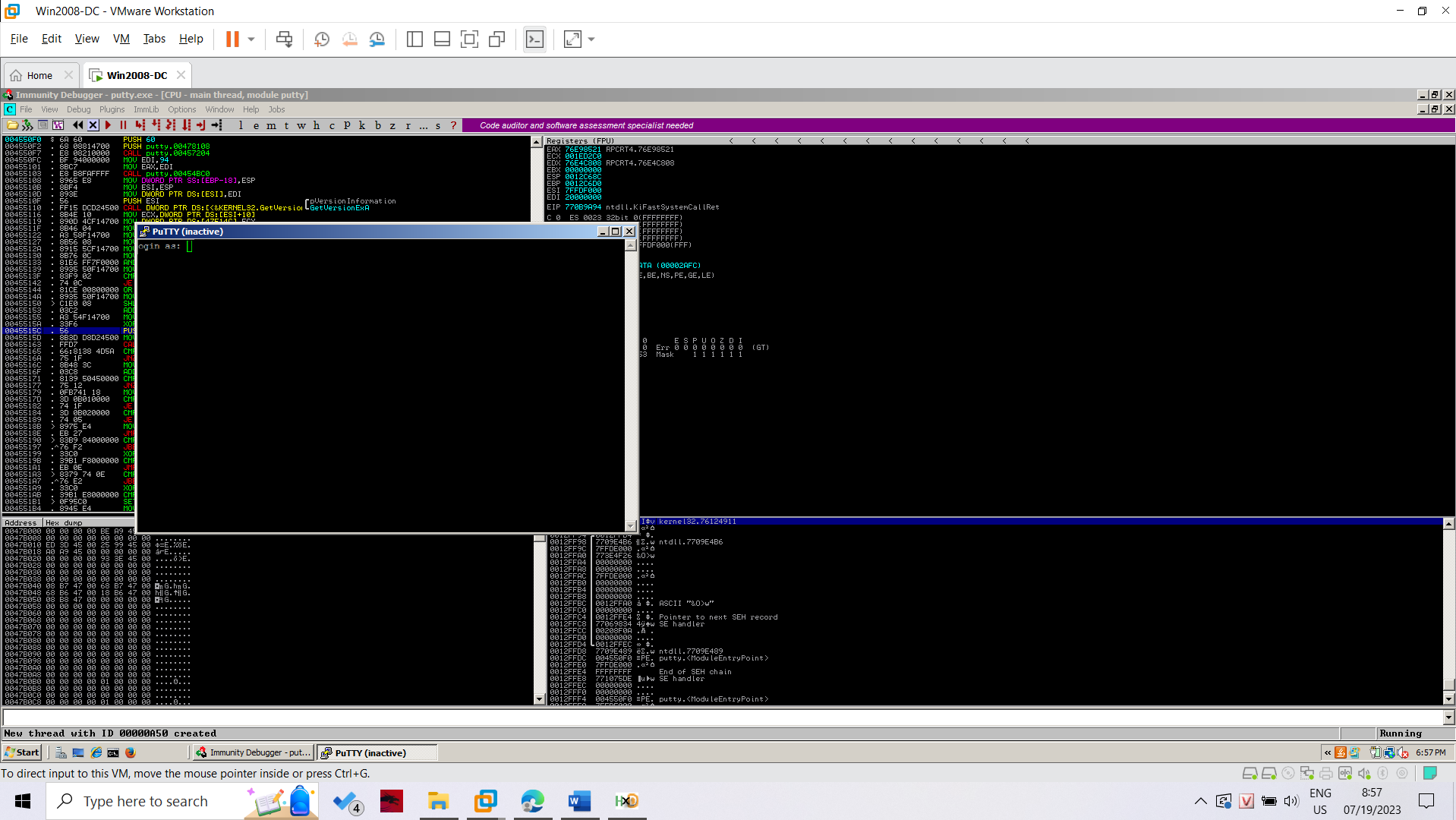
The message on the right now says "ogin as: ", as shown below.



Running the Modified Program

In Immunity, from the menu bar, click Debug, Run.

