# Global Information Assurance Certification Paper


# Global Information Assurance Certification Paper

# Task Manager Forensics

*GIAC GCFA Gold Certification*

Author: Larisa April Long, lapril@dc.rr.com
Advisor: Egan Hadsell

Abstract

Have you ever opened Task Manager and been mystified by a bizarrely named Windows process such as toaster, fuel service or seaport? Whether pursuing a forensic investigation or troubleshooting, Task Manager is the perfect tool to display information about Windows files. There are several alternatives to Task Manager, but few computer users take advantage of the simple yet powerful tool already installed on every Windows OS.

# 1. Introduction

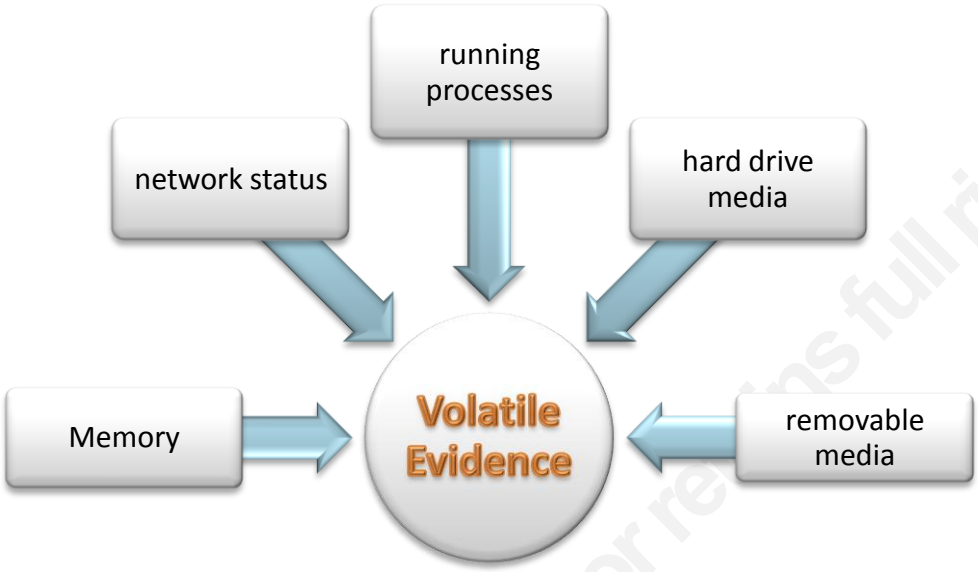
When a system has been compromised, forensic analysts have to be part researcher and part investigator. They must be able to parse out known or healthy files to eliminate them as possible clues. Like the old saying goes: know what you don't know, but know where to find the answers.

There are several definitions of a digital forensic investigation. Brian Carrier describes a digital investigation "where we develop and test hypotheses that answer questions about digital events" (Carrier, 2005). He believes the inclusion of the word forensic automatically implies a court of law (Carrier, 2005). Whether or not a court of law will be the ultimate goal, volatile evidence is crucial in any digital investigation. "Evidence is the core of what an investigator is going to seek. Evidence is anything that can be used to prove or disprove a fact" (Lee, 2010).

There are two main investigations in forensic analysis: live and dead. "Dead" forensics or traditional forensics entails examining powered down systems, creating bit copies of hard drives, constructing timelines and performing file system analysis. This traditional forensic path is the most common forensics investigation used for criminal cases that must be proven in court.

A live investigation is "often used in incident handling to determine if an event has occurred" and "may or may not proceed a full traditional forensic analysis" (McDougal, 2006). An investigation might have to be attempted on a live, or active, machine if it cannot be disconnected or powered down due to business or production purposes. There are also problems with active machines: "the process of proving a live image that's forensically sound and unaltered is more complex than with dead system images. Running systems write to memory many times each second" (Vacca & Rudolph, 2011).

Larisa April Long, lapril@dc.rr.com



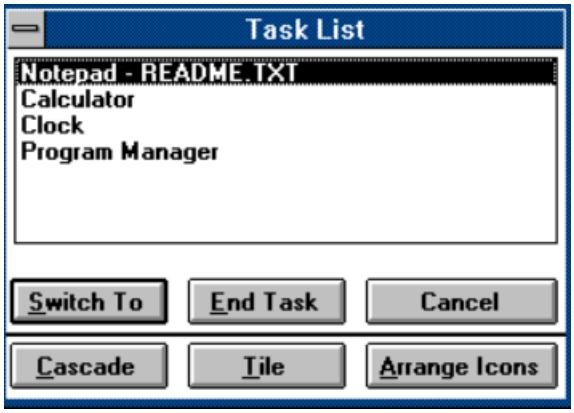

Volatile evidence, or evidence that will be lost when the computer is powered down, is essential to every investigation. Evidence in memory, network connections and running processes are the most volatile of evidence and must be collected first (Lee, 2010).

"An investigator will always want to know what processes are running on a potentially compromised system. Note the word always" (Carvey, 2009). Turn on a Windows computer, and dozens of processes are automatically opened. Many of the programs are core files needed to operate the OS, and some are user initiated. A list of open processes will help create a timeline of events by detailing what programs were open prior to, during and after an incident.

There are plenty of forensic tools included in Helix that will gather a list of running processes, but a quick and dirty solution is the Task Manager. It is already installed on every Windows computer and experts and novices alike can use Task Manager to get a quick snapshot of potential problems.

"In the early days of Windows, the Task Manager was more important than it is now. That's because those early versions of Windows lacked a Taskbar" (Gookin, 2007). Early versions of Task Manager, like the image shown below in a computer running Windows 3.0, were necessary to list programs and choose between them (Sinofsky, 2011).

Larisa April Long, lapril@dc.rr.com



(Sinofsky, 2011)

Windows 7 Task Manager obviously provides more information than just a way to switch between programs. Even with advances, however, Task Manager tends to denigrated by advanced computer users who opt for installing replacement software. Process Hacker, Anvir Task Manager, Process Explorer, System Explorer, or What's Running 3.0. are some of the examples of Task Manager alternatives (Williams, 2010; Lifehacker, 2009).

