Purpose To modify a Windows EXE file and save an altered version.

This gives you practice with very simple features of the Ollydbg debugger

Task 1: Target EXE Recon

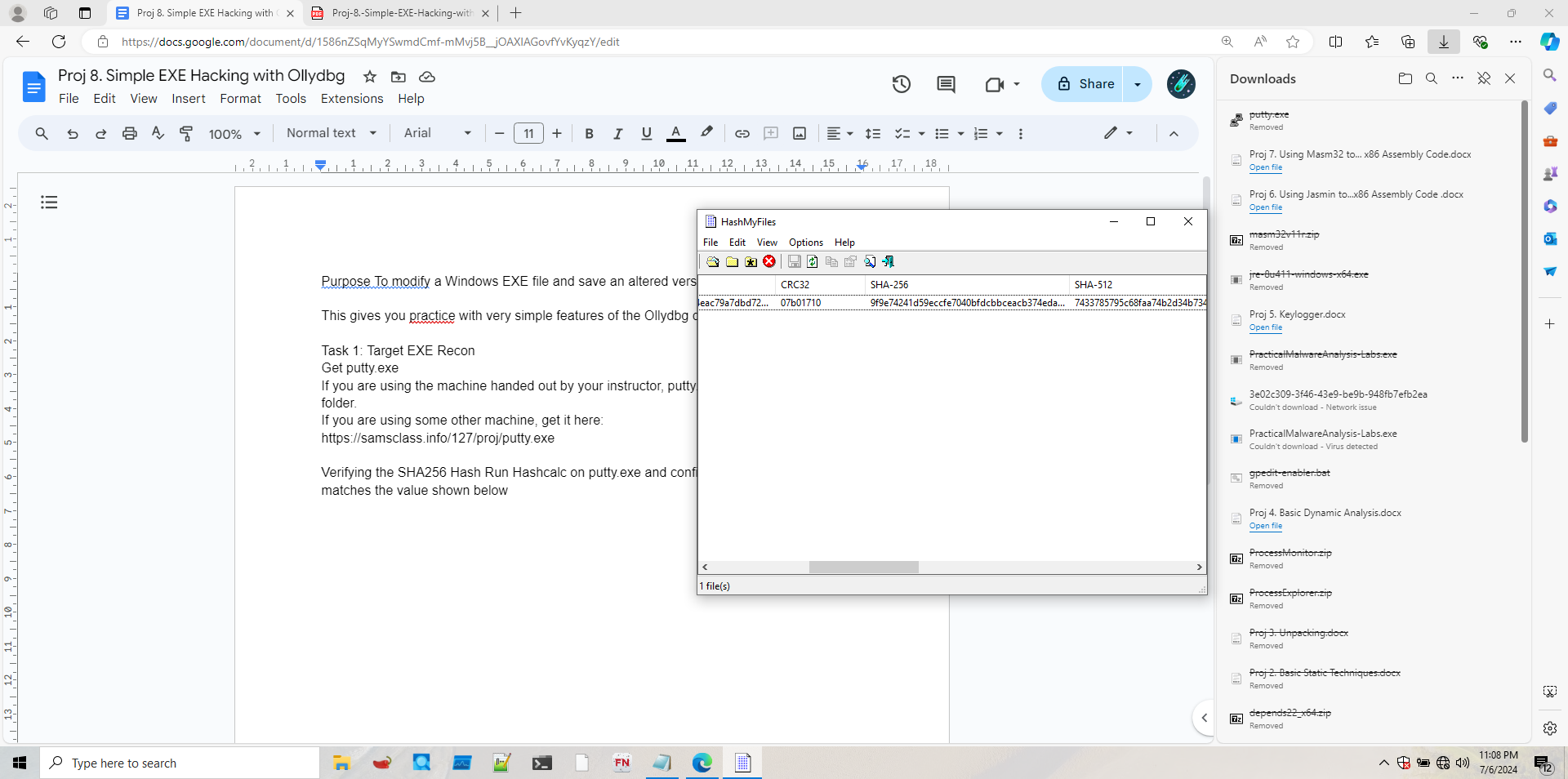
Get putty.exe

If you are using the machine handed out by your instructor, putty.exe is in the Downloads folder.

If you are using some other machine, get it here:

https://samsclass.info/127/proj/putty.exe

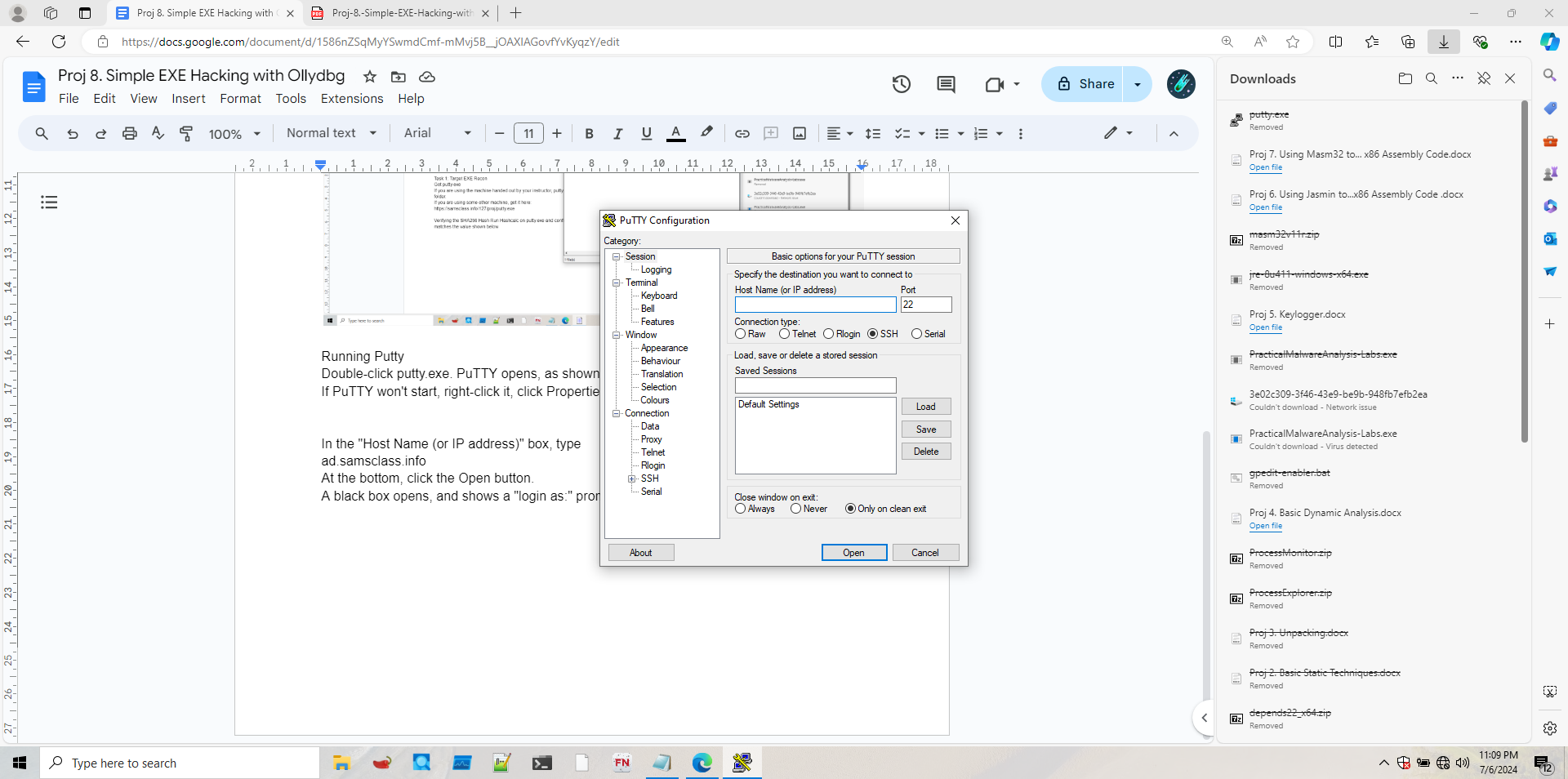
Verifying the SHA256 Hash Run Hashcalc on putty.exe and confirm that the SHA256 value matches the value shown below