The black login window appears, with the message "ogin as: ", as shown below.



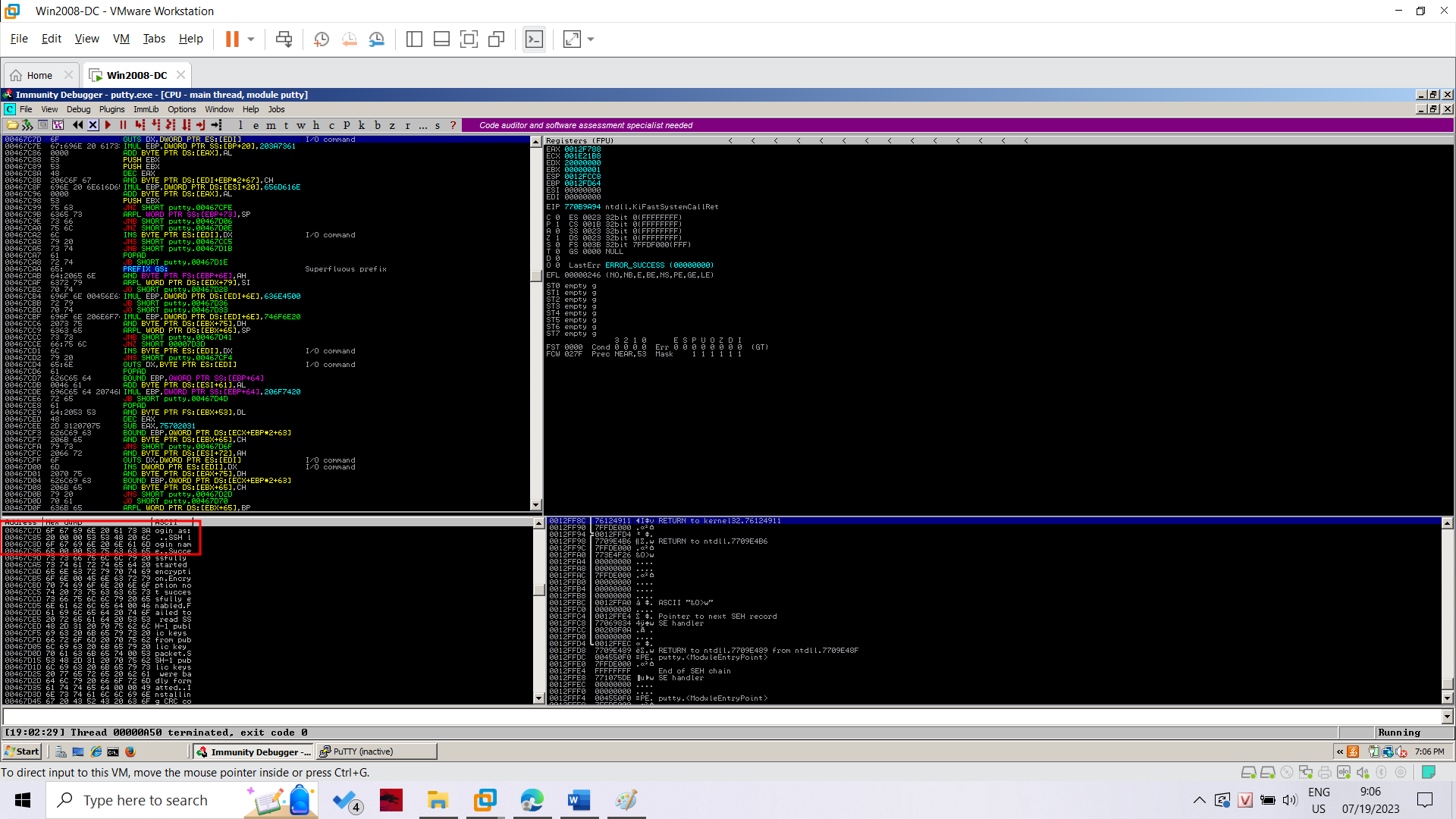
