What You Need

A Windows 10 machine with Livekd working, as prepared in the previous project. This project should work on Win 7 or any later version, but I only tested it on

Windows 10.

Purpose

Practice using simple WinDbg commands.

Starting Configuration

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

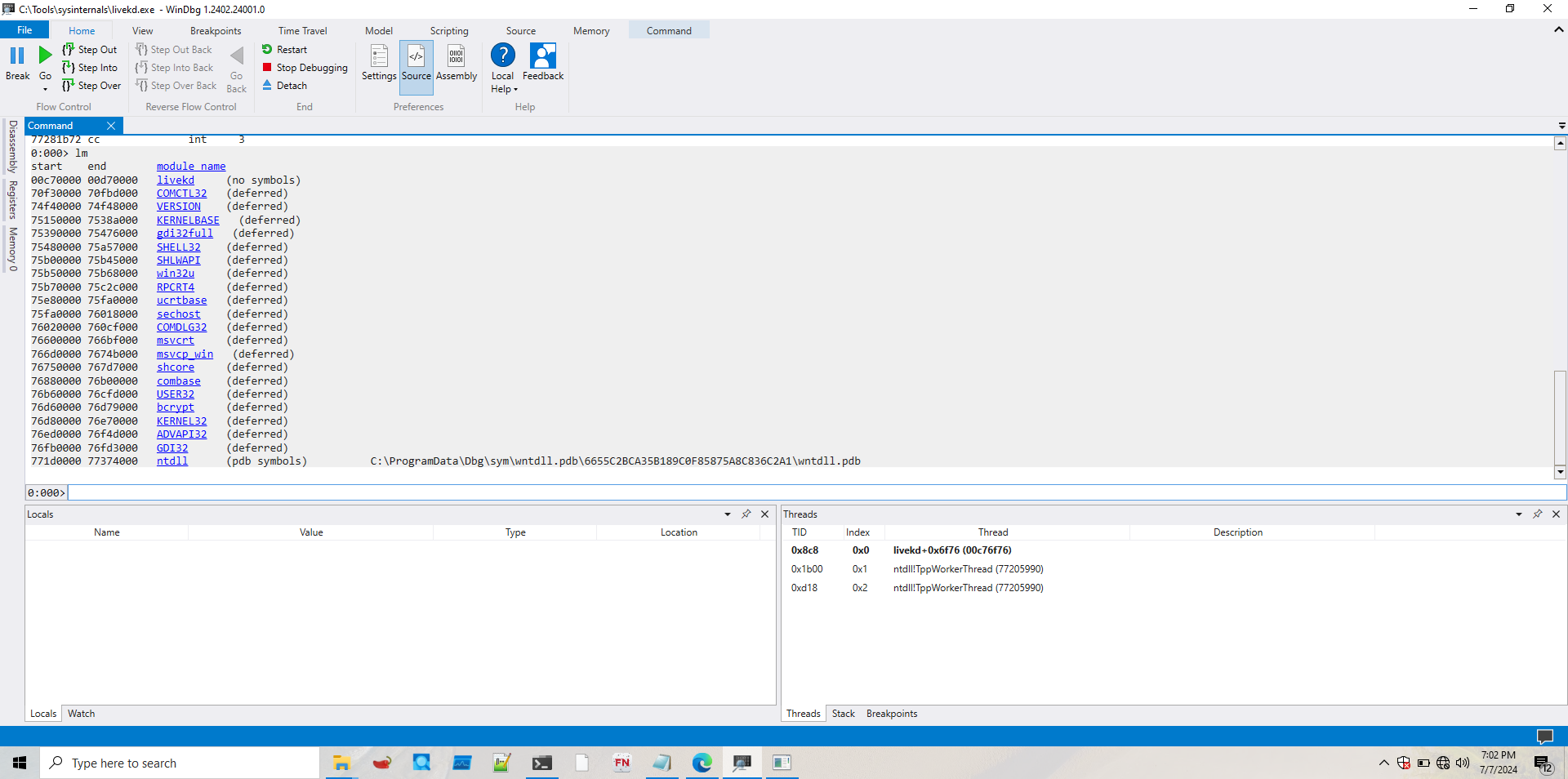
Listing Modules with lm

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.