Running Putty

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

If PuTTY won't start, right-click it, click Properties, and click Unblock

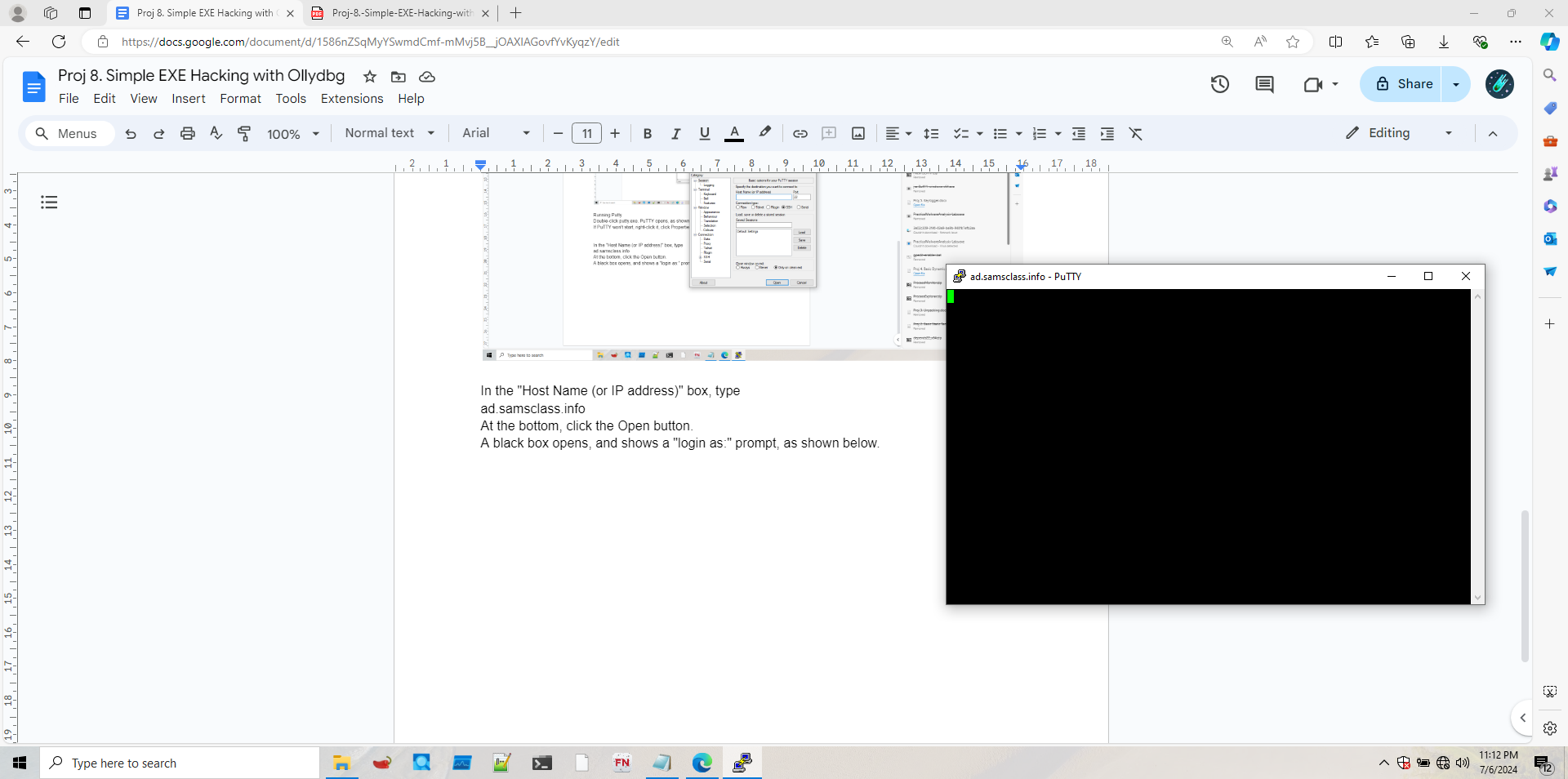


In the "Host Name (or IP address)" box, type

ad.samsclass.info

At the bottom, click the Open button.

A black box opens, and shows a "login as:" prompt, as shown below.

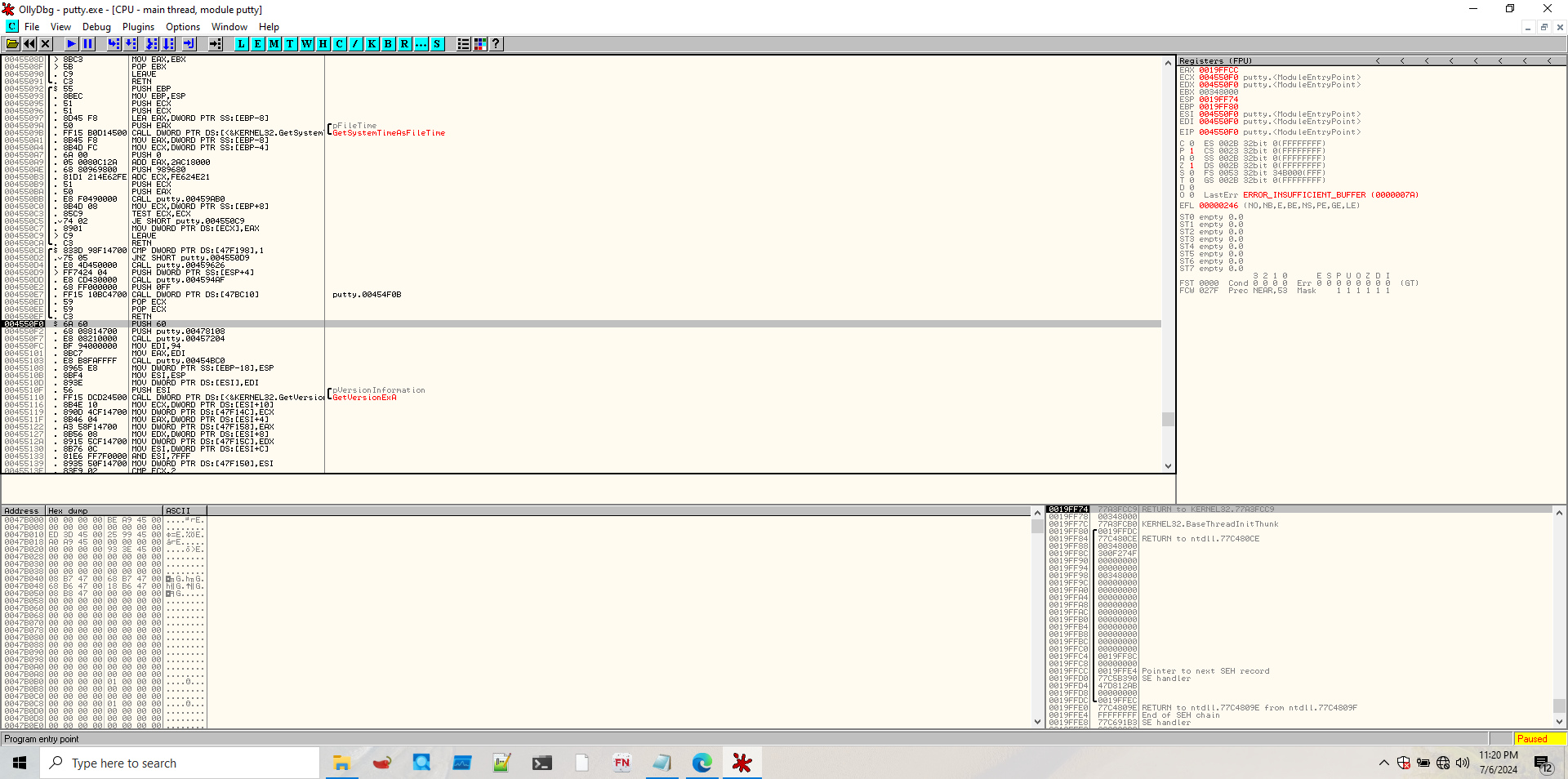


Starting Ollydbg

Click Start. Search for Ollydbg and start it.

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

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



Ollydbg 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.