Inserting Your Name

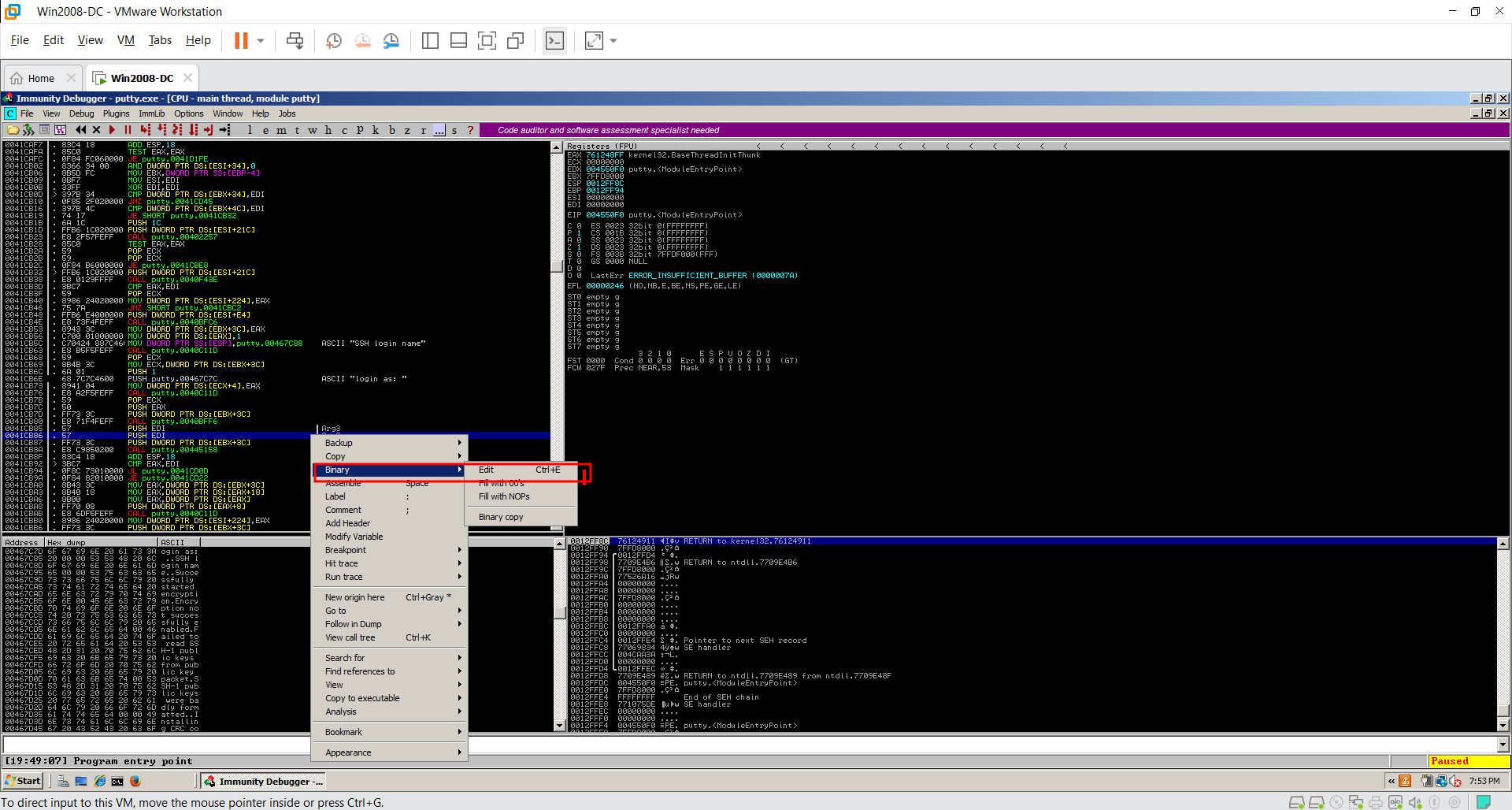
Now we want to change the text from "ogin as: " to your name.

