

4417/5417

System Administration

Lecture 3
OS Concepts



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Outline

32 or 64 bit?

Windows Architecture

Linux Architecture

Processes and threads

Linux / Windows

Next class



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Modern OS Architecture

32 bit Vs 64 bit OS

Processor, MB, and OS all need to support

Number of address lines on the CPU

32 = 4 gigabytes

64 = 16 million terabytes

Move more data efficiently per clock cycle

2008 R2 / 2012 R2 only 64bit

Linux = both



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Modern OS Architecture

32-bit vs. 64-bit OS and Processor

- 32-bit Windows Operating System and x86 Processor Architecture
 - Capable of addressing 4 GB of RAM
 - Each virtual machine receives 1 MB of memory and access to hardware
 - x86 uses a Complex Instruction Set Computer (CISC)
 - x86 processors use fewer registers than x64 processors
- 64-bit Windows Operating System and x64 Processor Architecture
 - Capable of addressing 128 GB of RAM
 - Enhanced performance for memory management
 - Additional security features
 - x64 architecture is backward compatible with x86
 - Process much more complex instructions at a much higher rate

Windows



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Windows Architecture

Two Major Components

User

Kernel

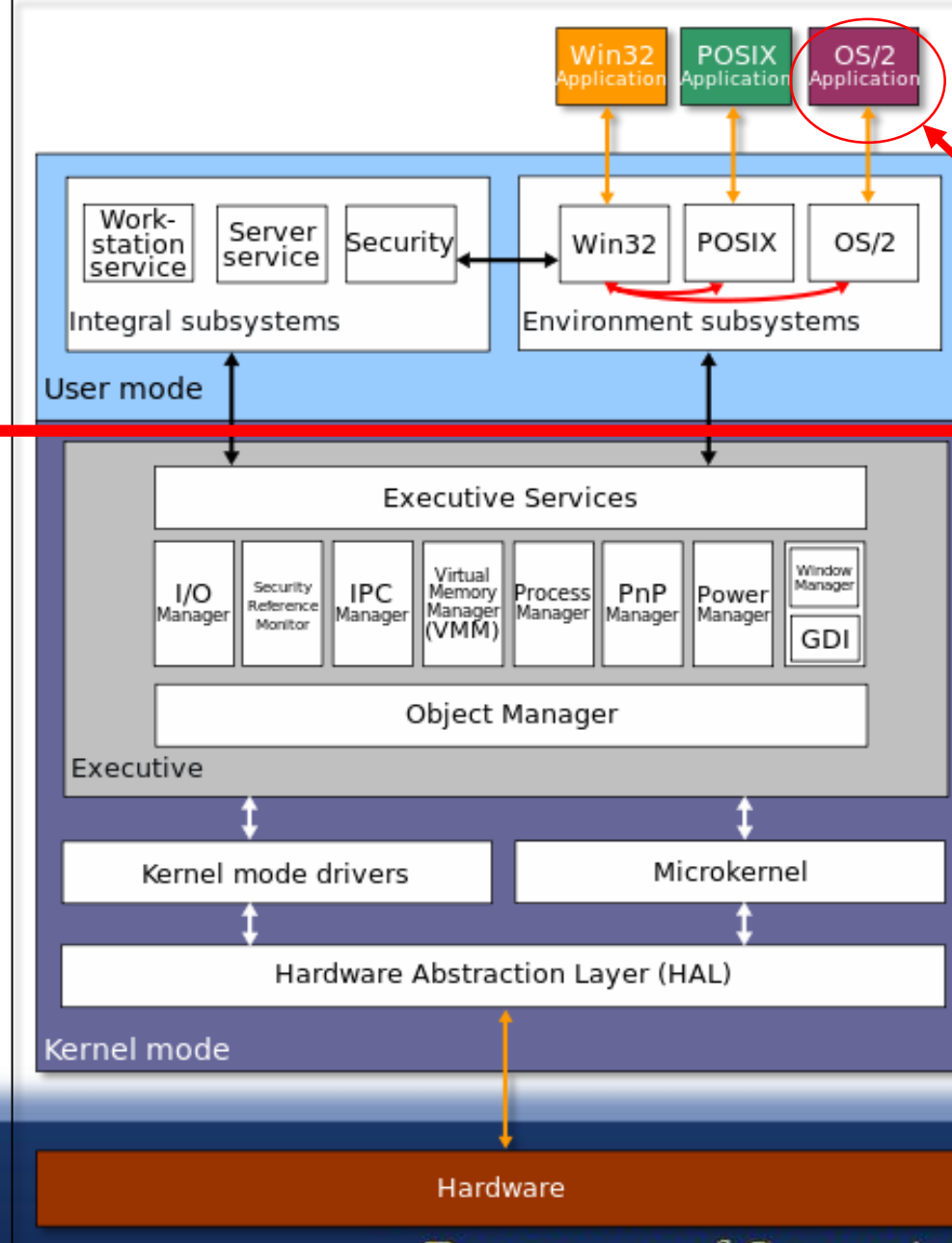
Preemptive multi-threaded architecture (eh?)

Apps -> user mode -> kernel mode -> HW



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

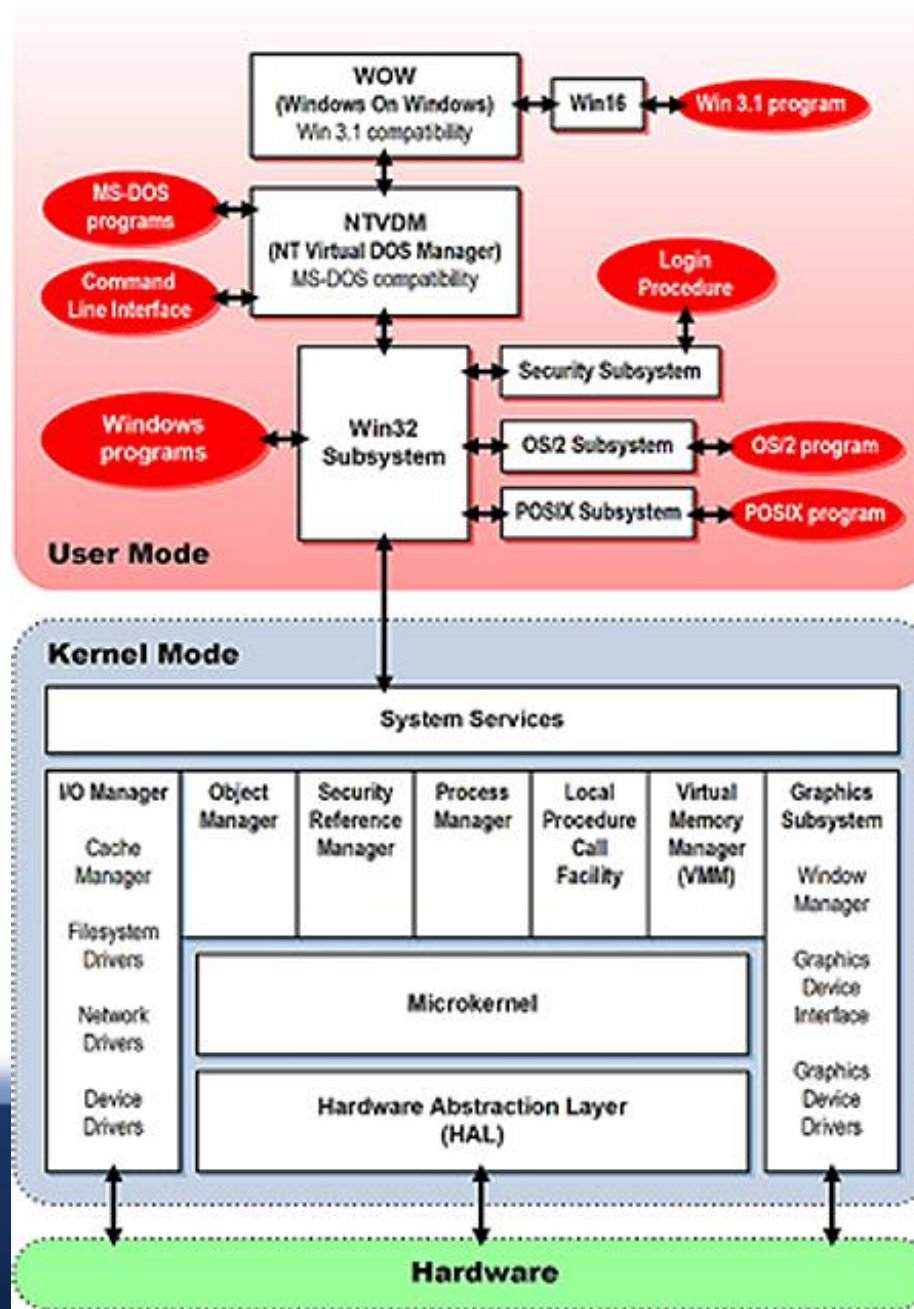
Windows Architecture



No longer present,
Starting with XP

POSIX (Portable Operating System Interface) is a set of standard operating system interfaces based on the Unix operating system.

Windows Architecture



User Mode

Applications programs run in user mode:

No direct access to hardware

Programs are limited to assigned memory address spaces

The Win32 subsystem is the primary application subsystem. All 32-bit Windows applications run in the Win32 Subsystem.

Programs use Win32's Application Program Interface (API) to request system services from a kernel mode component. This protects applications from crashing the system, and against unauthorized user access.



User Mode

DOS and Windows 16-bit applications are handled by a series of nested subsystems (culminating as always with the Win32 Subsystem)

The NT Virtual DOS Machine (NTVDM) provides a DOS-compatible environment for DOS programs

16-bit Windows program communicate first with a subsystem designed to handle such applications

16-bit system calls; these calls are converted to the 32-bit calls used by Windows NT in a subsystem called Windows on Win32 (WOW).

These applications also require a NTVDM environment because they also depend on DOS services



User Mode

In 64-bit versions of Windows the main subsystem is Win64

A Windows-on-Win64 (WoW64) subsystem allows 32-bit programs to interact with the 64-bit Windows executive. Thus programs designed for Win32 can run on Win64

The OS/2 and Posix subsystems allow Windows to run programs built for OS/2 or Posix operating systems, where supported

Security Subsystem supports the logon process. The Security Subsystem also communicates with the Win32 Subsystem



Kernel Mode

All code that runs in kernel mode can:

Access the hardware directly

Access all memory.

The entire set of services that comprise kernel mode is called Executive Services (or sometimes the Windows NT Executive).

The I/O Manager controls most input and output on the system.

The Object Manager creates, modifies and deletes system objects. These objects represent a specific instance of a resource (for example, a file, a process, or a port).



Kernel Mode

The Security Reference Manager (SRM) is responsible for enforcing system security settings by granting or denying access to objects and system resources upon request from the Object Manager. This process relies on data structures known as security access tokens (SATs)

The Process Manager creates and manages system processes. However, process scheduling is handled by the microkernel

The Local Procedure Call Facility is responsible for communication between processes



Kernel Mode

The Virtual Memory Manager handles the allocation and use of the system's memory. Virtual memory is the physical space on a hard disk that NT treats as though it were RAM. Virtual memory can also be thought of as an extension of RAM, or "fake" RAM. Memory is divided into 'pages' and is stored in a pagefile on disk

Window Manager is responsible for providing all of the GUI. It communicates directly with the Graphics Device Drivers, which in turn communicate directly with hardware

The five other kernel mode subsystems communicate directly with the microkernel, the very heart of the NT operating system. It handles interrupts, schedules threads, and synchronizes processing activity. The microkernel, in turn, communicates with the hardware abstraction layer (HAL)



The Kernel

Handles basic I/O

Interfaces between Executive Services and HW

ntoskrnl.exe



64 bit Windows

64 bit OS, 64 bit CPU, 64 bit App = native

64 bit OS, 64 bit CPU, 32 bit App = VM

WOW64 (Windows On Windows)

Creates mini VMs for each 32 bit app on a 64 bit OS

Wow64.dll is loaded to be the middle man between the 32 bit app and the 64 bit OS



Linux



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

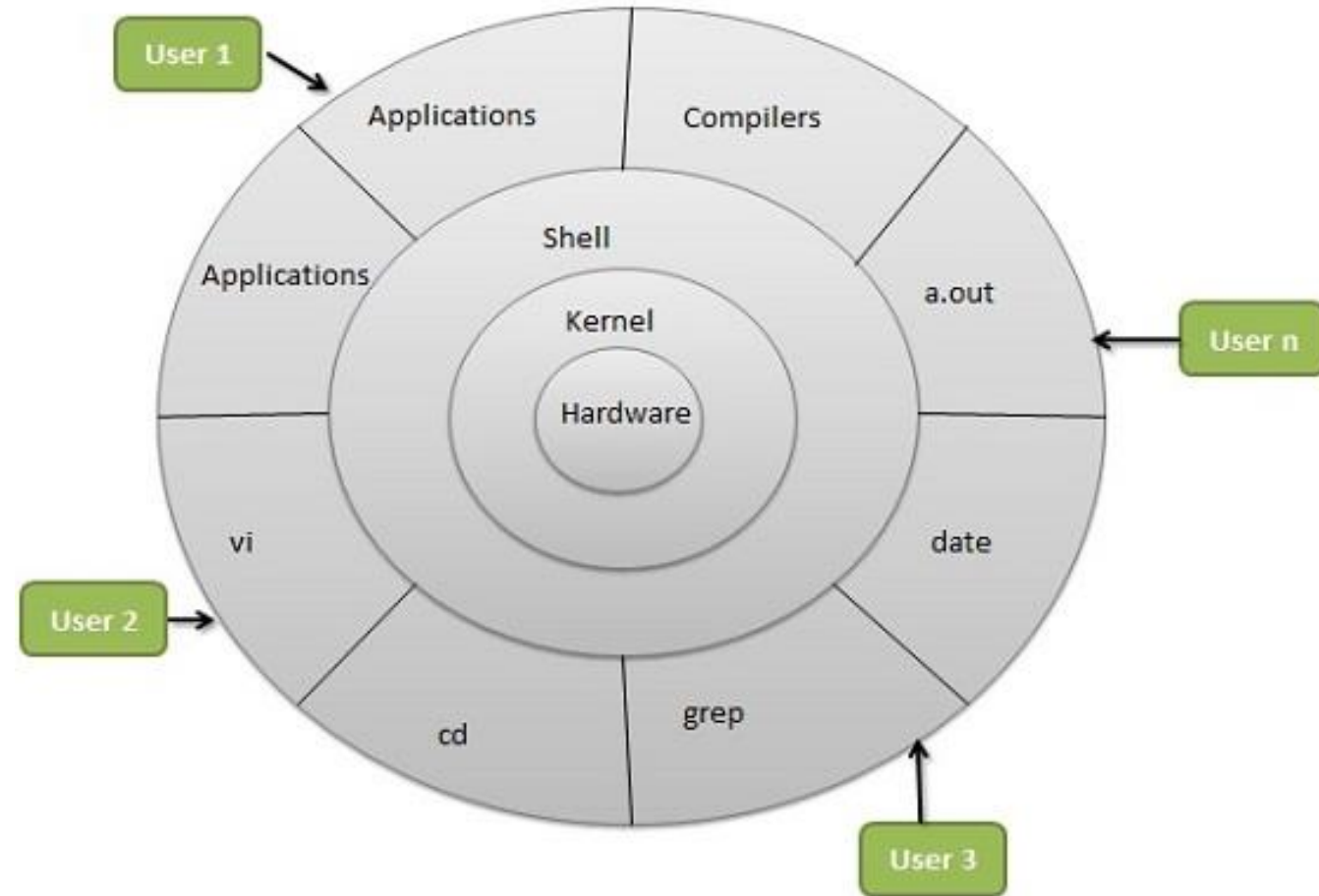
A View from Linux

Hardware layer - Hardware consists of all peripheral devices (RAM/ HDD/ CPU etc).