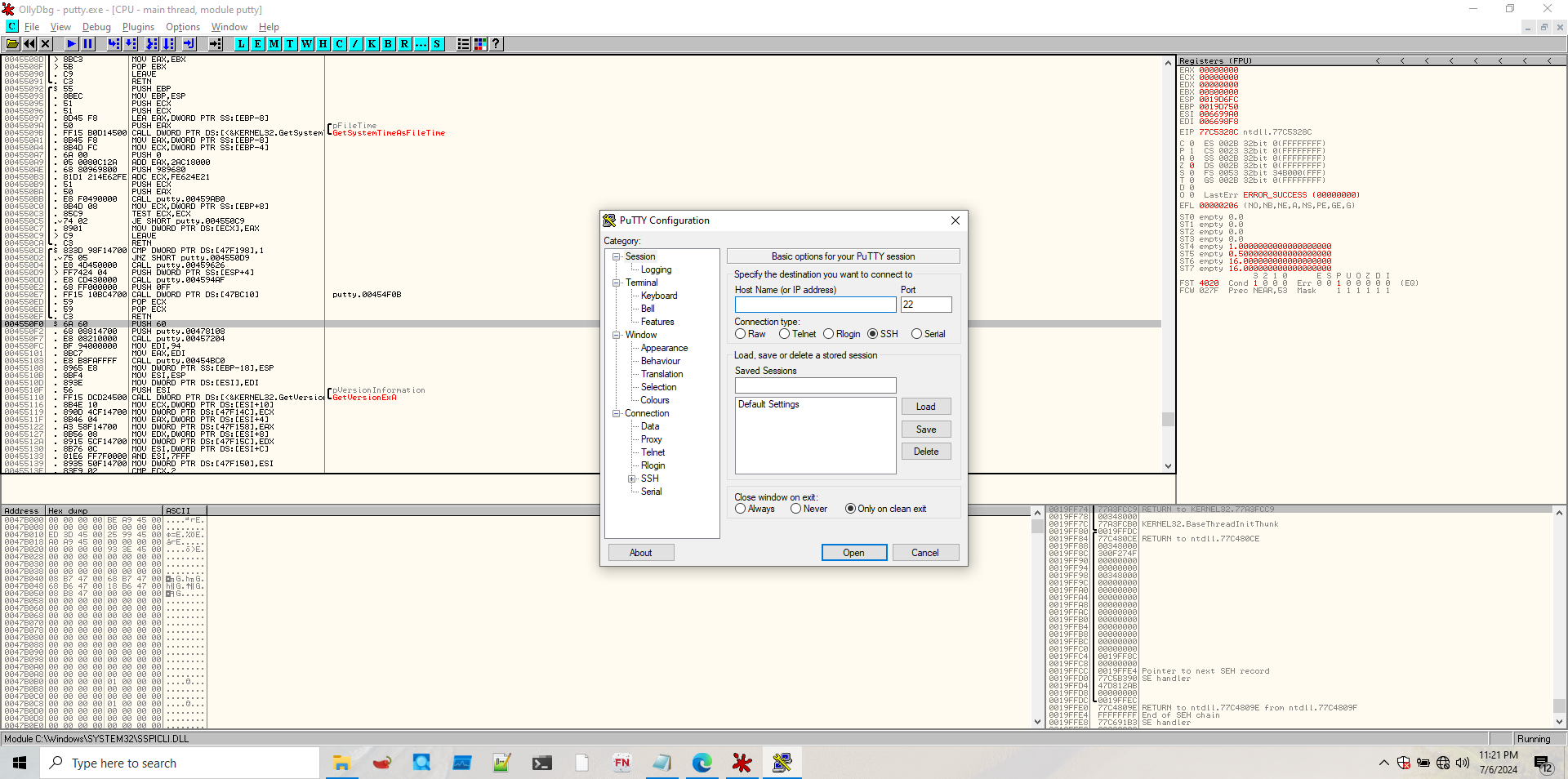
When you load a program into Ollydbg, it starts in a "Paused" state, with the Assembly Code window showing the first instruction.

Running Putty in Ollydbg

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

A Putty window opens, but it's behind the Olly window. At the bottom of the screen, in the taskbar, click the "PuTTY Configuration" button to

bring the PuTTY window to the front, as shown below



Click in the Putty window. In the "Host Name (or IP address)" box, type

ad.samsclass.info

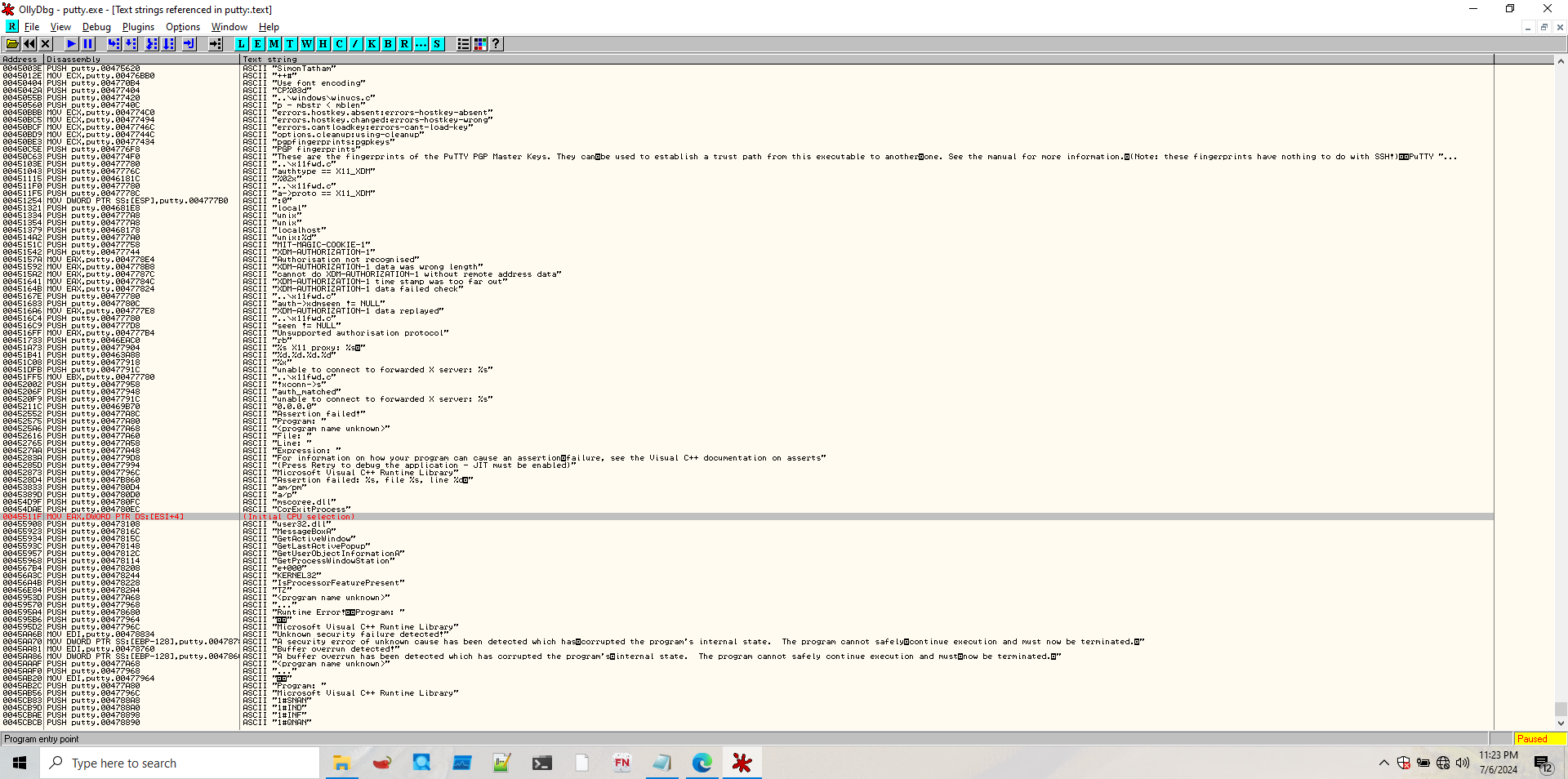
At the bottom, click the Open button. The "login as" message appears, as shown below

Finding the "login as" Code

Close the Putty window. A box asks "Are you sure..." Click OK.