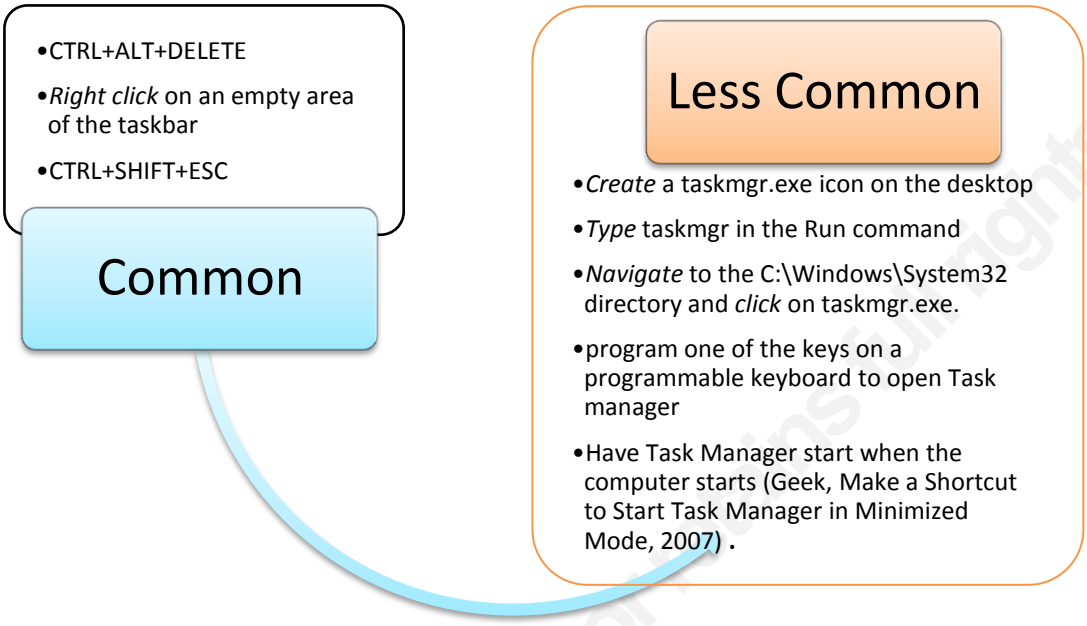
Even though Windows 7 Task Manager has evolved, Microsoft found that up to 85% used only the Applications and Processes Tabs (Sinofsky, 2011) . This, in essence, means Task Manager's sole purpose is closing an unresponsive program (Albanesius, 2011; Paul, 2011).

(Sinofsky, 2011)

## 2. Task Manager

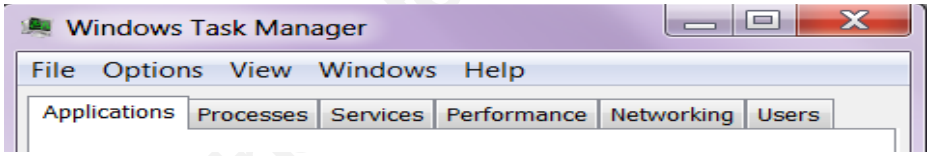
How do you open Task Manager? Like the majority of computer tasks, there are many different ways to achieve the same result:

Larisa April Long, lapril@dc.rr.com



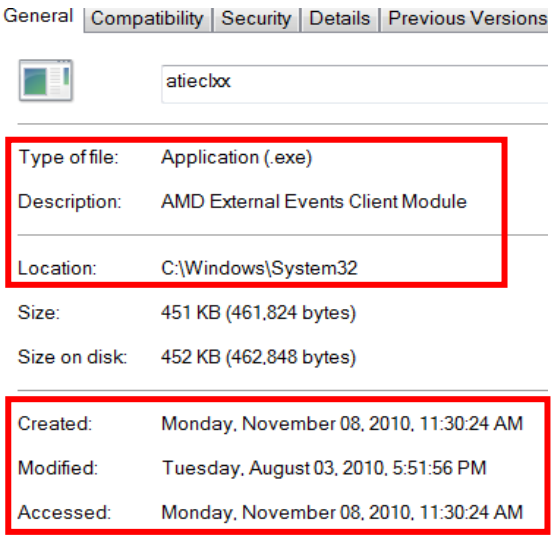

## 2.1 Task Manager Deconstructed

Once Task Manager is opened, there are six tabs.




The first tab, **Applications,** will list the name of each task plus their status, and the second tab, **Processes,** will list open processes. Right clicking on any process will provide choices such as ending a process, opening the specific file location or checking on properties. The properties option provides information such as the name, type, location and description of a file as well as the date when the file was created, modified and accessed.

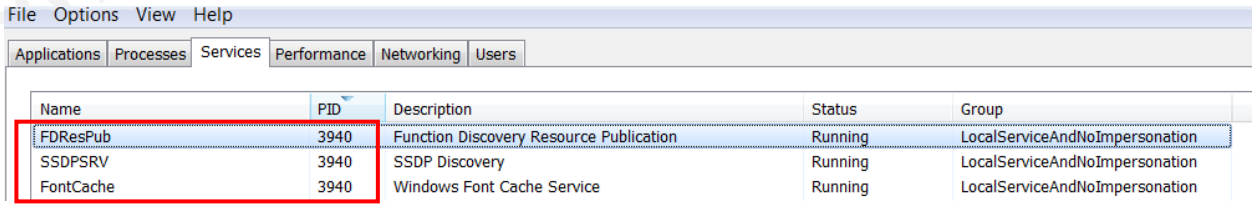
Larisa April Long, lapril@dc.rr.com



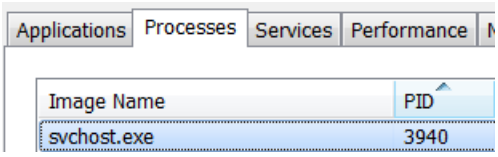

The third tab, **Services**, details the names of the services as well as the Process Identifier (PID), description, status and group. "A service is a specialized program that performs a function to support other programs" (Bott, Siechert, & Stinson, 2007). Right clicking on any service will allow users to start, stop or go to process, and clicking the Services button will open the Microsoft Management Console (MMC).

The Processes and Services tab can be used together to link running processes with the particular service they are using. While in the Processes tab, right clicking on any process will open a dialog box that will allow users to 'Go to Service.' In the Services tab, right clicking on a service will open a choice to 'Go to Process.' Doing this allows users to determine which process opens up which service and vice versa.

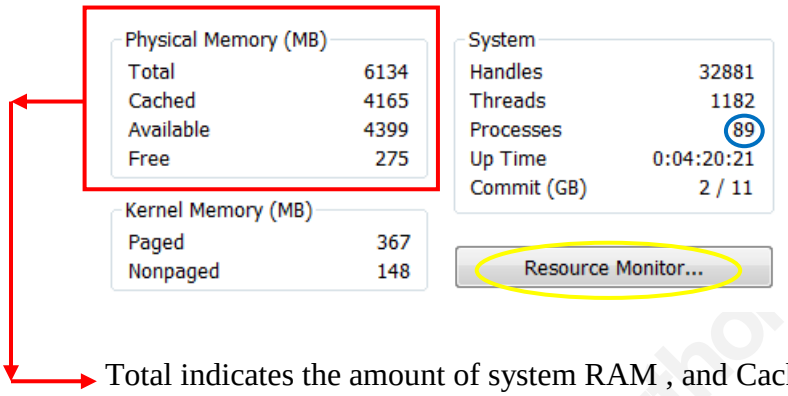
Each field in the Services and Processes tab can be sorted, and sorting the PID in both can provide a good view as to what process is using which services.




