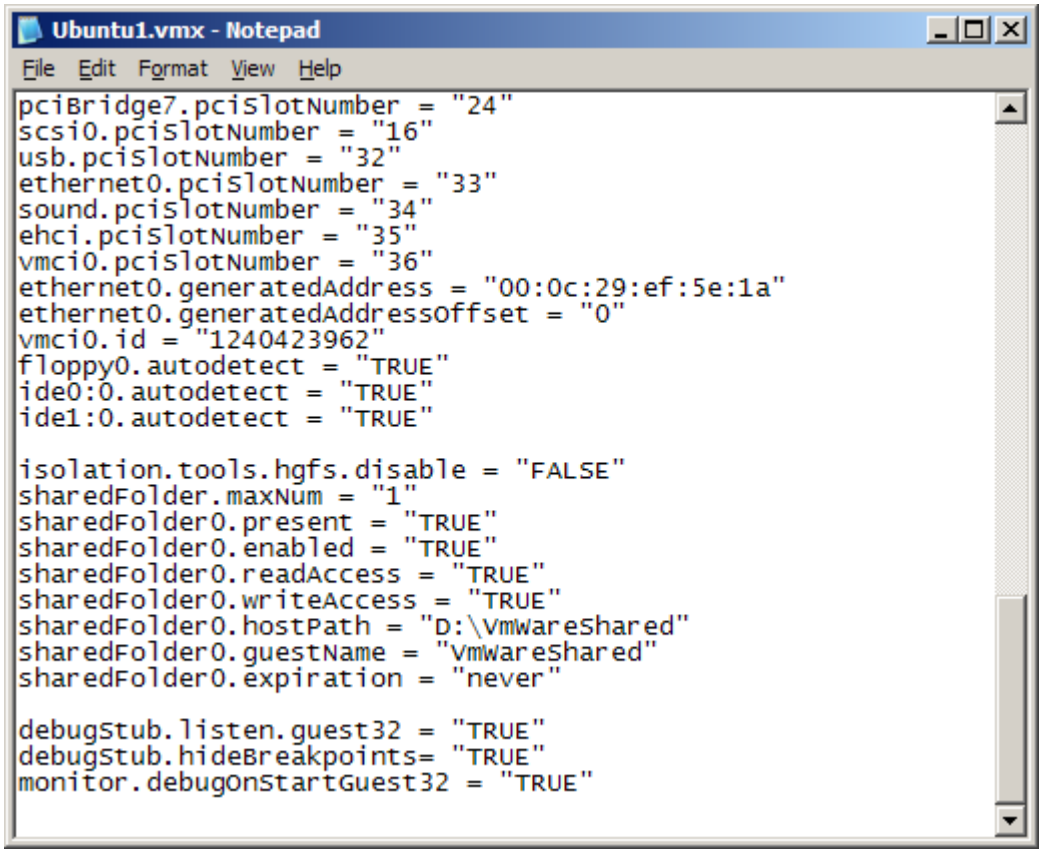
Debugging Linux kenel under VMWare using IDA's GDB debugger

Current versions of VMWare Workstation include a GDB stub for remote debugging of the virtual machines running inside it. In version 5.4, IDA includes a debugger module which supports the remote GDB protocol. This document describes how to use it with VMWare. As an example, we'll debug a Linux kernel.

Debugging a Linux kernel

Let's assume that you already have a VM with Linux installed. Before starting the debugging, we will copy symbols for the kernel for easier navigation later. Copy either /proc/kallsyms or /boot/Sytem.map* file from the VM to host.