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

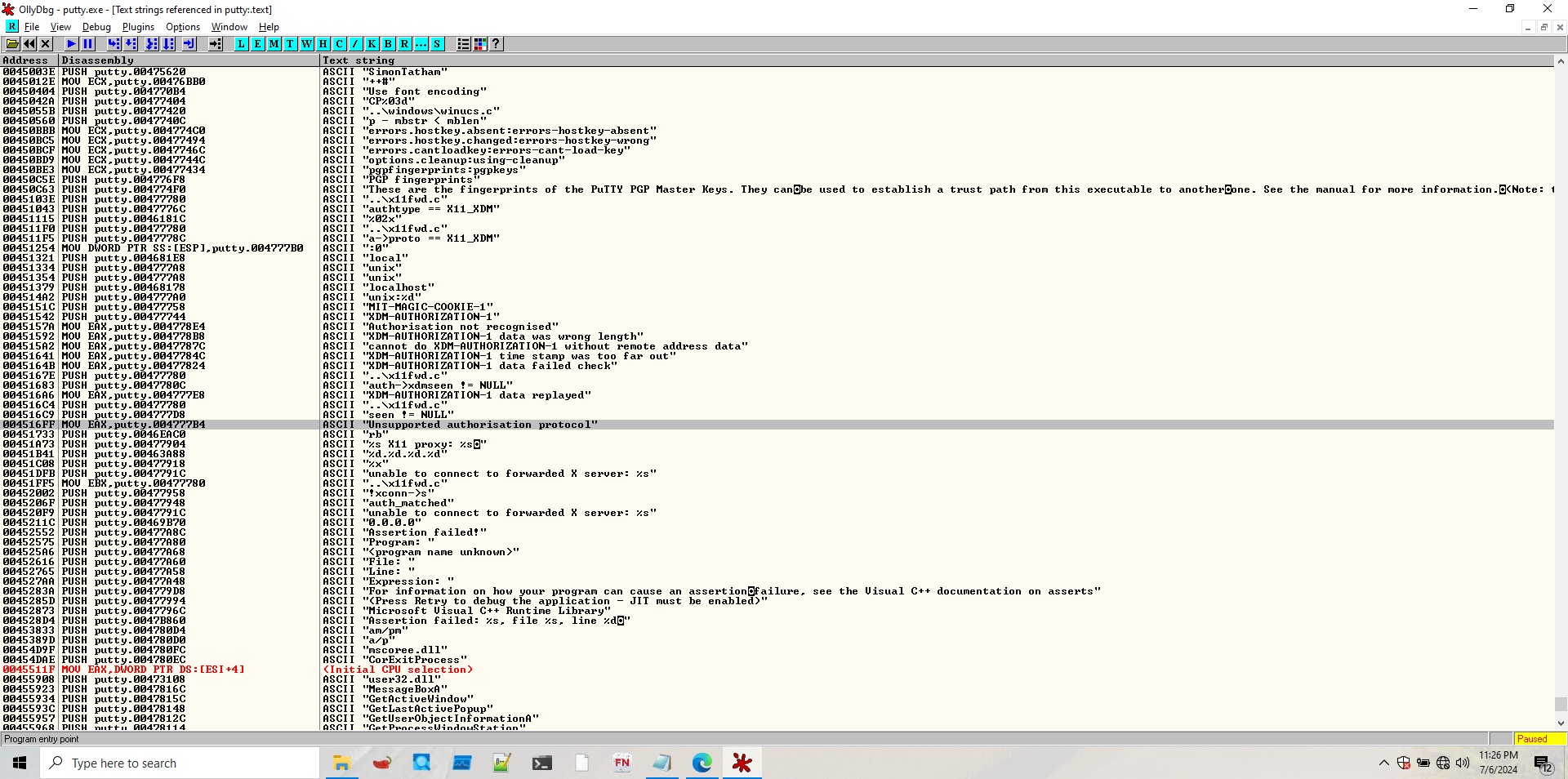
In Ollydbg, in the "Assembly Code" pane, right-click. Point to "Search for". Click "All referenced text strings", as shown below



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

To make this text easier to read, right-click, point to Appearance, Font, and click "OEM Fixed Font".

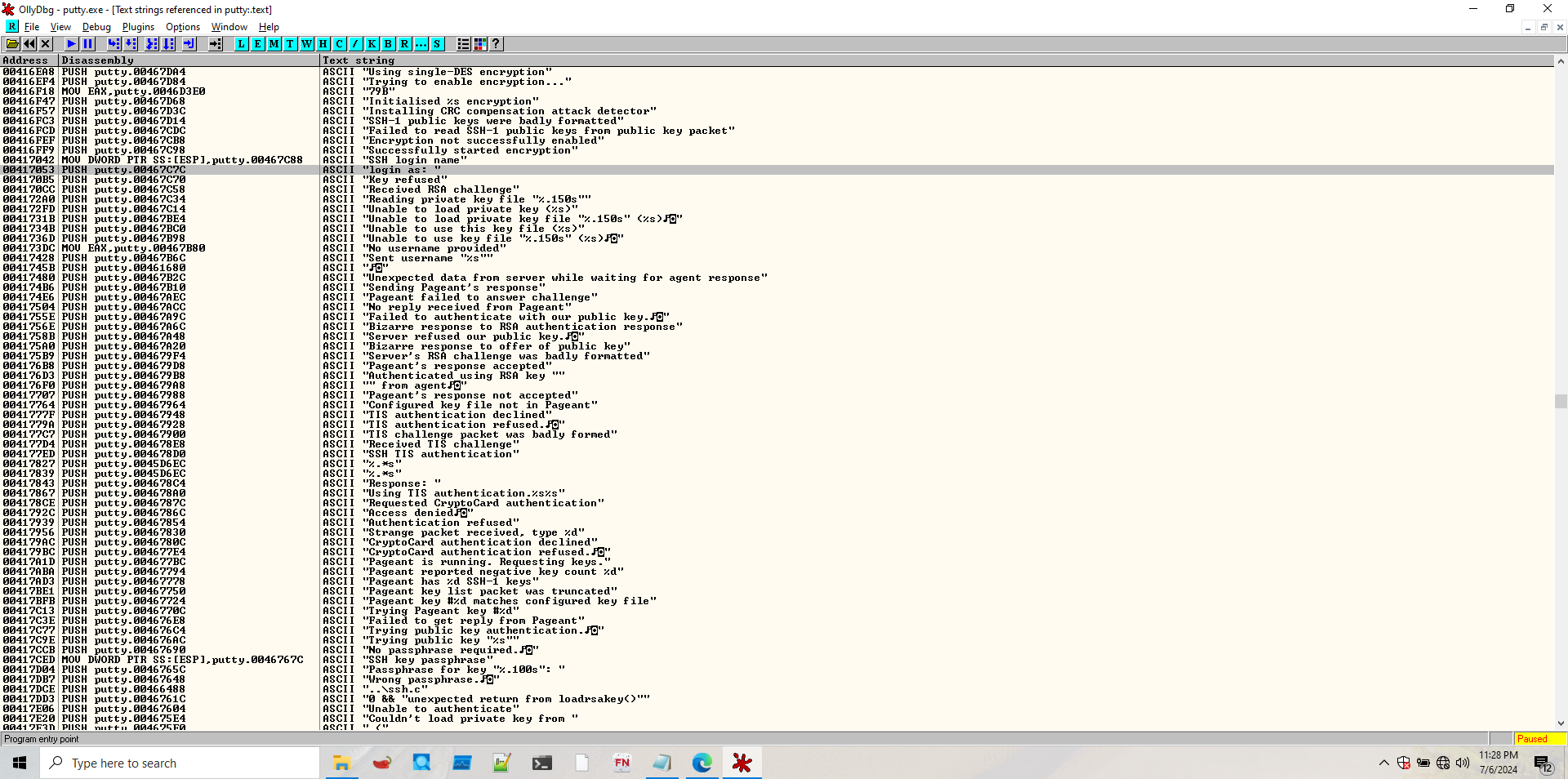
Right-click in that window, and click "Search for text", as shown below.



In the "Enter text to search for" box, type

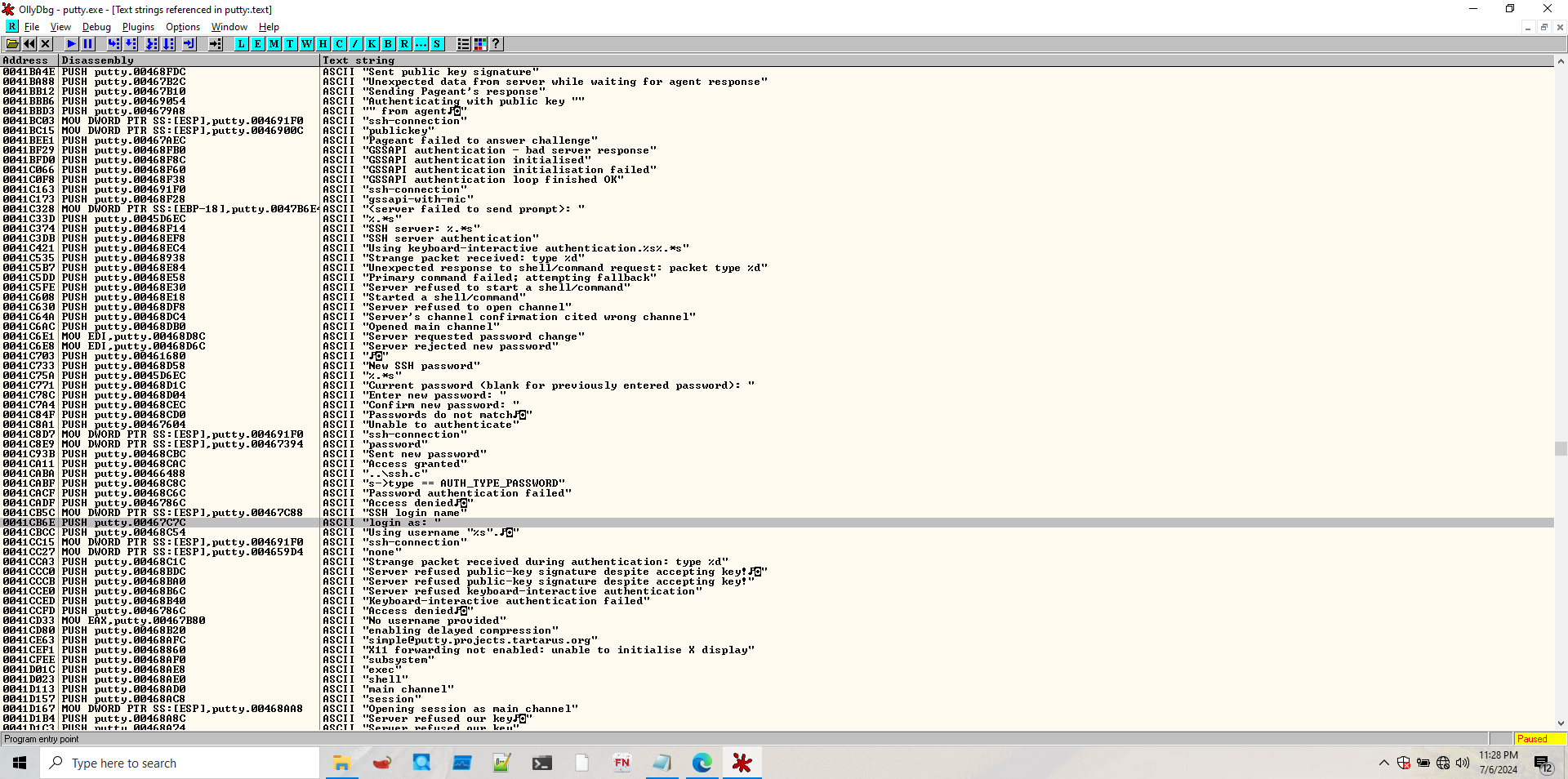
login as

as shown below. Check the "Entire scope" box.