Larisa April Long, lapril@dc.rr.com




The forth tab, **Performance,** provides a quick snapshot as to the relationship between RAM and processes:



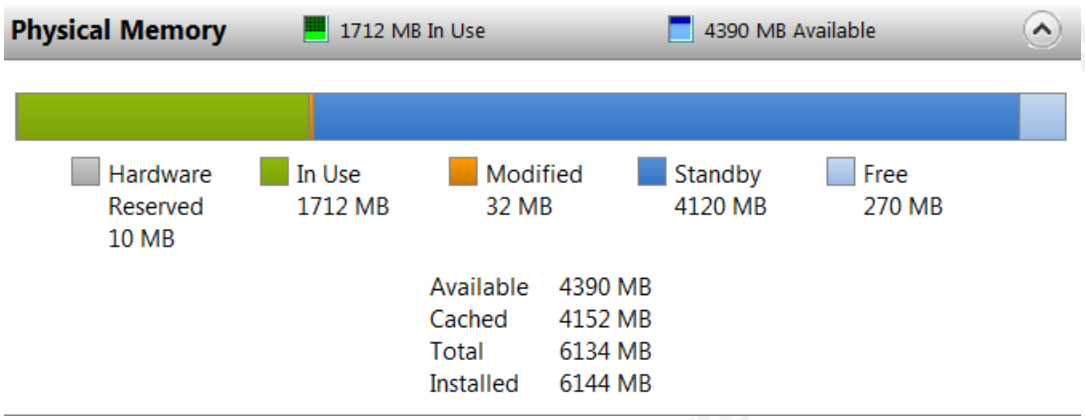

Total indicates the amount of system RAM , and Cached lists the RAM recently used. "This memory will remain in the cache in case the system resources are needed again, but it's available should other operations need it" (Shultz, 2010). The RAM not being used (Available) is listed as well as how much RAM is being cached that does not hold necessary information (Free).

The number of Processes are listed as well as Handles and Threads. The amount of time from the last computer restart (Up Time) and the usage of Page files – both the amount being used and the amount available for use (Commit) – give a clear picture of memory usage. "The page file is used by Windows to hold temporary data which is swapped in and out of physical memory in order to provide a larger virtual memory set" (Hameed, 2007).

For an even more in-depth view of the relationship between memory and open processes, clicking on the Resource Monitor button will monitor "resource usage in real time" (Microsoft, 2009).

Once in the Resource Monitor, there are tabs that will give a more visual representation of TCP connections and listening ports. It will show the processes that have network or disk activity, handles and modules. "Handles are pointers that refer to system elements including (but not limited to) files, registry keys, events, or directories. Modules are helper files or programs

including (but not limited to) dynamic-link library (DLL) files" (Microsoft, 2011d). Below, is a graphic of the physical memory in Resource Monitor:

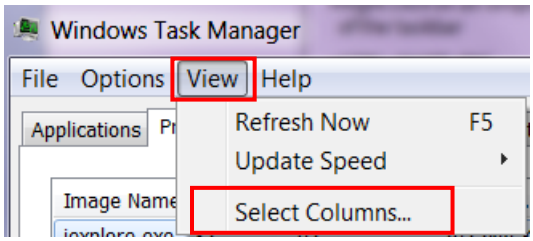



The fifth tab, **Networking,** displays active network connections and a graphical representation of the number of bytes sent and received. Suspicious activity can be seen in high bandwidth or usage on a network adapter that should not be currently in use.

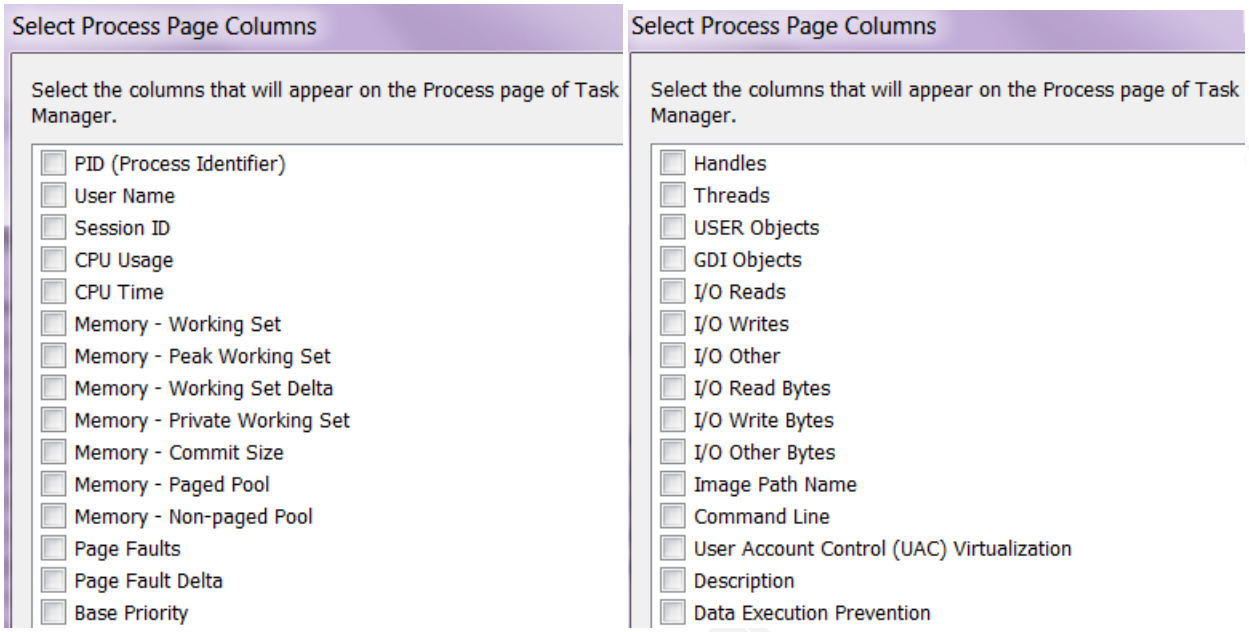
Finally, the sixth tab, **Users,** will provide information about the name and number of users logged on. At the bottom of the screen, there are buttons for disconnecting, logging off and sending another user a message.