Now edit the VM's .vmx file to enable GDB debugger stub:



Add these lines to the file:

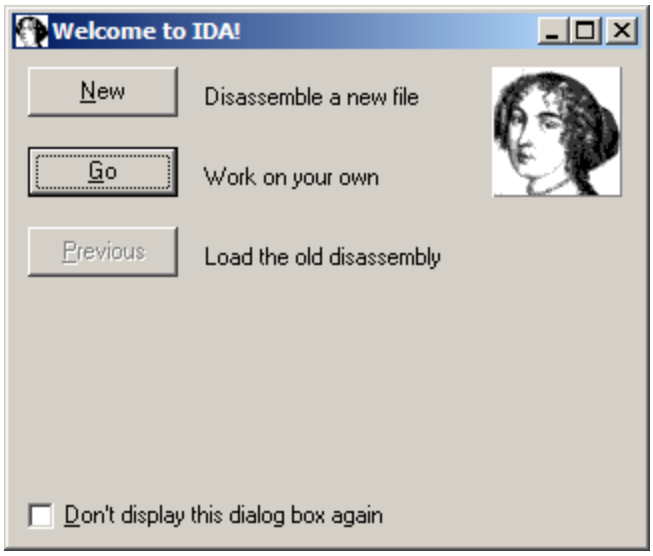
```
debugStub.listen.guest32 = "TRUE"
debugStub.hideBreakpoints= "TRUE"
monitor.debugOnStartGuest32 = "TRUE"
```

Save the file.

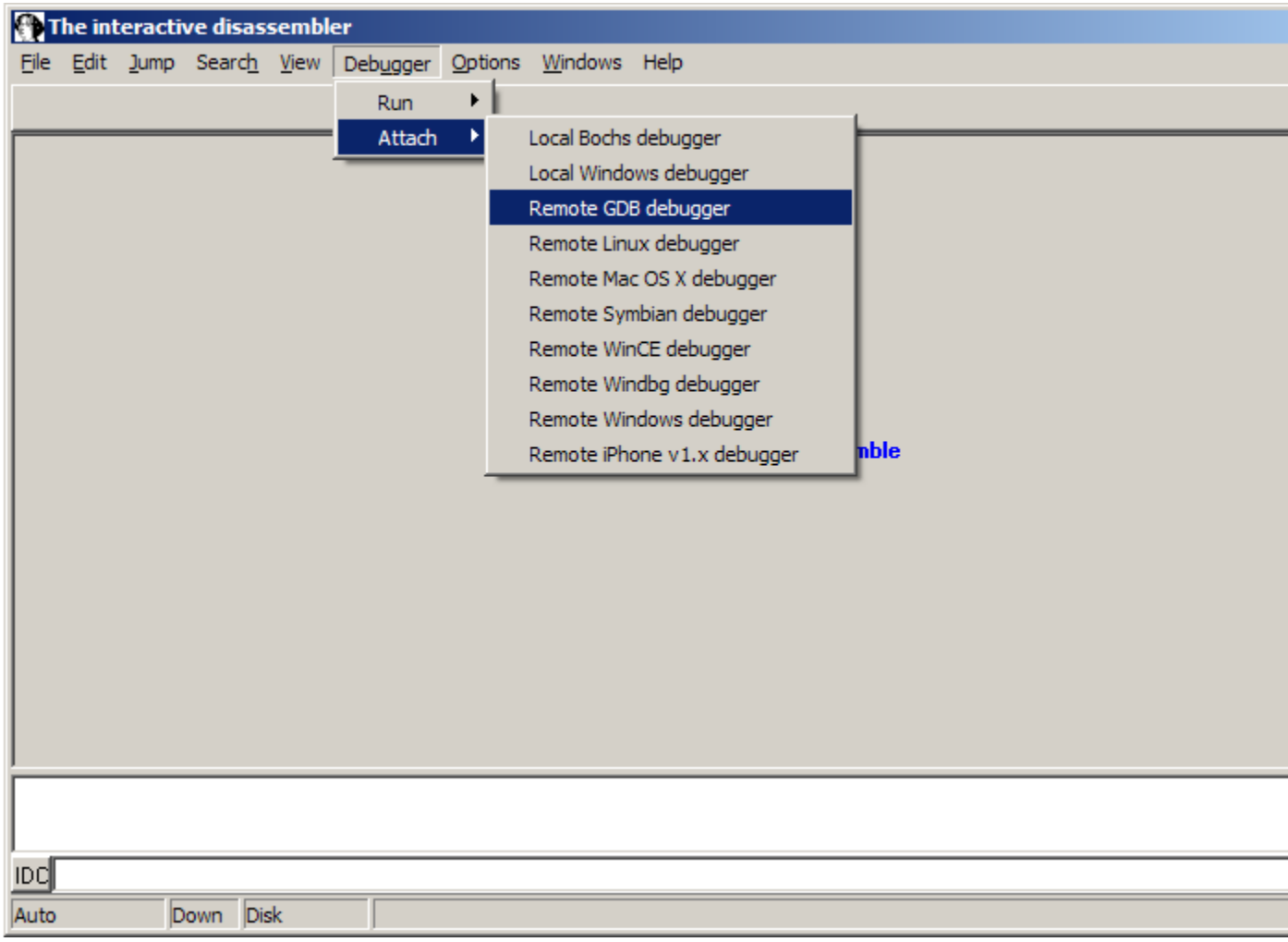
In VMWare, click "Power on this virtual machine" or click the green Play button on the toolbar.