Kernel - Core component of Operating System, interacts directly with hardware, provides low level services to upper layer components.

Shell - An interface to kernel, hiding complexity of kernel's functions from users. Takes commands from user and executes kernel's functions.

Utilities - Utility programs giving user most of the functionalities of an operating system.



* http://www.tutorialspoint.com/operating_system/os_linux.htm

Linux Features

Portable - software works on different types of hardware in same

Open Source - Linux source code is freely available and it is community based development project.

Multi-User - multiple users can access system resources like memory/ram/ application programs at same time.

Multiprogramming - multiple applications can run at same time.

* http://www.tutorialspoint.com/operating_system/os_linux.htm



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Linux Features

Hierarchical File System - standard file structure in which system files/ user files are arranged.

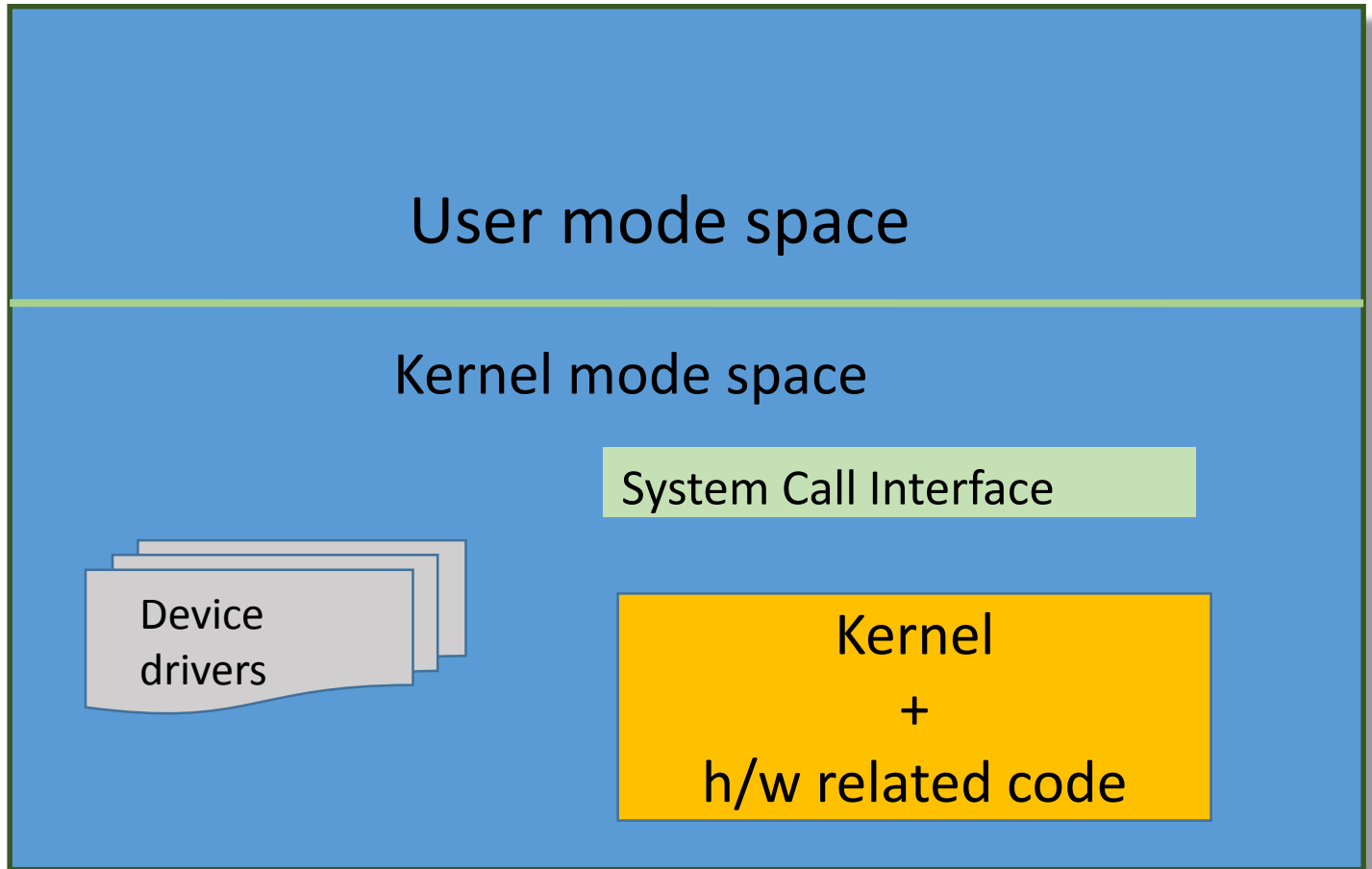
Shell - Linux provides a special interpreter program which can be used to execute commands of the operating system. It can be used to do various types of operations, call application programs etc.

Security - Linux provides user security using authentication features like password protection/ controlled access to specific files/ encryption of data.

* http://www.tutorialspoint.com/operating_system/os_linux.htm



System Structure (Simplified)



Processes



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Processes

Program vs. Process

A program is a static sequence of instructions

A process is a container for a set of resources used to execute a program*

*Russinovich, M. & Margosis, A. (2011). *Windows Sysinternals Administrator's Reference*. Redmond, WA: Microsoft Press.



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Processes

Process is comprised of address space and data (instructions)

Address spaces allocated in pages

Pages may reside in virtual memory (nothing to do with VMware Player) and physical memory

Virtual memory referred to as swap space or pagefile



Processes

Virtual memory is a feature of an operating system (OS) that allows a computer to compensate for shortages of physical **memory** by temporarily transferring pages of data from random access **memory** (RAM) to disk storage.*

This is referred to as the swap space (vs. Windows' pagefile)

Separate partition on disk

*<http://searchstorage.techtarget.com/definition/virtual-memory>



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Processes

Process MAY = application

More accurately the part of an application that is running



Processes

The kernel keeps track of the following:

Processes address space

Current state of process (sleeping, running, etc)

Priority

Signal mask

Files and ports in use

Resource list

ID

owner



Threads

Part that runs on the processor

Processes fork threads to accomplish specific tasks

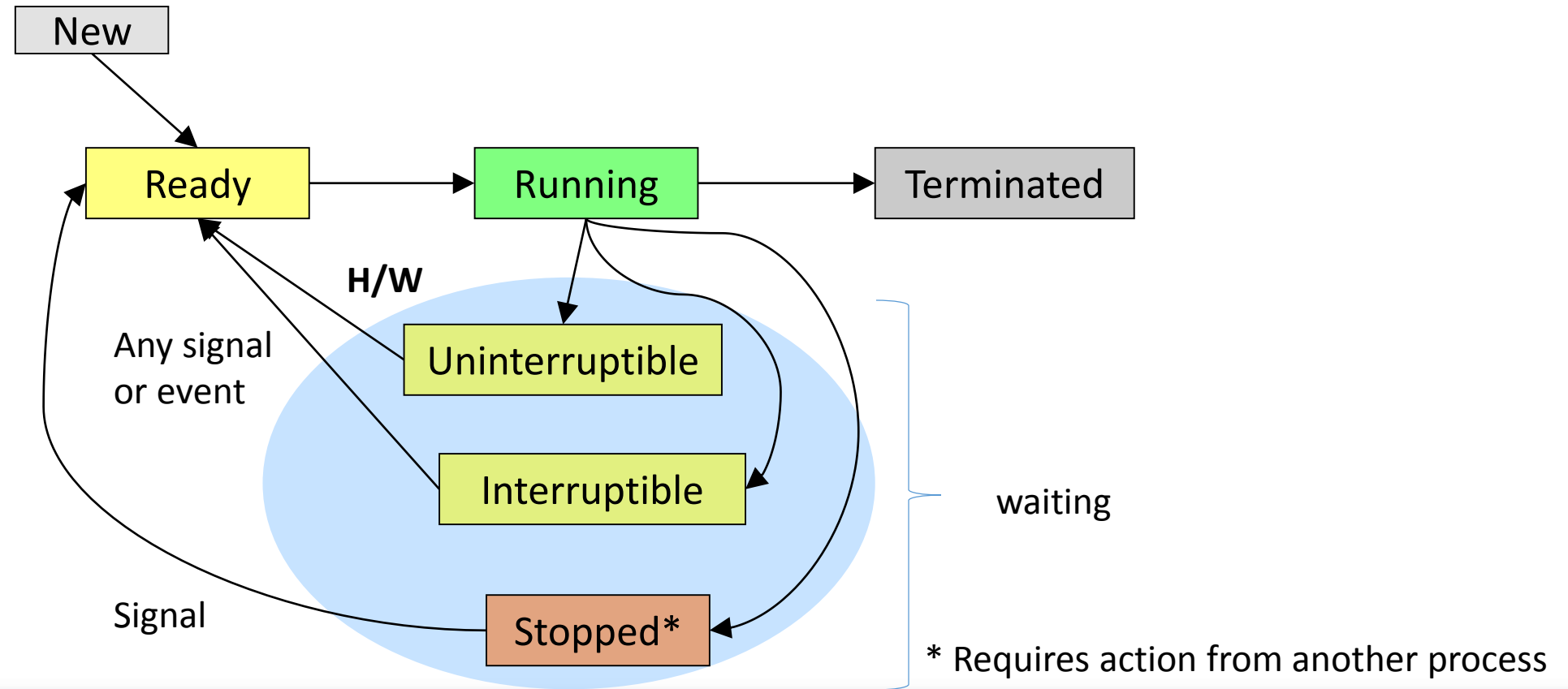
Inherits many attributes of the parent process

Multiple threads can run in parallel, hence

“Multithreaded OS”



Linux Process/Thread States



fork

1 process can spawn another process by issuing the `fork` command

The resulting child will then issue an `exec` command to start execution



init (SysV)

At system boot, in Linux, the kernel creates and installs the init process

PID = 1

Execute startup scripts

Similar to startup folder or other initialization registry entries in Windows



init (SysV)

Continues to run after startup

Handles calls to shut down or reboot

“As time went on, it became clear that init was getting too slow and inflexible for today’s computers.” *

*<http://www.zdnet.com/article/after-linux-civil-war-ubuntu-to-adopt-systemd/>



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Upstart - 2006

Canonical (the company that manages Ubuntu), created Upstart

Event-based replacement

Handles starting of tasks & services during boot, stopping them during shutdown & supervising them while running*

Last version release: 4 September 2014

*<http://upstart.ubuntu.com/>



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

systemd - 2010

freedesktop.org*

Starts system resources in parallel, instead of running a series of scripts

Supports System-V startup scripts

Same services as System-V, but faster

*<http://www.freedesktop.org/wiki/Software/systemd/>



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

systemd - 2010

Debate between Upstart supporters (Canonical wanted to make it the Linux standard) became what ZDNet describes as “heated” *

Eventually Canonical threw in the towel in favor of systemd

systemd is currently available as an option on Ubuntu (since 15.04)

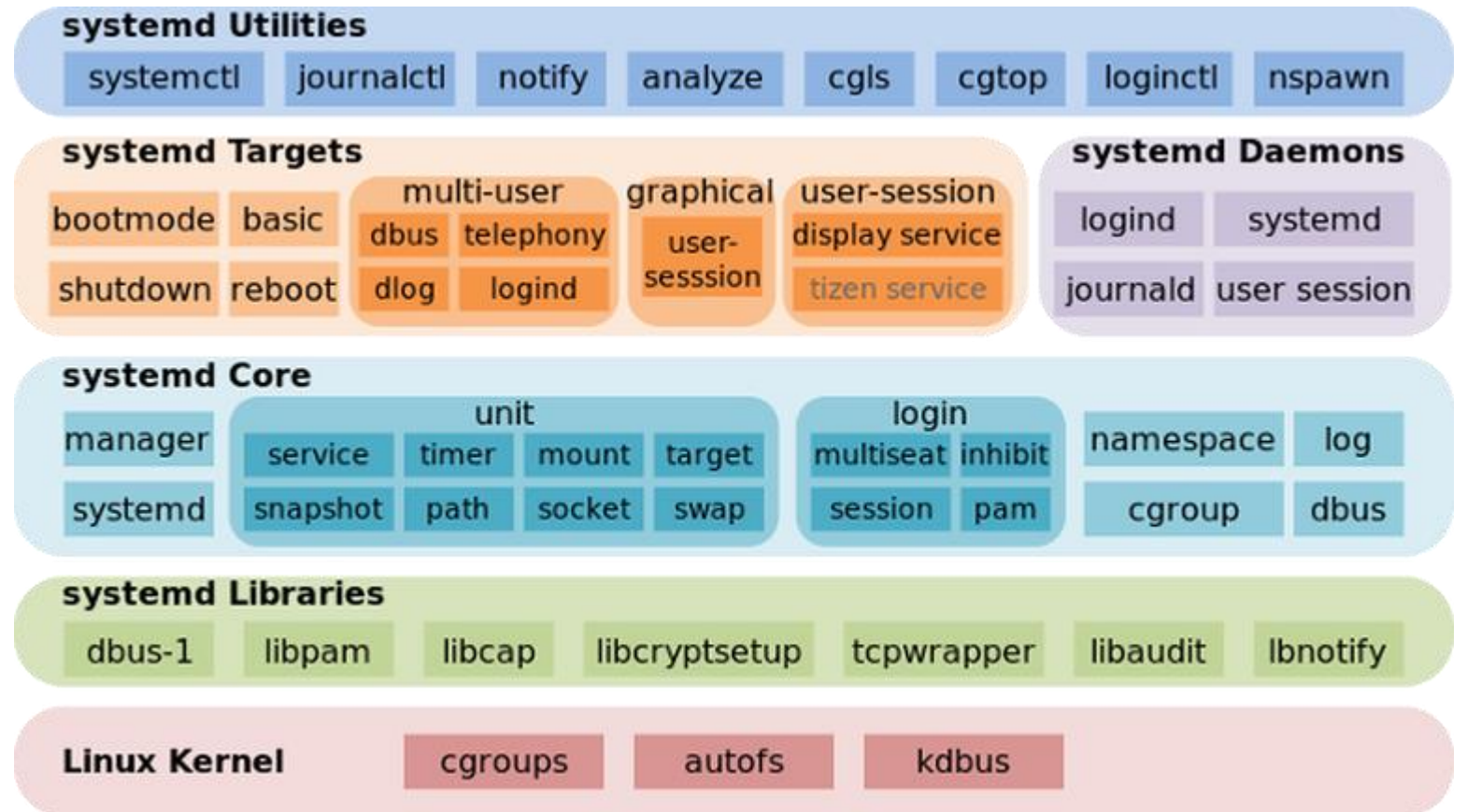
*<http://www.zdnet.com/article/after-linux-civil-war-ubuntu-to-adopt-systemd/>