### 2.1.1 Task Manager Columns In Processes Tab

It is important to use Task Manager to the fullest. The information under the Applications, Services and Performance tabs cannot be changed, but different columns can be added to expand the information available in the Processes, Networking and Users tabs. While in the Processes Tab, clicking on the View menu and clicking on Select Columns can expand the information available for each process.




Larisa April Long, lapril@dc.rr.com




Thirty different columns can be chosen (Microsoft, 2011b).

**PID (Process Identifier)**: the number that identifies a process. "The operating system accesses all processes by their numbers, not their names" (Boyce, 2009).
**User Name**: the user account the process is running under
**Session ID**: the number that identifies the user. Each user will have their own ID if there are multiple users logged on. According Jim Boyce, the number will be zero unless Terminal Services are used (Boyce, 2009).
**CPU Usage**: the % of CPU that a process is using

While the CPU usage time is normally a good indicator of what percentage of a processor is being used, there is an exception. The system idle process should have an extremely high number. Normally, a high number in CPU usage would indicate how much of the CPU is being used for the process. A high number in System Idle Process indicates how much of the CPU is actually available. For instance, if the System Idle Process is at 99. That means 99% of the CPU is available. "The computer should perform better when the System Idle process has a higher percentage, because the System Idle process stores remaining resources. Lower amounts means the system is being taxed at a greater rate" (Mikael, 2011).

**CPU Time**: time used by process (measured in seconds)
**Memory – Working Set**: the amount of memory the process is using

**Memory – Peak Working Set**: largest amount of memory the process has used
**Memory – Working Set Delta**: amount of change in the working set memory
**Memory – Private Working Set**: amount of memory a process is using that cannot be shared
**Memory – Commit Size**: amount of virtual memory a process has reserved
**Memory – Paged Pool**: amount of virtual memory that can be written to another medium (like a hard disk) for storage
**Memory** – **Non-Paged Pool**: amount of virtual memory that cannot be written to another medium
**Page Faults**: number of times data has to be disk retrieved because it was not in memory
**Page Fault Data**: change in number of page faults since the last update
**Base Priority**: a ranking of the order the process threads are scheduled
**Handles**: number of object handles
**Threads**: number of threads in process
**USER Objects**: number of user objects being used. "A USER object is an object from Window Manager, which includes windows, menus, cursors, icons, hooks, accelerators, monitors, keyboard layouts, and other internal objects" (Microsoft, 2011e).
**GDI Objects**: the number of objects from the GDI (Graphics Device Interface) library
**I/O Reads**: the number of read input/output operations ordered by process
**I/O Writes**: the number of write input/output operations ordered by process
**I/O Other**: the number of input/output operations that are not read or write
**I/O Read Bytes**: number of bytes read in input/output operations
**I/O Write Bytes**: number of bytes written in input/output operations
**I/O Other Bytes**: number of bytes transferred in input/output operations that are not read or write
**Image Path Name**: the exact directory where file is located
**Command Line**: the command used to launch the process
**User Account Control (UAC) Virtualization**: identifies if UAC is used, disabled or not allowed for process
**Description**: will list, usually brief, an explanation of the process
**Data Execution Prevention:** identifies whether data execution prevention, a Windows security feature that tries to prevent data from being executed, is enabled or disabled

At the very least, CPU Usage, Image Path Name, Command Line and the Description fields should be checked. Memory – Working Set and Memory - Peak Working Set can be checked in order to compare any difference between the memory the process is currently using versus the most it has ever used. A vast difference between past and present usage amounts could help with a timeline.

Larisa April Long, lapril@dc.rr.com

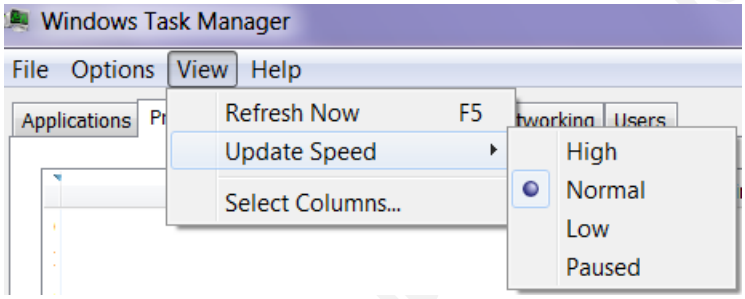
Once the columns are chosen, use the double arrow resize cursor to increase the size of the final columns to ensure the entire information field can be seen. The column width can go from this:

| | | | | | | |
|---|---|---|---|---|---|---|
| SetPoi... | 00 | 0... | 9,5... | C:\Program Files\L... | "C:\Program Files\Lo... | Log |

…to this:

| | | | | | |
|---|---|---|---|---|---|
| SetPoint.exe | 00 | 0:00:01 | 9,544 K | C:\Program Files\Logitech\SetPoint\SetPoint.exe | "C:\Program Files\Logitech\SetPoint\SetPoint.exe" |

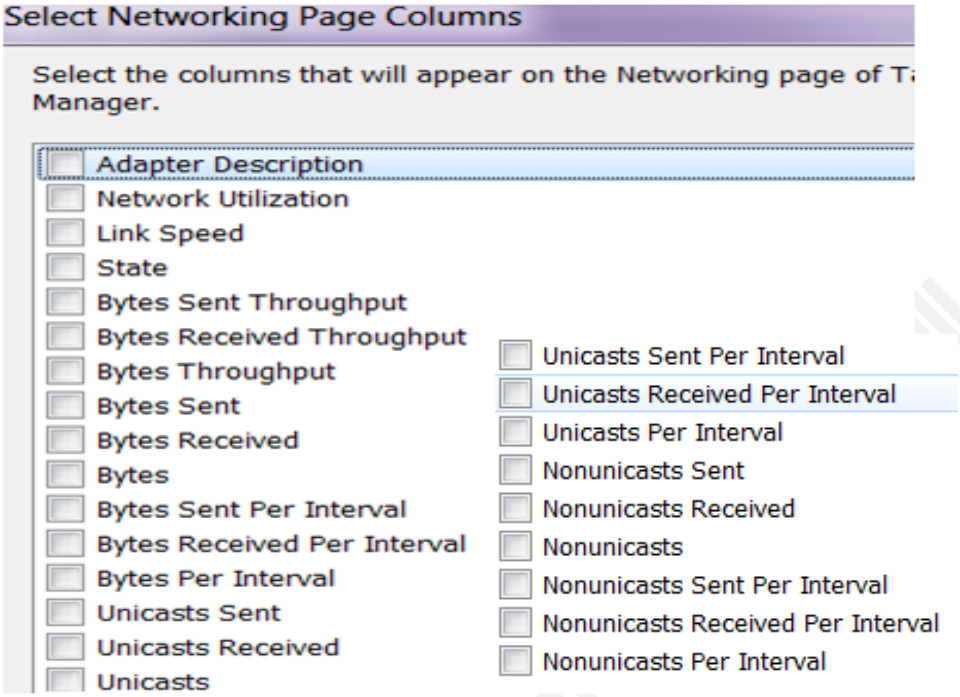
Also, in the View Menu, there is an option for setting the speed at which Task Manager updates.