This instruction is at address 00417053

Right-click again, and click "Search next". Ollydbg finds another line of code that uses this string, as shown below. This instruction is at address 0041CB6E

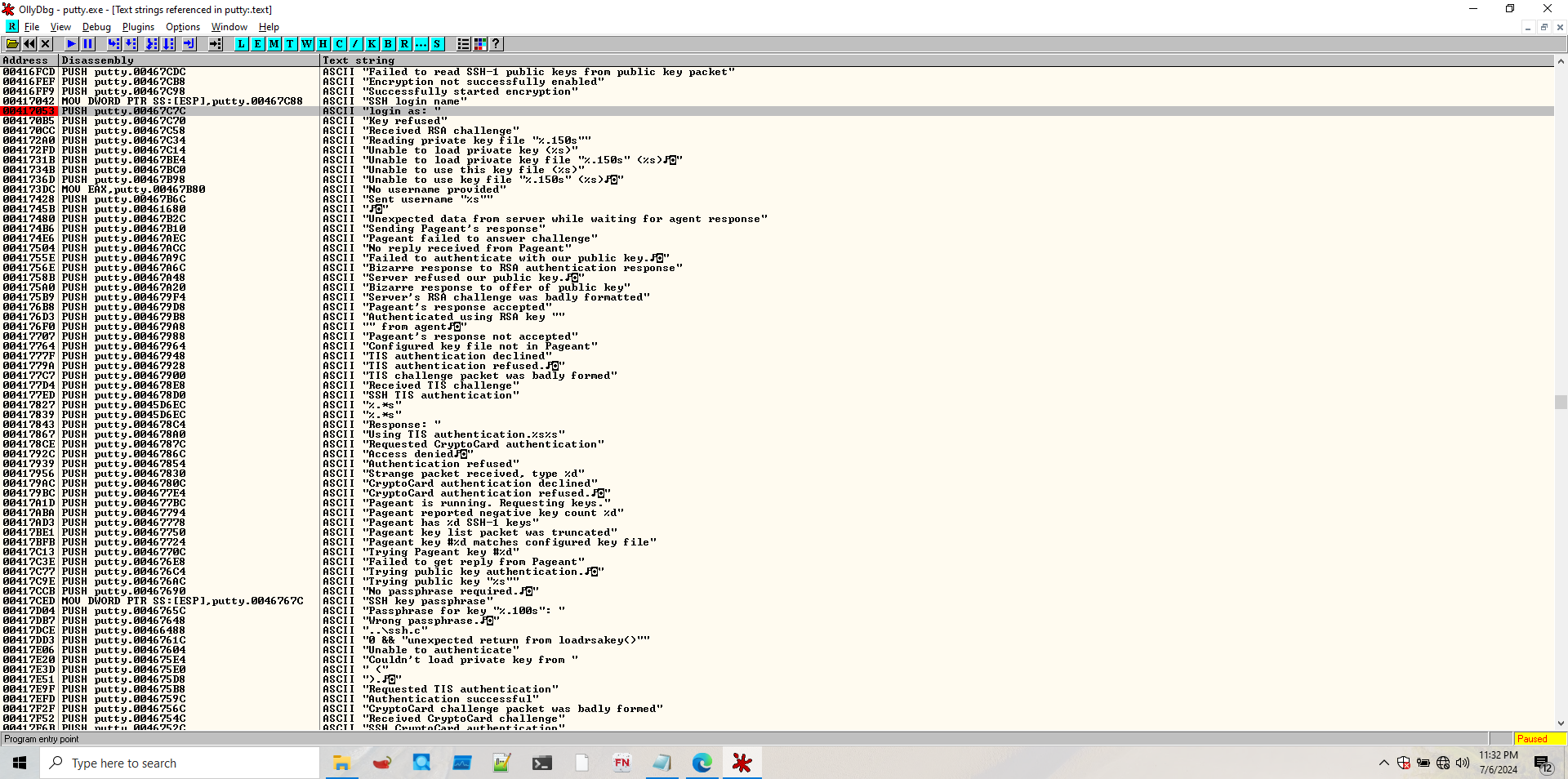


Using Breakpoints

We'll set breakpoints at those instructions to see which one is used when logging in to an SSH server.

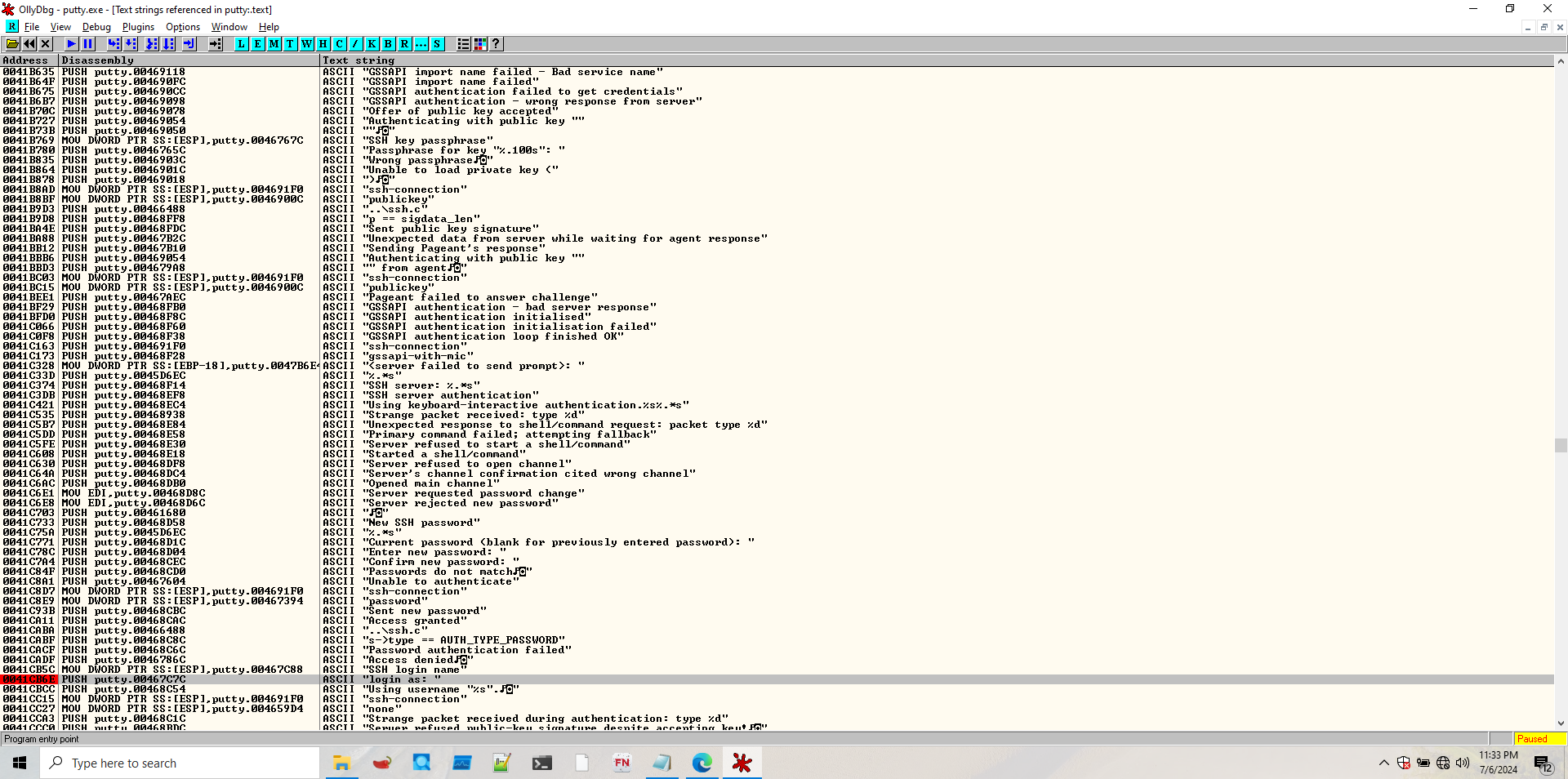
In the "Text strings referenced in putty:.text" window, right-click again, and click "Search text". In the "Enter text to search for" box, click OK.

