

Topics: Viewing Process and Thread Attributes and Activity.
Using different Tools for Monitoring System Activity.

Exercise 1 (may still be changed)

Install your own virtual machine as follows:

- Boot and log in to Linux.
- Create your own directory for the virtual machine:
mkdir /usr/local/VmWare/work/<dir>
cd /usr/local/VmWare/work/<dir>
- Unpack the virtual machine into your own directory:
tar xzvf ../../OS-WinXP/OS-WinXP.tgz
- Boot the virtual machine by double-clicking on the .vmx file .

The virtual machine contains a Windows XP operating system including

- the Windows Support Tools (from the XP installation CD),
- the Debugging Tools for Windows (free download from MS),
- livekd.exe (free download from www.sysinternals.com) in the directory C:\Programme\Debugging Tools for Windows,
- Visual Studio 2005.

Further tools or programs for the lab assignments will be provided on my web pages.

Exercise 2

Using the normal Windows Task Manager, answer the following questions:

- a) How many processes and threads are there on the system?
- b) What are the minimum and maximum number of threads in a process (which processes)?

Exercise 3

Start the program in C:\Kits\sysinternals\ProcessExplorer 10\procxp.exe (free download from sysinternals.com), which extends the functionality of the Windows Task Manager.

- a) Get an overview of which information about processes is available in Task Manager (Processes Tab, View -> Select Columns), then do the same for the Process Explorer (also View -> Select Columns).
- b) In Process Explorer, add the columns for "CPU time" and "Context Switch Delta". Observe how the values in those columns change. What does look strange here? Do you have an explanation for this behavior? (There actually are two reasons. The second one will be explained in the chapter about Scheduling.)
- c) Double-click on one of the processes to see detailed information about the threads of this process. Again, get an overview of which information is available here.
- d) Give an explanation for the line labeled "Interrupts" in Process Explorer and for the (only possible) meaning of Context Switch Delta in this case.

Exercise 4

Start the Live Kernel Debugger `livekd.exe` (from www.sysinternals.com) available in `C:\Programme\Debugging Tools for Windows`.

- a) To get an idea of the data structures used to implement a process, use the command `dt _eprocess`, and then `dt _kprocess` to view the fields of the most interesting substructure, the process control block (PCB). Read through the names of the fields in the structure to see which ones you can understand. These commands show the layout (format) of the blocks, not any actual contents. To view the contents of an actual process block, use `dt _eprocess <address of EPROCESS structure>`. The addresses of all EPROCESS structures can be obtained with the command `!process 0 0`. The corresponding commands for threads are `dt _ethread` and `dt _kthread`.
- b) Use the `!idt` command to look at the contents of the Interrupt dispatch table. What information is contained there?

Exercise 5

Get the programs `CreateThreads_def.exe` (and/or `CreateThreads_def_slow.exe`), and `CreateThreads_mod.exe` from my website. Both programs create threads in an infinite loop (the "slow" one with waits in between), one using the default value for one particular parameter, the other using a modified value for this parameter.

- a) Run `CreateThreads_def[_slow].exe`. Which error message do you get after the creation of how many threads?
- b) The error message is somewhere between imprecise and misleading. Add some memory related columns to both Task Manager and Process Explorer (make an "educated guess" or add all columns), and watch the running program. Note which counters go up.
- c) One of the counters going up in Task Manager is the one for the "Nonpaged Pool", which shows the use of memory resident operating system data caused by the process. Why does the program need (quite a lot of) space in the Nonpaged Pool? However, the reason for the error is not the exhaustion of this pool.
- d) Which of the counters indicates the cause of the error message, and why does this cause an error?
- e) Verify your conclusions from part d) by running `CreateThreads_mod.exe`, which will be able to create more threads, but then run into the same error, and hence should show the same behavior in Process Explorer.
- f) Deduce from your results which parameter value was changed in this program, and also give the numerical values used for this parameter by default, and in the modified program.

Turn in the solutions to **Exercises 2, 3b, 3d, 4b, and 5** on paper, in groups of at most two students (either in English or German). The **due date** will be announced in class.

Beachten Sie den **Beschluss der Prüfungskommission**:

"Ab sofort sind alle Studienarbeiten und Leistungsnachweise mit einer Erklärung des Studierenden zu versehen, dass er/sie die Arbeit selbständig verfasst, keine anderen als die angegebenen Quellen oder Hilfsmittel benutzt sowie wörtliche und sinngemäße Zitate als solche gekennzeichnet hat. Diese Erklärung ist vom Studierenden zu unterschreiben. "