A black screen is displayed since VMWare is waiting for a debugger to connect.

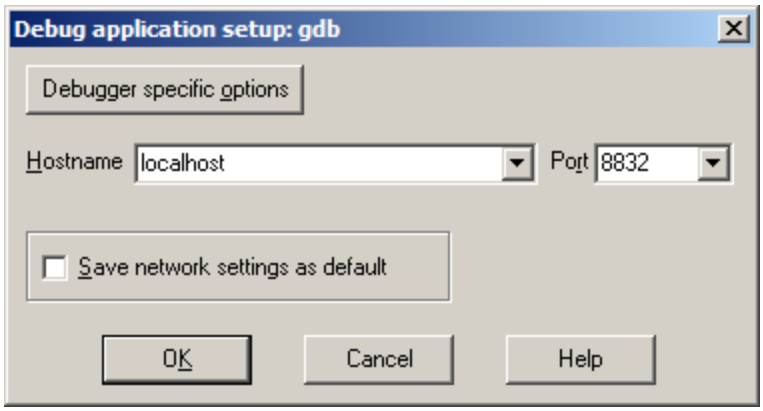
Start IDA.



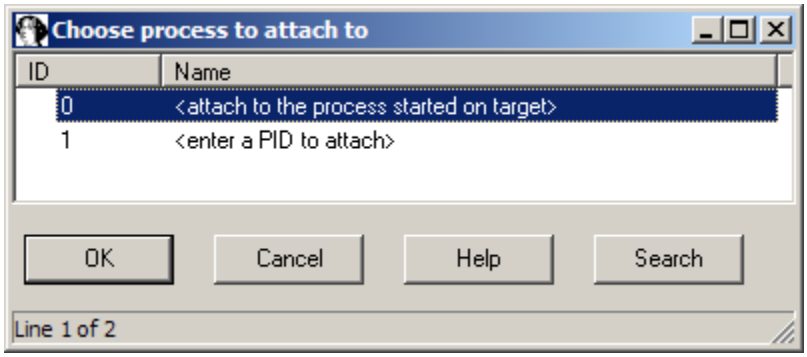
If you get the welcome dialog, choose "Go".