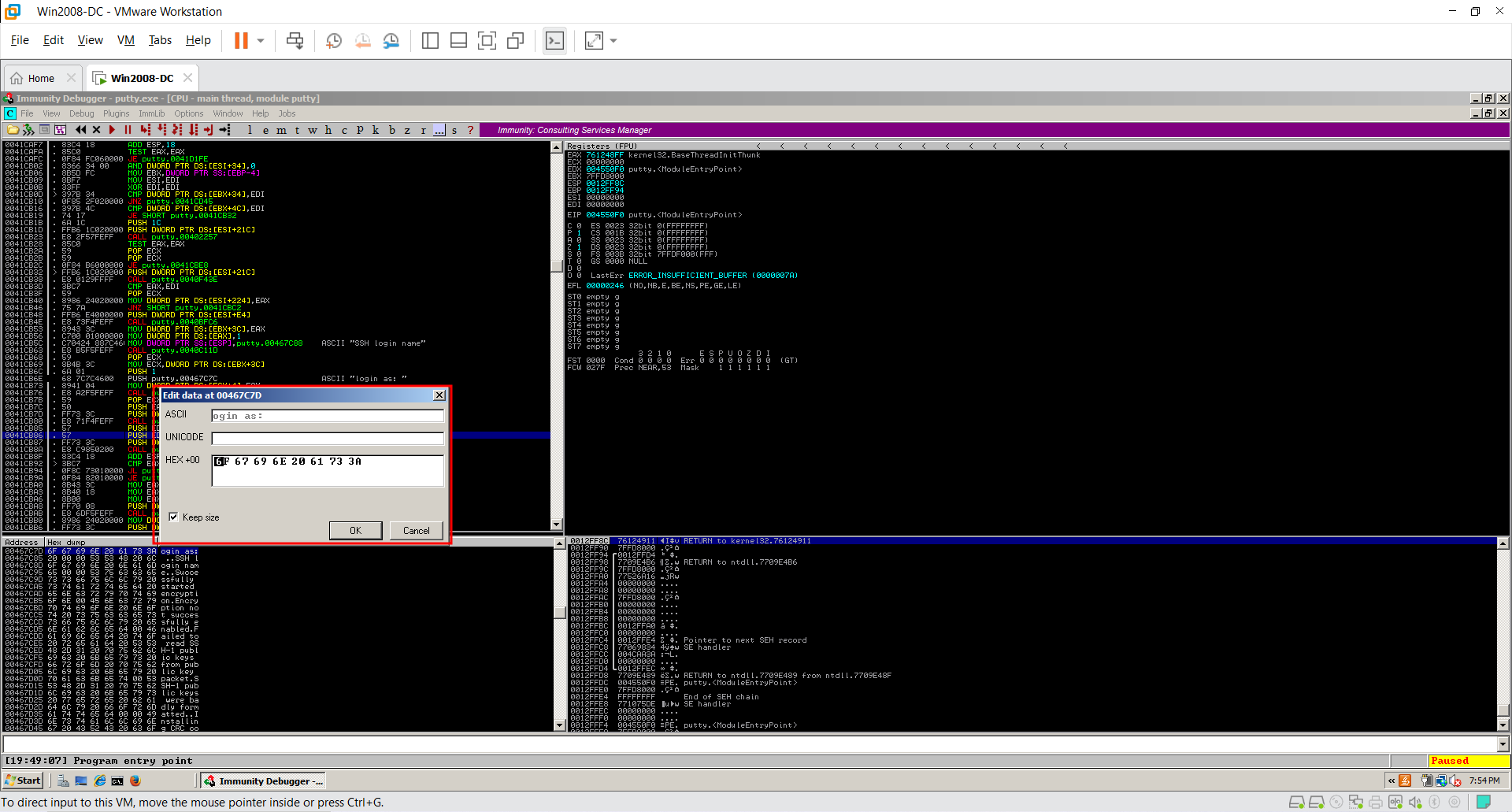
Move your mouse into the lower left pane of the CPU window, which is the "hex dump" pane.