The instruction at 00417053 appears again. Right-click this instruction and click "Toggle breakpoint", as shown below



Right-click again, and click "Search next". The instruction at address 0041CB6E appears. Right-click it and click "Toggle breakpoint".

The address turns red, as shown below



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

A Putty window opens. Bring it to the front, as shown below

Click in the Putty window. In the "Host Name (or IP address)" box, type

ad.samsclass.info

At the bottom, click the Open button.

A black window opens and closes quickly, and the program stops, as shown below

Task 2: Alter the Login Message

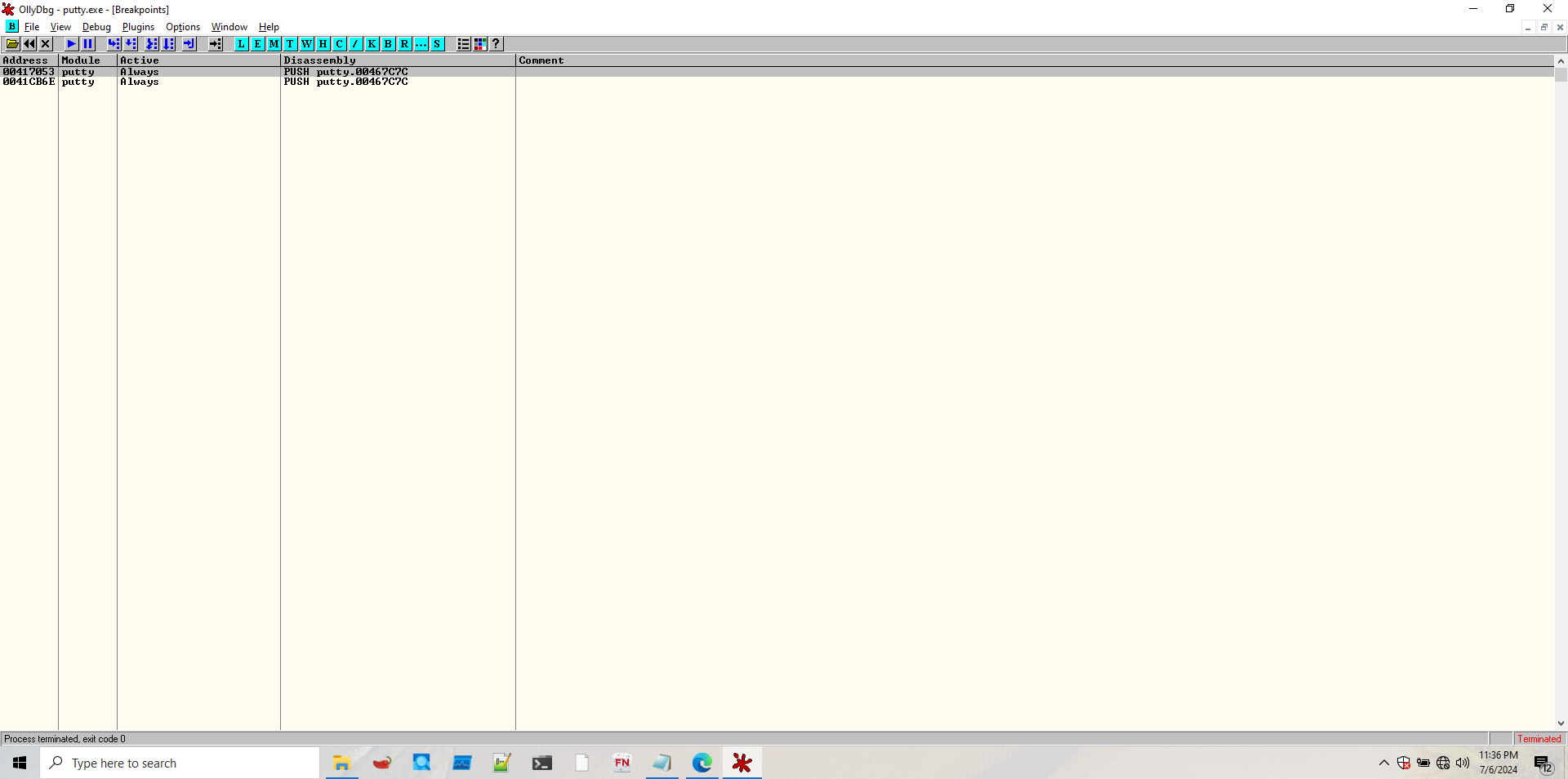
Removing the Breakpoints

We don't need the breakpoints any more, so we'll remove them.

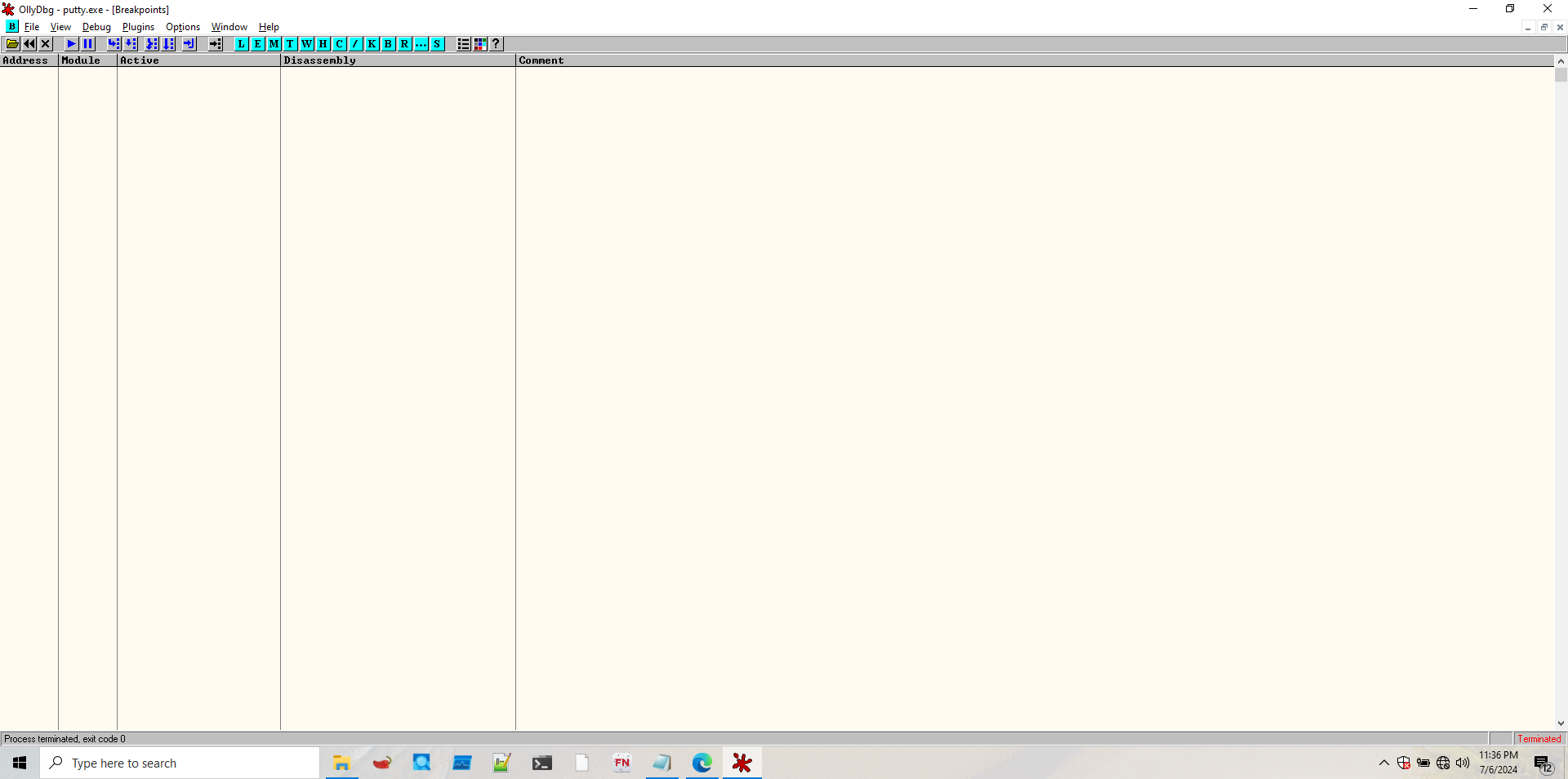
In Ollydbg, from the menu bar, click View, Breakpoints.

