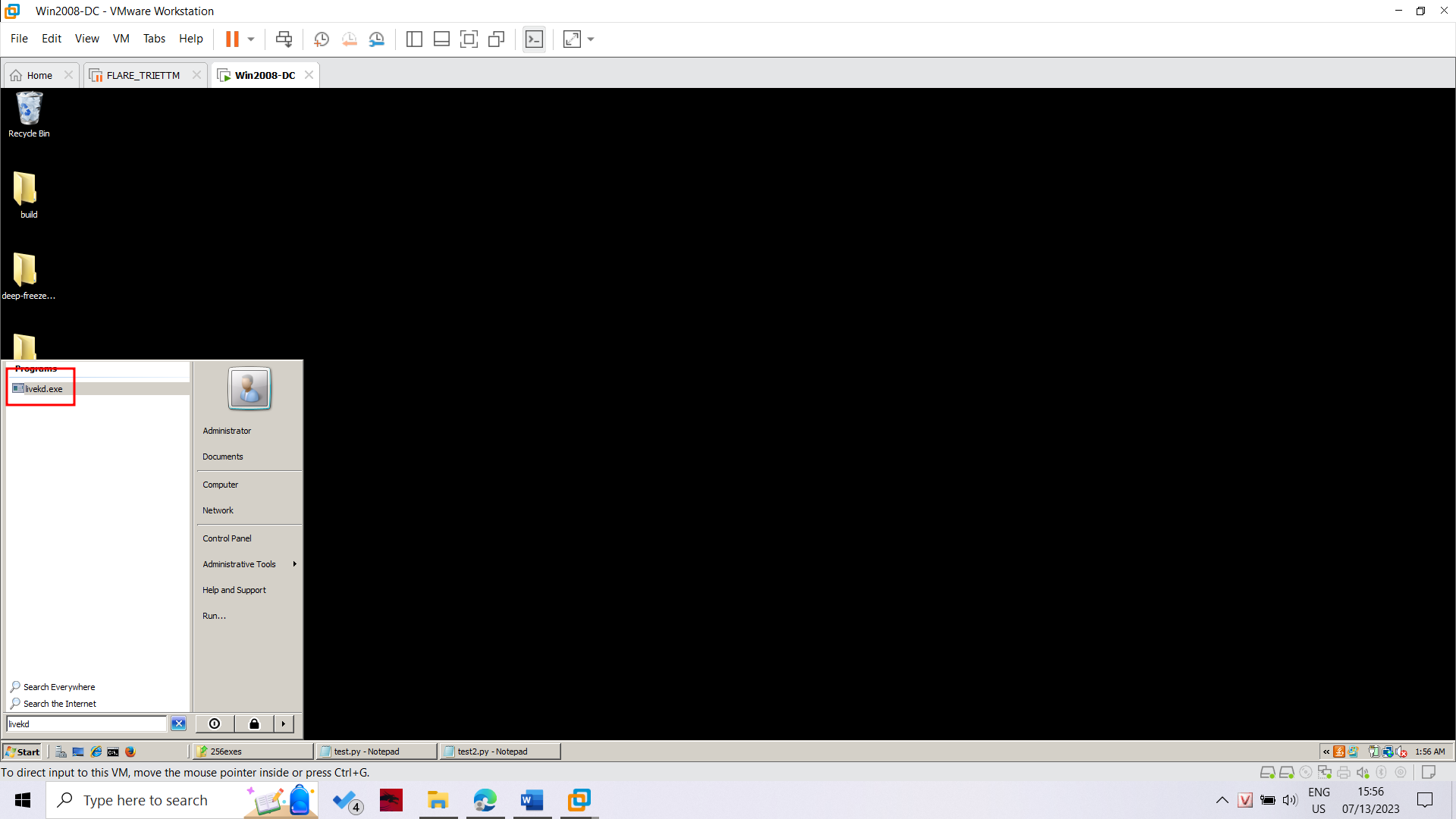
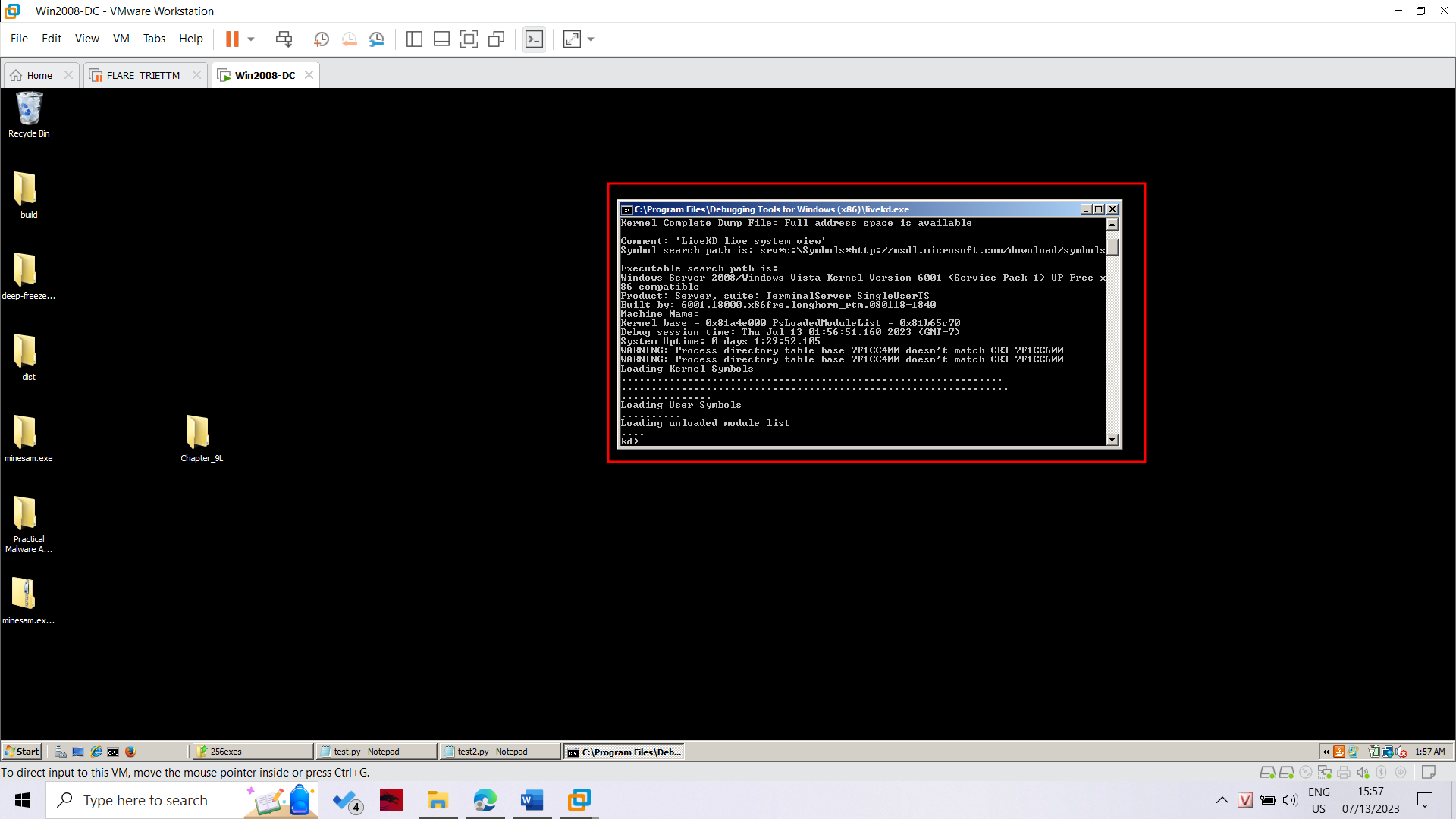
**Lab 16: Using Kernel Debugging Commands with WinDbg**

Starting Configuration

You should have Livekd running, which launched WinDbg, as you did at the end of the previous project.