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

systemd - 2010

*



*<http://www.zdnet.com/article/after-linux-civil-war-ubuntu-to-adopt-systemd/>



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Signals

Used for

- Process to process communication

- Kill, interrupt, suspend processes

- Admin kill

- Programming errors

- Notification of interesting occurrences within the OS

 - Death of a child

 - I/O channel is available



Ending a Process

Linux

kill -9 *pid*

Not graceful (SIGTERM
much more graceful), i.e.,

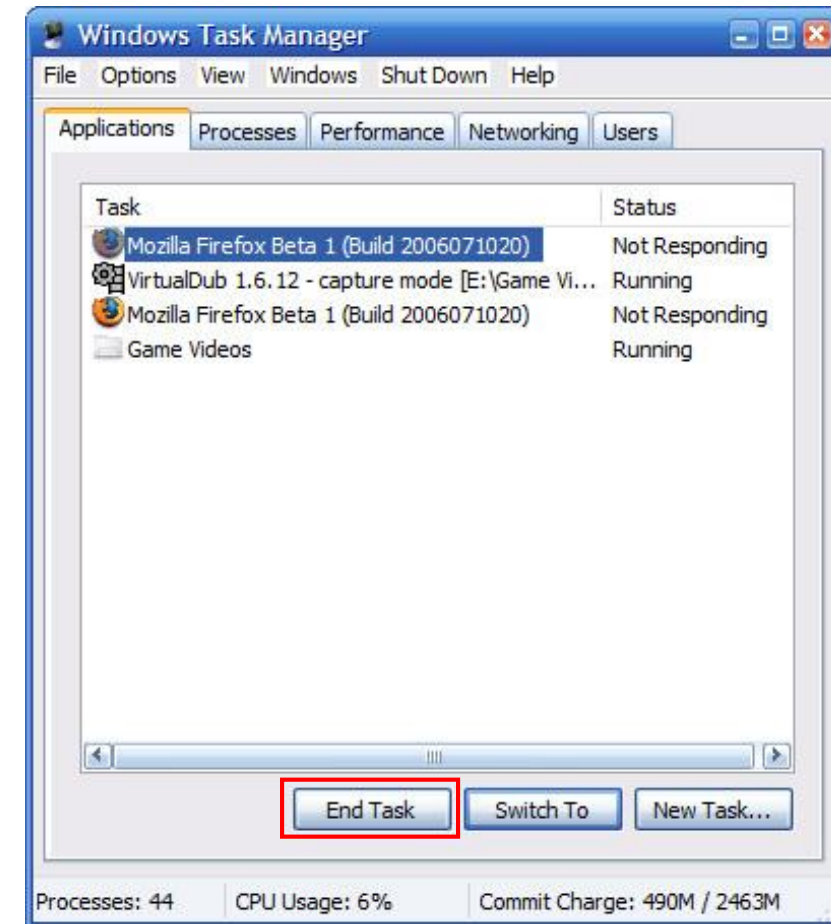
kill -s 15 *pid*

```
jack@jram: ~  
jack@jram:~$ ps aux | grep ping  
jack      2543  0.0  0.0 14884   964 pts/6    S+   07:43   0:00 ping yahoo.com  
jack      2546  0.0  0.0 15936   940 pts/16    S+   07:43   0:00 grep --color=au  
to ping  
jack@jram:~$ kill -s 15 2543  
jack@jram:~$  
  
jack@jram: ~  
=78.7 ms  
64 bytes from ir1.fp.vip.gq1.yahoo.com (206.190.36.45): icmp_seq=39 ttl=128 time  
=79.4 ms  
64 bytes from ir1.fp.vip.gq1.yahoo.com (206.190.36.45): icmp_seq=40 ttl=128 time  
=81.1 ms  
64 bytes from ir1.fp.vip.gq1.yahoo.com (206.190.36.45): icmp_seq=41 ttl=128 time  
=83.9 ms  
64 bytes from ir1.fp.vip.gq1.yahoo.com (206.190.36.45): icmp_seq=42 ttl=128 time  
=81.9 ms  
64 bytes from ir1.fp.vip.gq1.yahoo.com (206.190.36.45): icmp_seq=43 ttl=128 time  
=78.5 ms  
64 bytes from ir1.fp.vip.gq1.yahoo.com (206.190.36.45): icmp_seq=44 ttl=128 time  
=81.6 ms  
64 bytes from ir1.fp.vip.gq1.yahoo.com (206.190.36.45): icmp_seq=45 ttl=128 time  
=79.5 ms  
Terminated  
jack@jram:~$
```


Ending a Process

Windows Task Manager

Process Explorer provides more fine-grained control than TM



Listing Processes

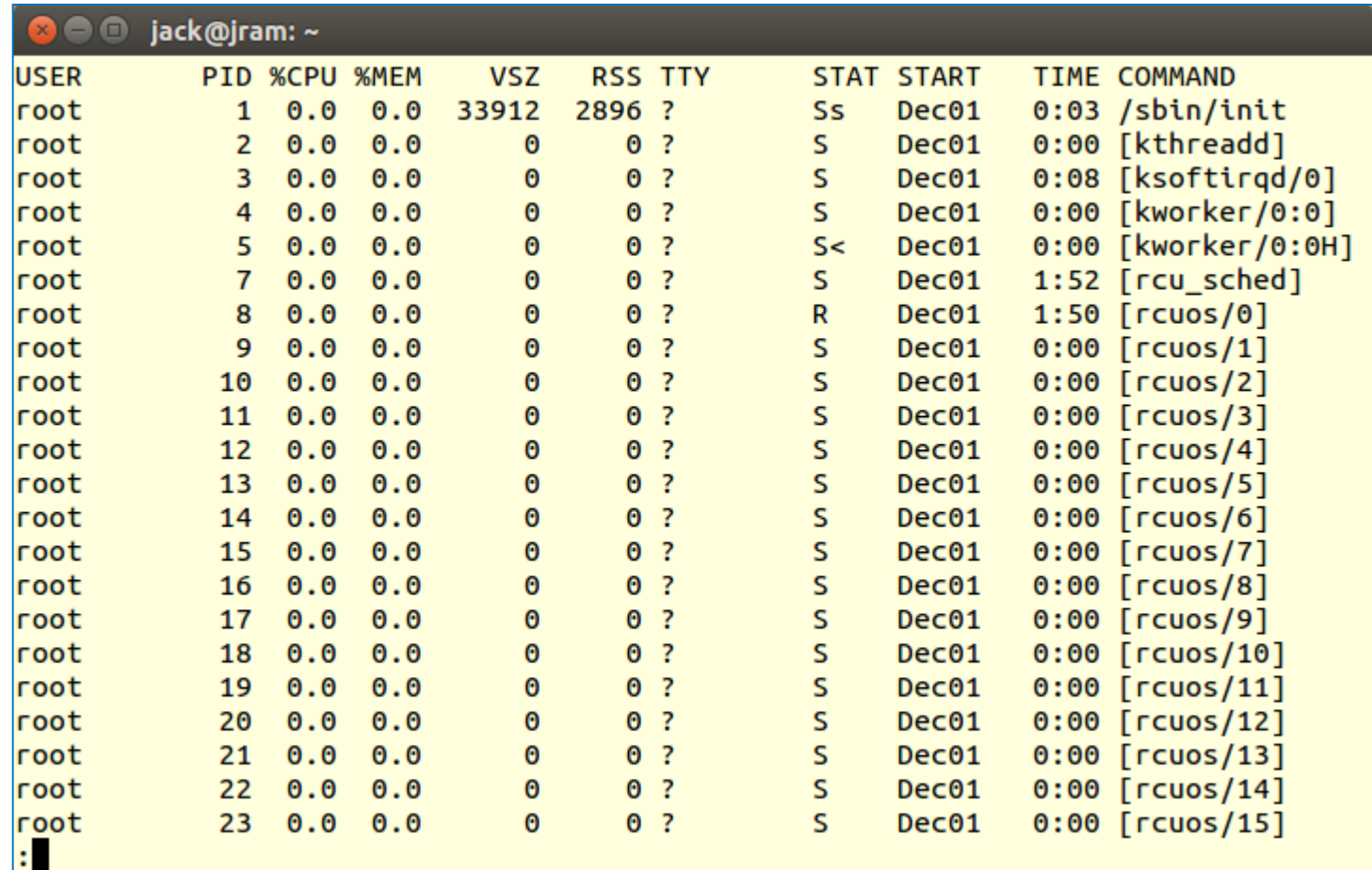
Linux

`ps aux`

a = show all processes

u = user orientated format

x = no control terminal



USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	1	0.0	0.0	33912	2896	?	Ss	Dec01	0:03	/sbin/init
root	2	0.0	0.0	0	0	?	S	Dec01	0:00	[kthreadd]
root	3	0.0	0.0	0	0	?	S	Dec01	0:08	[ksoftirqd/0]
root	4	0.0	0.0	0	0	?	S	Dec01	0:00	[kworker/0:0]
root	5	0.0	0.0	0	0	?	S<	Dec01	0:00	[kworker/0:0H]
root	7	0.0	0.0	0	0	?	S	Dec01	1:52	[rcu_sched]
root	8	0.0	0.0	0	0	?	R	Dec01	1:50	[rcuos/0]
root	9	0.0	0.0	0	0	?	S	Dec01	0:00	[rcuos/1]
root	10	0.0	0.0	0	0	?	S	Dec01	0:00	[rcuos/2]
root	11	0.0	0.0	0	0	?	S	Dec01	0:00	[rcuos/3]
root	12	0.0	0.0	0	0	?	S	Dec01	0:00	[rcuos/4]
root	13	0.0	0.0	0	0	?	S	Dec01	0:00	[rcuos/5]
root	14	0.0	0.0	0	0	?	S	Dec01	0:00	[rcuos/6]
root	15	0.0	0.0	0	0	?	S	Dec01	0:00	[rcuos/7]
root	16	0.0	0.0	0	0	?	S	Dec01	0:00	[rcuos/8]
root	17	0.0	0.0	0	0	?	S	Dec01	0:00	[rcuos/9]
root	18	0.0	0.0	0	0	?	S	Dec01	0:00	[rcuos/10]
root	19	0.0	0.0	0	0	?	S	Dec01	0:00	[rcuos/11]
root	20	0.0	0.0	0	0	?	S	Dec01	0:00	[rcuos/12]
root	21	0.0	0.0	0	0	?	S	Dec01	0:00	[rcuos/13]
root	22	0.0	0.0	0	0	?	S	Dec01	0:00	[rcuos/14]
root	23	0.0	0.0	0	0	?	S	Dec01	0:00	[rcuos/15]



Listing Processes

Linux

Processes owned by
a given user

```
jack@jram: ~  
jack      2483  0.0  0.1  27564  4544 pts/6    Ss   07:37   0:00 bash  
jack      2516  0.0  0.1  27564  4548 pts/16   Ss+  07:39   0:00 bash  
jack      2568  0.0  0.0  22640  1332 pts/6    R+   07:52   0:00 ps aux  
jack      2569  0.0  0.0  15936   936 pts/6    S+   07:52   0:00 grep --color=au  
to jack  
jack      2570  0.0  0.0  13740   972 pts/6    S+   07:52   0:00 less  
jack      3169  0.0  0.1 375732  4816 ?        Sl   Dec01   0:00 /usr/bin/pulsea  
udio --start --log-target=syslog  
jack      44321  0.0  0.1 297028  3548 ?        Sl   Dec05   0:00 /usr/bin/gnome-  
keyring-daemon --daemonize --login  
jack      44326  0.0  0.0  40280  2472 ?        Ss   Dec05   0:00 init --user  
jack      44423  0.0  0.0  40092  2344 ?        Ss   Dec05   0:09 dbus-daemon --f  
ork --session --address=unix:abstract=/tmp/dbus-IiKyDKiRZE  
jack      44434  0.0  0.0  22296  1076 ?        Ss   Dec05   0:00 upstart-event-b  
ridge  
jack      44451  0.0  0.1  78192  3296 ?        Ss   Dec05   0:00 /usr/lib/x86_64  
-linux-gnu/hud/window-stack-bridge  
jack      44453  0.0  0.4 550580 15204 ?        Sl   Dec05   0:02 /usr/lib/x86_64  
-linux-gnu/bamf/bamfdaemon  
jack      44462  0.0  0.0 337584  2904 ?        Sl   Dec05   0:00 /usr/lib/at-spi  
2-core/at-spi-bus-launcher  
jack      44475  0.0  0.0  39376  1888 ?        S    Dec05   0:00 /bin/dbus-daemo  
n --config-file=/etc/at-spi2/accessibility.conf --nofork --print-address 3  
:█
```