A "Breakpoints" window opens, showing two breakpoints.

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



Repeat the process to remove the other breakpoint. Close the "Breakpoints" window



Removing One Letter From the Message

In Ollydbg, in the CPU window, in the Assembly Code pane, right-click the instruction at address 0041CB6E and click Assemble, as shown

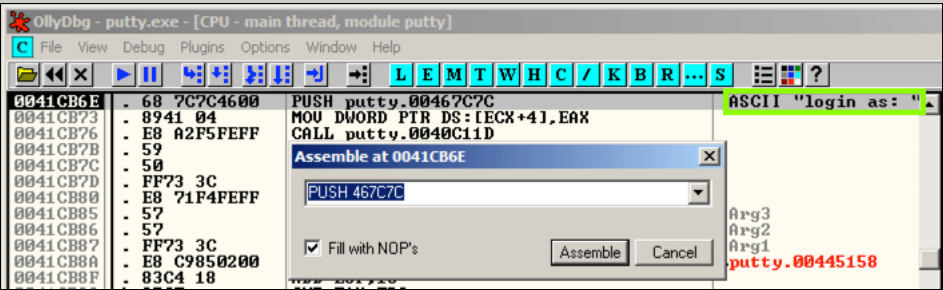
below



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

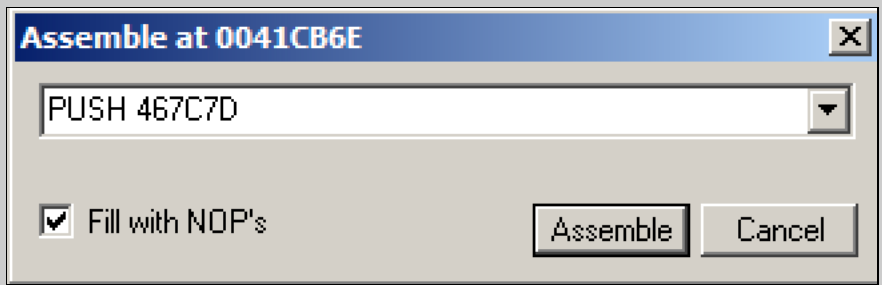
This shows the command at this location. It's a PUSH instruction, placing the address 467C7C onto the stack. That address points to the

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



In the "Assemble at 0041CB6E" box, change the last character to D, as shown below. This will move the pointer from the "l" to the "o" in the

string "login as: "



Click the Assemble button.

Click the Cancel button.

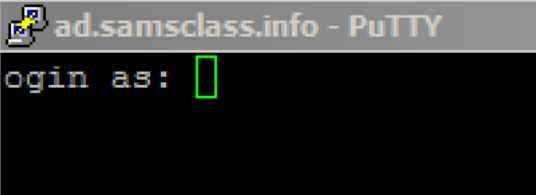
The message on the right now says "ogin as: ", as shown below.



Running the Modified Program

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

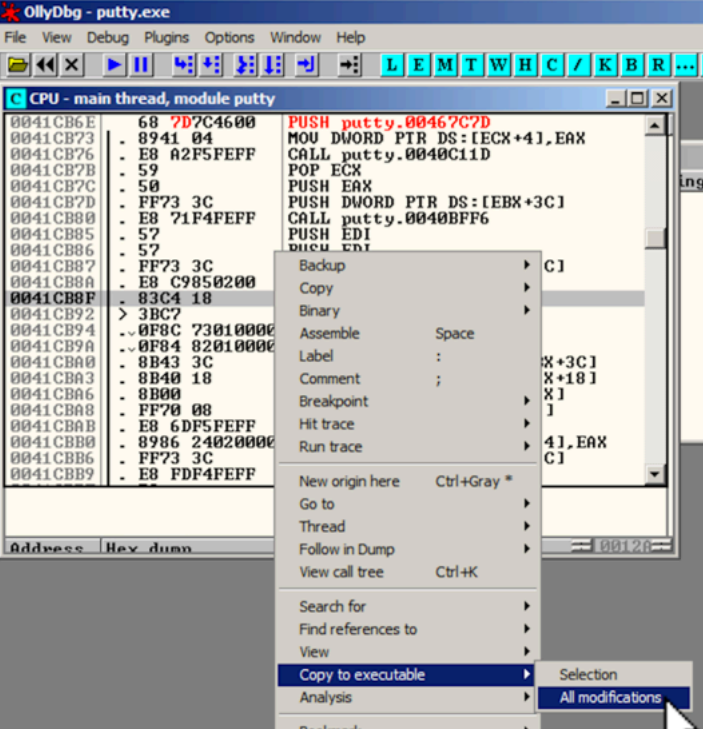
The black login window appears, with the message "ogin as: ", as shown below



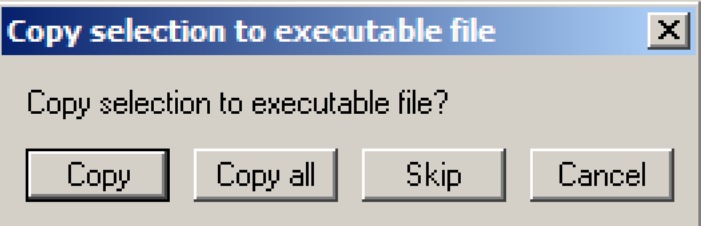
Saving the Modified .text Section

We have now changed an assembly language instruction; all executable code is in the .text section of the file.

In Ollydbg, in the top left pane of the CPU window, right-click, point to "Copy to Executable", and click "All modifications", as shown below



A "Copy selection to executable file" box pops up, as shown below. Click the "Copy all" button.



Save the file as puttymod.exe.

Running the Modified EXE

Close Ollydbg.

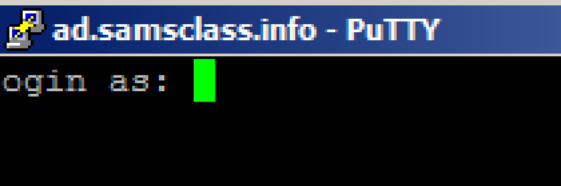
Double-click puttymod.exe.

In the "Host Name (or IP address)" box, type

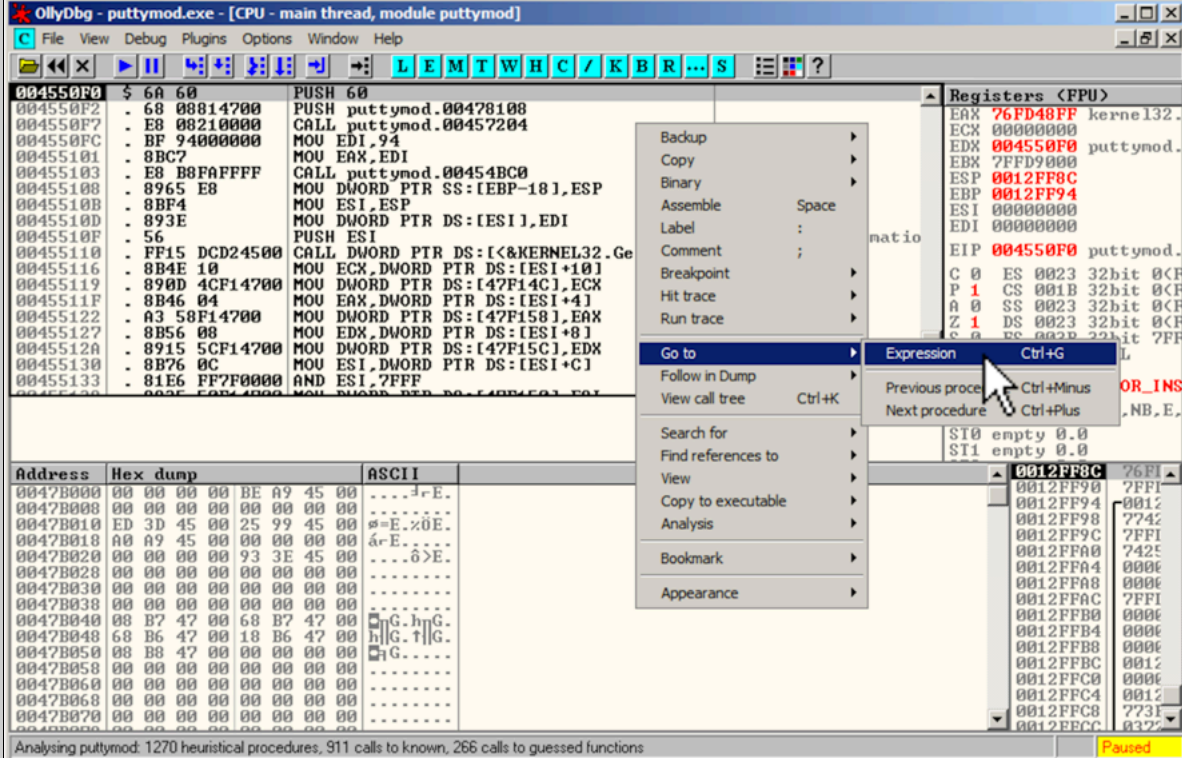
ad.samsclass.info

At the bottom, click the Open button.