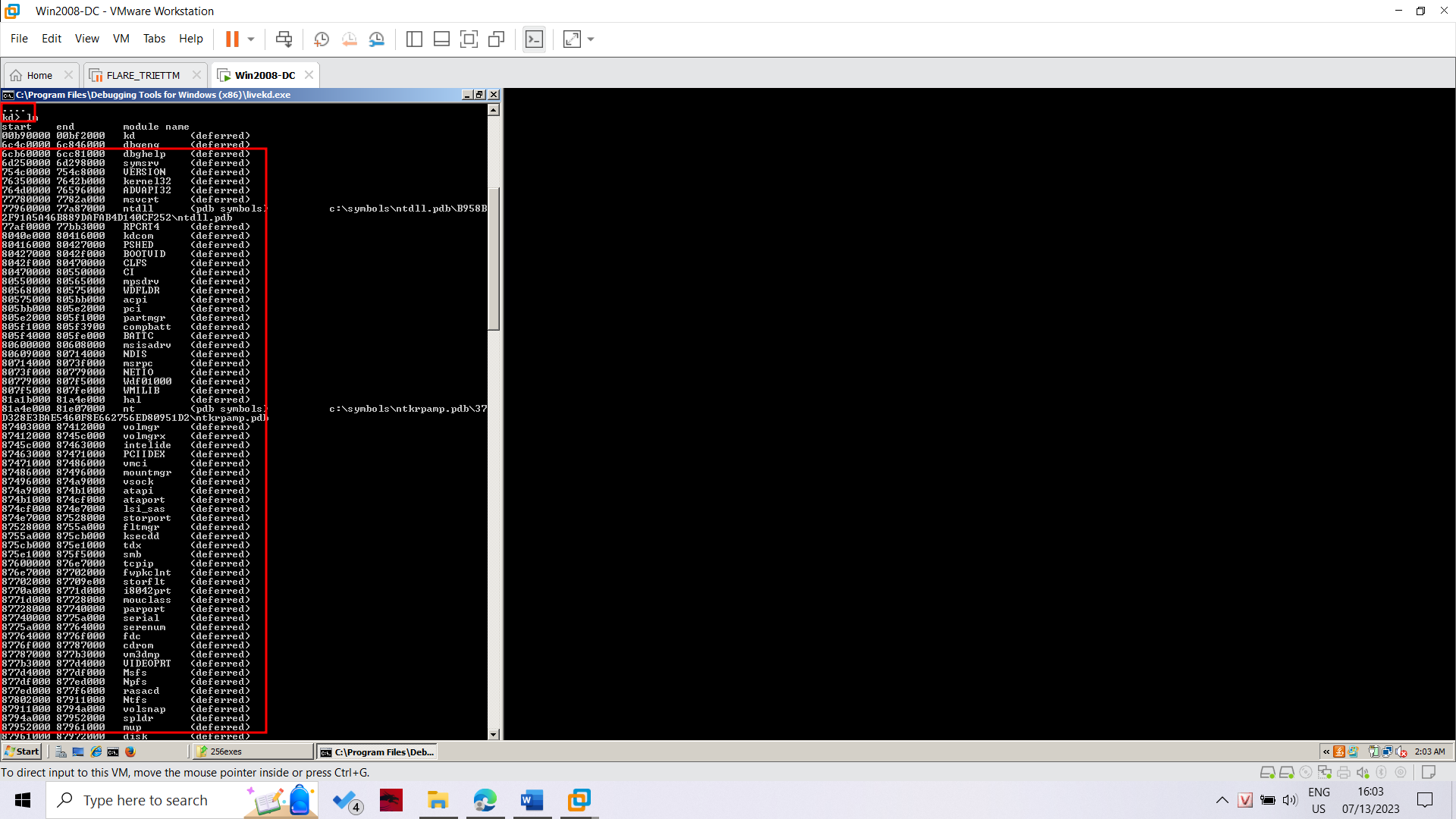
Listing Modules with lm

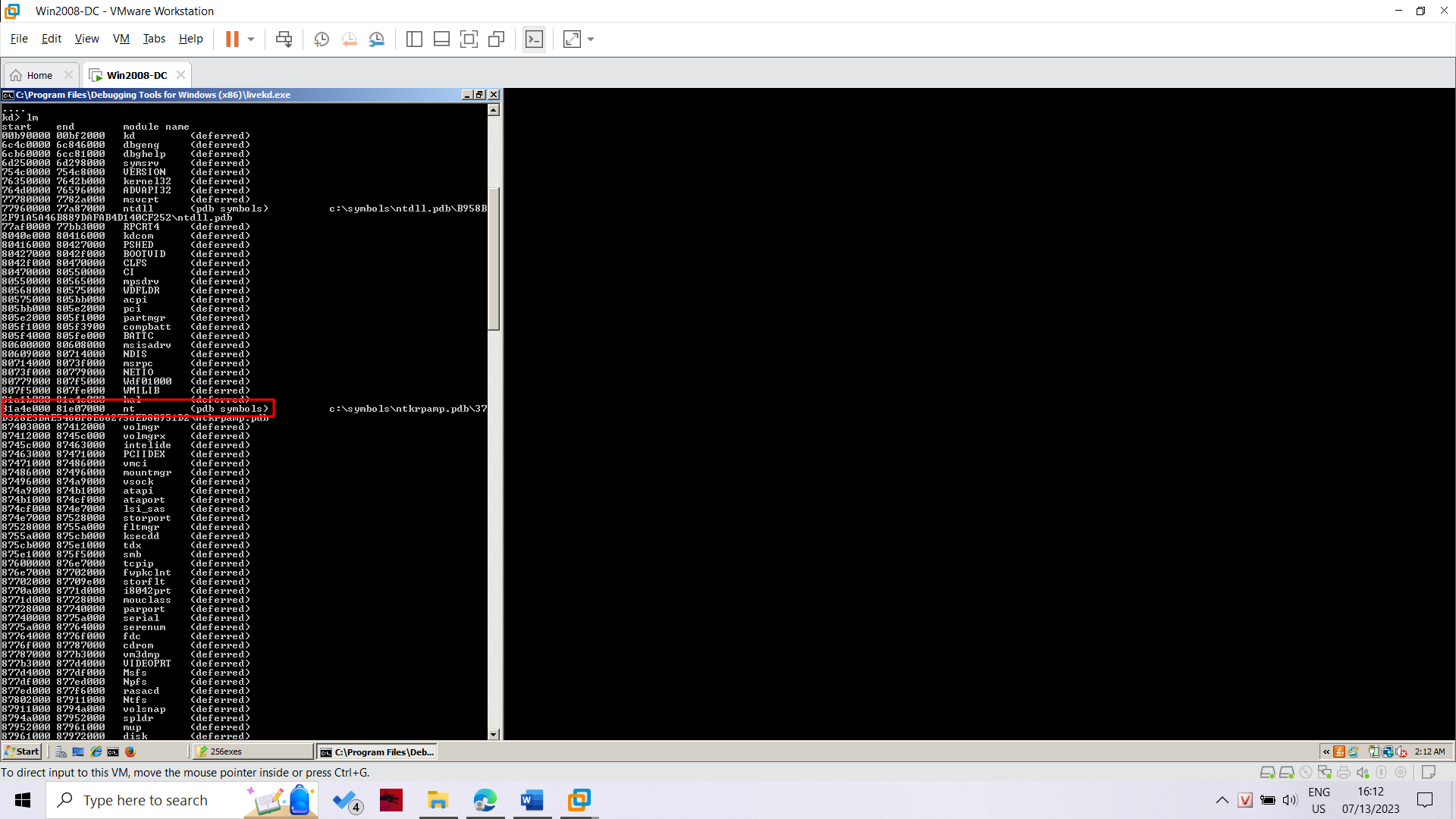
At the bottom of the Command window, in the command bar, execute this command:

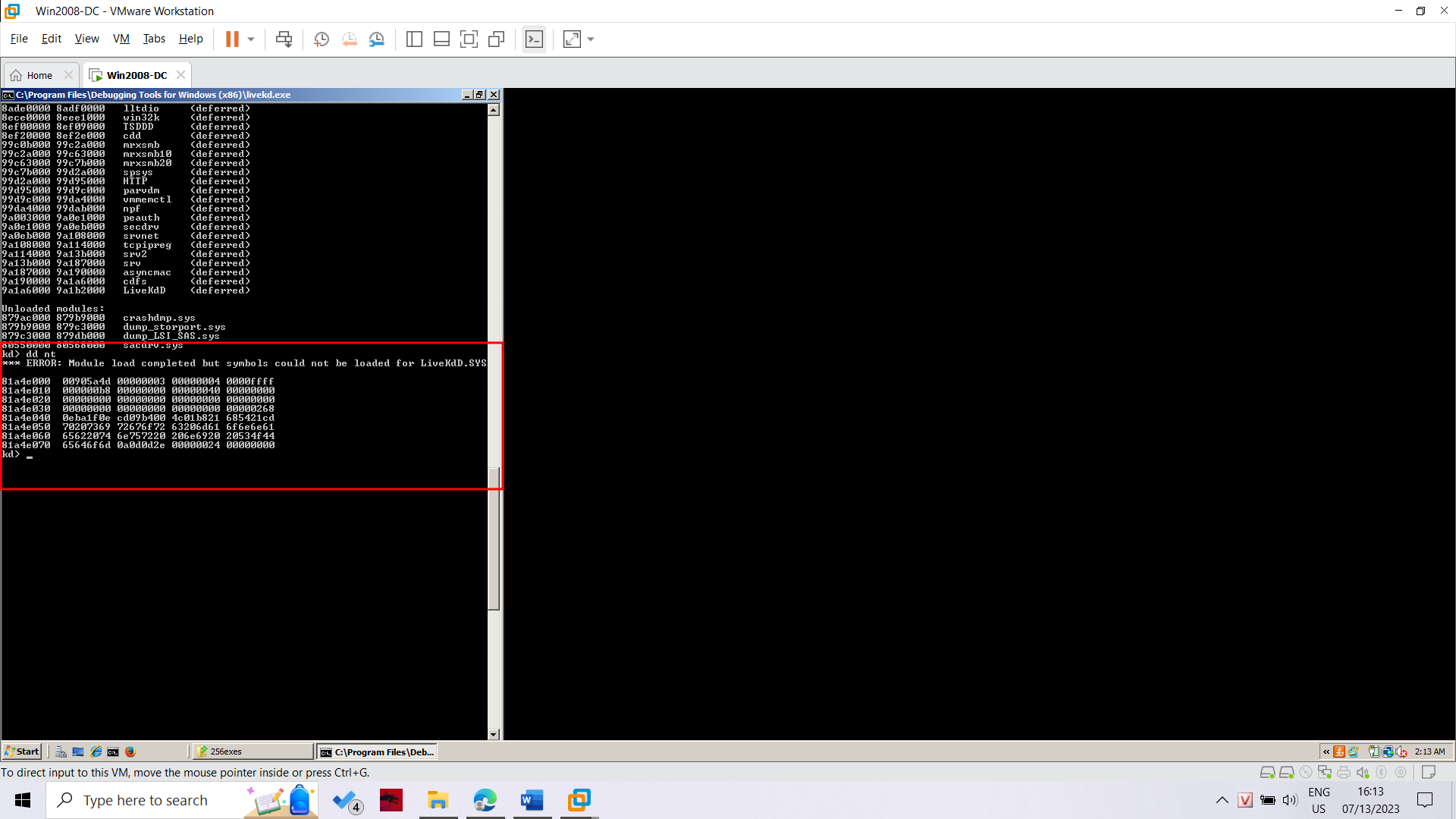
lm

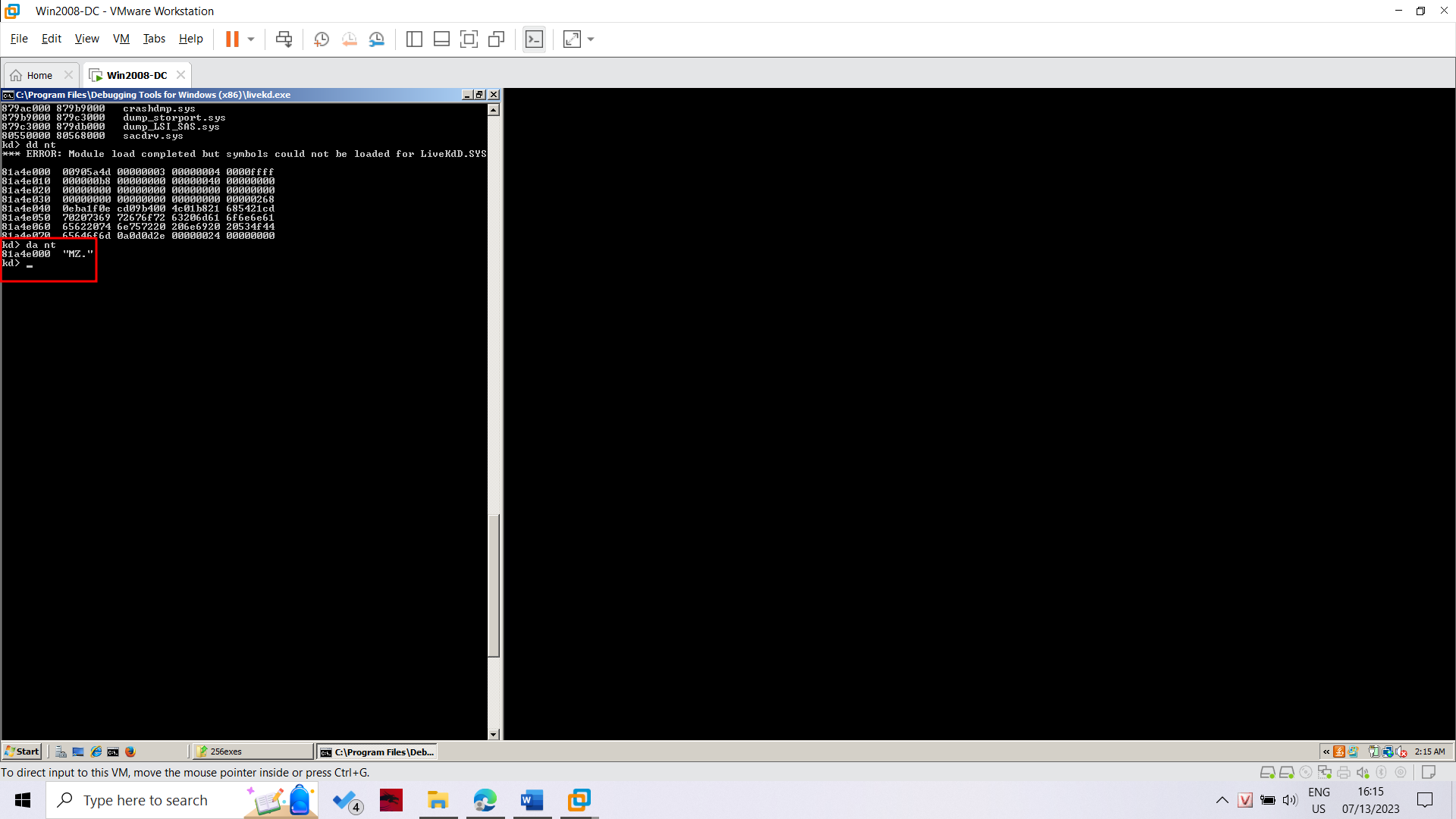
A long list of loaded modules scrolls by.

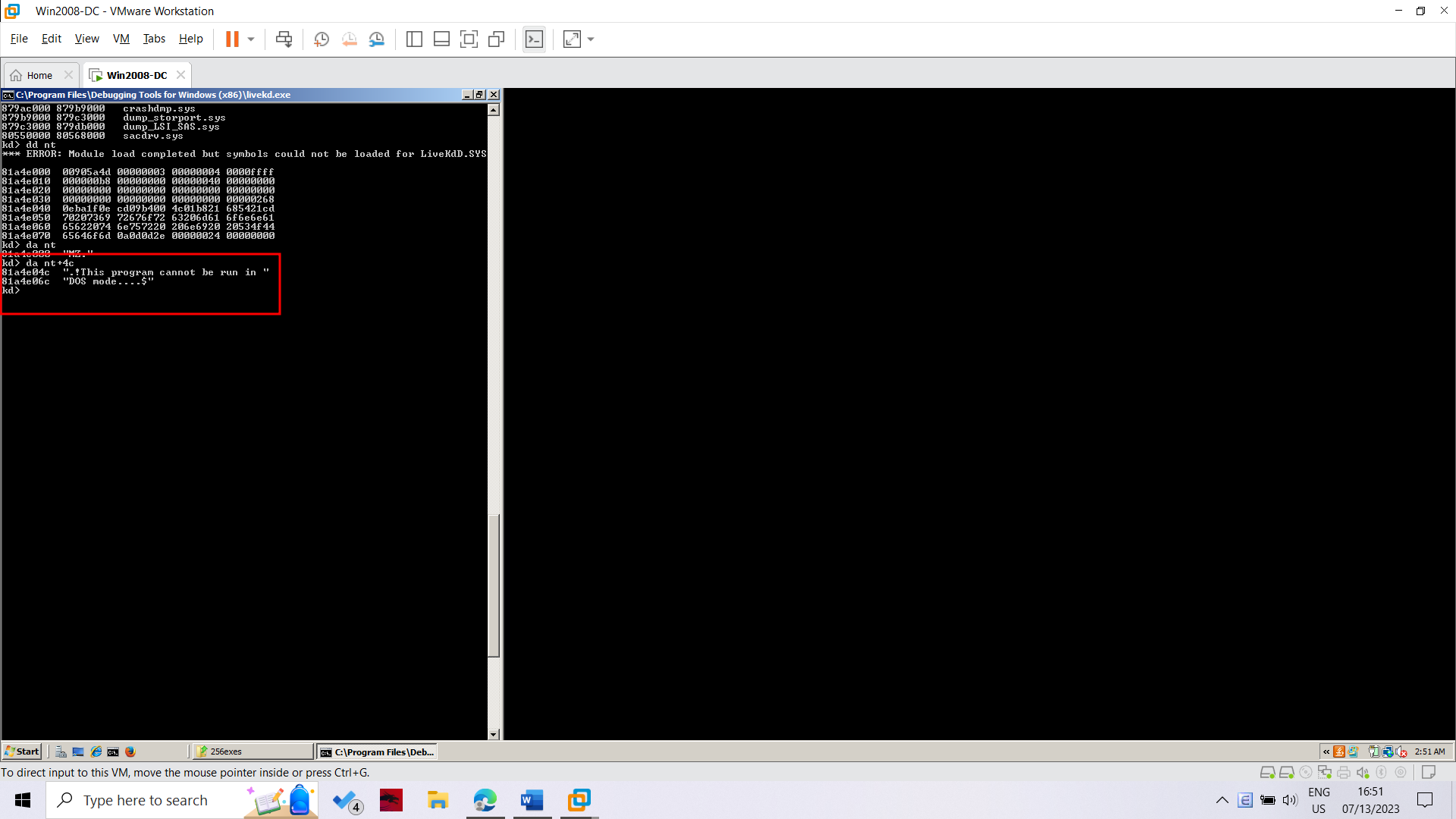
Scroll back to see the lm command you entered, and the first few loaded kernel modules, as shown below.

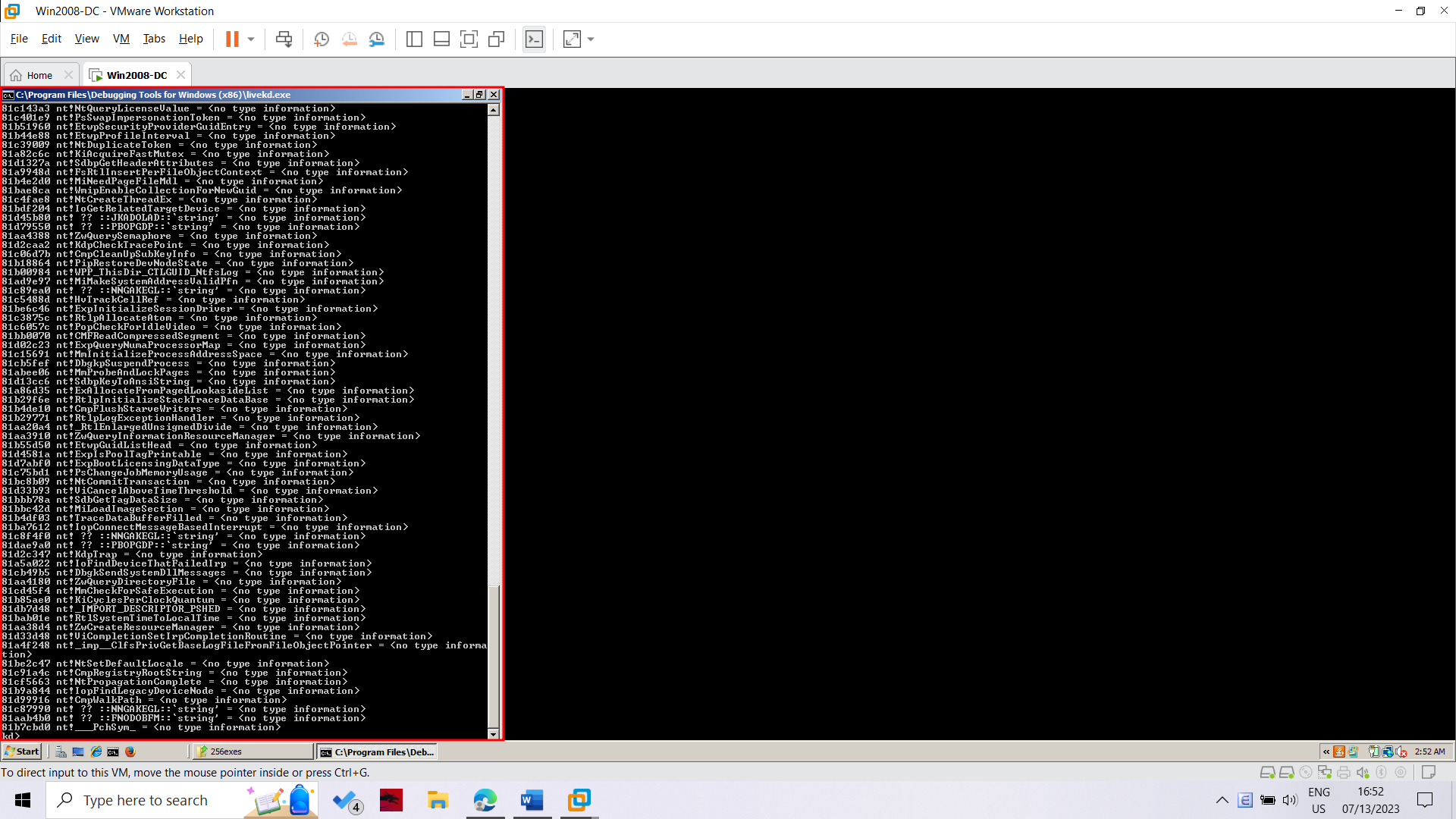












In WinDbg, execute this command:

x nt!\*Create\*

This finds all the functions in Ntoskrnl that contain the word "Create".