ps aux | grep jack | less

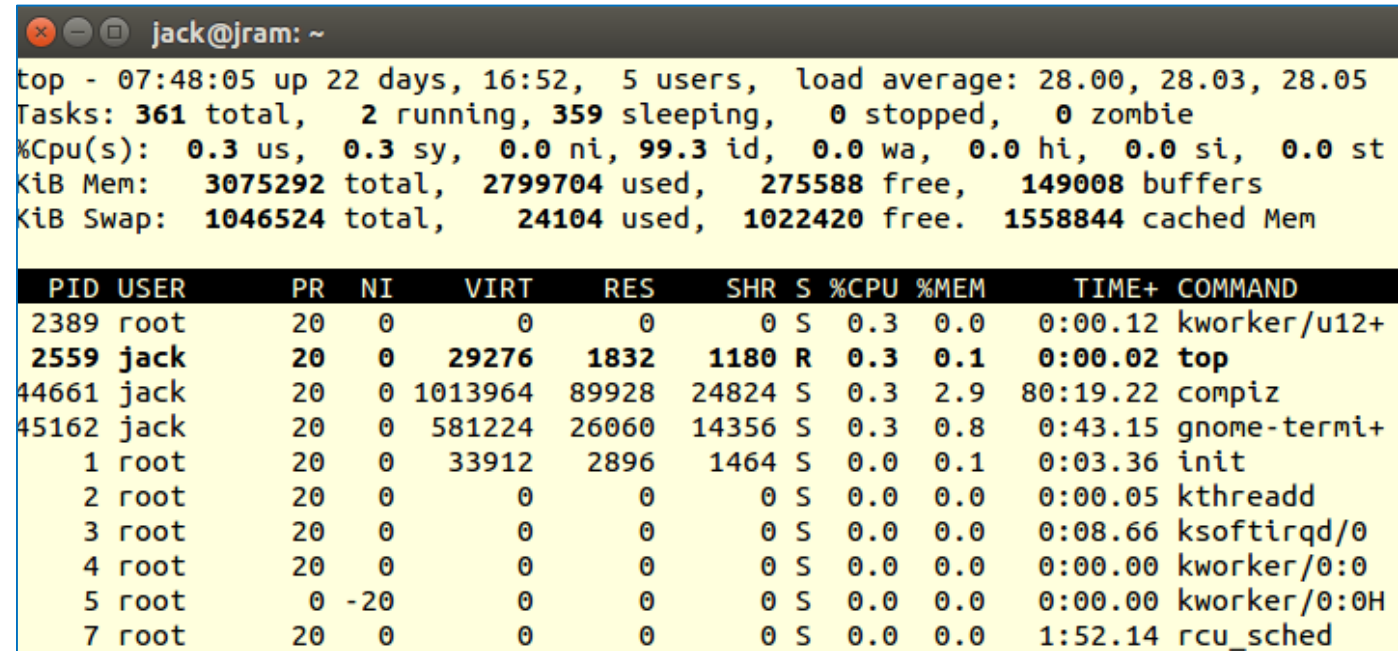


Process Monitoring

top

Unlike `ps`, `top` auto-updates to provide real-time monitoring information

Several options available while running (press 'h' for a list).



The screenshot shows a terminal window titled 'jack@jram: ~'. The output of the 'top' command is displayed, showing system statistics and a list of running processes. The system statistics include: top - 07:48:05 up 22 days, 16:52, 5 users, load average: 28.00, 28.03, 28.05; Tasks: 361 total, 2 running, 359 sleeping, 0 stopped, 0 zombie; %Cpu(s): 0.3 us, 0.3 sy, 0.0 ni, 99.3 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st; KiB Mem: 3075292 total, 2799704 used, 275588 free, 149008 buffers; KiB Swap: 1046524 total, 24104 used, 1022420 free. 1558844 cached Mem.

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
2389	root	20	0	0	0	0	S	0.3	0.0	0:00.12	kworker/u12+
2559	jack	20	0	29276	1832	1180	R	0.3	0.1	0:00.02	top
44661	jack	20	0	1013964	89928	24824	S	0.3	2.9	80:19.22	compiz
45162	jack	20	0	581224	26060	14356	S	0.3	0.8	0:43.15	gnome-termi+
1	root	20	0	33912	2896	1464	S	0.0	0.1	0:03.36	init
2	root	20	0	0	0	0	S	0.0	0.0	0:00.05	kthreadd
3	root	20	0	0	0	0	S	0.0	0.0	0:08.66	ksoftirqd/0
4	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kworker/0:0
5	root	0	-20	0	0	0	S	0.0	0.0	0:00.00	kworker/0:0H
7	root	20	0	0	0	0	S	0.0	0.0	1:52.14	rcu_sched



/proc

Logical directory maintained by the system

Apps can query it to get system state information

File usually have zero size because it is built on the fly

```
jack@jram: ~  
dr-xr-xr-x 9 root      root      0 Dec 24 07:37 2389/  
dr-xr-xr-x 9 rtkit     rtkit     0 Sep 10 11:11 2391/  
dr-xr-xr-x 9 root      root      0 Sep 10 11:10 24/  
dr-xr-xr-x 9 root      root      0 Dec 24 07:37 2407/  
dr-xr-xr-x 9 root      root      0 Dec 24 07:37 2408/  
dr-xr-xr-x 9 root      root      0 Dec 24 07:37 2416/  
dr-xr-xr-x 9 root      root      0 Dec 24 07:37 2468/  
dr-xr-xr-x 9 root      root      0 Dec 24 07:37 2477/  
dr-xr-xr-x 9 root      root      0 Sep 10 11:10 248/  
dr-xr-xr-x 9 jack      jack      0 Dec 24 07:37 2483/  
dr-xr-xr-x 9 root      root      0 Sep 10 11:10 249/  
dr-xr-xr-x 9 root      root      0 Sep 10 11:10 25/  
dr-xr-xr-x 9 root      root      0 Sep 10 11:10 250/  
dr-xr-xr-x 9 root      root      0 Sep 10 11:10 251/  
dr-xr-xr-x 9 jack      jack      0 Dec 24 07:39 2516/  
dr-xr-xr-x 9 root      root      0 Sep 10 11:10 252/  
dr-xr-xr-x 9 root      root      0 Sep 10 11:10 253/  
dr-xr-xr-x 9 root      root      0 Sep 10 11:10 254/  
dr-xr-xr-x 9 root      root      0 Sep 10 11:10 255/  
dr-xr-xr-x 9 root      root      0 Sep 10 11:10 256/  
dr-xr-xr-x 9 root      root      0 Sep 10 11:10 257/  
dr-xr-xr-x 9 root      root      0 Sep 10 11:10 258/  
dr-xr-xr-x 9 jack      jack      0 Dec 24 07:56 2588/  
:
```

Output from `ll /proc | less`



Other Process Killers

pkill - kill process by its name, user name, group name, terminal, UID, and GID

e.g., **pkill -s 15 -u jack firefox**

killall - sends the signal to all processes.

e.g., **sudo killall -s 15 httpd**



Process Explorer

The following material is from Chapter 3, Russinovich, M. & Margosis, A. (2011). *Windows Sysinternals Administrator's Reference*. Redmond, WA: Microsoft Press.



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Handles

Windows kernel-mode consists of various subsystems (e.g., Process Manager)

Each defines one or more objects to represent resources they expose to applications (e.g., Process objects)

*Russinovich, M. & Margosis, A. (2011). *Windows Sysinternals Administrator's Reference*. Redmond, WA: Microsoft Press.



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Handles

When an application wants to use a resource, it must call the appropriate API to create or open the resource (e.g., CreateFile function opens or creates a file)

If successful, Windows allocates a reference to the object

*Russinovich, M. & Margosis, A. (2011). *Windows Sysinternals Administrator's Reference*. Redmond, WA: Microsoft Press.

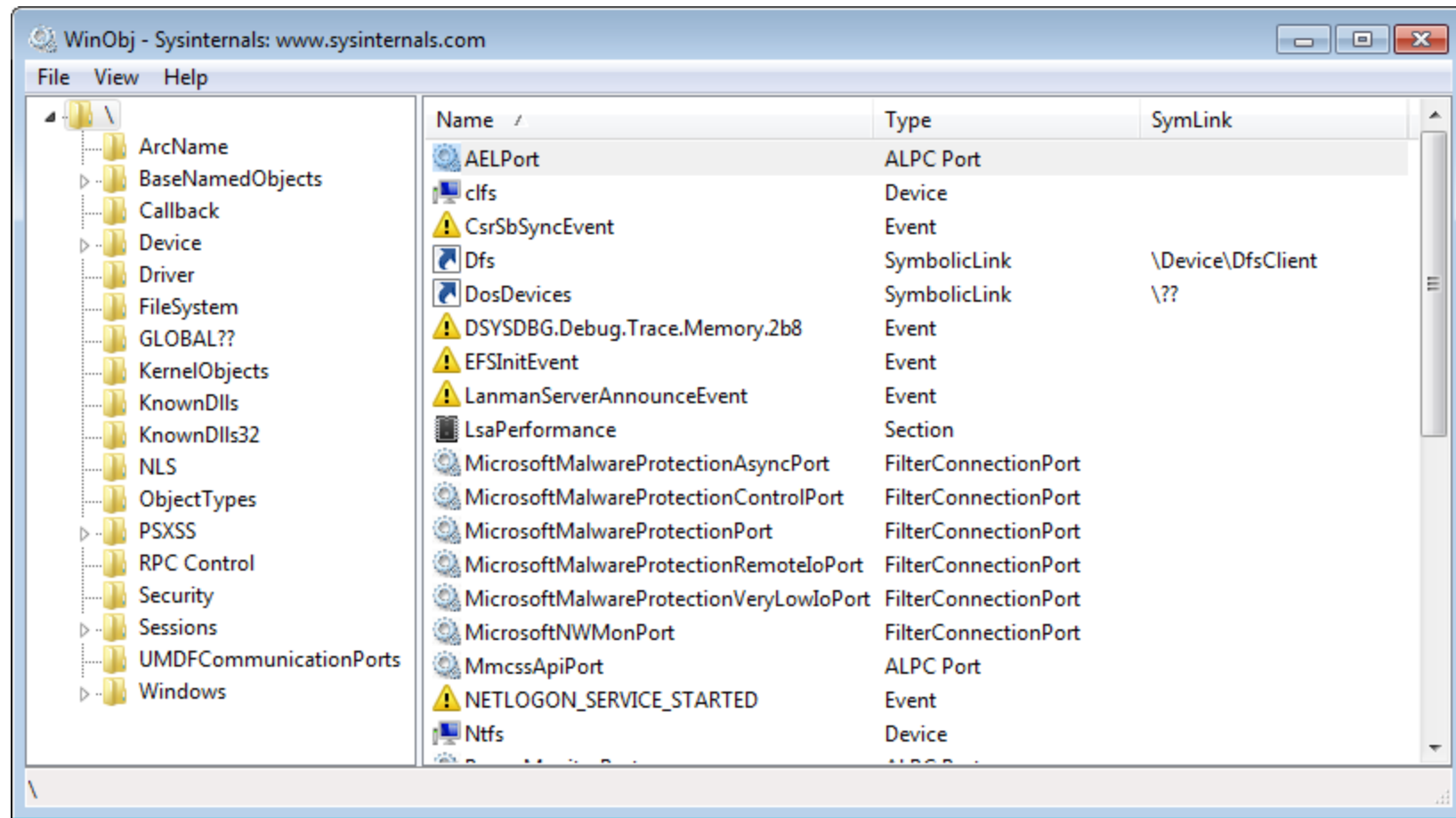


East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Handles

WinObj

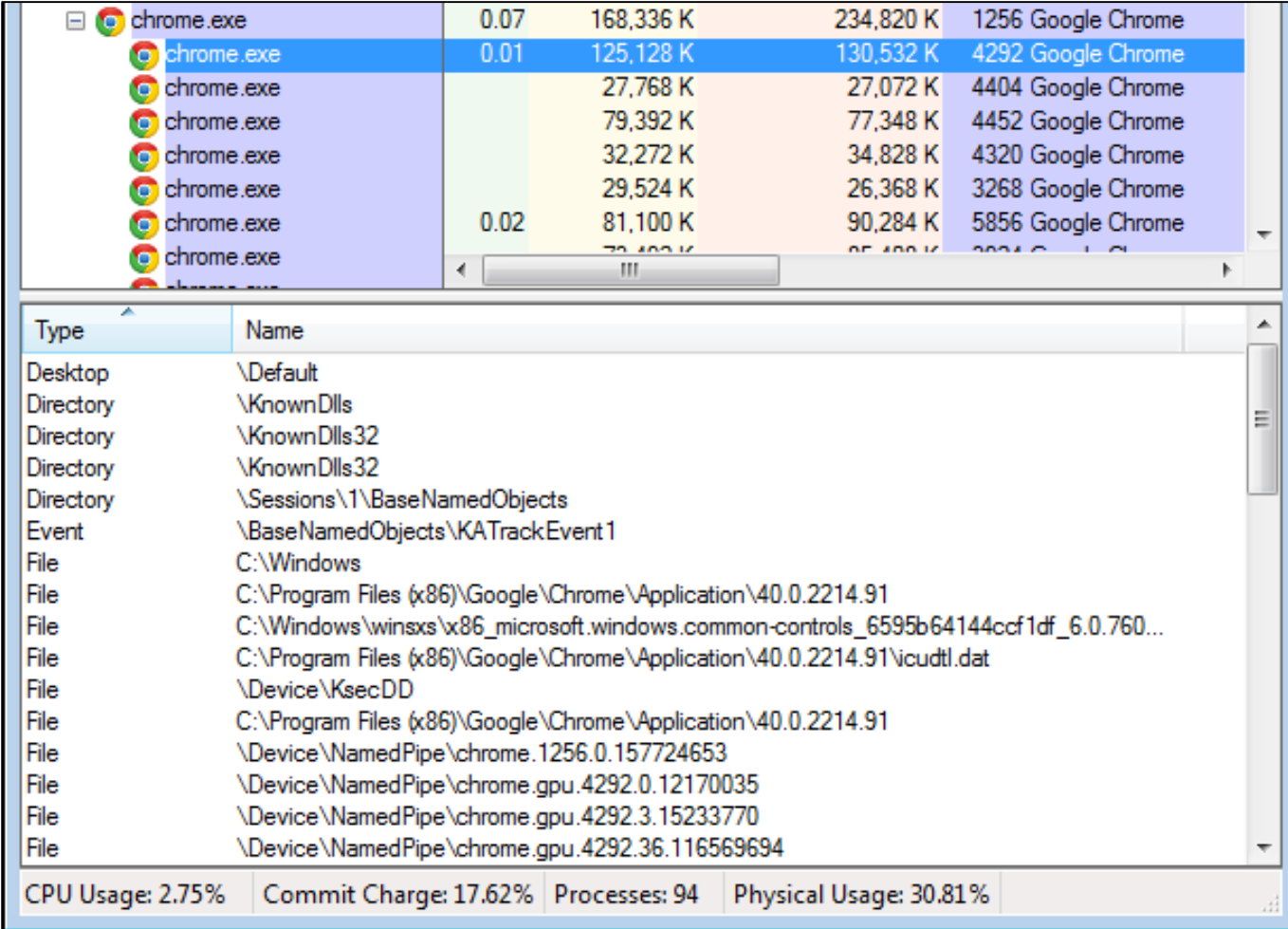
Displays Object types that
Windows defines



*Rusinovich, M. & Margosis, A. (2011). *Windows Sysinternals Administrator's Reference*. Redmond, WA: Microsoft Press.