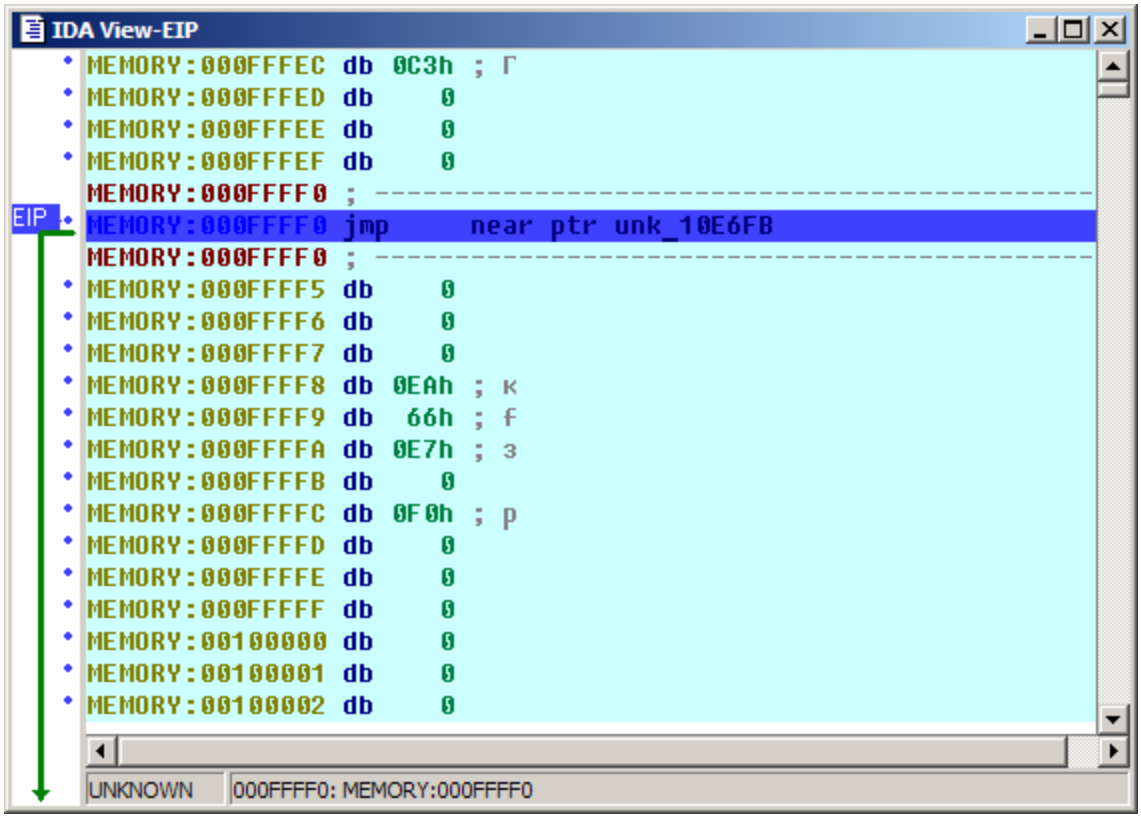
Choose Debugger | Attach | Remote GDB debugger.



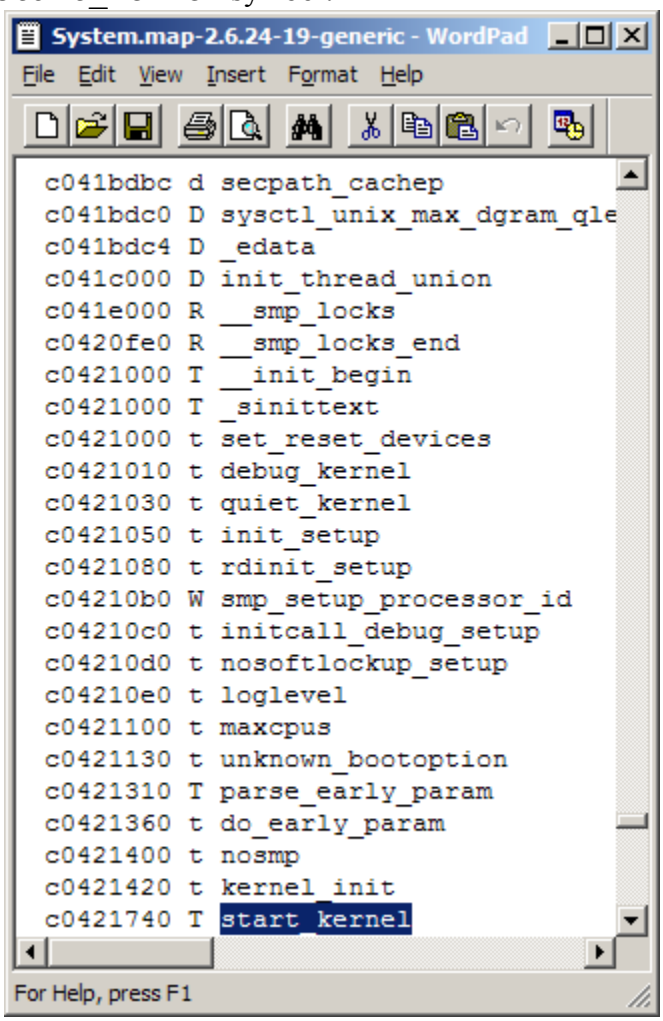
Enter "localhost" for hostname and 8832 for the port number.