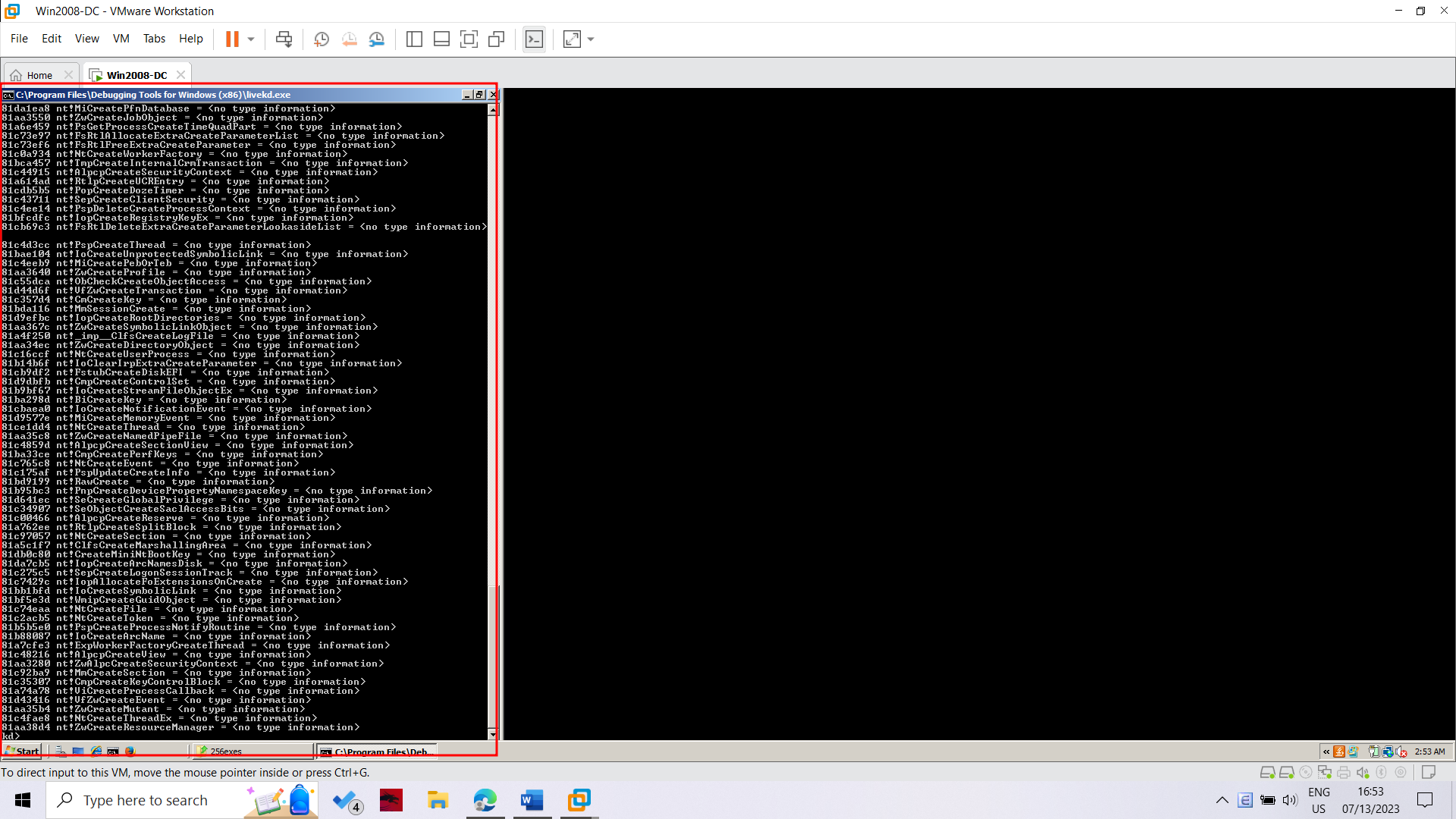
There are a lot of them, too.

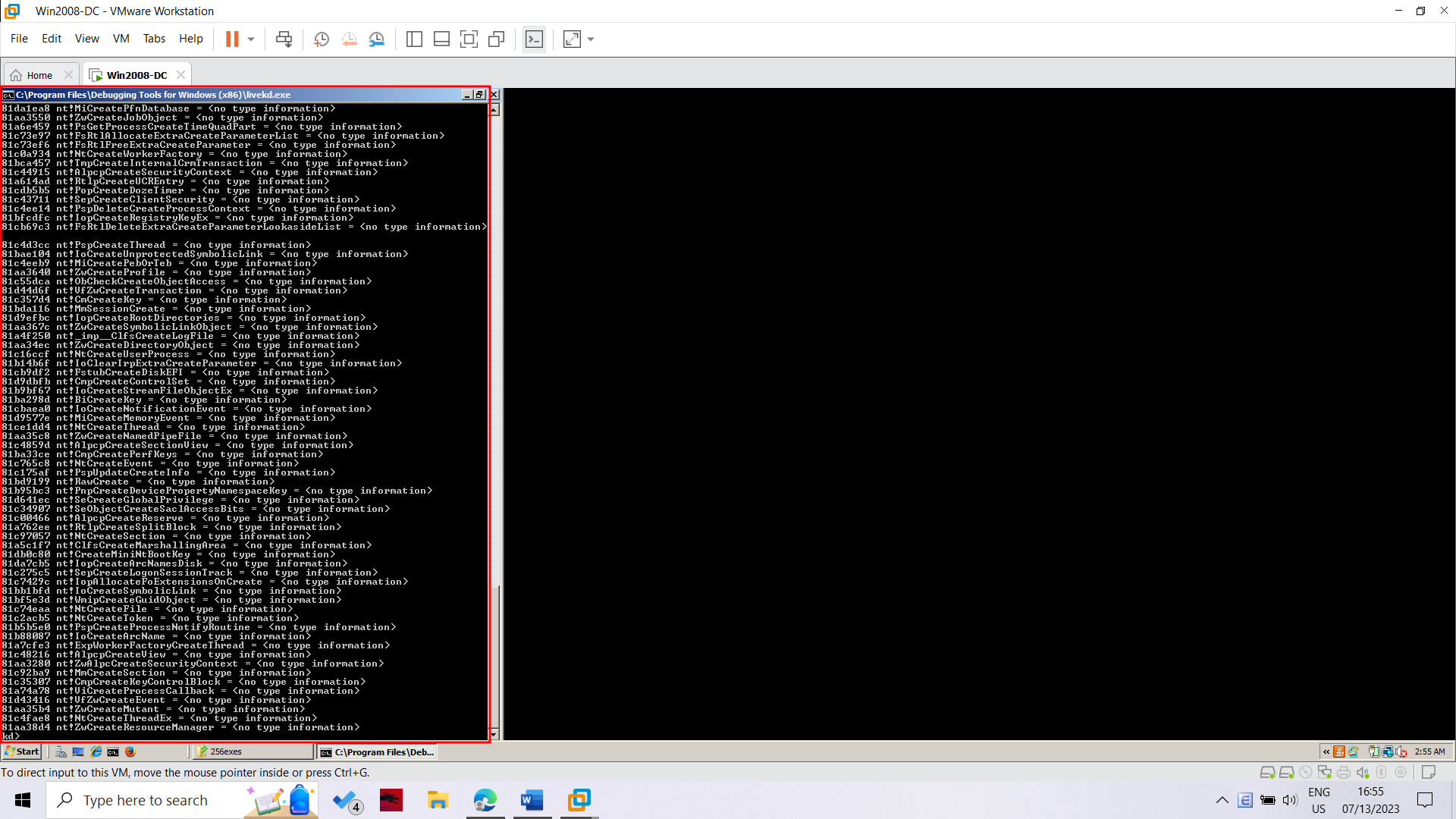
In WinDbg, execute this command:

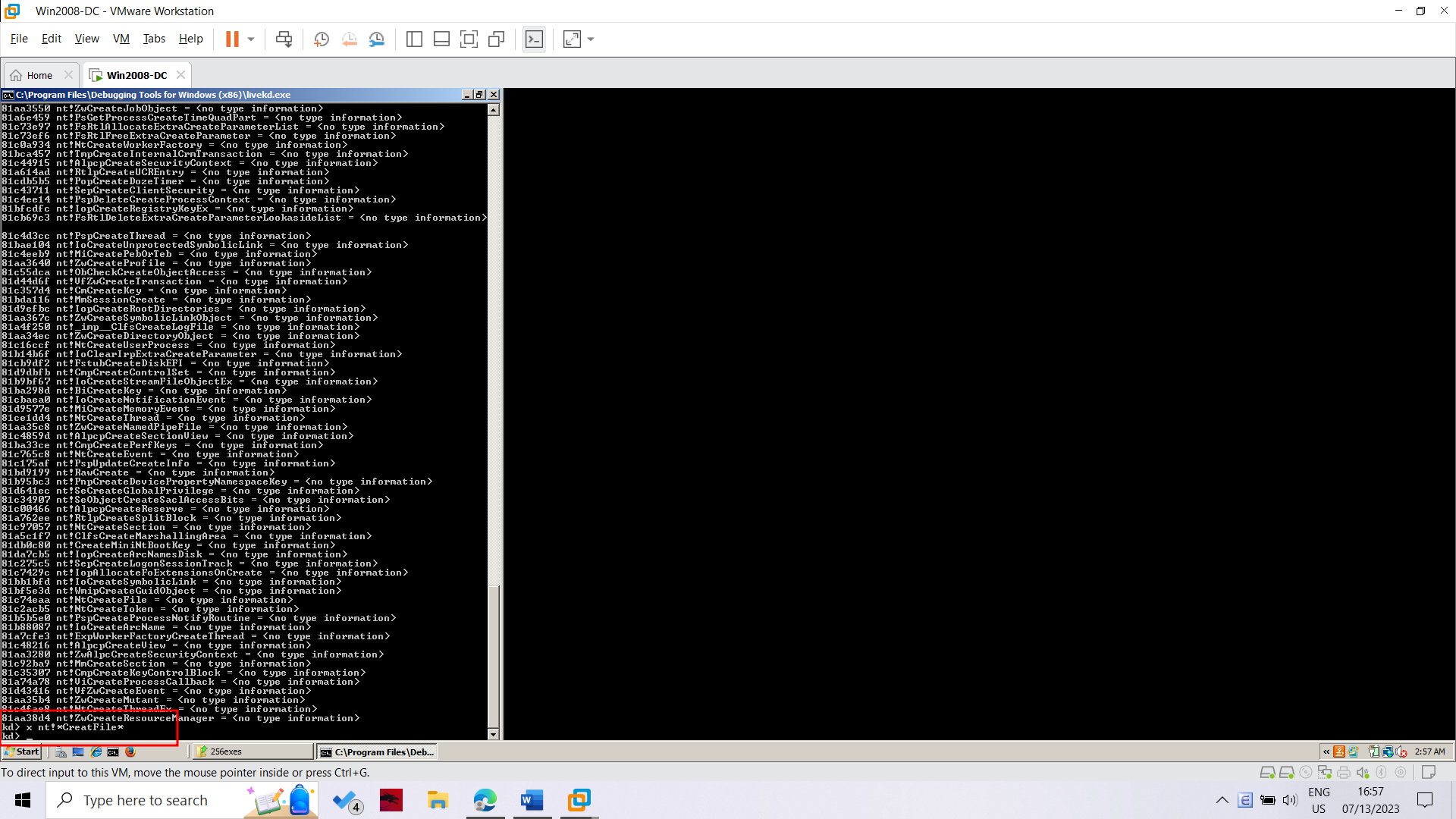
x nt!\*CreateFile\*

This finds all the functions in Ntoskrnl that contain the word "CreateFile".

There are only about ten of those, including "nt!NtCreateFile", as shown below:



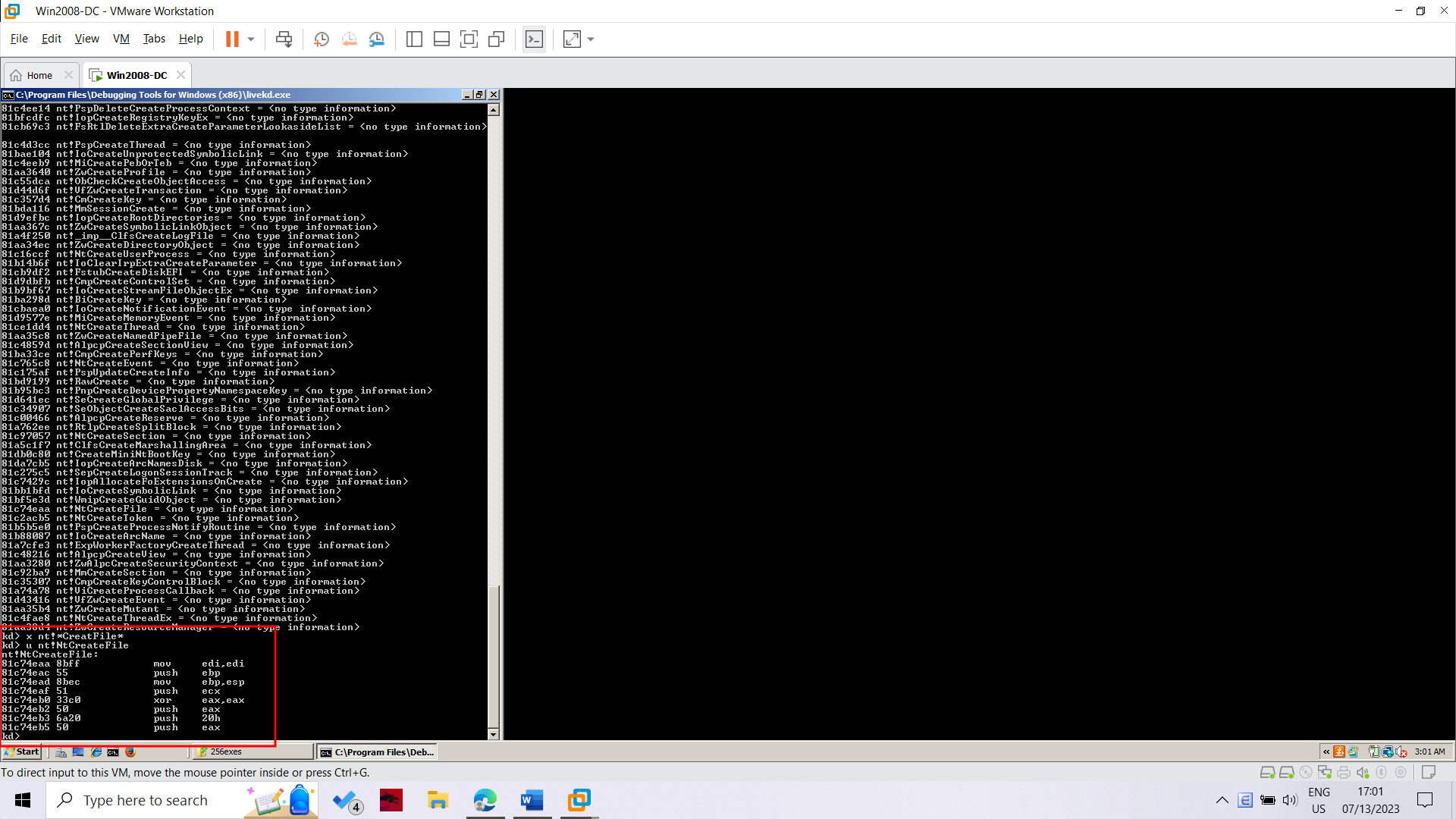


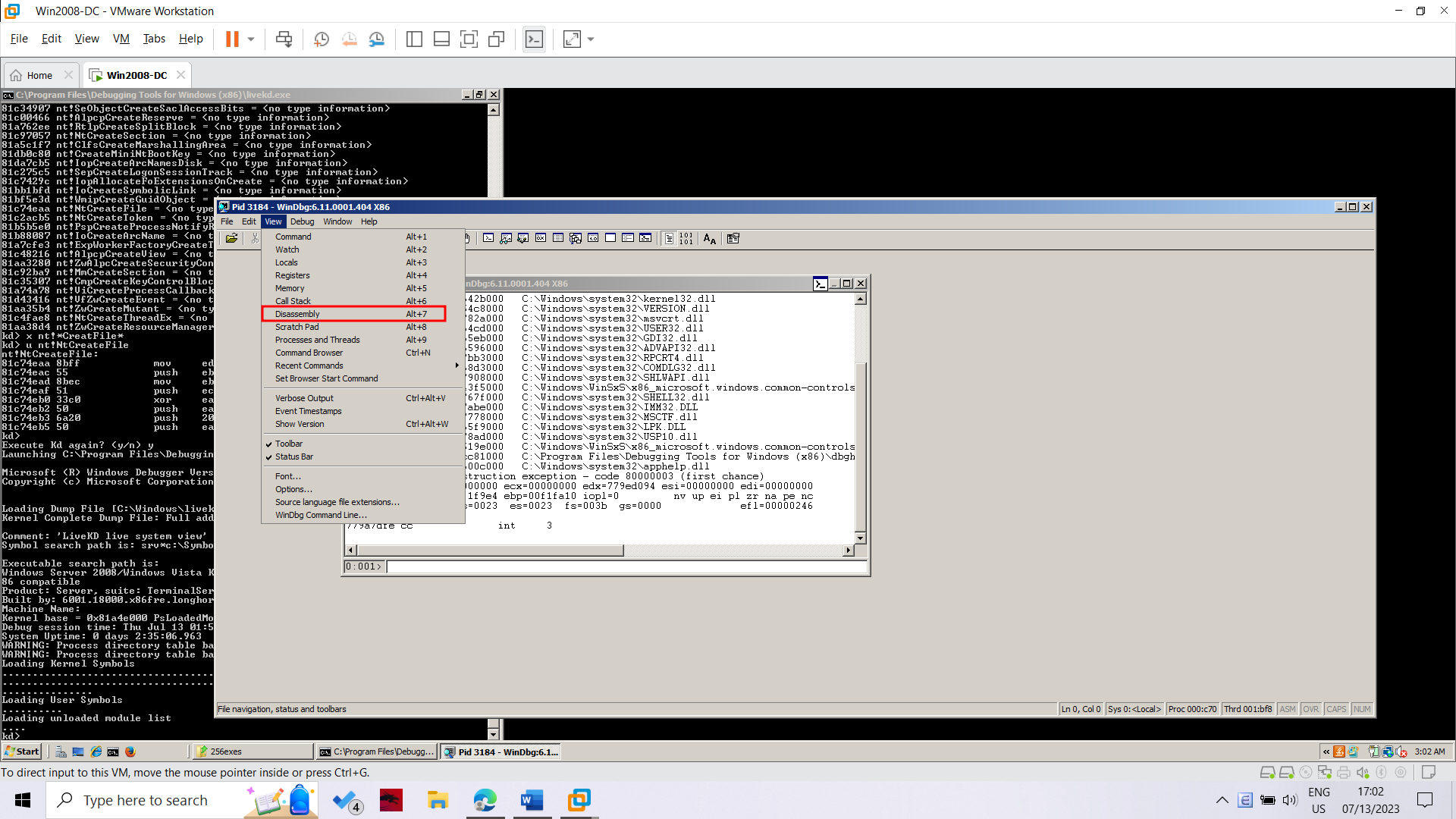


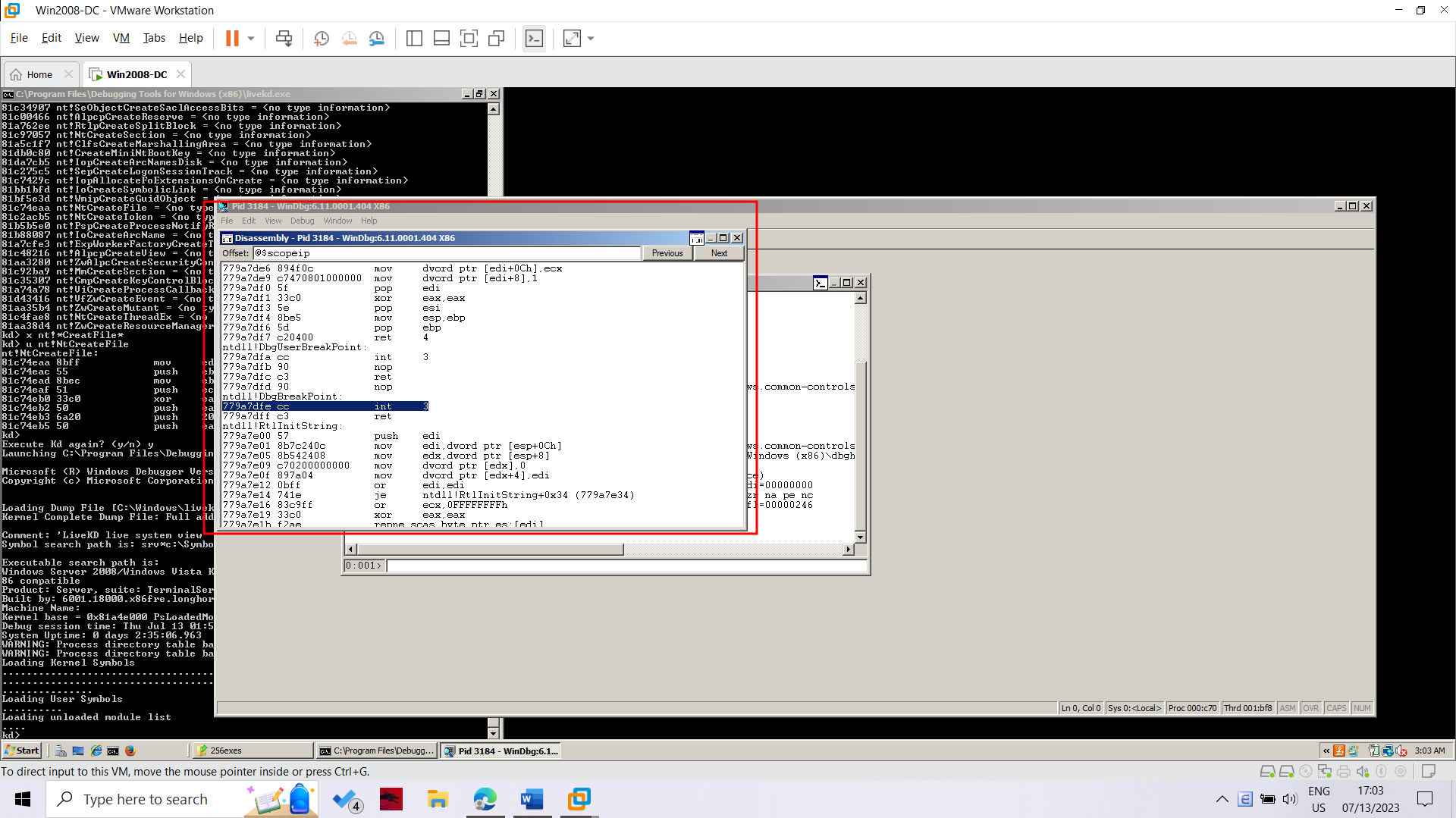
Unassembling a Function

In WinDbg, execute this command:

u nt!NtCreateFile

This shows the first few bytes of the function, disassembled, as shown below: 

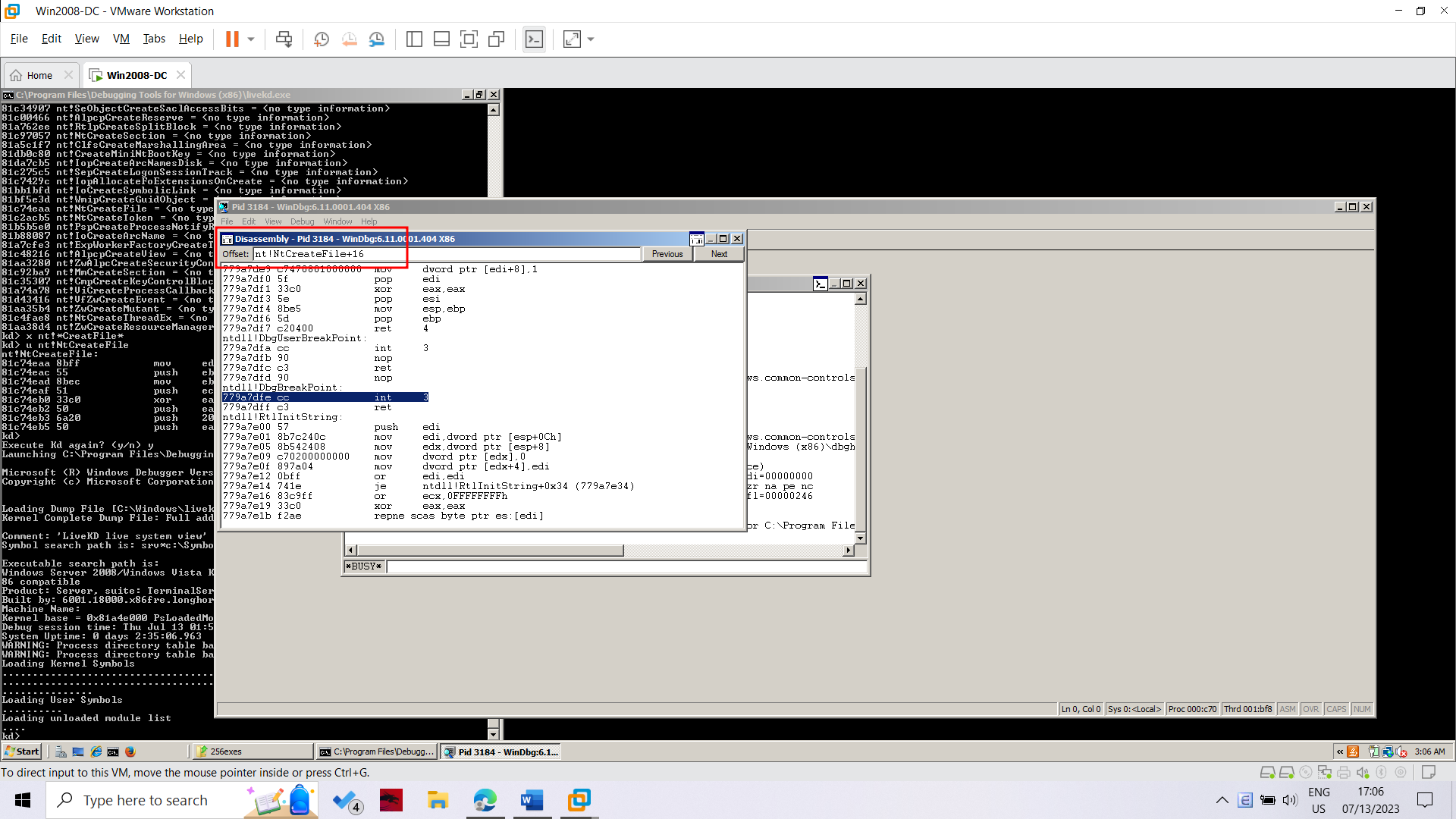




In the Offset bar at the top, enter

nt!NtCreateFile+16

Resize this window to make the entire function visible. Drag the mouse through it to highlight the entire function, as shown below.



**Lab 17: Kernel Debugging with WinDbg**

Adding a Boot Menu Item to the TARGET machine

Start the Windows XPSP3 virtual machine.

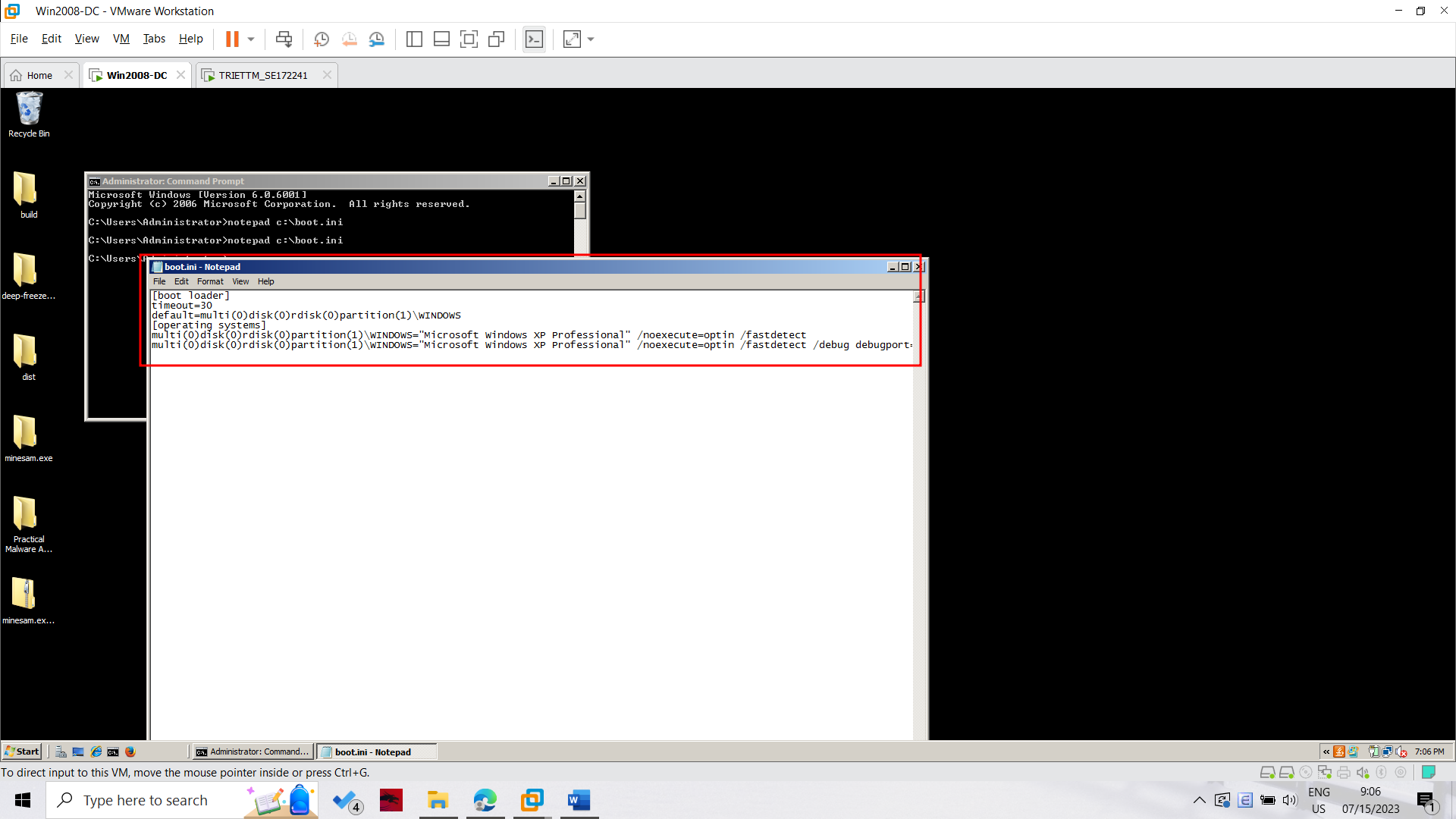
Click Start, Run.