A black box opens, and shows a "ogin as:" prompt, as shown below



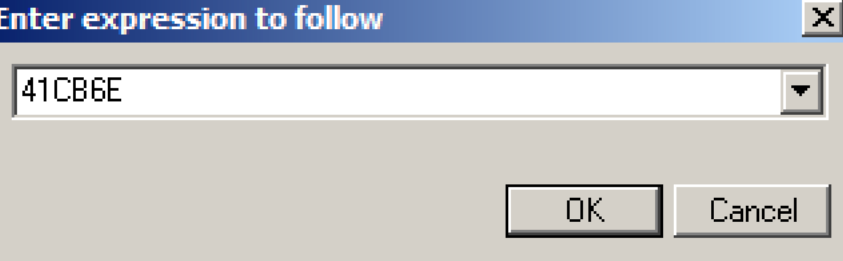
Modifying the puttymod File Open Ollydbg and load the puttymod.exe file. In the top left pane of the CPU window, right-click, point to "Go to", and click Expression, as shown below



In the "Enter expression to follow" box, enter

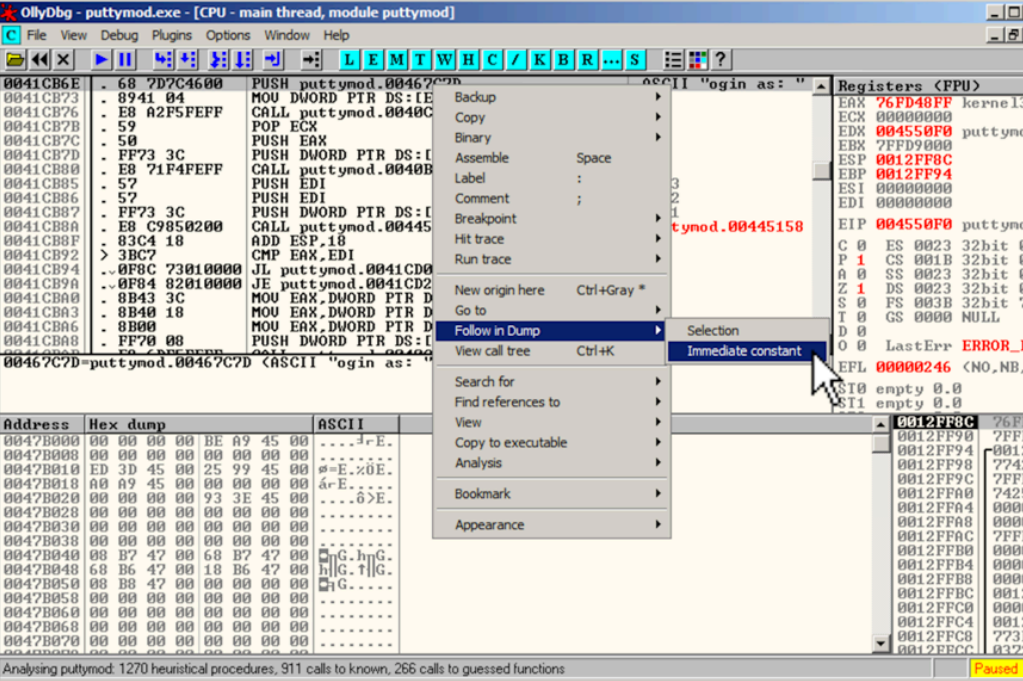
41CB6E

as shown below. Click OK



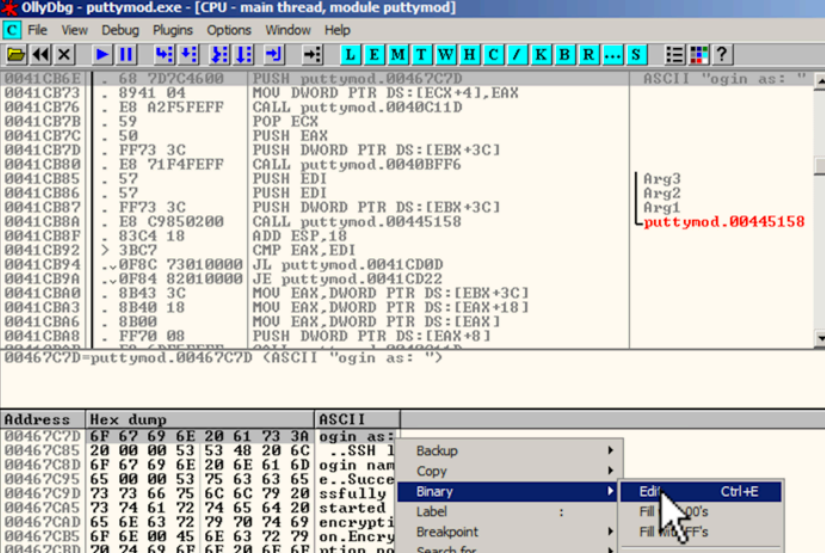
Changing the Login Message

In the top left pane of the CPU window, right-click 00467C7D, as shown below. Point to "Follow in Dump" and click "Immediate constant"

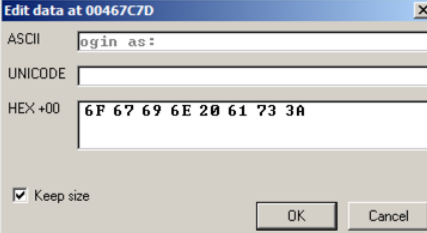


The Hex Dump pane, in the lower left, shows the text "ogin as: ", as shown below.

In the Hex Dump pane, highlight "ogin as:", as shown below. Right-click the highlighted text. Point to Binary. Click Edit

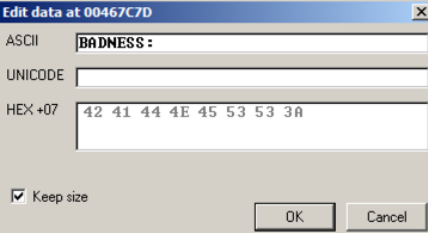


An "Edit data at 00467C7D" box opens, as shown below



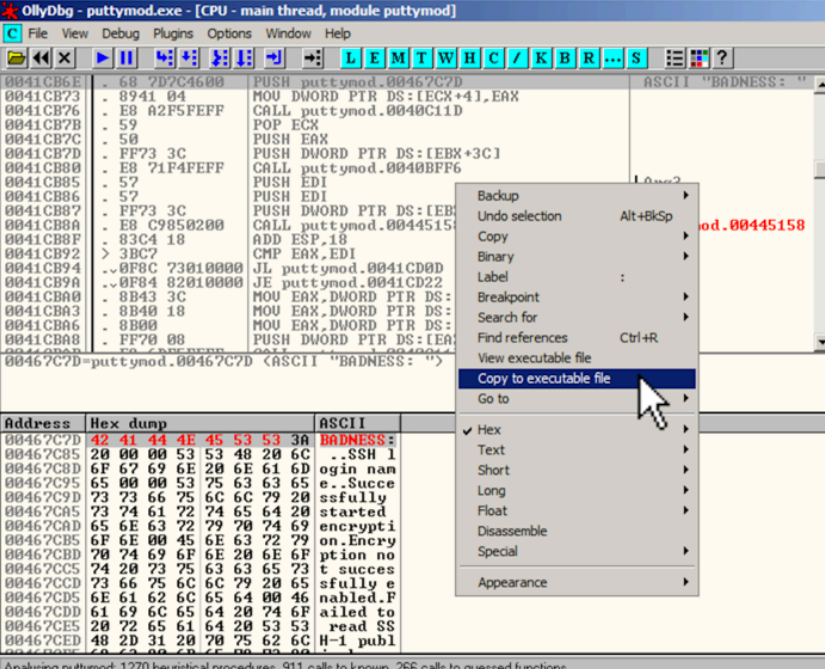
Click in the ASCII field, press Backspace to move back to the start, and overwrite the message with this text, as shown below:

BADNESS



Saving the Modified ASCII Text

In Ollydbg, in the lower left "Dump" pane of the CPU window, right-click and click "Copy to executable file", as shown below



In the "Save file as" box, change the File name to puttymod2.exe, as shown below, and click Save.

Running the Modified EXE

Close Ollydbg.

Double-click puttymod2.exe.

In the "Host Name (or IP address)" box, type

ad.samsclass.info

At the bottom, click the Open button.

A black box opens, and shows a "BADNESS:" prompt, as shown below