Scroll down to find the module named nt, as shown below. It's easy to spot because it'e one of the few modules that shows a Symbols path.

This is Ntoskrnl, the main kernel modul



Viewing Memory

In WinDbg, execute this command:

dd nt

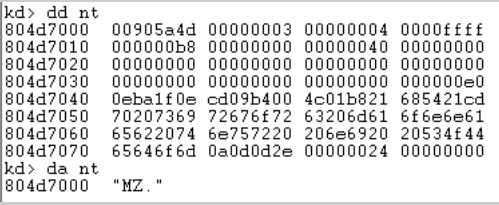
You see the first several bytes of Ntoskrnl.exe, as shown below.

This may be more familiar in ASCII.

In WinDbg, execute this command:

da nt

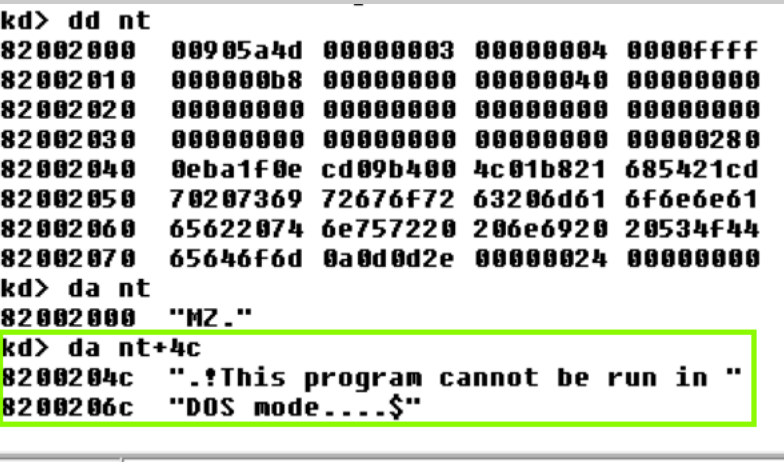
You see the characters "MZ" --they are at the start of every EXE file



In WinDbg, execute this command:

da nt+4c

You see the message "This program cannot be run in DOS mode", as shown below



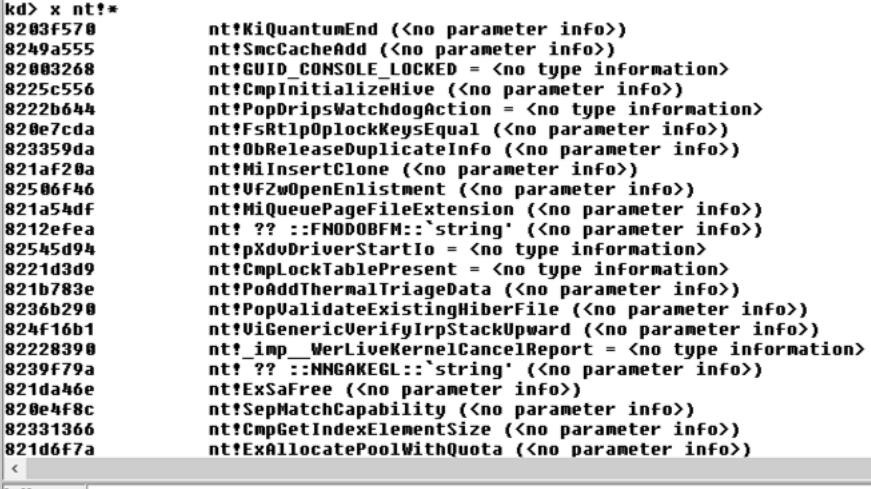
Searching for Functions

In WinDbg, execute this command:

x nt!\*

This finds all the functions in Ntoskrnl.