High refreshes Task Manager twice each second. Normal updates every two seconds. Low updates every four seconds, and paused will not allow Task Manager to update automatically (Boyce, 2009). Like the Refresh Now option, hitting F5 will update in Paused mode.

### 2.1.2 Task Manager Columns in Networking Tab

While in the Networking Tab, clicking on the View menu and clicking on Select Columns can expand the information available.




The twenty-five columns (Microsoft, 2011c) are described below:

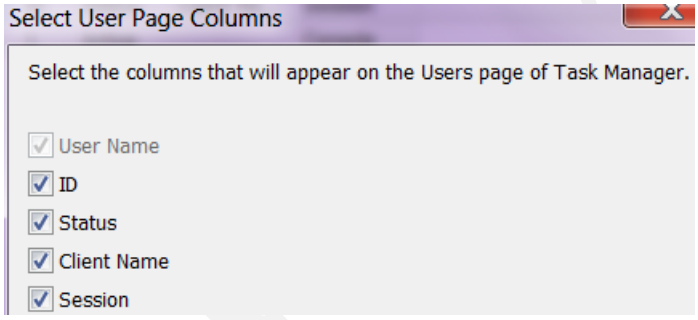
**Adapter Description**: Description of adapter; usually same name as given to device in network connections folder
**Network Utilization**: initial connection speed percentage of network utilization
**Link Speed**: initial speed of connection
**State**: the network connection would be connected or disconnected
**Bytes Sent Throughput**: connection bandwidth used (in percentage) by traffic sent
**Bytes Received Throughput**: connection bandwidth used (in percentage) by traffic received
**Bytes Throughput**: connection bandwidth percentage used by both sending and receiving traffic
**Bytes Sent**: total bytes sent
**Bytes Received**: total bytes received
**Bytes**: combination of sent and received bytes
**Bytes Sent Per Interval**: total number of bytes sent in interval
**Bytes Received Per Interval**: total number of bytes received in interval
**Bytes Per Interval**: total number of sending and receiving bytes
**Unicasts Sent**: number of bytes requested to unicast addresses (will include packets that were not sent or otherwise discarded) "Unicast is a one-to one connection between the client and the server. Unicast uses IP delivery methods such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), which are session-based protocols" (Microsoft, 2003).
**Unicasts Received**: number of bytes received from unicast addresses
**Unicasts**: total number of sending and receiving bytes

Larisa April Long, lapril@dc.rr.com

**Unicasts Sent Per Interval**: total number of bytes sent to subnet unicast addresses
**Unicasts Received Per Interval**: total number of bytes received from subnet unicast addresses
**Unicasts Per Interval**: total number of sending and receiving unicast packets
**Nonunicasts Sent**: total number of bytes sent to nonsubnet unicast addresses
**Nonunicasts Received**: total number of bytes received from non subnet unicast addresses
**Nonunicasts**: total number of sending and receiving non unicast packets
**Nonunicasts Sent Per Interval**: total number of bytes sent to non subnet unicast addresses
**Nonunicasts Received Per Interval**: total number of bytes received from non subnet unicast addresses
**Nonunicasts Per Interval**: total number of sending and receiving non unicast packets

Clicking on network utilization, link speed, state as well as bytes sent, bytes received and bytes can provide a good explanation to how the network is processing information. Clicking on each of the columns can help create a timeline of network events as the Options menu can be reset or show cumulative data to get a better view of what happened previously.

### 2.1.3 Task Manager Columns in User's Tab




**User Name**: the name of the user logged onto system
**ID**: the numeric ID identifier
**Status**: the status of the connection; active or disconnected
**Client Name**: name of the client computer; sometimes left blank if not applicable
**Session**: session name of computer

## 2.2 Down and Dirty with Windows Directories

When a process is opened either by a user or by the computer, it will be listed in the Task Manager, and the original file can be located in one of the core windows directories.

Windows files are confusing. There's no other way around it. It takes tens of thousands of files for Windows to run properly, and that's only counting core files and not user initiated software installations.

### 2.2.1. Core directories of C:\Program Files, C:\Program Files(x86) and C:\ProgramData

Many forensic types love Linux based systems because of their user friendly simplicity, and most forensic tools are Linux based. However, the majority of computer users still use Windows OS: it is essential to understand core Windows directories.

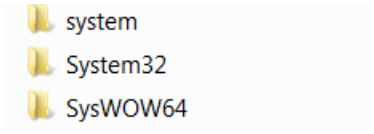

C:\Program Files is a folder that keeps 64 bit program files. 32 bit and 64 bit refers to how the computer's processor manages information. Processes that can manage 64 bits means they have access to more RAM and process information much faster than a 32 bit computer (Microsoft, 2011a).

C:\Program Files (x86) is a folder for 32 bit program files compatible with older x86 processors. The (x86) of the C:\Program Files (x86) refers to the name of a 32 bit process architecture whose other process names include 8086 and 80186.

In other words, all 64-bit applications must be installed in the c:\Program Files directory, and all 32-bit applications must be installed in the c:\Program Files (x86) directory.

The C:\ProgramData folder holds application data, including user and program settings, for installed processes.

### 2.2.2. C:\Windows directories of system, System32 and SysWOW64




C:\windows\system includes backward compatibility files. Windows likes to make things more interesting by having core OS files for 64 bit systems inside the System 32 directory and 32 bit files included under the c:\Windows\sysWOW64 directory.

WOW64 means windows on windows 64 bit which allows 32 bit applications to run in 64 bit OS. According to Microsoft, WOW64 provides Windows 32-bit On Windows 64-bit by using a layer that allows 32 bit applications to run on the more advanced 64 bit OS. "At a high level, WOW64 is a collection of user-mode DLLs that intercepts calls to and from 32-bit processes and translates them" (Microsoft, 2010).