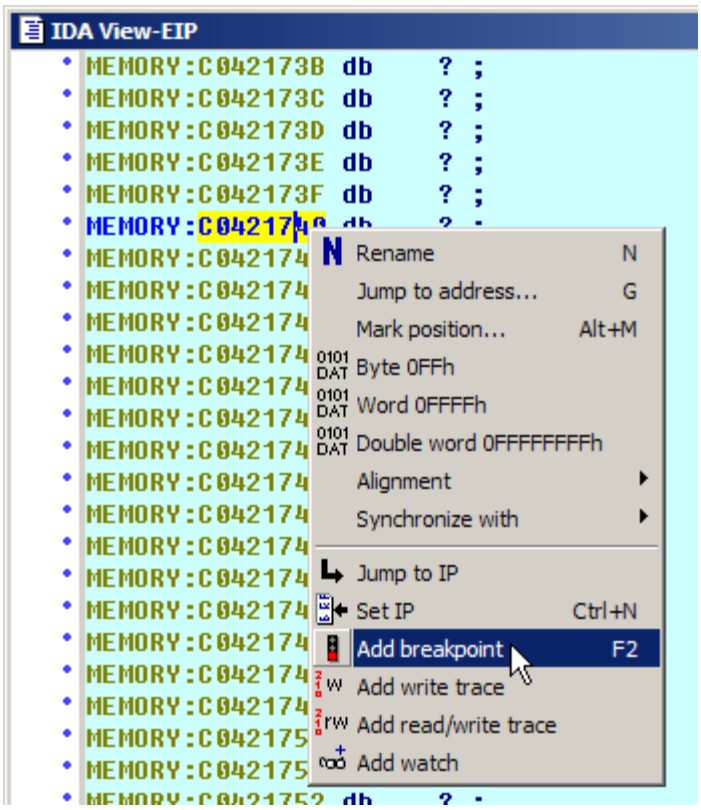
Choose <attach to the process started on target> and click OK.



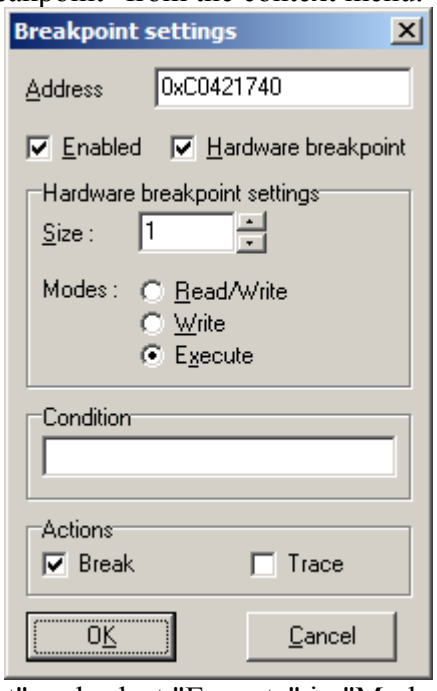
We land in the BIOS, but since we're not interested in debugging it, we can skip directly to the kernel. Inspect the kallsyms or System.map file you downloaded from the guest and search for the `start_kernel` symbol:



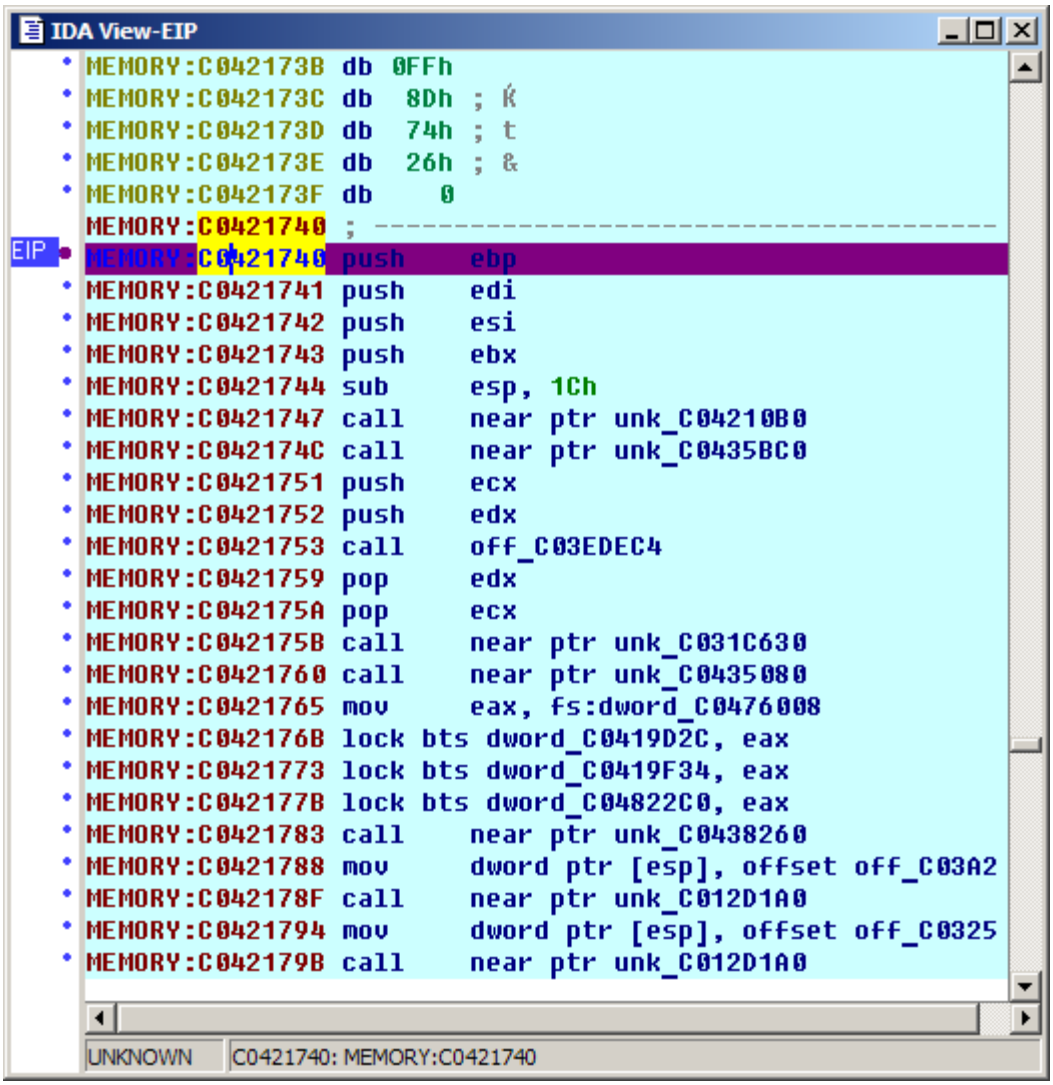
Copy the address, and navigate to it in IDA (Jump | Jump to addres... or just "g").



Press F2 or choose "Add breakpoint" from the context menu.



Check "Hardware breakpoint" and select "Execute" in "Modes". Click OK. Press F9. You will see loading messages and then the execution will stop at the entrypoint.



