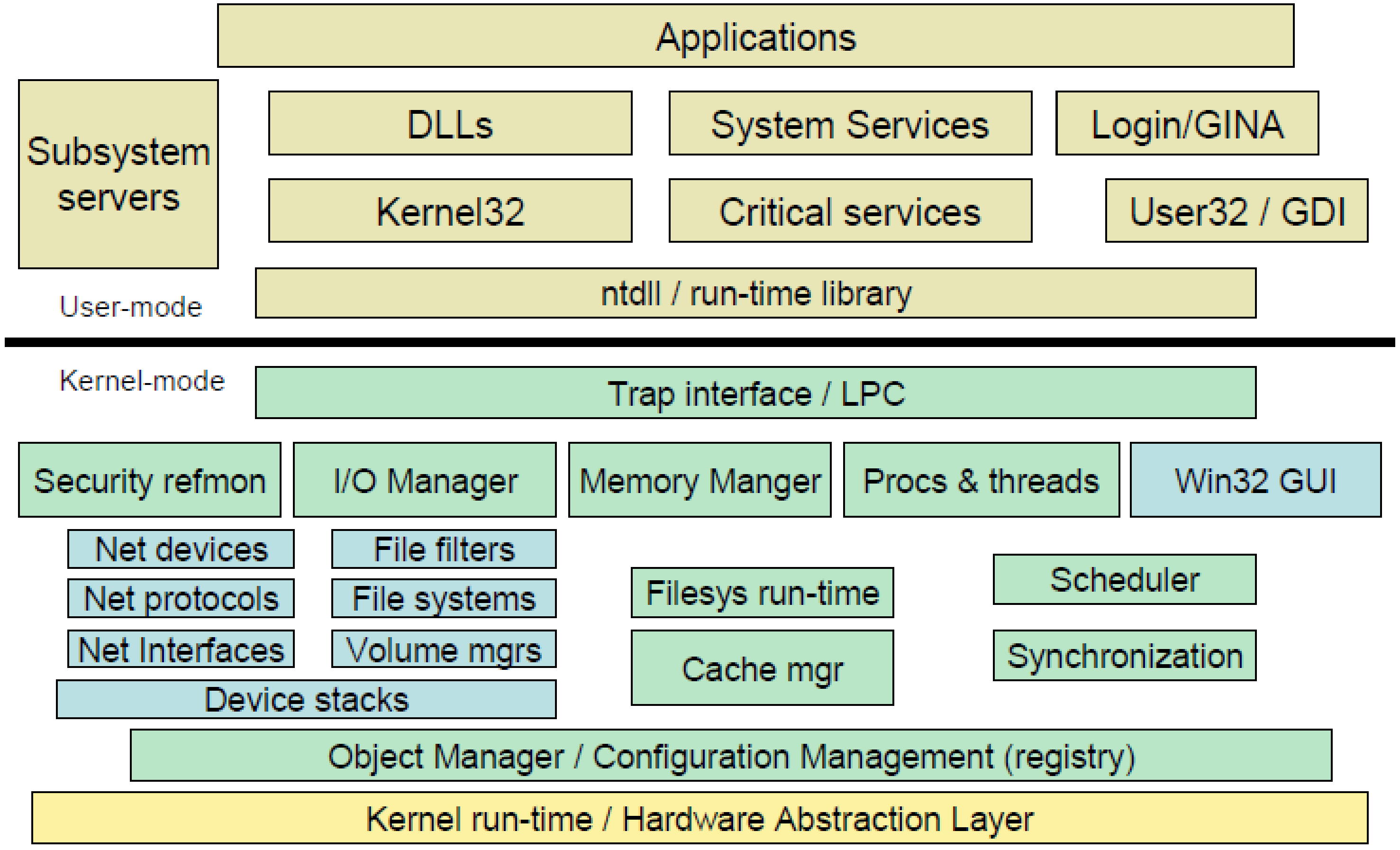
Windows 101

Processes, Memory

Windows Architecture



v3

Source: https://blogs.msdn.microsoft.com/hanybarakat/2007/02/25/deeper-into-windows-architecture/

Process Execution

- Represents an instance of running program
- Process defined by
  - Address space
  - Resources (e.g. open handles)
  - Security profile (token)
- System Call
  - Primary argument to CreateProcess is image file name (or even command line)

Threads

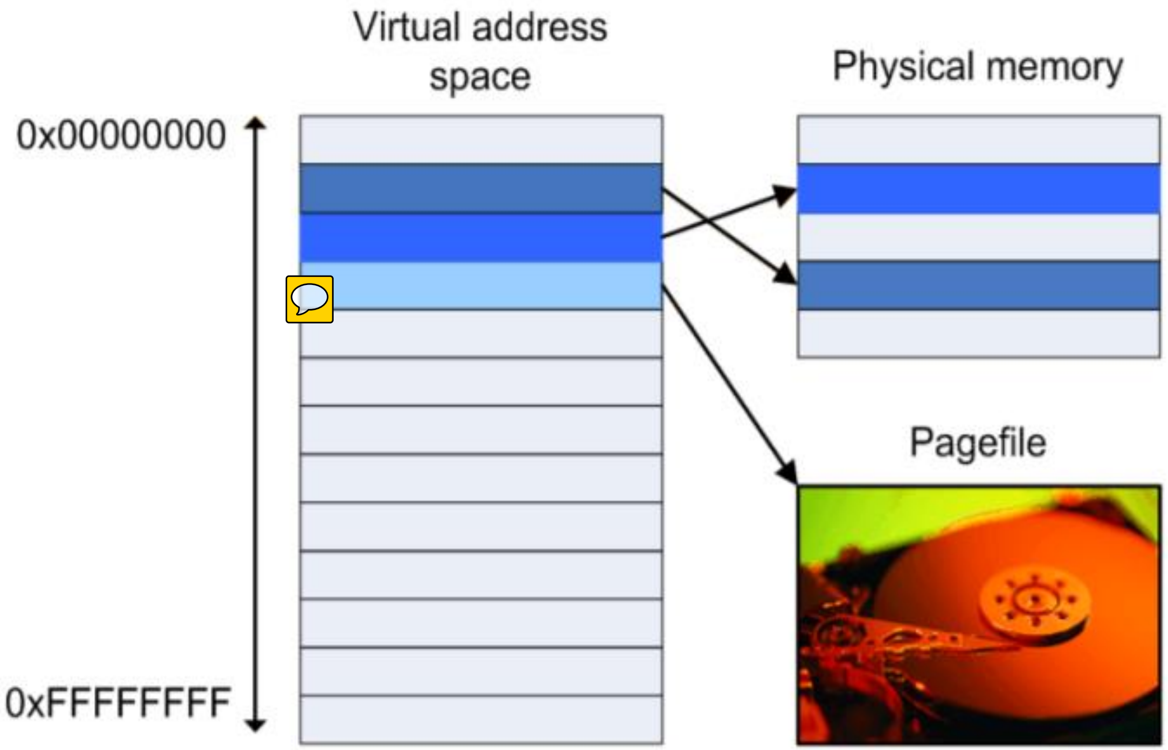
- Thread is an execution context within a process
- Threads share same per-process address space
- Threads in system are scheduled as peers to all others
- System call
    - Primary argument to CreateThread is a function entry point address

Memory Management

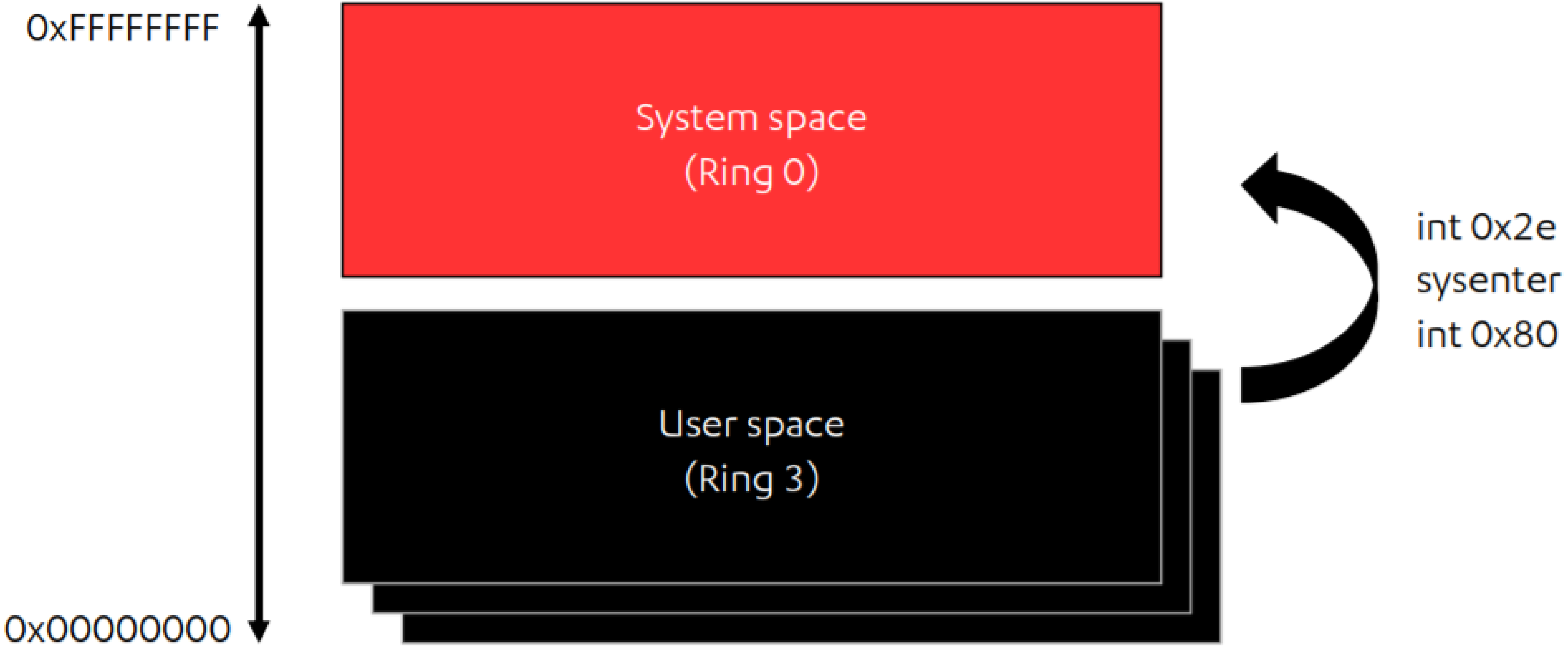
- Each processes sees a large and contiguous private address space
- Has two important tasks
  - Mapping access to virtual memory into physical memory
  - Paging contents of memory to disk as physical memory runs out and paging back when needed

Virtual Memory

- Each process has its own virtual address space
- Provides logical view of memory that not correspond to physical layout
- Virtual memory can exceed available physical memory



Kernel Mode and User Mode Memory


0xFFFFFFFF
System space
(Ring 0)
int 0x2e
sysenter
int 0x80
User space
(Ring 3)
0x00000000