## 3. What's In a Name?

"Many investigators and even system administrators are not familiar enough with Windows systems to recognize default or 'normal' processes at a glance" (Carvey, 2009). This is where knowledge of core Windows files is a necessity.

Computer professionals have borrowed their fair share of originally non-computer terms like virus, worm, and Trojan to describe the nastiest bytes. What does etymology have to do with it? Even though windows files can be confusing, there are clues.

| within name | Most Likely Description | Examples |
|---|---|---|
| **ati** | most likely – ATI technologies dealing with ATI Radeon family of video graphics; also likely: advanced micro devices (AMD) desktop component | atieclxx.exe<br>atiesrxx.exe |
| **bing** | Microsoft Bing Bar related | bingapp.exe<br>bingbar.exe |
| **cn** | Canon printer related | CNMSUT.exe |
| **explore** | Microsoft Windows application | explorer.exe |

| | | |
|---|---|---|
| | | iexplore.exe |
| **firefox** | Mozilla Firefox Browser | firefox.exe |
| **host** | provides a host function | WUDFHost.exe<br>taskhost.exe<br>svchost.exe |
| **mc** | McAfee | mcsacore.exe |
| **msi** | Microsoft installer (MSI) package files | msiexec.exe |
| **ra** | Realtek Audio | RAVCpl64.exe |
| **rundll** | runs dynamic link library (dll) files | rundll.exe |
| **search** | Search function | SearchIndexer.exe<br>searchprotocolhost.exe |
| **services** | Services function | services.exe<br>SftService.exe |
| **shwicon** | show icon | shwiconXP9106.exe |
| **spl**<br>**spool** | spooler, spool | spoolsv.exe<br>splwow64.exe |
| **svc** | service | vssvc.exe<br>armsvc.exe<br>ccSvcHst.exe<br>svchost.exe<br>FusionSVC.exe |
| **system** | system core file | System<br>System Idle Process |
| **task** | task | taskeng.exe<br>taskhost.exe<br>taskmgr.exe |
| **updchk**<br>**usched** | update check<br>update schedule | dpupdchk.exe<br>jusched.exe |
| **vm** | VMWare | vmnat.exe<br>VMware-authd.exe<br>vmware-usarbitrator.exe<br>vmnetdhcp.exe |
| **win** | windows | wininit.exe<br>winlogon.exe<br>winmsgballoon<br>WINWORD.EXE |
| **wmp** | windows media player | wmpnetwk.exe |

Larisa April Long, lapril@dc.rr.com

## 3.1 Acronyms

| Acronyms | Descriptions | Examples |
|---|---|---|
| **ccc** | Catalyst Control Centre | CCC.exe |
| **csrss** | Microsoft Client Server Runtime Server Subsystem | csrss.exe |
| **dwm** | Desktop Windows Manager | dwm.exe |
| **lsass** | Local Security Authority Process | lsass.exe |
| **lsm** | Local Session Manager | lsm.exe |
| **smss** | Session Manager Subsystem | smss.exe |
| **wmi** | Windows Management Instrumentation | WmiPrvSe.exe |

### 3.1.1 Reveal Nothing

Some files prefer to use names that give nothing away. Seaport and fuel service do not indicate anything of what they are unless they have something to do with a fueling depot at an airport. Runkbot sounds like the latest run amok robot. Files with names like q, b, xad and raccoom could be spy names. The bizarrely named files are actually (System Explorer, 2011):

| file name | Description |
|---|---|
| **b.exe** | Boxer software text editor |
| **fuel.service.exe** | part of AMD/ATI graphics cards |
| **q.exe** | System Internals rootkit revealer |
| **raccoom** | Raccoom company tree view folder browser |
| **runkbot.exe** | Dell executable |
| **seaport.exe** | Microsoft windows live seaport search enhancement pack; used when performing searches |
| **Toaster.exe** | Dell DataSafe Local Backup; SoftThinks |
| **xad.exe** | Microsoft console based script host |

## 3.2 Multiple Instances & (*32) after Process Name

There are several files that will open multiple times in Task Manager such as conhost.exe, csrss.exe, rundll.exe and svchost.exe. Most of the multiple instances files will be located in the windows\system32 or windows\sysWOW64 directories (Geek, What is conhost.exe and Why Is It Running?, 2009). Usually, the multiple instances are harmless

because each one is performing a different task. Since malware can be hidden in processes, it is important to be aware of each purpose.

Sometimes processes appear with *32 after the process name. This just means it's a 32-bit process running on a 64-bit OS.

## 4. Task Manager's Drawback: Suspect Everything

When forensic analysts need to quickly verify that an incident has taken place and acquire evidence, tediously parsing through unknown windows files can slow down an investigation. Several questions can arise: How do you know what is legitimate and what isn't supposed to be there? Is there a way to determine from the file name itself what the file is?

Use Task Manager to get the basics of running processes. If you can't open a process or file locations by right clicking in Windows Task Manager, be sure to click 'show processes from all users'.

If there is a question about a process, it is important to locate the file and research whether the file is legitimate or not. The main drawback to Task Manager: "When a program is running, there is no way in the Task Manager to really distinguish it from the legitimate version…" (Carvey, 2009).

While Task Manager will list the detailed information, how can you tell if a file has been corrupted by malware? Suspect "any file which uses system filename and is not stored in system directory or has invalid file version information. Correct system file contains full file version information from Microsoft" (System Explorer, 2011).

The first step is to use Task Manager to determine what can be learned initially such as complete file name, location and size of file. Next, research the file itself. Some may just use a search engine, like Google, to research a file name, but it is important to verify with reputable sources. Anyone can look up confusing file names with specialized websites like:

http://www.processlibrary.com

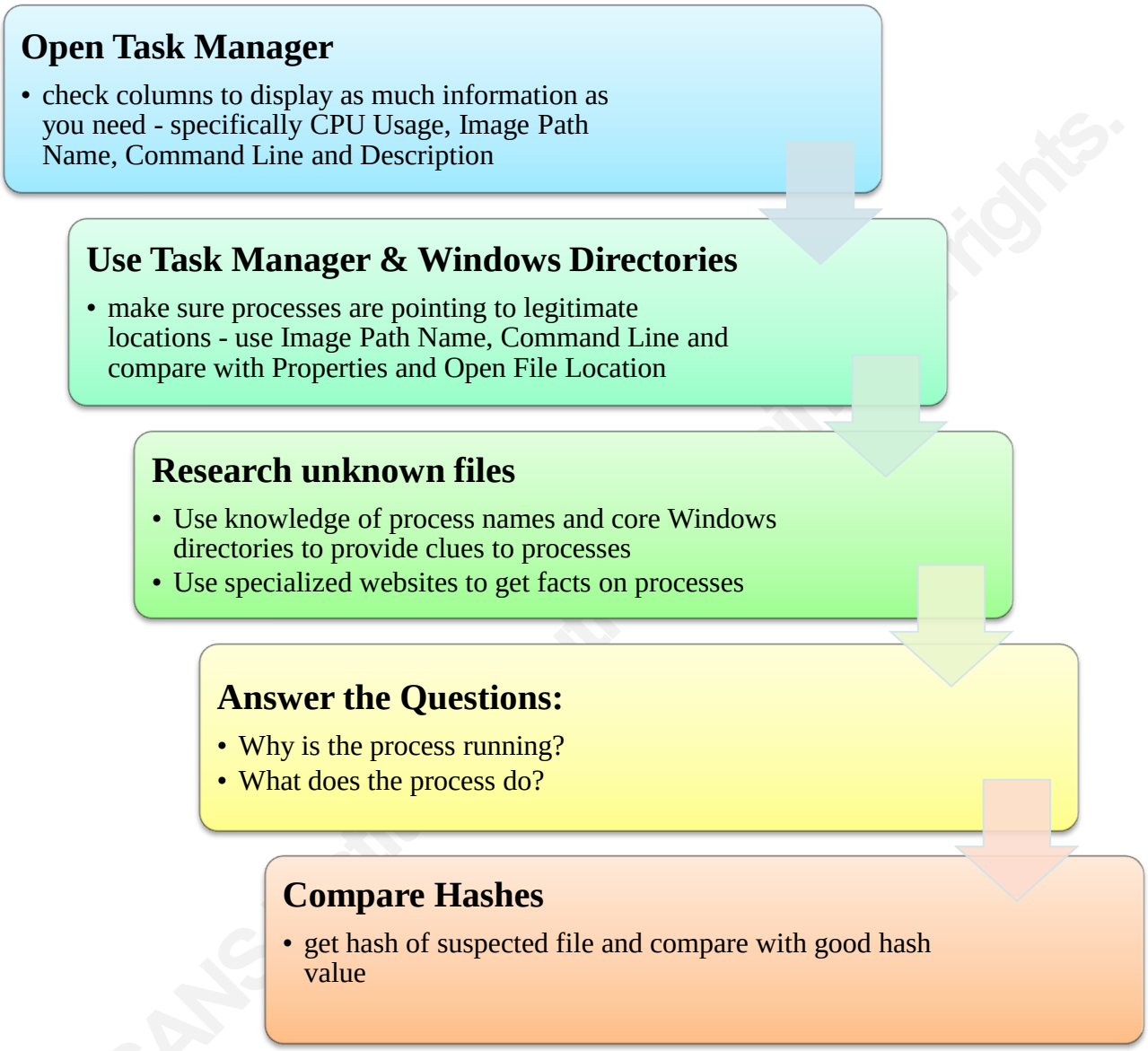
http://systemexplorer.net/filedb.php
http://support.microsoft.com/
http://www.systemlookup.com/
http://www.howtogeek.com
http://www.what-is-exe.com/
http://www.file.net/process/

If a file is still suspected, check the hash files of the suspected file with the original. Download an MD5 or SHA program or use forensic tools such as Helix or Knoppix to compare checksums to good known hash values. Check hash files with sources such as System Explorer at http://systemexplorer.net/filedb.php, the Internet Storm Center at http://isc.sans.edu/tools/hashsearch.html or download them directly from the National Software Reference Library (NSRL) at http://www.nsrl.nist.gov/. Make sure the correct file and product version match the correct hash.

## 5. The Future of Windows Task Manager

In Windows 8, Microsoft has promised to improve on Task Manager (Paul, 2011) by automatically grouping processes according to user, windows and background. Also, it promises to decrypt windows names into more user friendly versions. Until Windows 8 becomes mainstream, there is a need to understand the conventional terms and names Microsoft uses in pre-Windows 8 computers.

## 6. Conclusion




Knowing the baseline of a computer is ideal before a suspected incident but not always possible. Whether troubleshooting a suspected process or pursuing a complex digital forensic investigation, understanding the basics of core windows files and directories is essential.

When in doubt of the validity of a file, use Task Manager to locate file specifics. Employ knowledge of the etymology of file names to narrow down the meaning of the file. Research unknown files, and validate the file by comparing hash values with reputable sources. By knowing a little more about the core windows processes and where they are located, users can determine why a process is open in Task Manager and troubleshoot.

Larisa April Long, lapril@dc.rr.com

Forensic analysts must take advantage of every tool at their disposal, and Task Manager's many uses go far beyond simply ending a process. Obviously Task Manager isn't the only tool in a digital investigation, but it can be the first line of defense and provides a good foundation for further analysis.

If the investigation includes a forensic examination of a live system, performing basic troubleshooting, or wanting to know more about the files running on a computer, Task Manager is one of the simplest programs to use that doesn't require an installation of another software program.

## 7. References

Albanesius, C. (2011, October 17). *Windows 8 Simplifies Task Manager for Easy App Killing.* Retrieved October 20, 2011, from PC Magazine: http://www.pcmag.com/article2/0,2817,2394773,00.asp#fbid=jPKaTrSQnKf

Bott, E., Siechert, C., & Stinson, C. (2007). *Windows Vista Inside Out.* Redmond: Microsoft Press.

Boyce, J. (2009). *Windows 7 Bible.* Indianapolis: Wiley.

Carrier, B. (2005). *File System Forensic Analysis.* Upper Saddle River: Pearson Educational.

Carvey, H. (2009). *Windows Forensic Analysis DVD Toolkit.* Burlington: Syngress.

Geek, T. (2007). *Make a Shortcut to Start Task Manager in Minimized Mode.* Retrieved October 20, 2011, from howtogeek: http://www.howtogeek.com/howto/windows-vista/make-a-shortcut-to-start-task-manager-in-minimized-mode/

Geek, T. (2009). *What is conhost.exe and Why Is It Running?* Retrieved November 3, 2011, from howtogeek: http://www.howtogeek.com/howto/4996/what-is-conhost.exe-and-why-is-it-running/

Gookin, D. (2007). *Find Gold In Windows Vista.* Indianapolis: Wiley.

Larisa April Long, lapril@dc.rr.com

Hameed, C. (2007). *What is the Page File for Anyway?* Retrieved November 13, 2011, from Microsoft Corporation: http://blogs.technet.com/b/askperf/archive/2007/12/14/what-is-the-page-file-for-anyway.aspx

Lee, R. (2010). Forensic and Investigative Essentials. In R. Lee, *Forensics 508 Advanced Computer Forensic Analysis and Incident Response.* The Sans Institute.