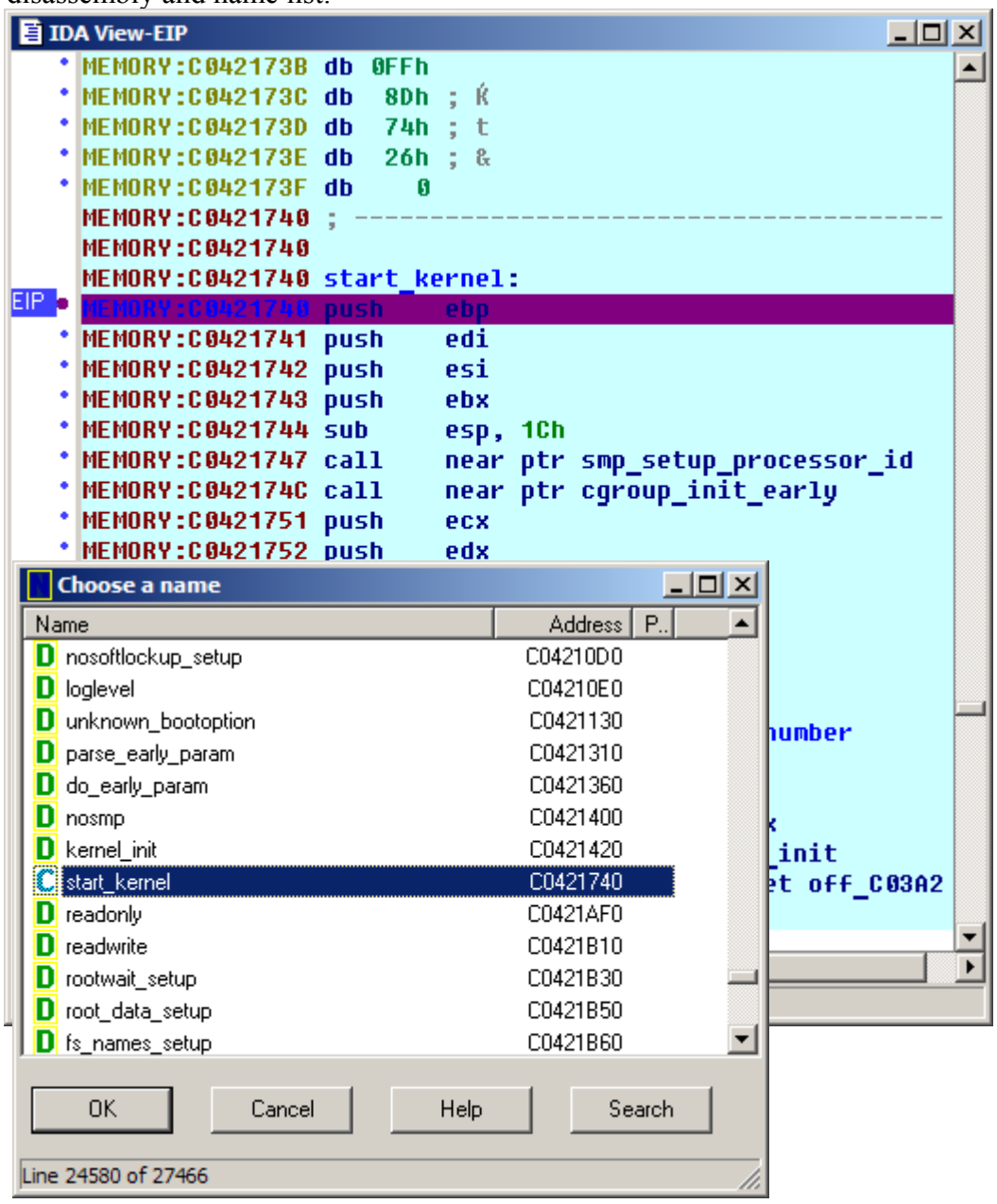
Adding symbols

Symbols are very useful during debugging, and we can use the kallsyms or System.map file to add them to IDA. Go to File | Python command... and paste the following short script (don't forget to edit the file path):

```
ksyms = open(r"D:\kallsyms") # path to the kallsyms/map file
for line in ksyms:
  if line[9]=='A': continue # skip absolute symbols
  addr = int(line[:8], 16)
  name = line[11:-1]
  if name[-1]==']': continue # skip module symbols
  idaapi.set_debug_name(addr, name)
  MakeNameEx(addr, name, SN_NOWARN)
  Message("%08X: %s\n"%(addr, name))
```

Click OK and wait a bit until it finishes. After that you should see the symbols in the

disassembly and name list:



Happy debugging!