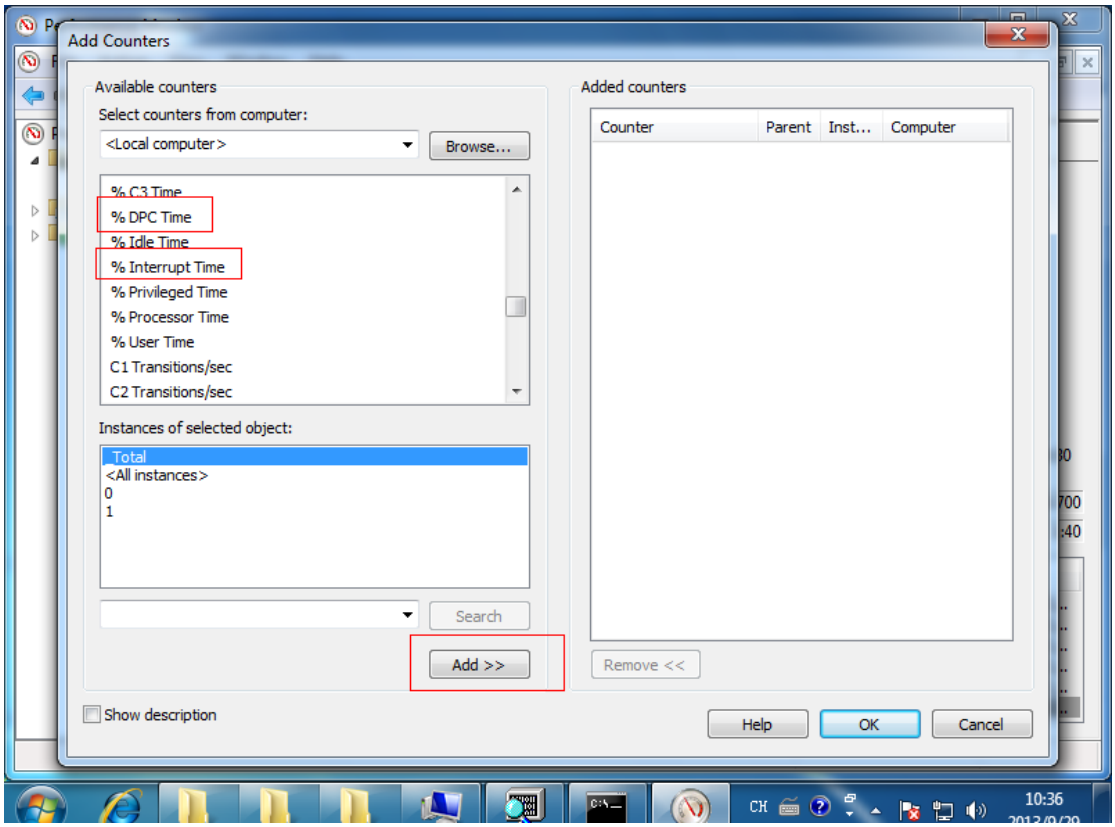
CS490 Windows Internals Lab

Sept 29, 2013

Monitoring DPC

Using Process Explorer

Monitoring interrupts/sec, %Interrupt time, %DPC time, and other DPC, which are under the category of ***Processor***.



Synchronization in Windows

Viewing Global Queued Spin-locks

You can view the state of the global queued spin-locks (the ones pointed to by the queued spin-lock array in each processor's PCR) by using the !qlock kernel debugger command. This command is meaningful only on a multiprocessor system because uni-processor HALs don't implement spin-locks.

In the following example, taken from a Windows 7 system, no queued spin-locks are acquired.

```
lkd> !qlocks
Key: O = Owner, 1-n = Wait order, blank = not owned/waiting, C = Corrupt

                         Processor Number
    Lock Name          0   1   2   3

KE   - Dispatcher
MM   - Expansion
MM   - PFN
MM   - System Space
CC   - Vacb
CC   - Master
EX   - NonPagedPool
IO   - Cancel
EX   - WorkQueue
IO   - Vpb
IO   - Database
IO   - Completion
NTFS - Struct
AFD  - WorkQueue
CC   - Bcb
MM   - NonPagedPool
```

Looking at Waiting Threads

Use the pstat command, you can see waiting threads in detail. From the state column, you can see what one thread is waiting.

```
D:\Desktop\Windows_Internal_Lab\CRK-Tools>pstat
```

```
pid:a70 pri: 8 Hnd:  153 Pf:   1819 Ws:   4664K svchost.exe
 tid pri Ctx Swtch StrtAddr    User Time  Kernel Time  State
 a74   9          32 771D6328  0:00:00.000  0:00:00.000 Wait:UserRequest
 a78  10        3921 771D6328  0:00:00.000  0:00:00.031 Wait:UserRequest
 a88   9          15 00000000  0:00:00.000  0:00:00.000 Wait:EventPairLow
 a9c  10         161 00000000  0:00:00.000  0:00:00.000 Wait:UserRequest
 aa0   9        1981 00000000  0:00:00.093  0:00:00.015 Wait:UserRequest
 aa4   9           9 771D6328  0:00:00.000  0:00:00.000 Wait:UserRequest
 af8   8         109 771D6328  0:00:00.000  0:00:00.000 Wait:LpcReceive
 afc   8         185 771D6328  0:00:00.000  0:00:00.000 Wait:UserRequest
 fdc   8           9 00000000  0:00:00.031  0:00:00.031 Wait:UserRequest
 b2c   9         198 771D6328  0:00:00.000  0:00:00.000 Wait:EventPairLow
 ed8   8           1 771D6328  0:00:00.000  0:00:00.000 Wait:EventPairLow

pid:b6c pri: 8 Hnd:  607 Pf:   7122 Ws:   6784K SearchIndexer.exe
 tid pri Ctx Swtch StrtAddr    User Time  Kernel Time  State
 b70   9         125 00000000  0:00:00.000  0:00:00.000 Wait:UserRequest
 b74   8         630 771D6328  0:00:00.000  0:00:00.000 Wait:UserRequest
 b80  13         498 771D6328  0:00:00.078  0:00:00.031 Wait:UserRequest
 b98   8          59 771D6328  0:00:00.000  0:00:00.000 Wait:EventPairLow
 ba0   8           2 771D6328  0:00:00.000  0:00:00.000 Wait:UserRequest
 ba8   8         322 00000000  0:00:00.000  0:00:00.000 Wait:UserRequest
 bac   8         441 771D6328  0:00:00.000  0:00:00.000 Wait:UserRequest
 bb0   8         434 771D6328  0:00:00.015  0:00:00.000 Wait:UserRequest
 bb4   9       22161 771D6328  0:00:00.187  0:00:00.561 Wait:UserRequest
 c04   8         648 771D6328  0:00:00.000  0:00:00.015 Wait:EventPairLow
 df4   8          49 771D6328  0:00:00.000  0:00:00.000 Wait:EventPairLow
 e44   8          10 771D6328  0:00:00.000  0:00:00.000 Wait:EventPairLow
```