Lifehacker. (2009). *Five Best Windows Task Manager Alternatives.* Retrieved October 20, 2011, from Lifehacker: http://lifehacker.com/5378494/five-best-windows-task-manager-alternatives

McDougal, M. (2006). *Live Forensics on a Windows System: Using Windows Forensic Toolchest (WFT).* Retrieved November 29, 2011, from foolmoon: http://www.foolmoon.net/downloads/Live_Forensics_Using_WFT.pdf

Microsoft . (2010). *Best Practices for WOW64.*

Microsoft. (2011a). *32 bit and 64 bit Windows: frequently asked questions.* Retrieved November 13, 2011, from Microsoft Corporation: http://windows.microsoft.com/en-US/windows-vista/32-bit-and-64-bit-Windows-frequently-asked-questions

Microsoft. (2003, November 3). *Differences Between Multicast and Unicast.* Retrieved November 29, 2011, from Microsoft Corporation: http://support.microsoft.com/kb/291786

Microsoft. (2011b). *How to Use and Troubleshoot Issues with Windows Task Manager.* Retrieved October 20, 2011, from Microsoft Corporation: http://support.microsoft.com/kb/323527

Microsoft. (2011c). *Networking overview: Windows XP Professional Product Documentation.* Retrieved November 3, 2011, from Microsoft Corporation: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/taskman_networking_overview.mspx?mfr=true

Microsoft. (2011d). *Use Resource Monitor to View Handles and Modules.* Retrieved November 3, 2011, from Mircosoft Corporation: http://technet.microsoft.com/en-us/library/dd883276(WS.10).aspx

Microsoft. (2011e). *What do the Task Manager Memory Columns Mean?* Retrieved November 13, 2011, from Microsoft Corporation:

Larisa April Long, lapril@dc.rr.com

http://windows.microsoft.com/en-US/windows-vista/What-do-the-Task-Manager-memory-columns-mean

Microsoft. (2009). *What's new in Performance and Reliability Monitoring.* Retrieved October 20, 2011, from Microsoft Corporation: http://technet.microsoft.com/en-us/library/ee731897(WS.10).aspx

Microsoft. (2011). *Windows 7 Features: 64-bit Support.* Retrieved November 13, 2011g, from Microsoft Corporation: http://windows.microsoft.com/en-US/windows7/products/features/64-bit-support

Mikael, A. (2011). *Why Does My System Idle Process Take Up So Much Memory & Slow My Computer?* Retrieved November 3, 2011, from ehow: http://www.ehow.com/facts_7252301_system-much-memory-slow-computer_.html

Paul, I. (2011, October 14). *Meet the Windows 8 Task Manager.* Retrieved October 20, 2011, from PC World: http://www.pcworld.com/article/241932/meet_the_windows_8_task_manager.html

Shultz, G. (2010). *Reap the Benefits of Windows 7 Task Manager.* Retrieved November 3, 2011, from Tech Republic: http://www.techrepublic.com/blog/window-on-windows/reap-the-benefits-of-windows-7s-task-manager/2576

Sinofsky, S. (2011, October 13). *The Windows 8 Task Manager.* Retrieved October 20, 2011, from MSDN Blogs: http://blogs.msdn.com/b/b8/archive/2011/10/13/the-windows-8-task-manager.aspx

System Explorer. (2011). *What is the "svchost.exe?".* Retrieved October 20, 2011, from systemexplorer: http://systemexplorer.net/db/svchost.exe.html

Vacca, J., & Rudolph, K. (2011). *System Forensics, Investigation, and Response.* Sudbury: Jones & Bartlett Learning, LLC.

whatis.com. (2005). *process.* Retrieved November 3, 2011, from whatis.com: http://whatis.techtarget.com/definition/0,,sid9_gci212832,00.html

Williams, M. (2010). *5 Best Alternatives to the Windows Task Manager.* Retrieved October 20, 2011, from Techradar: http://www.techradar.com/news/software/applications/5-best-alternatives-to-the-windows-task-manager-665974

Larisa April Long, lapril@dc.rr.com

Last Updated: April 8th, 2014

# Upcoming Training


| | | | |
|---|---|---|---|
| SANS Security West 2014 | San Diego, CA | May 08, 2014 - May 17, 2014 | Live Event |
| SANS Malaysia @MCMC 2014 | Cyberjaya, Malaysia | May 12, 2014 - May 24, 2014 | Live Event |
| Digital Forensics & Incident Response Summit | Austin, TX | Jun 03, 2014 - Jun 10, 2014 | Live Event |
| SANSFIRE 2014 | Baltimore, MD | Jun 21, 2014 - Jun 30, 2014 | Live Event |
| SANS Canberra 2014 | Canberra, Australia | Jun 30, 2014 - Jul 12, 2014 | Live Event |
| SANS London Summer 2014 | London, United Kingdom | Jul 14, 2014 - Jul 21, 2014 | Live Event |
| SANS vLive - FOR508: Advanced Computer Forensic Analysis and Incident Response | FOR508 - 201407, | Jul 21, 2014 - Aug 27, 2014 | vLive |
| Mentor Session - FOR 508 | Saint Louis, MO | Aug 06, 2014 - Oct 08, 2014 | Mentor |
| SANS Virginia Beach 2014 | Virginia Beach, VA | Aug 18, 2014 - Aug 29, 2014 | Live Event |
| SANS Chicago 2014 | Chicago, IL | Aug 24, 2014 - Aug 29, 2014 | Live Event |
| SANS Bangalore 2014 | Bangalore, India | Sep 15, 2014 - Sep 27, 2014 | Live Event |
| SANS DFIR Prague 2014 | Prague, Czech Republic | Sep 29, 2014 - Oct 11, 2014 | Live Event |
| SOS: SANS October Singapore 2014 | Singapore, Singapore | Oct 07, 2014 - Oct 18, 2014 | Live Event |
| SANS vLive - FOR508: Advanced Computer Forensic Analysis and Incident Response | FOR508 - 201410, | Oct 14, 2014 - Nov 20, 2014 | vLive |
| Community SANS Paris @ HSC - FOR508 (in French) | Paris, France | Nov 03, 2014 - Nov 07, 2014 | Community SANS |
| SANS London 2014 | London, United Kingdom | Nov 15, 2014 - Nov 24, 2014 | Live Event |
| SANS OnDemand | Online | Anytime | Self Paced |
| SANS SelfStudy | Books & MP3s Only | Anytime | Self Paced |