Handles

Process Explorer can display the handles associated with a given process



The screenshot shows the Windows Process Explorer interface. The top pane displays a list of processes, with several instances of 'chrome.exe' selected. The bottom pane shows the 'Handles' tab for one of the selected processes, listing various system objects and files it has opened. The status bar at the bottom indicates system performance metrics.

Type	Name
Desktop	\Default
Directory	\KnownDlls
Directory	\KnownDlls32
Directory	\KnownDlls32
Directory	\Sessions\1\BaseNamedObjects
Event	\BaseNamedObjects\KATrackEvent1
File	C:\Windows
File	C:\Program Files (x86)\Google\Chrome\Application\40.0.2214.91
File	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.760...
File	C:\Program Files (x86)\Google\Chrome\Application\40.0.2214.91\icudtl.dat
File	\Device\KsecDD
File	C:\Program Files (x86)\Google\Chrome\Application\40.0.2214.91
File	\Device\NamedPipe\chrome.1256.0.157724653
File	\Device\NamedPipe\chrome.gpu.4292.0.12170035
File	\Device\NamedPipe\chrome.gpu.4292.3.15233770
File	\Device\NamedPipe\chrome.gpu.4292.36.116569694

CPU Usage: 2.75% Commit Charge: 17.62% Processes: 94 Physical Usage: 30.81%

*Rusinovich, M. & Margosis, A. (2011). *Windows Sysinternals Administrator's Reference*. Redmond, WA: Microsoft Press.

Jobs

Windows provides an extension to the process model called a job

Allows groups of processes to be managed and manipulated as a unit

Example:

A job can be used to terminate a group of processes all at once, rather than one at a time & without the calling process having to know which processes are in the group

*Russinovich, M. & Margosis, A. (2011). *Windows Sysinternals Administrator's Reference*. Redmond, WA: Microsoft Press.



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Jobs

Allows control of certain attributes

Provides limits for the process or processes associated with the job.

*Rusinovich, M. & Margosis, A. (2011). *Windows Sysinternals Administrator's Reference*. Redmond, WA: Microsoft Press.



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Process Explorer

If possible, Run as Administrator

View -> Show lower pane

Ctrl+D: Lists DLLs

Ctrl+H: Lists Handles

Ctrl+L: Toggles lower pane open or closed

The screenshot shows the Process Explorer window from Sysinternals. The top pane displays a list of running processes with columns for CPU, Private Bytes, Working Set, PID, and Description. The bottom pane, which is expanded, shows a list of loaded DLLs with columns for Name, Description, Company Name, and Path. The DLL list includes system DLLs like advapi32.dll and user-space DLLs like chrome.exe.

Process	CPU	Private Bytes	Working Set	PID	Description
System Idle Process	97.30	0 K	24 K	0	
System	0.10	400 K	13,936 K	4	
csrss.exe	< 0.01	3,776 K	6,032 K	508	
csrss.exe	0.21	20,284 K	31,604 K	596	
wininit.exe		1,948 K	5,044 K	616	
winlogon.exe		3,424 K	8,376 K	652	
explorer.exe	0.12	62,992 K	89,560 K	3652	Windows Explorer
kass.exe	< 0.01	1,224 K	3,276 K	2972	KeyAccess Messenger for Windows (64-bit)
mssec.exe	0.01	8,500 K	18,276 K	3952	Microsoft Security Client User Interface
chrome.exe	0.38	169,104 K	235,212 K	1256	Google Chrome
chrome.exe	0.01	125,128 K	130,520 K	4292	Google Chrome
chrome.exe		27,768 K	27,072 K	4404	Google Chrome
chrome.exe		80,656 K	78,920 K	4452	Google Chrome
chrome.exe	< 0.01	32,296 K	34,836 K	4320	Google Chrome
chrome.exe		29,524 K	26,368 K	3268	Google Chrome
chrome.exe	0.03	83,144 K	90,356 K	5856	Google Chrome
chrome.exe		73,092 K	84,708 K	3924	Google Chrome
chrome.exe	0.14	201,520 K	203,088 K	6900	Google Chrome
RtDCpl64.exe		4,532 K	8,892 K	3460	HD Audio Control Panel
SkyDrive.exe	0.12	18,976 K	35,272 K	2984	Microsoft OneDrive
AlertusDesktopAlert.exe	0.01	38,424 K	26,636 K	4164	Alertus Desktop Alert
OcsSystray.exe		4,440 K	9,188 K	4176	OCS Inventory NG Systray applet
Dropbox.exe	0.26	76,544 K	100,080 K	4324	Dropbox
POWERPNT.EXE	0.02	273,892 K	292,560 K	4916	Microsoft PowerPoint
filezilla.exe	< 0.01	9,460 K	25,800 K	3984	FileZilla FTP Client
vmware.exe					

Name	Description	Company Name	Path
advapi32.dll	Advanced Windows 32 Base API	Microsoft Corporation	C:\Windows\SysWOW64\advapi32.dll
api-ms-win-downlev...	ApiSet Stub DLL	Microsoft Corporation	C:\Windows\SysWOW64\api-ms-win-downlevel-advapi32
api-ms-win-downlev...	ApiSet Stub DLL	Microsoft Corporation	C:\Windows\SysWOW64\api-ms-win-downlevel-normaliz4
api-ms-win-downlev...	ApiSet Stub DLL	Microsoft Corporation	C:\Windows\SysWOW64\api-ms-win-downlevel-shlwapi4
api-ms-win-downlev...	ApiSet Stub DLL	Microsoft Corporation	C:\Windows\SysWOW64\api-ms-win-downlevel-user32+1
api-ms-win-downlev...	ApiSet Stub DLL	Microsoft Corporation	C:\Windows\SysWOW64\api-ms-win-downlevel-version4
apisetschema.dll	ApiSet Schema DLL	Microsoft Corporation	C:\Windows\System32\apisetschema.dll
chrome.exe	Google Chrome	Google Inc.	C:\Program Files (x86)\Google\Chrome\Application\chrom
chrome_100.exe			C:\Program Files (x86)\Google\Chrome\Application\40.0.0

CPU Usage: 2.70% Commit Charge: 15.02% Processes: 89 Physical Usage: 28.05%



Process Explorer

Top Pane

Processes arranged in parent/child format,
displaying which processes 'own' others

CPU time more accurate than Task Manager

Process Explorer - Sysinternals: www.sysinternals.com [ETSU\ramseyjw]

File Options View Process Find DLL Users Help

Process	CPU	Private Bytes	Working Set	PID	Description
System Idle Process	97.26	0 K	24 K	0	
System	0.15	400 K	13,936 K	4	
csrss.exe	< 0.01	3,776 K	6,036 K	508	
csrss.exe	0.11	20,284 K	31,596 K	596	
wininit.exe		1,948 K	5,044 K	616	
services.exe	< 0.01	9,792 K	17,196 K	680	
svchost.exe	0.01	5,392 K	11,032 K	828	Host Process for Windows Services
WmiPrvSE.exe	< 0.01	16,676 K	26,480 K	3384	
WmiPrvSE.exe	< 0.01	12,224 K	18,396 K	3392	
WmiPrvSE.exe		11,572 K	13,792 K	3508	
WmiPrvSE.exe		2,976 K	6,836 K	3832	
WmiPrvSE.exe	< 0.01	21,456 K	28,412 K	932	
dllhost.exe		2,380 K	5,904 K	4144	COM Surrogate
CSISYNCCCLIENT.EXE		33,816 K	45,524 K	5272	Microsoft Office Document Cache Sync Client In
MSOSYNC.EXE	< 0.01	38,136 K	52,680 K	7508	Microsoft Office Document Cache
WmiPrvSE.exe		7,600 K	13,192 K	3404	
svchost.exe		7,432 K	11,716 K	904	Host Process for Windows Services
MsMpEng.exe	0.01	121,880 K	126,460 K	988	Antimalware Service Executable
atiesrxx.exe		1,980 K	5,052 K	388	AMD External Events Service Module
atiecbox.exe		2,656 K	6,824 K	2464	
svchost.exe	0.02	22,840 K	24,672 K	584	Host Process for Windows Services
audiodg.exe		17,068 K	17,328 K	6060	
svchost.exe	< 0.01	264,568 K	266,344 K	920	Host Process for Windows Services
dwm.exe		2,316 K	6,668 K	1252	Desktop Window Manager
wisptis.exe	0.01	3,264 K	8,608 K	5324	
svchost.exe					

Name	Description	Company Name	Path
advapi32.dll	Advanced Windows 32 Base API	Microsoft Corporation	C:\Windows\SysWOW64\advapi32.dll
api-ms-win-downlev...	ApiSet Stub DLL	Microsoft Corporation	C:\Windows\SysWOW64\api-ms-win-downlevel-advapi32
api-ms-win-downlev...	ApiSet Stub DLL	Microsoft Corporation	C:\Windows\SysWOW64\api-ms-win-downlevel-normaliz-4
api-ms-win-downlev...	ApiSet Stub DLL	Microsoft Corporation	C:\Windows\SysWOW64\api-ms-win-downlevel-shlwapi-1
api-ms-win-downlev...	ApiSet Stub DLL	Microsoft Corporation	C:\Windows\SysWOW64\api-ms-win-downlevel-user32-1
api-ms-win-downlev...	ApiSet Stub DLL	Microsoft Corporation	C:\Windows\SysWOW64\api-ms-win-downlevel-version-1
apisetschema.dll	ApiSet Schema DLL	Microsoft Corporation	C:\Windows\System32\apisetschema.dll
chrome.exe	Google Chrome	Google Inc.	C:\Program Files (x86)\Google\Chrome\Application\chrom
chrome_100_perce...			C:\Program Files (x86)\Google\Chrome\Application\40.0.2

CPU Usage: 2.74% Commit Charge: 14.91% Processes: 89 Physical Usage: 27.80%



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

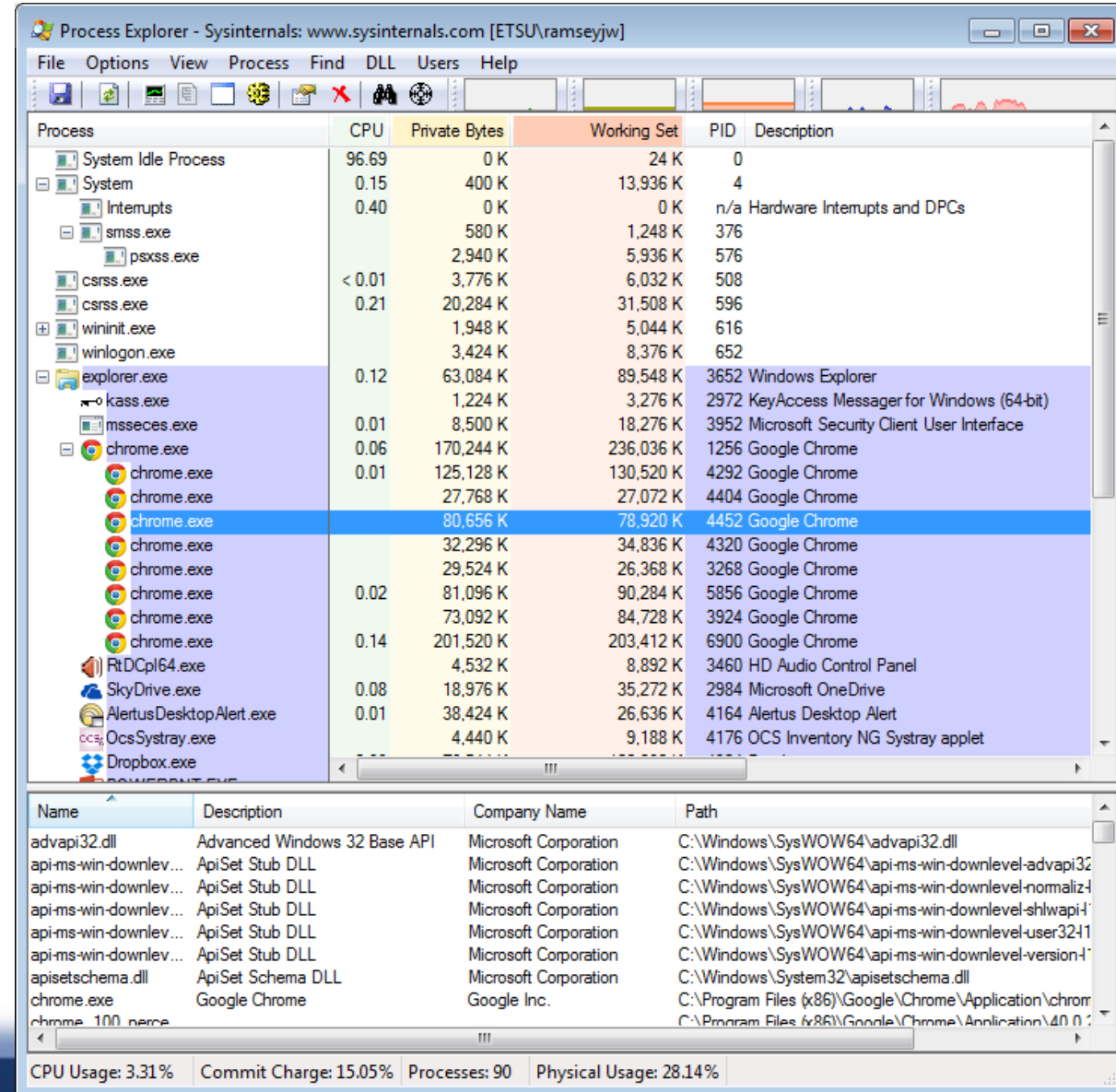
Process Explorer

Top half (collapsed on pic) represents system-level processes

1st three aren't actual processes

System Idle used to account for unused CPU time

System hosts only kernel-mode threads



The screenshot shows the Windows Process Explorer window. The top pane displays a list of processes with columns for CPU, Private Bytes, Working Set, PID, and Description. The bottom pane shows the loaded DLLs for the selected process (chrome.exe).