In the Run box, execute this command:

notepad c:\boot.ini

In Notepad, copy the existing boot line, paste it at the end of the file, and add these switches to the end of the line, as shown below:

/debug /debugport=com1 /baudrate=115200



If you cannot save the file, open a Command Prompt and execute this command, to remove the Read-only, System, and Hidden flags from the file:

attrib -R -S -H c:\boot.ini

**Adding a Virtual Serial Adapter**

Power off the TARGET virtual machine. You cannot make this change while the virtual machine is running or suspended.

On the WINDBG machine, start VMware Player.

In the left pane of VMware Player, click your TARGET machine.

At the lower right of VMware Player, click "Edit virtual machine settings".

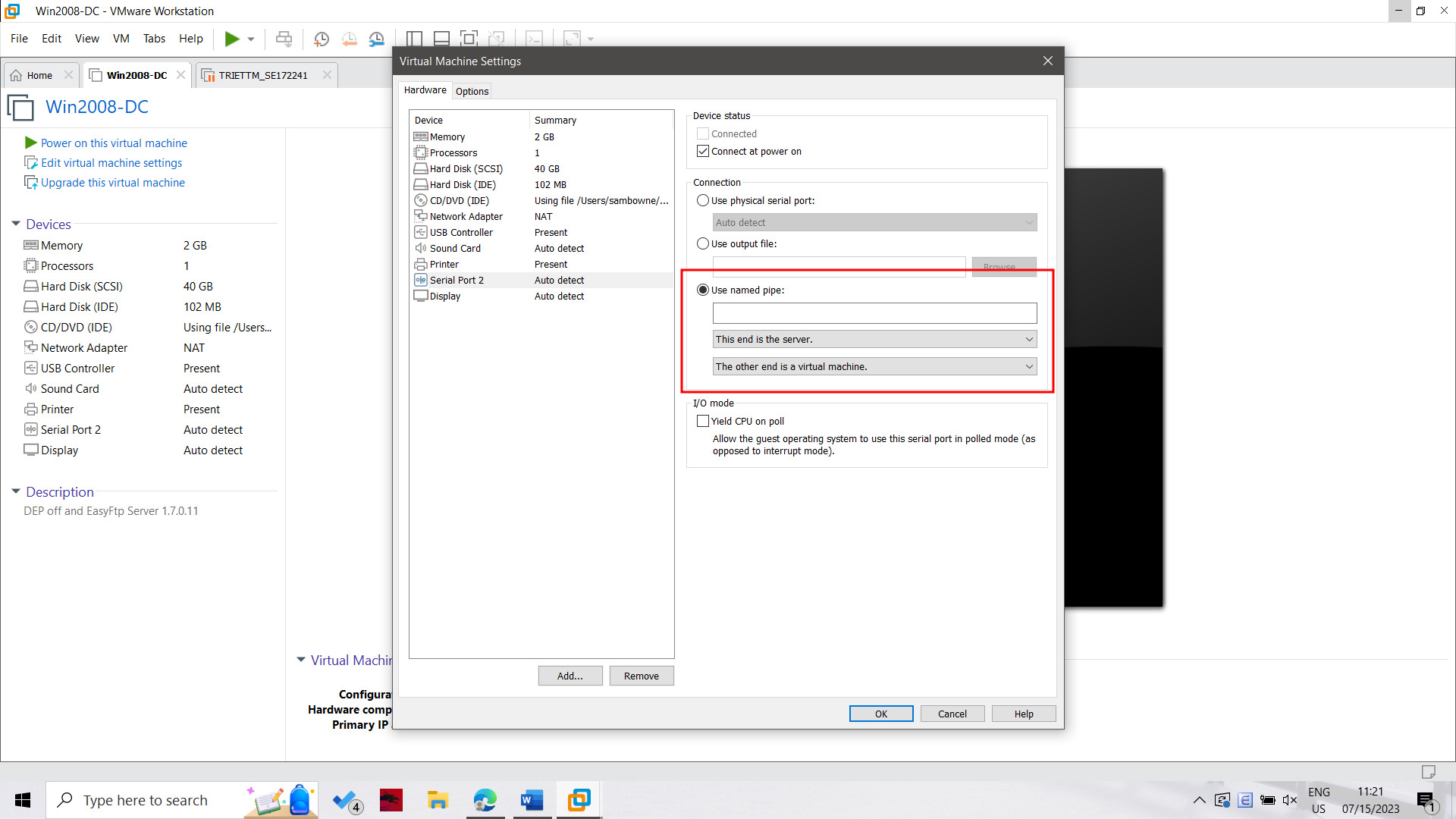
In the left side of the "Virtual Machine Settings" box, click the Add... button.

In the "Hardware Type" box, select "Serial Port", as shown below.



Click Next.

In the "Serial Port Type" box, click "Output to named pipe", as shown below.



Click Next.

In the "Specify Socket" box, enter a Named Pipe of

\\.\pipe\com\_1

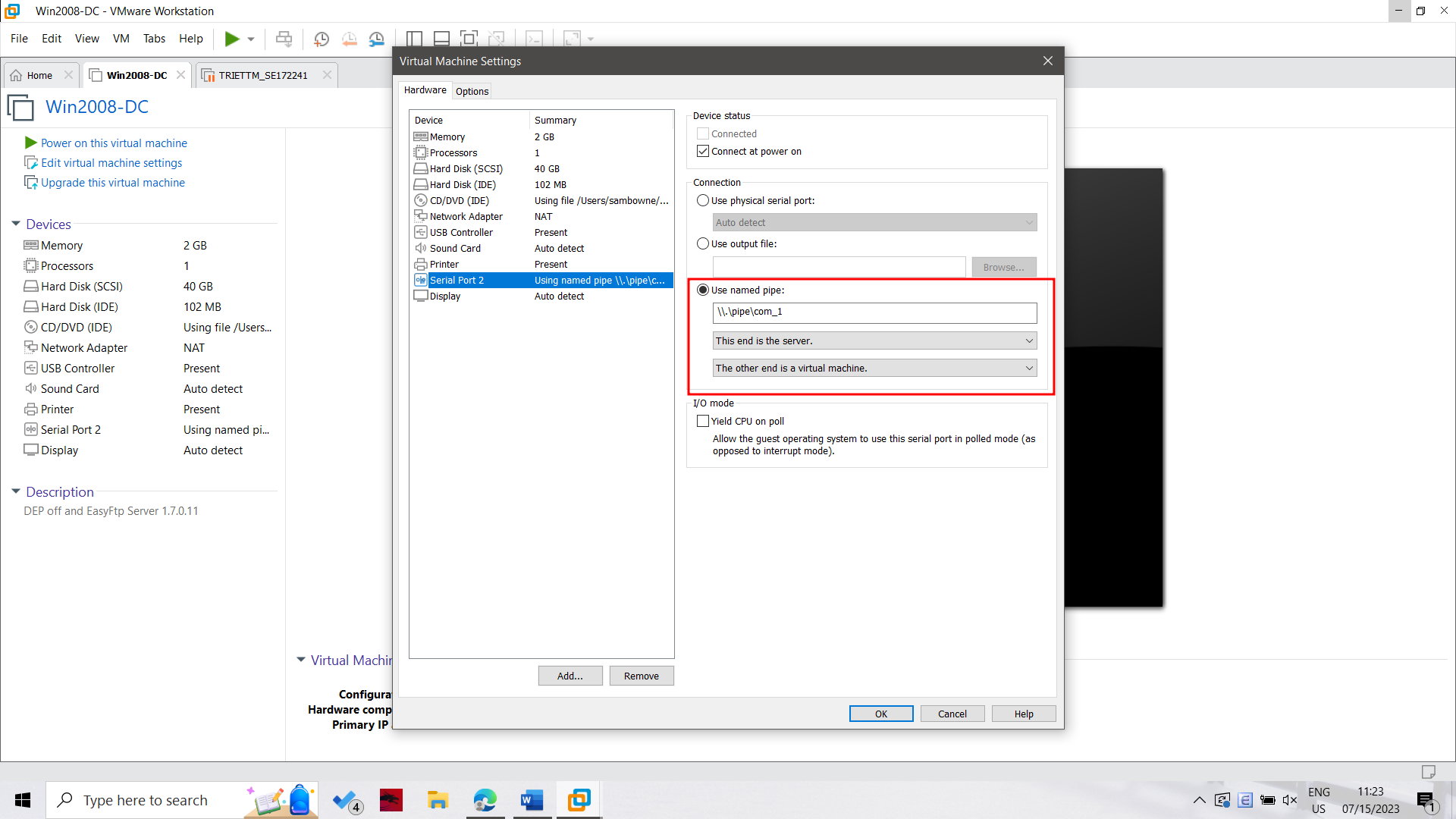
In the two drop-down list boxes, select

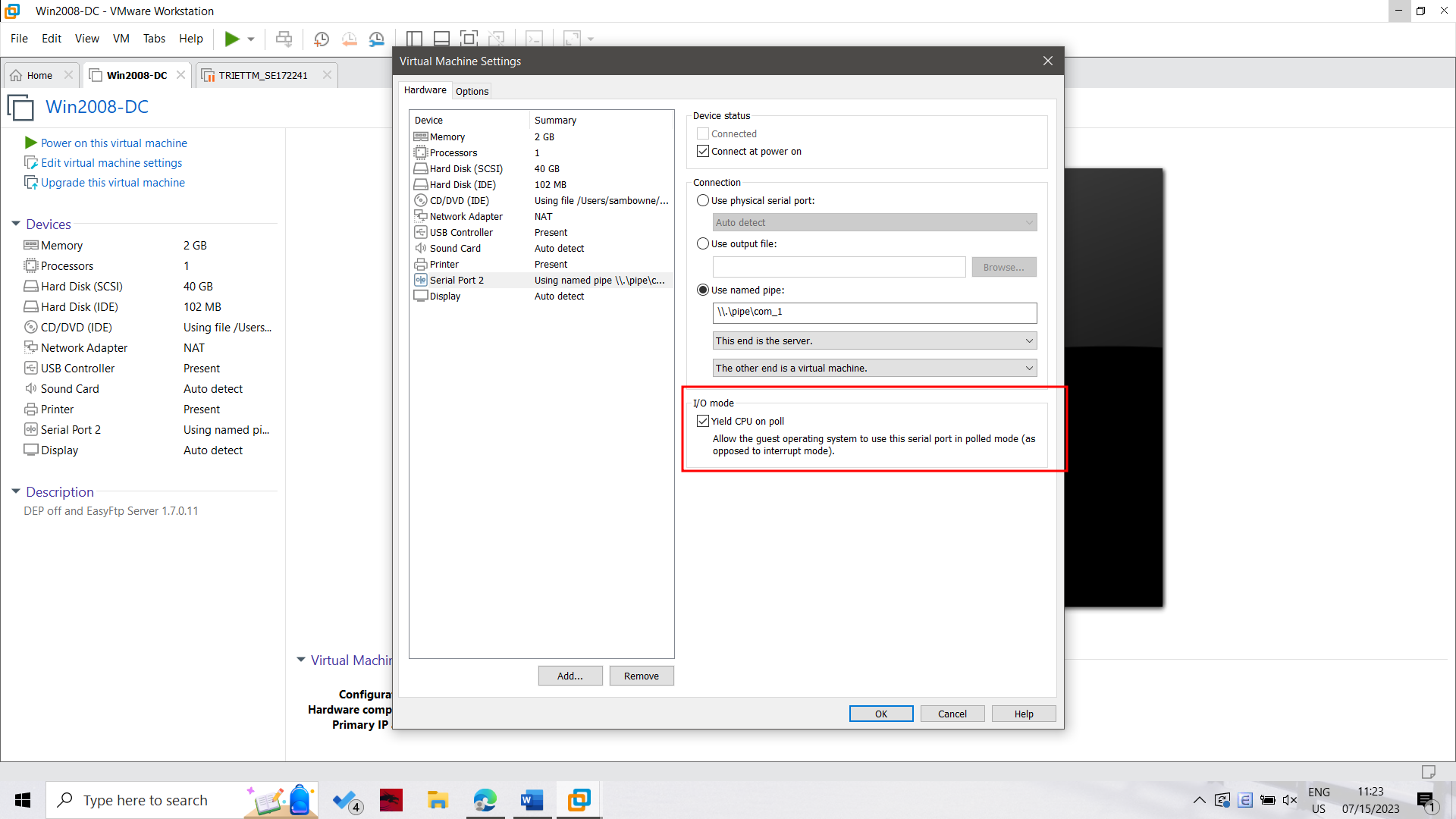
This end is the server.

and

The other end is an application.

as shown below.





Downloading Microsoft Symbols

Kernel debugging is much easier with symbols.

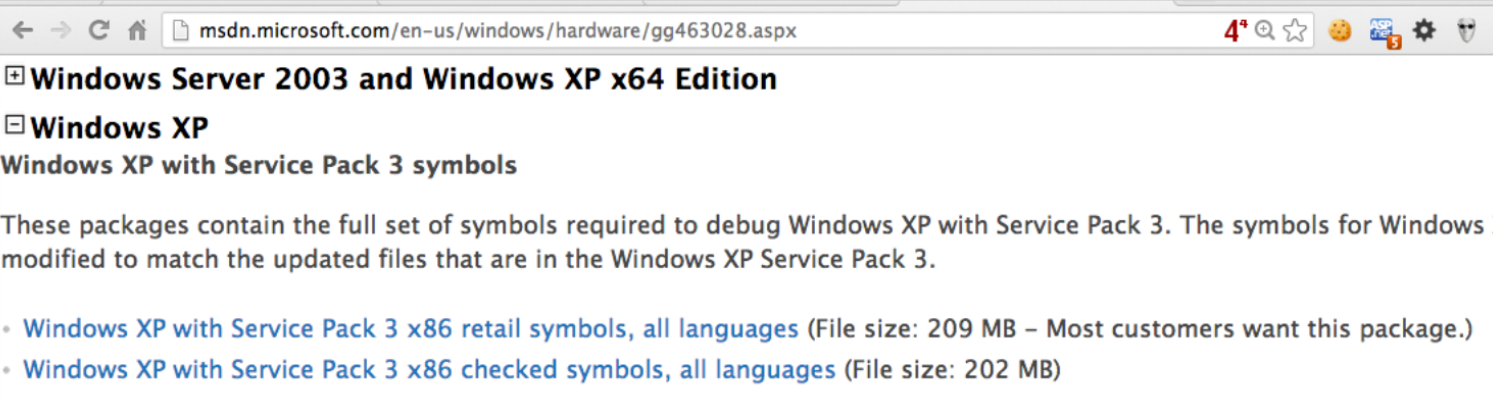
WinDbg can download them automatically as needed, but downloading them separately is the best procedure if you plan to work without always being connected to a

reliable, high-speed Internet connection.

Start the WINDBG machine. in a Web browser, go to

http://msdn.microsoft.com/en-us/windows/hardware/gg463028.aspx

Download the symbol file for "Windows XP with Service Pack 3 x86 retail symbols, all languages", as shown below



You end up with an EXE file. Run it in the WINDBG machine. Accept all the default options.

First it will extract into a temporary directory with a long name, then it will automatically extract into C:\Windows\Symbols. Accept that selection.

**Installing WinDbg on the WINDBG Machine**

On the WINDBG machine, open a browser and go to

http://msdn.microsoft.com/en-US/windows/desktop/bg162891

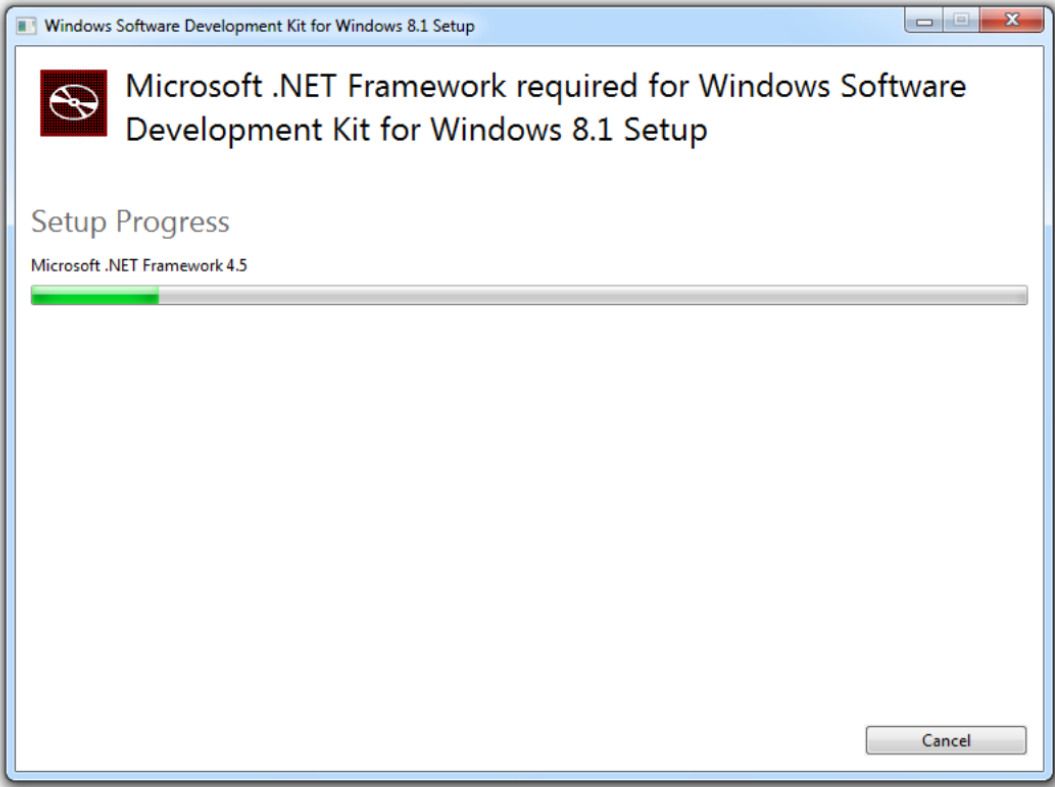
Click the blue Download button.

Save the sdksetup.exe file on your desktop.

Double-click the sdksetup.exe file.

Accept the agreement and click the "Accept & Install" button.

Wait while .NET installs, as shown below.



Starting Kernel Debugging

In WinDbg, click File, "Kernel Debug".

In the "Kernel Debugging" box, click the COM tab.

Change the Port to

\\.\pipe\com\_1

and check the Pipe box, as shown below. Then click OK