There are a lot of them, as shown below



In WinDbg, execute this command:

x nt!\*Create\*

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

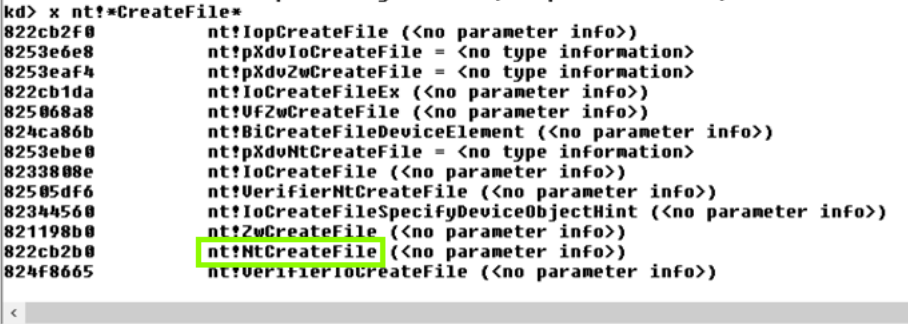
There are a lot of them, too.

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

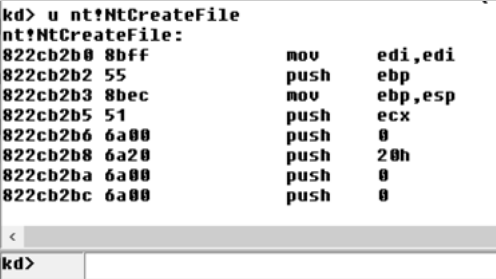


Unassembling a Function

In WinDbg, execute this command:

u nt!NtCreateFile

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



To see more of this function, it helps to use the WinDbg Disassembly window.

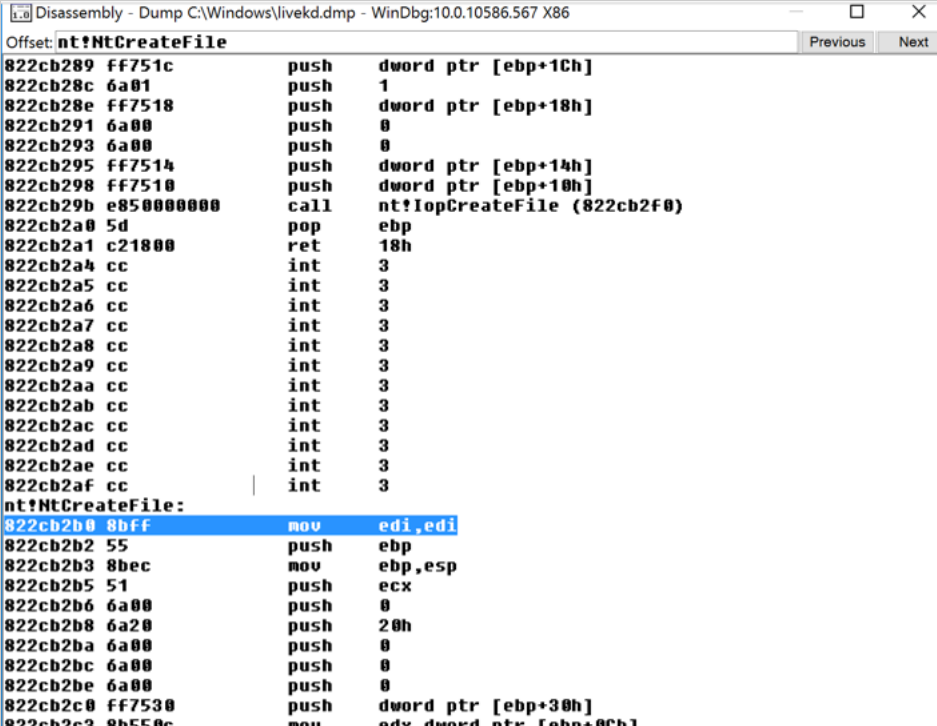
If the Command window is maximized, make it smaller.

From the WinDbg menu bar, click View, Disassembly.

In the Offset bar at the top, enter

nt!NtCreateFile

This shows the assembly code before and after the start of the NtCreateFile function, 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