Process	CPU	Private Bytes	Working Set	PID	Description
System Idle Process	96.69	0 K	24 K	0	
System	0.15	400 K	13,936 K	4	
Interrupts	0.40	0 K	0 K	n/a	Hardware Interrupts and DPCs
smss.exe		580 K	1,248 K	376	
psxs.exe		2,940 K	5,936 K	576	
csrss.exe	< 0.01	3,776 K	6,032 K	508	
csrss.exe	0.21	20,284 K	31,508 K	596	
wininit.exe		1,948 K	5,044 K	616	
winlogon.exe		3,424 K	8,376 K	652	
explorer.exe	0.12	63,084 K	89,548 K	3652	Windows Explorer
kass.exe		1,224 K	3,276 K	2972	KeyAccess Messenger for Windows (64-bit)
mssec.exe	0.01	8,500 K	18,276 K	3952	Microsoft Security Client User Interface
chrome.exe	0.06	170,244 K	236,036 K	1256	Google Chrome
chrome.exe	0.01	125,128 K	130,520 K	4292	Google Chrome
chrome.exe		27,768 K	27,072 K	4404	Google Chrome
chrome.exe		80,656 K	78,920 K	4452	Google Chrome
chrome.exe		32,296 K	34,836 K	4320	Google Chrome
chrome.exe		29,524 K	26,368 K	3268	Google Chrome
chrome.exe	0.02	81,096 K	90,284 K	5856	Google Chrome
chrome.exe		73,092 K	84,728 K	3924	Google Chrome
chrome.exe	0.14	201,520 K	203,412 K	6900	Google Chrome
RtDCpl64.exe		4,532 K	8,892 K	3460	HD Audio Control Panel
SkyDrive.exe	0.08	18,976 K	35,272 K	2984	Microsoft OneDrive
AlertusDesktop.Alert.exe	0.01	38,424 K	26,636 K	4164	Alertus Desktop Alert
OcsSystray.exe		4,440 K	9,188 K	4176	OCS Inventory NG Systray applet
Dropbox.exe					

Name	Description	Company Name	Path
advapi32.dll	Advanced Windows 32 Base API	Microsoft Corporation	C:\Windows\SysWOW64\advapi32.dll
api-ms-win-downlev...	ApiSet Stub DLL	Microsoft Corporation	C:\Windows\SysWOW64\api-ms-win-downlevel-advapi32
api-ms-win-downlev...	ApiSet Stub DLL	Microsoft Corporation	C:\Windows\SysWOW64\api-ms-win-downlevel-normaliz4
api-ms-win-downlev...	ApiSet Stub DLL	Microsoft Corporation	C:\Windows\SysWOW64\api-ms-win-downlevel-shlwapi4
api-ms-win-downlev...	ApiSet Stub DLL	Microsoft Corporation	C:\Windows\SysWOW64\api-ms-win-downlevel-user3241
api-ms-win-downlev...	ApiSet Stub DLL	Microsoft Corporation	C:\Windows\SysWOW64\api-ms-win-downlevel-version4
apisetschema.dll	ApiSet Schema DLL	Microsoft Corporation	C:\Windows\System32\apisetschema.dll
chrome.exe	Google Chrome	Google Inc.	C:\Program Files (x86)\Google\Chrome\Application\chrom
chrome_100.exe			C:\Program Files (x86)\Google\Chrome\Application\40.0.2

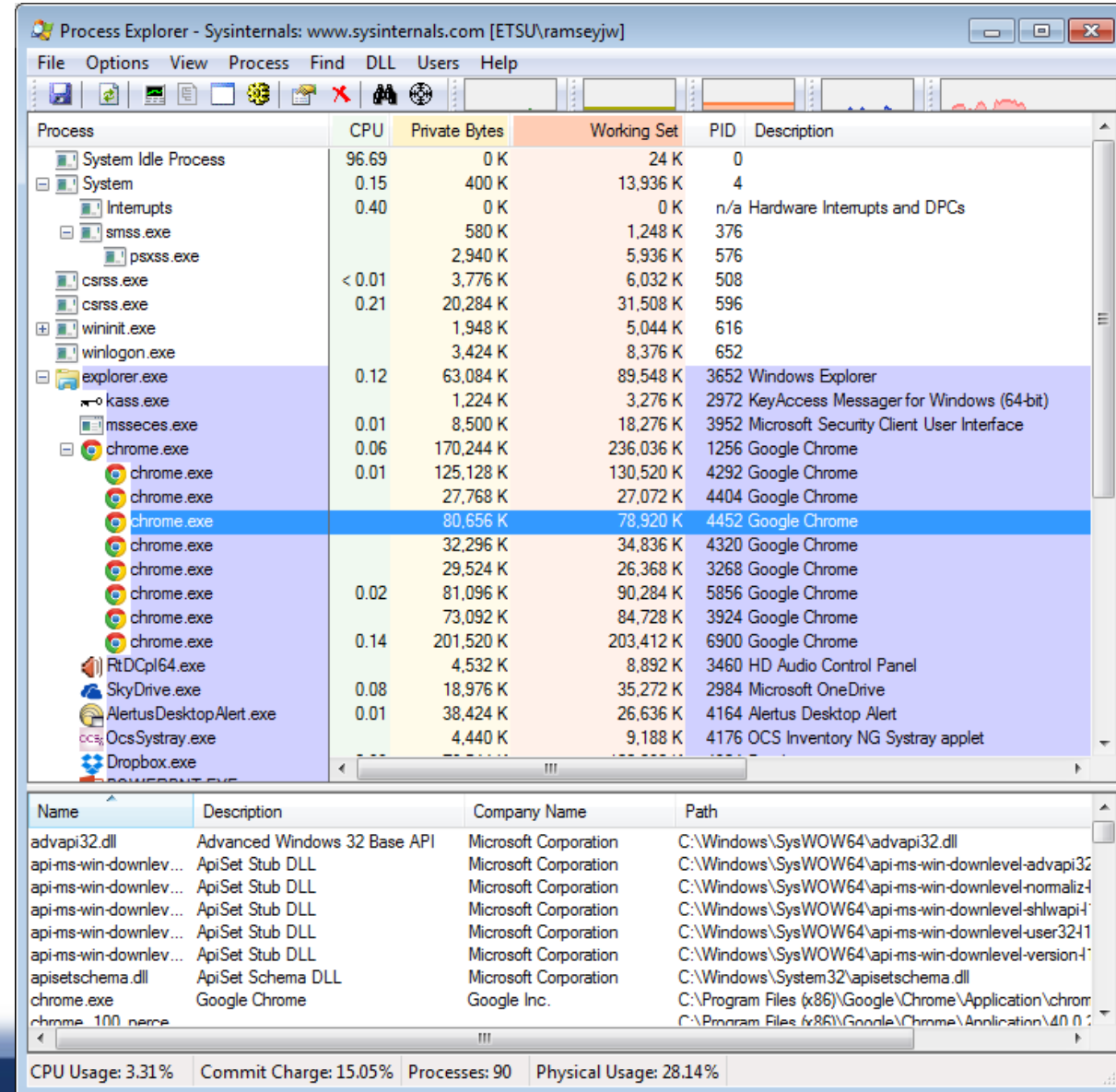
CPU Usage: 3.31% Commit Charge: 15.05% Processes: 90 Physical Usage: 28.14%



Process Explorer

User shell (explorer.exe)

Hosts user applications



The screenshot shows the Process Explorer window from Sysinternals. The top pane displays a list of processes with columns for CPU, Private Bytes, Working Set, PID, and Description. The bottom pane shows the loaded DLLs for the selected process (chrome.exe), with columns for Name, Description, Company Name, and Path.

Process	CPU	Private Bytes	Working Set	PID	Description
System Idle Process	96.69	0 K	24 K	0	
System	0.15	400 K	13,936 K	4	
Interrupts	0.40	0 K	0 K	n/a	Hardware Interrupts and DPCs
smss.exe		580 K	1,248 K	376	
psxss.exe		2,940 K	5,936 K	576	
csrss.exe	< 0.01	3,776 K	6,032 K	508	
csrss.exe	0.21	20,284 K	31,508 K	596	
wininit.exe		1,948 K	5,044 K	616	
winlogon.exe		3,424 K	8,376 K	652	
explorer.exe	0.12	63,084 K	89,548 K	3652	Windows Explorer
kass.exe		1,224 K	3,276 K	2972	KeyAccess Messenger for Windows (64-bit)
msseces.exe	0.01	8,500 K	18,276 K	3952	Microsoft Security Client User Interface
chrome.exe	0.06	170,244 K	236,036 K	1256	Google Chrome
chrome.exe	0.01	125,128 K	130,520 K	4292	Google Chrome
chrome.exe		27,768 K	27,072 K	4404	Google Chrome
chrome.exe		80,656 K	78,920 K	4452	Google Chrome
chrome.exe		32,296 K	34,836 K	4320	Google Chrome
chrome.exe		29,524 K	26,368 K	3268	Google Chrome
chrome.exe	0.02	81,096 K	90,284 K	5856	Google Chrome
chrome.exe		73,092 K	84,728 K	3924	Google Chrome
chrome.exe	0.14	201,520 K	203,412 K	6900	Google Chrome
RtDCpl64.exe		4,532 K	8,892 K	3460	HD Audio Control Panel
SkyDrive.exe	0.08	18,976 K	35,272 K	2984	Microsoft OneDrive
AlertusDesktop.Alert.exe	0.01	38,424 K	26,636 K	4164	Alertus Desktop Alert
OcsSystray.exe		4,440 K	9,188 K	4176	OCS Inventory NG Systray applet
Dropbox.exe					

Name	Description	Company Name	Path
advapi32.dll	Advanced Windows 32 Base API	Microsoft Corporation	C:\Windows\SysWOW64\advapi32.dll
api-ms-win-downlev...	ApiSet Stub DLL	Microsoft Corporation	C:\Windows\SysWOW64\api-ms-win-downlevel-advapi32-
api-ms-win-downlev...	ApiSet Stub DLL	Microsoft Corporation	C:\Windows\SysWOW64\api-ms-win-downlevel-normaliz-
api-ms-win-downlev...	ApiSet Stub DLL	Microsoft Corporation	C:\Windows\SysWOW64\api-ms-win-downlevel-shlwapi-
api-ms-win-downlev...	ApiSet Stub DLL	Microsoft Corporation	C:\Windows\SysWOW64\api-ms-win-downlevel-user32-
api-ms-win-downlev...	ApiSet Stub DLL	Microsoft Corporation	C:\Windows\SysWOW64\api-ms-win-downlevel-version-
apisetschema.dll	ApiSet Schema DLL	Microsoft Corporation	C:\Windows\System32\apisetschema.dll
chrome.exe	Google Chrome	Google Inc.	C:\Program Files (x86)\Google\Chrome\Application\chrom
chrome_100.n...			C:\Program Files (x86)\Google\Chrome\Application\40.0.2

CPU Usage: 3.31% Commit Charge: 15.05% Processes: 90 Physical Usage: 28.14%



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Process Explorer

Color Coding

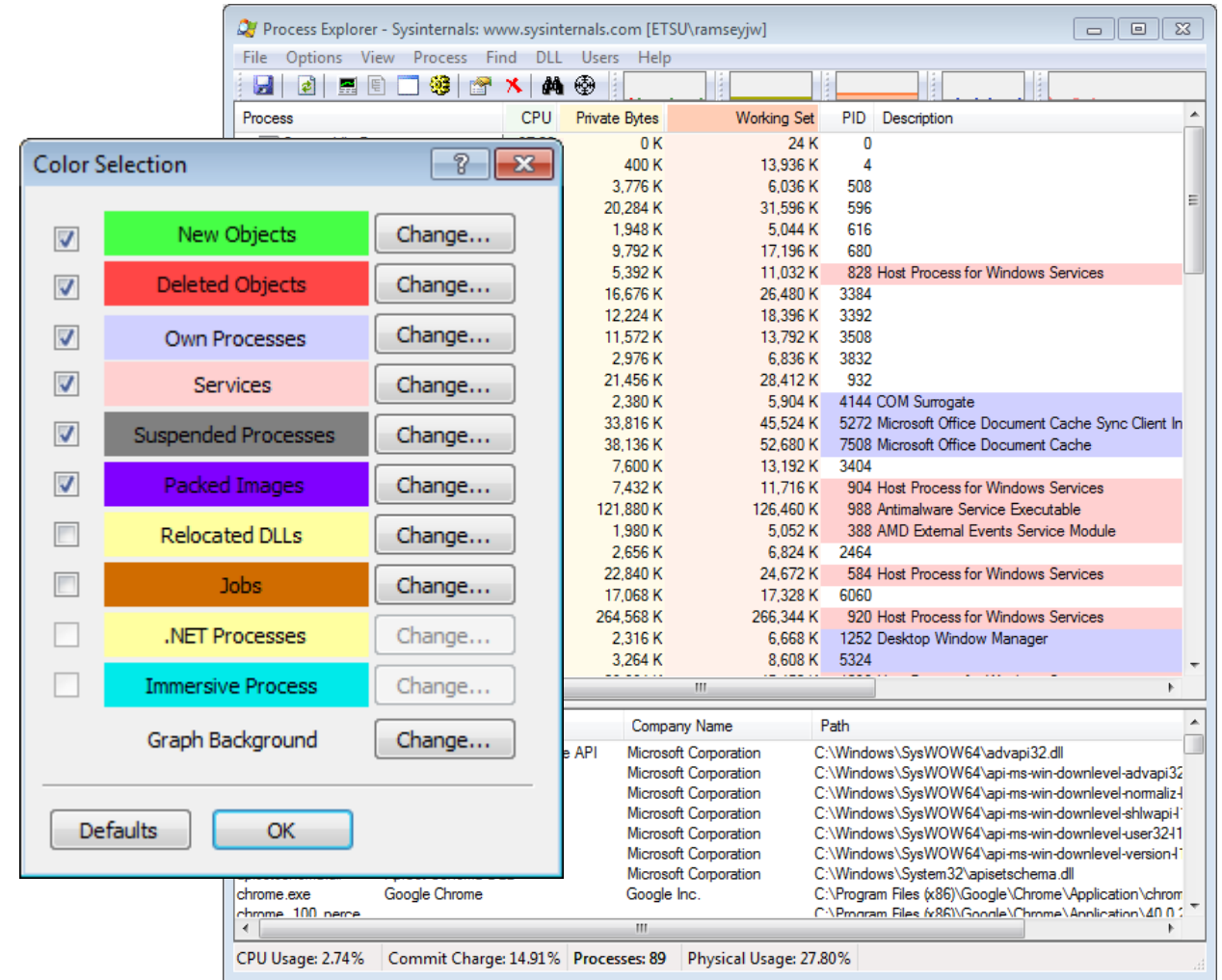
Distinguishes different types of processes

Configurable (Default shown)

Green = new process

Red = process terminated

Access: Options -> Configure Colors...