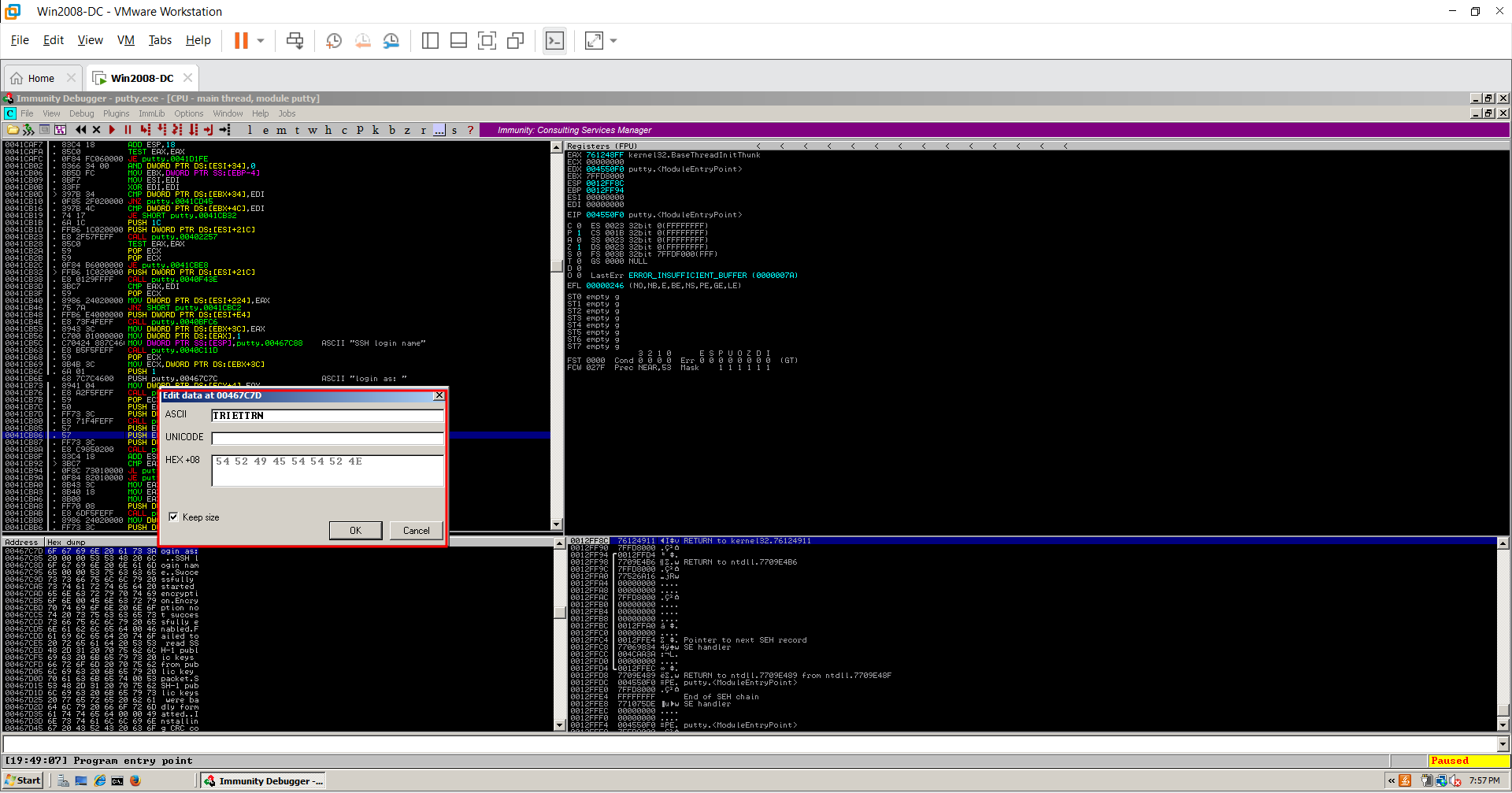
Right click, point to "Go to", and click Expression, as shown below.

Enter 467C7D into the box, as shown below. Click OK









Saving the Modified EXE

In Immunity, in the lower left pane of the CPU window, right-click and click "Copy to Executable File", as shown below.