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

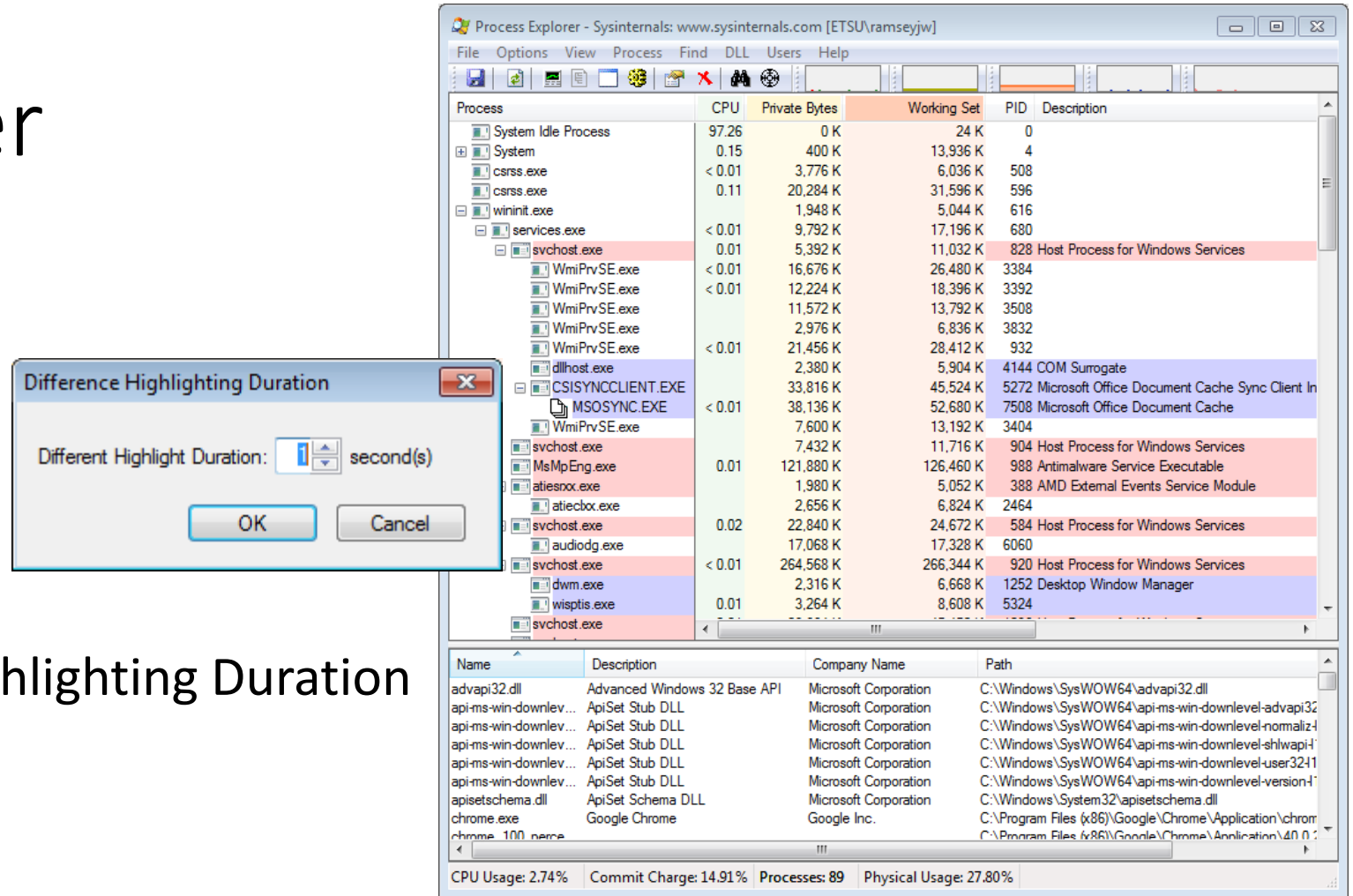
Process Explorer

Highlighting Duration

Configurable: .5-9 sec

Default: 1 sec

Access: Options->Difference Highlighting Duration

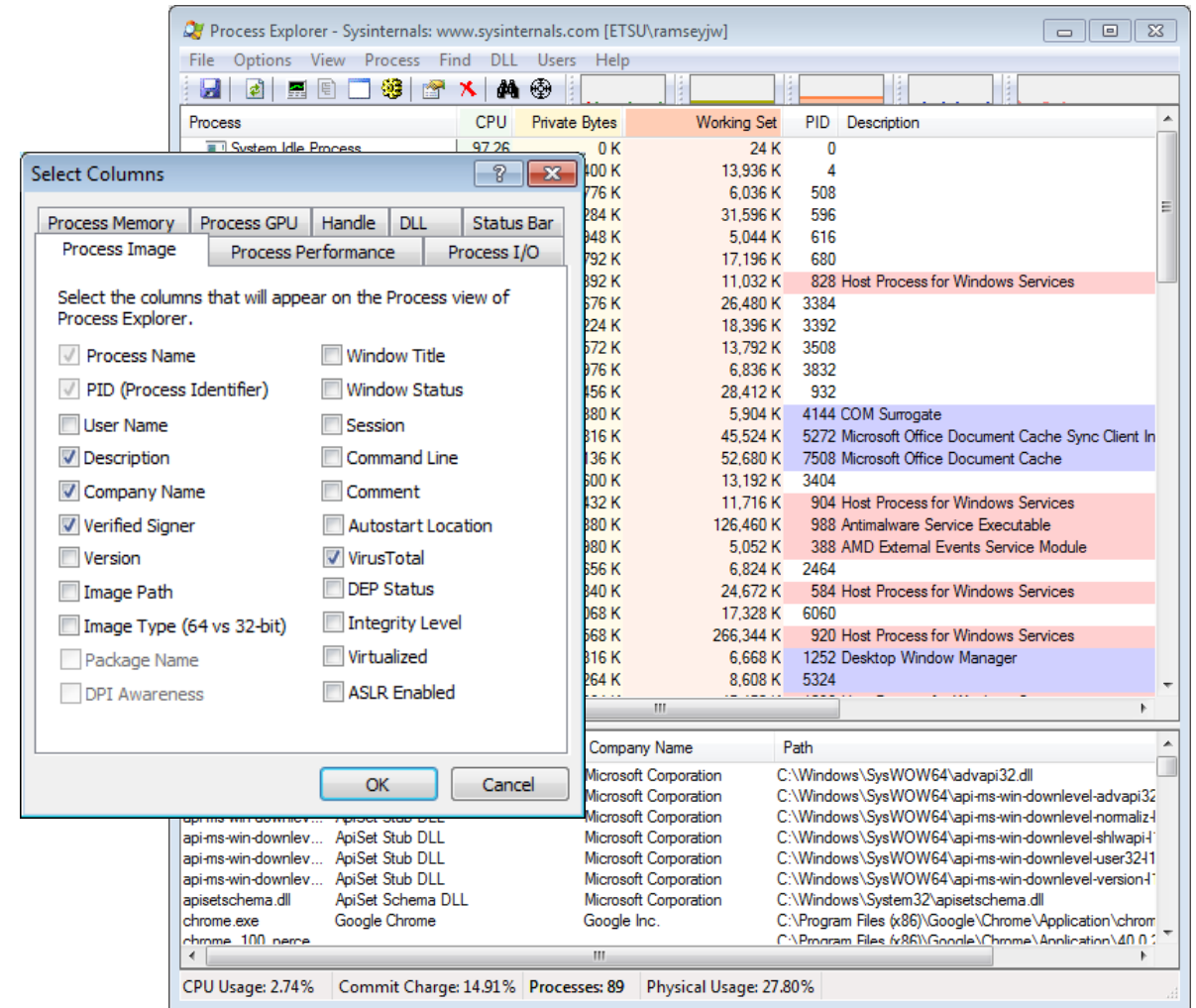


East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Process Explorer

Highly Configurable

View->Select Columns



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

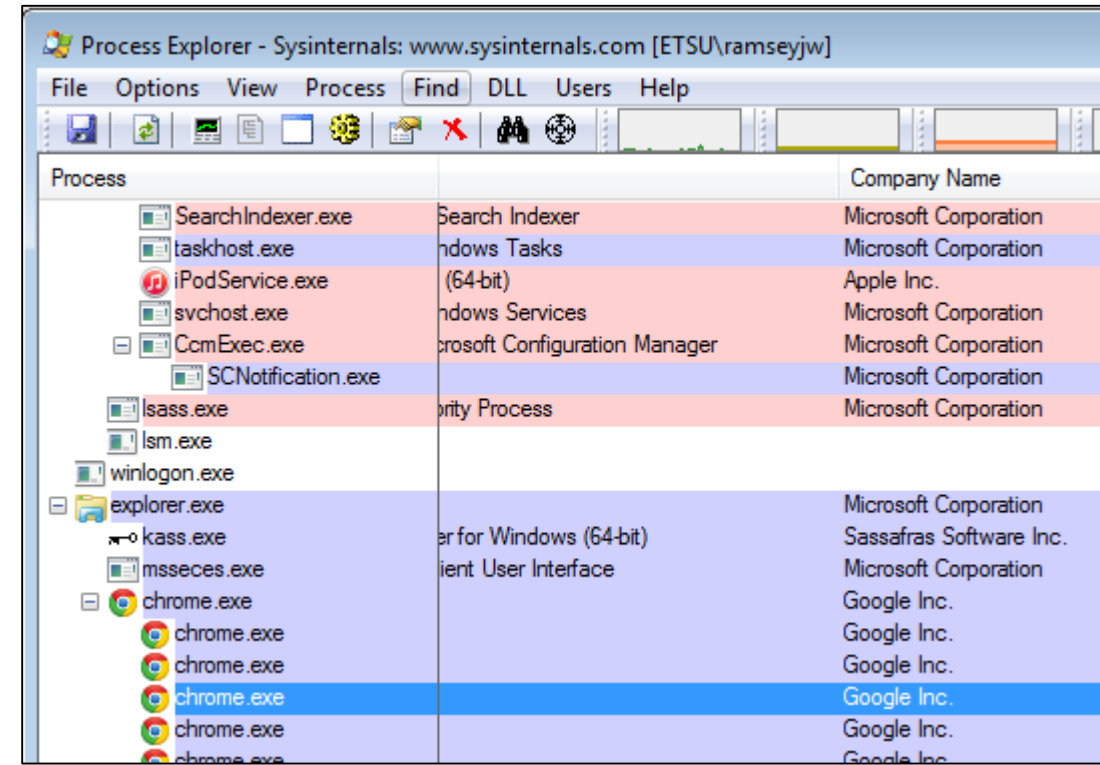
Process Explorer

Company Name & Description

Run as Administrator

Can be helpful in identifying malware

Often not signed

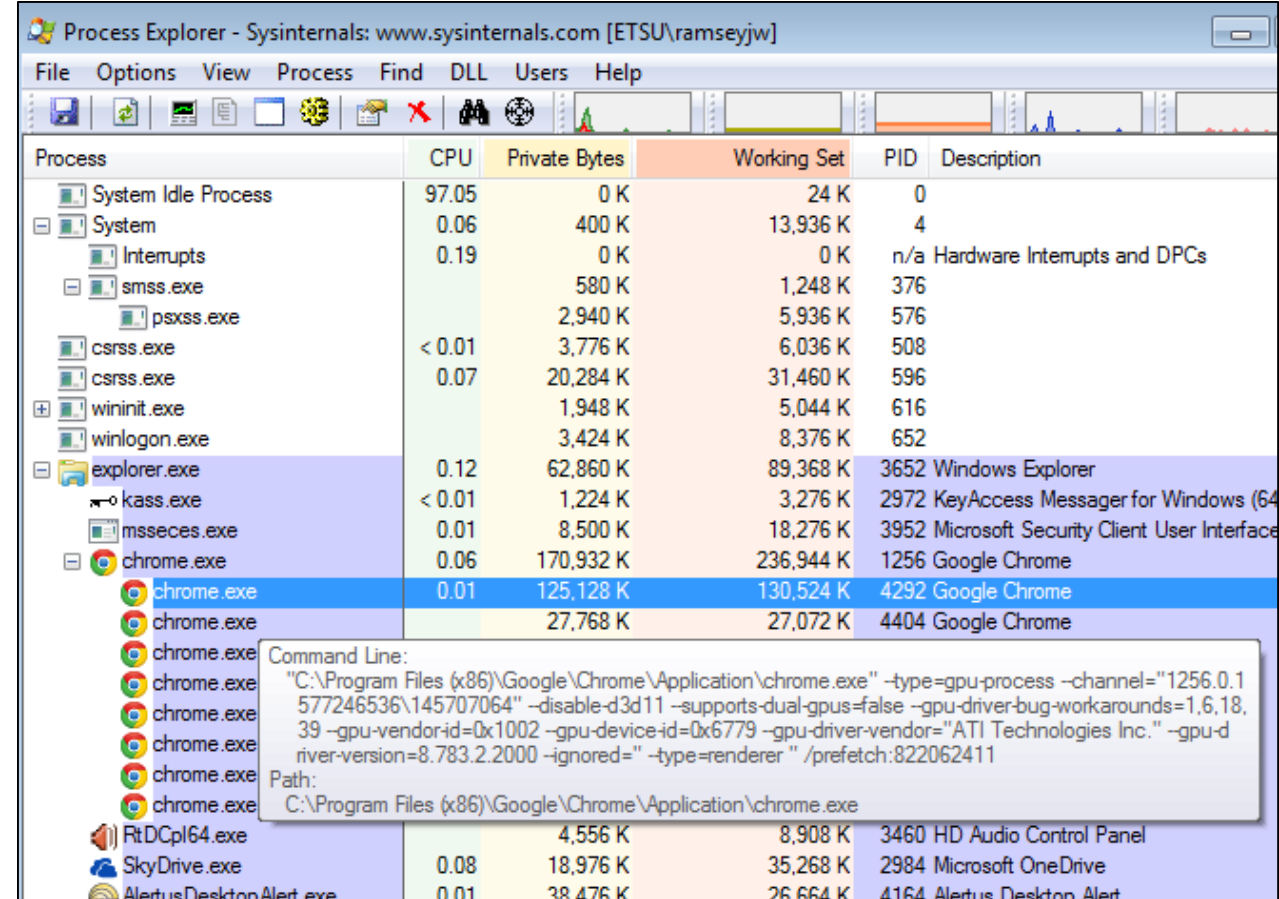


East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Process Explorer

Tool-tip information

Hovering the cursor over a process provides command-line and path information



Process Explorer - Sysinternals: www.sysinternals.com [ETSU\ramseyjw]

Process	CPU	Private Bytes	Working Set	PID	Description
System Idle Process	97.05	0 K	24 K	0	
System	0.06	400 K	13,936 K	4	
Interrupts	0.19	0 K	0 K	n/a	Hardware Interrupts and DPCs
smss.exe		580 K	1,248 K	376	
psxss.exe		2,940 K	5,936 K	576	
csrss.exe	< 0.01	3,776 K	6,036 K	508	
csrss.exe	0.07	20,284 K	31,460 K	596	
wininit.exe		1,948 K	5,044 K	616	
winlogon.exe		3,424 K	8,376 K	652	
explorer.exe	0.12	62,860 K	89,368 K	3652	Windows Explorer
kass.exe	< 0.01	1,224 K	3,276 K	2972	KeyAccess Messenger for Windows (64
msseces.exe	0.01	8,500 K	18,276 K	3952	Microsoft Security Client User Interface
chrome.exe	0.06	170,932 K	236,944 K	1256	Google Chrome
chrome.exe	0.01	125,128 K	130,524 K	4292	Google Chrome
chrome.exe		27,768 K	27,072 K	4404	Google Chrome
chrome.exe					
chrome.exe					
chrome.exe					
chrome.exe					
chrome.exe					
chrome.exe					
RtDCpl64.exe		4,556 K	8,908 K	3460	HD Audio Control Panel
SkyDrive.exe	0.08	18,976 K	35,268 K	2984	Microsoft OneDrive
AlertusDesktopAlert.exe	0.01	38,476 K	26,664 K	4164	Alertus Desktop Alert

Command Line:
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -type=gpu-process -channel="1256.0.1577246536\145707064" -disable-d3d11 -supports-dual-gpus=false -gpu-driver-bug-workarounds=1,6,18,39 -gpu-vendor-id=0x1002 -gpu-device-id=0x6779 -gpu-driver-vendor="ATI Technologies Inc." -gpu-driver-version=8.783.2.2000 -ignored=" " -type=renderer " /prefetch:822062411

Path:
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

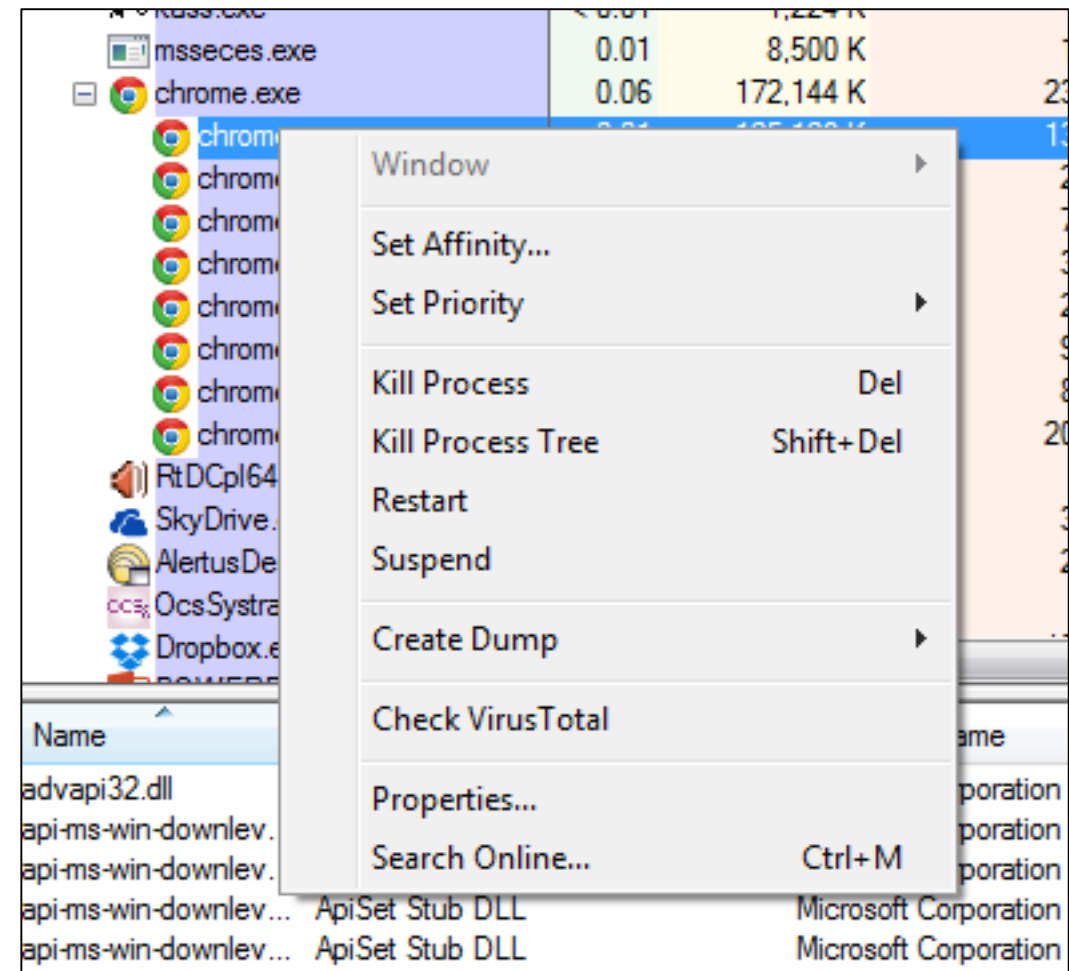
Process Explorer

Process Actions

Right-click on a process

Pop-up window with collection of actions displays

Can also select the process and click on the Process menu

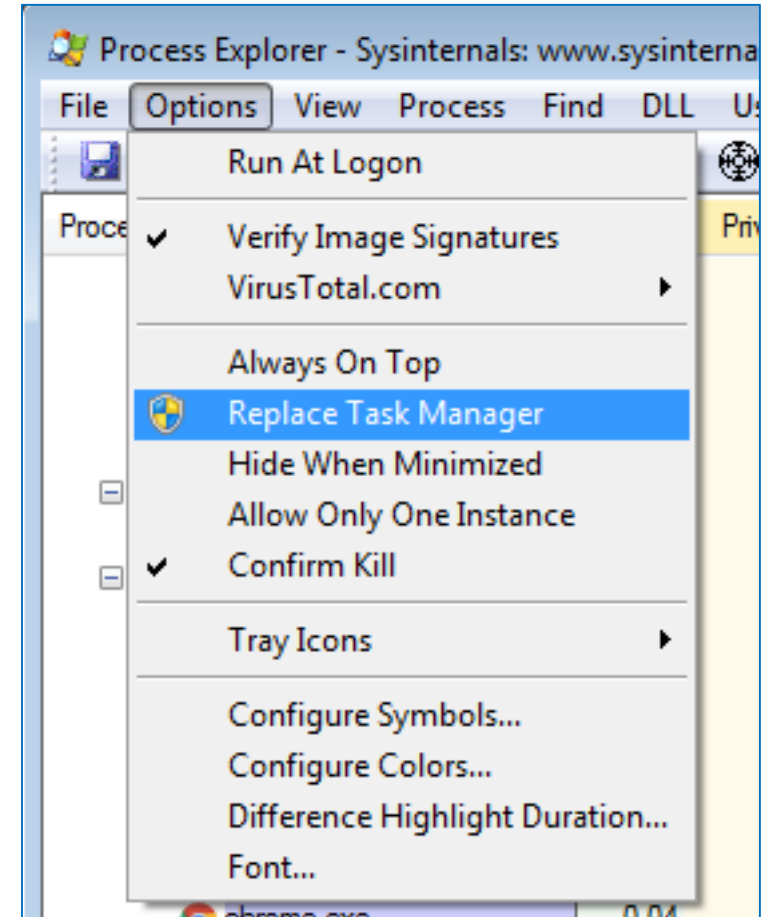


East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Process Explorer

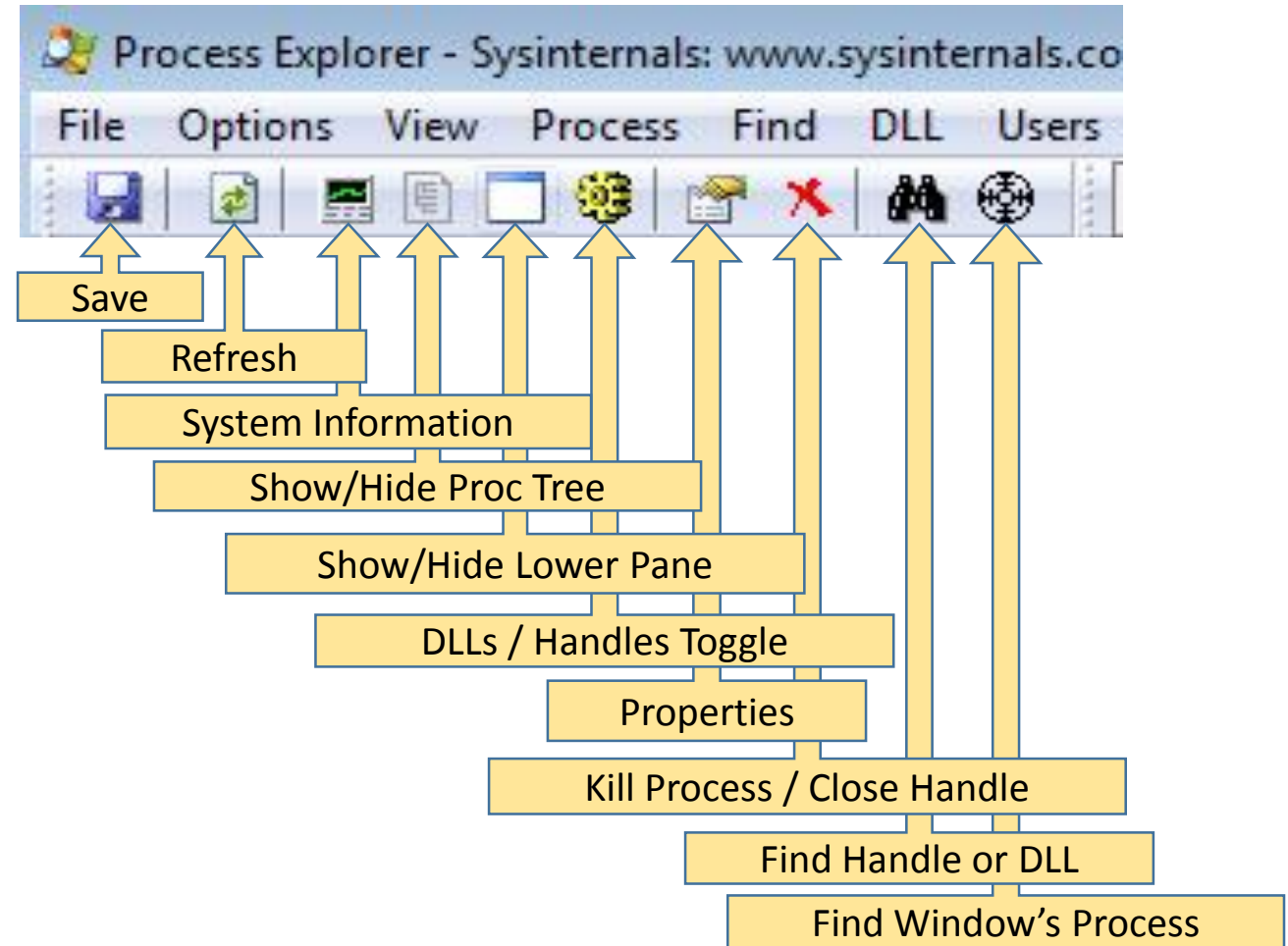
Replace Task Manager

Options->Replace Task Manager



Process Explorer

Toolbar Buttons



Other Sysinternals Tools Related to Processes

Process Monitor

PsTools

VMMMap

ProcDump

TCPView

RAMMap

(We may explore some or all of these as we move through the semester. I hope.)



For Lab (2/9/2016)

Read <http://www.howtogeek.com/school/sysinternals-pro/lesson2/>
(The first page, at least)



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Next Class (2/11/2015)

Microsoft Active Directory

(if we have time) Linux management via web console



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Questions?



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Copyrights



Presentation prepared by and copyright of John Ramsey,
East Tennessee State University, Department of
Computing . (ramseyjw@etsu.edu)



- Microsoft, Windows, Excel, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.
- IBM, DB2, DB2 Universal Database, System i, System i5, System p, System p5, System x, System z, System z10, System z9, z10, z9, iSeries, pSeries, xSeries, zSeries, eServer, z/VM, z/OS, i5/OS, S/390, OS/390, OS/400, AS/400, S/390 Parallel Enterprise Server, PowerVM, Power Architecture, POWER6+, POWER6, POWER5+, POWER5, POWER, OpenPower, PowerPC, BatchPipes, BladeCenter, System Storage, GPFS, HACMP, RETAIN, DB2 Connect, RACF, Redbooks, OS/2, Parallel Sysplex, MVS/ESA, AIX, Intelligent Miner, WebSphere, Netfinity, Tivoli and Informix are trademarks or registered trademarks of IBM Corporation.
- Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.
- Oracle is a registered trademark of Oracle Corporation.
- HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.
- Java is a registered trademark of Sun Microsystems, Inc.
- JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.
- SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.
- Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects S.A. in the United States and in other countries. Business Objects is an SAP company.
- ERPsims is a registered copyright of ERPsims Labs, HEC Montreal.
- Other products mentioned in this presentation are trademarks of their respective owners.



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer